Secure User Plane Location Architecture

Approved Version 1.0 – 15 Jun 2007

Open Mobile Alliance

OMA-AD-SUPL-V1_0-20070615-A

Contents

Figures

Tables

1. Scope (Informative)

The scope of the Secure User Plane Location (SUPL) architecture document is to define the architecture for the SUPL service enabler.

A reference architecture is defined including:

- Context model
- Functional blocks
- Logical entities
- Reference points / Interfaces
- Messages and message flows

In addition a number of deployment scenarios are considered including different roaming models as well as different mapping of logical functions to architectural elements.

This architecture is based on the requirements listed for the system in the SUPL Requirements document [SUPL RD].

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

[3GPP 33.978] 3GPP TR 33.978, "Security Aspects of Early IP Multimedia Subsystem (IMS) (Release 6).",
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)", V5.12.0 (2005-01)
URL: http://www.3gpp.org/

[3GPP2 C.S0022-0] 3GPP2 C.S0022-0 v3.0, Position Determination Service for cdma2000 Spread Spectrum Systems; April 2001
URL: http://www.3gpp2.org

[3GPP2 C.S0022-A] 3GPP2 C.S0022-A v1.0: "Position Determination Service Standard for Dual Mode Spread Spectrum Systems" March 2004
URL: http://www.3gpp2.org

[3GPP2 IP LCS Stage 1] 3GPP2 S.R0066-0, "IP Based Location Services Stage 1 Requirements", Version 1.0, 17 April 2003.
URL: http://www.3gpp2.org

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

[OMA MLP] OMA-TS-MLP, "Mobile Location Protocol"
URL: http://www.openmobilealliance.org/

[OMA MLS AD] OMA-AD-MLS-V1_0 "OMA Mobile Location Service Architecture",
URL: http://www.openmobilealliance.org/

[OMA MLS RD] OMA-RD-MLS-V1_0, "OMA Mobile Location Service Enabler Requirements",
URL: http://www.openmobilealliance.org/

[OMA RLP] OMA-TS-RLP-V1_0 "Inter-Location Server Interface Specification",
URL: http://www.openmobilealliance.org/

[OMA ULP] "UserPlane Location Protocol v1.0", Open Mobile Alliance™, OMA-TS-SUPL-V1_0,
URL: http://www.openmobilealliance.org/

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

[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

[RFC2119] "Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, March 1997,
URL: http://www.ietf.org/rfc/rfc2119.txt

[SHA-1] FIPS PUB 180-2 (2002): "Secure Hash Standard".
URL: http://csrc.nist.gov/

[SUPL RD] OMA-RD-SUPL-V1_0. Open Mobile Alliance™.
URL: http://www.openmobilealliance.org/

[TLS] "Transport Layer Security (TLS) Version 1.0", IETF RFC 2246, Jan 1999,
URL: http://www.ietf.org/rfc/rfc2246.txt

[TLS] "Transport Layer Security (TLS) Version 1.0"
URL: http://www.ietf.org/rfc/rfc2246.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",
URL: http://www.openmobilealliance.org/

[WAP PAP] "WAP Push Access Protocol", WAP-247-PAP, Open Mobile Alliance™
URL: http://www.openmobilealliance.org/

[WAP POTAP] "WAP Push Over The Air Protocol", WAP-235-PushOTA, Open Mobile Alliance™
URL: http://www.openmobilealliance.org/

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

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

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

2.2 Informative References

[3GPP GSM LCS] 3GPP TS 43.059, "Functional stage 2 description of Location Services (LCS) in GERAN", Release 6
URL: http://www.3gpp.org/

[3GPP TS 23.271] 3GPP TS 23.271: "Functional stage 2 description of Location Services (LCS)", Release 6.
URL: http://www.3gpp.org/

[3GPP WCDMA LCS] 3GPP TS 25.305, "Stage 2 functional specification of User Equipment (UE) positioning in UTRAN", Release 6
URL: http://www.3gpp.org/

[3GPP2 X.S0024-0] 3GPP2 X.S0024-0 v1.0, "IP-Based Location Services", to be published.
URL: http://www.3gpp2.org

[ARCH-PRINC] "OMA Architecture Principles V1.2", Open Mobile Alliance™, OMA-ArchitecturePrinciples-V1_2,
URL: http://www.openmobilealliance.org/

[ARCH-REVIEW] "OMA-ARCHReviewProcess", Open Mobile Alliance™, OMA-ARCHReviewProcess-V1_1,
URL: http://www.openmobilealliance.org/

[OMA AD] "Inventory of Architectures and Services", Open Mobile Alliance™, OMA-Inventory-of-Architectures-and-Services-V1_0,
URL: http://www.openmobilealliance.org/

[OMA-DICT] "Dictionary for OMA Specifications V2.1", Open Mobile Alliance™, OMA-Dictionary-V2_1,
URL: http://www.openmobilealliance.org/

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

[SUPL MO] "OMA SUPL Management Object", Open Mobile Alliance™, OMA-TS-SUPL-MO-V1_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 [RFC2119].

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

3.2 Definitions

Context Model	A model that identifies all contextual items relevant to understanding architecture.
Control Plane	This plane has a layered structure and performs the call control and connection control functions; it deals with the signalling necessary to set up, supervise and release calls and connections.
Deferred Location Service	Location service where the location information is required after a specific event has occurred. The event may or may not occur immediately
Immediate Location Service	Location service where a single location information is needed immediately
Interface	The common boundary between two associated systems. See [OMA-DICT]
MLS application	An application which requests and consumes the location information
MLS application and SUPL Agent classes	Class1: MLS application and SUPL Agent are in the SET Class 2: MLS application is in the network and the SUPL Agent is in the SET Class 3: MLS application is in the SET and SUPL Agent is in the network Class 4: MLS application and the SUPL Agent are in the network
Network Initiated SUPL Services	Network Initiated SUPL Services are services, which originate from within the SUPL network as opposed to the SET. For these services the SUPL Agent resides in the Network.
Non-Proxy Mode	The SPC system will have direct communication with the SET
Periodic Location Service	Location service where a multiple periodic location information is needed
Proxy Mode	The SPC system will not have direct communication with the SET. In this environment the SLC system will act as a proxy between the SET and the SPC.
Quality of Position	A set of attributes associated with a request for the geographic position of a SET. The attributes include the required horizontal accuracy, vertical accuracy, max location age and response time of the SET position.
Reference Point	See [OMA-DICT]
SET Initiated SUPL Services	SET Initiated SUPL Services are services which originate from the SET. For these services the SUPL Agent resides within the SET.
SET User	The user of a SET.
SUPL Agent	Service access point which accesses the network resources to obtain location information.
SUPL Enabled Terminal (SET)	A device that is capable of communicating with a SUPL network. Examples of this could be a UE in UMTS, a MS in GSM or IS-95, or a PC over an IP-based transport.
SUPL Interface	Interface between SUPL Enabled Terminal and SUPL network

SUPL Location Center (SLC)	Coordinates the operations of SUPL in the network and interacts with the SUPL Enabled Terminal (SET) over User Plane bearer.
SUPL Location Platform (SLP)	Entity responsible for SUPL Service Management and Position Determination. SLP contains the SLC and SPC Functions.
SUPL Network	Access network which facilitates the Location determination functionality and provides the SUPL bearer
SUPL Position Calculation	The position calculation function performs the function of calculating the position of a SET. Various positioning calculation modes may be supported by a SUPL service
SUPL Positioning Center (SPC)	Entity in the SUPL network responsible for all messages and procedures required for position calculation and for the delivery of assistance data.
SUPL Provider	Location information is sensitive personal information and requires specific care with privacy and security. In the case of a Mobile Network Operator it is important that whatever policy the Network Operator decides to implement SUPL functionality cannot be breached. Valid scenarios for MNO controlled SUPL would be: • The network operator is the single SUPL provider • The network operator and roaming partners are the only SUPL providers. • The network operator out-sources the SUPL functionality and there is a single 3rd party SUPL provider • The network operator has an open policy on the provision of SUPL functionality and there are multiple 3rd party SUPL providers • The SUPL Provider may be independent of an MNO
SUPL Security Function	SUPL Security function manages the Authentication and Authorization for SUPL Agents and MLS Applications to access SUPL Services. This function also provides confidentiality and data integrity.
SUPL Service Management	SUPL Service Management is the function of managing locations of SETs. The function stores, extracts, and modifies the location information of a target SET
SUPL User	The user of the SUPL functionality, hence, when the transaction is SET initiated, the SUPL User equals the SET User.
System	A functional entity
User Plane	The User Plane, with its layered structure, provides for user information flow transfer, along with associated controls (e.g., flow control, and recovery from errors, etc).

3.3 Abbreviations

AD	Architecture Document
AFLT	Advanced Forward Link Trilateration
A-GPS	Assisted GPS
ANSI	American National Standards Institute
B-TID	Bootstrapping Transaction Identifier
DNS	Domain Name Server
DTD	Document Type Definition
E-CGI	Enhanced Cell Global Identifier
EOTD	Enhanced Observed Time Difference

FQDN	Fully Qualified Domain Name
GMLC	Gateway Mobile Location Center
GMT	Greenwich Mean Time
GPS	Global Positioning System
HPLMN	Home Public Land Mobile Network
H-SLP	Home SLP
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
IETF	Internet Engineering Task Force
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
LCS	Location Services
LDC	Location Distribution Control
MAC	Message Authentication Code
MC	Message Center
MLC	Mobile Location Center
MLP	Mobile Location Protocol
MLS	Mobile Location Services
MNO	Mobile Network Operator
MSID	Mobile Station Identifier
NAF	Network Application Function
NMR	Network Measurement Report
OMA	Open Mobile Alliance
OTDOA	Observed Time Difference of Arrival
PAP	Push Access Protocol
PC	Personal Computer
PDE	Position Determination Entity
PLMN	Public Land Mobile Network
PPG	Push Proxy Gateway
PPR	Privacy Profile Register
QoP	Quality of Position
RD	Requirement Document
RLP	Roaming Location Protocol
RRC	Radio Resource Control
RRLP	Radio Resource LCS Protocol
R-SLP	Requesting SLP

R-UIM	Removable User Identity Module
SADF	SUPL Assistance Delivery Function
SCF	SUPL Charging Function
SET	SUPL Enabled Terminal
SIF	SUPL Initiation Function
SIM	Subscriber Identity Module
SLC	SUPL Location Center
SLIA	Standard Location Immediate Answer
SLIR	Standard Location Immediate Request
SLP	SUPL Location Platform
SMLC	Serving Mobile Location Center
SMPP	Short Message Peer to peer Protocol
SMS	Short Message Service
SMSC	Short Message Service Center
SPC	SUPL Positioning Center
SPCF	SUPL Position Calculation Function
SPF	SUPL Privacy Function
SRLIA	Standard Roaming Location Immediate Answer
SRLIR	Standard Roaming Location Immediate Request
SRRF	SUPL Reference Retrieval Function
SRRF	SUPL Reference Retrieval Function
SRSF	SUPL Roaming Security Function
SSF	SUPL Security Function
SSMF	SUPL Service Management Function
SSPF	SUPL SET Provisioning Function
SSRLIA	Standard SUPL Roaming Location Immediate Answer
SSRLIR	Standard SUPL Roaming Location Immediate Request
SSRP	Standard SUPL Roaming Position
SUPL	Secure User Plane Location
TLS	Transport Layer Security
UE	User Equipment
UICC	Universal Integrated Circuit Card
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
USIM	UMTS Subscriber Identity Module
UTM	Universal Transverse Mercator

V-SLP	Visited SLP
WAP	Wireless Application Protocol
WGS	World Geodetic System

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 SET (SUPL Enabled Terminal(s)) and the network. SUPL is considered to be an effective way of transferring location information required for computing the SET's location. The effects of deploying SUPL are mostly restricted to providing a SUPL Location Platform (SLP) and SET to support SUPL.

To serve a location service to a client, considerable signalling and position information is transferred between actors such as a SET and a location server. Currently, assisted-GPS (A-GPS) provides a 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 signalling procedures between the SET and the network). Location over User Plane (SUPL) as described in this specification 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 utilises existing standards where available and possible, and SUPL should be extensible to enabling more positioning technologies as the need arises so that they utilise the same mechanism. In the initial phase, SUPL will provide full functionality of A-GPS with minimum changes of current network elements.

This document describes the architecture for SUPL.

4.1 Target Audience

The target audience for this document includes but is not limited to the following:

- The Working Group(s) that will create specifications based on this subject matter
- Working Groups that need to understand the architecture of this subject matter
- Architecture Working Group (e.g., during Architecture Reviews as defined in [ARCH-REVIEW], to determine compliance of [ARCH-PRINC], etc.)
- Interoperability Working Group (e.g., for early analysis of interoperability requirements)
- Security Working Group
- Implementors of SET's and SLP's

4.2 Use Cases

This AD does not describe its own use cases. The corresponding Requirements Document [SUPL RD] describes use cases in Section 5. These use cases are informative only and intended to derive normative requirements (see below), there is no further elaboration on use cases at this point.

The major actors in the SUPL architecture are as follows:

- SET User, see Section 3.2 "Definitions"
- SUPL User, see Section 3.2 "Definitions"
- SET (SUPL Enabled Terminal) , see Section 3.2 "Definitions"
- SUPL Agent, see Section 3.2 "Definitions"
- SLP (SUPL Location Platform), see Section 6.4 "SUPL Reference Architecture"
  - SLC (SUPL Location Center) , see Section 6.4 "SUPL Reference Architecture"
  - SPC (SUPL Positioning Center) , see Section 6.4 "SUPL Reference Architecture"

4.3 Requirements

This AD satisfies all of the requirements in [SUPL RD] except the following:

Requirement ID/Number	Subject matter	Targeted Release
6.1.1#8	Deferred location requests	2.0
6.1.1#9	Periodic location requests	2.0
6.1.1#12	Different priorities for requests	2.0

Table 1: Requirements postponed to SUPL Rel 2

4.4 Planned Phases

SUPL will be published in different versions. This architecture document specifies SUPL Version 1. The forthcoming SUPL Version 2 will address the requirements not fulfilled in Version 1 and, in addition, new requirements not known today.

SUPL Version 1 supports the following modes of operation for selected deployments:

- Proxy flows for GSM/WCDMA deployments
- Proxy flows for CDMA/CDMA2000 deployments
- Non-proxy flows for CDMA/CDMA2000 deployments

Non-proxy flows for GSM/WCDMA deployments will be considered for inclusion after publication of the first Candidate Enabler Release.

5. Context Model

Secure User Plane Location (SUPL) is an Enabler which utilises existing standards where available and possible, to transfer assistance data and positioning data over a User Plane bearer, such as IP, to aid network and SET based positioning technologies in the calculation of a SET's position. SUPL includes but is not limited to the definition of a Location User Plane (Lup) reference point and corresponding interface between the SUPL network and SET, security functions (e.g., authentication, authorization), charging functions, roaming functions, privacy function.

SUPL is used by MLS Applications via a SUPL Agent to determine the position of a SET. SUPL itself does not specify an API for direct use by MLS Applications.

The SUPL architecture depends on [OMA RLP].

6. Architectural Model

6.1 SUPL Services

The SUPL Location Services can be categorized into Network initiated and SET initiated services.

The following services must be considered:

- Immediate Location Service
  - Commercial Services
  - Emergency Services
- Deferred Location Service
- Periodic Location Services

Complete Emergency Services support, based on local regulations and available technology, is for further study.

Deferred and Periodic Services are not in scope for SUPL Release 1.

6.1.1 Network Initiated SUPL Services

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

6.1.2 SET Initiated SUPL Services

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

6.2 SUPL Location Services Functional Group

This section identifies and describes the logical functional entities within the SUPL location services functional group. The purpose of this section is to ensure that all possible functions are identified which are required to enable a SUPL service.

