User Plane Location Protocol

Approve Version 2.0.6 – 04 Aug 2020

Open Mobile Alliance

OMA-TS-ULP-V2_0_6-20200804-A

Contents

Figures

Tables

1. Scope

This document describes the UserPlane Location Protocol (ULP) for SUPL 2.0. ULP is a protocol-level instantiation of the Lup reference point described in [SUPLAD2]. The protocol is used between the SLP (SUPL Location Platform) and a SET (SUPL Enabled Terminal). For more details about SUPL Requirements refer to [SUPLRD2].

2. References

2.1 Normative References

[3GPP 11.11] 3GPP TS 11.11 "Specification of the Subscriber Identity Module –Mobile Equipment (SIM – ME) interface"
URL:http://www.3gpp.org/

[3GPP 23.003] 3GPP TS 23.003. "Numbering, addressing and identification",
URL:http://www.3GPP.org/

[3GPP 23.038] 3GPP TS 23.038, "Alphabets and language-specific information",
URL:http://www.3GPP.org/

[3GPP 23.167] 3GPP TS 23.167, "IP Multimedia Subsystem (IMS) emergency sessions",
URL:http://www.3GPP.org/

[3GPP 24.109] 3GPP TS 24.109, "Bootstrapping interface (Ub) and Network application function interface (Ua)",
URL:http://www.3gpp.org/

[3GPP 24.501] 3GPP TS 24.501, "Non-Access-Stratum (NAS) protocol for 5G System (5GS); Stage 3"
URL:http://www.3gpp.org/

[3GPP 25.225] 3GPP TS 25.225 "Physical Layer Measurements (TDD)"
URL:http://www.3gpp.org/

[3GPP 31.101] 3GPP TS 31.101, "UICC-terminal interface; Physical and logical characteristics"
URL:http://www.3gpp.org/

[3GPP 31.102] 3GPP TS 31.102, "Universal Subscriber Identity Module (USIM) application"
URL:http://www.3gpp.org/

[3GPP 33.220] 3GPP TS 33.220, "Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture"
URL:http://www.3gpp.org/

[3GPP 33.222] 3GPP TS 33.222, "Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)"
URL:http://www.3gpp.org/

[3GPP 36.213] 3GPP TS 36.213, " Evolved Universal Terrestrial Radio Access (E-UTRA); Physical layer procedures"
URL:http://www.3GPP.org/

[3GPP 36.321] 3GPP TS 36.321, " Evolved Universal Terrestrial Radio Access (E-UTRA) Medium Access Control (MAC) protocol specification"
URL:http://www.3GPP.org/

[3GPP 38.133] 3GPP TS 38.133, "NR; Requirements for support of radio resource management"
URL:http://www.3GPP.org/

[3GPP 38.213] 3GPP TS 38.213, "NR; Physical layer procedures for control"
URL:http://www.3GPP.org/

[3GPP 38.215] 3GPP TS 38.215, "NR; Physical layer measurements"
URL:http://www.3GPP.org/

[3GPP 38.413] 3GPP TS 38.413, "NG-RAN; NG Application Protocol (NGAP)"
URL:http://www.3GPP.org/

[3GPP 49.031] 3GPP TS 49.031 "Base Station System Application Part LCS Extension (BSSAP-LE)"
URL:http://www.3GPP.org/

[3GPP GAD] 3GPP TS 23.032, "Universal Geographical Area Description (GAD)", URL:http://www.3GPP.org

[3GPP LPP] 3GPP TS 37.355 "LTE Positioning Protocol (LPP)" URL:http://www.3gpp.org/

[3GPP LTE] 3GPP TS 36.331 "Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification" URL:http://www.3GPP.org/

[3GPP NR] 3GPP TS 38.331 "NR; Radio Resource Control (RRC) protocol specification", URL:http://www.3GPP.org/

[3GPP RRC] 3GPP TS 25.331, "Radio Resource Control (RRC) Protocol Specification", URL:http://www.3GPP.org/

[3GPP RRLP] 3GPP TS 44.031, "Location Services (LCS); Mobile Station (MS) – Serving Mobile Location Centre (SMLC) Radio Resource LCS Protocol (RRLP)", URL:http://www.3GPP.org/

[3GPP2 HRPD] 3GPP2 C.S0024-A Version 3.0, September 2006; cdma2000 High Rate Packet Data Air Interface Specification, URL:http://www.3GPP.org/

[3GPP2 S.S0109] 3GPP2 S.S0109-A, "Generic Bootstrapping Architecture (GBA) Framework, V1.0, February 2008, URL:http://www.3gpp2.org/

[3GPP2 S.S0114] 3GPP2 S.S0114-A, "Security Mechanisms using GBA", Version 1.0, February 2008, URL:http://www.3gpp2.org/

[3GPP2 UMB] 3GPP2 C.S0084-006 Version 2.0, August 2007, "Connection Control Plane for Ultra Mobile Broadband (UMB) Air Interface Specification", URL:http://www.3gpp2.org/

[3GPP2 X.S0049-0] 3GPP2 X.S0049-0, "All-IP Network Emergency Call Support ", Version 1.0, February 2008, URL:http://www.3gpp2.org/

[ASN.1] ITU-T Recommendation X.680: "Information technology – Abstract Syntax Notation One, (ASN.1): Specification of basic notation", URL:http://www.itu.int/ITU-T/

[HMAC] HMAC: Keyed-Hashing for Message Authentication, Krawczyk, H. et al, IETF RFC 2104, February 1997 URL:http://www.ietf.org

[IEEE 802.11] IEEE 802.11 URL:http://www.ieee.org

[IEEE 802.11v] "Wireless Network Management" Standard, IEEE 802.11v URL:http://www.ieee.org

NOTE: The reference IEEE draft is a work in progress.

[IEEE 802.16-2004] IEEE Std 802.16-2004, "IEEE Standard for Local and metropolitan area networks, Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems", IEEE, 01-Oct-2004 URL:http://www.ieee802.org/16/published.html

[IEEE 802.16e-2005] IEEE Std 802.16e-2005 and IEEE Std 80216-2004/Cor1-2005, "IEEE Standard for Local and metropolitan area networks, Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems, Amendment 2: Physical and Medium Access Control Layers for Combined Fixed and Mobile Operation in Licensed Bands, And Corrigendum 1", IEEE, 28-Feb-2006
URL:http://www.ieee802.org/16/published.html

[IOPPROC] "OMA Interoperability Policy and Process", Version 1.1, Open Mobile Alliance™, OMA-IOP-Process-V1_1,
URL:http://www.openmobilealliance.org/

[NWG 1.2.0 stage 2] "WiMAX Forum Network Architecture, Stage 2: Architecture Tenets, Reference Model and Reference Points", Release 1, Version 2.0, WiMAX Forum, 11-Jan-2008
URL:http://www.wimaxforum.org/technology/documents/

[NWG 1.2.0 stage3] "WiMAX Forum Network Architecture, Stage 3: Detailed Protocols and Procedures", Release 1 Version 2.0, WiMAX Forum, 11-Jan-2008
URL:http://www.wimaxforum.org/technology/documents/

[OMA PUSH] OMA WAP-251-PushMessage-20010322-a, "Push Message", Open Mobile Alliance™.
URL:http://www.openmobilealliance.org/

[OMA-DM] "OMA Device Management Enabler Release ", Version 1.2, Open Mobile Alliance™,
URL:http://www.openmobilealliance.org/

[OMA-LPPe] "LPP Extension Specification", Open Mobile Alliance™,
URL:http://www.openmobilealliance.org/

[OMAOPS] "OMA Organization and Process", Version 1.6, Open Mobile Alliance™,
URL:http://www.openmobilealliance.org/

[OMNA] http://www.openmobilealliance.org/Tech/OMNA/

[PER] ITU-T Recommendation X.691: "Information technology – ASN.1 encoding rules: Specification of Packed Encoding Rules (PER)",
URL:http://www.itu.int/ITU-T/

[PROVCONT] "Provisioning Content", WAP Forum, WAP-183-ProvCont-20010724-a
URL:http://www.openmobilealliance.org/

[PSK-TLS] "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)", IETF RFC 4279, December 2005
URL:http://www.ietf.org/rfc/rfc4279.txt

[RFC 2119] "Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, March 1997,
URL:http://www.ietf.org/rfc/rfc2119.txt

[RFC 3546] "Transport Layer Security (TLS) Extensions", S. Blake-Wilson et al, June 2003,
URL:http://www.ietf.org/**rfc**/rfc3546.txt

[RFC 3825] "Dynamic Host Configuration Protocol Option for Coordinate-based Location Configuration Information", J. Polk, J. Schnizlein, M. Linsner, July 2004,
URL:http://www.ietf.org/rfc/rfc3825.txt

[RFC 4279] "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)", P. Eronen, H. Tschofenig, December 2005, URL:http://www.ietf.org/rfc/rfc4279.txt

[RFC 6655] " AES-CCM Cipher Suites for Transport Layer Security (TLS)", IETF RFC 6655, July 2012,
URL:http://www.ietf.org/rfc/rfc6655.txt

[SIP PUSH] "SIP_Push", Version 1.0, Open Mobile Alliance™. OMA-ERP_SIP_PUSH-V1_0,
URL:http://www.openmobilealliance.org/

[SUPL2 ILP TS] "Internal Location Protocol", Version 2.0, Open Mobile Alliance™, OMA-TS-ILP-V2_0, URL:http://www.openmobilealliance.org/

[SUPLAD1] "Secure User Plane Location Architecture", Version 1.0, Open Mobile Alliance™, OMA-AD-SUPL-V1_0, URL:http://www.openmobilealliance.org/

[SUPLAD2] "Secure User Plane Location Architecture", Version 2.0, Open Mobile Alliance™, OMA-AD-SUPL-V2_0, URL:http://www.openmobilealliance.org/

[SUPLRD2] "Secure User Plane Location Requirements", Version 2.0, Open Mobile Alliance™, OMA-RD-SUPL-V2_0, URL:http://www.openmobilealliance.org/

[TIA-41] 3GPP2 X.S0004-E v1.0, "Wireless Radiotelecommuncations Intersystem Operations", March 2004, URL:http://www.3gpp2.org/Public_html/specs/

[TIA-553] Mobile Station –Land Station Compatibility Specification (AMPS), September 1989 URL:http://www.tiaonline.org/standards/

[TIA-637] 3GPP2 C.S0015-B v1.0, "Short Message Service (SMS) For Wideband Spread Spectrum Systems – Release B" June 2004, URL:http://www.3gpp2.org/Public_html/specs/

[TIA-801] C.S0022, Position Determination Service for cdma2000 Spread Spectrum Systems URL:http://www.3gpp2.org/Public_html/specs/

[TLS] "The Transport Layer Security (TLS) Protocol Version 1.1", IETF RFC 4346, April 2006 URL:http://www.ietf.org/rfc/rfc4346.txt

[TLS 1.2] "The Transport Layer Security (TLS) Protocol Version 1.2", IETF RFC 5246, August 2008 URL:http://www.ietf.org/rfc/rfc5246.txt

[TLS-AES] "Advanced Encryption Standard (AES) Ciphersuites for Transport Layer Security (TLS)", IETF RFC 3268, June 2002 URL:http://www.ietf.org/rfc/rfc3268.txt

[WAP Cert] OMA WAP-211-WAPCert, "WAP Certificate profile Specification", Open Mobile Alliance™, URL:http://www.openmobilealliance.org/

[WAP PAP] OMA-WAP-TS-PAP-V2_2-20071002-C, "Push Access Protocol", Open Mobile Alliance™, URL:http://www.openmobilealliance.org/

[WAP POTAP] OMA-TS-PushOTA-V2_2-20071002-C, "Push Over The Air", Open Mobile Alliance™, URL:http://www.openmobilealliance.org/

[WAP PROVSC] OMA-WAP-ProvSC-V1_1-20040428-C, "WAP Provisioning Smart Card", Open Mobile Alliance™ URL:http://www.openmobilealliance.org/

[WAP TLS] OMA WAP-219-TLS, " WAP TLS Profile and Tunneling Specification", Open Mobile Alliance™ URL:http://www.openmobilealliance.org/

[WAP WDP] "WAP Wireless Datagram Protocol", Open Mobile Alliance™, URL:http://www.openmobilealliance.org//

[X.694] ITU-T Recommendation X.694: "Information technology – ASN.1 encoding rules: Mapping W3C XML schema definitions into ASN.1",
URL:http://www.itu.int/ITU-T/studygroups/com17/languages/X694.pdf

2.2 Informative References

[SUPL CP] "OMA SUPL Client Provisioning", Version 1.0, Open Mobile Alliance™, OMA-TS-SUPL-Client-Provisioning-V1_0,
URL:http://www.openmobilealliance.org/

[SUPL MO] "OMA Management Object for SUPL", Version 2.0, Open MobileAlliance™, OMA-TS-SUPL-MO-V2_0,
URL:http://www.openmobilealliance.org/

3. Terminology and Conventions

3.1 Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC 2119].

All sections and appendixes, except “Scope” and “Introduction”, are normative, unless they are explicitly indicated to be informative.

3.2 Definitions

Area ID	Area ID is the identity of an area in a wireless network.
I-WLAN	The interworking WLAN refers to the system for interworking between 3GPP/3GPP2 systems and WLAN. The intent of 3GPP/3GPP2–WLAN Interworking is to extend 3GPP/3GPP2 services and functionality to the WLAN access environment. The 3GPP/3GPP2–WLAN Interworking System provides bearer services allowing a 3GPP/3GPP2 subscriber to use a WLAN to access 3GPP/3GPP2 PS based services.
Location ID	The Location ID defines the current serving cell, current serving WLAN AP or current serving WiMAX BS information of the SET.
LPP	LPP [3GPP LPP] implies use of LPP only
LPPe	LPPe [OMA-LPPe] implies use of LPP and LPPe
Major Version	Major versions are likely to contain major feature additions; MAY contain incompatibilities with previous specification revisions; and though unlikely, could change, drop, or replace standard or existing interfaces. Initial releases are “1_0”. [OMAOPS]
Minor Version	Minor versions are likely to contain minor feature additions, be compatible with the preceding Major version. Minor specification revision include existing interfaces, although it MAY provide evolving interfaces. The initial minor release for any major release is “0”, i.e. 1_0 [OMAOPS]
Multiple Location IDs	The Multiple Location IDs parameter may contain current non-serving cell, current non-serving WLAN AP or current non-serving WiMAX BS information for the SET and/or historic serving or non-serving cell, WLAN AP or WiMAX BS information for the SET.
Quality of Position	A set of attributes associated with a request for the geographic position of SET. The attributes include the required horizontal accuracy, vertical accuracy, max location age, and response time of the SET position.
Service Indicator	Service indicators are intended to be compatible with the Major_ Minor release they relate to but add bug fixes. No new functions will be added through the release of Service Indicators. [OMAOPS]

SUPL Roaming

For positioning not associated with an emergency services call, SUPL roaming occurs when a SET leaves the service area of its H-SLP. For positioning associated with an emergency services call, SUPL roaming occurs when the SET is not within the service area of the E-SLP. The service area of an H-SLP or E-SLP includes the area within which the H-SLP or E-SLP can provide a position estimate for a SET or relevant assistance data to a SET without contacting other SLPs. It should be noted that an H-SLP or E-SLP service area is not necessarily associated with the service area(s) of the underlying wireless network(s).

There are variants of SUPL roaming which are summarized below:

- The H-SLP or E-SLP may request the V-SLP to provide an initial position estimate, e.g., based upon Location ID.
- The H-SLP or E-SLP may request the V-SLP to provide the Lup Position Determination and SPC functionality.

The decision of which variant is applied is implementation specific and out of the scope of this specification. For information purposes, the decision will depend upon such factors as:

(i) Roaming agreements between SUPL providers;

(ii) Location ID;

(iii) Cached information;

(iv) H-SLP/SET or E-SLP/SET negotiation parameters such as positioning method.

3.3 Abbreviations

5GCN	5G Core Network
ACA	Alternative Client Authentication
AP	Access Point (WLAN)
ARFCN	Absolute Radio Frequency Channel Number
BDS	BeiDou Navigation Satellite System
BS	Base Station (WiMAX)
BSF	Bootstrapping Server Function
CI	Cell Identity (3GPP)
CSI-RS	Channel-State Information Reference Signal
DL-AoD	Downlink Angle-of-Departure
DL-E-CID	Downlink Enhanced Cell-ID
DL-TDOA	Downlink Time Difference Of Arrival
FQDN	Fully Qualified Domain Name
GANSS	Galileo and Additional Navigation Satellite Systems
GBA	Generic Bootstrapping Architecture
GLONASS	**GLO**bal'naya **Na**vigatsionnaya **S**putnikovaya **S**istema (Engl.: Global Navigation Satellite System)
GNSS	Global Navigation Satellite System
LAC	Location Area Code (3GPP)
lid	Location ID
LPP	LTE Positioning Protocol
LPPe	LPP Extensions
LRF	Location Retrieval Function
LTE	Long Term Evolution
MBS	Metropolitan Beacon System

MCC	Mobile Country Code (3GPP)
MLP	Mobile Location Protocol
MNC	Mobile Network Code (3GPP)
Multi-RTT	Multi-Round Trip Time
NID	Network ID (C.S0022-A V1.0)
NR	New Radio
OMA	Open Mobile Alliance
OMNA	Open Mobile Naming Authority
OSR	Observation Space Representation
PAP	OMA Push Access Protocol
PEI	Permanent Equipment Identifier
POTAP	OMA Push Over the Air Protocol
PSAP	Public Safety Answering Point
QoP	Quality of Position
QZSS	Quasi-Zenith Satellite System
RB	Resource Block
RE	Resource Element
RLP	Roaming Location Protocol
RNC	Radio Network Controller
RS-SINR	Reference Signal Signal to Noise and Interference Ratio
RTK	Real Time Kinematic
SBAS	Satellite Based Augmentation System
SEK	SUPL Encryption Key
SET	SUPL Enabled Terminal
SID	System ID (C.S0022-A V1.0)
SINR	Signal to Noise and Interference Ratio
SIP	Session Initiation Protocol
SLC	SUPL Location Center
SLP	SUPL Location Platform
SM	Short Message
SMS	Short Message Service
SSB	Synchronization Signal Block
SUPI	Subscription Permanent Identifier
TCP	Transmission Control Protocol
TD-SCDMA	Time Division-Synchronous Code Division Multiple Access
TLS	Transport Layer Security
UL-AoA	Uplink Angle of Arrival
ULP	Userplane Location Protocol
UL-TDOA	Uplink Time Difference of Arrival
UMB	Ultra Mobile Broadband

WAP	Wireless Application Protocol
WCDMA	Wideband Code Division Multiple Access
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network

4. Introduction

Location services based on the location of mobile devices are becoming increasingly widespread. SUPL (Secure User Plane Location) employs user plane data bearers for transferring location information (e.g GPS assistance) and for carrying positioning technology-related protocols between a SUPL Enabled Terminal (SET) and the network. SUPL is considered to be an effective way of transferring location information required for computing the target SET's location.

To serve a location service to a client, considerable signaling and position information are transferred between actors such as a SET and a location server. Currently, assisted-GPS (A-GPS) provides more accurate position of a SET than other available standardized positioning technologies. However, A-GPS over control plane requires modifications to existing network elements, and interfaces (for signaling procedures between the terminal and the network). SUPL needs only an IP capable network and requires minimum modification to the network, and this is an efficient solution that can be deployed rapidly.

SUPL utilizes existing standards where available and possible, and SUPL should be extensible to enabling more positioning technologies as the need arises so that they utilize the same mechanism. In the initial phase, SUPL 1.0 provides functionality of A-GPS with minimum changes of current network elements. SUPL 2.0 introduces the A-GNSS concept to allow additional Navigation Satellite System assisted positioning technology to be utilized, e.g. A-Galileo.

NOTE: Applicability of a particular A-GNSS is subject to the support in relevant 3GPP and 3GPP2 specifications that SUPL is reliant on.

The SUPL 2.0 work item adds new functionality, and based on experience with SUPL 1.0, enhances the existing functionality while maintaining the SUPL 1.0 requirements.

The new functionality will include:

- Triggered positioning procedures, both periodic and area event.
- Emergency positioning procedures.
- Support of A-GANSS positioning method and improvements to enhanced cell id positioning method
- Support of I-WLAN, WiMAX and I-WiMAX networks.
- Positioning procedures for delivery to third party and retrieval of location of another SET.

Note that a WLAN-capable SET must be an I-WLAN SET in order to be supported in SUPL2.0. A WLAN-only SET is not supported.

This protocol specification can be used to implement SUPL both in the SET and in the SLP.

The target audience for this specification is developers and systems engineers implementing SUPL in SETs or SLPs.

5. Detailed Call Flows

Note regarding the use of LPP and LPPe in SUPL 2.0: It is possible to use LPP (by itself) or in combination with LPPe (LPP+LPPe) as a positioning protocol. Thereby the following convention applies: *LPP* implies use of *LPP only* (i.e. without LPPe); *LPPe* implies use of *LPP and LPPe*; and *LPP/LPPe* implies use of either *LPP* without *LPPe* or *LPP* with *LPPe*. A SUPL POS (RRLP/RRC/TIA-801/LPP/LPPe) message means a SUPL POS message carrying either RRLP, RRC, TIA-801, LPP or LPP+LPPe positioning payload.

5.1 SUPL Collaboration Network Initiated

Network Initiated Services are services, which originate from within the SUPL network. For these services the SUPL Agent resides in the Network.

Set up and release of connections:

Before sending any ULP messages the SET SHALL take needed actions such that a TLS connection exists to the SLP/SLC. This can be achieved by establishing a new connection, resume a connection or reuse an existing TLS connection. This includes establishment or utilization of various data connectivity resources that depends on the terminal in which the SET resides and the type of access network. Data connectivity below IP-level is out of scope of this document.

The detailed call flows in this section describes when a TLS connection no longer is needed. The TLS connection shall then be released unless another SUPL session is using the TLS connection.

In the Roaming cases described with an R-SLP in the flow, the R-SLP can be omitted in the flow descriptions having the H-SLP interacting directly with SUPL Agent. In the call flows without R-SLP, an R-SLP can be inserted between SUPL Agent and H-SLP.

5.1.1 Non-Roaming Successful Case – Proxy mode

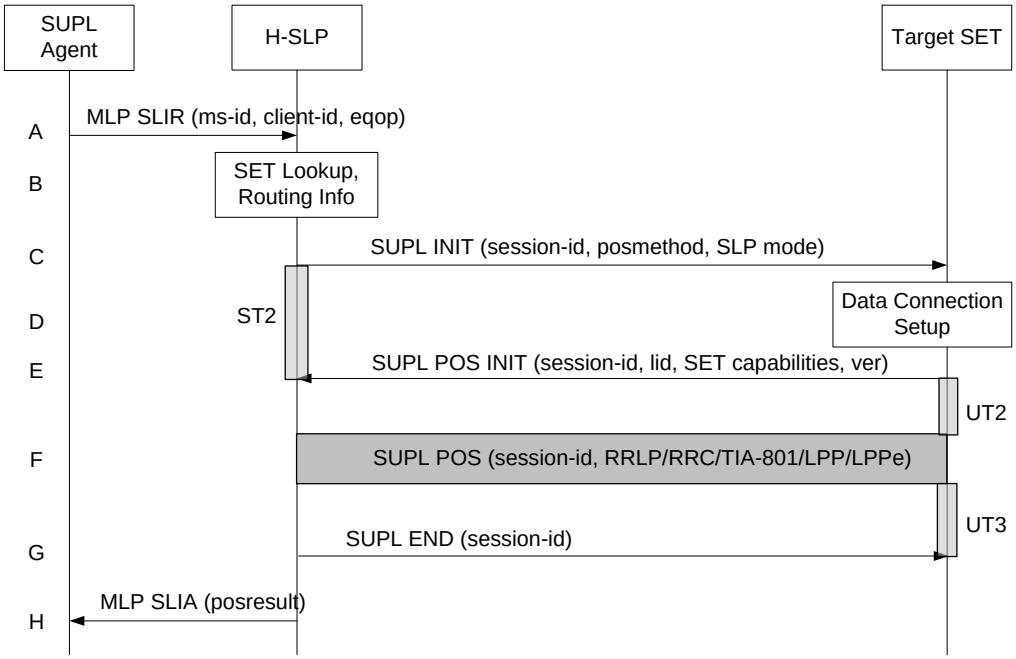

Figure 1: Network Initiated Non-Roaming Successful Case – Proxy Mode

NOTE: See Appendix D for timer descriptions.

A. SUPL Agent issues an MLP SLIR message to the H-SLP, with which SUPL Agent is associated. The H-SLP shall authenticate the SUPL Agent and check if the SUPL Agent is authorized for the service it requests, based on the client-id received. Further, based on the received ms-id the H-SLP shall apply subscriber privacy against the client-id.
If a previously computed position which meets the requested QoP is available at the H-SLP and no notification and

verification is required, the H-SLP SHALL directly proceed to step H. If notification and verification or notification only is required, the H-SLP SHALL proceed to step B.

B. The H-SLP verifies that the target SET is currently not SUPL roaming.
The H-SLP MAY also verify that the target SET supports SUPL.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside the scope of SUPL. However, there are various environment dependent mechanisms.

NOTE: Alternatively, the H-SLP may determine whether the SET is SUPL roaming in a later step using the location identifier (lid) received from the SET.

NOTE: The specifics for determining if the SET supports SUPL are beyond SUPL 2.0 scope.

C. The H-SLP initiates the location session with the SET using the SUPL INIT message. The SUPL INIT message contains at least session-id, proxy/non-proxy mode indicator and the intended positioning method. If the result of the privacy check in Step A indicates that notification or verification to the target subscriber is needed, the H-SLP SHALL also include Notification element in the SUPL INIT message. Before the SUPL INIT message is sent the H-SLP also computes and stores a hash of the message.
If in step A the H-SLP decided to use a previously computed position, the SUPL INIT message SHALL indicate this in a 'no position' posmethod parameter value and the SET SHALL respond with a SUPL END message carrying the results of the verification process (access granted, or access denied). If no explicit verification is required (notification only) the SET SHALL respond with a SUPL END message. The H-SLP SHALL then directly proceed to step H.

NOTE: Before sending the SUPL END message the SET SHALL perform the data connection setup procedure of step D and use the procedures described in step E to establish a secure connection to the H-SLP.

D. The SET analyses the received SUPL INIT. If found to be non authentic SET takes not further actions. Otherwise the SET takes needed action preparing for establishment or resumption of a secure connection.

E. The SET will evaluate the Notification rules and follow the appropriate actions. The SET also checks the proxy/non-proxy mode indicator to determine if the H-SLP uses proxy or non-proxy mode. In this case, proxy mode is used, and the SET SHALL establish a secure connection to the H-SLP using SLP address that has been provisioned by the Home Network to the SET. The SET then sends a SUPL POS INIT message to start a positioning session with the H-SLP. The SET SHALL send the SUPL POS INIT message even if the SET supported positioning technologies do not include the intended positioning method indicated in the SUPL INIT message. The SUPL POS INIT message contains at least session-id, SET capabilities, a hash of the received SUPL INIT message (ver) and Location ID (lid). The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe). The SET MAY provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if this is supported. The SET MAY set the Requested Assistance Data element in the SUPL POS INIT.
If a position retrieved from or calculated based on information received in the SUPL POS INIT message is available that meets the required QoP, the H-SLP MAY directly proceed to step G and not engage in a SUPL POS session.

F. The H-SLP SHALL check that the hash of SUPL INIT matches the one it has computed for this particular session. Based on the SUPL POS INIT message including posmethod(s) supported by the SET the H-SLP SHALL then determine the posmethod. If required for the posmethod the H-SLP SHALL use the supported positioning protocol (e.g., RRLP, RRC, TIA-801 or LPP/LPPe) from the SUPL POS INIT message.
The SET and the H-SLP exchange several successive positioning procedure messages.
The H-SLP calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance obtained from the H-SLP (SET-Based).

G. Once the position calculation is complete the H-SLP sends the SUPL END message to the SET informing it that no further positioning procedure will be started and that the location session is finished. The SET SHALL release the secure connection to the H-SLP and release all resources related to this session.

H. The H-SLP sends the position estimate back to the SUPL Agent in an MLP SLIA message and the H-SLP SHALL release all resources related to this session.

5.1.2 Non-Roaming Successful Case – Non-Proxy mode

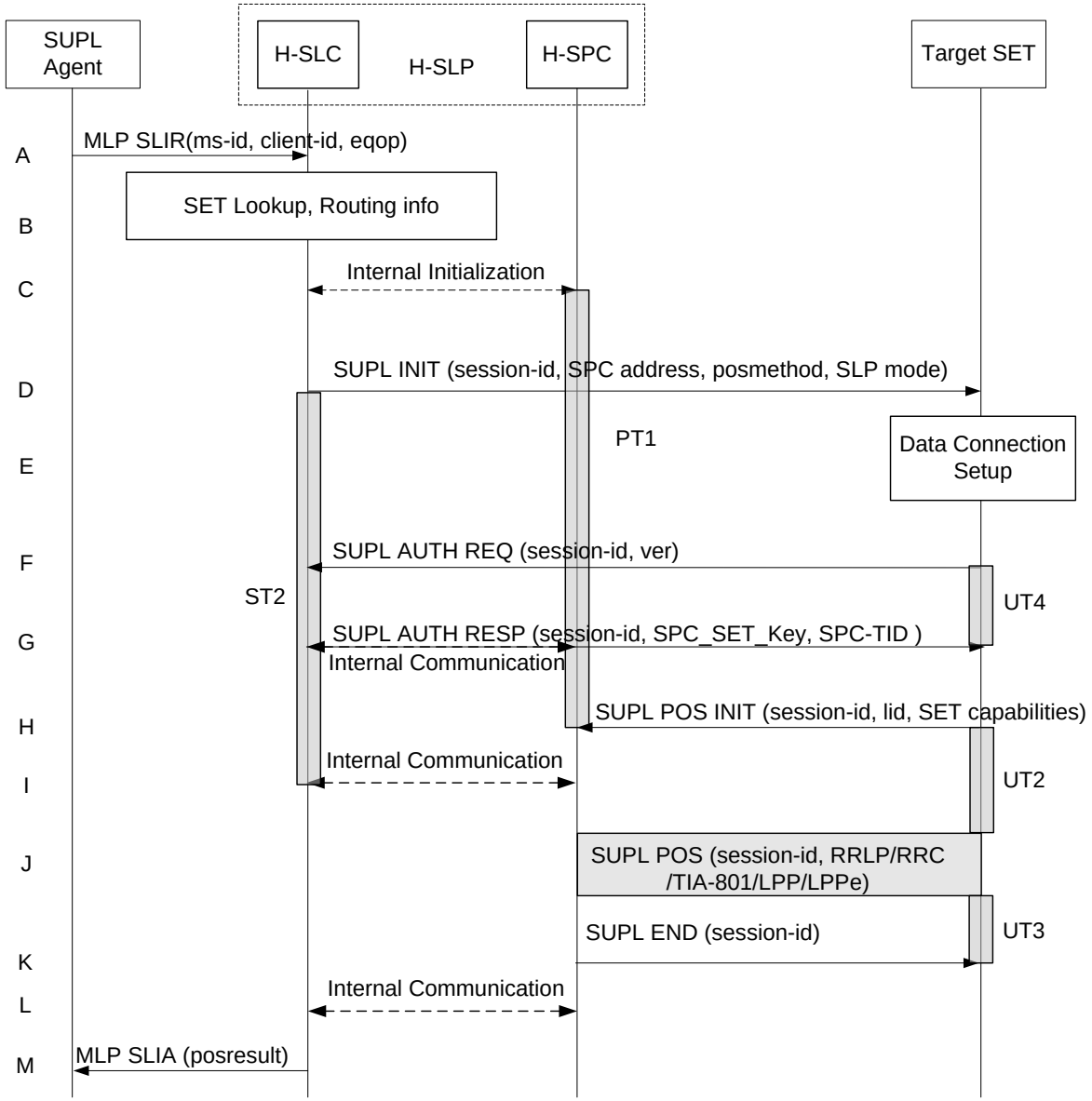

Figure 2: Network Initiated Non-Roaming Successful Case – Non-Proxy mode

NOTE: See Appendix D for timer descriptions.

A. SUPL Agent issues an MLP SLIR message to the H-SLC, with which SUPL Agent is associated. The H-SLC shall authenticate the SUPL Agent and check if the SUPL Agent is authorized for the service it requests, based on the client-id received. Further, based on the received ms-id the H-SLC shall apply subscriber privacy against the client-id.
If a previously computed position which meets the requested QoP is available at the H-SLC and no notification and verification is required, the H-SLC SHALL directly proceed to step M. If notification and verification or notification only is required, the H-SLC SHALL proceed to step D after having performed step B.

B. The H-SLC verifies that the target SET is currently not SUPL roaming.
The H-SLC MAY also verify that the target SET supports SUPL.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside scope of SUPL. However, there are various environment dependent mechanisms.

NOTE: The specifics for determining if the SET supports SUPL are beyond SUPL 2.0 scope.

C. The H-SLC and H-SPC may exchange information necessary to setup the SUPL POS session.

NOTE: The interface between the H-SLC and the H-SPC is specified in [SUPL2 ILP TS]. The implementation of ILP is optional hence the presence(or absence) of ILP is implementation dependent

D. The H-SLC initiates the location session with the SET using the SUPL INIT message. The SUPL INIT message contains at least session-id, address of the H-SPC, proxy/non-proxy mode indicator and the intended positioning method. If the result of the privacy check in Step A indicates that notification or verification to the target subscriber is needed, the H-SLC shall also include the Notification element in the SUPL INIT message.

If in step A the H-SLC decided to use a previously computed position, the SUPL INIT message SHALL indicate this in a 'no position' posmethod parameter value and the SET SHALL respond with a SUPL END message carrying the results of the verification process (access granted, or access denied). If no explicit verification is required (notification only) the SET SHALL respond with a SUPL END message. The H-SLC SHALL then directly proceed to step M.

NOTE: Before sending the SUPL END message the SET SHALL perform the data connection setup procedure of step E and use the procedures described in step F to establish a secure connection to the H-SLC.

E. The SET analyses the received SUPL INIT. If found to be non authentic SET takes not further actions. Otherwise the SET takes needed action preparing for establishment or resumption of a secure connection.

F. The SET uses the address provisioned by the Home Network to establish a secure connection to the H-SLC. The SET then checks the proxy/non-proxy mode indicator to determine if the H-SLP uses proxy or non-proxy mode. In this case non-proxy mode is used and the SET SHALL send a SUPL AUTH REQ message to the H-SLC.The SUPL AUTH REQ message contains the session-id and a hash of the received SUPL INIT message (ver).

G. The H-SLC creates SPC_SET_Key and SPC-TID to be used for mutual H-SPC/SET authentication and sends both in an SUPL AUTH RESP message to the SET. The H-SLC also forwards SPC_SET_Key and SPC-TID to the H-SPC through internal communication.

H. The SET will evaluate the Notification rules and follow the appropriate actions. The SET establishes a secure connection to the H-SPC according to the address received in step D. The SET and H-SPC perform mutual authentication and the SET sends a SUPL POS INIT message to start a positioning session with the H-SPC. The SET SHALL send the SUPL POS INIT message even if the SET supported positioning technologies do not include the intended positioning method indicated in the SUPL INIT message. The SUPL POS INIT message contains at least session-id, SET capabilities and Location ID (lid). The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe). The SET MAY provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if this is supported. The SET MAY set the Requested Assistance Data element in the SUPL POS INIT. The SET SHALL also release the connection to the H-SLC.

I. The H-SLC and H-SPC may collaborate to determine an initial position of the SET to aid in the position determination process. If the initial position calculated based on information received in the SUPL POS INIT message meets the requested QoP, the H-SPC MAY directly proceed to step K and not engage in a SUPL POS session.

J. Based on the SUPL POS INIT message including posmethod(s) supported by the SET the H-SPC SHALL determine the posmethod. If required for the posmethod the H-SPC SHALL use the supported positioning protocol (e.g., RRLP, RRC, TIA-801 or LPP/LPPe) from the SUPL POS INIT message
The SET and the H-SPC exchange several successive positioning procedure messages.
The H-SPC calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance obtained from the SPC (SET-Based).

K. Once the position calculation is complete the H-SPC sends the SUPL END message to the SET informing it that no further positioning procedure will be started and that the SUPL session is finished. The SET SHALL release the secure connection to the H-SPC and release all resources related to this session.

L. The H-SPC informs the H-SLC about the end of the SUPL session. Unless the H-SLC already knows the position, e.g., from step I, the H-SPC informs the H-SLC of the determined position from step J. The H-SPC SHALL release all resources related to this session.

M. The H-SLC sends the position estimate back to the SUPL Agent in an MLP SLIA message. The H-SLC SHALL release all resources related to this session.

5.1.3 Roaming with V-SLP Positioning Successful Case – Proxy mode

SUPL Roaming where the V-SLP is involved in the positioning calculation.

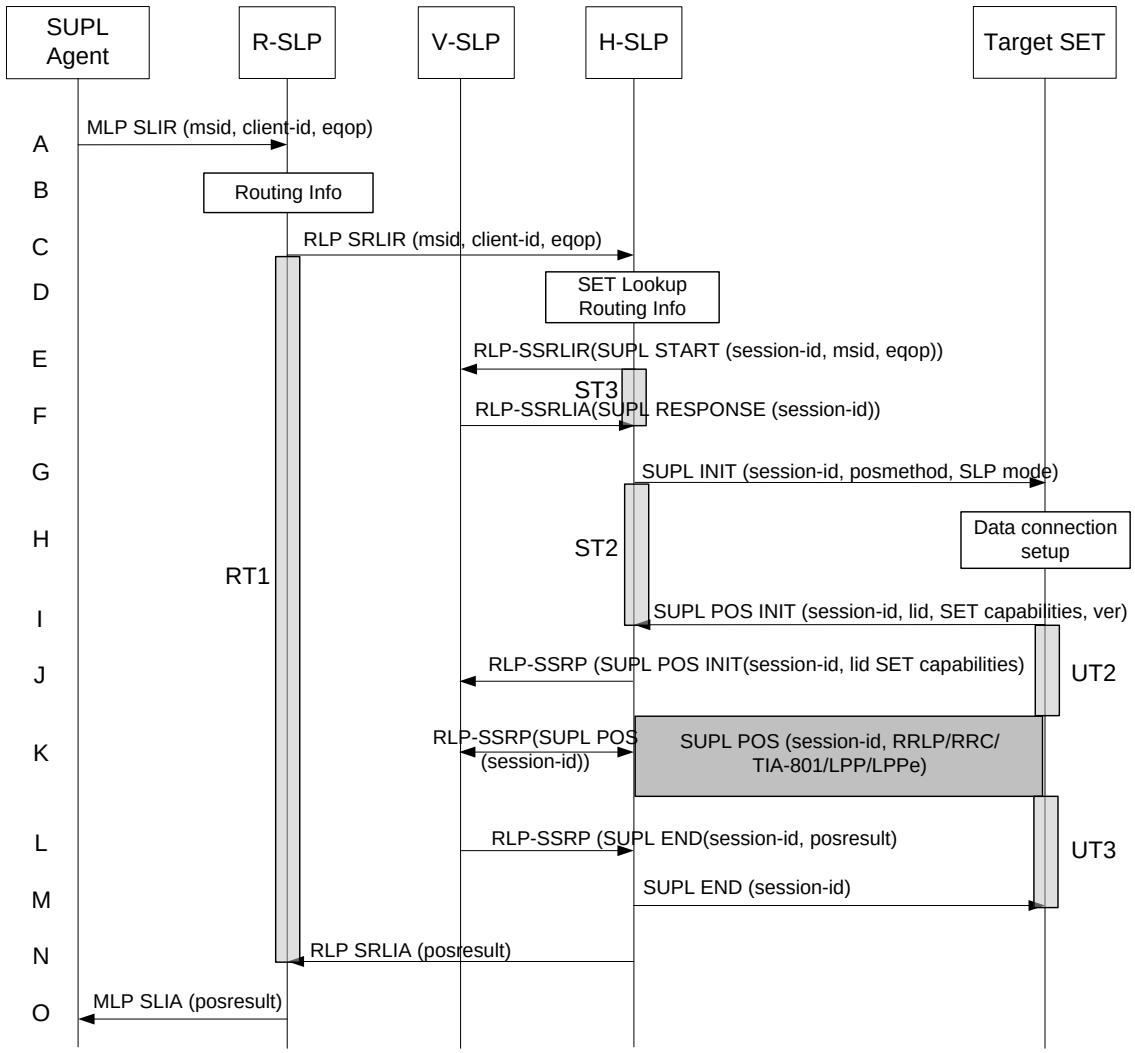

Figure 3: Network Initiated Roaming with V-SLP Positioning Successful Case – Proxy mode

NOTE: See Appendix D for timer descriptions.

A. SUPL Agent issues an MLP SLIR message to the R-SLP, with which SUPL Agent is associated. The R-SLP SHALL authenticate the SUPL Agent and check if the SUPL Agent is authorized for the service it requests, based on the client-id received.

B. The R-SLP determines the H-SLP based on the received msid. If the R-SLP determines that the SUPL Agent is not authorized for this request, Step O will be returned with the applicable MLP return code.

NOTE: The specifics for determining the H-SLP are considered outside scope of SUPL. However, there are various environment dependent mechanisms.

C. The R-SLP then forwards the location request to the H-SLP of the target subscriber, using RLP protocol. Based on the received ms-id the H-SLP SHALL apply subscriber privacy against the client-id. If a previously computed position which meets the requested QoP is available at the H-SLP and no notification and verification is required,

the H-SLP SHALL directly proceed to step N. If notification and verification or notification only is required, the H-SLP SHALL proceed to step G after having performed the step D.

D. The H-SLP verifies that the target SET is currently SUPL roaming. In addition the H-SLP MAY also verify that the target SET supports SUPL.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside the scope of SUPL. However, there are various environment dependent mechanisms.

NOTE: The specifics for determining if the SET supports SUPL are beyond SUPL 2.0 scope

E. The H-SLP sends an RLP SSRLIR to the V-SLP to inform the V-SLP that the target SET will initiate a SUPL positioning procedure. Mandatory parameters in SUPL START that are not known to H-SLP (lid and SET capabilities) shall be populated with arbitrary values by H-SLP and be ignored by V-SLP. The SET part of the session-id will not be included in this message by the H-SLP to distinguish this scenario from a SET Initiated scenario.

F. The V-SLP acknowledges that it is ready to initiate a SUPL positioning procedure with an RLP SSRLIA back to the H-SLP.

G. The H-SLP initiates the location session with the SET using the SUPL INIT message. The SUPL INIT message contains at least session-id, proxy/non-proxy mode indicator and the intended positioning method. If the result of the privacy check in Step C indicates that notification or verification to the target subscriber is needed, the H-SLP SHALL also include the Notification element in the SUPL INIT message. Before the SUPL INIT message is sent the H-SLP also computes and stores a hash of the message.
If in step C the H-SLP decided to use a previously computed position the SUPL INIT message SHALL indicate this in a 'no position' posmethod parameter value and the SET SHALL respond with a SUPL END message to the H-SLP carrying the results of the verification process (access granted, or access denied). If no verification is required (notification only) the SET SHALL respond with a SUPL END message to the H-SLP. The H-SLP SHALL then directly proceed to step N.

NOTE: Before sending the SUPL END message the SET SHALL perform the data connection setup procedure of step H and use the procedures described in step I to establish a secure connection to the H-SLP.

H. The SET analyses the received SUPL INIT. If found to be non authentic SET takes not further actions. Otherwise the SET takes needed action preparing for establishment or resumption of a secure connection.

I. The SET will evaluate the Notification rules and follow the appropriate actions. The SET also checks the proxy/non-proxy mode indicator to determine if the SLP uses proxy or non-proxy mode. In this case, proxy mode is used, and the SET SHALL establish a secure connection to the H-SLP using SLP address that has been provisioned by the Home Network to the SET. The SET then sends a SUPL POS INIT message to start a positioning session with the H-SLP. The SET SHALL send the SUPL POS INIT message even if the SET supported positioning technologies do not include the intended positioning method indicated in the SUPL INIT message. The SUPL POS INIT message contains at least session-id, SET capabilities, a hash of the received SUPL INIT message (ver) and Location ID (lid). The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe). The SET MAY optionally provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if this is supported. The SET MAY set the Requested Assistance Data element in the SUPL POS INIT.

J. The H-SLP SHALL check that the hash of SUPL INIT matches the one it has computed for this particular session. The H-SLP then tunnels the SUPL POS INIT message to the V-SLP.

K. Based on the SUPL POS INIT message including posmethod(s) supported by the SET, the V-SLP SHALL determine the posmethod. If required for the posmethod, the V-SLP SHALL use the supported positioning protocol (e.g., RRLP, RRC, TIA-801 or LPP/LPPe) from the SUPL POS INIT message.
If the V-SLP already calculated an initial position based on information received in the SUPL POS INIT message which satisfies the requested QoP the V-SLP MAY directly proceed to step L and not engage in a SUPL POS session.
Otherwise the SET and the V-SLP exchange several successive positioning procedure messages, tunnelled over RLP via the H-SLP.
The V-SLP calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance obtained from the V-SLP via H-SLP (SET-Based).

L. Once the position calculation is complete the V-SLP sends the SUPL END message to the SET, which is tunnelled over RLP via the H-SLP. The V-SLP SHALL release all resources related to this session.

M. The H-SLP forwards the SUPL END to the SET informing it that no further positioning procedure will be started and that the location session is finished. The SET SHALL release the secure connection to the H-SLP and release all resources related to this session.

N. The H-SLP sends the position estimate back to the R-SLP in an RLP SRLIA message. The H-SLP SHALL release all resources related to this session.

O. The R-SLP sends the position estimate back to the SUPL Agent in an MLP SLIA message.

5.1.4 Roaming with V-SPC Positioning Successful Case – Non-Proxy-mode

SET Roaming where the V-SLP is involved in the positioning calculation.

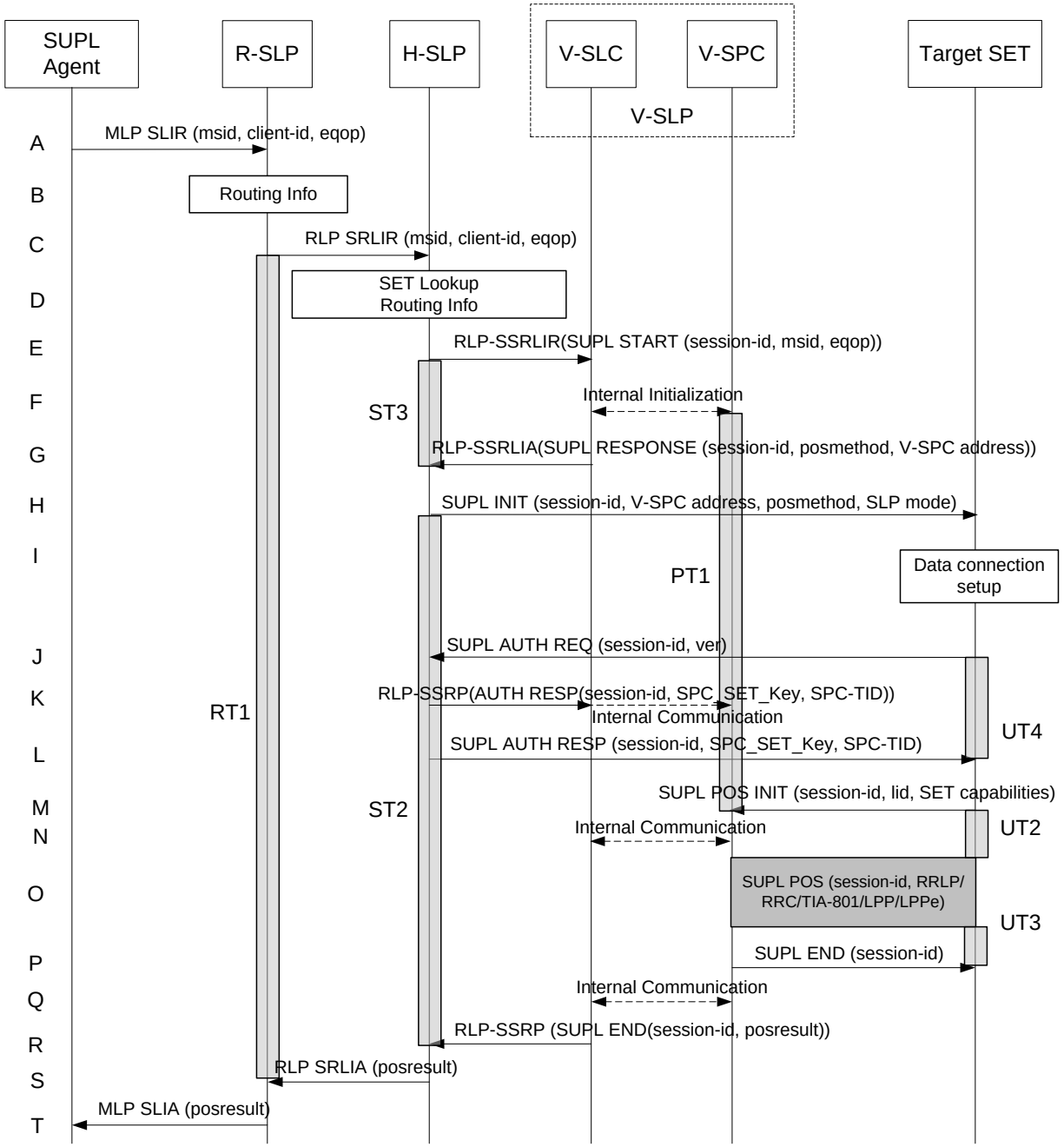

Figure 4: Network Initiated Roaming with V-SPC Positioning Successful Case – Non-Proxy-mode

NOTE: See Appendix D for timer descriptions.

A. SUPL Agent issues an MLP SLIR message to the R-SLP, with which SUPL Agent is associated. The R-SLP SHALL authenticate the SUPL Agent and check if the SUPL Agent is authorized for the service it requests, based on the client-id received.

B. The R-SLP determines the H-SLP based on the received msid. If the R-SLP determines that the SUPL Agent is not authorized for this request, Step T will be returned with the applicable MLP return code.

NOTE: The specifics for determining the H-SLP are considered outside scope of SUPL. However, there are various environment dependent mechanisms.

C. The R-SLP then forwards the location request to the H-SLP of the target subscriber, using RLP protocol. Based on the received ms-id the H-SLP SHALL apply subscriber privacy against the client-id. If a previously computed position which meets the requested QoP is available at the H-SLP and no notification and verification is required, the H-SLP SHALL directly proceed to step S. If notification and verification or notification only is required, the H-SLP SHALL proceed to step H after having performed the step D.

D. The H-SLP verifies that the target SET is currently SUPL roaming. In addition the H-SLP MAY also verify that the target SET supports SUPL.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside scope of SUPL. However, there are various environment dependent mechanisms.

NOTE: The specifics for determining if the SET supports SUPL are beyond SUPL 2.0 scope.

E. The H-SLP allocates a session-id for the SUPL session and decides that the V-SPC will provide assistance data or perform the position calculation. The H-SLP sends an RLP SSRLIR to the V-SLC to inform the V-SLC that the target SET will initiate a SUPL positioning procedure. Mandatory parameters in SUPL START that are not known to H-SLP (lid and SET capabilities) shall be populated with arbitrary values by H-SLP and be ignored by V-SLP. The SET part of the session-id will not be included in this message by the H-SLP to distinguish this scenario from a SET Initiated scenario.

F. The V-SLC informs the V-SPC of an incoming SUPL positioning session.

G. The V-SLC acknowledges that V-SPC is ready to initiate a SUPL positioning procedure with an RLP SSRLIA back to the H-SLP. The message includes at least session-id, posmethod and the address of the V-SPC.

H. The H-SLP initiates the location session with the SET using the SUPL INIT message. The SUPL INIT message contains at least session-id, address of the V-SPC, proxy/non-proxy mode indicator and the intended positioning method. If the result of the privacy check in Step C indicates that notification or verification to the target subscriber is needed, the H-SLP SHALL also include Notification element in the SUPL INIT message.

If in step C the H-SLP decided to use a previously computed position the SUPL INIT message SHALL indicate this in a ‘no position’ posmethod parameter value and the SET SHALL respond with a SUPL END message to the H-SLP carrying the results of the verification process (access granted, or access denied). If no verification is required (notification only) the SET SHALL respond with a SUPL END message to the H-SLP. The H-SLP SHALL then directly proceed to step S.

NOTE: Before sending the SUPL END message the SET SHALL perform the data connection setup procedure of step I and use the procedures described in step J to establish a secure connection to the H-SLP.

I. The SET analyses the received SUPL INIT. If found to be non authentic SET takes not further actions. Otherwise the SET takes needed action preparing for establishment or resumption of a secure connection.

J. The SET uses the address provisioned by the Home Network to establish a connection to the H-SLP. The SET then checks the proxy/non-proxy mode indicator to determine if the H-SLP uses proxy or non-proxy mode. In this case non-proxy mode is used and the SET SHALL send a SUPL AUTH REQ message to the H-SLP. The SUPL AUTH REQ message contains the session-id and a hash of the received SUPL INIT message (ver).

K. The H-SLP creates SPC_SET_Key and SPC-TID to be used for mutual V-SPC/SET authentication. The H-SLP forwards SPC_SET_Key and SPC-TID to the V-SLC through an RLP SSRP message. The V-SLC forwards SPC_SET_Key and SPC-TID to the V-SPC through internal communication.

L. The H-SLP returns a SUPL AUTH RESP to the SET. The SUPL AUTH RESP message SHALL contain the session-id, SPC_SET_Key and SPC-TID.

M. The SET will evaluate the Notification rules and follow the appropriate actions. The SET establishes a secure connection to the V-SPC according to the address received in step H. The SET and V-SPC perform mutual authentication and the SET sends a SUPL POS INIT message to start a SUPL positioning session with the V-SPC. The SET SHALL send the SUPL POS INIT message even if the SET supported positioning technologies do not include the intended positioning method indicated in the SUPL INIT message. The SUPL POS INIT message contains at least session-id, SET capabilities and Location ID (lid). The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe). The SET MAY provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if this is supported. The SET MAY set the

Requested Assistance Data element in the SUPL POS INIT. The SET SHALL also release the connection to the H-SLP.

N. The V-SLC and V-SPC may collaborate to determine an initial position of the SET to aid in the position determination process. If the initial position calculated based on information received in the SUPL POS INIT message meets the requested QoP, the V-SPC MAY directly proceed to step P and not engage in a SUPL POS session.

O. Based on the SUPL POS INIT message including posmethod(s) supported by the SET, the V-SPC SHALL determine the posmethod. If required for the posmethod, the V-SPC SHALL use the supported positioning protocol (e.g., RRLP, RRC, TIA-801 or LPP/LPPe) from the SUPL POS INIT message.
The SET and the V-SPC exchange several successive positioning procedure messages.
The V-SPC calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance obtained from the V-SPC (SET-Based).

P. Once the position calculation is complete the V-SPC sends a SUPL END message to the SET informing it that no further positioning procedure will be started and that the positioning session is finished. The SET SHALL release all resources related to this session.

Q. The V-SPC informs the V-SLC that the positioning procedure is completed and returns the position result. The V-SPC SHALL release all resources related to this session.

R. The V-SLC sends a RLP SSRP to the H-SLP carrying the position result. The V-SLC SHALL release all resources related to this session.

S. The H-SLP sends the position estimate back to the R-SLP in an RLP SRLIA message. The H-SLP SHALL release all resources related to this session.

T. The R-SLP sends the position estimate back to the SUPL Agent in an MLP SLIA message.

5.1.5 Roaming with H-SLP Positioning Successful case – Proxy mode

SUPL Roaming where the H-SLP is involved in the positioning calculation.

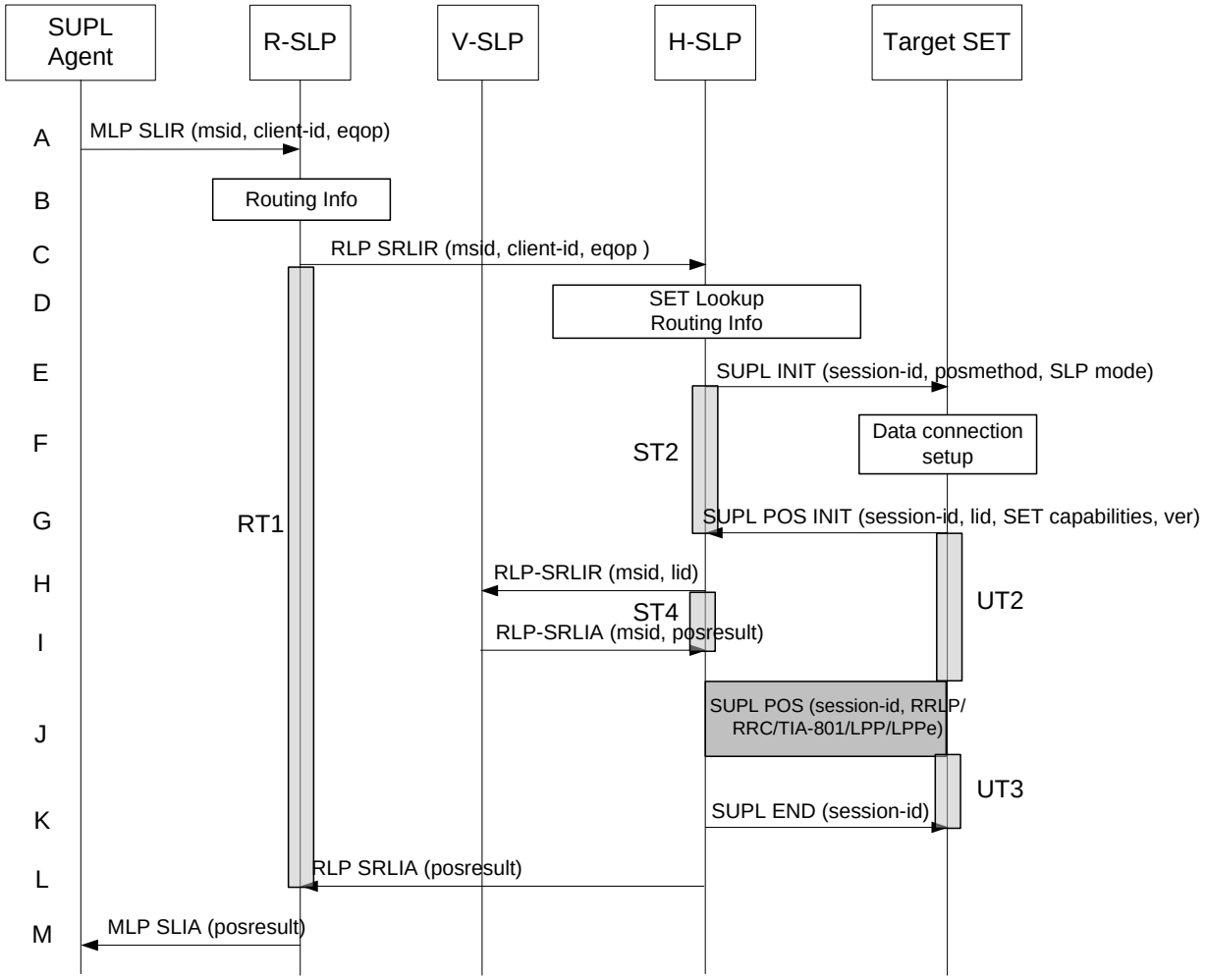

Figure 5: Network Initiated Roaming with H-SLP Positioning Successful case – Proxy mode

NOTE: See Appendix D for timer descriptions.

A. SUPL Agent issues an MLP SLIR message to the R-SLP, with which SUPL Agent is associated. The R-SLP SHALL authenticate the SUPL Agent and check if the SUPL Agent is authorized for the service it requests, based on the client-id received.

B. The R-SLP determines the H-SLP based on the received msid. If the R-SLP determines that the SUPL Agent is not authorized for this request, Step M will be returned with the applicable MLP return code.

NOTE: The specifics for determining the H-SLP are considered outside scope of SUPL. However, there are various environment dependent mechanisms.

C. The R-SLP then forwards the location request to the H-SLP of the target subscriber, using RLP protocol. Based on the received ms-id the H-SLP SHALL apply subscriber privacy against the client-id. If a previously computed position which meets the requested QoP is available at the H-SLP and no notification and verification is required, the H-SLP SHALL directly proceed to step L. If notification and verification or notification only is required, the H-SLP SHALL proceed to step E after having performed the step D.

D. The H-SLP verifies that the target SET is currently SUPL roaming. In addition the H-SLP MAY also verify that the target SET supports SUPL.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside scope of SUPL. However, there are various environment dependent mechanisms.

NOTE: Alternatively, the H-SLP may determine whether the SET is SUPL roaming in a later step using the location identifier (lid) received from the SET.

NOTE: The specifics for determining if the SET supports SUPL are beyond SUPL 2.0 scope.

E. The H-SLP initiates the location session with the SET using the SUPL INIT message. The SUPL INIT message contains at least session-id, proxy/non-proxy mode indicator and the intended positioning method. If the result of the privacy check in Step C indicates that notification or verification to the target subscriber is needed, the H-SLP SHALL also include Notification element in the SUPL INIT message. Before the SUPL INIT message is sent the SLP also computes and stores a hash of the message.
If in step C the H-SLP decided to use a previously computed position the SUPL INIT message SHALL indicate this in a 'no position' posmethod parameter value and the SET SHALL respond with a SUPL END message to the H-SLP carrying the results of the verification process (access granted, or access denied). If no verification is required (notification only) the SET SHALL respond with a SUPL END message to the H-SLP. The H-SLP SHALL then directly proceed to step L.

NOTE: Before sending the SUPL END message the SET shall follow the data connection setup procedure of step F and use the procedures described in step G to establish a secure connection to the H-SLP.

F. The SET analyses the received SUPL INIT. If found to be non authentic SET takes not further actions. Otherwise the SET takes needed action preparing for establishment or resumption of a secure connection.

G. The SET will evaluate the Notification rules and follow the appropriate actions. The SET also checks the proxy/non-proxy mode indicator to determine if the H-SLP uses proxy or non-proxy mode. In this case, proxy mode is used, and the SET SHALL establish a secure connection to the H-SLP using SLP address that has been provisioned by the Home Network to the SET. The SET then sends a SUPL POS INIT message to start a positioning session with the H-SLP. The SET SHALL send the SUPL POS INIT message even if the SET supported positioning technologies do not include the intended positioning method indicated in the SUPL INIT message. The SUPL POS INIT message contains at least session-id, SET capabilities and Location ID (lid) and a hash of the received SUPL INIT message (ver). The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe). The SET MAY provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if this is supported. The SET MAY set the Requested Assistance Data element in the SUPL POS INIT.

H. The H-SLP SHALL check that the hash of SUPL INIT matches the one it has computed for this particular session. If an initial position calculated based on information received in the SUPL POS INIT message is available which meets the requested QoP, the H-SLP MAY directly proceed to step K. The H-SLP then decides that the H-SLP will provide assistance/position calculation and the H-SLP sends an RLP SRLIR request to the V-SLP to determine an initial position for the SET. The RLP request contains at least the msid and the Location ID (lid). Optionally the H-SLP MAY forward NMR provided by the SET to the V-SLP.

I. The V-SLP returns an RLP SRLIA message. The RLP SRLIA message contains at least the position result (i.e. initial position of the SET). If the computed position meets the requested QoP, the H-SLP MAY proceed directly to step K and not engage in a SUPL POS session.

J. Based on the SUPL POS INIT message including posmethod(s) supported by the SET, the H-SLP SHALL determine the posmethod. If required for the posmethod, the H-SLP SHALL use the supported positioning protocol (e.g., RRLP, RRC, TIA-801 or LPP/LPPe) from the SUPL POS INIT message.
The SET and the H-SLP exchange several successive positioning procedure messages.
The H-SLP calculates the position estimate based on the received positioning measurements (SET assisted) or the SET calculates the position estimate based on assistance obtained from the H-SLP (SET based).

K. Once the position calculation is complete the H-SLP sends a SUPL END message to the SET informing it that no further positioning procedure will be started and that the location session is finished. The SET SHALL release the secure connection to the H-SLP and release all resources related to this session.

L. The H-SLP forwards the location estimate to R-SLP if the position estimate is allowed by the privacy settings of the target subscriber. The H-SLP SHALL release all resources related to this session.

M. The R-SLP sends the position estimate back to the SUPL Agent in an MLP SLIA message.

5.1.6 Roaming with H-SPC Positioning Successful Case – Non-Proxy-mode

SUPL Roaming where the H-SPC is involved in the positioning calculation.

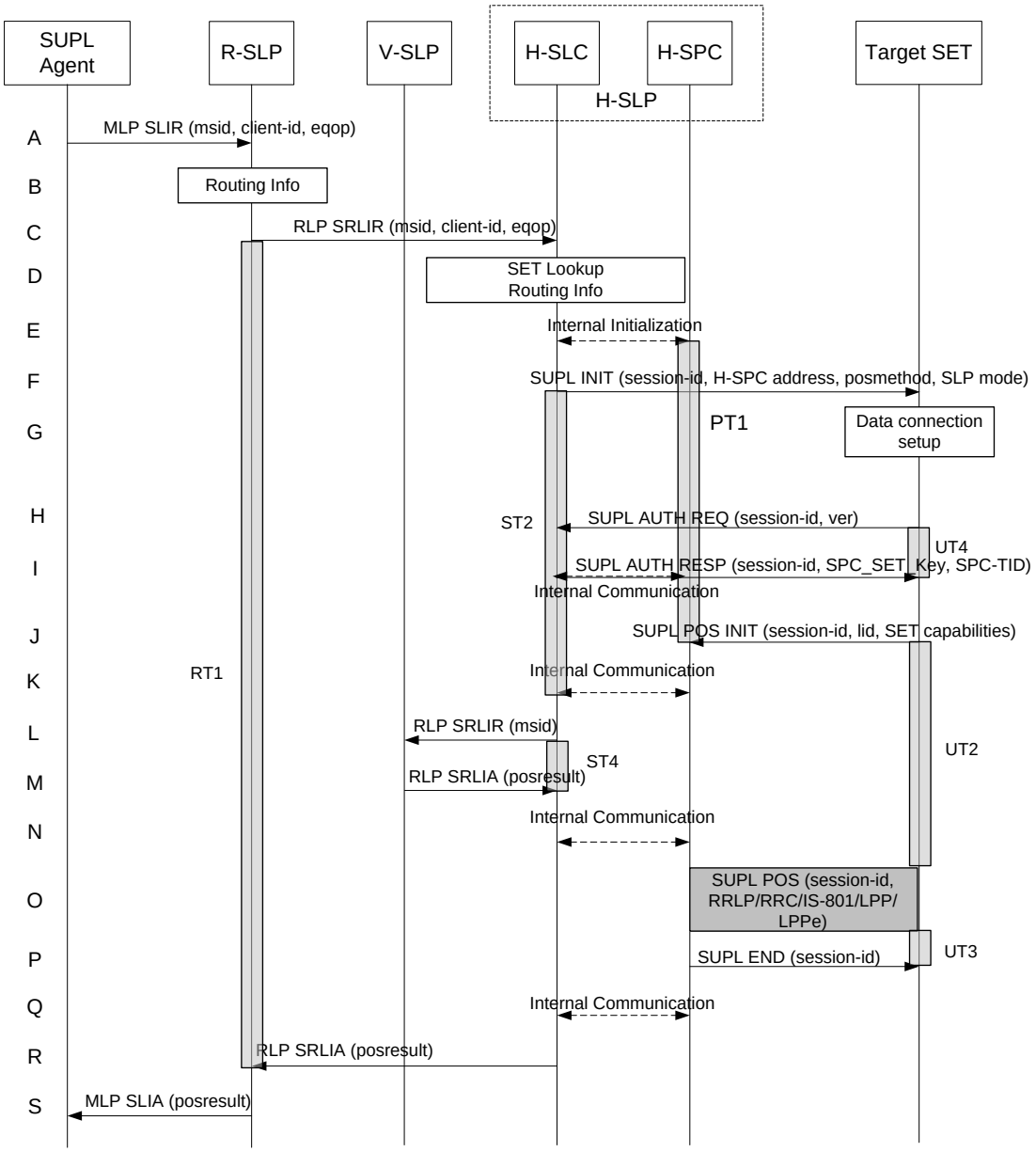

Figure 6: Network Initiated Roaming with H-SPC Positioning Successful Case – Non-Proxy-mode

NOTE: See Appendix D for timer descriptions.

A. SUPL Agent issues an MLP SLIR message to the R-SLP, with which SUPL Agent is associated. The R-SLP SHALL authenticate the SUPL Agent and check if the SUPL Agent is authorized for the service it requests, based on the client-id received.

B. The R-SLP determines the H-SLP based on the received msid. If the R-SLP determines that the SUPL Agent is not authorized for this request, Step S will be returned with the applicable MLP return code.

NOTE: The specifics for determining the H-SLP are considered outside scope of SUPL. However, there are various environment dependent mechanisms.

C. The R-SLP then forwards the location request to the H-SLC of the target subscriber, using RLP protocol. Based on the received ms-id the H-SLC SHALL apply subscriber privacy against the client-id. If a previously computed position which meets the requested QoP is available at the H-SLC and no notification and verification is required, the H-SLC SHALL directly proceed to step R. If notification and verification or notification only is required, the H-SLC SHALL proceed to step F after having performed the step D.

D. The H-SLC verifies that the target SET is currently SUPL roaming. In addition the H-SLC MAY also verify that the target SET supports SUPL.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside scope of SUPL. However, there are various environment dependent mechanisms.

NOTE: Alternatively, the H-SLC may determine whether the SET is SUPL roaming in a later step using the location identifier (lid) received from the SET.

NOTE: The specifics for determining if the SET supports SUPL are beyond SUPL 2.0 scope.

E. The H-SLC informs the H-SPC of the pending SUPL positioning session.

F. The H-SLC initiates the location session with the SET using the SUPL INIT message. The SUPL INIT message contains at least session-id, address of the H-SPC, proxy/non-proxy mode indicator and the intended positioning method. If the result of the privacy check in Step C indicates that notification or verification to the target subscriber is needed, the H-SLC SHALL also include the Notification element in the SUPL INIT message.
If in step C the H-SLC decided to use a previously computed position the SUPL INIT message SHALL indicate this in a 'no position' posmethod parameter value and the SET SHALL respond with a SUPL END message to the H-SLC carrying the results of the verification process (access granted, or access denied). If no verification is required (notification only) the SET SHALL respond with a SUPL END message to the H-SLC. The H-SLC SHALL then directly proceed to step R.

NOTE: Before sending the SUPL END message the SET SHALL perform the data connection setup procedure of step G and use the procedures described in step H to establish a secure connection to the H-SLC.

G. The SET analyses the received SUPL INIT. If found to be non authentic SET takes not further actions. Otherwise the SET takes needed action preparing for establishment or resumption of a secure connection.

H. The SET uses the address provisioned by the Home Network to establish a secure connection to the H-SLC. The SET then checks the proxy/non-proxy mode indicator to determine if the H-SLC uses proxy or non-proxy mode. In this case non-proxy mode is used and the SET SHALL send a SUPL AUTH REQ message to the H-SLC. The SUPL AUTH REQ message contains the session-id and a hash of the received SUPL INIT message (ver).

I. The H-SLC creates SPC_SET_Key and SPC-TID to be used for mutual H-SPC/SET authentication. The H-SLC forwards SPC_SET_Key and SPC-TID to the H-SPC through internal communication and returns a SUPL AUTH RESP message including SPC_SET_Key and SPC-TID to the SET.

J. The SET will evaluate the Notification rules and follow the appropriate actions. The SET establishes a secure connection to the H-SPC according to the address received in step F. The SET and H-SPC perform mutual authentication and the SET then sends a SUPL POS INIT message to start a positioning session with the H-SPC. The SET SHALL send the SUPL POS INIT message even if the SET supported positioning technologies do not include the intended positioning method indicated in the SUPL INIT message. The SUPL POS INIT message contains at least session-id, SET capabilities and Location ID (lid). The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe). The SET MAY provide NMR specific data for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if this is supported. The SET MAY set the Requested Assistance Data element in the SUPL POS INIT. The SET SHALL also release the connection to the H-SLC.

K. The H-SLC and H-SPC may collaborate to determine an initial position of the SET to aid in the position determination process. If the initial position calculated based on information received in the SUPL POS INIT message meets the requested QoP, the H-SPC MAY directly proceed to step P.

L. The H-SLC sends an RLP SRLIR request to the V-SLP to determine an initial position for the SET. The RLP request contains at least the msid and the Location ID (lid). Optionally the H-SLC MAY forward NMR provided by the SET to the V-SLP.

M. The V-SLP returns a RLP SRLIA message. The RLP SRLIA message contains at least the position result (i.e. initial position of the SET).

N. The H-SLC sends the initial position to the H-SPC. If the initial position meets the requested QoP, the H-SPC proceeds directly to step P without engaging in a SUPL POS session.

O. Based on the SUPL POS INIT message including posmethod(s) supported by the SET the H-SPC SHALL determine the posmethod. If required for the posmethod the H-SPC SHALL use the supported positioning protocol (e.g., RRLP, RRC, TIA-801 or LPP/LPPe) from the SUPL POS INIT message.
The SET and the H-SPC exchange several successive positioning procedure messages.
The H-SPC calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance obtained from the H-SPC (SET-Based).

P. Once the position calculation is complete the H-SPC sends SUPL END message to the SET informing it that no further positioning procedure will be started and that the positioning session is finished. The SET SHALL release all resources related to this session.

Q. The H-SPC informs the H-SLC that the positioning procedure is completed and returns the position result. The H-SPC SHALL release all resources related to this session.

R. The H-SLC sends the position estimate back to the R-SLP in an RLP SRLIA message. The H-SLC SHALL release all resources related to this session.

S. The R-SLP sends the position estimate back to the SUPL Agent in an MLP SLIA message.

5.1.7 Network Initiated Proxy Mode – Triggered Services: Periodic Triggers

This section describes the call flows for Network Initiated periodic triggered services for proxy mode. The periodic trigger mechanism resides in the SET which means the SET periodically performs the actions required to determine a position estimate.

5.1.7.1 Non-Roaming Successful Case

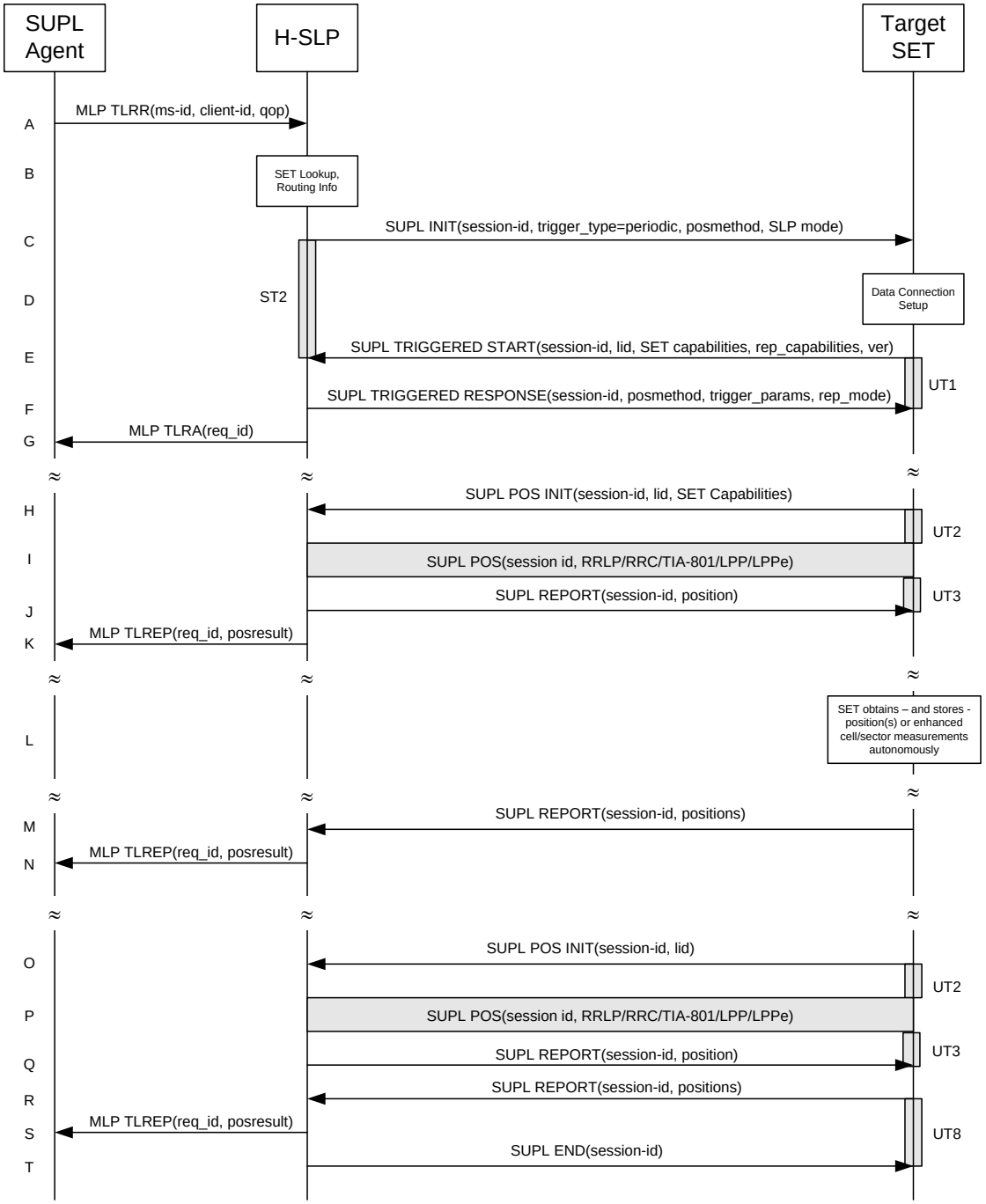

Figure 7: Network Initiated Periodic Trigger Service Non-Roaming Successful Case – Proxy Mode

NOTE: See Appendix D for timer descriptions.

A. SUPL Agent issues an MLP TLRR message to the H-SLP, with which SUPL Agent is associated. The H-SLP shall authenticate the SUPL Agent and check if the SUPL Agent is authorized for the service it requests, based on the client-id received. Further, based on the received ms-id the H-SLP shall apply subscriber privacy against the client-id. The TLRR message may indicate that batch reporting or quasi-real time reporting is to be used instead of real time reporting. In the case of batch reporting, the TLRR indicates the conditions for sending batch reports to the H-SLP and any criteria, when the conditions for sending arise, for including or excluding particular stored position estimates (e.g. QoP, time window).

B. The H-SLP verifies that the target SET is currently not SUPL roaming.
The H-SLP MAY also verify that the target SET supports SUPL.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside the scope of SUPL. However, there are various environment dependent mechanisms.

NOTE: Alternatively, the H-SLP may determine whether the SET is SUPL roaming in a later step using the location identifier (lid) received from the SET.

NOTE: The specifics for determining if the SET supports SUPL are beyond SUPL 2.0 scope.

C. The H-SLP initiates the periodic trigger session with the SET using the SUPL INIT message. The SUPL INIT message contains at least session-id, trigger type indicator (in this case periodic), proxy/non-proxy mode indicator and the intended positioning method. If the result of the privacy check in Step A indicates that notification or verification to the target subscriber is needed, the H-SLP SHALL also include the Notification element in the SUPL INIT message. Before the SUPL INIT message is sent, the H-SLP also computes and stores a hash of the message.

D. The SET analyses the received SUPL INIT. If found to be non authentic SET takes not further actions. Otherwise the SET takes needed action preparing for establishment or resumption of a secure connection.

E. The SET will evaluate the Notification rules and follow the appropriate actions. The SET also checks the proxy/non-proxy mode indicator to determine if the H-SLP uses proxy or non-proxy mode. In this case, proxy mode is used, and the SET SHALL establish a secure connection to the H-SLP using SLP address that has been provisioned by the Home Network to the SET.
The SET then sends a SUPL TRIGGERED START message to start a periodic triggered session with the H-SLP. The SET SHALL send the SUPL TRIGGERED START message even if the SET supported positioning technologies do not include the intended positioning method indicated in the SUPL INIT message. The SUPL TRIGGERED START message contains at least session-id, SET capabilities, a hash of the received SUPL INIT message (ver) and Location ID (lid) and reporting capabilities (rep_capabilities). The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe). The rep_capabilities parameter indicates whether the SET is capable of batch reporting, real time reporting and/or quasi-real time reporting.

F. Consistent with the SET capabilities received in the SUPL TRIGGERED START message the H-SLP selects an intended positioning method to be used for the periodic triggered session and responds with a SUPL TRIGGERED RESPONSE message including session-id, posmethod and periodic trigger parameters. Consistent with the rep_capabilities of the SET, the H-SLP also indicates the reporting mode (rep_mode parameter) to be used by the SET: real time reporting, quasi-real time reporting or batch reporting. In the case of batch reporting, the SUPL TRIGGERED RESPONSE message indicates the conditions for sending batch reports to the H-SLP and any criteria, when the conditions for sending arise, for including or excluding particular stored position estimates and/or (if allowed) particular stored enhanced cell/sector measurements. In the case of quasi-real time reporting, the SUPL TRIGGERED RESPONSE message indicates whether the SET is allowed to send enhanced cell/sector measurements in lieu of or in addition to position estimates. If enhanced cell/sector positioning was selected for batch or quasi-real time reporting, the SUPL TRIGGERED RESPONSE message indicates if the SET is permitted to send stored enhanced cell/sector measurements. In this case, if batch reporting was selected, the SET MAY skip steps H, I and J.

G. The H-SLP informs the SUPL Agent in an MLP TLRA message that the triggered location response request has been accepted and also includes a req_id parameter to be used as a transaction id for the entire duration of the periodic triggered session. The SET and the H-SLP MAY release the secure connection.

NOTE: The MLP TLRA may be sent earlier at any time after the H-SLP receives the MLP TLRR.

H. When the periodic trigger in the SET indicates that a position fix has to be performed, the SET attaches itself to the Packet Data Network if it is not already attached or establishes a circuit switched data connection. The SET then sends a SUPL POS INIT message to start a positioning session with the H-SLP. The SUPL POS INIT message contains at least session-id, Location ID (lid) and the SET Capabilities parameter. The SET MAY provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if this is supported. The SET MAY set the Requested Assistance Data element in the SUPL POS INIT.
If a position calculated based on information received in the SUPL POS INIT message is available (e.g. a cell-id

based position fix) that meets the required QoP, the H-SLP MAY directly proceed to step J and not engage in a SUPL POS session.

I. The SET and the H-SLP exchange several successive positioning procedure messages.
The H-SLP calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance obtained from the H-SLP (SET-Based).

J. Once the position calculation is complete the H-SLP sends the SUPL REPORT message to the SET informing it that the positioning procedure is completed. The SET MAY release the secure connection to the H-SLP. If the reporting mode is batch reporting, the SET stores all calculated position estimates. In SET Assisted mode the position is calculated by the H-SLP and therefore needs to be included in the message for batch reporting mode.

If a SET Based positioning method was chosen which allows the SET to autonomously calculate a position estimate (e.g. autonomous GPS or A-GPS SET Based mode where the SET has current GPS assistance data and does not require an assistance data update from the H-SLP) steps H to J are not performed. Instead, the SET autonomously calculates the position estimate and – for real time or quasi-real time reporting – sends the calculated position estimate to the H-SLP using a SUPL REPORT message containing the session-id and the position estimate.

K. This step is optional: Once the position calculation is complete and if real time or quasi-real time reporting is used, the H-SLP sends a MLP TLREP message to the SUPL Agent. The MLP TLREP message includes the req_id and the position result. If the reporting mode is set to batch reporting, this message is not used.

L. This step is optional: If the SET cannot communicate with the H-SLP (e.g. no radio coverage available) and quasi-real time reporting is used or if batch reporting is used, the SET MAY – if supported – perform SET Based position fixes (autonomous GPS or SET Based A-GPS where the SET has current assistance data) and/or, if allowed by the H-SLP, enhanced cell/sector measurements. In the case of batch reporting, and if explicitly allowed by the H-SLP, enhanced cell/sector measurements are permitted even when the SET can communicate with the H-SLP.

M. This step is optional and is executed if batch reporting is used and if any of the conditions for sending batch reports have occurred. It is also executed, once the SET is able to re-establish communication with the H-SLP, if quasi-real time reporting is used if one or more previous reports have been missed. The SET sends the stored position estimates and/or, if allowed, the stored enhanced cell/sector measurements in an unsolicited SUPL REPORT message to the H-SLP. The SUPL REPORT message contains the session-id and the position result(s) including date and time information for each position result and optionally the position method used. In the case of batch reporting, the stored position estimates and/or enhanced cell/sector measurements included in the SUPL REPORT message may be chosen according to criteria received in step F. If no criteria are received in step F, the SET shall include all stored position estimates and/or enhanced cell/sector measurements not previously reported.

N. If enhanced cell/sector measurements are received in step M, the H-SLP calculates corresponding position estimates.
The H-SLP forwards the reported and/or calculated position estimate(s) to the SUPL Agent in an MLP TLREP message.

Steps H to N are repeated as applicable. When the last position estimate needs to be calculated i.e. the end of the periodic triggered session has been reached, steps O to Q may be performed (a repeat of steps H to J). Alternatively – and if applicable – step L is repeated.

R. This step is optional. When real-time reporting is used, it is executed after the last position estimate or, if allowed, last set of enhanced cell/sector measurements has been obtained or was due. When batch or quasi real-time reporting is used, step R is executed if and as soon as the following conditions apply:

   i. The SET has stored historic location reports and/or stored historic enhanced cell/sector measurements that have not yet been sent to the H-SLP.
   ii. The SET is able to establish communication with the H-SLP
   iii. In the case of batch reporting, the conditions for sending have arisen or the SET has obtained the last fix according to the number of fixes (in which case an incomplete batch of positions is sent).

   The SUPL REPORT message is used to send all or a subset of stored position fixes and/or stored enhanced cell/sector measurements not previously reported to the H-SLP. In the case of batch reporting, the stored position estimates and/or stored enhanced cell/sector measurements included in the SUPL REPORT message may be chosen according to criteria received in step F. If no criteria are

received in step F, the SET shall include all stored position estimates and/or stored enhanced cell/sector measurements not previously reported.

S. If enhanced cell/sector measurements are received in step R, the H-SLP calculates corresponding position estimates. The H-SLP forwards the reported and/or calculated historical position estimate(s) to the SUPL Agent in an MLP TLREP message. As an option (e.g. if the SUPL Agent is not available), the H-SLP could retain the historic position fixes for later retrieval by the SUPL Agent

T. After the last position result has been reported to the SUPL Agent in step S or following some timeout on not receiving stored position estimates in step R, the H-SLP ends the periodic triggered session by sending a SUPL END message to the SET.

5.1.7.2 Roaming with V-SLP Positioning Successful Case

SUPL Roaming where the V-SLP is involved in the positioning calculation.

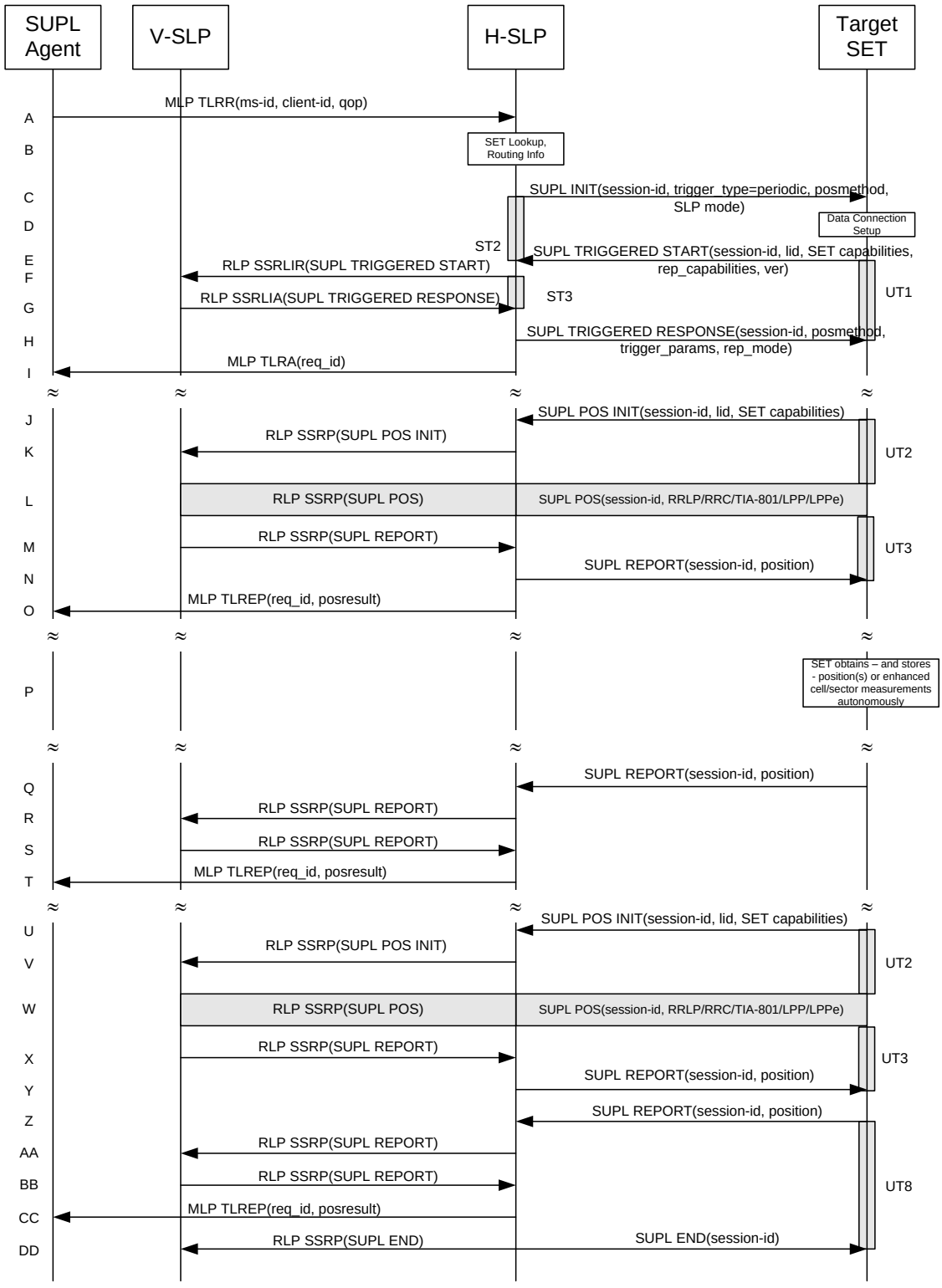

Figure 8: Network Initiated Periodic Trigger Service Roaming with V-SLP Positioning Successful Case – Proxy Mode

NOTE: See Appendix D for timer descriptions.

A. SUPL Agent issues an MLP TLRR message to the H-SLP, with which SUPL Agent is associated. The H-SLP shall authenticate the SUPL Agent and check if the SUPL Agent is authorized for the service it requests, based on the client-id received. Further, based on the received ms-id the H-SLP shall apply subscriber privacy against the client-id. The TLRR message may indicate that batch reporting or quasi-real time reporting is to be used instead of real time reporting. In the case of batch reporting, the TLRR indicates the conditions for sending batch reports to the H-SLP and any criteria, when the conditions for sending arise, for including or excluding particular stored position estimates (e.g. QoP, time window).

B. The H-SLP verifies that the target SET is currently SUPL roaming.
The H-SLP MAY also verify that the target SET supports SUPL.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside the scope of SUPL. However, there are various environment dependent mechanisms.

NOTE: Alternatively, the H-SLP may determine whether the SET is SUPL roaming in a later step using the location identifier (lid) received from the SET.

NOTE: The specifics for determining if the SET supports SUPL are beyond SUPL 2.0 scope.

C. The H-SLP initiates the periodic trigger session with the SET using the SUPL INIT message. The SUPL INIT message contains at least session-id, trigger type indicator (in this case periodic), proxy/non-proxy mode indicator and the intended positioning method. If the result of the privacy check in Step A indicates that notification or verification to the target subscriber is needed, the H-SLP SHALL also include the Notification element in the SUPL INIT message. Before the SUPL INIT message is sent, the H-SLP also computes and stores a hash of the message.

D. The SET analyses the received SUPL INIT. If found to be non authentic SET takes not further actions. Otherwise the SET takes needed action preparing for establishment or resumption of a secure connection.

E. The SET will evaluate the Notification rules and follow the appropriate actions. The SET also checks the proxy/non-proxy mode indicator to determine if the H-SLP uses proxy or non-proxy mode. In this case, proxy mode is used, and the SET SHALL establish a secure connection to the H-SLP using SLP address that has been provisioned by the Home Network to the SET.
The SET then sends a SUPL TRIGGERED START message to start a periodic triggered session with the H-SLP. The SET SHALL send the SUPL TRIGGERED START message even if the SET supported positioning technologies do not include the intended positioning method indicated in the SUPL INIT message. The SUPL TRIGGERED START message contains at least session-id, SET capabilities, a hash of the received SUPL INIT message (ver), Location ID (lid) and reporting capabilities (rep_capabilities). The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe). The rep_capabilities parameter indicates whether the SET is capable of batch reporting, real time reporting and/or quasi-real time reporting.

F. Based on the received lid or other mechanisms, the H-SLP determines the V-SLP and sends an RLP SSRLIR including the SUPL TRIGGERED START message to the V-SLP to inform the V-SLP that the target SET will initiate a SUPL positioning procedure.

G. Consistent with the SET capabilities received in step F, the V-SLP selects the intended positioning method to be used for the periodic triggered session and indicates its readiness for a periodic triggered session by sending a SUPL TRIGGERED RESPONSE message back to the H-SLP in a RLP SSRLIA message.

H. The H-SLP forwards the received SUPL TRIGGERED RESPONSE message to the SET including session-id, posmethod and periodic trigger parameters. Consistent with the rep_capabilities of the SET, the H-SLP also indicates the reporting mode (rep_mode parameter) to be used by the SET: real time reporting, quasi-real time reporting or batch reporting. In the case of batch reporting, the SUPL TRIGGERED RESPONSE message indicates the conditions for sending batch reports to the H-SLP and any criteria, when the conditions for sending arise, for including or excluding particular stored position estimates and/or (if allowed) particular stored enhanced cell/sector measurements. In the case of quasi-real time reporting, the SUPL TRIGGERED RESPONSE message indicates whether the SET is allowed to send enhanced cell/sector measurements in lieu of or in addition to position estimates. If enhanced cell/sector positioning was selected for batch or quasi-real time reporting, the SUPL TRIGGERED RESPONSE message indicates if the SET is permitted to send stored enhanced cell/sector measurements. In this case, if batch reporting was selected the SET MAY skip steps J to N.

I. The H-SLP informs the SUPL Agent in an MLP TLRA message that the triggered location response request has been accepted and also includes a req_id parameter to be used as a transaction id for the entire duration of the periodic triggered session. The SET and the H-SLP MAY release the secure connection.

NOTE: The MLP TLRA may be sent earlier at any time after the H-SLP receives the MLP TLRR.

J. When the periodic trigger in the SET indicates that a position fix has to be performed, the SET attaches itself to the Packet Data Network if it is not already attached or establishes a circuit switched data connection. The SET then sends a SUPL POS INIT message to the H-SLP to start a positioning session with the V-SLP. The SUPL POS INIT message contains at least session-id, the Location ID (lid) and the SET capabilities parameter. The SET MAY provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if this is supported. The SET MAY set the Requested Assistance Data element in the SUPL POS INIT.
If the SUPL POS INIT message contains a position that meets the required QoP, the H-SLP MAY directly proceed to step N.

K. The H-SLP forwards the SUPL POS INIT message to the V-SLP using a RLP SSRP message.
If a position calculated based on information received in the SUPL POS INIT message is available (e.g. a cell-id based position fix) that meets the required QoP, the V-SLP MAY directly proceed to step M and not engage in a SUPL POS session.

L. The SET and the V-SLP exchange several successive positioning procedure messages, tunnelled over RLP via the H-SLP.
The V-SLP calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance obtained from the V-SLP (SET-Based).

M. Once the position calculation is complete, the V-SLP sends a SUPL REPORT message including the postion to the H-SLP in an RLP tunnel using an SSRP message.

N. Once the position calculation is complete the H-SLP sends the SUPL REPORT message to the SET informing it that the positioning procedure is completed. The SET MAY release the secure connection to the H-SLP. If the reporting mode is batch reporting, the SET stores all calculated position estimates. In SET Assisted mode the position is calculated by the V-SLP and therefore needs to be included in the message for batch reporting mode.

If a SET Based positioning method was chosen which allows the SET to autonomously calculate a position estimate (e.g. autonomous GPS or A-GPS SET Based mode where the SET has current GPS assistance data and does not require an assistance data update from the H-SLP) steps J to N are not performed. Instead, the SET autonomously calculates the position estimate and – for real time or quasi-real time reporting – sends the calculated position estimate to the H-SLP using a SUPL REPORT message containing the session-id and the position estimate.

O. This step is optional: once the position calculation is complete and if real time or quasi-real time reporting is used, the H-SLP forwards the received position estimate from the V-SLP in an MLP TLREP message to the SUPL Agent. The MLP TLREP message includes the req_id and the position result. If the reporting mode is set to batch reporting, this message is not used.

P. This step is optional: if the SET cannot communicate with the H-SLP (e.g. no radio coverage available) and quasi-real time reporting is used or if batch reporting is used, the SET MAY – if supported – perform SET Based position fixes (autonomous GPS or SET Based A-GPS where the SET has current assistance data) and/or, if allowed by the H-SLP, enhanced cell/sector measurements. In the case of batch reporting, and if explicitly allowed by the H-SLP, enhanced cell/sector measurements are permitted even when the SET can communicate with the H-SLP.

Q. This step is optional and is executed if batch reporting is used and if any of the conditions for sending batch reports have occurred. It is also executed, once the SET is able to re-establish communication with the H-SLP, if quasi-real time reporting is used if one or more previous reports have been missed. The SET sends the stored position estimates and/or, if allowed, the stored enhanced cell/sector measurements in an unsolicited SUPL REPORT message to the H-SLP. The SUPL REPORT message contains the session-id and the position result(s) including data and time information for each position result and optionally the position method used. In the case of batch reporting, the stored position estimates and/or enhanced cell/sector measurements included in the SUPL REPORT message may be chosen according to criteria received in step H. If no criteria are received in step H, the SET shall include all stored position estimates and/or enhanced cell/sector measurements not previously reported.

R. This step is optional: if in step Q the SET sent enhanced cell/sector measurements, the H-SLP needs to engage the help of the V-SLP to translate the enhanced cell/sector measurements into actual position estimates. To this end the

H-SLP sends the received enhanced cell/sector measurements in a SUPL REPORT message to the V-SLP using an SSRP message over RLP tunnel.

S. This step is optional and only takes place if step R has occurred: after receiving the enhanced cell/sector measurements the V-SLP calculates the actual position estimates and returns them in a SUPL REPORT message to the H-SLP using an SSRP message over RLP tunnel.

T. The H-SLP forwards the reported and/or calculated position estimate(s) to the SUPL Agent in an MLP TLREP message.

Steps J to T are repeated as applicable. When the last position estimate needs to be calculated i.e. the end of the periodic triggered session has been reached, steps U to Y may be performed (a repeat of steps J to N). Alternatively – and if applicable – step P is repeated.

Z. This step is optional. When real-time reporting is used, it is executed after the last position estimate or, if allowed, last set of enhanced cell/sector measurements has been obtained or was due. When batch or quasi real-time reporting is used, step Z is executed if and as soon as the following conditions apply:

   i. The SET has stored historic location reports and/or stored historic enhanced cell/sector measurements that have not yet been sent to the H-SLP.

   ii. The SET is able to establish communication with the H-SLP.

   iii. In the case of batch reporting, the conditions for sending have arisen or the SET has obtained the last fix according to the number of fixes (in which case an incomplete batch of positions is sent).

The SUPL REPORT message is used to send all or a subset of stored position fixes and/or stored enhanced cell/sector measurements not previously reported to the H-SLP. In the case of batch reporting, the stored position estimates and/or stored enhanced cell/sector measurements included in the SUPL REPORT message may be chosen according to criteria received in step H. If no criteria are received in step H, the SET shall include all stored position estimates and/or stored enhanced cell/sector measurements not previously reported.

AA. This step is optional: if in step Z the SET sent enhanced cell/sector measurements, the H-SLP needs to engage the help of the V-SLP to translate the enhanced cell/sector measurements into actual position estimates. To this end the H-SLP sends the received enhanced cell/sector measurements in a SUPL REPORT message to the V-SLP using an SSRP message over RLP tunnel.

BB. This step is optional and only takes place if step AA has occurred: after receiving the enhanced cell/sector measurements the V-SLP calculates the actual position estimates and returns them in a SUPL REPORT message to the H-SLP using an SSRP message over RLP tunnel.

CC. The H-SLP forwards the reported and/or calculated historical position estimate(s) to the SUPL Agent in an MLP TLREP message. As an option (e.g. if the SUPL Agent is not available), the H-SLP could retain the historic position fixes for later retrieval by the SUPL Agent.

DD. After the last position result has been reported to the SUPL Agent in step CC, or following some timeout on not receiving stored position estimates in step Z, the H-SLP ends the periodic triggered session by sending a SUPL END message to the SET and informs the V-SLP about the end of the periodic triggered session by sending a SUPL END message using an RLP SSRP tunnel message to the V-SLP.

5.1.7.3 Roaming with H-SLP Positioning Successful Case

SUPL Roaming where the H-SLP is involved in the positioning calculation.

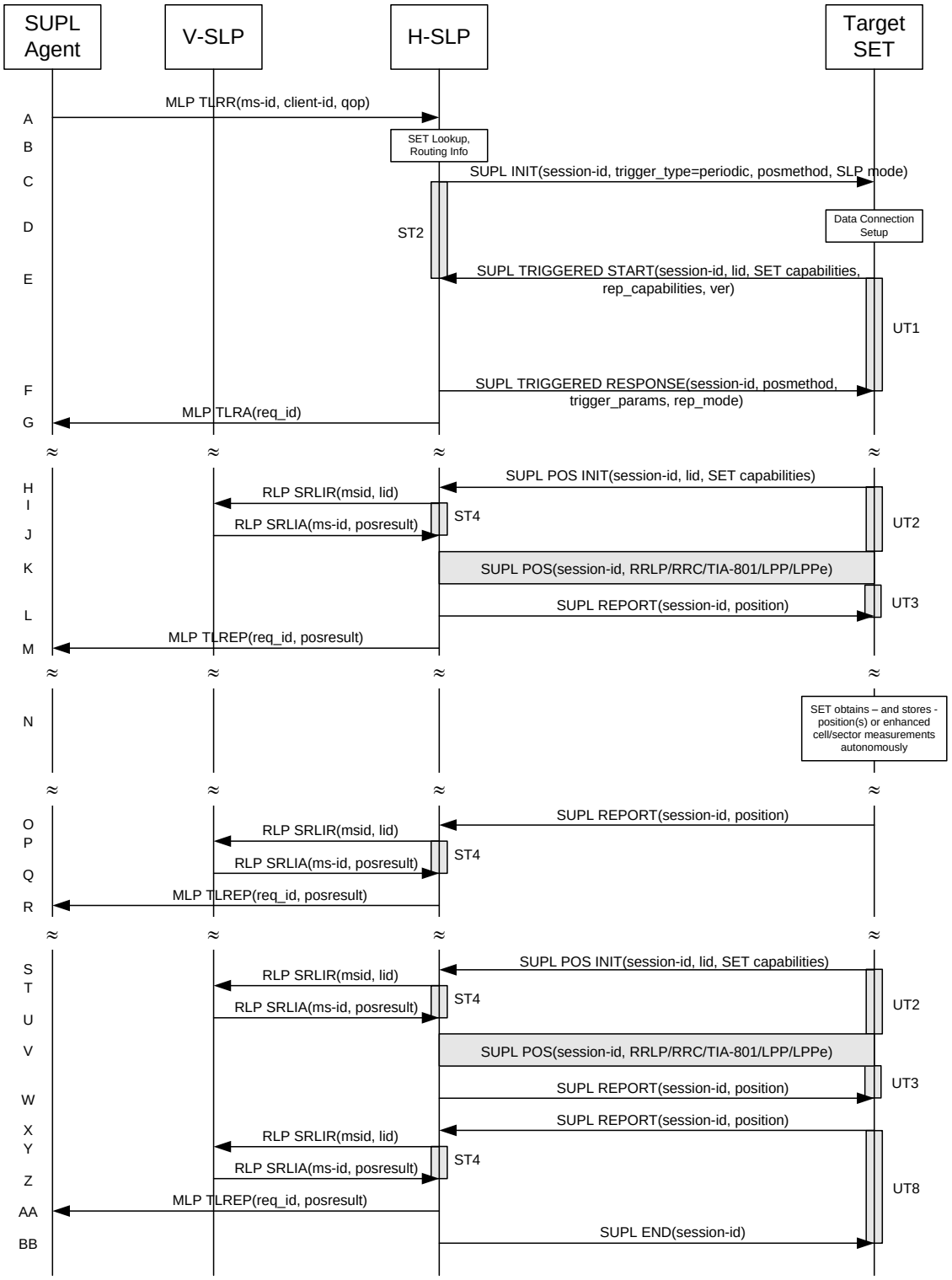

Figure 9: Network Initiated Periodic Trigger Service Roaming with H-SLP Positioning Successful Case – Proxy Mode

NOTE: See Appendix D for timer descriptions

A. SUPL Agent issues an MLP TLRR message to the H-SLP, with which SUPL Agent is associated. The H-SLP shall authenticate the SUPL Agent and check if the SUPL Agent is authorized for the service it requests, based on the client-id received. Further, based on the received ms-id the H-SLP shall apply subscriber privacy against the client-

id. The TLRR message may indicate that batch reporting or quasi-real time reporting is to be used instead of real time reporting. In the case of batch reporting, the TLRR indicates the conditions for sending batch reports to the H-SLP and any criteria, when the conditions for sending arise, for including or excluding particular stored position estimates (e.g. QoP, time window).

B. The H-SLP verifies that the target SET is currently SUPL roaming.
The H-SLP MAY also verify that the target SET supports SUPL.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside the scope of SUPL. However, there are various environment dependent mechanisms.

NOTE: Alternatively, the H-SLP may determine whether the SET is SUPL roaming in a later step using the location identifier (lid) received from the SET.

NOTE: The specifics for determining if the SET supports SUPL are beyond SUPL 2.0 scope.

C. The H-SLP initiates the periodic trigger session with the SET using the SUPL INIT message. The SUPL INIT message contains at least session-id, trigger type indicator (in this case periodic), proxy/non-proxy mode indicator and the intended positioning method. If the result of the privacy check in Step A indicates that notification or verification to the target subscriber is needed, the H-SLP SHALL also include the Notification element in the SUPL INIT message. Before the SUPL INIT message is sent, the H-SLP also computes and stores a hash of the message.

D. The SET analyses the received SUPL INIT. If found to be non authentic SET takes not further actions. Otherwise the SET takes needed action preparing for establishment or resumption of a secure connection.

E. The SET will evaluate the Notification rules and follow the appropriate actions. The SET also checks the proxy/non-proxy mode indicator to determine if the H-SLP uses proxy or non-proxy mode. In this case, proxy mode is used, and the SET SHALL establish a secure connection to the H-SLP using SLP address that has been provisioned by the Home Network to the SET.
The SET then sends a SUPL TRIGGERED START message to start a periodic triggered session with the H-SLP. The SET SHALL send the SUPL TRIGGERED START message even if the SET supported positioning technologies do not include the intended positioning method indicated in the SUPL INIT message. The SUPL TRIGGERED START message contains at least session-id, SET capabilities, a hash of the received SUPL INIT message (ver), Location ID (lid) and reporting capabilities (rep_capabilities). The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe). The rep_capabilities parameter indicates whether the SET is capable of batch reporting, real-time reporting and/or quasi-real time reporting.

F. Consistent with the SET capabilities received in step E the H-SLP selects the intended positioning method to be used for the periodic triggered session and indicates its readiness for a periodic triggered session by sending a SUPL TRIGGERED RESPONSE message back to the SET. The SUPL TRIGGERED RESPONSE message to the SET includes at a minimum the session-id, posmethod and periodic trigger parameters. Consistent with the rep_capabilities of the SET, the H-SLP also indicates the reporting mode (rep_mode parameter) to be used by the SET: real time reporting, quasi-real time reporting or batch reporting. In the case of batch reporting, the SUPL TRIGGERED RESPONSE message indicates the conditions for sending batch reports to the H-SLP and any criteria, when the conditions for sending arise, for including or excluding particular stored position estimates and/or (if allowed) particular stored enhanced cell/sector measurements. In the case of quasi-real time reporting, the SUPL TRIGGERED RESPONSE message indicates whether the SET is allowed to send enhanced cell/sector measurements in lieu of or in addition to position estimates. If enhanced cell/sector positioning was selected for batch or quasi-real time reporting, the SUPL TRIGGERED RESPONSE message indicates if the SET is permitted to send stored enhanced cell/sector measurements. In this case, if batch reporting was selected, the SET MAY skip steps H to L.

G. The H-SLP informs the SUPL Agent in an MLP TLRA message that the triggered location response request has been accepted and also includes a req_id parameter to be used as a transaction id for the entire duration of the periodic triggered session. The SET and the H-SLP MAY release the secure connection.

NOTE: The MLP TLRA may be sent earlier at any time after the H-SLP receives the MLP TLRR.

H. When the periodic trigger in the SET indicates that a position fix has to be performed, the SET attaches itself to the Packet Data Network if it is not already attached or establishes a circuit switched data connection. The SET then sends a SUPL POS INIT message to the H-SLP to start a positioning session with the H-SLP. The SUPL POS INIT

message contains at least session-id, the Location ID (lid) and the SET capabilities parameter. The SET MAY provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if this is supported. The SET MAY set the Requested Assistance Data element in the SUPL POS INIT.
If the SUPL POS INIT message contains a position that meets the required QoP, the H-SLP MAY directly proceed to step L and not engage in a SUPL POS session

I. To obtain a coarse position based on lid received in step H, the H-SLP sends an RLP SRLIR message to the V-SLP.

J. The V-SLP translates the received lid into a position estimate and returns the result to the H-SLP in an RLP SRLIA message.
If the received position estimate meets the required QoP, the H-SLP MAY directly proceed to step L and not engage in a SUPL POS session.

K. The SET and the H-SLP exchange several successive positioning procedure messages.
The H-SLP calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance obtained from the H-SLP (SET-Based).

L. Once the position calculation is complete the H-SLP sends the SUPL REPORT message to the SET informing it that the positioning procedure is completed. The SET MAY release the secure connection to the H-SLP. If the reporting mode is batch reporting, the SET stores all calculated position estimates. In SET Assisted mode the position is calculated by the H-SLP and therefore needs to be included in the message for batch reporting mode.

If a SET Based positioning method was chosen which allows the SET to autonomously calculate a position estimate (e.g. autonomous GPS or A-GPS SET Based mode where the SET has current GPS assistance data and does not require an assistance data update from the H-SLP) steps H to L are not performed. Instead, the SET autonomously calculates the position estimate and – for real time or quasi-real time reporting – sends the calculated position estimate to the H-SLP using a SUPL REPORT message containing the session-id and the position estimate.

M. This step is optional: once the position calculation is complete and if real time or quasi-real time reporting is used, the H-SLP sends a MLP TLREP message to the SUPL Agent. The MLP TLREP message includes the req_id and the position result. If the reporting mode is set to batch reporting, this message is not used.

N. This step is optional: if the SET cannot communicate with the H-SLP (e.g. no radio coverage available) and quasi-real time reporting is used or if batch reporting is used, the SET MAY – if supported – perform SET Based position fixes (autonomous GPS or SET Based A-GPS where the SET has current assistance data) and/or, if allowed by the H-SLP, enhanced cell/sector measurements. In the case of batch reporting, and if explicitly allowed by the H-SLP, enhanced cell/sector measurements are permitted even when the SET can communicate with the H-SLP.

O. This step is optional and is executed if batch reporting is used and if any of the conditions for sending batch reports have occurred. It is also executed, once the SET is able to re-establish communication with the H-SLP, if quasi-real time reporting is used if one or more previous reports have been missed. The SET sends the stored position estimates and/or, if allowed, the stored enhanced cell/sector measurements in an unsolicited SUPL REPORT message to the H-SLP. The SUPL REPORT message contains the session-id and the position result(s) including data and time information for each position result and optionally the position method used. In the case of batch reporting, the stored position estimates and/or enhanced cell/sector measurements included in the SUPL REPORT message may be chosen according to criteria received in step F. If no criteria are received in step F, the SET shall include all stored position estimates and/or enhanced cell/sector measurements not previously reported.

P. This step is optional: if in step O the SET sent enhanced cell/sector measurements, the H-SLP needs to engage the help of the V-SLP to translate the enhanced cell/sector measurements into actual position estimates. To this end the H-SLP sends an RLP SRLIR message to the V-SLP.

Q. This step is optional and only takes place if step P has occurred: The V-SLP translates the received enhanced cell/sector measurements into position estimates and returns the results to the H-SLP in an RLP SRLIA message.

R. The H-SLP forwards the reported and/or calculated position estimate(s) to the SUPL Agent in an MLP TLREP message.

Steps H to R are repeated as applicable. When the last position estimate needs to be calculated i.e. the end of the periodic triggered session has been reached, steps S to W may be performed (a repeat of steps H to L). Alternatively – and if applicable – step N is repeated

X. This step is optional. When real-time reporting is used, it is executed after the last position estimate or, if allowed, last set of enhanced cell/sector measurements has been obtained or was due. When batch or quasi real-time reporting is used, step X is executed if and as soon as the following conditions apply:

    i. The SET has stored historic location reports and/or stored historic enhanced cell/sector measurements that have not yet been sent to the H-SLP.

    ii. The SET is able to establish communication with the H-SLP.

    iii. In the case of batch reporting, the conditions for sending have arisen or the SET has obtained the last fix according to the number of fixes (in which case an incomplete batch of positions is sent).

The SUPL REPORT message is used to send all or a subset of stored position fixes and/or stored enhanced cell/sector measurements not previously reported to the H-SLP. In the case of batch reporting, the stored position estimates and/or stored enhanced cell/sector measurements included in the SUPL REPORT message may be chosen according to criteria received in step F. If no criteria are received in step F, the SET shall include all stored position estimates and/or stored enhanced cell/sector measurements not previously reported.

Y. This step is optional: if in step X the SET sent enhanced cell/sector measurements, the H-SLP needs to engage the help of the V-SLP to translate the enhanced cell/sector measurements into actual position estimates. To this end the H-SLP sends an RLP SRLIR message to the V-SLP.

Z. This step is optional and only takes place if step Y has occurred: after receiving the enhanced cell/sector measurements the V-SLP translates the received enhanced cell/sector measurements into position estimates and returns the results to the H-SLP in an RLP SRLIA message.

AA. The H-SLP forwards the reported and/or calculated historical position estimate(s) to the SUPL Agent in an MLP TLREP message. As an option (e.g. if the SUPL Agent is not available), the H-SLP could retain the historic position fixes for later retrieval by the SUPL Agent.

BB. After the last position result has been reported to the SUPL Agent in step AA or following some timeout on not receiving stored position estimates in step X, the H-SLP ends the periodic triggered session by sending a SUPL END message to the SET.

5.1.8 Network Initiated Proxy Mode – Triggered Services: Event Trigger

This section describes the call flows for Network Initiated area event triggered services for proxy mode. The trigger thereby resides in the SET and the SET makes the decision if an area event occurred based on continuously repeated position determinations.

5.1.8.1 Non-Roaming Successful Case

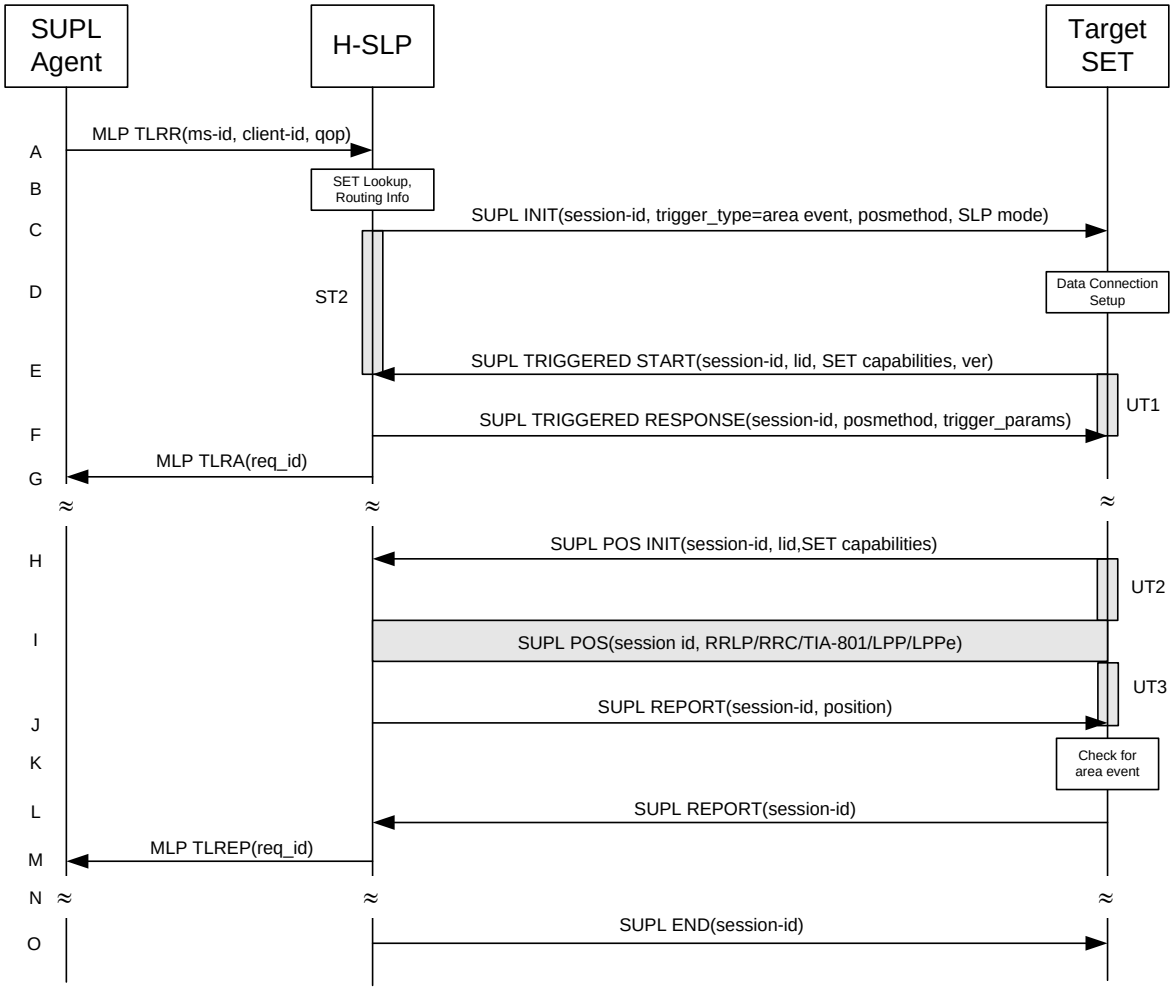

Figure 10: Network Initiated Area Event Trigger Service Non-Roaming Successful Case – Proxy Mode

NOTE: See Appendix D for timer descriptions

A. SUPL Agent issues an MLP TLRR message to the H-SLP, with which SUPL Agent is associated. The H-SLP shall authenticate the SUPL Agent and check if the SUPL Agent is authorized for the service it requests, based on the client-id received. Further, based on the received ms-id the H-SLP shall apply subscriber privacy against the client-id.

B. The H-SLP verifies that the target SET is currently not SUPL roaming.
The H-SLP MAY also verify that the target SET supports SUPL.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside the scope of SUPL. However, there are various environment dependent mechanisms.

NOTE: Alternatively, the H-SLP may determine whether the SET is SUPL roaming in a later step using the location identifier (lid) received from the SET.

NOTE: The specifics for determining if the SET supports SUPL are beyond SUPL 2.0 scope.

C. The H-SLP initiates the area event trigger session with the SET using the SUPL INIT message. The SUPL INIT message contains at least session-id, trigger type indicator (in this case area event), proxy/non-proxy mode indicator and the intended positioning method. If the result of the privacy check in Step A indicates that notification or verification to the target subscriber is needed, the H-SLP SHALL also include the Notification element in the SUPL INIT message. Before the SUPL INIT message is sent, the H-SLP also computes and stores a hash of the message.

D. The SET analyses the received SUPL INIT. If found to be non authentic SET takes not further actions. Otherwise the SET takes needed action preparing for establishment or resumption of a secure connection.

E. The SET will evaluate the Notification rules and follow the appropriate actions. The SET also checks the proxy/non-proxy mode indicator to determine if the H-SLP uses proxy or non-proxy mode. In this case, proxy mode is used, and the SET SHALL establish a secure connection to the H-SLP using SLP address that has been provisioned by the Home Network to the SET.
The SET then sends a SUPL TRIGGERED START message to start an area event triggered session with the H-SLP. The SET SHALL send the SUPL TRIGGERED START message even if the SET supported positioning technologies do not include the intended positioning method indicated in the SUPL INIT message. The SUPL TRIGGERED START message contains at least session-id, SET capabilities, a hash of the received SUPL INIT message (ver) and Location ID (lid). The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe).

F. Consistent with the SET capabilities received in the SUPL TRIGGERED START message the H-SLP selects the intended positioning method to be used for the area event triggered session and responds with a SUPL TRIGGERED RESPONSE message including session-id, posmethod and area event trigger parameters. The SUPL TRIGGERED RESPONSE message may contain the area ids of the specified area for the area event triggered session.

G. The H-SLP informs the SUPL Agent in an MLP TLRA message that the triggered location response request has been accepted and also includes a req_id parameter to be used as a transaction id for the entire duration of the area event triggered session. The SET and the H-SLP MAY release the secure connection.

NOTE: The MLP TLRA may be sent earlier at any time after the H-SLP receives the MLP TLRR.

H. If the area ids are downloaded in step F, the SET SHALL compare the current area id to the downloaded area ids. When the area event trigger mechanism in the SET or the comparison of the current area id to the downloaded area ids indicates that a position fix is to be executed, the SET attaches itself to the Packet Data Network if it is not already attached or establishes a circuit switched data connection. The SET then sends a SUPL POS INIT message to start a positioning session with the H-SLP. The SUPL POS INIT message contains at least session-id and the Location ID (lid), and the SET capabilities parameter. The SET MAY provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if this is supported. The SET MAY set the Requested Assistance Data element in the SUPL POS INIT.
If a position calculated based on information received in the SUPL POS INIT message is available (e.g. a cell-id based position fix) that meets the required QoP, the H-SLP MAY directly proceed to step J and not engage in a SUPL POS session.

I. The SET and the H-SLP exchange several successive positioning procedure messages.
The H-SLP calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance obtained from the H-SLP (SET-Based).

J. Once the position calculation is complete the H-SLP sends a SUPL REPORT message to the SET. The SET MAY release the secure connection to the H-SLP.
The SUPL REPORT message includes the position result if the position estimate is calculated in the H-SLP and therefore needs to be sent to the SET.

K. The SET compares the calculated position estimate with the event area to check if the event trigger condition has been met. If no area event is triggered, the SET SHALL return to step H. If area event is triggered SET SHALL proceed to step L.

L. The SET sends a SUPL REPORT message including the session id and the position estimate to the H-SLP unless the Location estimate parameter is set to “false” in which case no position estimate is included..

M. The H-SLP sends a MLP TLREP message to the SUPL Agent which may include the position result.

N. If SUPL Agent has requested several reports and more reports are to be sent, the SET repeats step H to M or step H to K depending on if the area event condition is fulfilled or not. Note that in this case, step L occurs only after the minimum time between reports has elapsed.

O. When the last report has been sent the H-SLP ends the area event triggered session by sending a SUPL END message to the SET

The call flow described in Figure 10 is applicable to all positioning methods. However, individual steps within the call flows are optional:

- Step I (SUPL POS) is not performed for cell-id based positioning methods.
- In A-GPS SET Based mode where no GPS assistance data is required from the network, no interaction with the H-SLP is required to calculate a position estimate. Interaction with the H-SLP is only required for GPS assistance data update in which case steps H to J are performed.

5.1.8.2 Roaming with V-SLP Positioning Successful Case

SUPL Roaming where the V-SLP is involved in the positioning calculation.

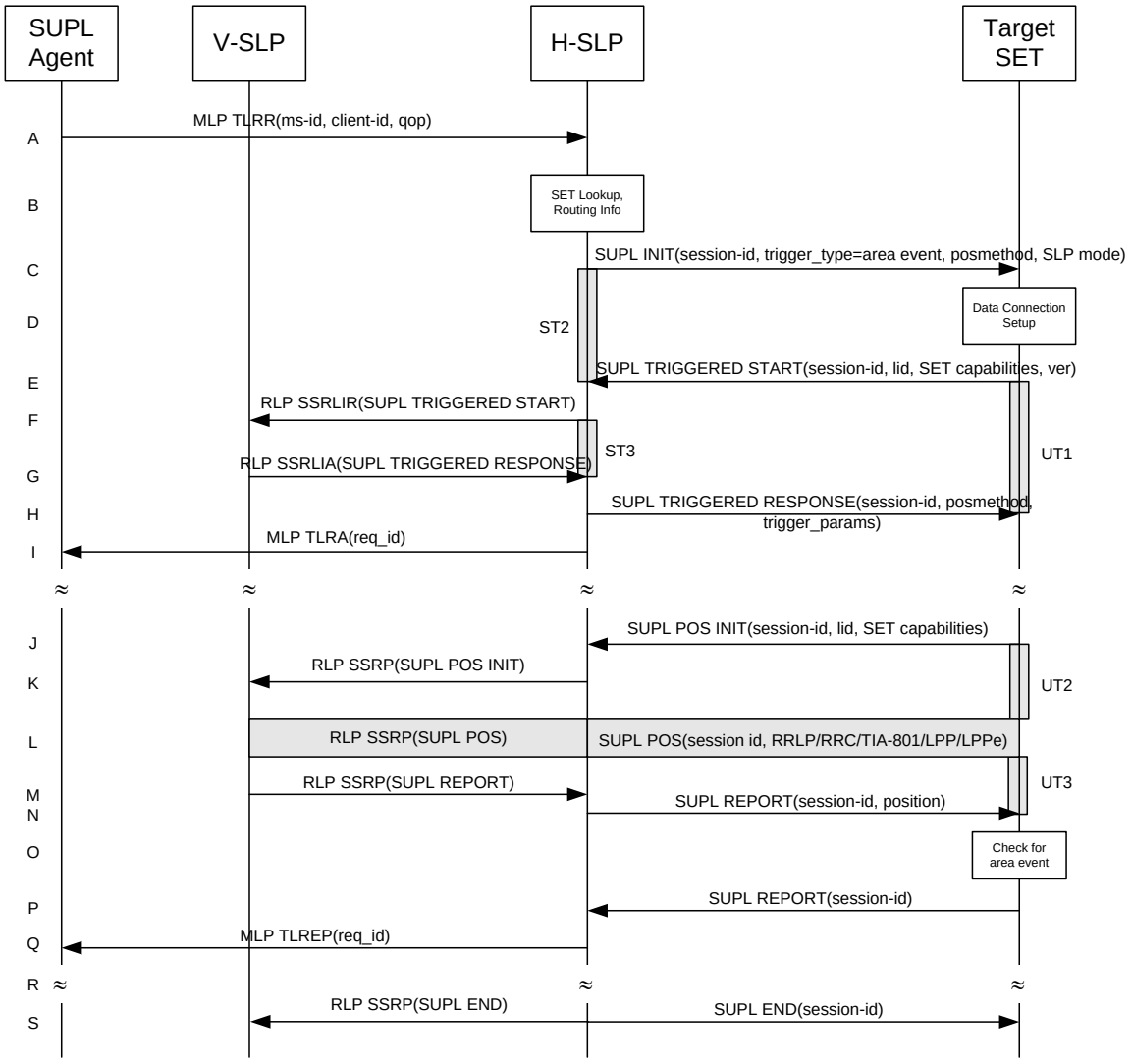

Figure 11: Network Initiated Area Event Trigger Service Roaming with V-SLP Positioning Successful Case – Proxy Mode

NOTE: See Appendix D for timer descriptions

A. SUPL Agent issues an MLP TLRR message to the H-SLP, with which SUPL Agent is associated. The H-SLP shall authenticate the SUPL Agent and check if the SUPL Agent is authorized for the service it requests, based on the client-id received. Further, based on the received ms-id the H-SLP shall apply subscriber privacy against the client-id.

B. The H-SLP verifies that the target SET is currently SUPL roaming.
The H-SLP MAY also verify that the target SET supports SUPL.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside the scope of SUPL. However, there are various environment dependent mechanisms.

NOTE: Alternatively, the H-SLP may determine whether the SET is SUPL roaming in a later step using the location identifier (lid) received from the SET.

NOTE: The specifics for determining if the SET supports SUPL are beyond SUPL 2.0 scope.

C. The H-SLP initiates the area event trigger session with the SET using the SUPL INIT message. The SUPL INIT message contains at least session-id, trigger type indicator (in this case area event), proxy/non-proxy mode indicator and the intended positioning method. If the result of the privacy check in Step A indicates that notification or verification to the target subscriber is needed, the H-SLP SHALL also include the Notification element in the SUPL INIT message. Before the SUPL INIT message is sent, the H-SLP also computes and stores a hash of the message.

D. The SET analyses the received SUPL INIT. If found to be non authentic SET takes not further actions. Otherwise the SET takes needed action preparing for establishment or resumption of a secure connection.

E. The SET will evaluate the Notification rules and follow the appropriate actions. The SET also checks the proxy/non-proxy mode indicator to determine if the H-SLP uses proxy or non-proxy mode. In this case, proxy mode is used, and the SET SHALL establish a secure connection to the H-SLP using SLP address that has been provisioned by the Home Network to the SET.
The SET then sends a SUPL TRIGGERED START message to start an area event triggered session with the H-SLP. The SET SHALL send the SUPL TRIGGERED START message even if the SET supported positioning technologies do not include the intended positioning method indicated in the SUPL INIT message. The SUPL TRIGGERED START message contains at least session-id, SET capabilities, a hash of the received SUPL INIT message (ver) and Location ID (lid). The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe).

F. The H-SLP sends an RLP SSRLIR including the SUPL TRIGGERED START message to the V-SLP to inform the V-SLP that the target SET will initiate a SUPL positioning procedure. The area event trigger parameters such as area information requested by SUPL Agent for the area event triggered session MAY be included in this message by the H-SLP.

G. Consistent with the SET capabilities received in step F, the V-SLP determines the intended positioning method to be used for the area event triggered session and indicates its readiness for an area event triggered session by sending a SUPL TRIGGERED RESPONSE message back to the H-SLP in a RLP SSRLIA message. The V-SLP MAY include area ids corresponding to the area for the area event trigger session in the SUPL TRIGGERED RESPONSE message.

H. The H-SLP forwards the received SUPL TRIGGERED RESPONSE message to the SET including session-id, posmethod and area event trigger parameters. The SUPL TRIGGERED RESPONSE message may contain the area ids of the specified area for the area event triggered session.

I. The H-SLP informs the SUPL Agent in an MLP TLRA message that the triggered location response request has been accepted and also includes a req_id parameter to be used as a transaction id for the entire duration of the area event triggered session. The SET and the H-SLP MAY release the secure connection.

NOTE: The MLP TLRA may be sent earlier at any time after the H-SLP receives the MLP TLRR.

J. If the area ids are downloaded in step H, the SET SHALL compare the current area id to the downloaded area ids. When the area event trigger in the SET or the comparison of the current area id to the downloaded area ids indicates that a position fix has to be performed, the SET attaches itself to the Packet Data Network if it is not already attached or establishes a circuit switched data connection. The SET then sends a SUPL POS INIT message to the H-SLP to start a positioning session with the V-SLP. The SUPL POS INIT message contains at least session-id and the Location ID (lid) and the SET capabilities parameter. The SET MAY provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if this is supported. The SET MAY set the Requested Assistance Data element in the SUPL POS INIT.

If a position is received in the SUPL POS INIT message that meets the required QoP, the H-SLP MAY directly proceed to step N and not engage in a SUPL POS session.

K. The H-SLP forwards the SUPL POS INIT message to the V-SLP using a RLP SSRP message.
If a position calculated based on information received in the SUPL POS INIT message is available (e.g. a cell-id based position fix) that meets the required QoP, the V-SLP MAY directly proceed to step M and not engage in a SUPL POS session.

L. The SET and the V-SLP exchange several successive positioning procedure messages, tunnelled over RLP via the H-SLP.
The V-SLP calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance obtained from the V-SLP (SET-Based).

M. Once the position calculation is complete, the V-SLP sends a SUPL REPORT message to the H-SLP carried within an RLP SSRP message.
The SUPL REPORT message includes the position estimate if the position estimate is calculated in the V-SLP and therefore needs to be sent to the SET.

N. The H-SLP forwards the received SUPL REPORT message to the SET. The SET MAY release the secure connection to the H-SLP.
The SUPL REPORT message includes the position estimate if the position estimate is calculated in the V-SLP (or the H-SLP) and therefore needs to be sent to the SET.

O. The SET compares the calculated position estimate with the event area to check if the event trigger condition has been met. If no area event is triggered, the SET SHALL return to step J. If area event is triggered SET SHALL proceed to step P.

P. The SET sends a SUPL REPORT message including the session id and the position estimate to the H-SLP unless the Location estimate parameter is set to “false” in which case no position estimate is included.

Q. The H-SLP sends a MLP TLREP message to the SUPL Agent which may include the position result.

R. If SUPL Agent has requested several report and more reports are to be sent, the SET repeats step J to Q or step J to O depending on if the area event condition is fulfilled or not. Note that in this case, step P occurs only after the minimum time between reports has elapsed.

S. When the last report has been sent the H-SLP ends the area event triggered session by sending a SUPL END message to the SET and by sending a SUPL END message using an RLP SSRP tunnel message to the V-SLP.

The call flow described in Figure 11 is applicable to all positioning methods. However, individual steps within the call flows are optional:

- Step L (SUPL POS) is not performed for cell-id based positioning methods.
- In A-GPS SET Based mode where no GPS assistance data is required from the network, no interaction with the H-SLP is required to calculate a position estimate. Interaction with the H-SLP is only required for GPS assistance data update in which case steps J to N are performed.

5.1.8.3 Roaming with H-SLP Positioning Successful Case

SUPL Roaming where the H-SLP is involved in the positioning calculation.

