
# Enabler Test Requirements for SUPL 3.0

Candidate Version 3.0 – 20 Sep 2011

**Open Mobile Alliance**

OMA-ETR-SUPL-V3_0-20110920-C

# Contents

# 1. Scope

The Enabler Test Requirements (ETR) document for the SUPL Enabler is created and maintained by the OMA-LOC Technical Working Group.

The ETR document is intended to cover at least those requirements collected in the Requirements Document (RD) and the Architecture Document (AD) in addition to any other items the OMA-LOC Working Group has identified as important enough to warrant attention from interoperability perspective and identify any technical functionalities that should be covered by testing. Specifically the OMA-TS-ULP-V3_0 [OMA-ULP], OMA-TS-ILP-V3_0 [OMA-ILP], and OMA-ERELD-SUPL-V3_0 are considered to be of relevance in that respect.

# 2. References

## 2.1 Normative References


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

**[OMA-RLP]** "Inter-Location Server Interface Specification", Version 1.1, Open Mobile Alliance™, OMA-TS-RLP-Spec-V1.1, URL:http://www.openmobilealliance.org/

**[OMA-ULP]** "UserPlane for Location Protocol", Version 3.0, Open Mobile Alliance™, OMA-TS-ULP-Spec-V3.0, URL:http://www.openmobilealliance.org/

**[OMA-ILP]** "Internal Location Protocol", Version 3.1, Open Mobile Alliance™, OMA-TS-ILP-Spec-V3.0, URL:http://www.openmobilealliance.org/


## 2.2 Informative References

# 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

| | |
|---|---|
| **Test Fest** | Multi-lateral interoperability testing event |
| **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 contains the initial Target SET User Notification and Confirmation Privacy rules. |

## 3.3 Abbreviations

| | |
|---|---|
| **ACA** | Alternative Client authentication |
| **AD** | Architecture Document |
| **D-SLP** | Discovered SLP |
| **E-SLP** | Emergency SLP |
| **H-SLP** | Home SLP |
| **MLP** | Mobile Location Protocol |
| **MLS** | Mobile Location Service |
| **OMA** | Open Mobile Alliance |
| **QoP** | Quality of Position |
| **RD** | Requirements Document |
| **RLP** | Roaming Location Protocol |
| **SEK** | SUPL Encryption Key |
| **SET** | SUPL Enabled Terminal |
| **SLC** | SUPL Location Center |
| **SLP** | SUPL Location Platform |
| **SPC** | SUPL Positioning Center |
| **V-SLP** | Visited SLP |
| **V-SPC** | Visited SPC |

# 4. Introduction

The purpose of this Enabler Test Requirements document is to help guide the testing effort for the Enabler SUPL V3.0, documenting those areas where testing is most important to ensure interoperability of implementations.

The Enabler under consideration comprises the following specifications:

- OMA-SUPL V3.0: Secure User Plane Location
  - OMA-RD-SUPL-V3_0
  - OMA-AD-SUPL-V3_0
  - OMA-TS-ULP-V3_0
  - OMA-TS-ILP-V3_0
  - OMA-TS-SUPL-MO-V3_0

Generally, the testing activity aims at validating the normal working behaviour of the client/server interactions, as well as testing the error conditions whenever it is possible to set up the appropriate scenarios. The following sections provide a more detailed description of the testing requirements for SUPL V3.0.

This document also intends to provide some guidance on the prioritization of the specifications and features to be tested within Enabler SUPL V3.0

# 5. Test Requirements

Enabler SUPL V3.0 is intended to provide secure positioning over IP networks between a SET and an SLP. In principle any positioning method may be supported over any IP network.

Roaming between SUPL providers is facilitated by RLP V1.1 [OMA-RLP], which is part of the OMA - MLS enabler.

## 5.1 Enabler test requirements

The test requirements collected in this section are related to the Enabler SUPL V3.0.

In this section, it should be defined what specific functionalities of this Enabler shall or should be tested to ensure adequate operational of the implementations, including any security requirements and constraints on usage if specified (e.g. user can forward a media object but can not visualize it). That means that devices (clients/serves) shall do what they have to do and they shall not do what they are not allowed to do. Both types of test requirements (positive and negative testing) should be included here if so required.

Besides this information, OMA Architecture specifies a “Framework Architecture”, consisting of a set of common functions that need to be invoked in most use cases involving the different Service Enablers. The functionality requirements defined in the OMA Framework Architecture, i.e. authentication, authorization, charging, billing, common directory, etc. should also be listed in this table. Use cases are the main input to identify test requirements.

The following test requirements should cover both Conformance test requirements (i.e. functionality to be tested to verify whether it is implemented either in the client side or in the server side) and Interoperability test requirements (i.e. client/server interactions one with another)

The following sections (Mandatory and Optional test requirements) could also be separated for client and server test requirements.

