User Plane Location Protocol

Candidate Version 3.0 – 16 Sep 2014

Open Mobile Alliance

OMA-TS-ULP-V3_0-20140916-C

Contents

Figures

Tables

1. Scope

This document describes the UserPlane Location Protocol (ULP) for SUPL 3.0. ULP is a protocol-level instantiation of the Lup reference point described in [SUPLAD3]. The protocol is used between the SLP (SUPL Location Platform) and a SET (SUPL Enabled Terminal). For details about SUPL Requirements refer to [SUPLRD3].

2. References

2.1 Normative References

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

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

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

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

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

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

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

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

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

[3GPP 49.031] 3GPP TS 49.031 “Base Station System Application Part LCS Extension (BSSAP-LE)”

URL:http://www.3GPP.org/

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

[3GPP LPP] 3GPP TS 36.355 "Evolved Universal Terrestrial Radio Access (E-UTRA); LTE Positioning Protocol (LPP)"
URL:http://www.3gpp.org/

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

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

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

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

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

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

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

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

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

[IEEE 802.11] IEEE 802.11

URL:http://www.ieee.org

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

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

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

URL:http://www.ieee802.org/16/published.html

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

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

[OMA-LOCSIP] “Enabler Release Definition for Location in SIP/IP Core”, Version 1.0, Open Mobile Alliance™,
URL:http://www.openmobilealliance.org/

[OMA-LPPe] “LPP Extension Specification”, Version 1.0, Open Mobile Alliance™,
URL:http://www.openmobilealliance.org/

[OMAOPS] “OMA Organization and Process”, Version 1.9, Open Mobile Alliance™,
URL:http://www.openmobilealliance.org/

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

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

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

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

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

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

[RFC 3856] "A Presence Event Package for the Session Initiation Protocol (SIP)", August 2004,
URL:http://www.ietf.org/rfc/rfc3856.txt

[RFC 3986] "Uniform Resource Identifier (URI): Generic Syntax ", January 2005,
URL:http://www.ietf.org/rfc/rfc3986.txt

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

[RFC 5985] "HTTP-Enabled Location Delivery (HELD)", September 2010, URL:http://www.ietf.org/rfc/rfc5985.txt

[SCRRULES] “SCR Rules and Procedures”, Open Mobile Alliance™, OMA-ORG-SCR_Rules_and_Procedures,
URL:http://www.openmobilealliance.org/

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

[SUPLAD3] "Secure User Plane Location Architecture", Version 3.0, Open Mobile Alliance™, OMA-AD-SUPL-V3_0,
URL:http://www.openmobilealliance.org/

[SUPLRD3] "Secure User Plane Location Requirements", Version 3.0, Open Mobile Alliance™, OMA-RD-SUPL-V3_0,
URL:http://www.openmobilealliance.org/

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

[TIA-553] Mobile Station -Land Station Compatibility Specification (AMPS), September 1989

URL:http://www.tiaonline.org/standards/

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

[TIA-801] C.S0022, Position Determination Service for cdma2000 Spread Spectrum Systems

URL:http://www.3gpp2.org/Public_html/specs/

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

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

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

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

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

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

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

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

2.2 Informative References

[SUPL MO] "OMA Management Object for SUPL", Version 3.0, Open Mobile Alliance™, OMA-TS-SUPL-MO-V3_0,
URL:http//www.openmobilealliance.org/

3. Terminology and Conventions

3.1 Conventions

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

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

3.2 Definitions

AN	Access Network
Area ID	Area ID is the identity of an area in a wireless network.
I-WLAN	The interworking WLAN refers to the system for interworking between 3GPP/3GPP2 systems and WLAN. The intent of 3GPP/3GPP2–WLAN Interworking is to extend 3GPP/3GPP2 services and functionality to the WLAN access environment. The 3GPP/3GPP2–WLAN Interworking System provides bearer services allowing a 3GPP/3GPP2 subscriber to use a WLAN to access 3GPP/3GPP2 PS based services.
Location ID	The Location ID defines the current serving cell, current serving WLAN AP or current serving WiMAX BS information of the SET.
Location URI	A URI that enables the current location of a target SET to be obtained from a particular location server using a particular dereferencing protocol.
LPP	LPP [3GPP LPP] implies use of LPP only
LPPe	LPPe [OMA-LPPe] implies use of LPP and LPPe
Major Version	Major versions are likely to contain major feature additions; MAY contain incompatibilities with previous specification revisions; and though unlikely, could change, drop, or replace standard or existing interfaces. Initial releases are “1_0”. [OMAOPS]
Minor Version	Minor versions are likely to contain minor feature additions, be compatible with the preceding Major version. Minor specification revision include existing interfaces, although it MAY provide evolving interfaces. The initial minor release for any major release is “0”, i.e. 1_0 [OMAOPS]
Multiple Location IDs	The Multiple Location IDs parameter may contain current non-serving cell, current non-serving WLAN AP or current non-serving WiMAX BS information for the SET and/or historic serving or non-serving cell, WLAN AP or WiMAX BS information for the SET.
Quality of Position	A set of attributes associated with a request for the geographic position of SET. The attributes include the required horizontal accuracy, vertical accuracy, max location age, and response time of the SET position.
Service Indicator	Service indicators are intended to be compatible with the Major_ Minor release they relate to but add bug fixes. No new functions will be added through the release of Service Indicators. [OMAOPS]
SET assisted	Positioning methods where the SLP calculates the position estimate based on received positioning measurements from the SET.
SET based	Positioning methods where the SET calculates the position estimate utilizing assistance data from SLP.
SUPL Roaming	For positioning not associated with an emergency services call, SUPL roaming occurs when a SET leaves the service area of its H-SLP. For positioning associated with an emergency services call, SUPL roaming occurs when the SET is not within the service area of the E-SLP. The service area of an H-SLP or E-SLP includes the area within which the H-SLP or E-SLP can provide a position estimate for a SET or relevant assistance data to a SET without contacting other SLPs. It should be noted that an H-SLP or E-SLP service area is not necessarily associated with the service area(s) of the underlying wireless network(s). In the case of service from a D-SLP, the H-SLP will normally assign a geographic service area within which the SET may access the D-SLP. Service from a D-SLP where the SET is roaming outside the assigned service area of the D-SLP is not supported.