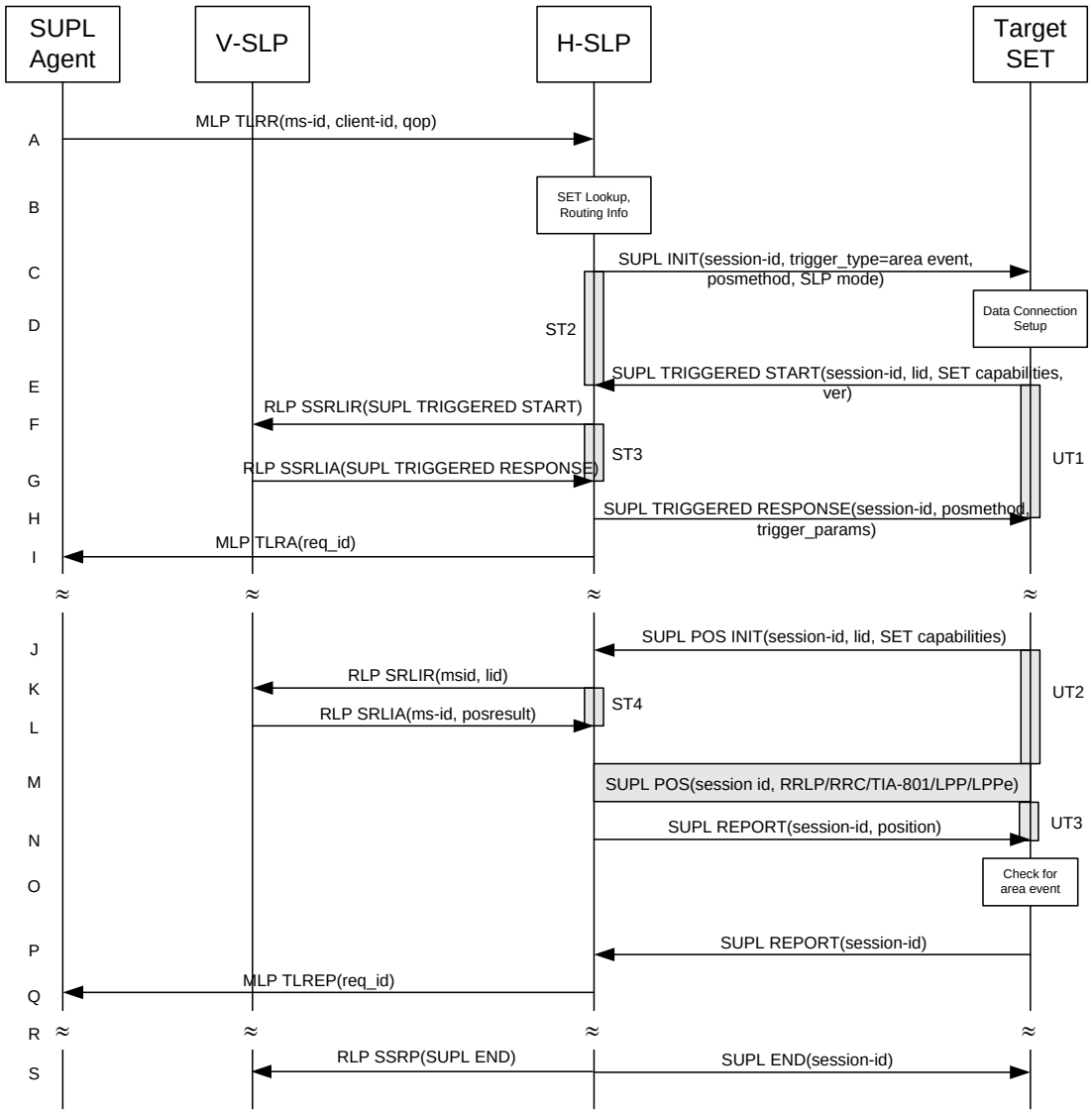

Figure 12: Network Initiated Area Event Trigger Service Roaming with H-SLP Positioning Successful Case – Proxy Mode

NOTE: See Appendix D for timer descriptions

A. SUPL Agent issues an MLP TLRR message to the H-SLP, with which SUPL Agent is associated. The H-SLP shall authenticate the SUPL Agent and check if the SUPL Agent is authorized for the service it requests, based on the client-id received. Further, based on the received ms-id the H-SLP shall apply subscriber privacy against the client-id.

B. The H-SLP verifies that the target SET is currently SUPL roaming.
The H-SLP MAY also verify that the target SET supports SUPL.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside the scope of SUPL. However, there are various environment dependent mechanisms.

NOTE: Alternatively, the H-SLP may determine whether the SET is SUPL roaming in a later step using the location identifier (lid) received from the SET.

NOTE: The specifics for determining if the SET supports SUPL are beyond SUPL 2.0 scope.

C. The H-SLP initiates the area event trigger session with the SET using the SUPL INIT message. The SUPL INIT message contains at least session-id, trigger type indicator (in this case area event), proxy/non-proxy mode indicator and the intended positioning method. If the result of the privacy check in Step A indicates that notification or verification to the target subscriber is needed, the H-SLP SHALL also include the Notification element in the SUPL INIT message. Before the SUPL INIT message is sent, the H-SLP also computes and stores a hash of the message.

D. The SET analyses the received SUPL INIT. If found to be non authentic SET takes not further actions. Otherwise the SET takes needed action preparing for establishment or resumption of a secure connection.

E. The SET will evaluate the Notification rules and follow the appropriate actions. The SET also checks the proxy/non-proxy mode indicator to determine if the H-SLP uses proxy or non-proxy mode. In this case, proxy mode is used, and the SET SHALL establish a secure connection to the H-SLP using SLP address that has been provisioned by the Home Network to the SET.
The SET then sends a SUPL TRIGGERED START message to start an area event triggered session with the H-SLP. The SET SHALL send the SUPL TRIGGERED START message even if the SET supported positioning technologies do not include the intended positioning method indicated in the SUPL INIT message. The SUPL TRIGGERED START message contains at least session-id, SET capabilities, a hash of the received SUPL INIT message (ver) and Location ID (lid). The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe).

F. Based on the received lid or other mechanisms, the H-SLP determines the V-SLP and sends an RLP SSRLIR including a SUPL TRIGGERED START to the V-SLP to inform the V-SLP that an area event triggered session is in the progress of being initiated with the H-SLP. The area event trigger parameters such as area information requested by SUPL Agent for the area event triggered session MAY be included in this message by the H-SLP.

G. The V-SLP acknowledges the RLP request received in step F with a SUPL TRIGGERED RESPONSE message which is carried inside an RLP SSRLIA message. The V-SLP MAY include area ids corresponding to the area for the area event trigger session in the SUPL TRIGGERED RESPONSE message.

H. Consistent with the SET capabilities received in step E, the H-SLP determines the intended positioning method to be used for the area event triggered session and indicates its readiness for an area event triggered session by sending a SUPL TRIGGERED RESPONSE message back to the SET. The SUPL TRIGGERED RESPONSE message to the SET includes at a minimum the session-id, posmethod and area event trigger parameters. The SUPL TRIGGERED RESPONSE message may contain the area ids of the specified area for the area event triggered session.

I. The H-SLP informs the SUPL Agent in an MLP TLRA message that the triggered location response request has been accepted and also includes a req_id parameter to be used as a transaction id for the entire duration of the area event triggered session. The SET and the H-SLP MAY release the secure connection.

NOTE: The MLP TLRA may be sent earlier at any time after the H-SLP receives the MLP TLRR.

J. If the area ids are downloaded in step H, the SET SHALL compare the current area id to the downloaded area ids. When the area event trigger in the SET or the comparison of the current area id to the downloaded area ids indicates that a position fix has to be performed, the SET attaches itself to the Packet Data Network if it is not already attached or establishes a circuit switched data connection. The SET then sends a SUPL POS INIT message to the H-SLP to start a positioning session with the H-SLP. The SUPL POS INIT message contains at least session-id and the Location ID (lid) and the SET capabilities parameter. The SET MAY provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if this is supported. The SET MAY set the Requested Assistance Data element in the SUPL POS INIT.
If the SUPL POS INIT message contains a position that meets the required QoP, the H-SLP MAY directly proceed to step N.

K. To obtain a coarse position based on lid received in step J, the H-SLP sends an RLP SRLIR message to the V-SLP.

L. The V-SLP translates the received lid into a position estimate and returns the result to the H-SLP in an RLP SRLIA message.
If the position estimate meets the required QoP, the H-SLP MAY directly proceed to step N and not engage in a SUPL POS session.

M. The SET and the H-SLP exchange several successive positioning procedure messages.
The H-SLP calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance obtained from the H-SLP (SET-Based).

N. Once the position calculation is complete, the H-SLP sends a SUPL REPORT message to the SET. The SET MAY release the secure connection to the H-SLP.
The SUPL REPORT message includes the position estimate if the position estimate is calculated in the H-SLP (or V-SLP) and therefore needs to be sent to the SET.

O. The SET compares the calculated position estimate with the event area to check if the event trigger condition has been met. If no area event is triggered, the SET SHALL return to step J. If area event is triggered SET SHALL proceed to step P.

P. The SET sends a SUPL REPORT message including the session id and the position estimate to the H-SLP unless the Location estimate parameter is set to "false" in which case no position estimate is included.

Q. The H-SLP sends a MLP TLREP message to the SUPL Agent which may include the position result.

R. If SUPL Agent has requested several report and more reports are to be sent, the SET repeats step J to Q or step J to O depending on if the area event condition is fulfilled or not. Note that in this case, step P occurs only after the minimum time between reports has elapsed.

S. When the last report has been sent the H-SLP ends the area event triggered session by sending a SUPL END message to the SET and by sending a SUPL END message using an RLP SSRP tunnel message to the V-SLP.

The call flow described in Figure 12 is applicable to all positioning methods. However, individual steps within the call flows are optional:

- Step M (SUPL POS) is not performed for cell-id based positioning methods.
- In A-GPS SET Based mode where no GPS assistance data is required from the network, no interaction with the H-SLP is required to calculate a position estimate. Interaction with the H-SLP is only required for GPS assistance data update in which case steps J to N are performed.

5.1.9 Network Initiated Non-Proxy Mode – Triggered Services: Periodic Triggers

This section describes the call flows for Network Initiated periodic triggered services for non-proxy mode. The trigger thereby resides in the SET.

5.1.9.1 Non-Roaming Successful Case

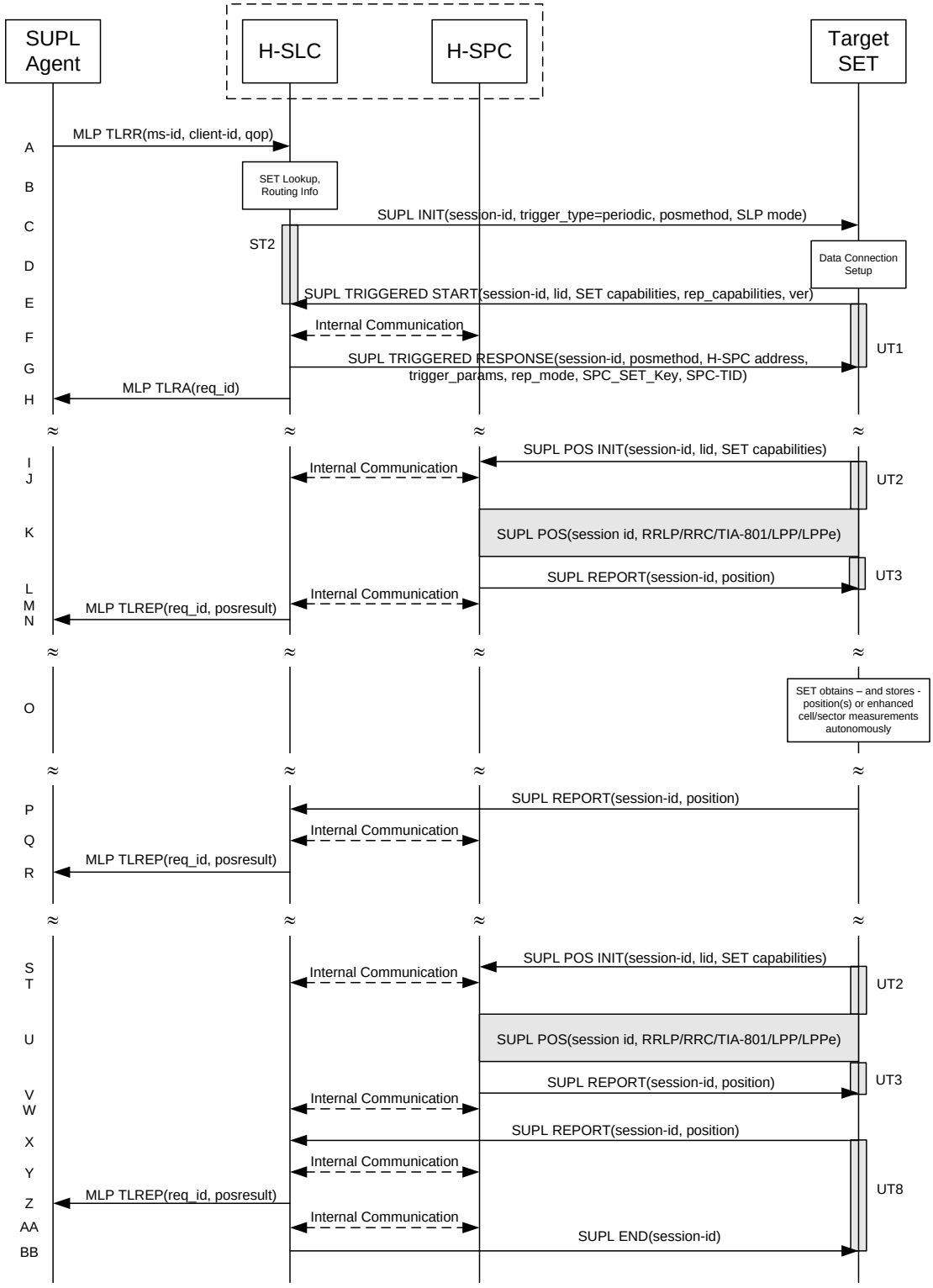

Figure 13: Network Initiated Periodic Trigger Service Non-Roaming Successful Case – Non-Proxy Mode

NOTE: See Appendix D for timer descriptions.

A. SUPL Agent issues an MLP TLRR message to the H-SLC, with which SUPL Agent is associated. The H-SLC shall authenticate the SUPL Agent and check if the SUPL Agent is authorized for the service it requests, based on the client-id received. Further, based on the received ms-id the H-SLC shall apply subscriber privacy against the client-id. The TLRR message may indicate that batch reporting or quasi-real time reporting is to be used instead of real time reporting. In the case of batch reporting, the TLRR indicates the conditions for sending batch reports to the H-SLC and any criteria, when the conditions for sending arise, for including or excluding particular stored position estimates (e.g. QoP, time window).

B. The H-SLC verifies that the target SET is currently not SUPL roaming.
The H-SLC MAY also verify that the target SET supports SUPL.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside the scope of SUPL. However, there are various environment dependent mechanisms.

NOTE: Alternatively, the H-SLC may determine whether the SET is SUPL roaming in a later step using the location identifier (lid) received from the SET.

NOTE: The specifics for determining if the SET supports SUPL are beyond SUPL 2.0 scope.

C. The H-SLC initiates the periodic trigger session with the SET using the SUPL INIT message. The SUPL INIT message contains at least session-id, trigger type indicator (in this case periodic), proxy/non-proxy mode indicator and the intended positioning method. If the result of the privacy check in Step A indicates that notification or verification to the target subscriber is needed, the H-SLC SHALL also include the Notification element in the SUPL INIT message. Before the SUPL INIT message is sent, the H-SLC also computes and stores a hash of the message.

D. The SET analyses the received SUPL INIT. If found to be non authentic SET takes not further actions. Otherwise the SET takes needed action preparing for establishment or resumption of a secure connection.

E. The SET will evaluate the Notification rules and follow the appropriate actions. The SET also checks the proxy/non-proxy mode indicator to determine if the H-SLP uses proxy or non-proxy mode. In this case, non-proxy mode is used, and the SET SHALL establish a secure connection to the H-SLC using the H-SLC address which has been provisioned by the Home Network to the SET.
The SET then sends a SUPL TRIGGERED START message to start a periodic triggered session with the H-SLP. The SET SHALL send the SUPL TRIGGERED START message even if the SET supported positioning technologies do not include the intended positioning method indicated in the SUPL INIT message. The SUPL TRIGGERED START message contains at least session-id, SET capabilities, a hash of the received SUPL INIT message (ver), Location ID (lid) and reporting capabilities (rep_capabilities). The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe). The rep_capabilities parameter indicates whether the SET is capable of batch reporting, real-time reporting and/or quasi-real time reporting.

F. The H-SLC informs the H-SPC through internal communication about the periodic triggered session. The H-SLC generates SPC_SET_Key and SPC-TID to be used for mutual H-SPC/SET authentication and forwards both to the H-SPC through internal communication. The H-SPC grants or denies the request and informs the H-SLC accordingly.

G. Consistent with the SET capabilities received in the SUPL TRIGGERED START message the H-SLC selects the intended positioning method to be used for the periodic triggered session and responds with a SUPL TRIGGERED RESPONSE message including session-id, posmethod, H-SPC address, periodic trigger parameters and SPC_SET_Key and SPC-TID. Consistent with the rep_capabilities of the SET, the H-SLC also indicates the reporting mode (rep_mode parameter) to be used by the SET: real time reporting, quasi-real time reporting or batch reporting. In the case of batch reporting, the SUPL TRIGGERED RESPONSE message indicates the conditions for sending batch reports to the H-SLC and any criteria, when the conditions for sending arise, for including or excluding particular stored position estimates and/or (if allowed) particular stored enhanced cell/sector measurements. In the case of quasi-real time reporting, the SUPL TRIGGERED RESPONSE message indicates whether the SET is allowed to send enhanced cell/sector measurements in lieu of or in addition to position estimates. If enhanced cell/sector positioning was selected for batch or quasi-real time reporting, the SUPL TRIGGERED RESPONSE message indicates if the SET is permitted to send stored enhanced cell/sector measurements. In this case, if batch reporting was selected, the SET MAY skip steps I to L.

H. The H-SLC informs the SUPL Agent in an MLP TLRA message that the triggered location response request has been accepted and also includes a req_id parameter to be used as a transaction id for the entire duration of the periodic triggered session.
The SET and the H-SLC MAY release the secure connection.

NOTE: The MLP TLRA may be sent earlier at any time after the H-SLP receives the MLP TLRR.

I. When the periodic trigger in the SET indicates that a position fix has to be performed, the SET attaches itself to the Packet Data Network if it is not already attached or establishes a circuit switched data connection. The SET then sends a SUPL POS INIT message to start a positioning session with the H-SPC. The SUPL POS INIT message contains at least session-id, the Location ID (lid) and the SET capabilities parameter. The SET MAY provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if this is supported. The SET MAY set the Requested Assistance Data element in the SUPL POS INIT.
If a position calculated based on information received in the SUPL POS INIT message is available (e.g. a cell-id based position fix) that meets the required QoP, the H-SPC MAY directly proceed to step L and not engage in a SUPL POS session.

J. Through internal communication the H-SPC may request a coarse position from the H-SLC based on the lid received in the SUPL POS INIT message.

K. The SET and the H-SPC exchange several successive positioning procedure messages.
The H-SPC calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance obtained from the H-SPC (SET-Based).

L. Once the position calculation is complete the H-SPC sends the SUPL REPORT message to the SET informing it that the positioning procedure is completed. The SET MAY release the secure connection to the H-SLP. If the reporting mode is batch reporting, the SET stores all calculated position estimates. In SET Assisted mode the position is calculated by the H-SPC and therefore needs to be included in the message for batch reporting mode.

M. This step is optional: Once the position calculation is complete and if real time or quasi-real time reporting is used, the H-SPC sends the position estimate through internal communication to the H-SLC.

If a SET Based positioning method was chosen which allows the SET to autonomously calculate a position estimate (e.g. autonomous GPS or A-GPS SET Based mode where the SET has current GPS assistance data and does not require an assistance data update from the H-SLP) steps I to M are not performed. Instead, the SET autonomously calculates the position estimate and – for real time or quasi-real time reporting – sends the calculated position estimate to the H-SLC using a SUPL REPORT message containing the session-id and the position estimate.

N. This step is optional: once the position calculation is complete and if real time or quasi-real time reporting is used, the H-SLC sends a MLP TLREP message to the SUPL Agent. The MLP TLREP message includes the req_id and the position result. If the reporting mode is set to batch reporting, this message is not used.

O. This step is optional: If the SET cannot communicate with the H-SLP (e.g. no radio coverage available) and quasi-real time reporting is used or if batch reporting is used, the SET MAY – if supported – perform SET Based position fixes (autonomous GPS or SET Based A-GPS where the SET has current assistance data) and/or, if allowed by the H-SLP, enhanced cell/sector measurements. In the case of batch reporting, and if explicitly allowed by the H-SLP, enhanced cell/sector measurements are permitted even when the SET can communicate with the H-SLP.

P. This step is optional and is executed if batch reporting is used and if any of the conditions for sending batch reports have occurred. It is also executed, once the SET is able to re-establish communication with the H-SLP, if quasi-real time reporting is used if one or more previous reports have been missed. The SET sends the stored position estimates and/or, if allowed, the stored enhanced cell/sector measurements in an unsolicited SUPL REPORT message to the H-SLC. The SUPL REPORT message contains the session-id and the position result(s) including date and time information for each position result and optionally the position method used. In the case of batch reporting, the stored position estimates and/or enhanced cell/sector measurements included in the SUPL REPORT message may be chosen according to criteria received in step G. If no criteria are received in step G, the SET shall include all stored position estimates and/or enhanced cell/sector measurements not previously reported.

Q. This step is optional: if the H-SLC received stored enhanced cell/sector measurements in the SUPL REPORT message in step P, the H-SPC may need to be involved to translate the enhanced cell/sector measurements into actual position estimates. To this end the H-SLC and the H-SPC may engage in internal communication.

R. The H-SLP forwards the reported and/or calculated position estimate(s) to the SUPL Agent in an MLP TLREP message.

Steps I to R are repeated as applicable. When the last position estimate needs to be calculated i.e. the end of the periodic triggered session has been reached, steps S to W may be performed (a repeat of steps I to M). Alternatively – and if applicable – step O is repeated.

X. This step is optional. When real-time reporting is used, it is executed after the last position estimate or, if allowed, last set of enhanced cell/sector measurements has been obtained or was due. When batch or quasi real-time reporting is used, step X is executed if and as soon as the following conditions apply:

   i. The SET has stored historic location reports and/or stored historic enhanced cell/sector measurements that have not yet been sent to the H-SLC.

   ii. The SET is able to establish communication with the H-SLP

   iii. In the case of batch reporting, the conditions for sending have arisen or the SET has obtained the last fix according to the number of fixes (in which case an incomplete batch of positions is sent).

   The SUPL REPORT message is used to send all or a subset of stored position fixes and/or stored enhanced cell/sector measurements not previously reported to the H-SLC. In the case of batch reporting, the stored position estimates and/or stored enhanced cell/sector measurements included in the SUPL REPORT message may be chosen according to criteria received in step G. If no criteria are received in step G, the SET shall include all stored position estimates and/or stored enhanced cell/sector measurements not previously reported.

Y. This step is optional: if the H-SLC received stored enhanced cell/sector measurements in the SUPL REPORT message in step X, the H-SPC may need to be involved to translate the enhanced cell/sector measurements into actual position estimates. To this end the H-SLC and the H-SPC may engage in internal communication.

Z. The H-SLC forwards the reported and/or calculated historical position estimate(s) to the SUPL Agent in an MLP TLREP message. As an option (e.g. if the SUPL Agent is not available), the H-SLC could retain the historic position fixes for later retrieval by the SUPL Agent.

AA. The H-SLC indicates the end of the periodic triggered session to the H-SPC through internal communication.

BB. After the last position result has been reported to the SUPL Agent in step Z, the H-SLC ends the periodic triggered session by sending a SUPL END message to the SET. Please note that if the last position was calculated in step T and step X was not performed, the SUPL END message is sent from the H-SPC to the SET (as opposed to from the H-SLC to the SET).

5.1.9.2 Roaming with V-SPC Positioning Successful Case

SUPL Roaming where the V-SPC is involved in the positioning calculation.

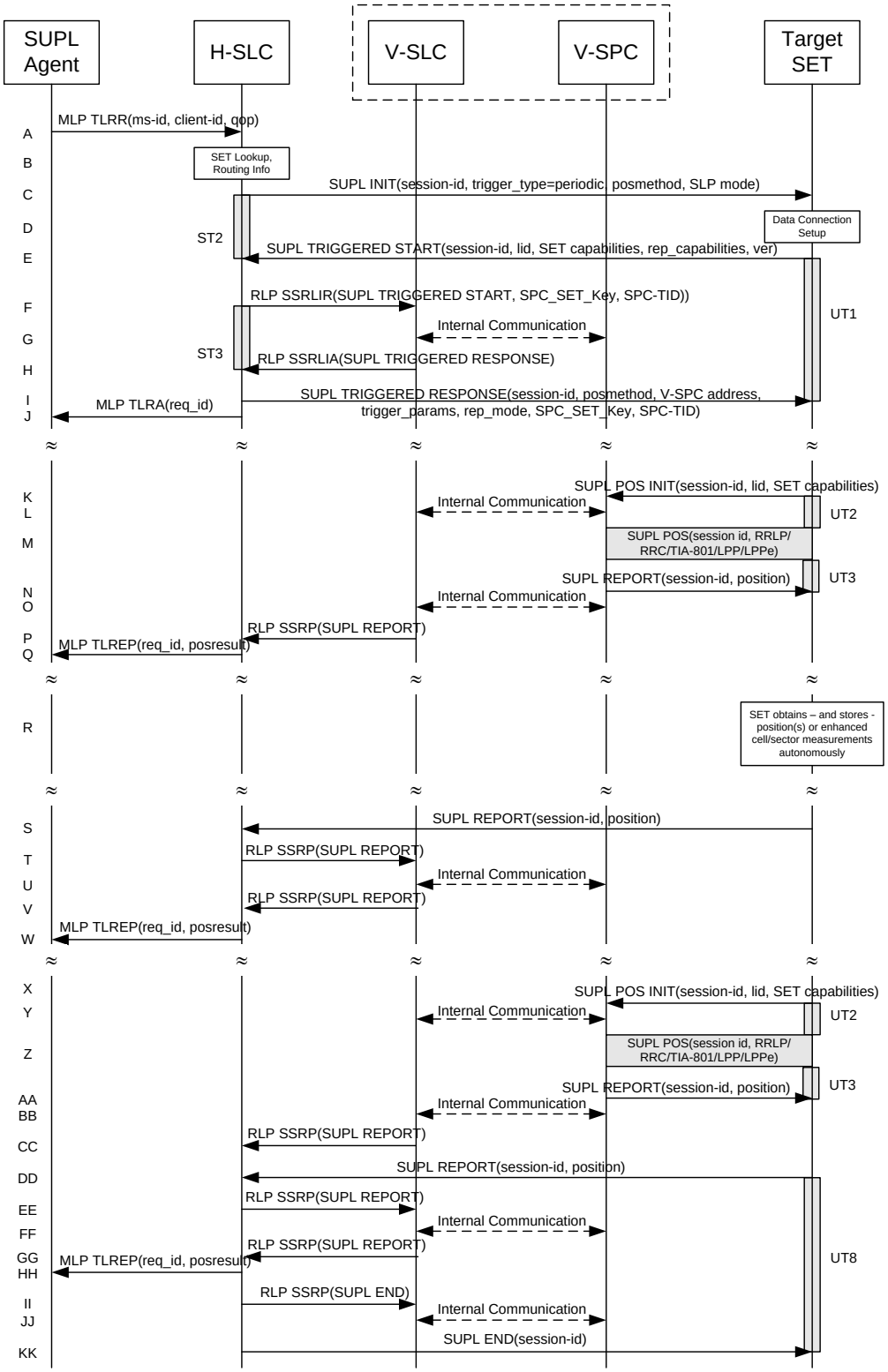

Figure 14: Network Initiated Periodic Trigger Service Roaming with V-SPC Positioning Successful Case – Non-Proxy Mode

NOTE: See Appendix D for timer descriptions.

A. SUPL Agent issues an MLP TLRR message to the H-SLC, with which SUPL Agent is associated. The H-SLC shall authenticate the SUPL Agent and check if the SUPL Agent is authorized for the service it requests, based on the client-id received. Further, based on the received ms-id the H-SLC shall apply subscriber privacy against the client-id. The TLRR message may indicate that batch reporting or quasi-real time reporting is to be used instead of real time reporting. In the case of batch reporting, the TLRR indicates the conditions for sending batch reports to the H-SLP and any criteria, when the conditions for sending arise, for including or excluding particular stored position estimates (e.g. QoP, time window).

B. The H-SLC verifies that the target SET is currently SUPL roaming.
The H-SLC MAY also verify that the target SET supports SUPL.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside the scope of SUPL. However, there are various environment dependent mechanisms.

NOTE: Alternatively, the H-SLC may determine whether the SET is SUPL roaming in a later step using the location identifier (lid) received from the SET.

NOTE: The specifics for determining if the SET supports SUPL are beyond SUPL 2.0 scope.

C. The H-SLC initiates the periodic trigger session with the SET using the SUPL INIT message. The SUPL INIT message contains at least session-id, trigger type indicator (in this case periodic), proxy/non-proxy mode indicator and the intended positioning method. If the result of the privacy check in Step A indicates that notification or verification to the target subscriber is needed, the H-SLC SHALL also include the Notification element in the SUPL INIT message. Before the SUPL INIT message is sent, the H-SLC also computes and stores a hash of the message.

D. The SET analyses the received SUPL INIT. If found to be non authentic SET takes not further actions. Otherwise the SET takes needed action preparing for establishment or resumption of a secure connection.

E. The SET will evaluate the Notification rules and follow the appropriate actions. The SET also checks the proxy/non-proxy mode indicator to determine if the H-SLC uses proxy or non-proxy mode. In this case, non-proxy mode is used, and the SET SHALL establish a secure connection to the H-SLC using the H-SLC address which has been provisioned by the Home Network to the SET.
The SET then sends a SUPL TRIGGERED START message to start a periodic triggered session with the H-SLP. The SET SHALL send the SUPL TRIGGERED START message even if the SET supported positioning technologies do not include the intended positioning method indicated in the SUPL INIT message. The SUPL TRIGGERED START message contains at least session-id, SET capabilities, a hash of the received SUPL INIT message (ver), Location ID (lid) and reporting capabilities (rep_capabilities). The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe). The rep_capabilities parameter indicates whether the SET is capable of batch reporting, real-time reporting and/or quasi-real time reporting.

F. Based on the received lid or other mechanisms, the H-SLC determines the V-SLC and sends an RLP SSRLIR message including the SUPL TRIGGERED START message to the V-SLC to inform the V-SLC that the target SET will initiate a SUPL positioning procedure. The H-SLC also generates SPC_SET_Key and SPC-TID to be used for V-SPC/SET mutual authentication and includes both in the RLP SSRLIR message.

G. The V-SLC informs the V-SPC through internal communication about the periodic triggered session. The V-SLC also forwards SPC_SET_Key and SPC-TID to the V-SPC through internal communication. The V-SPC grants or denies the request and informs the V-SLC accordingly.

H. Consistent with the SET capabilities received in step F the V-SLC selects the intended positioning method to be used for the periodic triggered session and indicates its readiness for a periodic triggered session by sending a SUPL TRIGGERED RESPONSE message back to the H-SLC in an RLP SSRLIA message.

I. The H-SLC forwards the received SUPL TRIGGERED RESPONSE message to the SET including session-id, posmethod, V-SPC address, periodic trigger parameters and SPC_SET_Key and SPC-TID. Consistent with the rep_capabilities of the SET, the H-SLC also indicates the reporting mode (rep_mode parameter) to be used by the SET: real time reporting, quasi-real time reporting or batch reporting. In the case of batch reporting, the SUPL TRIGGERED RESPONSE message indicates the conditions for sending batch reports to the H-SLC and any criteria, when the conditions for sending arise, for including or excluding particular stored position estimates and/or (if allowed) particular stored enhanced cell/sector measurements. In the case of quasi-real time reporting, the SUPL TRIGGERED RESPONSE message indicates whether the SET is allowed to send enhanced cell/sector

measurements in lieu of or in addition to position estimates. If enhanced cell/sector positioning was selected for batch or quasi-real time reporting, the SUPL TRIGGERED RESPONSE message indicates if the SET is permitted to send stored enhanced cell/sector measurements. In this case, if batch reporting was selected, the SET MAY skip steps K to N.

J. The H-SLC informs the SUPL Agent in an MLP TLRA message that the triggered location response request has been accepted and also includes a req_id parameter to be used as a transaction id for the entire duration of the periodic triggered session. The SET and the H-SLC MAY release the secure connection.

NOTE: The MLP TLRA may be sent earlier at any time after the H-SLP receives the MLP TLRR.

K. When the periodic trigger in the SET indicates that a position fix has to be performed, the SET attaches itself to the Packet Data Network if it is not already attached or establishes a circuit switched data connection. The SET then sends a SUPL POS INIT message to the V-SPC to start a positioning session with the V-SPC. The SUPL POS INIT message contains at least session-id, the Location ID (lid) and the SET capabilities parameter. The SET MAY provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if this is supported. The SET MAY set the Requested Assistance Data element in the SUPL POS INIT.
If a position calculated based on information received in the SUPL POS INIT message is available (e.g. a cell-id based position fix) that meets the required QoP, the V-SPC MAY directly proceed to step N and not engage in a SUPL POS session.

L. Through internal communication the V-SPC may request a coarse position from the V-SLC based on the lid received in the SUPL POS INIT message.

M. The SET and the V-SPC exchange several successive positioning procedure messages.
The V-SPC calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance obtained from the V-SPC (SET-Based).

N. Once the position calculation is complete the V-SPC sends the SUPL REPORT message to the SET informing it that the positioning procedure is completed. The SET MAY release the secure connection to the V-SLP. If the reporting mode is batch reporting, the SET stores all calculated position estimates. In SET Assisted mode the position is calculated by the V-SPC and therefore needs to be included in the message for batch reporting mode.

O. This step is optional: once the position calculation is complete and if real time or quasi-real time reporting is used, the V-SPC sends the position estimate through internal communication to the V-SLC.

P. This step is conditional and is only used after step O occurred. The V-SLC sends the position estimate to the H-SLC in a SUPL REPORT message. The SUPL REPORT message includes at a minimum the session-id and the position estimate. The SUPL REPORT message is carried within an RLP SSRP message.

If a SET Based positioning method was chosen which allows the SET to autonomously calculate a position estimate (e.g. autonomous GPS or A-GPS SET Based mode where the SET has current GPS assistance data and does not require an assistance data update from the V-SLP) steps K to P are not performed. Instead, the SET autonomously calculates the position estimate and – for real time or quasi-real time reporting – sends the calculated position estimate to the H-SLC using a SUPL REPORT message containing the session-id and the position estimate.

Q. This step is optional: if real time or quasi-real time reporting is used, the H-SLC forwards the position estimate received in an MLP TLREP message to the SUPL Agent. The MLP TLREP message includes the req_id and the position result. If the reporting mode is set to batch reporting, this message is not needed.

R. This step is optional: If the SET cannot communicate with the V-SLP (e.g. no radio coverage available) and quasi-real time reporting is used or if batch reporting is used, the SET MAY – if supported – perform SET Based position fixes (autonomous GPS or SET Based A-GPS where the SET has current assistance data) and/or, if allowed by the H-SLP, enhanced cell/sector measurements. In the case, of batch reporting, and if explicitly allowed by the H-SLP, enhanced cell/sector measurements are permitted even when the SET can communicate with the V-SLP.

S. This step is optional and is executed if batch reporting is used and if any of the conditions for sending batch reports have occurred. It is also executed, once the SET is able to re-establish communication with the H-SLP/V-SLP, if quasi-real time reporting is used if one or more previous reports have been missed. The SET sends the stored position estimates and/or, if allowed, the stored enhanced cell/sector measurements in an unsolicited SUPL REPORT message to the H-SLC. The SUPL REPORT message contains the session-id and the position result(s) including date and time information for each position result and optionally the position method used. In the case of batch reporting, the stored position estimates and/or enhanced cell/sector measurements included in the SUPL

REPORT message may be chosen according to criteria received in step I. If no criteria are received in step I, the SET shall include all stored position estimates and/or enhanced cell/sector measurements not previously reported.

T. This step is optional: if the H-SLC received stored enhanced cell/sector measurements in the SUPL REPORT message in step S, the V-SLP may need to be involved to translate the enhanced cell/sector measurements into actual position estimates. To this end the H-SLC sends a SUPL REPORT message to the V-SLC using an SSRP message over RLP tunnel.

U. This step is optional and only used if the V-SPC is required to translate stored enhanced cell/sector measurements received by the V-SLC into actual position estimates. In this case, internal communication between the V-SLC and the V-SPC takes place.

V. This step is conditional and takes place after step T and – optionally – step U. A SUPL REPORT message containing position estimates calculated from enhanced cell/sector measurements received in step T is sent from the V-SLC to the H-SLC using an SSRP message over RLP tunnel.

W. The H-SLC forwards the reported and/or calculated position estimate(s) to the SUPL Agent in an MLP TLREP message.

Steps K to W are repeated as applicable. When the last position estimate needs to be calculated i.e. the end of the periodic triggered session has been reached, steps X to CC may be performed (a repeat of steps K to P). Alternatively – and if applicable – step R is repeated.

DD. This step is optional. When real-time reporting is used, it is executed after the last position estimate or, if allowed, last set of enhanced cell/sector measurements has been obtained or was due. When batch or quasi real-time reporting is used, step DD is executed if and as soon as the following conditions apply:

   i. The SET has stored historic location reports and/or stored historic enhanced cell/sector measurements that have not yet been sent to the H-SLC.

   ii. The SET is able to establish communication with the H-SLP.

   iii. In the case of batch reporting, the conditions for sending have arisen or the SET has obtained the last fix according to the number of fixes (in which case an incomplete batch of positions is sent.

The SUPL REPORT message is used to send all or a subset of stored position fixes and/or stored enhanced cell/sector measurements not previously reported to the H-SLC. In the case of batch reporting, the stored position estimates and/or stored enhanced cell/sector measurements included in the SUPL REPORT message may be chosen according to criteria received in step I. If no criteria are received in step I, the SET shall include all stored position estimates and/or stored enhanced cell/sector measurements not previously reported.

EE. This step is optional: if the H-SLC received stored enhanced cell/sector measurements in the SUPL REPORT message in step DD, the V-SLP may need to be involved to translate the enhanced cell/sector measurements into actual position estimates. To this end the H-SLC sends a SUPL REPORT message to the V-SLC using an SSRP message over RLP tunnel.

FF. This step is optional and only used if the V-SPC is required to translate stored enhanced cell/sector measurements received by the V-SLC into actual position estimates. In this case, internal communication between the V-SLC and the V-SPC takes place.

GG. This step is conditional and takes place after step EE and – optionally – step FF. A SUPL REPORT message containing position estimates calculated from enhanced cell/sector measurements received in step EE is sent from the V-SLC to the H-SLC using an SSRP message over RLP tunnel.

HH. The H-SLC forwards the reported and/or calculated historical position estimate(s) to the SUPL Agent in an MLP TLREP message. As an option (e.g. if the SUPL Agent is not available), the H-SLC could retain the historic position fixes for later retrieval by the SUPL Agent.

II. The H-SLC informs the V-SLC about the end of the periodic triggered session through an SUPL END message carried within an SSRP message over RLP tunnel.

JJ. The V-SLC informs the V-SPC about the end of the periodic triggered session through internal communication.

KK. The H-SLC ends the periodic triggered session with the SET by sending a SUPL END message. The SUPL END message includes at least the session-id. Please note that if the last position was calculated in step Z and step DD was not performed, the SUPL END message is sent from the V-SPC to the SET.

5.1.9.3 Roaming with H-SPC Positioning Successful Case

SUPL Roaming where the H-SPC is involved in the positioning calculation.

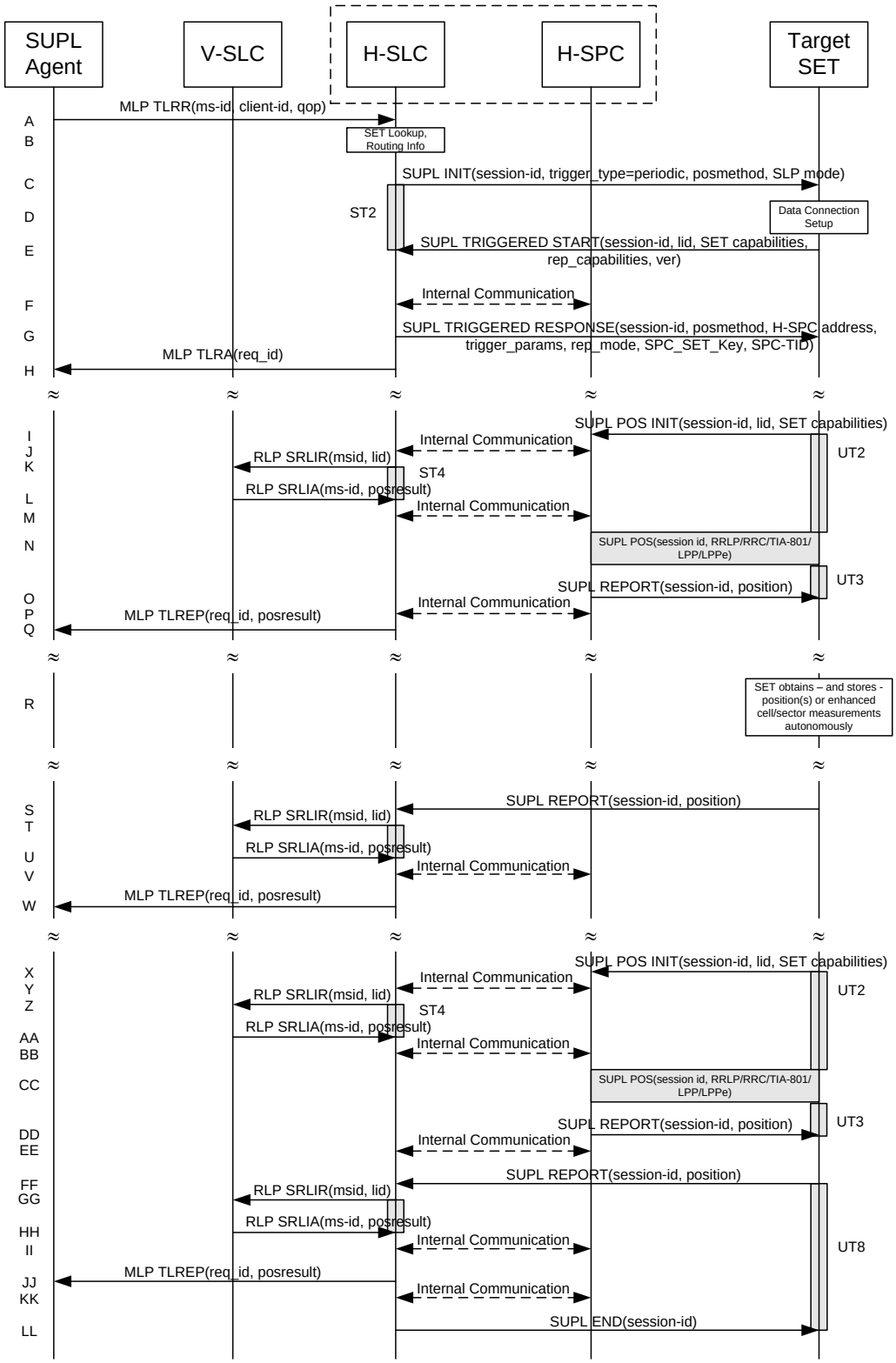

Figure 15: Network Initiated Periodic Trigger Service Roaming with H-SLP Positioning Successful Case – Non-Proxy Mode

NOTE: See Appendix D for timer descriptions

A. SUPL Agent issues an MLP TLRR message to the H-SLC, with which SUPL Agent is associated. The H-SLC shall authenticate the SUPL Agent and check if the SUPL Agent is authorized for the service it requests, based on the client-id received. Further, based on the received ms-id the H-SLC shall apply subscriber privacy against the client-id. The TLRR message may indicate that batch reporting or quasi-real time reporting is to be used instead of real time reporting. In the case of batch reporting, the TLRR indicates the conditions for sending batch reports to the H-SLP and any criteria, when the conditions for sending arise, for including or excluding particular stored position estimates (e.g. QoP, time window).

B. The H-SLC verifies that the target SET is currently SUPL roaming.
The H-SLC MAY also verify that the target SET supports SUPL.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside the scope of SUPL. However, there are various environment dependent mechanisms.

NOTE: Alternatively, the H-SLC may determine whether the SET is SUPL roaming in a later step using the location identifier (lid) received from the SET.

NOTE: The specifics for determining if the SET supports SUPL are beyond SUPL 2.0 scope.

C. The H-SLC initiates the periodic trigger session with the SET using the SUPL INIT message. The SUPL INIT message contains at least session-id, trigger type indicator (in this case periodic), proxy/non-proxy mode indicator and the intended positioning method. If the result of the privacy check in Step A indicates that notification or verification to the target subscriber is needed, the H-SLC SHALL also include the Notification element in the SUPL INIT message. Before the SUPL INIT message is sent, the H-SLC also computes and stores a hash of the message.

D. The SET analyses the received SUPL INIT. If found to be non authentic SET takes not further actions. Otherwise the SET takes needed action preparing for establishment or resumption of a secure connection.

E. The SET will evaluate the Notification rules and follow the appropriate actions. The SET also checks the proxy/non-proxy mode indicator to determine if the H-SLP uses proxy or non-proxy mode. In this case, non-proxy mode is used, and the SET SHALL establish a secure connection to the H-SLC using the H-SLC address that has been provisioned by the Home Network to the SET.
The SET then sends a SUPL TRIGGERED START message to start a periodic triggered session with the H-SLC. The SET SHALL send the SUPL TRIGGERED START message even if the SET supported positioning technologies do not include the intended positioning method indicated in the SUPL INIT message. The SUPL TRIGGERED START message contains at least session-id, SET capabilities, a hash of the received SUPL INIT message (ver), Location ID (lid) and reporting capabilities (rep_capabilities). The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe). The rep_capabilities parameter indicates whether the SET is capable of batch reporting, real-time reporting and/or quasi-real time reporting.

F. The H-SLC informs the H-SPC through internal communication about the periodic triggered session. The H-SLC generates SPC_SET_Key and SPC-TID for mutual H-SPC/SET authentication and forwards both to the H-SPC through internal communication. The H-SPC grants or denies the request and informs the H-SLC accordingly.

G. Consistent with the SET capabilities received in step E the H-SLC selects the indended positioning method to be used for the periodic triggered session and indicates its readiness for a periodic triggered session by sending a SUPL TRIGGERED RESPONSE message back to the SET. The SUPL TRIGGERED RESPONSE message to the SET includes at a minimum the session-id, posmethod, H-SPC address, periodic trigger parameters and SPC_SET_Key and SPC-TID. Consistent with the rep_capabilities of the SET, the H-SLC also indicates the reporting mode (rep_mode parameter) to be used by the SET: real time reporting, quasi-real time reporting or batch reporting. In the case of batch reporting, the SUPL TRIGGERED RESPONSE message indicates the conditions for sending batch reports to the H-SLC and any criteria, when the conditions for sending arise, for including or excluding particular stored position estimates and/or (if allowed) particular stored enhanced cell/sector measurements. In the case of quasi-real time reporting, the SUPL TRIGGERED RESPONSE message indicates whether the SET is allowed to send enhanced cell/sector measurements in lieu of or in addition to position estimates. If enhanced cell/sector positioning was selected for batch or quasi-real time reporting, the SUPL TRIGGERED RESPONSE message indicates if the SET is permitted to send stored enhanced cell/sector measurements. In this case, if batch reporting was selected, the SET MAY skip steps I to O.

H. The H-SLC informs the SUPL Agent in an MLP TLRA message that the triggered location response request has been accepted and also includes a req_id parameter to be used as a transaction id for the entire duration of the periodic triggered session. The SET and the H-SLC MAY release the secure connection.

NOTE: The MLP TLRA may be sent earlier at any time after the H-SLP receives the MLP TLRR.

I. When the periodic trigger in the SET indicates that a position fix has to be performed, the SET attaches itself to the Packet Data Network if it is not already attached or establishes a circuit switched data connection. The SET then sends a SUPL POS INIT message to the H-SPC to start a positioning session with the H-SPC. The SUPL POS INIT message contains at least session-id, the Location ID (lid) and the SET capabilities parameter. The SET MAY provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if this is supported. The SET MAY set the Requested Assistance Data element in the SUPL POS INIT.
If the SUPL POS INIT message contains a position that meets the required QoP, the H-SPC MAY directly proceed to step O.

J. Through internal communication the H-SPC requests a coarse position estimate from the H-SLC based on the lid received in step I.

K. To obtain a coarse position the H-SLC sends an RLP SRLIR message to the V-SLP.

L. The V-SLP translates the received lid into a position estimate and returns the result to the H-SLC in an RLP SRLIA message.
For real-time or quasi-real time reporting, if the returned position meets the required QoP, the H-SLC MAY directly proceed to step O and not engage in a SUPL POS session. For batch reporting, if the returned position meets the required QoP, the H-SLC MAY send the position result through internal communication to the H-SPC (step M) and the H-SPC will forward the position result to the SET using a SUPL REPORT message (step O) without engaging in a SUPL POS session (step N).

M. The H-SLC forwards the coarse position to the H-SPC through internal communication.

N. The SET and the H-SPC exchange several successive positioning procedure messages.
The H-SPC calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance obtained from the H-SPC (SET-Based).

O. Once the position calculation is complete the H-SPC sends the SUPL REPORT message to the SET informing it that the positioning procedure is completed. The SET MAY release the secure connection to the H-SLP. If the reporting mode is batch reporting, the SET stores all calculated position estimates. In SET Assisted mode the position is calculated by the H-SPC and therefore needs to be included in the message for batch reporting mode.

P. This step is optional and only used for real-time reporting: once the position calculation is complete, the H-SPC sends the position estimate to the H-SLC through internal communication.

If a SET Based positioning method was chosen which allows the SET to autonomously calculate a position estimate (e.g. autonomous GPS or A-GPS SET Based mode where the SET has current GPS assistance data and does not require an assistance data update from the H-SLP) steps I to P are not performed. Instead, the SET autonomously calculates the position estimate and – for real time or quasi-real time reporting – sends the calculated position estimate to the H-SLC using a SUPL REPORT message containing the session-id and the position estimate.

Q. This step is optional: if real time or quasi-real time reporting is used, the H-SLC forwards the calculated position estimate to the SUPL Agent in an MLP TLREP message. The MLP TLREP message includes the req_id and the position result. If the reporting mode is set to batch reporting, this message is not needed.

R. This step is optional: If the SET cannot communicate with the H-SLP (e.g. no radio coverage available) and quasi-real time reporting is used or if batch reporting is used, the SET MAY – if supported – perform SET Based position fixes (autonomous GPS or SET Based A-GPS where the SET has current assistance data) and/or, if allowed by the H-SLP, enhanced cell/sector measurements. In the case, of batch reporting, and if explicitly allowed by the H-SLP, enhanced cell/sector measurements are permitted even when the SET can communicate with the H-SLP.

S. This step is optional and is executed if batch reporting is used and if any of the conditions for sending batch reports have occurred. It is also executed, once the SET is able to re-establish communication with the H-SLP, if quasi-real time reporting is used if one or more previous reports have been missed. The SET sends the stored position estimates and/or, if allowed, the stored enhanced cell/sector measurements in an unsolicited SUPL REPORT message to the H-SLC. The SUPL REPORT message contains the session-id and the position result(s) including

date and time information for each position result and optionally the position method used. In the case of batch reporting, the stored position estimates and/or enhanced cell/sector measurements included in the SUPL REPORT message may be chosen according to criteria received in step G. If no criteria are received in step G, the SET shall include all stored position estimates and/or enhanced cell/sector measurements not previously reported.

T. This step is optional: if the H-SLC received stored enhanced cell/sector measurements in the SUPL REPORT message in step S, the V-SLP may need to be involved to translate the enhanced cell/sector measurements into actual position estimates. To this end the H-SLC sends an RLP SRLIR message to the V-SLC.

U. This step is conditional and takes place only if step T occurred. The V-SLC sends the position result calculated based on the enhanced cell/sector measurements received in step T to the H-SLC.

V. This step is optional and only takes place if after the translation into a position estimate in steps T and U the H-SPC is required to calculate the position estimate. In this case, internal communication between the H-SLC and H-SPC takes place.

W. The H-SLC forwards the reported and/or calculated position estimate(s) to the SUPL Agent in an MLP TLREP message.

Steps I to W are repeated as applicable. When the last position estimate needs to be calculated i.e. the end of the periodic triggered session has been reached, steps X to EE may be performed (a repeat of steps I to P). Alternatively – and if applicable – step R is repeated.

FF. This step is optional. When real-time reporting is used, it is executed after the last position estimate or, if allowed, last set of enhanced cell/sector measurements has been obtained or was due. When batch or quasi real-time reporting is used, step FF is executed if and as soon as the following conditions apply:

i. The SET has stored historic location reports and/or stored historic enhanced cell/sector measurements that have not yet been sent to the H-SLC.

ii. The SET is able to establish communication with the H-SLP.

iii. In the case of batch reporting, the conditions for sending have arisen or the SET has obtained the last fix according to the number of fixes (in which case an incomplete batch of positions is sent).

The SUPL REPORT message is used to send all or a subset of stored position fixes and/or stored enhanced cell/sector measurements not previously reported to the H-SLC. In the case of batch reporting, the stored position estimates and/or stored enhanced cell/sector measurements included in the SUPL REPORT message may be chosen according to criteria received in step G. If no criteria are received in step G, the SET shall include all stored position estimates and/or stored enhanced cell/sector measurements not previously reported.

GG. This step is optional: if the H-SLC received stored enhanced cell/sector measurements in the SUPL REPORT message in step FF, the V-SLP may need to be involved to translate the enhanced cell/sector measurements into actual position estimates To this end the H-SLC sends an RLP SRLIR message to the V-SLC.

HH. This step is conditional and takes place only if step GG occurred. The V-SLC sends the position result calculated based on the enhanced cell/sector measurements received in step GG to the H-SLC.

II. This step is optional and only takes place if after the translation into a position estimate in steps GG and HH the H-SPC is required to calculate the position estimate. In this case, internal communication between the H-SLC and H-SPC takes place.

JJ. The H-SLC forwards the reported and/or calculated historical position estimate(s) to the SUPL Agent in an MLP TLREP message. As an option (e.g. if the SUPL Agent is not available), the H-SLC could retain the historic position fixes for later retrieval by the SUPL Agent.

KK. Using internal communication, the H-SLC informs the H-SPC of the end of the periodic triggered session.

LL. The H-SLC ends the periodic triggered session with the SET by sending a SUPL END message. The SUPL END message includes at least the session-id. Please note that if the last position was calculated in step CC and step FF was not performed, the SUPL END message is sent from the H-SPC to the SET (as opposed to from the H-SLC to the SET).

5.1.10 Network Initiated Non-Proxy Mode – Triggered Services: Event Triggers

This section describes the call flows for Network Initiated area event triggered services for non-proxy mode. The trigger thereby resides in the SET and the SET makes the decision if an area event occurred based on continuously repeated position determinations.

5.1.10.1 Non-Roaming Successful Case

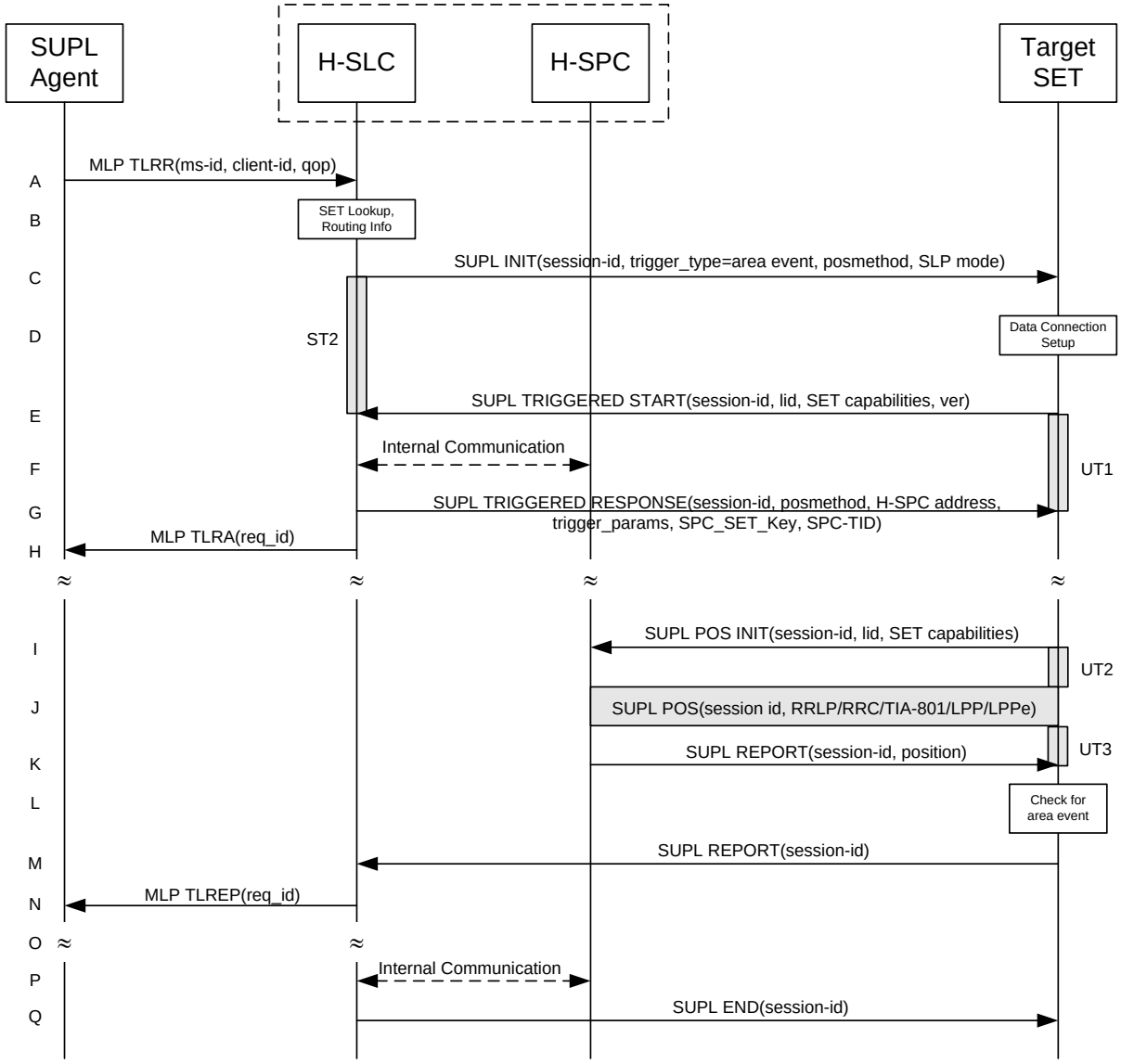

Figure 16: Network Initiated Area Event Trigger Service Non-Roaming Successful Case – Non-Proxy Mode

NOTE: See Appendix D for timer descriptions

A. SUPL Agent issues an MLP TLRR message to the H-SLC, with which SUPL Agent is associated. The H-SLC shall authenticate the SUPL Agent and check if the SUPL Agent is authorized for the service it requests, based on the client-id received. Further, based on the received ms-id the H-SLC shall apply subscriber privacy against the client-id.

B. The H-SLC verifies that the target SET is currently not SUPL roaming.
The H-SLC MAY also verify that the target SET supports SUPL.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside the scope of SUPL. However, there are various environment dependent mechanisms.

NOTE: Alternatively, the H-SLC may determine whether the SET is SUPL roaming in a later step using the location identifier (lid) received from the SET.

NOTE: The specifics for determining if the SET supports SUPL are beyond SUPL 2.0 scope.

C. The H-SLC initiates the area event trigger session with the SET using the SUPL INIT message. The SUPL INIT message contains at least session-id, trigger type indicator (in this case area event), proxy/non-proxy mode indicator and the intended positioning method. If the result of the privacy check in Step A indicates that notification or verification to the target subscriber is needed, the H-SLC SHALL also include the Notification element in the SUPL INIT message. Before the SUPL INIT message is sent, the H-SLC also computes and stores a hash of the message.

D. The SET analyses the received SUPL INIT. If found to be non authentic SET takes not further actions. Otherwise the SET takes needed action preparing for establishment or resumption of a secure connection.

E. The SET will evaluate the Notification rules and follow the appropriate actions. The SET also checks the proxy/non-proxy mode indicator to determine if the H-SLP uses proxy or non-proxy mode. In this case, non-proxy mode is used, and the SET SHALL establish a secure connection to the H-SLC using the H-SLC address which has been provisioned by the Home Network to the SET.
The SET then sends a SUPL TRIGGERED START message to start an area event triggered session with the H-SLP. The SET SHALL send the SUPL TRIGGERED START message even if the SET supported positioning technologies do not include the intended positioning method indicated in the SUPL INIT message. The SUPL TRIGGERED START message contains at least session-id, SET capabilities, a hash of the received SUPL INIT message (ver) and Location ID (lid). The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe).

F. The H-SLC informs the H-SPC through internal communication about the area event triggered session. The H-SLC generates SPC_SET_Key and SPC-TID to be used for mutual H-SPC/SET authentication and forwards both to the H-SPC through internal communication. The H-SPC grants or denies the request and informs the H-SLC.

G. Consistent with the SET capabilities received in the SUPL TRIGGERED START message the H-SLC selects the intended positioning method to be used for the area event triggered session and responds with a SUPL TRIGGERED RESPONSE message including session-id, posmethod, H-SPC address, area event trigger parameters and SPC_SET_Key and SPC-TID. The SUPL TRIGGERED RESPONSE message may contain the area ids of the specified area for the area event triggered session.

H. The H-SLC informs the SUPL Agent in an MLP TLRA message that the triggered location response request has been accepted and also includes a req_id parameter to be used as a transaction id for the entire duration of the area event triggered session.
The SET and the H-SLC MAY release the secure connection.

NOTE: The MLP TLRA may be sent earlier at any time after the H-SLP receives the MLP TLRR.

I. If the area ids are downloaded in step G, the SET SHALL compare the current area id to the downloaded area ids. When the area event trigger in the SET or the comparison of the current area id to the downloaded area ids indicates that a position fix has to be performed, the SET attaches itself to the Packet Data Network if it is not already attached or establishes a circuit switched data connection. The SET then sends a SUPL POS INIT message to start a positioning session with the H-SPC. The SUPL POS INIT message contains at least session-id and the Location ID (lid) and the SET capabilities parameter. The SET MAY provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if this is supported. The SET MAY set the Requested Assistance Data element in the SUPL POS INIT.
If a position calculated based on information received in the SUPL POS INIT message is available (e.g. a cell-id based position fix) that meets the required QoP, the H-SPC MAY directly proceed to step K and not engage in a SUPL POS session.

J. The SET and the H-SPC exchange several successive positioning procedure messages.
The H-SPC calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance obtained from the H-SPC (SET-Based).

K. Once the position calculation is complete the H-SPC sends a SUPL REPORT message to the SET. The SET MAY release the secure connection to the H-SPC.
The SUPL REPORT message includes the position result if the position estimate is calculated in the H-SPC and therefore needs to be sent to the SET.

L. The SET compares the calculated position estimate with the event area to check if the event trigger condition has been met. If no area event is triggered, the SET SHALL return to step I. If area event is triggered SET SHALL proceed to step M.

M. The SET sends a SUPL REPORT message including the session id and the position estimate to the H-SLC unless the Location estimate parameter is set to "false" in which case no position estimate is included.

N. The H-SLC sends a MLP TLREP message to the SUPL Agent which may include the position result.

O. If SUPL Agent has requested several report and more reports are to be sent, the SET repeats step I to N or step I to L depending on if the area event condition is fulfilled or not. Note that in this case, step M occurs only after the minimum time between reports has elapsed.

P. When the last report has been sent the H-SLC informs the H-SPC about the end of the area event triggered session through internal communication.

Q. The H-SLC ends the area event triggered session by sending a SUPL END message to the SET.

The call flow described in Figure 16 is applicable to all positioning methods, however, individual steps within the call flows are optional:

- Step J (SUPL POS) is not performed for cell-id based positioning methods.
- In A-GPS SET Based mode where no GPS assistance data is required from the network, no interaction with the H-SPC is required to calculate a position estimate. Interaction with the H-SPC is only required for GPS assistance data update in which case steps I to K are performed.

5.1.10.2 Roaming with V-SLP Positioning Successful Case

SUPL Roaming where the V-SLP is involved in the positioning calculation.

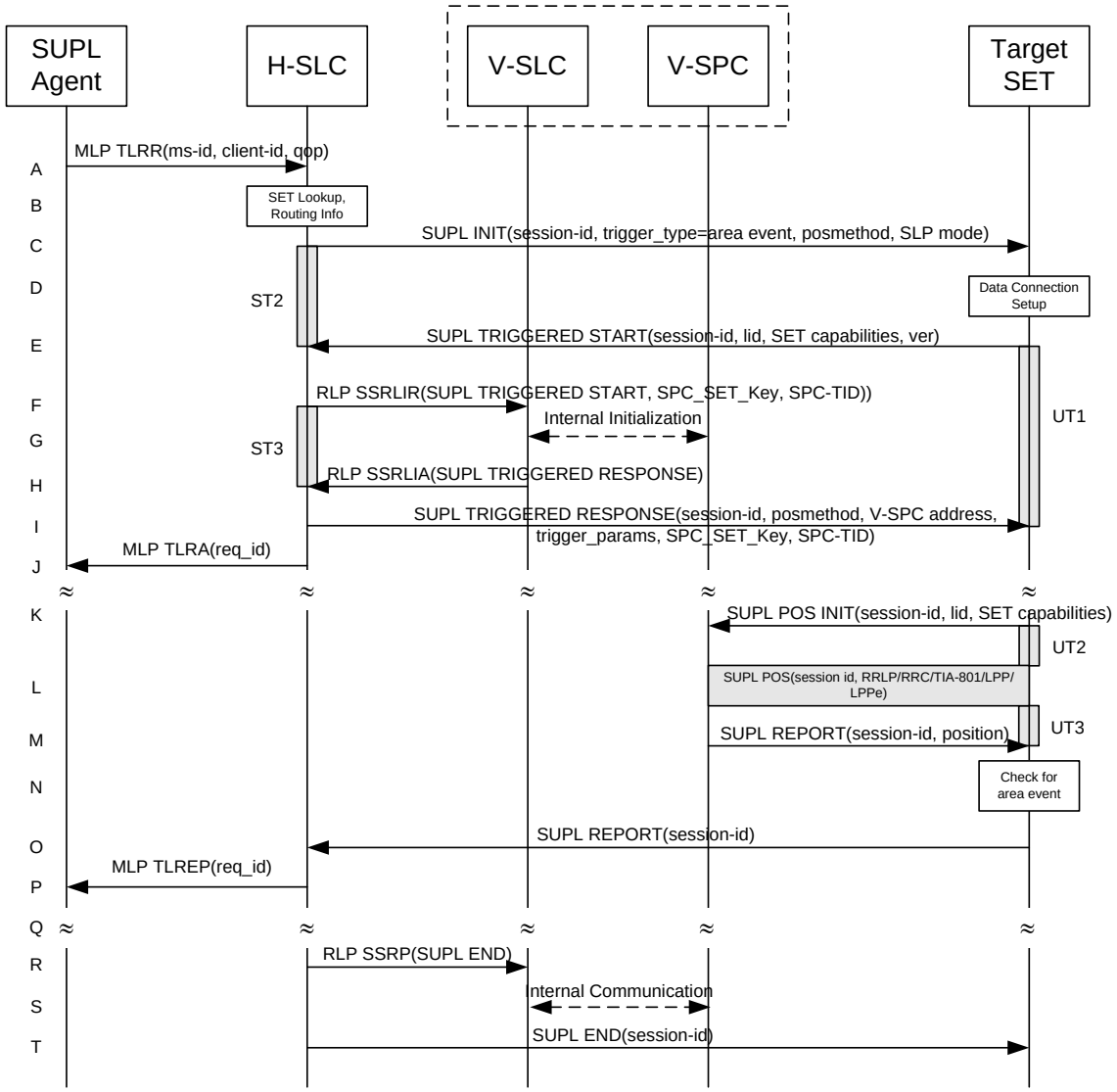

Figure 17: Network Initiated Area Event Trigger Service Roaming with V-SLP Positioning Successful Case – Non-Proxy Mode

NOTE: See Appendix D for timer descriptions.

A. SUPL Agent issues an MLP TLRR message to the H-SLC, with which SUPL Agent is associated. The H-SLC shall authenticate the SUPL Agent and check if the SUPL Agent is authorized for the service it requests, based on the client-id received. Further, based on the received ms-id the H-SLC shall apply subscriber privacy against the client-id.

B. The H-SLC verifies that the target SET is currently SUPL roaming.
The H-SLC MAY also verify that the target SET supports SUPL.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside the scope of SUPL. However, there are various environment dependent mechanisms.

NOTE: Alternatively, the H-SLC may determine whether the SET is SUPL roaming in a later step using the location identifier (lid) received from the SET.

NOTE: The specifics for determining if the SET supports SUPL are beyond SUPL 2.0 scope.

C. The H-SLC initiates the area event trigger session with the SET using the SUPL INIT message. The SUPL INIT message contains at least session-id, trigger type indicator (in this case area event), proxy/non-proxy mode indicator

and the intended positioning methods. If the result of the privacy check in Step A indicates that notification or verification to the target subscriber is needed, the H-SLC SHALL also include the Notification element in the SUPL INIT message. Before the SUPL INIT message is sent, the H-SLC also computes and stores a hash of the message.

D. The SET analyses the received SUPL INIT. If found to be non authentic SET takes not further actions. Otherwise the SET takes needed action preparing for establishment or resumption of a secure connection.

E. The SET will evaluate the Notification rules and follow the appropriate actions. The SET also checks the proxy/non-proxy mode indicator to determine if the H-SLC uses proxy or non-proxy mode. In this case, non-proxy mode is used, and the SET SHALL establish a secure connection to the H-SLC using the H-SLC address which has been provisioned by the Home Network to the SET.
The SET then sends a SUPL TRIGGERED START message to start an area event triggered session with the H-SLP. The SET SHALL send the SUPL TRIGGERED START message even if the SET supported positioning technologies do not include the intended positioning method indicated in the SUPL INIT message. The SUPL TRIGGERED START message contains at least session-id, SET capabilities, a hash of the received SUPL INIT message (ver) and Location ID (lid). The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe).

F. Based on the received lid or other mechanisms, the H-SLC determines the V-SLC and sends an RLP SSRLIR message including the SUPL TRIGGERED START message to the V-SLC to inform the V-SLC that the target SET will initiate a SUPL positioning procedure. The H-SLC also generates SPC_SET_Key and SPC-TID to be used for V-SPC/SET mutual authentication and includes both in the RLP SSRLIR message. The area event trigger parameters such as area information requested by SUPL Agent for the area event triggered session MAY be included in this message by the H-SLC.

G. The V-SLC informs the V-SPC through internal communication about the area event triggered session. The V-SLC also forwards SPC_SET_Key and SPC-TID to the V-SPC through internal communication. The V-SPC grants or denies the request and informs the V-SLC accordingly.

H. Consistent with the SET capabilities received in step F, the V-SLC determines the intended positioning method to be used for the area event triggered session and indicates its readiness for an area event triggered session by sending a SUPL TRIGGERED RESPONSE message back to the H-SLC in an RLP SSRLIA message. If area-ids are requested by the H-SLC, the V-SLC MAY include area-ids corresponding to the area for the area event trigger session in the SUPL TRIGGERED RESPONSE message.

I. The H-SLC forwards the received SUPL TRIGGERED RESPONSE message to the SET including session-id, posmethod, V-SPC address, area event trigger parameters and SPC_SET_Key and SPC-TID. The SUPL TRIGGERED RESPONSE message may contain the area ids of the specified area for the area event triggered session.

J. The H-SLC informs the SUPL Agent in an MLP TLRA message that the triggered location response request has been accepted and also includes a req_id parameter to be used as a transaction id for the entire duration of the area event triggered session. The SET and the H-SLC MAY release the secure connection.

NOTE: The MLP TLRA may be sent earlier at any time after the H-SLP receives the MLP TLRR.

K. If the area ids are downloaded in step I, the SET SHALL compare the current area id to the downloaded area ids. When the area event trigger in the SET or the comparison of the current area id to the downloaded area ids indicates that a position fix has to be performed, the SET attaches itself to the Packet Data Network if it is not already attached or establishes a circuit switched data connection. The SET then sends a SUPL POS INIT message to the V-SPC to start a positioning session with the V-SPC. The SUPL POS INIT message contains at least session-id, the Location ID (lid) and the SET capabilities parameter. The SET MAY provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if this is supported. The SET MAY set the Requested Assistance Data element in the SUPL POS INIT.
If a position calculated based on information received in the SUPL POS INIT message is available (e.g. a cell-id based position fix) that meets the required QoP, the V-SPC MAY directly proceed to step M and not engage in a SUPL POS session.

L. The SET and the V-SPC exchange several successive positioning procedure messages.
The V-SPC calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance obtained from the V-SPC (SET-Based).

M. Once the position calculation is complete the V-SPC sends a SUPL REPORT message to the SET. The SET MAY release the secure connection to the V-SPC.
The SUPL REPORT message includes the position result if the position estimate is calculated in the V-SPC and therefore needs to be sent to the SET.

N. The SET compares the calculated position estimate with the event area to check if the event trigger condition has been met. If no area event is triggered, the SET SHALL return to step K. If area event is triggered SET SHALL proceed to step O.

O. The SET sends a SUPL REPORT message including the session id and the position estimate to the H-SLC unless the Location estimate parameter is set to "false" in which case no position estimate is included.

P. The H-SLC sends a MLP TLREP message to the SUPL Agent which may include the position result.

Q. If the SUPL Agent has requested several reports and more reports are to be sent, the SET repeats step K to P or step K to N depending on if the area event condition is fulfilled or not. Note that in this case, step O occurs only after the minimum time between reports has elapsed.

R. When the last report has been sent the H-SLC informs the V-SLC about the end of the triggered session by sending a SUPL END message over an RLP SSRP message.

S. The V-SLC informs the V-SPC about the end of the area event triggered session through internal communication.

T. The H-SLC ends the area event triggered session by sending a SUPL END message to the SET.

The call flow described in Figure 17 is applicable to all positioning methods, however, individual steps within the call flows are optional:

- Step L (SUPL POS) is not performed for cell-id based positioning methods.
- In A-GPS SET Based mode where no GPS assistance data is required from the network, no interaction with the V-SPC is required to calculate a position estimate. Interaction with the V-SPC is only required for GPS assistance data update in which case steps K to M are performed.

5.1.10.3 Roaming with H-SLP Positioning Successful Case

SUPL Roaming where the H-SLP is involved in the positioning calculation.

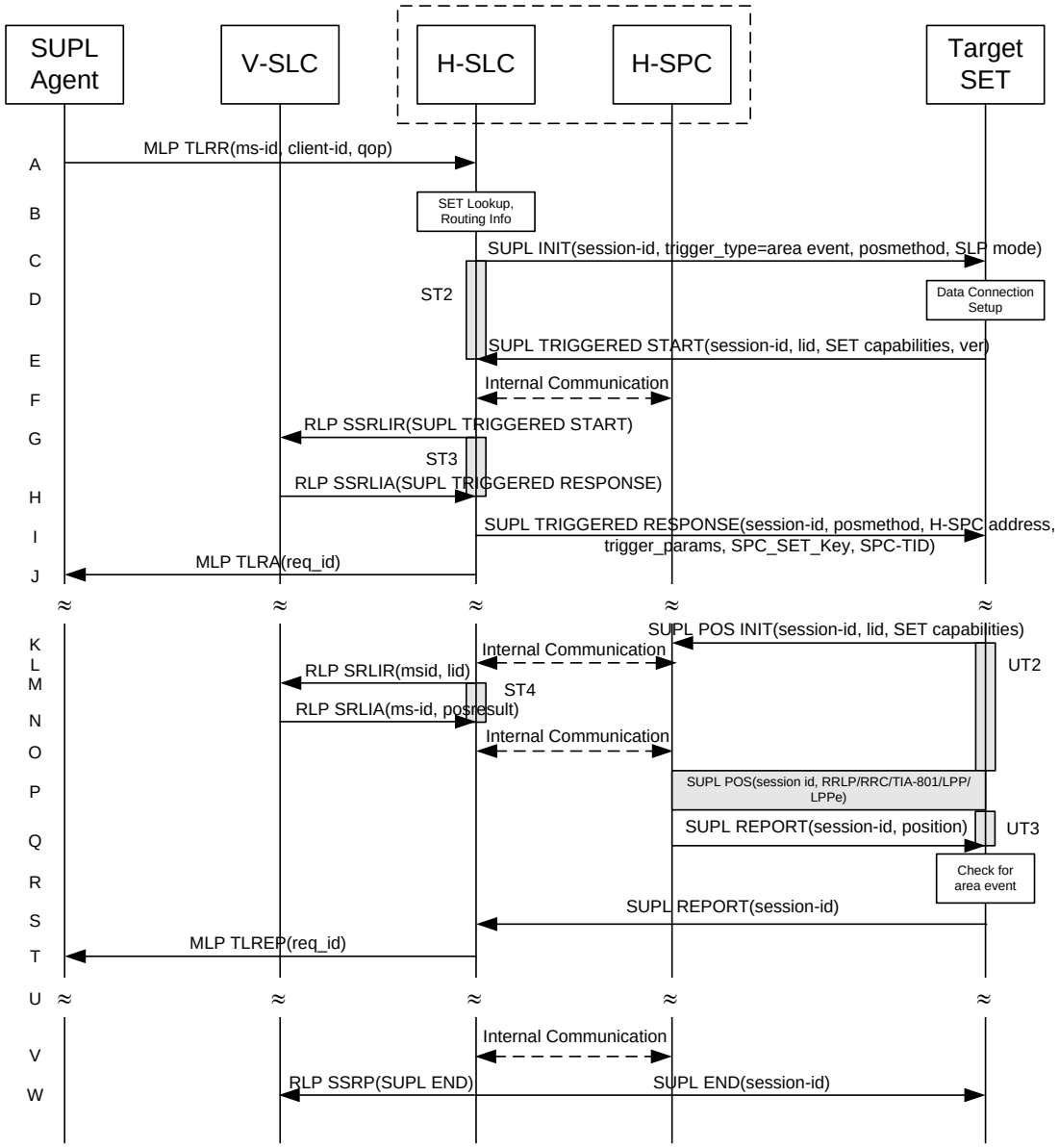

Figure 18: Network Initiated Area Event Trigger Service Roaming with H-SLP Positioning Successful Case – Non-Proxy Mode

NOTE: See Appendix D for timer descriptions.

A. SUPL Agent issues an MLP TLRR message to the H-SLC, with which SUPL Agent is associated. The H-SLC shall authenticate the SUPL Agent and check if the SUPL Agent is authorized for the service it requests, based on the client-id received. Further, based on the received ms-id the H-SLC shall apply subscriber privacy against the client-id.

B. The H-SLC verifies that the target SET is currently SUPL roaming.
The H-SLC MAY also verify that the target SET supports SUPL.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside the scope of SUPL. However, there are various environment dependent mechanisms.

NOTE: Alternatively, the H-SLC may determine whether the SET is SUPL roaming in a later step using the location identifier (lid) received from the SET.

NOTE: The specifics for determining if the SET supports SUPL are beyond SUPL 2.0 scope.

C. The H-SLC initiates the area event trigger session with the SET using the SUPL INIT message. The SUPL INIT message contains at least session-id, trigger type indicator (in this case area event), proxy/non-proxy mode indicator and the intended positioning method. If the result of the privacy check in Step A indicates that notification or verification to the target subscriber is needed, the H-SLC SHALL also include the Notification element in the SUPL INIT message. Before the SUPL INIT message is sent, the H-SLC also computes and stores a hash of the message.

D. The SET analyses the received SUPL INIT. If found to be non authentic SET takes not further actions. Otherwise the SET takes needed action preparing for establishment or resumption of a secure connection.

E. The SET will evaluate the Notification rules and follow the appropriate actions. The SET also checks the proxy/non-proxy mode indicator to determine if the H-SLP uses proxy or non-proxy mode. In this case, non-proxy mode is used, and the SET SHALL establish a secure connection to the H-SLC using the H-SLC address that has been provisioned by the Home Network to the SET.
The SET then sends a SUPL TRIGGERED START message to start an area event triggered session with the H-SLC. The SET SHALL send the SUPL TRIGGERED START message even if the SET supported positioning technologies do not include the intended positioning method indicated in the SUPL INIT message. The SUPL TRIGGERED START message contains at least session-id, SET capabilities, a hash of the received SUPL INIT message (ver) and Location ID (lid). The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe).

F. The H-SLC informs the H-SPC through internal communication about the periodic triggered session. The H-SLC generates SPC_SET_Key and SPC-TID to be used for mutual H-SPC/SET authentication and forwards both to the H-SPC through internal communication. The H-SPC grants or denies the request and informs the H-SLC accordingly.

G. Based on the received lid or other mechanisms, the H-SLC determines the V-SLC and sends an RLP SSRLIR including a SUPL TRIGGERED START message to the V-SLC to inform the V-SLC that an area event triggered session is in the progress of being initiated with the H-SLP. The area event trigger parameters such as area information requested by SUPL Agent for the area event triggered session MAY be included in this message by the H-SLC.

H. The V-SLC acknowledges the RLP request received in step G with a SUPL TRIGGERED RESPONSE message which is carried inside an RLP SSRLIA message. The V-SLC MAY include area ids corresponding to the area for the area event trigger session in the SUPL TRIGGERED RESPONSE message.

I. Consistent with the SET capabilities received in step E, the H-SLC determines the indended positioning method to be used for the area event triggered session and indicates its readiness for an area event triggered session by sending a SUPL TRIGGERED RESPONSE message back to the SET. The SUPL TRIGGERED RESPONSE message to the SET includes at a minimum the session-id, posmethod, H-SPC address, area event trigger parameters and SPC_SET_Key and SPC-TID. The SUPL TRIGGERED RESPONSE message may contain the area ids of the specified area for the area event triggered session.

J. The H-SLC informs the SUPL Agent in an MLP TLRA message that the triggered location response request has been accepted and also includes a req_id parameter to be used as a transaction id for the entire duration of the area event triggered session. The SET and the H-SLC MAY release the secure connection.

NOTE: The MLP TLRA may be sent earlier at any time after the H-SLP receives the MLP TLRR.

K. If the area ids are downloaded in step I, the SET SHALL compare the current area id to the downloaded area ids. When the area event trigger in the SET or the comparison of the current area id to the downloaded area ids indicates that a position fix has to be performed, the SET attaches itself to the Packet Data Network if it is not already attached or establishes a circuit switched data connection. The SET then sends a SUPL POS INIT message to the H-SPC to start a positioning session with the H-SPC. The SUPL POS INIT message contains at least session-id and the Location ID (lid) and the SET capabilities parameter. The SET MAY provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if this is supported. The SET MAY set the Requested Assistance Data element in the SUPL POS INIT.
If the SUPL POS INIT message contains a position that meets the required QoP, the H-SPC MAY directly proceed to step Q.

L. Through internal communication the H-SPC requests a coarse position estimate from the H-SLC based on the lid received in step K.

M. To obtain a coarse position the H-SLC sends an RLP SRLIR message to the V-SLC.

N. The V-SLC translates the received lid into a position estimate and returns the result to the H-SLC in an RLP SRLIA message.

O. The H-SLC forwards the coarse position to the H-SPC through internal communication.
If the coarse position meets the required QoP, the H-SPC MAY directly proceed to step Q and not engage in a SUPL POS session.

P. The SET and the H-SPC exchange several successive positioning procedure messages.
The H-SPC calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance obtained from the H-SPC (SET-Based).

Q. Once the position calculation is complete the H-SPC sends a SUPL REPORT message to the SET. The SET MAY release the secure connection to the H-SPC.
The SUPL REPORT message includes the position result if the position estimate is calculated in the H-SPC and therefore needs to be sent to the SET.

R. The SET compares the calculated position estimate with the event area to check if the event trigger condition has been met. If no area event is triggered, the SET SHALL return to step K. If area event is triggered SET SHALL proceed to step S.

S. The SET sends a SUPL REPORT message including the session id and the position estimate to the H-SLC unless the Location estimate parameter is set to "false" in which case no position estimate is included.

T. The H-SLC sends a MLP TLREP message to the SUPL Agent which may include the position result.

U. If SUPL Agent has requested several report and more reports are to be sent, the SET repeats step K to T or step K to R depending on if the area event condition is fulfilled or not. Note that in this case, step S occurs only after the minimum time between reports has elapsed.

V. When the last report has been sent the H-SLC informs the H-SPC about the end of the area event triggered session through internal communication.

W. The H-SLC ends the area event triggered session by sending a SUPL END message to the SET and by sending a SUPL END message using an RLP SSRP tunnel message to the V-SLC

The call flow described in Figure 18 is applicable to all positioning methods, however, individual steps within the call flows are optional:

- Step P (SUPL POS) is not performed for cell-id based positioning methods.
- In A-GPS SET Based mode where no GPS assistance data is required from the network, no interaction with the H-SPC is required to calculate a position estimate. Interaction with the H-SPC is only required for GPS assistance data update in which case steps K to Q are performed.

5.1.11 V-SLP to V-SLP Handover

This section describes V-SLP to V-SLP handover during an ongoing triggered session. The handover is required for SUPL roaming with V-SLP scenarios (for a definition of SUPL roaming see section 3.2)

5.1.11.1 V-SLP to V-SLP Handover – Network initiated Proxy mode

This section describes the case where the V-SLP detects that the target SET is out of the V-SLP coverage area and informs the SET accordingly. The target SET then request new trigger parameters and subsequently the H-SLP selects and initiates a new V-SLP and send new trigger parameters to the target SET which then continues the session. The described mechanism applies to both Network Initiated and SET Initiated proxy mode scenarios.

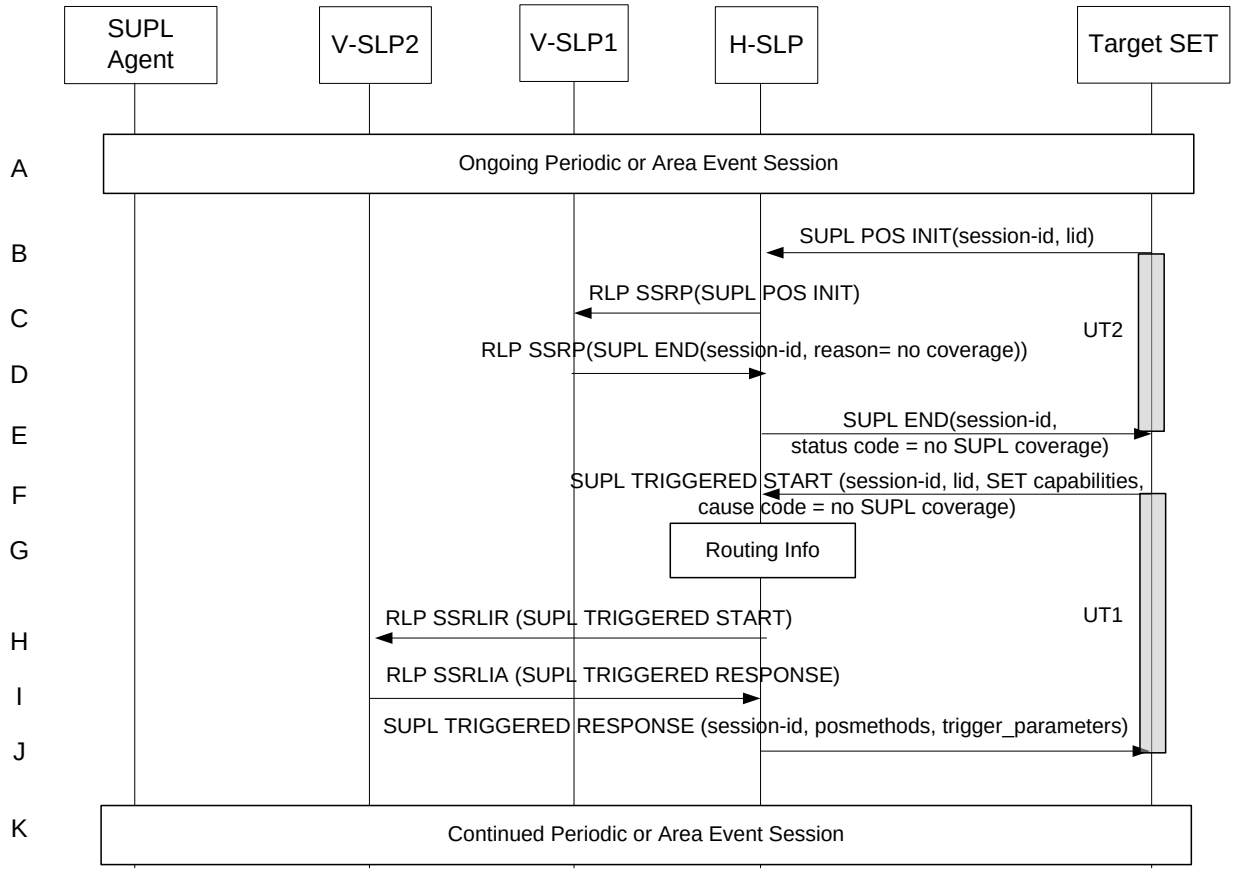

Figure 19: Network initiated Proxy mode – V-SLP to V-SLP Handover

NOTE: See Appendix D for timer descriptions.

A. A triggered session is ongoing.

B. The SET sends a SUPL POS INIT message to the H-SLP to start a positioning session with the V-SLP1.

C. The H-SLP forwards the SUPL POS INIT message to V-SLP1 using a RLP SSRP message.

D. V-SLP1 detects it does not support the lid included in the SUPL POS INIT and sends a SUPL END message to the H-SLP using a RLP SSRP message. The V-SLP1 SHALL release all resources related to this session.

E. The H-SLP sends the SUPL END message to the SET indicating that the SET lost SUPL coverage (i.e. the SET is outside the SUPL coverage area of V-SLP1).

F. The SET then sends a SUPL TRIGGERED START message. The SUPL TRIGGERED START message contains at least the same session-id as in step E, SET capabilities, Location ID (lid) and cause code (no SUPL coverage) for re-sending the SUPL TRIGGERED START message. The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe).

G. The H-SLP verifies that the target SET is currently SUPL roaming and is outside of the coverage area of V- SLP1. The H-SLP determines the V- SLP2 based on the lid received in the SUPL TRIGGERED START message.

H. The H-SLP sends an RLP SSRLIR including the SUPL TRIGGERED START message to the V- SLP2 to inform that the target SET will initiate a SUPL positioning procedure. Any area information requested by SUPL Agent for an area event triggered session SHALL be included in this message by the H-SLP.

I. The V- SLP2 acknowledges that it is ready to initiate a SUPL positioning procedure with an RLP SSRLIA including SUPL TRIGGERED RESPONSE message back to the H-SLP. The V-SLP2 MAY include area ids corresponding to the area for the area event trigger session in the SUPL TRIGGERED RESPONSE message.

J. The H-SLP forwards the received SUPL TRIGGERED RESPONSE message to the SET including session-id, the positioning method to be used for the periodic triggered session and trigger parameters. The SUPL TRIGGERED RESPONSE message may contain the area ids of the specified area for the area event triggered session.

K. The triggered session is continued.

5.1.11.2 V-SPC to V-SPC Handover – Network initiated Non-Proxy mode

This section describes the case where the V-SPC detects that the target SET is out of the V-SPC coverage area and informs the SET accordingly. The target SET then request new trigger parameters and subsequently the H-SLC selects and initiates a new V-SPC and sends new trigger parameters to the target SET which then continues the session. The described mechanism applies to both Network Initiated and SET Initiated non-proxy mode scenarios.

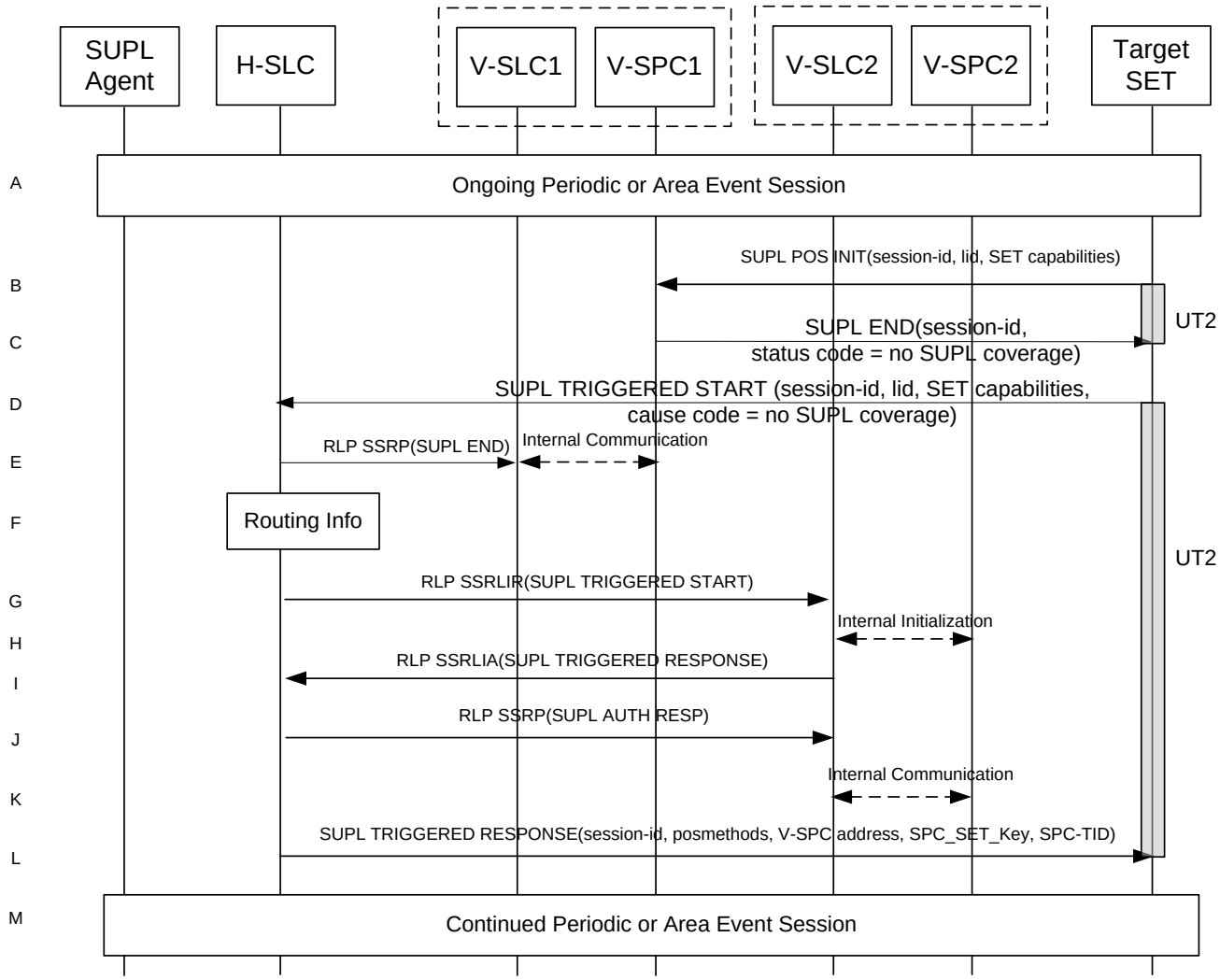

Figure 20: Network initiated Non-Proxy mode – V-SLP to V-SLP Handover

NOTE: See Appendix D for timer descriptions.

A. A triggered session is ongoing.

B. The SET sends a SUPL POS INIT message to the V-SPC1 to start a positioning session with the V-SPC1.

C. V-SPC1 detects it does not support the lid included in the SUPL POS INIT and sends a SUPL END message to the SET indicating that the SET lost SUPL coverage (i.e. the SET is outside the SUPL coverage area of V-SLP1).

D. The SET then sends a SUPL TRIGGERED START message. The SUPL TRIGGERED START message contains at least the same session-id as in step C, SET capabilities, Location ID (lid) and cause code (no SUPL coverage) for re-sending the SUPL TRIGGERED START message. The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe).

E. The H-SLC informs V-SLC1 about the end of the triggered session by sending a SUPL END message using an RLP SSRP tunnel message to the V-SLC1. Through internal communication the V-SLC1 informs the V-SPC1 of the end of the SUPL session. The V-SLC1 and the V-SPC1 SHALL release all resources related to this session.

F. The H-SLC verifies that the target SET is currently SUPL roaming and is outside of the coverage area of V- SLP1. The H-SLC determines the V- SLP2 based on the lid received in the SUPL TRIGGERED START message.

G. The H-SLC sends an RLP SSRLIR including the SUPL TRIGGERED START message to the V- SLP2 to inform that the target SET will initiate a SUPL positioning procedure. Any area information requested by SET for an area event triggered session SHALL be included in this message by the H-SLC.

H. Through internal communication the V-SLC2 requests service for an area event triggered session from the V-SPC2. The V-SPC2 grants or denies the request and informs the V-SLC2 accordingly.

I. The V- SLC2 acknowledges that it is ready to initiate a SUPL positioning procedure with an RLP SSRLIA including SUPL TRIGGERED RESPONSE message back to the H-SLC. The V-SLP2 MAY include area ids corresponding to the area for the area event trigger session in the SUPL TRIGGERED RESPONSE message.

J. The H-SLC generates a SPC_SET_Key and a SPC-TID to be used for mutual V-SPC/SET authentication. The H-SLC forwards the SPC_SET_Key and a SPC-TID to the V-SLC2 through a SUPL AUTH RESP message using an RLP SSRP tunnel.

K. V-SLC2 forwards the key to V-SPC2 through internal communication.

L. The H-SLC sends a SUPL TRIGGERED RESPONSE message to the SET. The SUPL TRIGGERED RESPONSE message contains session-id, the positioning method to be used for the periodic triggered session and V-SPC2 address. The SUPL TRIGGERED RESPONSE message may contain the area ids of the specified area for the area event triggered session.
For mutual V-SPC2/SET authentication the SUPL TRIGGERED RESPONSE message also includes SPC_SET_Key and SPC-TID to be used by the SET..

M. The triggered session is continued.

5.1.12 Notification/Verification based on current location

This section describes scenarios where notification and/or verification is based on the user's current position. Before invoking the notification/verification process, the user's current position is determined unbeknownst to the user. The actual notification/verification process (no notification and no verification, notification only, notification and verification and privacy override) is then decided based on the user's current position.

5.1.12.1 Non Roaming Successful Case – Proxy Mode

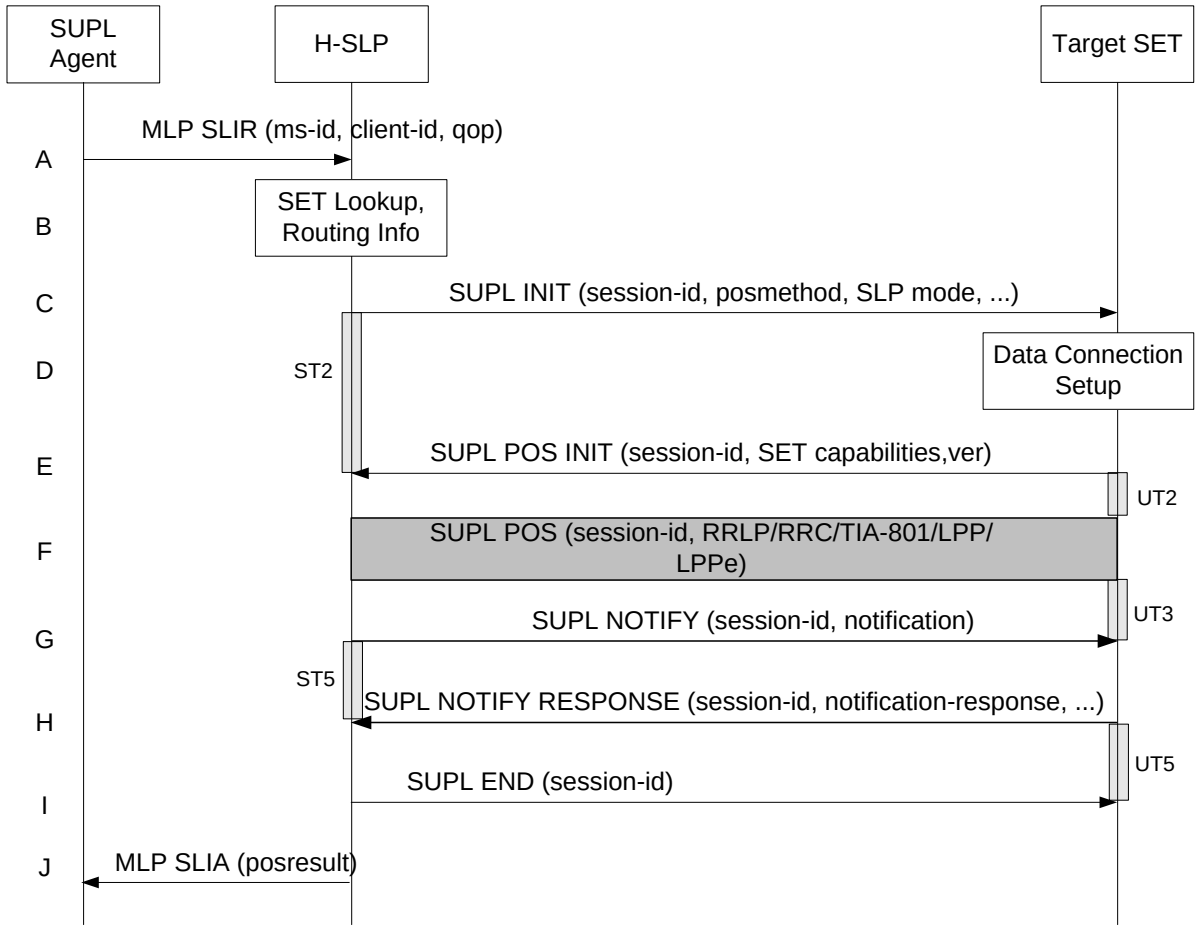

Figure 21: Notification/Verification based on current location. Network Initiated Non-Roaming Successful Case – Proxy Mode

NOTE: See Appendix D for timer descriptions.

A. The SUPL Agent issues an MLP SLIR message to the H-SLP, with which SUPL Agent is associated. The H-SLP shall authenticate the SUPL Agent and check if the SUPL Agent is authorized for the service it requests, based on the client-id received. Further, based on the received ms-id the H-SLP shall apply subscriber privacy against the client-id.
If a previously computed position which meets the requested QoP is available at the H-SLP and, based on that position, no notification or verification is required, the H-SLP SHALL directly proceed to step J. If, based on that position, notification and verification or notification only is required, the H-SLP SHALL proceed to step B.

B. The SLP verifies that the target terminal is currently within the service area of the SLP, i.e. the target terminal is not roaming. The SLP may also verify that the target terminal supports SUPL.

NOTE: The specifics for determining if the SET is roaming or not is considered outside scope of SUPL. However, there are various environment dependent mechanisms.

C. The H-SLP initiates the location session with the SET using the SUPL INIT message. The SUPL INIT message contains at least session-id, proxy/non-proxy mode indicator and the intended positioning method. As in this case the result of the privacy check in Step A indicates that subscriber privacy check based on current location is required, the H-SLP SHALL include the Notification Mode element in the SUPL INIT message to indicate notification based on current location and SHALL NOT include the notification element in the SUPL INIT message. Before the SUPL INIT message is sent the H-SLP also computes and stores a hash of the message.
If in step A the H-SLP decided to use a previously computed position, the SUPL INIT message SHALL indicate this in a ‘no position’ posmethod parameter value and the SET SHALL respond with a SUPL END message carrying the

results of the verification process (access granted, or access denied). If no explicit verification is required (notification only) the SET SHALL respond with a SUPL END message. The H-SLP SHALL then directly proceed to step J.

NOTE: Before sending the SUPL END message the SET SHALL perform the data connection setup procedure of step D.

D. The SET analyses the received SUPL INIT. If found to be non authentic SET takes not further actions. Otherwise the SET takes needed action preparing for establishment or resumption of a secure connection.

E. The SET will evaluate the Notification rules and follow the appropriate actions. The SET checks the notification mode indicator and determines that in this case the notification is performed based on the location of the SET. The SET also checks the proxy/non-proxy mode indicator to determine if the H-SLP uses proxy or non-proxy mode. In this case, proxy mode is used, and the SET SHALL establish a secure connection to the H-SLP using H-SLP address that has been provisioned by the Home Network to the SET. The SET then sends a SUPL POS INIT message to start a positioning session with the H-SLP. The SUPL POS INIT message contains at least session-id, SET capabilities, a hash of the received SUPL INIT message (ver) and Location ID (lid). The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe). The SET MAY provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if these are available and supported by both SET and H-SLP. The SET MAY set the Requested Assistance Data element in the SUPL POS INIT.
If a position received from or calculated based on information received in the SUPL POS INIT message is available that meets the required QoP, the H-SLP MAY directly proceed to step G and not engage in a SUPL POS session.

F. The H-SLP SHALL check that the hash of SUPL INIT matches the one it has computed for this particular session. Based on the SUPL POS INIT message including posmethod(s) supported by the SET the H-SLP SHALL then determine the posmethod. If required for the posmethod the H-SLP SHALL use the supported positioning protocol (e.g., RRLP, RRC, TIA-801 or LPP/LPPe) from the SUPL POS INIT message.
The SET and the H-SLP exchange several successive positioning procedure messages.
The H-SLP calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance obtained from the H-SLP (SET-Based).

G. The H-SLP applies subscriber privacy against the SET position estimate determined in Step F. If, based on this position, notification and verification or notification only is required, the H-SLP SHALL send a SUPL NOTIFY message to the SET. The SUPL NOTIFY message contains the notification element. If, based on this position, no notification and verification is required, the H-SLP SHALL directly proceed to Step I.

H. The SET SHALL send a SUPL NOTIFY RESPONSE message to the H-SLP. If notification and verification was required in step G then this will contain the notification response from the user.

I. Once the position calculation is complete the H-SLP sends the SUPL END message to the SET informing it that no further positioning procedure will be started and that the location session is finished. The SET SHALL release the secure connection to the H-SLP and release all resources related to this session.

J. The H-SLP sends the position estimate back to the SUPL Agent in an MLP SLIA message and the H-SLP SHALL release all resources related to this session.

5.1.12.2 Non Roaming Successful Case – Non-Proxy Mode

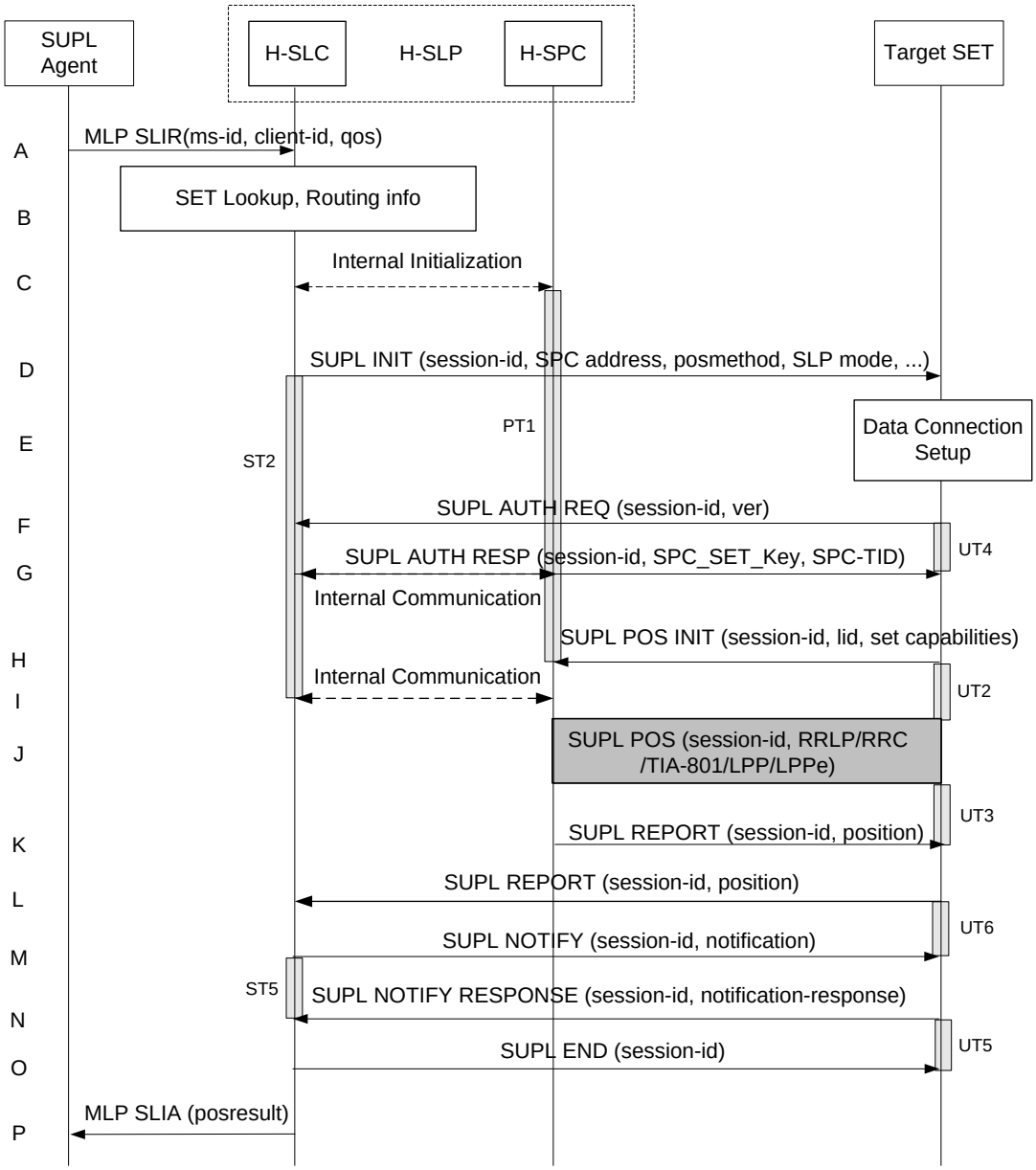

Figure 22: Notification/Verification based on current location. Network Initiated Non-Roaming Successful Case – Non-Proxy mode

NOTE: See Appendix D for timer descriptions.

A. The SUPL Agent issues an MLP SLIR message to the H-SLC, with which SUPL Agent is associated. The H-SLC shall authenticate the SUPL Agent and check if the SUPL Agent is authorized for the service it requests, based on the client-id received. Further, based on the received ms-id the H-SLC shall apply subscriber privacy against the client-id.
If a previously computed position which meets the requested QoP is available at the H-SLC and, based on that position, no notification or verification is required, the H-SLC SHALL directly proceed to step P. If, based on that position, notification and verification or notification only is required, the H-SLC SHALL proceed to step B.

B. The H-SLC verifies that the target SET is currently not SUPL roaming.
The H-SLC MAY also verify that the target SET supports SUPL.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside scope of SUPL. However, there are various environment dependent mechanisms.

C. The H-SLC and H-SPC may exchange information necessary to setup the SUPL session.

D. The H-SLC initiates the location session with the SET using the SUPL INIT message. The SUPL INIT message contains at least session-id, address of the SPC, proxy/non-proxy mode indicator and the intended positioning method. As in this case the result of the privacy check in Step A indicates that subscriber privacy check based on current location is required, the H-SLC SHALL include the Notification Mode element in the SUPL INIT message to indicate notification based on current location and SHALL NOT include the notification element in the SUPL INIT message. If in step A the H-SLC decided to use a previously computed position, the SUPL INIT message SHALL indicate this in a 'no position' posmethod parameter value and the SET SHALL respond with a SUPL END message carrying the results of the verification process (access granted, or access denied). If no explicit verification is required (notification only) the SET SHALL respond with a SUPL END message. The H-SLC SHALL then directly proceed to step P.

NOTE: Before sending the SUPL END message the SET SHALL perform the data connection setup procedure of step E.

E. The SET analyses the received SUPL INIT. If found to be non authentic SET takes not further actions. Otherwise the SET takes needed action preparing for establishment or resumption of a secure connection..

F. The SET uses the address provisioned by the Home Network to establish a secure connection to the H-SLC. The SET then checks the proxy/non-proxy mode indicator to determine if the H-SLP uses proxy or non-proxy mode. In this case non-proxy mode is used and the SET SHALL send a SUPL AUTH REQ message to the H-SLC. The SUPL AUTH REQ message contains the session-id and a hash of the received SUPL INIT message (ver).

G. The H-SLC creates SPC_SET_Key and SPC-TID to be used for mutual H-SPC/SET authentication. The H-SLC forwards SPC_SET_Key and SPC-TID to the H-SPC through internal communication and returns a SUPL AUTH RESP message including SPC_SET_Key and SPC-TID to the SET.

H. The SET will evaluate the Notification rules and follow the appropriate actions. The SET checks the notification mode indicator and determines that in this case the notification is performed based on the location of the SET. The SET establishes a secure connection to the H-SPC according to the address received in step D. The SET and H-SPC perform mutual authentication and the SET sends a SUPL POS INIT message to start a positioning session with the H-SPC. The SUPL POS INIT message contains at least session-id, SET capabilities and Location ID (lid). The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe). The SET MAY provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if these are available and supported by both SET and H-SPC. The SET MAY set the Requested Assistance Data element in the SUPL POS INIT. The SET SHALL also release the connection to the H-SLC.

I. The H-SLC and H-SPC may collaborate to determine an initial position of the SET to aid in the position determination process. If the initial position calculated based on information received in the SUPL POS INIT message meets the requested QoP, the H-SPC MAY directly proceed to step K and not engage in a SUPL POS session.

J. Based on the SUPL POS INIT message including posmethod(s) supported by the SET the H-SPC SHALL determine the posmethod. If required for the posmethod the H-SPC SHALL use the supported positioning protocol (e.g., RRLP, RRC, TIA-801 or LPP/LPPe) from the SUPL POS INIT message
The SET and the H-SPC exchange several successive positioning procedure messages.
The H-SPC calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance obtained from the H-SPC (SET-Based).

K. As in this case in step C the H-SLC indicated that notification or verification is based on the position of the SET, the H-SPC sends the calculated position to the SET in a SUPL REPORT message.

L. As in this case in step D the H-SLC indicated that notification or verification is based on the position of the SET, the SET sends the calculated position to the H-SLC in a SUPL REPORT message.

M. The H-SLC applies subscriber privacy against the SET position estimate. If, based on this position, notification and verification or notification only is required, the H-SLP SHALL send a SUPL NOTIFY message to the SET. The SUPL NOTIFY message contains notification element. If, based on this position, no notification and verification is required, the H-SLP SHALL directly proceed to Step O.

N. The SET SHALL then send an SUPL NOTIFY RESPONSE message to the H-SLC. If notification and verification was required in step M then this will contain the notification response from the user.

O. Once the position calculation is complete the H-SLC sends the SUPL END message to the SET informing it that no further positioning procedure will be started and that the SUPL session is finished. The SET SHALL release the secure connection to the H-SLC and release all resources related to this session.

P. The H-SLC sends the position estimate back to the SUPL Agent in an MLP SLIA message and the H-SLC releases all resources related to this session.

5.1.12.3 Roaming with V-SLP Positioning Successful Case – Proxy mode

SUPL Roaming where the V-SLP is involved in the positioning calculation.

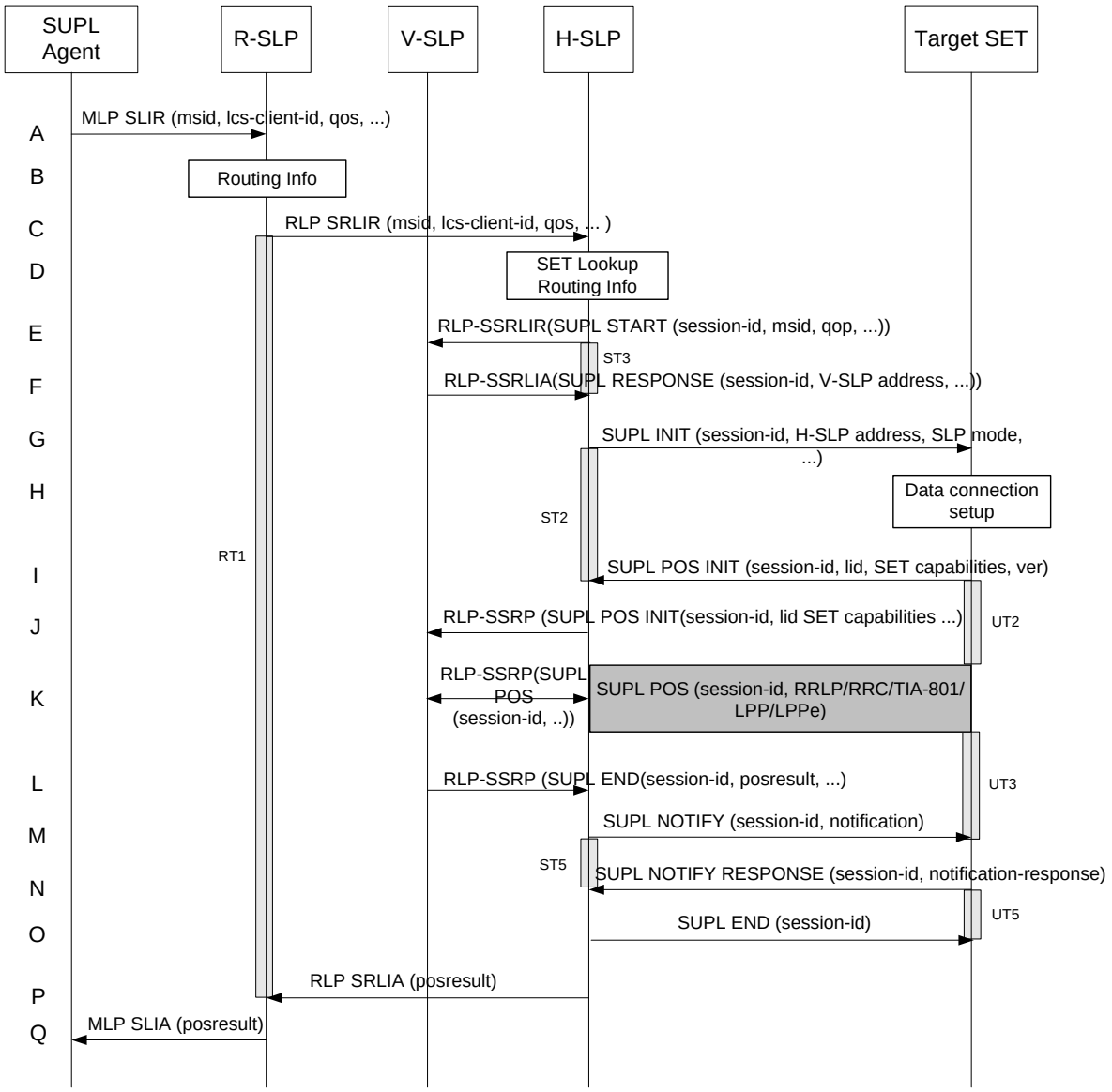

Figure 23: Notification/Verification based on current location. Network Initiated Roaming with V-SLP Positioning Successful Case – Proxy mode

NOTE: See Appendix D for timer descriptions.

A. The SUPL Agent issues an MLP SLIR message to the R-SLP, with which SUPL Agent is associated. The R-SLP SHALL authenticate the SUPL Agent and check if the SUPL Agent is authorized for the service it requests, based on the client-id received.

B. The R-SLP determines the H-SLP based on the received msid. If the R-SLP determines that the SUPL Agent is not authorized for this request, Step Q will be returned with the applicable MLP return code.

NOTE: The specifics for determining the H-SLP are considered outside scope of SUPL. However, there are various environment dependent mechanisms.

C. The R-SLP then forwards the location request to the H-SLP of the target subscriber, using RLP protocol. If a previously computed position which meets the requested QoP is available at the H-SLP and, based on that position, no notification or verification is required, the H-SLP SHALL directly proceed to step P. If, based on that position, notification and verification or notification only is required, the H-SLP SHALL proceed to step G after having performed the SET Lookup and Routing Info procedures of step D.

D. Based on the received ms-id the H-SLP SHALL apply subscriber privacy against the client-id. The H-SLP verifies that the target SET is currently SUPL roaming. In addition the H-SLP MAY also verify that the target SET supports SUPL.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside the scope of SUPL. However, there are various environment dependent mechanisms.

E. The H-SLP sends an RLP SSRLIR to the V-SLP to inform the V-SLP that the target SET will initiate a SUPL positioning procedure. Mandatory parameters in SUPL START that are not known to H-SLP (lid and SET capabilities) shall be populated with arbitrary values by H-SLP and be ignored by V-SLP

F. The V-SLP acknowledges that it is ready to initiate a SUPL positioning procedure with an RLP SSRLIA back to the H-SLP.

G. The H-SLP initiates the location session with the SET using the SUPL INIT message. The SUPL INIT message contains at least session-id, proxy/non-proxy mode indicator and the intended positioning method. As in this case the result of the privacy check in Step D indicates that subscriber privacy check based on current location is required, the H-SLP SHALL include the Notification Mode element in the SUPL INIT message to indicate notification based on current location and SHALL NOT include the notification element in the SUPL INIT message. This step MAY be performed immediately after step D. Before the SUPL INIT message is sent the H-SLP also computes and stores a hash of the message.
If in step C the H-SLP decided to use a previously computed position the SUPL INIT message SHALL indicate this in a ‘no position’ posmethod parameter value and the SET SHALL respond with a SUPL END message to the H-SLP carrying the results of the verification process (access granted, or access denied). If no verification is required (notification only) the SET SHALL respond with a SUPL END message to the H-SLP. The H-SLP SHALL then directly proceed to step P.

NOTE: Before sending the SUPL END message the SET SHALL perform the data connection setup procedure of step H.

Step G MAY be performed immediately after step D, however, H-SLP SHALL not proceed with step J before step F has returned..

H. The SET analyses the received SUPL INIT. If found to be non authentic SET takes not further actions. Otherwise the SET takes needed action preparing for establishment or resumption of a secure connection.

I. The SET will evaluate the Notification rules and follow the appropriate actions. The SET checks the notification mode indicator and determines that in this case the notification is performed based on the location of the SET. The SET also checks the proxy/non-proxy mode indicator to determine if the SLP uses proxy or non-proxy mode. In this case, proxy mode is used, and the SET SHALL establish a secure connection to the H-SLP using the H-SLP address that has been provisioned by the Home Network to the SET. The SET then sends a SUPL POS INIT message to start a positioning session with the H-SLP. The SUPL POS INIT message contains at least session-id, SET capabilities, a hash of the received SUPL INIT message (ver) and Location ID (lid). The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe). The SET MAY optionally provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY optionally provide its position or network timing

information, if these are available and supported by both SET and H-SLP. The SET MAY optionally set the Requested Assistance Data element in the SUPL POS INIT.

J. The H-SLP SHALL check that the hash of SUPL INIT matches the one it has computed for this particular session. The H-SLP then tunnels the SUPL POS INIT message to the V-SLP.

K. Based on the SUPL POS INIT message including posmethod(s) supported by the SET, the V-SLP SHALL determine the posmethod. If required for the posmethod, the V-SLP SHALL use the supported positioning protocol (e.g., RRLP, RRC, TIA-801 or LPP/LPPe) from the SUPL POS INIT message.
If the V-SLP already calculated an initial position based on information received in the SUPL POS INIT message which satisfyies the requested QoP, the V-SLP MAY directly proceed to step L and not engage in a SUPL POS session. Otherwise, the SET and the V-SLP exchange several successive positioning procedure messages, tunnelled over RLP via the H-SLP.
The V-SLP calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance obtained from the V-SLP via H-SLP (SET-Based).

L. Once the position calculation is complete the V-SLP sends the SUPL END message tunnelled over RLP to the H-SLP . The V-SLP SHALL release all resources related to this session.

M. The H-SLP applies subscriber privacy against the SET position estimate obtained in Step L. If, based on this position, notification and verification or notification only is required, the H-SLP SHALL send a SUPL NOTIFY message to the SET. The SUPL NOTIFY message contains notification element. If, based on this position, no notification and verification is required, the H-SLP SHALL directly proceed to Step O.

N. The SET SHALL send a SUPL NOTIFY RESPONSE message to the H-SLP. If notification and verification was required in step M then this will contain the notification response from the user.

O. The H-SLP forwards the SUPL END to the SET informing it that no further positioning procedure will be started and that the location session is finished. The SET SHALL release the secure connection to the H-SLP and release all resources related to this session.

P. The H-SLP sends the position estimate back to the R-SLP in an RLP SRLIA message. The H-SLP SHALL release all resources related to this session.

Q. The R-SLP sends the position estimate back to the SUPL Agent in an MLP SLIA message.

5.1.12.4 Roaming with H-SLP Positioning Successful Case – Proxy mode

SUPL Roaming where the H-SLP is involved in the positioning calculation.

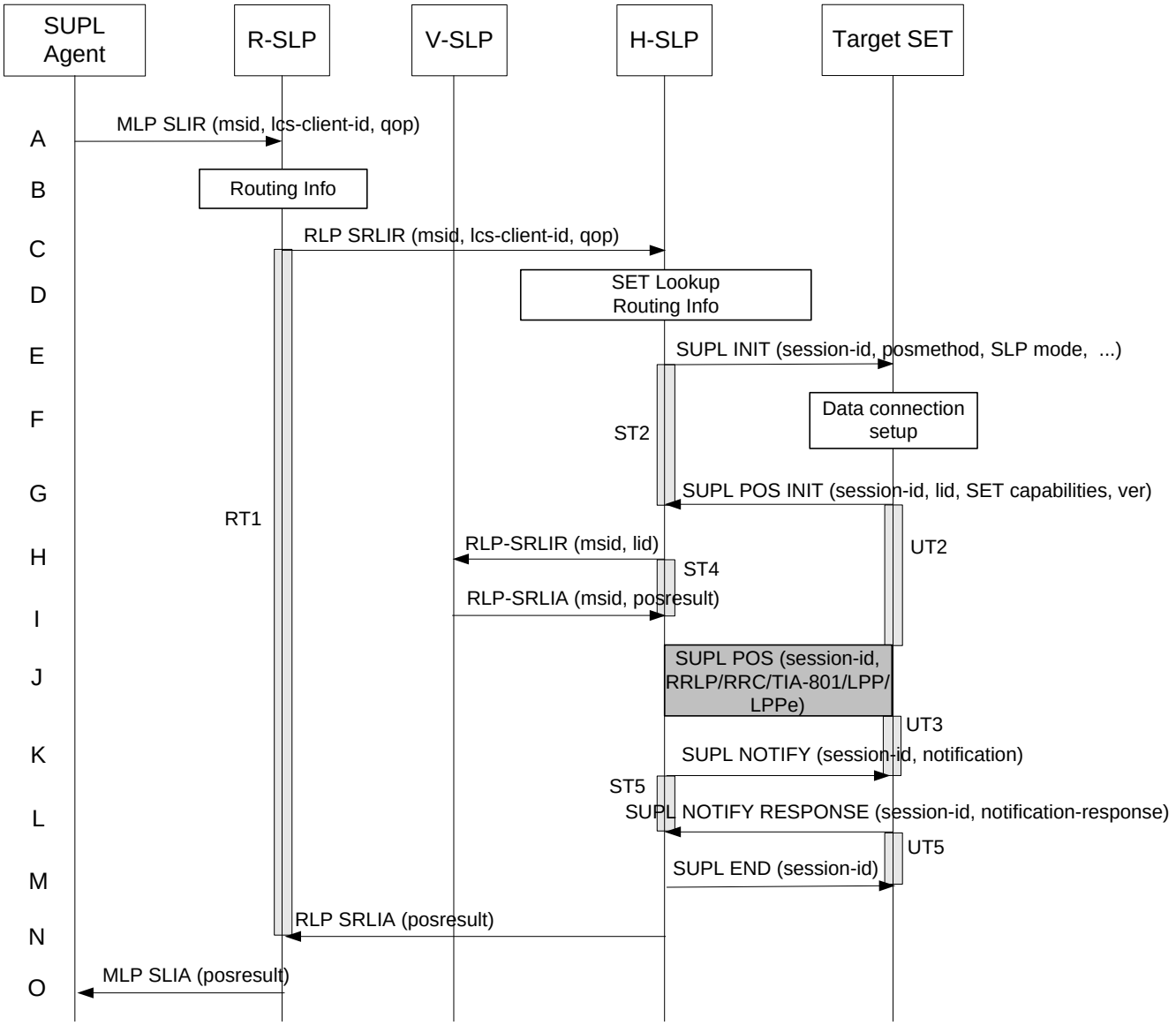

Figure 24: Notification/Verification based on current location. Network Initiated Roaming with H-SLP Positioning Successful case – Proxy mode

NOTE: See Appendix D for timer descriptions.

A. The SUPL Agent issues an MLP SLIR message to the R-SLP, with which SUPL Agent is associated. The R-SLP SHALL authenticate the SUPL Agent and check if the SUPL Agent is authorized for the service it requests, based on the client-id received.

B. The R-SLP determines the H-SLP based on the received msid. If the R-SLP determines that the SUPL Agent is not authorized for this request, Step O will be returned with the applicable MLP return code.

NOTE: The specifics for determining the H-SLP are considered outside scope of SUPL. However, there are various environment dependent mechanisms.

C. The R-SLP then forwards the location request to the H-SLP of the target subscriber, using RLP protocol. If a previously computed position which meets the requested QoP is available at the H-SLP and, based on that position, no notification or verification is required, the H-SLP SHALL directly proceed to step N. If, based on that position, notification and verification or notification only is required, the H-SLP SHALL proceed to step E after having performed the SET Lookup and Routing Info procedures of step D.

D. Based on the received ms-id the H-SLP SHALL apply subscriber privacy against the client-id. The H-SLP verifies that the target SET is currently SUPL roaming. In addition the H-SLP MAY also verify that the target SET supports SUPL.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside scope of SUPL. However, there are various environment dependent mechanisms.

NOTE: Alternatively, the H-SLP may determine whether the SET is SUPL roaming in a later step using the location identifier (lid) received from the SET.

E. The H-SLP initiates the location session with the SET using the SUPL INIT message. The SUPL INIT message contains at least session-id, proxy/non-proxy mode indicator and the intended positioning method. As in this case the result of the privacy check in Step D indicates that subscriber privacy check based on current location is required, the H-SLP SHALL include the Notification Mode element in the SUPL INIT message to indicate notification based on current location and SHALL NOT include the notification element in the SUPL INIT message. Before the SUPL INIT message is sent the H-SLP also computes and stores a hash of the message.
If in step C the H-SLP decided to use a previously computed position the SUPL INIT message SHALL indicate this in a 'no position' posmethod parameter value and the SET SHALL respond with a SUPL END message to the H-SLP carrying the results of the verification process (access granted, or access denied). If no verification is required (notification only) the SET SHALL respond with a SUPL END message to the H-SLP. The H-SLP SHALL then directly proceed to step N.

NOTE: Before sending the SUPL END message the SET shall follow the data connection setup procedure of step F.

F. The SET analyses the received SUPL INIT. If found to be non authentic SET takes not further actions. Otherwise the SET takes needed action preparing for establishment or resumption of a secure connection.

G. The SET will evaluate the Notification rules and follow the appropriate actions. The SET checks the notification mode indicator and determines that in this case the notification is performed based on the location of the SET. The SET also checks the proxy/non-proxy mode indicator to determine if the H-SLP uses proxy or non-proxy mode. In this case, proxy mode is used, and the SET SHALL establish a secure connection to the H-SLP using the H-SLP address that has been provisioned by the Home Network to the SET. The SET then sends a SUPL POS INIT message to start a positioning session with the H-SLP. The SUPL POS INIT message contains at least session-id, SET capabilities and Location ID (lid). The SUPL POS INIT MAY contain a hash of the received SUPL INIT message (ver). The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe). The SET MAY provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if these are available and supported by both SET and H-SLP. The SET MAY set the Requested Assistance Data element in the SUPL POS INIT.

H. The H-SLP SHALL check that the hash of SUPL INIT matches the one it has computed for this particular session. If an initial position calculated based on information received in the SUPL POS INIT message is available which meets the requested QoP, the H-SLP MAY directly proceed to step K.

The H-SLP then decides that the H-SLP will provide assistance/position calculation and the H-SLP sends an RLP SRLIR request to the V-SLP to determine an initial position for the SET. The RLP request contains at least the msid and the Location ID (lid). Optionally the H-SLP MAY forward NMR provided by the SET to the V-SLP.

I. The V-SLP returns an RLP SRLIA message. The RLP SRLIA message contains the position result (i.e. the initial position of the SET). If the computed position meets the requested QoP, the H-SLP MAY proceed directly to step K and not engage in a SUPL POS session.

J. Based on the SUPL POS INIT message including posmethod(s) supported by the SET, the H-SLP SHALL determine the posmethod. If required for the posmethod, the H-SLP SHALL use the supported positioning protocol (e.g., RRLP, RRC, TIA-801 or LPP/LPPe) from the SUPL POS INIT message.
The SET and the H-SLP exchange several successive positioning procedure messages.
The H-SLP calculates the position estimate based on the received positioning measurements (SET assisted) or the SET calculates the position estimate based on assistance obtained from the H-SLP (SET based).

K. The H-SLP applies subscriber privacy against the SET position estimate determined in Step J. If, based on this position, notification and verification or notification only is required, the H-SLP SHALL send a SUPL NOTIFY

message to the SET. The SUPL NOTIFY message contains notification element. If, based on this position, no notification and verification is required, the H-SLP SHALL directly proceed to Step M.

L. The SET SHALL send a SUPL NOTIFY RESPONSE message to the H-SLP. If notification and verification was required in step K then this will contain the notification response from the user.

M. Once the position calculation is complete the H-SLP sends a SUPL END message to the SET informing it that no further positioning procedure will be started and that the location session is finished. The SET SHALL release the secure connection to the H-SLP and release all resources related to this session.

N. The H-SLP forwards the location estimate to R-SLP if the position estimate is allowed by the privacy settings of the target subscriber. The H-SLP SHALL release all resources related to this session.

O. The R-SLP sends the position estimate back to the SUPL Agent in an MLP SLIA message.

5.1.12.5 Roaming with V-SPC Positioning Successful Case – Non-Proxy-mode

SET Roaming where the V-SPC is involved in the positioning calculation.