The tables for the mandatory and optional test requirements include the following columns:

| | |
|---|---|
| **FEATURE KEY:** | A set of characters uniquely identifying the enabler test requirement to be tested. It is suggested that the Feature Key is no longer than 4 to 5 characters. The purpose of the Feature Key is that when used, it distinctly refers to only one feature to be tested. |
| **FEATURE DESCRIPTION**: | A description of a technical specification feature to be tested. |
| **FEATURE TEST REQUIREMENTS**: | A description of what shall be tested for the feature, |

The requirements have been split into two sections to cover the following

- Basic Functionality and non-roaming call-flows

Basic Functionality and non-roaming call-flows cover all basic functionality applicable to all modes of SUPL. The call flows should cover both Network Initiated and SET Initiated SUPL sessions. The test requirements apply to all Air Interfaces supported by SUPL 3.0

- Roaming call-flows

In general the Roaming call flows should be tested as part of RLP / MLS testing and therefore do not need to be re-tested as part of SUPL 3.0.

### 5.1.1 Mandatory test requirements

Mandatory test requirements are covering mandatory features/functions of an Enabler which shall always be implemented in the client/server

NOTE: This table needs to be filled out at a level where ambiguity is not present but details are not overwhelming.

Ambiguity means that the details do not have several meanings nor have more than one possible implementation path following.

#### 5.1.1.1 Basic Functionality

| | Feature Key | Feature Description | Feature Test Requirements |
|---|---|---|---|
| **Normal Flow** | CP | Common Part of ULP Message | Verify the Common Part of ULP message including Version support and Session ID support |
| | SID | SUPL INIT delivery | Verify the possible transport mechanisms used for the SUPL INIT message. |
| | KM1 | Key Management for SUPL Authentication - Deployments Supporting GBA | Verify correct operation |
| | TLS | TLS Handshake and Negotiation of SET-SLC Mutual-Authentication Method | Verify correct operation |
| | ACA | Alternative Client Authentication (ACA) Mechanisms - ACA Procedures | Verify correct operation |
| | SI1 | Processing of the SUPL INIT Messages - Network Based Authentication of the SUPL INIT Message | Verify correct operation |
| | SI2 | Processing of the SUPL INIT Messages - Negotiating the Level of SUPL INIT Protection | Verify correct operation with alternative Protection levels |
| | CDI | Confidentiality and Data Integrity | Verify correct operation with alternative Ciphering suites |
| | NV | Notification and Verification | Verify the correct operation and call flows for all the Notification & Verification values. |
| | NB | Basic Network Initiated flows | Verify the call flows using all possible positioning methods and verify that a successful positioning procedure is completed in each case. |
| | SB | Basic SET Initiated flows | Verify the call flows using all possible positioning methods and verify that a successful positioning procedure is completed in each case. |
| | NPP | Negotiation of Positioning method and Protocol | Verify that a consistent choice of positioning method and positioning protocol are made based upon the capabilities of SLP and SET. |
| | ES1 | Network Initiated Emergency Services Location Requests | Verify the call flows using all possible positioning methods and verify that a successful positioning procedure is completed in each case. |
| **Error Flow** | CPE | Common Part of ULP Message errors | Verify correct operation of the Common Part of ULP message with incompatible Versions and Invalid Session IDs |
| | SAF | SET Authorization Failure | Verify correct operation |
| | NCT | Network cancels the triggered location request | Verify correct call flow. |
| | SCT | SET cancels the triggered location request | Verify correct call flow. |
| | STE | SUPL timer expiration | Verify correct operation |
| | PST | Premature Session Termination | Verify correct operation when the SET or the Network prematurely ends the SUPL session |

**Table 1: Applicability Table for Basic Functionality Mandatory Test Requirements**

## 5.1.2 Optional test requirements

Optional test requirements are covering optional features/functions of an Enabler.

If an optional requirement of the Enabler is implemented in the client/server, this requirement SHALL be tested.

NOTE: This table needs to be filled out at a level where ambiguity is not present but details are not overwhelming.

Ambiguity means that the details do not have several meanings nor have more than one possible implementation path following.