Triggered Location Request	A location request for triggered periodic events, triggered area events or triggered velocity events.

3.3 Abbreviations

ACA	Alternative Client Authentication
AP	Access Point (WLAN)
BDS	BeiDou Navigation Satellite System
BS	Base Station (WiMAX)
BSF	Bootstrapping Server Function
CI	Cell Identity (3GPP)
D/E/H-SLP	A Discovered SLP, Emergency SLP or Home SLP
D/E-SLP	A Discovered SLP or Emergency SLP
D/H-SLP	A Discovered SLP or Home SLP
D-SLP	Discovered SLP
E-SLP	Emergency SLP
FQDN	Fully Qualified Domain Name
GANSS	Galileo and Additional Navigation Satellite Systems
GBA	Generic Bootstrapping Architecture
GLONASS	**GLO**bal'naya **NA**vigatsionnaya **S**putnikovaya **S**istema (Engl.: Global Navigation Satellite System)
GNSS	Global Navigation Satellite System
HELD	HTTP-Enabled Location Delivery
H-SLP	Home SLP
LAC	Location Area Code (3GPP)
lid	Location ID
LPP	LTE Positioning Protocol
LPPe	LPP Extensions
LRF	Location Retrieval Function
LTE	Long Term Evolution
MCC	Mobile Country Code (3GPP)
MLP	Mobile Location Protocol
MNC	Mobile Network Code (3GPP)
NID	Network ID (C.S0022-A V1.0)
OMA	Open Mobile Alliance
OMNA	Open Mobile Naming Authority
PAP	OMA Push Access Protocol
POTAP	OMA Push Over the Air Protocol
PSAP	Public Safety Answering Point
QoP	Quality of Position
QZSS	Quasi-Zenith Satellite System
RLP	Roaming Location Protocol
RNC	Radio Network Controller

R-SLP	Requesting SLP
SBAS	Satellite Based Augmentation System
SEK	SUPL Encryption Key
SET	SUPL Enabled Terminal
SID	System ID (C.S0022-A V1.0)
SIP	Session Initiation Protocol
SLC	SUPL Location Center
SLP	SUPL Location Platform
SM	Short Message
SMS	Short Message Service
SPC	SUPL Positioning Center
SSID	Service Set Identifier
TCP	Transmission Control Protocol
TD-SCDMA	Time Division-Synchronous Code Division Multiple Access
TLS	Transport Layer Security
ULP	Userplane Location Protocol
URI	Uniform Resource Identifier
V-SLP	Visited SLP
WAP	Wireless Application Protocol
WCDMA	Wideband Code Division Multiple Access
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network

4. Introduction

This protocol specification presents the OMA implementation for Location Based Services over the User Plane called SUPL (Secure User Plane Location). SUPL enables SUPL Enabled Terminals (SETs) and SUPL Location Platforms (SLPs) to communicate over an IP bearer to exchange location information (e.g., GNSS assistance data, etc.) and other information needed for positioning. In contrast to Control Plane, SUPL only requires an end to end IP bearer between the SET and the SLP and some minimum modifications to the network in order to be able to perform secure location based services.

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

The target audience for this specification is developers and systems engineers developing SUPL products or service providers deploying SUPL services.

4.1 Version 1.0

The main features of SUPL Version 1.0 are:

- Immediate Fix service for Network Initiated and SET Initiated use cases
- Support of GSM/WCDMA and CDMA radio access networks
- Support of the following positioning methods:
    - A-GPS (both SET Based and SET Assisted)
    - Autonomous GPS
    - E-OTD for GSM radio access networks
    - OTDOA for WCDMA radio access networks
    - AFLT for CDMA radio access networks
    - E-CID for GSM/WCDMA and CDMA radio access networks
- Support of the following positioning protocols:
    - RRLP V5.12.0 for GSM and WCDMA (mandatory)
    - RRC V5.11.0 for WCDMA (optional)
    - TIA-801 for CDMA (mandatory)
- Security model for all access networks
- Two different modes of operation:
    - Proxy mode: the SET communicates with the SLC only and positioning layer messages are proxied through the SLC to the SPC.
    - Non-Proxy mode: the SET communicates directly with the SPC when exchanging positioning layer messages.
- Two different roaming models:
    - Roaming with the H-SLP: in this roaming mode, the positioning session is conducted between the SET and the H-SLP and the V-SLP is only invoked for cell info translation

  - Roaming with V-SLP: in this roaming mode, the positioning session is conducted directly between the SET and the V-SLP.