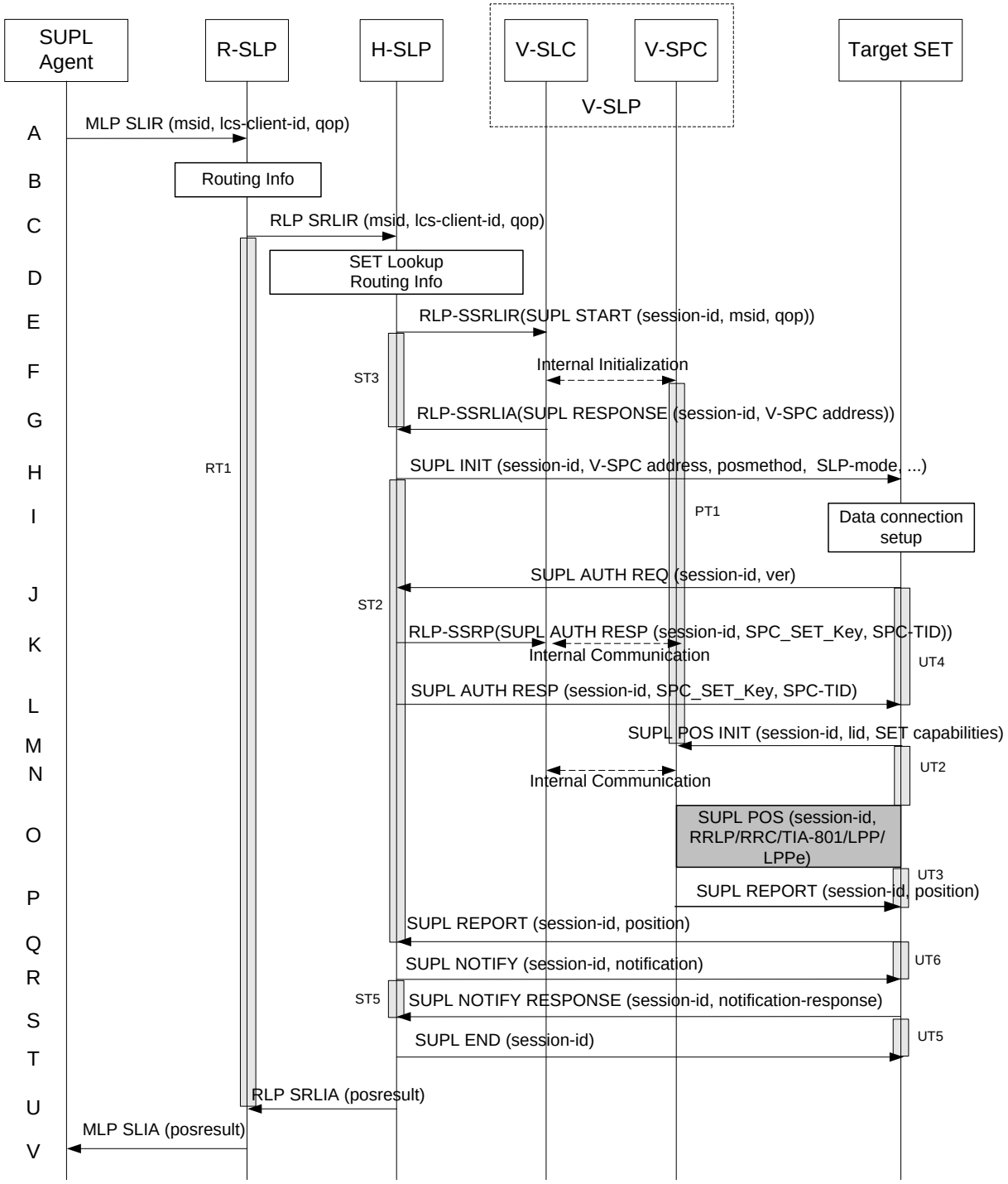

Figure 25: Notification/Verification based on current location. Network Initiated Roaming with V-SPC Positioning Successful Case – Non-Proxy-mode

NOTE: See Appendix D for timer descriptions.

A. The SUPL Agent issues an MLP SLIR message to the R-SLC, with which SUPL Agent is associated. The R-SLP SHALL authenticate the SUPL Agent and check if the SUPL Agent is authorized for the service it requests, based on the client-id received.

B. The R-SLP determines the H-SLP based on the received msid. If the R-SLP determines that the SUPL Agent is not authorized for this request, Step V will be returned with the applicable MLP return code.

NOTE: The specifics for determining the H-SLP are considered outside scope of SUPL. However, there are various environment dependent mechanisms.

C. The R-SLP then forwards the location request to the H-SLP of the target subscriber, using RLP protocol. If a previously computed position which meets the requested QoP is available at the H-SLP and, based on that position, no notification or verification is required, the H-SLP SHALL directly proceed to step U. If, based on that position, notification and verification or notification only is required, the H-SLP SHALL proceed to step H after having performed the SET Lookup and Routing Info procedures of step D. Based on the received ms-id the H-SLP SHALL apply subscriber privacy against the client-id.

D. The H-SLP verifies that the target SET is currently SUPL roaming. In addition the H-SLP MAY also verify that the target SET supports SUPL.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside scope of SUPL. However, there are various environment dependent mechanisms.

E. The H-SLP allocates a session-id for the SUPL session and decides that the V-SPC will provide assistance data or perform the position calculation. The H-SLP sends an RLP SSRLIR to the V-SLC to inform the V-SLC that the target SET will initiate a SUPL positioning procedure. Mandatory parameters in SUPL START that are not known to H-SLP (lid and SET capabilities) shall be populated with arbitrary values by H-SLP and be ignored by V-SLP. If the result of the privacy check in Step C indicates that notification and verification is based on the actual location of the target SET user, the H-SLP will inform the V-SLC accordingly.

F. The V-SLC informs the V-SPC of a SUPL positioning session. As in this case the result of the privacy check in Step D indicates that notification or verification is based on the actual location of the target SET user, the V-SLC will inform the V-SPC that the collaboration between V-SLC and V-SPC is needed to apply subscriber privacy against the client-id once location is computed.

G. The V-SLC acknowledges that V-SPC is ready to engage in a SUPL positioning procedure with an RLP SSRLIA back to the H-SLP. The message includes the address of the V-SPC.

H. The H-SLP initiates the location session with the SET using the SUPL INIT message. The SUPL INIT message contains at least session-id, address of the V-SPC, proxy/non-proxy mode indicator and the intended positioning method. If the result of the privacy check in Step D indicates that subscriber privacy check based on current location is required, the H-SLP SHALL include the Notification Mode element in the SUPL INIT message to indicate notification based on current location and SHALL NOT include the notification element in the SUPL INIT message.

I. The SET analyses the received SUPL INIT. If found to be non authentic SET takes not further actions. Otherwise the SET takes needed action preparing for establishment or resumption of a secure connection. If in step C the H-SLP decided to use a previously computed position the SUPL INIT message SHALL indicate this in a ‘no position’ posmethod parameter value and the SET SHALL respond with a SUPL END message to the H-SLP carrying the results of the verification process (access granted, or access denied). If no verification is required (notification only) the SET SHALL respond with a SUPL END message to the H-SLP. The H-SLP SHALL then directly proceed to step U.

J. The SET uses the address provisioned by the Home Network to establish a connection to the H-SLP. The SET then checks the proxy/non-proxy mode indicator to determine if the H-SLP uses proxy or non-proxy mode. In this case non-proxy mode is used and the SET SHALL send a SUPL AUTH REQ message to the H-SLP. The SUPL AUTH REQ message contains the session-id and a hash of the received SUPL INIT message (ver).

K. The H-SLC creates SPC_SET_Key and SPC-TID to be used for mutual V-SPC/SET authentication. The H-SLP forwards SPC_SET_Key and SPC-TID to the V-SLC through an RLP SSRP message. The V-SLC forwards SPC_SET_Key and SPC-TID to the V-SPC through internal communication.

L. The H-SLP returns a SUPL AUTH RESP to the SET. The SUPL AUTH RESP message SHALL contain the session-id, SPC_SET_Key and SPC-TID.

M. The SET will evaluate the Notification rules and follow the appropriate actions. The SET checks the notification mode indicator and determines that in this case the notification is performed based on the location of the SET. The SET establishes a secure connection to the V-SPC according to the address received in step H. The SET and V-SPC perform mutual authentication and the SET sends a SUPL POS INIT message to start a SUPL positioning session with the V-SPC. The SUPL POS INIT message contains at least session-id, SET capabilities and Location ID (lid). The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS)

and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe). The SET MAY provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if these are available and supported by both SET and V-SPC. The SET MAY set the Requested Assistance Data element in the SUPL POS INIT. The SET SHALL also release the connection to the H-SLP.

N. The V-SPC informs the V-SLC that the positioning procedure is started. The V-SLC and the V-SPC may collaborate to determine an initial position of the SET to aid in the position determination process. If the initial position calculated based on information received in the SUPL POS INIT message meets the requested QoP, the V-SPC MAY directly proceed to step P and not engage in a SUPL POS session.

O. Based on the SUPL POS INIT message including posmethod(s) supported by the SET, the V-SPC SHALL determine the posmethod. If required for the posmethod, the V-SPC SHALL use the supported positioning protocol (e.g., RRLP, RRC, TIA-801 or LPP/LPPe) from the SUPL POS INIT message.
The SET and the V-SPC exchange several successive positioning procedure messages.
The V-SPC calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance obtained from the V-SPC (SET-Based).

P. As in this case in step F the V-SLC indicated that notification or verification is based on the position of the SET, the V-SPC sends the calculated position to the SET in a SUPL REPORT message

Q. As in this case in step H the H-SLP indicated that notification or verification is based on the position of the SET, the SET sends the calculated position to the H-SLP in a SUPL REPORT message.

R. The H-SLP applies subscriber privacy against the SET position estimate. If, based on this position, notification and verification or notification only is required, the H-SLP SHALL send a SUPL NOTIFY message to the SET. The SUPL NOTIFY message contains notification element. If, based on this position, no notification and verification is required, the H-SLP SHALL directly proceed to Step T.

S. The SET SHALL then send an SUPL NOTIFY RESPONSE message to the H-SLP. If notification and verification was required in step R then this will contain the notification response from the user.

T. Once the position calculation is complete the H-SLP sends a SUPL END message to the SET informing it that no further positioning procedure will be started and that the positioning session is finished. The SET SHALL release all resources related to this session.

U. The H-SLP sends the position estimate back to the R-SLP in an RLP SRLIA message. The H-SLP SHALL release all resources related to this session.

V. The R-SLP sends the position estimate back to the SUPL Agent in an MLP SLIA message.

5.1.12.6 Roaming with H-SPC Positioning Successful Case – Non-Proxy-mode

SUPL Roaming where the H-SPC is involved in the positioning calculation.

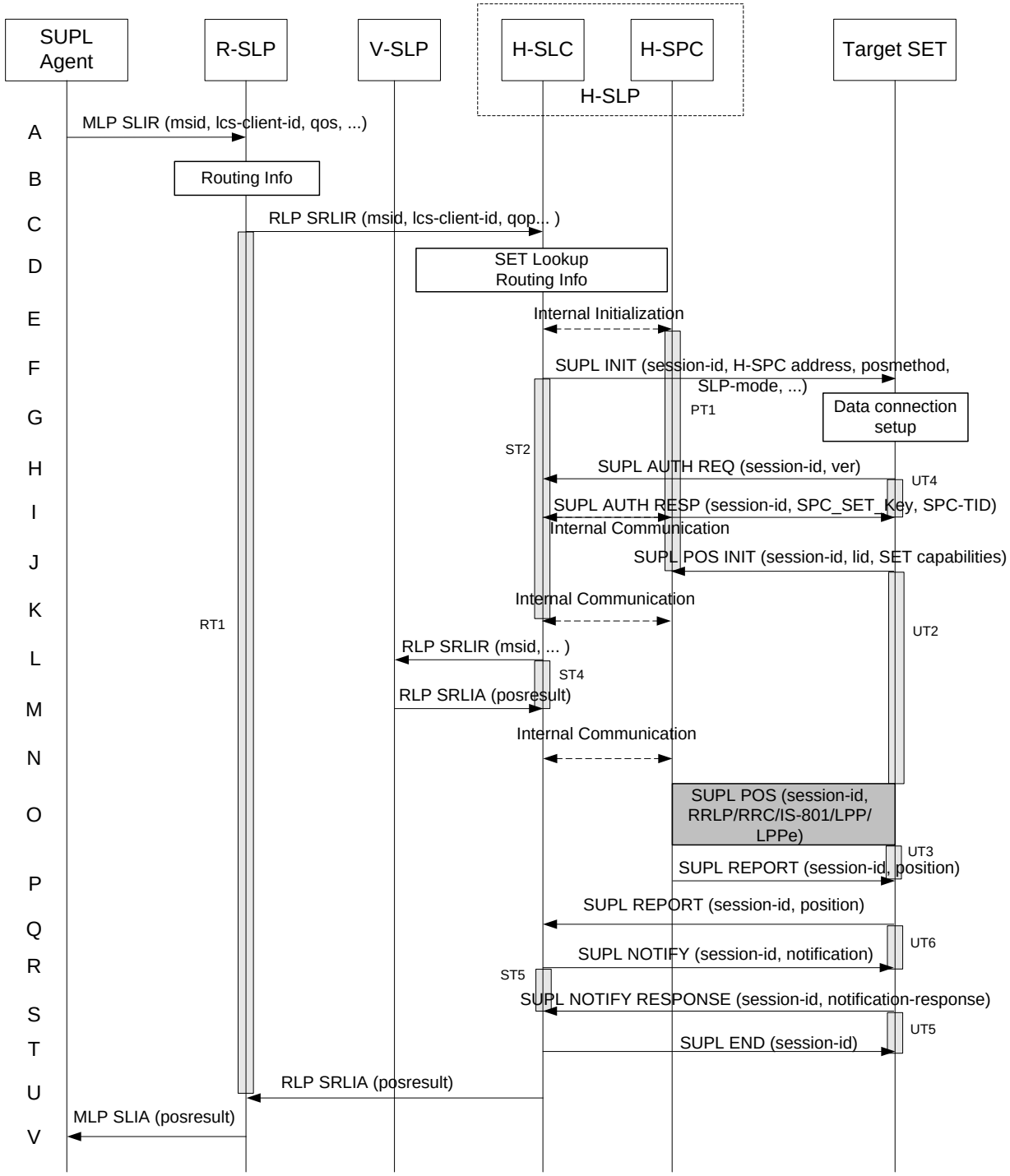

Figure 26: Notification/Verification based on current location. Network Initiated Roaming with H-SPC Positioning Successful Case – Non-Proxy-mode

NOTE: See Appendix D for timer descriptions.

A. The SUPL Agent issues an MLP SLIR message to the Requesting-SLP, with which SUPL Agent is associated. The Requesting-SLP SHALL authenticate the SUPL Agent and check if the SUPL Agent is authorized for the service it requests, based on the client-id received.

B. The R-SLP determines the H-SLP based on the received msid. If the R-SLP determines that the SUPL Agent is not authorized for this request, Step V will be returned with the applicable MLP return code.

NOTE: The specifics for determining the H-SLP are considered outside scope of SUPL. However, there are various environment dependent mechanisms.

C. The R-SLP then forwards the location request to the H-SLC of the target subscriber, using RLP protocol. If a previously computed position which meets the requested QoP is available at the H-SLC and, based on that position, no notification or verification is required, the H-SLC SHALL directly proceed to step U. If, based on that position, notification and verification or notification only is required, the H-SLC SHALL proceed to step F after having performed the SET Lookup and Routing Info procedures of step D.

D. Based on the received ms-id the H-SLC SHALL apply subscriber privacy against the client-id. The H-SLC verifies that the target SET is currently SUPL roaming. In addition the H-SLC MAY also verify that the target SET supports SUPL.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside scope of SUPL. However, there are various environment dependent mechanisms.

NOTE: Alternatively, the H-SLC may determine whether the SET is SUPL roaming in a later step using the location identifier (lid) received from the SET.

E. The H-SLC informs the H-SPC of the pending SUPL positioning session.

F. The H-SLC initiates the location session with the SET using the SUPL INIT message. The SUPL INIT message contains at least session-id, address of the H-SPC, proxy/non-proxy mode indicator and the intended positioning method. As in this case the result of the privacy check in Step D indicates that subscriber privacy check based on current location is required, the H-SLC SHALL include the Notification Mode element in the SUPL INIT message to indicate notification based on current location and SHALL NOT include the notification element in the SUPL INIT message.
If in step C the H-SLC decided to use a previously computed position the SUPL INIT message SHALL indicate this in a 'no position' posmethod parameter value and the SET SHALL respond with a SUPL END message to the H-SLC carrying the results of the verification process (access granted, or access denied). If no verification is required (notification only) the SET SHALL respond with a SUPL END message to the H-SLC. The H-SLC SHALL then directly proceed to step U.

NOTE: Before sending the SUPL END message the SET SHALL perform the data connection setup procedure of step G.

G. The SET analyses the received SUPL INIT. If found to be non authentic SET takes not further actions. Otherwise the SET takes needed action preparing for establishment or resumption of a secure connection.

H. The SET uses the address provisioned by the Home Network to establish a secure connection to the H-SLC. The SET then checks the proxy/non-proxy mode indicator to determine if the H-SLC uses proxy or non-proxy mode. In this case non-proxy mode is used and the SET SHALL send a SUPL AUTH REQ message to the H-SLC. The SUPL AUTH REQ message contains the session-id and a hash of the received SUPL INIT message (ver).

I. The H-SLC creates SPC_SET_Key and SPC-TID to be used for mutual H-SPC/SET authentication. The H-SLC forwards SPC_SET_Key and SPC-TID to the H-SPC through internal communication and returns a SUPL AUTH RESP message including SPC_SET_Key and SPC-TID to the SET.

J. The SET will evaluate the Notification rules and follow the appropriate actions. The SET checks the notification mode indicator and determines that in this case the notification is performed based on the location of the SET. The SET establishes a secure connection to the H-SPC according to the address received in step F. The SET and H-SPC perform mutual authentication and the SET then sends a SUPL POS INIT message to start a positioning session with the H-SPC. The SUPL POS INIT message contains at least session-id, SET capabilities and Location ID (lid). The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe). The SET MAY provide NMR specific data for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if these are available and supported by both SET and H-SPC. The SET MAY set the Requested Assistance Data element in the SUPL POS INIT. The SET SHALL also release the connection to the H-SLC and release all resources related to this session.

K. The H-SLC and H-SPC may collaborate to determine an initial position of the SET to aid in the position determination process. If the initial position calculated based on information received in the SUPL POS INIT message meets the requested QoP, the H-SPC MAY directly proceed to step P.

L. The H-SLC sends an RLP SRLIR request to the V-SLP to determine an initial position for the SET . The RLP request contains at least the msid and the Location ID (lid). Optionally the H-SLC MAY forward NMR provided by the SET to the V-SLP.

M. The V-SLP returns an RLP SRLIA message. The RLP SRLIA message contains the position result (i.e. the initial position of the SET).

N. The H-SLC sends the initial position to the H-SPC. If the initial position meets the requested QoP, the H-SPC MAY proceed directlyto step P without engaging in a SUPL POS session.

O. Based on the SUPL POS INIT message including posmethod(s) supported by the SET the H-SPC SHALL determine the posmethod. If required for the posmethod the H-SPC SHALL use the supported positioning protocol (e.g., RRLP, RRC, TIA-801 or LPP/LPPe) from the SUPL POS INIT message.
The SET and the H-SPC exchange several successive positioning procedure messages.
The H-SPC calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance obtained from the H-SPC (SET-Based).

P. As in this case in step E the H-SLC indicated that notification or verification is based on the position of the SET, the H-SPC sends the calculated position to the SET in a SUPL REPORT message.

Q. As in this case in step F the H-SLC indicated that notification or verification is based on the position of the SET, the SET sends the calculated position to the H-SLC in a SUPL REPORT message.

R. The H-SLC applies subscriber privacy against the SET position estimate. If, based on this position, notification and verification or notification only is required, the H-SLP SHALL send a SUPL NOTIFY message to the SET. The SUPL NOTIFY message contains notification element. If, based on this position, no notification and verification is required, the H-SLP SHALL directly proceed to Step T.

S. The SET SHALL then send an SUPL NOTIFY RESPONSE message to the H-SLC. If notification and verification was required in step R then this will contain the notification response from the user.

T. Once the position calculation is complete the H-SLC sends SUPL END message to the SET informing it that no further positioning procedure will be started and that the positioning session is finished. The SET SHALL release all resources related to this session.

U. The H-SLC sends the position estimate back to the R-SLP in an RLP SRLIA message. The H-SLC SHALL release all resources related to this session.

V. The R-SLP sends the position estimate back to the SUPL Agent by means in an MLP SLIA message.

5.1.13 Retrieval of Historical Positions and/or Enhanced Cell Sector Measurements

In SUPL 2.0 a SET may store calculated positions and/or network measurements for later retrieval by the network. This section describes the retrieval of stored historical positions and/or enhanced cell/sector measurements.

Please note that the concept of non-proxy mode does not apply since the SET is not involved in a positioning session i.e. does not directly communicate with the SPC.

5.1.13.1 Retrieval of Historical Position Results – non-roaming successful case

The following call flow defines the retrieval of historical position results from the SET for non-roaming.. In the context of retrieval of historical position and/or enhanced cell/sector measurements non-roaming means that enhanced cell/sector measurements which the SET reports were taken while the SET was not SUPL roaming.

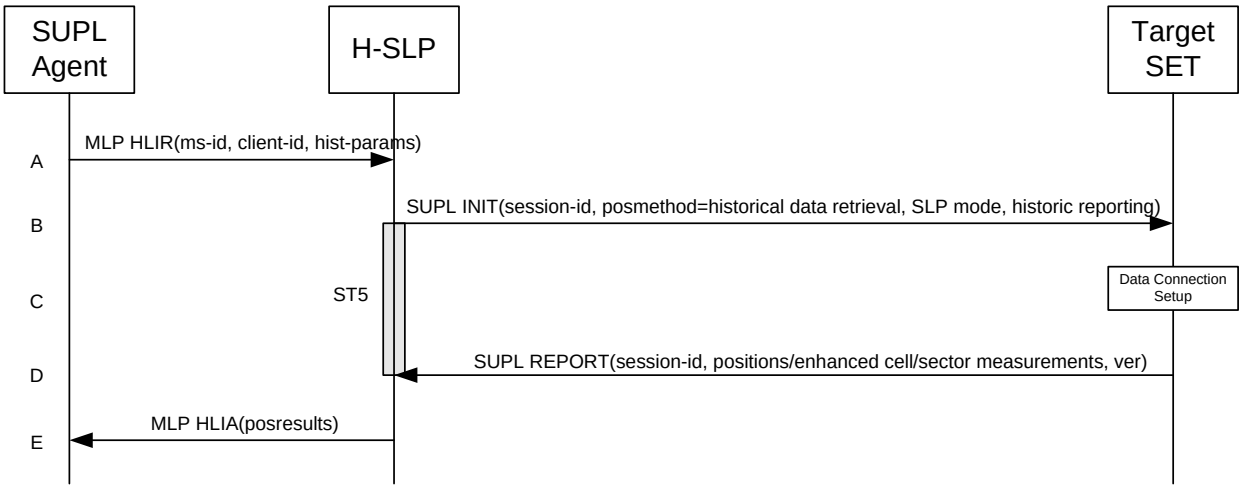

Figure 27: Retrieval of historical positions and/or enhanced cell/sector measurements – non-roaming

NOTE: See Appendix D for timer descriptions.

A. The SUPL Agent issues an MLP HLIR message to the H-SLP, with which SUPL Agent is associated. The H-SLP SHALL authenticate the SUPL Agent and check if the SUPL Agent is authorized for the service it requests, based on the client-id received. Further, based on the received ms-id the H-SLP SHALL apply subscriber privacy against the client-id. The hist-params parameter in the HLIR message defines criteria to be applied by the SET when selecting historical position to be reported to the SUPL Agent (e.g. time window, QoP, etc.).

B. The H-SLP initiates the retrieval of historical positions with the SET using the SUPL INIT message. The SUPL INIT message contains at least session-id, posmethod, SLP mode and criteria for selecting stored historical position estimates and/or stored enhanced cell/sector measurements (historic reporting and optionally QoP). Historical data retrieval is indicated by posmethod: *historical data retrieval*. If the result of the privacy check in Step A indicates that notification or verification to the target subscriber is needed, the H-SLP SHALL also include the Notification element in the SUPL INIT message. Before the SUPL INIT message is sent, the H-SLP also computes and stores a hash of the message.

C. The SET analyses the received SUPL INIT. If found to be non authentic SET takes not further actions. Otherwise the SET takes needed action preparing for establishment or resumption of a secure connection.

D. The SET will evaluate the Notification rules and follow the appropriate actions. The SET then establishes a secure connection to the H-SLP using an H-SLP address that has been provisioned by the Home Network to the SET. The SET selects historical position estimates and/or historic enhanced cell/sector measurements based on the criteria received in step B and sends the positions and/or enhanced cell/sector measurements in a SUPL REPORT message to the H-SLP. The SUPL REPORT message contains at least the session-id and a hash of the received SUPL INIT message (ver). After sending the SUPL REPORT message, the SET SHALL release all resources related to this session.

E. The H-SLP converts any enhanced cell/sector measurements received in step D into corresponding position estimates and reports the historical position estimates to the SUPL Agent in a MLP HLIA message.

5.1.13.2 Retrieval of Historical Position Results – roaming successful case

The following call flow defines the retrieval of historical position results from the SET for roaming. In the context of retrieval of historical position and/or enhanced cell/sector measurements roaming means that enhanced cell/sector measurements reported by the SET were taken while the SET was SUPL roaming.

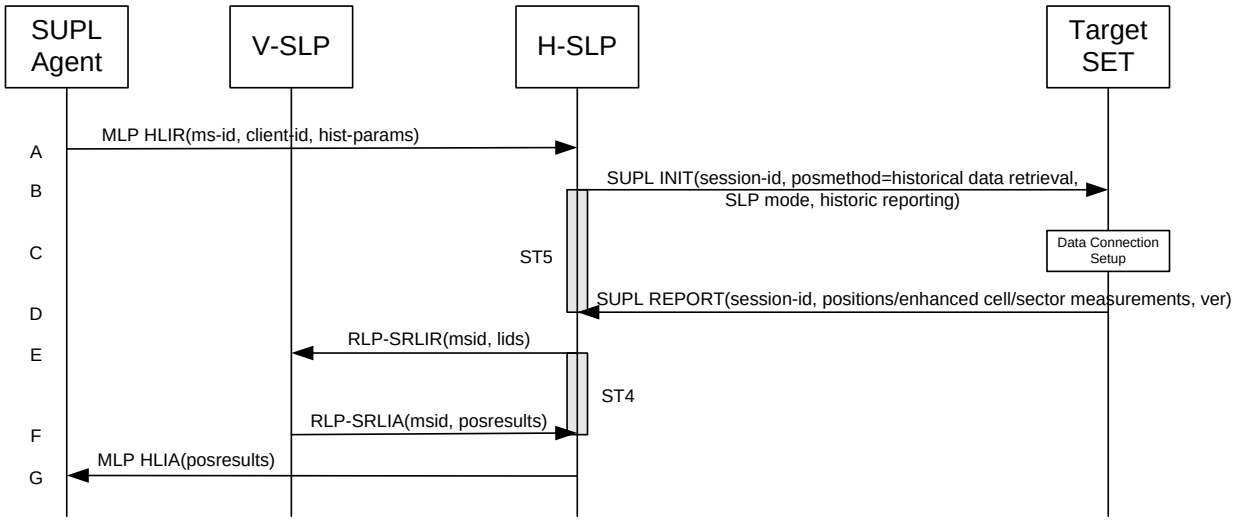

Figure 28: Retrieval of historical positions and/or enhanced cell/sector measurements – roaming

NOTE: See Appendix D for timer descriptions.

A. The SUPL Agent issues an MLP HLIR message to the H-SLP, with which SUPL Agent is associated. The H-SLP shall authenticate the SUPL Agent and check if the SUPL Agent is authorized for the service it requests, based on the client-id received. Further, based on the received ms-id the H-SLP shall apply subscriber privacy against the client-id. The hist-params parameter in the HLIR message defines criteria to be applied by the SET when selecting historical position to be reported to the SUPL Agent (e.g. time window, QoP, etc.).

B. The H-SLP initiates the retrieval of historical positions with the SET using the SUPL INIT message. The SUPL INIT message contains at least session-id, posmethod, SLP mode and criteria for selecting stored historical position estimates and/or stored enhanced cell/sector measurements (historic reporting). Historical data retrieval is indicated by posmethod: *historical data retrieval*. If the result of the privacy check in Step A indicates that notification or verification to the target subscriber is needed, the H-SLP SHALL also include the Notification element in the SUPL INIT message. Before the SUPL INIT message is sent, the H-SLP also computes and stores a hash of the message.

C. The SET analyses the received SUPL INIT. If found to be non authentic SET takes not further actions. Otherwise the SET takes needed action preparing for establishment or resumption of a secure connection.

D. The SET will evaluate the Notification rules and follow the appropriate actions. The SET then establishes a secure connection to the H-SLP using a H-SLP address that has been provisioned by the Home Network to the SET. The SET selects historical position estimates and/or historic enhanced cell/sector measurements based on the criteria received in step B and sends the positions and/or enhanced cell/sector measurements in a SUPL REPORT message to the H-SLP. The SUPL REPORT message contains at least the session-id and a hash of the received SUPL INIT message (ver). After sending the SUPL REPORT message, the SET SHALL release all resources related to this session.

E. If in step D the H-SLP received enhanced cell/sector measurements, the H-SLP converts them into position estimates. However, enhanced cell/sector measurements taken while the SET was SUPL roaming, cannot to be converted into position estimates by the H-SLP. These measurements are instead forwarded to the respective V-SLP in a RLP-SRLIR message.

F. The V-SLP converts the enhanced cell/sector measurements into position estimates and returns the results to the H-SLP in a RLP-SRLIA message.

G. The H-SLP reports the historical position estimates to the SUPL Agent in an MLP HLIA message.

5.1.14 Network/SET capabilities Change for Area Event Triggered Scenarios

Area Event trigger scenarios which rely on area-ids to determine the trigger condition require updating of trigger parameters after network change. The described mechanism applies to Network Initiated, SET Initiated, Proxy and Non-Proxy scenarios in the exact same way.

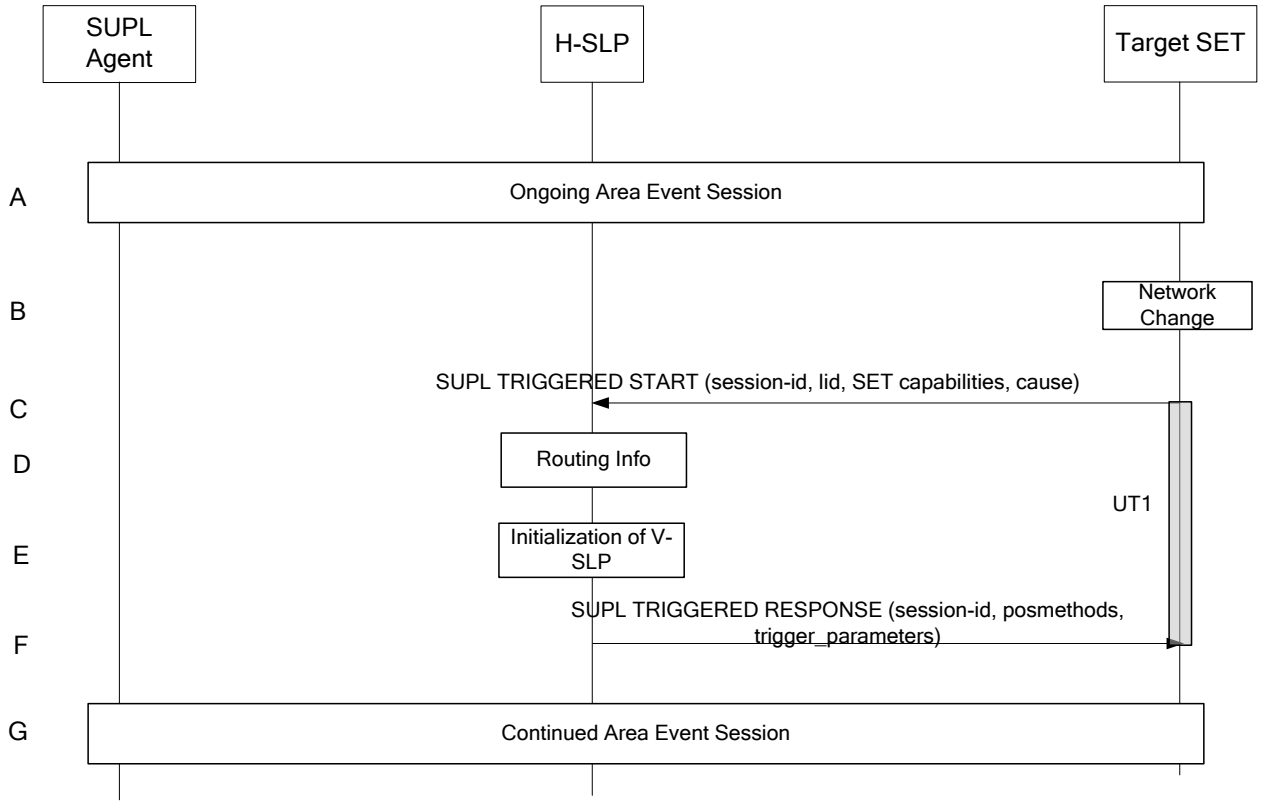

Figure 29: Network/SET capabilities change for Area Event Trigger Scenarios

NOTE: See Appendix D for timer descriptions.

A. An Area Event session is ongoing.

B. The SET monitors serving network identity and SET capabilities. If the SET detects that it has changed networks and the new serving network is not part of any downloaded area id lists or if the SET detects that the SET capabilities have changed the SET continues to step C.

C. The SET attaches itself to the Packet Data Network if it is not already attached or establishes a circuit switched data connection. The SET then sends a SUPL TRIGGERED START message to request new event trigger parameters. The SUPL TRIGGERED START message contains at least session-id, SET capabilities, Location ID (lid) and cause for re-sending the SUPL TRIGGERED START message. The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe).

D. The H-SLP determines based on the lid received in the SUPL TRIGGERED START message if a session with a V-SLP need to be established, terminated or handed over to another V-SLP. If no communication with V-SLP is needed H-SLP proceed to step F.

E. Based on result in step D, H-SLP informs concerned V-SLP's of the change according to section 5.1.9.2 step F & G or section 5.1.11.1 steps G to I.

F. The H-SLP sends SUPL TRIGGERED RESPONSE message to the SET including session-id, the positioning method to be used for the area event triggered session and area event trigger parameters. The SUPL TRIGGERED

RESPONSE message may contain the area ids of the specified area for the area event triggered session. If the H-SLP does not provide new trigger parameters in the SUPL TRIGGERED RESPONSE then the SET SHALL maintain the previous trigger parameters.

G. The Area Event session continues.

5.1.15 Emergency Services Location Requests

Regulatory requirements will dictate the conditions under which the SET should accept emergency SUPL INIT messages. For example, in many cases, the regulatory requirements only require the SET to process emergency SUPL INIT messages if the SET is currently engaged in an emergency call. Consequently, the conditions (under which the SET should accept emergency SUPL INIT messages) are outside the scope of this document.

5.1.15.1 Non-Roaming Successful Case – Proxy mode

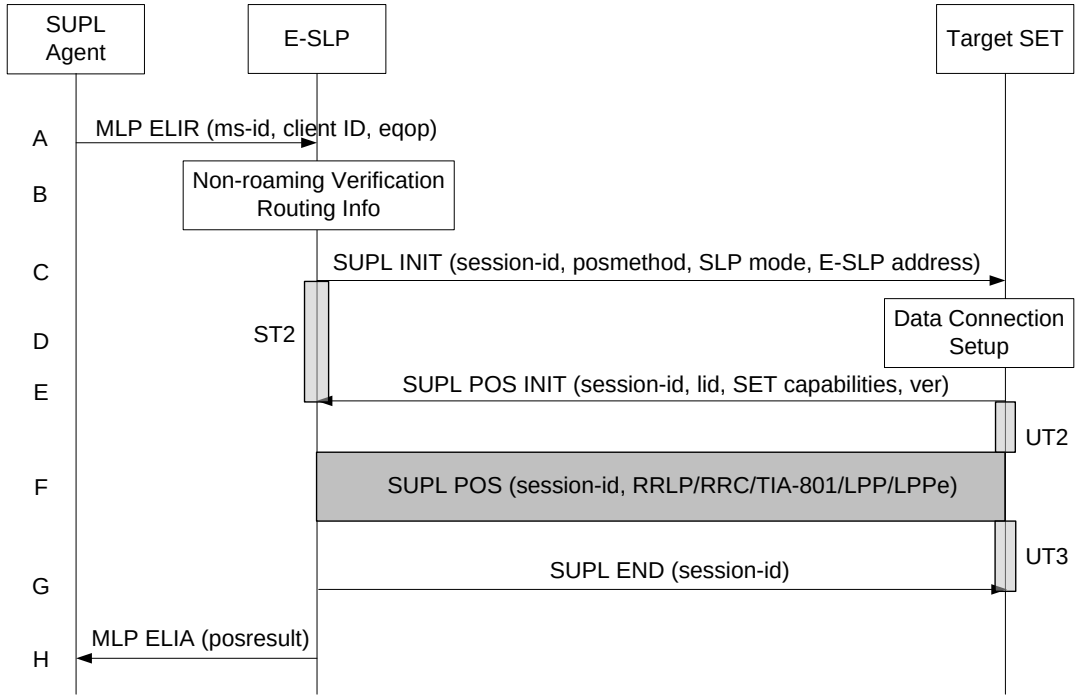

Figure 30: Network Initiated Emergency Services Non-Roaming Successful Case – Proxy Mode

NOTE: See Appendix D for timer descriptions.

A. SUPL Agent issues an MLP ELIR message to the E-SLP, with which SUPL Agent is associated. The MLP ELIR message may include the SET IP address and location data. The E-SLP shall authenticate the SUPL Agent and check if the SUPL Agent is authorized for the service it requests, based on the client-id received.
If a previously computed position which meets the requested QoP is available at the E-SLP and no notification and verification is required according to local regulatory requirements, the E-SLP SHALL directly proceed to step H. If notification and verification or notification only is required, the E-SLP SHALL proceed to step B.

B. The E-SLP verifies that the target SET is currently not SUPL roaming.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside the scope of SUPL. However, there are various environment dependent mechanisms.

C. The E-SLP initiates the location session with the SET using the SUPL INIT message. The SUPL INIT message contains at least session-id, proxy/non-proxy mode indicator and the intended positioning method. The SUPL INIT SHALL contain the E-SLP address if the E-SLP is not the H-SLP for the SET. The SUPL INIT MAY contain the desired QoP. The E-SLP SHALL also include Notification element in the SUPL INIT message indicating location for emergency services and, according to local regulatory requirements, whether notification or verification to the target SET is or is not required. Before the SUPL INIT message is sent the E-SLP also computes and stores a hash of the message.

If in step A the E-SLP decided to use a previously computed position, the SUPL INIT message SHALL indicate this in a 'no position' posmethod parameter value and the SET SHALL respond with a SUPL END message carrying the results of the verification process (access granted, or access denied). If no explicit verification is required (notification only) the SET SHALL respond with a SUPL END message. The E-SLP SHALL then directly proceed to step H.

NOTE: Before sending the SUPL END message the SET SHALL perform the data connection setup procedure of step D and use the procedures described in step E to establish an IP connection to the E-SLP.

D. The SET takes needed action preparing for establishment or resumption of a secure connection.

E. The SET will evaluate the Notification rules and follow the appropriate actions. The SET also checks the proxy/non-proxy mode indicator to determine if the E-SLP uses proxy or non-proxy mode. In this case, proxy mode is used, and the SET SHALL establish a secure connection to the E-SLP using either the provisioned H-SLP or defaulted E-SLP address, if no E-SLP address was received in step C, or the E-SLP address received in step C. The SET then sends a SUPL POS INIT message to start a positioning session with the E-SLP. The SET SHALL send the SUPL POS INIT message even if the SET supported positioning technologies do not include the intended positioning method indicated in the SUPL INIT message. The SUPL POS INIT message contains at least session-id, SET capabilities, a hash of the received SUPL INIT message (ver) and Location ID (lid). The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe). The SET MAY provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if this is supported. The SET MAY set the Requested Assistance Data element in the SUPL POS INIT.
If a coarse position calculated based on information received in the SUPL POS INIT message is available that meets the required QoP, the E-SLP SHALL directly proceed to step G and not engage in a SUPL POS session.

F. The E-SLP SHALL check that the hash of SUPL INIT matches the one it has computed for this particular session. Based on the SUPL POS INIT message including posmethod(s) supported by the SET the E-SLP SHALL then determine the posmethod. If required for the posmethod the E-SLP SHALL use the supported positioning protocol (e.g., RRLP, RRC, TIA-801 or LPP/LPPe) from the SUPL POS INIT message.
The SET and the E-SLP MAY exchange several successive positioning procedure messages.
The E-SLP calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance obtained from the E-SLP (SET-Based).

G. Once the position calculation is complete the E-SLP sends the SUPL END message to the SET informing it that no further positioning procedure will be started and that the location session is finished. The SET SHALL release the IP connection to the E-SLP and release all resources related to this session.

H. The E-SLP sends the position estimate back to the SUPL Agent by means of the MLP ELIA message and the E-SLP SHALL release all resources related to this session.

5.1.15.2 Non-Roaming Successful Case – Non-Proxy mode

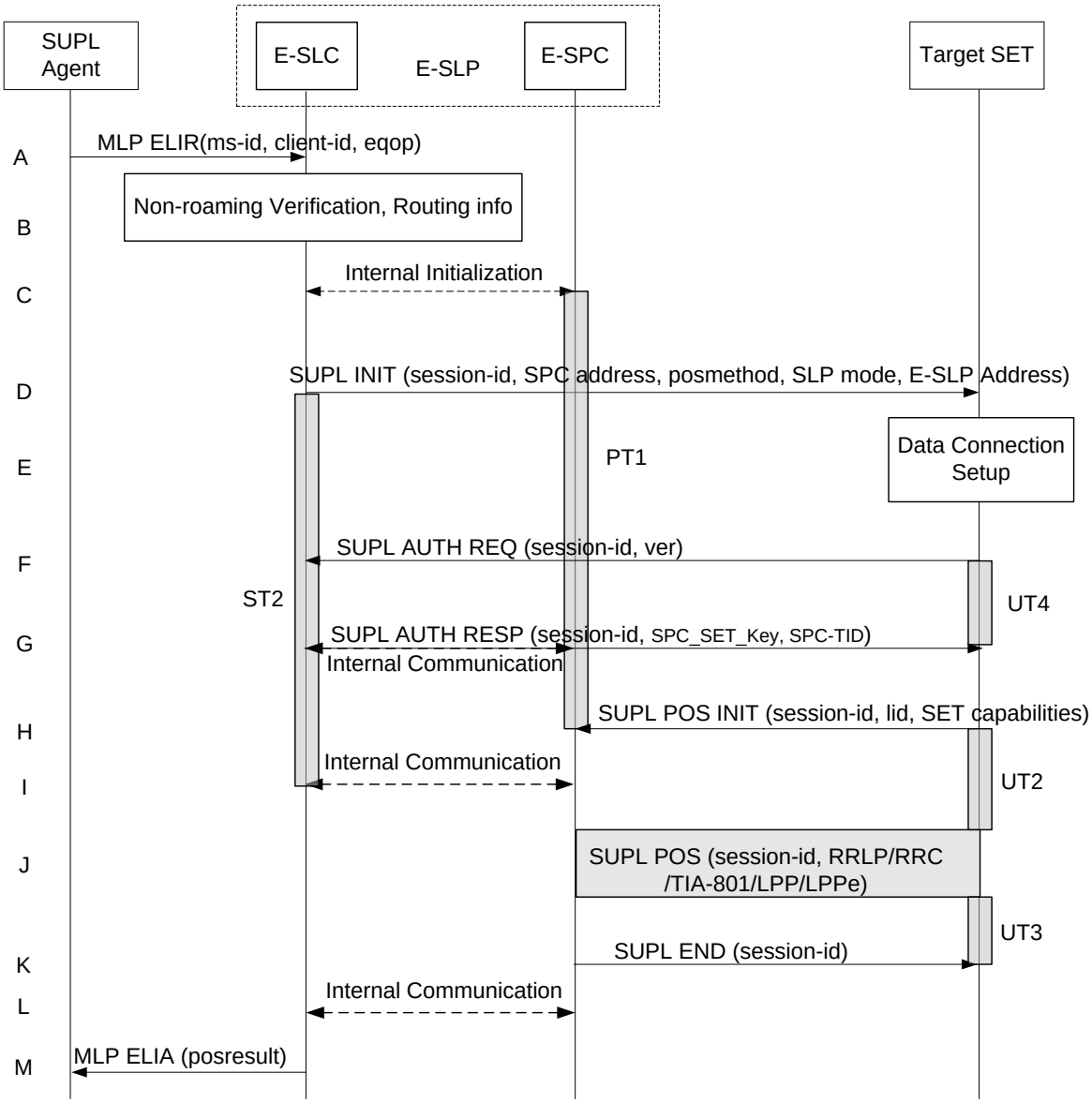

Figure 31: Network Initiated Emergency Sevices Non-Roaming Successful Case – Non-Proxy mode

NOTE: See Appendix D for timer descriptions.

A. SUPL Agent issues an MLP ELIR message to the SLC component of the E-SLP, with which SUPL Agent is associated. The MLP ELIR message may include the SET IP address and location data. The E-SLC shall authenticate the SUPL Agent and check if the SUPL Agent is authorized for the service it requests, based on the client-id received.
If a previously computed position which meets the requested QoP is available at the E-SLC and no notification and verification is required according to local regulatory requirements, the E-SLC SHALL directly proceed to step M. If notification and verification or notification only is required, the E-SLC SHALL proceed to step B.

B. The E-SLP verifies that the target SET is currently not SUPL roaming.
The E-SLC MAY also verify that the target SET supports SUPL.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside scope of SUPL. However, there are various environment dependent mechanisms.

C. The E-SLC and E-SPC may exchange information necessary to setup the SUPL POS session.

D. The E-SLC initiates the location session with the SET using the SUPL INIT message. The SUPL INIT message contains at least session-id, address of the SPC, proxy/non-proxy mode indicator and the intended positioning method. The SUPL INIT SHALL contain the E-SLP address if the E-SLP is not the H-SLP for the SET. The SUPL INIT MAY contain the desired QoP. The E-SLC shall also include the Notification element in the SUPL INIT message indicating location for emergency services and, according to local regulatory requirements, whether notification or verification to the target SET is or is not required.
If in step A the E-SLC decided to use a previously computed position, the SUPL INIT message SHALL indicate this in a 'no position' posmethod parameter value and the SET SHALL respond with a SUPL END message carrying the results of the verification process (access granted, or access denied). If no explicit verification is required (notification only) the SET SHALL respond with a SUPL END message. The E-SLC SHALL then directly proceed to step M.

NOTE: Before sending the SUPL END message the SET SHALL perform the data connection setup procedure of step E and use the procedures described in step F to establish an IP connection to the E-SLC.

E. The SET takes needed action preparing for establishment or resumption of a secure connection.

F. The SET establishes a secure connection to the E-SLC using either the provisioned H-SLP or defaulted E-SLP address, if no E-SLP address was received in step D, or the E-SLP address provided in step D. The SET then checks the proxy/non-proxy mode indicator to determine if the E-SLP uses proxy or non-proxy mode. In this case non-proxy mode is used and the SET SHALL send a SUPL AUTH REQ message to the E-SLC.The SUPL AUTH REQ message contains the session-id and a hash of the received SUPL INIT message (ver).

G. The E-SLC creates SPC_SET_Key and SPC-TID to be used for mutual E-SPC/SET authentication and sends both in an SUPL AUTH RESP message to the SET. The E-SLC also forwards SPC_SET_Key and SPC-TID to the E-SPC through internal communication.

H. The SET will evaluate the Notification rules and follow the appropriate actions. The SET establishes an IP connection to the E-SPC according to the address received in step D. The SET and E-SPC may perform mutual authentication and the SET sends a SUPL POS INIT message to start a positioning session with the E-SPC. The SET SHALL send the SUPL POS INIT message even if the SET supported positioning technologies do not include the intended positioning method indicated in the SUPL INIT message. The SUPL POS INIT message contains at least session-id, SET capabilities and Location ID (lid). The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe). The SET MAY provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if this is supported. The SET MAY set the Requested Assistance Data element in the SUPL POS INIT. The SET SHALL also release the IP connection to the E-SLC and release all resources related to this session.

I. The E-SLC and E-SPC may collaborate to determine the initial location or coarse location of the SET to aid in the position determination process. If the initial location meets the requested QoP, the E-SLP proceeds directly to step K.

J. Based on the SUPL POS INIT message including posmethod(s) supported by the SET the E-SPC SHALL determine the posmethod. If required for the posmethod the E-SPC SHALL use the supported positioning protocol (e.g., RRLP, RRC, TIA-801 or LPP/LPPe) from the SUPL POS INIT message
The SET and the E-SPC MAY exchange several successive positioning procedure messages.
The E-SPC calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance obtained from the E-SPC (SET-Based).

K. Once the position calculation is complete the E-SPC sends the SUPL END message to the SET informing it that no further positioning procedure will be started and that the SUPL session is finished. The SET SHALL release the IP connection to the E-SPC and release all resources related to this session.

L. The E-SPC also informs the E-SLC of the end of the SUPL session. Unless the E-SLC already knows the position, e.g., from step I, the E-SPC informs the E-SLC of the determined position from step J. The E-SPC SHALL release all resources related to this session.

M. The E-SLC sends the position estimate back to the SUPL Agent using an MLP ELIA message. The E-SLC SHALL release all resources related to this session.

5.1.15.3 Roaming with V-SLP Positioning Successful Case – Proxy mode

SUPL Roaming where the V-SLP is involved in the positioning calculation.

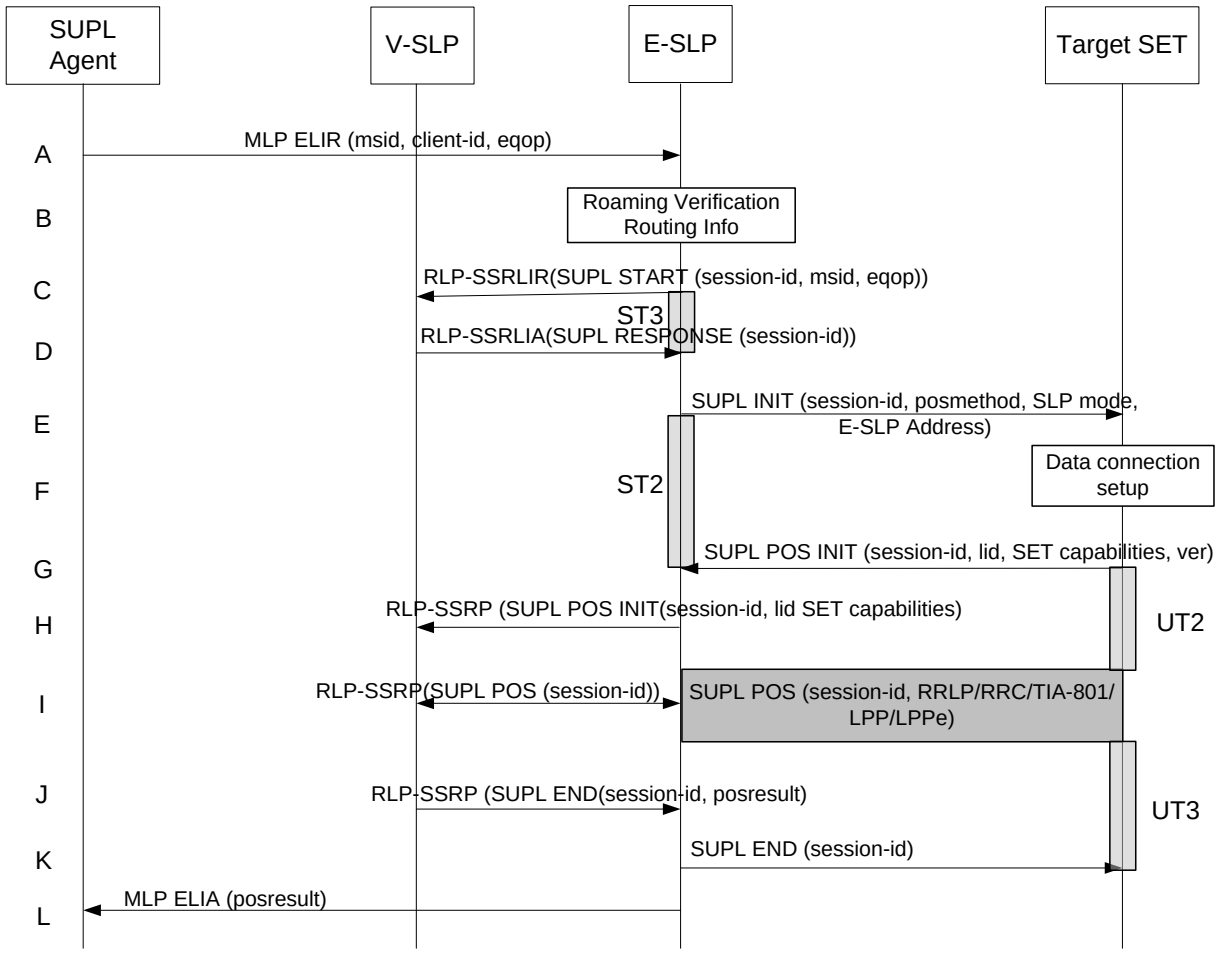

Figure 32: Network Initiated Emergency Services Roaming with V-SLP Positioning Successful Case – Proxy mode

NOTE: See Appendix D for timer descriptions.

A. SUPL Agent issues an MLP ELIR message to the E-SLP, with which SUPL Agent is associated. The MLP ELIR message may include the SET IP address and location data. The E-SLP SHALL authenticate the SUPL Agent and check if the SUPL Agent is authorized for the service it requests, based on the client-id received. If a previously computed position which meets the requested QoP is available at the E-SLP and no notification and verification is required according to local regulatory requirements, the E-SLP SHALL directly proceed to step L. If notification and verification or notification only is required, the E-SLP SHALL proceed to step E.

B. The E-SLP verifies that the target SET is currently SUPL roaming.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside the scope of SUPL. However, there are various environment dependent mechanisms.

C. The E-SLP sends an RLP SSRLIR to the V-SLP to inform the V-SLP that the target SET will initiate a SUPL positioning procedure. Mandatory parameters in SUPL START that are not known to E-SLP (lid and SET capabilities) shall be populated with arbitrary values by E-SLP and be ignored by V-SLP. The SET part of the session-id will not be included in this message by the E-SLP to distinguish this scenario from a SET Initiated scenario.

D. The V-SLP acknowledges that it is ready to initiate a SUPL positioning procedure with an RLP SSRLIA back to the E-SLP.

E. The E-SLP initiates the location session with the SET using the SUPL INIT message. The SUPL INIT message contains at least session-id, proxy/non-proxy mode indicator and the intended positioning method. The SUPL INIT SHALL contain the E-SLP address if the E-SLP is not the H-SLP for the SET. The SUPL INIT MAY contain the desired QoP. The E-SLP SHALL also include Notification element in the SUPL INIT message indicating location for emergency services and, according to local regulatory requirements, whether notification or verification to the target SET is or is not required. Before the SUPL INIT message is sent the E-SLP also computes and stores a hash of the message.
If in step A the E-SLP decided to use a previously computed position the SUPL INIT message SHALL indicate this in a 'no position' posmethod parameter value and the SET SHALL respond with a SUPL END message to the E-SLP carrying the results of the verification process (access granted, or access denied). If no verification is required (notification only) the SET SHALL respond with a SUPL END message to the E-SLP. The E-SLP SHALL then directly proceed to step L.

NOTE: Before sending the SUPL END message the SET SHALL perform the data connection setup procedure of step F and use the procedures described in step G to establish an IP connection to the E-SLP.

F. The SET takes needed action preparing for establishment or resumption of a secure connection.

G. The SET will evaluate the Notification rules and follow the appropriate actions. The SET also checks the proxy/non-proxy mode indicator to determine if the E-SLP uses proxy or non-proxy mode. In this case, proxy mode is used, and the SET SHALL establish a secure connection to the E-SLP using either the provisioned H-SLP or defaulted E-SLP address, if no E-SLP address was received in step E, or the E-SLP address received in step E. The SET then sends a SUPL POS INIT message to start a positioning session with the E-SLP. The SET SHALL send the SUPL POS INIT message even if the SET supported positioning technologies do not include the intended positioning method indicated in the SUPL INIT message. The SUPL POS INIT message contains at least session-id, SET capabilities, a hash of the received SUPL INIT message (ver) and Location ID (lid). The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe). The SET MAY optionally provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if this is supported. The SET MAY set the Requested Assistance Data element in the SUPL POS INIT.

H. The E-SLP SHALL check that the hash of SUPL INIT matches the one it has computed for this particular session. The E-SLP then tunnels the SUPL POS INIT message to the V-SLP.

I. Based on the SUPL POS INIT message including posmethod(s) supported by the SET, the V-SLP SHALL determine the posmethod. If required for the posmethod, the V-SLP SHALL use the supported positioning protocol (e.g., RRLP, RRC, TIA-801 or LPP/LPPe) from the SUPL POS INIT message. If the V-SLP already calculated a position satisfying the requested QoP the V-SLP terminates the positioning session and informs the E-SLP about the termination and position by sending a SUPL END to the E-SLP tunnelled over RLP. The E-SLP proceeds to step K and returns the positioning result. The SET and the V-SLP MAY exchange several successive positioning procedure messages, tunnelled over RLP via the E-SLP.
The V-SLP calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance obtained from the V-SLP via E-SLP (SET-Based).

J. Once the position calculation is complete the V-SLP sends the SUPL END message towards the SET, which is tunnelled over RLP via the E-SLP. The V-SLP SHALL release all resources related to this session.

K. The E-SLP forwards the SUPL END to the SET informing it that no further positioning procedure will be started and that the location session is finished. The SET SHALL release the IP connection to the E-SLP and release all resources related to this session.

L. The E-SLP sends the position estimate back to the SUPL Agent by means of the MLP ELIA message.

5.1.15.4 Roaming with V-SPC Positioning Successful Case – Non-Proxy-mode

SET Roaming where the V-SLP is involved in the positioning calculation.

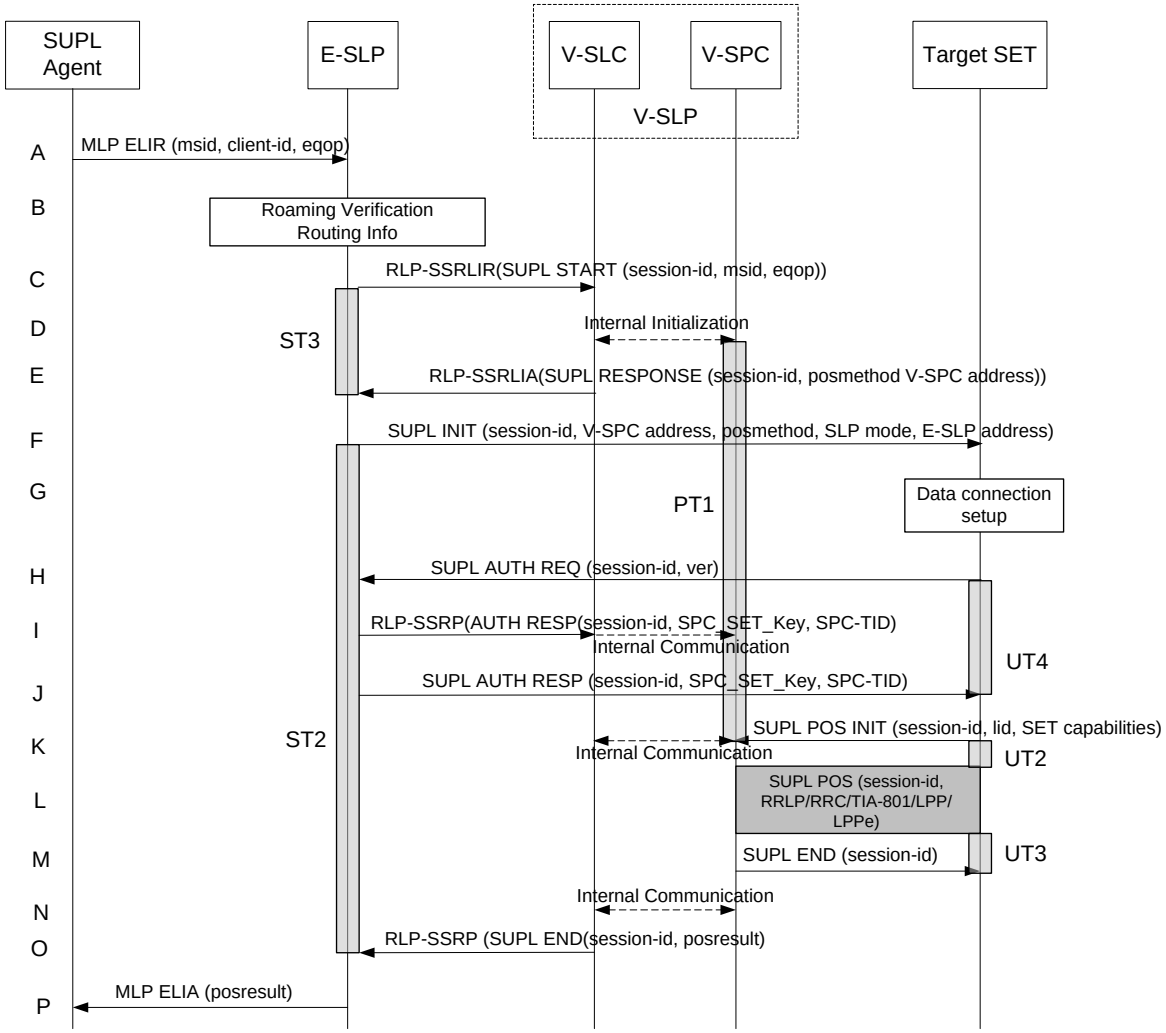

Figure 33: Network Initiated Emergency Services Roaming with V-SPC Positioning Successful Case – Non-Proxy-mode

NOTE: See Appendix D for timer descriptions.

A. SUPL Agent issues an MLP ELIR message to the E-SLP, with which SUPL Agent is associated. The MLP ELIR message may include the SET IP address and location data. The E-SLP SHALL authenticate the SUPL Agent and check if the SUPL Agent is authorized for the service it requests, based on the client-id received. If a previously computed position which meets the requested QoP is available at the E-SLP and no notification and verification is required according to local regulatory requirements, the E-SLP SHALL directly proceed to step P. If notification and verification or notification only is required, the E-SLP SHALL proceed to step F after having performed the Roaming Verification and Routing Info procedures of step B.

B. The E-SLP verifies that the target SET is currently SUPL roaming.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside scope of SUPL. However, there are various environment dependent mechanisms.

C. The E-SLP allocates a session-id for the SUPL session and decides that the V-SPC will provide assistance data or perform the position calculation. The E-SLP sends an RLP SSRLIR to the V-SLC to inform the V-SLC that the target SET will initiate a SUPL positioning procedure. Mandatory parameters in SUPL START that are not known to E-SLP (lid and SET capabilities) shall be populated with arbitrary values by E-SLP and be ignored by V-SLP. The SET part of the session-id will not be included in this message by the E-SLP to distinguish this scenario from a SET Initiated scenario.

D. The V-SLC informs the V-SPC of an incoming SUPL positioning session.

E. The V-SLC acknowledges that V-SPC is ready to initiate a SUPL positioning procedure with an RLP SSRLIA back to the E-SLP. The message includes at least session-id, posmethod and the address of the V-SPC.

F. The E-SLP initiates the location session with the SET using the SUPL INIT message. The SUPL INIT message contains at least session-id, address of the V-SPC, proxy/non-proxy mode indicator and the intended positioning method. The SUPL INIT SHALL contain the E-SLP address if the E-SLP is not the H-SLP for the SET. The SUPL INIT MAY contain the desired QoP. The E-SLP SHALL also include Notification element in the SUPL INIT message indicating location for emergency services and, according to local regulatory requirements, whether notification or verification to the target SET is or is not required.
If in step A the E-SLP decided to use a previously computed position the SUPL INIT message SHALL indicate this in a 'no position' posmethod parameter value and the SET SHALL respond with a SUPL END message to the E-SLP carrying the results of the verification process (access granted, or access denied). If no verification is required (notification only) the SET SHALL respond with a SUPL END message to the E-SLP. The E-SLP SHALL then directly proceed to step P.

NOTE: Before sending the SUPL END message the SET SHALL perform the data connection setup procedure of step G and use the procedures described in step H to establish an IP connection to the E-SLP.

G. The SET takes needed action preparing for establishment or resumption of a secure connection.

H. The SET establishes a secure connection to the E-SLP using either the provisioned H-SLP or defaulted E-SLP address, if no E-SLP address was received in step F, or the E-SLP address provided in step F. The SET then checks the proxy/non-proxy mode indicator to determine if the E-SLP uses proxy or non-proxy mode. In this case non-proxy mode is used and the SET SHALL send a SUPL AUTH REQ message to the E-SLP. The SUPL AUTH REQ message contains the session-id and a hash of the received SUPL INIT message (ver).

I. The E-SLC creates SPC_SET_Key and SPC-TID to be used for mutual V-SPC/SET authentication. The E-SLP forwards SPC_SET_Key and SPC-TID to the V-SLC through an RLP SSRP message. The V-SLC forwards SPC_SET_Key and SPC-TID to the V-SPC through internal communication.

J. The E-SLP returns a SUPL AUTH RESP to the SET. The SUPL AUTH RESP message SHALL contain the session-id, SPC_SET_Key and SPC-TID.

K. The SET will evaluate the Notification rules and follow the appropriate actions. The SET establishes an IP connection to the V-SPC according to the address received in step F. The SET and V-SPC may perform mutual authentication and the SET sends a SUPL POS INIT message to start a SUPL positioning session with the V-SPC. The SET SHALL send the SUPL POS INIT message even if the SET supported positioning technologies do not include the intended positioning method indicated in the SUPL INIT message. The SUPL POS INIT message contains at least session-id, SET capabilities and Location ID (lid). The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe). The SET MAY provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if this is supported. The SET MAY set the Requested Assistance Data element in the SUPL POS INIT. The SET SHALL also release the IP connection to the E-SLP and release all resources related to this session.
The V-SPC informs the V-SLC that the positioning procedure is started.

L. Based on the SUPL POS INIT message including posmethod(s) supported by the SET, the V-SPC SHALL determine the posmethod. If required for the posmethod, the V-SPC SHALL use the supported positioning protocol (e.g., RRLP, RRC, TIA-801 or LPP/LPPe) from the SUPL POS INIT message.
The SET and the V-SPC MAY exchange several successive positioning procedure messages. If the V-SPC already calculated a position satisfying the requested QoP the V-SPC terminates the positioning session with a SUPL END and informs the V-SLC about the termination. The V-SLC proceeds to step O and returns the positioning result.
The V-SPC calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance obtained from the V-SPC (SET-Based).

M. Once the position calculation is complete the V-SPC sends a SUPL END message to the SET informing it that no further positioning procedure will be started and that the positioning session is finished. The SET SHALL release all resources related to this session.

N. The V-SPC informs the V-SLC that the positioning procedure is completed and returns the position result. The V-SPC SHALL release all resources related to this session.

O. The V-SLC sends a RLP SSRP to the E-SLP carrying the position result. The V-SLC SHALL release all resources related to this session.

P. The E-SLP sends the position estimate back to the SUPL Agent by means of the MLP ELIA message

5.1.16 Immediate Location Request Exception Procedures

5.1.16.1 SET does not allow Positioning for non roaming

After receiving a SUPL INIT message the SET executes the notification/verification procedure. In this scenario, the subscriber rejects the location request. The call flow shown in Figure 34 applies to both proxy and non-proxy mode.

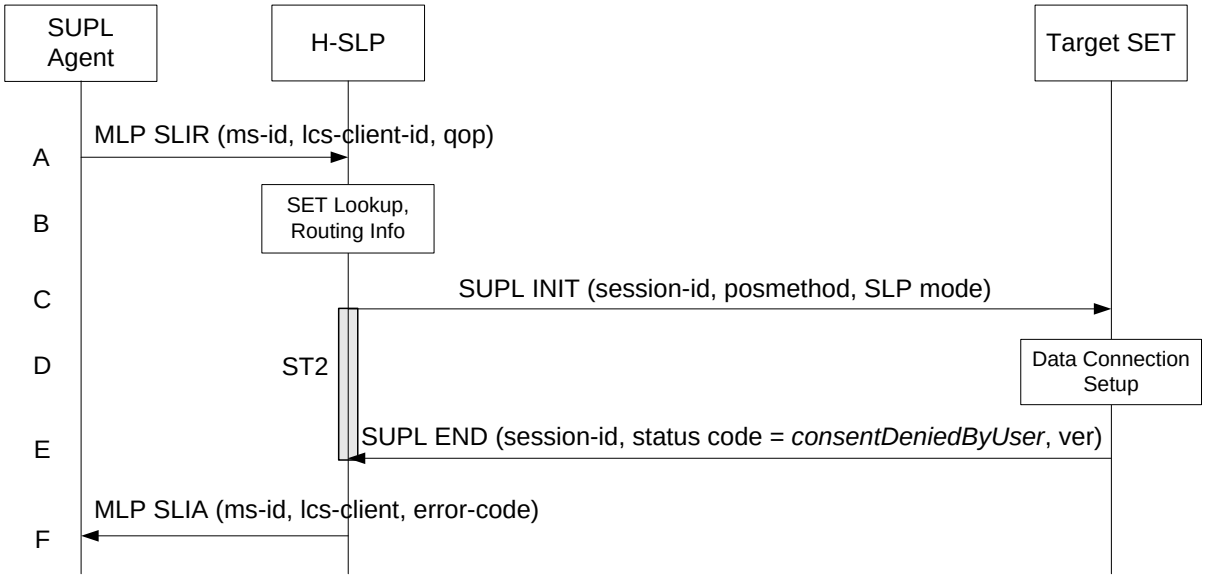

Figure 34: Network Initiated SET User denies Positioning for non roaming

NOTE: See Appendix D for timer descriptions.

A. SUPL Agent sends an MLP SLIR message to the H-SLP, with which the SUPL Agent is associated. The H-SLP SHALL authenticate the SUPL Agent and check if the SUPL Agent is authorized for the service it requested, based on the client-id received. Further, based on the received ms-id the H-SLP SHALL apply subscriber privacy against the client-id.

B. The H-SLP verifies that the target SET is currently not SUPL roaming. The H-SLP may also verify that the target SET supports SUPL.

NOTE: The specifics for determining if the SET is SUPL roaming or if the SET supports SUPL is considered out of scope for SUPL (there are various environment dependent mechanisms).

C. The H-SLP initiates the location session with the SET using the SUPL INIT message. The SUPL INIT message contains at least session-id, proxy/non-proxy mode indicator and the intended positioning method. In this case the result of the privacy check in Step A indicated that notification or verification to the target subscriber is needed, and the H-SLP therefore includes the Notification element in the SUPL INIT message.

D. The SET analyses the received SUPL INIT. If found to be non authentic SET takes not further actions. Otherwise the SET takes needed action preparing for establishment or resumption of a secure connection.

E. The SET SHALL establish a secure connection to the H-SLP. The SET evaluates the notification rules and alerts the subscriber of the position request. In this case the user rejects the location request, either by explicit action or implicitly by not responding to the notification, and the SET returns to the H-SLP the SUPL END message

containing the session-id, a hash of the received SUPL INIT message (ver) and the status code *consentDeniedByUser*.

F. The H-SLP sends the position response, containing the ms-id, client-id, and the appropriate error-code back to the SUPL Agent using an MLP SLIA message.

5.1.16.2 SET does not allow Positioning for roaming with V-SLP Positioning

After receiving a SUPL INIT message the SET executes the notification/verification procedure. In this scenario, the subscriber rejects the location request. The call flow shown in Figure 35 applies to both proxy and non-proxy mode for roaming with V-SLP.

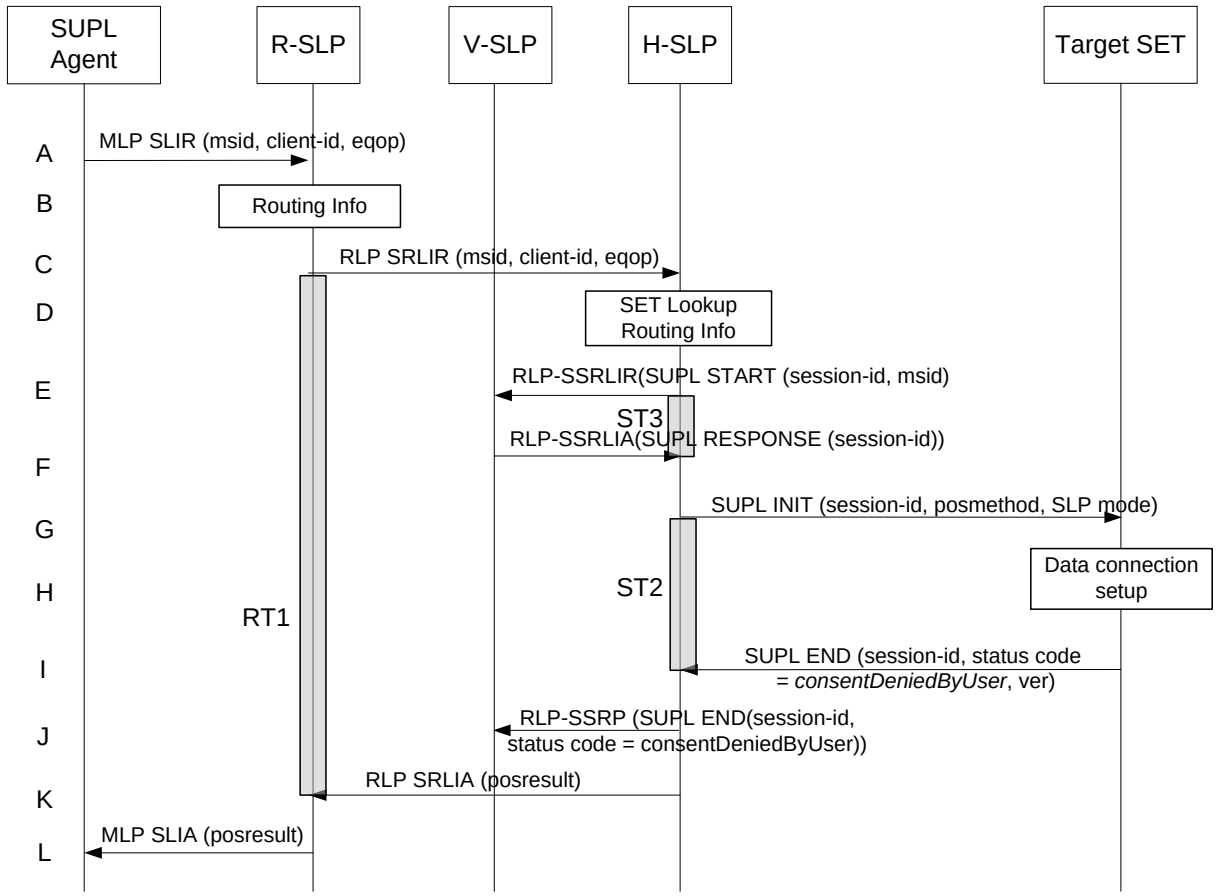

Figure 35: Network Initiated SET User denies Positioning for roaming with V-SLP Positioning

NOTE: See Appendix D for timer descriptions.

A. SUPL Agent issues an MLP SLIR message to the R-SLP, with which SUPL Agent is associated. The R-SLP SHALL authenticate the SUPL Agent and check if the SUPL Agent is authorized for the service it requests, based on the client-id received.

B. The R-SLP determines the H-SLP based on the received msid. If the R-SLP determines that the SUPL Agent is not authorized for this request, Step L will be returned with the applicable MLP return code.

NOTE: The specifics for determining the H-SLP are considered outside scope of SUPL (there are various environment dependent mechanisms).

C. The R-SLP forwards the location request to the H-SLP of the target subscriber, using the RLP protocol. Based on the received ms-id the H-SLP SHALL apply subscriber privacy against the client-id. If a previously computed position which meets the requested QoP is available at the H-SLP, the H-SLP SHALL proceed to step G after having performed the step D.

D. The H-SLP verifies that the target SET is currently SUPL roaming. In addition the H-SLP MAY also verify that the target SET supports SUPL.

NOTE: The specifics for determining if the SET is SUPL roaming or if the SET supports SUPL is considered out of scope for SUPL (there are various environment dependent mechanisms).

E. The H-SLP sends an RLP SSRLIR to the V-SLP to inform the V-SLP that the target SET will initiate a SUPL positioning procedure. Mandatory parameters in SUPL START that are not known to H-SLP (lid and SET capabilities) shall be populated with arbitrary values by H-SLP and be ignored by V-SLP. The SET part of the session-id will not be included in this message by the H-SLP to distinguish this scenario from a SET Initiated scenario.

F. The V-SLP acknowledges that it is ready to initiate a SUPL positioning procedure with an RLP SSRLIA back to the H-SLP.

G. The H-SLP initiates the location session with the SET using the SUPL INIT message. The SUPL INIT message contains at least session-id, proxy/non-proxy mode indicator and the intended positioning method. In this case the result of the privacy check in Step C indicated that notification or verification to the target subscriber is needed and the H-SLP therefore includes the Notification element in the SUPL INIT message. Before the SUPL INIT message is sent the H-SLP also computes and stores a hash of the message.
If in step C the H-SLP decided to use a previously computed position the SUPL INIT message SHALL indicate this in a 'no position' posmethod parameter value.

H. The SET analyses the received SUPL INIT. If found to be non authentic SET takes not further actions. Otherwise the SET takes needed action preparing for establishment or resumption of a secure connection.

I. The SET SHALL establish a secure connection to the H-SLP. The SET evaluates the notification rules and alerts the subscriber of the position request. In this case the user rejects the location request, either by explicit action or implicitly by not responding to the notification, and the SET returns a SUPL END message to the H-SLP containing the session-id, a hash of the received SUPL INIT message (ver) and the status code *consentDeniedByUser*

J. The H-SLP SHALL check that the hash of SUPL INIT matches the one it has computed for this particular session. The H-SLP then tunnels the SUPL END message to the V-SLP.

K. The H-SLP sends an RLP SRLIA message to the R-SLP indicating the error condition user rejected location request. The H-SLP SHALL release all resources related to this session.

L. The R-SLP sends an MLP SLIA message to the SUPL Agent indicating the error condition user rejected location request.

5.1.16.3 SET does not allow Positioning for roaming with H-SLP Positioning

This scenario is identical for ULP messaging to the non-roaming scenario (see section 5.1.16.1).

5.1.16.4 Notification based on current location – SET denies permission

During a Network-Initiated SUPL session in which the SET is asked for verification based on current location, if the SET returns a SUPL NOTIFY RESPONSE with a response type of Not Allowed, the H-SLP SHALL respond with a SUPL END which may contain a status code of "consentDeniedByUser".

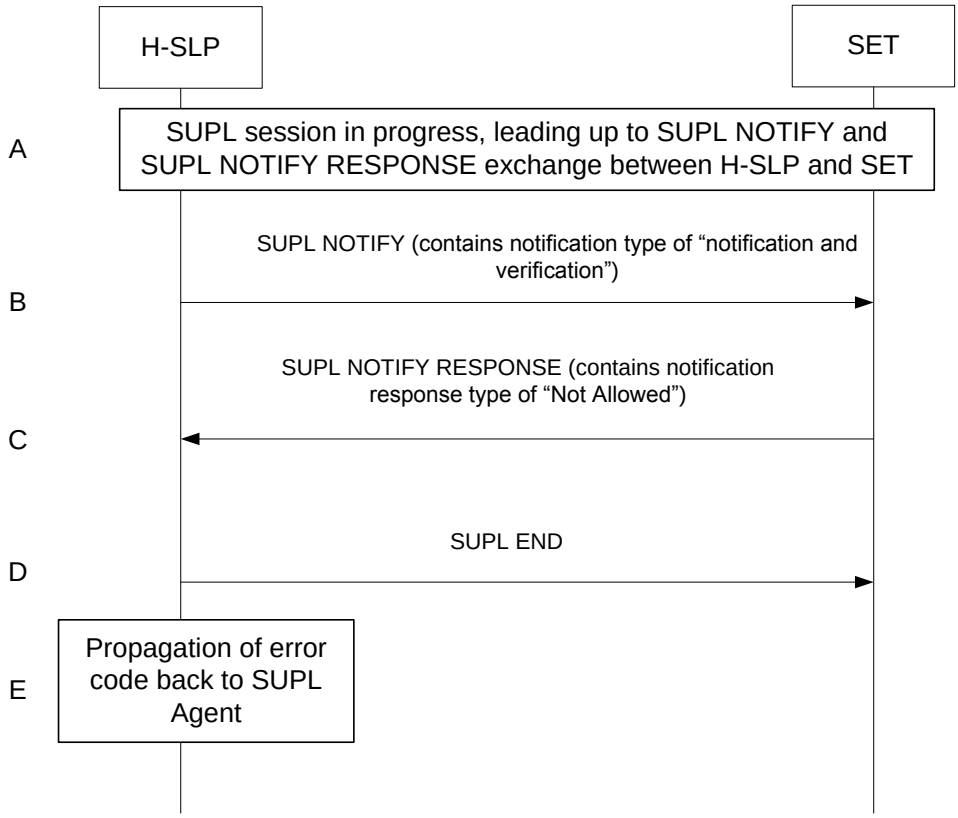

Figure 36: Notification based on current location – SET denies permission

NOTE: If the SUPL NOTIFY contains notification type "notification only", the contents of the SUPL Notify response SHALL be ignored by the H-SLP and the SUPL session shall continue as per the success case of that session.

A. A Network-initiated location request has occurred, in either a roaming or non-roaming scenario, in which the call flow has progressed to a SUPL NOTIFY message with a notification type of "notification and verification" being sent from the H-SLP to the SET.

B. A SUPL NOTIFY message sent from the H-SLP to the SET with a notification type of "notification and verification".

C. The SET responds with a SUPL NOTIFY RESPONSE containing a response type of "Not Allowed" to deny consent for the location attempt

D. The H-SLP SHALL send a SUPL END which may contain a statusCode of "consentDeniedByUser" to the SET. The SET SHALL release all resources related to this session.

E. The H-SLP then propagates the appropriate error code back to the SUPL Agent using the same messaging used when notification based on current location is not required.

5.1.16.5 Authorization Failure at H-SLP

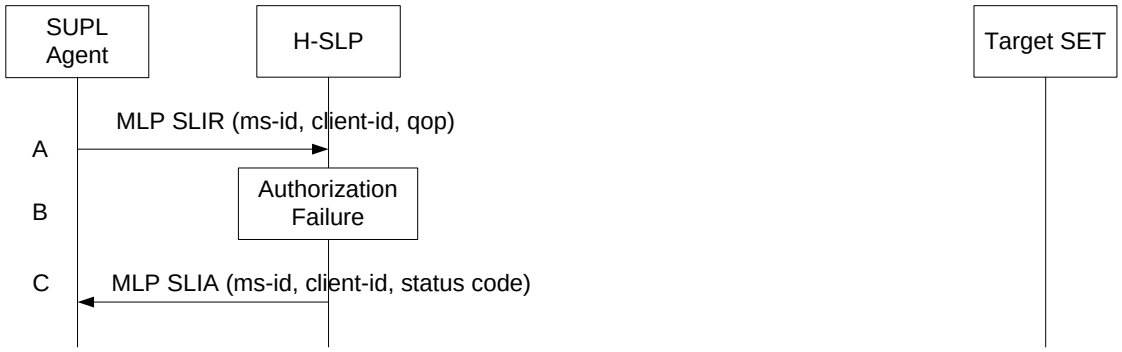

Figure 37: Network Initiated Authorization Failure H-SLP

A. SUPL Agent issues an MLP SLIR message to the H-SLP, with which the SUPL Agent is associated. The H-SLP shall authenticate the SUPL Agent and check if the SUPL Agent is authorized for the service it requests, based on the client-id received. Further, based on the received ms-id the H-SLP shall apply subscriber privacy against the client-id.

B. Authorization failure occurs at the H-SLP. This may be due to i) the SUPL Agent is not registered at the H-SLP for location requests, or ii) the H-SLP determines that the location request should be barred upon performing privacy check.

C. The H-SLP sends the position response, containing the ms-id, client-id, and the appropriate error-code back to the SUPL Agent by means of the MLP SLIA message.

5.1.16.6 Authorization Procedure at V-SLP

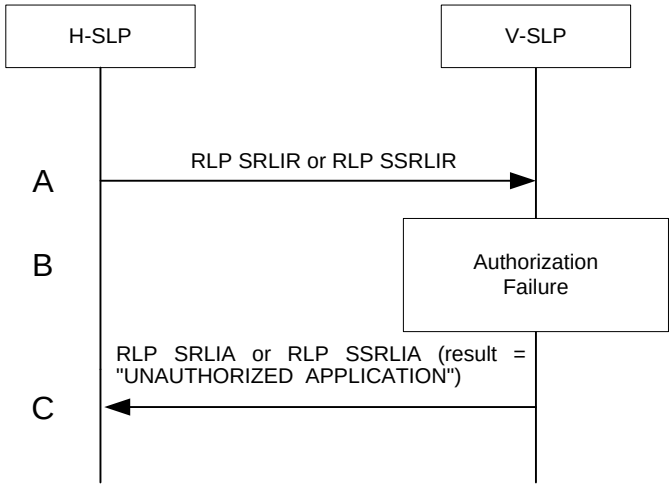

Figure 38: Network Initiated Authorization Failure V-SLP

A. H-SLP sends an RLP SRLIR or RLP SSRLIR to V-SLP.

B. Authorization failure occurs at the V-SLP. The V-SLP will send RLP SRLIA or RLP SSRLIA with result code "UNAUTHORIZED APPLICATION" to the H-SLP. This may be due to the fact that there is no roaming agreement between SUPL providers of V-SLP and H-SLP.

C. The V-SLP sends an authorization failure to H-SLP.

5.1.16.7 SUPL Protocol Error

When during a SUPL session either the SLP or the SET receives a message, which cannot be processed by the receiving entity due to SUPL protocol error, the receiving entity shall send a SUPL END message to the sending entity including a status code indicating protocol error.

Possible protocol error cases can be

- mandatory and/or conditional parameter is missing
- wrong parameter value
- unexpected message
- invalid session-id
- positioning protocol mismatch

A SUPL INIT message that is found to be non-authentic (see 6.1.6) does not constitute a protocol error and no SUPL END message shall be sent.

The SUPL END message includes the valid session-id actually being used in the session. When an invalid session-id has been received the invalid session-id shall be returned to the sending entity along with the status code.

A received session-id is invalid if:

- It does not correspond to an open session
- In case of the SUPL INIT message, the session-id is missing SLP Session ID or contains SET Session ID.

Afterwards, the SLP and the SET release the resources related to this session at the Lup interface.

The SLP sends a positioning error back to the SUPL Agent by means of the MLP SLIA message if no position estimate can be evaluated out of the available data. Otherwise, if privacy checks passed, the SLP sends the evaluated position estimate back to the SUPL Agent.

The described processing for protocol error does only apply to messages on the SUPL level. Exceptions, which occur during application of the specific positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe) shall be handled by means of the exception procedure specific for this positioning protocol along with the related messages.

The following SUPL protocol error types, attributable to either the SLP or the SET, are addressed by the general exception procedure shown below:

- Missing mandatory parameter(s)
- Wrong parameter value
- Unexpected message
- Positioning protocol mismatch

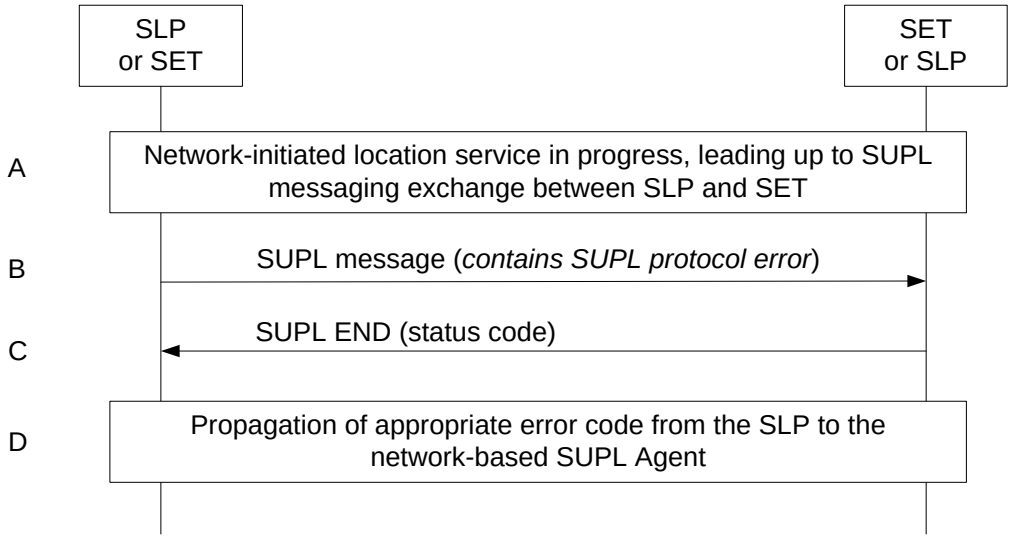

Figure 39: Network Initiated SUPL Protocol Error

A. A network-initiated location request has occurred in which the call flow has progressed to the SUPL messaging exchange between the SLP and the SET.

B. A SUPL message sent from either the SLP or the SET contains a protocol error (i.e., missing mandatory parameters, wrong parameter value, or unexpected message). Such message, if sent by the SLP, may be SUPL INIT; such message, if sent by the SET, may be SUPL POS INIT.

C. The recipient (either the SLP or SET) of the SUPL message containing the protocol error responds with a SUPL END message containing the status code for the specific protocol error. Afterwards, both sides release all resources related to this session at the Lup interface.

D. The SLP sends the position response, containing the ms-id, client-id, and the appropriate error-code back to the SUPL Agent by means of the MLP SLIA message

5.1.16.8 SUPL timer expiration

When either a SLP or a SET timer expires, the procedure described in Appendix D shall be followed.

5.1.17 Triggered Location Requests Exception Procedures

5.1.17.1 SET does not allow the Triggered Positioning

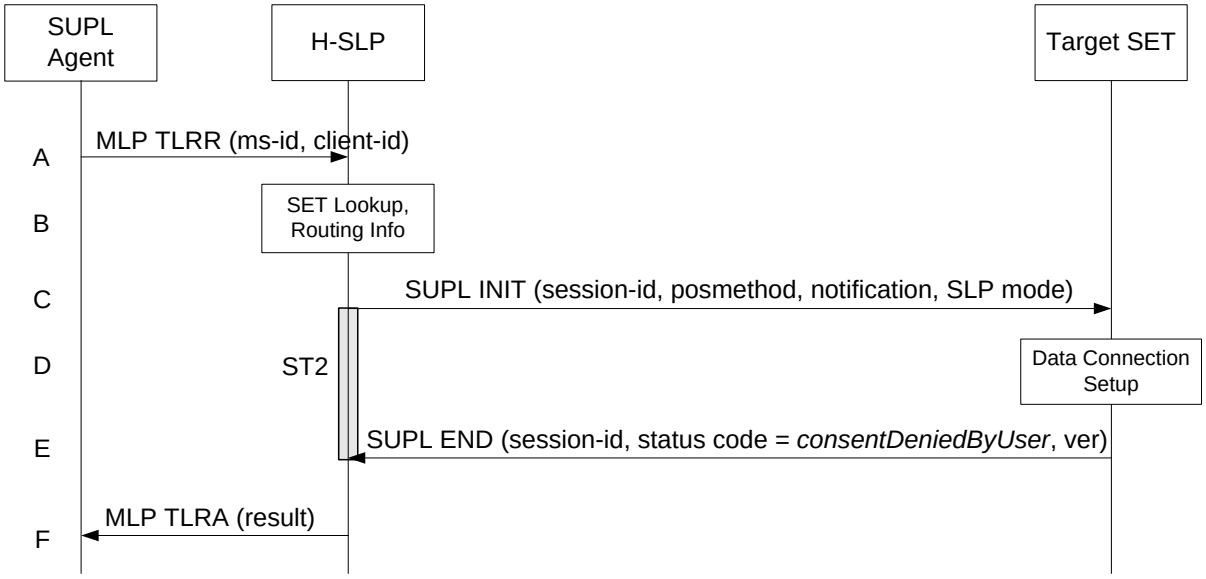

Figure 40: Network Initiated Triggered location, SET User denies Positioning

NOTE: See Appendix D for timer descriptions.

A. The SUPL Agent issues an MLP TLRR message to the H-SLP for the target SET. The H-SLP shall authenticate the SUPL Agent and check if the SUPL Agent is authorized for the service it requests, based on the client-id recived. Further, based on the received msid the H-SLP shall apply subscriber privacy against the client-id.

B. The H-SLP verifies that the garget SET is currently not SUPL roaming. The H-SLP may also verify that the target SET supports SUPL.

C. The H-SLP initiates the location session with the SET using the SUPL INIT message. In this case the SUPL INIT message contains at least session-id, trigger type, proxy/non-proxy mode indicator and the intended positioning. If the result of the privacy check in Step A indicates that notification or verification to the target subscriber is needed, the H-SLP SHALL also include Notification element in the SUPL INIT message.

D. When the SUPL INIT is received by the SET it will either attach itself to Packet Data Network if it is not attached at the time being or establish a circuit switched data connection.

E. The SET evaluates the notification rules and alerts the subscriber of the position request. In this case the user rejects the Triggered location request, either by explicit action or implicitly by not responding to the notification, and the SET returns to the H-SLP the SUPL END message containing the session-id, hash of the SUPL INIT message and the status code indicating the error reason.

F. The H-SLP sends the SLP TLRA message to SUPL Agent. The message contains result which including result code indicating the error reason.

NOTE: The MLP TLRA may be sent earlier at any time after the H-SLP receives the MLP TLRR. In this case the MLP TLREP should be sent instead.

5.1.17.2 Network cancels a Triggered Location Request

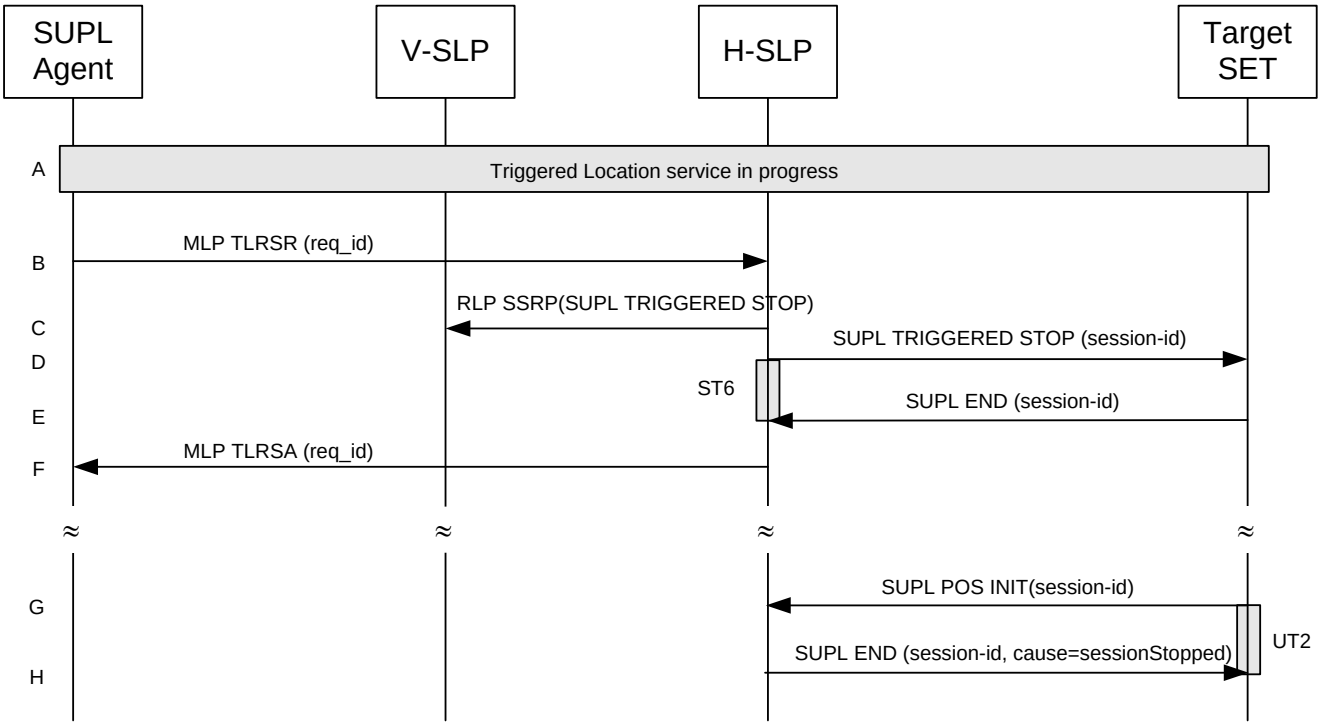

Figure 41: Network Initiated Triggered location, Network cancels the triggered location request

NOTE: See Appendix D for timer descriptions.

NOTE: This sequence assumes an open data connection exists between the H-SLP and the SET. For network triggered session cancellation in the absence of a data connection, the SLP may establish a data connection by first initiating a Session Info Query, as described in section 5.1.18 Session Info Query.

A. A triggered location session is in progress.

B. The SUPL Agent requests cancellation of the triggered location session by sending an MLP TLRSR message to the H-SLP.

NOTE: The cancellation of the triggered location session could have been initiated by the H-SLP itself i.e. without the SUPL Agent. In this case the MLP messages shown in steps B and F are superfluous.

C. This step is optional: for roaming with V-SLP scenarios, the H-SLP sends an RLP SSRP message including a SUPL TRIGGERED STOP message to the V-SLP in order to inform the V-SLP about the cancellation of the triggered session and to release all resource allocated to this session.

D. The H-SLP sends a SUPL TRIGGERED STOP message including the session-id to the target SET to request cancellation of the triggered session. If the H-SLP deems the sending of the SUPL TRIGGERED STOP message unsuccessful (i.e. timer ST6 expired after no SUPL END message was received as acknowledgement that the SET has received and accepted the triggered session cancellation request), the H-SLP considers the triggered session as cancelled and proceeds directly to step F.

E. The target SET acknowledges that it has cancelled the triggered session with the SUPL END message back to the H-SLP. If that cancellation is failed, the message contains the result code indicating the error reason.

F. The H-SLP sends an MLP TLRSA message to the SUPL Agent confirming cancellation of the triggered session.

NOTE: If the cancellation of the triggered request was successful, the call flow ends with step F. If, however, the cancellation of the triggered request was unsuccessful (e.g. SUPL TRIGGERED STOP message was not received by the SET, no SUPL END confirmation was received by the H-SLP, etc.), the SET may try to continue a triggered session which the H-SLP deems cancelled. In this case the following steps are executed:

G. The SET sends a SUPL POS INIT message to the H-SLP (could also be any other SUPL message which the SET is allowed to send to the H-SLP) containing a session-id which the H-SLP deems non-existent.

H. The H-SLP sends the SUPL END message with status code ‘sessionStopped’ or ‘invalidSessionId’.

5.1.17.3 SET cancels the triggered location request

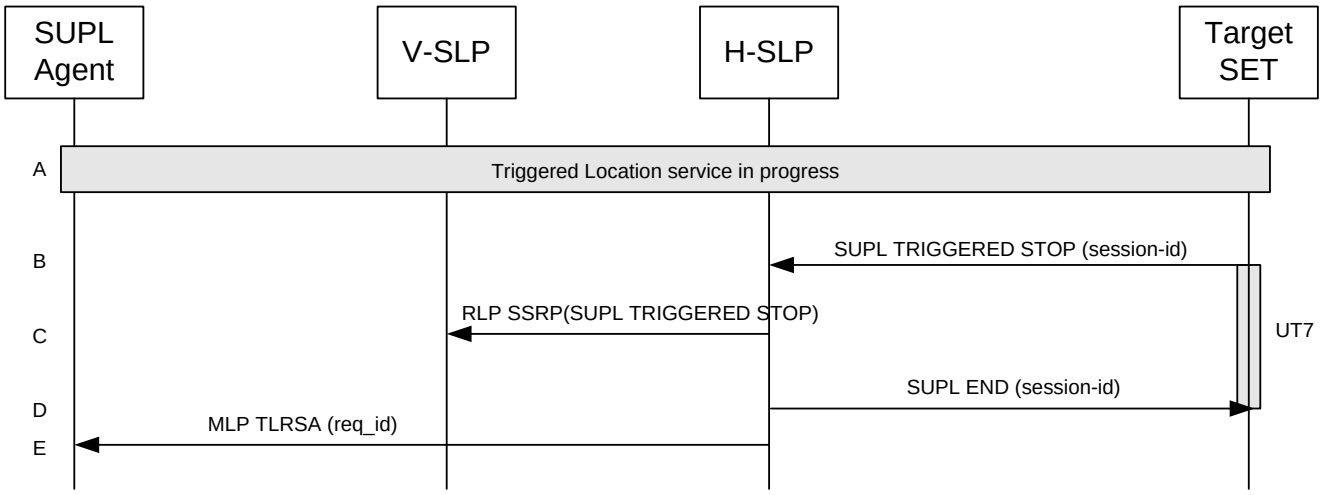

Figure 42: Network Initiated Triggered location, SET cancels the triggered location request

NOTE: See Appendix D for timer descriptions.

A. The triggered location procedure is in progress.

B. The SET sends a SUPL TRIGGERED STOP message with the session-id to H-SLP to request cancel this triggered location.

C. This step is optional. If H-SLP has roaming session with one V-SLP, it should send RLP SSRP message including SUPL TRIGGERED STOP to notify the VSLP to release resource allocated for this session.

D. The H-SLP sends the SUPL END message to the SET. The SET SHALL release the secure IP connection and release all resources related to this session.

E. The H-SLP sends the answer back to the SUPL Agent by means of the MLP TLRSA message. This message contains at least req_id or result. The H-SLP SHALL release all resources related to this session.

5.1.17.4 Network Initiated Event Trigger timer expiry

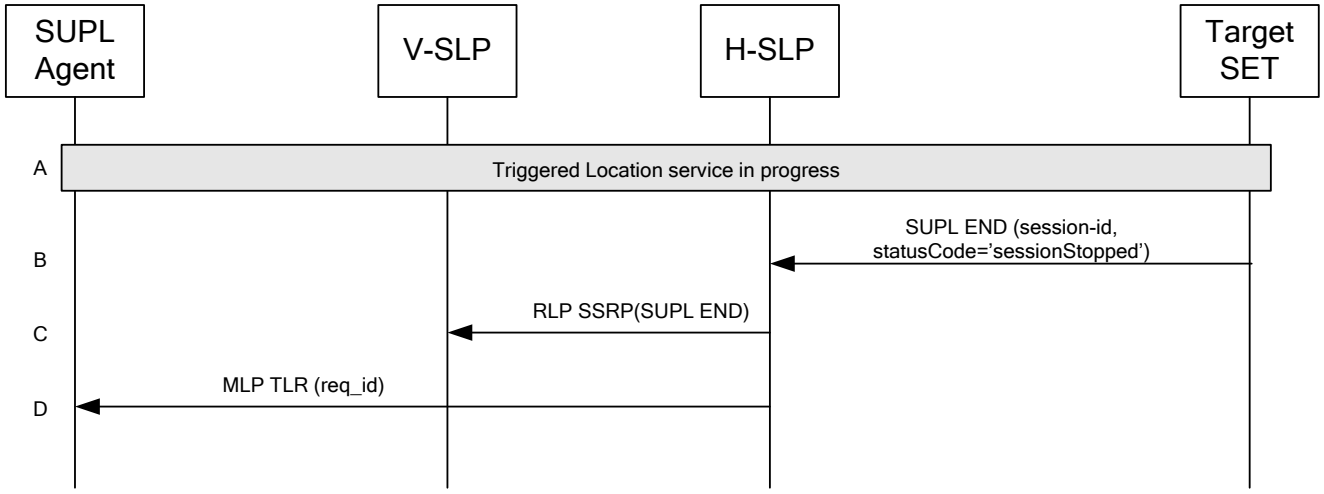

Figure 43: Network Initiated Event Trigger timer expiry

A. The event triggered location procedure is in progress.

B. When the StopTime of the event trigger is reached, the SET sends a SUPL END message with the session-id and a status code of "sessionStopped" to H-SLP . The SET releases all resources related to the session.

C. This step is optional. If H-SLP has roaming session with one V-SLP, it should send RLP SSRP message including SUPL END to notify the VSLP to release resource allocated for this session.

D. The H-SLP MAY send the answer back to the SUPL Agent by means of the MLP TLR message. The H-SLP releases all resources related to the session.

NOTE: If the H-SLP detects that SET does not send a SUPL END by a configured time interval after the Stop Time, it MAY proceed straight to step C and discard all resources for the session.

5.1.18 Session Info Query

The following call flow enables the H-SLP to perform one or more of the following operations:

1. Query the SET for active SUPL session information.
2. Perform re-notification or re-notification and verification for active Network Initiated sessions.
3. Terminate any ongoing Triggered sessions without waiting for the next report interval.

Note that procedures 2 and 3 above may not work in all SET implementations. Thus, if either of these procedures are attempted and the SET does not support the service, the SET SHALL send a SUPL END message containing the SessionInfoQuery session-id and the status code "serviceNotSupported" to the H-SLP.

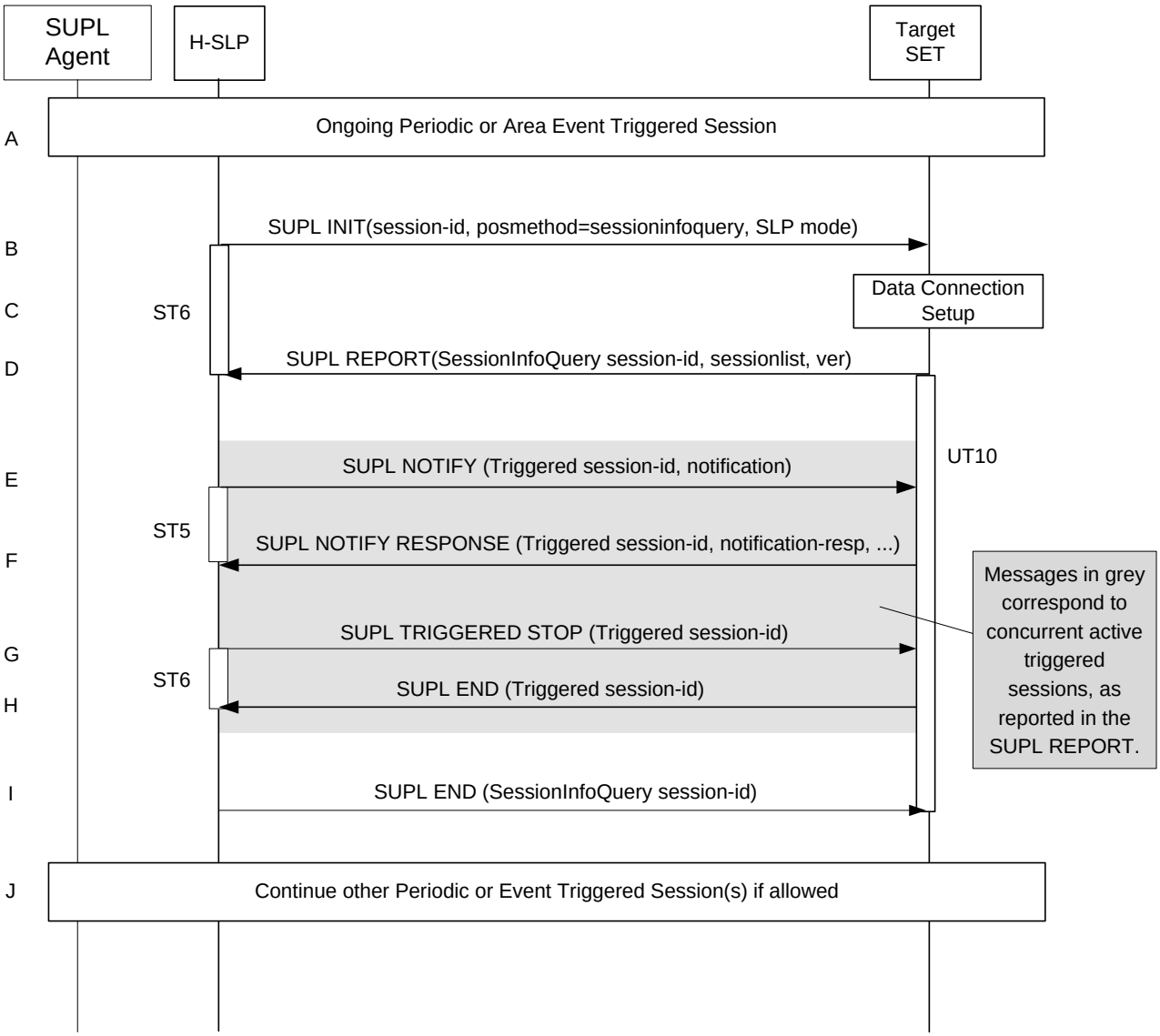

Figure 44: Session Info Query

NOTE: See Appendix D for timer descriptions.

A. Other Triggered SUPL sessions may be in progress.

B. The H-SLP initiates the "query for session info" session with the SET using a SUPL INIT message. The SUPL INIT message contains the session-id, posmethod and SLP mode. Query for session information is indicated by posmethod: *sessioninfoquery*. Before the SUPL INIT message is sent, the H-SLP also computes and stores a hash of the message.

C. The SET analyses the received SUPL INIT message. If found to be non authentic, the SET takes no further actions. Otherwise the SET takes needed action preparing for establishment or resumption of a secure connection.

D. The SET returns a SUPL REPORT message to the H-SLP including a list of session-ids (sessionlist) of all currently active sessions. The SET MAY also send the SET Capabilities in the SUPL REPORT message. The SUPL REPORT message also contains a hash of the received SUPL INIT message (ver). The SET starts UT10 to wait for SUPL END in step I.

E. This step is performed if re-notification or re-notification and verification is needed based upon a check of the subscriber privacy and the elapsed time since notification / verification last occurred for any active Triggered

sessions as indicated in the SUPL REPORT. A SUPL NOTIFY is sent to the SET. The H-SLP starts ST5 to wait for the SUPL NOTIFY RESPONSE.

F. If step E is performed the SET SHALL send a SUPL NOTIFY RESPONSE message to the H-SLP. If notification and verification was required in step E then this will contain the verification response from the user. The SET waits for a SUPL TRIGGERED STOP or SUPL NOTIFY for another active Triggered session, or the SUPL END for this Session Info Query Session.

G. This step can be performed for two independent cases:

   a. The SUPL TRIGGERED STOP is conditionally sent when step F occurs and the SET responded with a SUPL NOTIFY RESPONSE containing a response type of "Not Allowed" to deny consent for the re-verification. In this case the SUPL TRIGGERED STOP shall contain a statusCode of "consentDeniedByUser". The SUPL TRIGGERED STOP shall identify the Triggered session associated with the re-verification.

   b. The SUPL TRIGGERED STOP is sent, independently of steps E and F, to cancel any active Triggered session, without waiting for the next Periodic or Area Event trigger. The H-SLP may end any active sessions as reported in the SUPL REPORT of step D.

H. For both cases the H-SLP starts ST6 to wait for a SUPL END from the SET. The target SET acknowledges that it has cancelled the triggered session with the SUPL END message sent back to the H-SLP. If that cancellation failed, the message contains the result code indicating the error reason. The SET shall wait for a subsequent SUPL TRIGGERED STOP for an active triggered session or the SUPL END for this Session Info Query Session.

Steps E, F, G, H may be repeated for any active sessions reported in step D which require re-notification/re-notification and verification, or termination as determined by the H-SLP.

I. The H-SLP sends the SUPL END message to the SET informing it that no further positioning procedure will be started and that the Session Info Query session is finished. The SET SHALL release all resources related to this Session Info Query session. This step shall occur before the expiry of UT10 when started in Steps D.

5.1.19 Other Exception Procedures

5.1.19.1 SET does not support the service requested in SUPL INIT

During a Network Initiated SUPL Session, if a SUPL INIT message is received by the SET requesting a service which is not supported by the SET, the SET shall send a SUPL END message to the requesting H-SLP including the status code "Service Not Supported".

Possible use cases for service not supported scenarios are:

1. The requested Trigger (Periodic / AreaEvent) is not supported by the SET.
2. Historical Data Retrieval Feature is not supported by the SET.
3. Session Info Query Feature is not supported by the SET.
4. Notification Based on Current Location Feature is not supported by the SET.

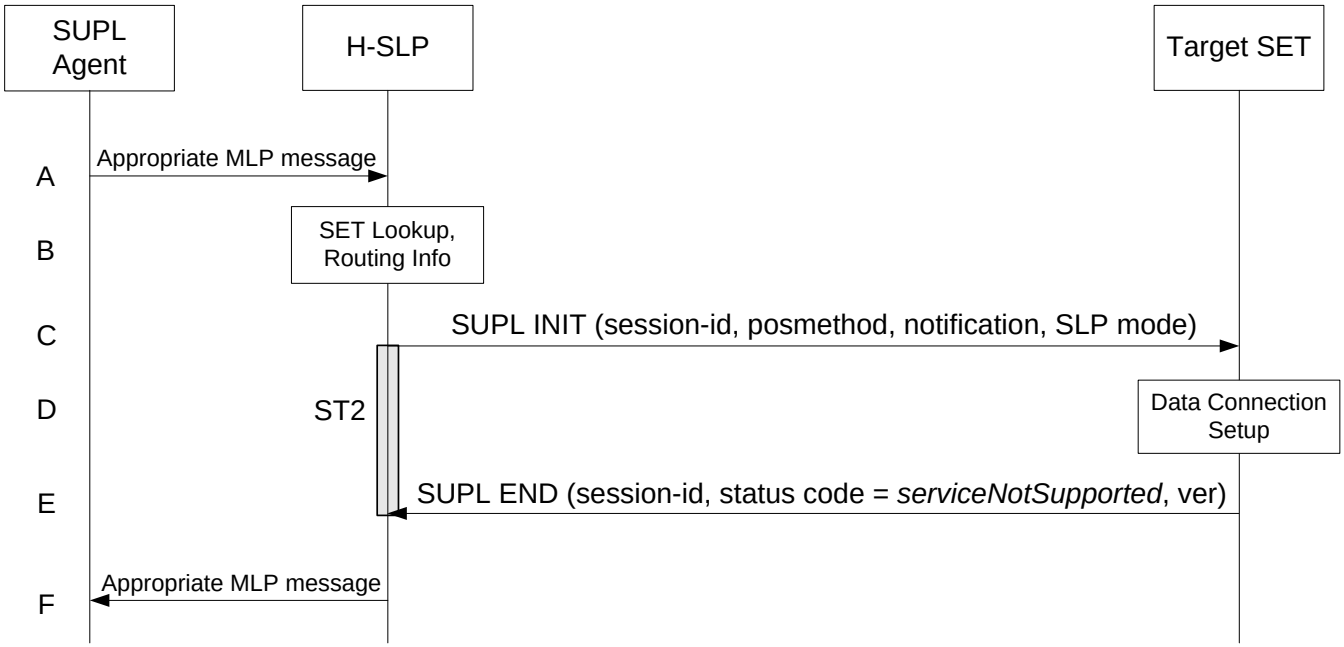

Figure 45: Network Initiated, SET does not support the service requested in SUPL INIT

NOTE: See Appendix D for timer descriptions.

A. The SUPL Agent issues an appropriate MLP message to the H-SLP to invoke the desired service for the target SET. The H-SLP shall authenticate the SUPL Agent and check if the SUPL Agent is authorized for the service it requests, based on the client-id recived. Further, based on the received msid the H-SLP shall apply subscriber privacy against the client-id.

B. The H-SLP verifies that the target SET is currently not SUPL roaming. The H-SLP may also verify that the target SET supports SUPL.

C. The H-SLP initiates a SUPL session with the SET using by sending a SUPL INIT message to the SET requesting the desired service. If the result of the privacy check in Step A indicates that notification or verification to the target subscriber is needed, the H-SLP SHALL also include Notification element in the SUPL INIT message.

D. When the SUPL INIT is received by the SET, it will either attach itself to Packet Data Network if it is not already attached or establish a circuit switched data connection.

E. The SET evaluates the requested service. If the SET does not support the requested service, the SET sends a SUPL END message containing the session-id, hash of the SUPL INIT message and a status code indicating “Service Not Supported” to the H-SLP.

F. The H-SLP notifies the SUPL Agent using the appropriate MLP message.

5.2 SUPL Collaboration SET Initiated

SET Initiated Services are services, which originate from the SET. For these services the SUPL Agent resides within the SET.

Set up and release of connections:

Before sending any ULP messages the SET SHALL take needed actions such that a TLS connection exists to the SLP/SLC. This can be achieved by establishing a new connection, resume a connection or reuse an existing TLS connection. This includes establishment or utilization of various data connectivity resources that depends on the terminal in which the SET resides and the type of access network. Data connectivity below IP-level is out of scope of this document.

The detailed call flows in this section describes when a TLS connection no longer is needed. The TLS connection shall then be released unless another SUPL session is using the TLS connection.

5.2.1 Non-Roaming Successful Case – Proxy mode

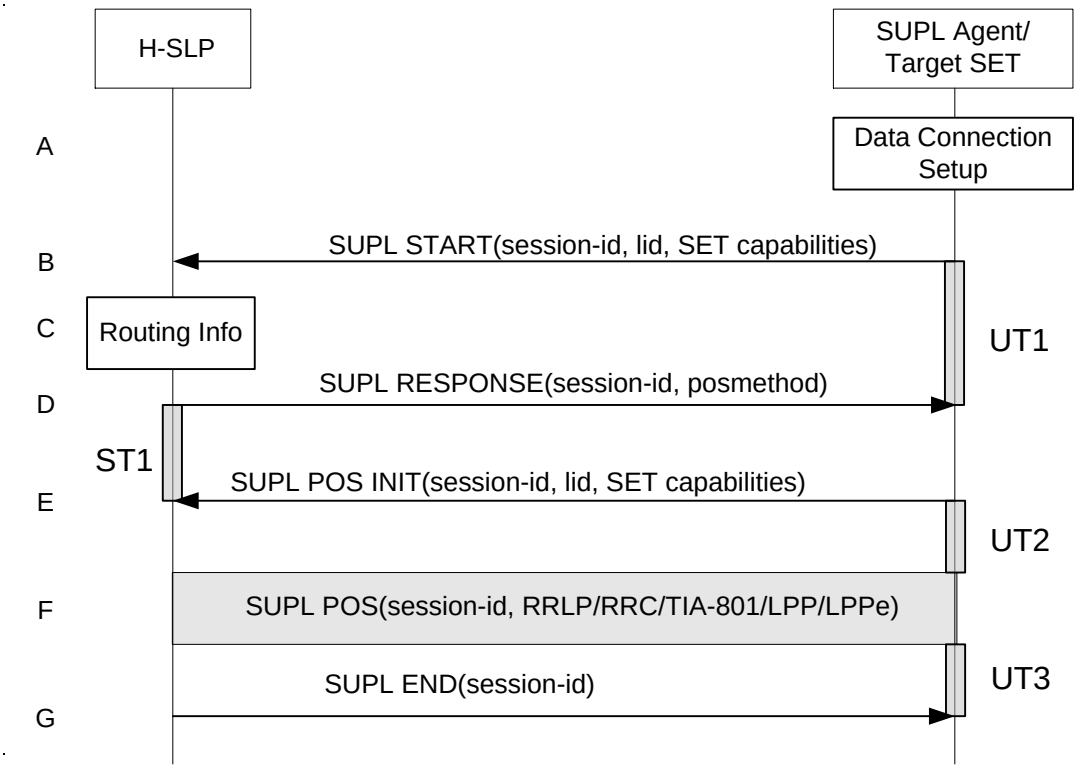

Figure 46: SET-Initiated Non-Roaming Successful Case – Proxy mode

NOTE: See Appendix D for timer descriptions

A. The SUPL Agent on the SET receives a request for position from an application running on the SET. The SET takes appropriate action establishing or resuming a secure connection.

B. The SUPL Agent on the SET uses the default address provisioned by the Home Network to establish a secure connection to the H-SLP and sends a SUPL START message to start a positioning session with the H-SLP. The SUPL START message contains session-id, SET capabilities and Location ID (lid). The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe).
If a previously computed position which meets a requested QoP is available at the H-SLP the H-SLP SHALL directly proceed to step G and send the position to the SET in the SUPL END message.

C. The H-SLP verifies that the target SET is currently not SUPL roaming.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside scope of SUPL. However, there are various environment dependent mechanisms.

D. Consistent with the SUPL START message including posmethod(s) supported by the SET, the H-SLP SHALL determine the posmethod. If required for the posmethod, the H-SLP SHALL use the supported positioning protocol (e.g., RRLP, RRC, TIA-801 or LPP/LPPe) from the SUPL START message. The H-SLP SHALL respond with the SUPL RESPONSE to the SET. The SUPL RESPONSE contains the session-id but no H-SLP address, to indicate to the SET that a new connection SHALL NOT be established. The SUPL RESPONSE also contains the posmethod. It MAY also contain location information, not meeting the QoP, but giving a coarse approximation of the position, based on information received in the SUPL START message.
If, however, a position retrieved or calculated based on information received in the SUPL START message meets the requested QoP, the H-SLP MAY directly proceed to step G.

E. After the SET receives the SUPL RESPONSE from H-SLP, the SET sends a SUPL POS INIT message. The SUPL POS INIT message contains at least session-id, SET capabilities and Location ID (lid). The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe). The SET MAY optionally provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if this is supported. The SET MAY include the first SUPL POS element in the SUPL POS INIT message. The SET MAY set the Requested Assistance Data element in the SUPL POS INIT. If a position retrieved or calculated based on information received in the SUPL POS INIT message is available which meets a required QoP, the H-SLP MAY directly proceed to step G and not engage in a SUPL POS session.

F. The SET and the H-SLP exchange several successive positioning procedure messages.
The H-SLP calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance obtained from the H-SLP (SET-Based).

G. Once the position calculation is complete the H-SLP SHALL send the SUPL END message to the SET informing it that no further positioning procedure will be started and that the location session is finished. Depending on positioning method and used positioning protocol the H-SLP MAY add the determined position to the SUPL END message. The SET SHALL release the secure connection and release all resources related to this session. The H-SLP SHALL release all resources related to this session.

5.2.2 Non-Roaming Successful Case – Non-Proxy mode

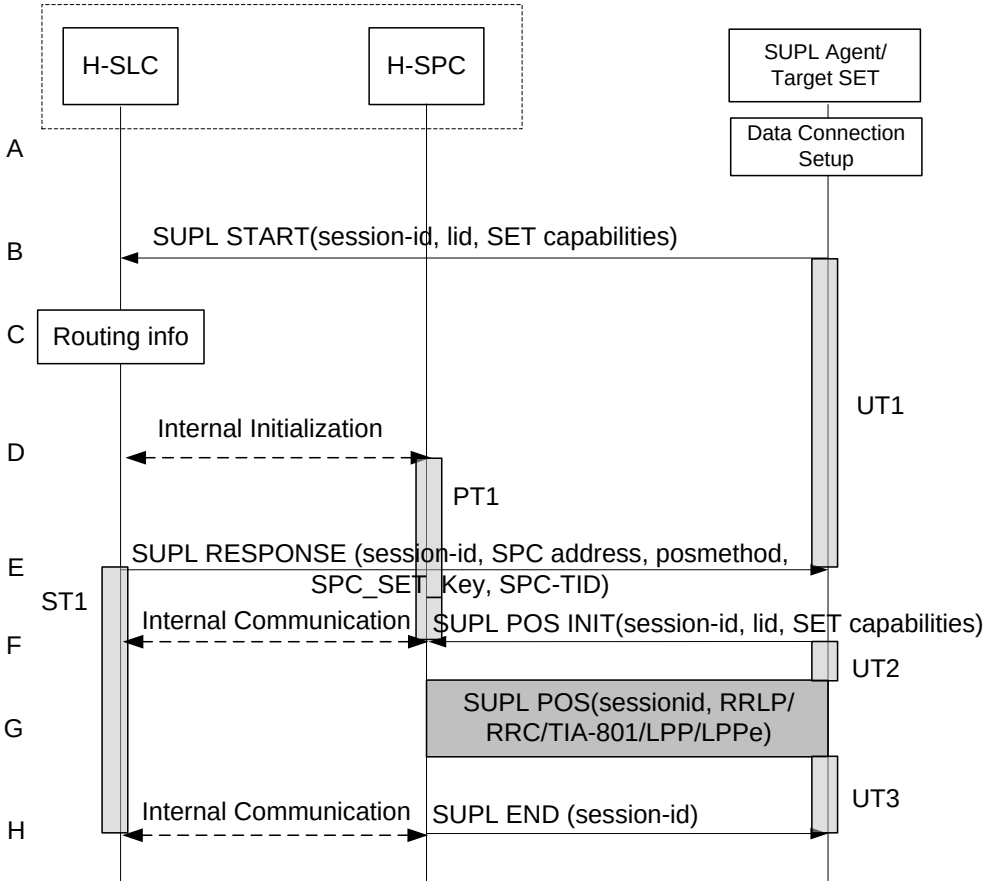

Figure 47: SET-Initiated Non-Roaming Successful Case – Non-Proxy mode

NOTE: See Appendix D for timer descriptions

A. The SUPL Agent on the SET receives a request for position from an application running on the SET. The SET takes appropriate action establishing or resuming a secure connection.

B. The SUPL Agent on the SET uses the address provisioned by the Home Network to establish a secure connection to the H-SLC and sends a SUPL START message to start a positioning session with the H-SLC. The SUPL START message contains session-id, SET capabilities and Location ID (lid). The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe).
If a previously computed position which meets a requested QoP is available at the H-SLC, the H-SLC SHALL respond with a SUPL END message to the SET containing the position and end the SUPL session.

C. The H-SLC verifies that the target SET is currently not SUPL roaming.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside scope of SUPL. However, there are various environment dependent mechanisms.

D. The H-SLC will inspect the SUPL START message and determine if the SET is allowed to directly access the H-SPC. The H-SLC generates a session id for the SUPL session and informs the H-SPC of an incoming SUPL POS session from a SET identified by the generated session-id. The H-SLC also generates SPC_SET_Key and SPC-TID to be used for mutual H-SPC/SET authentication. SPC_SET_Key and SPC-TID are also forwarded to the H-SPC through internal communication. In collaboration the H-SLC and H-SPC determine the initial location based on the lid received in the SUPL START message received from the SET.

NOTE: The interface between the H-SLC and the H-SPC is specified in [SUPL2 ILP TS]. The implementation of ILP is optional hence the presence(or absence) of ILP is implementation dependent.

E. Consistent with the SUPL START message including posmethod(s) supported by the SET, the H-SLC SHALL determine the posmethod. If required for the posmethod, the H-SLC SHALL use the supported positioning protocol (e.g., RRLP, RRC, TIA-801 or LPP/LPPe) from the SUPL START message.
The H-SLC SHALL respond with a SUPL RESPONSE to the SET. The SUPL RESPONSE contains the session-id, SPC_SET_Key and SPC-TID to be used by the SET for mutual H-SPC/SET authentication, and the address of the H-SPC to indicate to the SET that a new secure connection SHALL be established. The SUPL RESPONSE also contains the posmethod. It MAY also contain location information, not meeting the QoP, but giving an initial approximation of the position, based on information received in the SUPL START message. If, however, a position retrieved or calculated based on information received in the SUPL START message which meets a requested QoP is available, the H-SLC MAY respond with a SUPL END message (instead of the SUPL RESPONSE) to the SET containing the position and end the SUPL session.

F. To initiate the actual positioning session the SET opens a new secure connection to the H-SPC using the address indicated in step E. The SET and H-SPC perform mutual authentication through the keys received in step D and step E, and the SET sends a SUPL POS INIT message. Before the new secure connection is established the existing secure connection to the H-SLC is closed. The SUPL POS INIT message contains at least session-id, SET capabilities and Location ID (lid). The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe). The SET MAY provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if this is supported. The SET MAY include the first SUPL POS element in the SUPL POS INIT message. If a position retrieved or calculated based on information received in the SUPL POS INIT message is available which meets a required QoP, the H-SLP MAY directly proceed to step H and not engage in a SUPL POS session . The SET MAY set the Requested Assistance Data element in the SUPL POS INIT.
The H-SPC informs the H-SLC that the positioning procedure is started.

G. The SET and the H-SPC exchange several successive positioning procedure messages.

The H-SPC calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance obtained from the H-SPC (SET-Based).

H. Once the position calculation is complete the H-SPC SHALL send the SUPL END message to the SET informing it that no further positioning procedure will be started and that the location session is finished. Depending on positioning method and used positioning protocol the H-SPC MAY add the determined position to the SUPL END message. When the SUPL END is received the SET SHALL release the secure connection to the H-SPC and release all resources related to this session. The H-SPC informs the SLC that the positioning procedure is finished. The H-SLP SHALL release all resources related to this session.

5.2.3 Roaming with V-SLP Positioning Successful Case – Proxy mode

SET Roaming where the V-SLP is involved in the positioning calculation.

A policy of a single SET to H-SLP SUPL session is maintained by encapsulating the messages between the SET and V-SLP through the use of the RLP protocol.

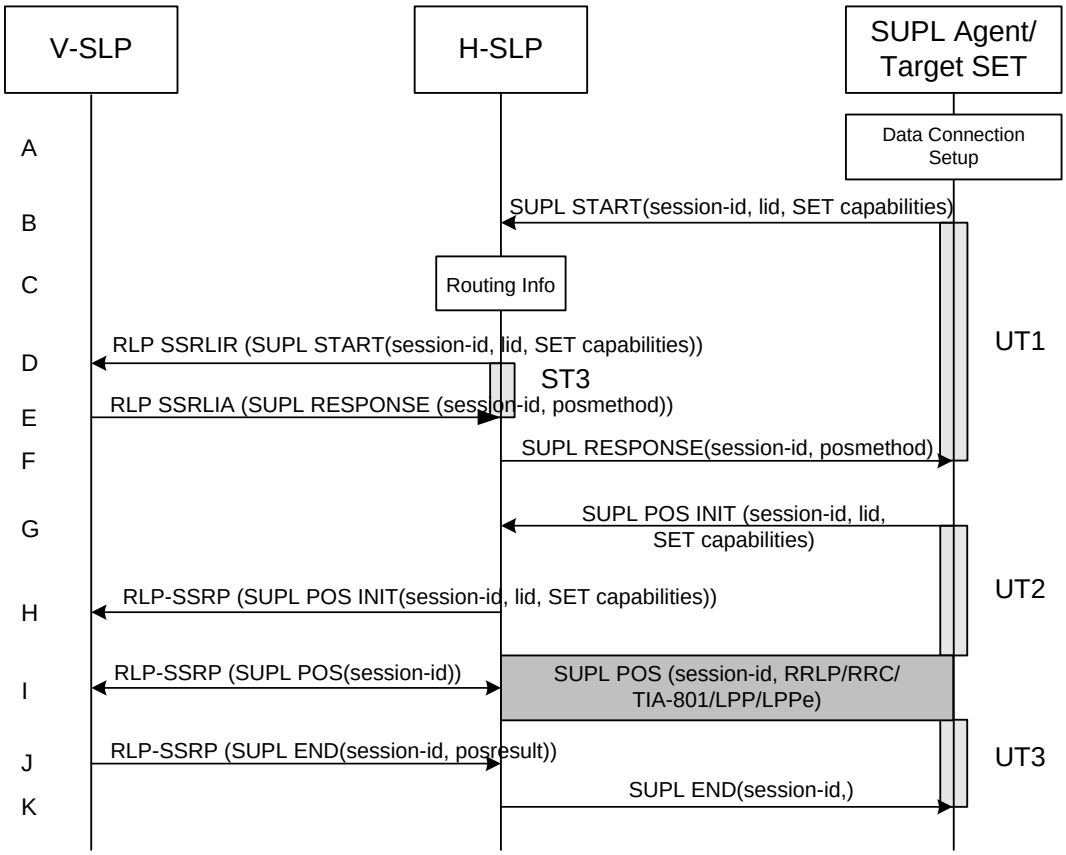

Figure 48: SET-Initiated Roaming with V-SLP Positioning Successful Case – Proxy mode

NOTE: See Appendix D for timer descriptions

A. The SUPL Agent on the SET receives a request for position from an application running on the SET. The SET takes appropriate action establishing or resuming a secure connection.

B. The SUPL Agent on the SET uses the default address provisioned by the Home Network to establish a secure connection to the H-SLP and sends a SUPL START message to start a positioning session with the H-SLP. The SUPL START message contains session-id, SET capabilities and Location ID (lid). The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe).
If a previously computed position which meets a requested QoP is available at the H-SLP the H-SLP SHALL directly proceed to step K and send the position to the SET in the SUPL END message.

C. The H-SLP verifies that the target SET is currently SUPL roaming.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside scope of SUPL. However, there are various environment dependent mechanisms.

D. The H-SLP decides that the assistance data/position calculation is done by the V-SLP and sends a RLP SSRLIR tunnelling the SUPL START message to the V-SLP.

E. Consistent with the SUPL START message including posmethod(s) supported by the SET, the V-SLP SHALL determine the posmethod. If required for the posmethod, the V-SLP SHALL use the supported positioning protocol (e.g., RRLP, RRC, TIA-801 or LPP/LPPe) from the SUPL START message. The V-SLP responds with a SUPL

RESPONSE tunnelled over RLP back to the H-SLP that it is capable of supporting this request. The SUPL RESPONSE contains at least the sessionid and posmethod. It MAY also contain location information, not meeting the QoP, but giving an initial approximation of the position, based on information received in the SUPL START message.
If a position retrieved or calculated based on information received in the RLP SSRLIR (SUPL START) message which meets a requested QoP is available, the V-SLP MAY send a RLP SSRLIA (SUPL END) message – as opposed to RLP SSRLIA (SUPL RESPONSE) – including the position estimate to the H-SLP and the H-SLP MAY then proceed to step K.

F. The H-SLP forwards the SUPL RESPONSE to the SET. The SUPL RESPONSE contains the session-id but no H-SLP address, to indicate to the SET that a new connection SHALL NOT be established. The SUPL RESPONSE also contains the posmethod. It MAY also contain location information, not meeting the QoP, but giving an initial approximation of the position, based on information received in the SUPL START message.

G. After the SET receives the SUPL RESPONSE from H-SLP, the SET sends a SUPL POS INIT message. The SUPL POS INIT message contains at least session-id, SET capabilities and Location ID (lid). The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe). The SET MAY provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if this is supported. The SET MAY include the first SUPL POS element in the SUPL POS INIT message. The SET MAY set the Requested Assistance Data element in the SUPL POS INIT.

H. The H-SLP forwards the SUPL POS INIT to the V-SLP over the RLP tunnel.

I. If the V-SLP already calculated an initial position based on information received in the SUPL POS INIT message which meets the requested QoP, the V-SLP MAY directly proceed to step J and not engage in a SUPL POS session. Otherwise the SET and the V-SLP exchange several successive positioning procedure messages, tunnelled over RLP via the H-SLP.
The V-SLP calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance obtained from the V-SLP via H-SLP (SET-Based).