### 5.1.2.1 Basic Functionality

| | Feature Key | Feature Description | Feature Test Requirements |
|---|---|---|---|
| **Normal Flow** | AE | Authentication Mechanisms applicable to an E-SLP - Processing Emergency SUPL INIT messages | Verify correct operation |
| | NCL | Notification/Verification based on current location. | Verify the correct operation and call flows for all the Notification & Verification values. |
| | QOP | QoP | Verify the correct call flows when the various QoPs are specified. |
| | VEL | Velocity | Verify correct operation |
| | ALT | Altitude | Verify correct operation |
| | NPT | Network Initiated– Triggered Services: Periodic Triggers | Verify representative call flows using suitable positioning methods and verify that successful positioning procedures are completed in each case. |
| | SPT | SET Initiated– Triggered Services: Periodic Triggers | Verify representative call flows using suitable positioning methods and a variety of parameter values and verify that successful positioning procedures are completed in each case. |
| | NET | Network Initiated– Triggered Services: Event Triggers | Verify representative call flows using suitable positioning methods and a variety of parameter values and verify that successful positioning procedures are completed in each case. |
| | SET | SET Initiated– Triggered Services: Event Triggers | Verify representative call flows using suitable positioning methods and verify that successful positioning procedures are completed in each case. |
| | NVT | Network Initiated– Triggered Services: Velocity Triggers | Verify representative call flows using suitable positioning methods and a variety of parameter values and verify that successful positioning procedures are completed in each case. |
| | SVT | SET Initiated– Triggered Services: Velocity Triggers | Verify representative call flows using suitable positioning methods and verify that successful positioning procedures are completed in each case. |
| | NGS | Network Initiated – GSS | Verify representative call flows using suitable positioning methods and verify that successful positioning procedures are completed in each case. |
| | SGS | SET Initiated – GSS | Verify representative call flows using suitable positioning methods and verify that successful positioning procedures are completed in each case. |
| | STPR1 | SET-Initiated 3rd Party Location Request | Verify correct call flow. |
| | STPR2 | SET-Initiated 3rd Party Relative Location Request | Verify correct call flow. |
| | STT | SET-Initiated Location Request with Transfer to Third Party | Verify correct call flow. |
| | HP | Retrieval of Historical Positions and/or Enhanced Cell Sector Measurements | Verify correct call flow. |

| | Feature Key | Feature Description | Feature Test Requirements |
|---|---|---|---|
| | CAT | Network / SET Capabilities Change for Area Event Triggered Scenarios | Verify correct call flows. |
| | SIQ1 | Session Info Query with Re-notification | Verify correct call flows. |
| | SIQ2 | Session Info Query with Session Termination | Verify correct call flows. |
| | LUI | Location URI Request | Verify correct call flow. |
| | DEA1 | D-SLP and E-SLP Authorization by the H-SLP | Verify correct call flow. |
| | DEA2 | D-SLP or E-SLP Authorization by a Proxy D-SLP or Proxy E-SLP | Verify correct call flow. |
| | DAN | D-SLP Access Notification to the H-SLP | Verify correct call flow. |
| | ES2 | SET Initiated Emergency Services Location Requests | Verify the call flows using all possible positioning methods and verify that a successful positioning procedure is completed in each case. |
| | DCT | Device Certificate (DCert) Security Mechanisms | Verify correct operation |
| | SEK | SEK based Security Mechanisms | Verify correct operation |
| **Error Flow** | | | |
| | | | |

**Table 2: Applicability Table for Basic Functionality Optional Test Requirements**

## 5.2 Cross Version compatibility

Cross version compatibility is an important feature of SUPL V3.0 and should be tested. As a minimum, the following cases should be tested to ensure compliance with the requirements of SUPL V3.0

### 5.2.1 SET V3.0

Compatibility with:

- SLP supporting V1.0
- SLP supporting V2.0
- SLP supporting <V3.0
- SLP supporting >V3.0

### 5.2.2 SLP V3.0 supporting <V3.0

Compatibility with:

- SET supporting V1.0
- SET supporting V2.0
- SET supporting <V3.0
- SET supporting >V3.0

### 5.2.3 SLP V3.0 not supporting <V3.0

Compatibility with:

- SET supporting V1.0
- SET supporting V2.0
- SET supporting <V3.0

- SET supporting >V3.0

## 5.3 Enabler dependencies

Enabler SUPL V3.0 has a dependency on the following:

- RLP V1.1 for SUPL roaming.
- MLP V3.3 for Network Initiated scenarios.
- LPP/LPPe and TIA-801 positioning protocols.
- ASN.1 BASIC-PER, unaligned encoding for the Lup protocol.
- TCP as transport protocol.
- UDP as transport protocol.

# Appendix A. Change History (Informative)

## A.1 Approved Version History

| Reference | Date | Description |
|---|---|---|
| OMA-ETR-SUPL-V1_0_1 | 27 Jan 2006 | Aproved version SUPL V1.0. |
| | | |

## A.2 Draft/Candidate Version History

| Document Identifier | Date | Sections | Description |
|---|---|---|---|
| Draft versions<br>OMA-ETR-SUPL-V3.0 | 29 Jun 2011 | N/A | Initial Draft |
| | 22 Aug 2011 | Throughout the document | Applied all changes assigned to the editor from OMA-CONRR-SUPL-V3_0-20110804-D |
| | 31 Aug 2011 | 5.1.1.1 | CR implemented:<br>OMA-LOC-2011-0274 |
| Candidate versions<br>OMA-ETR-SUPL-V3.0 | 20 Sep 2011 | All | TP approved via R&A:<br>OMA-TP-2011-0332-INP_SUPL_3.0_ERP_for_Candidate_approval |