- SUPL INIT transport:
  - MT-SMS
  - OMA-Push

4.2 Version 2.0

In version 2.0 of SUPL, the following main features were added :

- Triggered Periodic and Triggered Area Event services for Network Initiated and SET Initiated use cases
- Positioning procedures for emergency calls, support for E-SLP
- Positioning procedures for delivery to third party and retrieval of location of another SET
- Support of TD-SCDMA, LTE, HRPD [3GPP2 HRPD], I-WLAN and WiMAX [IEEE 802.16e-2005] radio access networks
- Support of the following positioning methods :
  - A-GANSS (both SET Based and SET Assisted)
  - Autonomous GANSS
  - OTDOA for LTE radio access networks
  - E-CID for TD-SCDMA, LTE, HRPD, I-WLAN and WiMAX radio access networks
- Support of the following positioning protocols
  - RRLP with floating release for GSM/WCDMA/LTE, I-WLAN and WiMAX (mandatory)
  - RRC with floating release for WCDMA/TD-SCDMA (optional)
  - LPP with floating release for LTE (optional)
  - TIA-801 with floating release for CDMA/HRPD (mandatory)
  - TIA-801 with floating release for LTE, I-WLAN and WiMAX (optional)
- Security models :
  - GBA-based security model for 3GPP2 network deployments
  - SEK-based security model for WiMAX deployments
- SUPL INIT transport :
  - SIP Push
  - UDP

4.3 Version 3.0

In version 3.0 of SUPL, the following changes were made:

- Removal of RRLP and RRC as supported positioning protocols: only LPP, LPP+LPPe and TIA-801 are supported

- Removal of non-proxy mode: only proxy mode is supported
- Removal of Roaming with V-SLP mode: only Roaming with H-SLP is supported.

In version 3.0 of SUPL, the following new features and services were added:

- Support for LPPe
- Generic SUPL Session
- 3rd Party Relative Location
- Support for Velocity Trigger
- Security model for non-UICC devices using client certificates stored on the device
- Support for D-SLP
- Support for a Location URI

4.4 L1/Le Interface

The message flows in chapter 5 assume use of OMA MLP on the L1/Le interface between an SLP and a SUPL Agent. However, other protocols are possible for some message flows. The use of other protocols, while permitted, is outside the scope of this specification.

A SUPL Agent will normally access the H-SLP of a SET using the L1/Le interface to invoke any NI associated service (e.g. obtain an immediate location fix for the SET). Access to a D-SLP that has been authorized either by the H-SLP or by an authorized Proxy D-SLP to perform NI services is allowed provided the SUPL Agent is able to access the D-SLP either diectly or indirectly via the H-SLP. Direct access can be possible when the H-SLP provides the D-SLP address to the SUPL Agent (e.g. following an initial query from the SUPL Agent to the H-SLP and if the SET has been reporting D-SLP access back to the H-SLP using the procedure in section 5.1.2.10). Indirect access can be possible when the H-SLP forwards a request from a SUPL Agent to a D-SLP (e.g. using RLP or some other protocol if the SET has been reporting D-SLP access back to the H-SLP using the procedure in section 5.1.2.10). Other forms of access are not precluded – e.g. a SET may interact with a remote SUPL Agent and provide a D-SLP address to enable location services for the SUPL Agent. Note that while access to a D-SLP by a SUPL Agent can be possible as described, exact details are outside the scope of this specification.

5. Message Flows

The message flows shown in this chapter cover Immediate Services, Emergency Services and Deferred Services including both successful and exception procedures.

Message flows define how different SUPL 3.0 services are provided to a SUPL Agent through specific interactions between the SUPL Agent, one or more SLPs and one or more SETs. The type of SLP that may appear in a message flow is limited to one of an H-SLP, D-SLP, E-SLP or V-SLP. However, some message flows apply to several types of SLP. For a message flow that applies to an SLP that can be either a D-SLP or H-SLP, the SLP is referred to in the message flow as a D/H-SLP. For a message flow that applies to an SLP that can be a D-SLP, E-SLP or H-SLP, the SLP is referred to in the message flow as a D/E/H-SLP.

For all scenarios described in this chapter, the following rule applies: A ULP message sent in direct response to SUPL INIT or SUPL REINIT SHALL contain the hash (*ver* parameter) of the SUPL INIT or SUPL REINIT message, respectively. Upon receipt of this parameter, the SLP SHALL check whether the value of *ver* matches the one calculated and stored by the SLP for that same SUPL session. If the values match, the SLP SHALL continue the SUPL session otherwise the SLP SHALL end the SUPL session by sending a SUPL END message with status code '*authSuplinitFailure*'. If a position estimate was returned to the SLP in the message carrying the *ver* parameter, that position estimate SHALL NOT be forwarded to the SUPL Agent if the value of *ver* doesn't match the one in the SLP.