J. Once the position calculation is complete the V-SLP sends a SUPL END message to the SET, which is tunnelled over the RLP via the H-SLP, informing it that no further positioning procedure will be started and that the location session is finished. Depending on positioning method and used positioning protocol the V-SLP MAY add the determined position to the SUPL END message. The V-SLP SHALL release all resources related to this session.

K. The H-SLP forwards the SUPL END to the SET informing it that no further positioning procedure will be started and that the location session is finished. The SET SHALL release the secure connection and release all resources related to this session. The H-SLP SHALL release all resources related to this session.

5.2.4 Roaming with V-SPC Positioning Successful Case – Non-Proxy mode

SET Roaming where the V-SPC is involved in the positioning calculation.

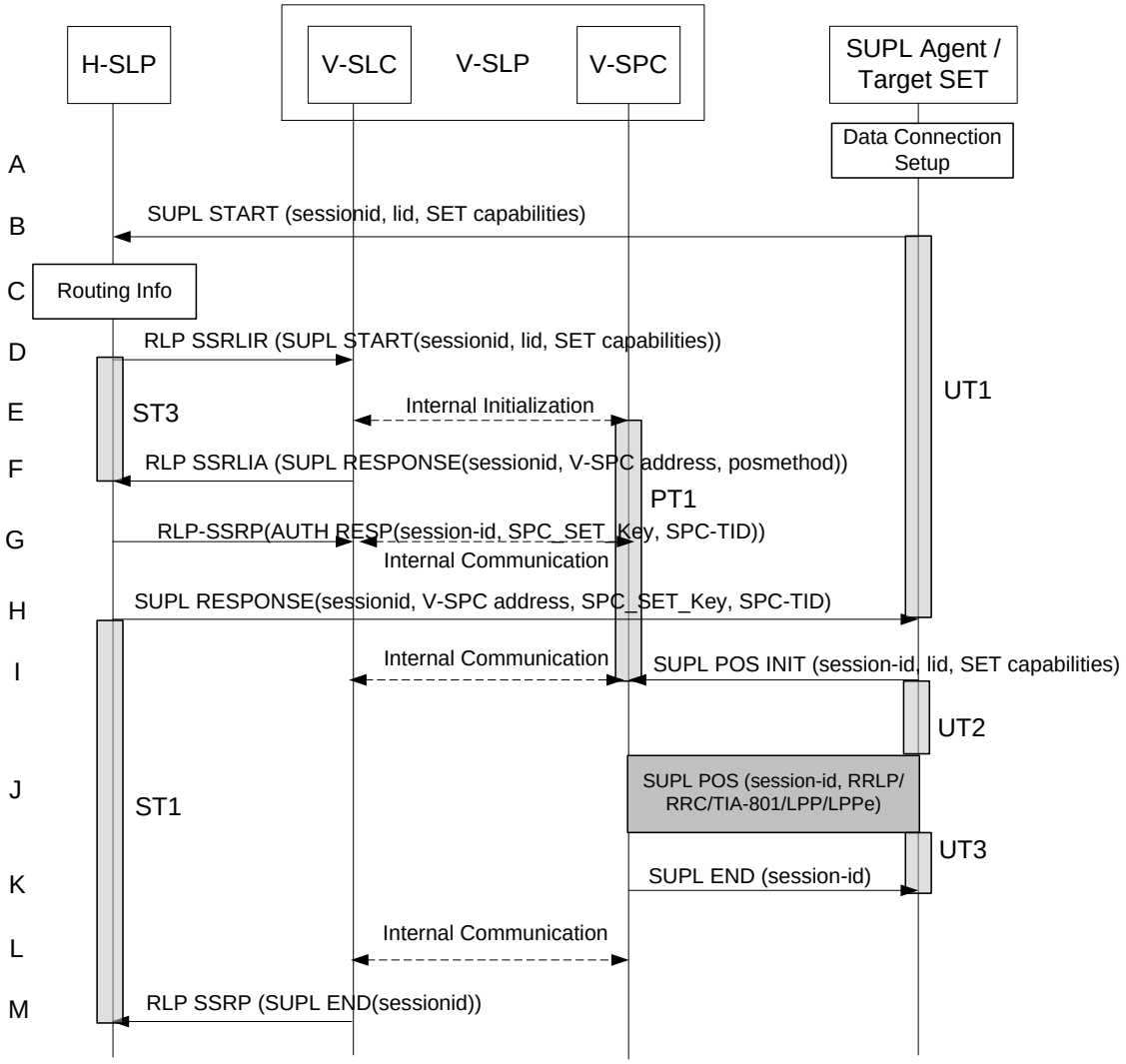

Figure 49: SET-Initiated Roaming with V-SPC Positioning Successful Case – Non-Proxy mode

NOTE: See Appendix D for timer descriptions.

A. The SUPL Agent on the SET receives a request for position from an application running on the SET. The SET takes appropriate action establishing or resuming a secure connection.

B. The SUPL Agent on the SET uses the address provisioned by the Home Network to establish a secure connection to the H-SLC and sends a SUPL START message to start a positioning session with the H-SLP. The SUPL START message contains session-id, SET capabilities and Location ID (lid). The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe).
If a previously computed position which meets a requested QoP is available at the H-SLP the H-SLC SHALL send a SUPL END message including the position to the SET and end the session.

C. The H-SLC verifies that the target SET is currently SUPL roaming.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside scope of SUPL. However, there are various environment dependent mechanisms.

D. The H-SLC decides that the assistance data/position calculation is done by the V-SPC and allocates a sessionid and sends an RLP SSRLIR tunnelling the SUPL START message to the V-SLC.

E. The V-SLC informs the V-SPC of the incoming session.

F. Consistent with the SUPL START message including posmethod(s) supported by the SET, the V-SLP SHALL determine the posmethod. If required for the posmethod, the V-SLP SHALL use the supported positioning protocol (e.g., RRLP, RRC, TIA-801 or LPP/LPPe) from the SUPL START message.
The V-SLC responds with a SUPL RESPONSE tunnelled over RLP back to the H-SLC that it is capable of supporting this request. The SUPL RESPONSE contains at least the sessionid, and the V-SPC address. The SUPL RESPONSE also contains the posmethod. It MAY also contain location information, not meeting the QoP, but giving an initial approximation of the position, based on information received in the SUPL START message.
If a position retrieved or calculated based on information received in the RLP SSRLIR (SUPL START) message which meets a requested QoP is available, the V-SLC MAY send a RLP SSRLIA (SUPL END) message – as opposed to RLP SSRLIA (SUPL RESPONSE) – including the position estimate to the H-SLC and the H-SLC MAY then send a SUPL END message carrying the session id and including the position estimate to the SET (as opposed to the SUPL RESPONSE message) and MAY terminate the session.

G. The H-SLC generates SPC_SET_Key and SPC-TID to be used for mutual V-SPC/SET authentication. The H-SLC forwards SPC_SET_Key and SPC-TID to the V-SLC through an RLP SSRP message. The V-SLC forwards SPC_SET_Key and SPC-TID to the V-SPC through internal communication.

H. The H-SLC forwards the SUPL RESPONSE to the SET. The SUPL RESPONSE contains at least session-id, SPC_SET_Key and SPC-TID to be used by the SET for mutual V-SPC/SET authentication, and the address of the V-SPC to indicate to the SET that a new secure connection SHALL be established. The SUPL RESPONSE MAY also contain location information, not meeting the QoP, but giving an initial approximation of the position, based on information received in the SUPL START message.

I. To initiate the actual positioning session the SET opens a new secure connection to the V-SPC using the address indicated in step H. The SET and V-SPC perform mutual authentication through the keys received in step G and step H and the SET sends a SUPL POS INIT message. Before the new secure connection is established the existing secure connection to the H-SLC is closed. The SUPL POS INIT message contains at least session-id, SET capabilities and Location ID (lid). The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe). The SET MAY provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if this is supported. The SET MAY include the first SUPL POS element in the SUPL POS INIT message. The SET MAY set the Requested Assistance Data element in the SUPL POS INIT. If a position retrieved or calculated based on information received in the SUPL POS INIT message is available which meets a required QoP, the V-SPC MAY directly proceed to step K and not engage in a SUPL POS session otherwise the V-SPC informs the V-SLC that the positioning procedure has started.

J. The SET and the V-SPC exchange several successive positioning procedure messages.
The V-SPC calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance obtained from the V-SPC (SET-Based).

K. Once the position estimate or calculation is complete, the V-SPC sends a SUPL END to the SET and depending on positioning method and positioning protocol optionally includes the position. The SET SHALL release the secure connection and release all resources related to this session.

L. The V-SPC informs the V-SLC of the end of the SUPL positioning session. The V-SPC SHALL release all resources related to this session.

M. The V-SLC sends a RLP SSRP to the H-SLC to inform about the end of the SUPL session. The H-SLP and the V-SLC SHALL release all resources related to this session.

5.2.5 Roaming with H-SLP Positioning Successful Case – Proxy mode

SET Roaming where the H-SLP is involved in the positioning calculation.

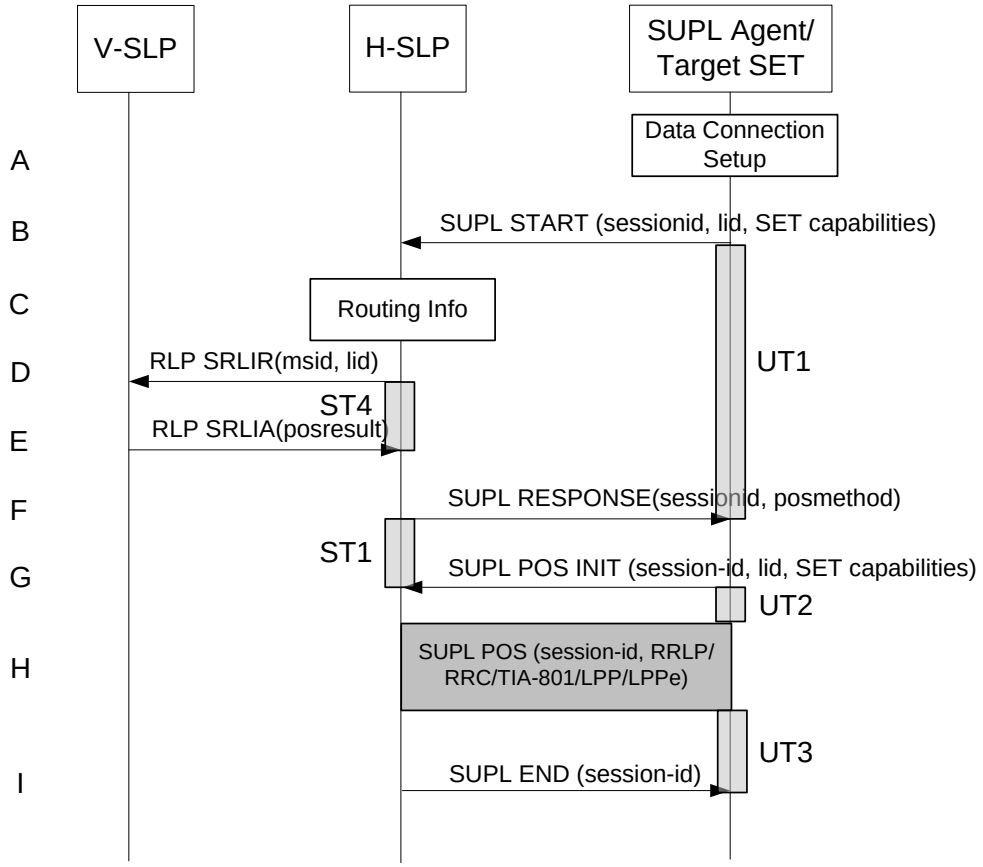

Figure 50: SET-Initiated Roaming with H-SLP Positioning Successful Case – Proxy mode

NOTE: See Appendix D for timer descriptions.

A. The SUPL Agent on the SET receives a request for position from an application running on the SET. The SET takes appropriate action establishing or resuming a secure connection.

B. The SUPL Agent on the SET uses the default address provisioned by the Home Network to establish a secure connection to the H-SLP and sends a SUPL START message to start a positioning session with the H-SLP. The SUPL START message contains session-id, SET capabilities and Location ID (lid). The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe).
If a previously computed position which meets a requested QoP is available at the H-SLP the H-SLP SHALL directly proceed to step I and send a SUPL END message including the position to the SET and end the session.

C. The H-SLP verifies that the target SET is currently SUPL roaming.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside scope of SUPL. However, there are various environment dependent mechanisms.

D. The H-SLP decides that the H-SLP will provide assistance/position calculation and the H-SLP sends a plain RLP SRLIR request to the V-SLP to determine a coarse position for further exchange of SUPL POS messages between SET and H-SLP. The RLP request contains at least the msid and the Location ID (lid).

E. The V-SLP returns a RLP SRLIA message. The RLP SRLIA message contains at least the position result (e.g., coarse position for A-GPS positioning). If the computed position meets the requested QoP, the H-SLP MAY directly proceed to step I.

F. Consistent with the SUPL START message including posmethod(s) supported by the SET, the H-SLP SHALL determine the posmethod. If required for the posmethod, the H-SLP SHALL use the supported positioning protocol (e.g., RRLP, RRC, TIA-801 or LPP/LPPe) from the SUPL START message
The H-SLP responds with the SUPL RESPONSE to the SET. The SUPL RESPONSE contains the session-id but no

H-SLP address, to indicate to the SET that a new connection SHALL NOT be established. The SUPL RESPONSE also contains the posmethod. The SUPL RESPONSE MAY also contain location information, not meeting the QoP, but giving an initial approximation of the position, based on information received in the SUPL START message.

G. After the SET receives the SUPL RESPONSE from H-SLP, the SET sends a SUPL POS INIT message. The SUPL POS INIT message contains at least session-id, SET capabilities and Location ID (lid). The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe). The SET MAY provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if this is supported. The SET MAY include the first SUPL POS element in the SUPL POS INIT message. The SET MAY set the Requested Assistance Data element in the SUPL POS INIT. If a position retrieved or calculated based on information received in the SUPL POS INIT message is available which meets a required QoP, the H-SLP MAY directly proceed to step I and not engage in a SUPL POS session.

H. The SET and the H-SLP exchange several successive positioning procedure messages.
The H-HSLP calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance obtained from the H-SLP (SET-Based).

I. Once the position calculation is complete the H-SLP sends a SUPL END message to the SET informing it that no further positioning procedure will be started and that the location session is finished. Depending on positioning method and used positioning protocol the SLP MAY add the determined position to the SUPL END message. The SET SHALL release the secure connection and release all resources related to this session. The H-SLP SHALL release all resources related to this session.

5.2.6 Roaming with H-SPC Positioning Successful Case – Non-Proxy mode

SET Roaming where the H-SPC is involved in the positioning calculation.

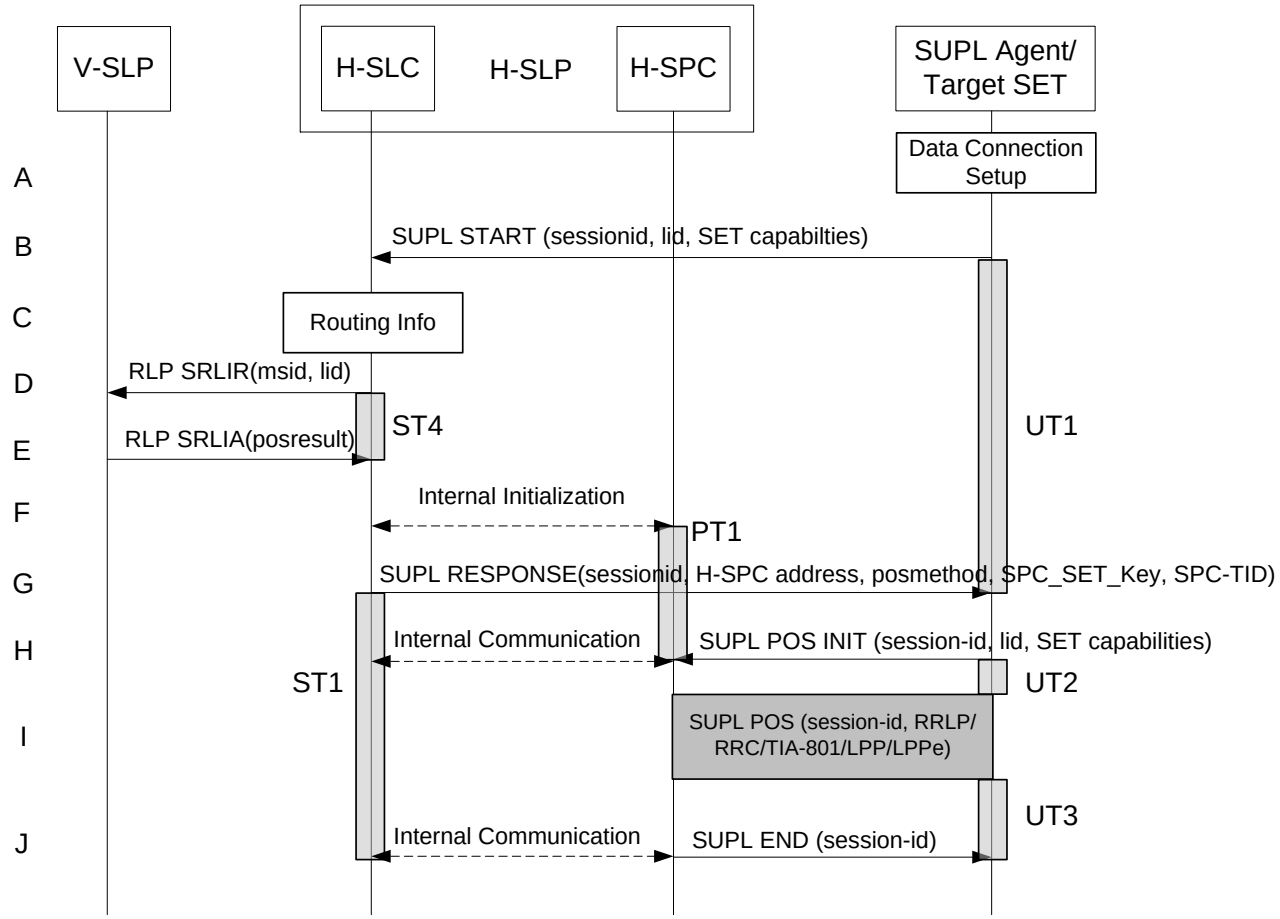

Figure 51: SET-Initiated Roaming with H-SPC Positioning Successful Case – Non-Proxy mode

NOTE: See Appendix D for timer descriptions.

A. The SUPL Agent on the SET receives a request for position from an application running on the SET. The SET takes appropriate action establishing or resuming a secure connection.

B. The SUPL Agent on the SET uses the address provisioned by the Home Network to establish a secure connection to the H-SLC and sends a SUPL START message to the H-SLC to start a SUPL session with the H-SLC and to request authorization to start a SUPL positioning session with the H-SPC.The SUPL START message contains session-id, SET capabilities and Location ID (lid). The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe).
If a previously computed position which meets a requested QoP is available at the H-SLC the H-SLC SHALL send a SUPL END message including the position to the SET and end the session.

C. The H-SLP verifies that the target SET is currently SUPL roaming.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside scope of SUPL.

D. The H-SLC decides that the H-SPC will provide assistance/position calculation and the H-SLC sends an RLP SRLIR request to the V-SLP to determine a coarse position for further exchange of SUPL POS messages between SET and H-SPC. The RLP request contains at least the msid and the Location ID (lid).

E. The V-SLP returns a RLP SRLIA message. The RLP SRLIA message contains at least the position result (e.g., coarse position for A-GPS positioning). If the position received or calculated based on information received in the SUPL START message which meets a requested QoP is available, the H-SLC MAY send a SUPL END to the SET carrying the sessionid and the position result and terminate the SUPL session.

F. The H-SLC allocates a sessionid and informs the H-SPC of the incoming SUPL positioning session from the target SET. The H-SLC also generates SPC_SET_Key and SPC-TID a key to be used for mutual SPC/SET authentication. SPC_SET_Key and SPC-TIDa key are forwarded to the H-SPC through internal communication. The H-SLC also informs the H-SPC of the coarse position obtained from the V-SLP through internal communication..

G. Consistent with the SUPL START message including posmethod(s) supported by the SET, the H-SLP SHALL determine the posmethod. If required for the posmethod, the H-SLP SHALL use the supported positioning protocol (e.g., RRLP, RRC, TIA-801 or LPP/LPPe) from the SUPL START message.
The H-SLC responds with the SUPL RESPONSE to the SET. The SUPL RESPONSE contains the session-id, SPC_SET_Key and SPC-TID a key to be used by the SET for mutual H-SPC/SET authentication, and the H-SPC address. The SUPL RESPONSE also contains the posmethod. The SUPL RESPONSE MAY also contain location information, not meeting the QoP, but giving an initial approximation of the position, based on information received in the SUPL START message.

H. To initiate the actual positioning session the SET opens a new secure connection to the H-SPC using the address indicated in step G. The SET and H-SPC perform mutual authentication through the keys received in step F and step G, and the SET sends a SUPL POS INIT message. Before the new secure connection is established the existing secure connection to the H-SLC is closed. The SUPL POS INIT message contains at least session-id, SET capabilities and Location ID (lid). The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe). The SET MAY provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if this is supported. The SET MAY include the first SUPL POS element in the SUPL POS INIT message. The SET MAY set the Requested Assistance Data element in the SUPL POS INIT. If a position retrieved or calculated based on information received in the SUPL POS INIT message is available which meets a required QoP, the H-SPC MAY directly proceed to step J and not engage in a SUPL POS session. Otherwise the H-SPC informs the H-SLC that the positioning procedure is started.

I. The SET and the H-SPC exchange several successive positioning procedure messages.
The H-SPC calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance obtained from the H-SPC (SET-Based).

J. Once the position calculation is complete the H-SPC sends a SUPL END message to the SET informing it that no further positioning procedure will be started and that the location session is finished. Depending on the positioning protocol used and positioning method the location estimate is optionally included in the SUPL END message. The SET SHALL release the secure connection and release all resources related to this session. The H-SPC informs the H-SLC that the positioning procedure is finished. The H-SPC and the H-SLC SHALL release all resources related to this session.

5.2.7 SET-Initiated Location Request of another SET: Successful Case

In this call scenario, it is assumed that SET_1, the initiating SET, is not roaming, however, this case will also be applicable if the SET_1 is roaming. Figure 52 illustrates the SET-initiated location request of another SET.

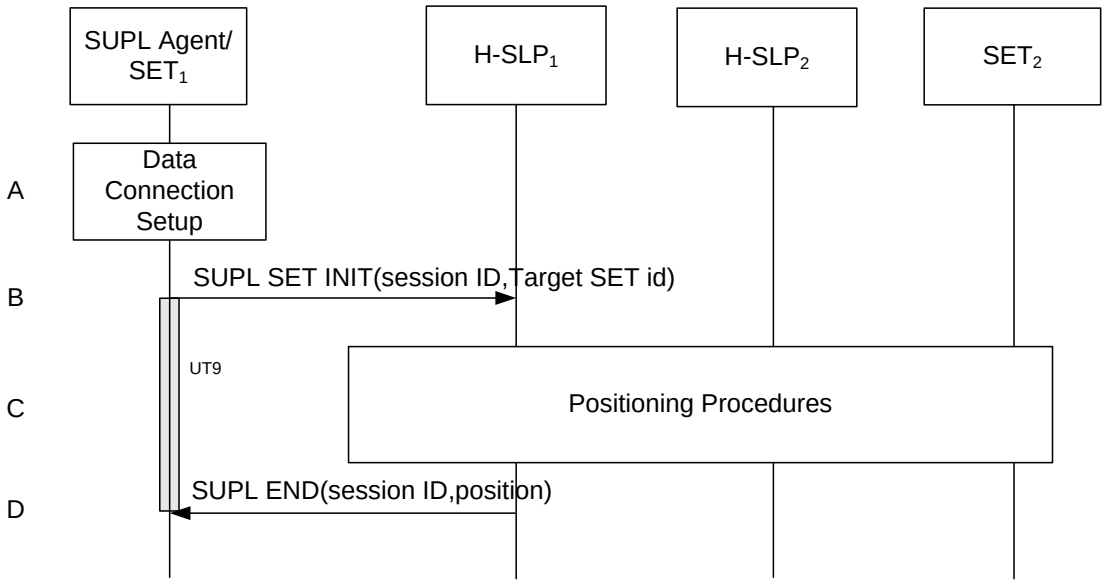

Figure 52: SET-Initiated Location Request of another SET- Successful Case

A. The SUPL Agent on SET_1 receives a request for position of Target SET_2. The SET_1 takes required action establishing or resuming a secure connection.

B. The SUPL Agent on SET_1 uses the default address provisioned by the Home Network to establish a secure connection to the $H\text{-}SLP_1$ and sends a SUPL SET INIT message to start a positioning session of the Target SET_2. The SUPL SET INIT message contains session ID, Target SETid. It MAY also contain the desired QoP. The Target SETid is the identity of the Target SET_2 that will be used by the SLP_1 to identify the home network (SLP_2)of SET_2.

C. The $H\text{-}SLP_1$ determines the location of SET_2. This may involve the use of other SLPs. The MLS enabler and SUPL procedures for Network Initiated queries may be used.

D. The $H\text{-}SLP_1$ sends a SUPL END message containing the position estimate to the SET_1. The SET_1 sends the position estimate back to the SUPL Agent. The SET_1 SHALL release the secure connection and release all resources related to this session. The $H\text{-}SLP_1$ SHALL releases all resources related to this session.

NOTE: the SET MUST NOT release the secure data connection between steps B and D.

5.2.8 SET Initiated Proxy Mode – Triggered Services: Periodic Triggers

This section describes the call flows for SET Initiated periodic triggered services for proxy mode. The trigger thereby resides in the SET.

5.2.8.1 Non-Roaming Successful Case

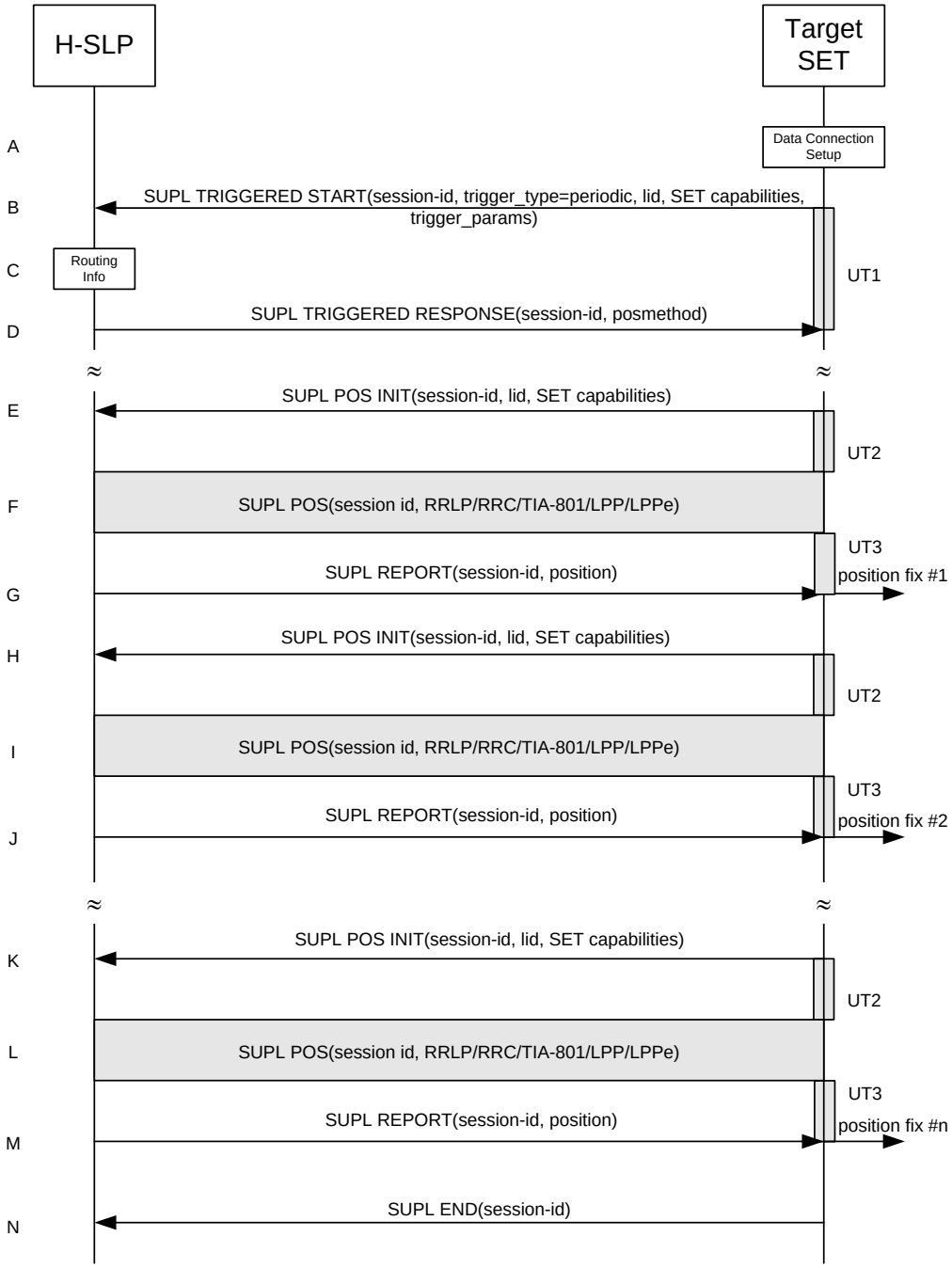

Figure 53: SET Initiated Periodic Trigger Service Non-Roaming Successful Case – Proxy Mode

NOTE: See Appendix D for timer descriptions.

A. The SUPL Agent on the SET receives a request for a periodic triggered service from an application running on the SET. The SET takes appropriate action establishing or resuming a secure connection.

B. The SUPL Agent on the SET uses the default address provisioned by the Home Network to establish a secure connection to the H-SLP and sends a SUPL TRIGGERED START message to start a positioning session with the H-SLP. The SUPL TRIGGERED START message contains session-id, SET capabilities, trigger type indicator (in this case periodic), Location ID (lid) and periodic trigger parameters. The SET capabilities include the supported

positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe).

C. The H-SLP verifies that the target SET is currently not SUPL roaming.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside the scope of SUPL 2.0. However, there are various environment dependent mechanisms.

D. Consistent with the SUPL TRIGGERED START message including the SET capabilities of the SET, the H-SLP SHALL determine the intended positioning method to be used for the periodic triggered session. If required for the posmethod, the H-SLP SHALL use the supported positioning protocol (e.g., RRLP, RRC, TIA-801 or LPP/LPPe) from the SUPL TRIGGERED START message. The H-SLP SHALL respond with a SUPL TRIGGERED RESPONSE message to the SET. The SUPL TRIGGERED RESPONSE contains the session-id but no H-SLP address, to indicate to the SET that a new connection SHALL NOT be established. The SUPL TRIGGERED RESPONSE also contains the posmethod. The SET and the H-SLP MAY release the secure connection.

E. When the periodic trigger in the SET indicates that the first position fix has to be calculated the SET takes appropriate action establishing or resuming a secure connection. The SET then sends a SUPL POS INIT message to start a positioning session with the H-SLP. The SUPL POS INIT message contains at least session-id, SET capabilities and Location ID (lid) parameter. The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe). The SET MAY optionally provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if this is supported. The SET MAY include the first SUPL POS element in the SUPL POS INIT message. The SET MAY set the Requested Assistance Data element in the SUPL POS INIT.
If a position calculated based on information received in the SUPL POS INIT message is available (e.g. a cell-id based position fix) that meets a required QoP, the H-SLP MAY directly proceed to step G and not engage in a SUPL POS session.

F. The SET and the H-SLP exchange several successive positioning procedure messages.
The H-SLP calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance obtained from the H-SLP (SET-Based).

G. Once the position calculation is complete the H-SLP sends a SUPL REPORT message to the SET. The SUPL REPORT message includes the position result if the position estimate is calculated in the H-SLP and therefore needs to be sent to the SET. The SET MAY release the secure connection to the H-SLP.

NOTE: steps E to G are optional and not performed for A-GPS SET Based in the case where no GPS assistance data is required from the network. In this case the SET autonomously calculates a position fix based on the currently available GPS assistance data stored in the SET.

Steps H to M are a repeat of steps E to G.

N. After the last position result has been calculated, the SET ends the periodic triggered session by sending a SUPL END message to the H-SLP.

NOTE: For A-GPS SET Based mode where the SET calculates the position estimate based on GPS assistance data available in the SET, steps E to G are performed whenever new GPS assistance data is required by the SET.

5.2.8.2 Roaming with V-SLP Positioning Successful Case

SUPL Roaming where the V-SLP is involved in the positioning calculation.

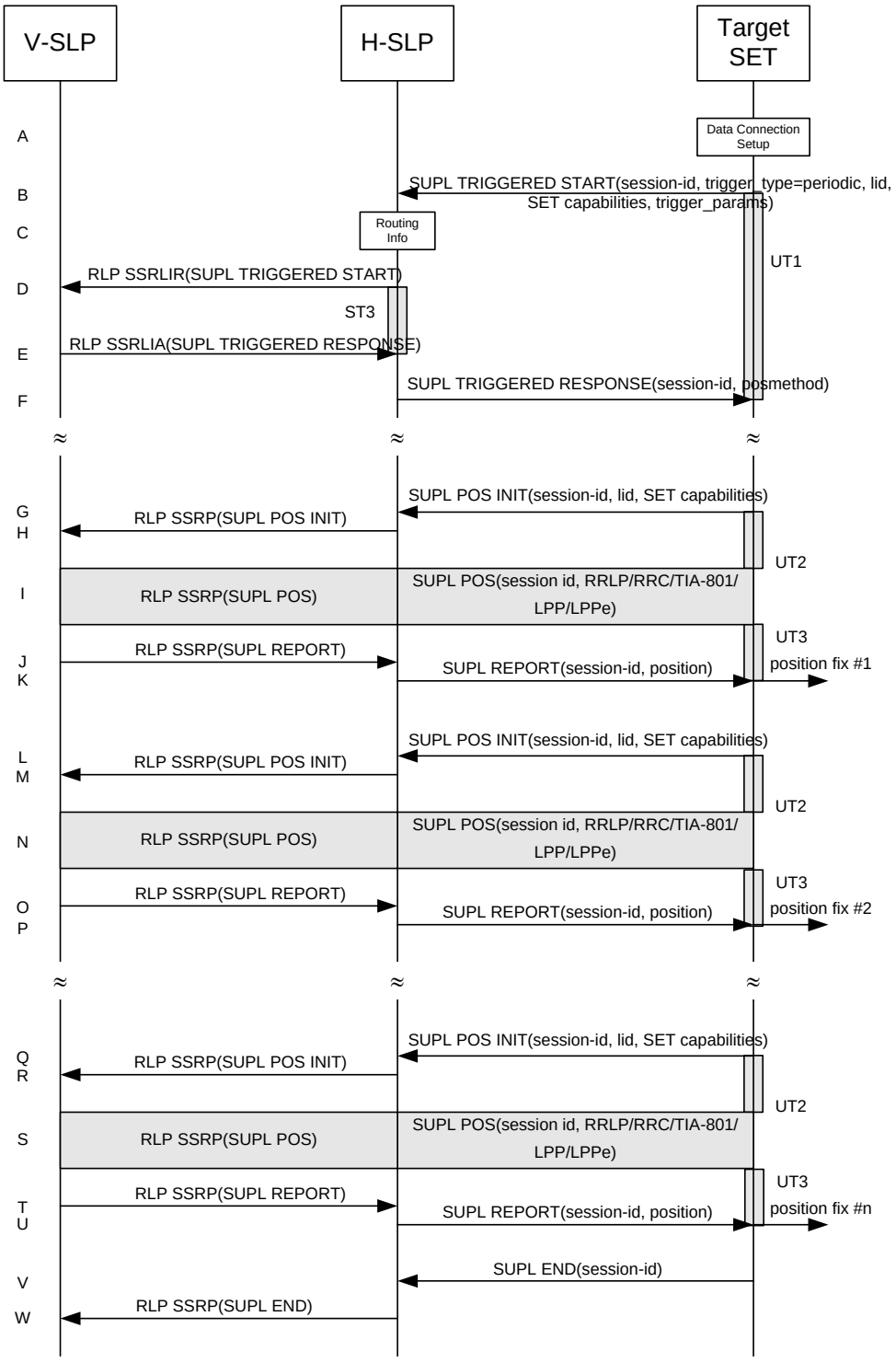

Figure 54: SET Initiated Periodic Trigger Service Roaming with V-SLP Positioning Successful Case – Proxy Mode

NOTE: See Appendix D for timer descriptions.

A. The SUPL Agent on the SET receives a request for a periodic triggered service from an application running on the SET. The SET takes appropriate action establishing or resuming a secure connection.

B. The SUPL Agent on the SET uses the default address provisioned by the Home Network to establish a secure connection to the H-SLP and sends a SUPL TRIGGERED START message to start a positioning session with the

H-SLP. The SUPL TRIGGERED START message contains session-id, SET capabilities, trigger type indicator (in this case periodic), Location ID (lid) and periodic trigger parameters. The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe).

C. The H-SLP verifies that the target SET is currently SUPL roaming.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside scope of SUPL 2.0. However, there are various environment dependent mechanisms.

D. The H-SLP decides that the assistance data/position calculation is done by the V-SLP and sends an RLP SSRLIR tunnelling the SUPL TRIGGERED START message to the V-SLP.

E. Consistent with the SUPL TRIGGERED START message including posmethod(s) supported by the SET, the V-SLP SHALL determine the intended positioning method to be used for the periodic triggered session. If required for the posmethod, the V-SLP SHALL use the supported positioning protocol (e.g., RRLP, RRC, TIA-801 or LPP/LPPe) from the SUPL TRIGGERED START message. The V-SLP responds with a SUPL TRIGGERED RESPONSE tunnelled over RLP in a SSRLIA message back to the H-SLP that it is capable of supporting this request. The SUPL TRIGGERED RESPONSE contains at least the sessionid and posmethod.

F. The H-SLP forwards the SUPL TRIGGERED RESPONSE message to the SET. The SUPL TRIGGERED RESPONSE contains the session-id but no H-SLP address, to indicate to the SET that a new connection SHALL NOT be established. The SUPL TRIGGERED RESPONSE also contains the posmethod. The SET and the H-SLP MAY release the secure connection.

G. When the periodic trigger in the SET indicates that the first position fix has to be calculated the SET takes appropriate action establishing or resuming a secure connection. The SET then sends a SUPL POS INIT message to start a positioning session with the H-SLP. The SUPL POS INIT message contains at least session-id, SET capabilities and Location ID (lid) parameter. The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe). The SET MAY optionally provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if this is supported. The SET MAY include the first SUPL POS element in the SUPL POS INIT message. The SET MAY set the Requested Assistance Data element in the SUPL POS INIT.
If the SUPL POS INIT message contains a position that meets a required QoP, the H-SLP MAY directly proceed to step K.

H. The H-SLP forwards the SUPL POS INIT message to the V-SLP over the RLP tunnel in an SSRP message.
If a position calculated based on information received in the SUPL POS INIT message is available (e.g. a cell-id based position fix) that meets a required QoP, the V-SLP MAY directly proceed to step J and not engage in a SUPL POS session.

I. The SET and the V-SLP exchange several successive positioning procedure messages, tunnelled over RLP in SSRP messages via the H-SLP.
The V-SLP calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance obtained from the V-SLP via H-SLP (SET-Based).

J. Once the position calculation is complete, the V-SLP sends a SUPL REPORT message in an RLP tunnel using an SSRP message to the H-SLP.

K. The H-SLP forwards the SUPL REPORT message to the SET. The SUPL REPORT message includes the position result if the position estimate is calculated in the H-SLP and therefore needs to be sent to the SET. The SET and the H-SLP MAY release the secure connection.

NOTE: steps G to K are optional and not performed for A-GPS SET Based in the case where no GPS assistance data is required from the network. In this case the SET autonomously calculates a position fix based on the currently available GPS assistance data stored in the SET.

Steps L to U are a repeat of steps G to K.

V. After the last position result has been calculated, the SET ends the periodic triggered session by sending a SUPL END message to the H-SLP.

W. The H-SLP informs the V-SLP about the end of the periodic triggered session by sending a SUPL END message using an RLP SSRP tunnel message to the V-SLP.

NOTE: For A-GPS SET Based mode where the SET calculates the position estimate based on GPS assistance data available in the SET, steps G to K are performed whenever new GPS assistance data is required by the SET.

5.2.8.3 Roaming with H-SLP Positioning Successful Case

SUPL Roaming where the H-SLP is involved in the positioning calculation.

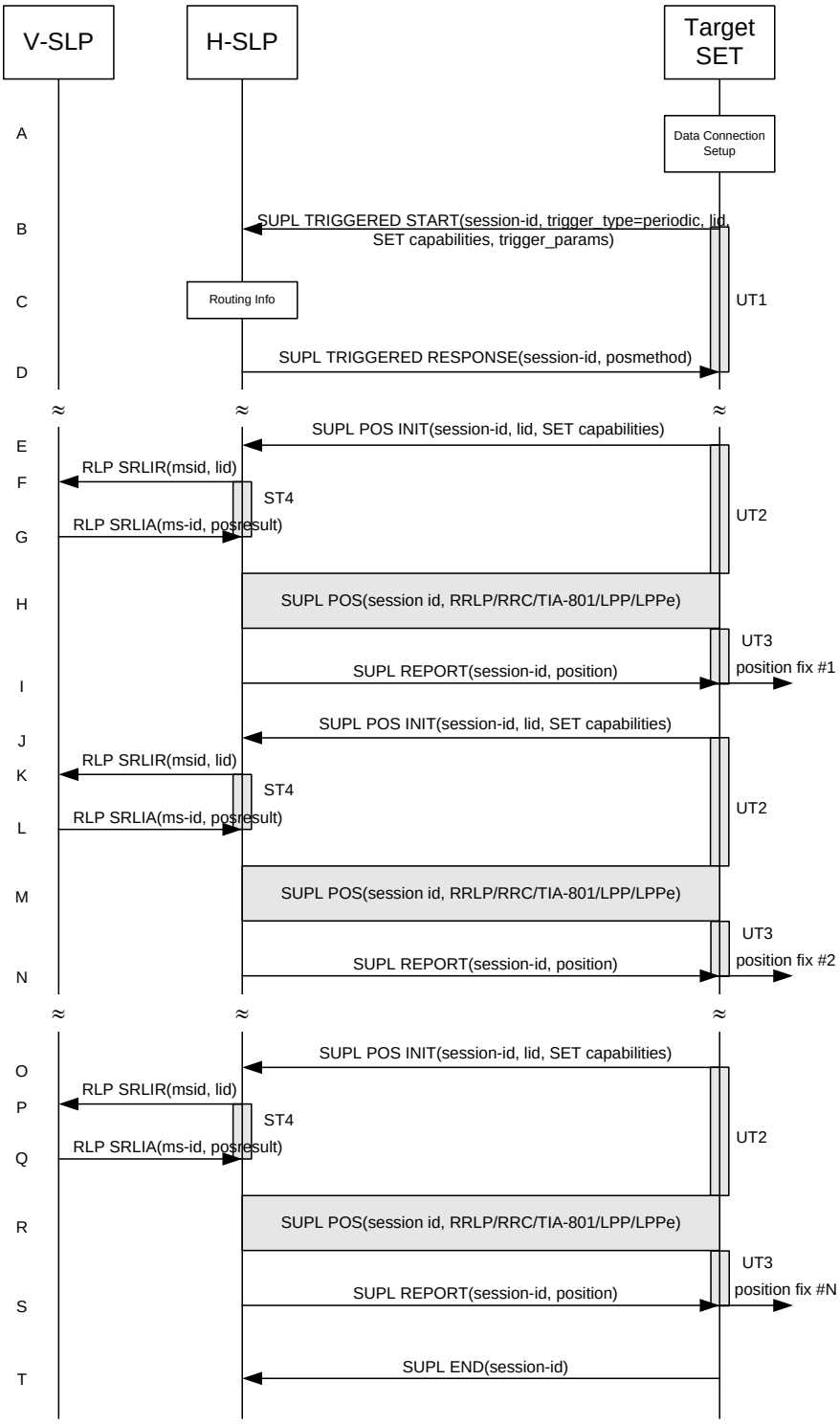

Figure 55: SET Initiated Periodic Trigger Service Roaming with H-SLP Positioning Successful Case – Proxy Mode

NOTE: See Appendix D for timer descriptions.

A. The SUPL Agent on the SET receives a request for a periodic triggered service from an application running on the SET. The SET takes appropriate action establishing or resuming a secure connection.

B. The SUPL Agent on the SET uses the default address provisioned by the Home Network to establish a secure connection to the H-SLP and sends a SUPL TRIGGERED START message to start a positioning session with the

H-SLP. The SUPL TRIGGERED START message contains session-id, SET capabilities, trigger type indicator (in this case periodic), Location ID (lid) and periodic trigger parameters. The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe).

C. The H-SLP verifies that the target SET is currently SUPL roaming.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside scope of SUPL 2.0. However, there are various environment dependent mechanisms.

D. Consistent with the SUPL TRIGGERED START message including posmethod(s) supported by the SET, the H-SLP SHALL determine the intended positioning method to be used for the periodic triggered session. If required for the posmethod, the H-SLP SHALL use the supported positioning protocol (e.g., RRLP, RRC, TIA-801 or LPP/LPPe) from the SUPL TRIGGERED START message. The H-SLP sends a SUPL TRIGGERED RESPONSE message to the SET. The SUPL TRIGGERED RESPONSE contains the session-id but no H-SLP address, to indicate to the SET that a new connection SHALL NOT be established. The SUPL TRIGGERED RESPONSE also contains the posmethod. The SET and the H-SLP MAY release the secure connection.

E. When the periodic trigger in the SET indicates that the first position fix has to be calculated the SET takes appropriate action establishing or resuming a secure connection. The SET then sends a SUPL POS INIT message to start a positioning session with the H-SLP. The SUPL POS INIT message contains at least session-id, SET capabilities and Location ID (lid) parameter. The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe). The SET MAY optionally provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if this is supported. The SET MAY include the first SUPL POS element in the SUPL POS INIT message. The SET MAY set the Requested Assistance Data element in the SUPL POS INIT.
If the SUPL POS INIT message contains a position that meets a required QoP, the H-SLP MAY directly proceed to step I.

F. To obtain a coarse position based on lid received in step E, the H-SLP sends an RLP SRLIR message to the V-SLP.

G. The V-SLP translates the received lid into a position estimate and returns the result to the H-SLP in an RLP SRLIA message.
If the position estimate meets a required QoP, the H-SLP MAY directly proceed to step I and not engage in a SUPL POS session.

H. The SET and the H-SLP exchange several successive positioning procedure messages.
The H-SLP calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance obtained from the H-SLP (SET-Based).

I. Once the position calculation is complete, the H-SLP sends the position estimate in a SUPL REPORT message to the SET. The SUPL REPORT message includes the position result if the position estimate is calculated in the H-SLP and therefore needs to be sent to the SET. The SET MAY release the secure connection to the H-SLP.

NOTE: steps E to I are optional and not performed for A-GPS SET Based in the case where no GPS assistance data is required from the network. In this case the SET autonomously calculates a position fix based on the currently available GPS assistance data stored in the SET.

Steps J to S are a repeat of steps E to I.

T. After the last position result has been calculated, the SET ends the periodic triggered session by sending a SUPL END message to the H-SLP.

NOTE: For A-GPS SET Based mode where the SET calculates the position estimate based on GPS assistance data available in the SET, steps E to I are performed whenever new GPS assistance data is required by the SET.

5.2.9 SET Initiated Proxy Mode – Triggered Services: Event Triggers

This section describes the call flows for SET Initiated area event triggered services for proxy mode. The trigger thereby resides in the SET and the SET makes the decision if an area event occurred based on continuously repeated position determinations.

5.2.9.1 Non-Roaming Successful Case

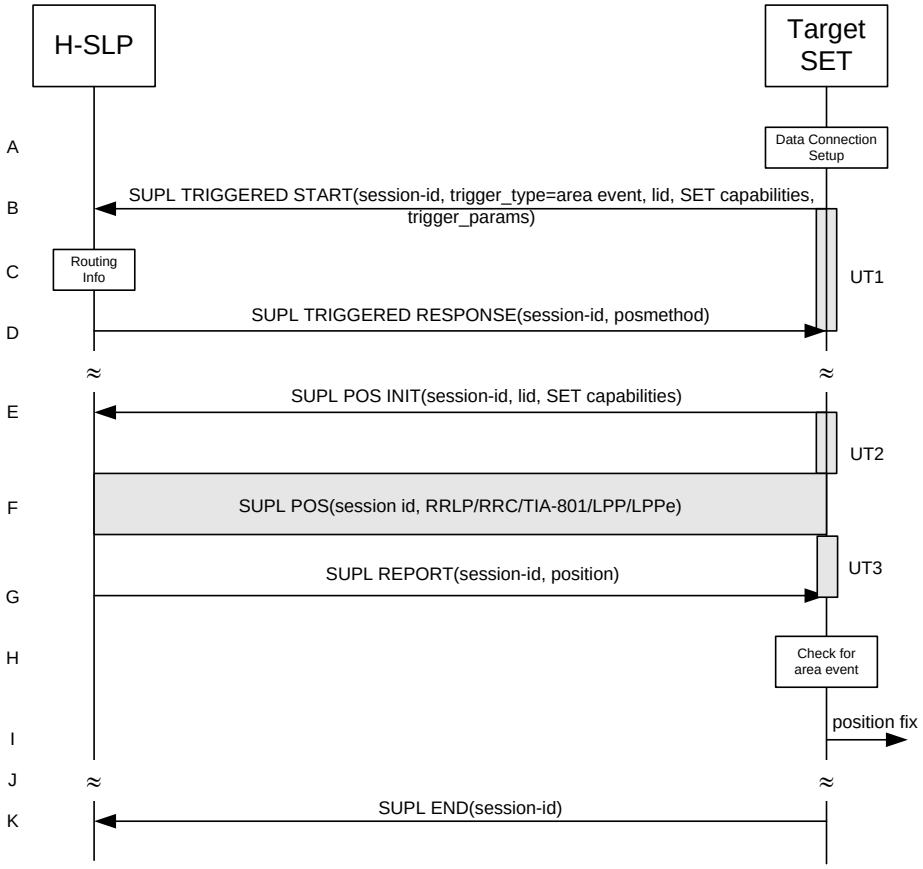

Figure 56: SET Initiated Area Event Trigger Service Non-Roaming Successful Case – Proxy Mode

NOTE: See Appendix D for timer descriptions.

A. The SUPL Agent on the SET receives a request for an area event triggered service from an application running on the SET. The SET takes appropriate action establishing or resuming a secure connection.

B. The SUPL Agent on the SET uses the default address provisioned by the Home Network to establish a secure connection to the H-SLP and sends a SUPL TRIGGERED START message to start a positioning session with the H-SLP. The SUPL TRIGGERED START message contains session-id, SET capabilities, trigger type indicator (in this case area event), Location ID (lid) and area event trigger parameters. The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe).

C. The H-SLP verifies that the target SET is currently not SUPL roaming.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside the scope of SUPL 2.0. However, there are various environment dependent mechanisms.

D. Consistent with the SUPL TRIGGERED START message including the SET capabilities of the SET, the H-SLP SHALL determine the intended positioning method to be used for the area event triggered session. If required for the posmethod, the H-SLP SHALL use the supported positioning protocol (e.g., RRLP, RRC, TIA-801 or LPP/LPPe) from the SUPL TRIGGERED START message. The H-SLP SHALL respond with a SUPL TRIGGERED RESPONSE message to the SET. The SUPL TRIGGERED RESPONSE contains the session-id but no H-SLP address, to indicate to the SET that a new connection SHALL NOT be established. The SUPL TRIGGERED RESPONSE also contains the posmethod. The SUPL TRIGGERED RESPONSE message may contain the area ids of the specified area for the area event triggered session. The SET and the H-SLP MAY release the secure connection.

E. If the area ids are downloaded in step D, the SET SHALL compare the current area id to the downloaded area ids. When the area event trigger in the SET or the comparison of the current area id to the downloaded area ids indicates that a position fix has to be calculated, the SET takes appropriate action establishing or resuming a secure connection. The SET then sends a SUPL POS INIT message to start a positioning session with the H-SLP. The SUPL POS INIT message contains at least session-id, SET capabilities and Location ID (lid) parameter. The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe). The SET MAY optionally provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if this is supported. The SET MAY include the first SUPL POS element in the SUPL POS INIT message. The SET MAY set the Requested Assistance Data element in the SUPL POS INIT.
If a position calculated based on information received in the SUPL POS INIT message is available (e.g. a cell-id based position fix) that meets a required QoP, the H-SLP MAY directly proceed to step G and not engage in a SUPL POS session.

F. The SET and the H-SLP exchange several successive positioning procedure messages.
The H-SLP calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance obtained from the H-SLP (SET-Based).

G. Once the position calculation is complete the H-SLP sends a SUPL REPORT message to the SET. The SET MAY release the secure connection to the H-SLP.
The SUPL REPORT message includes the position result if the position estimate is calculated in the H-SLP and therefore needs to be sent to the SET.

H. The SET compares the calculated position estimate with the event area to check if the event trigger condition has been met.

I. If the area event was triggered the SET forwards the calculated position estimate to the internal SUPL Agent.

J. If the SET decides to end the triggered session the SET proceeds to step K. Otherwise whenever the area event trigger mechanism in the SET indicates that a new position fix has to be performed, steps E to I are repeated.

K. The SET ends the triggered session by sending a SUPL END message to the H-SLP.

The call flow described in Figure 56 is applicable to all positioning methods, however, individual steps within the call flows are optional:

- Step F (SUPL POS) is not performed for cell-id based positioning methods.
- In A-GPS SET Based mode where no GPS assistance data is required from the network, no interaction with the H-SLP is required to calculate a position estimate. Interaction with the H-SLP is only required for GPS assistance data update in which case steps E to G are performed.

5.2.9.2 Roaming with V-SLP Positioning Successful Case

SUPL Roaming where the V-SLP is involved in the positioning calculation.

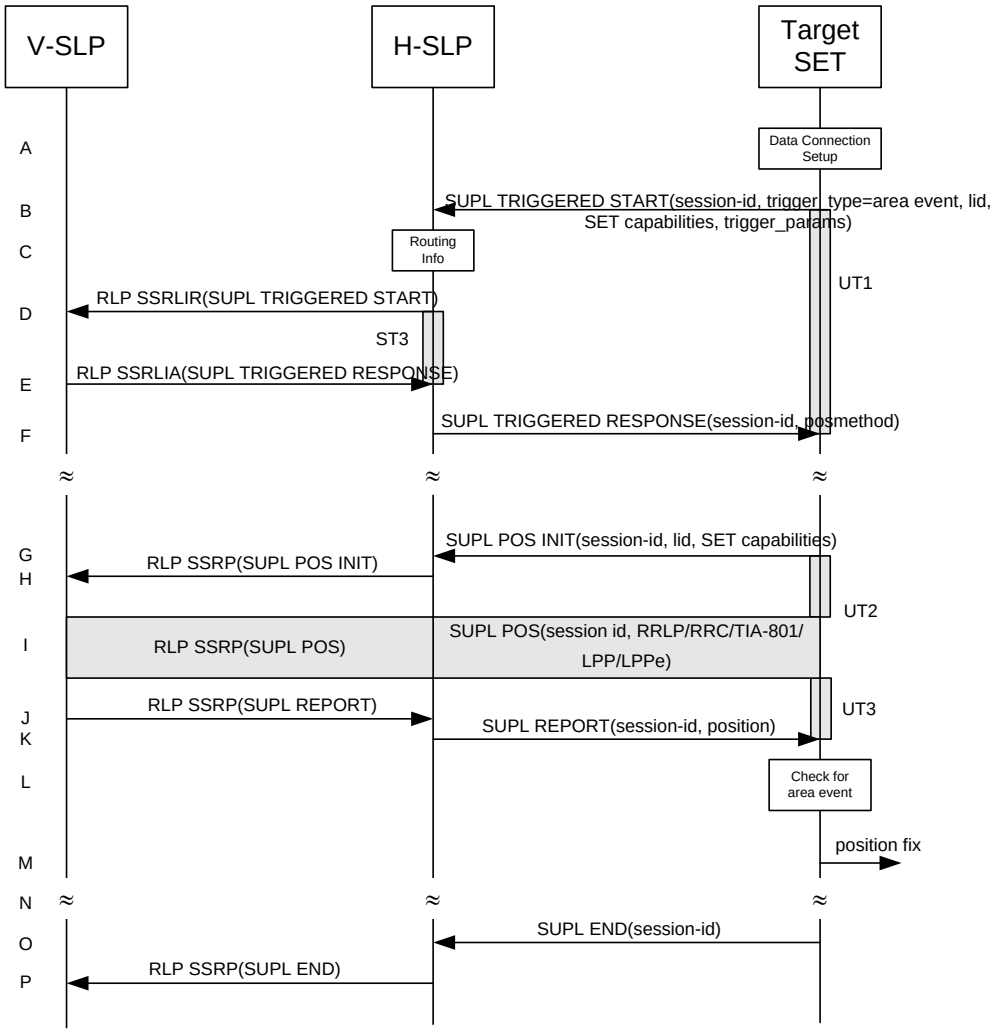

Figure 57: SET Initiated Area Event Trigger Service Roaming with V-SLP Positioning Successful Case – Proxy Mode

NOTE: See Appendix D for timer descriptions.

A. The SUPL Agent on the SET receives a request for an area event triggered service from an application running on the SET. The SET takes appropriate action establishing or resuming a secure connection.

B. The SUPL Agent on the SET uses the default address provisioned by the Home Network to establish a secure connection to the H-SLP and sends a SUPL TRIGGERED START message to start a positioning session with the H-SLP. The SUPL TRIGGERED START message contains session-id, SET capabilities, trigger type indicator (in this case area event), Location ID (lid) and area event trigger parameters. The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe).

C. The H-SLP verifies that the target SET is currently SUPL roaming.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside scope of SUPL 2.0. However, there are various environment dependent mechanisms.

D. The H-SLP decides that the assistance data/position calculation is done by the V-SLP and sends an RLP SSRLIR tunnelling the SUPL TRIGGERED START message to the V-SLP. The area event trigger parameters such as area information requested by SUPL Agent for the area event triggered session MAY be included in this message by the H-SLP.

E. Consistent with the SUPL TRIGGERED START message including posmethod(s) supported by the SET, the V-SLP SHALL determine the intended positioning method to be used for the area event triggered session. If required

for the posmethod, the V-SLP SHALL use the supported positioning protocol (e.g., RRLP, RRC, TIA-801 or LPP/LPPe) from the SUPL TRIGGERED START message. The V-SLP responds with a SUPL TRIGGERED RESPONSE tunnelled over RLP in a SSRLIA message back to the H-SLP that it is capable of supporting this request. The SUPL TRIGGERED RESPONSE contains at least the sessionid and posmethod. The V-SLP MAY include area ids corresponding to the area for the area event trigger session in the SUPL TRIGGERED RESPONSE message.

F. The H-SLP forwards the SUPL TRIGGERED RESPONSE message to the SET. The SUPL TRIGGERED RESPONSE contains the session-id but no H-SLP address, to indicate to the SET that a new connection SHALL NOT be established. The SUPL TRIGGERED RESPONSE also contains the posmethod. The SUPL TRIGGERED RESPONSE message may contain the area ids of the specified area for the area event triggered session. The SET and the H-SLP MAY release the secure connection.

G. If the area ids are downloaded in step F, the SET SHALL compare the current area id to the downloaded area ids. When the area event trigger in the SET or the comparison of the current area id to the downloaded area ids indicates that a position fix has to be calculated the SET takes appropriate action establishing or resuming a secure connection. The SET then sends a SUPL POS INIT message to start a positioning session with the H-SLP. The SUPL POS INIT message contains at least session-id, SET capabilities and Location ID (lid) parameter. The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe). The SET MAY optionally provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if this is supported. The SET MAY include the first SUPL POS element in the SUPL POS INIT message. The SET MAY set the Requested Assistance Data element in the SUPL POS INIT.
If a position is received in the SUPL POS INIT message that meets a required QoP, the H-SLP MAY directly proceed to step K and not engage in a SUPL POS session.

H. The H-SLP forwards the SUPL POS INIT message to the V-SLP over the RLP tunnel in an SSRP message.
If a position calculated based on information received in the SUPL POS INIT message is available (e.g. a cell-id based position fix) that meets a required QoP, the V-SLP MAY directly proceed to step J and not engage in a SUPL POS session.

I. The SET and the V-SLP exchange several successive positioning procedure messages, tunnelled over RLP in SSRP messages via the H-SLP.
The V-SLP calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance obtained from the V-SLP via H-SLP (SET-Based).

J. Once the position calculation is complete, the V-SLP sends a SUPL REPORT message in an RLP tunnel using an SSRP message to the H-SLP.
The SUPL REPORT message includes the position result if the position estimate is calculated in the V-SLP and therefore needs to be sent to the SET.

K. The H-SLP forwards the SUPL REPORT message to the SET. The SET and the H-SLP MAY release the secure connection.
The SUPL REPORT message includes the position result if the position estimate is calculated in the V-SLP (or the H-SLP) and therefore needs to be sent to the SET.

L. The SET compares the calculated position estimate with the event area to check if the event trigger condition has been met.

M. If the area event was triggered the SET forwards the calculated position estimate to the internal SUPL Agent

N. If the SET decides to end the triggered session the SET proceeds to step O. Otherwise whenever the area event trigger mechanism in the SET indicates that a new position fix has to be performed, steps G to M are repeated.

O. The SET ends the triggered session by sending a SUPL END message to the H-SLP.

P. The H-SLP informs the V-SLP about the end of the triggered session by sending a SUPL END message in an RLP SSRP tunnel message.

The call flow described in Figure 57 is applicable to all positioning methods, however, individual steps within the call flows are optional:

- Step I (SUPL POS) is not performed for cell-id based positioning methods.
- In A-GPS SET Based mode where no GPS assistance data is required from the network, no interaction with the H-SLP is required to calculate a position estimate. Interaction with the H-SLP is only required for GPS assistance data update in which case steps G to K are performed.

5.2.9.3 Roaming with H-SLP Positioning Successful Case

SUPL Roaming where the H-SLP is involved in the positioning calculation.

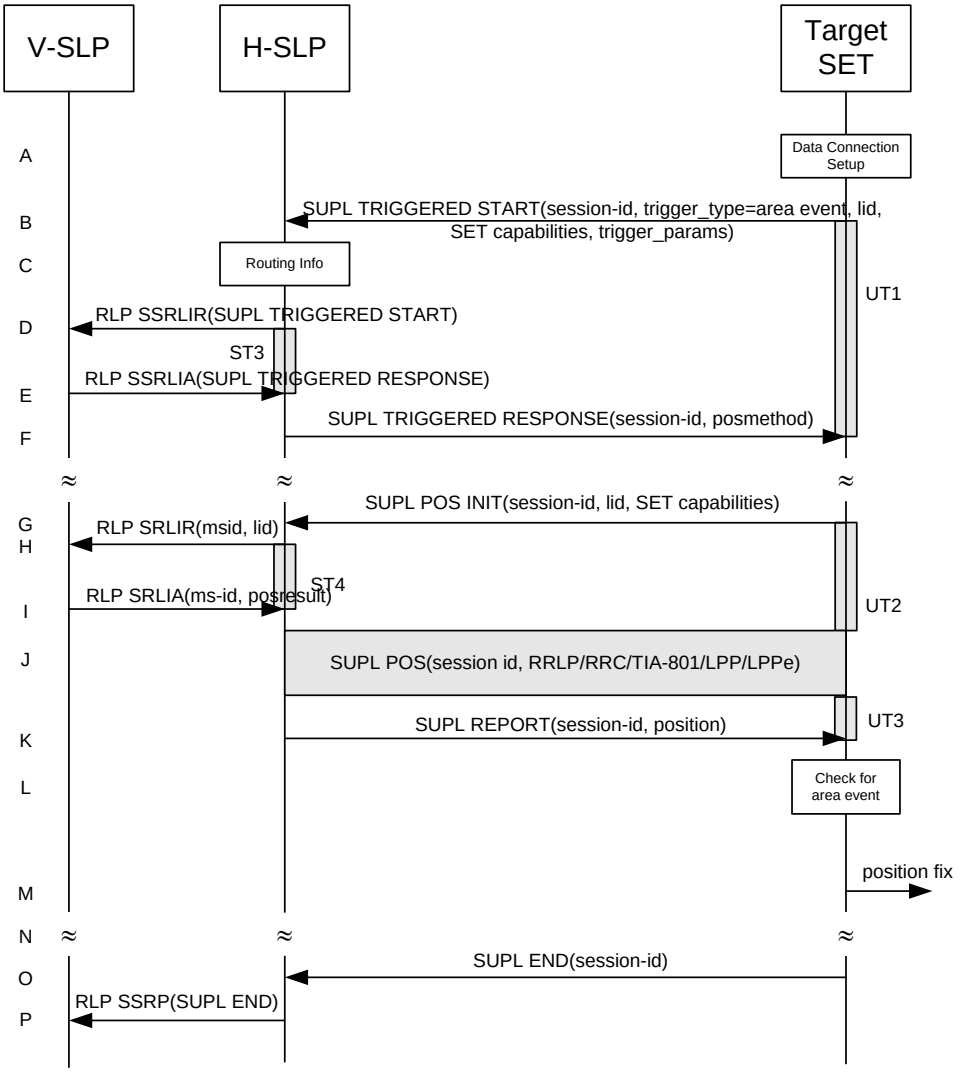

Figure 58: SET Initiated Area Event Trigger Service Roaming with H-SLP Positioning Successful Case – Proxy Mode

NOTE: See Appendix D for timer descriptions.

A. The SUPL Agent on the SET receives a request for an area event triggered service from an application running on the SET. The SET takes appropriate action establishing or resuming a secure connection.

B. The SUPL Agent on the SET uses the default address provisioned by the Home Network to establish a secure connection to the H-SLP and sends a SUPL TRIGGERED START message to start a positioning session with the H-SLP. The SUPL TRIGGERED START message contains session-id, SET capabilities, trigger type indicator (in this case area event), Location ID (lid) and area event trigger parameters. The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe).

C. The H-SLP verifies that the target SET is currently SUPL roaming.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside scope of SUPL 2.0. However, there are various environment dependent mechanisms.

D. Based on the received lid or other mechanisms, the H-SLP determines the V-SLP and sends an RLP SSRLIR including a SUPL TRIGGERED START to the V-SLP to inform the V-SLP that an area event triggered session is in the progress of being initiated with the H-SLP. The area event trigger parameters such as area information requested by SUPL Agent for the area event triggered session MAY be included in this message by the H-SLP.

E. The V-SLP acknowledges the RLP request received in step D with a SUPL TRIGGERED RESPONSE message which is carried inside an RLP SSRLIA message. The V-SLP MAY include area ids corresponding to the area for the area event trigger session in the SUPL TRIGGERED RESPONSE message.

F. Consistent with the SUPL TRIGGERED START message including posmethod(s) supported by the SET, the H-SLP SHALL determine the intended positioning method to be used for the area event triggered session. If required for the posmethod, the H-SLP SHALL use the supported positioning protocol (e.g., RRLP, RRC, TIA-801 or LPP/LPPe) from the SUPL TRIGGERED START message. The H-SLP sends a SUPL TRIGGERED RESPONSE message to the SET. The SUPL TRIGGERED RESPONSE contains the session-id but no H-SLP address, to indicate to the SET that a new connection SHALL NOT be established. The SUPL TRIGGERED RESPONSE also contains the posmethod. The SUPL TRIGGERED RESPONSE message may contain the area ids of the specified area for the area event triggered session. The SET and the H-SLP MAY release the secure connection.

G. If the area ids are downloaded in step F, the SET SHALL compare the current area id to the downloaded area ids. When the area event trigger in the SET or the comparison of the current area id to the downloaded area ids indicates that a position fix has to be calculated the SET takes appropriate action establishing or resuming a secure connection. The SET then sends a SUPL POS INIT message to start a positioning session with the H-SLP. The SUPL POS INIT message contains at least session-id, SET capabilities and Location ID (lid) parameter. The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe). The SET MAY optionally provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if this is supported. The SET MAY include the first SUPL POS element in the SUPL POS INIT message. The SET MAY set the Requested Assistance Data element in the SUPL POS INIT.
If a position is received in the SUPL POS INIT message that meets a required QoP, the H-SLP MAY directly proceed to step K and not engage in a SUPL POS session.

H. To obtain a coarse position based on lid received in step G, the H-SLP sends an RLP SRLIR message to the V-SLP.

I. The V-SLP translates the received lid into a position estimate and returns the result to the H-SLP in an RLP SRLIA message.
If the received position meets a required QoP, the H-SLP MAY directly proceed to step K and not engage in a SUPL POS session.

J. The SET and the H-SLP exchange several successive positioning procedure messages.
The H-SLP calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance obtained from the H-SLP (SET-Based).

K. Once the position calculation is complete, the H-SLP sends a SUPL REPORT message to the SET.
The SUPL REPORT message includes the position result if the position estimate is calculated in the H-SLP and therefore needs to be sent to the SET.

L. The SET compares the calculated position estimate with the event area to check if the event trigger condition has been met.

M. If the area event was triggered the SET forwards the calculated position estimate to the internal SUPL Agent.

N. If the SET decides to end the triggered session the SET proceeds to step O. Otherwise whenever the area event trigger mechanism in the SET indicates that a new position fix has to be performed, steps G to M are repeated.

O. The SET ends the triggered session by sending a SUPL END message to the H-SLP.

P. The H-SLP informs the V-SLP about the end of the triggered session by sending a SUPL END message in an RLP SSRP tunnel message.

The call flow described in Figure 58 is applicable to all positioning methods, however, individual steps within the call flows are optional:

- Step J (SUPL POS) is not performed for cell-id based positioning methods.
- In A-GPS SET Based mode where no GPS assistance data is required from the network, no interaction with the H-SLP is required to calculate a position estimate. Interaction with the H-SLP is only required for GPS assistance data update in which case steps G to K are performed.

5.2.10 SET Initiated Non-Proxy Mode – Triggered Services: Periodic Triggers

This section describes the call flows for SET Initiated periodic triggered services for non-proxy mode. The trigger thereby resides in the SET.

5.2.10.1 Non-Roaming Successful Case

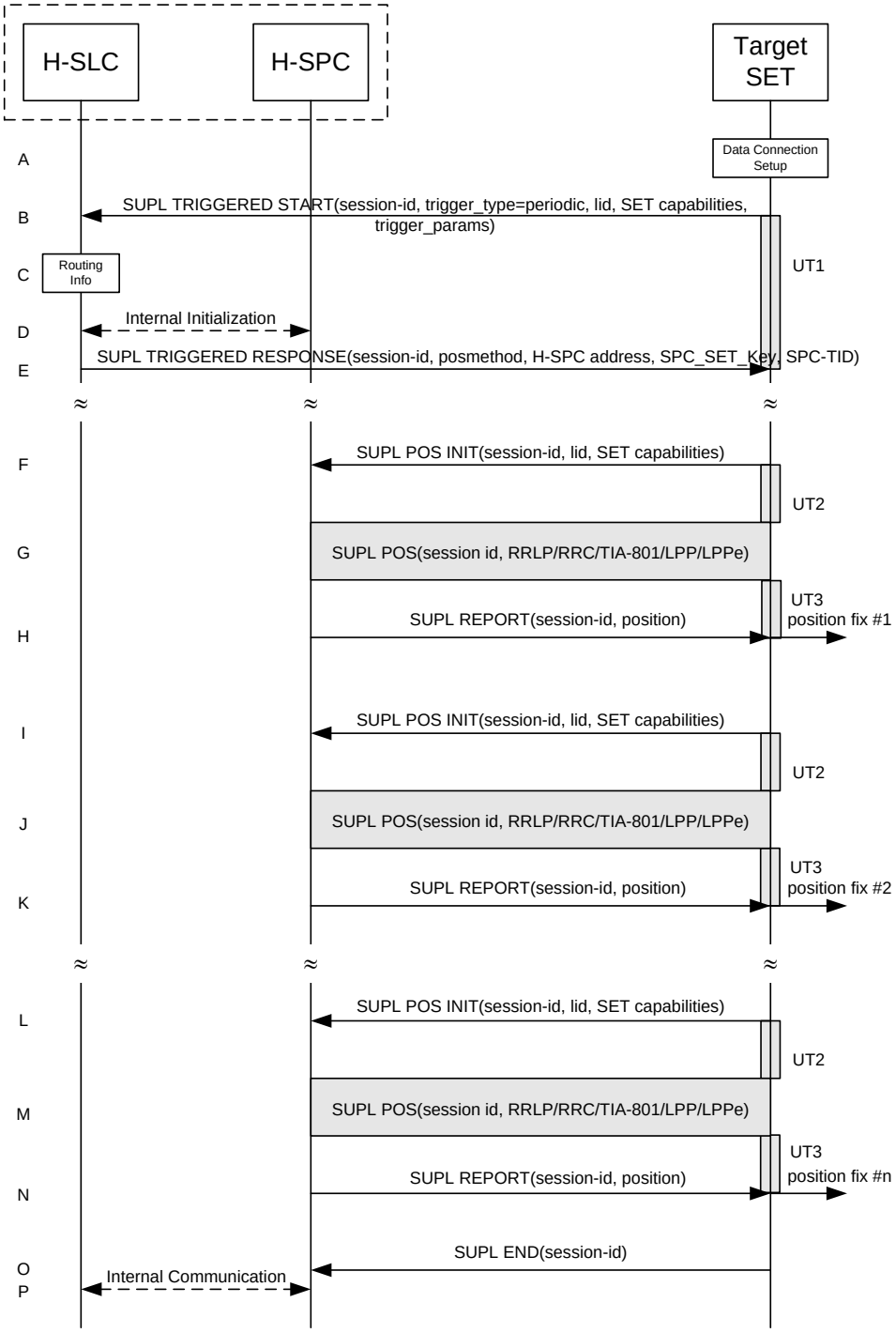

Figure 59: SET Initiated Periodic Trigger Service Non-Roaming Successful Case – Non-Proxy Mode

NOTE: See Appendix D for timer descriptions.

A. The SUPL Agent on the SET receives a request for a periodic triggered service from an application running on the SET. The SET takes appropriate action establishing or resuming a secure connection.

B. The SUPL Agent on the SET uses the default address provisioned by the Home Network to establish a secure connection to the H-SLC and sends a SUPL TRIGGERED START message to start a positioning session with the

H-SLP. The SUPL TRIGGERED START message contains session-id, SET capabilities, trigger type indicator (in this case periodic), Location ID (lid) and periodic trigger parameters. The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe).

C. The H-SLC verifies that the target SET is currently not SUPL roaming.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside the scope of SUPL 2.0. However, there are various environment dependent mechanisms.

D. Through internal communication the H-SLC requests service for a periodic triggered session from the H-SPC. The H-SLC also generates SPC_SET_Key and SPC-TID to be used for mutual H-SPC/SET authentication and forwards both to the H-SPC. The H-SPC grants or denies the request and informs the H-SLC accordingly.

E. Consistent with the SUPL TRIGGERED START message including the SET capabilities of the SET, the H-SLC SHALL determine the intended positioning method to be used for the area event triggered session. If required for the posmethod, the H-SLC SHALL use the supported positioning protocol (e.g., RRLP, RRC, TIA-801 or LPP/LPPe) from the SUPL TRIGGERED START message. The H-SLC SHALL respond with a SUPL TRIGGERED RESPONSE message to the SET. The SUPL TRIGGERED RESPONSE message contains session-id, posmethod, H-SPC address and SPC_SET_Key and SPC-TID. The SET and the H-SLP MAY release the secure connection.

F. When the periodic trigger in the SET indicates that the first position fix has to be calculated the SET takes appropriate action establishing or resuming a secure connection. The SET then sends a SUPL POS INIT message to start a positioning session with the H-SPC. The SUPL POS INIT message contains at least session-id, SET capabilities and Location ID (lid) parameter. The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe). The SET MAY optionally provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if this is supported. The SET MAY include the first SUPL POS element in the SUPL POS INIT message. The SET MAY set the Requested Assistance Data element in the SUPL POS INIT.
If a position calculated based on information received in the SUPL POS INIT message is available (e.g. a cell-id based position fix) that meets a required QoP, the H-SPC MAY directly proceed to step H and not engage in a SUPL POS session.

G. The SET and the H-SPC exchange several successive positioning procedure messages.
The H-SPC calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance data obtained from the H-SPC (SET-Based).

H. Once the position calculation is complete the H-SPC sends a SUPL REPORT message to the SET. The SUPL REPORT message includes the position result if the position estimate is calculated in the H-SLP and therefore needs to be sent to the SET. The SET MAY release the secure connection to the H-SLP.

NOTE: steps F to H are optional and not performed for A-GPS SET Based in the case where no GPS assistance data is required from the network. In this case the SET autonomously calculates a position fix based on the currently available GPS assistance data stored in the SET.

Steps I to N are a repeat of steps F to H.

O. After the last position result has been calculated, the SET ends the periodic triggered session by sending a SUPL END message to the H-SPC.

P. The H-SPC informs the H-SLC through internal communication that the periodic triggered session has ended.

NOTE: For A-GPS SET Based mode where the SET calculates the position estimate based on GPS assistance data available in the SET, steps F to H are performed whenever new GPS assistance data is required by the SET.

5.2.10.2 Roaming with V-SLP Positioning Successful Case

SUPL Roaming where the V-SLP is involved in the positioning calculation.

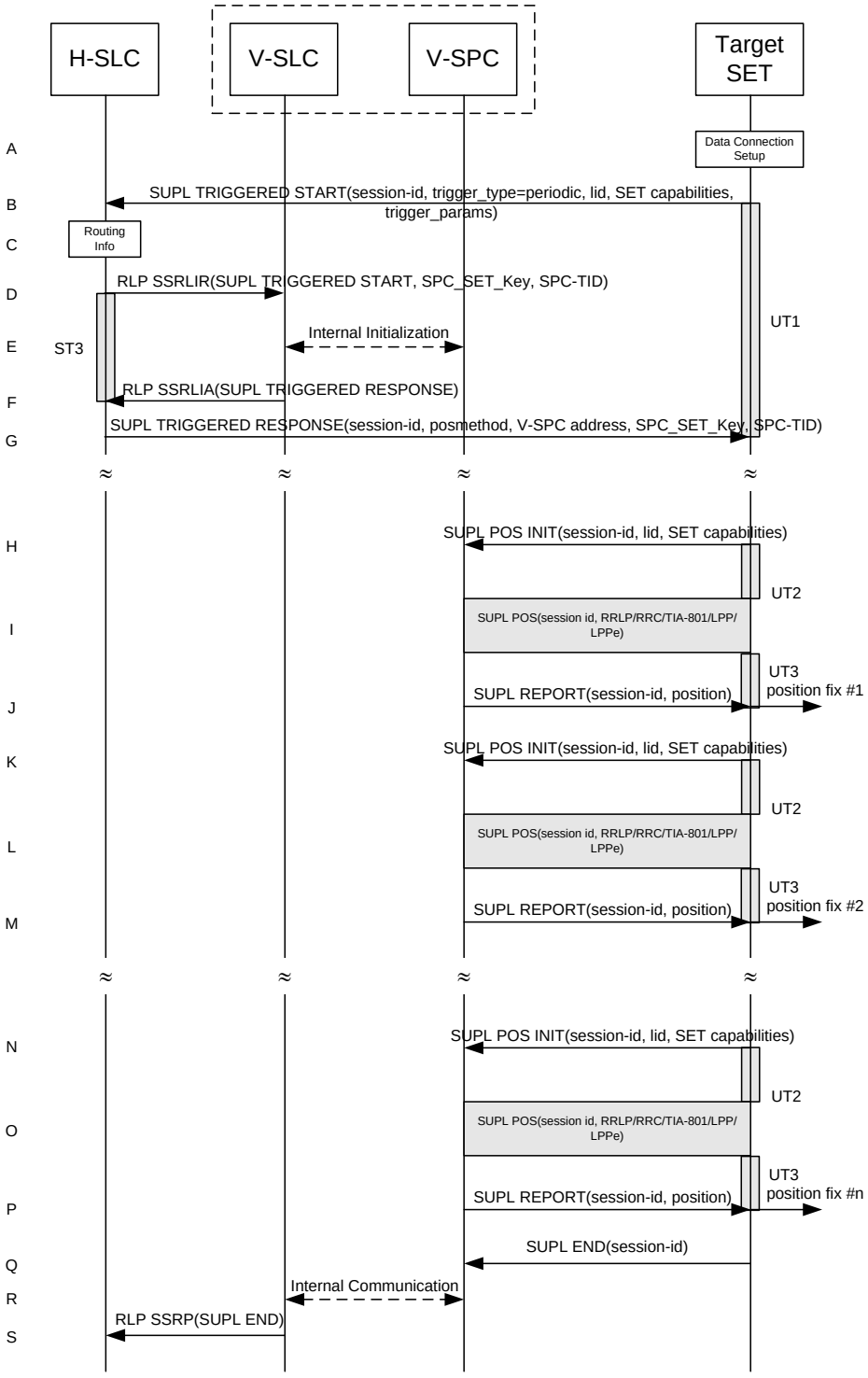

Figure 60: SET Initiated Periodic Trigger Service Roaming with V-SLP Positioning Successful Case – Non-Proxy Mode

NOTE: See Appendix D for timer descriptions.

A. The SUPL Agent on the SET receives a request for a periodic triggered service from an application running on the SET. The SET takes appropriate action establishing or resuming a secure connection.

B. The SUPL Agent on the SET uses the default address provisioned by the Home Network to establish a secure connection to the H-SLC and sends a SUPL TRIGGERED START message to start a positioning session with the H-SLP. The SUPL TRIGGERED START message contains session-id, SET capabilities, trigger type indicator (in this case periodic), Location ID (lid) and periodic trigger parameters. The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe).

C. The H-SLC verifies that the target SET is currently SUPL roaming.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside scope of SUPL 2.0. However, there are various environment dependent mechanisms.

D. The H-SLC decides that the assistance data/position calculation is done by the V-SLP and sends an RLP SSRLIR message tunnelling the SUPL TRIGGERED START message to the V-SLC. The H-SLC also generates SPC_SET_Key and SPC-TID to be used for V-SPC/SET mutual authentication and includes both in the RLP SSRLIR message.

E. Through internal communication the V-SLC requests service for a periodic triggered session from the V-SPC. The V-SLC also forwards the SPC_SET_Key and SPC-TID to the V-SPC. The V-SPC grants or denies the request and informs the V-SLC accordingly.

F. Consistent with the SUPL TRIGGERED START message including posmethod(s) supported by the SET, the V-SLC SHALL determine the intended positioning method to be used for the periodic triggered session. If required for the posmethod, the V-SLC SHALL use the supported positioning protocol (e.g., RRLP, RRC, TIA-801 or LPP/LPPe) from the SUPL TRIGGERED START message. The V-SLC responds with a SUPL TRIGGERED RESPONSE tunnelled over RLP in a SSRLIA message back to the H-SLC that it is capable of supporting this request. The SUPL TRIGGERED RESPONSE contains at least the sessionid, posmethod and the V-SPC address.

G. The H-SLC sends a SUPL TRIGGERED RESPONSE message to the SET. The SUPL TRIGGERED RESPONSE message contains session-id, posmethod, V-SPC address and SPC_SET_Key and SPC-TID. The SET and the H-SLC MAY release the secure connection.

H. When the periodic trigger in the SET indicates that the first position fix has to be calculated the SET takes appropriate action establishing or resuming a secure connection. The SET then sends a SUPL POS INIT message to start a positioning session with the V-SPC. The SUPL POS INIT message contains at least session-id, SET capabilities and Location ID (lid) parameter. The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe). The SET MAY optionally provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if this is supported. The SET MAY include the first SUPL POS element in the SUPL POS INIT message. The SET MAY set the Requested Assistance Data element in the SUPL POS INIT.
If a position calculated based on information received in the SUPL POS INIT message is available (e.g. a cell-id based position fix) that meets a required QoP, the V-SPC MAY directly proceed to step J and not engage in a SUPL POS session.

I. The SET and the V-SPC exchange several successive positioning procedure messages.
The V-SPC calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance data obtained from the V-SPC (SET-Based).

J. Once the position calculation is complete, the V-SPC sends a SUPL REPORT message to the SET. The SUPL REPORT message includes the position result if the position estimate is calculated in the H-SLP and therefore needs to be sent to the SET. The SET and the H-SPC MAY release the secure connection.

NOTE: steps H to J are optional and not performed for A-GPS SET Based in the case where no GPS assistance data is required from the network. In this case the SET autonomously calculates a position fix based on the currently available GPS assistance data stored in the SET.

Steps K to P are a repeat of steps H to J.

Q. After the last position result has been calculated, the SET ends the periodic triggered session by sending a SUPL END message to the V-SPC.

R. Through internal communication the V-SPC informs the V-SLC about the end of the periodic triggered session.

S. The V-SLC informs the H-SLC about the end of the periodic triggered session by sending a SUPL END message using an RLP SSRP tunnel message to the H-SLC.

NOTE: For A-GPS SET Based mode where the SET calculates the position estimate based on GPS assistance data available in the SET, steps H to J are performed whenever new GPS assistance data is required by the SET.

5.2.10.3 Roaming with H-SLP Positioning Successful Case

SUPL Roaming where the H-SLP is involved in the positioning calculation.

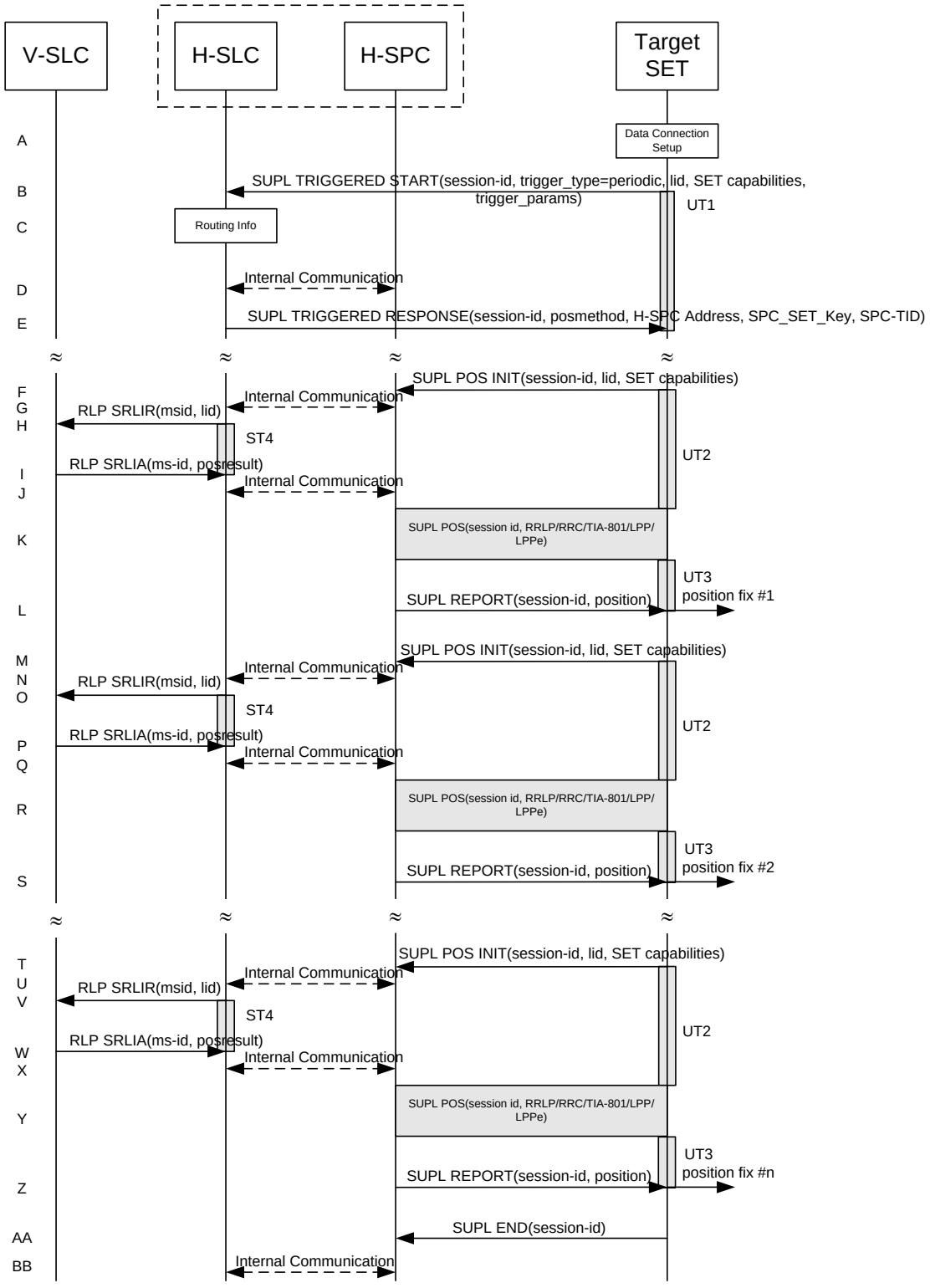

Figure 61: SET Initiated Periodic Trigger Service Roaming with H-SLP Positioning Successful Case – Non-Proxy Mode

NOTE: See Appendix D for timer descriptions.

A. The SUPL Agent on the SET receives a request for a periodic triggered service from an application running on the SET. The SET takes appropriate action establishing or resuming a secure connection.

B. The SUPL Agent on the SET uses the default address provisioned by the Home Network to establish a secure connection to the H-SLC and sends a SUPL TRIGGERED START message to start a positioning session with the H-SLP. The SUPL TRIGGERED START message contains session-id, SET capabilities, trigger type indicator (in this case periodic), Location ID (lid) and periodic trigger parameters. The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe).

C. The H-SLC verifies that the target SET is currently SUPL roaming.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside scope of SUPL 2.0. However, there are various environment dependent mechanisms.

D. Through internal communication the H-SLC requests service for a periodic triggered session from the H-SPC. The H-SLC also creates SPC_SET_Key and SPC-TID to be used for mutual H-SPC/SET authentication and forwards both to the H-SPC through internal communication. The H-SPC grants or denies the request and informs the H-SLC accordingly.

E. Consistent with the SUPL TRIGGERED START message including posmethod(s) supported by the SET, the H-SLC SHALL determine the intended positioning method to be used for the periodic triggered session. If required for the posmethod, the H-SLC SHALL use the supported positioning protocol (e.g., RRLP, RRC, TIA-801 or LPP/LPPe) from the SUPL TRIGGERED START message. The H-SLC sends a SUPL TRIGGERED RESPONSE message to the SET. The SUPL TRIGGERED RESPONSE message contains session-id, posmethod, H-SPC address and SPC_SET_Key and SPC-TID. The SET and the H-SLC MAY release the secure connection.

F. When the periodic trigger in the SET indicates that the first position fix has to be calculated the SET takes appropriate action establishing or resuming a secure connection. The SET then sends a SUPL POS INIT message to start a positioning session with the H-SPC. The SUPL POS INIT message contains at least session-id, SET capabilities and Location ID (lid) parameter. The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe). The SET MAY optionally provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if this is supported. The SET MAY include the first SUPL POS element in the SUPL POS INIT message. The SET MAY set the Requested Assistance Data element in the SUPL POS INIT.
If the SUPL POS INIT message contains a position that meets a required QoP, the H-SPC MAY directly proceed to step L.

G. Through internal communication the H-SPC requests a coarse position estimate from the H-SLC based on the lid received in step F.

H. To obtain a coarse position the H-SLC sends an RLP SRLIR message to the V-SLP.

I. The V-SLC translates the received lid into a position estimate and returns the result to the H-SLC in an RLP SRLIA message.

J. The H-SLC forwards the coarse position to the H-SPC through internal communication.
If the coarse position meets a required QoP, the H-SPC MAY directly proceed to step L and not engage in a SUPL POS session.

K. The SET and the H-SPC exchange several successive positioning procedure messages.
The H-SPC calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance data obtained from the H-SPC (SET-Based).

L. Once the position calculation is complete, the H-SPC sends a SUPL REPORT message to the SET. The SUPL REPORT message includes the position result if the position estimate is calculated in the H-SLP and therefore needs to be sent to the SET. The SET and the H-SPC MAY release the secure connection.

NOTE: steps F to L are optional and not performed for A-GPS SET Based in the case where no GPS assistance data is required from the network. In this case the SET autonomously calculates a position fix based on the currently available GPS assistance data stored in the SET.

Steps M to Z are a repeat of steps F to L.

AA. After the last position result has been calculated, the SET ends the periodic triggered session by sending a SUPL END message to the H-SPC.

BB. Through internal communication the H-SPC informs the H-SLC about the end of the periodic triggered session.

NOTE: For A-GPS SET Based mode where the SET calculates the position estimate based on GPS assistance data available in the SET, steps F to L are performed whenever new GPS assistance data is required by the SET.

5.2.11 SET Initiated Non-Proxy Mode – Triggered Services: Event Triggers

This section describes the call flows for SET Initiated area event triggered services for proxy mode. The trigger thereby resides in the SET and the SET makes the decision if an area event occurred based on continuously repeated position determinations.

5.2.11.1 Non-Roaming Successful Case

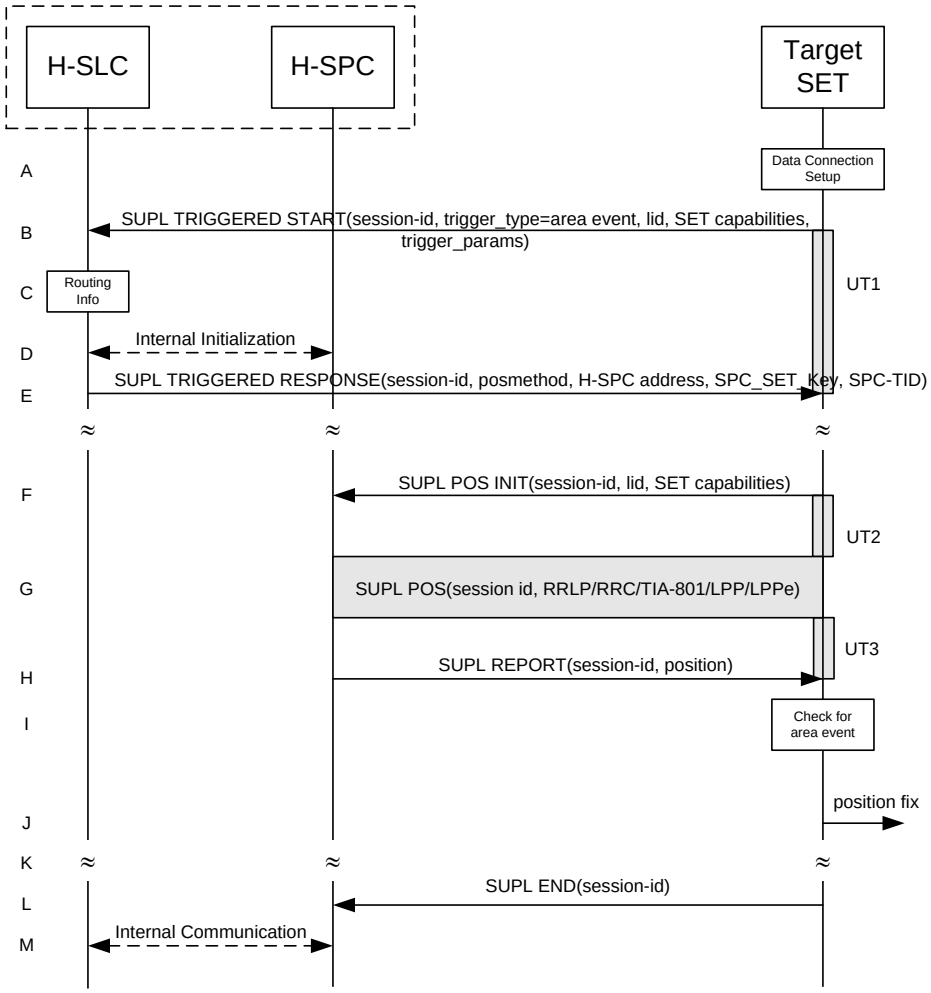

Figure 62: SET Initiated Area Event Trigger Service Non-Roaming Successful Case – Non-Proxy Mode

NOTE: See Appendix D for timer descriptions.

A. The SUPL Agent on the SET receives a request for an area event triggered service from an application running on the SET. The SET takes appropriate action establishing or resuming a secure connection.

B. The SUPL Agent on the SET uses the default address provisioned by the Home Network to establish a secure connection to the H-SLC and sends a SUPL TRIGGERED START message to start a positioning session with the H-SLP. The SUPL TRIGGERED START message contains session-id, SET capabilities, trigger type indicator (in this case area event), Location ID (lid) and area event trigger parameters. The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe).

C. The H-SLC verifies that the target SET is currently not SUPL roaming.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside the scope of SUPL 2.0. However, there are various environment dependent mechanisms.

D. Through internal communication the H-SLC requests service for an area event triggered session from the H-SPC. The H-SLC also generates SPC_SET_Key and SPC-TID to be used for mutual H-SPC/SET authentication and forwards both to the H-SPC. The H-SPC grants or denies the request and informs the H-SLC accordingly.

E. Consistent with the SUPL TRIGGERED START message including the SET capabilities of the SET, the H-SLC SHALL determine the intended positioning method to be used for the area event triggered session and responds. If required for the posmethod, the H-SLC SHALL use the supported positioning protocol (e.g., RRLP, RRC, TIA-801 or LPP/LPPe) from the SUPL TRIGGERED START message. The H-SLC SHALL respond with a SUPL TRIGGERED RESPONSE message to the SET. The SUPL TRIGGERED RESPONSE message contains session-id, posmethod, H-SPC address and SPC_SET_Key and SPC-TID. The SUPL TRIGGERED RESPONSE message may contain the area ids of the specified area for the area event triggered session. The SET and the H-SLP MAY release the secure connection.

F. If the area ids are downloaded in step E, the SET SHALL compare the current area id to the downloaded area ids. When the area event trigger in the SET or the comparison of the current area id to the downloaded area ids indicates that a position fix has to be calculated the SET takes appropriate action establishing or resuming a secure connection. The SET then sends a SUPL POS INIT message to start a positioning session with the H-SPC. The SUPL POS INIT message contains at least session-id, SET capabilities and Location ID (lid) parameter. The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe). The SET MAY optionally provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if this is supported. The SET MAY include the first SUPL POS element in the SUPL POS INIT message. The SET MAY set the Requested Assistance Data element in the SUPL POS INIT.
If a position calculated based on information received in the SUPL POS INIT message is available (e.g. a cell-id based position fix) that meets a required QoP, the H-SPC MAY directly proceed to step H and not engage in a SUPL POS session.

G. The SET and the H-SPC exchange several successive positioning procedure messages.
The H-SPC calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance data obtained from the H-SPC (SET-Based).

H. Once the position calculation is complete the H-SPC sends a SUPL REPORT message to the SET. The SET MAY release the secure connection to the H-SPC.
The SUPL REPORT message includes the position result if the position estimate is calculated in the H-SPC and therefore needs to be sent to the SET.

I. The SET compares the calculated position estimate with the event area to check if the event trigger condition has been met.

J. If the area event was triggered the SET forwards the calculated position estimate to the internal SUPL Agent.

K. If the SET decides to end the triggered session the SET proceeds to step L. Otherwise whenever the area event trigger mechanism in the SET indicates that a new position fix has to be performed, steps F to J are repeated.

L. The SET ends the triggered session by sending a SUPL END message to the H-SPC.

M. The H-SPC informs the H-SLC about the end of the triggered session through internal communication.

The call flow described in Figure 62 is applicable to all positioning methods, however, individual steps within the call flows are optional:

- Step G (SUPL POS) is not performed for cell-id based positioning methods.
- In A-GPS SET Based mode where no GPS assistance data is required from the network, no interaction with the H-SPC is required to calculate a position estimate. Interaction with the H-SPC is only required for GPS assistance data update in which case steps F to H are performed.

5.2.11.2 Roaming with V-SLP Positioning Successful Case

SUPL Roaming where the V-SLP is involved in the positioning calculation.

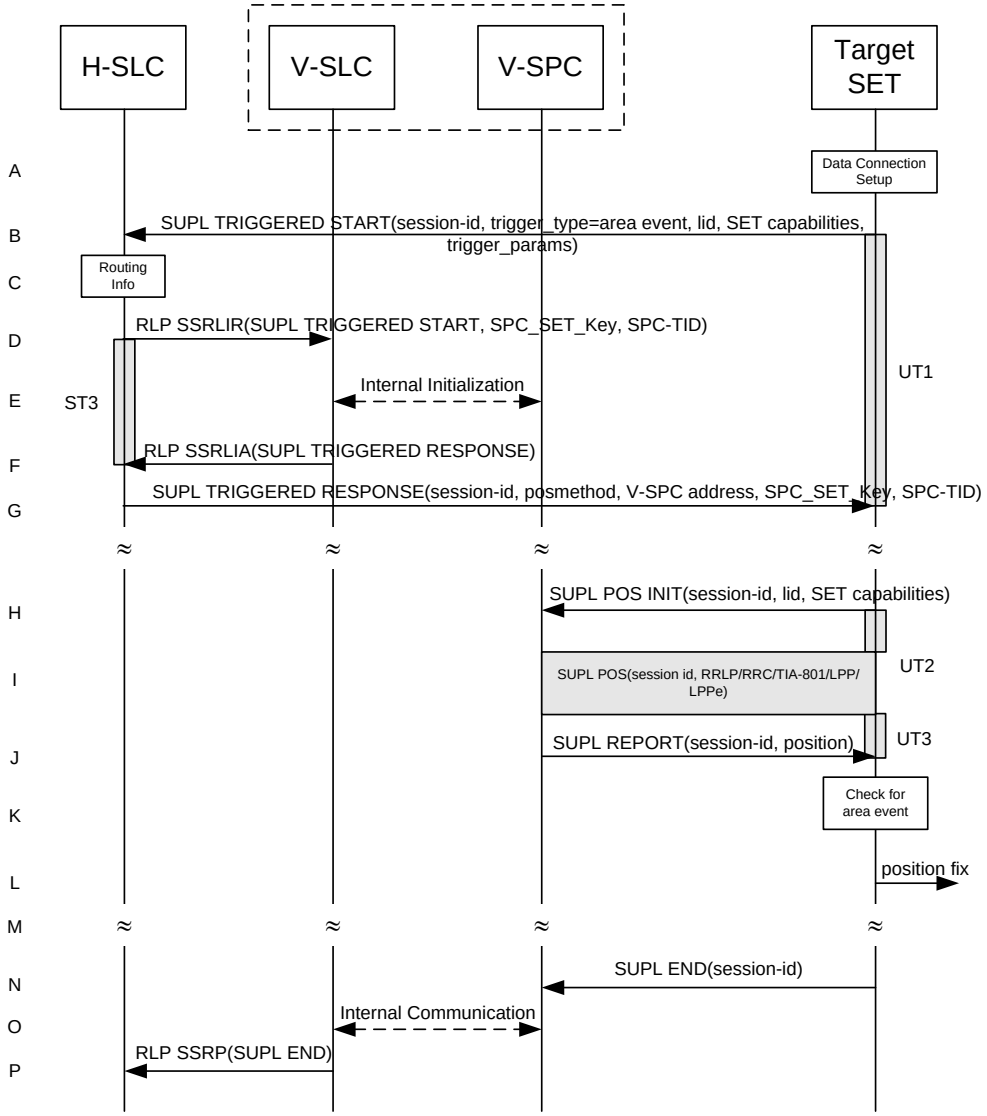

Figure 63: SET Initiated Area Event Trigger Service Roaming with V-SLP Positioning Successful Case – Non-Proxy Mode

NOTE: See Appendix D for timer descriptions.

A. The SUPL Agent on the SET receives a request for an area event triggered service from an application running on the SET. The SET takes appropriate action establishing or resuming a secure connection.

B. The SUPL Agent on the SET uses the default address provisioned by the Home Network to establish a secure connection to the H-SLC and sends a SUPL TRIGGERED START message to start a positioning session with the H-SLP. The SUPL TRIGGERED START message contains session-id, SET capabilities, trigger type indicator (in this case area event), Location ID (lid) and area event trigger parameters. The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe).

C. The H-SLC verifies that the target SET is currently SUPL roaming.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside scope of SUPL 2.0. However, there are various environment dependent mechanisms.

D. The H-SLC decides that the assistance data/position calculation is done by the V-SLP and sends an RLP SSRLIR message tunnelling the SUPL TRIGGERED START message to the V-SLC. The area event trigger parameters such as area information requested by SUPL Agent for the area event triggered session MAY be included in this message by the H-SLP. The H-SLC also generates SPC_SET_Key and SPC-TID to be used for V-SPC/SET mutual authentication and includes both in the RLP SSRLIR message.

E. Through internal communication the V-SLC requests service for an area event triggered session from the V-SPC. The V-SLC also forwards the SPC_SET_Key and SPC-TID to the V-SPC. The V-SPC grants or denies the request and informs the V-SLC accordingly.

F. Consistent with the SUPL TRIGGERED START message including posmethod(s) supported by the SET, the V-SLC SHALL determine the intended positioning method to be used for the area event triggered session. If required for the posmethod, the V-SLC SHALL use the supported positioning protocol (e.g., RRLP, RRC, TIA-801 or LPP/LPPe) from the SUPL TRIGGERED START message. The V-SLC responds with a SUPL TRIGGERED RESPONSE tunnelled over RLP in a SSRLIA message back to the H-SLC that it is capable of supporting this request. The SUPL TRIGGERED RESPONSE contains at least the sessionid, posmethod and the V-SPC address. The V-SLC MAY include area ids corresponding to the area for the area event trigger session in the SUPL TRIGGERED RESPONSE message.

G. The H-SLC sends a SUPL TRIGGERED RESPONSE message to the SET. The SUPL TRIGGERED RESPONSE message contains session-id, posmethod, V-SPC address and SPC_SET_Key and SPC-TID. The SUPL TRIGGERED RESPONSE message may contain the area ids of the specified area for the area event triggered session. The SET and the H-SLC MAY release the secure connection.

H. If the area ids are downloaded in step G, the SET SHALL compare the current area id to the downloaded area ids. When the area event trigger in the SET the comparison of the current area id to the downloaded area ids indicates that a position fix has to be calculated the SET takes appropriate action establishing or resuming a secure connection. The SET then sends a SUPL POS INIT message to start a positioning session with the V-SPC. The SUPL POS INIT message contains at least session-id, SET capabilities and Location ID (lid) parameter. The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe). The SET MAY optionally provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if this is supported. The SET MAY include the first SUPL POS element in the SUPL POS INIT message. The SET MAY set the Requested Assistance Data element in the SUPL POS INIT.
If a position calculated based on information received in the SUPL POS INIT message is available (e.g. a cell-id based position fix) that meets a required QoP, the V-SPC MAY directly proceed to step J and not engage in a SUPL POS session.

I. The SET and the V-SPC exchange several successive positioning procedure messages.
The V-SPC calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance data obtained from the V-SPC (SET-Based).

J. Once the position calculation is complete, the V-SPC sends a SUPL REPORT message to the SET. The SET and the H-SPC MAY release the secure connection.
The SUPL REPORT message includes the position result if the position estimate is calculated in the V-SPC and therefore needs to be sent to the SET.

K. The SET compares the calculated position estimate with the event area to check if the event trigger condition has been met.

L. If the area event was triggered the SET forwards the calculated position estimate to the internal SUPL Agent.

M. If the SET decides to end the triggered session the SET proceeds to step N. Otherwise whenever the area event trigger mechanism in the SET indicates that a new position fix has to be performed, steps H to L are repeated.

N. The SET ends the triggered session by sending a SUPL END message to the V-SPC.

O. The V-SPC informs the V-SLC about the end of the triggered session through internal communication.

P. The V-SLC informs the H-SLC about the end of the triggered session by sending a SUPL END message using an RLP SSRP tunnel message to the H-SLC.

The call flow described in Figure 63 is applicable to all positioning methods, however, individual steps within the call flows are optional:

- Step I (SUPL POS) is not performed for cell-id based positioning methods.
- In A-GPS SET Based mode where no GPS assistance data is required from the network, no interaction with the H-SLP is required to calculate a position estimate. Interaction with the V-SPC is only required for GPS assistance data update in which case steps H to J are performed.

5.2.11.3 Roaming with H-SLP Positioning Successful Case

SUPL Roaming where the H-SLP is involved in the positioning calculation.

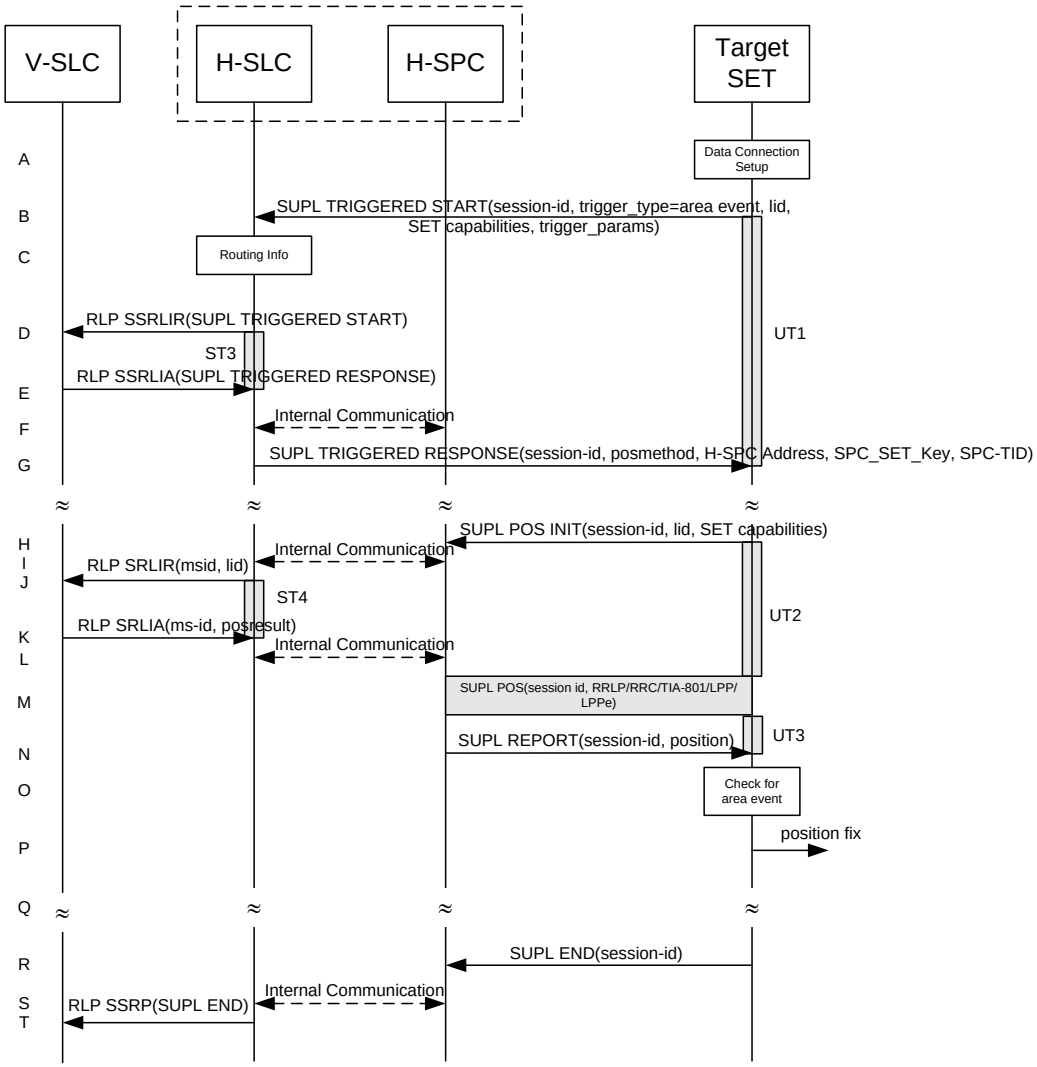

Figure 64: SET Initiated Area Event Trigger Service Roaming with H-SLP Positioning Successful Case – Non-Proxy Mode

NOTE: See Appendix D for timer descriptions.

A. The SUPL Agent on the SET receives a request for an area event triggered service from an application running on the SET. The SET takes appropriate action establishing or resuming a secure connection.

B. The SUPL Agent on the SET uses the default address provisioned by the Home Network to establish a secure connection to the H-SLC and sends a SUPL TRIGGERED START message to start a positioning session with the H-SLP. The SUPL TRIGGERED START message contains session-id, SET capabilities, trigger type indicator (in this case area event), Location ID (lid) and area event trigger parameters. The SET capabilities include the supported

positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe).

C. The H-SLC verifies that the target SET is currently SUPL roaming.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside scope of SUPL 2.0. However, there are various environment dependent mechanisms.

D. Based on the received lid or other mechanisms, the H-SLC determines the V-SLP and sends an RLP SSRLIR including a SUPL TRIGGERED START message to the V-SLC to inform the V-SLP that an area event triggered session is in the progress of being initiated with the H-SLP. The area event trigger parameters such as area information requested by SUPL Agent for the area event triggered session MAY be included in this message by the H-SLP..

E. The V-SLC acknowledges the RLP request received in step E with a SUPL TRIGGERED RESPONSE message which is carried inside an RLP SSRLIA message. The V-SLC MAY include area ids corresponding to the area for the area event trigger session in the SUPL TRIGGERED RESPONSE message.

F. Though internal communication the H-SLC requests service for an area event triggered session from the H-SPC. The H-SLC also creates SPC_SET_Key and SPC_TID to be used for mutual H-SPC/SET authentication and forwards both to the H-SPC through internal communication. The H-SPC grants or denies the request and informs the H-SLC accordingly.

G. Consistent with the SUPL TRIGGERED START message including posmethod(s) supported by the SET, the H-SLC SHALL determine the intended positioning method to be used for the area event triggered session. If required for the posmethod, the H-SLC SHALL use the supported positioning protocol (e.g., RRLP, RRC, TIA-801 or LPP/LPPe) from the SUPL TRIGGERED START message. The H-SLC sends a SUPL TRIGGERED RESPONSE message to the SET. The SUPL TRIGGERED RESPONSE message contains session-id, posmethod, H-SPC address and SPC_SET_Key and SPC_TID. The SUPL TRIGGERED RESPONSE message may contain the area ids of the specified area for the area event triggered session. The SET and the H-SLC MAY release the secure connection.

H. If the area ids are downloaded in step G, the SET SHALL compare the current area id to the downloaded area ids. When the area event trigger in the SET or the comparison of the current area id to the downloaded area ids indicates that a position fix has to be calculated the SET takes appropriate action establishing or resuming a secure connection. The SET then sends a SUPL POS INIT message to start a positioning session with the H-SPC. The SUPL POS INIT message contains at least session-id, SET capabilities and Location ID (lid) parameter. The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe). The SET MAY optionally provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if this is supported. The SET MAY include the first SUPL POS element in the SUPL POS INIT message. The SET MAY set the Requested Assistance Data element in the SUPL POS INIT.
If a position is received in the SUPL POS INIT message that meets a required QoP, the H-SPC MAY directly proceed to step N and not engage in a SUPL POS session.

I. Through internal communication the H-SPC requests a coarse position estimate from the H-SLC based on the lid received in step H.

J. To obtain a coarse position the H-SLC sends an RLP SRLIR message to the V-SLP.

K. The V-SLC translates the received lid into a position estimate and returns the result to the H-SLC in an RLP SRLIA message.

L. The H-SLC forwards the coarse position to the H-SPC through internal communication.
If the coarse position meets a required QoP, the H-SPC MAY directly proceed to step N and not engage in a SUPL POS session.

M. The SET and the H-SPC exchange several successive positioning procedure messages.
The H-SPC calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance data obtained from the H-SPC (SET-Based).

N. Once the position calculation is complete, the H-SPC sends a SUPL REPORT message to the SET. The SET and the H-SPC MAY release the secure connection.

The SUPL REPORT message includes the position result if the position estimate is calculated in the V-SPC and therefore needs to be sent to the SET.

O. The SET compares the calculated position with the event area to check if the event trigger condition has been met.

P. If the area event was triggered the SET forwards the calculated position estimate to the internal SUPL Agent.

Q. If the SET decides to end the triggered session the SET proceeds to step R. Otherwise whenever the area event trigger mechanism in the SET indicates that a new position fix has to be performed, steps H to P are repeated.

R. The SET ends the triggered session by sending a SUPL END message to the H-SPC.

S. The H-SPC informs the H-SLC about the end of the triggered session through internal communication.

T. The H-SLC informs the V-SLC about the end of the triggered session by sending a SUPL END message using an RLP SSRP tunnel message to the V-SLC.

The call flow described in Figure 64 is applicable to all positioning methods, however, individual steps within the call flows are optional:

- Step M (SUPL POS) is not performed for cell-id based positioning methods.
- In A-GPS SET Based mode where no GPS assistance data is required from the network, no interaction with the H-SLP is required to calculate a position estimate. Interaction with the H-SPC is only required for GPS assistance data update in which case steps H to N are performed.

5.2.12 V-SLP to V-SLP Handover – SET initiated Proxy mode

See section 5.1.11.1.

5.2.13 V-SPC to V-SPC Handover – SET initiated Non-Proxy mode

See section 5.1.11.2.

5.2.14 SET-Initiated Periodic Location Request with Transfer to Third Party

This section describes the call flows for SET Initiated Periodic Location Requests with transfer of the position results to a 3rd party.

5.2.14.1 Non-Roaming Successful Case – Proxy Mode

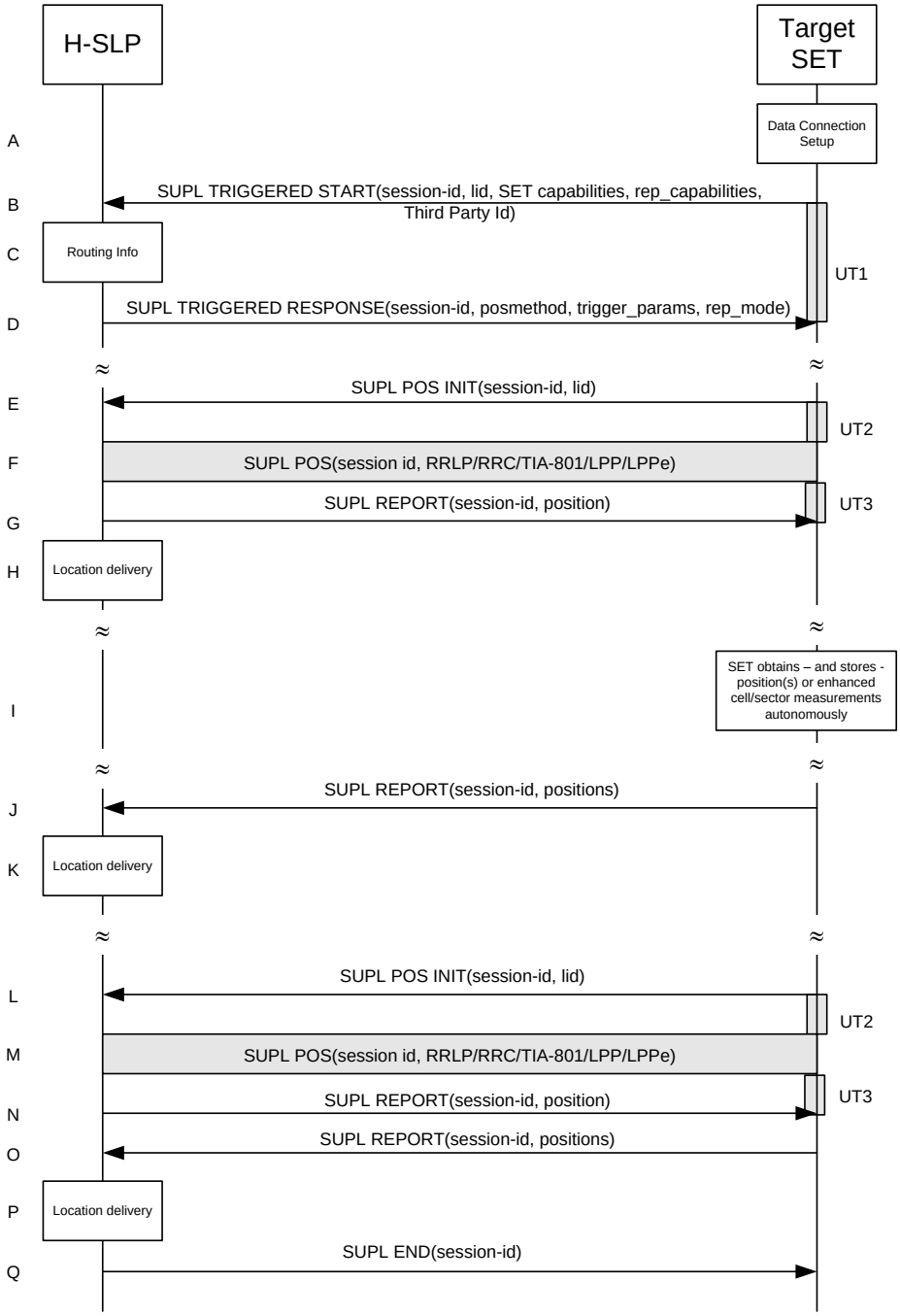

Figure 65: SET Initiated Periodic Location Request with transfer of the position result to 3rd party – non-roaming – proxy mode

NOTE: See Appendix D for timer descriptions.

A. The SUPL Agent on the SET receives a request for a periodic triggered service with transfer to a 3rd party from an application running on the SET. The SET takes appropriate action establishing or resuming a secure connection.

B. The SUPL Agent on the SET uses the default address provisioned by the Home Network to establish a secure connection to the H-SLP and sends a SUPL TRIGGERED START message to start a positioning session with the H-SLP. The SUPL TRIGGERED START message contains session-id, SET capabilities, trigger type indicator (in this case periodic), Location ID (lid), periodic trigger parameters and Third Party ID. The SET capabilities include

the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe).

C. The H-SLP verifies that the target SET is currently not SUPL roaming.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside the scope of SUPL. However, there are various environment dependent mechanisms.

D. Consistent with the SUPL TRIGGERED START message including the SET capabilities of the SET, the H-SLP SHALL determine the intended positioning method to be used for the periodic triggered session. If required for the posmethod, the H-SLP SHALL use the supported positioning protocol (e.g., RRLP, RRC, TIA-801 or LPP/LPPe) from the SUPL TRIGGERED START message. The H-SLP SHALL respond with a SUPL TRIGGERED RESPONSE message to the SET. The SUPL TRIGGERED RESPONSE contains the session-id but no H-SLP address, to indicate to the SET that a new connection SHALL NOT be established. The SUPL TRIGGERED RESPONSE also contains the posmethod. The SET and the H-SLP MAY release the secure connection.

E. When the periodic trigger in the SET indicates that the first position fix has to be performed, the SET takes appropriate action establishing or resuming a secure connection. The SET then sends a SUPL POS INIT message to start a positioning session with the H-SLP. The SUPL POS INIT message contains at least session-id, the Location ID (lid) parameter. The SET MAY provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if this is supported. The SET MAY set the Requested Assistance Data element in the SUPL POS INIT.
If a position calculated based on information received in the SUPL POS INIT message is available (e.g. a cell-id based position fix) that meets a required QoP, the H-SLP SHALL directly proceed to step G and not engage in a SUPL POS session.

F. The SET and the H-SLP MAY exchange several successive positioning procedure messages.
The H-SLP calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance obtained from the H-SLP (SET-Based).

G. Once the position calculation is complete the H-SLP sends the SUPL REPORT message to the SET informing it that the positioning procedure is completed. The SET MAY release the secure connection to the H-SLP. If the reporting mode is batch reporting, the SET stores all calculated position estimates. In SET Assisted mode the position is calculated by the H-SLP and therefore needs to be included in the message for batch reporting mode.

If a SET Based positioning method was chosen which allows the SET to autonomously calculate a position estimate (e.g. autonomous GPS or A-GPS SET Based mode where the SET has current GPS assistance data and does not require an assistance data update from the H-SLP) steps E to G are not performed. Instead, the SET autonomously calculates the position estimate and – for real time or quasi-real time reporting – sends the calculated position estimate to the H-SLP using a SUPL REPORT message containing the session-id and the position estimate.

H. The H-SLP delivers the position result to the 3rd party.

I. This step is optional: If the SET cannot communicate with the H-SLP (e.g. no radio coverage available) and if batch reporting or quasi-real time reporting is used, the SET MAY – if supported – perform SET Based position fixes (autonomous GPS or SET Based A-GPS where the SET has current assistance data) and/or, if allowed by the H-SLP, enhanced cell/sector measurements. In the case, of batch reporting, and if explicitly allowed by the H-SLP, enhanced cell/sector measurements are permitted even when the SET can communicate with the H-SLP.

J. This step is optional and is executed if batch reporting is used and if any of the conditions for sending batch reports have occurred. It is also executed, once the SET is able to re-establish communication with the H-SLP, if quasi-real time reporting is used if one or more previous reports have been missed. The SET sends the stored position estimates and/or, if allowed, the stored enhanced cell/sector measurements in an unsolicited SUPL REPORT message to the H-SLP. The SUPL REPORT message contains the session-id and the position result(s) including date and time information for each position result and optionally the position method used. In the case of batch reporting, the stored position estimates and/or enhanced cell/sector measurements included in the SUPL REPORT message may be chosen according to criteria received in step D. If no criteria are received in step D, the SET shall include all stored position estimates and/or enhanced cell/sector measurements not previously reported.

K. If enhanced cell/sector measurements are received in step J, the H-SLP calculates the corresponding position estimates.

The H-SLP forwards the reported and/or calculated position estimate(s) to the 3rd party.
When the last position estimate needs to be calculated i.e. the end of the periodic triggered session has been reached, steps L to N may be performed (a repeat of steps E to G). Alternatively – and if applicable – step I is repeated.

O. This step is optional and is executed after the last position estimate or, if allowed, last set of enhanced cell/sector measurements has been obtained or was due, and at any time up until step Q, if and as soon as all the following conditions apply:
    i. Batch reporting or quasi-real time reporting is used.
    ii. The SET has stored historic location reports and/or stored historic enhanced cell/sector measurements that have not yet been sent to the H-SLP.
    iii. The SET is able to establish communication with the H-SLP
    iv. In the case of batch reporting, the conditions for sending have arisen (e.g. the conditions define sending after the last position estimate is obtained).

   The SUPL REPORT message is used to send all or a subset of stored position fixes and/or stored enhanced cell/sector measurements not previously reported to the H-SLP. In the case of batch reporting, the stored position estimates and/or stored enhanced cell/sector measurements included in the SUPL REPORT message may be chosen according to criteria received in step D. If no criteria are received in step D, the SET shall include all stored position estimates and/or stored enhanced cell/sector measurements not previously reported.

P. If enhanced cell/sector measurements are received in step O, the H-SLP calculates corresponding position estimates. The H-SLP transfers the reported and/or calculated historical position estimate(s) to the 3rd party.

Q. After the last position result has been transferred to the 3rd party in step P or following some timeout on not receiving stored position estimates in step O, the H-SLP ends the periodic triggered session by sending a SUPL END message to the SET.

5.2.14.2 Roaming with V-SLP Positioning Successful Case – Proxy Mode

SUPL Roaming where the V-SLP is involved in the positioning calculation.

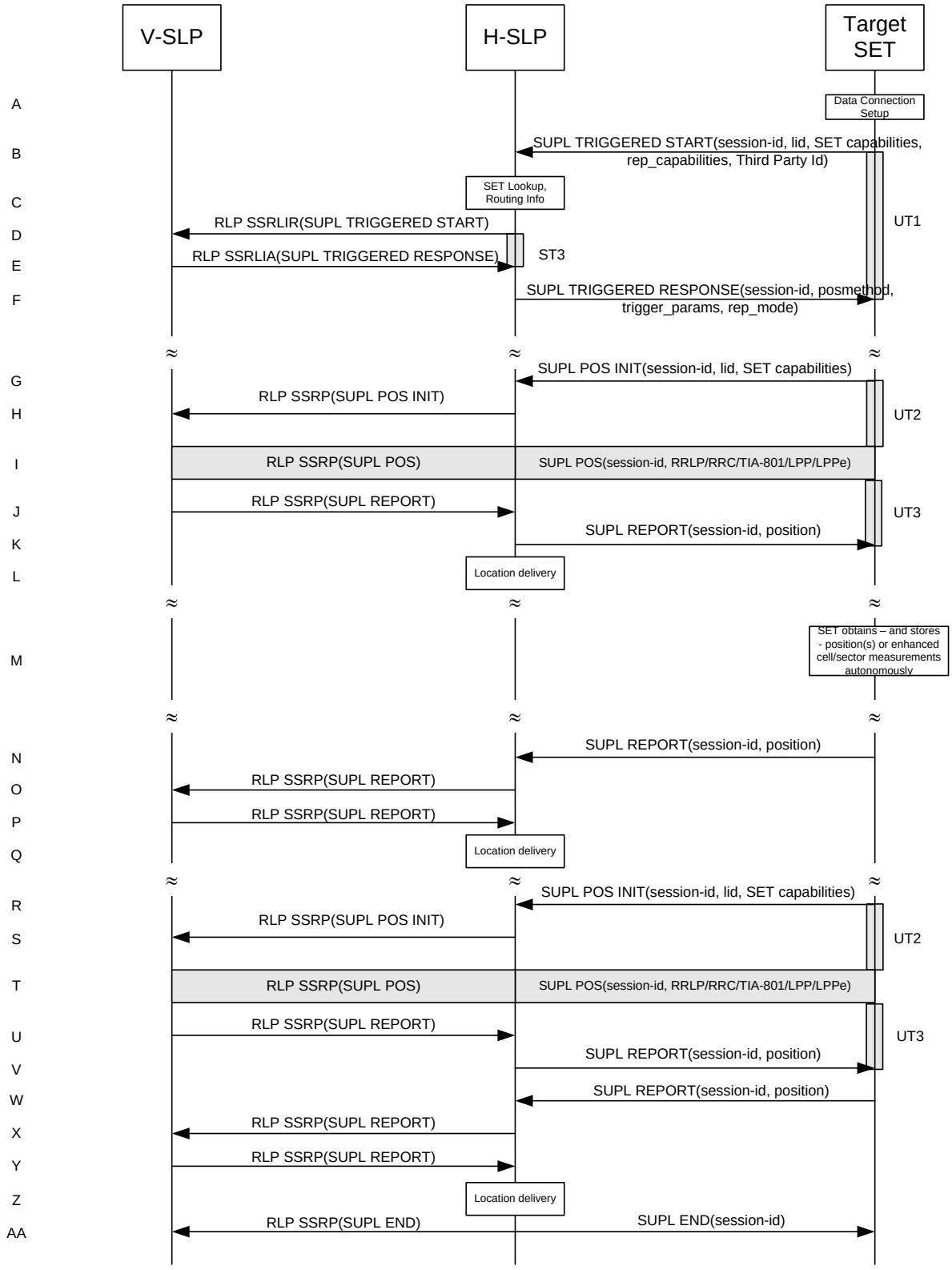

Figure 66: SET Initiated Periodic Location Request with transfer of the position result to 3rd party – roaming with V-SLP Positioning – proxy mode

NOTE: See Appendix D for timer descriptions.

A. The SUPL Agent on the SET receives a request for a periodic triggered service with transfer to a 3rd party from an application running on the SET. The SET takes appropriate action establishing or resuming a secure connection.

B. The SUPL Agent on the SET uses the default address provisioned by the Home Network to establish a secure connection to the H-SLP and sends a SUPL TRIGGERED START message to start a positioning session with the H-SLP. The SUPL TRIGGERED START message contains session-id, SET capabilities, trigger type indicator (in this case periodic), Location ID (lid), periodic trigger parameters and Third Party ID. The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe).

C. The H-SLP verifies that the target SET is currently SUPL roaming.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside scope of SUPL 2.0. However, there are various environment dependent mechanisms.

D. The H-SLP decides that the assistance data/position calculation is done by the V-SLP and sends an RLP SSRLIR tunnelling the SUPL TRIGGERED START message to the V-SLP.

E. Consistent with the SUPL TRIGGERED START message including posmethod(s) supported by the SET, the V-SLP SHALL determine the intended positioning method to be used for the periodic triggered session. If required for the posmethod, the V-SLP SHALL use the supported positioning protocol (e.g., RRLP, RRC, TIA-801 or LPP/LPPe) from the SUPL TRIGGERED START message. The V-SLP responds with a SUPL TRIGGERED RESPONSE tunnelled over RLP in a SSRLIA message back to the H-SLP that it is capable of supporting this request. The SUPL TRIGGERED RESPONSE contains at least the sessionid and posmethod.

F. The H-SLP forwards the SUPL TRIGGERED RESPONSE message to the SET. The SUPL TRIGGERED RESPONSE contains the session-id but no H-SLP address, to indicate to the SET that a new connection SHALL NOT be established. The SUPL TRIGGERED RESPONSE also contains the posmethod. The SET and the H-SLP MAY release the secure connection.

G. When the periodic trigger in the SET indicates that the first position fix has to be performed, the SET takes appropriate action establishing or resuming a secure connection. The SET then sends a SUPL POS INIT message to the H-SLP to start a positioning session with the V-SLP. The SUPL POS INIT message contains at least session-id, the Location ID (lid) and the SET capabilities parameter. The SET MAY provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if this is supported. The SET MAY set the Requested Assistance Data element in the SUPL POS INIT.
If the SUPL POS INIT message contains a position that meets a required QoP, the H-SLP SHALL directly proceed to step K.

H. The H-SLP forwards the SUPL POS INIT message to the V-SLP using a RLP SSRP message.
If a position calculated based on information received in the SUPL POS INIT message is available (e.g. a cell-id based position fix) that meets a required QoP, the V-SLP SHALL directly proceed to step J and not engage in a SUPL POS session.

I. The SET and the V-SLP MAY exchange several successive positioning procedure messages, tunnelled over RLP via the H-SLP.
The V-SLP calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance obtained from the V-SLP (SET-Based).

J. Once the position calculation is complete, the V-SLP sends a SUPL REPORT message to the H-SLP in an RLP tunnel using an SSRP message.

K. Once the position calculation is complete the H-SLP sends the SUPL REPORT message to the SET informing it that the positioning procedure is completed. The SET MAY release the secure connection to the H-SLP. If the reporting mode is batch reporting, the SET stores all calculated position estimates. In SET Assisted mode the position is calculated by the H-SLP and therefore needs to be included in the message for batch reporting mode.

If a SET Based positioning method was chosen which allows the SET to autonomously calculate a position estimate (e.g. autonomous GPS or A-GPS SET Based mode where the SET has current GPS assistance data and does not require an assistance data update from the H-SLP) steps G to K are not performed. Instead, the SET autonomously calculates the position estimate and – for real time or quasi-real time reporting – sends the calculated position estimate to the H-SLP using a SUPL REPORT message containing the session-id and the position estimate.