6.2.1 SUPL Privacy Function (SPF)

The SUPL Privacy Function is the function of ensuring the privacy of a SET User is honored. The following must be considered:

- Adhere to the target SET User privacy setting regardless of Network Initiated or SET Initiated services
- Adhere to notification and verification settings of the target SET User
- Allow for future emergency and lawful override regulations that may apply to the target SET User

SUPL may use existing privacy nodes such as Privacy Profile Register (PPR) or Location Distribution Control (LDC) to implement the privacy function. Alternatively, the SPF may be implemented in the SET.

6.2.2 SUPL Initiation Function (SIF)

The SUPL Initiation function provides a mechanism for a SUPL network to start a transaction with a SET. The initiation function is of special importance in enabling SUPL Network Initiated Services.

In case of a SUPL Network Initiated Service the SUPL network starts the SUPL transaction by using one of the following methods:

- WAP Push Access Protocol (PAP)
- SMS directly in an MNO environment

Depending upon SET capabilities the applicable SUPL Initiation method is applied by the SUPL network (determination of SET capabilities is out of scope of SUPL).

A SET SHALL support at least one of these SUPL Initiation methods.

6.2.3 SUPL Security Function (SSF)

The SUPL Security function enables the SUPL network to authenticate and authorize the SET and enables the SET to authenticate and authorize the SUPL network. This is important in safely enabling both Network Initiated and SET Initiated SUPL Service.

The SUPL Security function also provides confidentiality and data integrity.Refer to section 7 for details of the SUPL Security Function implementation.

6.2.4 SUPL Roaming Support Function (SRSF)

SUPL roaming occurs when a SET leaves the service area of its H-SLP. The service area of an H-SLP includes the area within which the H-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 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 summarised below:

- The H-SLP may request the V-SLP to provide an initial position estimate, e.g., based upon Location ID.
- The H-SLP may request the V-SLP to provide the Lup Positioning 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 negotiation parameters such as positioning method.

The most important variants of roaming are described in sections 6.8 and 6.9.

6.2.5 SUPL Charging Function (SCF)

The SUPL Charging Function (SCF) is responsible for charging activities within the SLP. This includes charging of MLS Application, SUPL Agents and SET Users.

The main task for SCF is to collect appropriate charging related data and data for accounting between SUPL providers. Additionally, SCF may authorise activities in SLP (e.g., assistance data and location delivery) based on assessment of available charging data. Further details of SCF are out of scope of SUPL.

6.2.6 SUPL Service Management Function (SSMF)

SUPL Service Management Function is the function of managing locations of SETs. This function stores, extracts, and modifies the location information of a target SET. During the execution of this function, the integration with charging, privacy, security, QoP functions SHALL be considered.

6.2.7 SUPL SET Provisioning Function (SSPF)

SUPL SET Provisioning Function is the function that manages the provisioning for the SET. The SET SHALL be provisioned with the address of the Home SLP. 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].

6.3 SUPL Positioning Functional Group

This section identifies and describes the logical functional entities within the SUPL positioning services functional group.

6.3.1 SUPL Assistance Delivery Function (SADF)

The assistance data delivery function generates and delivers available assistance data, which is used for the measurement or the calculation of a SET position. The assistance data delivery may be based on a selected subset of GPS reference data retrieved from SRRF function [section 6.3.2], the capability of SET and network, and the approximate position information of the target SET.

Assistance data may consist of the elements defined in [3GPP RRLP], [3GPP RRC] or [3GPP2 C.S0022-A, 3GPP2 C.S0022-0].

6.3.2 SUPL Reference Retrieval Function (SRRF)

The reference data retrieval function is the function of retrieving GPS reference data from a GPS reference network. Reference data is needed to generate assistance data. The interface between this function and GPS reference network is out of the scope of this document.

6.3.3 SUPL Position Calculation Function (SPCF)

The position calculation function performs the function of calculating the position of a SET. One or more of the following positioning calculation modes may be supported by a SUPL service.

- A-GPS SET assisted
- A-GPS SET based
- Autonomous GPS
- Enhanced Cell/sector
- AFLT
- EOTD
- OTDOA
- Location ID – SHALL be supported
    - Perform translation of a location identifier to a geographic location expressed in latitude and longitude. In MNO environments this is often referred to as Cell-ID location.

6.4 SUPL Reference Architecture

This section identifies the SUPL network architecture model, comprised of the User Plane location services related network entities and associated reference points.

A network entity (i.e system and subsystem) represents a group of functions, and not necessarily a physical device. The physical realization is an implementation decision: a manufacturer may choose any physical implementation of network entities, either individually or in combination, as long as the implementation meets the functional requirements.

A reference point is a conceptual demarcation of two groups of functions. It is not necessarily a physical interface. A reference point only becomes one or several physical interfaces when the network entities on each of its sides are contained in different physical devices. One or more protocols may be defined for the instantiation of an interface. As the Lup reference point is instantiated by one interface, we use both terms in this document. The corresponding protocol is defined in the detailed technical specification [OMA ULP].

In generic environments, the required SUPL components are the SET and the network component SLP containing the SLC and SPC systems. The SET communicates with the network over the Lup interface.

In MNO environments, several entities and their interfaces may also be needed as illustrated in the figure in this section.

The detailed functions and definitions of the components defined in this figure are explained in Section 6.5, 6.8 and 6.9 and in the SUPL TS [OMA ULP].

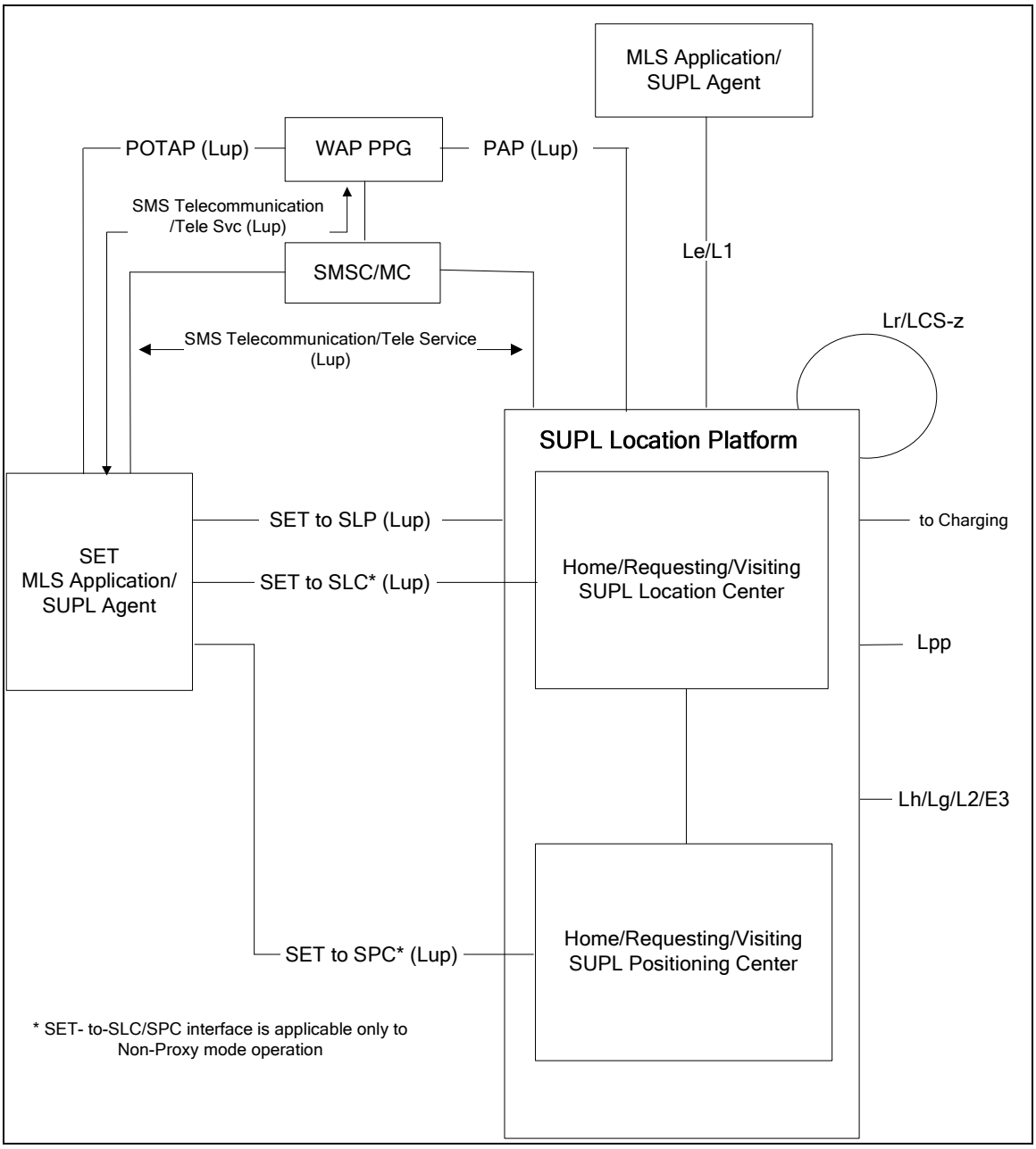

Figure 1: SUPL Architecture

Existing deployments may choose to adapt existing physical nodes to include SUPL functionality. In those cases, there is an embedded dependency for signalling on an interface between distributed SLCs and SPCs. This version of the architecture is dependent on that signalling for those deployments.

6.4.1 Communication Mechanisms and Interfaces Covered by Lup

The protocols involved in WAP Push are PAP (Push Access Protocol) for conveying location request notification from the SLP to the PPG (Push Proxy Gateway), and POTAP (Push Over-The-Air Protocol) for conveying such notification from the PPG to the SET. SMS delivery of notification is another option, and can be initiated either by SMS Trigger from the SLP, or by WAP notification. Protocol interfaces for SMS delivery are not specified in the diagram, since the interface between SLP and SMSC/MC is proprietary (e.g., SMPP) and is not defined by 3GPP/3GPP2. The communication path from SMSC/MC to the SET is outside the scope of this document. In proxy-mode the SUPL application message exchange for service

management and positioning determination occurs between the SLP and the SET. In non-proxy-mode the service management related message exchange occurs between the SLC and the SET, where the positioning determination related message exchange occurs between the SPC and the SET.

6.5 SUPL and OMA Architecture models

This section provides an informative mapping of the SUPL architecture as it relates to the OMA Architecture defined in [OMA AD].

- The SUPL SLP is contained within the OMA Architecture [OMA AD] node called "Location Server".
- The SUPL SET is contained within the OMA Architecture [OMA AD] node called "End User Device".
- The MLS Application/SUPL Agent corresponds to the OMA AD node "Location Based Application." contained within "Requesting Applications".
- The SUPL Le/L1 reference point refers to the OMA Architecture [OMA AD] reference point L-1.
- The SUPL architecture provides two alternatives for implementing the SUPL Initiation Function (SIF).
  - The SUPL Initiation Function using a WAP PPG refers to the P-1/P-1s per OMA Architecture [OMA AD]. Reference point P-2/P-2s of the OMA AD is situated between the WAP PPG and the SET.
  - The SUPL Initiation Function using the SMS related Core and Access Network support has no direct mapping to the OMA Architecture [OMA AD].

6.6 SUPL System and Subsystem Descriptions

6.6.1 SUPL Location Platform

The SUPL Location Platform (SLP) consists of an SUPL Location Center (SLC) and SUPL Positioning Center (SPC). The SLC and SPC may be integrated into a single system. The Lup interface is used between the SLP and the SET. The Lup interface is used to deliver messages for SUPL Service Management and SUPL Positioning Determination.

It may also be possible to separate the SLC and SPC functionality into separate systems within the SLP.

There are two different communication modes between SET and SLP:

- **Proxy Mode**: The SPC system will not have direct communication with the SET. In this environment the SLC system will act as a proxy between the SET and the SPC.Non-Proxy Mode: The SPC system will have direct communication with the SET

The Lup interface is used between the SLP and SET. The Lup carries two types of messaging:

- Messaging destined to the SLC system within the SLP – Lup Service Management Messages
- Messaging destined to the SPC system within the SLP – Lup Positioning Determination Messages

6.6.1.1 SUPL Location Center (SLC)

The SLC system coordinates the operations of SUPL in the network and performs the following functions as it interacts with the SUPL Enabled Terminal (SET) over User Plane bearer:

- SUPL Privacy Function (SPF)
- SUPL Initiation Function (SIF)

- SUPL Security Function (SSF)
- SUPL Roaming Support Function (SRSF)
- SUPL Charging Function (SCF)
- SUPL Service Management Function (SSMF)
- SUPL Positioning Calculation Function (SPCF)
  - The SLC may perform the translation of a location identifier to a geographic location expressed in latitude and longitude data. This location may meet the requested QoP of the SUPL Agent. In MNO environments this is often referred to as Cell-ID location.

6.6.1.2 SUPL Positioning Center (SPC)

The SPC supports the following functions:

- SUPL Security Function (SSF)
- SUPL Assistance Delivery Function (SADF)
- SUPL Reference Retrieval Function (SRRF)
- SUPL Positioning Calculation Function (SPCF)

6.6.2 SUPL Enabled Terminal (SET)

The SET supports the procedures defined in SUPL as it interacts with the network over the User Plane bearer. The SET may support one or more of the following functions depending on its capabilities and the SUPL Provider's business rules:

- SUPL Privacy Function (SPF)
- SUPL Security Function (SSF)
- SUPL SET Provisioning Function (SSPF)

The SET supports SET-based and/or SET-assisted positioning calculation. The SET may support the following functions:

- SUPL Positioning Calculation Function (SPCF)
- SUPL Assistance Delivery Function (SADF)

There is overlap between functionalities of SLC/SPC and SET.

6.6.3 Allocation of SUPL functions to SUPL Subsystems

Table 2**Error! Reference source not found.** shows the allocation of functional entities in the reference configuration of SUPL.

	SLC	SPC	SET
Location Services Functional Group			
SUPL Privacy Function (**SPF**)	O		O
SUPL Initiation Function (**SIF**)	O		
SUPL Security Function (**SSF**)	O	O	O
SUPL Roaming Support Functions (**SRSF**)	O		
SUPL Charging Function (**SCF**)	O		
SUPL Service Management Function (**SSMF**)	O		
SUPL SET Provisioning Function (**SSPF**)			O
Positioning Functional Group			

SUPL Assistance Delivery Function (**SADF**)		O	O
SUPL Reference Retrieval Function (**SRRF**)		O	
SUPL Positioning Calculation Function (**SPCF**)	O	O	O
	SLC	**SPC**	**SET**

Table 2: Allocation of SUPL functional entities to SUPL subsystems

6.7 SUPL Interface Definition

This section defines the interfaces identified in the SUPL architecture. The SUPL architecture identifies one new interface.

6.7.1 Lup

The function of the Lup reference point is logically separated into Location Service Management and Positioning Determination.

6.7.1.1 Service Management

This interface is used to enable the SLP to establish a session with the SET and performs the functions listed in section 6.6.1.1.

Table 3**Error! Reference source not found.** 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. This message MAY contain the initial Target SET User Notification, Confirmation Privacy instructions, MAC and KeyIdentity.
SUPL START	The SUPL START message is used by the SET to start a 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 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.

Table 3: Lup Service Management

6.7.1.2 Positioning Determination

The Lup Positioning Determination interface is used to transport information used for the calculation of position between the SET and SLP. It performs the functions listed in section 6.6.1.2.

Table 4 shows the messages in the Lup Positioning 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) 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) with the SLP.
SUPL END	The SUPL END message is used by the SLP or SET to end an existing SUPL session.

Table 4: Lup Positioning Determination

A SET and SLP MUST provide support for Location ID positioning.

A GSM and/or WCDMA capable SET and SLP providing support for this SET type SHALL support RRLP if A-GPS or E-OTD positioning is supported.

A CDMA capable SET and SLP providing support for this SET type SHALL support TIA-801 if A-GPS or AFLT positioning is supported.

The SET and SLP support for other positioning protocols is OPTIONAL.