NOTE: A session in SLP or SET SHALL only release its TLS connection if the TLS connection is not required by another session.

NOTE[1]: In SUPL 3.0 it is possible to use LPP (by itself), LPP+LPPe or TIA-801 as positioning protocol. Therefore the following convention applies: *LPP* implies use of *LPP only* (i.e. without LPPe), *LPPe* implies use of *LPP and LPPe* and *TIA-801* implies use of *TIA-801 only*. A SUPL POS (LPP/LPPe/TIA-801) message means a SUPL POS message carrying either LPP, LPP+LPPe or TIA-801 positioning payload. A single SUPL POS message MAY contain either LPP/LPPe or TIA-801 messages, but not both.

NOTE: The optional parameters *QoP* and *High Accuracy QoP* used in SUPL INIT, SUPL SET INIT, SUPL START and SUPL TRIGGERED START are mutually exclusive. *High Accuracy QoP* is not explicitly mentioned in the call flows of this section. It is assumed that either *QoP* or *High Accuracy QoP* – but not both - may be used as optional parameters defining the desired quality of position.

NOTE: Timers used in the call flow diagrams shown in this chapter are described in Appendix C.

NOTE: Optional parameters in the call flow diagrams of this chapter are shown in gray.

5.1 Immediate Services

5.1.1 Network Initiated

For Network Initiated services, the SUPL Agent resides within the network and the service request is directed at the SLP.

Before sending any ULP messages, the SET SHALL establish a secure connection (i.e., TLS connection) with the SLP. This can be achieved by establishing a new TLS connection, resuming a suspended TLS connection or reusing an existing TLS connection. Details of the TLS session (establishment, termination, etc.) are not shown in this section.

The roaming case described in this section assumes that R-SLP and D/H-SLP are the same i.e., the SUPL Agent communicates directly with the D/H-SLP. Whereas the flows in this section illustrate the use of MLP messages for the Le/L1 Reference Point between the SUPL Agent and the D/H-SLP, other protocols can be used for these interactions.

NOTE: Appendix D illustrates various flows based on the use of OMA LOCSIP 1.0 [OMA-LOCSIP] for the Le/L1 Reference Point.

[1] This Note applies to all sections of the document

5.1.1.1 Single Fix – Non Roaming

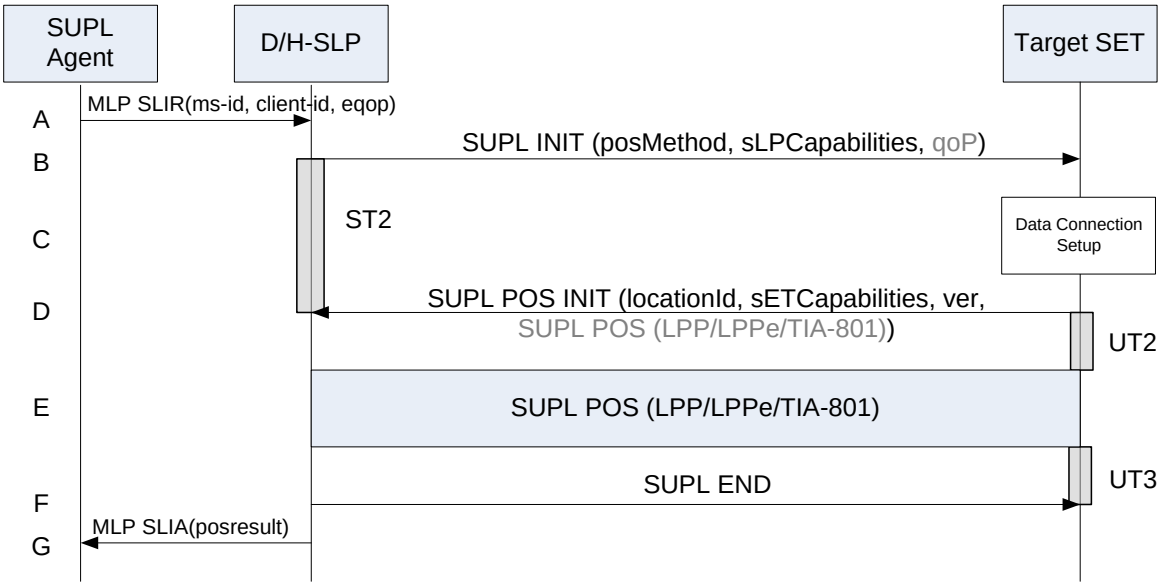

Figure 1: Network Initiated Non-Roaming

A. SUPL Agent sends an MLP SLIR message to the D/H-SLP, with which it is associated. The D/H-SLP SHALL authenticate the SUPL Agent and check if the SUPL Agent is authorized for the service requested based on the *client-id* received. The D/H-SLP shall also provide privacy checking based on *ms-id* and *client-id*. The D/H-SLP MAY also verify that the target SET supports SUPL.
If a previously computed position which meets the requested QoP (*eqop*) is available at the D/H-SLP and no notification and verification is required, the D/H-SLP SHALL directly proceed to step G. If notification and verification or notification only is required, the D/H-SLP SHALL proceed to step B.