L. This step is optional: once the position calculation is complete and if real time or quasi-real time reporting is used, the H-SLP transfers the received position estimate from the V-SLP to the 3rd party. If the reporting mode is set to batch reporting, this message is not used.

M. This step is optional: if the SET cannot communicate with the H-SLP (e.g. no radio coverage available) and if batch reporting or quasi-real time reporting is used, the SET MAY – if supported – perform SET Based position fixes (autonomous GPS or SET Based A-GPS where the SET has current assistance data) and/or, if allowed by the H-SLP, enhanced cell/sector measurements. In the case of batch reporting, and if explicitly allowed by the H-SLP, enhanced cell/sector measurements are permitted even when the SET can communicate with the H-SLP.

N. This step is optional and is executed if batch reporting is used and if any of the conditions for sending batch reports have occurred. It is also executed, once the SET is able to re-establish communication with the H-SLP, if quasi-real time reporting is used if one or more previous reports have been missed. The SET sends the stored position estimates and/or, if allowed, the stored enhanced cell/sector measurements in an unsolicited SUPL REPORT message to the H-SLP. The SUPL REPORT message contains the session-id and the position result(s) including data and time information for each position result and optionally the position method used. In the case of batch reporting, the stored position estimates and/or enhanced cell/sector measurements included in the SUPL REPORT message may be chosen according to criteria received in step F. If no criteria are received in step F, the SET shall include all stored position estimates and/or enhanced cell/sector measurements not previously reported.

O. This step is optional: if in step N the SET sent enhanced cell/sector measurements, the H-SLP needs to engage the help of the V-SLP to translate the enhanced cell/sector measurements into actual position estimates. To this end the H-SLP sends the received enhanced cell/sector measurements in a SUPL REPORT message to the V-SLP using an SSRP message over RLP tunnel.

P. This step is optional and only takes place if step O has occurred: after receiving the enhanced cell/sector measurements the V-SLP calculates the actual position estimates and returns them in a SUPL REPORT message to the H-SLP using an SSRP message over RLP tunnel.

Q. The H-SLP transfers the reported and/or calculated position estimate(s) to the 3rd party.

When the last position estimate needs to be calculated i.e. the end of the periodic triggered session has been reached, steps R to V may be performed (a repeat of steps G to K). Alternatively – and if applicable – step M is repeated.

W. This step is optional and is executed after the last position estimate or, if allowed, last set of enhanced cell/sector measurements has been obtained or was due, and at any time up until step AA, if and as soon as all of the following conditions apply:

   i. Batch reporting or quasi-real time reporting is used.

   ii. The SET has stored historic location reports and/or stored historic enhanced cell/sector measurements that have not yet been sent to the H-SLP.

   iii. The SET is able to establish communication with the H-SLP.

   iv. In the case of batch reporting, the conditions for sending have arisen (e.g. the conditions define sending after the last position estimate is obtained).

The SUPL REPORT message is used to send all or a subset of stored position fixes and/or stored enhanced cell/sector measurements not previously reported to the H-SLP. In the case of batch reporting, the stored position estimates and/or stored enhanced cell/sector measurements included in the SUPL REPORT message may be chosen according to criteria received in step F. If no criteria are received in step F, the SET shall include all stored position estimates and/or stored enhanced cell/sector measurements not previously reported.

X. This step is optional: if in step W the SET sent enhanced cell/sector measurements, the H-SLP needs to engage the help of the V-SLP to translate the enhanced cell/sector measurements into actual position estimates. To this end the H-SLP sends the received enhanced cell/sector measurements in a SUPL REPORT message to the V-SLP using an SSRP message over RLP tunnel.

Y. This step is optional and only takes place if step X has occurred: after receiving the enhanced cell/sector measurements the V-SLP calculates the actual position estimates and returns them in a SUPL REPORT message to the H-SLP using an SSRP message over RLP tunnel.

Z. The H-SLP transfers the reported and/or calculated historical position estimate(s) to the 3rd party.

AA. After the last position result has been transferred to the 3rd party in step Z, or following some timeout on not receiving stored position estimates in step W, the H-SLP ends the periodic triggered session by sending a SUPL END message to the SET and informs the V-SLP about the end of the periodic triggered session by sending a SUPL END message using an RLP SSRP tunnel message to the V-SLP.

5.2.14.3 Roaming with H-SLP Positioning Successful Case – Proxy Mode

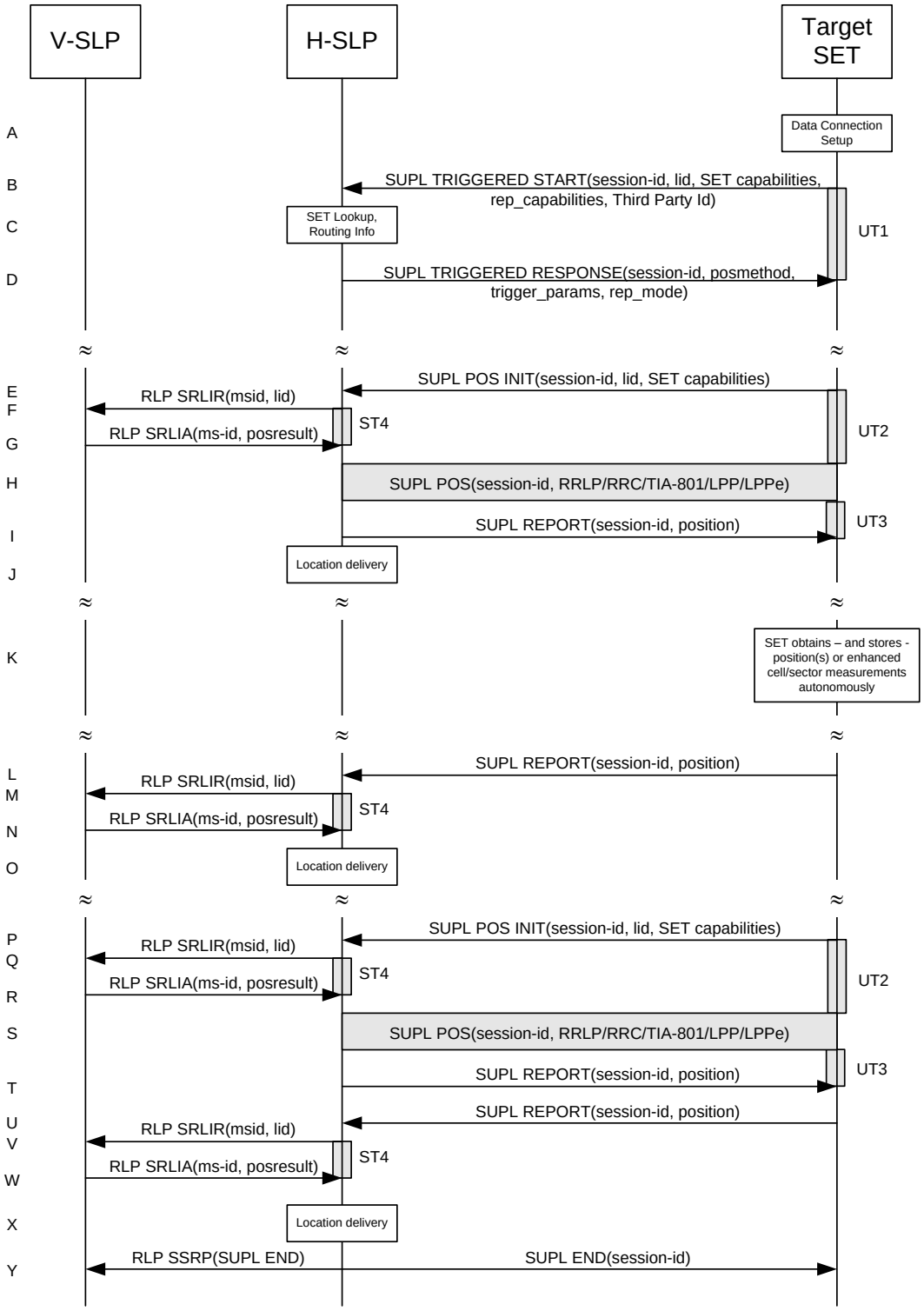

Figure 67: SET Initiated Periodic Location Request with transfer of the position result to 3rd party – roaming with H-SLP Positioning – proxy mode

NOTE: See Appendix D for timer descriptions.

A. The SUPL Agent on the SET receives a request for a periodic triggered service with transfer to a 3rd party from an application running on the SET. The SET takes appropriate action establishing or resuming a secure connection.

B. The SUPL Agent on the SET uses the default address provisioned by the Home Network to establish a secure connection to the H-SLP and sends a SUPL TRIGGERED START message to start a positioning session with the H-SLP. The SUPL TRIGGERED START message contains session-id, SET capabilities, trigger type indicator (in this case periodic), Location ID (lid), periodic trigger parameters and Third Party ID. The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe).

C. The H-SLP verifies that the target SET is currently SUPL roaming.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside scope of SUPL 2.0. However, there are various environment dependent mechanisms.

D. Consistent with the SUPL TRIGGERED START message including posmethod(s) supported by the SET, the H-SLP SHALL determine the intended positioning method to be used for the periodic triggered session. If required for the posmethod, the H-SLP SHALL use the supported positioning protocol (e.g., RRLP, RRC, TIA-801 or LPP/LPPe) from the SUPL TRIGGERED START message. The H-SLP sends a SUPL TRIGGERED RESPONSE message to the SET. The SUPL TRIGGERED RESPONSE contains the session-id but no H-SLP address, to indicate to the SET that a new connection SHALL NOT be established. The SUPL TRIGGERED RESPONSE also contains the posmethod. The SET and the H-SLP MAY release the secure connection.

E. When the periodic trigger in the SET indicates that the first position fix has to be performed, the SET takes appropriate action establishing or resuming a secure connection. The SET then sends a SUPL POS INIT message to the H-SLP to start a positioning session with the H-SLP. The SUPL POS INIT message contains at least session-id, the Location ID (lid) and the SET capabilities parameter. The SET MAY provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if this is supported. The SET MAY set the Requested Assistance Data element in the SUPL POS INIT.
If the SUPL POS INIT message contains a position that meets a required QoP, the H-SLP SHALL directly proceed to step I and not engage in a SUPL POS session

F. To obtain a coarse position based on lid received in step E, the H-SLP sends an RLP SRLIR message to the V-SLP.

G. The V-SLP translates the received lid into a position estimate and returns the result to the H-SLP in an RLP SRLIA message.
If the received position estimate meets a required QoP, the H-SLP SHALL directly proceed to step I and not engage in a SUPL POS session.

H. The SET and the H-SLP MAY exchange several successive positioning procedure messages.
The H-SLP calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance obtained from the H-SLP (SET-Based).

I. Once the position calculation is complete the H-SLP sends the SUPL REPORT message to the SET informing it that the positioning procedure is completed. The SET MAY release the secure connection to the H-SLP. If the reporting mode is batch reporting, the SET stores all calculated position estimates. In SET Assisted mode the position is calculated by the H-SLP and therefore needs to be included in the message for batch reporting mode.

If a SET Based positioning method was chosen which allows the SET to autonomously calculate a position estimate (e.g. autonomous GPS or A-GPS SET Based mode where the SET has current GPS assistance data and does not require an assistance data update from the H-SLP) steps E to I are not performed. Instead, the SET autonomously calculates the position estimate and – for real time or quasi-real time reporting – sends the calculated position estimate to the H-SLP using a SUPL REPORT message containing the session-id and the position estimate.

J. This step is optional: once the position calculation is complete and if real time or quasi-real time reporting is used, the H-SLP transfers the position result to the 3rd party. If the reporting mode is set to batch reporting, no transfer occurs.

K. This step is optional: if the SET cannot communicate with the H-SLP (e.g. no radio coverage available) and if batch reporting or quasi-real time reporting is used, the SET MAY – if supported – perform SET Based position fixes (autonomous GPS or SET Based A-GPS where the SET has current assistance data) and/or, if allowed by the H-SLP, enhanced cell/sector measurements. In the case of batch reporting, and if explicitly allowed by the H-SLP, enhanced cell/sector measurements are permitted even when the SET can communicate with the H-SLP.

L. This step is optional and is executed if batch reporting is used and if any of the conditions for sending batch reports have occurred. It is also executed, once the SET is able to re-establish communication with the H-SLP, if quasi-real time reporting is used if one or more previous reports have been missed. The SET sends the stored position estimates and/or, if allowed, the stored enhanced cell/sector measurements in an unsolicited SUPL REPORT message to the H-SLP. The SUPL REPORT message contains the session-id and the position result(s) including data and time information for each position result and optionally the position method used. In the case of batch reporting, the stored position estimates and/or enhanced cell/sector measurements included in the SUPL REPORT message may be chosen according to criteria received in step D. If no criteria are received in step D, the SET shall include all stored position estimates and/or enhanced cell/sector measurements not previously reported.

M. This step is optional: if in step L the SET sent enhanced cell/sector measurements, the H-SLP needs to engage the help of the V-SLP to translate the enhanced cell/sector measurements into actual position estimates. To this end the H-SLP sends an RLP SRLIR message to the V-SLP.

N. This step is optional and only takes place if step M has occurred: The V-SLP translates the received enhanced cell/sector measurements into position estimates and returns the results to the H-SLP in an RLP SRLIA message.

O. The H-SLP transfers the reported and/or calculated position estimate(s) to the 3rd party.

When the last position estimate needs to be calculated i.e. the end of the periodic triggered session has been reached, steps P to T may be performed (a repeat of steps E to I). Alternatively – and if applicable – step K is repeated

U. This step is optional and is executed after the last position estimate or, if allowed, last set of enhanced cell/sector measurements has been obtained or was due, and at any time up until step Y, if and as soon as all of the following conditions apply:

   i. Batch reporting or quasi-real time reporting is used.

   ii. The SET has stored historic location reports and/or stored historic enhanced cell/sector measurements that have not yet been sent to the H-SLP.

   iii. The SET is able to establish communication with the H-SLP.

   iv. In the case of batch reporting, the conditions for sending have arisen (e.g. the conditions define sending after the last position estimate is obtained).

The SUPL REPORT message is used to send all or a subset of stored position fixes and/or stored enhanced cell/sector measurements not previously reported to the H-SLP. In the case of batch reporting, the stored position estimates and/or stored enhanced cell/sector measurements included in the SUPL REPORT message may be chosen according to criteria received in step D. If no criteria are received in step D, the SET shall include all stored position estimates and/or stored enhanced cell/sector measurements not previously reported.

V. This step is optional: if in step U the SET sent enhanced cell/sector measurements, the H-SLP needs to engage the help of the V-SLP to translate the enhanced cell/sector measurements into actual position estimates. To this end the H-SLP sends an RLP SRLIR message to the V-SLP.

W. This step is optional and only takes place if step V has occurred: after receiving the enhanced cell/sector measurements the V-SLP translates the received enhanced cell/sector measurements into position estimates and returns the results to the H-SLP in an RLP SRLIA message.

X. The H-SLP transfers the reported and/or calculated historical position estimate(s) to the 3rd party.

Y. After the last position result has been reported to the SUPL Agent in step X or following some timeout on not receiving stored position estimates in step U, the H-SLP ends the periodic triggered session by sending a SUPL END message to the SET and informs the V-SLP about the end of the periodic triggered session by sending a SUPL END message using an RLP SSRP tunnel message to the V-SLP.

5.2.14.4 Non-Roaming Successful Case – Non-Proxy Mode

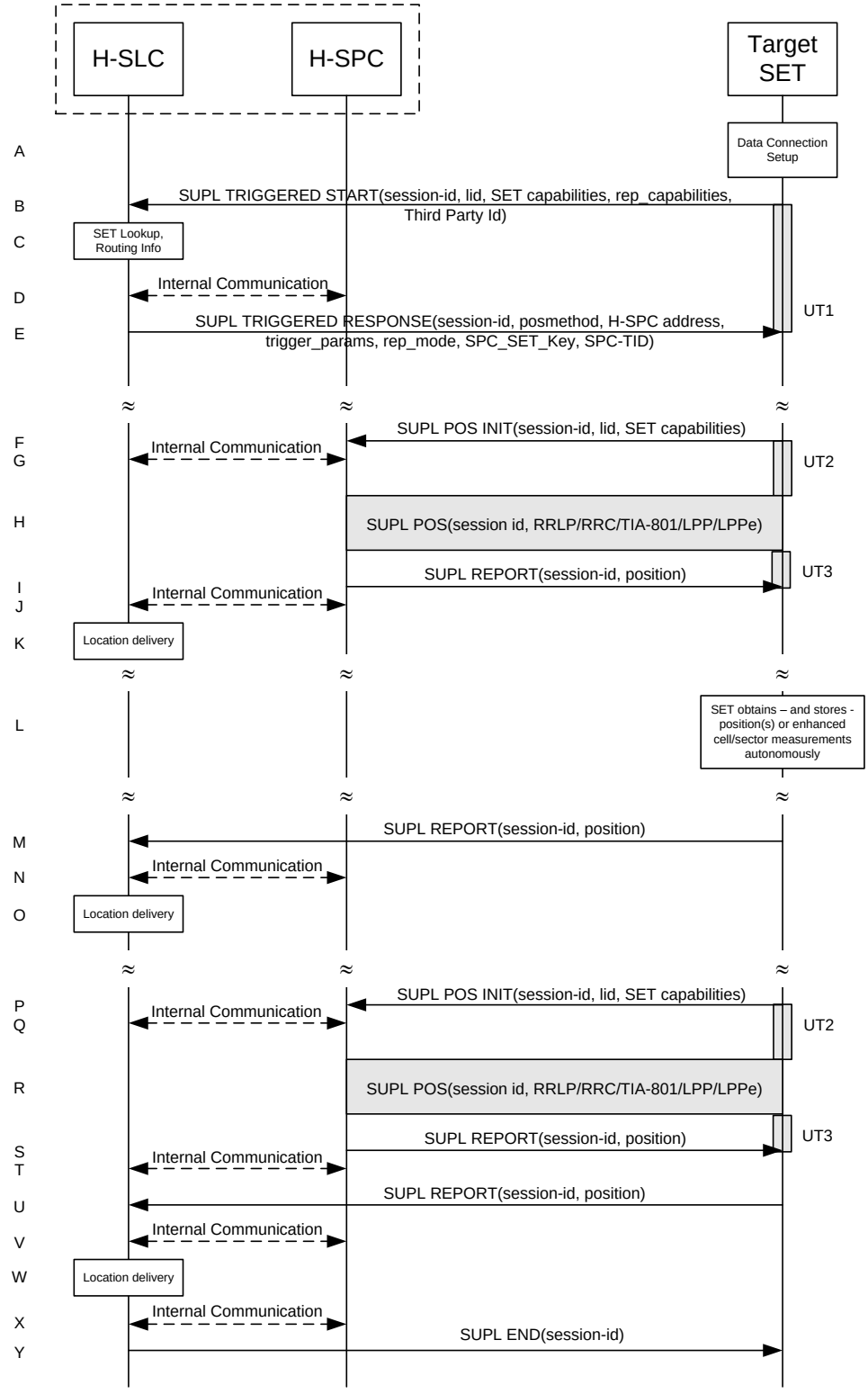

Figure 68: SET Initiated Periodic Location Request with transfer of the position result to 3rd party – non-roaming – non-proxy mode

NOTE: See Appendix D for timer descriptions.

A. The SUPL Agent on the SET receives a request for a periodic triggered service with transfer to a 3rd party from an application running on the SET. The SET takes appropriate action establishing or resuming a secure connection.

B. The SUPL Agent on the SET uses the default address provisioned by the Home Network to establish a secure connection to the H-SLC and sends a SUPL TRIGGERED START message to start a positioning session with the H-SLP. The SUPL TRIGGERED START message contains session-id, SET capabilities, trigger type indicator (in this case periodic), Location ID (lid), periodic trigger parameters and Third Party ID. The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe).

C. The H-SLC verifies that the target SET is currently not SUPL roaming.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside the scope of SUPL 2.0. However, there are various environment dependent mechanisms.

D. Through internal communication the H-SLC requests service for a periodic triggered session from the H-SPC. The H-SLC generates SPC_SET_Key and SPC-TID to be used for mutual H-SPC/SET authentication and forwards both to the H-SPC. The H-SPC grants or denies the request and informs the H-SLC accordingly.

E. Consistent with the SUPL TRIGGERED START message including the SET capabilities of the SET, the H-SLC SHALL determine the intended positioning method to be used for the area event triggered session. If required for the posmethod, the H-SLC SHALL use the supported positioning protocol (e.g., RRLP, RRC, TIA-801 or LPP/LPPe) from the SUPL TRIGGERED START message. The H-SLC SHALL respond with a SUPL TRIGGERED RESPONSE message to the SET. The SUPL TRIGGERED RESPONSE message contains session-id, posmethod, H-SPC address and SPC_SET_Key and SPC-TID. The SET and the H-SLP MAY release the secure connection.

F. When the periodic trigger in the SET indicates that the first position fix has to be performed, the SET takes appropriate action establishing or resuming a secure connection. The SET then sends a SUPL POS INIT message to start a positioning session with the H-SPC. The SUPL POS INIT message contains at least session-id, the Location ID (lid) and the SET capabilities parameter. The SET MAY provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if this is supported. The SET MAY set the Requested Assistance Data element in the SUPL POS INIT.
If a position calculated based on information received in the SUPL POS INIT message is available (e.g. a cell-id based position fix) that meets a required QoP, the H-SPC SHALL directly proceed to step I and not engage in a SUPL POS session.

G. Through internal communication the H-SPC may request a coarse position from the H-SLC based on the lid received in the SUPL POS INIT message.

H. The SET and the H-SPC MAY exchange several successive positioning procedure messages.
The H-SPC calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance obtained from the H-SPC (SET-Based).

I. Once the position calculation is complete the H-SPC sends the SUPL REPORT message to the SET informing it that the positioning procedure is completed. The SET MAY release the secure connection to the H-SLP. If the reporting mode is batch reporting, the SET stores all calculated position estimates. In SET Assisted mode the position is calculated by the H-SPC and therefore needs to be included in the message for batch reporting mode.

J. This step is optional: Once the position calculation is complete and if real time or quasi-real time reporting is used, the H-SPC sends the position estimate through internal communication to the H-SLC.

If a SET Based positioning method was chosen which allows the SET to autonomously calculate a position estimate (e.g. autonomous GPS or A-GPS SET Based mode where the SET has current GPS assistance data and does not require an assistance data update from the H-SLP) steps F to J are not performed. Instead, the SET autonomously calculates the position estimate and – for real time or quasi-real time reporting – sends the calculated position estimate to the H-SLC using a SUPL REPORT message containing the session-id and the position estimate.

K. This step is optional: once the position calculation is complete and if real time or quasi-real time reporting is used, the H-SLC transfers the position result to the 3rd party. If the reporting mode is set to batch reporting, no transfer takes place.

L. This step is optional: If the SET cannot communicate with the H-SLP (e.g. no radio coverage available) and if batch reporting or quasi-real time reporting is used, the SET MAY – if supported – perform SET Based position fixes

(autonomous GPS or SET Based A-GPS where the SET has current assistance data) and/or, if allowed by the H-SLP, enhanced cell/sector measurements. In the case of batch reporting, and if explicitly allowed by the H-SLP, enhanced cell/sector measurements are permitted even when the SET can communicate with the H-SLP.

M. This step is optional and is executed if batch reporting is used and if any of the conditions for sending batch reports have occurred. It is also executed, once the SET is able to re-establish communication with the H-SLP, if quasi-real time reporting is used if one or more previous reports have been missed. The SET sends the stored position estimates and/or, if allowed, the stored enhanced cell/sector measurements in an unsolicited SUPL REPORT message to the H-SLC. The SUPL REPORT message contains the session-id and the position result(s) including date and time information for each position result and optionally the position method used. In the case of batch reporting, the stored position estimates and/or enhanced cell/sector measurements included in the SUPL REPORT message may be chosen according to criteria received in step E. If no criteria are received in step E, the SET shall include all stored position estimates and/or enhanced cell/sector measurements not previously reported.

N. This step is optional: if the H-SLC received stored enhanced cell/sector measurements in the SUPL REPORT message in step M, the H-SPC may need to be involved to translate the enhanced cell/sector measurements into actual position estimates. To this end the H-SLC and the H-SPC may engage in internal communication.

O. The H-SLP transfers the reported and/or calculated position estimate(s) to the 3rd party.

When the last position estimate needs to be calculated i.e. the end of the periodic triggered session has been reached, steps P to V may be performed (a repeat of steps F to J). Alternatively – and if applicable – step L is repeated.

U. This step is optional and is executed after the last position estimate or, if allowed, last set of enhanced cell/sector measurements has been obtained or was due, and at any time up until step Y, if and as soon as all the following conditions apply:

   i. Batch reporting or quasi-real time reporting is used.

   ii. The SET has stored historic location reports and/or stored historic enhanced cell/sector measurements that have not yet been sent to the H-SLC.

   iii. The SET is able to establish communication with the H-SLP

   iv. In the case of batch reporting, the conditions for sending have arisen (e.g. the conditions define sending after the last position estimate is obtained).

   The SUPL REPORT message is used to send all or a subset of stored position fixes and/or stored enhanced cell/sector measurements not previously reported to the H-SLC. In the case of batch reporting, the stored position estimates and/or stored enhanced cell/sector measurements included in the SUPL REPORT message may be chosen according to criteria received in step E. If no criteria are received in step E, the SET shall include all stored position estimates and/or stored enhanced cell/sector measurements not previously reported.

V. This step is optional: if the H-SLC received stored enhanced cell/sector measurements in the SUPL REPORT message in step U, the H-SPC may need to be involved to translate the enhanced cell/sector measurements into actual position estimates. To this end the H-SLC and the H-SPC may engage in internal communication.

W. The H-SLC transfers the reported and/or calculated historical position estimate(s) to the 3rd party.

X. The H-SLC indicates the end of the periodic triggered session to the H-SLP through internal communication.

Y. After the last position result has been transferred to the 3rd party in step W, the H-SLC ends the periodic triggered session by sending a SUPL END message to the SET. Please note that if the last position was calculated in step Q and step U was not performed, the SUPL END message is sent from the H-SPC to the SET (as opposed to from the H-SLC to the SET).

5.2.14.5 Roaming with V-SLP Positioning Successful Case – Non-Proxy Mode

SUPL Roaming where the V-SLP is involved in the positioning calculation.

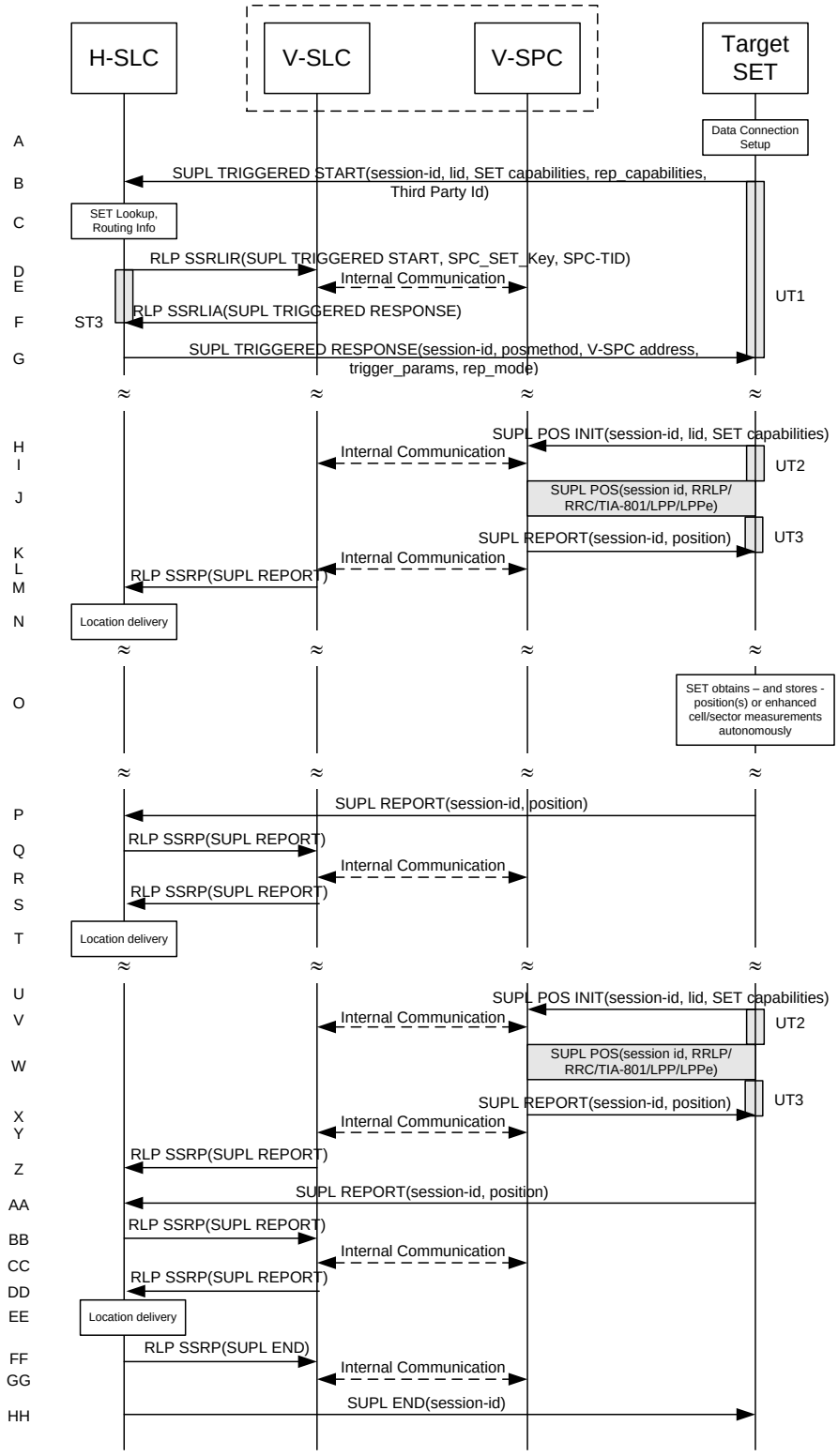

Figure 69: SET Initiated Periodic Location Request with transfer of the position result to 3rd party – roaming with V-SLP Positioning – non-proxy mode

NOTE: See Appendix D for timer descriptions.

A. The SUPL Agent on the SET receives a request for a periodic triggered service with transfer to a 3rd party from an application running on the SET. The SET takes appropriate action establishing or resuming a secure connection.

B. The SUPL Agent on the SET uses the default address provisioned by the Home Network to establish a secure connection to the H-SLC and sends a SUPL TRIGGERED START message to start a positioning session with the H-SLP. The SUPL TRIGGERED START message contains session-id, SET capabilities, trigger type indicator (in this case periodic), Location ID (lid), periodic trigger parameters and Third Party ID. The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe).

C. The H-SLC verifies that the target SET is currently SUPL roaming.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside scope of SUPL 2.0. However, there are various environment dependent mechanisms.

D. The H-SLC decides that the assistance data/position calculation is done by the V-SLP and sends an RLP SSRLIR message tunnelling the SUPL TRIGGERED START message to the V-SLC. The H-SLC also generates SPC_SET_Key and SPC-TID to be used for V-SPC/SET mutual authentication and includes both in the RRLP SSRLIR message.

E. Through internal communication the V-SLC requests service for a periodic triggered session from the V-SPC. The V-SLC also forwards the SPC_SET_Key and SPC-TID to the V-SPC. The V-SPC grants or denies the request and informs the V-SLC accordingly.

F. Consistent with the SUPL TRIGGERED START message including posmethod(s) supported by the SET, the V-SLC SHALL determine the intended positioning method to be used for the periodic triggered session. If required for the posmethod, the V-SLC SHALL use the supported positioning protocol (e.g., RRLP, RRC, TIA-801 or LPP/LPPe) from the SUPL TRIGGERED START message. The V-SLC responds with a SUPL TRIGGERED RESPONSE tunnelled over RLP in a SSRLIA message back to the H-SLC that it is capable of supporting this request. The SUPL TRIGGERED RESPONSE contains at least the sessionid, posmethod and the V-SPC address.

G. The H-SLC sends a SUPL TRIGGERED RESPONSE message to the SET. The SUPL TRIGGERED RESPONSE message contains session-id, posmethod, V-SPC address and SPC_SET_Key and SPC-TID.The SET and the H-SLC MAY release the secure connection.

H. When the periodic trigger in the SET indicates that the first position fix has to be performed, the SET takes appropriate action establishing or resuming a secure connection. The SET then sends a SUPL POS INIT message to the V-SPC to start a positioning session with the V-SPC. The SUPL POS INIT message contains at least session-id, the Location ID (lid) and the SET capabilities parameter. The SET MAY provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if this is supported. The SET MAY set the Requested Assistance Data element in the SUPL POS INIT.
If a position calculated based on information received in the SUPL POS INIT message is available (e.g. a cell-id based position fix) that meets a required QoP, the V-SPC SHALL directly proceed to step K and not engage in a SUPL POS session.

I. Through internal communication the V-SPC may request a coarse position from the V-SLC based on the lid received in the SUPL POS INIT message.

J. The SET and the V-SPC MAY exchange several successive positioning procedure messages.
The V-SPC calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance obtained from the V-SPC (SET-Based).

K. Once the position calculation is complete the V-SPC sends the SUPL REPORT message to the SET informing it that the positioning procedure is completed. The SET MAY release the secure connection to the V-SPC. If the reporting mode is batch reporting, the SET stores all calculated position estimates. In SET Assisted mode the position is calculated by the V-SPC and therefore needs to be included in the message for batch reporting mode.

L. This step is optional: once the position calculation is complete and if real time or quasi-real time reporting is used, the V-SPC sends the position estimate through internal communication to the V-SLC.

M. This step is conditional and is only used after step L occurred. The V-SLC sends the position estimate to the H-SLC in a SUPL REPORT message. The SUPL REPORT message includes at a minimum the session-id and the position estimate. The SUPL REPORT message is carried within an RLP SSRP message.

If a SET Based positioning method was chosen which allows the SET to autonomously calculate a position estimate (e.g. autonomous GPS or A-GPS SET Based mode where the SET has current GPS assistance data and does not require an

assistance data update from the H-SLP) steps H to M are not performed. Instead, the SET autonomously calculates the position estimate and – for real time or quasi-real time reporting – sends the calculated position estimate to the H-SLC using a SUPL REPORT message containing the session-id and the position estimate.

N. This step is optional: if real time or quasi-real time reporting is used, the H-SLC transfers the position estimate to the 3rd party. If the reporting mode is set to batch reporting, no transfer occurs.

O. This step is optional: If the SET cannot communicate with the V-SLP (e.g. no radio coverage available) and if batch reporting or quasi-real time reporting is used, the SET MAY – if supported – perform SET Based position fixes (autonomous GPS or SET Based A-GPS where the SET has current assistance data) and/or, if allowed by the H-SLP, enhanced cell/sector measurements. In the case, of batch reporting, and if explicitly allowed by the H-SLP, enhanced cell/sector measurements are permitted even when the SET can communicate with the V-SLP.

P. This step is optional and is executed if batch reporting is used and if any of the conditions for sending batch reports have occurred. It is also executed, once the SET is able to re-establish communication with the H-SLP/V-SLP, if quasi-real time reporting is used if one or more previous reports have been missed. The SET sends the stored position estimates and/or, if allowed, the stored enhanced cell/sector measurements in an unsolicited SUPL REPORT message to the H-SLC. The SUPL REPORT message contains the session-id and the position result(s) including date and time information for each position result and optionally the position method used. In the case of batch reporting, the stored position estimates and/or enhanced cell/sector measurements included in the SUPL REPORT message may be chosen according to criteria received in step G. If no criteria are received in step G, the SET shall include all stored position estimates and/or enhanced cell/sector measurements not previously reported.

Q. This step is optional: if the H-SLC received stored enhanced cell/sector measurements in the SUPL REPORT message in step P, the V-SLP may need to be involved to translate the enhanced cell/sector measurements into actual position estimates. To this end the H-SLC sends a SUPL REPORT message to the V-SLC using an SSRP message over RLP tunnel.

R. This step is optional and only used if the V-SPC is required to translate stored enhanced cell/sector measurements received by the V-SLC into actual position estimates. In this case, internal communication between the V-SLC and the V-SPC takes place.

S. This step is conditional and takes place after step Q and – optionally – step R. A SUPL REPORT message containing position estimates calculated from enhanced cell/sector measurements received in step Q is sent from the V-SLC to the H-SLC using an SSRP message over RLP tunnel.

T. The H-SLC transfers the reported and/or calculated position estimate(s) to the 3rd party.

When the last position estimate needs to be calculated i.e. the end of the periodic triggered session has been reached, steps U to Z may be performed (a repeat of steps H to M). Alternatively – and if applicable – step O is repeated.

AA. This step is optional and is executed after the last position estimate or, if allowed, last set of enhanced cell/sector measurements has been obtained or was due, and at any time up until step HH, if and as soon as all the following conditions apply:

   i. Batch reporting or quasi-real time reporting is used.

   ii. The SET has stored historic location reports and/or stored historic enhanced cell/sector measurements that have not yet been sent to the H-SLC.

   iii. The SET is able to establish communication with the H-SLP.

   iv. In the case of batch reporting, the conditions for sending have arisen (e.g. the conditions define sending after the last position estimate is obtained).

The SUPL REPORT message is used to send all or a subset of stored position fixes and/or stored enhanced cell/sector measurements not previously reported to the H-SLC. In the case of batch reporting, the stored position estimates and/or stored enhanced cell/sector measurements included in the SUPL REPORT message may be chosen according to criteria received in step G. If no criteria are received in step G, the SET shall include all stored position estimates and/or stored enhanced cell/sector measurements not previously reported.

BB. This step is optional: if the H-SLC received stored enhanced cell/sector measurements in the SUPL REPORT message in step AA, the V-SLP may need to be involved to translate the enhanced cell/sector measurements into

actual position estimates. To this end the H-SLC sends a SUPL REPORT message to the V-SLC using an SSRP message over RLP tunnel.

CC. This step is optional and only used if the V-SPC is required to translate stored enhanced cell/sector measurements received by the V-SLC into actual position estimates. In this case, internal communication between the V-SLC and the V-SPC takes place.

DD. This step is conditional and takes place after step BB and – optionally – step CC. A SUPL REPORT message containing position estimates calculated from enhanced cell/sector measurements received in step BB is sent from the V-SLC to the H-SLC using an SSRP message over RLP tunnel.

EE. The H-SLC transfers the reported and/or calculated historical position estimate(s) to the 3rd party.

FF. The H-SLC informs the V-SLC about the end of the periodic triggered session through an SUPL END message carried within an SSRP message over RLP tunnel.

GG. The V-SLC informs the V-SPC about the end of the periodic triggered session through internal communication.

HH. The H-SLC ends the periodic triggered session with the SET by sending a SUPL END message. The SUPL END message includes at least the session-id. Please note that if the last position was calculated in step W and step AA was not performed, the SUPL END message is sent from the V-SPC to the SET.

5.2.14.6 Roaming with H-SLP Positioning Successful Case – Non-Proxy Mode

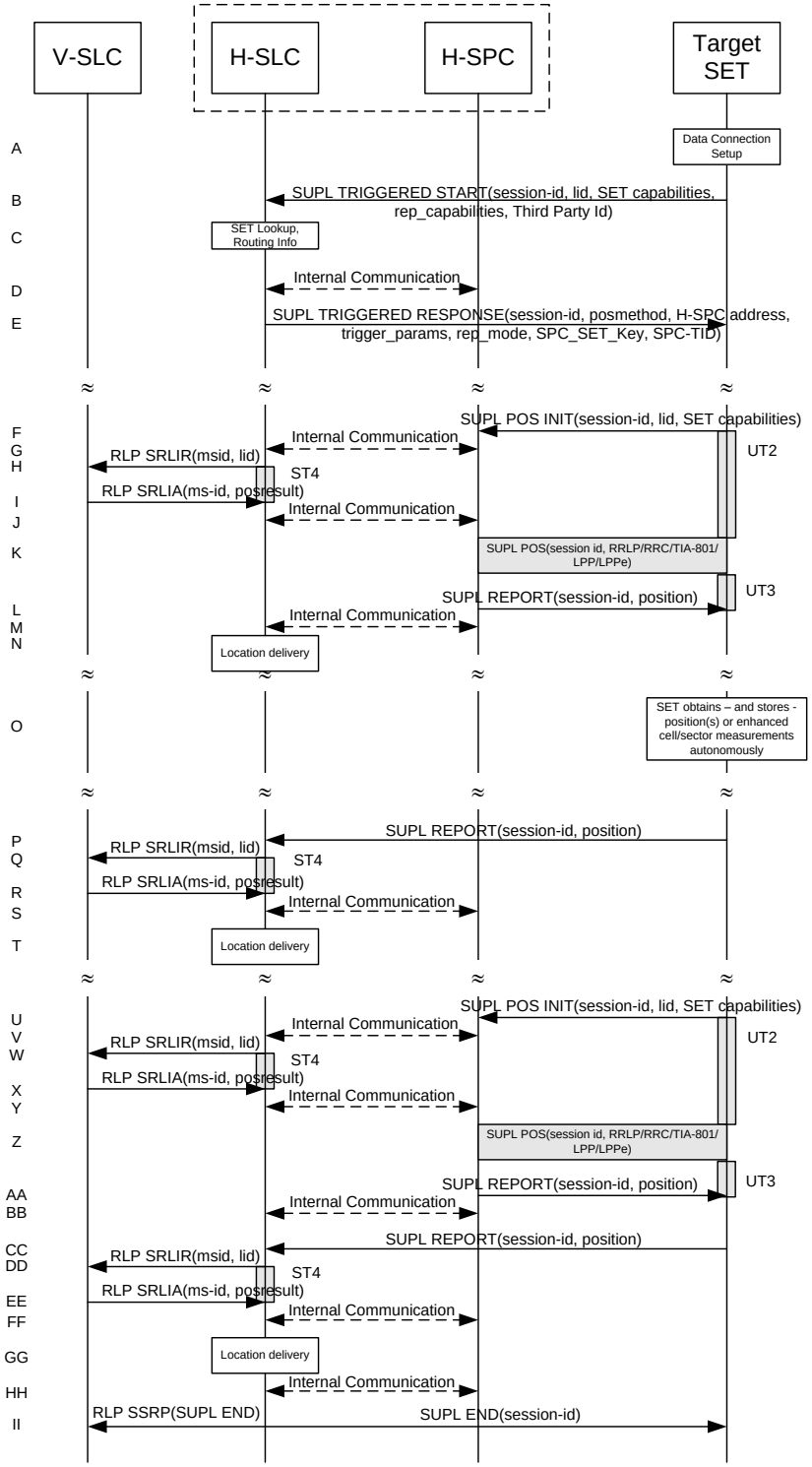

Figure 70: SET Initiated Periodic Location Request with transfer of the position result to 3rd party – roaming with H-SLP Positioning – non-proxy mode

NOTE: See Appendix D for timer descriptions.

A. The SUPL Agent on the SET receives a request for a periodic triggered service with transfer to a 3rd party from an application running on the SET. The SET takes appropriate action establishing or resuming a secure connection.

B. The SUPL Agent on the SET uses the default address provisioned by the Home Network to establish a secure connection to the H-SLC and sends a SUPL TRIGGERED START message to start a positioning session with the H-SLP. The SUPL TRIGGERED START message contains session-id, SET capabilities, trigger type indicator (in this case periodic), Location ID (lid), periodic trigger parameters and Third Party ID. The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe).

C. The H-SLC verifies that the target SET is currently SUPL roaming.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside scope of SUPL 2.0. However, there are various environment dependent mechanisms.

D. Through internal communication the H-SLC requests service for a periodic triggered session from the H-SPC. The H-SLC also creates SPC_SET_Key and SPC-TID to be used for mutual H-SPC/SET authentication and forwards both to the H-SPC through internal communication. The H-SPC grants or denies the request and informs the H-SLC accordingly.

E. Consistent with the SUPL TRIGGERED START message including posmethod(s) supported by the SET, the H-SLC SHALL determine the intended positioning method to be used for the periodic triggered session. If required for the posmethod, the H-SLC SHALL use the supported positioning protocol (e.g., RRLP, RRC, TIA-801 or LPP/LPPe) from the SUPL TRIGGERED START message. The H-SLC sends a SUPL TRIGGERED RESPONSE message to the SET. The SUPL TRIGGERED RESPONSE message contains session-id, posmethod, H-SPC address and SPC_SET_Key and SPC-TID. The SET and the H-SLC MAY release the secure connection.

F. When the periodic trigger in the SET indicates that the first position fix has to be performed, the SET takes appropriate action establishing or resuming a secure connection. The SET then sends a SUPL POS INIT message to the H-SPC to start a positioning session with the H-SPC. The SUPL POS INIT message contains at least session-id, the Location ID (lid) and the SET capabilities parameter. The SET MAY provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if this is supported. The SET MAY set the Requested Assistance Data element in the SUPL POS INIT.
If the SUPL POS INIT message contains a position that meets a required QoP, the H-SPC SHALL directly proceed to step L.

G. Through internal communication the H-SPC requests a coarse position estimate from the H-SLC based on the lid received in step F.

H. To obtain a coarse position the H-SLC sends an RLP SRLIR message to the V-SLP.

I. The V-SLP translates the received lid into a position estimate and returns the result to the H-SLC in an RLP SRLIA message.
For real-time or quasi-real time reporting, if the returned position meets a required QoP, the H-SLC SHALL directly proceed to step L and not engage in a SUPL POS session. For batch reporting, if the returned position meets a required QoP, the H-SLC SHALL send the position result through internal communication to the H-SPC (step J) and the H-SPC will forward the position result to the SET using a SUPL REPORT message (step L) without engaging in a SUPL POS session (step K).

J. The H-SLC forwards the coarse position to the H-SPC through internal communication.

K. The SET and the H-SPC MAY exchange several successive positioning procedure messages.
The H-SPC calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance obtained from the H-SPC (SET-Based).

L. Once the position calculation is complete the H-SPC sends the SUPL REPORT message to the SET informing it that the positioning procedure is completed. The SET MAY release the secure connection to the H-SLP. If the reporting mode is batch reporting, the SET stores all calculated position estimates. In SET Assisted mode the position is calculated by the H-SPC and therefore needs to be included in the message for batch reporting mode.

M. This step is optional and only used for real-time reporting: once the position calculation is complete, the H-SPC sends the position estimate to the H-SLC through internal communication.

If a SET Based positioning method was chosen which allows the SET to autonomously calculate a position estimate (e.g. autonomous GPS or A-GPS SET Based mode where the SET has current GPS assistance data and does not require an assistance data update from the H-SLP) steps F to M are not performed. Instead, the SET autonomously calculates the

position estimate and – for real time or quasi-real time reporting – sends the calculated position estimate to the H-SLC using a SUPL REPORT message containing the session-id and the position estimate.

N. This step is optional: if real time or quasi-real time reporting is used, the H-SLC transfers the calculated position estimate to the 3rd party. If the reporting mode is set to batch reporting, no transfer occurs.

O. This step is optional: If the SET cannot communicate with the H-SLP (e.g. no radio coverage available) and if batch reporting or quasi-real time reporting is used, the SET MAY – if supported – perform SET Based position fixes (autonomous GPS or SET Based A-GPS where the SET has current assistance data) and/or, if allowed by the H-SLP, enhanced cell/sector measurements. In the case, of batch reporting, and if explicitly allowed by the H-SLP, enhanced cell/sector measurements are permitted even when the SET can communicate with the H-SLP.

P. This step is optional and is executed if batch reporting is used and if any of the conditions for sending batch reports have occurred. It is also executed, once the SET is able to re-establish communication with the H-SLP, if quasi-real time reporting is used if one or more previous reports have been missed. The SET sends the stored position estimates and/or, if allowed, the stored enhanced cell/sector measurements in an unsolicited SUPL REPORT message to the H-SLC. The SUPL REPORT message contains the session-id and the position result(s) including date and time information for each position result and optionally the position method used. In the case of batch reporting, the stored position estimates and/or enhanced cell/sector measurements included in the SUPL REPORT message may be chosen according to criteria received in step E. If no criteria are received in step E, the SET shall include all stored position estimates and/or enhanced cell/sector measurements not previously reported.

Q. This step is optional: if the H-SLC received stored enhanced cell/sector measurements in the SUPL REPORT message in step P, the V-SLP may need to be involved to translate the enhanced cell/sector measurements into actual position estimates To this end the H-SLC sends an RLP SRLIR message to the V-SLC.

R. This step is conditional and takes place only if step Q occurred. The V-SLC sends the position result calculated based on the enhanced cell/sector measurements received in step Q to the H-SLC.

S. This step is optional and only takes place if after the translation into a position estimate in steps Q and R the H-SPC is required to calculate the position estimate. In this case, internal communication between the H-SLC and H-SPC takes place.

T. The H-SLC transfers the reported and/or calculated position estimate(s) to the 3rd party.

When the last position estimate needs to be calculated i.e. the end of the periodic triggered session has been reached, steps U to BB may be performed (a repeat of steps F to M). Alternatively – and if applicable – step O is repeated.

CC. This step is optional and is executed after the last position estimate or, if allowed, last set of enhanced cell/sector measurements has been obtained or was due, and at any time up until step II, if and as soon as all the following conditions apply:

   i. Batch reporting or quasi-real time reporting is used.

   ii. The SET has stored historic location reports and/or stored historic enhanced cell/sector measurements that have not yet been sent to the H-SLC.

   iii. The SET is able to establish communication with the H-SLP.

   iv. In the case of batch reporting, the conditions for sending have arisen (e.g. the conditions define sending after the last position estimate is obtained).

The SUPL REPORT message is used to send all or a subset of stored position fixes and/or stored enhanced cell/sector measurements not previously reported to the H-SLC. In the case of batch reporting, the stored position estimates and/or stored enhanced cell/sector measurements included in the SUPL REPORT message may be chosen according to criteria received in step E. If no criteria are received in step E, the SET shall include all stored position estimates and/or stored enhanced cell/sector measurements not previously reported.

DD. This step is optional: if the H-SLC received stored enhanced cell/sector measurements in the SUPL REPORT message in step CC, the V-SLP may need to be involved to translate the enhanced cell/sector measurements into actual position estimates To this end the H-SLC sends an RLP SRLIR message to the V-SLC.

EE. This step is conditional and takes place only if step DD occurred. The V-SLC sends the position result calculated based on the enhanced cell/sector measurements received in step DD to the H-SLC.

FF. This step is optional and only takes place if after the translation into a position estimate in steps DD and EE the H-SPC is required to calculate the position estimate. In this case, internal communication between the H-SLC and H-SPC takes place.

GG. The H-SLC transfers the reported and/or calculated historical position estimate(s) to the 3rd party.

HH. Using internal communication, the H-SLC informs the H-SPC of the end of the periodic triggered session.

II. The H-SLC ends the periodic triggered session with the SET by sending a SUPL END message. The SUPL END message includes at least the session-id. Please note that if the last position was calculated in step Z and step CC was not performed, the SUPL END message is sent from the H-SPC to the SET (as opposed to from the H-SLC to the SET).

5.2.15 SET-Initiated Location Request of Transfer Location to Third Party

This section describes the call flow for SET Initiated Location Request with transfer to Third Party. The location delivery to a Third Party takes place at the end of the call flow and can be viewed as independent of the actual SET Initiated SUPL session. For this reason, only the proxy mode, non roaming scenarios are described in this section. The procedure for transfer to Third Party applies to all other scenarios (roaming proxy mode, non proxy mode roaming and non-roaming) in the same way i.e. the transfer to Third Party takes place after the SET Initiated call flow has finished.

NOTE: The call flow diagram of this section, shows the transfer of the location to a Third Party indicated by a place holder "Location delivery". The specifics of the actual delivery of the location to the Third Party are outside the scope of SUPL. Please refer to section 8.1.6.2 for the proper use of RRLP/RRC in step F of Figure 71.

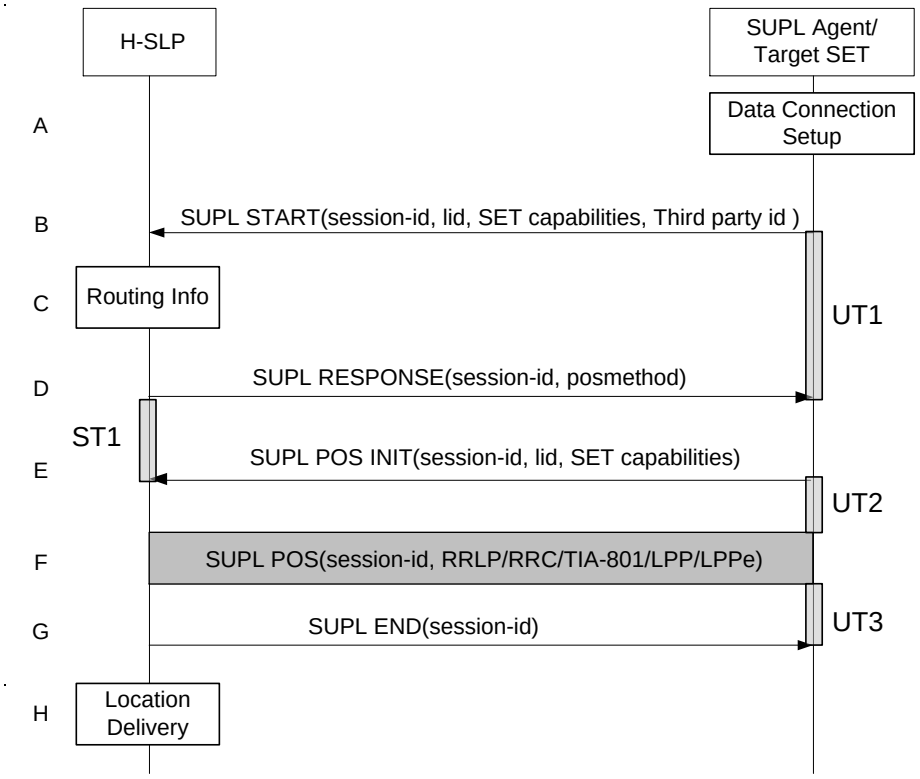

Figure 71: SET Initiated Location Request of Transfer Location to Third party

NOTE: See Appendix D for timer descriptions.

A. The SUPL Agent on the Target SET initiates a SET Initiated location request with Transfer to Third Party. The SET takes appropriate action to establish or resume a secure connection.

B. The SUPL Agent on the Target SET uses the default address provisioned by the Home Network to establish a secure connection to the H-SLP and sends a SUPL START message to start a positioning session with the H-SLP. The SUPL START message contains session-id, SET capabilities and Third Party ID.

C. The H-SLP verifies that the Target SET is currently not SUPL roaming.

NOTE: The specifics for determining if the SET is SUPL roaming or not is considered outside scope of SUPL. However, there are various environment dependent mechanisms.

D. Consistent with the SUPL START message including posmethod(s) supported by the SET, the H-SLP SHALL determine the posmethod. If required for the posmethod, the H-SLP SHALL use the supported positioning protocol (e.g., RRLP, RRC, TIA-801 or LPP/LPPe) from the SUPL START message. The H-SLP SHALL respond with the SUPL RESPONSE to the SET. The SUPL RESPONSE contains the session-id but no H-SLP address, to indicate to the SET that a new connection SHALL NOT be established. The SUPL RESPONSE also contains the posmethod. If, however, a position retrieved or calculated based on information received in the SUPL START message meets a requested QoP, the H-SLP MAY directly proceed to step G.

E. After the SET receives the SUPL RESPONSE from H-SLP, the SET sends a SUPL POS INIT message. The SUPL POS INIT message contains at least session-id, SET capabilities and Location ID (lid). The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe). The SET MAY optionally provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET MAY provide its position, if this is supported. The SET MAY include the first SUPL POS element in the SUPL POS INIT message. The SET MAY set the Requested Assistance Data element in the SUPL POS INIT.

F. The SET and the H-SLP MAY exchange several successive positioning procedure messages.
The H-SLP calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance obtained from the H-SLP (SET-Based).

G. The H-SLP sends the SUPL END message to the Target SET informing it that no further positioning procedure will be started and that the session is finished. The SET releases all resources related to the session .

H. The H-SLP transfers the position result to the Third party and releases all resources related to the session.

5.2.16 Network Change for Area Event Triggered Scenarios

See section 5.1.14.

5.2.17 Exception Procedures

5.2.17.1 SET Authorization Failure

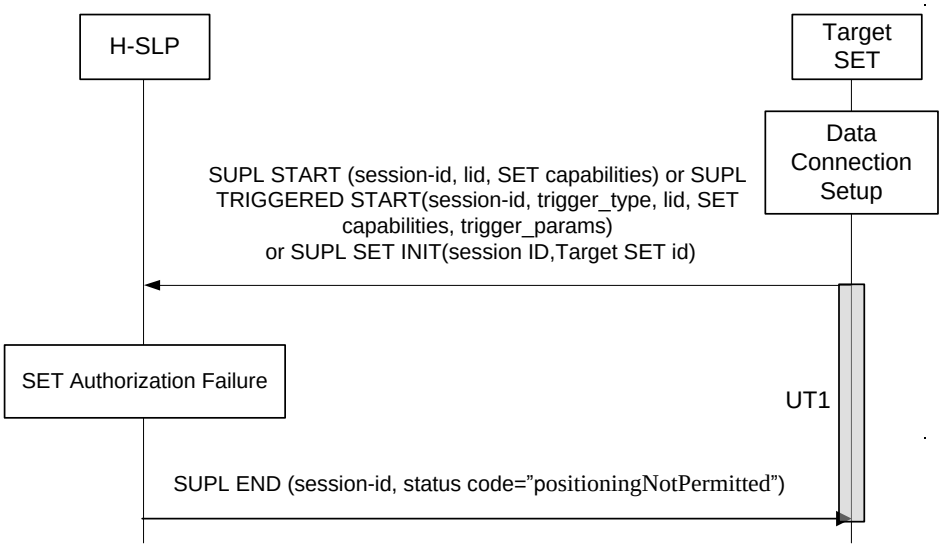

Figure 72: SET-Initiated Error SET Authorization Failure

NOTE: See Appendix D for timer descriptions.

A. The SUPL Agent on the SET receives a request for position from an application running on the SET. The SET takes appropriate action establishing or resuming a secure connection.

B. The SUPL Agent on the SET uses the default address provisioned by the Home Network to establish a secure IP connection to the H-SLP and sends a SUPL START, or a SUPL TRIGGERED START, or a SUPL SET INIT message to start a positioning session with the H-SLP.

C. Authorization of the SET-initiated positioning request fails at the H-SLP (for example, the SET User has not subscribed to SET-initiated location services).

D. The H-SLP returns to the SET a SUPL END message containing the session-id and the status code indicating the error reason ("positioning not permitted"). Afterwards the SET releases the secure IP connection and all resources related to this session at the Lup interface.

5.2.17.2 SUPL Protocol Error

When during a SUPL session either the SLP or the SET receives a message, which cannot be processed by the receiving entity due to SUPL protocol error, the receiving entity shall send a SUPL END message to the sending entity including a status code indicating protocol error.

Possible protocol error cases can be

- mandatory and/or conditional parameter is missing
- wrong parameter value
- unexpected message
- invalid session-id
- positioning protocol mismatch

The SUPL END message includes the valid session-id actually being used in the session. When an invalid session-id has been received the invalid session-id shall be returned to the sending entity along with the status code. A received session-id shall be treated as invalid if no open session can be assigned to this session-id or in case of the SUPL INIT message, the session-id is not treated as SLP-generated by the SET.

Afterwards, the SLP and the SET release the resources related to this session at the Lup interface.

The described processing for protocol error does only apply to messages on the SUPL level. Exceptions, which occur during application of the specific positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe) shall be handled by means of the exception procedure specific for this positioning protocol along with the related messages.

The following SUPL protocol error types, attributable to either the SLP or the SET, are addressed by the general exception procedure shown below:

- Missing mandatory parameter(s)
- Wrong parameter value
- Unexpected message
- Positioning protocol mismatch

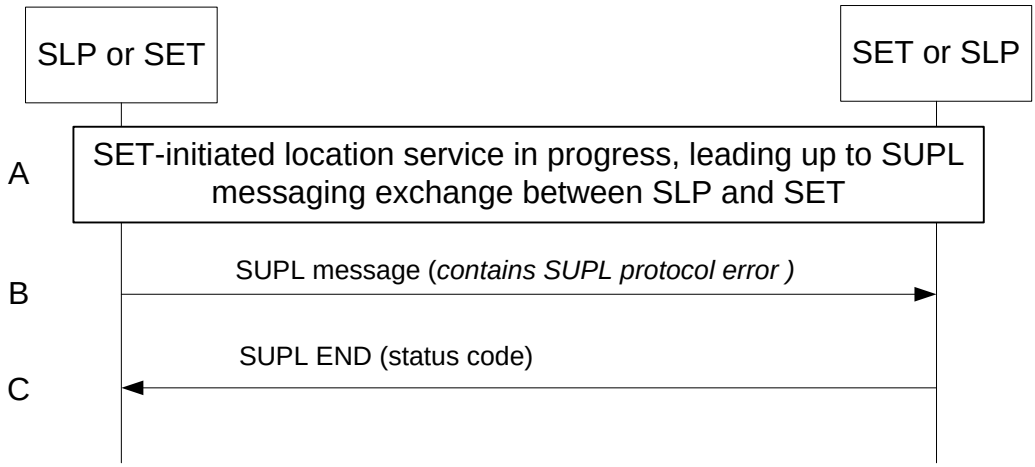

Figure 73: SET-Initiated Error SUPL Protocol Error

A. A SET-initiated location request has occurred, in either roaming or non-roaming SET scenario, in which the call flow has progressed to the SUPL messaging exchange between the SLP and the SET.

B. A SUPL message sent from either the SLP or the SET contains a protocol error. Such message, if sent by the SLP, may be SUPL RESPONSE; such message, if sent by the SET, may be SUPL START or SUPL POS INIT.

C. The recipient (either the SLP or SET) of the SUPL message containing the protocol error responds with a SUPL END message containing the status code for the specific protocol error. Afterwards, both sides release all resources related to this session at the Lup reference point.

5.2.17.3 SUPL timer expiration

When either a SLP or a SET timer expires, the procedure described in Appendix D shall be followed.

5.2.17.4 SET cancels the triggered location request

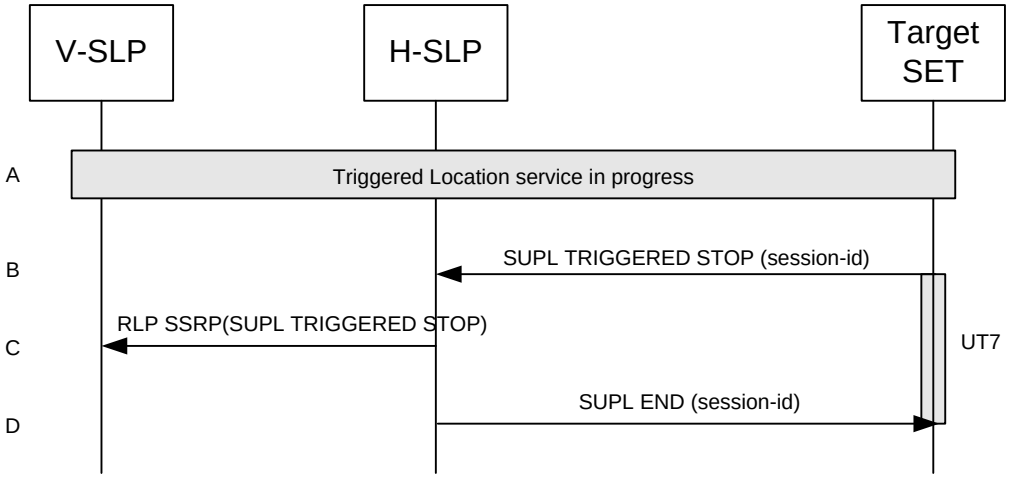

Figure 74: SET Initiated Triggered location, SET cancels the triggered location request

NOTE: See Appendix D for timer descriptions.

A. The triggered location procedure is in progress.

B. The SET sends a SUPL TRIGGERED STOP message with the session-id to H-SLP to request cancel this triggered location.

C. This step is optional. If H-SLP has roaming session with one V-SLP, it should send RLP SSRP message including SUPL TRIGGERED STOP to notify the VSLP to release resource allocated for this session.

D. The H-SLP sends the SUPL END message to the SET. The SET SHALL release the secure IP connection and release all resources related to this session.

5.2.17.5 Network cancels the Triggered Location Request

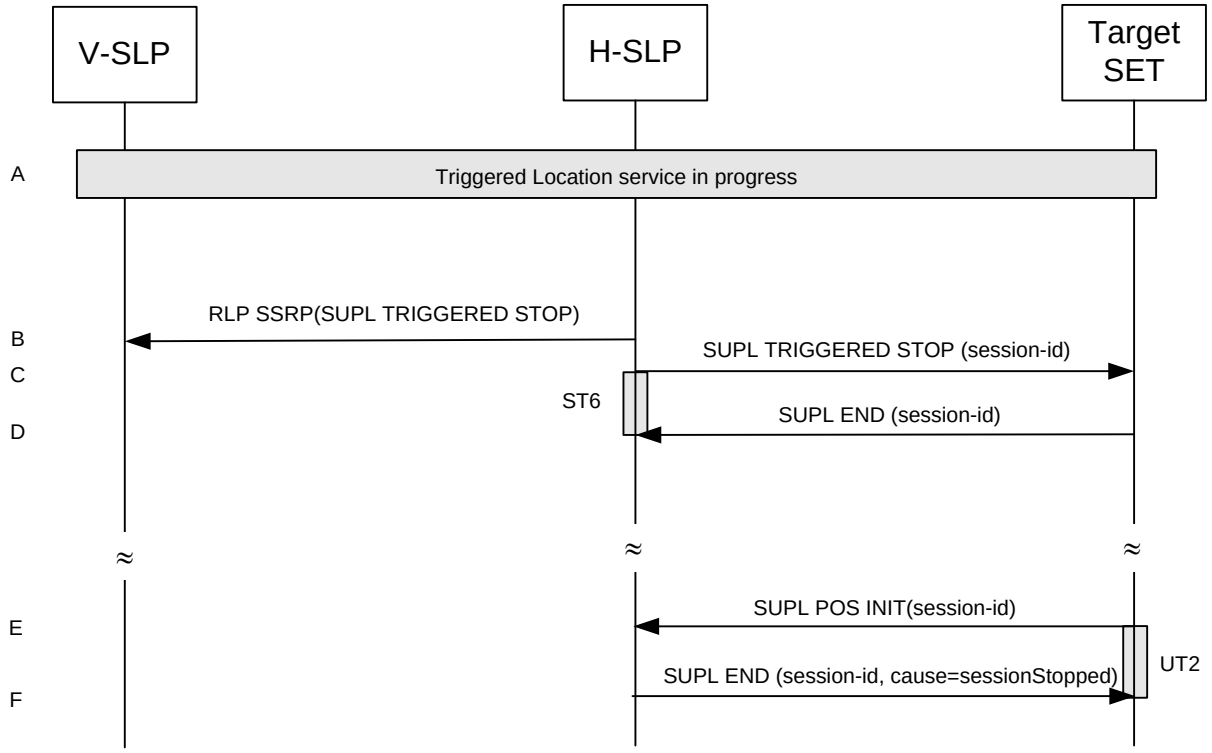

Figure 75: SET Initiated Triggered location, Network cancels the triggered location request

NOTE: See Appendix D for timer descriptions.

NOTE: This sequence assumes an open data connection exists between the H-SLP and the SET. For network triggered session cancellation in the absence of a data connection, the SLP may establish a data connection by first initiating a Session Info Query, as described in section 5.1.18 Session Info Query.

A. A triggered location session is in progress.

B. This step is optional: for roaming with V-SLP scenarios, the H-SLP sends an RLP SSRP message including a SUPL TRIGGERED STOP message to the V-SLP in order to inform the V-SLP about the cancellation of the triggered session and to release all resource allocated to this session.

C. The H-SLP sends a SUPL TRIGGERED STOP message including the session-id to the target SET to request cancellation of the triggered session. If the H-SLP deems the sending of the SUPL TRIGGERED STOP message unsuccessful (i.e. timer ST6 expired after no SUPL END message was received as acknowledgement that the SET has received and accepted the triggered session cancellation request), the H-SLP considers the triggered session as cancelled.

D. The target SET acknowledges that it has cancelled the triggered session with the SUPL END message back to the H-SLP. If that cancellation fails, the message contains the result code indicating the error reason.

NOTE: If the cancellation of the triggered request was successful, the call flow ends with step D. If, however, the cancellation of the triggered request was unsuccessful (e.g. SUPL TRIGGERED STOP message was not received by the SET, no SUPL END confirmation was received by the H-SLP, etc.), the SET may try to continue a triggered session which the H-SLP deems cancelled. In this case the following steps are executed:

E. The SET sends a SUPL POS INIT message to the H-SLP (could also be any other SUPL message which the SET is allowed to send to the H-SLP) containing a session-id which the H-SLP deems non-existent..

F. The H-SLP sends the SUPL END message with status code ‘sessionStopped’ or ‘invalidSessionId’.

5.2.17.6 SET Initiated Event Trigger timer expiry

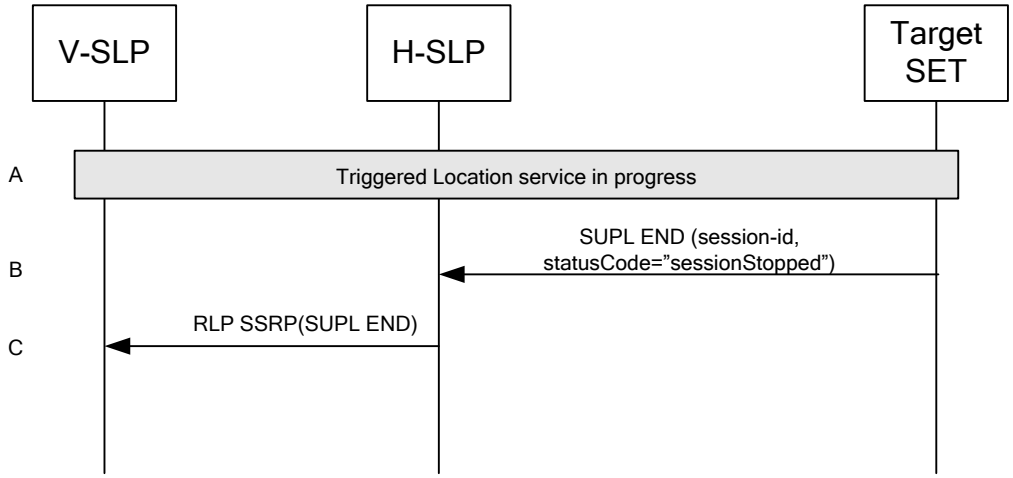

Figure 76: SET Initiated Event Trigger timer expiry

NOTE: See Appendix D for timer descriptions.

E. The triggered location procedure is in progress.

F. When the StopTime associated with the event trigger is reached, the SET sends a SUPL END message with the session-id and statusCode of “sessionStopped” to H-SLP to request cancel this triggered location. The SET releases all resources related to this session.

G. If H-SLP has roaming session with one V-SLP, it MAY send a RLP SSRP message including SUPL END to notify the VSLP to release resource allocated for this session. The H-SLP releases all resources related to this session

NOTE: If the H-SLP detects that SET does not send a SUPL END by a configured time interval after the Stop Time, it MAY proceed straight to step C and discard all resources for the session.

6. Security Considerations

This section describes the SUPL Security function that enables the SUPL network to authenticate and authorize the SET and enables the SET to authenticate and authorize the SUPL network.

NOTE: Unless otherwise specified, the use of the acronym TLS refers to any session that can be negotiated using a TLS handshake: this includes TLS 1.1 ciphersuites, TLS 1.2 ciphersuites and TLS-PSK ciphersuites.

NOTE: In this section, the following definitions apply. A *3GPP bearer network* is one for which the standards are maintained by 3GPP; these include GSM, GPRS, EDGE, WCDMA/TD-SCDMA, LTE and NR bearer networks. A *3GPP2 bearer network* is one for which the standards are maintained by 3GPP2; these include cdmaOne, cdma2000 1x, cdma200 EV-DO and UMB bearer networks. A 3GPP SET (3GPP2 SET respectively) is a SET that supports data access via a 3GPP bearer network (3GPP2 bearer network respectively). A WiMAX SET is a SET that supports data access via a WiMAX bearer network ([NWG 1.2.0 stage 2], [NWG 1.2.0 stage3]).

NOTE: H-SLP operators should note that the authentication methods described herein do not take into account scenarios where the SET moves from one access network to another. It is assumed, that after the hand over to another access system, the security context may not be available in the terminal and the network and the level of trust between the network and terminal may change.

On powering up and shutting down, detection of a new UICC or removal of a UICC, the SET handset MUST delete any keys on the SET handset associated with SUPL 2.0, including

- **GBA Keys:** such as Ks, Ks_NAF, Ks_ext_NAF
- **WIMAX Keys:** such as SEK
- **TLS Keys**: such as pre_master_secret, master_secret, and PSK values such as PSK_SPC_SET_Key.
- **SUPL Specific Keys**: such as keys associated with protection of SUPL INIT messages.

6.1 SUPL Authentication Model

Mutual authentication SHALL be supported between a SET and an H-SLP. Server authentication SHALL be supported between a SET and an E-SLP, and mutual authentication MAY be supported between a SET and E-SLP.

When mutual authentication is performed, the SET SHALL act on behalf of the SET User via a SUPL Agent contained in the SET using the security credentials associated with the SET User.

Note that a successful authentication of the SET User MUST result in a successful identification of the SET User's ID (e.g., MSISDN, WIMAX user ID).

Note that when MSISDN is used for identification, the SLP MUST perform an IMSI to MSISDN binding before the MSISDN of the authenticated SET User is securely identified.

The details of Key Management can be found in section 6.1.2.

6.1.1 SET-SLC Mutual-Authentication Methods

Section 6.1.1.1 lists the SET-SLC authentication methods supported in this specification. An informative overview of these methods is provided in section 6.1.1.2. Section 6.1.1.3 describes which methods are mandatory or optional in the various SUPL 2.0 entities, and lists the protocols required in each entity if it is to support a given SET-SLC mutual-authentication method.

6.1.1.1 List of Supported SET-SLC Mutual-Authentication Methods

The SUPL Authentication model requires shared secret keys between the SLC and the SET, preferably bound to a removable token such as a R-UIM/UICC/SIM/USIM.

There are two classes of SET-SLC authentication methods specified in this document:

- PSK-based methods, consisting of the following methods:
    - Generic Bootstrapping Architecture (GBA)-based method
    - SEK based method (only applicable to WIMAX Home-SLC)

- Server-certificate based methods, consisting of the following methods:
    - Alternative Client authentication (ACA)-based method,
    - SLC-only method (only applicable in emergency cases).

6.1.1.2 Overview of Supported SET-SLC Mutual-Authentication Methods (Informative)

(1) Generic Bootstrapping Architecture (GBA)-Based. TLS-PSK with Generic Bootstrapping Architecture (GBA) ([3GPP 33.220], [3GPP 33.222], [3GPP2 S.S0109], [3GPP2 S.S0114]). GBA provides mutual authentication capability based on shared secret that is derived using existing 3GPP/3GPP2 authentication mechanisms.

- SET and SLC are mutually authenticated using TLS-PSK with Generic Bootstrapping Architecture (GBA) ([3GPP 33.220], [3GPP 33.222], [3GPP2 S.S0109], [3GPP2 S.S0114]).

(2) SEK based (only applicable to WIMAX Home-SLC).

- SET and SLC are mutually authenticated using TLS-PSK with SEK. The details of SEK method can be found in section 6.1.2.2.

(3) Alternative Client authentication (ACA)-based. This uses TLS with

- RSA certificate to authenticate the SLC to the SET,
- Alternative Client authentication of the SET to the SLC (see section 6.1.4). In this case, the SLC authenticates the SET by getting the bearer network to confirm the IP address associated with the SET Identifier (MSISDN etc.).

(4) SLC-only. This is used in scenarios where it is not possible for the SLC to authenticate the SET. This method SHALL NOT be used for non-emergency cases. The SET cannot distinguish between this method and ACA-based. This uses TLS with

- An RSA certificate to authenticate the SLC to the SET,
- The SET is not authenticated.

6.1.1.3 Supported SET-SLC Mutual-Authentication Methods by Entity

Table 1 and Table 2 indicate those methods that are mandatory and those methods that are optional to implement in the Home-SLC, Emergency-SLC, SET handset and SET (R-)UIM/ SIM/USIM for SUPL 2.0; Table 3 lists the required protocols for the H-SLC, SET Handset and SET (R-)UIM/ SIM/USIM for supporting each the various authentication methods.

Entity	Requirement Status for SUPL Authentication Method in GSM and UMTS systems		
	PSK-based methods	Server-Certificate Based Methods	
	GBA-based	ACA-based	SLC-only (E-SLC only)
Home-SLC	**Mandatory** to support one of these **two** methods.		**Not supported**
Emergency-SLC	**Optional**	**Optional**	**Mandatory**
SET Handset	**Optional**	**Mandatory**	**Mandatory**
SET SIM/USIM/(R)-UIM	SIM/USIM/(R)-UIM is involved in this method, but it already supports the necessary algorithm	This entity is not involved in this method	This entity is not involved in this method

Table 1: Requirement status (mandatory or optional) of the various authentication methods for the H-SLC, Emergency- SLC, SET handset and SET SIM/USIM for systems supporting 3GPP SETs and systems supporting 3GPP2 SETs.

NOTE: SET Handset support for the ACA-based method (only for 3GPP and 3GPP2) and the SLC-only method are required for emergency cases.

Entity	Requirement Status for SUPL Authentication Method in WiMAX systems		
	PSK-based methods	Server-Certificate Based Methods	
	SEK based	ACA-based	SLC-only (E-SLC only)
Home-SLC	**Mandatory**	**Not Supported**	**Not Supported**
Emergency-SLC	**Optional**	**Not Supported**	**Mandatory**
SET Handset	**Mandatory**	**Not Supported**	**Mandatory**

Table 2: Requirement status (mandatory or optional) of the various authentication methods for the H-SLC, Emergency- SLC and the SET handset for WIMAX systems

Entity	Algorithms required to support the Authentication Method between SET and SLC			
	PSK-based methods		Server-Certificate Based Methods	
	GBA-based	SEK-based (WiMAX only)	ACA-based (3GPP & 3GPP2 only)	SLC-only (E-SLC only)
SLC	GBA & TLS-PSK	SEK & TLS-PSK	TLS using server certificates & IP Address/SET ID binding	TLS using server certificates
SET Handset	GBA & TLS-PSK	SEK & TLS-PSK	TLS using server certificates	
SET R-UIM/UICC/SIM/USIM	No additional algorithms required	Not applicable	No additional algorithms required	

Table 3: Required protocols for the SLC, SET Handset and SET R-UIM/UICC/SIM/USIM for supporting the various mutual authentication methods.

Where the GBA-based method is supported, the BSF stores user security settings (USS) associated with the H-SLP applications. When the H-SLP requests the USS, the BSF must include a SET user identity (e.g. IMPI, IMSI or MSISDN) in the USS.

6.1.1.4 Techniques for Minimizing the TLS Handshake Workload

The procedures in this section will minimize the workload associated with establishing TLS sessions between the H-SLC and SET. Where there is a conflict with [TLS] or [TLS 1.2], [TLS] or [TLS 1.2] takes precedence.

If a SET and H-SLC are communicating SUPL messages associated with more than one SUPL sessions simultaneously, then the SET and H-SLC SHOULD use a single TLS session to secure these messages; that is, the SET and H-SLC SHOULD NOT establish distinct TLS sessions if SUPL sessions are simultaneous.

If the SET and H-SLC establish a TLS session, then the H-SLC MAY allow the session to be resumed using the abbreviated handshake shown in Figure 2 of [TLS] and [TLS 1.2]. The advantage of resuming a TLS session is that resuming a TLS session based on server certificates does not require the public-key operations: only symmetric cryptographic algorithms are required (which require significantly less processing).

NOTE: The H-SLC allows the session to be resumed by allocating a TLS SessionID as described in [TLS] and [TLS 1.2].

NOTE: There is no advantage to resuming a TLS-PSK session (as used for GBA and SEK-based authentication), since the same computations are performed. However, a H-SLP may still allow resuming a TLS-PSK session.

NOTE: A SET indicates the choice to resume a TLS session by including the TLS SessionID (of the TLS session to be resumed) in the TLS SessionID parameter in the ClientHello message of the TLS Handshake. If the SET does not wish to resume a TLS session, then the SET sends the TLS ClientHello message without including the TLS SessionID, in which case the full handshake will be performed. If the TLS SessionID parameter is present in the TLS ClientHello message, the H-SLC then chooses whether or not to resume the TLS session. If no SessionID parameter is present in the TLS ClientHello message, then the H-SLC cannot associate the TLS handshake with a previous TLS Session, so the TLS handshake establishes a completely fresh TLS session using a full handshake. The details are specified in [TLS] and [TLS 1.2].

The SET chooses whether or not to resume a TLS session, using the following guidelines.

- The SET MUST NOT resume a TLS session if the underlying credentials (Ks(_ext)_NAF or H-SLC certificate or SEK) are expired.
- The SET MAY choose to not resume a TLS session earlier than the expiry of the underlying credentials, if desired.
- The SET MUST NOT resume a session that was established prior to power-up or detection of a new R-UIM/ SIM/USIM.

The H-SLC chooses whether or not to resume a TLS session, using the following guidelines.

- The H-SLC MUST NOT resume a TLS session if the underlying credentials (Ks(_ext)_NAF or H-SLC certificate or SEK) are expired.
- The H-SLC MAY choose to not resume a TLS session earlier than the expiry of the underlying credentials if desired.

NOTE: Each H-SLC must decide for itself whether or not to allow abbreviated handshakes, and this decision can even be made on a SET-by-SET basis. The H-SLC is taking a small risk when it accepts to resume an existing TLS session. This risk is the possibility of a "naughty" SET distributing the master_secret (established during a full TLS handshake), so that others may resume that TLS session, thus allowing multiple SETs to obtain service that will be charged to a single SET. The "naughty" SET could be doing this without the knowledge of the SET owner (for example, a malicious code could be at fault). Note that the loss can be easily limited: if a H-SLC detects (or suspects) that such abuse is occurring, then the H-SLC can easily (a) end the TLS sessions using that master_secret, (b) identify the "naughty" SET and (c) re-authenticate the "naughty" SET using full handshake to allow the user to continue to have service if required. In summary, the benefit of resuming sessions (in terms of reduced computation) for the ACA-based method and SLC-only method is thought to exceed the risk of attack

6.1.2 Key Management for SUPL Authentication

The SUPL Authentication model requires shared secret keys between the H-SLP and the SET, preferably bound to either a removable token such as a R-UIM/SIM/USIM or a CDMA UIM integrated into the handset.

6.1.2.1 Deployments Supporting GBA

In the case of deployments supporting GBA [3GPP 33.220], the shared keys are established as follows:

- When the SLP requests key material form the BSF (for securing IP communication and for protecting SUPL INIT), the SLP MUST also request the USS (User security settings). The USS MUST include a permanent user identity (e.g. IMPI, IMSI or MSISDN).
- For securing IP communication between the SET and SLP, the SET and the SLP MUST derive a shared secret key and operate according to TLS-PSK using GBA [3GPP 33.220]. The SLP MUST have well defined domain name SLP_Address_FQDN designating the SLP, e.g., slp.operator.com. The GBA Ua security protocol identifier that shall be used for TLS-PSK is defined in OMNA Registry [OMNA]. The SLP MUST confirm that the permanent user identity provided by the BSF corresponds to the SET identity in SUPL messages received by the SLP over the corresponding secured connection.

- The key management for non-proxy communication between the SET and an authorized SPC is outlined in section 6.1.2.4.
- For MAC protection of SUPL INIT, keys are derived according to GBA [3GPP 33.220]. The GBA Ua security protocol identifier that shall be used for SUPL INT protection is defined in OMNA Registry [OMNA]. The keyIdentifier of the basicMAC included in the SUPL INIT message MUST be the B-TID of the Ks from which the Ks_NAF is generated. **NOTE**: The H-SLP request for SUPL INIT protection keys from the BSF would typically occur simultaneously with the H-SLP request for the keys securing IP communication.
- The SET MUST ensure that it is always provisioned with a valid Ks. If no valid Ks is present then the SET MUST initiate the GBA Bootstrapping procedure to provision Ks. A new Ks MUST be established each time a new UICC (USIM/SIM/R-UIM) is detected by the SET. Additionally, the SET MUST establish new shared keys when the Ks_NAFs lifetime (set by the Home Network operator) expires.

6.1.2.2 Deployments Supporting SEK

In the case of deployments supporting SEK, the shared keys are established as follows:

- For securing IP communication between the SET and SLP, the SET and SLP MUST derive a shared secret key and confirm that the permanent user identity provided by the WiMAX AAA server corresponds to the SET identity in the SUPL messages received by the SLP over the corresponding secured connection. The shared keys are derived in the following way:
    - SEK = the 16 most significant (leftmost) octets of HMAC-SHA256(LSK, "slp.operator.com") where 'operator.com' is the FQDN of the WIMAX operator and LSK is derived as specified in WiMAX Network Protocols and Architecture for Location Based Services.
    - SEK will inherit the Location Key Identifier (LSK-ID) (as defined in WiMAX Network Protocols and Architecture for Location Based Services) associated with the LSK and the key identity will be used as the B-TID for WiMAX deployments.
- For MAC integrity protection of SUPL INIT, keys are derived the following way:
    - SEK_MAC = the 16 most significant (leftmost) octets of HMAC-SHA256(LSK, "mac.slp.operator.com") where 'operator.com' is the FQDN of the SLP operator and LSK is derived as specified in WiMAX Network Protocols and Architecture for Location Based Services.
    - The keyIdentifier of the basicMAC included in the SUPL INIT message MUST be the B-TID of the LSK from which the SEK_MAC is generated. **NOTE**: The H-SLP request for SUPL INIT protection keys from the WiMAX AAA would typically occur simultaneously with the H-SLP request for the keys securing IP communication.

The SET MUST ensure that it is always provided with a valid SEK. If no valid SEK is present then the SET MUST derive the SEK as specified above. Additionally, the SET MUST establish new shared keys when the lifetime of the LSK expires. The interface between the SLP and the WiMAX AAA server is out of scope of SUPL 2.0.

6.1.2.3 Deployments not Supporting GBA or SEK

In the case of deployments that do not support GBA [3GPP 33.220] or SEK, the shared keys are established as follows:

- For securing IP communication between the SET and SLP, the SET and SLP MUST use TLS-RSA [TLS] [TLS 1.2] with a server-certificate authenticating the SLP. SET authentication (which binds the resulting shared secret keys to either the removable or integrated token discussed above) is described in section 6.1.4 for non-emergency cases and sections 6.1.5.3 and 6.1.5.4 for emergency cases.
- The key management for non-proxy communication between the SET and an authorized SPC is outlined in section 6.1.2.4.
- MAC protection of SUPL INIT is not supported in these cases.

6.1.2.4 Non-Proxy Communication

If an SLC authorizes a non-proxy session between the SET and a SPC, then the SET and SPC obtain a shared key as follows:

- The SLC generates a fresh key and passes this to the SPC (in some cases, via a visited SLC).

- The SLC sends the key to the SET over an existing secure TLS session established between the SET and SLC. This TLS session would be established using one of the key management schemes discussed in sections 6.1.2.1 and 6.1.2.2.

6.1.3 TLS Handshake and Negotiation of SET-SLC Mutual-Authentication Method

The SET and SLC need to agree on a mutually-supported authentication method to be applied.

For 3GPP SETs, the negotiation of authentication method is incorporated into the relevant GBA specifications (see [3GPP 33.220]), and is outside of scope of this document. 3GPP2 SETs SHALL use the same method for negotiation of the authentication method (see [3GPP 33.220]), with the references "TS 24.109 [18]" "TS 33.220 [3]" replaced by [3GPP2 S.S0109].

6.1.3.1 Regarding negotiating a Mutual-Authentication Method (Informative)

When establishing a TLS connection to the H-SLC, the SET first attempts to establish a connection using the mutually-supported authentication mechanism with highest preference, according to the following order of preference:

- PSK-based methods: GBA or SEK-based method first preference,
- Server Certificate methods: second preference (from the SET's perspective there is no difference between the ACA-based method and the SLC-only method).

If there is no mutually-supported authentication method, then the SET shall be unable to perform SUPL session.

A SET that supports PSK based methods may be unable to use the GBA or SEK-based method at a given point in time due to a BSF or WiMAX AAA experiencing problems. Therefore, an attempt by the SET to establish authentication using GBA or SEK does not guarantee that the SET shall be able to establish GBA or SEK-based keys.

Consequently, the SET may not always be able to use the mutually-supported authentication mechanism with highest preference. The SET may have to revert to a less preferable mutually-supported authentication mechanism if available.

If only PSK based methods are indicated (in the H-SLC Certificate) as supported by the H-SLC, and the bootstrapping fails, then the SET may want to wait a little while before re-attempting the TLS handshake, in order to give the appropriate entities a chance to get back on-line.

If the H-SLC supports only GBA or SEK, then SUPL 2.0 can only be used by subscribers of carriers that have deployed GBA or SEK. If the H-SLC supports only ACA, then SUPL 2.0 can only be used in circumstances discussed in detail in section 6.1.4. Note that in such a case, if the SET communicates via an alterative bearer (such as wireless LAN) for which the H-SLC cannot obtain IP binding, then the H-SLC will be unable to authenticate the SET.

If the E-SLC supports only ACA, then there are caveats on SET authentication, as discussed in detail in sections 6.1.5.3 and 6.1.5.4.

6.1.3.2 Principles for authentication and key re-negotiation for WiMAX SET and SLC (Informative)

The key re-negotiation can happen in two ways:

1. when the Location Rootkey (as defined in WiMAX Network Protocols and Architecture for Location Based Services) expires the SET automatically re-authenticates itself with the wimax network and the SUPL associated root keys will be re-generated by the SET, or
2. SLC notices that SEK or Location Rootkey (as defined in WiMAX Network Protocols and Architecture for Location Based Services) has expired and it will request a new key from the WiMAX AAA-server

6.1.3.2.1 Authentication procedure

In WiMAX deployments, the PSK TLS [RFC 4279] handshake shall be used with SEK as follows:

- the ClientHello message shall contain one or more PSK-based ciphersuites;
- the ClientHello message shall contain the server_name TLS extension as specified in [RFC 3546] and it shall contain the hostname of the SLC;

- the ServerHello message shall contain a PSK-based ciphersuite selected by the SLC;
- the ServerKeyExchange shall be sent by the server and it shall contain the psk_identity_hint field and it shall contain the static string "SUPL WIMAX bootstrapping"
- the ClientKeyExchange shall contain the psk_identity field and it shall contain a prefix "SUPL WIMAX bootstrapping", a separator character ";" and the current B-TID as specified in section 6.1.2.2;
- the SET shall derive the TLS premaster secret from the SLC specific key material i.e. SEK as specified in [RFC 4279].

6.1.3.2.2 Authentication failures

Authentication failures are handled as they are described in [TLS], [TLS 1.2] and in [RFC 4279].

6.1.3.2.3 Bootstrapping required indication

During TLS handshake, the SLC shall indicate to the SET that the SEK key is required by sending a ServerHello message containing a PSK-based ciphersuite, and a ServerKeyExchange message containing the psk_identity_hint field, which contains a static string "SUPL WIMAX bootstrapping". If the SET does not have a valid SEK this shall trigger the SET to derive a new SEK as defined in section 6.1.2.2.

6.1.3.2.4 Bootstrapping renegotiation indication

During usage of TLS session, the SLC shall indicate to the SET that SEK has expired by sending close_notify alert message to the SET. If the SET attempts to resume the old TLS session by sending a ClientHello message containing the old session ID. The SLC shall refuse to use the old session ID by sending a ServerHello message with a new session ID. This will indicate to the SET that the SEK it used has expired.

During TLS handshake, the SLC shall indicate to the SET that the SEK has expired by sending handshake_failure message as a response to the finished message sent by the SET. This will indicate to the SET that the SEK it used has expired.

6.1.4 Alternative Client Authentication (ACA) Mechanisms

NOTE: Throughout this section, SET_ID refers to either the MSISDN (if the SET is on a 3GPP bearer network) or one of the MDN, MIN or IMSI (if the SET is on a 3GPP2 bearer network).

Section 6.1.3 outlines the circumstances under which the ACA-based method may be selected by the SLC. If the SLP selects the ACA-method during the TLS handshake, then an SET_ID/IP Address Mapping based client authentication SHALL be used by the SLPs to authenticate the SET. The rest of this section describes the details of this mechanism, known as the Alternative Client Authentication mechanism. If an SLP implements the Alternative Client Authentication mechanism, then the SLP is recommended to implement the method using PSK-TLS with GBA as well.

Section 6.1.1.3 describes which entities must support the ACA-based method, and the algorithms that must be supported by an entity that supports ACA-based method. For informative purposes, this information is repeated here:

- A bearer network may support the ACA-based method. A bearer network must support the ACA-based method if a H-SLC wishes to support the ACA-based method for the bearer network's subscribers.
- An SLC MAY support the ACA-based method.
- GSM/UMTS and CDMA SET handsets MUST support the ACA-based method.
- The ACA-based method does not involve the SET UICC/UIM/SIM/USIM.
- The ACA-based method does not involve SPC entities.

SETs that support Alternative Client Authentication MUST also support TLS 1.1, and MAY support TLS 1.2, with certificate-based server (SLP) authentication. In addition, the SET MUST be provisioned with a root certificate enabling it to verify SLP server certificates. As various different methods exist for provisioning of root certificates to SETs no particular mechanism is defined by this specification. SUPL operators need to ensure that when TLS 1.1 or TLS 1.2 is used for Alternative Client Authentication the relevant root certificates exist in the SET.

SLPs that support Alternative Client Authentication MUST support TLS 1.1, MAY support TLS 1.2, and MUST have a valid TLS Server Certificate, which can be verified by the SETs that implement Alternative Client Authentication.

The Alternative Client Authentication (ACA) mechanism is a mechanism where the H-SLP can check the binding of the SET's IP address to the SET_ID assigned to the SET. If the ACA mechanism is implemented, then the H-SLP MUST be able

to map the source IP address of a SUPL message received from the SET to the SET_ID used by the SLP to address the SET. In order for an SLP to use the ACA mechanism, the bearer network MUST prevent IP Address Spoofing at the bearer level. A successful mapping between the source IP address and the SET's SET_ID would imply that the SET is securely identified (i.e., authenticated) on the bearer network. This solution does not require any specific client (SET) authentication implementation on the SET but requires the SLP to support acquiring the correct source IP address for a particular SET_ID from the bearer.

3GPP-Bearer-Specific issues: The acquisition of the source IP address will not be possible in all cases – e.g. for GPRS roaming access using a GGSN in the visited rather than home network. Therefore, the alternative client authentication mechanism should only be relied on when the home network assigns the source IP address or has access to it – e.g. as applies for GPRS access when the SET is required to use a GGSN in the home network.

3GPP2-Bearer-Specific issues: The acquisition of the source IP address will not be possible in all cases – e.g. for roaming HRPD access using simple IP or MIP access within the visited network. Therefore, the alternative client authentication mechanism should only be relied on when the home network assigns the source IP address or has access to it – e.g. as applies for HRPD access when the SET is required to use MIP to an HA in the home network.

Section 6.1.4.1 describes how this mechanism is used for client authentication in SUPL 2.0.

In the case that UDP/IP is used to transfer a SUPL INIT, the H-SLP SHALL first verify the IP address by querying the bearer network for the SET IP address using the SET_ID or by querying the bearer network for the SET_ID using the IP address.

6.1.4.1 ACA Procedures

Network-Initiated Scenarios: If, after receiving a SUPL INIT message from the H-SLP (and after applying the appropriate security mechanisms and notification/verification as described elsewhere in this document), the SET is authorized to continue with the corresponding SUPL sessions, then an existing, open mutually-authenticated TLS session SHOULD be used, or a previous resumable TLS session MAY be resumed as discussed in section 6.1.1.4. If there is no open TLS session, or the SET or H-SLP choose not to resume a session, then the SET and H-SLP require a fresh TLS session, and the SET and H-SLP perform the appropriate steps as described in section 6.1.3 for negotiating a SET-SLC authentication method.

The following steps are used by the H-SLP when the Alternative Client Authentication Mechanism is to be applied for authenticating the SET in a Network-initiated scenario:

1. Note that the SUPL INIT message was sent in response to an MLP request that supplied a SET_ID. The H-SLP assigns a SLP Session ID for the MLP request and sends a SUPL INIT. The H-SLP associates the response from the SET with the request from the MLP using the SLP Session ID. However, the H-SLP must first verify that the responding SET corresponds to the correct SET_ID. The remaining steps describe this authentication process.
2. The SET establishes a TLS 1.1 or TLS 1.2 session with the H-SLP. The SET MUST check that the TLS server certificate presented by the H-SLP is bound to the FQDN of the H-SLP configured in the SET.
3. The H-SLP determines if the SLP Session ID in the first SUPL message from the SET (in response to SUPL INIT) corresponds to a currently valid SLP Session ID assigned by the H-SLP. If the SLP Session ID in the first SUPL message does not correspond to a valid SLP Session ID, then the H-SLP ends the SUPL Session with the appropriate message. Otherwise, the H-SLP notes the corresponding SET ID.
4. Prior to responding to the first SUPL Message from the SET (SUPL POS INIT, SUPL START, SUPL AUTH REQUEST, SUPL TRIGGERED START, SUPL REPORT or SUPL END), the H-SLP MUST verify the SET_ID of the SET. There are two methods for achieving this.
    a. Requesting the SET_ID.
        i. The H-SLP queries the underlying bearer network to find out the current SET_ID using the source IP address used by the SET.
            1. If a valid SET_ID is returned from the bearer for the source IP address of the first SUPL message sent by the SET then the H-SLP checks that the returned SET_ID is internally associated with the correct SET_ID (see Step 3). If this check fails, then the H-SLP ends the SUPL session with the appropriate message. Otherwise, the SET is considered authentic, and the H-SLP continues with the SUPL session.
            2. If a valid SET_ID cannot be found, then the H-SLP MUST terminate the SUPL session with the relevant SUPL error messages.

b. Requesting the IP address.

i. The H-SLP queries the underlying bearer network to find out the source IP address being used by the SET associated with this SET_ID (see Step 3).

1. If the bearer network returns an IP address, then the H-SLP checks that this IP address corresponds to the Source IP address of the first SUPL message. If this check fails, then the H-SLP ends the SUPL session with the appropriate SUPL message. Otherwise, the SET is considered authentic and the H-SLP continues with the SUPL session.

2. If an IP address cannot be found, then the H-SLP MUST terminate the SUPL session with the relevant SUPL error messages.

NOTE: a bearer network might support only one of the two types of query (requesting IP address or requesting SET_ID) in Step 4 for obtaining an SET_ID/IP address binding. The H-SLP is responsible for conforming with the method supported by the bearer network.

SET-Initiated Scenarios: When the SET wishes to initiate a SUPL session, an existing, open mutually-authenticated TLS session SHOULD be used, or a previous resumable TLS session MAY be resumed as discussed in section 6.1.1.4. If there is no open TLS session, or the SET or H-SLP chooses not to resume a session, then the SET and H-SLP require a fresh TLS session, and the SET and H-SLP perform the appropriate steps as described in section 6.1.3 for negotiating a SET-SLC authentication method.

The following steps are used by the H-SLP when the Alternative Client Authentication Mechanism is to be applied for authenticating the SET in a SET-initiated scenario.

1. The SET establishes a TLS 1.1 or TLS 1.2 session with the H-SLP. The SET MUST check that the TLS server certificate presented by the H-SLP is bound to the FQDN of the H-SLP configured in the SET.
2. Prior to responding to the first SUPL Message (e.g. SUPL START, SUPL TRIGGERED START), the H-SLP MUST verify the SET_ID of the SET. There are two methods for achieving this.

a. Requesting the SET_ID.

i. The H-SLP queries the underlying bearer network to find out the current SET_ID using the source IP address used by the SET.

1. If a valid SET_ID is returned from the bearer for the source IP address of the first SUPL message sent by the SET then the H-SLP checks that the returned SET_ID is same as provided by the SET. If this check fails, then the H-SLP ends the SUPL session with the appropriate message. Otherwise, the SET is considered authentic, and the H-SLP continues with the SUPL session.

2. If a valid SET_ID cannot be found the H-SLP MUST terminate the SUPL session with the relevant SUPL error messages.

b. Requesting the IP address.

i. The H-SLP queries the underlying bearer network to find out the source IP address being used by the SET associated with this SET_ID.

1. If the bearer network returns an IP address, then the H-SLP checks that this IP address corresponds to the Source IP address of the first SUPL message. If this check fails, then the H-SLP ends the SUPL session with the appropriate message. Otherwise, the SET is considered authentic and the H-SLP continues with the SUPL session.

2. If an IP address cannot be found the H-SLP MUST terminate the SUPL session with the relevant SUPL error messages.

NOTE: In both the H-SLP-Initiated and SET-Initiated scenarios, the H-SLP can re-authenticate the SET by sending an appropriate query to the bearer network to bind the SET_ID to the source IP address currently in use. There are various circumstances where this could be useful, for example: (A) if the IP address of the SET changes during a TLS session, then the H-SLP can send the appropriate query to the bearer network to ensure that the SET_ID is associated with the new IP address; (B) when resuming a TLS session, the H-SLP can re-use a previous TLS session as discussed in section

6.1.1.4, thereby saving computation, and simply send the appropriate query to the bearer network to authenticate the SET. Note that re-authenticating the SET in this manner does not involve interaction with the SET itself..

6.1.5 Authentication Mechanisms applicable to an E-SLP

NOTE: emergency SUPL sessions are always Network Initiated.

Support for this feature will be dictated by the appropriate emergency services regulatory bodies.

For the duration of an emergency SUPL session on a SET, all SUPL resources on the SET MUST be made available for that emergency session. Consequently:

- When a SET begins an emergency SUPL session, any SUPL communication related to non-emergency sessions MUST be terminated immediately by the SET. If non-emergency SUPL INIT messages are being processed by the SET at this time (e.g. having MAC verified or obtaining user permission), then those processes SHALL be aborted and the SUPL INIT messages SHALL be discarded.
- If a SET receives non-emergency SUPL INIT message(s) while in emergency SUPL session, these SUPL INIT message(s) SHALL be discarded.

6.1.5.1 E-SLP FQDN

The FQDN of the E-SLP shall be:

1. The FQDN provided to the SET as E-SLP address in the SUPL INIT. The E-SLP FQDN shall have format "e-slp.xxx.xxx.xxx.xxx.xxx" where "xxx" can be any valid string.
2. If FQDN is not provided in SUPL INIT, the provisioned H-SLP address shall be used if the SET is in its home PLMN (or its equivalent). If the SET is not in its home PLMN (or its equivalent), then the SET shall skip this step and move to step 3. If a SET is unable to determine whether it is or is not in its home PLMN, it SHALL directly proceed to step 3.
3. If FQDN is not available as per 1 or 2 above, the FQDN shall be defaulted to one of the three alternatives below:
   - (if connected to a 3GPP bearer network) "e-slp.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org" if no FQDN is explicitly provided. In this case, the MCC and MNC correspond to the serving 3GPP network as defined in [3GPP 23.167].
   - (if connected to a 3GPP2 bearer network) "e-slp.mnc<MNC>.mcc<MCC>.pub.3gpp2network.org" if no FQDN is explicitly provided. In this case, the MCC and MNC correspond to the serving 3GPP2 network as defined in [3GPP2 X.S0049-0].
   - (if connected to a WiMAX bearer network) "e-slp.operator.com" where operator.com is the FQDN of the H-SLP operator.

6.1.5.2 Processing Emergency SUPL INIT messages

SET based integrity verification and message origin authentication of SUPL INIT messages is not used by an E-SLP. Thus, the MAC field in an emergency SUPL INIT MUST NOT be populated.

During an emergency call, a SET SHALL NOT apply end-to-end protection of emergency SUPL INIT messages.

Some protection is offered by the use of E-SLP whitelists. The E-SLP whitelist is based on the current position estimate of the SET (such as CellID and/or NetworkID). The E-SLP whitelist is used by a SET to determine the order in which the SET should process received emergency SUPL INIT messages: the E-SLP whitelist SHALL NOT be used for discarding emergency SUPL INIT messages.

6.1.5.2.1 E-SLP Whitelist

If an emergency SUPL INIT message is received over a channel that is not secured end-to-end (such as SMS or OMA Push) then the emergency SUPL INIT message may be fake or altered. The remainder of this section describes the security countermeasures used to ensure that the SET is able to contact the genuine E-SLP server as soon as possible.

NOTE: regulatory requirements will dictate the conditions under which the SET should accept and process emergency SUPL INIT messages. For example, in many cases, the regulatory requirements only require the SET to accept and process emergency SUPL INIT messages if the SET is currently engaged in an emergency call. Consequently, the conditions (under which the SET should accept and process emergency SUPL INIT messages) are outside the scope of this document.

When a SET receives an emergency SUPL INIT message, the SET MUST first verify that the conditions (under which the SET should accept emergency SUPL INIT messages) are currently satisfied. If the conditions are not satisfied, then the SET SHALL ignore the SUPL INIT message. The description from hereon assumes that the conditions were satisfied when the SET received the emergency SUPL INIT message.

NOTE: Attackers could send multiple (fake) emergency messages to the SET at the same time that the SET is expecting a genuine emergency SUPL INIT message. There may be cases where the SET could not be told (in advance) from which Emergency SLP to expect the emergency SUPL INIT message. This attack is motivation for the following procedures.

For the period of time that the "accept and process" conditions are satisfied, the SET MUST NOT delete received emergency SUPL INIT messages even if the emergency SUPL INIT message lists an un-expected address for the E-SLP. Once the SET determines that the conditions are no longer satisfied (for example, once the correct E-SLP has been contacted, or sufficient time has passed after the emergency call) then the SET MUST silently discard any received emergency SUPL INIT messages.

If the SET receives, accepts and processes a fake emergency SUPL INIT message (while the "accept and process" conditions are still satisfied), then the SET might not receive an indication that emergency SUPL INIT message is fake until after attempting to contact the E-SLP indicated in the emergency SUPL INIT message. The indication occurs when the E-SLP rejects the SUPL session. This process is not immediate, so it may be necessary for the SET to queue emergency SUPL INIT messages if it receives more than one emergency SUPL INIT message.

An E-SLP whitelist contains a list of E-SLP FQDNs (see section 6.1.5.1) that the SET could expect to receive emergency SUPL INIT messages from. The SET uses the E-SLP whitelist to ensure that emergency SUPL INIT messages including an E-SLP FQDN that is on the whitelist SHOULD be processed before emergency SUPL INIT messages including an E-SLP FQDN that is not on the whitelist.

Example: Emergency SUPL INIT messages containing an E-SLP FQDN on the whitelist are pushed forward on the emergency SUPL INIT queue to ensure that the message is processed before emergency SUPL INIT messages containing an E-SLP FQDN that is not on the whitelist. E-SLP Whitelisting should be the first criteria for ordering the Emergency SUPL INIT queue. The second criteria is the arrival time, using the first-in first-out principle:

- If the SET has a current E-SLP whitelist for the SET's current locality, then the SET uses both criteria to order the queue.
- If the SET does not have a current E-SLP whitelist for the SET's current locality, then the SET uses the first-in-first-out principle to order the queue.

6.1.5.2.2 Obtaining an E-SLP whitelist

SUPL 2.0 does not define how the SET obtaines and maintains an E-SLP whitelist. This is considered out of scope for SUPL.

6.1.5.2.3 Procedures regarding Emergency SUPL INIT Messages

If an emergency SUPL INIT is received over a channel that is secured end-to-end (such as a secure SIP Push) then the emergency SUPL INIT message SHALL be processed immediately. The remaining considerations of this subsection are ignored in this case.

If an emergency SUPL INIT message is received over a channel that is not secured end-to-end (such as SMS or OMA Push), then the message is queued as in section 6.1.5.2.1. The SET works its way through the messages in the queue, applying the appropriate verification and notification before attempting to connect to the E-SLP to respond.

In responding to the SUPL INIT message, the SET shall establish a secure TLS session (See sections 6.1.5.3 and 6.1.5.4) with the associated E-SLP (see section 6.1.5.1), and one of the following takes place:

- If, after authenticating the SET (See section 6.1.5.3), the E-SLP cannot associate the SET with any outstanding SUPL sessions, then the E-SLP SHALL end the session. If the TLS Handshake is not yet complete, then the E-SLP SHOULD end the session using a TLS error message, in order to save un-necessary computation. If the TLS handshake is complete, then the E-SLP SHALL end the session using a SUPL error message indicating that the SET is not authorized. The SET SHALL interpret either form of error message as indication that the SUPL INIT message was fraudulent. The SET then processed to the next SUPL INIT message in order of priority in the queue.
- If, after authenticating the SET (See section 6.1.5.3), the E-SLP can associate the SET with an outstanding SUPL session, then the SET and E-SLP continue as normal.

The SET continues responding to emergency SUPL INIT messages until the genuine message is found. The SET MAY discard any new or queued SUPL INIT messages once the correct E-SLP has been identified. New or queued SUPL INIT messages from the correct E-SLP may still be processed.

The following two notes are suggestions that regulatory bodies may wish to consider.

NOTE: Once the correct E-SLP has been identified, then the SET should ensure that it remembers the FQDN of this correct E-SLP until the SUPL session successfully completes. If the TLS session with the E-SLP ends prematurely (for example, if there is a loss of data connectivity), the the SET should continue attempting to re-establish a TLS session with the E-SLP until the TLS session is re-established so that the SUPL session can continue to successful completion. In some circumstances, it is conceivable that the SET re-establishes the TLS session several times. If the SET is not having success at restablishing the TLS session, the SET should continue attempting regardless: since this is an emergency situation, the benefit of success outweighs the cost of a flat battery.

NOTE: If the E-SLP loses contact with SET after authentication, but prior to successful completion of the SUPL session, then the E-SLP SHOULD leave the SUPL session open with the hope that the SET is able to re-establish contact and complete the SUPL session.

6.1.5.3 Mutual Authentication and Registered SETs

NOTE: the mutual-authentication methods that may be supported by an E-SLP are specified in section 6.1.1.3. The SET and E-SLP negotiate the mutual-authentication method during the TLS handshake, as specified in section 6.1.3.

GBA-Based Method: SETs and E-SLPs MAY perform proxy mode authentication using PSK-TLS with GBA as described in section 6.1.3 with the E-SLP acting as the NAF. The FQDN of the E-SLP is discussed in section 6.1.5.1. The Ks_NAF obtained by an E-SLP for a particular SET may be retained in association with the SET identity (e.g. IMSI, MSISDN) for the lifetime set by the home network operator.

SEK Based Method: SET and E-SLPs MAY perform proxy mode authentication using PSK-TLS with SEK as described in section 6.1.3 with the E-SLP acting in the similar fashion as H-SLP. The FQDN of the E-SLP is discussed in section 6.1.5.1. The SEK obtained by an E-SLP for a particular SET may be retained in association with the SET identity (e.g. WiMAX user ID) for the lifetime set by the home network operator.

ACA-Based Method: For SUPL 2.0 implementations where GBA or SEK with PSK-TLS IS NOT supported in both the SET and in the E-SLP, the alternative client authentication mechanism defined in section 6.1.4 SHALL be supported with the following differences. The E-SLP SHALL authenticate the SET by binding the IP address used by the SET with the IP address for the SET provided to the E-SLP by the serving network – e.g. by the LRF or E-CSCF in a GSM/UMTS network [3GPP 23.167], or using [3GPP2 X.S0049-0] in a CDMA network. Since the SET IP address is used to initiate any emergency VoIP call and can be verified by the serving network before SUPL is invoked, it may be considered to be reliable by the E-SLP. In the case of an emergency call initiated in circuit mode, the SET IP address may not be known to the serving network (e.g. may be assigned by the home network) in which case the E-SLP cannot be provided with the IP address by the serving network and cannot verify the IP address when received later from the SET. In this case, the E-SLP can only authenticate the SET weakly using (e.g.) the session ID and the received hash of the SUPL INIT (this SET-SLC authentication is the SLC-only method, since only the SLC is properly authenticated).

The SET SHALL authenticate the E-SLP using a root certificate of the E-SLP contained in the SET and the FQDN of the E-SLP as defined in section 6.1.5.1. In order to use the alternative client authentication mechanism, the serving bearer network MUST prevent IP Address Spoofing at the bearer level.

6.1.5.4 Authentication and Unregistered SETs

If a SET makes an emergency services call but is not registered in and authenticated by the serving 3GPP or 3GPP2 bearer network (e.g. it contains no UICC or UIM), then the SET MAY establish a secure IP connection to an E-SLP using the ACA method or SLC-only method. If the ACA mechanism can be supported by the bearer network for authenticating an unregistered SET, then the E-SLP SHOULD apply the ACA mechanism. Otherwise the E-SLP can only authenticate the SET weakly using (e.g.) the session ID and the received hash of the SUPL INIT (this SET-SLC authentication is the SLC-only method, since only the SLC is properly authenticated).

6.1.5.5 Integrity Protection of SUPL INIT

If the E-SLP is able to authenticate the SET as discussed in section 6.1.5.3, and the E-SLP can associate the SET with an outstanding SUPL sessions, then the E-SLP checks if the SUPL INIT message was altered. If the E-SLP detects that the SUPL INIT message was altered (for example, if a SUPL AUTH REQ message was received when Proxy mode was

indicated, or if SLP Session ID is wrong or if VER fails verification as described in section 6.1.6.1) then the E-SLP MUST send SUPL INIT to the SET over the TLS session to ensure that the SET is provided with the correct parameters. In response, the SET will discard the SUPL session initiated using the SUPL INIT it originally received, and the SET shall begin a new SUPL session using the SUPL INIT received over the TLS session. The SET shall then process that SUPL INIT message immediately (that is, the SET does not evaluate the priority using an E-SLP whitelist), performing the appropriate actions for notification and verification, and provided the User does not reject the session, the SET then sends the appropriate message (SUPL POS INIT or SUPL AUTH REQ) to the E-SLC to continue the session.

The ability to resend SUPL INIT is only intended for emergency sessions. In non-emergency sessions, if alteration of SUPL INIT is detected, then the H-SLP shall end the SUPL session using SUPL END, as specified in the non-emergency call flows.

6.1.6 Processing of the SUPL INIT Messages

As network initiated SUPL sessions are triggered by a SUPL INIT message, it is essential to protect SUPL INIT messages against masquerading and (in some cases) against re-play attacks.

SUPL 2.0 specifies the following protection for SUPL INIT messages:

- Network-based security, in which the SLC shall perform checks to ensure authentication (section 6.1.6.1) and replay protection (section 6.1.6.2) of SUPL INIT messages. This verification occurs after the SET has processed the content of the SUPL INIT message and established a secure TLS session with the SLC for the purposes of performing the SUPL session.
- End-to-End security, in which the H-SLC may apply a combination of encryption, integrity protection and replay protection to the SUPL INIT message and the SET applies the corresponding combination of decryption, integrity verification and replay detection. The SET applies these security measures before processing the content of the SUPL INIT message. This security is applied only to non-emergency SUPL INIT messages.

Network-based security is mandatory, while End-to-End security is optional.

6.1.6.1 Network-Based Authentication of the SUPL INIT Message

The SLP always performs network verification of the integrity of the SUPL INIT message. The first message sent in response to the SUPL INIT message (that is, a SUPL POS INIT, SUPL AUTH REQ or SUPL TRIGGERED START message) MUST contain a verification field (VER). When the SLP receives the first message sent in response to the SUPL INIT message the SLP MUST check the received VER field against the corresponding value calculated over the transmitted SUPL INIT message. If this verification fails the SLP MUST terminate the session with the SUPL END message that contains status code ‘authSuplinitFailure’.

The value for the verification field MUST be calculated as follows:

- VER=H(SLP XOR opad, H(SLP XOR ipad, SUPL INIT))

where SLP is the FQDN of the SLP address. SHA-256 MUST be used as the hash (H) function, with opad and ipad as specified in [HMAC]. The output of the SHA-256 HASH function MUST be truncated to 64 bits, i.e., the function MUST be implemented as HMAC-SHA256-64. Note that the SLP address is not considered secret. The HMAC construct used here does not provide any data authentication but is only used as an alternative to a HASH function.

6.1.6.2 Network-Based Re-Play protection of SUPL INIT Message

For Network Initiated cases, protection against re-play attacks MUST be provided by the SLPs. SLPs MUST ensure that no SUPL messages are accepted from an authenticated SET unless a previous, non-expired SUPL INIT message has been sent with an “SLP Session Id” that corresponds to the one received inside the SUPL message. SLPs MUST also ensure that the type of SUPL message (e.g. SUPL POS INIT, SUPL AUTH REQ, SUPL TRIGGERED START) agrees with the parameters sent in the SUPL INIT message. Implementations MUST ensure that an “SLP Session Id” is correctly associated with the SET User ID (e.g., MSISDN, WiMAX user ID or MDN) that has been authenticated.

If the SET User authentication is performed using the Alternative Client Authentication method described in this document then a mapping between the source IP address of the response from the SET (SUPL POS INIT, SUPL AUTH REQ or SUPL TRIGGERED START) and the MSISDN or MDN of the SET User is already established and this MSISDN or MDN MUST be used as the authenticated MSISDN or MDN.

Discarding of an erroneous SUPL POS INIT, SUPL AUTH REQ or SUPL TRIGGERED START MUST NOT generate a chargeable event for the SET.

For Non-Proxy Network Initiated cases, SLPs MUST only create a chargeable event after receiving the confirmation from the SPC for the successful completion of the SUPL positioning.

6.1.6.3 End-to-End Protection of SUPL INIT Messages

NOTE: End-to-End Protection of SUPL INIT Messages applies only to non-emergency SUPL INIT messages.

Two levels of end-to-end SUPL INIT protection are provided for in this specification: Null and Basic-

- Null SUPL INIT protection provides no end-to-end integrity protection, no end-to-end replay protection and no confidentiality protection. The procedures for Null SUPL INIT protection are described in section 6.1.6.5.
- Basic SUPL INIT protection provides end-to-end integrity protection and end-to-end replay protection using default algorithms. The procedures for Basic SUPL INIT protection are described in section 6.1.6.6.

The order of preference for the level of protection is as follows:

- Null SUPL INIT protection has least preference.
- Basic SUPL INIT protection has higher preference than Null SUPL INIT protection.

In a SUPL INIT message the Protection Level parameter (in the following table) is assigned according to the current level of protection.

NOTE: this specification has been written to allow for more advanced levels of protection to be added in the future revisions. This advanced protection could allow the negotiation of other ways for securing SUPL INIT (for example, allowing encryption and allowing the negotiation of algorithms). The Protection Level parameter is included to aid the SET in determining whether it might be able to parse the SUPL INIT message or not: the Protection Level parameter is required for extensibility.

A SUPL INIT message may have a Protector parameter present for including security parameters: the presence of a Protector parameter is specified in the following table.

Level of End-to-End SUPL INIT Protection	Description	Protector parameter present in SUPL INIT?
Null	No end-to-end protection	Optional
Basic	Integrity protection and replay protection using default algorithms	Mandatory

Table 4: SUPL INIT Protection Level parameter values and presence of the Protector parameter in SUPL INIT.

A SET or H-SLP that supports the ACA-based method MUST support Null SUPL INIT protection.

A SET or H-SLP that supports the PSK-based method MUST support Basic SUPL INIT protection procedures.

The SPC and E-SLC entities are not involved in currently defined SUPL INIT protection.

6.1.6.4 Negotiating the Level of SUPL INIT Protection

An informal description of how the SUPL INIT protection level is negotiated is as follows: The initial protection level is always Null SUPL INIT protection. In this state the SET handles all SUPL INIT messages, i.e. no messages are silently dropped. If a SUPL INIT message is parsed with a failure condition, the SET sends an error message to the SLP.

The SET must apply Null SUPL INIT protection when there is no valid SUPL_INIT_Root_Key (e.g. at power-up or when the lifetime of the SUPL_INIT_Root_Key has expired)..

When the SET connects to the H-SLP, the SET-SLC authentication (section 6.1.3) will indicate the support for GBA or SEK. If GBA or SEK is not supported this indicates that Null SUPL INIT protection shall be applied. If GBA or SEK is supported then Basic SUPL INIT protection applies and the B-TID exchanged in the PSK-TLS handshake corresponds to the Ks or SEK that can be used to derive SUPL_INIT_ROOT_KEY that will be used as a Ks_NAF in 3GPP and 3GPP2 deployments. This Ks_NAF or SEK and the associated B-TID are used in the Basic SUPL INIT protection until either:

1. the key expires, in which case the SET and H-SLP revert to Null SUPL INIT protection

2. the SET and H-SLP use the ACA-method, in which case the SET and H-SLP revert to Null SUPL INIT protection, or
3. the Set and H-SLP use GBA's or SEK's bootstrapping re-negotiation methods to establish TLS using a fresh B-TID, in which case the B-TID and corresponding Ks_NAF or SEK are now used for Basic SUPL INIT protection.

Note that this means that the protection level is renegotiated every time the SET sets up a fresh TLS connection to the H-SLP.

For Basic SUPL INIT protection, the replay protection counter in the SLP is reset to zero the first time a key is used and the SET removes all information about "played" SUPL INIT messages.

6.1.6.4.1 Negotiation from the H-SLP Perspective

If the most recent IP session with the SET was authenticated using the ACA method, then the H-SLP assigns Null SUPL INIT protection level for that SET.

Otherwise, if the H-SLP has a current B-TID and the associated key for the SET, then

- If the B-TID is for a key obtained using GBA, then the H-SLP assigns SUPL_INIT_ROOT_KEY to be the Ks_(int/ext_)NAF corresponding to the most recent B-TID and generated as follows
  - The FQDN SHALL be the H-SLP_FQDN
  - The GBA Ua security protocol identifier that shall be used for TLS-PSK protection is defined in OMNA Registry [OMNA].
- If the B-TID is for a key derived using the SEK-method, then the SUPL_INIT_ROOT_KEY is the SEK as defined in 6.1.2.2.
- Assuming no other SUPL INIT protection has been negotiated, then the H-SLP assigns the Basic SUPL INIT protection level for that SET.

If no other level of protection is assigned, then the H-SLP assigns Null SUPL INIT protection level for that SET.

The H-SLP applies the procedures (for processing SUPL INIT messages prior to delivery) corresponding to the currently assigned level of SUPL INIT protection. This includes assigning the appropriate value for the Protection Level parameter in SUPL INIT messages.

6.1.6.4.2 Negotiation from the SET Perspective

If the most recent IP session with the H-SLP was authenticated using the ACA method, then the SET assigns Null SUPL INIT protection level for that SET.

Otherwise, if the SET has established a TLS-PSK session (with the H-SLP) using GBA or SEK, then

- If the B-TID is for a key obtained using GBA, then the SET assigns SUPL_INIT_ROOT_KEY to be the Ks_(int/ext_)NAF corresponding to the most recent B-TID and generated as follows
  - The FQDN SHALL be the H-SLP_FQDN
  - The GBA Ua security protocol identifier that shall be used for TLS-PSK protection is defined in OMNA Registry [OMNA].
- If the B-TID is for a key derived using the SEK-method, then the SUPL_INIT_ROOT_KEY is the SEK as defined in 6.1.2.2.
- Assuming no other SUPL INIT protection has been negotiated, then the SET assigns the Basic SUPL INIT protection level.

If no other level of protection is assigned, then the SET assigns Null SUPL INIT protection level.

The SET applies the procedures (for processing received SUPL INIT messages) corresponding to the currently assigned level of SUPL INIT protection.

6.1.6.4.3 Exception procedures

If the SET determines that the SET-internal SUPL INIT protection parameters have become corrupted, then the SET must establish a TLS session with the H-SLP: if GBA authentication is used, then the SET must initiate GBA bootstrapping to

establish fresh keys; for SETs using the SEK method, the SET must initiate SEK bootstapping to enable fresh keys, as defined in 6.1.2.2.

If the H-SLP loses security context (for example, massive loss of data) then the SLP will have no means of initiating positioning activities. The context would be re-established when the Ks_NAF or SEK expires, or the SET connects to the H-SLP. To prevent this "block out window" the H-SLP should ensure that all SUPL INIT security context information is stored with sufficient redundancy to recover from such a scenario.

6.1.6.5 Specifications when Null Level of Protection is Assigned

There are no security procedures for the H-SLP that are specific to Null SUPL INIT protection.

When Null SUPL INIT protection is assigned and the SET receives a SUPL INIT message, then the SET applies the following procedure:

- If the Protection Level parameter is correct, then the SET considers the message to be authentic, and no security related processing is required.
    - Suppose the H-SLP and SET can support a higher level of protection, but the SET has not yet been in contact with the H-SLP since being powered up: in this case the SET will have Null SUPL INIT protection assigned. In the period of time until the SET contacts the H-SLP, the SET will consider any received SUPL INIT message (with the correct Protection Level parameter) to be authentic. When the SET first contacts the H-SLP (which may or may not be in response to a received SUPL INIT message), the SET and H-SLP will transition to a higher level of protection. Once the two entities transition to the higher level of protection, the SET can detect non-authenticatic SUPL INIT messages. In between when the SET is powered up and when the SET first contacts the H-SLP, there is a period of time when the SET could receive an non-authentic SUPL INIT message that is processed by the SET as if the SUPL INIT message where authentic. If the SET decides to proceed with the SUPL session associated with the non-authentication SUPL INIT message, then the SET will contact the H-SLP and establish a secure TLS session. The H-SLP will not allow the SUPL session since it was established using a non-authentic SUPL INIT message. If the SET and H-SLP support a higher level of protection, then this will be established at the same time and the SET will be able to detect non-authentic SUPL messages after this time. This means that, if the SET and H-SLP can support a higher level of protection, then there is a very small window of opportunity for the attacker to get the SET to accept a non-authentic SUPL INIT message, and the SET will only attempt to proceed with a SUPL session for at most one non-authentic SUPL INIT message.
- If the Protection Level parameter is incorrect, then the SET sends the appropriate error message to the H-SLP.
    - In the event that the Protection Levels at the H-SLP and SET lose synchronization, this procedure allows the SET and H-SLP to resynchronize on a common Protection Level.

6.1.6.6 Specifications for Basic SUPL INIT Protection Level

A SUPL INIT Protector for Basic SUPL INIT Protection includes the following parameters:

- Key Identifier: corresponds to the current B-TID.
- BasicReplayCounter: length = 2 octets.
- BasicMAC: length = 4 octets.

The BasicMAC parameter is generated as follows:

- BasicMAC = HMAC-SHA256-32(SUPL_INIT_Basic_IK, SUPL_INIT'), where
- SUPL_INIT_Basic_IK = HMAC-SHA256-128(SUPL_INIT_ROOT_KEY, "Basic IK"),
- For GBA-based deployments the SUPL_INIT_ROOT_KEY is the Ks_(int/ext_)NAF corresponding to the most recent B-TID and generated using the GBA Ua security protocol identifier for SUPL INIT protection as defined in OMNA Registry [OMNA],
- For SEK-based deployments the SUPL_INIT_ROOT_KEY is the SEK_MAC as defined in section 6.1.2.2.
- SUPL_INIT' corresponding to the SUPL INIT message with all parameters except MAC assigned, and with the MAC parameter set to all zeroes, and

- HMAC-SHA256-32 and HMAC-SHA256-128 are specified in [HMAC].

The H-SLP is required to store a BasicLastReplayCounterValue of length equal to the length of BasicReplayCounter parameter for each SET for which Basic SUPL INIT protection level is assigned.

6.1.6.6.1 H-SLP Procedures

If Basic level of protection is assigned to a SET, then prior to the first time that the H-SLP processes a SUPL INIT message with a given SUPL_INIT_ROOT_KEY, the H-SLP resets the BasicLastReplayCounterValue to 0x0000.

If Basic level of protection is assigned to a SET, then the H-SLP composes the SUPL INIT messages as follows:

1. Parameters outside the SUPL INIT Protector are assigned as described elsewhere.
2. Key identity is set to the current B-TID associated with the SUPL_INIT_ROOT_KEY.
3. H-SLC increases the current value of BasicLastReplayCounterValue by 1, and inserts the new value into the BasicReplayCounter parameter.
4. Finally, after all other parameters are assigned the BasicMAC is calculated from SUPL INIT and SUPL_INIT_ROOT_KEY as specified above.

6.1.6.6.2 SET Procedures

If Basic level of protection is assigned by the SET, then prior to the first time that the SET processes a SUPL INIT message with a given SUPL_INIT_ROOT_KEY, the SET clears its cache of used values for BasicReplayCounter.

If Basic level of protection is assigned, then the SET processes a received SUPL INIT message as follows:

1. The SET discards the SUPL INIT message if the following parameters fail the appropriate verification:
   - Protection Level: must be the assigned value for Basic SUPL INIT protection in Table 4.
   - Key Identity: must be the current B-TID.
   - BasicReplayCounter: the SET uses this value to detect replay of messages. The technique may be implementation specific but must be robust enough to deal with situations where SUPL INIT messages are lost or delivered out of order.
   - BasicMAC: The SET computes an expected BasicMAC from SUPL INIT and SUPL_INIT_ROOT_KEY (as described above) and compares this to the received BasicMAC: the values must be equal.
2. If the SUPL INIT was not discarded in the previous step, then it is considered authentic, and the SET considers the BasicReplayCounterValue to be used. If BasicReplayCounterValue is close to $65535 = 2^{16}-1$ (which is highly unlikely), then the SET must establish a new SUPL_INIT_ROOT_KEY with the H-SLP to reset the counter.

6.1.7 Key Refresh for Triggered Scenario Non-Proxy mode

The H/V-SPC and the SET use SPC_SET_Key as the key for mutual authentication over TLS with identifier SPC-TID. The key is valid for the duration of SPC_SET_Key_lifetime. When SPC_SET_Key_lifetime expires, a new key and key identifier need to be generated by the H-SLC and distributed to the SET and the H/V-SPC. The key refresh mechanism only applies to non-proxy mode. In proxy mode, key refreshing is handled by the TLS layer. The key refresh mechanism defined in the following sections applies to both Network Initiated and SET Initiated scenarios.

6.1.7.1 Non-Roaming Successful Case

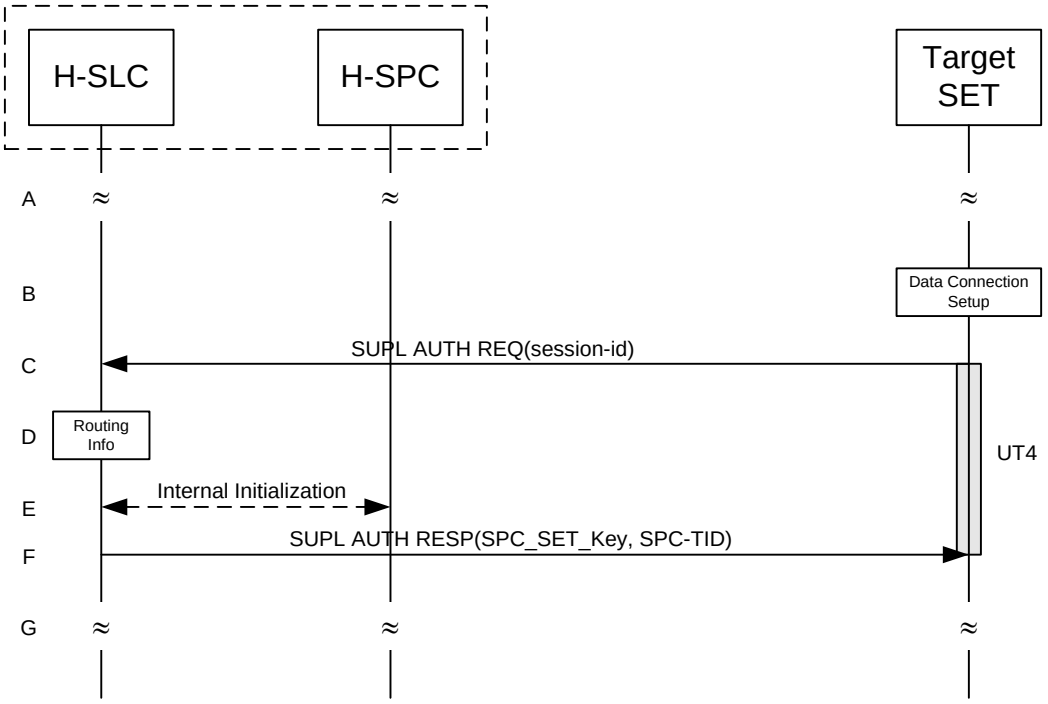

Figure 77: Example Figure Key Refresh for Triggered Scenarios – non-roaming

A. The SET and the H-SLP are engaged in a triggered session (periodic or area event) when the SET detects that SPC_SET_Key and SPC-TID require refreshing (i.e. SPC_SET_Key_lifetime has expired).

B. The SET uses the address provisioned by the Home Network to establish a secure IP connection to the H-SLC. If the SET is not already attached to the Packet Data Network it will attach itself or the SET establishes a circuit switched data connection.

C. The SET sends a SUPL AUTH REQ message to the H-SLC, implicitly requesting fresh SPC_SET_Key and SPC-TID. The SUPL AUTH REQ message contains the session-id.

D. The H-SLC verifies that the SET is currently not SUPL roaming.

NOTE: the specifics for determining if the SET is SUPL roaming or not is outside the scope of SUPL 2.0.

E. The H-SLC generates fresh SPC_SET_Key and SPC-TID (and optionally SPC_SET_Key_lifetime) which it forwards to the H-SPC through internal communication.

F. The H-SLC sends SPC_SET_Key and SPC-TID (and optionally SPC_SET_Key_lifetime) to the SET in a SUPL AUTH RESP message. The SET MAY release the IP connection with the H-SLC.

G. SET and H-SLP continue the triggered session (periodic or area event).

6.1.7.2 Roaming with V-SLP Successful Case

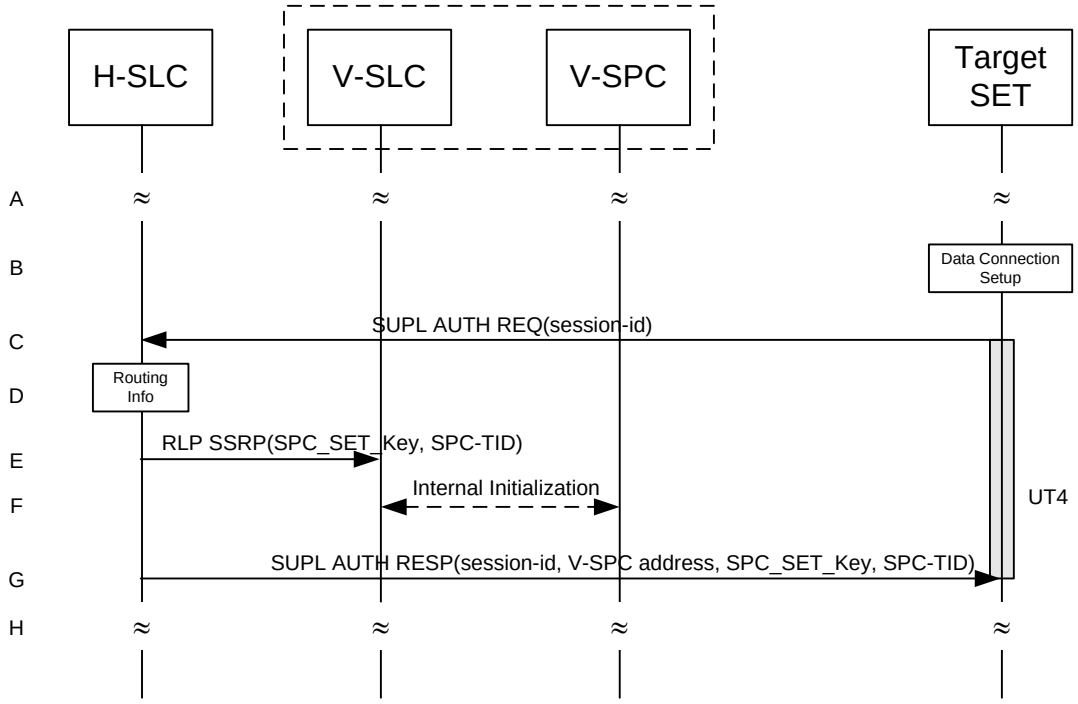

Figure 78: Key Refresh for Triggered Scenarios – roaming with V-SLP Positioning

A. The SET and the H/V-SLP are engaged in a triggered session (periodic or area event) when the SET detects that SPC_SET_Key and SPC-TID require refreshing (i.e. SPC_SET_Key_lifetime has expired).