In the case of RRLP and SET based location determination in the SET initiated case, the SLP SHALL send the RRLP Assistance Data message. The SET SHALL acknowledge the reception of assistance data with the RRLP Assistance Data Acknowledgement message.

In the case of RRC and SET based location determination in the SET initiated case, the SLP SHALL send the RRC Assistance Data Delivery message.

6.8 SUPL Collaboration Network Initiated

For Network Initiated applications, an SLP and SET SHALL support SUPL INIT, SUPL POS INIT and SUPL END. The support for SUPL POS is OPTIONAL and positioning method dependent, e.g. required for A-GPS positioning.

The SET MAY reuse the secure IP connection of an already ongoing SUPL session between the SET and the H-SLP. If a SET is reusing a secure IP connection, no new IP connection is established and the Secure IP connection is not released as long as one or more SUPL sessions are using it.

The Roaming cases are described with an R-SLP in the flow descriptions but the R-SLP can be omitted in the flow descriptions having the H-SLP interacting directly with SUPL Agent. In the Non-Roaming flow descriptions an R-SLP can be inserted between SUPL Agent and H-SLP.

6.8.1 Non-Roaming Successful Case – Proxy mode

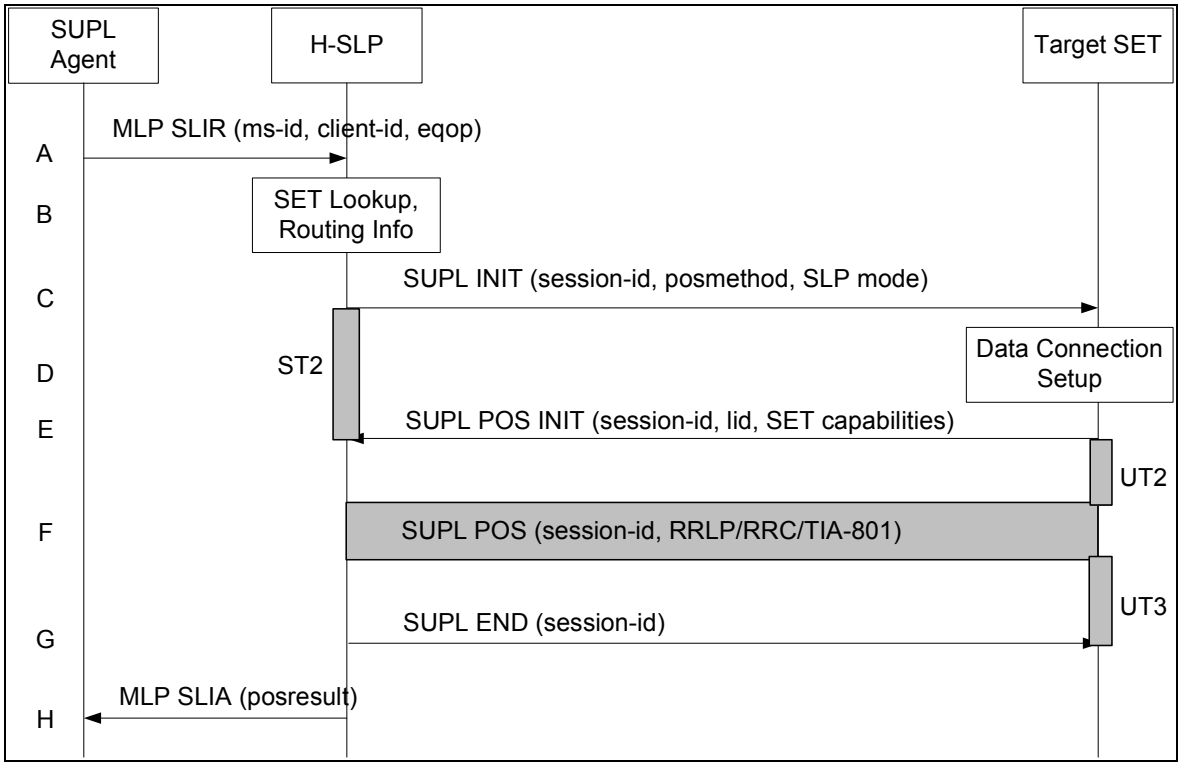

Figure 2: NW Initiated Non-Roaming Successful Case – Proxy Mode

(Note: See section 8 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: The specifics for determining if the SET supports SUPL are beyond SUPL 1.0 scope.

C. 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. The SUPL INIT MAY contain the desired QoP, a Key Id, and a MAC. The Key-Id corresponds to MAC_Master_Key in section 7.1.2 which MAY be used to verify SUPL INIT message is authentic. 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.

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. If a Key Id and a MAC is present in the received SUPL INIT message and the SET supports these parameters, the SET MAY use these parameters to determine if the SUPL INIT message is authentic.

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 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 identifier (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). 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 H-SLP SHALL 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) from the SUPL POS INIT message.

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 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.

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

6.8.2 Non-Roaming Successful Case – Non-Proxy mode

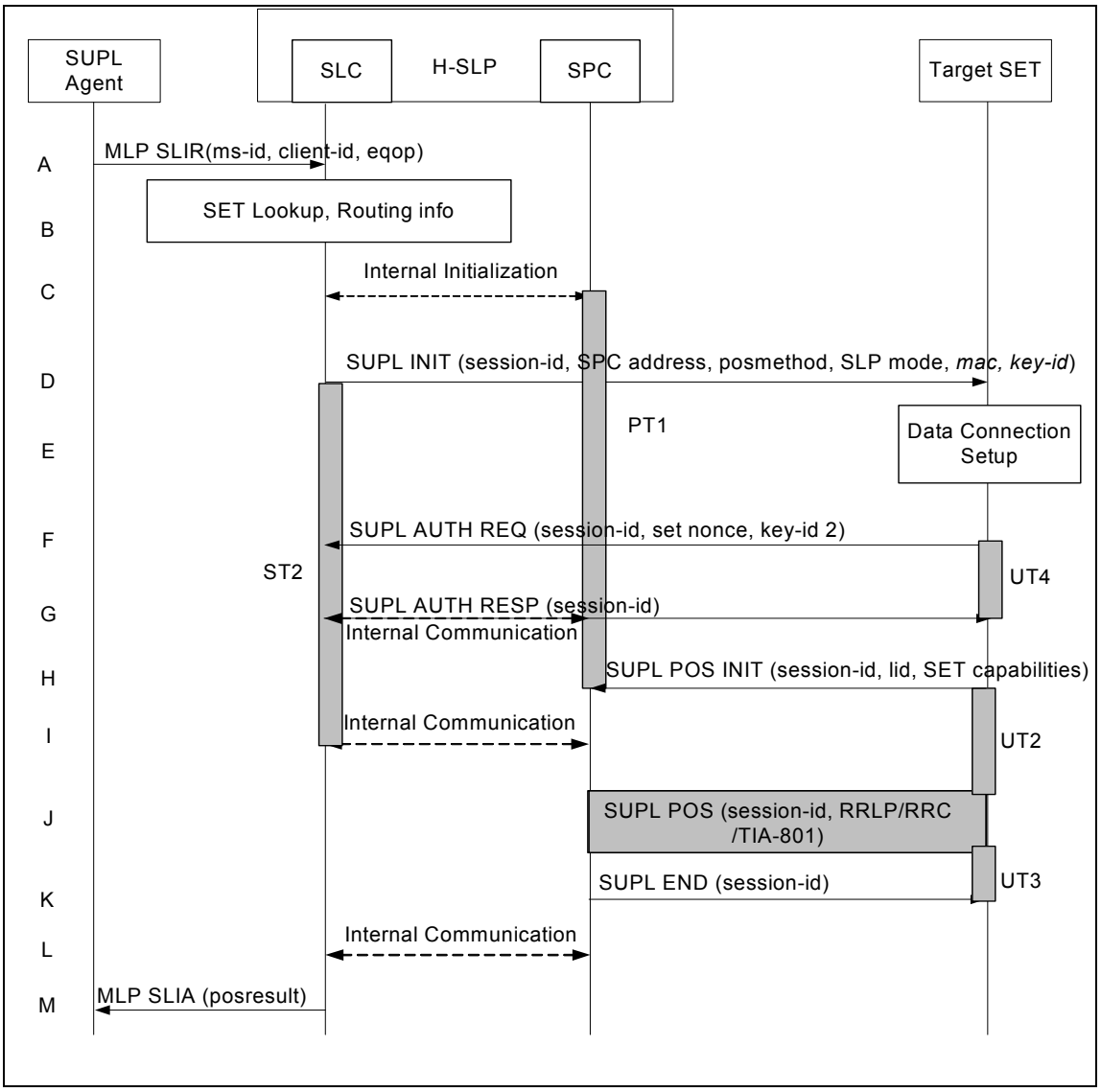

Figure 3: NW Initiated Non-Roaming Successful Case – Non-Proxy mode

(Note: See section 8 for timer descriptions.)

A. SUPL Agent issues an MLP SLIR message to the SLC, with which SUPL Agent is associated. The 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 SLC shall apply subscriber privacy against the client-id.

   If a previously computed position which meets the requested QoP is available at the SLC and no notification and verification is required, the SLC SHALL directly proceed to step M. If notification and verification or notification only is required, the SLC SHALL proceed to step B.

B. The SLC verifies that the target SET is currently not SUPL roaming.

   The 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 1.0 scope.

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

Note: The specifics for the interface between the SLC and SPC are beyond the scope for SUPL 1.0 and are thus implementation dependent.

D. The SLC 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, address of the SPC, proxy/non-proxy mode indicator, Key Id, MAC and the intended positioning method. The SUPL INIT MAY contain the desired QoP. If the result of the privacy check in Step A indicates that notification or verification to the target subscriber is needed, the SLC shall also include Notification element in the SUPL INIT message. The Key-Id corresponds to MAC_Master_Key in section 7.1.2 which SHALL be used to verify SUPL INIT message is authentic.

E. If in step A the 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 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 H to establish a secure IP connection to the SLC.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. The SET SHALL use the Key Id and MAC to determine if the SUPL INIT message is authentic.

F. The SET uses the address provisioned by the Home Network to establish a secure IP connection to the 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 SLC.The SUPL AUTH REQ message SHALL contain session-id, key-id 2 and SET nonce. The key-id 2 corresponds to PP2_SPC_Master_key in section 7.1.2 to generate PSK_SPC_Key which is used for PSK- TLS session between the SPC and the SET.

G. The SLC uses key-id 2 and set nonce to create a key to be used for mutual SPC/SET authentication. The SLC forwards the created key to the SPC through internal communication and returns a SUPL AUTH RESP message to the SET. The SUPL AUTH RESP message SHALL contain the session-id.

H. The SET will evaluate the Notification rules and follow the appropriate actions. The SET establishes a secure IP connection to the SPC according to the address received in step D. The SET and H-SLP perform mutual authentication and the SET sends a SUPL POS INIT message to start a positioning session with the 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 identifier (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). 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 SLC and release all resources related to this session.

I. The SLC and 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 H-SLP proceeds directly to step K.

J. Based on the SUPL POS INIT message including posmethod(s) supported by the SET the SPC SHALL determine the posmethod. If required for the posmethod the SPC SHALL use the supported positioning protocol (e.g., RRLP, RRC, TIA-801) from the SUPL POS INIT message

The SET and the SPC MAY exchange several successive positioning procedure messages.

The 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 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 IP connection to the SPC and release all resources related to this session.

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

M. The SLC sends the position estimate back to the SUPL Agent by means of the MLP SLIA message and SLC can release all resources related to this session. The SLC SHALL release all resources related to this session.

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

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

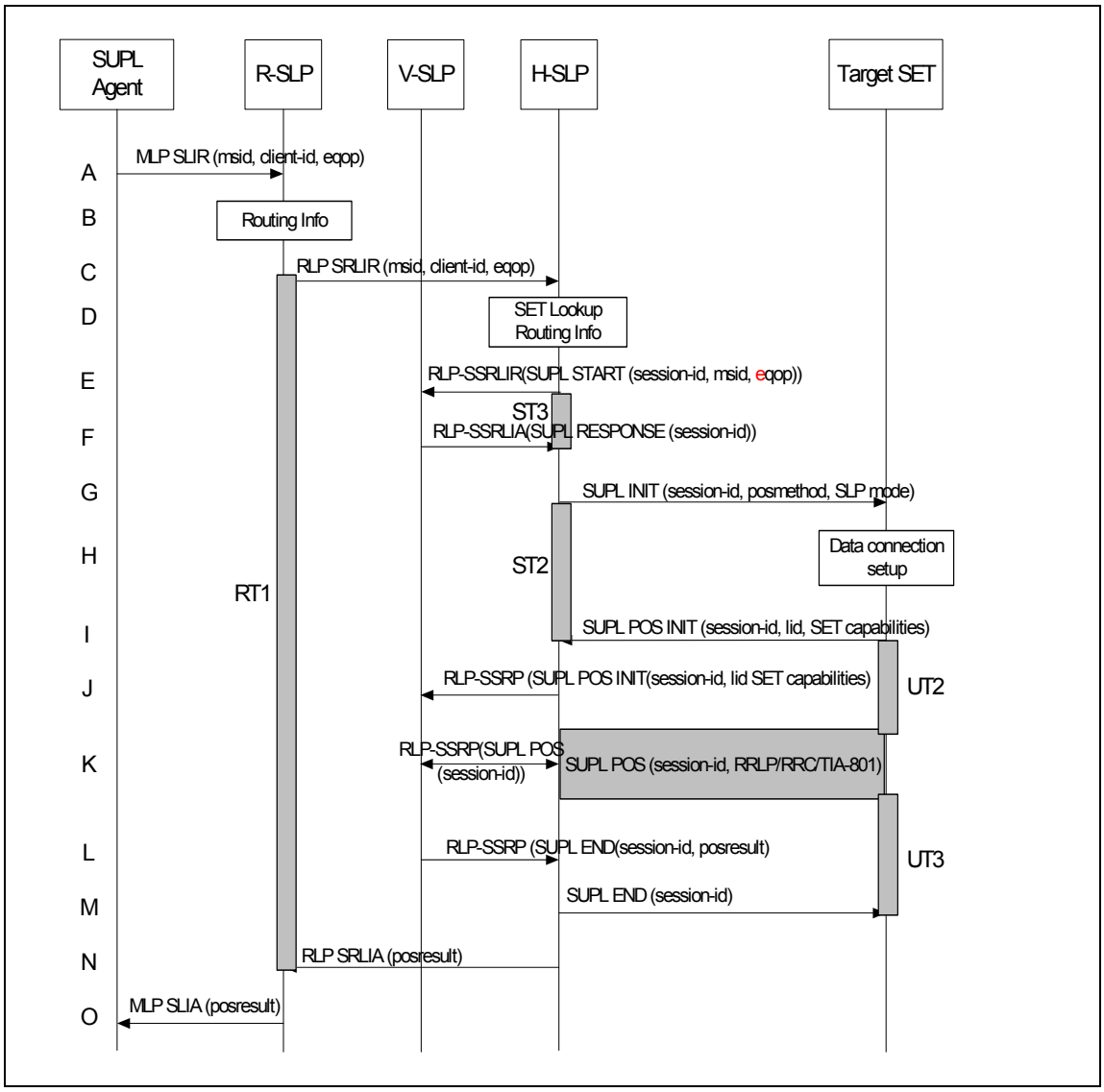

Figure 4: NW Initiated Roaming Successful Case – Proxy mode with V-SLP

(Note: See section 8 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. 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 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.

   Note: The specifics for determining if the SET supports SUPL are beyond SUPL 1.0 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, which could 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. The SUPL INIT MAY contain the desired QoP, a Key Id, and a MAC. The Key-Id corresponds to MAC_Master_Key in section 7.1.2 which MAY be used to verify SUPL INIT message is authentic. If the result of the privacy check in Step D 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 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 IP connection to the H-SLP.

H. 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. If a Key Id and a MAC is present in the received SUPL INIT message and the SET supports these parameters, the SET MAY use these parameters to determine if the SUPL INIT message is authentic.