NOTE: The specifics for determining if the SET supports SUPL are beyond the scope of SUPL 3.0.

B. The D/H-SLP initiates the location session with the SET using the SUPL INIT message. The SUPL INIT message contains the intended positioning method (*posMethod*), the SLP Capabilities (*sLPCapabilities*) and optionally the *QoP*. If the result of the privacy check in step A indicates that notification and/or verification of the target subscriber is needed, the D/H-SLP SHALL also include the Notification parameter in the SUPL INIT message. Before the SUPL INIT message is sent, the D/H-SLP also computes and stores the hash of the SUPL INIT message.
If in step A the D/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 D/H-SLP SHALL then directly proceed to step G.

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

C. The SET analyses the received SUPL INIT message. If found not to be authentic, the SET takes not further action. Otherwise, the SET takes required action to prepare for the establishment of a TLS connection with the D/H-SLP. The SET also calculates the hash of the received SUPL INIT message.

D. The SET evaluates the Notification rules and takes the appropriate action. The SET SHALL establish a TLS connection to the D/H-SLP using the D/H-SLP address which is either the H-SLP address provisioned by the Home Network or the D-SLP address provided or verified by the H-SLP or by a Proxy D-SLP authorized by the H-SLP. The SET then sends a SUPL POS INIT message to start a positioning session with the D/H-SLP. The SET SHALL send the SUPL POS INIT message even if the SET does not support the intended positioning method indicated in SUPL INIT. The SUPL POS INIT message contains the Location ID (*locationId*), SET capabilities

(*sETCapabilities*) and the hash (*ver*) of the received SUPL INIT message calculated in step C. The SUPL POS INIT message MAY also include a SUPL POS message carrying LPP/LPPe and/or TIA-801 positioning protocol messages in line with the D/H-SLP's positioning protocol capabilities (indicated in step B in *sLPCapabilities*). The SET MAY also provide its position, if this is supported (as part of LPP/LPPe/TIA-801 or explicitly through the optional position parameter). If a position retrieved in - or calculated based on information received in - the SUPL POS INIT message is available that meets the required QoP, the D/H-SLP MAY directly proceed to step F and not engage in a SUPL POS session.

E. SET and D/H-SLP engage in a SUPL POS message exchange to calculate a position. The positioning methods used for this session are determined based on the capabilities exchanged by the SET and the D/H-SLP during the SUPL POS message exchange or optionally in step D. The D/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 D/H-SLP (SET-Based).

F. Once the position calculation is complete, the D/H-SLP sends a SUPL END message to the SET indicating that the location session has ended. The SET SHALL release the TLS connection to the D/H-SLP and release all resources related to this session.

G. The D/H-SLP sends the position estimate (*posresult*) back to the SUPL Agent in an MLP SLIA message and the D/H-SLP SHALL release all resources related to this session.

5.1.1.2 Single Fix – Roaming

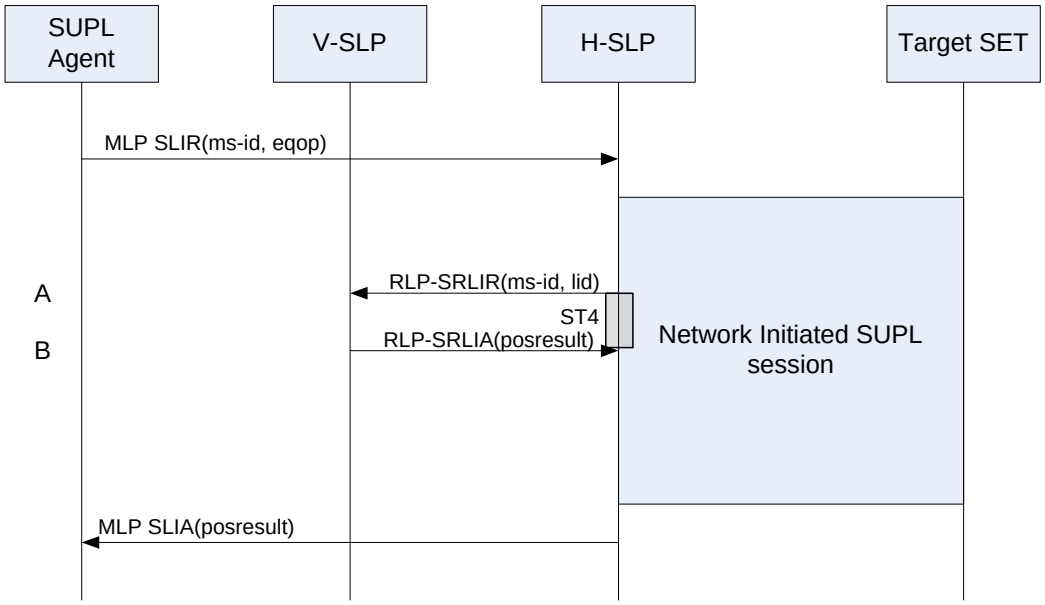

Figure 2: Network Initiated Roaming

For Network Initiated roaming, the ULP message exchange is the same as for non-roaming (see Figure 1). The ULP message exchange between SET and H-SLP is therefore not explicitly shown in Figure 2 but only indicated as "Network Initiated SUPL session" in the diagram. The V-SLP is invoked if and when the H-SLP requires translation of a cell or access point id into a position estimate.