B. The SET uses the address provisioned by the Home Network to establish a secure IP connection to the H-SLC. If the SET is not already attached to the Packet Data Network it will attach itself or the SET establishes a circuit switched data connection.

C. The SET sends a SUPL AUTH REQ message to the H-SLC, implicitly requesting fresh SPC_SET_Key and SPC-TID. The SUPL AUTH REQ message contains the session-id.

D. The H-SLC verifies that the SET is currently SUPL roaming.

NOTE: the specifics for determining if the SET is SUPL roaming is outside the scope of SUPL 2.0.

E. The H-SLC generates fresh SPC_SET_Key and SPC-TID (and optionally SPC_SET_Key_lifetime) and forwards them to the V-SLC in a RLP SSRP message.

F. The V-SLC forwards SPC_SET_Key and SPC-TID (and optionally SPC_SET_Key_lifetime) received in the previous step through internal communication to the V-SPC.

G. The H-SLC sends SPC_SET_Key and SPC-TID (and optionally SPC_SET_Key_lifetime) to the SET in a SUPL AUTH RESP message. The SET MAY release the IP connection with the H-SLC.

H. SET and H/V-SLP continue the triggered session (periodic or area event).

6.1.7.3 Roaming with H-SLP Successful Case

The key refresh mechanism for roaming with H-SLP follows the same call flow as for non-roaming (section 6.1.7.1).

6.2 Providing the H-SLP Address to the SET

The H-SLP address is made available to the SET by the provisioning of the H-SLP address in the UICC, SET or a default H-SLP address is derived as described below. This address MUST be in the form of a FQDN and SHOULD be securely provisioned by the Home Network of the SET.

6.2.1 CDMA/UMB SETs

For 3GPP2 SETs the H-SLP address MUST be securely provisioned in the UIM or R-UIM.

6.2.2 GSM/UMTS/LTE/NR SETs

A 3GPP SET MUST read the H-SLP address (in FQDN form) as a parameter "ADDR" under the "APPADDR/ADDR" characteristic as specified in WAP PROVCONT [PROVCONT]. In addition, the H-SLP address MUST be securely stored in the bootstrap file as defined in OMA Smartcard Provisioning specification [WAP PROVSC] on a 3GPP compliant UICC [3GPP 31.101] (USIM[3GPP 31.102]/SIM [3GPP 11.11]) or in an equivalently secure area of the SET. The SET MUST support OMA Smartcard Provisioning [WAP PROVSC] mechanisms to read the H-SLP address. The bootstrap file in the USIM/SIM application or SET that stores the H-SLP address MUST not be user changeable. If the H-SLP address is configured in the UICC (USIM/SIM), the SET MUST first read the H-SLP address provisioned in the UICC. If there is no H-SLP address provisioned in the UICC then the SET MAY read the H-SLP address from the secure area on the SET.

Provisioning of the H-SLP address in the SET: If the H-SLP address is to be stored in a secure location on the SET, it MUST be provisioned using OMA Device Management V1.2 or later [OMA-DM]. If the H-SLP address is provisioned using OMA DM the SET MUST authenticate the OMA DM Server based on the server side certificate presented by the DM Server during the TLS Handshake. If the SET supports storage of the H-SLP address it MUST NOT rely on the authentication scheme set forth in section 6.1.4, i.e., the Alternative Client authentication based on MSISDN/IP-Address mapping authentication. i.e. the SET MUST rely on the PSK-TLS mutual authentication method as described in section 6.1.1.

Auto configuration of the H-SLP address: If the H-SLP address can not be found in the secure storage area of the UICC (USIM/SIM), or in a secure area on the SET, the SET MUST configure the default H-SLP address in the SET based on the IMSI stored in the USIM/SIM.

In the case an H-SLP address has been found in the secure storage area of the UICC (USIM/SIM), or in a secure area on the SET, but its use has resulted in an authentication failure while initiating the SUPL session, the SET MUST configure the default H-SLP address in the SET based on the IMSI stored in the USIM/SIM.

The mechanism to configure a default H-SLP address is defined below.

Please note that the following example has been taken from 3GPP GBA specifications [3GPP 33.220] and adopted for the SUPL use case where a H-SLP address (based on a FQDN) is configured. Implementation of this default configuration mechanism does not require the implementation of the 3GPP GBA specification. The example below is given to illustrate the methodology and can be implemented independent of [3GPP 33.220].

Configuration of H-SLP based on IMSI:

Step 1) Take the first 5 or 6 digits of the IMSI, depending on whether a 2 or 3 digit MNC is used [3GPP 31.102] and separate them into MCC and MNC; if the MNC is 2 digits then a zero SHALL be added at the beginning;

Step 2) Use the MCC and MNC derived in step 1 to create the "mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org" domain name;
Add the label "h-slp." To the beginning of the domain name.

Example 1: If IMSI in use is "234150999999999", where MCC=234, MNC=15, and MSIN=0999999999, the H-SLP address would be "h-slp.mnc015.mcc234.pub.3gppnetwork.org".

If a new IMSI is detected by the SET during, or after power on, all previous H-SLP settings MUST be removed from the SET. More specifically, any H-SLP address stored in the SET MUST be removed.

In cases where the IMSI is changed the SET MUST first read the H-SLP address from the UICC (USIM/SIM). If no H-SLP address is stored on the UICC (USIM/SIM) the SET MAY check if the H-SLP address is stored in the SET. If no H-SLP address is found in the UICC or SET, then a default H-SLP address MUST be configured by the SET based on the new IMSI as described above.

Implementations MUST ensure that the address of the H-SLP cannot be changed via applications that are downloaded to the SET after the manufacturer software installation of the SET.

Figure 79 illustrates the flow diagram for the H-SLP address storage.

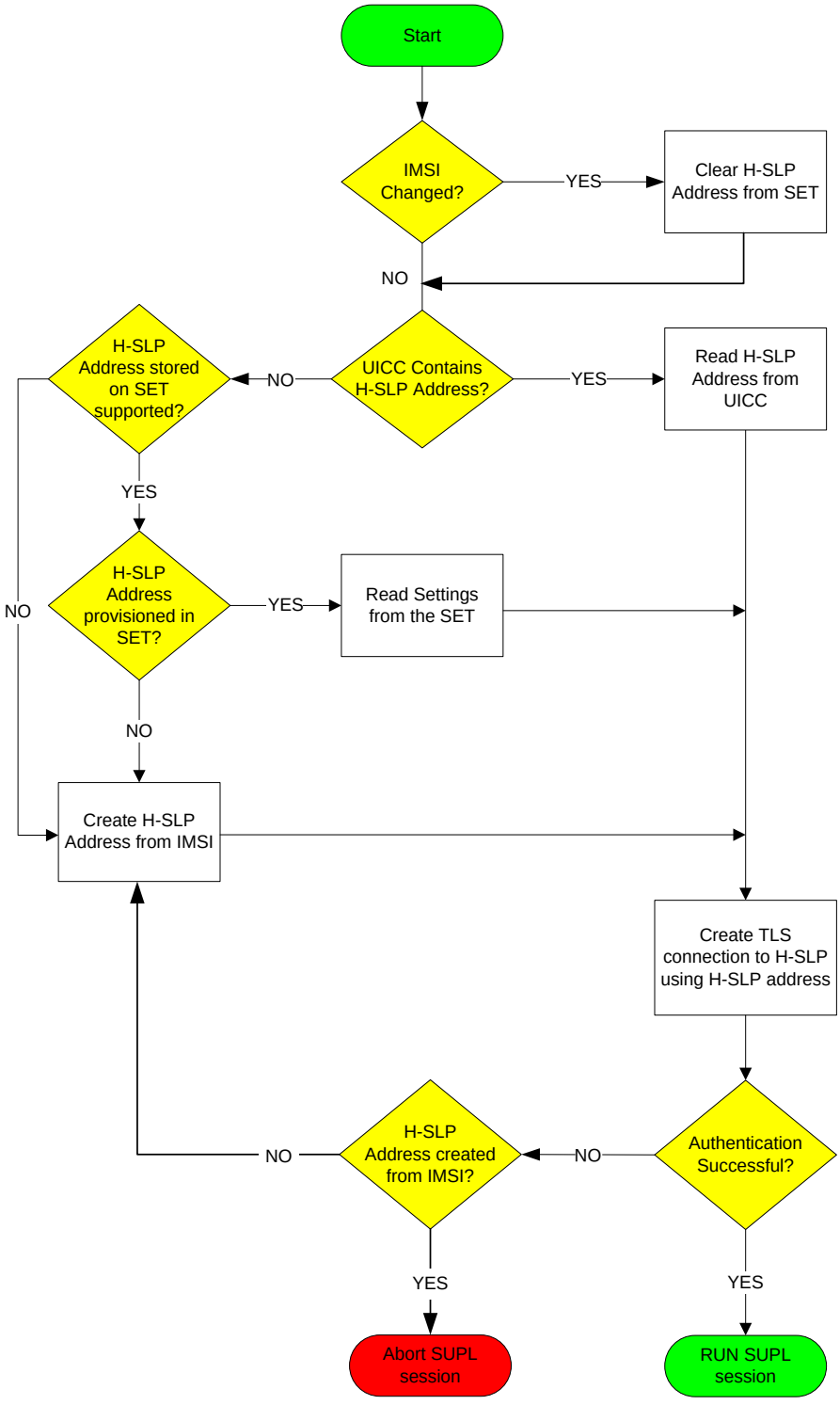

Figure 79: H-SLP address storage flow diagram for 3GPP SETs

6.2.3 WIMAX based deployments

When the SET attaches to the WiMAX network it MAY receive an updated H-SLP address via OMA DM. When the H-SLP address is provisioned in a secure manner to a WiMAX terminal and it must be stored in a protected environment.

6.3 Confidentiality and Data Integrity Protocols

TLS 1.1 [TLS] or TLS 1.2 [TLS 1.2] SHALL be used to provide Confidentiality and Data Integrity between a SET and an SLP. All SUPL Messages except "SUPL INIT" MUST be delivered within a TLS session between a SET and an SLP.

Section 6.1.1.3 provides details for determining which entities in a SUPL 2.0 deployment have TLS with server-certificate authentication and/or TLS-PSK as mandatory or optional.

6.3.1 TLS with Server-Certificates

Implementations of TLS 1.1 with server-certificates shall conform to [TLS] and WAP Profile of TLS 1.1 [WAP TLS]. Implementations of TLS 1.2 with server-certificates shall conform to [TLS] and WAP Profile of TLS 1.1 [WAP TLS], where [TLS 1.2] and this specification take precedence over [WAP TLS] where there is any conflict. The following clarifications apply in both cases:

SETs SHALL implement the following cipher suites:

- TLS_RSA_WITH_AES_128_CBC_SHA, specified in [TLS-AES] for TLS 1.1 and specified in [TLS 1.2] for TLS 1.2.

For SET implementations that prefer additional cipher suites SETs SHOULD implement the following cipher suites:

- TLS_RSA_WITH_3DES_EDE_CBC_SHA; specified in [TLS] for TLS 1.1 and specified in [TLS 1.2] for TLS 1.2.

For SET implementations that support TLS 1.2, SETs MAY implement the following cipher suites:

- TLS_RSA_WITH_AES_128_CCM [RFC 6655].

SLCs supporting TLS 1.1 or TLS 1.2 with server-certificates SHALL implement the following ciphersuites:

- TLS_RSA_WITH_3DES_EDE_CBC_SHA; specified in [TLS] for TLS 1.1 and specified in [TLS 1.2] for TLS 1.2.
- TLS_RSA_WITH_AES_128_CBC_SHA, specified in [TLS-AES] for TLS 1.1 and specified in [TLS 1.2] for TLS 1.2.

SLCs supporting TLS 1.2 with server-certificates SHOULD implement the following cipher suites:

- TLS_RSA_WITH_AES_128_CCM [RFC 6655].

For SLC implementations supporting TLS 1.1 or TLS 1.2 with server-certificates that prefer to support NULL encryption SLCs MAY implement TLS_RSA_WITH_NULL_SHA. Note that the use of TLS_RSA_WITH_NULL_SHA is not recommended, as it does not provide any confidentiality protection. However, it still provides authentication and integrity protection.

The WAP Certificate profile [WAP Cert] of TLS 1.1 SHALL be supported by SLPs supporting TLS 1.1 or TLS 1.2 with server-certificates and SETs.

6.3.2 TLS-PSK

SET implementations supporting TLS-PSK SHALL implement TLS 1.1 [TLS] and MAY implement TLS 1.2 [TLS 1.2].

TLS-PSK implementations SHALL conform to PSK-TLS [PSK-TLS].

SETs supporting TLS-PSK SHALL implement the following cipher suites:

- TLS_PSK_WITH_AES_128_CBC_SHA [PSK-TLS].

For SET implementations supporting TLS-PSK that prefer additional cipher suites, the SETs SHOULD implement the following cipher suites:

- TLS_PSK_WITH_3DES_EDE_CBC_SHA [PSK-TLS].

For SET implementations supporting TLS-PSK and TLS 1.2, the SETs MAY implement the following cipher suites:

- TLS_PSK_WITH_AES_128_CCM [RFC 6655]. See Note.

NOTE: The specification [RFC 6655] references the specification [PSK-TLS], so this cipher suite meets the requirement of conforming to [PSK-TLS].

SLP implementations supporting TLS-PSK SHALL implement TLS 1.1 [TLS] and MAY implement TLS 1.2 [TLS 1.2].

The following cipher suites SHALL be implemented by SLPs which support TLS-PSK:

- TLS_PSK_WITH_AES_128_CBC_SHA [PSK-TLS].

For SLP implementations supporting TLS-PSK that prefer additional cipher suites, the SLPs SHOULD implement the following cipher suites::

- TLS_PSK_WITH_3DES_EDE_CBC_SHA [PSK-TLS].

For SLP implementations supporting TLS-PSK and TLS 1.2, the SLPs SHOULD implement the following cipher suites:

- TLS_PSK_WITH_AES_128_CCM [RFC 6655]. See Note above.

The following cipher suites SHALL be implemented by SPCs that support non-proxy mode:

- TLS_PSK_WITH_AES_128_CBC_SHA [PSK-TLS].

For SPC implementations that support non-proxy mode that prefer additional cipher suites , the SPCs SHOULD implement:

- TLS_PSK_WITH_3DES_EDE_CBC_SHA [PSK-TLS].

For SPC implementations that support non-proxy mode and TLS 1.2, the SPCs SHOULD implement the following cipher suites:

- TLS_PSK_WITH_AES_128_CCM [RFC 6655]. See Note above.

7. ULP Version Negotiation

The ULP Version Negotiation mechanism is based on the assumption that an SLP may support more than one major version of SUPL with supported versions in one contiguous block down from the maximum supported version to the minimum supported version. It is further assumed that a SET only supports one version of SUPL (e.g. a SUPL 2.0 SET only supports SUPL 2.0).

Network Initiated scenarios:

For network initiated scenarios, the SUPL INIT message from the H-SLP or E-SLP to the SET carries the intended SUPL major and minor version M1.m1 (normally the highest version supported by the SLP) in the *version* parameter. The SUPL INIT message also carries the minimum SUPL major version number M2 for which continuation of the session by the SET is possible in the *minimum version* parameter. The value of M2 will depend on the intended SUPL service – e.g. for a single location fix M2 may be one; for triggered location M2 may be two. A SUPL session can be conducted between the SLP and the SET as long as the SET is using a SUPL major version between M2 and M1.

The SET continues the SUPL session normally if it supports a major version M of SUPL between M2 and M1 (i.e. $M2 \leq M \leq M1$) – and indicates this major version and a supported minor version m in the next message (i.e. implicitly in the *version* parameter of the message). The H-SLP or E-SLP then also reverts to the proposed SUPL major version M. and the same minor version m if supported (otherwise preferably and if supported to a minor version less than m or less preferably a minor version greater than m). If parameters were included in the SUPL INIT message that are not defined for SUPL version M.m, then the SET will ignore them and the SLP must act as if they had not been sent.

If the SET only supports a major version higher than M1 or a major version lower than M2, it returns a SUPL END.

SET Initiated scenarios:

For SET initiated SUPL sessions, the initial SUPL message from the SET carries the supported SUPL major and minor version M1.m1 (implicitly in the *version* parameter). The H-SLP continues the session if it supports the same major version M1 and otherwise sends a SUPL END and terminates the session.

Version negotiation for SUPL 1.0 is already defined and cannot be changed. Backward compatibility with SUPL 1.0 is achieved as follows:

Exceptions for SUPL 1.0:

For a network initiated SUPL session between an SLP supporting a version of SUPL above 1.0 and a SET that supports only 1.0, the SET will respond to the SUPL INIT message with a SUPL END (implicitly indicating support of SUPL 1.0 in the *version* parameter of SUPL END). The SLP will then restart the session using SUPL 1.0 if supported and if compatible with the intended SUPL service.

For a network initiated SUPL session between an SLP supporting only SUPL 1.0 and a SET that supports only a higher version, the SET will recognize that the SLP only supports SUPL 1.0 and will respond to the SUPL INIT message with SUPL END.

For a SET initiated SUPL session between an SLP supporting a version of SUPL above 1.0 and a SET that supports only 1.0, the SET will indicate SUPL 1.0 in the first SUPL message and the SLP, recognizing this, will either have to continue the session using SUPL 1.0 or reply with a SUPL END thereby terminating the session attempt.

For a SET initiated SUPL session between an SLP supporting only SUPL 1.0 and a SET that supports a higher version, the SLP will respond to the first SET message with a SUPL END and terminate the session.

7.1 Example Call Flows (Informative)

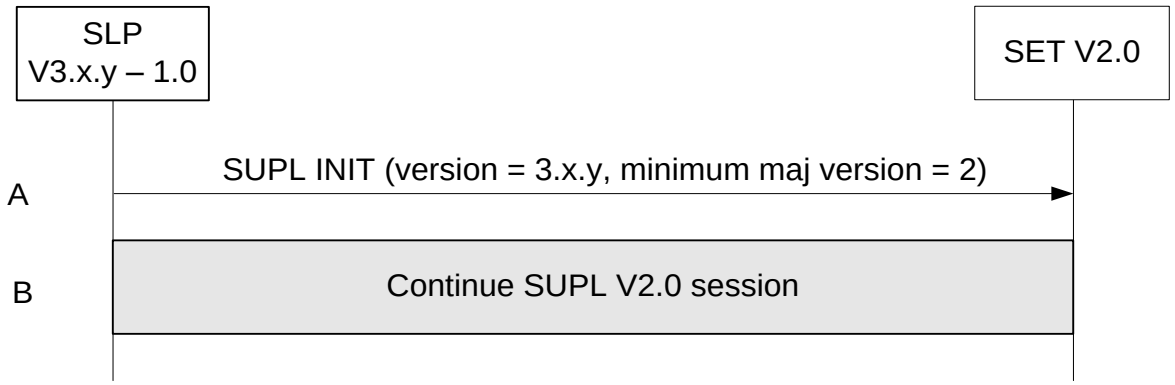

Figure 80: Network Initiated – SLP supports SUPL versions between 1.0 and 3.x.y and the requested service is V2.0 compatible.

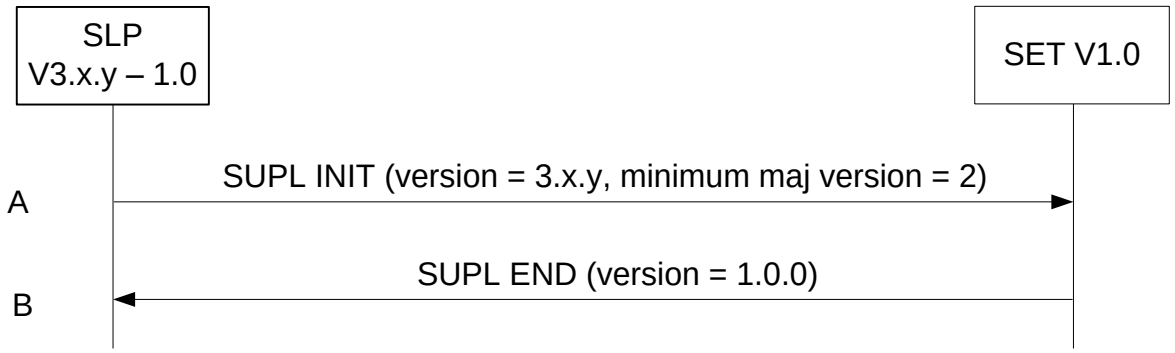

Figure 81: Network Initiated – SLP supports SUPL versions between 1.0 and 3.x.y but the requested service is not V1.0 compatible.

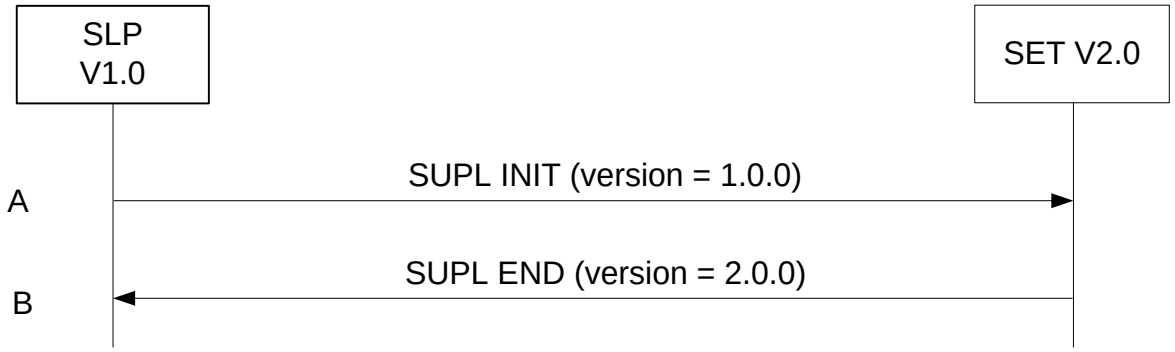

Figure 82: Network Initiated – SLP supports lower version than SET.

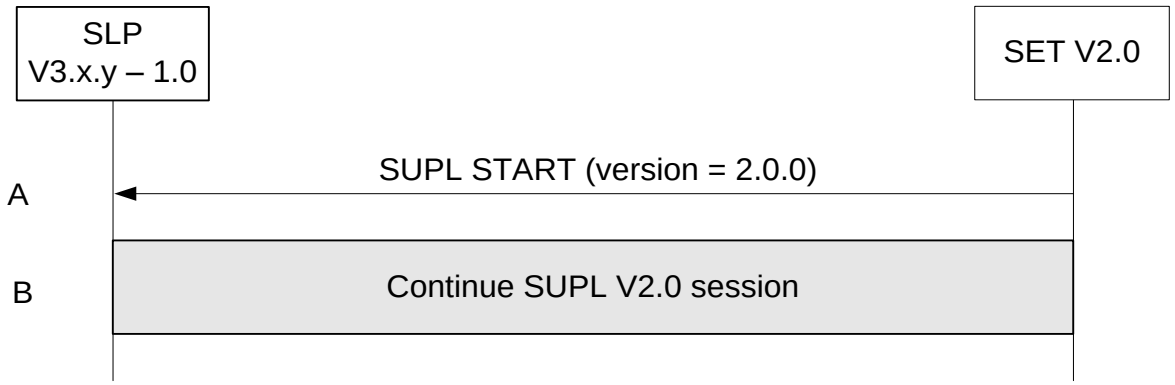

Figure 83: SET Initiated – SLP supports SUPL versions between 1.0 and 3.0 including requested version (V2.0).

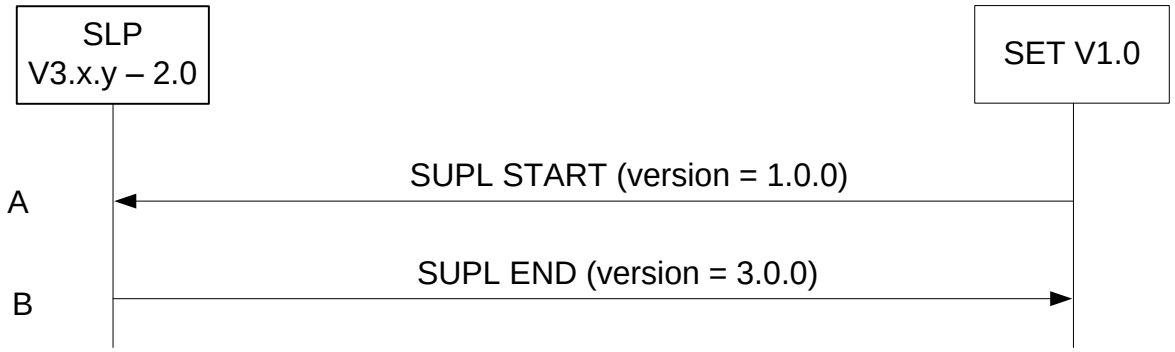

Figure 84: SET Initiated – SLP supports SUPL versions between 2.0 and 3.0 excluding requested version (V1.0).

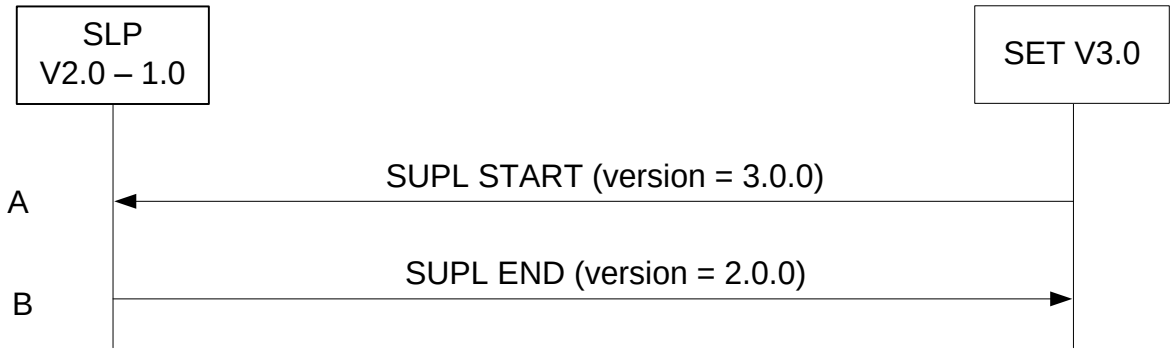

Figure 85: SET Initiated – SLP supports SUPL versions between 1.0 and 2.0 excluding requested version (V3.0).

8. Protocols and Interfaces

The encoding for the ULP protocol SHALL be ASN.1 [ASN.1].

The encoding is BASIC-PER, unaligned encoding [PER].

The transport protocol between SET and SLP (SET and SLC/SPC for non-proxy mode) SHALL be TCP/IP with the following exception: the initial SUPL INIT message SHALL be transported over OMA Push or SIP Push or Mobile Terminated SMS or UDP/IP. In case of OMA Push or SIP Push, the Push message from the PPG or SLP to SET SHALL follow the OMA Push specifications as per [WAP POTAP] for OMA Push or SIP Push specifications as per [SIP PUSH] for SIP Push with the clarifications given in sections 8.1.2 and 8.1.2.1. SUPL INIT can be sent over UDP/IP if the IP-address of the SET is known to the SLP or can be retrieved by the SLP.

For GSM/WCDMA/TD-SCDMA deployments, SUPL initiation using OMA Push SHALL be supported by both the SET and the SLP. For CDMA/CDMA2000 deployments, SUPL initiation using MT SMS SHALL be supported by both the SET and the SLP. Support of other transport protocols is optional.

8.1.1 TCP/IP and UDP/IP

The port number for ULP messages transported over TCP and UDP SHALL be as registered with IANA (Internet Assigned Numbers Authority). The port numbers are:

oma-ulp	7275/tcp	OMA UserPlane Location Protocol
oma-ulp	7275/udp	OMA UserPlane Location Protocol

8.1.2 SIP Push

SIP Push MESSAGE [SIP PUSH] SHALL be used with the following clarifications:

1. SIP MESSAGE method SHALL be used to deliver the SUPL INIT message.
2. Accept-Contact header SHALL include Application Resource Identifier +g.oma.pusheventapp= “ulp.ua”, where feature tag value “ulp.ua” is derived from the OMNA registered application id “x-oma-application:ulp.ua”.
3. Content-Type header SHALL be set to OMNA registered content type application/vnd.omaloc-supl-init.
4. SIP MESSAGE body SHALL contain PER encoded SUPL INIT message.

An example usage of the MESSAGE method is shown in Appendix 0.

8.1.2.1 SIP Push for IMS Emergency Location Services

In addition to the clarifications given in section 8.1.2, following clarifications SHALL apply when the E-SLP uses SIP Push [SIP PUSH] to deliver the SUPL INIT message to the SET via the Emergency IMS Core.

1. The E-SLP SHALL set the Request URI in the SIP MESSAGE to the SET SIP URI or TEL URI received from the Emergency IMS Core or PSAP in the emergency location request.

NOTE: The E-SLP receives the emergency location request from the Emergency IMS Core over 3GPP Ml interface or from the PSAP over the Le interface. The emergency location request contains the SIP URI or TEL URI of the SET initiated the IMS emergency call. The Emergency IMS Core uses the Request URI to correlate the SIP MESSAGE with the IMS emergency call and routes the SIP MESSAGE to the SET via the signaling path of the IMS emergency call. The specifics of 3GPP Ml interface and Le interface are considered outside scope of SUPL.

An example call flow is shown in Appendix B.5.

8.1.3 OMA Push

The OMA Push message [OMA PUSH] from an SLP (SLC for non-proxy mode) to a PPG SHALL contain the SUPL INIT message and SHALL follow [WAP PAP]. OMA Push over HTTP SHALL be used and SHALL contain the PAP control entity and the PER encoded SUPL INIT message. An example (informative only) is shown in Annex B. The PPG communicates with the SET over POTAP [WAP POTAP] or SIP Push [SIP PUSH] for an SIP enabled SET with the clarifications given in section 8.1.2.

The content type SHALL be as registered with IANA (content type: application/vnd.omaloc-supl-init) and OMNA (Open Mobile Naming Authority) (content type's assigned number: 0x312).

The WAP application id SHALL be as registered with OMNA (URN: x-oma-application:ulp.ua) and the assigned code value is (0x10).

8.1.4 MT SMS

For GSM/WCDMA/TD-SCDMA, the WDP [WAP WDP] framing SHALL be used for MT SMS. The port number SHALL be as registered with IANA.

This port number is:

oma-ulp 7275/udp OMA User Plane Location Protocol

For CDMA, the SUPL INIT message shall be sent as an MT SMS [TIA-637] using a dedicated Teleservice Identifier [TIA-41]. The dedicated Teleservice Identifier is: 4115.

8.1.5 SET Provisioning

The SET SHALL be provisioned with the address of the Home SLP in the form of FQDN.

The provisioning of the Home SLP address in the SET MAY use OMA enablers to provision the SET, e.g. as described in [SUPL CP] and [SUPL MO].

8.1.6 Lup Reference Point

The function of the Lup reference point is logically separated into Service Management and Position Determination.

This interface is used to enable the SLP to establish a session with the SET and performs the functions listed in section 8.1.6.1.

8.1.6.1 Service Management

This interface is used for service management and performs the functions listed in [SUPLAD2]

Table 5 shows the messages in the Lup Service Management interface.

Message Name	Description
SUPL INIT	The SUPL INIT message is used by the SLP to initiate a SUPL session with the SET. This message is used in Network Initiated SUPL Services.
SUPL SET INIT	The SUPL SET INIT message is used by the SET to initiate a SUPL session to locate the other SET.
SUPL START	The SUPL START message is used by the SET to start a SUPL session with the SLP.
SUPL TRIGGERED START	The SUPL TRIGGERED START message is used by the SET to start a triggered SUPL session with the SLP.
SUPL RESPONSE	The SUPL RESPONSE message is used by the SLP as a response to a SUPL START message in a SET initiated location request.
SUPL TRIGGERED RESPONSE	The SUPL TRIGGERED RESPONSE message is used by the SLP as a response to a SUPL TRIGGERED START message.
SUPL TRIGGERED STOP	The SUPL TRIGGERED STOP message is used by the SLP or SET to end an existing SUPL TRIGGERED session.
SUPL END	The SUPL END message is used by the SLP or SET to end an existing SUPL session.

SUPL AUTH REQ	The SUPL AUTH REQ message is only used in Non-Proxy mode for authentication of SET and SPC.
SUPL AUTH RESP	The SUPL AUTH RESP message is only used in Non-Proxy mode for authentication of SET and SPC.
SUPL NOTIFY	The SUPL NOTIFY message is only used by the SLP in notification based on the current location of the SET or for Session Info Query "re-notification" scenarios.
SUPL NOTIFY RESPONSE	The SUPL NOTIFY RESPONSE message is used by the SET as a response to a SUPL NOTIFy. Message.
SUPL REPORT	The SUPL REPORT message is used by the SLP or SET to report position estimate and/or network measurement results.

Table 5: Lup Service Management Messages

8.1.6.2 Position Determination

This interface is used for position calculation. It performs the functions listed in [SUPLAD2].

Table 6 shows the messages in the Lup Position Determination interface

Message Name	Description
SUPL POS	The SUPL POS message is used between the SLP and SET to exchange positioning procedure messages (RRLP/RRC/TIA-801/ LPP/LPPe) used to calculate the position of the SET.
SUPL POS INIT	The SUPL POS INIT message is used by the SET to initiate the positioning protocol session (RRLP/RRC/TIA-801/ LPP/LPPe) with the SLP.
SUPL REPORT	The SUPL REPORT message is used by the SLP or SET to report position estimate result.
SUPL END	The SUPL END message is used by the SLP or SET to end an existing SUPL session.

Table 6: Lup Position Determination Messages

A SET and SLP MUST provide support for Location ID positioning.

A GSM and/or WCDMA/TD-SCDMA capable SET and SLP providing support for this SET type SHALL support RRLP if A-GPS, A-GANSS or E-OTD positioning is supported.

An LTE [3GPP LTE] capable SET and SLP providing support for this SET type SHALL support at least one of RRLP, TIA-801 and LPP/LPPe if A-GPS or A-GANSS positioning is supported.

An NR [3GPP NR] capable SET and SLP providing support for this SET type SHALL support at least one of RRLP and LPP/LPPe if A-GPS or A-GANSS positioning is supported.

A CDMA/HRPD/UMB ([3GPP2 HRPD], [3GPP2 UMB]) capable SET and SLP providing support for this SET type SHALL support TIA-801 if A-GPS, A-GANSS or AFLT positioning is supported.

A WLAN capable SET and SLP providing support for this SET type SHALL support at least one of RRLP, TIA-801 and LPP/LPPe if A-GPS or A-GANSS positioning is supported.

A WiMAX [IEEE 802.16e-2005] capable SET and SLP providing support for this SET type SHALL support RRLP and/or TIA 801 if A-GPS or A-GANSS positioning is supported.

The SET and SLP support for other positioning protocols is OPTIONAL.

In the case of RRLP and SET based location determination for SET initiated scenarios with transfer to third party, the SLP SHALL send an RRLP Measure Position Request message. The SET SHALL respond with an RRLP Measure Position Response message.

In the case of RRC and SET based location determination for SET initiated scenarios with transfer to third party, the SLP SHALL send an RRC Measurement Control message. The SET SHALL respond with an RRC Measurement Response message.

The RRLP Positioning Capability Transfer procedure introduced in RRLP Release 7 (section 2.3a in [3GPP RRLP]) SHALL NOT be used.

9. ULP Message Definitions (Normative)

This section contains a normative description of the ULP messages. All messages defined in ULP contain a common part and a message specific part.

9.1 Common Part

The common part contains parameters that are present in all ULP messages.

Parameter	Presence	Description
Message Length	M	The length of the entire ULP Message in octets. **NOTE**: The first two octets of a PER encoded ULP message contains the length of the entire message. These octets are set to the Message Length when the PER encoding is complete and the entire message length is known.
Version	M	Version of the ULP protocol, in the form major, minor, service indicator
Session ID	M	The unique Session ID
Message Payload	M	This parameter contains one of the messages defined in ULP. Defined messages are: • SUPL INIT • SUPL START • SUPL RESPONSE • SUPL POS INIT • SUPL POS • SUPL END • SUPL AUTH REQ • SUPL AUTH RESP • SUPL SET INIT • SUPL NOTIFY • SUPL NOTIFY RESPONSE • SUPL TRIGGERED START • SUPL TRIGGERED RESPONSE • SUPL TRIGGERED STOP • SUPL REPORT

Table 7: Common Part for all ULP Messages

9.2 Message Specific Part

The message specific part contains further parameters that are unique for each ULP message. The following sub-sections describe the message specific part of ULP messages.

9.2.1 SUPL INIT

SUPL INIT is the initial message from the H-SLP (or E-SLP) to the SET in Network initiated cases.

Parameter	Presence	Description
Positioning Method	M	Defines the positioning technology desired by the SLP for the SUPL session (A-GPS SET Assisted, A-GPS SET Based, Autonomous GPS, EOTD, OTDOA, AFLT, Ecid, MBS, NR DL-TDOA, NR DL-AoD, NR Multi-RTT, NR DL-E-CID, NR UL-TDOA, NR UL-AoA, A-GNSS SET Assisted, A-GNSS SET Based or Autonomous GNSS). If Positioning Method is AGNSS SET Assisted or AGNSS SET Based, the parameter GNSS Positioning Technology MUST be present to indicate the actual positioning technologies. If Positioning Method is Autonomous GNSS, the parameter GNSS Positioning Technology MAY be present. In line with the SET Capabilities, the SLP MAY change the positioning method used in the actual positioning session regardless of the positioning method parameter.
Notification	O	When Notification Mode is Normal Notification /Verification, this field is used to provide instructions to the SET with respect to notification and privacy. If this field is not present the SET SHALL interpret the request as type “No notification & no verification“. When Notification Mode is Notification/Verification based on location, this field SHALL NOT be used by the SLP and the SET.
SLP Address	CV	This parameter contains an SLP address (SPC address for non-proxy mode). For proxy mode this parameter is OPTIONAL.

		For non-proxy mode this parameter is REQUIRED. This address is used by the SET when establishing a secure IP connection to the SLP or SPC
QoP	O	Desired Quality of Position. This parameter is also used as reporting criteria for stored historical position estimates. If used in this way, only the spacial components (horacc and veracc) apply and define the accuracy requirements which must be satisfied in order to report any historic position estimate.
SLP Mode	M	This parameter indicates if the SLP uses proxy or non-proxy mode.
MAC	O	Not used in SUPL 2.0 but needs to remain as empty placeholder for backwards compatibility with SUPL 1.0.
Key Identity	CV	This parameter is required when MAC is present. Not used in SUPL 2.0 but needs to remain as empty placeholder for backwards compatibility with SUPL 1.0.
Notification Mode	O	This parameter indicates whether the notification and verification is based on location or not. If not present, normal notification is assumed.
Supported Network Information	O	This parameter defines the type(s) of Network Measurement information which the SET is allowed to send as part of Location ID and Multiple Location IDs. If not present, the SET MAY send any Network Measurement information it supports and has available. This parameter is also used as reporting criteria for stored historical enhanced cell/sector measurements.
Trigger Type	CV	This parameter indicates network initiated service type: • Periodic • Area event This parameter is conditional and only used if a triggered session is requested in the SUPL INIT message.
E-SLP Address	CV	This parameter provides the E-SLP address.
Historic Reporting	CV	This parameter defines the criteria for reporting of stored historical position

		estimates and/or enhanced cell/sector measurements. This parameter is conditional and MUST be used if the SUPL INIT message is used to initiate retrieval of stored historical position estimates and/or enhanced cell/sector measurements. Otherwise this parameter is not used.
Protection Level	O	This parameter defines the protection level of the SUPL INIT protection. This parameter is optional. If not present, no protection is implicitly assumed.
GNSS Positioning Technology	O	Defines the GNSSs (and correction data) desired for AGNSS SET Assisted, AGNSS SET Based or Autonomous GNSS in the Positioning Method parameter. • GPS • Galileo • SBAS • Modernized GPS • QZSS • GLONASS • BDS • RTK OSR **NOTE 1**: If RTK OSR is not included, GPS MUST NOT be the only GNSS in this parameter. **NOTE 2**: If present, RTK OSR should be used in association with one or more GNSSs included in this parameter.
Minimum Major Version	O	This parameter defines the minimum major version supported by the SLP which is compatible with the requested service. This parameter is optional. If not present, the only version compatible with the requested service is the *version* parameter (see common part in section 9.1). The *minimum major version* must always be smaller than the *major version*. Range: 0 to 255

Table 8: SUPL INIT Message

9.2.2 SUPL SET INIT

The SUPL SET INIT message is the initial message where a SET can initiate location request to another target SET.

Parameter	Presence	Description

Target SET ID	M	Identifies the Target SET to be located where a SET can initiate location request to another target SET.
QoP	O	Desired Quality of Position
ApplicationID	O	The identifier of the requesting application on the SET.

Table 9: SUPL SET INIT Message

9.2.3 SUPL START

SUPL START is the initial message from the SET to the SLP.

Parameter	Presence	Description
SET capabilities	M	Defines the capabilities of the SET
Location ID	M	Defines the current serving cell, current serving WLAN AP or WiMAX BS information of the SET.
QoP	O	Desired Quality of Position
Multiple Location IDs	O	This parameter may contain current non-serving cell, current non-serving WLAN AP or current non-serving WiMAX BS information for the SET and/or historic serving or non-serving cell, WLAN AP or WiMAX BS information for the SET. Only information that was allowed according to the Supported Network Information element in a previous SUPL session SHALL be included.
Third Party	CV	This parameter defines a list of third party identities. For the SET Initiated location request without transfer to Third Party, this parameter is not REQUIRED. For the SET Initiated location request with transfer of location to Third Party mode, this parameter is REQUIRED.
>Third Party ID	M	The identity of the Third Party. There must be at least one Third Party ID. This parameter can be of type • Logical name • MSISDN • Email address • SIP URI • IMS Public Identity • MIN • MDN • URI
ApplicationID	O	The identifier of the requesting application on the SET.
Position	O	Defines the position of the SET.

Table 10: SUPL START Message

9.2.4 SUPL RESPONSE

SUPL RESPONSE is the response to a SUPL START message.

Parameter	Presence	Description
Positioning Method	M	The positioning method that SHALL be used for the SUPL session.
SLP Address	CV	This parameter is only required for non-proxy mode and contains an SPC address. A SET uses this address to establish a data connection to the SPC.
SET Auth key	O	This parameter SHALL NOT be used and is only provided for reasons of encoding backwards compatibility with SUPL 1.0.
Key Identity 4	O	This parameter SHALL NOT be used and is only provided for reasons of encoding backwards compatibility with SUPL 1.0.
SPC_SET_Key	O	This parameter defines the authentication key used by the SET for H/V-SPC authentication.
SPC-TID	O	This parameter defines the transaction ID used for H/V-SPC authentication.
SPC_SET_Key_lifetime	O	This parameter defines the lifetime of SPC_SET_Key. This parameter is optional. If not present, a default value of 24 hours is assumed. The units are in hours and the range is from 1 to 24 hours.
Supported Network Information	O	This parameter defines the type(s) of Network Measurement information which the SET is allowed to send as part of Location ID and Multiple Location IDs. If not present, the SET MAY send any Network Measurement information it supports and has available.
Initial Approximate Position	O	Defines the initial approximation for the position of the SET.
GNSS Positioning Technology	O	Defines the actual GNSSs (and correction data) allowed for AGNSS SET Assisted, AGNSS SET Based or Autonomous GNSS in the Positioning Method parameter. • GPS • Galileo • SBAS • Modernized GPS • QZSS • GLONASS • BDS

		• RTK OSR **NOTE 1**: If RTK OSR is not included, GPS MUST NOT be the only allowed GNSS in this parameter. **NOTE 2**: If present, RTK OSR should be used in association with one or more GNSSs included in this parameter.

Table 11: SUPL RESPONSE Message

9.2.5 SUPL POS INIT

SUPL POS INIT is the message following the SUPL INIT message in Network initiated cases or the SUPL RESPONSE message in SET initiated cases

Parameter	Presence	Description
SET Capabilities	M	Defines the capabilities of the SET.
Requested Assistance Data	O	Defines the requested GPS and GANSS assistance data. The presence of this element indicates that the SET wants to obtain specific GPS and GANSS assistance data from the SLP. The SET might use this element in any combination of A-GPS SET assisted / A-GPS SET based/A-GANSS SET assisted/A-GANSS SET based and Network initiated / SET initiated positioning. The Requested Assistance Data parameter is not applicable to TIA-801 [TIA-801] and LPP/LPPe [3GPP LPP]/[OMA-LPPe].
Location ID	M	Defines the current serving cell, current serving WLAN AP or current serving WiMAX BS information of the SET.
Position	O	Defines the position of the SET.
SUPLPOS	O	Contains the SUPLPOS message. **NOTE**: is only used if positioning protocol allows SET to send first message. Any positioning protocol messages in this parameter that are not supported by the SLP SHALL be ignored by that SLP.
Ver	CV	This parameter contains a hash of the SUPL INIT message. In Network initiated proxy mode a SET SHALL calculate a hash of a received SUPL INIT and include the result of the hash in this parameter.

Multiple Location IDs	O	This parameter may contain current non-serving cell, current non-serving WLAN AP or current non-serving WiMAX BS information for the SET and/or historic serving or non-serving cell, WLAN AP or WiMAX BS information for the SET. Only information allowed according to Supported Network Information received from the SLP SHALL be included.
UTRAN GPS Reference Time Result	O	The UTRAN GPS Reference Time Result as measured by the SET. This parameter is sent by the SET to the SLP if available and requested by the SLP in the Supported Network Information parameter (in SUPL INIT, SUPL RESPONSE or SUPL TRIGGERED RESPONSE) if the serving cell is WCDMA/TD-SCDMA and RRLP is used as positioning protocol.
UTRAN GANSS Reference Time Result	O	The UTRAN GANSS Reference Time Result as measured by the SET. This parameter is sent by the SET to the SLP if available and requested by the SLP in the Supported Network Information parameter (in SUPL INIT, SUPL RESPONSE or SUPL TRIGGERED RESPONSE) if the serving cell is WCDMA/TD-SCDMA and RRLP is used as positioning protocol.
Serving AMF Identifier	CV	The serving AMF Identifier indicates the serving AMF for a SET with 5G NR access. The serving AMF identifier is only provided by a SET when the Positioning method in a SUPL INIT, SUPL RESPONSE or SUPL TRIGGERED RESPONSE indicates NR Multi-RTT, NR UL-TDOA or NR-AoA and when the SET supports this positioning method.

Table 12: SUPL POS INIT Message

9.2.6 SUPL POS

SUPL POS is the message that wraps the underlying TIA-801, RRLP, RRC or LPP/LPPe elements and may contain additional information such as velocity, UTRAN GPS/GANSS Reference Time Assistance or UTRAN GPS/GANSS Reference Time Result.

Parameter	Presence	Description
Positioning Payload	M	The underlying TIA-801, RRLP, RRC or LPP/LPPe elements.
Velocity	O	Velocity of the SET, needed to overcome the lack of this information

		in RRLP and RRC. Defined in [3GPP GAD]
UTRAN GPS Reference Time Assistance	O	The UTRAN GPS Reference Time Assistance is sent by the SLP to the SET if requested by the SET in the Requested Assistance Data parameter (in SUPL POS INIT) if the serving cell is WCDMA/TD-SCDMA and RRLP is used as positioning protocol.
UTRAN GPS Reference Time Result	O	The UTRAN GPS Reference Time Result as measured by the SET. This parameter is sent by the SET to the SLP if available and requested by the SLP in the Supported Network Information parameter (in SUPL INIT, SUPL RESPONSE and SUPL TRIGGERED RESPONSE) if the serving cell is WCDMA/TD-SCDMA and RRLP is used as positioning protocol.
UTRAN GANSS Reference Time Assistance	O	The UTRAN GANSS Reference Time Assistance is sent by the SLP to the SET if requested by the SET in the Requested Assistance Data parameter (in SUPL POS INIT) if the serving cell is WCDMA/TD-SCDMA and RRLP is used as positioning protocol.
UTRAN GANSS Reference Time Result	O	The UTRAN GANSS Reference Time Result as measured by the SET. This parameter is sent by the SET to the SLP if available and requested by the SLP in the Supported Network Information parameter (in SUPL INIT, SUPL RESPONSE and SUPL TRIGGERED RESPONSE) if the serving cell is WCDMA/TD-SCDMA and RRLP is used as positioning protocol.

Table 13: SUPL POS Message

9.2.7 SUPL END

SUPL END is the message that ends the SUPL procedure, normally or abnormally.

Parameter	Presence	Description
Position	O	Defines the position result of the SET.
Status Code	O	Defines the Status of the message as either an error indication or an information indication. Error indications have values between 0 and 99, information indications have values between 100 and 199.
Ver	CV	This parameter contains a hash of the SUPL INIT message and is calculated by the SET. This parameter MUST be present in situations where the SUPL

		END message is sent as a direct response to SUPL INIT (both proxy and non-proxy mode).
SET Capabilities	O	Defines the SET Capabilities of the SET. This parameter MAY be used if the SUPL END message is sent from the SET to the SLP.
High Accuracy Position	O	Defines a high accuracy position result of the SET. NOTE: If the High Accuracy Position parameter is included, an SLP SHALL include the Position parameter, which shall be consistent with the High Accuracy Position parameter,

Table 14: SUPL END Message

9.2.8 SUPL AUTH REQ

SUPL AUTH REQ message is used in Network initiated cases (non-proxy mode). The message is sent from the SET to the H-SLP. The purpose of the message is to request key information from the H-SLC in non-proxy mode for mutual H/V-SPC to SET authentication.

Parameter	Presence	Description
ver	O	This parameter contains a hash of the SUPL INIT message.
SET Capabilities	O	Defines the service capabilities of the SET.

Table 15: SUPL AUTH REQ Message

9.2.9 SUPL AUTH RESP

SUPL AUTH RESP message is used in Network initiated cases (non-proxy mode). The message is sent from the H-SLC to the SET. The purpose of the message is to send key information required for mutual H/V-SPC to SET authentication to the SET.

This message may also be tunneled to a V-SLC in an RLP message and SHALL then include the authentication key and key identity to be used by the V-SPC.

Parameter	Presence	Description
SPC_SET_Key	M	This parameter defines the authentication key used by the SET for H/V-SPC authentication.
SPC-TID	M	This parameter defines the transaction ID used for H/V-SPC authentication.
SPC_SET_Key_lifetime	O	This parameter defines the lifetime of SPC_SET_Key. This parameter is optional. If not present, a default value of 24 hours is assumed. The units are in hours and the range is from 1 to 24 hours.

Table 16: SUPL AUTH RESP Message

9.2.10 SUPL TRIGGERED START

SUPL TRIGGERED START is the initial message from the SET to the H-SLP for establishing a triggered session or for re-initiating a triggered session during a V-SLP to V-SLP handover.

Parameter	Presence	Description
SET capabilities	M	Defines the capabilities of the SET
Location ID	M	Defines the current serving cell, current serving WLAN AP or WiMAX BS information of the SET.
Ver	CV	This parameter contains a hash of the SUPL INIT message. In Network initiated proxy mode a SET SHALL calculate a hash of a received SUPL INIT and include the result of the hash in this parameter. This parameter shall not be included in a SUPL TRIGGERED START sent to request new trigger parameters.
QoP	O	Desired Quality of Position
Multiple Location IDs	O	This parameter may contain current non-serving cell, current non-serving WLAN AP or WiMAX BS information for the SET and/or historic serving or non-serving cell or WLAN AP information for the SET. Only information that was allowed according to the Supported Network Information element in a previous SUPL session SHALL be included.
Third Party	CV	The identity of the Third Party. For the SET Initiated location request without transfer to Third Party, this parameter is not REQUIRED. For the SET Initiated location request with transfer of location to Third Party mode, this parameter is REQUIRED.
>Third Party ID	M	The identity of the Third Party.
ApplicationID	O	The identifier of the requesting application on the SET.
Trigger Type	CV	This parameter indicates SET initiated trigger service type: • Periodic • Area event For network initiated trigger service, it MUST not be present.
Trigger Params	CV	This parameter indicates parameters of the trigger session.

		For network initiated trigger service, this parameter MUST NOT be present. For SET initiated trigger service, this parameter MUST be present.
Position	O	Defines the position of the SET.
Reporting Capability	CV	This parameter defines the reporting capabilities of the SET on a per SUPL session basis (there is a Reporting Capability parameter as part of SET Capabilities -> Service Capabilities which reflects the generic SET Reporting Capabilities). This parameter is conditional and only used for triggered periodic scenarios. The values of this parameter MUST be consistent with the values of Reporting Capability as part of SET Capabilities. For periodic triggered services, this parameter MUST be present. For area event triggered services, this parameter MUST NOT be present.
>minimum interval between fixes	M	Defines the minimum interval between fixes allowed by the SET. This parameter is used by the H-SLP to avoid conflict between the desired interval between fixes and the SET's capabilities. Range: 1 to 3600, Units in seconds.
>maximum interval between fixes	O	Defines the maximum interval between fixes allowed by the SET. This parameter is used by the H-SLP to avoid conflict between the desired interval between fixes and the SET's capabilities. This parameter is optional. If not present, no maximum interval between fixes is specified. Range: 1 to 1440, Units in minutes.
>Rep Mode	M	This parameter is a bit map indicating the supported reporting mode(s): • Real time • Quasi real time • Batch reporting At least one of the three reporting modes must be supported.
>Batch Report Capability	CV	If batch reporting is supported as reporting mode, this parameter defines the type of reports which are supported:

		• Position • Measurement data • Position and Measurement data The maximum number of positions and/or measurements the SET is able to store are defined as: • Maximum number of positions • Maximum number of measurements These parameters are optional. If not present, no limit is specified.
Cause Code	O	This parameter indicates the reason for sending this message during an ongoing triggered session. The value could be: • Serving Network not in Area Id list • SET capabilities has changed • No SUPL coverage

Table 17: SUPL TRIGGERED START Message

9.2.11 SUPL TRIGGERED RESPONSE

SUPL TRIGGERED RESPONSE is the response to a SUPL TRIGGERED START message from the SLP to the SET

Parameter	Presence	Description
Positioning Method	M	The positioning method desired for the triggered SUPL session. In line with the SET Capabilities, the SLP MAY change the positioning method used in the positioning session in the course of the triggered SUPL session regardless of the positioning method parameter.
Trigger Params	CV	This parameter indicates parameters of trigger session For network initiated trigger service, this parameter MUST be present. For SET initiated trigger service, this parameter MAY be used to convey an Area Id List to the SET.
SLP Address	CV	This parameter is only required for non-proxy mode and contains an SPC address. A SET uses this address to establish a data connection to the SPC.
Supported Network Information	O	This parameter defines the type(s) of Network Measurement information which the SET is allowed to send as part of Location ID and Multiple Location IDs. If not present, the SET

		MAY send any Network Measurement information it supports and has available.
Reporting Mode	O	For periodic triggered sessions this parameter defines the reporting mode requested by the SLP. This parameter is optional. If not present, real time reporting is requested.
>Rep Mode	M	One of the following modes: • Real time • Quasi real time • Batch reporting
>Batch Reporting Conditions	CV	If batch reporting is chosen, the SLP selects one of the following reporting conditions: • Sending of a batch report after every N fixes/measurements • Sending of a batch report after every N minutes • Sending of only one batch report at the end of the session
>Batch Report Type	CV	If batch or quasi-real time reporting is chosen as reporting mode, this parameter defines the type of reports which are allowed to be reported: • Position • Measurement data • Intermediate reporting If set to false, the SET SHALL NOT report any earlier than requested even if it runs out of memory. If not all data could be reported, the SET SHALL indicate this with a result code of outofmemory. If set to true, the SET MAY send intermediate reports earlier than requested if it runs out of memory. The SET SHALL indicate intermediate reports with a result code of outofmemoryintermediatereporting. • Discard Oldest If set to true, the SET SHALL discard the oldest data first in the batch report if it runs out of memory and cannot use intermediate reporting. If set to false, the SET SHALL discard the latest data in the batch report first if it runs out of memory and cannot use intermediate reporting .

		If not present, it is up to the SET implementation to decide which data to discard first.
SPC_SET_Key	O	This parameter defines the authentication key used by the SET for H/V-SPC authentication.
SPC-TID	O	This parameter defines the transaction ID used for H/V-SPC authentication.
SPC_SET_Key_lifetime	O	This parameter defines the lifetime of SPC_SET_Key. This parameter is optional. If not present, a default value of 24 hours is assumed. The units are in hours and the range is from 1 to 24 hours.
GNSS Positioning Technology	O	Defines the actual GNSSs (and correction data) allowed for AGNSS SET Assisted, AGNSS SET Based or Autonomous GNSS in the Positioning Method parameter. • GPS • Galileo • SBAS • Modernized GPS • QZSS • GLONASS • BDS • RTK OSR **NOTE 1**: If RTK OSR is not included, GPS MUST NOT be the only allowed GNSS in this parameter. **NOTE 2**: If present, RTK OSR should be used in association with one or more GNSSs included in this parameter.

Table 18: SUPL TRIGGERED RESPONSE Message

9.2.12 SUPL TRIGGERED STOP

SUPL TRIGGERED STOP is used by the SLP or the SET to cancel a triggered session.

Parameter	Presence	Description
Status Code	O	Defines the status code of the message.

Table 19: SUPL TRIGGERED STOP Message

9.2.13 SUPL NOTIFY

SUPL NOTIFY is the message from the SLP to the SET in Network initiated cases.

Parameter	Presence	Description

Notification	M	The purpose of this field is to provide instructions to the SET with respect to notification and privacy.

Table 20: SUPL NOTIFY Message

9.2.14 SUPL NOTIFY RESPONSE

SUPL NOTIFY RESPONSE is the response to a SUPL NOTIFY message.

Parameter	Presence	Description
Notification Response	CV	The purpose of this field is to provide notification response from the user. This field MUST be present in response to a SUPL NOTIFY in which notification and verification was requested.

Table 21: SUPL NOTIFY RESPONSE Message

9.2.15 SUPL REPORT

The SUPL REPORT message is used in the following instances:

(1) For triggered applications, the SUPL REPORT message is used by the SLP to indicate the end of a positioning procedure (SUPL POS session) to the SET. In this case the SUPL REPORT message may or may not contain a calculated position.

(2) For triggered applications, the SUPL REPORT message may be used to send one or more position result(s) (calculated by the SET) and/or enhanced cell/sector measurement(s) from the SET to the SLP. The SUPL REPORT message may be used without a position result to indicate to the SLP that an Area Event has occurred. A result code may optionally be sent to indicate an error condition (e.g. no position available).

(3) As an intermediate report within a continuing batch reporting session, the SUPL REPORT message is used as in triggered applications, but the message should only contain the position result(s). This allows the SET to dynamically manage its memory by managing the amount of data stored in SET.

(4) For single fix notification/verification based on current location, the SUPL REPORT message is used in non-proxy mode to indicate the end of the positioning procedure (SUPL POS) session) to the SET. In this case the SUPL REPORT message may or may not contain a calculated position.

(5) SUPL REPORT is used by the SET in response to a session info query from the H-SLP. In this case the SUPL REPORT message contains a list of session-ids of all active SUPL sessions. The SUPL REPORT message MAY also include the SET Capabilities.

NOTE: For uplink reporting, if the amount of report data to be sent exceeds the maximum ULP message length (64K Octets), the SET SHALL send the report data in multiple SUPL REPORT messages.

Parameter	Presence	Description
SessionList	O	A list of the session-ids of all active SUPL sessions. The list does not contain the session-id of the “session-info query” session which is already included in the session-id parameter of the SUPL REPORT message
SET capabilities	O	Defines the capabilities of the SET. This parameter may only be used if the SUPL REPORT

		message is sent in the context of a "session-info query" session.
ReportDataList	O	The Report Data List comprises one up to 1024 occurrences of Report Data.
>Report Data	M	Report Data contains the actual data to be reported: Position Data, Measurement Data, Result Code and Time Stamp.
>>Position Data	O	A calculated position and the respective positioning mode used (optional).
>>>position	M	The calculated position of the SET (including a time stamp).
>>>posmethod	O	Positioning method with which the position was calculated (e.g. SET Based A-GPS, autonomous GPS, etc.).
>>>GNSS Positioning Technology	O	Defines the GNSSs (and correction data) used to calculate the position. • GPS • Galileo • SBAS • Modernized GPS • QZSS • GLONASS • BDS • RTK OSR **NOTE 1**: This parameter SHALL NOT be used if posmethod indicates A-GPS or autonomous GPS, and RTK OSR is not included. **NOTE 2**: If included, RTK OSR is used in association with one or more GNSSs included in this parameter.
>>>GANSS Signals Information	O	This parameter may be included to indicate the GANSS Signals (up to 16) used for calculation of the position. GANSS Signals Information defines a list of GANSS Signals.
>>>>GANSS Id	M	Defines the GANSS. Integer (0..15) 0: Galileo 1: SBAS 2: Modernized GPS 3: QZSS 4: GLONASS

		5: BDS 6-15: Reserved for future use
>>>>**GANSS Signals**	M	Bitmap (length 8 bits) defining the supported signals for GNSS indicated by GANSS ID. For Galileo, the bits are interpreted as : Bit 0: E1 Bit 1: E5a Bit 2: E5b Bit 3: E5a+E5b Bit 4: E6 Bits 5-7: Spare For Modernized GPS, the bits are interpreted as: Bit 0: L1 C Bit 1: L2 C Bit 2: L5 Bits 3-7: Spare For QZSS, the bits are interpreted as: Bit 0: L1 C/A Bit 1: L1 C Bit 2: L2 C Bit 3: L5 Bits 4-7: Spare For GLONASS, the bits are interpreted as: Bit 0: G1 Bit 1: G2 Bit 2: G3 Bits 3-7: Spare For SBAS, the bits are interpreted as: Bit 0: L1 Bits 1-7: Spare For BDS, the bits are interpreted as: Bit 0: B1I Bits 1-7: Spare
>>**Multiple Location Ids**	O	Multiple Location Ids.
>>**Result Code**	O	Result Code describing why no position or measurement could be reported: a. Out of radio coverage b. No position c. No measurement d. No position and no measurement e. Out of memory f. Out of memory, intermediate reporting

		g. Other
>>**Time Stamp**	O	Time Stamp in either absolute time (UTC Time) or relative time (relative to "now" i.e. when the SUPL REPORT message is sent. This parameter is only used if Position Data is not present. If Position Data is present, the timestamp parameter within position is used as timestamp.
Ver	CV	This parameter contains a hash of the SUPL INIT message. This parameter MUST be used if the SUPL REPORT message is sent in response to a SUPL INT message. Otherwise this parameter is not applicable.
More Components	CV	This parameter is used if the report data to be sent needs to be segmented into multiple SUPL REPORT messages. If present, this parameter indicates that more SUPL REPORT messages will be sent. The last SUPL REPORT message in a series of segments SHALL omit this parameter.

Table 22: SUPL REPORT Message

10.Parameter Definitions (Normative)

This section contains descriptions of the parameters used in ULP messages.

10.1 NMR

Parameter	Presence	Value/Description
NMR		Describes Contents of the Current Network Measurement Reports. Contains 1 to 15 NMR elements
> NMR element		The following fields shall be repeated for each channel for which measurements are available. The measurements shall be ordered by decreasing channel numbers.
>> ARFCN	M	ARFCN of the channel. This is an integer (0..1023)
>> BSIC	M	BSIC of the channel. This is an integer (0..63)
>> RxLEV	M	Measured power of the channel. Integer (0..63). The actual measured power X in dBm is derived from this value N by using the formula X = N-110.

Table 23: NMR Parameter

10.2 Positioning Payload

Parameter	Presence	Value/Description
Positioning payload		Describes the positioning payload for TIA-801 [TIA-801], RRLP [3GPP RRLP], RRC [3GPP RRC], LPP [3GPP LPP] and LPPe [OMA-LPPe]. The restrictions of maximum PDU size as specified in [3GPP RRLP] (242 octets) does not apply. If the size for "rrlpPayload" exceeds 65535 bits, pseudo segmentation according to [3GPP RRLP] SHALL be used. Up to three LPP/LPPe messages and/or up to three TIA801 messages are allowed to be sent in a single Positioning Payload IE.

Table 24: Positioning Payload Parameter

10.3 SLP Address

Parameter	Presence	Value/Description
SLP address		The SLP address (SLC or SPC address for non-proxy mode) can be of type • IPAddress

		○ Ipv4 ○ Ipv6 • FQDN

Table 25: SLP Address Parameter

10.4 Velocity

Parameter	Presence	Value/Description
Velocity		Describes the velocity of the SET as per [3GPP GAD]. One of the following four formats are supported: • Horizontal Velocity ○ Bearing ○ Horizontal speed • Horizontal and Vertical Velocity ○ Vertical Direction ○ Bearing ○ Horizontal speed ○ Vertical speed • Horizontal Velocity Uncertainty ○ Bearing ○ Horizontal speed ○ Horizontal speed uncertainty • Horizontal and Vertical Velocity Uncertainty ○ Vertical direction ○ Bearing ○ Horizontal speed ○ Vertical speed ○ Horizontal speed uncertainty ○ Vertical speed uncertainty

Table 26: Velocity Parameter

10.5 Version

Parameter	Presence	Value/Description
Version		Describes the protocol version of ULP When a SUPL message is received, the receiving entity SHALL determine if the major version part specified in

		the message is supported by the receiving entity.
>Maj	M	Major version, range: (0..255), MUST be 2 for the version described in this document
>Min	M	Minor version, range: (0..255), MUST be 0 for the version described in this document.
>Serv_ind	M	Service indicator, range: (0..255), MUST match the service level for this document.

Table 27: Version

10.6 Status Code

Parameter	Presence	Value/Description
Status Code		The different status codes, either error or information indicators, as described in the table below

Table 28: Status Code

Status Code	Description
Error Indicators	Used to indicate errors
unspecified	The error is unknown
systemFailure	System Failure
protocolError	Protocol parsing error
dataMissing	Needed data value is missing
unexpectedDataValue	A datavalue takes a value that cannot be used
posMethodFailure	The underlying positioning method returned a failure
posMethodMismatch	No positioning method could be found matching requested QoP, SET capabilities and positioning method specified by SLP
posProtocolMismatch	No positioning protocol could be found being available at SET and SLP
targetSETnotReachable	The SET was not responding
versionNotSupported	Wrong ULP version
resourceShortage	There were not enough resources available at the SLP to serve the SET or not enough resource available at the SET for the session.
InvalidSessionId	Invalid session identity
unexpectedMessage	Unexpected message received
nonProxyModeNotSupported	The SET does not support “Non-Proxy” mode of operation.
ProxyModeNotSupported	The SET does not support “Proxy” mode of operation.
PositioningNotPermitted	The SET is not authorized by the SLP to obtain a position or assistance data.
AuthNetFailure	The network does not authenticate the SET.
AuthSuplinitFailure	The SUPL INIT message is not authenticated by the SET or the SLP

serviceNotSupported	Service Capability not supported
incompatibleProtectionLevel	The Protection Level in the SUPL INIT message is not compatible with the protection level of the SET
insufficientInterval	The requested interval between fixes is not compatible with the capabilities of either the SET or the SLP.
NoSUPLCoverage	The SET lost SUPL coverage. This status code is used for V-SLP to V-SLP handover to indicate to the H-SLP that the SET lost SUPL coverage.
Information Indicators	Used to indicate information
consentDeniedByUser	User denied consent for location determination session.
ConsentGrantedByUser	User granted consent for location determination session.
SessionStopped	The triggered session has been stopped by the network or the SET.
AppIdDenied	The App Id was not authorized by the SLP and as a result, the requested service was denied.

Table 29: Status Code

10.7 Position

Parameter	Presence	Value/Description
Position		This parameter describes the position of the SET. The parameter also contains a timestamp and optionally the velocity.
>Timestamp	M	Time when position fix was calculated.
>Position Estimate	M	
>>Sign of latitude	M	Indicates North or South.
>>Latitude	M	Integer (0..2^{23}-1). The latitude encoded value (N) is derived from the actual latitude X in degrees (0°..90°) by this formula: $N \leq 2^{23} X /90 < N+1$
>>Longitude	M	Integer (-2^{23}.. 2^{23}-1). The longitude encoded value (N) is derived from the actual longitude X in degrees (-180°..+180°) by this formula: $N \leq 2^{24} X /360 < N+1$
>>Uncertainty ellipse (semi major, semi minor, major axis)	O	Contains the latitude/longitude uncertainty code associated with the major axis, and the uncertainty code associated with the minor axis and the orientation, in degrees, of the major axis with respect to the North. For the correspondence between the latitude/longitude uncertainty code

		and meters refer to [3GPP GAD] for details.
>>Confidence	O	Represents the confidence by which the position of a target entity is known to be within the shape description (i.e., uncertainty ellipse for 2D-description, uncertainty ellipsoid for 3D-description) and is expressed as a percentage. This is an integer (0..100).
>>Altitude information	O	Shall be present for a 3D position information; it shall remain absent for 2D position information.
>>>Altitude direction	M	Indicates height (above the WGS84 ellipsoid) or depth (below the WGS84 ellipsoid).
>>>Altitude	M	Provides altitude information in meters. Integer (0..2^{15}-1). Refer to [3GPP GAD] for details
>>>Altitude uncertainty	M	Contains the altitude uncertainty code. Refer to [3GPP GAD] for details
>Velocity	O	Speed and bearing values as defined by the Velocity type and as defined in [3GPP GAD]

Table 30: Position Parameter

The definition and coding of the position estimate parameter (ellipsoid point with altitude, uncertainty ellipse and altitude uncertainty) is based on [3GPP GAD]. The Datum used for all positions are WGS-84.

10.8 Positioning Method

Parameter	Presence	Value/Description
Position Method		Describes the positioning method: • A-GPS SET assisted only • A-GPS SET based only • A-GPS SET assisted preferred (A-GPS SET based is the fallback mode) • A-GPS SET based preferred (A-GPS SET assisted is the fallback mode) • A-GNSS SET Assisted only • A-GNSS SET Based only • A-GNSS SET Assisted preferred (A-GANSS SET Based is the fallback mode) • A-GNSS SET Based preferred (A-GANSS SET Assisted is the fallback mode)

		• Autonomous GPS • Autonomous GNSS • AFLT • Enhanced Cell/sector **NOTE**: Cell-ID is considered as a subset positioning method of Enhanced Cell/sector. When a SET receives the Ecid indicator the SET SHALL respond with the mandatory Location ID (lid) elements and the optional Location ID (lid) elements if these optional elements are supported by the SET. If these elements are sent by the SET the SLP MAY choose to utilise or ignore the elements in the position calculation. • EOTD • OTDOA • MBS • NR DL-TDOA • NR DL-AoD • NR Multi-RTT • NR DL-E-CID • NR UL-TDOA • NR UL-AoA • No position • Historical Data Retrieval • Session-Info Query For Network Initiated scenarios, if a particular Positioning Method is desired by the SLP (i.e. sent in SUPL INIT), and if the following SUPL POS INIT message (or SUPL TRIGGERED START message) from the SET indicates support of that same Positioning Method, then this Positioning Method SHALL be used during the entire SUPL session. If the Positioning Method desired by the SLP is not supported by the SET (as indicated in the SET Capability parameter in SUPL POS INIT or SUPL TRIGGERED START) then another mutually acceptable Positioning Method (i.e. a positioning

		method consistent with the SET's capabilities) may be used by the SLP in the positioning session. Otherwise the SLP will respond with a SUPL END message with status code *posMethodMismatch* and terminate the session. For SET Initiated scenarios, the Positioning Method parameter is used by the SLP (sent in SUPL RESPONSE or SUPL TRIGGERED RESPONSE) to indicate the Positioning Method that SHALL be used for the entire SUPL session. For Network Initiated scenarios the positioning method "no position" is used for single fix location requests when no SUPL POS session is to be conducted and the SUPL INIT message was only sent for notification and verification purposes. In this case the SET will respond with a SUPL END message including the appropriate status code ("consentDeniedByUser" or "consentGrantedByUser"). In case no verification was required ("notification only"), the SET will respond with a SUPL END message containing no status code. The positioning method "historical data retrieval" is used to retrieve stored historical position estimates and/or enhanced cell/sector measurements. In case of A-GNSS SET Based and/or, A-GNSS SET Assisted, the GNSS Positioning Technology parameter MUST be used in addition to the Positioning Method parameter (i.e. must be included in SUPL INIT for Network Initiated and must be included in SUPL RESPONSE for SET Initiated scenarios) to specify which GNSS(s) is (are) to be used. For Autonomous GNSS, the GNSS Positioning Technology MAY be used to specify which GNSS(s) is (are) to be used. The GNSS Positioning Technology parameter is only used if at least one GNSS other than GPS is selected as positioning method.

		NOTE: Once a SUPL session has been established and a positioning method determined, positioning methods may only be switched from SET Assisted to SET Based or visa versa if the positioning method selected was a *preferred* positioning method (i.e. SET Assisted Preferred & SET Based Allowed or SET Based Preferred & SET Assisted Allowed. An exception is the fallback to cell-id positioning method which is always available in case the selected positioning method failed to produce a positioning result during a positioning session. Session-Info Query is used to retrieve the session-ids of all active SUPL sessions at the SET and optionally also the SET Capabilities. No position fix is calculated during a "Session-Info Query" session.

Table 31: Positioning Method Parameter

10.9 Requested Assistance Data

Parameter	Presence	Value/Description
Requested assistance data	-	This parameter is applicable for A-GPS positioning methods. It describes the requested A-GPS assistance data in form of a bitmap: • Almanac indicator • UTC model • Ionospheric model • DGPS corrections • Reference location • Reference time • Acquisition assistance • Real-time integrity • Navigation model **NOTE**: Reference location Bit is used for requesting Reference Location also for GANSS.
Navigation Model	CV	When the navigation model indicator is set, this field is present.
>GPS week	M	Contains the GPS week of the assistance data currently held in the SET; range is 0 to 1023

>GPS Toe	M	Contains the GPS time of Ephemeris in hours of the newest set of Ephemeris contained in the SET; range is 0 to 167
>NSAT	M	Contains the number of satellites to be considered for the current GPS assistance data request (number of satellites for which ephemeris data is available in the SET); range is 0 to 31. If the SET has no ephemeris data, this field SHALL be set to zero. If the SET has ephemeris data whose age exceeds the T-Toe limit, this field may be set to zero. If the network receives a zero value for this field, it shall ignore the GPS week and GPS Toe fields and assume that the SET has no ephemeris data
>T-Toe limit	M	Contains the Ephemeris age tolerance of the SET to the network in hours; range is 0 to 10
>Satellite information	CV	Present if NSAT > 0, repeated NSAT times
>>SatId	M	Identifies the satellite and is equal to (SV ID No-1) where SV ID No is defined in ICD-GPS-200C. Range is 0 to 63
>>IODE	M	Represents the satellite sequence number, range is 0 to 255
GANSS Requested Common Assistance Data	O	
>GANSS Reference Time	M	GANSS reference time. Boolean, “true” if requested, “false” otherwise.
>GANSS Ionospheric model	M	GANSS Ionospheric model. Boolean, “true” if requested, “false” otherwise.
>GANSS Additional Ionospheric Model for Data ID=’00’	M	GANSS Ionospheric model, see [3GPP 49.031] for further information on Data ID
>GANSS Additional Ionospheric Model for Data ID=’11’	M	GANSS Ionospheric model, see [3GPP 49.031] for further information on Data ID
>GANSS Earth-Orientation Parameters	M	Earth-Orientation Parameters for precise coordinate transformations
>GANSS Additional Ionospheric Model for Data ID=’01’	M	GANSS Ionospheric model. The value ‘01’ indicates that the parameters have been generated by BDS.
GANSS Requested Generic Assistance Data	O	Generic data requested for GANSS. If included, this parameter is repeated for each GANSS the assistance data is requested. In addition, in the case of

		SBAS this parameter is repeated for each SBAS the assistance data is requested.
>GANSS ID	M	Defines the GANSS for which the assistance data is requested. 0: Galileo 1: SBAS 2: Modernized GPS 3: QZSS 4: GLONASS 5: BDS 6-15: Reserved for future use
> SBAS ID	CV	Present if GANSS ID indicates SBAS. Bit Sting interpreted as: 000: WAAS 001: EGNOS 010: MSAS 011: GAGAN
>GANSS Real-Time Integrity	M	Real Time integrity requested for a particular GANSS. Boolean, “true” if requested, “false” otherwise.
>DGANSS Differential Corrections	O	If present, differential corrections are requested. Bitmap (length 8 bits) defining for which signals the corrections are requested For Galileo, the bits are interpreted as: Bit 0: E1 Bit 1: E5a Bit 2: E5b Bit 3: E6 4-7: spare For Modernized GPS, the bits are interpreted as: Bit 0: L1 C Bit 1: L2 C Bit 2: L5 Bits 3-7: Spare For QZSS, the bits are interpreted as: Bit 0: L1 C/A Bit 1: L1 C Bit 2: L2 C Bit 3: L5 Bits 4-7: Spare For GLONASS, the bits are interpreted as: Bit 0: G1 Bit 1: G2 Bit 2: G3 Bits 3-7: Spare For SBAS, the bits are interpreted as: Bit 0: L1 Bits 1-7: Spare

		For BDS, the bits are interpreted as: Bit 0: B1I Bits 1-7: Spare
>GANSS Almanac	M	GANSS Almanacs for the particular GANSS Id. Boolean, "true" if requested, "false" otherwise. If GANSS ID indicates modernized GPS or QZSS and Almanac Model ID is not included in GANSS Additional Assistance Data Choices, this bit shall be interpreted as Model-4 for modernized GPS and as Model-2 for QZSS, defined in Table A.54 of [3GPP RRLP].
>GANSS Navigation Model	O	If present, GANSS navigation models are requested
>>GANSS Week or Day	M	Week or Day number of the assistance data currently held in the set. If GANSS ID does not indicate GLONASS this field is expressed in GANSS weeks. Range is 0 to 4095. If GANSS ID indicates GLONASS this field is expressed in days as defined in [3GPP 49.031].
>>GANSS_Toe	M	Time-of-Ephemeris of the assistance data currently held in the SET, If GANSS ID does not indicate GLONASS this field is expressed in hours. Range is 0 to 167. If GANSS ID indicates GLONASS Toe is expressed in units of 15 minutes. Range then is 0 to 95 (0 to 1425 minutes).
>>T-Toe limit	M	Ephemeris age tolerance of the UE to network. If GANSS ID does not indicate GLONASS this field is expressed in hours. Range is 0 to 10. If GANSS ID indicates GLONASS Toe is expressed in units of 30 minutes. Range then is 0 to 15 (0 to 450 minutes).
>>Satellites list related data	O	Information of the satellites for which the ephemeris data is available in SET.
>>>SatID	M	Identifies the satellite for which assistance is requested and is interpreted as in table A.10.14 in [3GPP RRLP].
>>>IOD	M	Issue of Data for SatID as defined in table A.48.2 in [3GPP RRLP].
>GANSS Time Model GNSS-GNSS	O	If present, time models to convert reference system time to GNSS system time are requested. Reference

		system is indicated by GANSS ID. Bitmap (length 16 bits) defining GNSS system for which GNSS the time models are requested: 0: GPS 1: Galileo 2: QZSS 3: GLONASS 4: BDS Bits 5-15: spare.
>GANSS Reference Measurement Information	M	Boolean value, if set to true reference code and Doppler measurement information of satellites of a GANSS constellation are requested.
>GANSS data bits	O	Request Bit stream of GANSS
>>GANSS TOD minute	M	The reference time modulo 60 s of the first data bit of the requested data in integer seconds in GNSS specific system time of the GNSS indicated by GANSS ID.
>>Data bit assistance	M	
>>>GANSS Signal	M	Bitmap (length 8 bits) defining the supported signals for GNSS indicated by GANSS ID. For Galileo, bits are interpreted as : Bit 0: E1 Bit 1: E5a Bit 2: E5b Bit 3: E5a+E5b Bit 4: E6 Bits 5-7: Spare For Modernized GPS, the bits are interpreted as: Bit 0: L1 C Bit 1: L2 C Bit 2: L5 Bits 3-7: Spare For QZSS, the bits are interpreted as: Bit 0: L1 C/A Bit 1: L1 C Bit 2: L2 C Bit 3: L5 Bits 4-7: Spare For GLONASS, the bits are interpreted as: Bit 0: G1 Bit 1: G2 Bit 2: G3 Bits 3-7: Spare For SBAS, the bits are interpreted as: Bit 0: L1 Bits 1-7: Spare

		For BDS, the bits are interpreted as: Bit 0: B1I Bits 1-7: Spare
>>>GANSS Data Bit Interval	M	This field represents the time length for which the Data Bit Assistance is requested. The Data Bit Assistance shall be relative to the time interval (GANSS TOD, GANSS TOD + Data Bit Interval). The Data Bit Interval *r*, expressed in seconds, is mapped to a binary number K with the following formula: $r = 0.1 * 2^K$ Value K=15 means that the time interval is not specified.
>>>Satellite Information	O	This parameter may be included to indicate a list of satellites (up to 64) for which the Data Bit Assistance Request is applicable
>>>>SatID	M	Identifies the satellite and is equal to (SV ID No – 1).
>GANSS UTC model	M	UTC model requested. Boolean, "true" if required, "false" otherwise. If GANSS ID indicates QZSS and UTC Model ID in GANSS Additional Assistance Data Choices is not included, this bit shall be interpreted as Model-1 as defined in Table A.55 of [3GPP RRLP].
>GANSS Additional Data Choices	O	If present, some GANSS Additional Assistance Data is requested.
>> Orbit Model ID	O	ID as defined in A.49.2 of [3GPP RRLP]. Missing field indicates request for the native model.
>> Clock Model ID	O	ID as defined in A.49.1 of [3GPP RRLP]. Missing field indicates request for the native model.
>>>UTC Model ID	O	ID as defined in A.55/A.55.17 of [3GPP RRLP]. Missing field indicates request for the native model.
>>Almanac Model ID	O	ID as defined in A.54 of [3GPP RRLP]. Missing field indicates request for the native model.
>GANSS Auxiliary Information	O	GANSS Auxiliary Information including signal availability for SVs and GLONASS frequency assignments requested.
>GANSS Extended Ephemeris	O	
>>Validity	M	Requested validity period for Extended ephemeris in steps of four hours

>GANSS Extended Ephemeris Check	O	See [3GPP 49.031] for further information on this field.
>>Begin Time	M	Begin time of the Extended ephemeris currently held by the SET
>>End Time	M	End time of the Extended ephemeris currently held by the SET
>BDS-Differential-Corrections	CV	This parameter is conditional and MAY be used if GANSS-ID = 5 (BDS). Otherwise this parameter MUST NOT be used. If present, differential corrections are requested. Bitmap (length 8 bits) defining for which signals the corrections are requested. The bits are interpreted as: Bit 0: B1I Bits 1-7: Spare
>BDS-GridModel	CV	This parameter is conditional and MAY be used if GANSS-ID = 5 (BDS). Otherwise this parameter MUST NOT be used. Boolean, “true” if requested, “false” otherwise.
GPS Extended Ephemeris	O	
>Validity Hours	M	Requested validity period for Extended ephemeris in steps of four hours
GPS Extended Ephemeris Check	O	See [3GPP 49.031] for further information on this field.
>Begin Time	M	Begin time of the Extended ephemeris currently held by the SET
>End Time	M	End time of the Extended ephemeris currently held by the SET

Table 32: Requested Assistance Data Parameter

10.10 SET capabilities

Parameter	Presence	Value/Description
SET capabilities	-	SET capabilities (not mutually exclusive) in terms of supported positioning technologies and positioning protocols. During a particular SUPL session, a SET may send its capabilities more than once – specifically, in SET initiated cases, the SET capabilities are sent in SUPL START, SUPL TRIGGERED START and in SUPL POS INIT. For immediate requests, the SET capabilities MUST NOT change during this particular session. For triggered requests, the SET capabilities MAY change during a session. The SET Capabilities parameter MAY also be used by the SET to inform the H-SLP about its service capabilities.
>Pos Technology	M	Defines the positioning technology.

		Zero or more of the following positioning technologies (including those listed in the optional GANSS Position Methods structure and the optional Additional Positioning Methods structure): • SET-assisted A-GPS • SET-based A-GPS • Autonomous GPS • AFLT • E-CID • E-OTD • OTDOA
>>GANSS Position Methods	O	Defines the supported GANSS (i.e. other than A-GPS). If included, this parameter is repeated for each supported GANSS. In addition, in the case of SBAS the parameter is repeated for each supported SBAS.
>>>GANSS ID	M	Defines the GANSS. Integer (0..15) 0: Galileo 1: SBAS 2: Modernized GPS 3: QZSS 4: GLONASS 5: BDS 6-15: Reserved for future use
>>>SBAS ID	CV	Present if GANSS ID indicates SBAS. Bit string interpreted as: 000: WAAS 001: EGNOS 010: MSAS 011: GAGAN
>>>GANSS Positioning Modes	M	Bitmap defining the supported modes for GNSS indicated by GANSS ID. Bit 0: SET Assisted Bit 1: SET Based Bit 2: Autonomous
>>>GANSS Signals	M	Bitmap (length 8 bits) defining the supported signals for GNSS indicated by GANSS ID. For Galileo, bits are interpreted as : Bit 0: E1 Bit 1: E5a Bit 2: E5b Bit 3: E5a+E5b Bit 4: E6 Bits 5-7: Spare For Modernized GPS, the bits are interpreted as:

		Bit 0: L1 C Bit 1: L2 C Bit 2: L5 Bits 3-7: Spare For QZSS, the bits are interpreted as: Bit 0: L1 C/A Bit 1: L1 C Bit 2: L2 C Bit 3: L5 Bits 4-7: Spare For GLONASS, the bits are interpreted as: Bit 0: G1 Bit 1: G2 Bit 2: G3 Bits 3-7: Spare For SBAS, the bits are interpreted as: Bit 0: L1 Bits 1-7: Spare For BDS, the bits are interpreted as: Bit 0: B1I Bits 1-7: Spare
>>>RTK	O	If present, indicates which variants of RTK are supported for a particular GANSS ID. The following variants may be included: • osr
>> Additional Positioning Methods	O	Defines the supported additional positioning methods. If included, this parameter is repeated for each supported additional positioning method.
>>>Additional Positioning ID	M	Defines the supported additional positioning technologies: • MBS • NR DL-TDOA • NR DL-AoD • NR Multi-RTT • NR DL-E-CID • NR UL-TDOA • NR UL-AoA
>>>Additional Positioning Modes	O	Bitmap defining the supported modes for additional positioning method indicated by Additional Positioning Identifiers: Bit 0: Standalone Bit 1: SET-based Bit 2: SET-assisted Bit 3-7: Reserved for future use
>Pref Method	M	One of the following preferred modes: • A-GNSS SET-assisted preferred

		• A-GNSS SET-based preferred • No preferred mode
>Pos Protocol	M	Zero or more of the following positioning protocols (bitmap): • RRLP • RRC • TIA-801 • LPP • LPPe
>>Pos Protocol Version RRLP	CV	Describes the protocol version of RRLP Positioning Protocol. It is required if RRLP is identified in the Pos Protocol parameter. The following RRLP versions are the lowest versions which are supported by the SET and the SLP: For Release 5: 5.12.0 and 5.14.0, for Release 6: 6.9.0, for Release 7: 7.11.0 and for Release 8: 8.3.0. No lower versions shall be supported. In addition, if some future version x.y.z of RRLP becomes non-backward compatible with earlier versions (e.g. due to an essential correction), an SLP should support at least one version earlier than x.y.z as well as at least one version equal to or later than x.y.z. For each release, the SET may support any version equal to or newer than the minimum versions listed above.
>>>Major Version Field	M	First (most significant) element of the version number for RRLP, range: (0..255)
>>>Technical Version Field	M	Second element of the version number for RRLP, range: (0..255)
>>>Editorial Version Field	M	Third (least significant) element of the version number for RRLP, range: (0..255)
>>Pos Protocol Version RRC	CV	Describes the protocol version of RRC Positioning Protocol. It is required if RRC is identified in the Pos Protocol parameter. The following RRC versions are the lowest versions which are supported by the SET and the SLP: For Release 5: 5.11.0 and 5.23.0, for Release 6: 6.21.0, for Release 7: 7.12.0 and for Release 8: 8.6.0. No lower versions shall be supported. In addition, if some future version x.y.z of RRC becomes non-backward compatible with earlier versions (e.g.

		due to an essential correction), an SLP should support at least one version earlier than x.y.z as well as at least one version equal to or later than x.y.z. For each release, the SET may support any version equal to or newer than the minimum versions listed above.
>>>Major Version Field	M	First (most significant) element of the version number for RRC, range: (0..255)
>>>Technical Version Field	M	Second element of the version number, range: (0..255)
>>>Editorial Version Field	M	Third (least significant) element of the version number for RRC, range: (0..255)
>>Pos Protocol Version TIA-801	CV	Describes the protocol version of 3GPP2 C.S0022 (TIA-801) Positioning Protocol. It is required if TIA-801 is identified in the Pos Protocol parameter.
>>>Supported Pos Protocol Version TIA-801	M	Specifies a list of up to 8 different supported 3GPP2 C.S0022 versions. This parameter is required (with at least one entry in the list) if TIA-801 is identified in the Pos Protocol parameter.
>>>>Revision Number	M	Revision part of document number for the specifications of C.S0022 Positioning Protocol. Value: [0,A-Z]
>>>>Point Release Number	M	Point Release number for C.S0022, range: (0..255)
>>>Internal Edit Level	M	Internal Edit Level for C.S0022, range: (0..255)
>>Pos Protocol Version LPP	CV	Describes the protocol version of LPP Positioning Protocol. It is required if LPP is identified in the Pos Protocol parameter.
>>>Major Version Field	M	First (most significant) element of the version number for LPP Positioning Protocol, range: (0..255)
>>>Technical Version Field	M	Second element of the version number for LPP Positioning Protocol, range: (0..255)
>>>Editorial Version Field	M	Third (least significant) element of the version number for LPP Positioning Protocol, range: (0..255)
>>Pos Protocol Version LPPe	CV	Describes the protocol version of LPPe Positioning Protocol. It is required if LPPe is identified in the Pos Protocol parameter.

>>>Major Version Field	M	First (most significant) element of the version number for LPPe Positioning Protocol, range: (0..255)
>>>Minor Version Field	M	Second element of the version number for LPPe Positioning Protocol, range: (0..255)
>Service Capabilities	CV	The service capabilities of the SET are described in this parameter. The SET MAY send this parameter in SUPL START, SUPL POS INIT, SUPL TRIGGERED START, SUPL AUTH REQ and SUPL END. This parameter is mandatory in SUPL TRIGGERED START in the case of a Network Initiated session. The purpose of this parameter is to inform the H-SLP about the service capabilities of the SET
>>services supported	M	Defines the supported services by the SET. Only Network Initiated services are relevant in this context. Zero or more of the following services are supported: • Periodic Trigger • Area Event Trigger
>>reporting capabilities	CV	Defines the reporting capabilities of the SET. This parameter is only required if periodic triggers are supported by the SET in which case the parameter is mandatory.
>>>minimum interval between fixes	M	Defines the minimum interval between fixes allowed by the SET. This parameter is used by the H-SLP to avoid conflict between the desired interval between fixes and the SET's capabilities. Range: 1 to 3600, Units in seconds.
>>>maximum interval between fixes	O	Defines the maximum interval between fixes allowed by the SET. This parameter is used by the H-SLP to avoid conflict between the desired interval between fixes and the SET's capabilities. This parameter is optional. If not present, no maximum interval between fixes is specified. Range: 1 to 1440, Units in minutes.
>>>rep mode	M	Supported reporting mode(s): • Real time • Quasi real time • Batch reporting (At least one of the three reporting modes must be supported)
>>>batch rep cap	CV	Defines the type of batch reporting capabilities supported by the SET

		(only applicable to quasi real time and batch reporting): • Report position (*true* if reporting of position is allowed, *false* otherwise) • Report measurements (*true* if reporting of measurements is supported, *false* otherwise) • Maximum number of positions (range: 1 to 1024) • Maximum number of measurements (range: 1 to 1024)
>>event trigger capabilities	CV	Defines the event trigger capabilities of the SET. This parameter is only required if area event triggers are supported by the SET in which case the parameter is mandatory.
>>> geo area shapes supported	M	This parameter defines the geographic target area shapes supported by the SET in addition to mandatory circular area: • Elliptical • Polygon
>>> max number of geographical target areas supported	O	This parameter defines the maximum number of geographic target areas the SET supports. (range: 1 to 32) This parameter is optional. If not present, the SET does not support geographical target areas.
>>> max number of Area Id Lists supported	O	This parameter defines the maximum number of Area Id Lists the SET supports. (range: 1 to 32) This parameter is optional. If not present, the SET does not support Area Ids.
>>> max number of Area Ids supported per Area Id List	CV	This parameter defines the maximum number of Area Ids per Area Id List the SET supports. (range: 1 to 256) This parameter is conditional: if max number of Area Id Lists is present, then this parameter MUST be present. Otherwise this parameter MUST NOT be present.
>>session capabilities	M	Defines the session capabilities of the SET: • Total number of simultaneous sessions (range: 1 to 128). • Maximum number of simultaneous periodic triggered sessions (only used for periodic triggers) (range: 1 to 32). • Maximum number of simultaneous area event triggered sessions (only used for

		area event triggers) (range: 1 to 32).
> supported bearers	O	This parameter indicates which bearers the SET supports Note that each bearer in this list must be supported by the SET, but not all at the same time. The parameter indicates support for one or more of the following: • GSM • WCDMA/TD-SCDMA • CDMA • HRPD • UMB • LTE • WLAN • WiMAX • NR

Table 33: SET capabilities Parameter

10.11 Location ID

Parameter	Presence	Value/Description
Location ID	-	Defines the current serving cell, current serving WLAN AP or current serving WiMAX BS information of the SET.
>Cell Info	M	The following cell IDs are supported: • GSM Cell Info • WCDMA/TD-SCDMA Cell Info • CDMA Cell Info • HRPD Cell Info • UMB Cell Info • LTE Cell Info • WLAN AP Info • WiMAX BS Info • NR Cell Info
>Status	M	Describes whether or not the cell, WLAN AP or WiMAX BS info is: • Not Current, last known cell/AP info • Current, the present cell/AP info • Unknown (i.e. not known whether the cell/AP id is current or not current)

		NOTE: The Status parameter does NOT apply to WCDMA/TD-SCDMA optional parameters (Frequency Info, Primary Scrambling Code/Cell Parameters ID and Measured Results List). Frequency Info, Primary Scrambling Code/Cell Parameters ID and Measured Results List, if present, are always considered to be correct for the current cell.

Table 34: Location ID Parameter

10.11.1 GSM Cell Info

The gsmCell parameter defines the parameter of a GSM radio cell.

Parameter	Presence	Value/Description
Gsm Cell Info	-	GSM Cell ID
>MCC	M	Mobile Country Code, range: (0..999)
>MNC	M	Mobile Network Code, range: (0..999)
>LAC	M	Location Area Code, range: (0..65535)
>CI	M	Cell Identity, range: (0..65535)
>NMR	O	Network Measurement Report – can be present for 1 to 15 cells.
>>ARFCN	M	ARFCN, range: (0..1023)
>>BSIC	M	BSIC, range: (0..63)
>>RXLev	M	RXLEV, range: (0..63)
>TA	O	Timing Advance, range: (0..255)

Table 35: GSM Cell Info Parameter

10.11.2 WCDMA/TD-SCDMA Cell Info

The wcdmaCell parameter defines the parameter of a WCDMA/TD-SCDMA radio cell.

Parameter	Presence	Value/Description
Wcdma/TD-SCDMA Cell Info	-	WCDMA/TD-SCDMA Cell ID
>MCC	M	Mobile Country Code, range: (0..999)
>MNC	M	Mobile Network Code, range: (0..999)
>UC-ID	M	Cell Identity, range: (0..268435455). NOTE: this information element contains the Cell Identity sent in SIB3 [3GPP RRC]
>Frequency Info	O	Frequency info can be: fdd: uarfcn-UL, ra nge: (0..16383) uarfcn-DL, ra nge: (0..16383) In case of fdd, uarfcn-UL is optional while uarfcn-DL is mandatory. If uarfcn-UL is not present, the default duplex distance defined for the operating frequency band shall be used [3GPP RRC].

		Tdd: uarfcn-Nt, range: (0..16383) **NOTE**: Frequency Info and Primary Scrambling Code are always those of the current cell.
>Primary Scrambling Code	O	Primary Scrambling Code, range: (0..511) **NOTE**: This field applies only to WCDMA **NOTE**: Frequency Info and Primary Scrambling Code/Cell Parameters ID are always those of the current cell.
>Measured Results List	O	Network Measurement Report for WCDMA/TD-SCDMA comprising both intra- and/or inter-frequency cell measurements (as per [3GPP RRC]).
>Cell Parameters ID	O	Cell Parameters ID, range: (0..127) **NOTE**: This field applies only to TD-SCDMA **NOTE**: Frequency info and Cell Parameters ID are always those of the current cell. **NOTE**: This parameter is mandatory for a TD-SCDMA cell
>Timing Advance	O	Timing advance **NOTE**: This field applies only to TD-SCDMA
>> TA	M	Timing advance measurement, range (0..8191) For 1.28Mcps TDD, it means uplink timing advance applied by the UE (as per 5.1.14 [3GPP 25.225]) For 3.84Mcps TDD, it means absolute timing advance value to be used to avoid large delay spread at the NodeB (as per 10.3.6.95 [3GPP RRC] and as per 10.3.6.95a [3GPP RRC]); In such case, 256 to 8191 value is spare; For 7.68Mcps TDD, it means absolute timing advance value to be used to avoid large delay spread at the NodeB (as per 10.3.6.95 [3GPP RRC] and as per 10.3.6.95a [3GPP RRC]); In such case, 512 to 8191 value is spare;

>>TA Resolution	O	Measurement resolution. Supported resolutions are 0.125, 0.5 and 1 chips. If this field is missing, the resolution is 0.125 chips.
>> Chip Rate	O	UTRA-TDD chip rate. Supported chip rates are 1.28, 3.84 and 7.68 Mchips/s. If this field is missing, the rate is 1.28 Mchips/s.

Table 36: WCDMA/TD-SCDMA Cell Info Parameter

10.11.3 LTE Cell Info

The LTE Cell Info parameter defines the parameter of a LTE radio cell.

Parameter	Presence	Value/Description
LTE Cell Info	-	LTE Cell ID. Parameter definitions in [3GPP 36.321].
>CellGlobalIdEUTRA	M	
>>PLMN-Identity	M	
>>>MCC	M	Mobile Country Code, range: (0..999)
>>>MNC	M	Mobile Network Code, range: (0..999)
>>CI	M	Cell Identity, length 28 bits.
>PhysCellId	M	Physical Cell ID, range: (0..503)
>TrackingAreaCode	M	Tracking Area Code, length 16 bits When ServingInformation5G is present, this parameter SHOULD be set to all zeros.
>RSRPResult	O	Reference Signal Received Power, range: (0..97) as in [3GPP 36.133]. If the parameter RSRPResult-EXT1 is included, this parameter SHALL either be excluded or set to 0.
>RSRQResult	O	Reference Signal Received Quality, range: (0..34) as in [3GPP 36.133]. If the parameter RSRQResult-EXT1 is included and is in the range 0 to 34, this parameter SHALL be included and set equal to RSRQResult-EXT1. If the parameter RSRQResult-EXT1 is included and is outside the range 0 to 34, this parameter SHALL either be excluded or set to 0 when RSRQResult-EXT1 is negative or to 34 when RSRQResult-EXT1 is positive.
>TA	O	Currently used Timing Advance value, range: (0..1282) (N_{TA}/16 as per [3GPP 36.213]).
>Measured Results List EUTRA	O	Network Measurement Report for LTE ([3GPP LTE]).

>>PhysCellId	M	Physical Cell ID, range: (0..503)
>>cgi-Info	O	
>>>CellGlobalIdEUTRA	M	
>>>TrackingAreaCode	M	Tracking Area Code, length 16 bits When NeighbourInformation5G is present, this parameter SHOULD be set to all zeros if included.
>>MeasResult	M	
>>>RSRPResult	O	Reference Signal Received Power, range: (0..97) as in [3GPP 36.133]. If the parameter RSRPResult-EXT2 is included, this parameter SHALL either be excluded or set to 0.
>>>RSRQResult	O	Reference Signal Received Quality, range: (0..34) as in [3GPP 36.133]. If the parameter RSRQResult-EXT2 is included and is in the range 0 to 34, this parameter SHALL be included and set equal to RSRQResult-EXT2. If the parameter RSRQResult-EXT2 is included and is outside the range 0 to 34, this parameter SHALL either be excluded or set to 0 when RSRQResult-EXT2 is negative or to 34 when RSRQResult-EXT2 is positive.
>>EARFCN	CV	This parameter represents E-UTRA ARFCN. This parameter is conditional and must be sent if cgi-Info is not present. If the cgi-Info is present, this parameter may be sent. If the above conditions for sending this parameter are met but the value of E-UTRA ARFCN is greater than 65535, this parameter SHALL be set to 65535. EARFCN, range: (0..65535)
>>EARFCN-EXT	CV	If the parameter EARFCN (immediately above) is sent and the value of E-UTRA ARFCN is > 65535, then this parameter SHALL be sent and set to the value of E-UTRA ARFCN. EARFCN-EXT, range: (65536..262143)
>>RSRPResult-EXT2	O	Reference Signal Received Power extension, range: (-17..-1) as in [3GPP 36.133]. This parameter is optional.
>>RSRQResult-EXT2	O	Reference Signal Received Quality extension, range: (-30..46) as in [3GPP 36.133]. This parameter is optional.

>>RS-SINRResult2	O	Reference Signal Signal to Noise and Interference Ratio, range: (0..127) as in [3GPP 36.133]. This parameter is optional.
>>NeighbourInformation5G	O	This parameter MAY be included for an LTE neighbour cell connected to a 5GCN
>>>TrackingAreaCode5G	O	Tracking Area Code, length 24 bits
>EARFCN	O	This parameter represents E-UTRA ARFCN. This parameter is optional. If the value of E-UTRA ARFCN is > 65535 then this parameter SHALL be set to 65535. EARFCN, range: (0..65535)
>EARFCN-EXT	CV	If the parameter EARFCN (immediately above) is sent and the value of E-UTRA ARFCN is > 65535, then this parameter SHALL be sent and set to the value of E-UTRA ARFCN. EARFCN-EXT, range: (65536..262143)
>RSRPResult-EXT1	O	Reference Signal Received Power extension, range: (-17..-1) as in [3GPP 36.133]. This parameter is optional.
>RSRQResult-EXT1	O	Reference Signal Received Quality extension, range: (-30..46) as in [3GPP 36.133]. This parameter is optional.
>RS-SINRResult1	O	Reference Signal Signal to Noise and Interference Ratio, range: (0..127) as in [3GPP 36.133]. This parameter is optional.
>ServingInformation5G	CV	This parameter SHALL be included for an LTE serving cell connected to a 5GCN
>>TrackingAreaCode5G	M	Tracking Area Code, length 24 bits

Table 37: LTE Cell Info

10.11.4 CDMA Cell Info

The cdmaCell Cell Info parameter defines the parameter of a CDMA radio cell.

Parameter	Presence	Value/Description
Cdma Cell Info	-	CDMA Cell ID
>NID	M	Network ID, range: (0..65535)
>SID	M	System ID, range: (0..32767)
>BASEID	M	Base Station ID, range: (0..65535)
>BASELAT	M	Base Station Latitude, range: (0..4194303)

>BASELONG	M	Base Station Longitude, range: (0..8388607)
>REFPN	M	Base Station PN Number, range: (0..511)
>WeekNumber	M	GPS Week number, range: (0..65535)
>Seconds	M	GPS Seconds, range: (0..4194303)

Table 38: CDMA Cell Info

10.11.5 HRPD Cell Info

The HRPD Cell Info parameter defines the parameter of a HRPD radio cell.

Parameter	Presence	Value/Description
Hrpd Cell Info	-	HRPD Cell ID
>SECTORID	M	Sector ID, length 128 bits
>BASELAT	M	Base Station Latitude, range: (0..4194303)
>BASELONG	M	Base Station Longitude, range: (0..8388607)
>WeekNumber	M	GPS Week number, range: (0..65535)
>Seconds	M	GPS Seconds, range: (0..4194303)

Table 39: HRPD Cell Info

10.11.6 UMB Cell Info

The UMB Cell Info parameter defines the parameter of a UMB radio cell.

Parameter	Presence	Value/Description
Umb Cell Info	-	UMB Cell ID
>SECTORID	M	Sector ID, length 128 bits
>MCC	M	Mobile Country Code, range: (0..999)
>MNC	M	Mobile Network Code, range: (0..999)
>BASELAT	M	Base Station Latitude, range: (0..4194303)
>BASELONG	M	Base Station Longitude, range: (0..8388607)
>WeekNumber	M	GPS Week number, range: (0..65535)
>Seconds	M	GPS Seconds, range: (0..4194303)

Table 40: UMB Cell Info

10.11.7 WLAN AP Info

The WLAN AP Info parameter defines the parameters of a WLAN access point [IEEE 802.11].

Parameter	Presence	Value/Description
WLAN AP Info	-	WLAN Access Point ID
>AP MAC Address	M	Access Point MAC Address
>AP Transmit Power	O	AP Transmit power in dBm
>AP Antenna Gain	O	AP antenna gain in dBi
>AP S/N	O	AP Signal to Noise ratio of a beacon, probe response or measurement pilot frame received at the SET in dB.
> Device Type	O	Options are:

		802.11a, 802.11b, 802.11g, 802.11n, 802.11ac and 802.11ad device. Future networks are permitted. Note: the device type refers to the type being used for signalling as opposed to the capability of the AP (e.g., an 802.11n capable AP in e.g., 802.11a signalling mode).
>AP Signal Strength	O	AP signal strength of a beacon, probe response or measurement pilot frame received at the SET in dBm. Range: (-127..128)
>AP Channel/Frequency	O	AP channel number of the reported WLAN AP
>Round Trip Delay	O	Round Trip Delay (RTD) between the SET and AP
>>RTD Value	M	Measured RTD value
>>RTD Units	M	Units for RTD value and RTD accuracy – 0.1, 1, 10, 100 or 1000 nanoseconds
>>RTD Accuracy	O	RTD standard deviation in relative units
>SET Transmit Power	O	SET Transmit power in dBm
>SET Antenna Gain	O	SET antenna gain in dBi
>SET S/N	O	SET Signal to Noise received at the AP in dB
>SET Signal Strength	O	SET signal strength received at the AP in dBm
>AP Reported Location	O	Location of the Access Point as reported by the AP. This parameter presents the AP's reported location using legacy encoding (this parameter is now deprecated).
>AP Rep Location	O	This parameter represents the AP's Location: - As defined in [IEEE 802.11] and [RFC 3825] - Future formats (Future formats may be supported as they become available).
>AP Signal Strength Delta	CV	This parameter is conditional and may be used if the AP Signal Strength IE is used. Otherwise this parameter MUST NOT be used. Range: INTEGER (0..1) Units: 0.5 dB This parameter is used when the AP Signal Strength resolution is 0.5 dB (as opposed to 1.0 dB when this parameter is not used). The AP Signal

		Strength is then: (AP Signal Strength + AP Signal Strength Delta).
>AP S/N Delta	CV	This parameter is conditional and may be used if the AP S/N parameter is used. Otherwise this parameter MUST NOT be used. Range: INTEGER (0..1) Units: 0.5 dB This parameter is used when the AP S/N resolution is 0.5 dB (as opposed to 1.0 dB when this parameter is not used). The AP S/N is then: (AP S/N + AP S/N Delta).
>SET Signal Strength Delta	CV	This parameter is conditional and may be used if the SET Signal Strength parameter is used. Otherwise this parameter MUST NOT be used. Range: INTEGER (0..1) Units: 0.5 dB This parameter is used when the SET Signal Strength resolution is 0.5 dB (as opposed to 1.0 dB when this parameter is not used). The SET Signal Strength is then: (SET Signal Strength + SET Signal Strength Delta).
>SET S/N Delta	CV	This parameter is conditional and may be used if the SET S/N parameter is used. Otherwise this parameter MUST NOT be used. Range: INTEGER (0..1) Units: 0.5 dB This parameter is used when the SET S/N resolution is 0.5 dB (as opposed to 1.0 dB when this parameter is not used). The SET S/N is then: (SET S/N + SET S/N Delta).
>Operating Class	O	Operating Class as defined in [IEEE 802.11]
>AP SSID	O	SSID of the wireless network served by the AP
>AP PHY Type	O	*This field provides the IEEE 802.11 PHY and media type. The enumerated values are as follows:*

		• *Unknown: specifies an unknown or uninitialized PHY type.* • *Any: specifies any PHY type.* • *Fhss: specifies a frequency-hopping spread-spectrum (FHSS) PHY.* • *Dsss: specifies a direct sequence spread spectrum (DSSS) PHY type.* • *Irbaseband: specifies an infrared (IR) baseband PHY type.* • *Ofdm: specifies an orthogonal frequency division multiplexing (OFDM) PHY type.* • *Hrdsss: specifies a high-rate DSSS (HRDSSS) PHY type.* • *Erp: specifies an extended rate PHY type (ERP).* • *Ht: specifies the 802.11n PHY type.* • *Ihv: specifies a PHY type that is developed by an independent hardware vendor (IHV).*
>SET MAC Address	O	The MAC Address by which the SET is known to the WLAN AP

Table 41: WLAN AP Info

10.11.8 WiMAX BS Info

The WiMAX BS Info parameter defines the parameters of a WiMAX base station [IEEE 802.16-2004].

Parameter	Presence	Value/Description
WiMAX BS Info	-	WiMAX Base Station Info
>BS ID	M	Base Station Identifier Bit string of fix length of 48
>RTD measurement	O	Round Trip Delay (RTD) or relative RTD measurement between the SET and the serving BS
>>Round Trip Delay	M	Round Trip Delay (RTD) between the SET and the serving BS in units of 10 ns Range (0 .. 65535)
>>Round Trip Delay Uncertainty	O	Standard deviation of the Round Trip Delay measurement in units of 10 ns Range (0 .. 1023)
>WiMAX NMR List	O	WiMAX network measurements. Repeated 1-32 times.
>> BS ID	M	Base Station for the serving and neighboring cell measurement. Bit string of fixed length of 48
>> Relative Delay	O	Relative Delay between the SET and the neighboring BS in units of 10 ns. Not applicable for the serving BS. Range (-32768..32767)

>> Relative Delay uncertainty	O	Relative Delay uncertainty in units of 10 ns. Range (0 .. 1023)
>>BS Signal Strength	O	BS signal strength received at the SET in dBm Range (0 .. 255)
>>BS Signal Strength Uncertainty	O	Standard deviation of BS signal strength received at the SET in Db Range (0 .. 63)
>>BS Tx Power	O	BS equivalent isotropic transmit power Range (0 .. 255)
>>BS CINR	O	BS Carrier to Noise and Interference Ratio as received at the SET in Db Range (0 .. 255)
>>BS CINR Uncertainty	O	Standard deviation of BS Carrier to Noise and Interference Ratio as received at the SET in Db Range (0 .. 63)
>> BS Location	O	Location of the BS as reported by the BS
>>>Location Encoding	M	Location encoding description - LCI as per [RFC 3825] - ASN.1 as per [X.694]
>>>>Location Data	M	Location Data
>>>>>Location Accuracy	O	Location Accuracy in units of 0.1m Integer (0..4294967295)
>>>>>Location Value	M	Location value in the format defined in Location Encoding Octet string of fix length of 128

Table 42: WiMAX BS Info

10.11.9 NR Cell Info

The NR Cell Info parameter defines the parameters of an NR radio cell.

Parameter	Presence	Value/Description
NR Cell Info	-	NR Cell Information
>ServingCellInformation	M	Information for the primary and any secondary serving cells as in [3GPP NR]. The first listed serving cell SHALL be the primary cell. Up to 32 serving cells can be included.
>>PhysCellId	M	Physical Cell ID, range: (0..1007) as in [3GPP NR].
>>ARFCN-NR	M	ARFCN used for SSB measurements or CSI-RS measurements, range (0.. 3279165) as in [3GPP NR].
>>CellGlobalIdNR	M	Cell Global ID NR as in [3GPP 38.413] and [3GPP NR].

>>>PLMN-Identity	M	
>>>>MCC	M	Mobile Country Code, range: (0..999)
>>>>MNC	M	Mobile Network Code, range: (0..999)
>>>CI	M	Cell Identity, length 36 bits.
>>TrackingAreaCode	M	Tracking Area Code, length 24 bits as in [3GPP 24.501] and [3GPP 38.413] and [3GPP NR].
>>SSB-Measurements	O	Measurements based on Synchronization Signal Block as in [3GPP 38.133], [3GPP 38.215] and [3GPP NR].
>>>RSRPResult	O	Reference Signal Received Power, range: (0..127).
>>>RSRQResult	O	Reference Signal Received Quality, range: (0..127).
>>>SINRResult	O	Signal to Noise and Interference Ratio, range: (0..127).
>>CSI-RS-Measurements	O	Measurements based on Channel-State Information Reference Signal as in [3GPP 38.133], [3GPP 38.215] and [3GPP NR].
>>>RSRPResult	O	Reference Signal Received Power, range: (0..127).
>>>RSRQResult	O	Reference Signal Received Quality, range: (0..127).
>>>SINRResult	O	Signal to Noise and Interference Ratio, range: (0..127).
>>TA	O	Currently used Timing Advance (T_A) value, range: (0..3846) as in [3GPP 38.213].
>>ARFCN-Type	O	This field indicates the type of the ARFCN-NR. Values are: - ssb (ARFCN of the first RE of SSB's RB#10) - csi-rs (ARFCN of the point A of the CSI-RS) The default value when not included is ssb.
>>SystemFrameNumber	O	This field specifies the system frame number of the measured cell during which the measurements were performed. This field shall be included when available. Value range: (0..1023) as defined in [3GPP NR].
>>SSB-IndexList-Measurements	O	Measurements for individual SSB resources as in [3GPP 38.133], [3GPP 38.215] and [3GPP NR]. Up to 64 SSB resources can be included.
>>>SSB-Index	M	Index of the SSB resource. Value range: (0..63).
>>>SSB-Measurements	M	Measurements for the SSB resource.

>>>>RSRPResult	O	Reference Signal Received Power, range: (0..127).
>>>>RSRQResult	O	Reference Signal Received Quality, range: (0..127).
>>>>SINRResult	O	Signal to Noise and Interference Ratio, range: (0..127).
>>CSI-RS-IndexList-Measurements	O	Measurements for individual CSI-RS resources as in [3GPP 38.133], [3GPP 38.215] and [3GPP NR]. Up to 64 CSI-RS resources can be included.
>>>CSI-RS-Index	M	Index of the CSI-RS resource. Value range: (0..95).
>>>CSI-RS-Measurements	M	Measurements for the CSI-RS resource.
>>>>RSRPResult	O	Reference Signal Received Power, range: (0..127).
>>>>RSRQResult	O	Reference Signal Received Quality, range: (0..127).
>>>>SINRResult	O	Signal to Noise and Interference Ratio, range: (0..127).
>MeasuredResultsListNR	O	Measurement Results for neighbour NR cells as in [3GPP NR]. Up to 32 neighbour cells can be included.
>>PhysCellId	M	Physical Cell ID, range: (0..1007)
>>ARFCN-NR	M	ARFCN used for SSB measurements or CSI-RS measurements, range (0.. 3279165) as in [3GPP NR].
>>CellGlobalIdNR	O	Cell Global ID NR
>>>PLMN-Identity	M	
>>>>MCC	M	Mobile Country Code, range: (0..999)
>>>>MNC	M	Mobile Network Code, range: (0..999)
>>>CI	M	Cell Identity, length 36 bits.
>>TrackingAreaCode	O	Tracking Area Code, length 24 bits
>>SSB-Measurements	O	Measurements based on Synchronization Signal Block as in [3GPP 38.133], [3GPP 38.215] and [3GPP 38.331].
>>>RSRPResult	O	Reference Signal Received Power, range: (0..127).
>>>RSRQResult	O	Reference Signal Received Quality, range: (0..127).
>>>SINRResult	O	Signal to Noise and Interference Ratio, range: (0..127).
>>CSI-RS-Measurements	O	Measurements based on Channel-State Information Reference Signal as in [3GPP 38.133], [3GPP 38.215] and [3GPP NR].
>>>RSRPResult	O	Reference Signal Received Power, range: (0..127).

>>>RSRQResult	O	Reference Signal Received Quality, range: (0..127).
>>>SINRResult	O	Signal to Noise and Interference Ratio, range: (0..127).
>>ARFCN-Type	O	This field indicates the type of the ARFCN-NR. Values are: - ssb (ARFCN of the first RE of SSB's RB#10) - csi-rs (ARFCN of the point A of the CSI-RS) The default value when not included is ssb.
>>SystemFrameNumber	O	This field specifies the system frame number of the measured cell during which the measurements were performed. This field shall be included when available. Value range: (0..1023) as defined in [3GPP NR].
>>SSB-IndexList-Measurements	O	Measurements for individual SSB resources as in [3GPP 38.133], [3GPP 38.215] and [3GPP NR]. Up to 64 SSB resources can be included.
>>>SSB-Index	M	Index of the SSB resource. Value range: (0..63).
>>>SSB-Measurements	M	Measurements for the SSB resource.
>>>>RSRPResult	O	Reference Signal Received Power, range: (0..127).
>>>>RSRQResult	O	Reference Signal Received Quality, range: (0..127).
>>>>SINRResult	O	Signal to Noise and Interference Ratio, range: (0..127).
>>CSI-RS-IndexList-Measurements	O	Measurements for individual CSI-RS resources as in [3GPP 38.133], [3GPP 38.215] and [3GPP NR]. Up to 64 CSI-RS resources can be included.
>>>CSI-RS-Index	M	Index of the CSI-RS resource. Value range: (0..95).
>>>CSI-RS-Measurements	M	Measurements for the CSI-RS resource.
>>>>RSRPResult	O	Reference Signal Received Power, range: (0..127).
>>>>RSRQResult	O	Reference Signal Received Quality, range: (0..127).
>>>>SINRResult	O	Signal to Noise and Interference Ratio, range: (0..127).

Table 42a: NR Cell Info

10.12 Notification

Parameter	Presence	Value/Description

Notification	-	Describes the notification/verification mechanism to be applied.

>Notification type	M	Type of notification:
		• No notification & no verification
		• Notification only
		• Notification and verification
		  ○ Allowed on no answer (if no answer is received from the SET User, the SET will assume that user consent has been granted and will proceed)
		  ○ Denied on no answer (if no answer is received from the SET User, the SET will assume that user consent has been denied and will abort)
		• Privacy override (is used for preventing notification and verification without leaving any traces of a performed position fix or position fix attempt in terms of log files etc. on the SET).
		For "Allowed on no answer" and "Denied on no answer", the SET SHOULD return a response to the H-SLP within 40 seconds of receiving the SUPL INIT. This allows the ST2 timer on the H-SLP to be configured to take user response time into account along with SUPL INIT delivery time, secure session initiation, etc.

>Encoding type	CV	Encoding type is required when Notification type is set to Notification only or Notification and verification and when RequestorID or ClientName is used. • ucs2 • gsm-default • UTF-8 **NOTE**: gsm-default refers to the 7-bit default alphabet and the SMS packing specified in [3GPP 23.038].
>RequestorID	O	Identity of the Requestor
>RequestorType	CV	Indicates the RequestorID type. It is required if RequestorID is present. The RequestorID type can be one of the following:

		• Logical name • MSISDN • E-mail address • URL • SIP URI • IMS public identity • MIN • MDN
>ClientName	O	The name of the Location Application.
>ClientNameType	CV	Indicates the type of the client name. It is required if ClientName is present. The type of the client name can be one of the following: • Logical name • MSISDN • E-mail address • URI • SIP URL • IMS public identity • MIN • MDN
Emergency Call Location	CV	Indicates location in association with an emergency call. Required in a SUPL INIT for an emergency call.

Table 43: Notification Parameter

10.13 QoP

Parameter	Presence	Value/Description
QoP	-	Describes the desired Quality of Position
>Horizontal accuracy	M	Horizontal accuracy as defined in [3GPP GAD]
>Vertical accuracy	O	Vertical accuracy as defined in [3GPP GAD]
> Maximum Location Age	O	Maximum tolerable age of position estimates used for cached position fixes. Units in seconds from 0 to 65535.
>Delay	O	Values as defined for element Response Time in [3GPP RRLP]: 2^N, N from (0..7), unit is seconds **NOTE**: the Delay value should be applied to the timer of the used

		positioning protocol i.e. any positioning protocol specific timers (timers within the SUPL POS block) MUST be equal to the Delay value. If the Response Time parameter is present and is supported, the SLP SHALL NOT use the Delay parameter.
>Response Time	O	Units in seconds from (1..128) **NOTE**: It is OPTIONAL for the SLP to support this parameter. If supported, the SLP SHALL apply the Response Time value to the timer of the used positioning protocol (i.e. *RequiredResponseTime* for RRLP *ResponseTime* for LPP).

Table 44: QoP

10.14 Session ID

The Session ID SHALL be a unique value, consisting of two parts, a SET value (SET Session ID) (see section 10.14.1) concatenated with an SLP value (SLP Session ID) (see section 10.14.2).

Parameter	Presence	Value/Description
SET Session ID	M	Part of Session ID pertaining to the SET
SLP Session ID	M	Part of Session ID pertaining to the SLP

Table 45: Session ID Parameter

For Network-Initiated flows, when sending a SUPL INIT to the SET, the SLP SHALL assign a value to the SLP Session ID, but to save bandwidth, the SLP SHALL not include the SET Session ID in the message. The SET SHALL then assign a value to the SET Session ID when it receives the message. Any further messages SHALL contain the resultant combined Session ID for the remainder of the session.

For SET-Initiated flows, when sending a SUPL START, SUPL TRIGGERED START or SUPL SET INIT message to the SLP, the SET SHALL assign a value to the SET Session ID. The SET will not send an SLP Session ID in these messages since no SLP Session ID yet exists. The SLP SHALL assign a value to the SLP Session ID when it receives one of these messages. All further messages SHALL contain the resultant combined Session ID for the remainder of the session. The exception to this rule is the sending of a SUPL TRIGGERED START message by the SET after receiving a SUPL END message with cause code “no SUPL coverage” during a V-SLP to V-SLP handover. In order to allow the SLP to continue (i.e. re-establish) the triggered SUPL session, the SET must include the full session id (i.e. SET Session ID and SLP Session ID) in the SUPL TRIGGERED START message (the full session id is the current active session id i.e. the session id received in the SUPL END message which initiated the V-SLP to V-SLP handover).

The Session ID SHALL allow for multiple simultaneous sessions on both the SLP and the SET. The main purpose of the Session ID is to allow both SLP and SET to distinguish between multiple simultaneous sessions. Taking advantage of this capability, the SLP SHALL be capable of supporting multiple SUPL sessions with the same SET over any number of one or more secure sockets.

10.14.1 SET Session ID

This section describes the construct of the SET Session ID.

Parameter	Presence	Value/Description

Session ID	M	Session identifier, unique from SET perspective. This value SHALL be unique over all concurrently active ULP sessions on that particular SET. This value may be reused by the SET after the ULP session for which it is being used has ended.
SET ID	M	SET identity value This parameter can be of type • MSISDN • MDN • MIN • IMSI • IMEI • NAI • IPAddress o Ipv4 o Ipv6 Note 1: IMEI SHALL NOT be used unless the SLP indicates support for SUPL ver 2.0.3 or greater. Note 2: For 5G access, SUPI is treated as synonymous with IMSI and PEI is treated as synonymous with IMEI.

Table 46: SET Session ID Parameter

10.14.2 SLP Session ID

This section describes the construct of the SLP Session ID.

Parameter	Presence	Value/Description
Session ID	M	Session identifier, unique from SLP perspective. This value SHALL be unique over all concurrently active ULP sessions on that particular SLP. This value may be reused by the SLP after the ULP session for which it is being used has ended. This parameter is written into a 4-octet-string.
SLP ID	M	The identity of the SLP. This parameter can be of type • IPAddress o Ipv4 o Ipv6 • FQDN.

		NOTE: SLP ID MAY be of different type and different value compared to the parameter SLP address in the messages SUPL INIT and SUPL RESPONSE.

Table 47: SLP Session ID Parameter

10.15 SLP Mode

Parameter	Presence	Value/Description
SLP Mode	-	Describes the mode that the SLP (SPC for non-proxy mode) uses. This parameter can be of type Proxy mode Non-proxy mode

Table 48: SLP Mode Parameter

10.16 MAC

Parameter	Presence	Value/Description
MAC	-	Not used in SUPL 2.0 but empty placeholder remains for SUPL 1.0 backwards compatibility (needed so that a SUPL 2.0 SET can still decode a SUPL 1.0 SUPL INIT message).

Table 49: MAC Parameter

10.17 Key Identity

Parameter	Presence	Value/Description
Key Identity	-	Not used in SUPL 2.0 but empty placeholder remains for SUPL 1.0 backwards compatibility (needed so that a SUPL 2.0 SET can still decode a SUPL 1.0 SUPL INIT message).

Table 50: Key Identity Parameter

10.18 Ver

Parameter	Presence	Value/Description
Ver	-	Describes the hash of the SUPL INIT message. For further details of the encoding of this parameter, see section 6.1.6.1.

Table 51: Ver Parameter

10.19 Multiple Location IDs

Parameter	Presence	Value/Description
Multiple Location IDs	-	This parameter contains a set of up to MaxLidSize (64) Location ID/Relative Timestamp/Serving Cell Flag data. If Relative Timestamp is

		present, the associated Location ID represents historical data; if Relative Timestamp is absent, the Location ID represents current data.
>Location ID	M	Describes measured globally unique cell/WLAN AP/WiMAX BS identification of the serving cell/WLAN AP/WiMAX BS or cell/WLAN AP/WiMAX BS identification from any receivable radio network. If this information is historical, the Relative Timestamp parameter must be present. If this data is current, the Relative Timestamp parameter need not be present.
>Relative Timestamp	CV	Time stamp of measured location Id relative to "current Location ID" in units of 0.01 sec. Range from 0 to 65535*0.01 sec. Time stamp for current Location Id if present is 0.
>Serving Cell Flag	M	This flag indicates whether the Location ID data represents a serving cell, WLAN AP or WiMAX BS or idle (i.e. camped-on) cell, WLAN AP or WiMAX BS. If set, the Location ID information represents serving cell, WLAN AP or WiMAX BS information; if not set, the Location ID information represents idle mode information or neighbor cell, WLAN AP or WiMAX BS information.

Table 52: Multiple Location IDs Parameter

10.20 Location Triggers

10.20.1 Trigger Type

Parameter	Presence	Value/Description
Trigger Type	--	This parameter defines the trigger type: • Periodic • Area Event

Table 53: Trigger Type Parameters

10.20.2 Trigger Params

Parameter	Presence	Value/Description
Trigger Params	--	This parameter can be of type Periodic Params or Area Event Params

Table 54: Trigger Params Parameters

10.20.2.1 Periodic Params

This section describes the construct of the Periodic Triggers Params. This parameter is required if trigger type is set to Periodic.

Parameter	Presence	Value/Description
Number Of Fixes	M	Describes the number of fixes during the periodic triggered session. (range: 1 to 8639999). For compatibility with MLP and RLP number of fixes * interval between fixes shall not exceed 8639999 (100 days).
Interval Between Fixes	M	Describes the interval between the start of position fixes for periodic trigger. Units in seconds (range: 1 to 8639999)
StartTime	O	It indicates when the SET is to start the first position fix. Start Time is interpreted relative to the current time i.e. to the time when the message containing the parameter is received by the H-SLP or the SET. Start Time is OPTIONAL. If not present, the SET is to start the first fix immediately. Units in seconds (range: 0 to 2678400).

Table 55: Periodic Params Parameters

10.20.2.2 Area Event Params

This section describes the construction of the Area Event trigger Params. This parameter is required if trigger type is set to Area Event.

The Area Event trigger can be one of the following types:

- Entering: the SET reports to the SLP when it first detects that it is inside the predefined area. If repeated reporting is present, the SET then reports once more for each time it detects that it has re-entered the predefined area after having left in the meantime.
- Inside: the SET reports to the SLP when it is within the predefined area.
- Outside: the SET reports to the SLP when it is outside the predefined area.
- Leaving: the SET reports to the SLP when it first detects that it is outside the predefined area. If repeated reporting is present, the SET then reports once more for each time it detect that it has exited the predefined area after having been inside again.

Parameter	Presence	Value/Description
Area Event Type	M	Describes the area event trigger type. This parameter describes what kind of event should trigger a report. The valid types are: • Entering event type • Inside event type

		• Outside event type • Leaving event type
Location estimate	M	The value of this parameter is "true" or "false". If true, it indicates the location estimates is required. If false, it indicates the location estimates is not required. For SET-Initiated triggered services this parameter is not useful and therefore in this case it SHALL be ignored by the SLP.
Repeated reporting	O	Defines the parameters for repeated reporting. If not present, only one report shall be sent. When repeated reporting is used, the SET and the SLP SHALL maintain the triggered event session until the maximum number of reports has been sent, the stop time (if included) has been reached, or either the SET or the SLP has sent a SUPL TRIGGERED STOP or a SUPL END to end the session.
>Minimum Interval Time	M	Defines the minimum time between reports from SET in an Area Event Trigger session. For repeated reporting, an area event trigger cannot be fulfilled unless the minimum time interval has elapsed since the last report. Range: (1..604800). Units in seconds.
>Maximum Number of Reports	M	Defines the maximum number of reports in an Area Event Trigger session. Range: (1..1024)
Start Time	O	Indicates the start of the period when the trigger condition is able to be fulfilled. Start Time is interpreted relative to the current time i.e. to the time when the message containing the parameter is received by the H-SLP or the SET. Start Time is OPTIONAL. If not present, a Start Time of 0 SHALL be used and the trigger condition is allowed to be fulfilled immediately. Units in seconds (range: 0 to 2678400).
Stop Time	O	Stop Time is interpreted relative to the current time i.e. to the time when the message containing the parameter is received by the H-SLP or the SET. It indicates when the SET shall stop the triggered session if it has not already been stopped for other reasons. The

		SET SHALL use a SUPL END message as defined in 5.1.17.4 for Network Initiated sessions. For SET Initiated sessions, the SET SHALL use a SUPL END message as defined in 5.2.17.6. Stop Time is OPTIONAL. If not present, a Stop Time of 8639999 seconds after the start time SHALL be used. Stop Time SHALL be greater than Start Time (if present). Stop Time – Start Time SHALL NOT be more than 8639999 (100 days in seconds) Units in seconds (range: 0 to 11318399).
Geographic Target Area List	O	Defines a list of geographic target areas. This parameter is OPTIONAL. Maximum number of areas are according to element Max Geo Target Area in SET capabilities. If this parameter is not included in the SUPL TRIGGERED RESPONSE message the SET SHALL NOT use the Geographic Target Area List to check if the event trigger condition has been met.
> Geographic Target Area	M	Defines a geographic target area in terms of either: • CircularArea • EllipticalArea • Polygon
Area Id Lists	CV	This parameter contains one or more Area Id lists. This parameter is REQUIRED when the Geographic Target Area List is NOT present and is OPTIONAL when the Geographic Target Areas are present. The maximum number of Area Id lists to be included is determined by the element "Max Area Id List" in SET capabilities. Note: if this parameter is included in the SUPL TRIGGERED START message it is ignored by the SLP.
>Area Id list	M	Each Area Id list consists of a set of Areas Ids. If Geographic Target Area List is present then it may include a Geographic Area Mapping List.
>>Area Id Set	M	A list of area ids. The area ids listed can be any combination of GSM Area Ids, WCDMA/TD-SCDMA Area Ids,

		CDMA Area Ids, HRPD-Area Ids, UMB-Area Ids, LTE-Area Ids, WLAN Area Ids, WiMAX Area Ids or NR Area Ids. Each set can contain from 1 to [MaxAreaId] area ids. Note that if Area Ids of different bearer networks are provided, Border and Within lists can only be considered complete if the SET monitors each of the bearers.
>>Area Id Set Type	CV	This parameter indicates the position of the Area Id Set relative to the Geographic Target Area, This parameter can be of type • "Border" (of the Geographic Target Area) • "Within" (the Geographic Target Area) This parameter is conditional and may only be present when the Geographic Target Area List parameter is present. The "within" area id list is completely within the geographic target area and the "border" area id list combined with the "within" area id list SHOULD completely cover the geographic target area. Both area id lists are mutually exclusive. Using this parameter the SET may decide whether or not to use high precision positioning. (See Appendix B.7 for additional information).
>> Geographic Area Mapping List	O	Represents the Geographic Target Areas to which the Area Id list applies. (Example: 1,3,7,8). The number of entries can be from 1 to the number of Geographic Target Area elements The value of each entry can be from 1 to the number of Geographic Target Area elements.