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 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 identifier (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). 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) 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 H-SLP about the termination and position by sending a SUPL END to the H-SLP tunnelled over RLP. The H-SLP proceeds to step M and returns the positioning result.

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 via H-SLP (SET-Based).

L. Once the position calculation is complete the V-SLP sends the SUPL END message towards 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 IP 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 by means of the 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 by means of the MLP SLIA message.

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

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

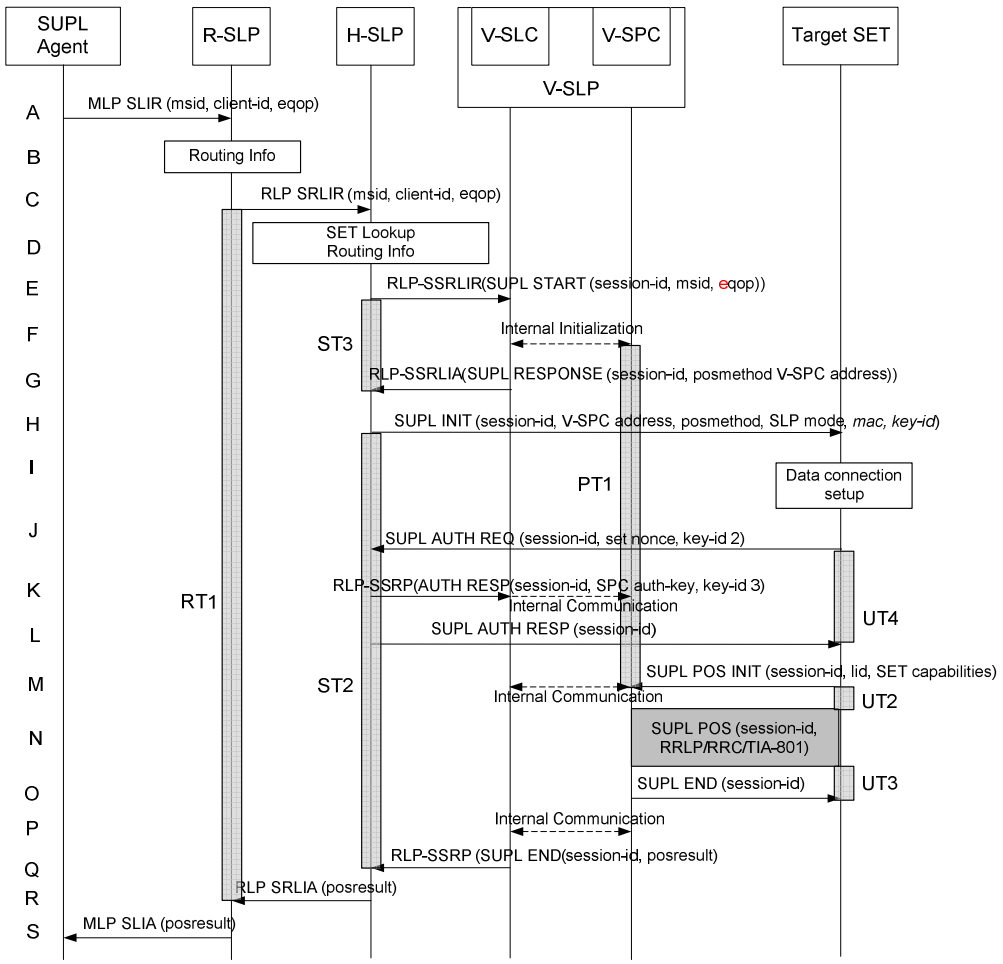

Figure 5: NW Initiated Roaming Successful Case – Non-Proxy-mode with V-SPC

(Note: See section 8 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-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 no notification and verification is required, the H-SLP SHALL directly proceed to step R. If 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.

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: The specifics for determining if the SET supports SUPL are beyond SUPL 1.0 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, which could be a WAP PUSH or an SMS Trigger. The SUPL INIT message contains at least session-id, address of the V-SPC, proxy/non-proxy mode indicator, Key Id, MAC and the intended positioning method. The SUPL INIT MAY contain the desired QoP. If the result of the privacy check in Step D indicates that notification or verification to the target subscriber is needed, the H-SLP SHALL also include Notification element in the SUPL INIT message.

I. 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 R. 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 IP connection to the H-SLP.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. The SET SHALL use the Key Id and MAC to determine if the SUPL INIT message is authentic. The Key-Id corresponds to MAC_Master_Key in section 7.1.2 which SHALL be used to verify SUPL INIT message is authentic.

J. The SET uses the address provisioned by the Home Network to establish a IP 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 SHALL contain session-id, key-id 2, and SET nonce.

K. The H-SLP uses key-id 2 and set nonce to create a key to be used for mutual V-SPC/SET authentication. The H-SLP forwards the created key to the V-SLC through an RLP SSRP message. The key-id 2 corresponds to PP2_SPC_Master_key in section 7.1.2 to generate PSK_SPC_Key which is used for PSK-TLS session between the V-SPC and the SET.

The V-SLC forwards the key 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. The key-id 3 corresponds to PSK_SPC_Key.

M. The SET will evaluate the Notification rules and follow the appropriate actions. The SET establishes a secure IP 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 identifier (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). 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 H-SLP and release all resources related to this session.

The V-SPC informs the V-SLC that the positioning procedure is started.

N. 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) 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 Q 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).

O. 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.

P. 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.

Q. 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.

R. The H-SLP sends the position estimate back to the R-SLP by means of the RLP SRLIA message. The H-SLP SHALL release all resources related to this session.

S. The R-SLP sends the position estimate back to the SUPL Agent by means of the MLP SLIA message

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

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

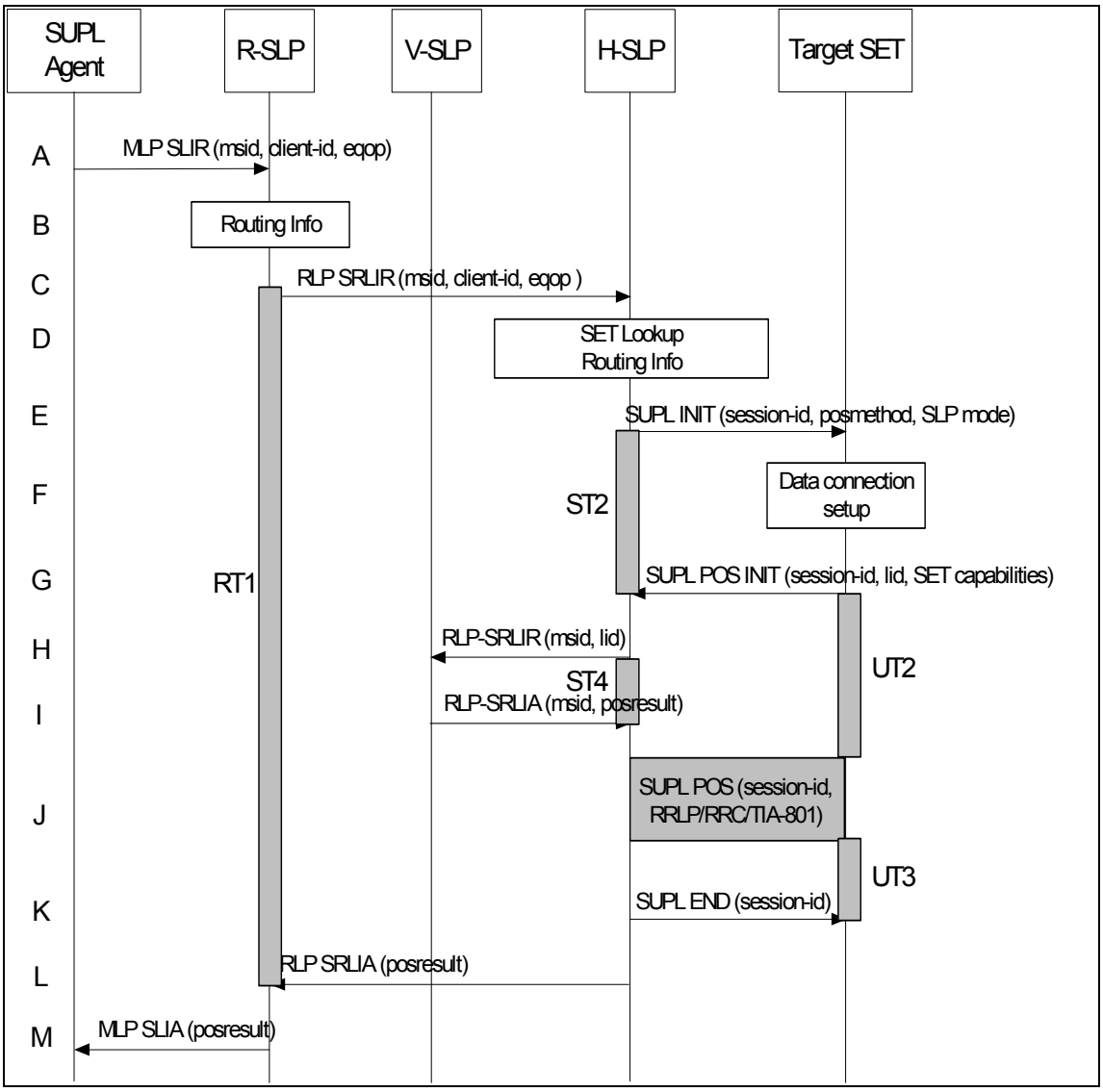

Figure 6: NW Initiated Roaming Successful case – Proxy mode with H-SLP

(Note: See section 8 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. 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 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: The specifics for determining if the SET supports SUPL are beyond SUPL 1.0 scope.

E. The H-SLP initiates the location session with the SET using the SUPL INIT message, which could 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. The SUPL INIT MAY contain the desired QoP, a Key Id, and a MAC. The Key-Id corresponds to MAC_Master_Key in section 7.1.2 which MAY be used to verify SUPL INIT message is authentic. If the result of the privacy check in Step D 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 IP connection to the H-SLP

F. 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. If a Key Id and a MAC is present in the received SUPL INIT message and the SET supports these parameters, the SET MAY use these parameters to determine if the SUPL INIT message is authentic.

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 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 and location identifier (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). 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. The H-SLP then 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 identifier (lid). Optionally the H-SLP MAY forward NMR provided by the SET to the V-SLP.

I. 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 proceeds directly to step K.

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) from the SUPL POS INIT message.

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).

K. 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.

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 by means of the MLP SLIA message.

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

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

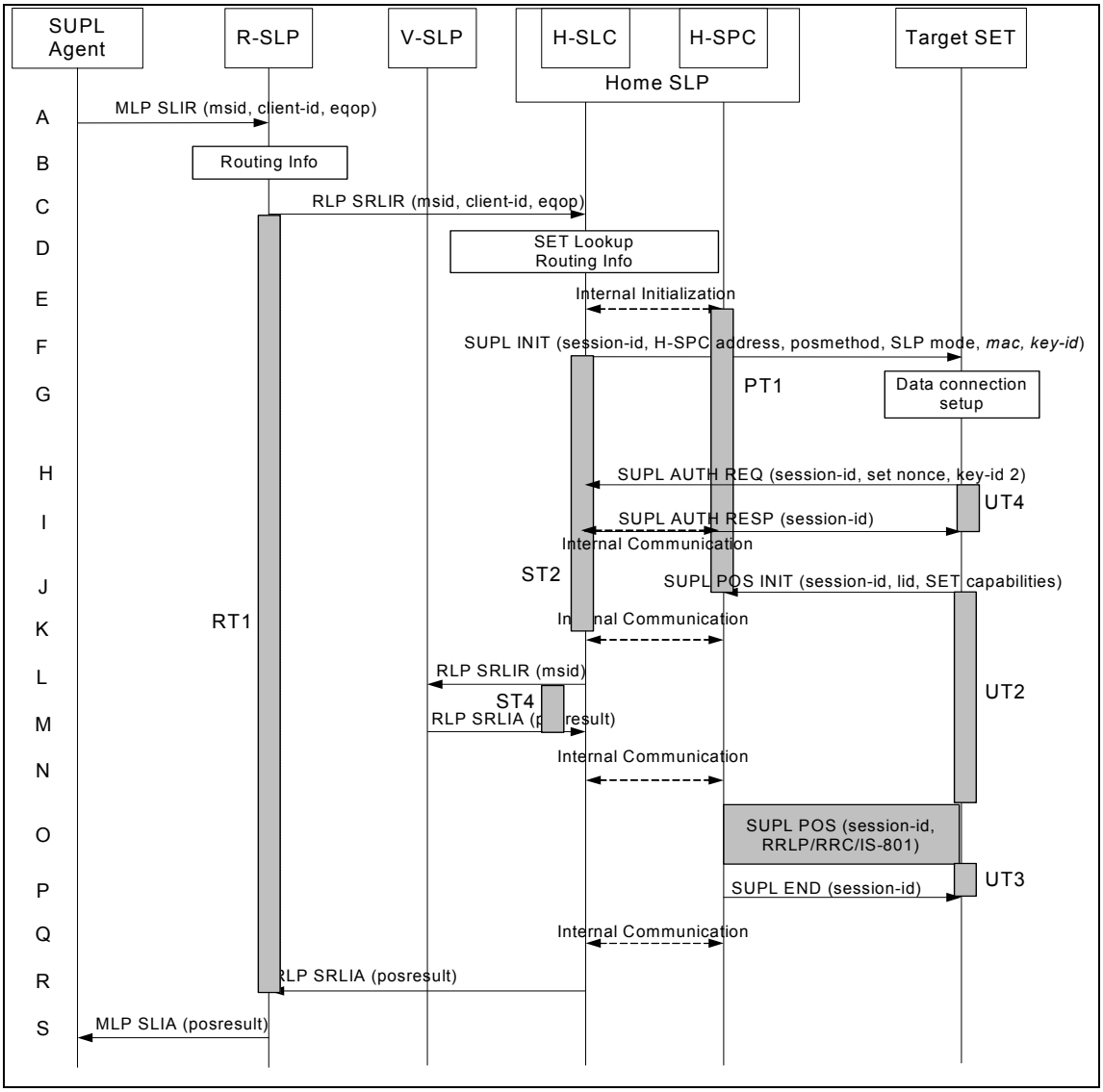

Figure 7: NW Initiated Roaming Successful Case – Non-Proxy-mode with H-SPC

(Note: See section 8 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. 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 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: The specifics for determining if the SET supports SUPL are beyond SUPL 1.0 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, which could be a WAP PUSH or an SMS Trigger. The SUPL INIT message contains at least session-id, address of the H-SPC, proxy/non-proxy mode indicator, Key Id, MAC and the intended positioning method. The Key-Id corresponds to MAC_Master_Key in section 7.1.2 which SHALL be used to verify SUPL INIT message is authentic. The SUPL INIT MAY contain the desired QoP. If the result of the privacy check in Step D indicates that notification or verification to the target subscriber is needed, the H-SLC SHALL also include 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 IP connection to the H-SLC.

G. 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. The SET SHALL use the Key Id and MAC to determine if the SUPL INIT message is authentic.

H. The SET uses the address provisioned by the Home Network to establish a secure IP 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 SHALL contain session-id, key-id 2, and SET nonce. The key-id 2 corresponds to PP2_SPC_Master_key in section 7.1.2 to generate PSK_SPC_Key which is used for PSK-TLS session between the H-SPC and the SET.

I. The H-SLC uses key-id 2 and set nonce to create a key to be used for mutual H-SPC/SET authentication. The H-SLC forwards the key to the H-SPC through internal communication and returns a SUPL AUTH RESP message to the SET. . The SUPL AUTH RESP message SHALL contain the session-id.

J. The SET will evaluate the Notification rules and follow the appropriate actions. The SET establishes a secure IP 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 identifier (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). 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 IP connection to the H-SLC and release all resources related to this session.