A. In the course of the SUPL session, the H-SLP requires translation of a cell or access point id into a position estimate. Since the SET is SUPL roaming, the H-SLP is unable to perform the translation on its own. The H-SLP therefore engages the V-SLP by sending an RLP-SRLIR message to the V-SLP including the ms-id and the location id (cell or access point id).

B. The V-SLP translates the received cell or access point id into a position estimate and returns an RLP-SRLIA message including the position (*posresult*) to the H-SLP.

5.1.1.3 Single Fix with Notification/Verification based on Current Location

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

Roaming scenarios are not considered here since they are the same as in section 5.1.1.2.

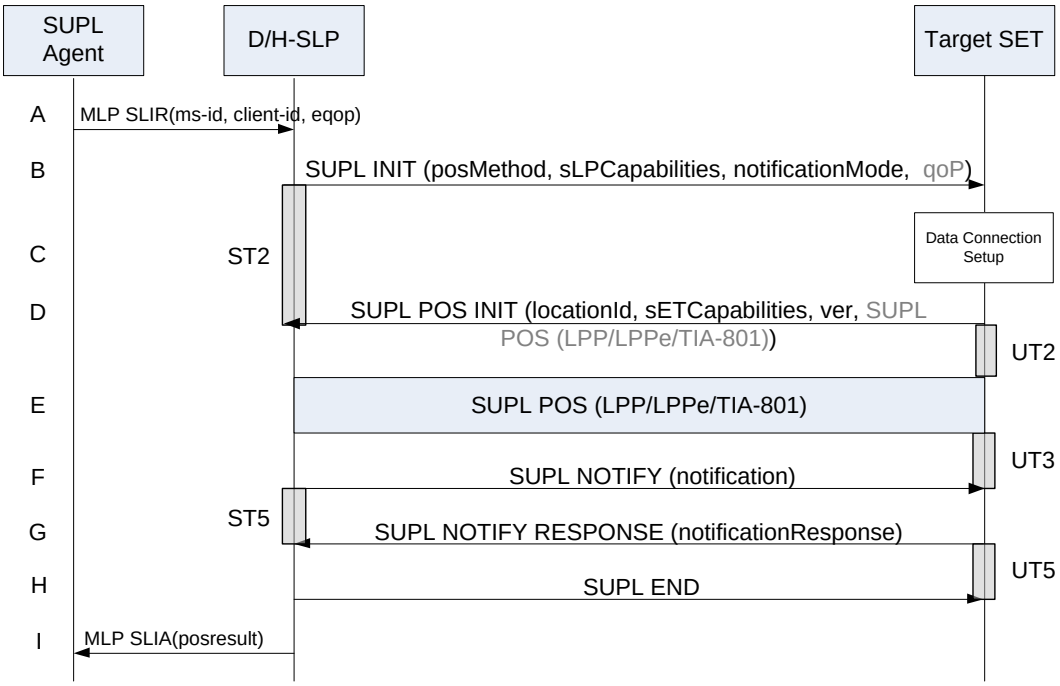

Figure 3: Single Fix with Notification/Verification based on Current Location

A. SUPL Agent sends an MLP SLIR message to the D/H-SLP, with which it is associated. The D/H-SLP SHALL authenticate the SUPL Agent and check if the SUPL Agent is authorized for the service requested based on the *client-id* received. The D/H-SLP shall also provide privacy checking based on *ms-id* and *client-id*. The D/H-SLP MAY also verify that the target SET supports SUPL.
If a previously computed position which meets the requested QoP (*eqop*) is available at the D/H-SLP and, based on that position, no notification and verification is required, the D/H-SLP SHALL directly proceed to step I. If, based on that position, notification and verification or notification only is required, the D/H-SLP SHALL proceed to step B.

NOTE: The specifics for determining if the SET supports SUPL are beyond the scope of SUPL 3.0.

B. The D/H-SLP initiates the location session with the SET using the SUPL INIT message. The SUPL INIT message contains the intended positioning method (*posMethod*), the SLP Capabilities (*sLPCapabilities*) and optionally the *QoP*. As in this case the result of the privacy check in Step A indicates that subscriber privacy check based on current location is required, the H-SLP SHALL include the Notification Mode element (*notificationMode*) in the SUPL INIT message to indicate notification based on current location and SHALL NOT include the notification element in the SUPL INIT message. Before the SUPL INIT message is sent, the D/H-SLP also computes and stores the hash of the SUPL INIT message.
If in step A the D/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 D/H-SLP SHALL then directly proceed to step I.

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

C. The SET analyses the received SUPL INIT message. If found not to be authentic, the SET takes not further action. Otherwise, the SET takes required action to prepare for the establishment of a TLS connection with the D/H-SLP. The SET also calculates the hash of the received SUPL INIT message.