Table 56: Area Event Parameters

10.20.2.2.1 GSM Area Id

Parameter	Presence	Value/Description
GSM Area Id	-	Can be of type: • Mobile Country Code • Mobile Country Code + Mobile Network Code

		• Mobile Country Code + Mobile Network Code +Location Area Code • Mobile Country Code + Mobile Network Code +Location Area Code + Cell Identity

Table 57: GSM Area Id Parameter

10.20.2.2.2 WCDMA/TD-SCDMA Area Id

Parameter	Presence	Value/Description
WCDMA/TD-SCDMA Area Id	-	Can be of type: • Mobile Country Code • Mobile Country Code + Mobile Network Code • Mobile Country Code + Mobile Network Code +Location Area Code • Mobile Country Code + Mobile Network Code +Location Area Code + Cell Identity

Table 58: WCDMA/TD-SCDMA Area Id Parameter

10.20.2.2.3 LTE Area Id

Parameter	Presence	Value/Description
LTE Area Id	-	Can be of type: • MCC • MCC+MNC • MCC+MNC+Cell-ID

Table 59: LTE Area Id Parameter

10.20.2.2.4 CDMA Area Id

Parameter	Presence	Value/Description
CDMA Area Id	-	Can be of type: • System ID • System ID + Network ID • System ID + Network ID + Base ID

Table 60: CDMA Area Id Parameter

10.20.2.2.5 HRPD Area Id

Parameter	Presence	Value/Description
HRPD Area Id	-	Can be of type: • Sector ID

Table 61: HRPD Area Id Parameter

10.20.2.2.6 UMB Area Id

Parameter	Presence	Value/Description
UMB Area Id	-	Can be of type:

		• Sector ID • Sector ID + MNC • Sector ID + MCC

Table 62: UMB Area Id Parameter

10.20.2.2.7 WLAN Area Id

Parameter	Presence	Value/Description
WLAN Area Id	-	Can be of type: • AP MAC Address

Table 63: WLAN Area Id Parameter

10.20.2.2.8 WiMAX Area Id

Parameter	Presence	Value/Description
WiMAX Area Id	-	Can be of type: • BS ID

Table 64: WiMAX Area Id Parameter

10.20.2.2.9 NR Area Id

Parameter	Presence	Value/Description
NR Area Id	-	Can be of type: • MCC • MCC+MNC • MCC+MNC+Cell-ID

Table 64a: NR Area Id Parameter

10.21 Notification Mode

Parameter	Presence	Value/Description
Notification Mode	-	Describes the mode whether the notification and verification is based on location or not. This parameter can be of type Normal Notification/Verification or Notification/Verification based on location

Table 65: Notification Mode Parameter

10.22 Notification Response

Parameter	Presence	Value/Description
Notification Response	-	Describes the notification/verification response from the user. The response can be either “allowed” or “not allowed”

Table 66: Notification Response Parameter

10.23 Third Party ID

Parameter	Presence	Value/Description
Third Party ID	CV	Indicates the identity of the third party. The type of the third party name can be one of the following: • Logical name • MSISDN • E-mail address • SIP URI • IMS public identity • MIN • MDN • URI

Table 67: Third party ID Parameter

10.24 Supported Network Information

The Supported Network Information parameter defines which type of network measurements the SET is allowed to send as part of the Location ID or Multiple Location IDs in a SUPL POS INIT message. This parameter is used in SUPL INIT, SUPL RESPONSE and SUPL TRIGGERED RESPONSE. The Supported Network Information parameter is also used to inform the SET that UTRAN GPS/GANSS Reference Time is requested by the SLP in case of WCDMA/TD-SCDMA.

The purpose of this parameter is to act as filter to prevent the SET from sending measurement information which the SLP does not support or does not want to process. In interpreting this parameter, the SET shall assume that non-permission overrides permission – i.e. the SET shall only send measurements if no part of the parameter forbids this.

Parameter	Presence	Value/Description
WLAN	M	The value of this parameter is "true" or "false". If true, it indicates the SET is allowed to send WLAN AP information within the Multiple Location IDs. If "false" the SET must not send WLAN AP information within the Multiple Location IDs.
Supported WLAN Information	O	This parameter provides a map of flags indicating which WLAN AP information the SET may send for a current serving WLAN AP in the Location ID parameter. It also indicates which WLAN AP information the SET may send in the Multiple Location IDs parameter when WLAN is set to "true": • AP transmit power • AP antenna gain • AP signal to noise received at the SET • Device type (802.11a/b/g)

		• AP signal strength at the SET • AP channel/frequency of TX/RX • Round trip delay between SET and AP • SET transmit power • SET antenna gain • SET signal to noise received at the AP • SET signal strength at AP • AP location as reported by AP (legacy encoding) Note: the following fields are OPTIONAL. Non-presence means the SET SHALL NOT send the respective information. • AP location as reported by AP (encoded as per IEEE 802.11) • Operating class as defined in 802.11 • SSID of the wireless network served by AP • AP PHY Type as defined in IEEE 802.11 • SET MAC Address by which the SET is known to the AP
Supported WLAN Aps List	O	This parameter provides a list of MAC addresses of Aps indicating WLAN AP information of which Aps the SET should send within the Multiple Location IDs parameter when WLAN is set to "true". It also contains device type information associated with each AP. It MAY also provides contain channel information associated with the AP device types. This information is the superset of all channels supported by the Aps of each device type. It is only intended to help the SET locate supported Aps and does not limit which Aps or WLAN measurements the SET is allowed to return. This parameter must not be sent over SUPL INIT.
GSM	M	The value of this parameter is "true" or "false". If true, it indicates the SET is allowed to send GSM information as part of Location ID within Multiple Location IDs. If "false" the SET must not send GSM information within Multiple Location IDs.
WCDMA/TD-SCDMA	M	The value of this parameter is "true" or "false". If true, it indicates the SET is allowed to send WCDMA

		information as part of Location ID within Multiple Location IDs. If "false" the SET must not send WCDMA/TD-SCDMA information within Multiple Location IDs.
Supported WCDMA/TD-SCDMA Information	CV	This parameter provides a map of flags indicating which WCDMA/TD-SCDMA Network Measurements the SET may send for the current serving cell i.e. in the Location ID parameter. It also indicates which WCDMA/TD-SCDMA network measurements the SET may send in the Multiple Location IDs parameter. This parameter is conditional and only used when the WCDMA/TD-SCDMA flag is set to "true".
CDMA	M	The value of this parameter is "true" or "false". If true, it indicates the SET is allowed to send CDMA information as part of Location ID within Multiple Location IDs. If "false" the SET must not send CDMA information within Multiple Location IDs.
HRPD	M	The value of this parameter is "true" or "false". If true, it indicates the SET is allowed to send HRPD information as part of Location ID within Multiple Location IDs. If "false" the SET must not send HRPD information within Multiple Location IDs.
UMB	M	The value of this parameter is "true" or "false". If true, it indicates the SET is allowed to send UMB information as part of Location ID within Multiple Location IDs. If "false" the SET must not send UMB information within Multiple Location IDs.
LTE	M	The value of this parameter is "true" or "false". If true, it indicates the SET is allowed to send LTE information as part of Location ID within Multiple Location IDs. If "false" the SET must not send LTE information within Multiple Location IDs.
WiMAX	M	The value of this parameter is "true" or "false". If true, it indicates the SET is allowed to send WiMAX information as part of Location ID within Multiple Location ID. If "false" the SET must not send WiMAX information within Multiple Location IDs.
NR	O	The value of this parameter is "true" or "false". If true, it indicates the SET

		is allowed to send NR information as part of Location ID within Multiple Location IDs. If "false" or not present, the SET must not send NR information within Multiple Location IDs.
Historic	M	The value of this parameter is "true" or "false". If true, it indicates the SET is allowed to send historic information as part of Location ID within Multiple Location IDs. If "false" the SET must not send historic information within Multiple Location IDs.
Non-serving	M	The value of this parameter is "true" or "false". If true, it indicates the SET is allowed to send information for non-serving as well as serving cells, WLAN Aps and WiMAX BSs as part of Location ID within Multiple Location IDs. If "false" the SET may only send information for serving cells, serving WLAN Aps or WiMAX BSs within Multiple Location IDs.
UTRAN GPS Reference Time	O	The value of this parameter is "true" or "false". If true, it indicates that the SLP is requesting UTRAN GPS Reference Time (i.e. the UTRAN GPS Reference Time as measured by the SET).
UTRAN GANSS Reference Time	O	The value of this parameter is "true" or "false". If true, it indicates that the SLP is requesting UTRAN GANSS Reference Time (i.e. the UTRAN GANSS Reference Time as measured by the SET).

Table 68: Supported Network Measurements

10.25 Historic Reporting

Parameter	Presence	Value/Description
Historic Reporting	-	This parameter defines the criteria for reporting of stored historical position estimates and/or enhanced cell/sector measurements.
>Allowed Reporting Type	M	This parameter defines what types of stored historical information the SET is allowed to report: – Position estimates only – Enhanced cell/sector measurements only – Both position estimates and enhanced cell/sector measurements
>Reporting Criteria	O	This parameter defines the criteria used to select stored historical position

		and/or enhanced cell/sector measurements for reporting. If this parameter is absent, no criteria apply and all stored historical data consistent with *allowed reporting type, QoP* and *supported network information* is reported by the SET up to a maximum number of 1024 reports.
>>Time Window	O	The *Time Window* parameter specifies a time window to be applied to all reported position estimates and/or enhanced cell/sector measurements. If present, the SET is only allowed to report stored historical position estimates and/or enhanced cell/sector measurements which fall within the time window. If not present, no time window applies. If no time window is specified, the SET SHALL report all stored data consistent with other selection criteria (*allowed reporting type*, *supported network information*, *QoP*, *etc.*).
>>>Start Time	M	The time window's start time. The start time is defined as relative time delta to the current time at the SET. Start time is a negative value (historical data) with a range of -525,600 to 1. The unit is in minutes i.e. the start time is up to one year in the past.
>>>Stop Time	O	The time window's stop time. If not present, the SET SHALL send ALL stored historical position estimates and/or enhanced cell/sector measurements (consistent with other selection criteria i.e. *allowed reporting type*, *supported network information*, *QoP*) beginning at Start Time. Stop time is defined as relative time to current time. Stop time must be AFTER start time. Stop time is a negative value (historical data) with a range of -525,599 to 0. The unit is in minutes.
>>Max Number of Reports	O	This parameter defines the maximum number of reports allowed to be reported by the SET. This parameter is optional. If not present, an implicit maximum number of reports of 1024 applies. The data range is 1 to 65536.
>>Minimum Time Interval	O	This parameter defines the minimum time interval between reported positions and/or enhanced cell/sector measurements. This parameter is optional. If not used, no minimum

		time interval exists. This parameter has a range of 1 to 86,400 in units of one second i.e. the maximum minimum time interval between historical data reports is 24 hours.

Table 69: Historic Reporting Parameter

10.26 UTRAN GPS Reference Time Assistance

The UTRAN GPS Reference Time Assistance parameter represents the UTRAN to GPS time relationship in the SET's current serving cell when this is WCDMA/TD-SCDMA and is sent from the SLP to the SET. This parameter may be used in SUPL POS.

Parameter	Presence	Value/Description
UTRAN GPS Reference Time Assistance	-	The UTRAN GPS Reference Time Assistance parameter provides UTRAN to GPS timing relationship assistance data for the current serving cell of the SET. This parameter is only applicable if the Location ID (lid) information is current.
> UTRAN GPS Reference Time	M	The UTRAN GPS Reference Time parameter describes the timing relationship between GPS time and WCDMA/TD-SCDMA cell frame timing [as per 10.3.7.96[3GPP RRC]].
>>GPS Timing of Cell Frames	M	UTRAN GPS timing of cell frames in steps of 1 UMTS chip [as per 10.3.7.96 [3GPP RRC]]. Range: (0..2322431999999)
>>Mode	O	The Mode value is either: • Primary CPICH Info for FDD [as per 10.3.6.60 [3GPP RRC]]. Or: • Cell Parameters Id for TDD [as per 10.3.6.9 [3GPP RRC]]
>>SFN	M	The SFN which the UTRAN GPS timing of cell frame time stamps. Range: (0..4095)

>GPS Reference Time Uncertainty	O	This element provides the accuracy of the provided relation between GPS and UTRAN time. If "GPS TOW" is the GPS time corresponding to the UTRAN time provided, then the true GPS time lies in the interval ["GPS TOW" – "GPS Reference Time Uncertainty", "GPS TOW" + "GPS Reference Time Uncertainty"]. The uncertainty *r*, expressed in microseconds, is mapped to a number K with the following formula: $r = C*(((1+x)^K)-1)$ with C = 0.0022 and x = 0.18. To encode any higher value of the uncertainty than that corresponding to K=127 in the formula above, or to indicate an undefined value of the "GPS TOW", the same value, K=127, shall be used. [[3GPP RRC] version 7.4.0]
>$T_{UTRAN-GPS}$ Drift Rate	O	Drift rate of UTRAN to GPS timing [as per 10.3.7.96 [3GPP RRC]]. Range (enumerated): -50, -25, -15, -10, -5, -2, -1, 0, 1, 2, 5, 10, 15, 25, 50 Units: 1/256 chips per sec.

Table 70: UTRAN GPS Reference Time Assistance

10.27 UTRAN GPS Reference Time Result

The UTRAN GPS Reference Time Result represents the UTRAN to GPS time relationship as measured by the SET in the case of WCDMA/TD-SCDMA and is sent from the SET to the SLP. This parameter may be used in SUPL POS and SUPL POS INIT.

Parameter	Presence	Value/Description
UTRAN GPS Reference Time Result	-	The UTRAN GPS Reference Time Result parameter describes the timing relationship between GPS time and WCDMA/TD-SCDMA cell frame timing as measured by the SET. This parameter is only applicable if the SET has sent current Location ID (lid) information.
>GPS Timing of Cell Frames	M	GPS Time of Week in units of $1/16^{th}$ UMTS chip [as per 10.3.7.93 [3GPP RRC]]. Range: (0..37158911999999)
>Mode	M	The Mode value is either: • Primary CPICH Info for FDD [as per 10.3.6.60 [3GPP RRC]]. Or: • Cell Parameters Id for TDD [as per 10.3.6.9 [3GPP RRC]]

>SFN	M	The SFN at which the SET timing of cell frames is captured. Range: (0..4095)
>GPS Reference Time Uncertainty	O	This element provides the accuracy of the provided relation between GPS and UTRAN time. If "GPS TOW" is the GPS time corresponding to the UTRAN time provided, then the true GPS time lies in the interval ["GPS TOW" – "GPS Reference Time Uncertainty", "GPS TOW" + "GPS Reference Time Uncertainty"]. The uncertainty *r*, expressed in microseconds, is mapped to a number K with the following formula: $r = C*(((1+x)^K)-1)$ with C = 0.0022 and x = 0.18. To encode any higher value of the uncertainty than that corresponding to K=127 in the formula above, or to indicate an undefined value of the "GPS TOW", the same value, K=127, shall be used. [[3GPP RRC] version 7.4.0]

Table 71: UTRAN GPS Reference Time

10.28 UTRAN GANSS Reference Time Assistance

The UTRAN GANSS Reference Time Assistance parameter represents the UTRAN to GANSS time relationship in the SET's current serving cell when this is WCDMA/TD-SCDMA and is sent from the SLP to the SET. This parameter may be used in SUPL POS.

Parameter	Presence	Value/Description
UTRAN GANSS Reference Time Assistance	-	The UTRAN GANSS Reference Time Assistance parameter provides UTRAN to GANSS timing relationship assistance data for the current serving cell of the SET. This parameter is only applicable if the Location ID (lid) information is current.
>GANSS Day	O	The number of days from the beginning of GANSS system time (mod 8192) [as per 10.3.7.96o [3GPP RRC]].
>GANSS Time ID	M	GANSS Time ID defines the satellite system used in UTRAN-GANSS time relation. 0: Galileo 1: QZSS 2: GLONASS 3: BDS Range: Enumerated (0..15). Values 4 – 15 reserved for future use.

> UTRAN GANSS Reference Time	M	The UTRAN GANSS Reference Time parameter describes the timing relationship between GANSS time and WCDMA/TD-SCDMA cell frame timing [as per 10.3.7.96o [3GPP RRC]].
>>GANSS TOD	M	GANSS time of day in seconds. Range: (0..86399)
>>UTRAN GANSS Timing of Cell Frames	O	UTRAN GANSS timing of cell frames sub-second part of GANSS Time of Day [as per 10.3.7.96o [3GPP RRC]]. Range: (0.. 999999750) by step of 250 ns
>>Mode	O	The Mode value is either: • Primary CPICH Info for FDD [as per 10.3.6.60 [3GPP RRC]]. Or: • Cell Parameters Id for TDD [as per 10.3.6.9 [3GPP RRC]]
>>SFN	M	The SFN which the UTRAN GANSS timing of cell frame time stamps. Range: (0..4095)
>>GANSS TOD Uncertainty	O	Uncertainty of the relation GANSS Time of Day/SFN [as per 10.3.7.96o [3GPP RRC]]. Range (0..127): The uncertainty *r*, expressed in microseconds, is mapped to a number K, with the following formula: $r = C*(((1+x)^K)-1)$, with C = 0.0022 and x = 0.18. [as per 10.3.7.96a [3GPP RRC]].
>$T_{UTRAN-GANSS}$ Drift Rate	O	Drift rate of UTRAN to GANSS timing [as per 10.3.7.96o [3GPP RRC]]. Range (enumerated): -50, -25, -15, -10, -5, -2, -1, 0, 1, 2, 5, 10, 15, 25, 50 Units: ns per sec.

Table 72: UTRAN GANSS Reference Time Assistance

10.29 UTRAN GANSS Reference Time Result

The UTRAN GANSS Reference Time Result represents the UTRAN to GANSS time relationship as measured by the SET in the case of WCDMA/TD-SCDMA and is sent from the SET to the SLP. This parameter may be used in SUPL POS and SUPL POS INIT.

Parameter	Presence	Value/Description
UTRAN GANSS Reference Time Result	-	The UTRAN GANSS Reference Time Result parameter describes the timing relationship between GANSS time and WCDMA/TD-SCDMA cell frame timing as measured by the SET. This parameter is only applicable if the SET has sent current Location ID (lid) information.

>GANSS Time ID	M	GANSS Time ID defines the satellite system used in UTRAN-GANSS time relation. 0: Galileo 1: QZSS 2: GLONASS 3: BDS Range: Enumerated (0..15). Values 4 – 15 reserved for future use.
>UE GANSS Timing of Cell Frames	M	UE GANSS timing of cell frames sub-second part of GANSS Time of Day [as per 10.3.7.93a [3GPP RRC]]. Range: (0.. 86399999999750) by step of 250 ns
>Mode	M	The Mode value is either: • Primary CPICH Info for FDD [as per 10.3.6.60 [3GPP RRC]]. Or: • Cell Parameters Id for TDD [as per 10.3.6.9 [3GPP RRC]]
>SFN	M	The SFN at which the SET timing of cell frames is captured. Range: (0..4095)
>GANSS TOD Uncertainty	O	Uncertainty of the relation GANSS Time of Day/SFN [as per 10.3.7.93a [3GPP RRC]]. Range (0..127): The uncertainty *r*, expressed in microseconds, is mapped to a number K, with the following formula: $r = C*(((1+x)^K)-1)$, with C = 0.0022 and x = 0.18. [as per 10.3.7.96a [3GPP RRC]].

Table 73: UTRAN GANSS Reference Time Result

10.30 SPC_SET_Key

Parameter	Presence	Value/Description
SPC_SET_Key	-	This parameter defines the authentication key used by the SET for H/V-SPC authentication.

Table 74: SPC_SET_Key

10.31 SPC-TID

Parameter	Presence	Value/Description
SPC-TID	-	This parameter defines the transaction ID used for H/V-SPC authentication: ▪ RAND (random number) ▪ SLP FQDN (FQDN of the H-SLP)

Table 75: SPC-TID

10.32 SPC_SET_Key_lifetime

Parameter	Presence	Value/Description
SPC_SET_Key_lifetime	-	This parameter defines the lifetime of SPC_SET_Key. This parameter is optional. If not present, a default value of 24 hours is assumed. The units are in hours and the range is from 1 to 24 hours.

Table 76: SPC_SET_Key_lifetime

10.33 Protection Level

The Protection Level parameter defines the level of protection for the SUPL INIT message.

Parameter	Presence	Value/Description
Protection Level	-	This parameter defines the protection level of the SUPL INIT protection. This parameter is optional. If not present, Null protection is assumed.
> Level	M	• Null Protection • Basic Protection
> Basic Protection Parameters	CV	This parameter is only present if the protection level is *Basic Protection*. • Key-Identifier (= B-TID) • Basic Replay Counter • Basic MAC

Table 77: Protection Level Parameter

10.34 GNSS Positioning Technology

Parameter	Presence	Value/Description
GNSS Positioning Technology	-	A list of GNSS Positioning Technologies (and correction data): • GPS • Galileo • SBAS • Modernized GPS • QZSS • GLONASS • BDS • RTK OSR **NOTE 1**: If RTK OSR is not included, this parameter SHALL NOT be used if posmethod indicates A-GPS or autonomous GPS.

		NOTE 2: If present, RTK OSR is used in association with one or more GNSSs included in this parameter.

Table 78: GNSS Positioning Technology

10.35 Target SET ID

Parameter	Presence	Value/Description

Target SET ID	-	Target SET identity value.
		This parameter can be of type
		• MSISDN
		• MDN
		• MIN
		• IMSI
		• NAI
		• IPAddress
		  ○ Ipv4
		  ○ Ipv6

Table 79: Target SET ID

10.36 Application ID

The Application ID parameter is used to pass information about the end application performing a location request to the SLP. This information is useful for gathering application usage statistical information. Application ID includes the application provider name, application name and optionally the application version. Application ID should only be included on SET Initiated use cases where the SLP is accessed.

Parameter	Presence	Value/Description
Application ID	O	Indicates the application ID for SET initiated call flows.
>App Provider	M	The application provider.
>App Name	M	The application name.
>App Version	O	The application version.

Table 80: Application ID Parameter

10.37 High Accuracy Position

The High Accuracy Position parameter provides a high accuracy estimate of the position of the SET.

Parameter	Presence	Value/Description
High Accuracy Position		This parameter describes the high accuracy position of the SET. The parameter also contains a timestamp and optionally the velocity.
>Timestamp	M	Time when position fix was calculated.

>High Accuracy Position Estimate	M	Contains a high accuracy position estimate.
>>Degrees Latitude	M	Integer ($-2^{31}..2^{31}-1$). The latitude encoded value (N) is derived from the actual latitude X in degrees (-90°..+90°) by this formula: $N = Floor (2^{31} X /90)$ where Floor (x) denotes the greatest integer less than or equal to x and where N is reduced by one when X=90.
>>Degrees Longitude	M	Integer ($-2^{31}.. 2^{31}-1$). The longitude encoded value (N) is derived from the actual longitude X in degrees (-180°..+180°) by this formula: $N = Floor (2^{31} X /180)$ where Floor (x) denotes the greatest integer less than or equal to x and where N is reduced by one when X=180.
>>Uncertainty Semi-Major	M	High accuracy uncertainty of the semi-major axis for the uncertainty ellipse. Refer to [3GPP GAD] for details.
>>Uncertainty Semi-Minor	M	High accuracy uncertainty of the semi-minor axis for the uncertainty ellipse. Refer to [3GPP GAD] for details.
>>Orientation Major Axis	M	Orientation of the major axis for the uncertainty ellipse. Refer to [3GPP GAD] for details.
>>Horizontal Confidence	M	Represents the confidence by which the position of a target entity is known to be within the 2D uncertainty ellipse and is expressed as a percentage. This is an integer (0..100).
>>High Accuracy Altitude information	O	SHALL be present for 3D position information; it SHALL remain absent for 2D position information.
>>>Altitude	M	Integer (-64000..1280000) The altitude a in the range -500 to 10000 meters is related to the encoded value N by this formula: $a = N / 2^7$
>>>Altitude uncertainty	M	High accuracy uncertainty of the altitude. Refer to [3GPP GAD] for details.
>>>Vertical Confidence	M	Represents the confidence by which the 3D position of a target entity is known to be within the uncertainty altitude and is expressed as a percentage. This is an integer (0..100).

>Velocity	O	Speed and bearing values as defined by the Velocity type and as defined in [3GPP GAD]

Table 81: High Accuracy Position Parameter

The definition and coding of the high accuracy position estimate parameter is based on [3GPP GAD]. The Datum used for all positions are WGS-84.

10.38 Serving AMF Identifier

The Serving AMF Identifier indicates the serving AMF for the SET as defined in [3GPP 23.003]. This parameter is required when the SLP indicates positioning using NR Multi-RTT, NR UL-TDOA or NR UL-AoA and when the SET also supports this positioning method.

Parameter	Presence	Value/Description
AMF Region ID	M	This parameter indicates the AMF region and is an 8 bit value.
AMF Set ID	M	This parameter indicates the AMF Set and is a 10 bit value.
AMF Pointer	M	This parameter is a pointer to an AMF and is a 6 bit value.

Table 81A: Serving AMF Identifier Parameters

11.ASN.1 Encoding of ULP messages (Normative)

This section defines the ULP messages and common elements with ASN.1 (Normative).

11.1 Common Part

```
ULP DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

IMPORTS
        Version, SessionID
FROM ULP-Components
        SUPLINIT
FROM SUPL-INIT
        SUPLSTART
FROM SUPL-START
        SUPLRESPONSE
FROM SUPL-RESPONSE
        SUPLPOSINIT
FROM SUPL-POS-INIT
        SUPLPOS
FROM SUPL-POS
        SUPLEND
FROM SUPL-END
        SUPLAUTHREQ
FROM SUPL-AUTH-REQ
        SUPLAUTHRESP
FROM SUPL-AUTH-RESP
        Ver2-SUPLTRIGGEREDSTART
FROM SUPL-TRIGGERED-START
        Ver2-SUPLTRIGGEREDRESPONSE
FROM SUPL-TRIGGERED-RESPONSE
        Ver2-SUPLREPORT
FROM SUPL-REPORT
        Ver2-SUPLTRIGGEREDSTOP
FROM SUPL-TRIGGERED-STOP
        Ver2-SUPLSETINIT
FROM SUPL-SET-INIT
        Ver2-SUPLNOTIFY
FROM SUPL-NOTIFY
        Ver2-SUPLNOTIFYRESPONSE
FROM SUPL-NOTIFY-RESPONSE;

-- general ULP PDU layout;--
ULP-PDU ::= SEQUENCE {
  length     INTEGER(0..65535),
  version    Version,
  sessionID  SessionID,
  message    UlpMessage}

UlpMessage ::= CHOICE {
  msSUPLINIT      SUPLINIT,
  msSUPLSTART     SUPLSTART,
  msSUPLRESPONSE  SUPLRESPONSE,
  msSUPLPOSINIT   SUPLPOSINIT,
  msSUPLPOS       SUPLPOS,
  msSUPLEND       SUPLEND,
  msSUPLAUTHREQ   SUPLAUTHREQ,
```

```
  msSUPLAUTHRESP  SUPLAUTHRESP,
 ...,
  msSUPLTRIGGEREDSTART    Ver2-SUPLTRIGGEREDSTART,
  msSUPLTRIGGEREDRESPONSE Ver2-SUPLTRIGGEREDRESPONSE,
  msSUPLTRIGGEREDSTOP     Ver2-SUPLTRIGGEREDSTOP,
  msSUPLNOTIFY            Ver2-SUPLNOTIFY,
  msSUPLNOTIFYRESPONSE    Ver2-SUPLNOTIFYRESPONSE,
  msSUPLSETINIT           Ver2-SUPLSETINIT,
  msSUPLREPORT            Ver2-SUPLREPORT}

END
```

11.2 Message Specific Part

11.2.1 SUPL INIT

```
SUPL-INIT DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

EXPORTS SUPLINIT, Notification;

IMPORTS
        SLPAddress, QoP, PosMethod
FROM ULP-Components
        Ver2-SUPL-INIT-extension
FROM ULP-Version-2-message-extensions
        Ver2-Notification-extension
FROM ULP-Version-2-parameter-extensions;

SUPLINIT ::= SEQUENCE {
  posMethod     PosMethod,
  notification  Notification OPTIONAL,
  sLPAddress    SLPAddress OPTIONAL,
  qoP           QoP OPTIONAL,
  sLPMode       SLPMode,
  mac           MAC OPTIONAL, -- included for backwards compatibility
  keyIdentity   KeyIdentity OPTIONAL, -- included for backwards compatibility
  ...,
-- version 2 extension element
  ver2-SUPL-INIT-extension        Ver2-SUPL-INIT-extension OPTIONAL}

Notification ::= SEQUENCE {
  notificationType  NotificationType,
  encodingType      EncodingType OPTIONAL,
  requestorId       OCTET STRING(SIZE (1..maxReqLength)) OPTIONAL,
  requestorIdType   FormatIndicator OPTIONAL,
  clientName        OCTET STRING(SIZE (1..maxClientLength)) OPTIONAL,
  clientNameType    FormatIndicator OPTIONAL,
  ...,
  ver2-Notification-extension     Ver2-Notification-extension OPTIONAL}

NotificationType ::= ENUMERATED {
  noNotificationNoVerification(0), notificationOnly(1),
  notificationAndVerficationAllowedNA(2),
  notificationAndVerficationDeniedNA(3), privacyOverride(4), ...}

EncodingType ::= ENUMERATED {ucs2(0), gsmDefault(1), utf8(2), ...}

maxReqLength INTEGER ::= 50
```

```
maxClientLength INTEGER ::= 50

FormatIndicator ::= ENUMERATED {
  logicalName(0), e-mailAddress(1), msisdn(2), url(3), sipUrl(4), min(5),
  mdn(6), iMSPublicidentity(7), ...}

SLPMode ::= ENUMERATED {proxy(0), nonProxy(1)}

MAC ::= BIT STRING(SIZE (64)) -- empty placeholder required for SUPL 1.0
backwards compatibility

KeyIdentity ::= BIT STRING(SIZE (128)) -- empty placeholder required for SUPL
1.0 backwards compatibility

END
```

11.2.2 SUPL START

```
SUPL-START DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

EXPORTS SUPLSTART, SETCapabilities;

IMPORTS
        LocationId, QoP
FROM ULP-Components
        Ver2-SUPL-START-extension
FROM ULP-Version-2-message-extensions
        Ver2-SETCapabilities-extension, Ver2-PosProtocol-extension, Ver2-
PosTechnology-extension
FROM ULP-Version-2-parameter-extensions;

SUPLSTART ::= SEQUENCE {
  sETCapabilities  SETCapabilities,
  locationId       LocationId,
  qoP              QoP OPTIONAL,
  ...,
-- version 2 extension element
  ver2-SUPL-START-extension        Ver2-SUPL-START-extension OPTIONAL}

SETCapabilities ::= SEQUENCE {
  posTechnology  PosTechnology,
  prefMethod     PrefMethod,
  posProtocol    PosProtocol,
  ...,
  ver2-SETCapabilities-extension   Ver2-SETCapabilities-extension OPTIONAL}

PosTechnology ::= SEQUENCE {
  agpsSETassisted  BOOLEAN,
  agpsSETBased     BOOLEAN,
  autonomousGPS    BOOLEAN,
  aflt             BOOLEAN,
  ecid             BOOLEAN,
  eotd             BOOLEAN,
  otdoa            BOOLEAN,
  ...,
  ver2-PosTechnology-extension     Ver2-PosTechnology-extension OPTIONAL}
```

```
PrefMethod ::= ENUMERATED {
  agpsSETassistedPreferred, agpsSETBasedPreferred, noPreference}
-- To achieve compatibility  with ULP V1.0 the names of the enumerations are
-- kept the same as in ULP V1.0. agps shall be interpreted as agnss.

PosProtocol ::= SEQUENCE {
  tia801  BOOLEAN,
  rrlp    BOOLEAN,
  rrc     BOOLEAN,
  ...,
  ver2-PosProtocol-extension       Ver2-PosProtocol-extension OPTIONAL}

END
```

11.2.3 SUPL RESPONSE

```
SUPL-RESPONSE DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

EXPORTS SUPLRESPONSE;

IMPORTS
        PosMethod, SLPAddress
FROM ULP-Components
        Ver2-SUPL-RESPONSE-extension
FROM ULP-Version-2-message-extensions;

SUPLRESPONSE ::= SEQUENCE {
  posMethod     PosMethod,
  sLPAddress    SLPAddress OPTIONAL,
  sETAuthKey    SETAuthKey OPTIONAL, -- included for backwards compatibility
  keyIdentity4  KeyIdentity4 OPTIONAL, -- included for backwards compatibility
  ...,
-- version 2 extension element
  ver2-SUPL-RESPONSE-extension     Ver2-SUPL-RESPONSE-extension OPTIONAL}

SETAuthKey ::= CHOICE {
  shortKey  BIT STRING(SIZE (128)),
  longKey   BIT STRING(SIZE (256)),
  ...}

KeyIdentity4 ::= BIT STRING(SIZE (128))

END
```

11.2.4 SUPL POS INIT

```
SUPL-POS-INIT DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

EXPORTS SUPLPOSINIT;

IMPORTS
        SUPLPOS
FROM SUPL-POS
        SETCapabilities
FROM SUPL-START
        LocationId, Position, Ver
FROM ULP-Components
```

```
        Ver2-SUPL-POS-INIT-extension
FROM ULP-Version-2-message-extensions
        Ver2-RequestedAssistData-extension
FROM ULP-Version-2-parameter-extensions;

SUPLPOSINIT ::= SEQUENCE {
  sETCapabilities      SETCapabilities,
  requestedAssistData  RequestedAssistData OPTIONAL,
  locationId           LocationId,
  position             Position OPTIONAL,
  suplpos              SUPLPOS OPTIONAL,
  ver                  Ver OPTIONAL,
  ...,
-- version 2 extension element
  ver2-SUPL-POS-INIT-extension     Ver2-SUPL-POS-INIT-extension OPTIONAL}

RequestedAssistData ::= SEQUENCE {
  almanacRequested                BOOLEAN,
  utcModelRequested               BOOLEAN,
  ionosphericModelRequested       BOOLEAN,
  dgpsCorrectionsRequested        BOOLEAN,
  referenceLocationRequested      BOOLEAN, -- Note: Used also for GANSS
  referenceTimeRequested          BOOLEAN,
  acquisitionAssistanceRequested  BOOLEAN,
  realTimeIntegrityRequested      BOOLEAN,
  navigationModelRequested        BOOLEAN,
  navigationModelData             NavigationModel OPTIONAL,
  ...,
  ver2-RequestedAssistData-extension Ver2-RequestedAssistData-extension
OPTIONAL}

NavigationModel ::= SEQUENCE {
  gpsWeek   INTEGER(0..1023),
  gpsToe    INTEGER(0..167),
  nsat      INTEGER(0..31),
  toeLimit  INTEGER(0..10),
  satInfo   SatelliteInfo OPTIONAL,
...}

-- Further information on this fields can be found
-- in [3GPP RRLP]and [3GPP 49.031]

SatelliteInfo ::= SEQUENCE (SIZE (1..31)) OF SatelliteInfoElement

SatelliteInfoElement ::= SEQUENCE {
  satId  INTEGER(0..63),
  iode   INTEGER(0..255),
  ...}

END
```

11.2.5 SUPL POS

```
SUPL-POS DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

EXPORTS SUPLPOS;

IMPORTS
```

```
        Velocity
FROM ULP-Components
        Ver2-SUPL-POS-extension
FROM ULP-Version-2-message-extensions
        Ver2-PosPayLoad-extension
FROM ULP-Version-2-parameter-extensions;

SUPLPOS ::= SEQUENCE {
  posPayLoad  PosPayLoad,
  velocity    Velocity OPTIONAL,
  ...,
-- version 2 extension element
  ver2-SUPL-POS-extension          Ver2-SUPL-POS-extension OPTIONAL}

PosPayLoad ::= CHOICE {
  tia801payload  OCTET STRING(SIZE (1..8192)),
  rrcPayload     OCTET STRING(SIZE (1..8192)),
  rrlpPayload    OCTET STRING(SIZE (1..8192)),
  ...,
  ver2-PosPayLoad-extension  Ver2-PosPayLoad-extension}

END
```

11.2.6 SUPL END

```
SUPL-END DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

EXPORTS SUPLEND;

IMPORTS
        StatusCode, Position, Ver
FROM ULP-Components
        Ver2-SUPL-END-extension
FROM ULP-Version-2-message-extensions;

SUPLEND ::= SEQUENCE {
  position            Position OPTIONAL,
  statusCode          StatusCode OPTIONAL,
  ver                 Ver OPTIONAL,
  ...,
-- version 2 extension element
  ver2-SUPL-END-extension          Ver2-SUPL-END-extension OPTIONAL}

END
```

11.2.7 SUPL AUTH REQ

```
SUPL-AUTH-REQ DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

EXPORTS SUPLAUTHREQ;

IMPORTS
        Ver
FROM ULP-Components
        SETCapabilities
FROM SUPL-START;
```

```
SUPLAUTHREQ ::= SEQUENCE {
  ver                 Ver OPTIONAL,
  sETCapabilities     SETCapabilities OPTIONAL,
  ...}

END
```

11.2.8 SUPL AUTH RESP

```
SUPL-AUTH-RESP DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

EXPORTS SUPLAUTHRESP;

IMPORTS
        SPCSETKey, SPCTID, SPCSETKeylifetime
FROM Ver2-ULP-Components;

SUPLAUTHRESP ::= SEQUENCE {
  sPCSETKey           SPCSETKey,
  spctid              SPCTID,
  sPCSETKeylifetime   SPCSETKeylifetime OPTIONAL,
  ...}

END
```

11.2.9 SUPL NOTIFY

```
SUPL-NOTIFY DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

EXPORTS Ver2-SUPLNOTIFY;

IMPORTS
        Notification
FROM SUPL-INIT;

Ver2-SUPLNOTIFY ::= SEQUENCE {
  notification  Notification,
  ...}
END
```

11.2.10 SUPL NOTIFY RESPONSE

```
SUPL-NOTIFY-RESPONSE DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

EXPORTS Ver2-SUPLNOTIFYRESPONSE;

Ver2-SUPLNOTIFYRESPONSE ::= SEQUENCE {
  notificationResponse  NotificationResponse OPTIONAL,
  ...}

NotificationResponse ::= ENUMERATED {allowed(0), notAllowed(1), ...}

END
```

11.2.11 SUPL SET INIT

```
SUPL-SET-INIT DEFINITIONS AUTOMATIC TAGS ::=
BEGIN
```

```
EXPORTS Ver2-SUPLSETINIT;

IMPORTS
        SETId, QoP
FROM ULP-Components
        ApplicationID
FROM Ver2-ULP-Components;


Ver2-SUPLSETINIT ::= SEQUENCE {
  targetSETID    SETId, --Target SETid identifies the target SET to be located
  qoP            QoP OPTIONAL,
  applicationID  ApplicationID OPTIONAL,
  ...}

END
```

11.2.12 SUPL TRIGGERED START

```
SUPL-TRIGGERED-START DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

EXPORTS Ver2-SUPLTRIGGEREDSTART, TriggerType, TriggerParams, maxNumGeoArea,
maxAreaId, maxAreaIdList;

IMPORTS
        LocationId, QoP, Ver, Position
FROM ULP-Components
        MultipleLocationIds, CauseCode, ThirdParty, ApplicationID,
ReportingCap, Coordinate, CircularArea, EllipticalArea, PolygonArea
FROM Ver2-ULP-Components
        SETCapabilities
FROM SUPL-START;

Ver2-SUPLTRIGGEREDSTART ::= SEQUENCE {
  sETCapabilities     SETCapabilities,
  locationId          LocationId,
  ver                 Ver OPTIONAL,
  qoP                 QoP OPTIONAL,
  multipleLocationIds MultipleLocationIds OPTIONAL,
  thirdParty          ThirdParty OPTIONAL,
  applicationID       ApplicationID OPTIONAL,
  triggerType         TriggerType OPTIONAL,
  triggerParams       TriggerParams OPTIONAL,
  position            Position OPTIONAL,
  reportingCap        ReportingCap OPTIONAL,
  causeCode           CauseCode OPTIONAL,
   ...}

TriggerType ::= ENUMERATED {
  periodic(0), areaEvent(1),
  ...}

TriggerParams ::= CHOICE {
   periodicParams     PeriodicParams,
   areaEventParams    AreaEventParams,
   ...}
```

```
PeriodicParams ::= SEQUENCE{
   numberOfFixes                   INTEGER(1.. 8639999),
   intervalBetweenFixes            INTEGER(1.. 8639999),
   startTime                       INTEGER(0..2678400) OPTIONAL,
...}
-- intervalBetweenFixes and startTime are in seconds.
-- numberOfFixes  * intervalBetweenFixes shall not exceed 8639999
-- (100 days in seconds) for compatibility with OMA MLP and RLP
-- startTime is in relative time in units of seconds measured from "now"
-- a value of 0 signifies "now", a value of "startTime" signifies startTime
-- seconds from "now"

AreaEventParams ::= SEQUENCE {
  areaEventType                   AreaEventType,
  locationEstimate                BOOLEAN,
  repeatedReportingParams         RepeatedReportingParams OPTIONAL,
  startTime                       INTEGER(0..2678400) OPTIONAL,
  stopTime                        INTEGER(0..11318399) OPTIONAL,
  geographicTargetAreaList        GeographicTargetAreaList  OPTIONAL,
  areaIdLists                     SEQUENCE (SIZE (1..maxAreaIdList)) OF
AreaIdList OPTIONAL,
  ...}

-- startTime and stopTime are in seconds.
-- startTime and stop Time are in relative time in units of seconds measured
-- from "now"
-- a value of 0 signifies "now"
-- stopTime must be > startTime
-- stopTime - startTime shall not exceed 8639999
-- (100 days in seconds) for compatibility with OMA MLP and RLP

AreaEventType ::= ENUMERATED {enteringArea(0), insideArea(1), outsideArea(2),
leavingArea(3), ...}

RepeatedReportingParams ::= SEQUENCE {
  minimumIntervalTime      INTEGER (1..604800), -- time in seconds
  maximumNumberOfReports   INTEGER (1..1024),
  ...}

GeographicTargetAreaList ::= SEQUENCE (SIZE (1..maxNumGeoArea)) OF
GeographicTargetArea

GeographicTargetArea ::= CHOICE {
 circularArea         CircularArea,
 ellipticalArea       EllipticalArea,
 polygonArea          PolygonArea,
 ...}

AreaIdList ::= SEQUENCE {
 areaIdSet            AreaIdSet,
 areaIdSetType        AreaIdSetType OPTIONAL,
 geoAreaMappingList               GeoAreaMappingList OPTIONAL}

AreaIdSet ::= SEQUENCE SIZE (1..maxAreaId) OF AreaId

AreaId ::= CHOICE {
 gSMAreaId            GSMAreaId,
```

```
 wCDMAAreaId          WCDMAAreaId, -- For TD-SCDMA networks, this parameter
indicates a TD-SCDMA Area ID
 cDMAAreaId           CDMAAreaId,
 hRPDAreaId           HRPDAareaId,
 uMBAreaId            UMBAreaId,
 lTEAreaId            LTEAreaId,
 wLANAreaId           WLANAreaId,
 wiMAXAreaId          WimaxAreaId,
 ...,
 nRAreaId             NRAreaId }

GSMAreaId ::= SEQUENCE {
 refMCC               INTEGER(0..999) OPTIONAL, -- Mobile Country Code
 refMNC               INTEGER(0..999) OPTIONAL, -- Mobile Network Code
 refLAC               INTEGER(0..65535) OPTIONAL, -- Location Area Code
 refCI                INTEGER(0..65535) OPTIONAL, -- Cell Id
 ...}
-- only one of the following four combinations are allowed: (1) refMCC, (2)
refMCC+refMNC, (3) refMCC+refMNC+refLAC or (4) refMCC+refMNC+refLAC+refCI

WCDMAAreaId ::= SEQUENCE {
  refMCC INTEGER(0..999) OPTIONAL, -- Mobile Country Code
  refMNC INTEGER(0..999) OPTIONAL, -- Mobile Network Code
  refLAC INTEGER(0..65535) OPTIONAL, -- Location Area Code
  refUC  INTEGER(0..268435455) OPTIONAL, -- Cell identity
...}
-- only one of the following four combinations are allowed: (1) refMCC, (2)
refMCC+refMNC, (3) refMCC+refMNC+refLAC, or (4) refMCC+refMNC+refLAC+refUC

CDMAAreaId::= SEQUENCE {
  refSID         INTEGER(0..65535) OPTIONAL, -- System Id
  refNID         INTEGER(0..32767) OPTIONAL, -- Network Id
  refBASEID      INTEGER(0..65535) OPTIONAL, -- Base Station Id
...}
-- only one of the following three combinations are allowed: (1) refSID, (2)
refSID+refNID, or (3) refSID+refNID+refBASEID

HRPDAreaId::= SEQUENCE {
  refSECTORID    BIT STRING(SIZE (128)), -- HRPD Sector Id
...}

UMBAreaId::= SEQUENCE {
  refMCC               INTEGER(0..999) OPTIONAL, -- Mobile Country Code
  refMNC               INTEGER(0..999) OPTIONAL, -- Mobile Network Code
  refSECTORID          BIT STRING(SIZE (128)) OPTIONAL, -- UMB Sector Id
...}

LTEAreaId::= SEQUENCE {
  refMCC INTEGER(0..999) OPTIONAL, -- Mobile Country Code
  refMNC INTEGER(0..999) OPTIONAL, -- Mobile Network Code
  refCI  BIT STRING(SIZE (29)) OPTIONAL, -- LTE Cell-Id
...}
-- only one of the following three combinations are allowed: (1) refMCC, (2)
refMCC+refMNC, or (3) refMCC+refMNC+refCI
-- The LTE Cell-Id is encoded in the 28 Least Significant Bits of refCI
-- The Most Significant Bit of refCI shall be ignored

WLANAreaId::= SEQUENCE {
```

```
  apMACAddress       BIT STRING(SIZE (48)), -- AP MAC Address
...}

WimaxAreaId ::= SEQUENCE {
  bsID-MSB      BIT STRING (SIZE(24)) OPTIONAL,
  bsID-LSB      BIT STRING (SIZE(24)) }
-- if only LSB is present, MSB is assumed to be identical to the current
serving BS or clamped on network value

NRAreaId ::= SEQUENCE {
  refMCC INTEGER(0..999) OPTIONAL, -- Mobile Country Code
  refMNC INTEGER(0..999) OPTIONAL, -- Mobile Network Code
  refCI  BIT STRING(SIZE (36)) OPTIONAL, -- NR Cell-Id
...}
-- only one of the following three combinations are allowed: (1) refMCC, (2)
-- refMCC+refMNC, or (3) refMCC+refMNC+refCI


AreaIdSetType ::=  ENUMERATED {border(0), within(1), ...}

GeoAreaMappingList ::= SEQUENCE (SIZE (1..maxNumGeoArea)) OF GeoAreaIndex

GeoAreaIndex ::= INTEGER (1..maxNumGeoArea)

maxNumGeoArea INTEGER ::= 32

maxAreaId INTEGER ::= 256

maxAreaIdList INTEGER ::= 32

END
```

11.2.13 SUPL TRIGGERED RESPONSE

```
SUPL-TRIGGERED-RESPONSE DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

EXPORTS Ver2-SUPLTRIGGEREDRESPONSE;

IMPORTS
        PosMethod, SLPAddress
FROM ULP-Components
        SupportedNetworkInformation, SPCSETKey, SPCTID, SPCSETKeylifetime,
GNSSPosTechnology
FROM Ver2-ULP-Components
        TriggerParams
FROM SUPL-TRIGGERED-START;

Ver2-SUPLTRIGGEREDRESPONSE::= SEQUENCE{
  posMethod                       PosMethod,
  triggerParams                   TriggerParams  OPTIONAL,
  sLPAddress                      SLPAddress OPTIONAL,
  supportedNetworkInformation     SupportedNetworkInformation OPTIONAL,
  reportingMode                   ReportingMode OPTIONAL,
  sPCSETKey                       SPCSETKey    OPTIONAL,
  spctid                          SPCTID       OPTIONAL,
  sPCSETKeylifetime               SPCSETKeylifetime OPTIONAL,
  gnssPosTechnology               GNSSPosTechnology OPTIONAL,
  ...}
```

```
ReportingMode ::= SEQUENCE {
  repMode             RepModee,
  batchRepConditions  BatchRepConditions OPTIONAL, -- only used for batch
reporting
  batchRepType        BatchRepType OPTIONAL, -- only used for batch reporting
  ...}

RepModee ::= ENUMERATED {realtime(1), quasirealtime(2), batch(3), ...}

BatchRepConditions ::= CHOICE {
 num-interval INTEGER (1..1024), -- number of periodic fixes/measurements after
which the batch report is sent to the SLP
 num-minutes INTEGER (1..2048), -- number of minutes after which the batch
report is sent to the SLP
 endofsession NULL, -- if selected batch report is to be sent at the end of the
session
 ...}

BatchRepType ::= SEQUENCE {
  reportPosition      BOOLEAN, -- set to "true" if reporting of position is
allowed
  reportMeasurements  BOOLEAN, -- set to "true" if reporting of measurements is
allowed
  intermediateReports   BOOLEAN, -- set to "true" if the SET is allowed to send
intermediate reports if it runs out of memory
  discardOldest       BOOLEAN OPTIONAL, -- set to "true" if the SET should
discard the oldest positions or measurements of the batch report in order to
save memory, set to "false" the SET should discard the latest positions or
measurements
  ...}

END
```

11.2.14 SUPL REPORT

```
SUPL-REPORT DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

EXPORTS Ver2-SUPLREPORT;

IMPORTS
        SETCapabilities
FROM SUPL-START
        Position, PosMethod, SessionID, Ver
FROM ULP-Components
        MultipleLocationIds, GNSSPosTechnology, GANSSSignals
FROM Ver2-ULP-Components
        maxGANSS
FROM ULP-Version-2-parameter-extensions;

Ver2-SUPLREPORT ::= SEQUENCE {
 sessionList          SessionList OPTIONAL,
 sETCapabilities      SETCapabilities OPTIONAL,
 reportDataList       ReportDataList OPTIONAL,
 ver                  Ver OPTIONAL,
 moreComponents       NULL OPTIONAL,
...}

SessionList ::= SEQUENCE SIZE (1..maxnumSessions) OF SessionInformation
```

```
SessionInformation ::= SEQUENCE {
 sessionID            SessionID,
 ...}

maxnumSessions    INTEGER ::= 64

ReportDataList ::= SEQUENCE SIZE (1.. 1024) OF ReportData

ReportData ::= SEQUENCE {
  positionData        PositionData OPTIONAL,
  multipleLocationIds MultipleLocationIds OPTIONAL,
  resultCode          ResultCode OPTIONAL,
  timestamp           TimeStamp OPTIONAL,
  ...}

PositionData ::= SEQUENCE {
 position                          Position,
 posMethod                         PosMethod OPTIONAL,
 gnssPosTechnology                 GNSSPosTechnology OPTIONAL,
 ganssSignalsInfo                  GANSSsignalsInfo OPTIONAL,
 ...}

GANSSsignalsInfo ::= SEQUENCE SIZE (1..maxGANSS) OF GANSSSignalsDescription

GANSSSignalsDescription ::= SEQUENCE {
 ganssId             INTEGER(0..15), -- coding according to parameter
definition in section 10.10
 gANSSSignals        GANSSSignals,
 ...}

ResultCode ::= ENUMERATED {outofradiocoverage(1), noposition(2),
nomeasurement(3), nopositionnomeasurement(4), outofmemory(5),
outofmemoryintermediatereporting(6), other(7), ...}

TimeStamp ::= CHOICE {
  absoluteTime  UTCTime,
  relativeTime  INTEGER (0..31536000)} -- relative time to when the SUPL REPORT
message is sent in units of 1 sec, where 0 signifies "now" and n signifies n
seconds in the past

END
```

11.2.15 SUPL TRIGGERED STOP

```
SUPL-TRIGGERED-STOP DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

EXPORTS Ver2-SUPLTRIGGEREDSTOP;

IMPORTS
        StatusCode
FROM ULP-Components;

Ver2-SUPLTRIGGEREDSTOP::= SEQUENCE{
  statusCode     StatusCode OPTIONAL,
  ...}

END
```

11.3 Message Extensions (SUPL Version 2)

```
ULP-Version-2-message-extensions DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

EXPORTS
Ver2-SUPL-INIT-extension, Ver2-SUPL-START-extension, Ver2-SUPL-RESPONSE-
extension, Ver2-SUPL-POS-INIT-extension, Ver2-SUPL-POS-extension, Ver2-SUPL-
END-extension;

IMPORTS
        SLPAddress, Position, Ver
FROM ULP-Components
        SETCapabilities
FROM SUPL-START
        SupportedNetworkInformation, GNSSPosTechnology, MultipleLocationIds,
UTRAN-GPSReferenceTimeResult, UTRAN-GANSSReferenceTimeResult, UTRAN-
GPSReferenceTimeAssistance, UTRAN-GANSSReferenceTimeAssistance, SPCSETKey,
SPCTID, SPCSETKeylifetime, ThirdParty, ApplicationID
FROM Ver2-ULP-Components
 TriggerType
FROM SUPL-TRIGGERED-START
 Ver2-HighAccuracyPosition
FROM Ver2-ULP-Components;

Ver2-SUPL-INIT-extension ::= SEQUENCE {
  notificationMode                NotificationMode OPTIONAL,
  supportedNetworkInformation     SupportedNetworkInformation OPTIONAL,
  triggerType                     TriggerType OPTIONAL,
  e-SLPAddress                    SLPAddress OPTIONAL,
  historicReporting               HistoricReporting OPTIONAL,
  protectionLevel                 ProtectionLevel OPTIONAL,
  gnssPosTechnology               GNSSPosTechnology OPTIONAL,
  minimumMajorVersion             INTEGER (0..255) OPTIONAL,
...}

NotificationMode ::= ENUMERATED {normal(0), basedOnLocation(1), ...}

HistoricReporting ::= SEQUENCE {
  allowedReportingType            AllowedReportingType,
  reportingCriteria               ReportingCriteria OPTIONAL, ...}

AllowedReportingType ::= ENUMERATED {
  positionsOnly(0), measurementsOnly(1), positionsAndMeasurements(2), ...}

ReportingCriteria ::= SEQUENCE {
  timeWindow          TimeWindow   OPTIONAL,
  maxNumberofReports  INTEGER(1..65536) OPTIONAL,
  minTimeInterval     INTEGER(1..86400) OPTIONAL,
...}

TimeWindow ::= SEQUENCE {
  startTime           INTEGER(-525600..-1), -- Time in minutes
  stopTime            INTEGER(-525599..0)} -- Time in minutes

ProtectionLevel ::= SEQUENCE {
 protlevel                        ProtLevel,
 basicProtectionParams            BasicProtectionParams     OPTIONAL,
```

```
...}

ProtLevel ::= ENUMERATED {
 nullProtection(0), basicProtection(1), ...}

BasicProtectionParams ::= SEQUENCE {
 keyIdentifier                    OCTET STRING(SIZE (8)),
 basicReplayCounter               INTEGER(0..65535),
 basicMAC                         BIT STRING(SIZE (32)),
...}

Ver2-SUPL-START-extension ::= SEQUENCE {
  multipleLocationIds MultipleLocationIds OPTIONAL,
  thirdParty          ThirdParty OPTIONAL,
  applicationID       ApplicationID OPTIONAL,
  position            Position OPTIONAL,
...}

Ver2-SUPL-RESPONSE-extension ::= SEQUENCE {
  supportedNetworkInformation      SupportedNetworkInformation OPTIONAL,
  sPCSETKey                        SPCSETKey    OPTIONAL,
  spctid                           SPCTID       OPTIONAL,
  sPCSETKeylifetime                SPCSETKeylifetime OPTIONAL,
  initialApproximateposition       Position     OPTIONAL,
  gnssPosTechnology                GNSSPosTechnology OPTIONAL,
...}

Ver2-SUPL-POS-INIT-extension ::= SEQUENCE {
  multipleLocationIds              MultipleLocationIds OPTIONAL,
  utran-GPSReferenceTimeResult     UTRAN-GPSReferenceTimeResult OPTIONAL,
  utran-GANSSReferenceTimeResult   UTRAN-GANSSReferenceTimeResult OPTIONAL,
...,
  servingAMF                       AMF-Identifier OPTIONAL}

AMF-Identifier ::= SEQUENCE {
  amf-Region-ID                    BIT STRING (SIZE (8)),
  amf-Set-ID                       BIT STRING (SIZE (10)),
  amf-Pointer                      BIT STRING (SIZE (6)) }

Ver2-SUPL-POS-extension ::= SEQUENCE {
utran-GPSReferenceTimeAssistance   UTRAN-GPSReferenceTimeAssistance OPTIONAL,
utran-GPSReferenceTimeResult       UTRAN-GPSReferenceTimeResult OPTIONAL,
utran-GANSSReferenceTimeAssistance UTRAN-GANSSReferenceTimeAssistance OPTIONAL,
utran-GANSSReferenceTimeResult     UTRAN-GANSSReferenceTimeResult OPTIONAL,
...}

Ver2-SUPL-END-extension ::= SEQUENCE {
  sETCapabilities     SETCapabilities OPTIONAL,
...,
  ver2-HighAccuracyPosition        Ver2-HighAccuracyPosition  OPTIONAL}

END
```

11.4 Parameter Extensions (SUPL Version 2)

```
ULP-Version-2-parameter-extensions DEFINITIONS AUTOMATIC TAGS ::=
BEGIN
```

```
EXPORTS
maxGANSS, Ver2-Notification-extension, Ver2-SETCapabilities-extension, Ver2-
PosProtocol-extension, Ver2-PosTechnology-extension, Ver2-RequestedAssistData-
extension, Ver2-PosPayLoad-extension;

IMPORTS
        GANSSSignals, ReportingCap
FROM Ver2-ULP-Components
        maxNumGeoArea, maxAreaId, maxAreaIdList
FROM SUPL-TRIGGERED-START;

Ver2-Notification-extension ::= SEQUENCE {
  emergencyCallLocation  NULL OPTIONAL,
  ...}

Ver2-SETCapabilities-extension ::= SEQUENCE {
  serviceCapabilities          ServiceCapabilities OPTIONAL,
...,
  supportedBearers SupportedBearers OPTIONAL}


ServiceCapabilities ::= SEQUENCE {
  servicesSupported               ServicesSupported,
  reportingCapabilities           ReportingCap OPTIONAL,
  eventTriggerCapabilities        EventTriggerCapabilities OPTIONAL,
  sessionCapabilities             SessionCapabilities,
...}

ServicesSupported ::= SEQUENCE {
  periodicTrigger     BOOLEAN,
  areaEventTrigger    BOOLEAN,
...}

EventTriggerCapabilities ::= SEQUENCE {
  geoAreaShapesSupported          GeoAreaShapesSupported,
  maxNumGeoAreaSupported          INTEGER (0..maxNumGeoArea) OPTIONAL,
  maxAreaIdListSupported          INTEGER (0..maxAreaIdList) OPTIONAL,
  maxAreaIdSupportedPerList       INTEGER (0..maxAreaId) OPTIONAL,
...}

GeoAreaShapesSupported ::= SEQUENCE {
  ellipticalArea   BOOLEAN,
  polygonArea      BOOLEAN,
...}

SessionCapabilities ::= SEQUENCE {
  maxNumberTotalSessions          INTEGER (1..128),
  maxNumberPeriodicSessions       INTEGER (1..32),
  maxNumberTriggeredSessions      INTEGER (1..32),
...}

SupportedBearers ::= SEQUENCE {
  gsm                BOOLEAN,
  wcdma              BOOLEAN,
  lte                BOOLEAN,
  cdma               BOOLEAN,
  hprd               BOOLEAN,
  umb                BOOLEAN,
```

```
  wlan                BOOLEAN,
  wiMAX               BOOLEAN,
...,
  nr                  BOOLEAN OPTIONAL}


Ver2-PosProtocol-extension ::= SEQUENCE {
  lpp     BOOLEAN,
  posProtocolVersionRRLP           PosProtocolVersion3GPP OPTIONAL,
  posProtocolVersionRRC            PosProtocolVersion3GPP OPTIONAL,
  posProtocolVersionTIA801         PosProtocolVersion3GPP2 OPTIONAL,
  posProtocolVersionLPP  PosProtocolVersion3GPP OPTIONAL,
...,
  lppe   BOOLEAN OPTIONAL,
  posProtocolVersionLPPe           PosProtocolVersionOMA OPTIONAL}

PosProtocolVersion3GPP ::= SEQUENCE {
  majorVersionField      INTEGER(0..255),
  technicalVersionField  INTEGER(0..255),
  editorialVersionField  INTEGER(0..255),
...}

PosProtocolVersion3GPP2 ::= SEQUENCE (SIZE(1..8)) OF
Supported3GPP2PosProtocolVersion

Supported3GPP2PosProtocolVersion ::= SEQUENCE {
  revisionNumber                   BIT STRING(SIZE (6)), -- the location
standard revision number the SET supports coded according to 3GPP2 C.S0022
  pointReleaseNumber               INTEGER(0..255),
  internalEditLevel                INTEGER(0..255),
...}

PosProtocolVersionOMA ::= SEQUENCE {
  majorVersionField      INTEGER(0..255),
  minorVersionField      INTEGER(0..255),
...}

Ver2-PosTechnology-extension ::= SEQUENCE {
  gANSSPositionMethods  GANSSPositionMethods OPTIONAL,
...,
  additionalPositioningMethods     AdditionalPositioningMethods OPTIONAL}

GANSSPositionMethods ::= SEQUENCE (SIZE(1..16)) OF GANSSPositionMethod

GANSSPositionMethod ::= SEQUENCE {
 ganssId                          INTEGER(0..15), -- coding according to
parameter definition in section 10.10
 ganssSBASid                      BIT STRING(SIZE(3)) OPTIONAL, --coding
according to parameter definition in section 10.10
 gANSSPositioningMethodTypes      GANSSPositioningMethodTypes,
 gANSSSignals                     GANSSSignals,
...,
  rtk                 RTK          OPTIONAL}

RTK ::= SEQUENCE {
  osr                 BOOLEAN,
...}
```

```
GANSSPositioningMethodTypes ::= SEQUENCE {
  setAssisted         BOOLEAN,
  setBased            BOOLEAN,
  autonomous          BOOLEAN,
...}

AdditionalPositioningMethods ::= SEQUENCE (SIZE(1..8)) OF AddPosSupport-Element

AddPosSupport-Element ::= SEQUENCE {
    addPosID          ENUMERATED {
                          mBS,
                          ...,
                          nr-DL-TDOA,
                          nr-DL-AoD,
                          nr-Multi-RTT,
                          nr-DL-E-CID,
                          nr-UL-TDOA,
                          nr-UL-AoA                    },
    addPosMode        BIT STRING {
                                  standalone   (0),
                                  setBased     (1),
                                  setAssisted  (2)} (SIZE (1..8)) OPTIONAL,
...}

Ver2-RequestedAssistData-extension ::= SEQUENCE {
  ganssRequestedCommonAssistanceDataList
GanssRequestedCommonAssistanceDataList OPTIONAL,
  ganssRequestedGenericAssistanceDataList
GanssRequestedGenericAssistanceDataList OPTIONAL,
  extendedEphemeris               ExtendedEphemeris OPTIONAL,
  extendedEphemerisCheck          ExtendedEphCheck OPTIONAL,
...}

GanssRequestedCommonAssistanceDataList ::= SEQUENCE {
  ganssReferenceTime                          BOOLEAN,
  ganssIonosphericModel                       BOOLEAN,
  ganssAdditionalIonosphericModelForDataID00  BOOLEAN,
  ganssAdditionalIonosphericModelForDataID11  BOOLEAN,
  ganssEarthOrientationParameters             BOOLEAN,
...,
  ganssAdditionalIonosphericModelForDataID01  BOOLEAN OPTIONAL}

GanssRequestedGenericAssistanceDataList ::= SEQUENCE(SIZE(1..maxGANSS)) OF
GanssReqGenericData

GanssReqGenericData ::= SEQUENCE {
  ganssId   INTEGER(0..15), -- coding according to parameter definition in
section 10.10
  ganssSBASid BIT STRING(SIZE(3)) OPTIONAL, --coding according to parameter
definition in section 10.10
  ganssRealTimeIntegrity          BOOLEAN,
  ganssDifferentialCorrection     DGANSS-Sig-Id-Req OPTIONAL,
  ganssAlmanac                    BOOLEAN,
  ganssNavigationModelData        GanssNavigationModelData OPTIONAL,
  ganssTimeModels                 BIT STRING(SIZE(16)) OPTIONAL,
  ganssReferenceMeasurementInfo   BOOLEAN,
  ganssDataBits                   GanssDataBits OPTIONAL,
  ganssUTCModel                   BOOLEAN,
```

```
  ganssAdditionalDataChoices GanssAdditionalDataChoices OPTIONAL,
  ganssAuxiliaryInformation        BOOLEAN,
  ganssExtendedEphemeris           ExtendedEphemeris OPTIONAL,
  ganssExtendedEphemerisCheck      GanssExtendedEphCheck OPTIONAL,
...,
  bds-DifferentialCorrection BDS-Sig-Id-Req OPTIONAL,
  bds-GridModelReq    BOOLEAN      OPTIONAL}

DGANSS-Sig-Id-Req ::= BIT STRING (SIZE(8)) -- coding according to parameter
definition in section 10.9

BDS-Sig-Id-Req ::= BIT STRING (SIZE(8)) -- coding according to parameter
definition in section 10.9

GanssNavigationModelData ::= SEQUENCE {
ganssWeek                        INTEGER(0..4095),
ganssToe                         INTEGER(0..167),
t-toeLimit                       INTEGER(0..15),
satellitesListRelatedDataList      SatellitesListRelatedDataList OPTIONAL,
...}

SatellitesListRelatedDataList ::= SEQUENCE(SIZE(0..maxGANSSSat)) OF
SatellitesListRelatedData

SatellitesListRelatedData ::= SEQUENCE {
  satId  INTEGER(0..63),
  iod    INTEGER(0..1023),
...}

maxGANSS    INTEGER ::= 16
maxGANSSSat INTEGER ::= 32

GanssDataBits ::= SEQUENCE {
  ganssTODmin                    INTEGER (0..59),
  reqDataBitAssistanceList       ReqDataBitAssistanceList,
...}

ReqDataBitAssistanceList ::= SEQUENCE {
  gnssSignals                    GANSSSignals,
  ganssDataBitInterval           INTEGER (0..15),
  ganssDataBitSatList            SEQUENCE (SIZE(1..maxGANSSSat)) OF INTEGER
(0..63) OPTIONAL,
...}

GanssAdditionalDataChoices ::= SEQUENCE {
  orbitModelID       INTEGER(0..7) OPTIONAL,
  clockModelID       INTEGER(0..7) OPTIONAL,
  utcModelID         INTEGER(0..7) OPTIONAL,
  almanacModelID     INTEGER(0..7) OPTIONAL,
...}

ExtendedEphemeris ::= SEQUENCE {
  validity        INTEGER (1..256), -- Requested validity in 4 hour steps
  ...}

ExtendedEphCheck ::= SEQUENCE {
  beginTime       GPSTime, -- Begin time of ephemeris extension held by SET
  endTime         GPSTime, -- End time of ephemeris extension held by SET
```

```
  ...}

GanssExtendedEphCheck ::= SEQUENCE {
  beginTime  GANSSextEphTime, -- Begin time of ephemeris extension held by SET
  endTime    GANSSextEphTime, -- End time of ephemeris extension held by SET
  ...}

GPSTime ::= SEQUENCE {
  gPSWeek    INTEGER (0..1023),
  gPSTOWhour INTEGER (0..167),
...}

GANSSextEphTime ::= SEQUENCE {
  gANSSday       INTEGER (0..8191),
  gANSSTODhour   INTEGER (0..23),
...}

Ver2-PosPayLoad-extension ::= SEQUENCE {
   lPPPayload SEQUENCE (SIZE (1..3)) OF OCTET STRING(SIZE (1..60000)) OPTIONAL,
   tia801Payload SEQUENCE (SIZE(1..3)) OF OCTET STRING(SIZE (1..60000))
OPTIONAL,
...}


END
```

11.5 Common elements (SUPL Version 1)

```
ULP-Components DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

EXPORTS Version, SessionID, IPAddress, SLPAddress, LocationId, Position,
StatusCode, Velocity, QoP, PosMethod, Ver, SETId, PrimaryCPICH-Info,
CellParametersID, FQDN;

IMPORTS
        Ver2-CellInfo-extension
FROM Ver2-ULP-Components;

-- protocol version expressed as x.y.z (e.g., 5.1.0)
Version ::= SEQUENCE {
  maj      INTEGER(0..255),
  min      INTEGER(0..255),
  servind  INTEGER(0..255)}

SessionID ::= SEQUENCE {
  setSessionID  SetSessionID OPTIONAL, -- the semantics of OPTIONAL applies to
the encoding only. The parameter itself is MANDATORY. This is introduced only
to minimize bandwidth for the SUPL INIT message. Since the setSessionID is
allocated by the SET, there is no setSessionID to be transmitted in the SUPL
INIT message.
  slpSessionID  SlpSessionID OPTIONAL -- the semantics of OPTIONAL applies to
the encoding only. The parameter itself is MANDATORY. This is introduced only
to minimize bandwidth for the SUPL START, SUPL TRIGGERED START and SUPL SET
INIT messages. Since the slpSessionID is allocated by the SLP, there is no
slpSessionID to be transmitted in these messages (with the exception described
in section 10.14).
}
```

```
SetSessionID ::= SEQUENCE {sessionId  INTEGER(0..65535),
                           setId      SETId}

SETId ::= CHOICE {
  msisdn     OCTET STRING(SIZE (8)),
  mdn        OCTET STRING(SIZE (8)),
  min        BIT STRING(SIZE (34)), -- coded according to TIA-553
  imsi       OCTET STRING(SIZE (8)),
  nai        IA5String(SIZE (1..1000)),
  iPAddress  IPAddress,
  ...,
  ver2-imei  OCTET STRING(SIZE(8))}
-- msisdn, mnd, imsi and imei are a BCD (Binary Coded Decimal) string
-- represent digits from 0 through 9,
-- two digits per octet, each digit encoded 0000 to 1001 (0 to 9)
-- bits 8765 of octet n encoding digit 2n
-- bits 4321 of octet n encoding digit 2(n-1) +1
-- not used digits in the string shall be filled with 1111
-- imei SHALL NOT be used unless the SLP indicates support for SUPL ver 2.0.3
-- or greater

SlpSessionID ::= SEQUENCE {
  sessionID  OCTET STRING(SIZE (4)),
  slpId      SLPAddress}

IPAddress ::= CHOICE {
  ipv4Address  OCTET STRING(SIZE (4)),
  ipv6Address  OCTET STRING(SIZE (16))}

SLPAddress ::= CHOICE {iPAddress  IPAddress,
                       fqdn       FQDN,
                       ...}

FQDN ::=
  VisibleString(FROM ("a".."z" | "A".."Z" | "0".."9" |".-"))(SIZE (1..255))

Ver ::= BIT STRING(SIZE (64))

LocationId ::= SEQUENCE {cellInfo  CellInfo,
                         status    Status,
                         ...}

Status ::= ENUMERATED {stale(0), current(1), unknown(2), ...}

CellInfo ::= CHOICE {
  gsmCell    GsmCellInformation,
  wcdmaCell  WcdmaCellInformation, --WCDMA Cell Information/TD-SCDMA Cell
Information
  cdmaCell   CdmaCellInformation,
  ...,
  ver2-CellInfo-extension          Ver2-CellInfo-extension}

Position ::= SEQUENCE {
  timestamp         UTCTime, -- shall include seconds and shall use UTC time.
  positionEstimate  PositionEstimate,
  velocity          Velocity OPTIONAL,
  ...}
```

```
PositionEstimate ::= SEQUENCE {
  latitudeSign  ENUMERATED {north, south},
  latitude      INTEGER(0..8388607),
  longitude     INTEGER(-8388608..8388607),
  uncertainty
    SEQUENCE {uncertaintySemiMajor  INTEGER(0..127),
              uncertaintySemiMinor  INTEGER(0..127),
              orientationMajorAxis  INTEGER(0..180)} OPTIONAL, -- angle in
degree between major axis and North
  confidence    INTEGER(0..100) OPTIONAL,
  altitudeInfo  AltitudeInfo OPTIONAL,
  ...} -- Coding as in [3GPP GAD]

AltitudeInfo ::= SEQUENCE {
  altitudeDirection  ENUMERATED {height, depth},
  altitude           INTEGER(0..32767),
  altUncertainty     INTEGER(0..127),
  ... } -- based on [3GPP GAD]

CdmaCellInformation ::= SEQUENCE {
  refNID         INTEGER(0..65535), -- Network Id
  refSID         INTEGER(0..32767), -- System Id
  refBASEID      INTEGER(0..65535), -- Base Station Id
  refBASELAT     INTEGER(0..4194303), -- Base Station Latitude
  reBASELONG     INTEGER(0..8388607), -- Base Station Longitude
  refREFPN       INTEGER(0..511), -- Base Station PN Code
  refWeekNumber  INTEGER(0..65535), -- GPS Week Number
  refSeconds     INTEGER(0..4194303), -- GPS Seconds
  ...}

GsmCellInformation ::= SEQUENCE {
  refMCC  INTEGER(0..999), -- Mobile Country Code
  refMNC  INTEGER(0..999), -- Mobile Network Code
  refLAC  INTEGER(0..65535), -- Location area code
  refCI   INTEGER(0..65535), -- Cell identity
  nmr     NMR OPTIONAL,
  ta      INTEGER(0..255) OPTIONAL, --Timing Advance
  ...}

WcdmaCellInformation ::= SEQUENCE {
  refMCC                 INTEGER(0..999), -- Mobile Country Code
  refMNC                 INTEGER(0..999), -- Mobile Network Code
  refUC                  INTEGER(0..268435455), -- Cell identity
  frequencyInfo          FrequencyInfo OPTIONAL,
  primaryScramblingCode  INTEGER(0..511) OPTIONAL, -- Not applicable for TDD
  measuredResultsList    MeasuredResultsList OPTIONAL,
  ...,
  cellParametersId       INTEGER(0..127) OPTIONAL, -- Not applicable for FDD
  timingAdvance          TimingAdvance OPTIONAL -- Not applicable for FDD
}

TimingAdvance ::= SEQUENCE {
 ta      INTEGER (0..8191),
 tAResolution    TAResolution OPTIONAL, --If missing, resolution is 0.125 chips
 chipRate        ChipRate OPTIONAL, --If missing, chip rate is 1.28 Mchip/s
...}
```

```
TAResolution ::= ENUMERATED {res10chip(0),res05chip(1),res0125chip(2), ...} --
Corresponding to 1.0-chip, 0.5-chip and 0.125-chip resolutions, respectively

ChipRate ::= ENUMERATED {tdd128(0),tdd384(1), tdd768(2), ...} --Corresponding
to 1.28-Mchips/s, 3.84-Mchips/s and 7.68-Mchips/s chip rates, respectively


FrequencyInfo ::= SEQUENCE {
  modeSpecificInfo  CHOICE {fdd  FrequencyInfoFDD,
                            tdd  FrequencyInfoTDD,
                            ...},
  ...}

FrequencyInfoFDD ::= SEQUENCE {
  uarfcn-UL  UARFCN OPTIONAL,
  uarfcn-DL  UARFCN,
  ...}

FrequencyInfoTDD ::= SEQUENCE {uarfcn-Nt  UARFCN,
                               ...}

UARFCN ::= INTEGER(0..16383)

NMR ::= SEQUENCE (SIZE (1..15)) OF NMRelement

NMRelement ::= SEQUENCE {
  arfcn  INTEGER(0..1023),
  bsic   INTEGER(0..63),
  rxLev  INTEGER(0..63),
  ...}

MeasuredResultsList ::= SEQUENCE (SIZE (1..maxFreq)) OF MeasuredResults

MeasuredResults ::= SEQUENCE {
  frequencyInfo            FrequencyInfo OPTIONAL,
  utra-CarrierRSSI         UTRA-CarrierRSSI OPTIONAL,
  cellMeasuredResultsList  CellMeasuredResultsList OPTIONAL}

CellMeasuredResultsList ::=
  SEQUENCE (SIZE (1..maxCellMeas)) OF CellMeasuredResults

-- SPARE: UTRA-CarrierRSSI, Max = 76
-- Values above Max are spare
UTRA-CarrierRSSI ::= INTEGER(0..127)

CellMeasuredResults ::= SEQUENCE {
  cellIdentity      INTEGER(0..268435455) OPTIONAL,
  modeSpecificInfo
    CHOICE {fdd
              SEQUENCE {primaryCPICH-Info  PrimaryCPICH-Info,
                        cpich-Ec-N0        CPICH-Ec-N0 OPTIONAL,
                        cpich-RSCP         CPICH-RSCP OPTIONAL,
                        pathloss           Pathloss OPTIONAL},
            tdd
              SEQUENCE {cellParametersID   CellParametersID,
                        proposedTGSN       TGSN OPTIONAL,
                        primaryCCPCH-RSCP  PrimaryCCPCH-RSCP OPTIONAL,
                        pathloss           Pathloss OPTIONAL,
```

```
                          timeslotISCP-List  TimeslotISCP-List OPTIONAL --NOTE:
TimeSlotISCP measurement list cannot be interpreted without the knowledge of
Cell Info as defined in [3GPP RRC]
}}}

CellParametersID ::= INTEGER(0..127)

TGSN ::= INTEGER(0..14)

PrimaryCCPCH-RSCP ::= INTEGER(0..127)

-- SPARE: TimeslotISCP, Max = 91
-- Values above Max are spare
TimeslotISCP ::= INTEGER(0..127)

TimeslotISCP-List ::= SEQUENCE (SIZE (1..maxTS)) OF TimeslotISCP

PrimaryCPICH-Info ::= SEQUENCE {primaryScramblingCode  INTEGER(0..511)}

-- SPARE: CPICH-Ec-No, Max = 49
-- Values above Max are spare
CPICH-Ec-N0 ::= INTEGER(0..63)

-- SPARE: CPICH- RSCP, data range from 0 to 91 and from 123 to 127.
-- Values from 92 to 122 are spare
-- the encoding of cpich-RSCP is (as per [3GPP RRC] V5.11.0)

-- cpich-RSCP = 123    CPICH RSCP <-120 dBm
-- cpich-RSCP = 124    -120 ≤ CPICH RSCP < -119 dBm
-- cpich-RSCP = 125    -119 ≤ CPICH RSCP < -118 dBm
-- cpich-RSCP = 126    -118 ≤ CPICH RSCP < -117 dBm
-- cpich-RSCP = 127    -117 ≤ CPICH RSCP < -116 dBm
-- cpich-RSCP = 0      -116 ≤ CPICH RSCP < -115 dBm
-- cpich-RSCP = 1      -115 ≤ CPICH RSCP < -114 dBm
-- ...       ...      ...
-- cpich-RSCP = 89     -27 ≤ CPICH RSCP < -26 dBm
-- cpich-RSCP = 90     -26 ≤ CPICH RSCP < -25 dBm
-- cpich-RSCP = 91     -25 ≤ CPICH RSCP       dBm

CPICH-RSCP ::= INTEGER(0..127)

-- SPARE: Pathloss, Max = 158
-- Values above Max are spare
Pathloss ::= INTEGER(46..173)

maxCellMeas INTEGER ::= 32

maxFreq INTEGER ::= 8

maxTS INTEGER ::= 14

StatusCode ::= ENUMERATED {
  unspecified(0), systemFailure(1), unexpectedMessage(2), protocolError(3),
  dataMissing(4), unexpectedDataValue(5), posMethodFailure(6),
  posMethodMismatch(7), posProtocolMismatch(8), targetSETnotReachable(9),
  versionNotSupported(10), resourceShortage(11), invalidSessionId(12),
  nonProxyModeNotSupported(13), proxyModeNotSupported(14),
```

```
  positioningNotPermitted(15), authNetFailure(16), authSuplinitFailure(17),
consentDeniedByUser(100), consentGrantedByUser(101), ..., ver2-
incompatibleProtectionLevel(18), ver2-serviceNotSupported(19), ver2-
insufficientInterval(20), ver2-noSUPLCoverage(21), ver2-sessionStopped(102),
ver2-appIdDenied(103)}

QoP ::= SEQUENCE {
  horacc     INTEGER(0..127),
  veracc     INTEGER(0..127) OPTIONAL, -- as defined in [3GPP GAD] "uncertainty
altitude"
  maxLocAge  INTEGER(0..65535) OPTIONAL,
  delay      INTEGER(0..7) OPTIONAL, -- as defined in [3GPP RRLP]
  ...,
  ver2-responseTime   INTEGER (1..128) OPTIONAL}

Velocity ::= CHOICE { -- velocity definition as per [3GPP GAD]
  horvel           Horvel,
  horandvervel     Horandvervel,
  horveluncert     Horveluncert,
  horandveruncert  Horandveruncert,
  ...}

Horvel ::= SEQUENCE {
  bearing   BIT STRING(SIZE (9)),
  horspeed  BIT STRING(SIZE (16)),
  ...}

Horandvervel ::= SEQUENCE {
  verdirect  BIT STRING(SIZE (1)),
  bearing    BIT STRING(SIZE (9)),
  horspeed   BIT STRING(SIZE (16)),
  verspeed   BIT STRING(SIZE (8)),
  ...}

Horveluncert ::= SEQUENCE {
  bearing      BIT STRING(SIZE (9)),
  horspeed     BIT STRING(SIZE (16)),
  uncertspeed  BIT STRING(SIZE (8)),
  ...}

Horandveruncert ::= SEQUENCE {
  verdirect       BIT STRING(SIZE (1)),
  bearing         BIT STRING(SIZE (9)),
  horspeed        BIT STRING(SIZE (16)),
  verspeed        BIT STRING(SIZE (8)),
  horuncertspeed  BIT STRING(SIZE (8)),
  veruncertspeed  BIT STRING(SIZE (8)),
  ...}

PosMethod ::= ENUMERATED {
agpsSETassisted(0), agpsSETbased(1), agpsSETassistedpref(2),
agpsSETbasedpref(3), autonomousGPS(4), aflt(5), ecid(6), eotd(7), otdoa(8),
noPosition(9), ..., ver2-historicalDataRetrieval(10), ver2-
agnssSETassisted(11), ver2-agnssSETbased(12), ver2-agnssSETassistedpref(13),
ver2-agnssSETbasedpref(14), ver2-autonomousGNSS(15), ver2-sessioninfoquery(16),
ver2-mbs(17), ver2-NR-DL-TDOA(18), ver2-NR-DL-AoD(19), ver2-NR-Multi-RTT(20),
ver2-NR-DL-E-CID(21), ver2-NR-UL-TDOA(22), ver2-NR-UL-AoA(23)}
```

```
END
```

11.6 Common elements (SUPL Version 2)

```
Ver2-ULP-Components DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

EXPORTS Ver2-CellInfo-extension, MultipleLocationIds,
SupportedNetworkInformation, CauseCode, UTRAN-GPSReferenceTimeAssistance,
UTRAN-GPSReferenceTimeResult, SPCSETKey, SPCTID, SPCSETKeylifetime, UTRAN-
GANSSReferenceTimeAssistance, UTRAN-GANSSReferenceTimeResult,
GNSSPosTechnology, GANSSSignals, ThirdParty, ApplicationID, ReportingCap,
Coordinate, CircularArea, EllipticalArea, PolygonArea, Ver2-
HighAccuracyPosition;

IMPORTS
 LocationId, PrimaryCPICH-Info, CellParametersID, FQDN, Velocity
FROM ULP-Components;

MultipleLocationIds ::= SEQUENCE SIZE (1..maxLidSize) OF LocationIdData

LocationIdData ::= SEQUENCE {
locationId           LocationId,
relativetimestamp    RelativeTime OPTIONAL, -- if relativetimestamp is
present, then data represents historical measurement, if absent, data
represents current measurements
servingFlag          BOOLEAN, -- if "true" measurements represent serving cell
...}

RelativeTime ::= INTEGER (0..65535) -- relative time to "current" Location Id
in multiples of 0.01sec

maxLidSize           INTEGER ::= 64

SupportedNetworkInformation ::= SEQUENCE {
  wlan                              BOOLEAN,
  supportedWLANInfo                 SupportedWLANInfo OPTIONAL,
  supportedWLANApsList              SupportedWLANApsList OPTIONAL,
  gsm                               BOOLEAN,
  wcdma                             BOOLEAN,
  supportedWCDMAInfo                SupportedWCDMAInfo OPTIONAL,
  cdma                              BOOLEAN,
  hrdp                              BOOLEAN,
  umb                               BOOLEAN,
  lte                               BOOLEAN,
  wimax                             BOOLEAN,
  historic                          BOOLEAN,
  nonServing                        BOOLEAN,
  uTRANGPSReferenceTime             BOOLEAN,
  uTRANGANSSReferenceTime           BOOLEAN,
  ...,
  nr                                              BOOLEAN OPTIONAL}

SupportedWLANInfo ::= SEQUENCE {
  apTP        BOOLEAN, -- AP transmit power
  apAG        BOOLEAN, -- AP antenna gain
  apSN        BOOLEAN, -- AP S/N received at SET
  apDevType   BOOLEAN, -- Device type
```

```
  apRSSI      BOOLEAN, -- AP signal strength at SET
  apChanFreq  BOOLEAN, -- AP channel/frequency of Tx/Rx
  apRTD       BOOLEAN, -- Round Trip Delay between SET and AP
  setTP       BOOLEAN, -- SET transmit power
  setAG       BOOLEAN, -- SET antenna gain
  setSN       BOOLEAN, -- SET S/N received at AP
  setRSSI     BOOLEAN, -- SET signal strength at AP
  apRepLoc    BOOLEAN, -- AP Location as reported by AP (legacy encoding)
  ...,
  apRL        BOOLEAN OPTIONAL,  -- AP Location as reported by AP (as per
IEEE802.11)
  opClass     BOOLEAN OPTIONAL,  -- operating class as defined in IEEE 802.11
  apSSID      BOOLEAN OPTIONAL,  -- SSID of the wireless network served by AP
  apPHYType   BOOLEAN OPTIONAL,  -- AP PHY Type as defined in IEEE 802.11
  setMACAddress BOOLEAN OPTIONAL   -- SET MAC Address as known to the WLAN AP
}

maxWLANApDataSize    INTEGER ::= 128

SupportedWLANApsList ::= SEQUENCE {
 supportedWLANApDataList     SEQUENCE (SIZE (1..maxWLANApDataSize)) OF
SupportedWLANApData,
 supportedWLANapsChannel11a  SupportedWLANApsChannel11a  OPTIONAL,
 supportedWLANapsChannel11bg SupportedWLANApsChannel11bg OPTIONAL,
 ...
}

SupportedWLANApsChannel11a ::= SEQUENCE {
 ch34    BOOLEAN,
 ch36    BOOLEAN,
 ch38    BOOLEAN,
 ch40    BOOLEAN,
 ch42    BOOLEAN,
 ch44    BOOLEAN,
 ch46    BOOLEAN,
 ch48    BOOLEAN,
 ch52    BOOLEAN,
 ch56    BOOLEAN,
 ch60    BOOLEAN,
 ch64    BOOLEAN,
 ch149   BOOLEAN,
 ch153   BOOLEAN,
 ch157   BOOLEAN,
 ch161   BOOLEAN
}

SupportedWLANApsChannel11bg ::= SEQUENCE {
 ch1  BOOLEAN,
 ch2  BOOLEAN,
 ch3  BOOLEAN,
 ch4  BOOLEAN,
 ch5  BOOLEAN,
 ch6  BOOLEAN,
 ch7  BOOLEAN,
 ch8  BOOLEAN,
 ch9  BOOLEAN,
 ch10 BOOLEAN,
 ch11 BOOLEAN,
```

```
 ch12 BOOLEAN,
 ch13 BOOLEAN,
 ch14 BOOLEAN
}

SupportedWLANApData ::= SEQUENCE {
 apMACAddress  BIT STRING (SIZE (48)),
 apDevType  ENUMERATED {wlan802-11a(0), wlan802-11b(1), wlan802-11g(2), ...},
 ...}

SupportedWCDMAInfo ::= SEQUENCE {
  mrl    BOOLEAN, -- Measured Results List
  ...}

Ver2-CellInfo-extension ::= CHOICE {
  hrpdCell   HrpdCellInformation,
  umbCell    UmbCellInformation,
  lteCell    LteCellInformation,
  wlanAP     WlanAPInformation,
  wimaxBS    WimaxBSInformation,
  ...,
  nrCell     NRCellInformation}

HrpdCellInformation ::= SEQUENCE {
  refSECTORID    BIT STRING(SIZE (128)) OPTIONAL, -- HRPD Sector Id
  refBASELAT     INTEGER(0..4194303), -- Base Station Latitude
  reBASELONG     INTEGER(0..8388607), -- Base Station Longitude
  refWeekNumber  INTEGER(0..65535), -- GPS Week Number
  refSeconds     INTEGER(0..4194303), -- GPS Seconds
  ...}

UmbCellInformation ::= SEQUENCE {
  refSECTORID         BIT STRING(SIZE (128)), -- UMB Sector Id
  refMCC              INTEGER(0..999), -- Mobile Country Code
  refMNC              INTEGER(0..999), -- Mobile Network Code
  refBASELAT          INTEGER(0..4194303), -- Base Station Latitude
  reBASELONG          INTEGER(0..8388607), -- Base Station Longitude
  refWeekNumber       INTEGER(0..65535), -- GPS Week Number
  refSeconds          INTEGER(0..4194303), -- GPS Seconds
  ...}

-- LTE Cell info per 3GPP TS 36.331.
-- If not otherwise stated info is related to serving cell

LteCellInformation ::= SEQUENCE {
  cellGlobalIdEUTRA               CellGlobalIdEUTRA,
  physCellId                      PhysCellId,
  trackingAreaCode                TrackingAreaCode,
  rsrpResult                      RSRP-Range   OPTIONAL,
  rsrqResult                      RSRQ-Range   OPTIONAL,
  ta      INTEGER(0..1282) OPTIONAL, -- Currently used Timing Advance value
(N_TA/16 as per [3GPP 36.213])
  measResultListEUTRA   MeasResultListEUTRA OPTIONAL, --Neighbour measurements
  ...,
  earfcn INTEGER(0..65535) OPTIONAL, -- see Table 37
  earfcn-ext INTEGER (65536..262143) OPTIONAL, -- see Table 37
  rsrpResult-ext      RSRP-Range-Ext            OPTIONAL,
  rsrqResult-ext      RSRQ-Range-Ext            OPTIONAL,
```

```
  rs-sinrResult       RS-SINR-Range             OPTIONAL,
  servingInformation5G             ServingInformation5G      OPTIONAL
}
-- If rsrpResult-ext is included, rsrpResult shall be excluded or set to 0
-- If rsrqResult-ext is included and in the range 0 to 34, rsrqResult shall
--   be included and set equal to rsrqResult-ext
-- If rsrqResult-ext is included and outside the range 0 to 34, rsrqResult
shall
--   be excluded or set to 0 when rsrqResult-ext is negative or to 34 when
--   rsrqResult-ext is positive
-- servingInformation5G shall be included for a serving cell connected to 5GCN

-- Measured results of neighbours cells per 3GPP TS 36.331

MeasResultListEUTRA ::= SEQUENCE (SIZE (1..maxCellReport)) OF MeasResultEUTRA

MeasResultEUTRA ::=   SEQUENCE {
 physCellId PhysCellId,
 cgi-Info SEQUENCE {
        cellGlobalId CellGlobalIdEUTRA,
        trackingAreaCode TrackingAreaCode
} OPTIONAL,
 measResult SEQUENCE {
        rsrpResult   RSRP-Range   OPTIONAL,  -- Mapping to measured values
        rsrqResult   RSRQ-Range   OPTIONAL,  -- in 3GPP TS 36.133
        ...,
        earfcn       INTEGER(0..65535) OPTIONAL, -- see Table 37
        earfcn-ext   INTEGER (65536..262143) OPTIONAL, -- see Table 37
  rsrpResult-ext      RSRP-Range-Ext            OPTIONAL,
  rsrqResult-ext      RSRQ-Range-Ext            OPTIONAL,
  rs-sinrResult       RS-SINR-Range             OPTIONAL,
  neighbourInformation5G           NeighbourInformation5G    OPTIONAL
 }
}
-- If rsrpResult-ext is included, rsrpResult shall be excluded or set to 0
-- If rsrqResult-ext is included and in the range 0 to 34, rsrqResult shall
--   be included and set equal to rsrqResult-ext
-- If rsrqResult-ext is included and outside the range 0 to 34, rsrqResult
shall
--   be excluded or set to 0 when rsrqResult-ext is negative or to 34 when
--   rsrqResult-ext is positive
-- neighbourInformation5G may only be included for a cell connected to 5GCN

PhysCellId ::=         INTEGER (0..503)

TrackingAreaCode ::=  BIT STRING (SIZE (16))

CellGlobalIdEUTRA ::= SEQUENCE {
 plmn-Identity        PLMN-Identity,
 cellIdentity         CellIdentity,
 ...
}

PLMN-Identity ::= SEQUENCE {
 mcc MCC OPTIONAL,
 mnc MNC
}
```

```
CellIdentity ::= BIT STRING (SIZE (28))

MCC ::= SEQUENCE (SIZE (3)) OF MCC-MNC-Digit

MNC ::=  SEQUENCE (SIZE (2..3)) OF MCC-MNC-Digit

MCC-MNC-Digit ::= INTEGER (0..9)

RSRP-Range ::= INTEGER(0..97)
RSRQ-Range ::= INTEGER(0..34)
RSRP-Range-Ext ::= INTEGER(-17..-1)
RSRQ-Range-Ext ::= INTEGER(-30..46)
RS-SINR-Range ::= INTEGER(0..127)

ServingInformation5G ::= SEQUENCE {
  trackingAreaCode                TrackingAreaCodeNR,
  ...
}

NeighbourInformation5G ::= SEQUENCE {
  trackingAreaCode                TrackingAreaCodeNR        OPTIONAL,
  ...
}

maxCellReport INTEGER ::= 8

WlanAPInformation ::= SEQUENCE { -- as per [IEEE 802.11]
  apMACAddress       BIT STRING(SIZE (48)), -- AP MAC Address
  apTransmitPower    INTEGER(-127..128) OPTIONAL, -- AP transmit power in dbm
  apAntennaGain      INTEGER(-127..128) OPTIONAL, -- AP antenna gain in dBi
  apSignaltoNoise    INTEGER(-127..128) OPTIONAL, -- AP S/N received at SET
  apDeviceType       ENUMERATED {wlan802-11a(0), wlan802-11b(1), wlan802-
11g(2), ..., wlan802-11n(3), wlan802-11ac(4), wlan802-11ad(5)} OPTIONAL,
  apSignalStrength   INTEGER(-127..128) OPTIONAL, -- AP signal strength at SET
  apChannelFrequency INTEGER(0..256) OPTIONAL, -- AP channel/frequency of Tx/Rx
  apRoundTripDelay   RTD OPTIONAL, -- Round Trip Delay between SET and AP
  setTransmitPower   INTEGER(-127..128) OPTIONAL, -- SET transmit power in dBm
  setAntennaGain     INTEGER (-127..128) OPTIONAL, -- SET antenna gain in dBi
  setSignaltoNoise   INTEGER (-127..128) OPTIONAL, -- SET S/N received at AP
  setSignalStrength  INTEGER(-127..128) OPTIONAL, -- SET signal strength at AP
  apReportedLocation ReportedLocation OPTIONAL, -- AP Location reported by AP
(legacy encoding)
  ...,
  apRepLocation         RepLocation OPTIONAL, -- AP Location reported by AP
  apSignalStrengthDelta            INTEGER (0..1) OPTIONAL, -- see Table 41
  apSignaltoNoiseDelta             INTEGER (0..1) OPTIONAL, -- see Table 41
  setSignalStrengthDelta           INTEGER (0..1) OPTIONAL, -- see Table 41
  setSignaltoNoiseDelta            INTEGER (0..1) OPTIONAL, -- see Table 41
  operatingClass                   INTEGER (0..255) OPTIONAL,
  apSSID              OCTET STRING (SIZE (1..32)) OPTIONAL,
  apPHYType           ENUMERATED {unknown(0), any(1), fhss(2), dsss(3),
irbaseband(4), ofdm(5), hrdsss(6), erp(7), ht(8), ihv(9), ...} OPTIONAL,
  setMACAddress         BIT STRING(SIZE (48)) OPTIONAL -- MAC Address used by
SET to connect to AP
}

RTD ::= SEQUENCE { -- as per [IEEE 802.11]
  rTDValue     INTEGER(0..16777216), -- measured RTD value corresponding to
```

```
-- about 500km in units of 1/10 of nanoseconds
  rTDUnits     RTDUnits, -- units of RTD
  rTDAccuracy  INTEGER(0..255) OPTIONAL, -- RTD accuracy
  ...}

RTDUnits ::= ENUMERATED {
  microseconds(0), hundredsofnanoseconds(1), tensofnanoseconds(2),
nanoseconds(3), tenthsofnanoseconds(4), ...}

ReportedLocation ::= SEQUENCE { -- as per [IEEE 802.11v]
  locationEncodingDescriptor  LocationEncodingDescriptor,
  locationData        LocationData, -- location data field
  ...}

LocationEncodingDescriptor ::= ENUMERATED {
  lci(0), asn1(1), ...}

LocationData ::= SEQUENCE {
  locationAccuracy   INTEGER(0..4294967295) OPTIONAL,
  locationValue      OCTET STRING (SIZE(1..128)),
  ...}

RepLocation ::= CHOICE {
  lciLocData                      LciLocData, -- location data field as per
[IEEE 802.11] and [RFC 3825]
  ...    -- future formats may be added here
}

LciLocData ::= SEQUENCE {
   locationDataLCI  LocationDataLCI  OPTIONAL,
...}

LocationDataLCI ::= SEQUENCE {
  latitudeResolution              BIT STRING (SIZE (6)),
  latitude                        BIT STRING (SIZE (34)),
  longitudeResolution             BIT STRING (SIZE (6)),
  longitude                       BIT STRING (SIZE (34)),
  altitudeType                    BIT STRING (SIZE (4)),
  altitudeResolution              BIT STRING (SIZE (6)),
  altitude                        BIT STRING (SIZE (30)),
  datum                           BIT STRING (SIZE (8)),
...}

WimaxBSInformation ::= SEQUENCE {
  wimaxBsID          WimaxBsID,   -- WiMax serving base station ID
  wimaxRTD           WimaxRTD     OPTIONAL, -- Round Trip Delay measurements
  wimaxNMRList       WimaxNMRList OPTIONAL, -- Network measurements
  ...}

WimaxBsID ::= SEQUENCE {
  bsID-MSB           BIT STRING (SIZE(24)) OPTIONAL,
  bsID-LSB           BIT STRING (SIZE(24)),
  ...}
-- if only LSB is present, MSB is assumed to be identical to the current
serving BS or clamped on network value

WimaxRTD ::= SEQUENCE {
```

```
  rtd    INTEGER (0..65535), -- Round trip delay of serving BS in units of 10
ns
  rTDstd INTEGER (0..1023) OPTIONAL, -- Standard deviation of round trip delay
in units of 10 ns
...}

WimaxNMRList ::= SEQUENCE  (SIZE (1..maxWimaxBSMeas)) OF WimaxNMR

WimaxNMR ::= SEQUENCE {
  wimaxBsID   WimaxBsID,           -- WiMax BS ID for the measurement
  relDelay    INTEGER (-32768..32767) OPTIONAL, -- Relative delay for this
neighbouring BSs to the serving cell in units of 10 ns
  relDelaystd  INTEGER (0..1023) OPTIONAL, -- Standard deviation of Relative
delay in units of 10 ns
  rssi        INTEGER (0..255) OPTIONAL, -- RSSI in 0.25 dBm steps, starting
from -103.75 dBm
  rSSIstd     INTEGER (0..63) OPTIONAL, -- Standard deviation of RSSI in dB
  bSTxPower   INTEGER (0..255) OPTIONAL, -- BS transmit power in 0.25 dBm
steps, starting from -103.75 dBm
  cinr        INTEGER (0..255) OPTIONAL, -- in dB
  cINRstd     INTEGER (0..63) OPTIONAL, -- Standard deviation of CINR in dB
  bSLocation  ReportedLocation OPTIONAL, -- Reported location of the BS
...}

maxWimaxBSMeas INTEGER ::= 32

NRCellInformation ::= SEQUENCE {
  servingCellInformation           ServingCellInformationNR, --Serving cell
information
  measuredResultsListNR   MeasResultListNR      OPTIONAL, --Neighbour
measurements
  ...
}

-- Information for serving cells per 3GPP TS 38.331

ServingCellInformationNR ::= SEQUENCE (SIZE (1..maxNRServingCell)) OF
ServCellNR
-- The first listed serving cell shall be the primary cell

ServCellNR ::= SEQUENCE {
  physCellId                                    PhysCellIdNR,
  arfcn-NR                                      ARFCN-NR,
  cellGlobalId                     CellGlobalIdNR,
  trackingAreaCode                 TrackingAreaCodeNR,
  ssb-Measurements                 NR-Measurements           OPTIONAL,
  csi-rs-Measurements              NR-Measurements           OPTIONAL,
  ta                               INTEGER(0..3846) OPTIONAL, --Timing Advance
value
  ...,
  arfcn-type                       ENUMERATED {ssb, csi-rs}  OPTIONAL,
  systemFrameNumber                BIT STRING (SIZE (10))    OPTIONAL,
  ssb-IndexList-Measurements       SSB-IndexList-Measurements    OPTIONAL,
  csi-rs-IndexList-Measurements    CSI-RS-IndexList-Measurements OPTIONAL
}

-- Measured results of neighbours cells per 3GPP TS 38.331
```

```
MeasResultListNR ::= SEQUENCE (SIZE (1..maxCellReportNR)) OF MeasResultNR

MeasResultNR ::= SEQUENCE {
  physCellId                      PhysCellIdNR,
  arfcn-NR                        ARFCN-NR,
  cellGlobalId                    CellGlobalIdNR            OPTIONAL,
  trackingAreaCode                TrackingAreaCodeNR        OPTIONAL,
  ssb-Measurements                NR-Measurements           OPTIONAL,
  csi-rs-Measurements             NR-Measurements           OPTIONAL,
  ...,
  arfcn-type                      ENUMERATED {ssb, csi-rs}  OPTIONAL,
  systemFrameNumber               BIT STRING (SIZE (10))    OPTIONAL,
  ssb-IndexList-Measurements      SSB-IndexList-Measurements    OPTIONAL,
  csi-rs-IndexList-Measurements   CSI-RS-IndexList-Measurements OPTIONAL
}

PhysCellIdNR ::= INTEGER (0..1007)

ARFCN-NR ::= INTEGER (0.. 3279165)

TrackingAreaCodeNR ::= BIT STRING (SIZE (24))

CellGlobalIdNR ::= SEQUENCE {
 plmn-Identity       PLMN-Identity,
 cellIdentityNR      CellIdentityNR,
 ...
}

CellIdentityNR ::= BIT STRING (SIZE (36))

NR-Measurements ::=   SEQUENCE {
  rsrp-Range          INTEGER (0..127)          OPTIONAL,
  rsrq-Range          INTEGER (0..127)          OPTIONAL,
  sinr-Range          INTEGER (0..127)          OPTIONAL,
  ...
}

SSB-IndexList-Measurements ::= SEQUENCE (SIZE (1..64)) OF SSB-Index-
Measurements

SSB-Index-Measurements ::= SEQUENCE {
  ssb-Index-r16                   INTEGER (0..63),
  ssb-Measurements                NR-Measurements
}

CSI-RS-IndexList-Measurements ::= SEQUENCE (SIZE (1..64)) OF CSI-RS-Index-
Measurements

CSI-RS-Index-Measurements ::= SEQUENCE {
  csi-rs-Index                    INTEGER (0..95),
  csi-rs-Measurements             NR-Measurements
}

maxNRServingCell INTEGER ::= 32
maxCellReportNR INTEGER ::= 32
UTRAN-GPSReferenceTimeAssistance ::= SEQUENCE {
utran-GPSReferenceTime            UTRAN-GPSReferenceTime,
gpsReferenceTimeUncertainty       INTEGER (0..127) OPTIONAL,
```

```
utranGPSDriftRate                   UTRANGPSDriftRate OPTIONAL}

UTRAN-GPSReferenceTime ::= SEQUENCE {
-- For utran-GPSTimingOfCell values above 2322431999999 are not used in this
version of the specification. Actual value utran-GPSTimingOfCell = (ms-part *
4294967296) + ls-part used on the downlink i.e. sent from the SLP to the SET
     utran-GPSTimingOfCell         SEQUENCE {
        ms-part       INTEGER (0..1023),
        ls-part       INTEGER (0..4294967295)},
            modeSpecificInfo      CHOICE {
                      fdd         SEQUENCE {
                        referenceIdentity      PrimaryCPICH-Info},
                      tdd         SEQUENCE {
                        referenceIdentity      CellParametersID}} OPTIONAL,
            sfn       INTEGER (0..4095)}

UTRANGPSDriftRate ::= ENUMERATED {
      utran-GPSDrift0, utran-GPSDrift1, utran-GPSDrift2,
      utran-GPSDrift5, utran-GPSDrift10, utran-GPSDrift15,
      utran-GPSDrift25, utran-GPSDrift50, utran-GPSDrift-1,
      utran-GPSDrift-2, utran-GPSDrift-5, utran-GPSDrift-10,
      utran-GPSDrift-15, utran-GPSDrift-25, utran-GPSDrift-50}

UTRAN-GPSReferenceTimeResult ::= SEQUENCE {
-- For ue-GPSTimingOfCell values above 37158911999999 are not used in this
version of the specification. Actual value utran-GPSTimingOfCell = (ms-part *
4294967296) + ls-part used on the uplink i.e. reported by the SET to the SLP
     set-GPSTimingOfCell           SEQUENCE {
        ms-part       INTEGER (0.. 16383),
        ls-part       INTEGER (0..4294967295)},
            modeSpecificInfo      CHOICE {
                      fdd         SEQUENCE {
                        referenceIdentity      PrimaryCPICH-Info},
                      tdd         SEQUENCE {
                        referenceIdentity      CellParametersID}} OPTIONAL,
            sfn       INTEGER (0..4095),
     gpsReferenceTimeUncertainty   INTEGER (0..127) OPTIONAL,
     ...}

UTRAN-GANSSReferenceTimeAssistance ::= SEQUENCE {
ganssDay INTEGER (0..8191) OPTIONAL,
ganssTimeID           INTEGER (0..15),
utran-GANSSReferenceTime           UTRAN-GANSSReferenceTime,
utranGANSSDriftRate   UTRANGANSSDriftRate       OPTIONAL}

UTRAN-GANSSReferenceTime ::= SEQUENCE {

     ganssTOD INTEGER (0..86399),
     utran-GANSSTimingOfCell       INTEGER (0..3999999)OPTIONAL,
            modeSpecificInfo      CHOICE {
                      fdd         SEQUENCE {
                        referenceIdentity      PrimaryCPICH-Info},
                      tdd         SEQUENCE {
                        referenceIdentity      CellParametersID}} OPTIONAL,
            sfn       INTEGER (0..4095),
            ganss-TODUncertainty INTEGER (0..127) OPTIONAL,
...}
```

```
UTRANGANSSDriftRate ::= ENUMERATED {
      utran-GANSSDrift0, utran-GANSSDrift1, utran-GANSSDrift2,
      utran-GANSSDrift5, utran-GANSSDrift10, utran-GANSSDrift15,
      utran-GANSSDrift25, utran-GANSSDrift50, utran-GANSSDrift-1,
      utran-GANSSDrift-2, utran-GANSSDrift-5, utran-GANSSDrift-10,
      utran-GANSSDrift-15, utran-GANSSDrift-25, utran-GANSSDrift-50}

UTRAN-GANSSReferenceTimeResult ::= SEQUENCE {
     ganssTimeID      INTEGER (0..15),
     set-GANSSReferenceTime        SET-GANSSReferenceTime,
            ...}

SET-GANSSReferenceTime ::= SEQUENCE {
-- Actual value [ns] = (ms-Part * 4294967296 + ls-Part) * 250
-- Actual values [ns] > 86399999999750 are reserved and are considered a
-- protocol error
            set-GANSSTimingOfCell  SEQUENCE {
                 ms-part           INTEGER (0..80),
                 ls-part           INTEGER (0..4294967295)} OPTIONAL,
            modeSpecificInfo       CHOICE {
                      fdd          SEQUENCE {
                        referenceIdentity       PrimaryCPICH-Info},
                      tdd          SEQUENCE {
                        referenceIdentity       CellParametersID}} OPTIONAL,
            sfn       INTEGER (0..4095),
            ganss-TODUncertainty INTEGER (0..127) OPTIONAL,
...}

GNSSPosTechnology ::= SEQUENCE {
  gps                 BOOLEAN,
  galileo             BOOLEAN,
  sbas                BOOLEAN,
  modernized-gps      BOOLEAN,
  qzss                BOOLEAN,
  glonass             BOOLEAN,
...,
  bds                 BOOLEAN      OPTIONAL,
  rtk-osr             BOOLEAN      OPTIONAL}

-- indicates MS support for particular GANSS signals and frequencies coding
according to parameter definition in section 10.9

GANSSSignals ::= BIT STRING {
  signal1 (0),
  signal2 (1),
  signal3 (2),
  signal4 (3),
  signal5 (4),
  signal6 (5),
  signal7 (6),
  signal8 (7)} (SIZE (1..8))

SPCSETKey ::= BIT STRING(SIZE (128))

SPCTID ::= SEQUENCE {
  rand                BIT STRING(SIZE (128)),
  slpFQDN             FQDN,
        ...}
```

```
SPCSETKeylifetime ::= INTEGER (1..24) -- units in hours

CauseCode ::= ENUMERATED {
  servingNetWorkNotInAreaIdList(0), sETCapabilitiesChanged(1),
noSUPLCoverage(2), ...}

ThirdParty ::= SEQUENCE (SIZE (1..64)) OF ThirdPartyID

ThirdPartyID ::= CHOICE {
        logicalName  IA5String(SIZE (1..1000)),
        msisdn       OCTET STRING(SIZE (8)),
        emailaddr    IA5String(SIZE (1..1000)),
        sip-uri      VisibleString(FROM ("a".."z" | "A".."Z" | "0".."9" |
":./-_~%#@?")) (SIZE (1..255)),
        ims-public-identity       VisibleString(FROM ("a".."z" | "A".."Z" |
"0".."9" | ":./-_~%#@?")) (SIZE (1..255)),
        min          BIT STRING(SIZE (34)), -- coded according to TIA-553
        mdn          OCTET STRING(SIZE (8)),
        uri          VisibleString(FROM ("a".."z" | "A".."Z" | "0".."9" | "./-
_~%#")) (SIZE (1..255)),
...}

ApplicationID ::= SEQUENCE {
        appProvider IA5String(SIZE (1..24)), -- The application provider
        appName IA5String(SIZE (1..32)), -- The application name
        appVersion IA5String(SIZE (1..8)) OPTIONAL,  -- The application
version
...}

ReportingCap ::= SEQUENCE {
  minInt INTEGER (1..3600), -- units in seconds
  maxInt INTEGER (1..1440) OPTIONAL, -- units in minutes
  repMode            RepMode,
  batchRepCap        BatchRepCap OPTIONAL, -- only used for batch and quasi
real time reporting
  ...}

RepMode ::= SEQUENCE {
  realtime           BOOLEAN,
  quasirealtime      BOOLEAN,
  batch              BOOLEAN,
  ...}

BatchRepCap ::= SEQUENCE {
  report-position    BOOLEAN, -- set to "true" if reporting of position is
supported
  report-measurements BOOLEAN, -- set to "true" if reporting of measurements is
supported
  max-num-positions   INTEGER (1..1024) OPTIONAL,
  max-num-measurements INTEGER (1..1024) OPTIONAL,
  ...}

Coordinate::= SEQUENCE {
 latitudeSign        ENUMERATED {north(0), south(1)},
 latitude            INTEGER(0..8388607),
 longitude           INTEGER(-8388608..8388607)} -- Coding as in [3GPP GAD]
```

```
CircularArea ::= SEQUENCE {
 coordinate           Coordinate,
 radius               INTEGER(1..1000000), -- radius in meters
 radius-min           INTEGER(1..1000000) OPTIONAL, -- hysteresis minimum
radius
 radius-max           INTEGER(1..1500000) OPTIONAL} -- hysteresis maximum
radius

EllipticalArea ::= SEQUENCE {
 coordinate           Coordinate,
 semiMajor            INTEGER(1..1000000), -- units in meters
 semiMajor-min        INTEGER(1..1000000) OPTIONAL, -- hysteresis minimum
semiMajor
 semiMajor-max        INTEGER(1..1500000) OPTIONAL, -- hysteresis maximum
semiMajor
 semiMinor            INTEGER(1..1000000), -- units in meters
 semiMinor-min        INTEGER(1..1000000) OPTIONAL, -- hysteresis minimum
semiMinor
 semiMinor-max        INTEGER(1..1500000) OPTIONAL, -- hysteresis maximum
semiMinor
 angle                INTEGER(0.. 179)} -- units in degrees. The angle is
defined as the angle between the semi-major axis and North, increasing in a
clockwise direction. An angle of 0 represents an ellipse with the semi-major
axis pointing North/South while an angle of 90 represents an ellipse with the
semi-major axis pointing East/West.

PolygonArea ::= SEQUENCE {
 polygonDescription   PolygonDescription,
 polygonHysteresis    INTEGER(1..100000) OPTIONAL} --units in meters

PolygonDescription ::= SEQUENCE (SIZE (3..15)) OF Coordinate

Ver2-HighAccuracyPosition ::= SEQUENCE {
  timestamp         UTCTime, -- shall include seconds and shall use UTC time.
  highAccuracyPositionEstimate     HighAccuracyPositionEstimate,
  velocity          Velocity OPTIONAL,
...}

HighAccuracyPositionEstimate ::= SEQUENCE {
  degreesLatitude                  INTEGER(-2147483648..2147483647),
  degreesLongitude                 INTEGER(-2147483648..2147483647),
  uncertaintySemiMajor             INTEGER (0..255),
  uncertaintySemiMinor             INTEGER (0..255),
  orientationMajorAxis             INTEGER (0..179),
  horizontalConfidence             INTEGER (0..100),
  highAccuracyAltitudeInfo         HighAccuracyAltitudeInfo OPTIONAL,
...} -- Coding as in [3GPP GAD]

HighAccuracyAltitudeInfo ::= SEQUENCE {
  altitude                         INTEGER(64000..1280000),
  uncertaintyAltitude              INTEGER (0..255),
  verticalConfidence               INTEGER (0..100),
...} -- Coding as in [3GPP GAD]

END
```

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
OMA-TS-ULP-V1_0-20070615-A	15 Jun 2007	No previous version within OMA
OMA-TS-ULP-V2_0-20120417-A	17 Apr 2012	Status changed to Approved by TP Ref TP Doc # OMA-TP-2012-0170-INP_SUPL_20_for_Final_Approval
OMA-TS-ULP-V2_0_1-20121205-A	05 Dec 2012	Status changed to Approved by TP Ref TP Doc # OMA-TP-2012-0455-INP_SUPL_2.0.1_ERP_for_Notification
OMA-TS-ULP-V2_0_2-20140708-A	08 Jul 2014	Status changed to Approved by TP TP Ref # OMA-TP-2014-0149R01-INP_SUPL_V2_0_2_ERP_for_Notification
OMA-TS-ULP-V2_0_3-20160524-A	24 May 2016	Status changed to Approved by TP TP Ref # OMA-TP-2016-0075-INP_SUPL_V2_0_3_ERP_for_Notification
OMA-TS-ULP-V2_0_4-20181213-A	13 Dec 2018	Status changed to Approved by LOC WG Ref LOC WG Doc# OMA-LOC-2018-0022-INP_Secure_User_Plane_Location_2.0_ERP_for_Final_Approval_notification
OMA-TS-ULP-V2_0_5-20191028-A	28 Oct 2019	Status changed to Approved by LOC WG Ref LOC WG Doc# OMA-LOC-2019-0015-INP_Secure_User_Plane_Location_2.0_for_Final_Approval
OMA-TS-ULP-V2_0_6-20200804-A	04 Aug 2020	Status changed to Approved by LOC WG Ref LOC WG Doc# OMA-LOC-2020-0019-INP_Secure_User_Plane_Location_2.0.6_for_Final_Approval

Appendix B. Additional Information

B.1 MLP asynchronous request (informative)

The following call flow is provided as an example of how MLP works together with ULP. The Standard Location Immediate Service can generate several Standard Location Immediate Reports in some cases. This call flow illustrates a typical sequence of events in one of these cases.

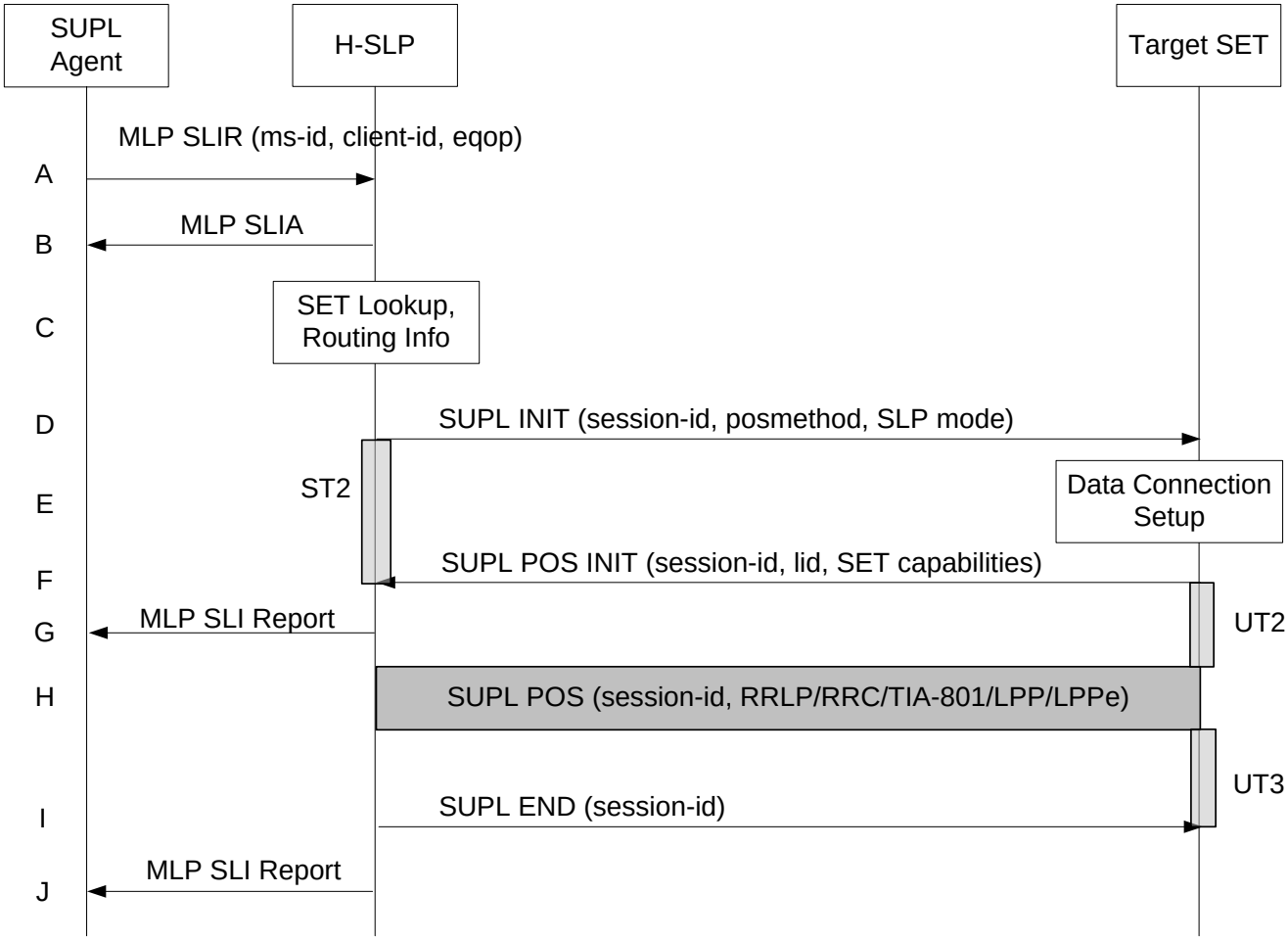

Figure 86: Network Initiated Non-Roaming Successful Case – Proxy Mode with asynchronous MLP request

A. SUPL Agent issues an MLP SLIR message to the H-SLP, with which SUPL Agent is associated. The res_type parameter is set to ASYNC. The loc_type parameter may be set to CURRENT_AND_INTERMEDIATE if the SUPL Agent wishes to receive coarse position estimates before the final position
The H-SLP shall authenticate the SUPL Agent and check if the SUPL Agent is authorized for the service it requests, based on the client-id received. Further, based on the received ms-id the H-SLP shall apply subscriber privacy against the client-id.

B. If a previously computed position which meets a requested QoP is available at the H-SLP and no notification and verification is required, the H-SLP sends the position estimate back to the SUPL Agent in an MLP SLIA message and the H-SLP shall release all resources related to this session. The result_type parameter shall be set to FINAL. If notification and verification or notification only is required, the H-SLP shall acknowledge the request in a MLP SLIA message to the SUPL Agent and proceed to step C.

C. The H-SLP verifies that the target SET is currently not SUPL roaming.
The H-SLP may also verify that the target SET supports SUPL.

NOTE: the specifics for determining if the SET is SUPL roaming or not is considered outside the scope of SUPL. However, there are various environment dependent mechanisms.

NOTE: The specifics for determining if the SET supports SUPL are beyond SUPL 2.0 scope.

D. The H-SLP initiates the location session with the SET using the SUPL INIT message, which may be a WAP PUSH or an SMS Trigger. The SUPL INIT message contains at least session-id, proxy/non-proxy mode indicator and the intended positioning method. If the result of the privacy check in Step A indicates that notification or verification to the target subscriber is needed, the H-SLP shall also include Notification element in the SUPL INIT message. Before the SUPL INIT message is sent the H-SLP also computes and stores a hash of the message.
If in step A the H-SLP decided to use a previously computed position, the SUPL INIT message shall indicate this in a 'no position' posmethod parameter value and the SET shall respond with a SUPL END message carrying the results of the verification process (access granted, or access denied). If no explicit verification is required (notification only) the SET shall respond with a SUPL END message. The H-SLP shall then directly proceed to step H.

NOTE: Before sending the SUPL END message the SET shall perform the data connection setup procedure of step D and use the procedures described in step E to establish a secure IP connection to the H-SLP.

E. The SET analyses the received SUPL INIT. If found to be non authentic SET takes not further actions. Otherwise the SET takes needed action preparing for establishment or resumption of a secure connection.

F. The SET will evaluate the Notification rules and follow the appropriate actions. The SET also checks the proxy/non-proxy mode indicator to determine if the H-SLP uses proxy or non-proxy mode. In this case, proxy mode is used, and the SET shall establish a secure IP connection to the H-SLP using SLP address that has been provisioned by the Home Network to the SET. The SET then sends a SUPL POS INIT message to start a positioning session with the H-SLP. The SET shall send the SUPL POS INIT message even if the SET supported positioning technologies do not include the intended positioning method indicated in the SUPL INIT message. The SUPL POS INIT message contains at least session-id, SET capabilities, a hash of the received SUPL INIT message (ver) and Location ID (lid). The SET capabilities include the supported positioning methods (e.g., SET-Assisted A-GPS, SET-Based A-GPS) and associated positioning protocols (e.g., RRLP, RRC, TIA-801 or LPP/LPPe). The SET may provide NMR specific for the radio technology being used (e.g., for GSM: TA, RXLEV). The SET may provide its position, if this is supported. The SET may set the Requested Assistance Data element in the SUPL POS INIT.
If a position retrieved from or calculated based on information received in the SUPL POS INIT message is available that meets a required QoP, the H-SLP may directly proceed to step J and not engage in a SUPL POS session.

G. As soon as the H-SLP gets a position estimate that does not meet the required QoP, it may send a MLP Standard Location Immediate Report with the position estimate. This step can actually happen at any time between steps C and I. The result_type parameter shall then be set to INTERMEDIATE.

H. The H-SLP shall check that the hash of SUPL INIT matches the one it has computed for this particular session. Based on the SUPL POS INIT message including posmethod(s) supported by the SET the H-SLP shall then determine the posmethod. If required for the posmethod the H-SLP shall use the supported positioning protocol (e.g., RRLP, RRC, TIA-801 or LPP/LPPe) from the SUPL POS INIT message.
The SET and the H-SLP exchange several successive positioning procedure messages.
The H-SLP calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance obtained from the H-SLP (SET-Based).

I. Once the position calculation is complete the H-SLP sends the SUPL END message to the SET informing it that no further positioning procedure will be started and that the location session is finished. The SET shall release the secure IP connection to the H-SLP and release all resources related to this session.

J. The H-SLP sends the position estimate back to the SUPL Agent in an MLP Standard Location Immediate Report message. The result_type parameter shall be set to FINAL. The H-SLP shall release all resources related to this session.

B.2 OMA Push Message Example (informative)

The Push message from the SLP (SLC for non-proxy mode) to the PPG contains the SUPL INIT message and follows [WAP PAP]. An example (informative only) is shown below:

POST / HTTP/1.1

Host: ppg.operator.com

Date: Thu, 2 December 2004 03:45:31 GMT

Content-Type: multipart/related; boundary=asdfghijkl; type=”application/xml”

Content-Length: XXX

--asdfghijkl

Content-Type: application/xml

<?xml version=”1.0”?><!DOCTYPE pap PUBLIC “-//WAPFORUM//DTD PAP 2.0//EN”

“http://www.wapforum.org/DTD/pap2.0.dtd” >

[<?wap-pap-ver supported-versions=”2.0”?>]>

<pap>

<push-message push-id=”faf34bcc3ca0f82cc0a8fd0c@slp.operator.com”>

<address address-value=”wappush=2063531234/TYPE=USER@ppg.operator.com”/ >

<quality-of-service priority=”medium”/>

</push-message>

</pap>

--asdfghijkl

Content-Length: 24

Content-Type: application/vnd.omaloc-supl-init

X-WAP-Application-Id: x-oma-application:ulp.ua

00180A00000000FAF34BCC3CA0F82CC0A8FD0CCAC1F8C010

--asdfghijkl--

The PAP elements used are:

- Push ID: the push ID is a unique value.
- Address Value: the subscriber is identified by a MSID. The full address value should be ”wappush=<msid>/TYPE=USER@<appropriate domain>”.
- Priority: set to the priority of this Location Service. This may be set to high for Emergency services and medium for other location services.
- Message Parameters:
    - Header:

- Content length should be set to the number of bytes in the SUPL INIT ASN.1 encoded body.
- Content type should be set to the value “application/vnd.omaloc-supl-init”
- Application ID should be set to “x-oma-application:ulp.ua”.

B.3 Body: the Body consists of the ASN.1 encoded SUPL INIT messagePOTAP Example (informative)

The detailed specification of the OMA Push message is described in Table 82.

Field	Reference	Size	Type	Value	Comments, with *Value* column alternatives
WSP PDU Header					
TID		1	Octet	—	Push ID (unique value)
PDU Type		1	Octet	0x06	Push
Push Header Length		1	Octet	(varies)	Length of Content Type plus Push Header excluding the actual Push Content (in hex).
content type		(depends on *Value* chosen)	Octet	(varies)	This field is the OMNA assigned WSP Content Type. Possible values are either the assigned number *0x312* WAP-encoded as *0x03020312*, or the NULL terminated ASCII string *application/vnd.omaloc-supl-init*
Push Header					
x-wap-application-id		1	Octet	0xAF	This field is the OMNA assigned number for registered PUSH Application ID field name *0x2F*, WAP short-integer-encoded as *0xAF*.
x-application-Id-field		(depends on *Value* chosen)	Octet	(varies)	This field is the OMNA assigned number for registered PUSH Application ID. Possible values are either the assigned number *0x10* WAP short-integer encoded as *0x90*, or the NULL terminated ASCII string *x-oma-application:ulp.ua*.
Push Content					
SUPL INIT Message		N	Octet	—	Message as specified in section 9.2.1.

Table 82: OMA Push user data

B.4 SIP Push Message Example (informative)

The following call flow is provided as an example of how SIP Push is used to support SUPL Initiation Function.

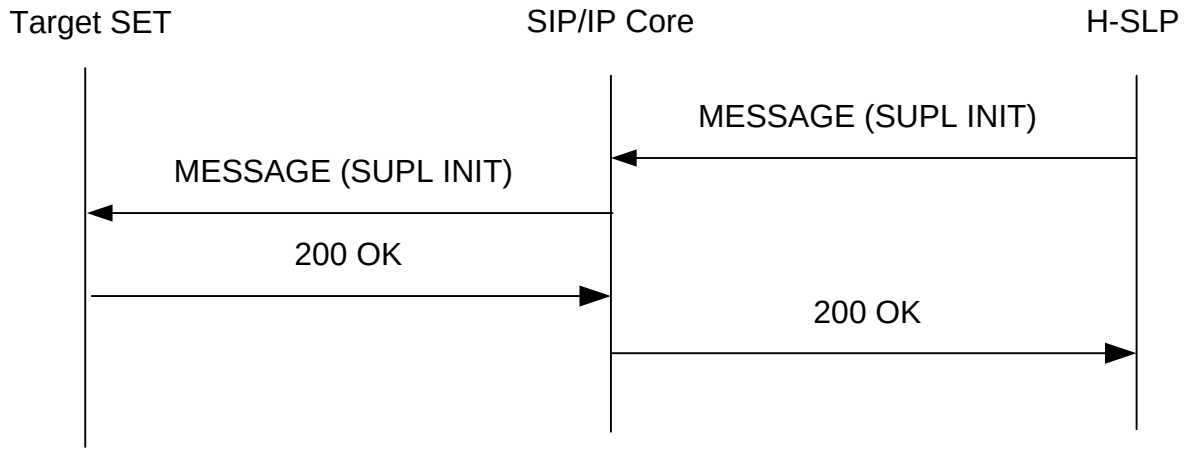

Figure 87: SIP Push Message flow

1. The H-SLP sends a MESSAGE request to the Target SET.

MESSAGE sip:targetsetuser@hslpoperator.com SIP/2.0

Via: SIP/2.0/TCP hslpserver.hslpoperator.com;branch=z9hG4bK776sgdkse

Max-Forwards: 70

From: sip:hslp@hslpoperator.com;tag=49583

To: sip:targetsetuser@hslpoperator.com

Accept-Contact: +g.oma.pusheventapp="ulp.ua”

Call-ID: asd88asd77a@1.2.3.4

CSeq: 1 MESSAGE

Content-Type: application/vnd.omaloc-supl-init

Content-Length: 24

00180A00000000FAF34BCC3CA0F82CC0A8FD0CCAC1F8C010

2. The SET returns a 200 OK to the H-SLP.

SIP/2.0 200 OK

Via: SIP/2.0/TCP proxy.hslpoperator.com;branch=z9hG4bK123dsghds

Via: SIP/2.0/TCP hslpserver.hslpoperator.com;branch=z9hG4bK776sgdkse

From: sip:hslp@hslpoperator.com;tag=49583

To: sip:targetsetuser@hslpoperator.com;tag=ab8asdasd9

Call-ID: asd88asd77a@1.2.3.4

CSeq: 1 MESSAGE

Content-Length: 0

B.5 SIP Push Message Example for IMS Emergency Location Services (informative)

The following call flow is provided as an example of how SIP Push is used to support SUPL Initiation Function in IMS Emergency Location Services.

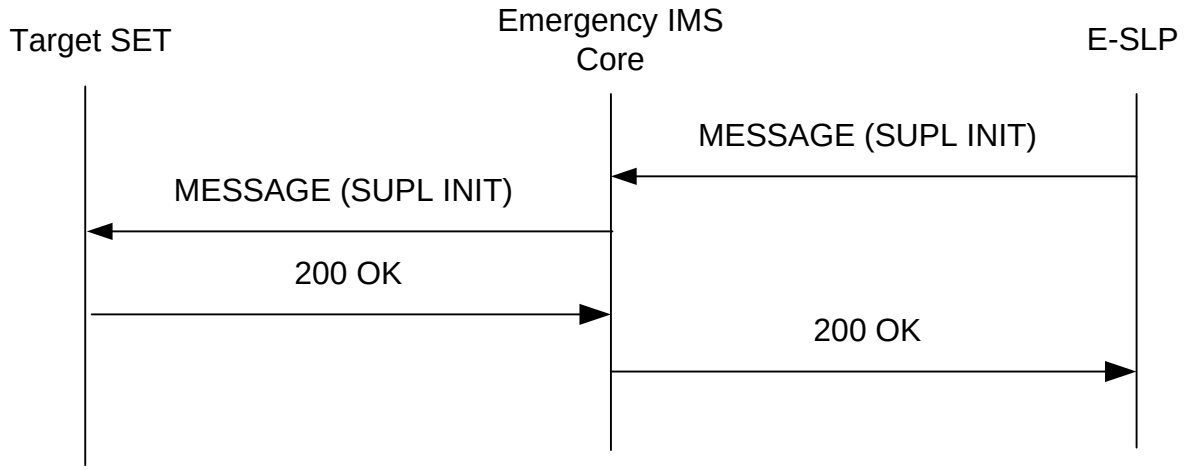

Figure 88: SIP Push Message Flow for IMS Emergency Location Services

1. The E-SLP sends a MESSAGE request to the Target SET.

MESSAGE sip:anonymous@1.2.3.4:1066 SIP/2.0

Via: SIP/2.0/TCP eslpserver.eslpoperator.com;branch=z9hG4bK776sgdkse

Max-Forwards: 70

From: sip:eslp@eslpoperator.com;tag=49583

To: sip:anonymous@1.2.3.4:1066

Accept-Contact: +g.oma.pusheventapp="ulp.ua”

Call-ID: asd88asd77a@5.6.7.8

CSeq: 1 MESSAGE

Content-Type: application/vnd.omaloc-supl-init

Content-Length: 24

00180A00000000FAF34BCC3CA0F82CC0A8FD0CCAC1F8C010

2. The SET returns a 200 OK to the E-SLP.

SIP/2.0 200 OK

Via: SIP/2.0/TCP pcscf.eslpoperator.com;branch=z9hG4bK123dsghds

Via: SIP/2.0/TCP ecscf.eslpoperator.com;branch=z9hG4bK889tcsxyp

Via: SIP/2.0/TCP eslpserver.eslpoperator.com;branch=z9hG4bK776sgdkse

From: sip:eslp@eslpoperator.com;tag=49583

To: sip: anonymous@1.2.3.4:1066;tag=ab8asdasd9

Call-ID: asd88asd77a@5.6.7.8

CSeq: 1 MESSAGE

Content-Length: 0

B.6 Area Event Trigger Examples (informative)

The following section provides examples of how area event triggers can be used singly or combined to support different use cases. These examples can themselves be combined for new use cases.

B.6.1 Single report when SET is inside target area

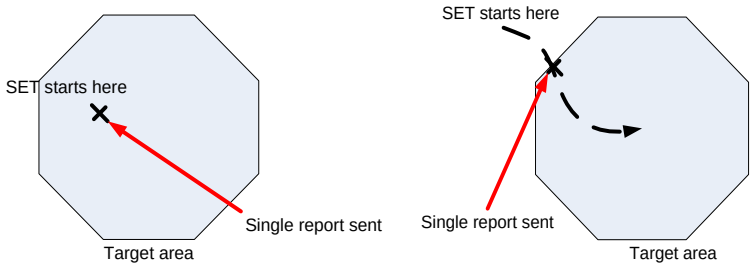

Figure 89: Single report when SET is inside area

Behaviour:	Report once only the first time the SET detects it is inside the target area.
Example use case:	An advertising service is triggered once a user is within a certain area.
Triggers:	“Entering” trigger with no repeated reporting OR “Inside” trigger with no repeated reporting.