K. The H-SPC informs the H-SLC that the target SET has established the session and informs the H-SLC of the lid and optionally the NMR specific data for the radio technology being used (e.g., for GSM: TA, RXLEV) and position if this is supported.

L. The H-SLC 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-SPC. The RLP request contains at least the msid and the location identifier (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 (e.g., coarse position for A-GPS positioning).

N. The H-SLC informs the H-SPC of the initial position. However, if the computed position meets the requested QoP, the H-SLC informs the H-SPC that a position was already obtained. The H-SPC proceeds to step P to terminate the SUPL positioning session and the H-SLC proceeds to step R.

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) from the SUPL POS INIT message.

The SET and the H-SPC MAY exchange several successive positioning procedure messages.

If the V-SLP already calculated a position satisfying the requested QoP the H-SPC terminates the positioning session with a SUPL END and informs the H-SLC about the termination. The H-SLC proceeds to step R and returns the positioning result.

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 by means of the 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 by means of the MLP SLIA message.

6.8.7 Exception Procedures

6.8.7.1 SET does not allow Positioning

When the SET receives a SUPL INIT message asking for notification or verification to the target subscriber, the SET starts the related procedure. The subscriber denies the request and the SET shall send the SUPL END message with a status code to the H-SLP indicating the error reason (e.g., consentDeniedByUser).

Afterwards, the H-SLP and the SET release the resources related to this session at the Lup interface.

The H-SLP sends a positioning error back to the SUPL Agent by means of the MLP SLIA message.

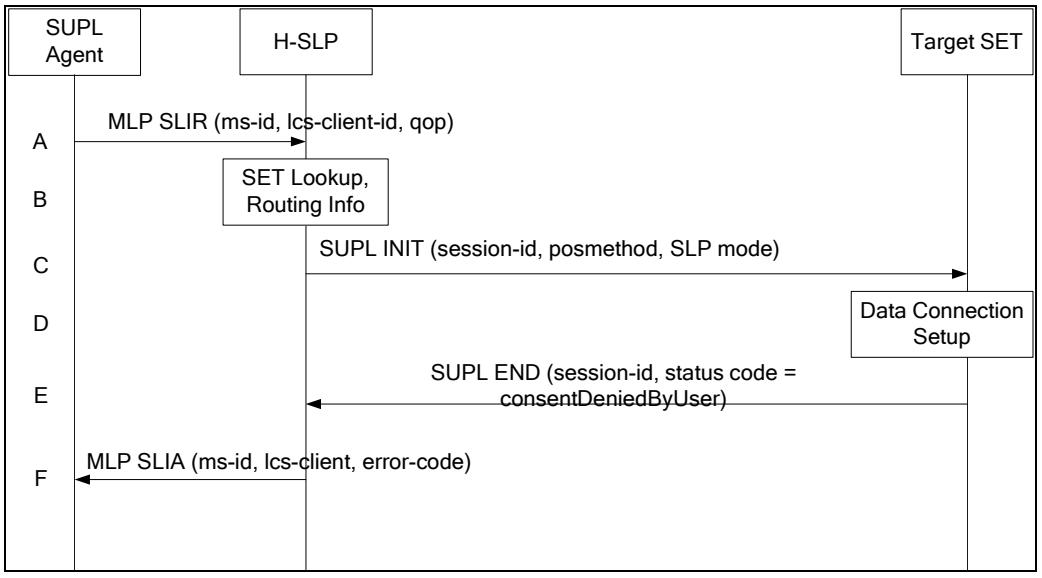

Figure 8: NW Initiated SET User denies Positioning

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. 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 scope of SUPL. However, there are various environment dependent mechanisms.

   Note: The specifics for determining if the SET supports SUPL are beyond SUPL 1.0 scope.

C. 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. The SUPL INIT MAY contain the desired QoP, address of the H-SLP, a Key Id, and a MAC. The Key-Id corresponds to MAC_Master_Key in section 7.1.2 which MAY be used to verify SUPL INIT message is authentic. 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 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 and the status code indicating the error reason ("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 by means of the MLP SLIA message.

6.8.7.2 Authorization Failure at H-SLP

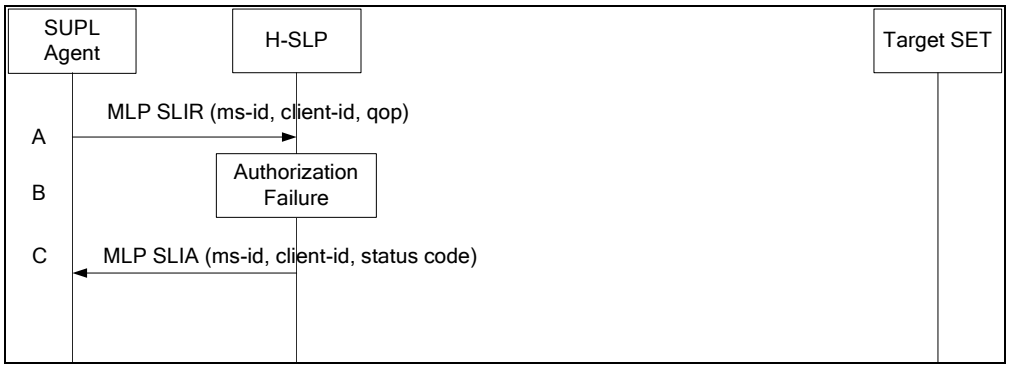

Figure 9: NW Initiated Authorization Failure H-SLP

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.

6.8.7.3 Authorization Procedure at V-SLP

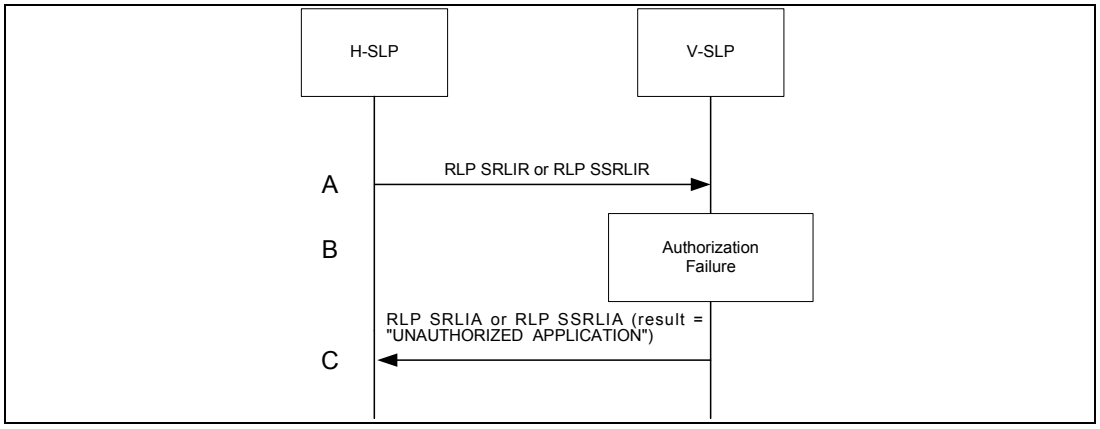

Figure 10: NW Initiated Authorization Failure V-SLP

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.

6.8.7.4 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 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.
- In case of the SUPL START message, the session-id is missing SET Session ID or contains SLP 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) 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

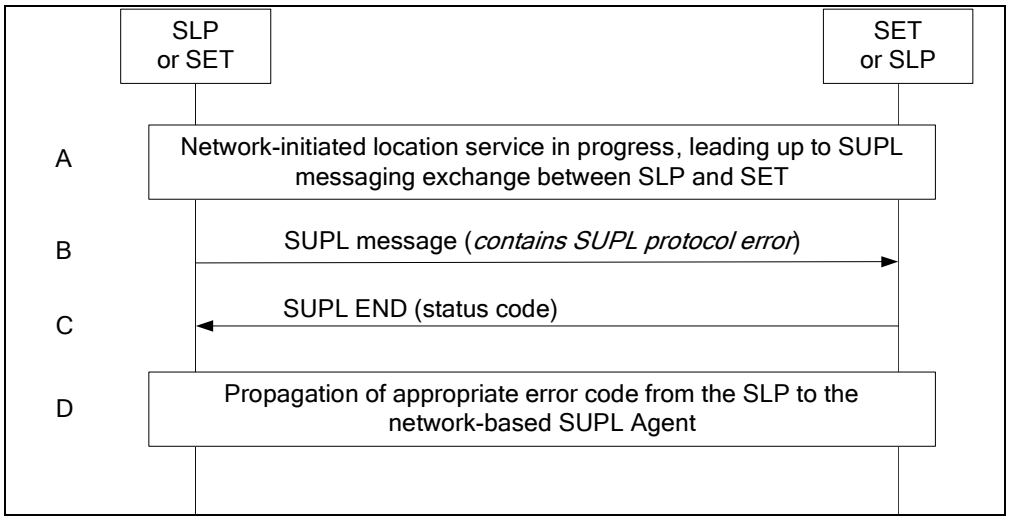

Figure 11: NW Initiated SUPL Protocol Error

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.

6.8.7.5 SUPL timer expiration

When either a SLP or a SET timer expires, the procedure described in section 8 shall be followed.

6.9 SUPL Collaboration SET Initiated

For SET Initiated applications, an SLP and SET SHALL support SUPL START, SUPL RESPONSE, SUPL POS INIT and SUPL END. The support for SUPL POS is OPTIONAL and positioning method dependent, e.g. required for A-GPS positioning.

The SET MAY reuse the secure IP connection of an already ongoing SUPL session between the SET and the H-SLP. If a SET is reusing a secure IP connection, no new IP connection is established and the Secure IP connection is not released as long as one or more SUPL sessions are using it.

6.9.1 Non-Roaming Successful Case - Proxy mode

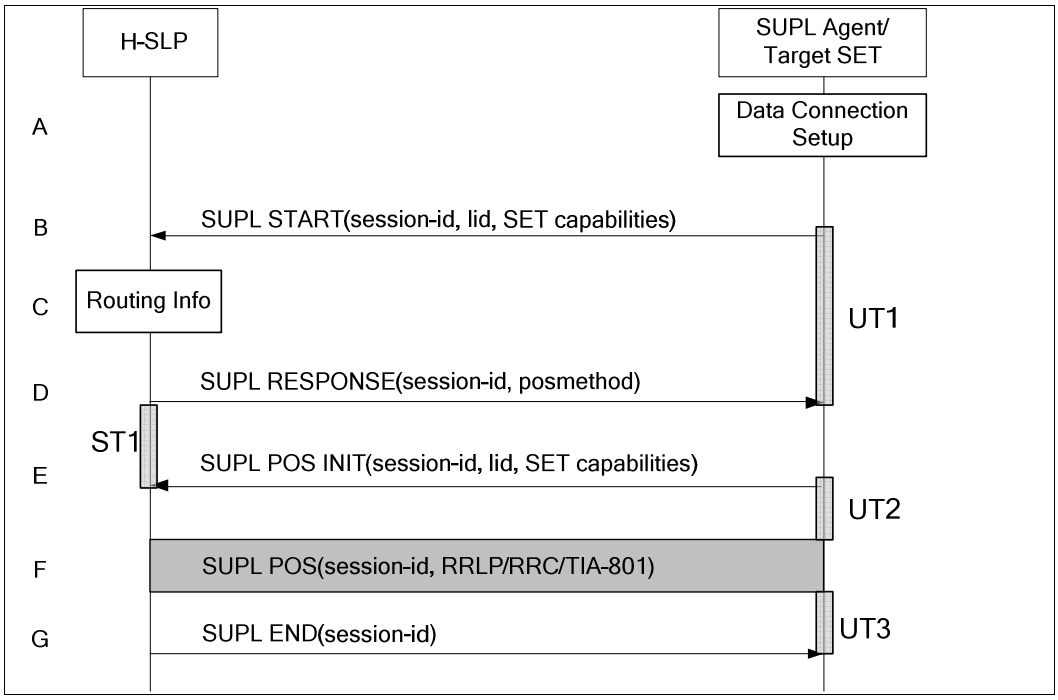

Figure 12: SET-Initiated Non-Roaming Successful Case - Proxy mode

(Note: See section 8 for timer descriptions.)

A. The SUPL Agent on the SET receives a request for position from an application running on the SET. If the SET is not already attached to Packet Data Network services it will attach itself or the SET establishes a circuit switched data 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 message to start a positioning session with the H-SLP. The SUPL START message contains session-id, SET capabilities and location identifier (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).

   If a previously computed position which meets the 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) 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 coarse position computed based on information received in the SUPL START message meets the requested QoP, the H-SLP SHALL 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 identifier (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). 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. 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 IP connection and release all resources related to this session. The H-SLP SHALL release all resources related to this session.

6.9.2 Non-Roaming Successful Case – Non-Proxy mode

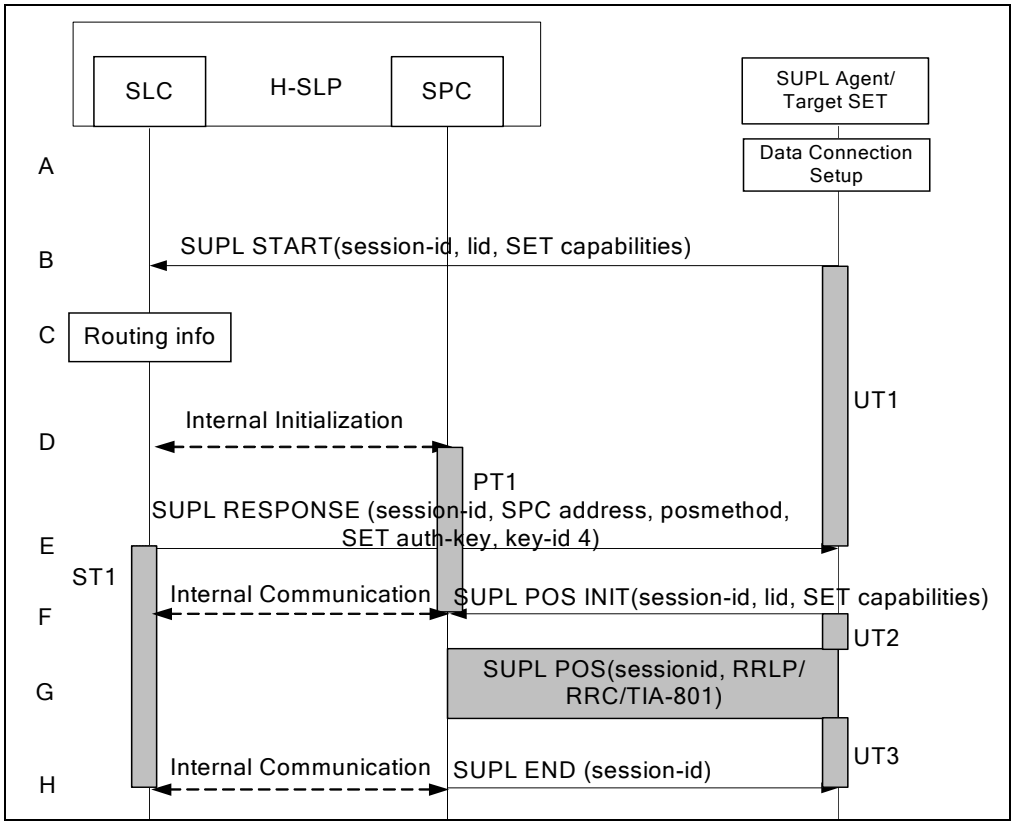

Figure 13: SET-Initiated Non-Roaming Successful Case – Non-Proxy mode

(Note: See section 8 for timer descriptions.)

A. The SUPL Agent on the SET receives a request for position from an application running on the SET. If the SET is not already attached to Packet Data Network services it will attach itself or the SET establishes a circuit switched data connection.

B. The SUPL Agent on the SET uses the address provisioned by the Home Network to establish a secure IP connection to the SLC and sends a SUPL START message to start a positioning session with the SLC. The SUPL START message contains session-id, SET capabilities and location identifier (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).