D. The SET evaluates the Notification rules and takes the appropriate action. The SET checks the notification mode indicator and determines that in this case the notification is performed based on the location of the SET. The SET SHALL establish a TLS connection to the D/H-SLP using the D/H-SLP address which is either the H-SLP address provisioned by the Home Network or the D-SLP address provided or verified by the H-SLP or by a Proxy D-SLP authorized by the H-SLP. The SET then sends a SUPL POS INIT message to start a positioning session with the D/H-SLP. The SET SHALL send the SUPL POS INIT message even if the SET does not support the intended positioning method indicated in SUPL INIT. The SUPL POS INIT message contains the Location ID (*locationId*), SET capabilities (*sETCapabilities*) and the hash (*ver*) of the received SUPL INIT message calculated in step C. The SUPL POS INIT message MAY also include a SUPL POS message carrying LPP/LPPe and/or TIA-801 positioning protocol messages in line with the D/H-SLP's positioning protocol capabilities (indicated in step B in *sLPCapabilities*). The SET MAY also provide its position, if this is supported (as part of LPP/LPPe/TIA-801 or explicitly through the optional position parameter). If a position retrieved in - or calculated based on information received in - the SUPL POS INIT message is available that meets the required QoP, the D/H-SLP MAY directly proceed to step F and not engage in a SUPL POS session.

E. SET and D/H-SLP engage in a SUPL POS message exchange to calculate a position. The positioning methods used for this session are determined based on the capabilities exchanged by the SET and the D/H-SLP during the SUPL POS message exchange or optionally in step D. The D/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 D/H-SLP (SET-Based).

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

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

H. The D/H-SLP sends a SUPL END message to the SET indicating that the location session has ended. The SET SHALL release the TLS connection to the D/H-SLP and release all resources related to this session.

I. The D/H-SLP sends the position estimate (*posresult*) back to the SUPL Agent in an MLP SLIA message and the D/H-SLP SHALL release all resources related to this session.

5.1.2 SET Initiated

For SET Initiated services, the SUPL Agent resides within the SET.

Before sending any ULP messages, the SET SHALL establish a secure connection (i.e., TLS connection) with the SLP. This can be achieved by establishing a new TLS connection, resuming a suspended TLS connection or reusing an existing TLS connection. Details of the TLS session (establishment, termination, etc.) are not shown in this section.

5.1.2.1 Single Fix – Non Roaming

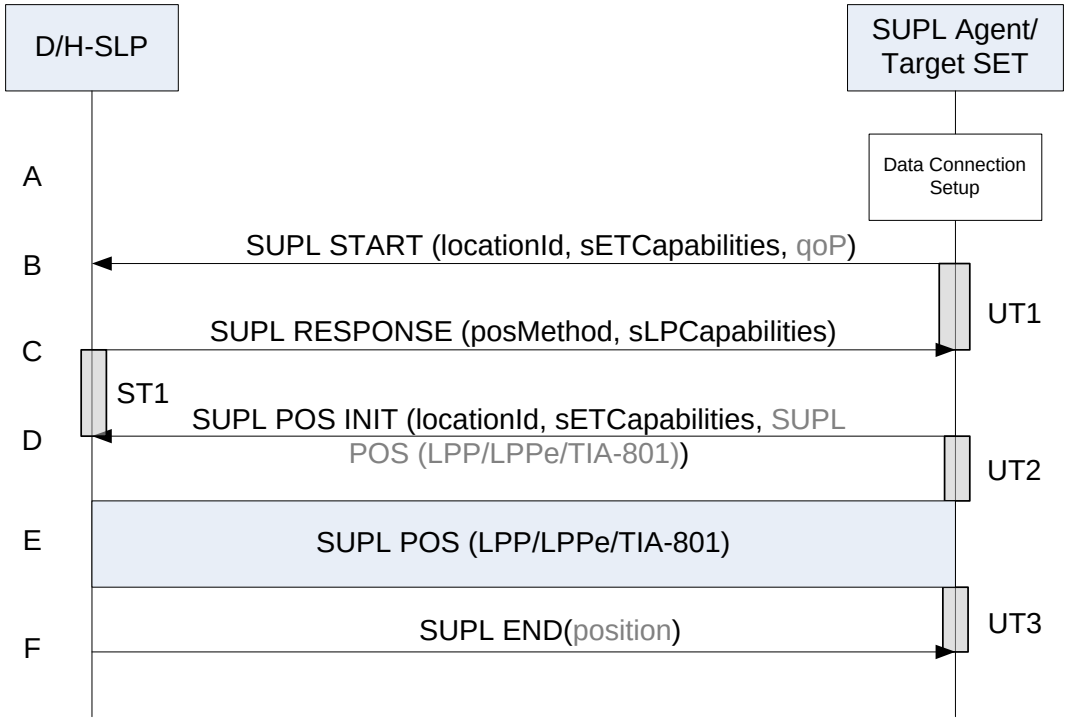

Figure 4: SET Initiated Non-Roaming

A. The SET receives a position request from a SUPL Agent (e.g., an application) on the SET. The SET takes appropriate action to establish a secure TLS connection to the D/H-SLP.