B.6.2 Single report when SET is outside target area

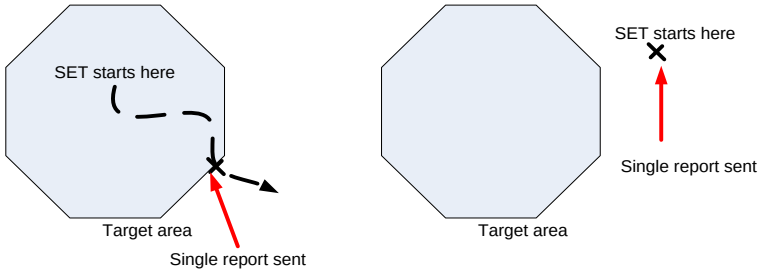

Figure 90: Single report when SET is outside area

Behaviour:	Report once only the first time the SET detects it is outside the target area.

Example use case:	An asset tracking service generates an alert if a vehicle goes outside a predetermined area.
Triggers:	"Leaving" trigger with no repeated reporting OR "Outside" trigger with no repeated reporting.

B.6.3 Repeated reports whenever SET is inside target area

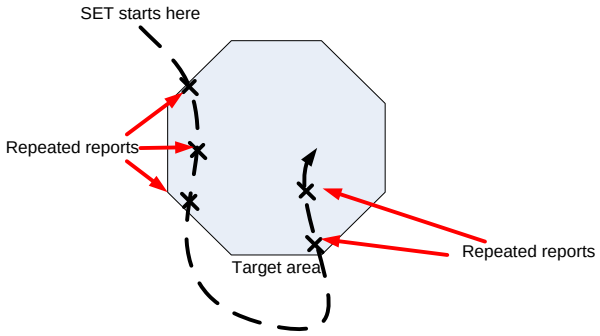

Figure 91: Repeated reports whenever SET is inside target area

Behaviour:	Report at regular intervals while the SET is inside the target area.
Example use case:	A staff locator service tracks the location of employees while they are on campus, but not while they are off-site.
Triggers:	"Inside" trigger with repeated reporting.

B.6.4 Repeated reports whenever SET is outside target area

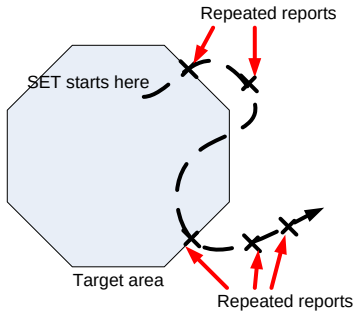

Figure 92: Repeated reports when SET is outside area

Behaviour:	Report at regular intervals while the SET is outside the target area.
Example use case:	An asset tracking service tracks the location of company vehicles while they are on the road, but not while they are within their compound.
Triggers:	"Outside" trigger with repeated reporting.

B.6.5 Repeated reports each time SET enters target area

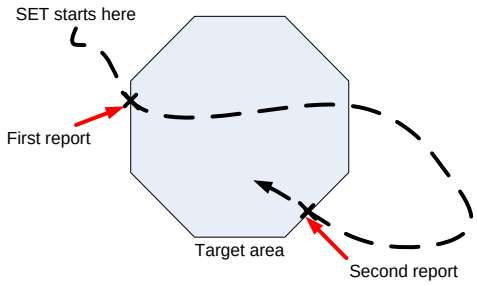

Figure 93: Repeated reports each time SET enters target area

Behaviour:	Report each time SET enters the target area.
Example use case:	A social networking service alerts friends whenever a user enters a predefined area.
Triggers:	"Entering" trigger with repeated reporting.

B.6.6 Repeated reports each time SET leaves target area

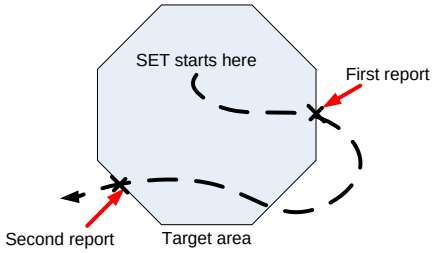

Figure 94: Repeated reports each time SET leaves target area

Behaviour:	Report each time SET enters the target area.
Example use case:	An employee tracking service records each time an employee leaves an assigned region.
Triggers:	"Leaving" trigger with repeated reporting.

B.6.7 Repeated reports for a fixed period after SET leaves target area

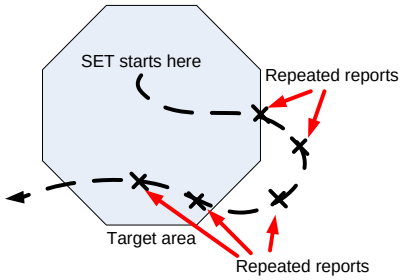

Figure 95: Repeated reports for a fixed period after SET leaves target area

Behaviour:	Report a fixed number of times after SET leaves the target area, regardless of whether it re-enters.
Example use case:	An asset tracking service tracks potentially stolen equipment after it has left an assigned area.
Triggers:	“Leaving” trigger without repeated reporting, followed by periodic trigger.

B.6.8 Repeated reports for a fixed period after SET enters target area

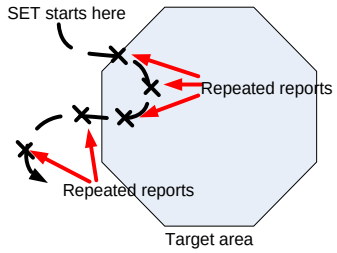

Figure 96: Repeated reports for a fixed period after SET enters target area

Behaviour:	Report a fixed number of times after SET enters the target area, regardless of whether it subsequently exits the target area
Example use case:	A vehicle tracking service generates notifications each time a vehicle enters a predefined area along with an estimated vector calculated by a new of multiple position reports in quick succession.
Triggers:	“Entering” trigger without repeated reporting, followed by periodic trigger.

B.7 Interpretation of Geographic Target Areas and Area Id Lists when both are present (informative)

The area id list concept is used to optimize the behavior of the SET (e.g. minimize battery consumption, save radio bandwidth, reduce the load on the SLP, etc.) and is defined as follows: for each geographic target area there may be two area id lists: (1) one area id list which is *completely* inside the geographic target area called "within" and (2) one area id list which covers the *entire* border area called "border" (refer to Figure 97). The type of the area id list is expressed in the parameter *Area Id Set Type* (part of *Area Event Params*) which can be of type "border" or "within". The following rules apply:

- If a "within" area id list is provided and the SET determines that it is inside the "within" area id list, the SET can assume that it is within the geographic target area.
- If a "border" area id list is provided and the SET determines it is not within either the "border" or the "within" area id list, the SET can assume it is outside the geographic target area. Note that it may be impossible for the H-SLP to completely verify the completeness of area id lists.

Please note that it is up to the SET to decide what action to take after determining that its position is either within or outside the geographic target area.

Depending on the shape and location of the geographic target area, the radio network coverage or the ability of the SLP to generate suitable area id lists, there may or may not be clearly defined "within" or "border" area id lists (examples: (1) one single large radio cell covers the entire geographic target area i.e. there is no "within" area id list but only a "border" area id list; (2) two single large radio cells each partially cover the geographic target area but fail to cover the entire geographic target area i.e. there is no "within" area id list nor is there a "border" area id list).

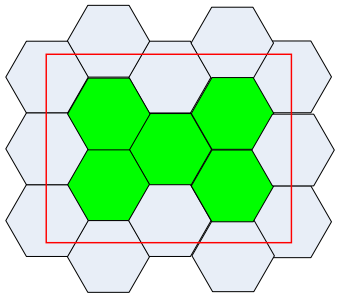

Figure 97: Area ID Lists and Geographic Target Area. The geographic Target Area is shown as bold red line. Note that in this example the green area id list constitutes the "within" area id list while the grey area id list constitutes the "border" area id list.

Appendix C. Static Conformance Requirements (Normative)

The notation used in this appendix is specified in [IOPPROC].

C.1 SCR for SUPL Server

C.1.1 SLP Procedures

Item	Function	Reference	Requirement
ULP-PRO-S-001-O	SLP supporting 3GPP defined system mode	-	ULP-PRO-S-009-O AND ULP-PRO-S-011-O AND ULP-PRO-S-023-O
ULP-PRO-S-002-O	SLP supporting 3GPP2 defined system mode	-	(ULP-PRO-S-009-O OR ULP-PRO-S-010-O) AND (ULP-PRO-S-011-O OR ULP-PRO-S-012-O) AND ULP-PRO-S-025-O
ULP-PRO-S-003-O	SLP supporting WiMAX mode		ULP-PRO-S-008-O AND (ULP-PRO-S-009-O OR ULP-PRO-S-011-O)
Security modes			
ULP-PRO-S-004-O	Security function, GBA authentication model	ULP 6	ULP-PRO-S-039-O
ULP-PRO-S-005-M	Security function, ACA authentication model	ULP 6	ULP-PRO-S-038-M
ULP-PRO-S-006-O	Security function, SSK authentication model	ULP 6	ULP-PRO-S-039-O
ULP-PRO-S-007-O	Security function, SLC only authentication model	ULP 6	ULP-PRO-S-038-M
ULP-PRO-S-008-O	Security function, SEK authentication model	ULP 6	ULP-PRO-S-039-O
High-level procedures			
ULP-PRO-S-009-O	Support of network initiated procedures in Proxy mode	ULP 5.1	
ULP-PRO-S-010-O	Support of network initiated procedures in Non-Proxy mode	ULP 5.1	ULP-MES-S-007-O AND ULP-MES-S-008-O
ULP-PRO-S-011-O	Support of SET initiated procedures in Proxy mode	ULP 5.2	
ULP-PRO-S-012-O	Support of SET initiated procedures in Non-Proxy mode	ULP 5.2	
Positioning methods			

Item	Function	Reference	Requirement
ULP-PRO-S-013-O	Support of Cell ID positioning method	AD 5.3.2.3	
ULP-PRO-S-014-O	Support of SET-assisted A-GPS positioning method	AD 5.3.2.3	ULP-MES-S-005-M
ULP-PRO-S-015-O	Support of SET-Based A-GPS positioning method	AD 5.3.2.3	ULP-MES-S-005-M
ULP-PRO-S-016-O	Support of Autonomous GPS/GANSS positioning method	AD 5.3.2.3	ULP-MES-S-005-M
ULP-PRO-S-017-O	Support of SET-assisted A-GANSS positioning method	AD 5.3.2.3	ULP-MES-S-005-M
ULP-PRO-S-018-O	Support of SET-Based A-GANSS positioning method	AD 5.3.2.3	ULP-MES-S-005-M
ULP-PRO-S-019-O	Support of AFLT positioning method	AD 5.3.2.3	ULP-MES-S-005-M
ULP-PRO-S-020-O	Support of Enhanced Cell ID positioning method	AD 5.3.2.3	
ULP-PRO-S-021-O	Support of E-OTD positioning method	AD 5.3.2.3	ULP-MES-S-005-M
ULP-PRO-S-022-O	Support of OTDOA positioning method	AD 5.3.2.3	ULP-MES-S-005-M
ULP-PRO-S-023-O	Support of RRLP positioning protocol	AD 5.3.3.1.2	
ULP-PRO-S-024-O	Support of RRC positioning protocol	AD 5.3.3.1.2	
ULP-PRO-S-025-O	Support of TIA-801 positioning protocol	AD 5.3.3.1.2	
ULP-PRO-S-026-O	Support of LPP/LPPe positioning protocol	AD 5.3.3.1.2	
ULP Version Negotiation			
ULP-PRO-S-027-M	Support of ULP version Negotiation	ULP 7	
Detailed procedures			
ULP-PRO-S-028-M	Support of Notification	ULP 9, 10, 11	
ULP-PRO-S-029-O	Support of reception of QoP	ULP 9, 10, 11	
ULP-PRO-S-030-O	Support of sending of QoP	ULP 9, 10, 11	
ULP-PRO-S-031-O	Support of Notification based on current location	ULP 9, 10, 11	
ULP-PRO-S-032-O	Support of initial position	ULP 9, 10, 11	
ULP-PRO-S-033-O	Support of Supported Network Information	ULP 9, 10, 11	

Item	Function	Reference	Requirement
ULP-PRO-S-034-O	Support of Trigger Type: Periodic	ULP 9, 10, 11	
ULP-PRO-S-035-O	Support of Trigger Type: Area Event	ULP 9, 10, 11	
ULP-PRO-S-036-M	Support of Emergency Services location request	ULP 9, 10, 11	
ULP-PRO-S-037-O	Support of Historic Reporting	ULP 9, 10, 11	
ULP-PRO-S-038-M	Support of Protection Level: Null Protection	ULP 9, 10, 11	
ULP-PRO-S-039-O	Support of Protection Level: Basic Protection	ULP 9, 10, 11	
ULP-PRO-S-040-O	Support of Location request of another SET	ULP 9, 10, 11	
ULP-PRO-S-041-O	Support of Multiple Location IDs	ULP 9, 10, 11	
ULP-PRO-S-042-O	Support of Location request with transfer to third Party	ULP 9, 10, 11	
ULP-PRO-S-043-O	Support of requested assistance data	ULP 9, 10, 11	
ULP-PRO-S-044-O	Support of UTRAN GPS Reference Time Result/Assistance	ULP 9, 10, 11	
ULP-PRO-S-045-O	Support of UTRAN GANSS Reference Time Result/Assistance	ULP 9, 10, 11	
ULP-PRO-S-046-O	Support of reception of velocity	ULP 9, 10, 11	
ULP-PRO-S-047-O	Support of sending of velocity	ULP 9, 10, 11	
ULP-PRO-S-048-O	Support of Reporting Capability: Real time	ULP 9, 10, 11	
ULP-PRO-S-049-O	Support of Reporting Capability: Quasi real time	ULP 9, 10, 11	
ULP-PRO-S-050-O	Support of Reporting Capability: Batch reporting	ULP 9, 10, 11	
ULP-PRO-S-051-O	Support of Session Info query	ULP 9, 10, 11	

C.1.2 ULP Protocol Interface

Item	Function	Reference	Requirement
ULP-PIN-S-001-M	ULP encoding	ULP 8	
ULP-PIN-S-002-M	ULP transport	ULP 8	ULP-PIN-S-003-M AND (ULP-PIN-S-004-O OR ULP-PIN-S-005-O)

Item	Function	Reference	Requirement
ULP-PIN-S-003-M	Support of TCP/IP port number	ULP 8	
ULP-PIN-S-004-O	Support of OMA Push	ULP 8	
ULP-PIN-S-005-O	Support of MT SMS	ULP 8	
ULP-PIN-S-006-O	Support of SIP Push	ULP 8	
ULP-PIN-S-007-O	Support of UDP	ULP 8	

C.1.3 ULP Messages

Item	Function	Reference	Requirement
ULP-MES-S-001-M	Support of SUPL INIT	ULP 9,10,11	
ULP-MES-S-002-M	Support of SUPL START	ULP 9,10,11	
ULP-MES-S-003-M	Support of SUPL RESPONSE	ULP 9,10,11	
ULP-MES-S-004-M	Support of SUPL POS INIT	ULP 9,10,11	
ULP-MES-S-005-M	Support of SUPL POS	ULP 9,10,11	
ULP-MES-S-006-M	Support of SUPL END	ULP 9,10,11	
ULP-MES-S-007-O	Support of SUPL AUTH REQ	ULP 9,10,11	
ULP-MES-S-008-O	Support of SUPL AUTH RESP	ULP 9,10,11	
ULP-MES-S-009-M	Support of SUPL TRIGGERED START	ULP 9,10,11	
ULP-MES-S-010-O	Support of SUPL TRIGGERED RESPONSE	ULP 9,10,11	
ULP-MES-S-011-O	Support of SUPL TRIGGERED STOP	ULP 9,10,11	
ULP-MES-S-012-O	Support of SUPL NOTIFY	ULP 9,10,11	
ULP-MES-S-013-O	Support of SUPL NOTIFY RESPONSE	ULP 9,10,11	
ULP-MES-S-014-O	Support of SUPL SET INIT	ULP 9,10,11	
ULP-MES-S-015-O	Support of SUPL REPORT	ULP 9,10,11	

C.2 SCR for SUPL CLIENT

C.2.1 SET Procedures

Item	Function	Reference	Requirement
ULP-PRO-C-001-O	SET supporting 3GPP defined system mode		ULP-PRO-C-007-O AND ULP-PRO-C-009-O AND ULP-PRO-C-021-O

Item	Function	Reference	Requirement
ULP-PRO-C-002-O	SET supporting 3GPP2 defined system mode		ULP-PRO-C-007-O AND ULP-PRO-C-008-O AND ULP-PRO-C-009-O AND ULP-PRO-C-010-O AND ULP-PRO-C-023-O
ULP-PRO-C-003-O	SET supporting WiMAX mode		ULP-PRO-C-006-O AND (ULP-PRO-S-007-O OR ULP-PRO-S-009-O)
Security modes			
ULP-PRO-C-004-O	Security function, GBA authentication model	ULP 6	ULP-PRO-C-037-O
ULP-PRO-C-005-M	Security function, ACA authentication model	ULP 6	ULP-PRO-C-036-M
ULP-PRO-C-006-O	Security function, SEK authentication model	ULP 6	ULP-PRO-C-037-O
High-level procedures			
ULP-PRO-C-007-O	Support of network initiated procedures in Proxy mode	ULP 5.1	
ULP-PRO-C-008-O	Support of network initiated procedures in Non-Proxy mode	ULP 5.1	ULP-MES-C-007-O AND ULP-MES-C-008-O
ULP-PRO-C-009-O	Support of SET initiated procedures in Proxy mode	ULP 5.2	
ULP-PRO-C-010-O	Support of SET initiated procedures in Non-Proxy mode	ULP 5.2	
Positioning methods			
ULP-PRO-C-011-M	Support of Cell ID positioning method	AD 5.3.2.3	
ULP-PRO-C-012-O	Support of SET-assisted A-GPS positioning method	AD 5.3.2.3	ULP-MES-C-005-O
ULP-PRO-C-013-O	Support of SET-Based A-GPS positioning method	AD 5.3.2.3	ULP-MES-C-005-O
ULP-PRO-C-014-O	Support of Autonomous GPS/GANSS positioning method	AD 5.3.2.3	ULP-MES-C-005-O
ULP-PRO-C-015-O	Support of SET-assisted A-GANSS positioning method	AD 5.3.2.3	ULP-MES-C-005-O
ULP-PRO-C-016-O	Support of SET-Based A- GANSS positioning method	AD 5.3.2.3	ULP-MES-C-005-O

Item	Function	Reference	Requirement
ULP-PRO-C-017-O	Support of AFLT positioning method	AD 5.3.2.3	ULP-MES-C-005-O
ULP-PRO-C-018-O	Support of Enhanced Cell ID positioning method	AD 5.3.2.3	
ULP-PRO-C-019-O	Support of E-OTD positioning method	AD 5.3.2.3	ULP-MES-C-005-O
ULP-PRO-C-020-O	Support of OTDOA positioning method	AD 5.3.2.3	ULP-MES-C-005-O
ULP-PRO-C-021-O	Support of RRLP positioning protocol	AD 5.3.3.1.2	
ULP-PRO-C-022-O	Support of RRC positioning protocol	AD 5.3.3.1.2	
ULP-PRO-C-023-O	Support of TIA-801 positioning protocol	AD 5.3.3.1.2	
ULP-PRO-C-024-O	Support of LPP/LPPe positioning protocol	AD 5.3.3.1.2	
ULP Version Negotiation			
ULP-PRO-C-025-M	Support of ULP version Negotiation	ULP 7	
Detailed procedures			
ULP-PRO-C-026-M	Support of Notification	ULP 9, 10, 11	
ULP-PRO-C-027-O	Support of reception of QoP	ULP 9, 10, 11	
ULP-PRO-C-028-O	Support of sending of QoP	ULP 9, 10, 11	
ULP-PRO-C-029-O	Support of Notification based on current location	ULP 9, 10, 11	
ULP-PRO-C-030-O	Support of initial position	ULP 9, 10, 11	
ULP-PRO-C-031-M	Support of Supported Network Information	ULP 9, 10, 11	
ULP-PRO-C-032-O	Support of Trigger Type: Periodic	ULP 9, 10, 11	
ULP-PRO-C-033-O	Support of Trigger Type: Area Event	ULP 9, 10, 11	
ULP-PRO-C-034-M	Support of Emergency Services location request	ULP 9, 10, 11	
ULP-PRO-C-035-O	Support of Historic Reporting	ULP 9, 10, 11	
ULP-PRO-C-036-M	Support of Protection Level: Null Protection	ULP 9, 10, 11	
ULP-PRO-C-037-O	Support of Protection Level: Basic Protection	ULP 9, 10, 11	
ULP-PRO-C-038-O	Support of Location request of another SET	ULP 9, 10, 11	
ULP-PRO-C-039-O	Support of Multiple Location IDs	ULP 9, 10, 11	

Item	Function	Reference	Requirement
ULP-PRO-C-040-O	Support of Location request with transfer to third Party	ULP 9, 10, 11	
ULP-PRO-C-041-O	Support of requested assistance data	ULP 9, 10, 11	
ULP-PRO-C-042-O	Support of UTRAN GPS Reference Time Result/Assistance	ULP 9, 10, 11	
ULP-PRO-C-043-O	Support of UTRAN GANSS Reference Time Result/Assistance	ULP 9, 10, 11	
ULP-PRO-C-044-O	Support of reception of velocity	ULP 9, 10, 11	
ULP-PRO-C-045-O	Support of sending of velocity	ULP 9, 10, 11	
ULP-PRO-C-046-O	Support of Reporting Capability: Real time	ULP 9, 10, 11	
ULP-PRO-C-047-O	Support of Reporting Capability: Quasi real time	ULP 9, 10, 11	
ULP-PRO-C-048-O	Support of Reporting Capability: Batch reporting	ULP 9, 10, 11	
ULP-PRO-C-049-O	Support of Session Info query	ULP 9, 10, 11	

C.2.2 ULP Protocol Interface

Item	Function	Reference	Requirement
ULP-PIN-C-001-M	ULP encoding	ULP 8	
ULP-PIN-C-002-M	ULP transport	ULP 8	
ULP-PIN-C-003-M	Support of TCP/IP port number	ULP 8	
ULP-PIN-C-004-M	Support of OMA Push	ULP 8	
ULP-PIN-C-005-M	Support of MT SMS	ULP 8	
ULP-PIN-C-006-O	Support of SIP Push	ULP 8	
ULP-PIN-C-007-O	Support of UDP	ULP 8	

C.2.3 ULP Messages

Item	Function	Reference	Requirement
ULP-MES-C-001-M	Support of SUPL INIT	ULP 9,10,11	
ULP-MES-C-002-M	Support of SUPL START	ULP 9,10,11	
ULP-MES-C-003-M	Support of SUPL RESPONSE	ULP 9,10,11	
ULP-MES-C-004-M	Support of SUPL POS INIT	ULP 9,10,11	
ULP-MES-C-005-O	Support of SUPL POS	ULP 9,10,11	

Item	Function	Reference	Requirement
ULP-MES-C-006-M	Support of SUPL END	ULP 9,10,11	
ULP-MES-C-007-O	Support of SUPL AUTH REQ	ULP 9,10,11	
ULP-MES-C-008-O	Support of SUPL AUTH RESP	ULP 9,10,11	
ULP-MES-C-009-O	Support of SUPL TRIGGERED START	ULP 9,10,11	
ULP-MES-C-010-O	Support of SUPL TRIGGERED RESPONSE	ULP 9,10,11	
ULP-MES-C-011-O	Support of SUPL TRIGGERED STOP	ULP 9,10,11	
ULP-MES-C-012-O	Support of SUPL NOTIFY	ULP 9,10,11	
ULP-MES-C-013-O	Support of SUPL NOTIFY RESPONSE	ULP 9,10,11	
ULP-MES-C-014-O	Support of SUPL SET INIT	ULP 9,10,11	
ULP-MES-C-015-O	Support of SUPL REPORT	ULP 9,10,11	

Appendix D. Timers

This section defines the SUPL timers. Note that default timer value is informative.

Timer	Default value (sec.)	Description	Actions on expiration
UT1	11	For immediate applications, from sending of SUPL START to receipt of SUPL RESPONSE or SUPL END. In trigger positioning, from sending of SUPL TRIGGERED START to receipt of SUPL TRIGGERED RESPONSE or SUPL END.	The SET sends SUPL END to the SLP. The SET clears all session resources at the SET.
UT2	11	From sending of SUPL POS INIT to receipt of first SUPL POS, SUPL REPORT or SUPL END message. UT2 is not needed if the SUPL POS INIT message contains the first SUPL POS element.	For immediate applications the SET sends SUPL END to the SLP and clears all session resources. For triggered applications, the SET skips the SUPL POS session and continues the triggered session.
UT3	10	From sending of the last SUPL POS message to receipt of SUPL END, SUPL REPORT or SUPL NOTIFY. In cases where there is no SUPL POS message sent from SET, timer UT3 is not used.	For immediate applications, the SET sends SUPL END to the SLP and clears all session resources. For triggered applications, the SET continues the triggered session.
UT4	10	Only applicable to non-proxy mode. From sending of SUPL AUTH REQ to receipt of SUPL AUTH RESP message.	The SET sends SUPL END to the SLP. The SET clears all session resources.
UT5	10	Only applicable to “notification based on location” scenarios. From sending of SUPL NOTIFY RESPONSE to receipt of SUPL END.	The SET sends SUPL END to the SLP. The SET clears all session resources.
UT6	10	Only applicable to “notification based on location” in non-proxy mode scenarios. From sending of SUPL REPORT to receipt of SUPL NOTIFY or SUPL END.	The SET sends SUPL END to the SLP. The SET clears all session resources.
UT7	10	Only applicable to triggered scenarios. From sending of SUPL TRIGGERED STOP to receipt of SUPL END.	The SET sends SUPL END to the SLP. The SET clears all session resources.
UT8	10	Only applicable to triggered periodic scenarios. From sending the last SUPL REPORT message to receipt of SUPL END.	The SET sends SUPL END to the SLP. The SET clears all session resources.
UT9	60	Only applicable to SET Initiated Location Request of Another SET. From sending of SUPL SET INIT to receipt of SUPL END.	The SET sends SUPL END to the SLP. The SET clears all session resources.
UT10	60	Only applicable to the Session Info Query scenarios. From sending of SUPL REPORT to receipt of SUPL END for the Session Info Query Session.	The SET sends SUPL END to the SLP. The SET clears all session resources.

Table 83: SET Timer Values

Timer	Default value (sec.)	Description	Actions on expiration
ST1	Proxy: 10 Non-proxy: 50+ (optionally) response time in QoP	For proxy mode: from sending of SUPL RESPONSE to receipt of SUPL POS INIT.	For proxy: Send SUPL END to SET Clear session resources at SLP

Timer	Default value (sec.)	Description	Actions on expiration
		For non-proxy mode: from sending of SUPL RESPONSE to receipt of the notification (internal communication between SPC and SLC) that SUPL END has been sent to the SET.	For non-proxy: Internal communication is used to send SUPL END to SET Clear session resources at SLC/SLP
ST2	Proxy: 10 Non-proxy: 50+ (optionally) response time in QoP **NOTE**: When user verification is required using "allow on no answer" or "deny on no answer", the H-SLP should allow at least 40 seconds for the SET to prompt the user and determine that no answer has been made.	For proxy mode: from sending of SUPL INIT to receipt of SUPL POS INIT, SUPL TRIGGERED START or SUPL END. For non-proxy mode: from sending SUPL INIT to (a) receipt of notification (internal communication between SPC and SLC) that SUPL POS INIT has been received, (b) receipt of RLP-SSRP(SUPL END) from V-SLP, (c) receipt of SUPL TRIGGERED START, (d) receipt of SUPL REPORT or (e) receipt of SUPL END.	For non-roaming scenario: Inform SUPL agent that the session has ended. For roaming scenario: Inform SUPL agent or, where applicable, R-SLP that the session has ended. For proxy: Clear session resources at SLP For non-proxy: Clear session resources at SLC and send internal communication to SPC to clear session resources at SPC where applicable.
ST3	10	From sending of RLP-SSRLIR(SUPL START) to receipt of RLP-SSRLIA(SUPL RESPONSE)	For network initiated scenario: Send RLP-SRLIA to R-SLP Clear session resources at SLP For SET initiated scenario: Send SUPL END to SET Clear session resources at SLP
ST4	10	From sending of RLP-SSRLIR(msid, lid) to receipt of RLP-SSRLIA(msid, posresult)	For network initiated scenario: Send SUPL END to SET Send RLP-SRLIA to R-SLP Clear session resources at SLP For SET initiated scenario: Send SUPL END to SET Clear session resources at SLP
ST5	10 **NOTE**: When user verification is required using "allow on no answer" or "deny on no answer", the H-SLP should allow at least 40 seconds for the SET to prompt the user and determine that no answer has been made.	From sending SUPL NOTIFY to receipt of SUPL NOTIFY RESPONSE.	Send SUPL END to SET. Clear session resources at SLP.
ST6	10	Only applicable to "session-info query" sessions. From sending SUPL INIT to receipt of SUPL REPORT for Session Info Query session OR from sending SUPL TRIGGERED STOP to receipt of SUPL END for stopped triggered session.	Clear session resources at SLP.

Table 84: SLP Timer Values

Timer	Default value (sec.)	Description	Actions on expiration
PT1	11+ (optionally) response time in QoP	Only applicable to non-proxy. From receiving the initial initialization message (internal communication between SLC and SPC) to receipt of the SUPL POS INIT.	Send timer expiration notification to the SLC on internal interface. Clear session resources at SPC.

Table 85: SPC Timer Values

Timer	Default value (sec.)	Description	Actions on expiration
RT1	21+ (optionally) response time in QoP	From sending of RLP SRLIR (msid, client-id, QoP) to receipt of RLP SSRLIA(posresult).	Send MLP SLIA (posresult) to the SUPL Agent.

Table 86: RLP Timer Values

Appendix E. State Transition Models for SUPL 2.0 Security (Informative)

This appendix provides some examples that may help clarify use of the security mechanisms used in SUPL 2.0.

These models consider a single pair of H-SLP and SET.

- A SET may support an H-SLP for each bearer subscription. Since a SET may support multiple bearer subscriptions, the SET must also support multiple H-SLP. The models associated with the SET (that is, those models described in section E.2) need to be repeated for each subscribed SET.
- Note that the H-SLP supports many SETS, so the models associated with the H-SLP (that is, those models described in section E.3) need to be repeated for each subscribed SET.

E.1 Introduction to the Models

For each entity (the H-SLP ands SET) are three models:

- Security Negotiation Model (See section E.2.1): This describes the entity's perspective of how negotiating (a) the method for authenticating the other entity in the TLS Handshake and (b) the level of SUPL INIT protection to be applied. This is a decision tree diagram in which decisions invoke triggers that may cause state transitions in the TLS Authentication Model and/or the SUPL INIT Protection Model. There is a generic version of this decision tree does not make a priori assumptions about whether PSK-based authentication is supported by the entity or whether TLS session resumption (Abbreviated TLS handshake) is allowed by the entity. Then there are four additional versions that apply when the entity always knows a priori whether PSK-based authentication and/or TLS Sessions resumption is supported.
- TLS Authentication Model (section E.2.2): This state transitions model describes the entity's perspective of whether the other entity is authenticated or otherwise. There are two versions: a generic version; and a version that applies when TLS Session Resumption is not supported (the generic version applies when TLS Session Resumption is supported).
- SUPL INIT Protection Level Model (section E.2.3): This state transitions model describes the entity's perspective of the SUPL INIT Protection Level. If the entity does not support a PSK-based authentication method, then this model does not apply since only NULL SUPL INIT Protection level applies in such cases.

There are two types of models used: a decision tree model, used for the Security Negotiation Model; and a state transition model, used for the SUPL INIT Protection Level model and the TLS Authentication Model.

E.1.1 Security Negotiation Models

The Security Negotiation Models follows a series of steps, beginning at a START step and ending at END. Aside from START and END, the intermediate steps are classified as follows.

- Decisions: requiring a Yes/NO decision. The next step is determined by the outcome of the decision. In figures, these steps are shown in hexagons.
- Procedures: self-explanatory. Following a procedure, there is only one possible next step. In figures, these steps are indicated using rectangles.
- Triggers: these triggers are sent to the other security models: the SUP INIT Protection Level model and the TLS Authentication Model. In the figures, these steps are indicated using circles.

Each step is given an identifier consisting of a classifier (D=Decision, P=Procedure, T=Trigger), a number, and in some cases an final A, B or C. The meaning of the final A, B or C corresponds to the method applied during the TLS handshake, as described in the following paragraphs.

There are three different methods that may be applied during the TLS handshake:

- The handshake may use the ACA-based authentication method, based on Server certificates.
- The handshake may use the PSK-based authentication method, based on GBA or a similar procedure for establishing a shared key in the SET and H-SLP.

- An abbreviated TLS handshake may be used: this handshake use secrets established during a previous TLS Session (this is also called resuming a TLS Sessions)

There are some steps that are identical for each authentication method, but where the following step(s) depend on the particular method used. In these cases, a single number is assigned for these steps, and an A, B or C follows the number to indicate which method the step applies to

- A: denotes the ACA-based authentication method.
- B: denotes the PSK-based authentication method
- C: denotes the Abbreviated TLS handshake.

The steps of the specific versions (when the entity always knows a priori whether PSK-based authentication and/or TLS Sessions resumption is supported) use the same identifiers as the generic model.

E.1.2 Models for SUPL INIT Protection Level and TLS Authentication

These are state transition models, in which the model begins at a START step and transitions to a new state based on external triggers (in this case sent from the Security Negotiation Model) or internal triggers (such as deletion of the only remaining B-TID and PSK). These models only show when triggers cause a state transition.

E.2 Models for the SET

In these models, it is assumed that

- If a PSK-based method is supported, then the SET may maintain a list of valid B-TID and corresponding keys: this list is called the *valid set*.
- If TLS Session resumption (that is, the Abbreviated TLS Handshake) is supported and allowed by the SET, then the SET may store the TLS Session ID associated with the last TLS session successfully established with the H-SLP.
    - If a PSK-based method is negotiated by the SET and H-SLP, then there is little computational advantage to resuming the TLS sessions: resuming such TLS sessions is not recommended.

E.2.1 Security Negotiation Model

This is a decision tree diagram in which decisions invoke triggers that may cause state transitions in the TLS Authentication Model and/or the SUPL INIT Protection Model. There is a generic version of this decision tree that is applicable for all SETs. This version does not make a priori assumptions about whether PSK-based authentication is supported by the SET or whether TLS session resumption (Abbreviated TLS handshake) is supported by the SET. Then there are four additional versions that apply to SETs for which the SET always knows a priori whether PSK-based authentication and/or TLS Sessions resumption is supported.

E.2.1.1 Generic Version

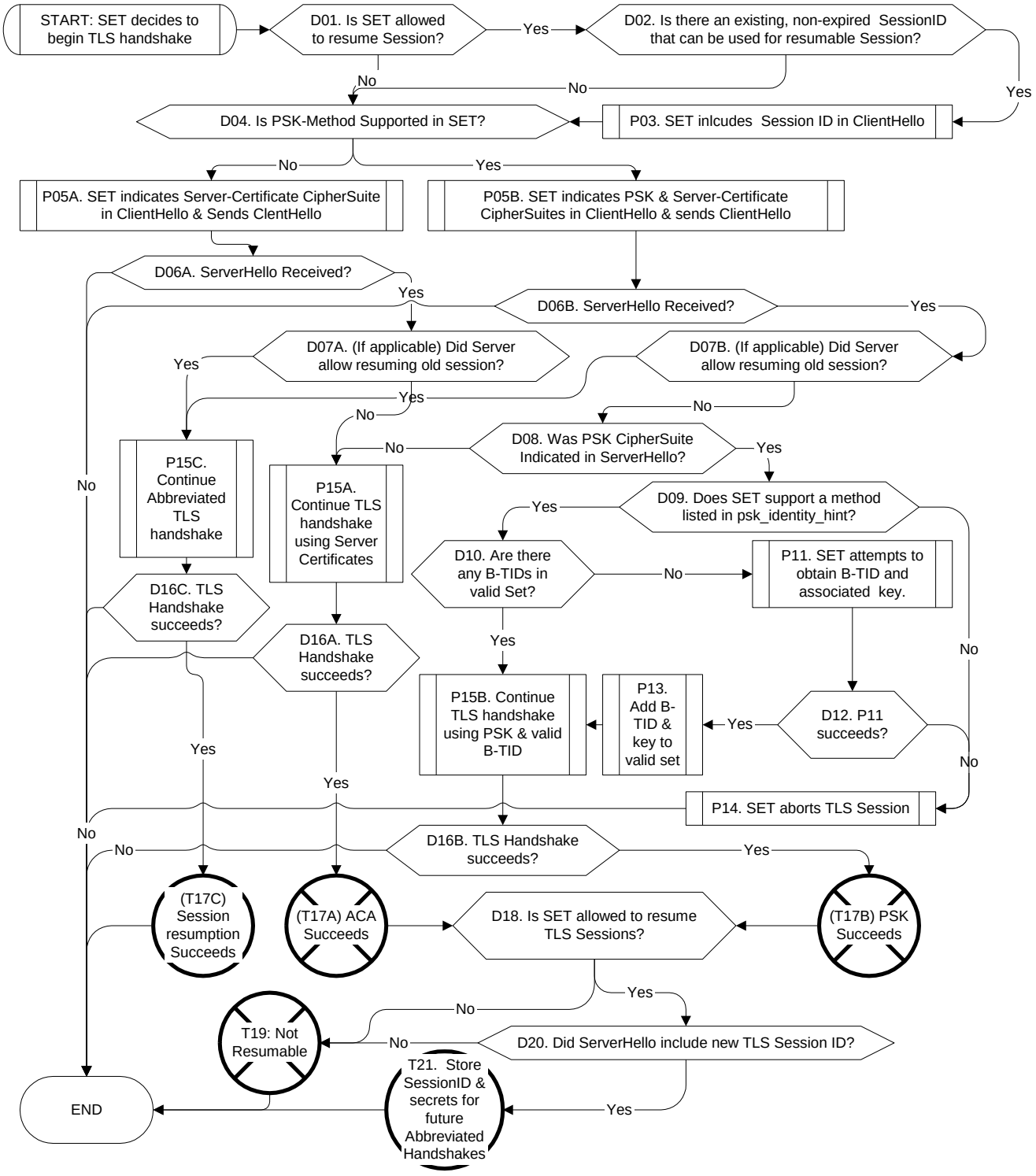

Figure 98: The generic version of the Security Negotiation Model for the SET.

Figure 98 shows the steps for the Security Negotiation Model for the SET. The details of the steps are provided in Table 87 through to Table 91.

Procedure, Decision or Trigger	Step	Description	Additional Notes	Transition after Procedures	Transition after Decision...	
					If Yes	If No
	START	-	-	D01		
Decision	D01	Is SET allowed to Resume a TLS Sessions?	SET needs to support resuming a session, AND also be permitted to do so	-	D02	D04
Decision	D02	Is there an existing, non-expired SessionID that can be used for resumable Session?	That is, is the SET in TLS Authentication State A3?	-	P03	D04
Procedure	P03	SET includes Session ID in ClientHello	-	D04	-	-
Decision	D04	Is PSK-Method Supported in SET?	-	-	P05B	P05A

Table 87: Steps START to D04 for the generic version of the Security Negotiation Model for a SET. These steps establish the capabilities of the SET.

Procedure, Decision or Trigger	Step	Description	Additional Notes	Transition after Procedures	Transition after Decision..	
					If Yes	If No
Procedure	P05A/B	SET indicates appropriate CipherSuites in ClientHello & Sends ClentHello	P05A: Use Server-Certificate CipherSuites	D06A	-	-
			P05B: Use PSK & Server Certificate CipherSuites	D06B	-	-
Decision	D06A/B	ServerHello Received?	D06A	-	D07A	END
			D06B	-	D07B	END
Decision	D07A/B	(If applicable) Did Server allow resuming old session?	D07A	-	P15C	P15A
			D07B	-	P15C	D08
Decision	D08	Was PSK CipherSuite Indicated in ServerHello?	Indicates if PSK or ACA method is to be used	-	D09	P15A

Table 88: Steps D05A/B to D08 for the generic version of the Security Negotiation Model for a SET. These steps establish what method will be used for this TLS Handshake (ACA-based Authentication, PSK-based Authentication or Session Resuming).

Procedure, Decision or Trigger	ID	Description	Additional Notes	Transition after Procedures	Transition after Decision..	
					If Yes	If No
Decision	D09	Does SET support a method listed in psk_identity_hint?	psk_identity_hint = “3GPP-bootstrapping” for GBA. psk-identity_hint = "SUPL	-	D10	P14

			WIMAX bootstrapping" for WiMAX. If the SET doesn't support either, then it should abort the TLS Session			
Decision	D10	Are there any B-TIDs in valid Set?	If not, bootstrapping is required	-	P15B	P11
Procedure	P11	SET attempts obtain B-TID and associated key.		D12	-	-
Decision	D12	P10 succeeds?	P10 may fail if bootstrapping server is down	-	P13	P14
Procedure	P13	Add B-TID & associated key to valid set	-	P15B	-	-
Procedure	P14	SET aborts TLS Session	SET needs to start a fresh TLS Sessions since it can't perform a PSK based TLS Session without keys	END	-	-

Table 89: Steps D09 to P14 for the generic version of the Security Negotiation Model for a SET. These steps apply only if the PSK-based Authentication will be used for this TLS Handshake. These steps determine which B-TID and associated keys will be used. Fresh B-TID and associated key are obtained if there are none already present on the SET.

Procedure, Decision or Trigger	ID	Description	Additional Notes	Transition after Procedures	Transition after Decision..	
					If Yes	If No
Procedure	P15	Continue TLS handshake	P15A: Using Server Cert's	D16A	-	-
			P15B: Using PSK & B-TID	D16B	-	-
			P15C: Using Abbrev. TLS Handshake	D16C	-	-
Decision	D16	TLS Handshake succeeds?	D15A	-	T17A	END
			D15B	-	T17B	END
			D15C	-	T17C	END
Trigger	T17	Trigger to the SUPL INIT Protection Level Model and TLS Authentication Model to indicate success of negotiation	T17A	D18	-	-
			T17B	D18	-	-
			T17C	END	-	-

Table 90: Steps P15A/B/C to T17A/B/C for the generic version of the Security Negotiation Model for a SET. There is a "version" of these steps for each used possible method used for this TLS Handshake (ACA-based Authentication, PSK-based Authentication or Session Resuming). Steps T17A/B/C send a trigger to the other Models.

Procedure, Decision or Trigger	ID	Description	Additional Notes	Transition after Procedures	Transition after Decision..	
					If Yes	If No

Decision	D18	Is SET allowed to resume TLS Sessions?	SET needs to support resuming a session, AND also be permitted to do so	-	T19	T20
Decision	D19	Did ServerHello include new TLS SessionID?	"Yes" indicates that a new Session has been established, and the new keys stored in H-SLP. The SET can resume this session in the future	-	T21	T20
Trigger	T20	TLS Session is not resumable		END	-	-
Trigger	T21	Store TLS Session ID & secrets for future Abbreviated Handshakes	Delete old Session ID and Secrets	END	-	-
	END	The relevant details from the negotiation have now been resolved	-	-	-	-

Table 91: Steps D18 to END for the generic version of the Security Negotiation Model for a SET. These are the final steps. These steps determine if the SET should save the TLS Session secrets and Session ID for resuming the TLS session in the future (the Abbreviated TLS Handshake can then be used in the next TLS Session).

E.2.1.2 PSK-based methods and TLS Session Resumption not supported

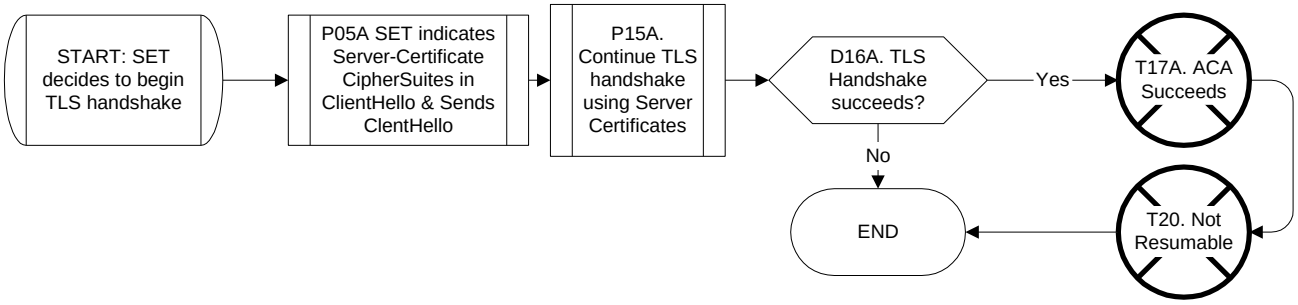

Figure 99: The Security Negotiation Model for a SET that does not support PSK-based methods and does not allow TLS Session Resumption.

Procedure, Decision or Trigger	Step	Description	Additional Notes	Transition after Procedures	Transition after Decision..	
					If Yes	If No
	START	-	-	D05A	-	-
Procedure	P05A	SET indicates appropriate CipherSuites in ClientHello & Sends ClentHello	P05A: Use Server-Certificate CipherSuites	P15A	-	-
Procedure	P15A	Continue TLS handshake	-	D16A	-	-
Decision	D16A	TLS Handshake succeeds?	-	-	T17A	END
Trigger	T17A	Trigger to the SUPL INIT Protection Level Model and TLS Authentication Model to indicate success of negotiation	-	T20	-	-
Trigger	T20	TLS Session is not resumable	-	END	-	-
	END	The relevant details from the negotiation have now been resolved	-	-	-	-

Table 92: Steps for the version of the Security Negotiation Model for a SET that does not support PSK-based methods and does not allow TLS Session Resumption.

E.2.1.3 PSK-based methods not supported, TLS Session Resumption Allowed

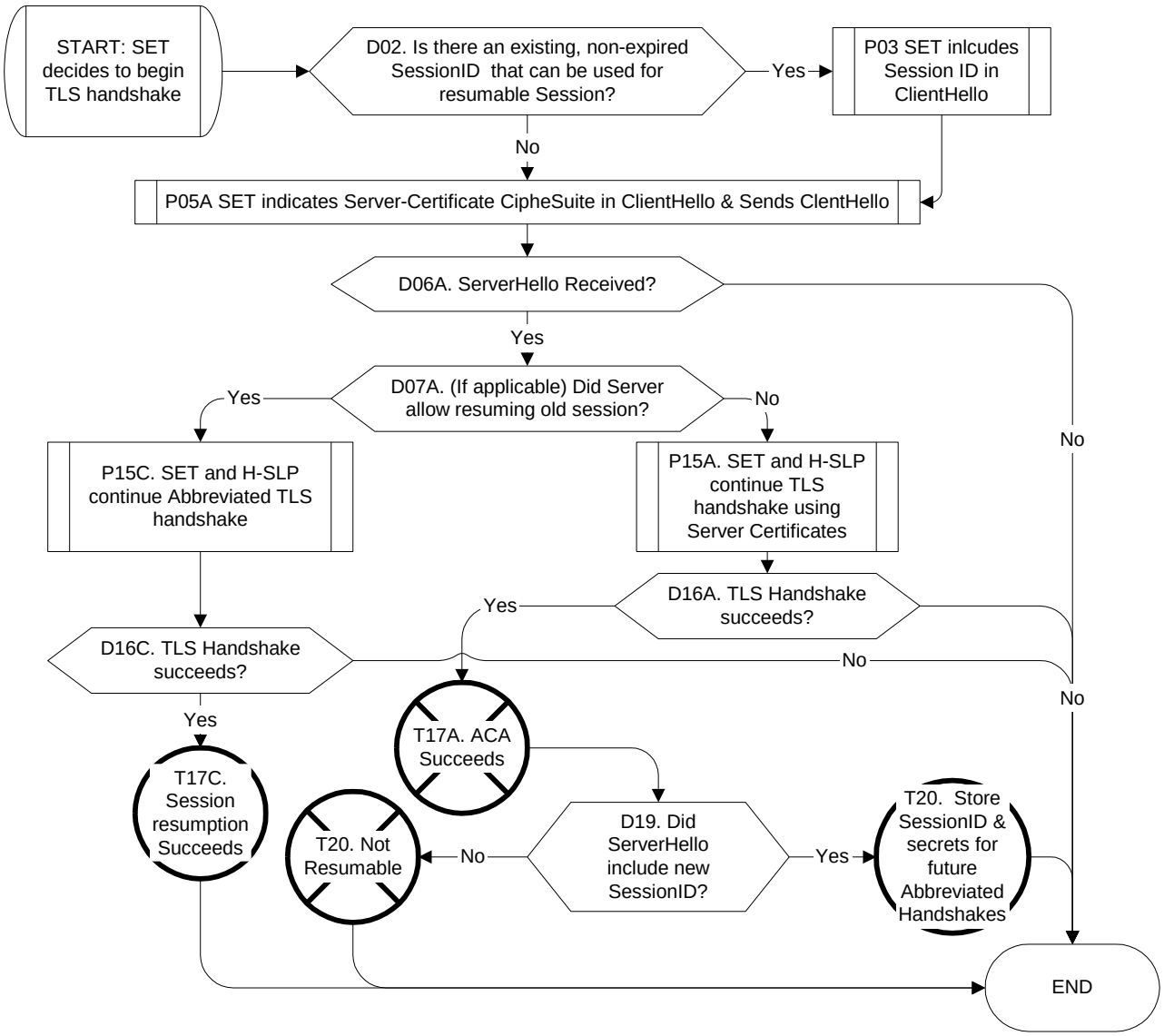

Figure 100: The Security Negotiation Model for a SET that does not support PSK-based methods and but does allow TLS Session Resumption.

Procedure, Decision or Trigger	Step	Description	Additional Notes	Transition after Procedures	Transition after Decision...	
					If Yes	If No
	START	-	-	D02		
Decision	D02	Is there an existing, non-expired SessionID that can be used for resumable Session?	That is, is the SET in TLS Authentication State A3?	-	P03	P05A
Procedure	P03	SET includes Session ID in ClientHello	-	P05A	-	-

Procedure	P05A	SET indicates appropriate CipherSuites in ClientHello & Sends ClentHello	P05A: Use Server-Certificate CipherSuites	D06A	-	-
Decision	D06A	ServerHello Received?		-	D07A	END
Decision	D07A	(If applicable) Did Server allow resuming old session?		-	P15C	P15A
Procedure	P15	Continue TLS handshake	P15A: Using Server Cert's	D16A	-	-
			P15C: Using Abbrev. TLS Handshake	D16C	-	-
Decision	D16	TLS Handshake succeeds?	D16A	-	T17A	END
			D16C	-	T17C	END
Trigger	T17	Trigger to the SUPL INIT Protection Level Model and TLS Authentication Model to indicate success of negotiation	T17A	D19	-	-
			T17C	END	-	-

Table 93: Steps START to T17A/B for the version of the Security Negotiation Model for a SET that does not support PSK-based methods and but does allow TLS Session Resumption. There is a "version" of these steps for each used possible method used for this TLS Handshake (ACA-based Authentication or Session Resuming).

Procedure, Decision or Trigger	Step	Description	Additional Notes	Transition after Procedures	Transition after Decision...	
					If Yes	If No
Decision	D19	Did ServerHello include new TLS SessionID?	"Yes" indicates that a new Session has been established, and the new keys stored in H-SLP. The SET can resume this session in the future	-	T20	END
Trigger	T20	TLS Session is not resumable	-	END	-	-
Trigger	T21	Store TLS Session ID & secrets for future Abbreviated Handshakes	Delete old Session ID and Secrets	END	-	-
	END	The relevant details from the negotiation have now been resolved	-	-	-	-

Table 94: Steps D19 to END for the version of the Security Negotiation Model for a SET that does not support PSK-based methods and but does allow TLS Session Resumption.

E.2.1.4 PSK-based method supported, TLS Session Resumption not supported

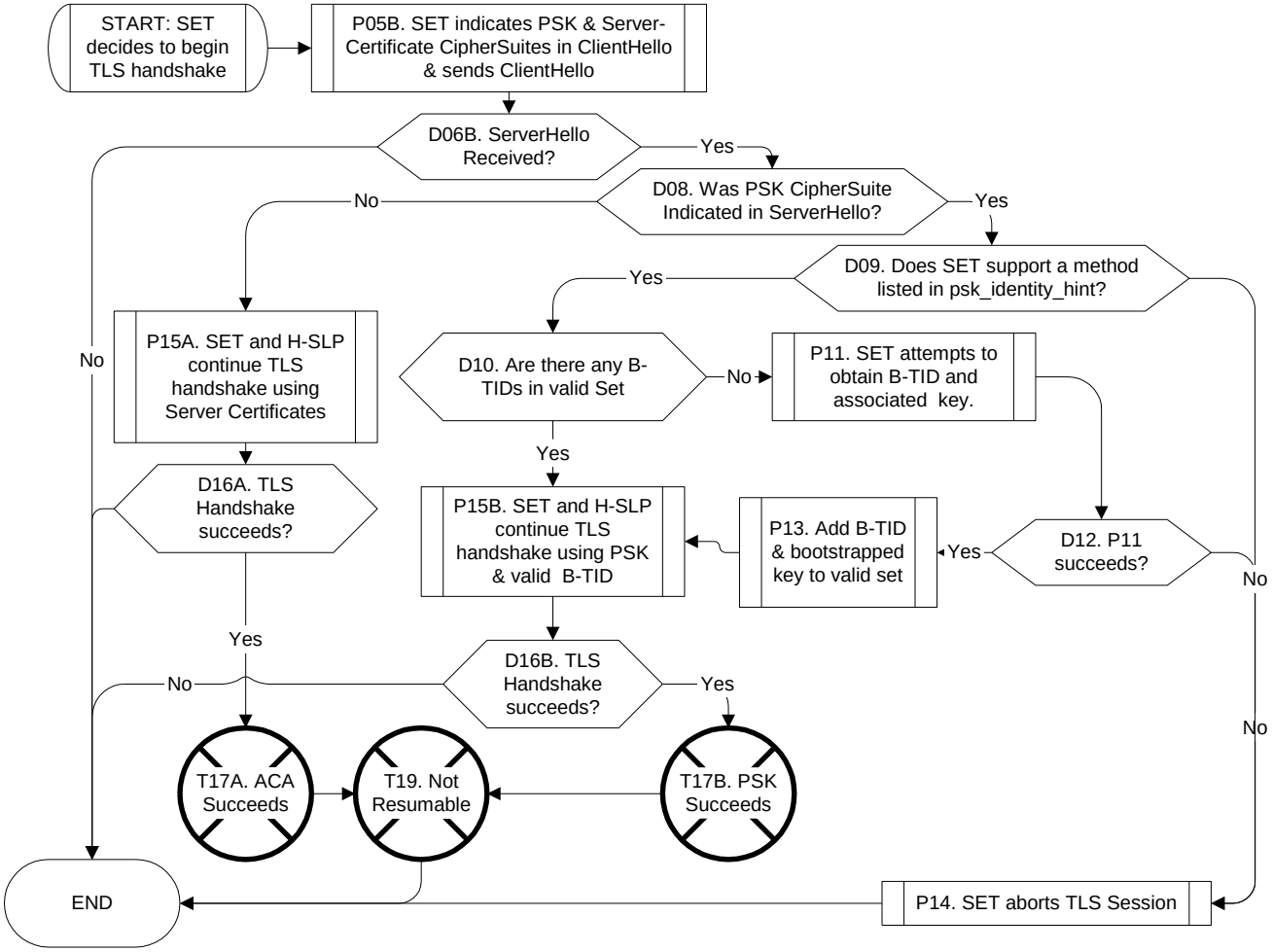

Figure 101: The Security Negotiation Model for a SET that supports PSK-based methods and but does not allow TLS Session Resumption.

Procedure, Decision or Trigger	Step	Description	Additional Notes	Transition after Procedures	Transition after Decision...	
					If Yes	If No
	START	-	-	P05B	-	-
Decision	D01	Is SET allowed to Resume a TLS Sessions?	SET needs to support resuming a session, AND also be permitted to do so	-	D02	D04
Procedure	P05A	SET indicates appropriate CipherSuites in ClientHello & Sends ClentHello	P05B: Use PSK & Server Certificate CipherSuites	D06B	-	-
Decision	D06A/B	ServerHello Received?	D06B	-	D07B	END

Decision	D08	Was PSK CipherSuite Indicated in ServerHello?	Indicates if PSK or ACA method is to be used	-	D09	P15A
Decision	D09	Does SET support a method listed in psk_identity_hint?	psk_identity_hint = “3GPP-bootstrapping” for GBA. psk-identity_hint = "SUPL WIMAX bootstrapping" for WiMAX. If the SET doesn’t support either, then it should abort the TLS Session	-	D10	P14
Decision	D10	Are there any B-TIDs in valid Set?	If not, bootstrapping is required	-	P15B	P11
Procedure	P11	SET attempts obtain B-TID and associated key.		D12	-	-
Decision	D12	P11 succeeds?	P11 may fail if bootstrapping server is down	-	P13	P14
Procedure	P13	Add B-TID & associated key to valid set	-	P15B	-	-
Procedure	P14	SET aborts TLS Session	SET needs to start a fresh TLS Sessions since it can’t perform a PSK based TLS Session without keys	END	-	-

Table 95: Steps START to P14 for the version of the Security Negotiation Model for a SET that supports PSK-based methods and but does not allow TLS Session Resumption.

Procedure, Decision or Trigger	Step	Description	Additional Notes	Transition after Procedures	Transition after Decision...	
					If Yes	If No
Procedure	P15A/B	Continue TLS handshake	P15A: Using Server Cert’s	D16A	-	-
			P15B: Using PSK & B-TID	D16B	-	-
Decision	D16A/B	TLS Handshake succeeds?	D16A	-	T17A	END
			D16B	-	T17B	END
Trigger	T17A/B	Trigger to the SUPL INIT Protection Level Model and TLS Authentication Model to indicate success of negotiation		T20	-	-
Trigger	T20	TLS Session is not resumable	-	END	-	-
	END	The relevant details from the negotiation have now been resolved	-	-	-	-

Table 96: Steps P15A/B to END for the version of the Security Negotiation Model for a SET that supports PSK-based methods and but does not allow TLS Session Resumption.

E.2.1.5 PSK-based method and TLS Session Resumption supported

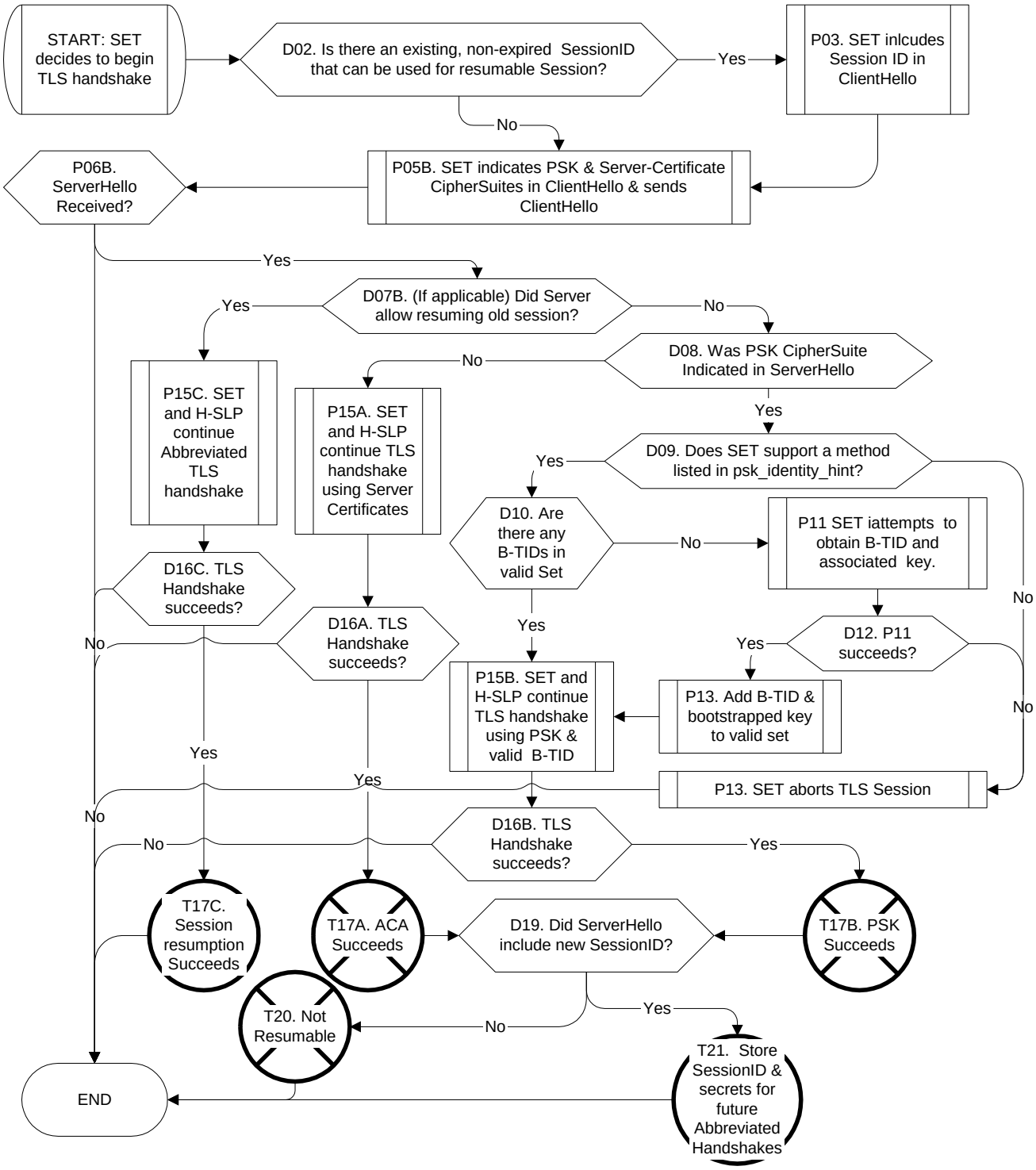

Figure 102: The Security Negotiation Model for a SET that supports PSK-based methods and allows TLS Session Resumption.

Procedure, Decision or Trigger	Step	Description	Additional Notes	Transition after Procedures	Transition after Decision...	
					If Yes	If No
	START	-	-	D02		
Decision	D02	Is there an existing, non-expired SessionID that can be used for resumable Session?	That is, is the SET in TLS Authentication State A3?	-	P03	P05B
Procedure	P03	SET includes Session ID in ClientHello	-	P05B	-	-
Procedure	P05B	SET indicates appropriate CipherSuites in ClientHello & Sends ClentHello	P05B: Use PSK & Server Certificate CipherSuites	D06B	-	-
Decision	D06A/B	ServerHello Received?	D06B	-	D07B	END
Decision	D07A/B	(If applicable) Did Server allow resuming old session?	D07B	-	P15C	D08
Decision	D08	Was PSK CipherSuite Indicated in ServerHello?	Indicates if PSK or ACA method is to be used	-	D09	P15A
Decision	D09	Does SET support a method listed in psk_identity_hint?	psk_identity_hint = “3GPP-bootstrapping” for GBA. psk-identity_hint = "SUPL WIMAX bootstrapping" for WiMAX. If the SET doesn’t support either, then it should abort the TLS Session	-	D10	P14
Decision	D10	Are there any B-TIDs in valid Set?	If not, bootstrapping is required	-	P15B	P11
Procedure	P11	SET attempts obtain B-TID and associated key.		D12	-	-
Decision	D12	P10 succeeds?	P10 may fail if bootstrapping server is down	-	P13	P14
Procedure	P13	Add B-TID & associated key to valid set	-	P15B	-	-
Procedure	P14	SET aborts TLS Session	SET needs to start a fresh TLS Sessions since it can’t perform a PSK based TLS Session without keys	END	-	-

Table 97: Steps from START to P13 for the version of the Security Negotiation Model for a SET that supports PSK-based methods and allows TLS Session Resumption.

Procedure, Decision or Trigger	ID	Description	Additional Notes	Transition after Procedures	Transition after Decision..	
					If Yes	If No

Procedure	P14	Continue TLS handshake	P14A: Using Server Cert's	D15A	-	-
			P14B: Using PSK & B-TID	D15B	-	-
			P14C: Using Abbrev. TLS Handshake	D15C	-	-
Decision	D15	TLS Handshake succeeds?	D15A	-	T16A	END
			D15B	-	T16B	END
			D15C	-	T16C	END
Trigger	T16	Trigger to the SUPL INIT Protection Level Model and TLS Authentication Model to indicate success of negotiation	T16A	D18	-	-
			T16B	D18	-	-
			T16C	END	-	-
Decision	D18	Did ServerHello include new TLS SessionID?	"Yes" indicates that a new Session has been established, and the new keys stored in H-SLP. The SET can resume this session in the future	-	T21	T20
Trigger	T20	TLS Session is not resumable	-	END	-	-
Trigger	T21	Store TLS Session ID & secrets for future Abbreviated Handshakes	Delete old Session ID and Secrets	END	-	-
	END	The relevant details from the negotiation have now been resolved	-	-	-	-

Table 98: Steps P14 to END for the version of the Security Negotiation Model for a SET that supports PSK-based methods and allows TLS Session Resumption.

E.2.2 SET TLS Authentication Model

E.2.2.1 Generic Version

E.2.2.1.1 List of States

State ID	Description	Can SET communicate securely with H-SLP?	Is there a resumable TLS Session?	Can Transition to
START				A1
A1	No Active Session. No Resumable Session exists	No	No	A2
A2	Active Session. Resumability not determined	Yes	Uncertain	A3,A5
A3	Active Session. Session is not Resumable	Yes	No	A1

A4	No active Session. Resumable Session exists	No	Yes	A1,A2,A5
A5	Active Session. Resumable Session exists	Yes	Yes	A3,A4

Table 99: List of the states in the generic TLS Authentication state transition model for SETs.

E.2.2.1.2 State Transitions

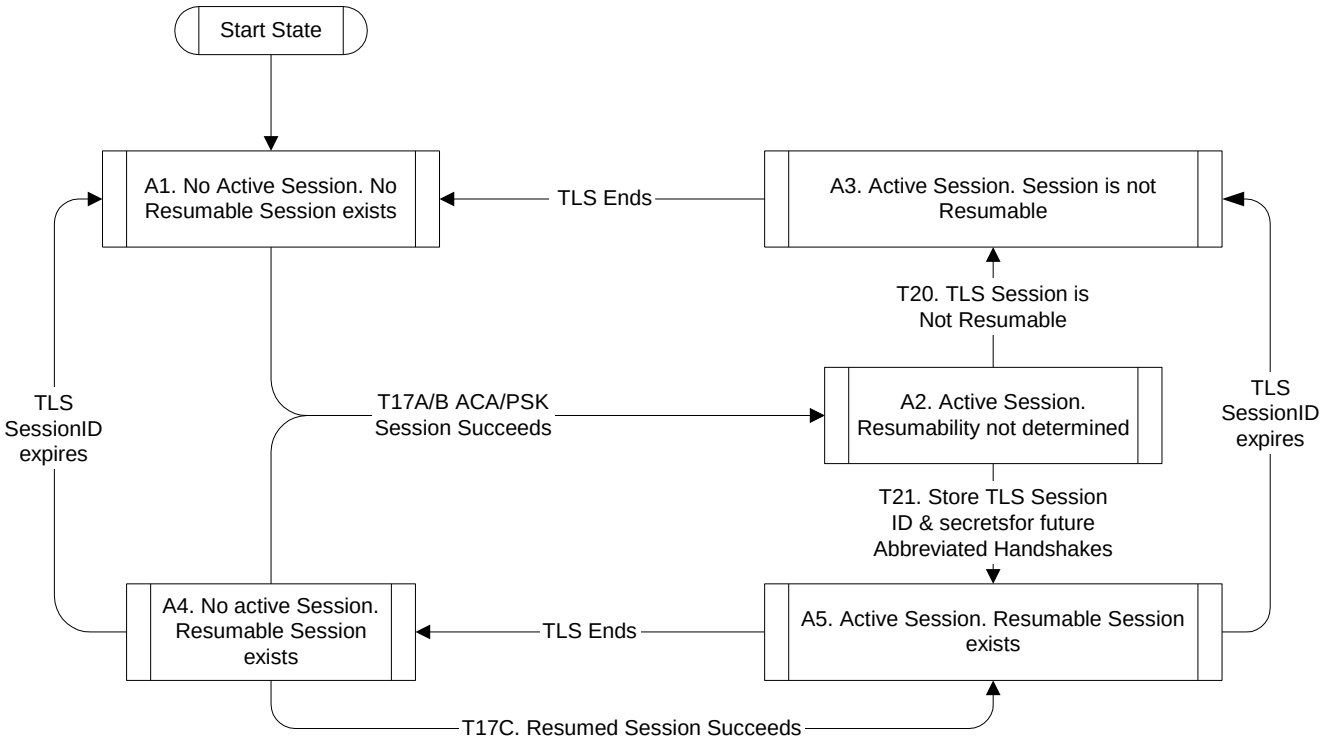

Figure 103: Generic Version of the TLS Authentication state transition model for the SET. Triggers T17A, T17B, T17C, T20 and T21 are sent from the Security Negotiation Model as described in section E.2.1.

Trigger Type	Trigger	Details	From	To
Internal	Automatic	After SET is subscribed.	START	A1
External	T17A/B	TLS Handshake succeeds using ACA-based or PSK-based methods. The SET and H-SLP can now exchange data securely using TLS	A1	A2
			A4	
External	T17C	Abbreviated TLS Handshake succeeds. The SET and H-SLP can now exchange data securely using TLS	A4	A5
External	T20	The TLS Session is not resumable.	A2	A3
External	T21	The SET stores the TLS Session ID and the secrets associated with the TLS Session so that they may be used in future abbreviated handshakes	A2	A5
Internal	TLS Ends	When the TLS Session ends, the SET and H-SLP can no longer exchange data securely.	A3	A1
			A5	A4

Internal	TLS Session ID expires	The SET can not use the Session ID and keys in future handshakes.	A4	A1
			A5	A3

Table 100: The state transitions in the generic TLS Authentication state transition model for SETs. Triggers T17A, T17B, T17C, T20 and T21 are sent from the Security Negotiation Model as described in section E.2.1

E.2.2.2 TLS Session Resumption not supported

NOTE: In the case where TLS Session Resumption is not supported, there is no need to wait for the trigger T20 that indicates that the session is not resumable.

E.2.2.2.1 List of States

State ID	Description	Can SET communicate securely with H-SLP?	Is there a resumable TLS Session?	Can Transition to
START				A1
A1	No Active Session. No Resumable Session exists	No	No	A2
A3	Active Session. Session is not Resumable	Yes	No	A1

Table 101: List of the states in the generic TLS Authentication state transition model for SETs where TLS Session Resumption is not supported.

E.2.2.2.2 State Transitions

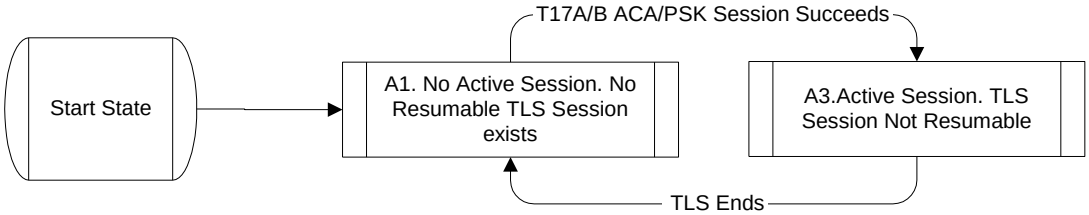

Figure 104: Version of the TLS Authentication state transition model for SETs where TLS Session Resumption is not supported. Triggers T17A, T17B are sent from the Security Negotiation Model as described in section E.2.1.

Trigger Type	Trigger	Details	From	To
Internal	Automatic	After SET powers up.	START	A1
External	T17A/B	TLS Handshake succeeds using ACA-based or PSK-based methods. The SET and H-SLP can now exchange data securely using TLS	A1	A3
Internal	TLS Ends	When the TLS Session ends, the SET and H-SLP can no longer exchange data securely.	A3	A1

Table 102: The state transitions in the TLS Authentication state transition model for SETs where TLS Session Resumption is not supported. Triggers T17A and T17B are sent from the Security Negotiation Model as described in section E.2.1

E.2.3 SUPL INIT Protection Model

NOTE: Trigger T17C does not cause a state transition in the SUPL INIT protection model.

Below is state transition diagram, from the view of the SET, for a given H-SLP's SUPL INIT Protection Level.

E.2.3.1.1 List of States

State ID	Description	Notes	Can Transition to
START			SI1
SI1	NULL SUPL INIT Protection	When in this state, the SET applies Null SUPL INIT Protection procedures to SUPL INIT messages received from this H-SLP.	SI2
SI2	Basic SUPL INIT Protection	When the in this state, the SET applies Basic SUPL INIT Protection procedures to SUPL INIT messages received from this H-SLP.	SI1

Table 103: List of the SUPL INIT Protection Level states.

E.2.3.1.2 State Transitions

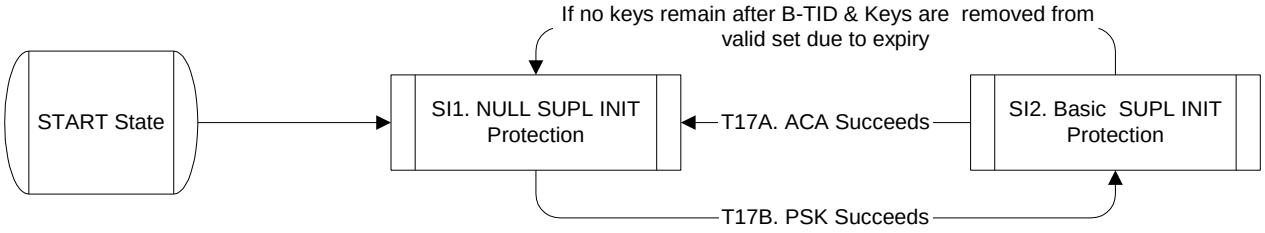

Figure 105: SUPL INIT Protection Level state transitions for the SET. Triggers T17A and T17B are sent from the Security Negotiation Model as described in section E.2.1.

Trigger Type	Trigger	Details	From	To
Internal	Automatic	After SET powers up.	START	SI1: NULL
External	T17B	TLS PSK Handshake succeeds. This implies that the keys for Basic SUPL INIT Protection have also been obtained by H-SLP, so Basic SUPL INIT Protection now applies	SI1:NULL	SI2: Basic
External	T17A	ACA-based TLS Handshake succeeds. The SET can no longer assume that the H-SLP has the keys for Basic SUPL INIT Protection	SI2: Basic	SI1: NULL
Internal	Valid Set is empty	When B-TID & Keys are removed from valid set due to expiry, it is possible that there are no more B-TID/Keys in the valid set. The SET can no longer perform Basic SUPL INIT protection	SI2: Basic	SI1: NULL

Table 104: The state transitions in the SUPL INIT Protection Level state transition model. Triggers T17A and T17B are sent from the Security Negotiation Model as described in section E.2.1

E.3 Models for the H-SLP

In these models, it is assumed that

- If a PSK-based method is supported, then the H-SLP may maintain a list of valid B-TID and corresponding keys associated with each user: this list is called the *valid set* for that user.
- If TLS Session resumption (that is, the Abbreviated TLS Handshake) is supported and allowed by the H-SLP, then the H-SLP may store the TLS Session ID associated with the last TLS session successfully established with the SET.

- If a PSK-based method is negotiated by the SET and H-SLP, then there is little computational advantage to resuming the TLS sessions: resuming such TLS sessions is not recommended.

E.3.1 Security Negotiation Model

E.3.1.1 Generic Version

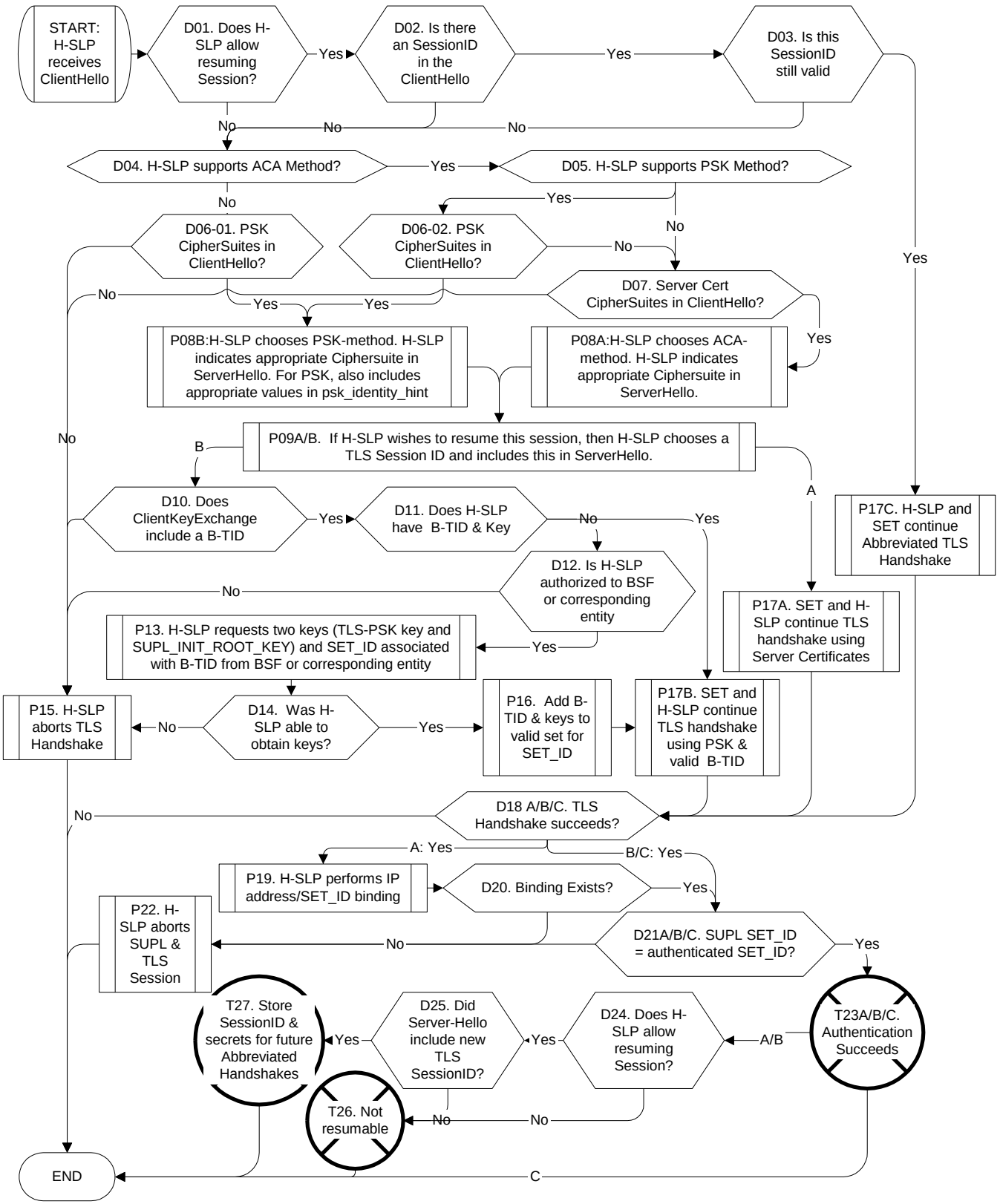

Figure 106: The generic version of the Security Negotiation Model for the H-SLP.

Procedure, Decision or Trigger	Step	Description	Additional Notes	Transition after Procedures	Transition after Decision...	
					If Yes	If No
	START	-	-	D01		
Decision	D01	Does H-SLP allow resuming a TLS Sessions?	H-SLP needs to support resuming a session, AND also be permitted to do so	-	D02	D04
Decision	D02	Is there a SessionID in the Client Hello?	That is, is the SET in TLS Authentication State A3?	-	D03	D04
Decision	D03	Is the SessionID still valid?	Can the TLS keys still be used?	-	P17C	D4
Decision	D04	Is ACA-Method Supported in H-SLP?	If No, then PSK method must be supported by H-SLP	-	D05	D06-1
Decision	D05	Is PSK-Method Supported in H-SLP?	-	-	D06-2	D07
Decision	D06-1/2	Are there PSK CipherSuites included in the ClientHello?	D06-1	-	P08B	P15
			D06-2	-	P08B	D07
Decision	D07	Are there Server Certificate CipherSuites included in the ClientHello?	If this is not indicated, then there is an error, and tehTLS session must be aborted	-	P08A	P15
Procedure	P08A/B	P08A: H-SLP chooses ACA method.	H-SLP indicates Server certificate Ciphersuites in ServerHello. Follow “A” options hereafter.	P09A	-	-
		P08A: H-SLP chooses PSK method.	H-SLP indicates PSK Ciphersuite in ServerHello and includes "3GPP-Bootstrapping" in psk_identity_hint (or WiMAX equivalent). Follow “B” options hereafter	P09B	-	-
Procedure	P09A/B	If H-SLP wishes to resume this session, then H-SLP chooses a TLS Session ID and includes this in ServerHello.	P09A	P17A	-	-
			P09B	D10	-	-

Table 105: Steps START to D09A/B for the generic version of the Security Negotiation Model for a H-SLP. These steps establish what method will be used for this TLS Handshake (ACA-based Authentication, PSK-based Authentication or Abbreviated Handshake).

	ID	Description	Additional Notes		Transition after Decision..

Procedure, Decision or Trigger				Transition after Procedures	If Yes	If No
Decision	D10	Does ClientKeyExchange include B-TID	If not, TLS handshake cannot proceed	-	D11	P15
Decision	D11	Does H-SLP have B-TID and corresponding Key and SET_ID	If not, must talk to BSF	-	P17B	D12
Decision	D12	Is H-SLP authorized to BSF or corresponding entity	If not, cannot obtain keys	-	P13	P15
Procedure	P13	H-SLP attempts obtain keys (TLS-PSK key and SUPL_INIT_ROOT_KEY) and SET_ID associated with B-TID from BSF or corresponding entity.		D14	-	-
Decision	D14	P13 succeeds?	P13 may fail if BSF or corresponding entity is down or if B-TID was false.	-	P16	P15
Procedure	P15	SET aborts TLS Session	SET needs to start a fresh TLS Sessions since it can't perform a PSK based TLS Session without keys	END	-	-
Procedure	P16	Add B-TID & associated key to valid set for SET_ID		P17B	-	-

Table 106: Steps D10 to P16 for the generic version of the Security Negotiation Model for a H-SLP. These steps apply only if the PSK-based Authentication will be used for this TLS Handshake. These steps determine which B-TID and associated keys will be used. Fresh B-TID and associated key are obtained if not already present on the H-SLP.

Procedure, Decision or Trigger	ID	Description	Additional Notes	Transition after Procedures	Transition after Decision..	
					If Yes	If No
Procedure	P17	Continue TLS handshake	P17A: Using Server Cert's	D18A	-	-
			P17B: Using PSK & B-TID	D18B	-	-
			P17C: Using Abbrev. TLS Handshake	D18C	-	-
Decision	D18	TLS Handshake succeeds?	D18A. The SET_ID is not yet authenticated	-	P19	END
			D18B. This provides authenticated SET_ID (associated with B-TID)	-	D21B	END
			D18C. This provides authenticated SET_ID (associated with original TLS session)	-	D21C	END

Table 107: Steps P17A/B/C and D18A/B/C for the generic version of the Security Negotiation Model for a H-SLP.

Procedure, Decision or Trigger	ID	Description	Additional Notes	Transition after Procedures	Transition after Decision..	
					If Yes	If No
Procedure	P19	H-SLP performs IP address/SET_ID binding		D20		
Decision	D20	Does Binding Exist?	This provides the authenticated SET_ID for ACA method	-	D21A	P22
Decision	D21	SET_ID provided in the SUPL message corresponds to authenticated SET_ID?	D21A	-	T23A	P22
			D21B	-	T23B	P22
			D21C	-	T23C	P22
Procedure	P22	H-SLP aborts SUPL and TLS Session	SET failed authentication.	END	-	-
Trigger	T23	Trigger to the SUPL INIT Protection Level Model and TLS Authentication Model to indicate success of negotiation	T23A	D24	-	-
			T23B	D22	-	-
			T23C	END	-	-

Table 108: Steps P19 to T23 for the generic version of the Security Negotiation Model for a H-SLP. Steps T23A/B/C send a trigger to the other Models.

Procedure, Decision or Trigger	ID	Description	Additional Notes	Transition after Procedures	Transition after Decision..	
					If Yes	If No
Decision	D24	Is H-SLP allowed to resume TLS Sessions?	Same decision as D01	-	D25	T27
Decision	D25	Did ServerHello include new TLS SessionID?	See Step P09A/B. "Yes" indicates that a new Session has been established, and the new keys should be stored in H-SLP.	-	T27	T26
Trigger	T26	TLS Session is not resumeable		END	-	-
Trigger	T27	Store TLS Session ID & secrets for future Abbreviated Handshakes	Delete old Session ID and Secrets	END	-	-
	END	The relevant details from the negotiation have now been resolved	-	-	-	-

Table 109: Steps D24 to END for the generic version of the Security Negotiation Model for a H-SLP. These are the final steps. These steps determine if the H-SLP should save the TLS Session secrets and Session ID for resuming the TLS session in the future (the Abbreviated TLS Handshake can then be used in the next TLS Session). See note below.

NOTE: The H-SLP should not save the TLS session secrets and Session ID unless the TLS handshake was successful. This is the reason that steps D24 to T27 cannot occur earlier in the process.

E.3.1.2 PSK-based methods and TLS Session Resumption not supported

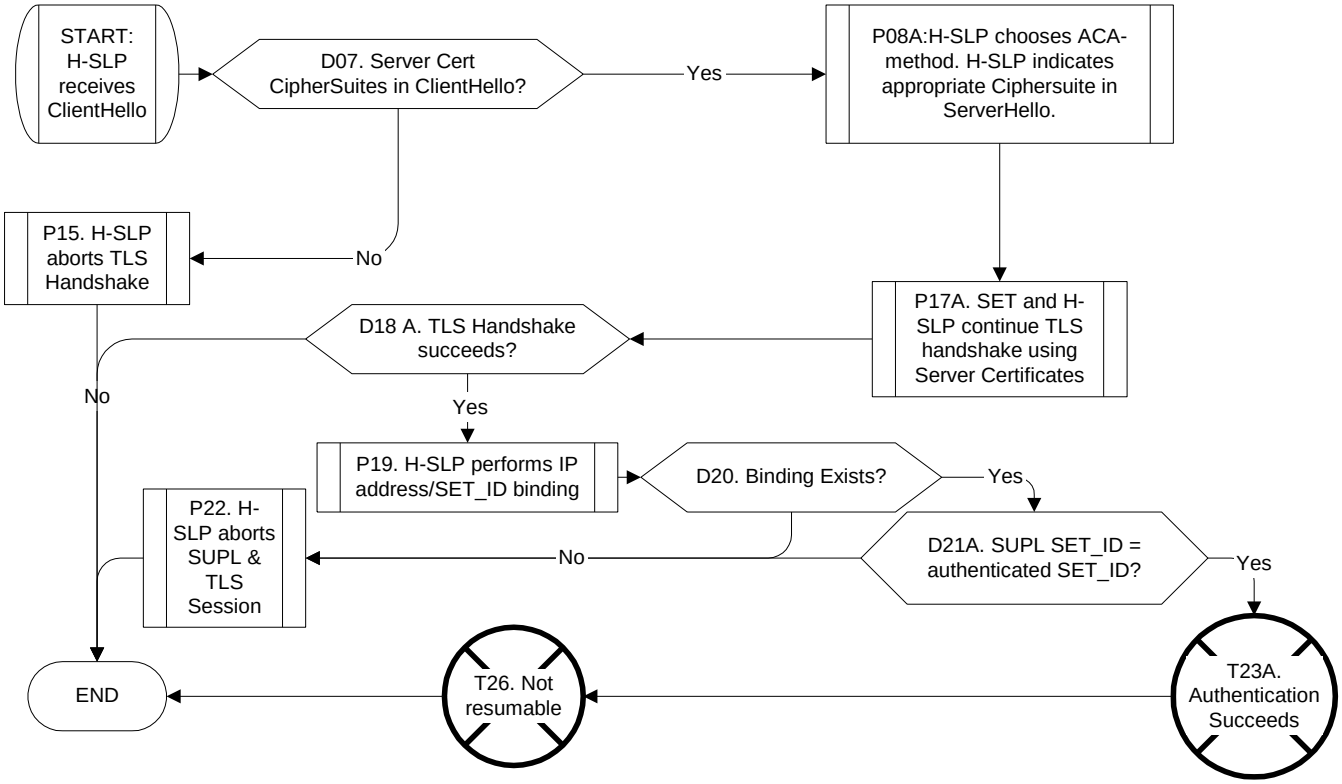

Figure 107: The Security Negotiation Model for an H-SLP that does not support PSK-based methods and does not allow TLS Session Resumption.

Procedure, Decision or Trigger	Step	Description	Additional Notes	Transition after Procedures	Transition after Decision...	
					If Yes	If No
	START	-	-	D07		
Decision	D07	Are there Server Certificate CipherSuites included in the ClientHello?	If this is not indicated, then there is an error, and tehTLS session must be aborted	-	P08A	P15
Procedure	P08A	P08A: H-SLP chooses ACA method.	H-SLP indicates Server certificate Ciphersuites in ServerHello. Follow “A” options hereafter.	P17A	-	-
Procedure	P15	SET aborts TLS Session	SET needs to start a fresh TLS Sessions since it can’t perform a PSK based TLS Session without keys	END	-	-

Procedure	P17A	Continue TLS handshake	P17A: Using Server Cert's	D18A	-	-
Decision	D18A	TLS Handshake succeeds?	D18A. The SET_ID is not yet authenticated	-	P19	END
Procedure	P19	H-SLP performs IP address/SET_ID binding		D18		
Decision	D20	Does Binding Exist?	This provides the authenticated SET_ID for ACA method	-	D21A	P22
Decision	D21A	SET_ID provided in the SUPL message corresponds to authenticated SET_ID?		-	T23A	P22
Procedure	P22	H-SLP aborts SUPL and TLS Session	SET failed authentication.	END	-	-
Trigger	T23A	Trigger to the SUPL INIT Protection Level Model and TLS Authentication Model to indicate success of negotiation		T26	-	-
Trigger	T26	TLS Session is not resumeable		END	-	-
	END	The relevant details from the negotiation have now been resolved	-	-	-	-

Table 110: Steps for the version of the Security Negotiation Model for a H-SLP does not support PSK-based methods and does not allow TLS Session Resumption.

E.3.1.3 PSK-based methods not supported, TLS Session Resumption supported

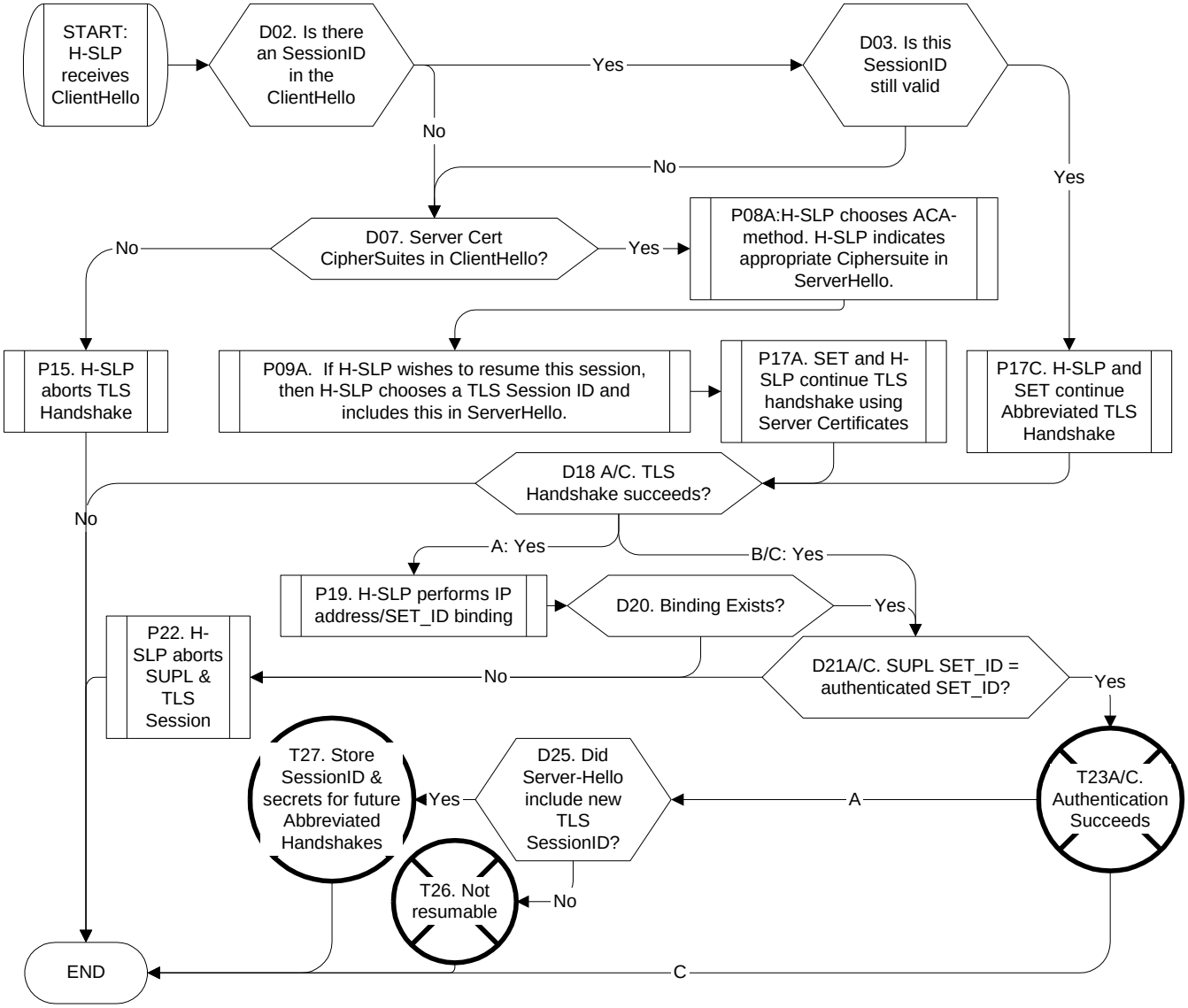

Figure 108: The Security Negotiation Model for an H-SLP that does not support PSK-based methods, but does allow TLS Session Resumption.

Procedure, Decision or Trigger	Step	Description	Additional Notes	Transition after Procedures	Transition after Decision...	
					If Yes	If No
	START	-	-	D02		
Decision	D02	Is there a SessionID in the Client Hello?	That is, is the SET in TLS Authentication State A3?	-	P03	D07
Decision	D03	Is the SessionID still valid?	Can the TLS keys still be used?	-	P17C	D07

Decision	D07	Are there Server Certificate CipherSuites included in the ClientHello?	If this is not indicated, then there is an error, and tehTLS session must be aborted	-	P08A	P15
Procedure	P08A/B	P08A: H-SLP chooses ACA method.	H-SLP indicates Server certificate Ciphersuites in ServerHello. Follow "A" options hereafter.	P09A	-	-
Procedure	P09A/B	If H-SLP wishes to resume this session, then H-SLP chooses a TLS Session ID and includes this in ServerHello.		P17A	-	-
Procedure	P15	SET aborts TLS Session	SET needs to start a fresh TLS Sessions since it can't perform a PSK based TLS Session without keys	END	-	-
Procedure	P17	Continue TLS handshake	P17A: Using Server Cert's	D18A	-	-
			P17C: Using Abbrev. TLS Handshake	D18C	-	-
Decision	D18	TLS Handshake succeeds?	D18A. The SET_ID is not yet authenticated	-	P19	END
			D18C. This provides authenticated SET_ID (associated with original TLS session)	-	D21C	END

Table 111: Steps START to D18 for the version of the Security Negotiation Model for a H-SLP does not support PSK-based methods, but allows TLS Session Resumption.

Procedure, Decision or Trigger	ID	Description	Additional Notes	Transition after Procedures	Transition after Decision..	
					If Yes	If No
Procedure	P19	H-SLP performs IP address/SET_ID binding		D20	-	-
Decision	D20	Does Binding Exist?	This provides the authenticated SET_ID for ACA method	-	D21A	P22
Decision	D21	SET_ID provided in the SUPL message corresponds to authenticated SET_ID?	D21A	-	T23A	P22
			D21C	-	T23C	P22
Procedure	P22	H-SLP aborts SUPL and TLS Session	SET failed authentication.	END	-	-
Trigger	T23	Trigger to the SUPL INIT Protection Level Model and TLS Authentication Model to indicate success of negotiation	T23A	D24	-	-
			T23C	END	-	-

Decision	D25	Did ServerHello include new TLS SessionID?	See Step P09A. "Yes" indicates that a new Session has been established, and the new keys should be stored in H-SLP.	-	T27	T26
Trigger	T26	TLS Session is not resumeable		END	-	-
Trigger	T27	Store TLS Session ID & secrets for future Abbreviated Handshakes	Delete old Session ID and Secrets	END	-	-
	END	The relevant details from the negotiation have now been resolved	-	-	-	-

Table 112: Steps P19 to END for the version of the Security Negotiation Model for a H-SLP does not support PSK-based methods, but allows TLS Session Resumption.

E.3.1.4 ACA-based method not supported, TLS Session Resumption not supported

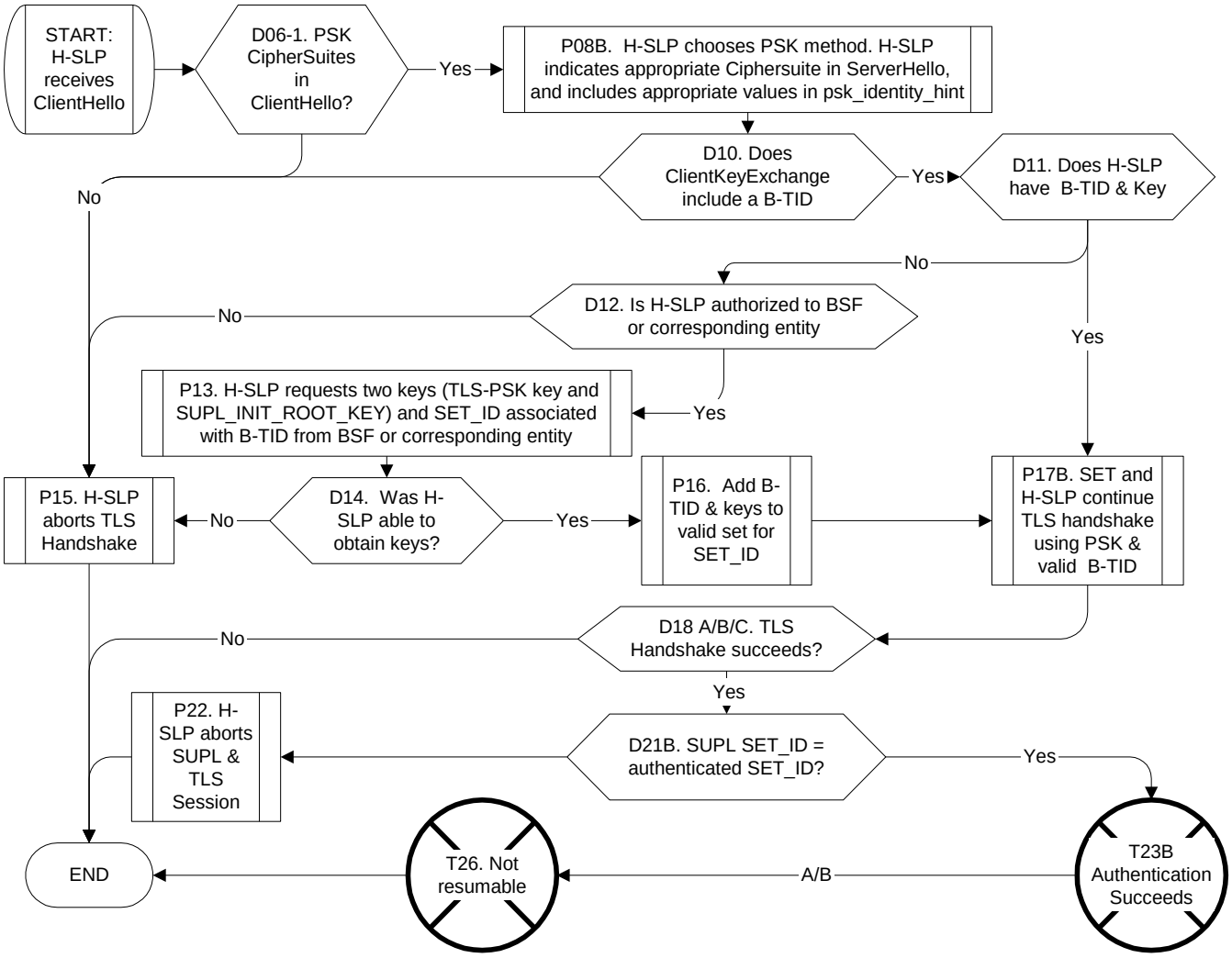

Figure 109: The Security Negotiation Model for an H-SLP that does not support ACA-based methods, and does not allow TLS Session Resumption.

Procedure, Decision or Trigger	Step	Description	Additional Notes	Transition after Procedures	Transition after Decision...	
					If Yes	If No
	START	-	-	D06-1		
Decision	D06-1	Are there PSK CipherSuites included in the ClientHello?		-	P08B	P15
Procedure	P08B	H-SLP chooses PSK method. H-SLP indicates PSK Ciphersuite in ServerHello and includes "3GPP-Bootstrapping" in psk_identity_hint (or WiMAX equivalent). Follow “B” options hereafter		D10	-	-
Decision	D10	Does ClientKeyExchange include B-TID	If not, TLS handshake cannot proceed	-	D11	P15
Decision	D11	Does H-SLP have B-TID and corresponding Key and SET_ID	If not, must talk to BSF	-	P17B	D12
Decision	D12	Is H-SLP authorized to BSF or corresponding entity	If not, cannot obtain key	-	P13	P15
Procedure	P13	H-SLP attempts obtain keys (TLS-PSK key and SUPL_INIT_ROOT_KEY) and SET_ID associated with B-TID from BSF or corresponding entity.		D14	-	-
Decision	D14	P13 succeeds?		-	P16	P15
Procedure	P15	SET aborts TLS Session	SET needs to start a fresh TLS Sessions since it can’t perform a PSK based TLS Session without keys	END	-	-
Procedure	P16	Add B-TID & associated key to valid set for SET_ID		P17B	-	-
Procedure	P17	Continue TLS handshake	P17B: Using PSK & B-TID	D18B	-	-
Decision	D18	TLS Handshake succeeds?	D18B. This provides authenticated SET_ID (associated with B-TID)	-	D21B	END
Decision	D21	SET_ID provided in the SUPL message corresponds to authenticated SET_ID?		-	T23B	P22
Procedure	P22	H-SLP aborts SUPL and TLS Session	SET failed authentication.	END	-	-
Trigger	T23	Trigger to the SUPL INIT Protection Level Model and TLS Authentication Model to indicate success of negotiation		D26	-	-
Trigger	T26	TLS Session is not resumeable		END	-	-
	END	The relevant details from the negotiation have now been resolved		-	-	-

Table 113: Steps for the version of the Security Negotiation Model for a H-SLP does not support ACA-based methods, and does not allow TLS Session Resumption.

E.3.1.5 ACA-based method not supported, TLS Session Resumption supported

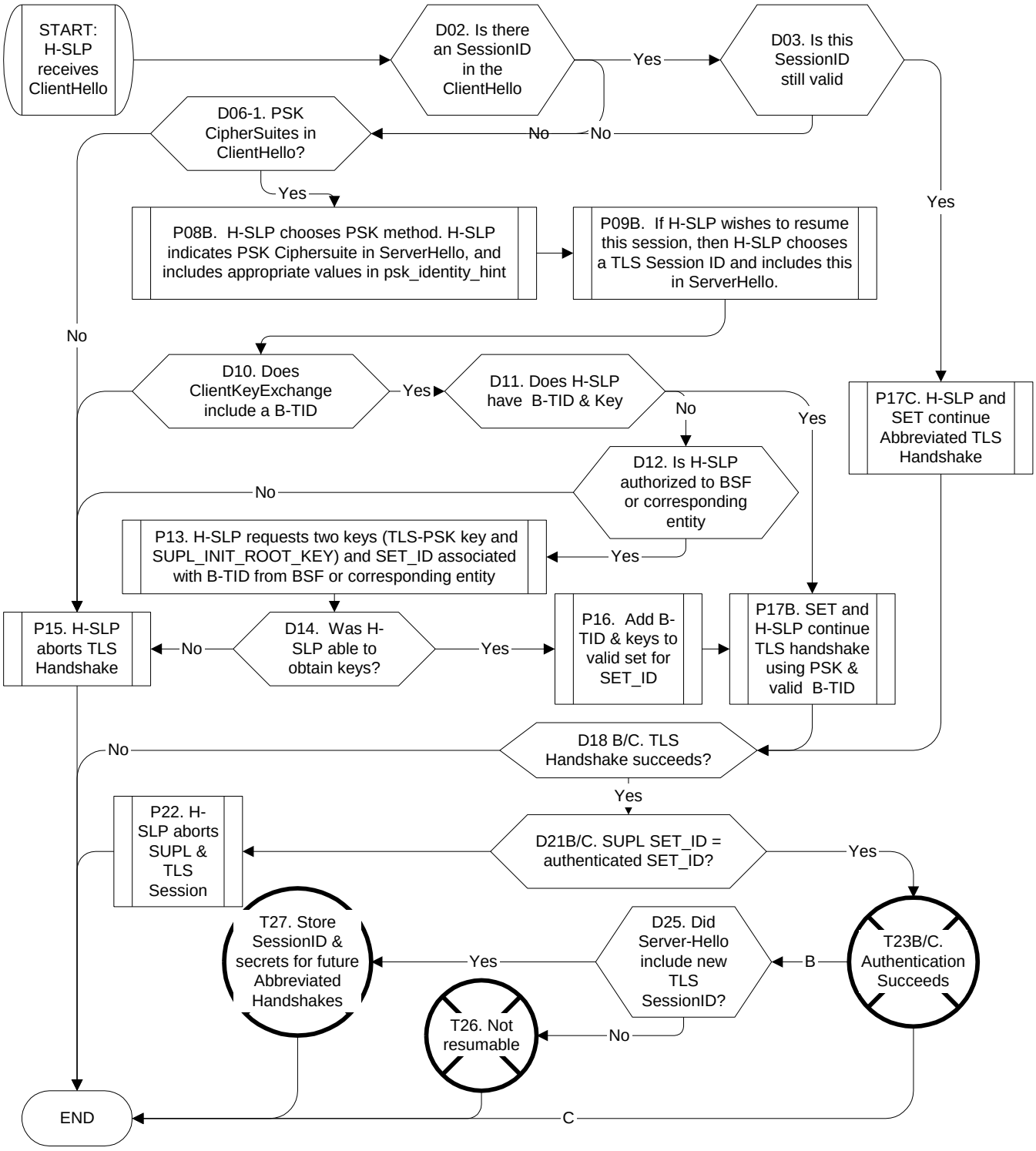

Figure 110: The Security Negotiation Model for an H-SLP that does not support ACA-based methods and allows TLS Session Resumption.

Procedure, Decision or Trigger	Step	Description	Additional Notes	Transition after Procedures	Transition after Decision...	
					If Yes	If No
	START	-	-	D02		
Decision	D02	Is there a SessionID in the Client Hello?	That is, is the SET in TLS Authentication State A3?	-	D03	D06-1
Decision	D03	Is the SessionID still valid?	Can the TLS keys still be used?	-	P17C	D06-1
Decision	D06-1/2	Are there PSK CipherSuites included in the ClientHello?		-	P08B	P15
Procedure	P08B	P08A: H-SLP chooses PSK method. H-SLP indicates PSK Ciphersuite in ServerHello and includes "3GPP-Bootstrapping" in psk_identity_hint (or WiMAX equivalent). Follow “B” options hereafter		P09B	-	-
Procedure	P09A/B	If H-SLP wishes to resume this session, then H-SLP chooses a TLS Session ID and includes this in ServerHello.		D10	-	-
Decision	D10	Does ClientKeyExchange include B-TID	If not, TLS handshake cannot proceed	-	D11	P15
Decision	D11	Does H-SLP have B-TID and corresponding Key and SET_ID	If not, must talk to BSF	-	P17B	D12
Decision	D12	Is H-SLP authorized to BSF or corresponding entity	If not, cannot obtain key	-	P13	P15
Procedure	P13	H-SLP attempts obtain keys (TLS-PSK key and SUPL_INIT_ROOT_KEY) and SET_ID associated with B-TID from BSF or corresponding entity.		D14	-	-
Decision	D14	P13 succeeds?	P13 may fail if BSF or corresponding entity is down or if B-TID was false.	-	P16	P15
Procedure	P15	SET aborts TLS Session	SET needs to start a fresh TLS Sessions since it can’t perform a PSK based TLS Session without keys	END	-	-
Procedure	P16	Add B-TID & associated key to valid set for SET_ID		P17B	-	-

Table 114: Steps START to P16 for the version of the Security Negotiation Model for a H-SLP where ACA-method is not supported and TLS session resumption is supported.

Procedure, Decision or Trigger	ID	Description	Additional Notes	Transition after Procedures	Transition after Decision..	
					If Yes	If No

Procedure	P17	Continue TLS handshake	P17B: Using PSK & B-TID	D18B	-	-
			P17C: Using Abbrev. TLS Handshake	D18C	-	-
Decision	D18	TLS Handshake succeeds? IN this case, SET_ID is authenticated	D18B.	-	D21B	END
			D18C.	-	D21C	END
Decision	D21	SET_ID provided in the SUPL message corresponds to authenticated SET_ID?	D21B	-	T23B	P22
			D21C	-	T23C	P22
Procedure	P22	H-SLP aborts SUPL and TLS Session	SET failed authentication.	END	-	-
Trigger	T23	Trigger to the SUPL INIT Protection Level Model and TLS Authentication Model to indicate success of negotiation	T23B	D25	-	-
			T23C	END	-	-
Decision	D25	Did ServerHello include new TLS SessionID?	See Step P09B. "Yes" indicates that a new Session has been established, and the new keys should be stored in H-SLP.	-	T26	T27
Trigger	T26	TLS Session is not resumeable		END	-	-
Trigger	T27	Store TLS Session ID & secrets for future Abbreviated Handshakes	Delete old Session ID and Secrets	END	-	-
	END	The relevant details from the negotiation have now been resolved	-	-	-	-

Table 115: Steps P17 to END for the version of the Security Negotiation Model for a H-SLP where ACA-method is not supported and TLS session resumption is supported.

E.3.1.6 ACA- and PSK-based method supported, TLS Session Resumption not supported

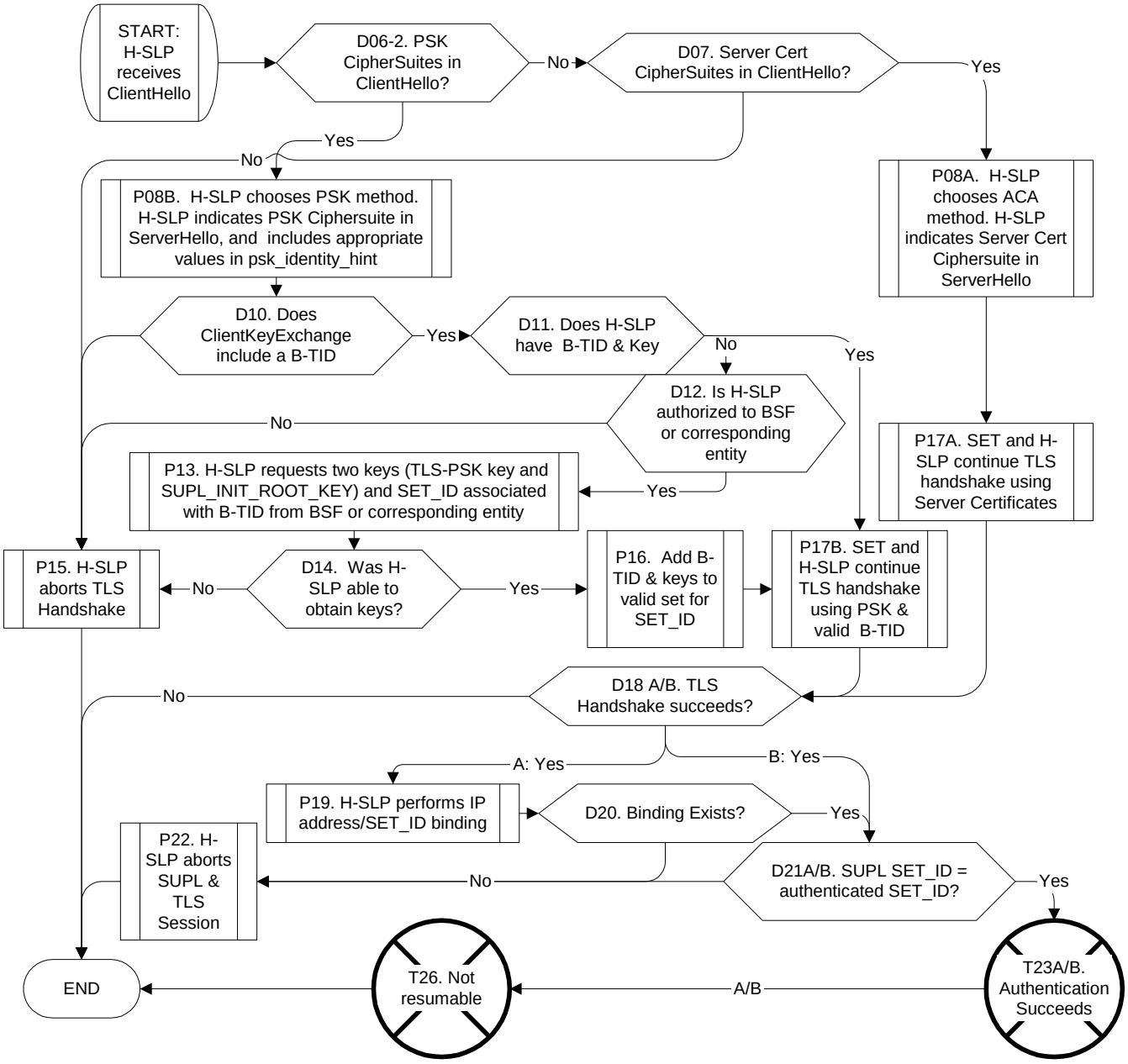

Figure 111: The Security Negotiation Model for an H-SLP that supports both ACA- and PSK-based methods, but does not allow TLS Session Resumption.

Procedure, Decision or Trigger	Step	Description	Additional Notes	Transition after Procedures	Transition after Decision...	
					If Yes	If No
	START	-	-	D06-2		
Decision	D06-2	Are there PSK CipherSuites included in the ClientHello?		-	P08B	D07

Decision	D07	Are there Server Certificate CipherSuites included in the ClientHello?	If this is not indicated, then there is an error, and tehTLS session must be aborted	-	P08A	P15
Procedure	P08A/B	P08A: H-SLP chooses ACA method.	H-SLP indicates Server certificate Ciphersuites in ServerHello. Follow "A" options hereafter.	P17A	-	-
		P08B: H-SLP chooses PSK method.	H-SLP indicates PSK Ciphersuite in ServerHello and includes "3GPP-Bootstrapping" in psk_identity_hint (or WiMAX equivalent). Follow "B" options hereafter	D10	-	-
Decision	D10	Does ClientKeyExchange include B-TID	If not, TLS handshake cannot proceed	-	D11	P15
Decision	D11	Does H-SLP have B-TID and corresponding Key and SET_ID	If not, must talk to BSF	-	P17B	D12
Decision	D12	Is H-SLP authorized to BSF or corresponding entity	If not, cannot obtain key	-	P13	P15
Procedure	P13	H-SLP attempts obtain keys (TLS-PSK key and SUPL_INIT_ROOT_KEY) and SET_ID associated with B-TID from BSF or corresponding entity.		D14	-	-
Decision	D14	P13 succeeds?	P13 may fail if BSF or corresponding entity is down or if B-TID was false.	-	P16	P15
Procedure	P15	SET aborts TLS Session	SET needs to start a fresh TLS Sessions since it can't perform a PSK based TLS Session without keys	END	-	-
Procedure	P16	Add B-TID & associated key to valid set for SET_ID		P17B	-	-

Table 116: Steps START to P16 for the version of the Security Negotiation Model for a H-SLP that supports the ACA-based method, the PSK-based method, but does not allow resuming TLS sessions.

Procedure, Decision or Trigger	ID	Description	Additional Notes	Transition after Procedures	Transition after Decision..	
					If Yes	If No
Procedure	P17	Continue TLS handshake	P17A: Using Server Cert's	D18A	-	-
			P17B: Using PSK & B-TID	D18B	-	-
Decision	D18	TLS Handshake succeeds?	D18A. The SET_ID is not yet authenticated	-	P19	END
				-	D21B	END

			D18B. This provides authenticated SET_ID (associated with B-TID)			
Procedure	P19	H-SLP performs IP address/SET_ID binding	-	D20	-	-
Decision	D20	Does Binding Exist?	This provides the authenticated SET_ID for ACA method	-	D21A	P22
Decision	D21	SET_ID provided in the SUPL message corresponds to authenticated SET_ID?	D21A	-	T23A	P22
			D21B	-	T23B	P22
Procedure	P22	H-SLP aborts SUPL and TLS Session	SET failed authentication.	END	-	-
Trigger	T23	Trigger to the SUPL INIT Protection Level Model and TLS Authentication Model to indicate success of negotiation	T23A	D26	-	-
			T23B	D26	-	-
Trigger	T26	TLS Session is not resumeable		END	-	-
	END	The relevant details from the negotiation have now been resolved	-	-	-	-

Table 117: Steps P17 to END for the version of the Security Negotiation Model for a H-SLP that supports the ACA-based method, the PSK-based method, but does not allow resuming TLS sessions.

E.3.1.7 ACA- and PSK-based method supported, TLS Session Resumption supported

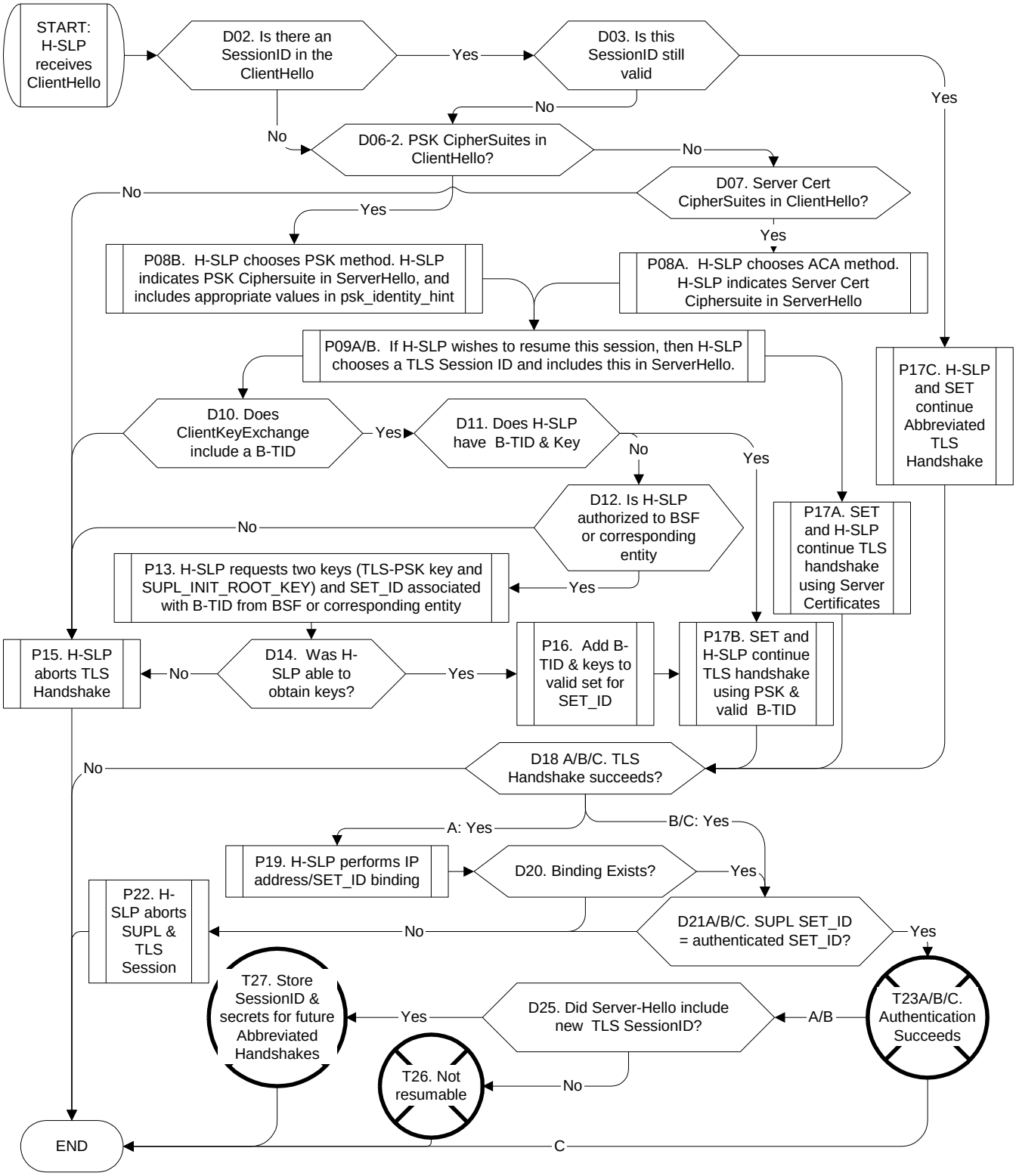

Figure 112: The Security Negotiation Model for an H-SLP that supports both ACA- and PSK-based methods and allows TLS Session Resumption.

Procedure, Decision or Trigger	Step	Description	Additional Notes	Transition after Procedures	Transition after Decision...	
					If Yes	If No
	START	-	-	D02		
Decision	D02	Is there a SessionID in the Client Hello?	That is, is the SET in TLS Authentication State A3?	-	D03	D06-2
Decision	D03	Is the SessionID still valid?	Can the TLS keys still be used?	-	P17C	D06-2
Decision	D06-2	Are there PSK CipherSuites included in the ClientHello?		-	P08B	D07
Decision	D07	Are there Server Certificate CipherSuites included in the ClientHello?	If this is not indicated, then there is an error, and tehTLS session must be aborted	-	P08A	P15
Procedure	P08A/B	P08A: H-SLP chooses ACA method.	H-SLP indicates Server certificate Ciphersuites in ServerHello. Follow “A” options hereafter.	P09A	-	-
		P08A: H-SLP chooses PSK method.	H-SLP indicates PSK Ciphersuite in ServerHello and includes "3GPP-Bootstrapping" in psk_identity_hint (or WiMAX equivalent). Follow “B” options hereafter	P09B	-	-
Procedure	P09A/B	If H-SLP wishes to resume this session, then H-SLP chooses a TLS Session ID and includes this in ServerHello.	P09A	P17A	-	-
			P09B	D10	-	-
Decision	D10	Does ClientKeyExchange include B-TID	If not, TLS handshake cannot proceed	-	D11	P15
Decision	D11	Does H-SLP have B-TID and corresponding Key and SET_ID	If not, must talk to BSF	-	P17B	D12
Decision	D12	Is H-SLP authorized to BSF or corresponding entity	If not, cannot obtain key	-	P13	P15
Procedure	P13	H-SLP attempts obtain keys (TLS-PSK key and SUPL_INIT_ROOT_KEY) and SET_ID associated with B-TID from BSF or corresponding entity.		D14	-	-
Decision	D14	P13 succeeds?	P13 may fail if BSF or corresponding entity is down or if B-TID was false.	-	P16	P15

Table 118: Steps START to D14 for version of the Security Negotiation Model for an H-SLP that supports the ACA-and method, the PSK-based method, and allows TLS session resumption.

Procedure, Decision or Trigger	Step	Description	Additional Notes	Transition after Procedures	Transition after Decision...	
					If Yes	If No
Procedure	P15	SET aborts TLS Session	SET needs to start a fresh TLS Sessions since it can't perform a PSK based TLS Session without keys	END	-	-
Procedure	P16	Add B-TID & associated key to valid set for SET_ID		P17B	-	-
Procedure	P17	Continue TLS handshake	P17A: Using Server Cert's	D18A	-	-
			P17B: Using PSK & B-TID	D18B	-	-
			P17C: Using Abbrev. TLS Handshake	D18C	-	-
Decision	D18	TLS Handshake succeeds?	D18A.	-	P19	END
			D18B.	-	D21B	END
			D18C.	-	D21C	END
Procedure	P19	H-SLP performs IP address/SET_ID binding		D20		
Decision	D20	Does Binding Exist?	This provides the authenticated SET_ID for ACA method	-	D21A	P22
Decision	D21	SET_ID provided in the SUPL message corresponds to authenticated SET_ID?	D21A	-	T23A	P22
			D21B	-	T23B	P22
			D21C	-	T23C	P22
Procedure	P22	H-SLP aborts SUPL and TLS Session	SET failed authentication.	END	-	-
Trigger	T23	Trigger to the SUPL INIT Protection Level Model and TLS Authentication Model to indicate success of negotiation	T23A	D25	-	-
			T23B	D25	-	-
			T23C	END	-	-
Decision	D25	Did ServerHello include new TLS SessionID?	See Step P09A/B. "Yes" indicates that a new Session has been established, and the new keys should be stored in H-SLP.	-	T26	T27
Trigger	T26	TLS Session is not resumeable		END	-	-
Trigger	T27	Store TLS Session ID & secrets for future Abbreviated Handshakes. Delete old Session ID and Secrets		END	-	-
	END	The relevant details from the negotiation have now been resolved		-	-	-

Table 119: Steps P19 to END for version of the Security Negotiation Model for an H-SLP that supports the ACA- and method, the PSK-based method, and allows TLS session resumption.

E.3.2 H-SLP TLS Authentication Model

E.3.2.1 General Model

E.3.2.1.1 List of States

State ID	Description	Can SET communicate securely with H-SLP?	Is there a resumable TLS Session?	Can Transition to
START				A1
A1	No Active Session. No Resumable Session exists	No	No	A2
A2	Active Session. Resumability not determined	Yes	Uncertain	A3,A5
A3	Active Session. Session is not Resumable	Yes	No	A1
A4	No active Session. Resumable Session exists	No	Yes	A1,A2,A5
A5	Active Session. Resumable Session exists	Yes	Yes	A3,A4

Table 120: List of the states in the generic TLS Authentication state transition model for SETs.

E.3.2.1.2 State Transitions

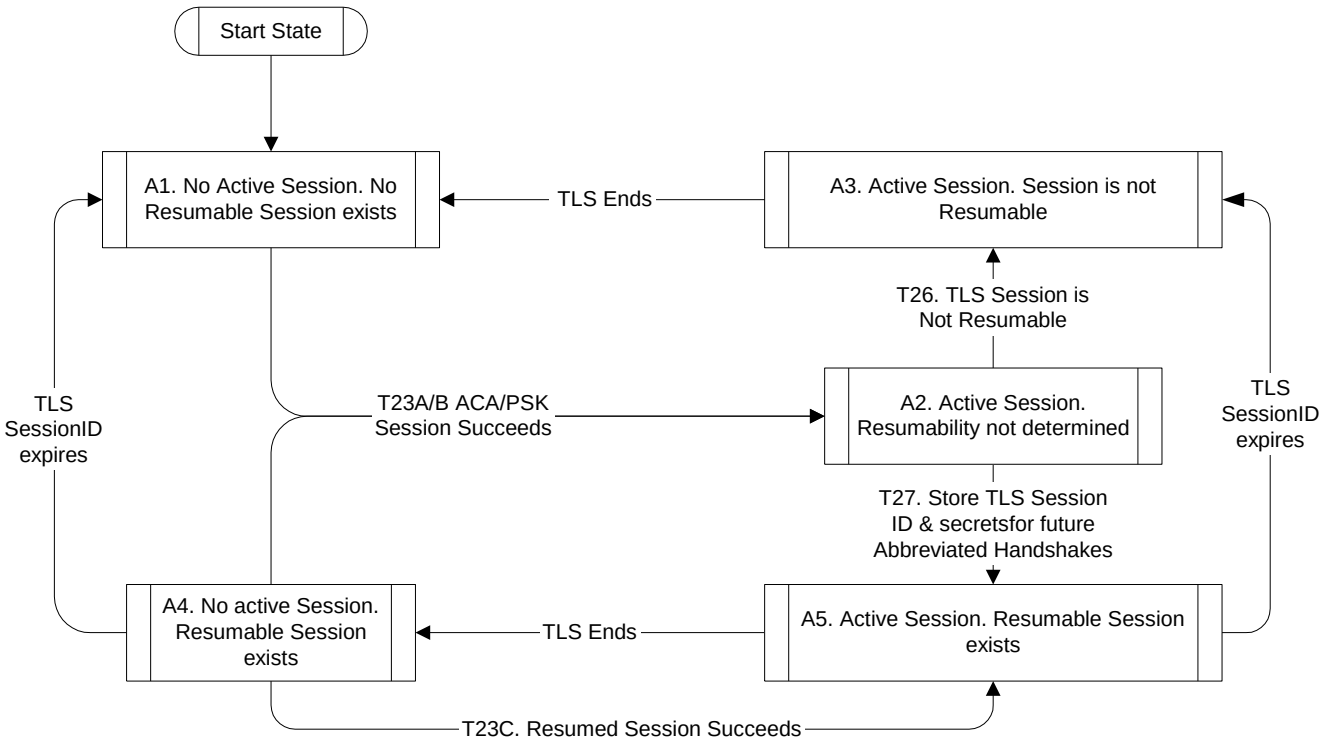

Figure 113: Generic Version of the TLS Authentication state transition model for the H-SLP. Triggers T20A, T20B, T20C, T24 and T25 are sent from the Security Negotiation Model as described in section E.3.1.

Trigger Type	Trigger	Details	From	To
Internal	Automatic	After SET is subscribed.	START	A1
External	T23A/B	TLS Handshake succeeds using ACA-based or PSK-based methods. The SET and H-SLP can now exchange data securely using TLS	A1	A2
			A4	
External	T23C	Abbreviated TLS Handshake succeeds. The SET and H-SLP can now exchange data securely using TLS	A4	A5
External	T26	The TLS Session is not resumable.	A2	A3
External	T27	The SET stores the TLS Session ID and the secrets associated with the TLS Session so that they may be used in future abbreviated handshakes	A2	A5
Internal	TLS Ends	When the TLS Session ends, the SET and H-SLP can no longer exchange data securely.	A3	A1
			A5	A4
Internal	TLS Session ID expires	The SET can not use the Session ID and keys in future handshakes.	A4	A1
			A5	A3

Table 121: The state transitions in the generic TLS Authentication state transition model for the H-SLP. Triggers T23A, T23B, T23C, T26 and T27 are sent from the Security Negotiation Model as described in section E.3.1.

E.3.2.2 TLS Session Resumption not supported

NOTE: In the case where TLS Session Resumption is not supported, there is no need to wait for the trigger T20 that indicates that the session is not resumable.

E.3.2.2.1 List of States

State ID	Description	Can SET communicate securely with H-SLP?	Is there a resumable TLS Session?	Can Transition to
START				A1
A1	No Active Session. No Resumable Session exists	No	No	A2
A3	Active Session. Session is not Resumable	Yes	No	A1

Table 122: List of the states in the generic TLS Authentication state transition model for H-SLPs where TLS Session Resumption is not supported.

E.3.2.2.2 State Transitions

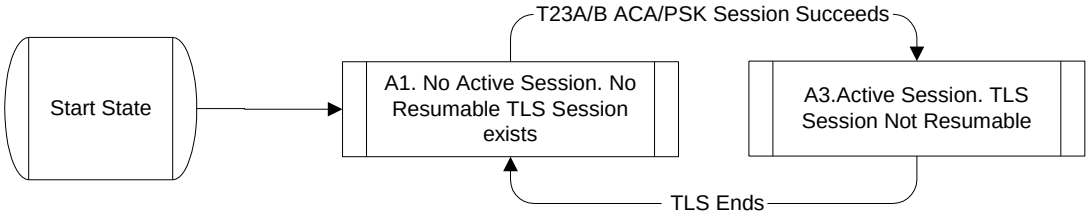

Figure 114: Version of the TLS Authentication state transition model for H-SLPs where TLS Session Resumption is not supported. Triggers T23A, T23B are sent from the Security Negotiation Model as described in section E.3.1.

Trigger Type	Trigger	Details	From	To
Internal	Automatic	After SET powers up.	START	A1
External	T23A/B	TLS Handshake succeeds using ACA-based or PSK-based methods. The SET and H-SLP can now exchange data securely using TLS	A1	A3
Internal	TLS Ends	When the TLS Session ends, the SET and H-SLP can no longer exchange data securely.	A3	A1

Table 123: The state transitions in the TLS Authentication state transition model for SETs where TLS Session Resumption is not supported. Triggers T23A and T23B are sent from the Security Negotiation Model as described in section E.3.1.

E.3.3 SUPL INIT Protection Model

E.3.3.1.1 State Transitions

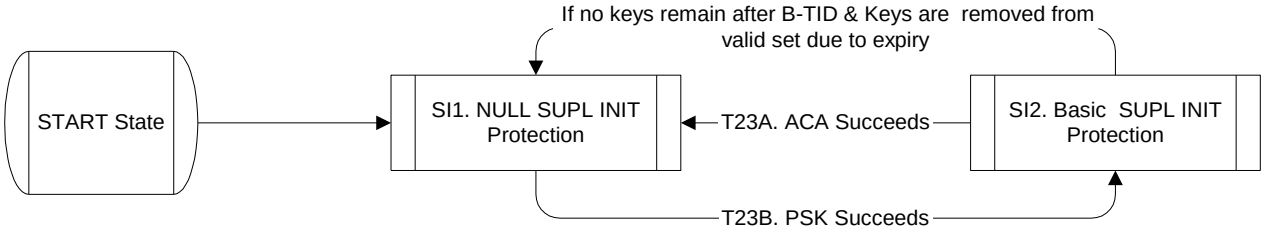

Figure 115: SUPL INIT Protection Level state transitions for the H-SLP. Triggers T23A and T23B are sent from the Security Negotiation Model as described in section E.3.1.

Trigger Type	Trigger	Details	From	To
Internal	Automatic	After SET powers up.	START	SI1: NULL
External	T23B	TLS PSK Handshake succeeds. This implies that the keys for Basic SUPL INIT Protection have also been obtained by SET, so Basic SUPL INIT Protection now applies	SI1:NULL	SI2: Basic
External	T23A	ACA-based TLS Handshake succeeds. The H-SLP can no longer assume that the SET has the keys for Basic SUPL INIT Protection	SI2: Basic	SI1: NULL

Internal	Valid Set is empty	When B-TID & Keys are removed from valid set due to expiry, it is possible that there are no more B-TID/Keys in the valid set. The H-SLP can no longer perform Basic SUPL INIT protection	SI2: Basic	SI1: NULL

Table 124: The state transitions in the SUPL INIT Protection Level state transition model for the H-SLP. Triggers T23A and T23B are sent from the Security Negotiation Model as described in section E.3.1.