   If a previously computed position which meets the requested QoP is available at the SLC the SLC shall respond with a SUPL END message to the SET containing the position and end the SUPL session.

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. The SLC will inspect the SUPL START message and determine if the SET is allowed to directly access the SPC. The SLC generates a session id for the SUPL session and informs the SPC of an incoming SUPL POS session from a SET identified by the generated session-id. The SLC also generates a key to be used for mutual SPC/SET authentication. This key is also forwarded to the SPC. In collaboration the SLC and SPC determines the initial

location based on the lid received in the SUPL START message received from the SET.

Note: The specifics for the interface between the SLC and SPC are beyond the scope for SUPL 1.0 and are thus implementation dependent.

E. Consistent with the SUPL START message including posmethod(s) supported by the SET, the SLC SHALL determine the posmethod. If required for the posmethod, the SLC SHALL use the supported positioning protocol (e.g., RRLP, RRC, TIA-801) from the SUPL START message.

The H-SLP SHALL respond with a SUPL RESPONSE to the SET. The SUPL RESPONSE contains the session-id, the created key, and key id, to be used by the SET for mutual SPC/SET authentication, and the address of the SPC to indicate to the SET that a new secure IP connection SHALL be established. The SUPL RESPONSE also contains the posmethod. If, however, a coarse position computed based on information received in the SUPL START message meets the requested QoP, the SLC shall respond with a SUPL END message (instead of the SUPL RESPONSE) to the SET containing the position and end the SUPL session. The key-id 4 corresponds to PP2_SPC_Master_Key to generate PSK_SPC_Key which is used for PSK TLS session between the SPC and the SET.

F. To initiate the actual positioning session the SET opens a new secure IP connection to the SPC using the address indicated in step E. The SET and 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 IP connection is established the existing secure IP connection to the SLC is closed. The SUPL POS INIT message contains at least session-id, SET capabilities and location identifier (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). 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.

The SPC informs the SLC that the positioning procedure is started.

G. The SET and the SPC MAY exchange several successive positioning procedure messages.

The 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).

H. Once the position calculation is complete the 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 SPC MAY add the determined position to the SUPL END message. When the SUPL END is received the SET SHALL release the secure IP connection to the SPC and release all resources related to this session. The SPC informs the SLC that the positioning procedure is finished. The H-SLP SHALL release all resources related to this session.

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

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.

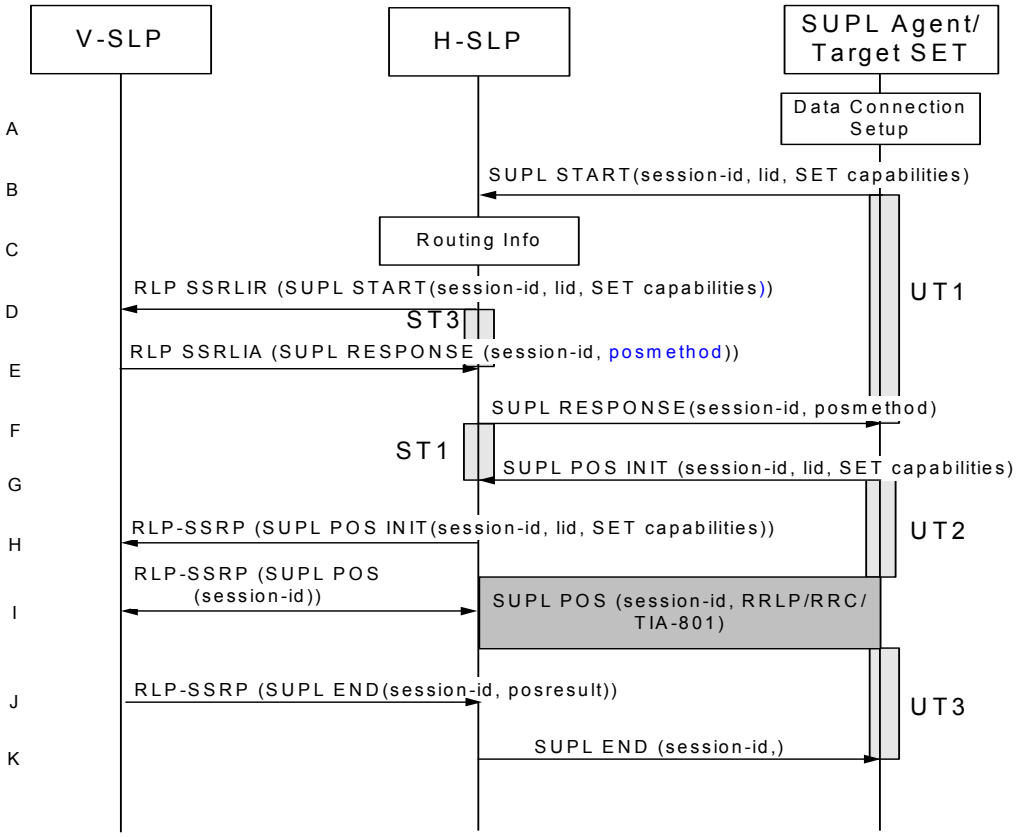

Figure 14: SET-Initiated Roaming Successful Case – Proxy mode with V-SLP

(Note: See section 8 for timer descriptions.)

A. The SUPL Agent on the SET receives a request for position from an application running on the SET. If the SET is not already attached to Packet Data Network services it will attach itself or the SET establishes a circuit switched data 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 message to start a positioning session with the H-SLP. The SUPL START message contains session-id, SET capabilities and location identifier (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).

   If a previously computed position which meets the 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) 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.

If a coarse position calculated based on information received in the RLP SSRLIR (SUPL START) message meets the requested QoP, the V-SLP SHALL send a RLP SSRLIA (SUPL END) message - as opposed to RLP SSRLIA (SUPL RESPONSE) - including the position estimate to the H-SLP. The H-SLP SHALL 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.

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 identifier (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). 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. 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 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 IP connection and release all resources related to this session. The H-SLP SHALL release all resources related to this session.

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

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

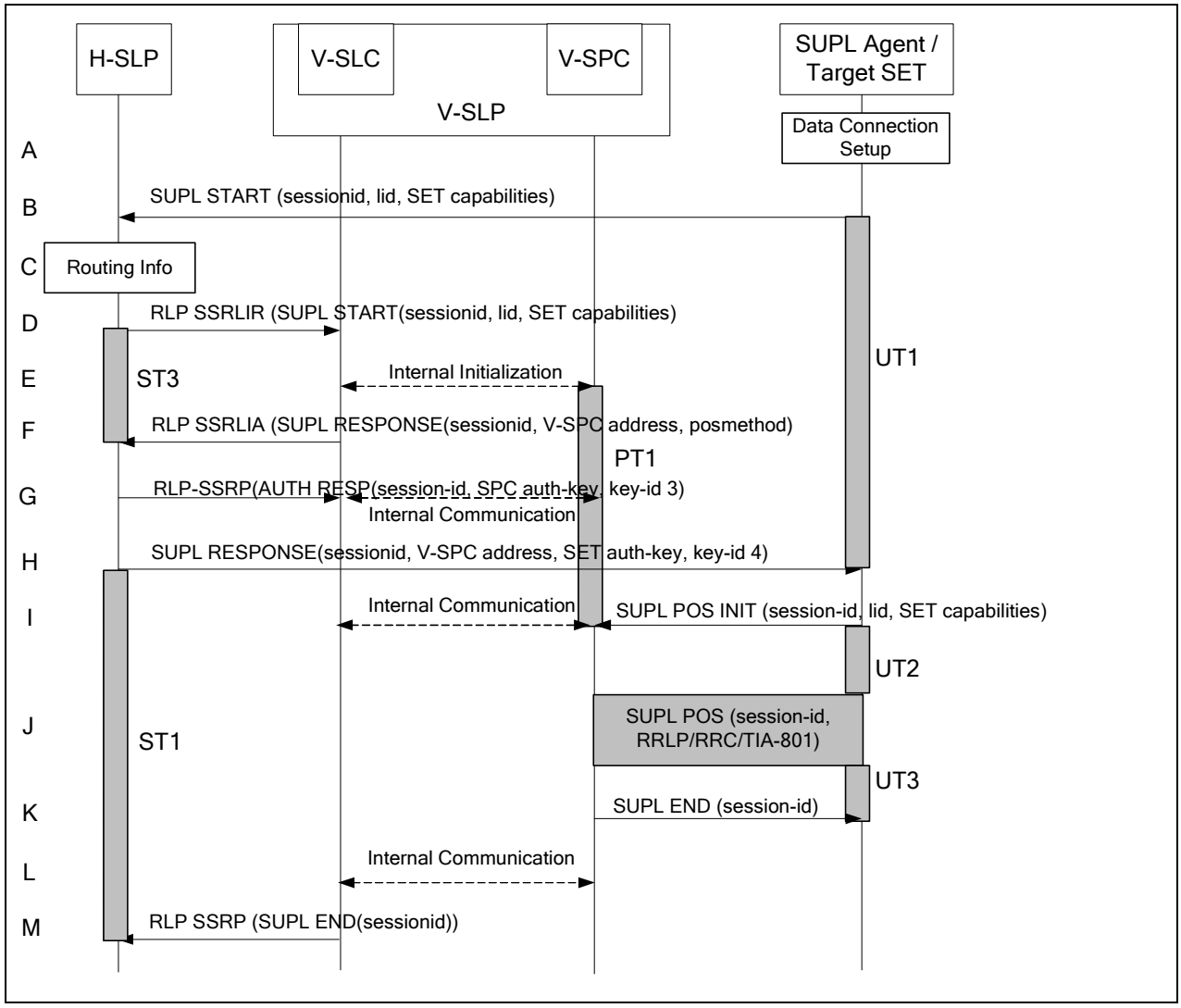

Figure 15: SET-Initiated Roaming Successful Case – Non-Proxy mode with V-SPC

(Note: See section 8 for timer descriptions.)

A. The SUPL Agent on the SET receives a request for position from an application running on the SET. If the SET is not already attached to Packet Data Network services it will attach itself or the SET establishes a circuit switched data connection.

B. The SUPL Agent on the SET uses the address provisioned by the Home Network to establish a secure IP 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 identifier (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).

If a previously computed position which meets the requested QoP is available at the H-SLP the H-SLP 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. However, there are various environment dependent mechanisms.

D. The H-SLP 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) from the SUPL START message.

The V-SLC 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 the V-SPC address. The SUPL RESPONSE also contains the posmethod.

If a coarse position calculated based on information received in the RLP SSRLIR (SUPL START) message meets the requested QoP, the V-SLC SHALL send a RLP SSRLIA (SUPL END) message - as opposed to RLP SSRLIA (SUPL RESPONSE) - including the position estimate to the H-SLP. The H-SLP SHALL 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 SHALL terminates the session.

G. The H-SLP generates a key as indicated by key-id 3 to be used for mutual V-SPC/SET authentication. The H-SLP forwards the key to the V-SLC through an RLP SSRP message. The key-id 3 corresponds to PSK_SPC_Key which is used for PSK-TLS session between the V-SPC and the SET.

The V-SLC forwards the key to the V-SPC through internal communication.

H. The H-SLP forwards the SUPL RESPONSE to the SET. The SUPL RESPONSE contains at least session-id, the created key, posmethod and key-id 4, 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 IP connection SHALL be established. The key-id 4 corresponds to PSK_SPC_Key which is used for PSK-TLS session between the V-SPC and the SET.

I. To initiate the actual positioning session the SET opens a new secure IP 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 IP connection is established the existing secure IP connection to the H-SLP is closed. The SUPL POS INIT message contains at least session-id, SET capabilities and location identifier (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). 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.

The V-SPC informs the V-SLC that the positioning procedure is started.

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 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 IP 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 and V-SLC SHALL release all resources related to this session.

M. The V-SLC sends a RLP SSRP to the H-SLP to inform about the end of the SUPL session. The H-SLP SHALL release all resources related to this session.

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

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

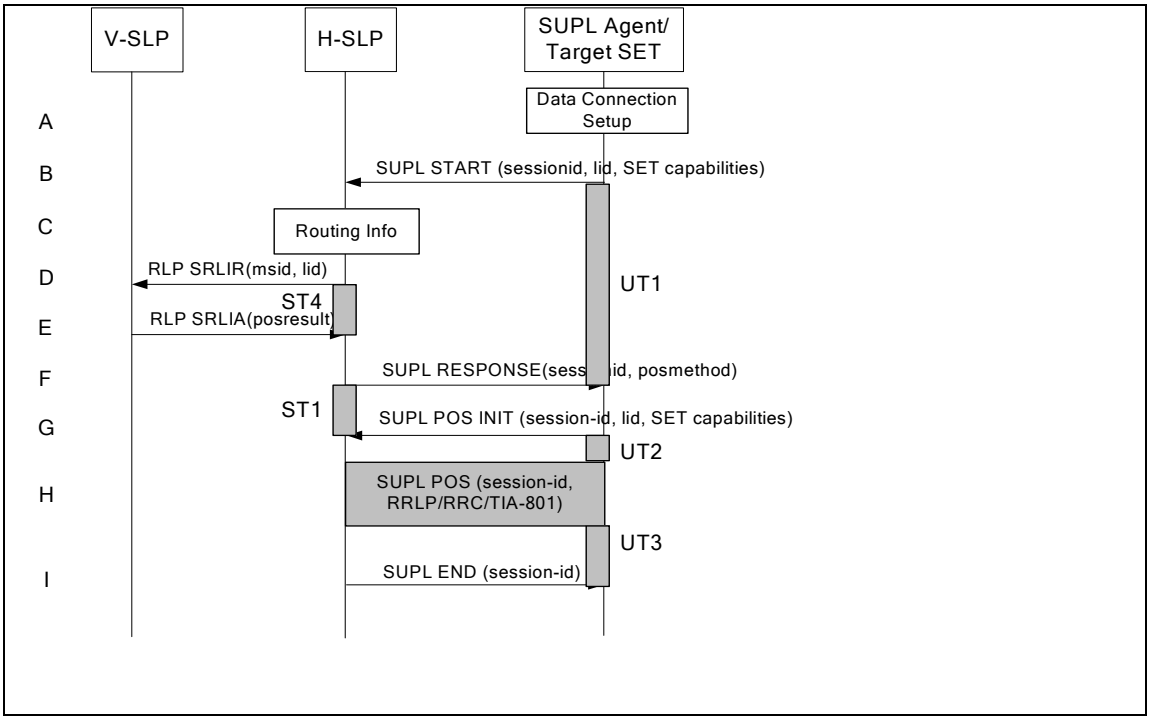

Figure 16: SET-Initiated Roaming Successful Case – Proxy mode with H-SLP

(Note: See section 8 for timer descriptions.)

A. The SUPL Agent on the SET receives a request for position from an application running on the SET. If the SET is not already attached to Packet Data Network services it will attach itself or the SET establishes a circuit switched data 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 message to start a positioning session with the H-SLP. The SUPL START message contains session-id, SET capabilities and location identifier (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).

If a previously computed position which meets the 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 identifier (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 proceeds directly 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) 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.

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 identifier (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). 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 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 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 IP connection and release all resources related to this session. The H-SLP SHALL release all resources related to this session.

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

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

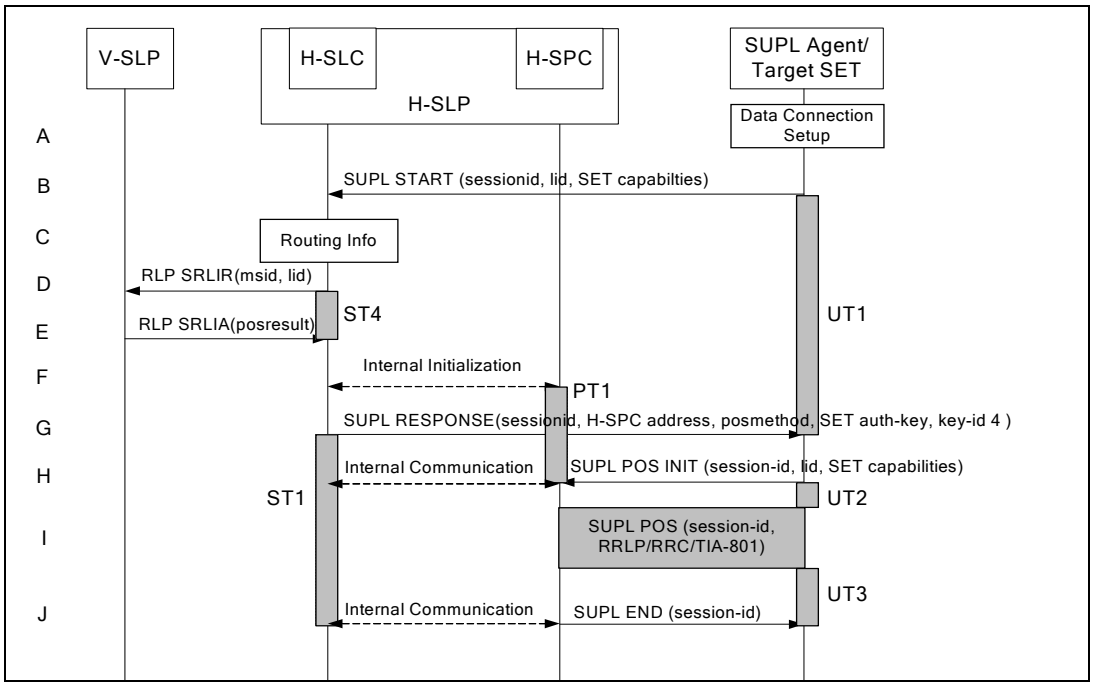

Figure 17: SET-Initiated Roaming Successful Case – Non-Proxy mode with H-SPC

(Note: See section 8 for timer descriptions.)

A. The SUPL Agent on the SET receives a request for position from an application running on the SET. If the SET is not already attached to Packet Data Network services it will attach itself or the SET establishes a circuit switched data connection.

B. The SUPL Agent on the SET uses the address provisioned by the Home Network to establish a secure IP 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 identifier (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).

   If a previously computed position which meets the 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 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-SPC. The RLP request contains at least the msid and the location identifier (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 coarse position received from the V-SLP meets the requested QoP the H-SLC SHALL send a SUPL END to the SET carrying the sessionid and the position result and SHALL 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 a key to be used for mutual SPC/SET authentication. This key is also forwarded to the H-SPC. The H-SLC also informs the H-SPC of the coarse position obtained from the V-SLP.

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) from the SUPL START message.

   The H-SLC responds with the SUPL RESPONSE to the SET. The SUPL RESPONSE contains the session-id, the created key, and key-id 4, 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 key-id 4 corresponds to PSK_SPC_Key which is used for PSK-TLS session between the H-SPC and the SET.

H. To initiate the actual positioning session the SET opens a new secure IP 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 IP connection is established the existing secure IP connection to the H-SLC is closed. The SUPL POS INIT message contains at least session-id, SET capabilities and location identifier (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). 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.

   The H-SPC informs the H-SLC that the positioning procedure is started.

I. 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).

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 IP 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.

6.9.7 Exception Procedures

6.9.7.1 SET Authorization Failure

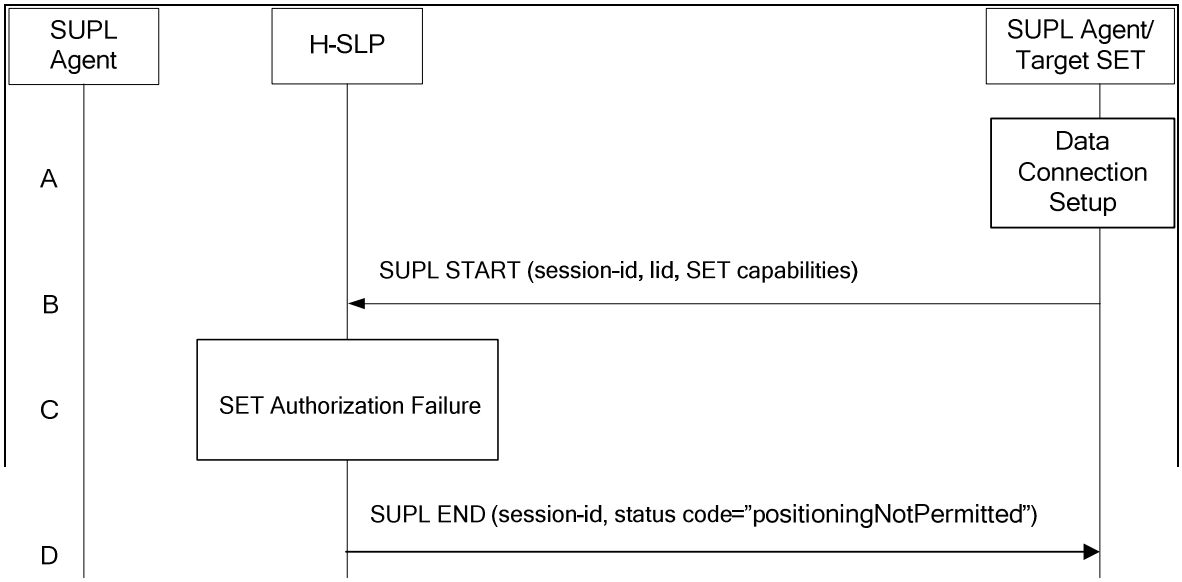

Figure 18: SET-Initiated Error SET Authorization Failure

A. The SUPL Agent on the SET receives a request for position from an application running on the SET. If the SET is not already attached to Packet Data Network services it will attach itself or the SET establishes a circuit switched data 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 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.

6.9.7.2 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) 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

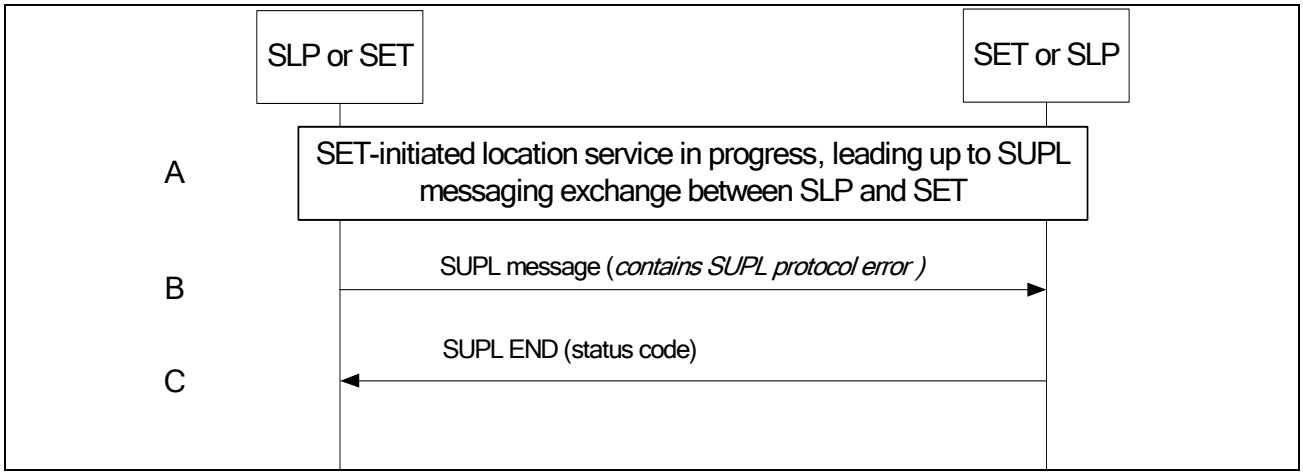

Figure 19: SET-Initiated Error SUPL Protocol Error

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.

6.9.7.3 SUPL timer expiration

When either a SLP or a SET timer expires, the procedure described in section 8 shall be followed.

7. SUPL Security Function (SSF)

IMPORTANT NOTE: SUPL 1.0 does not provide any mandatory Denial of Service (DoS) protection mechanism. Implementers of SUPL 1.0 MUST consider the Denial of Service requirements of a location service before realizing it with SUPL 1.0.

7.1 SUPL Authentication Model

Mutual authentication SHALL be supported between a SET and an 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, which in turn are provisioned by the SUPL Service Provider.

Note that a successful authentication of the SET User MUST result in a successful identification of SET User's ID (e.g., MSISDN).

7.1.1 PSK-TLS Authentication

This mode requires mutual authentication between SET and H-SLP. For improved security and interoperability SETs and SLPs SHOULD perform Proxy Mode authentication with PSK-TLS with the following clarifications:

3GPP compliant SETs and SLPs SHOULD perform PSK-TLS with the GBA [3GPP 33.220] as described in TS 33.222 with relevant key management mechanisms (Refer to Section 7.1.2).

3GPP2 compliant SETs and SLPs SHOULD perform PSK-TLS with the following clarifications:

- Key Identifiers used in PSK-TLS MUST be in the form of RAND@SLP where SLP is in the FQDN format and RAND is a 128bits number. The following Key Identifiers are defined for SUPL 1.0:
  - RAND3@SPC MUST correspond to PSK_SPC_Key to be used for serving (Home or Visited) SPC authentication for Non-Proxy mode operations.
  - RAND1@H-SLP MUST correspond to PSK_H-SLP_Master_Key to be used for H-SLP authentication for Proxy mode operations.
  - RAND1 and RAND3 MUST be 128bits long. PSK_H-SLP_Master_Key and PSK_SPC_Key MUST be either 128bits or 256bits long. Key Hints used in the PSK-TLS protocol MUST be set to "3GPP2 SUPL 1.0 Keys"

Note that an 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 7.1.2.

7.1.2 Key Management for SUPL Authentication

The SUPL Authentication model requires shared secret keys between the H-SLP and the SET, bound to a removable token such as a R-UIM/UICC(SIM/USIM).

7.1.2.1 3GPP Deployments

In the case of 3GPP deployments supporting 3GPP GBA [3GPP 33.220], the shared keys are established as follows:

- SETs and SLPs MUST derive a shared secret key and operate according to GBA [3GPP 33.220]. The NAF MUST have well defined domain name SLP_Address_FQDN designating the H-SLP, e.g., slp.operator.com.
- For MAC protection of SUPL INIT keys are derived according to GBA [3GPP 33.220]. The NAF performing this operation MUST have a secondary FQDN with the word "mac" prefixed to the well defined domain name, e.g., slp.operator.comas FQDN and mac.slp.operator.com as the secondary SLP address. Implementations

MUST ensure that both FQDNs (well defined and prefixed) point to the same SLP. The MAC_KeyID of the MAC_KEY included in the SUPL INIT message MUST be the B-TID of the Ks from which the Ks_NAF is generated.

- The SET MUST ensure that it is always provisioned with a valid Ks_NAF. If no valid Ks_NAF is present then the SET MUST initiate the GBA procedure to provision Ks_NAF. A new Ks_NAF MUST be established each time a new UICC (USIM/SIM) 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.

7.1.2.2 3GPP2 Deployments

In the case of 3GPP2 deployments the SUPL authentication model assumes shared secret keys between the H-SLP and the SET, bound where applicable to an R-UIM.

- PSK_H-SLP_Master_Key, PP2_SPC_Master_Key, MAC_Master_Key and their corresponding identifiers (RAND1, RAND2, MAC_KEYID) MUST be provisioned by the SLP provider in the UIM/R-UIM.
- For Non-Proxy mode SET initiated SUPL call flows PSK_SPC_Key and RAND3 are randomly generated by the H-SLP and delivered to the SET using the SUPL RESPONSE Message. The H-SLP also forwards the PSK_SPC_Key to the serving SPC in an RLP message where appropriate. Note that the key identifier for PSK_SPC_Key MUST be constructed in the SET in the form of RAND3@SPC.
- For Non-Proxy mode Network Initiated SUPL call flows the SET generates a nonce (SET_NONCE) and derives the corresponding PSK_SPC_Key as an HMAC-SHA2-256 [HMAC] as follows:
  - PSK_SPC_Key= H(PP2_SPC_Master_Key XOR opad, H(PP2_SPC_Master_Key XOR ipad, SPC ||SET_NONCE||VER)) where H is defined as SHA-1. The output of the SHA-1 HASH function MUST be truncated to 128 bits, i.e., the HMAC MUST be implemented as HMAC-SHA-1-128.
  - RAND3=SET_NONCE

In order to enable the corresponding PSK_SPC_Key derivation in the H-SLP, the SET includes the RAND3 field in the Authentication REQ message. Upon receipt of this message the H-SLP derives the PSK_SPC_Key using the same HMAC as described above and forwards the key to the serving SPC in an RLP message where appropriate.

Key-id mapping between the SLP and the R-UIM/UICC(SIM/USIM) is as follows:

Key-id in Section 6.8 and 6.9	Format of Key-id	Key	Description
Key-id	MAC_KEYID@SLP	PSK_MAC_Master_Key	MAC key established between the (H-)SLP and the SET
Key-id 2	RAND2@SPC	PP2_SPC_Master_Key	Master key of the PSK-TLS session key established between the (V- or H-)SPC and the SET
Key-id 3	RAND3@SPC	PSK_SPC_Key	PSK-TLS session key established between the (V-)SPC and the SET which is used by the (V-)SPC
Key-id 4	RAND3@SPC	PSK_SPC_Key	PSK-TLS session key established between the (V-)SPC and the SET which is used by the SET

7.1.3 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. A SUPL INIT message contains a parameter called SLP Mode that specifies the mode of SUPL operation to the SET. SLP Mode can be set to indicate Proxy or Non-Proxy mode SUPL operation.

SETs MUST always read the SLP Mode parameter first when they are processing a SUPL INIT message. If the SLP Mode is set to a mode that is not supported by the SET, the SET MUST terminate the SUPL session after sending the appropriate SUPL error code in a SUPL END message:

- In the case where a SET supports only proxy mode and non-proxy mode is required in SUPL INIT, the SET MUST send a SUPL END to H-SLP with error code nonProxyModeNotSupported.
- In the case where a SET supports only non-proxy mode and proxy mode is required in SUPL INIT, the SET MUST send a SUPL END to the H-SLP with error code proxyModeNotSupported.

SUPL INIT protection may be explicit or the verification of the contents may take place implicitly by agreeing or by using a hash of SUPL INIT in a key derivation mechanism. In order to ensure that SUPL INIT messages are authentic, i.e., originated from the H-SLP and not re-played the following security mechanisms (Sections 7.1.3.1 and 7.1.3.2) are defined.

7.1.3.1 Authentication of the SUPL INIT Message

Proxy mode network verification of the integrity of the SUPL INIT message is always performed by the H-SLP. The SUPL POS INIT message MUST contain a verification field (VER), which is an HMAC of the complete SUPL INIT message. When the H-SLP receives the SUPL POS INIT message it MUST check the received VER field against the corresponding value calculated over the transmitted SUPL INIT message. If this verification fails the Home SLP MUST terminate the session with the SUPL END message which contains status code ‘authSuplinitFailure’.

HMAC for the verification field MUST be calculated as follows:

VER=H(H-SLP XOR opad, H(H-SLP XOR ipad, SUPL INIT))

where H-SLP is the FQDN of the H-SLP address configured in the SET. Note that the H-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. SHA-1 MUST be used as the hash (H) function in the HMAC. The output of the HMAC function MUST be truncated to 64 bits, i.e., the HMAC MUST be implemented as HMAC-SHA1-64 [HMAC].

For **Non-Proxy mode** operations network verification of the integrity of the SUPL INIT message is always performed by the H-SLP. When the H-SLP receives the SUPL AUTH REQ, it MUST check the received “SLP Session Id” fields against the expected values. If this verification fails the H-SLP MUST drop the session with the SUPL END message which contains status code ‘authSuplinitFailure'.

For **3GPP** SET based integrity verification and message origin authentication of SUPL INIT messages, SLPs MAY include a cryptographic MAC in the SUPL INIT message. 3GPP SUPL 1.0 SETs MUST recognize the presence of the MAC field but SETs MUST not verify the MAC field even if it is included in the SUPL INIT message. The SLPs MUST check if a current MAC_KEY exists between the SET and the SLP before including a MAC and associated KeyID into the SUPL INIT messages. In cases where no KeyID and corresponding MAC_KEY is found the MAC field MUST NOT be populated.

For **3GPP2** SET based integrity verification and message origin authentication of SUPL INIT messages, SLPs MUST include a cryptographic MAC to authenticate the data in the SUPL INIT message. 3GPP2 SUPL 1.0 SETs MUST verify the MAC field if it is present (populated) in the SUPL INIT message sent by an SLP using the MAC_KEY provisioned in the SET. The correct MAC_Master_Key is found using the MAC_KeyID field in the SUPL INIT message. If MAC verification fails, the SET MUST silently discard the SUPL INIT message. If the MAC verification succeeds the SET considers the SUPL INIT authentic and continues with the rest of the SUPL call flows.

The MAC field MUST be calculated as HMAC-SHA1-64 [HMAC] as:

MAC=H(MAC_KEY XOR opad, H(MAC_KEY XOR ipad, SUPL_INIT’)) where SUPL_INIT’ consists of those fields of SUPL_INIT without the MAC appended.

7.1.3.2 Re-Play protection of SUPL INIT Message

For **Proxy** mode Network Initiated cases, protection against re-play attacks MUST be provided by the H-SLPs. SLPs MUST ensure that no SUPL POS INIT messages are accepted from an authenticated SET unless a previous SUPL INIT message has been sent with an “SLP Session Id” that corresponds to the one received inside the SUPL POS INIT message.

Implementations MUST ensure that an "SLP Session Id" is correctly associated with the SET User ID (e.g., MSISDN) that has been authenticated.

If the SET User authentication is performed using Alternative Client Authentication method described in this document then a mapping between the source IP address of the SUPL POS INIT and the MSISDN of the SET User is already established and this MSISDN MUST be used as the authenticated MSISDN. Discarding of an erroneous SUPL POS INIT MUST NOT generate a chargeable event for the SET.

For **Non-Proxy** Network Initiated cases protection against re-play attacks MUST be provided by the H-SLP. H-SLPs MUST ensure that no SUPL AUTH REQ messages are accepted from a SET unless an active (not expired) "SLP Session Id" exists that corresponds to the one received inside the SUPL AUTH REQ message. Discarding of an erroneous SUPL AUTH REQ MUST NOT generate a chargeable event for the SET. H-SLPs MUST only create a chargeable event after receiving the confirmation from the SPC for the successful completion of the SUPL positioning.

7.1.4 Alternative Client Authentication Mechanisms

For 3GPP SUPL implementations where GBA with PSK-TLS [3GPP 33.222] IS NOT supported either in the SET or in the SLP an MSISDN/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 the Alternative Client Authentication mechanism. It is recommended for SLPs to implement the PSK-TLS with GBA as well as the Alternative Client Authentication Mechanism.

SETs that support Alternative Client Authentication MUST also support TLS 1.0 for certificate based server (SLP) authentication. In addition, the SET MUST be provisioned with a root certificate of the SLP 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 1.0 is used for Alternative Client Authentication the relevant SLP root certificates exist in the SET.

SLPs that support Alternative Client Authentication MUST support TLS 1.0 and MUST have a TLS Server Certificate, which can be verified by the SETs that implement Alternative Client Authentication.

There could be cases where SETs and SLPs MAY support both PSK-TLS with GBA and the Alternative Client Authentication mechanism. There could also be cases where SLPs and SETs support ONLY one type of Client Authentication mechanism. In cases where SLPs and SETs do not implement the same authentication mechanism the SUPL Authentication will fail.

If a SET indicates its support for PSK-TLS/GBA [3GPP 33.222] to the H-SLP inside a TLS session and the H-SLP supports PSK-TLS/GBA then the H-SLP MUST always perform the PSK-TLS with GBA mechanism even if the H-SLP supports the Alternative Client Authentication mechanism as well. An H-SLP supporting the Alternative Client Authentication mechanism MUST only perform this form of authentication if the SET does not indicate any support for PSK-TLS with GBA inside a TLS session.

If a SET supports both the Alternative Client Authentication and the GBA/PSK-TLS mechanism it MUST always indicate its support for GBA/PSK-TLS to the H-SET by using the mechanisms defined in [3GPP 33.222]. A SET that supports both mechanisms MUST indicate to the H-SLP that it also supports Alternative Client Authentication mechanism by selecting TLS 1.0 only cipher suites as well as PSK-TLS specific cipher suites inside the TLS negotiation.

This version of SUPL only describes a mechanism where the H-SLP can check the binding of the SET's IP address to the MSISDN assigned to the SET. An example implementation of a similar scheme is described in the relevant 3GPP specifications [3GPP 33.978].

If a Client Authentication based on MSISDN to IP Address Mapping is implemented the H-SLP MUST be able to map the source IP address of a SUPL message received from the SET to the MSISDN used by the H-SLP to address the SET. In order to use client authentication based on IP address to MSISDN mapping the bearer network MUST prevent IP Address Spoofing at the bearer level. A successful mapping between the source IP address and the SET's MSISDN would imply that the SET is securely identified, i.e., authenticated. 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 MSISDN from the 3GPP bearer. Sections 7.1.4.1 and 7.1.4.2 describe how this mechanism is used for client authentication in SUPL.

7.1.4.1 Network-Initiated Scenario

H-SLP sends a SUPL INIT message to the SET storing the MSISDN of the SET internally. SUPL INIT message contains a parameter called SLP Mode**,** which specifies the mode of SUPL operation to the SET. SLP Mode can be set to indicate Proxy or Non-Proxy mode SUPL operation.

SETs MUST always read the SLP Mode parameter first when they are processing the SUPL INIT messages. SETs that support only Alternative Authentication Methods MUST only accept SUPL INIT messages where the SLP mode is set to Proxy mode.

The SET MUST establish a TLS 1.0 session with the H-SLP. The SET MUST check that the TLS server certificate presented by the H-SLP is bound to the FQDN (Fully Qualified Domain Name) of the H-SLP configured in the SET. When H-SLP receives the first SUPL Message (SUPL POS INIT), it must enquire the underlying bearer network to find out the current assigned IP address of the MSISDN belonging to the SET. The H-SLP then MUST check that the source IP address of the SUPL POS INIT message matches the one that it expects based on the MSISDN record it had stored before. If the source IP address of the SUPL POS INIT matches the one acquired from the bearer network then the SET is considered authentic and H-SLP continues with the SUPL session. If a match cannot be found then H-SLP MUST terminate the SUPL session with the relevant SUPL error messages. H-SLP MUST ensure that within a given SUPL Session source IP address of the SET MUST NOT change. If a change is detected the H-SLP MUST terminate the SUPL Session with the relevant SUPL error messages.

7.1.4.2 SET-Initiated Scenario

In the SET initiated SUPL scenarios the SET MUST establish a TLS 1.0 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. When the H-SLP receives the first SUPL Message (SUPL START), it MUST enquire the underlying bearer network to find out the current MSISDN using the source IP address used by the SET. The H-SLP then MUST record this MSISDN to identify the SET for authentication purposes. If a valid MSISDN is returned from the bearer for the source IP address of the SUPL START message then the SET is considered authentic and the H-SLP continues with the SUPL session. If a valid MSISDN cannot be found then H-SLP MUST terminate the SUPL session with the relevant SUPL error messages. The H-SLP MUST ensure that within a given SUPL Session the source IP address of the SET MUST NOT change. If a change is detected the H-SLP MUST terminate the SUPL Session with the relevant SUPL error message.

7.2 Authorization in SUPL

Authorization in nNon-Proxy mode is provided implicitly by using a derived authentication key (PSK_SPC_Key) with the serving SPC. Details of the key derivation can be found in Section 7.1.2.

Authorization in Proxy mode is provided by the provisioning of the H-SLP address in the UICC, SET or a default H-SLP address 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.

7.2.1 3GPP2 based deployments

For 3GPP2 based deployments the H-SLP address MUST be securely provisioned in the UIM or R-UIM.

7.2.2 3GPP based deployments

For 3GPP based deployments the 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 7.1.4, 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 7.1.1.

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 [TS 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 the 3GPP TS 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 TS 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 20 illustrates the flow diagram for the H-SLP address storage.

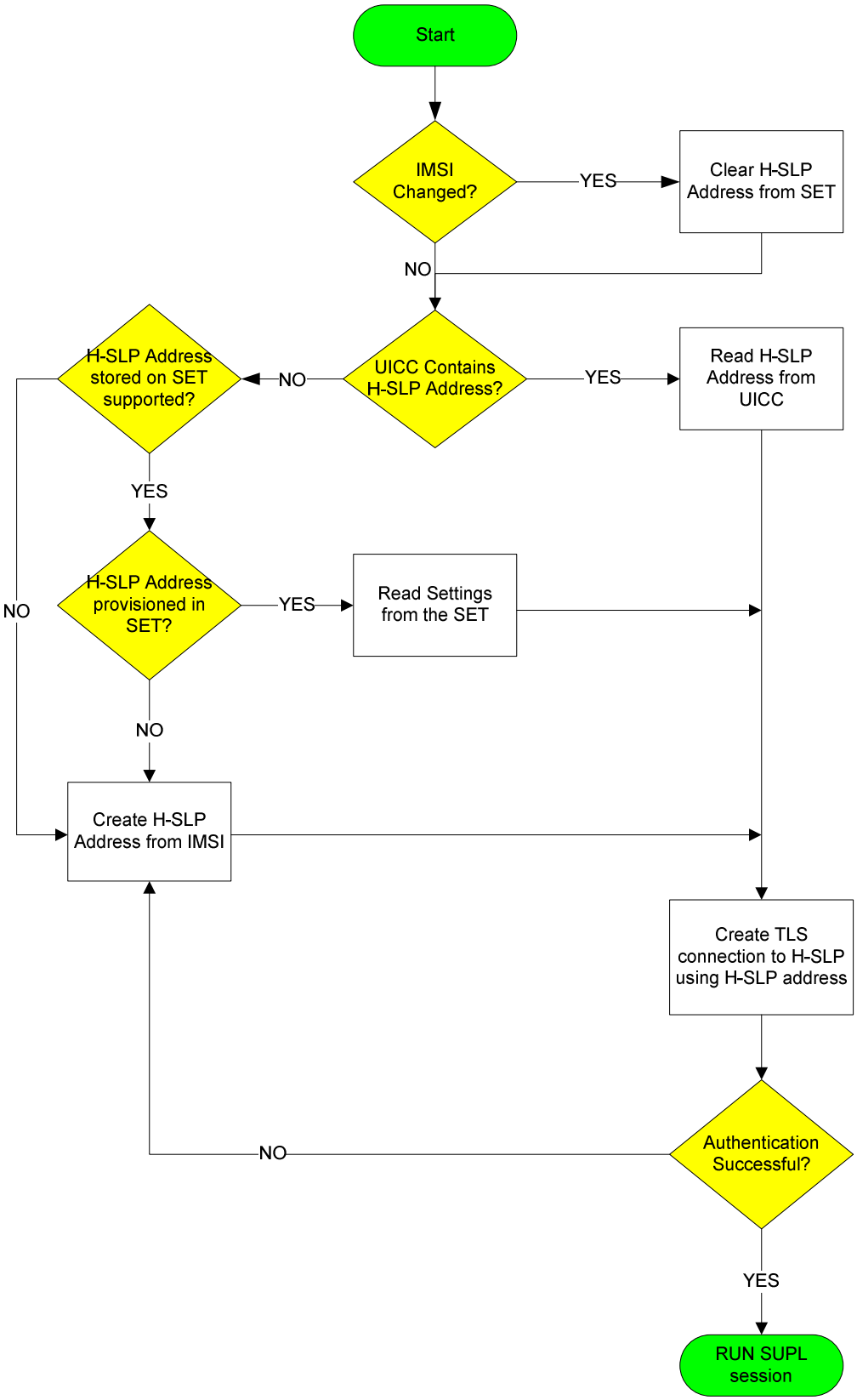

Figure 20: H-SLP address storage flow diagram

7.3 Confidentiality and Data Integrity

TLS [TLS] or PSK-TLS [PSK-TLS] SHALL be used to provide Confidentiality and Data Integrity between a SET and an SLP. All SUPL Messages except “Authentication REQ”, “Authentication RESPONSE”, and “SUPL INIT” MUST be delivered within a TLS or PSK-TLS session between a SET and an SLP.

The TLS implementation shall conform to RFC 2246 [TLS] and WAP Profile of TLS [WAP TLS] with the following clarifications:

SETs SHALL implement:

- TLS_RSA_WITH_AES_128_CBC_SHA [TLS-AES].

For SET implementations that prefer additional cipher suites SETs SHOULD implement:

- TLS_RSA_WITH_3DES_EDE_CBC_SHA.

The following cipher suites SHALL be implemented by SLPs:

- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA [TLS-AES].

For SLP implementations that prefer to support NULL encryption SLPs 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 SHALL be supported by SLPs and SETs.

PSK-TLS implementations SHALL conform to PSK-TLS [PSK-TLS]

SETs SHALL implement:

- TLS_PSK_WITH_AES_128_CBC_SHA [PSK-TLS].

For SET implementations that prefer additional cipher suites SETs SHOULD implement:

- TLS_PSK_WITH_3DES_EDE_CBC_SHA [PSK-TLS].

The following cipher suites SHALL be implemented by SLPs:

- TLS_PSK_WITH_AES_128_CBC_SHA [PSK-TLS].

For SLP implementations that prefer additional cipher suites SLPs SHOULD implement:

- TLS_PSK_WITH_3DES_EDE_CBC_SHA [PSK-TLS].

8. Timers

This Section defines the SUPL timers. Note that default timer value is informative.

Table 5: SET timer values

Timer	Default value (sec.)	Description	Actions on expiration
UT1	10	From sending of SUPL START to receipt of SUPL RESPONSE	• Send SUPL END to SLP • Clear session resources at SET
UT2	10	From sending of SUPL POS INIT to receipt of first SUPL POS message. UT2 is not needed if the SUPL POS INIT message contains the first SUPL POS element (SET initiated TIA-801). For cell id based scenarios, the UT2 will be reset by the SUPL END message. The SUPL END message is sent from the SLP to the SET after the SET sent a SUPL POS INIT message containing the lid to the SLP.	• Send SUPL END to SLP • Clear session resources at SET
UT3	10	From sending of last SUPL POS message to receipt of SUPL END. In cases where there is no SUPL POS message sent from SET, timer UT3 is not needed at all.	• Send SUPL END to SLP • Clear session resources at SET
UT4	10	Only applicable to non-proxy. From sending of SUPL AUTH REQ to receipt of SUPL AUTH RESP message.	• Send SUPL END to SLP • Clear session resources at SET

Table 6: SLP 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 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 proxy: • Send SUPL END to SET • Clear session resources at SLP • 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	For proxy mode: from sending of SUPL INIT to receipt of SUPL POS INIT. For non-proxy mode: from sending SUPL INIT to (a) receipt of notification (internal communitation between SPC and SLC) that SUPL POS INIT has been received or (b) receipt of RLP-SSRP(SUPL END) from V-SLP.	For non-roaming scenario: • Send MLP-SLIA to SUPL agent For roaming scenario: • Send RLP-SRLIA to R-SLP For proxy: • Clear session resources at SLP For non-proxy: • Clear session resources at

Timer	Default value (sec.)	Description	Actions on expiration
			SLC
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

Table 7: SPC timer values

Timer	Default value (sec.)	Description	Actions on expiration
PT1	10+ (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 8: RLP timer values

Timer	Default value (sec.)	Description	Actions on expiration
RT1	10+ (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.

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
OMA-AD-SUPL-V1_0	N15 Jun 2007	No prior version