B. The SET SHALL use either the default address provisioned by the Home Network for an H-SLP or the address provided or verified by the H-SLP or by a Proxy D-SLP authorized by the H-SLP for a D-SLP to establish a secure TLS connection to the D/H-SLP and send a SUPL START message to start a positioning session with the D/H-SLP. The SUPL START message contains the Location ID (*locationId*), SET capabilities (*sETCapabilities*) and optionally the desired QoP.
If a previously computed position which meets the requested QoP is available at the D/H-SLP, the D/H-SLP SHALL directly proceed to step F and send a SUPL END message to the SET including the position result (*position*).

C. The D/H-SLP sends a SUPL RESPONSE message to the SET. The SUPL RESPONSE contains the intended positioning method (*posMethod*) and the SLP Capabilities (sLPCapabilities).

D. The SET sends a SUPL POS INIT message to the D/H-SLP. The SET SHALL send the SUPL POS INIT message even if the SET does not support the intended positioning method indicated in SUPL RESPONSE. The SUPL POS INIT message contains the Location ID (*locationId*), SET capabilities (*sETCapabilities*) and optionally a SUPL POS message carrying LPP/LPPe and/or TIA-801 positioning protocol messages in line with the D/H-SLP's positioning protocol capabilities (indicated in step C in *sLPCapabilities*). The SET MAY also provide its position, if this is supported (as part of LPP/LPPe/TIA-801 or explicitly through the optional position parameter). If a position retrieved in - or calculated based on information received in - the SUPL POS INIT message is available that meets the required QoP, the D/H-SLP MAY directly proceed to step F and not engage in a SUPL POS session.

E. SET and D/H-SLP engage in a SUPL POS message exchange to calculate a position. The positioning methods used for this session are determined based on the capabilities exchanged by the SET and the D/H-SLP during the SUPL POS message exchange or optionally in step D. The D/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 D/H-SLP (SET-Based).

F. Once the position calculation is complete, the D/H-SLP sends a SUPL END message to the SET indicating that the location session has ended. If required, the D/H-SLP MAY also send the position result (*position*) in SUPL END. The SET SHALL release the TLS connection to the D/H-SLP and release all resources related to this session. The D/H-SLP SHALL release all resources related to this session.

5.1.2.2 Single Fix – Roaming

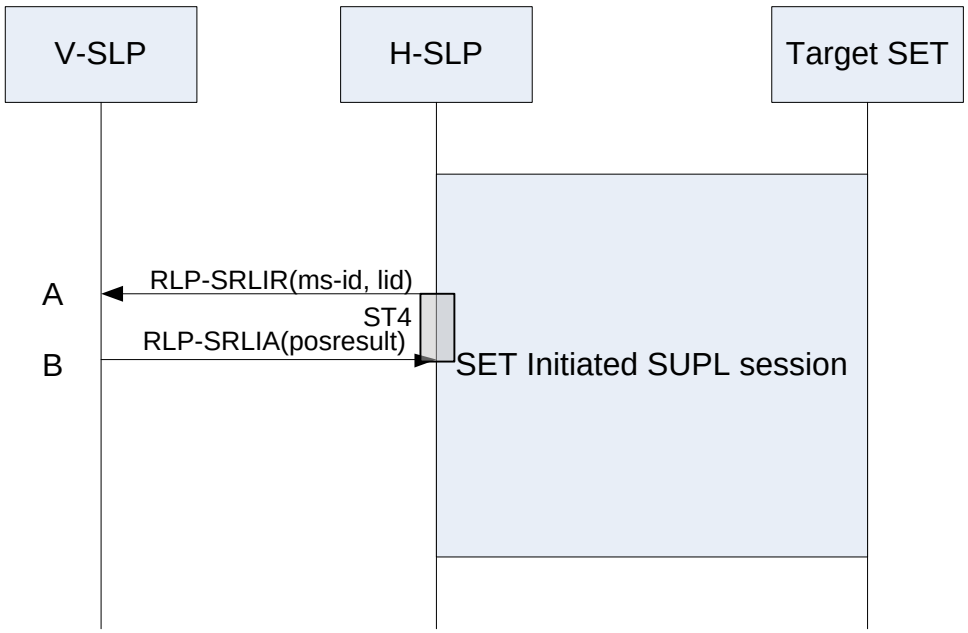

Figure 5: SET Initiated Roaming

For SET Initiated roaming, the ULP message exchange is the same as for non-roaming (see Figure 4). The ULP message exchange between SET and H-SLP is therefore not explicitly shown in Figure 5 but only indicated as "SET Initiated SUPL session" in the diagram. The V-SLP is invoked if and when the H-SLP requires translation of a cell or access point id into a position estimate.

A. In the course of the SUPL session, the H-SLP requires translation of a cell or access point id into a position estimate. Since the SET is SUPL roaming, the H-SLP is unable to perform the translation on its own. The H-SLP therefore engages the V-SLP by sending an RLP-SRLIR message including the ms-id and the location id (cell or access point id).

B. The V-SLP translates the received cell or access point id into a position estimate and returns an RLP-SRLIA message including the position (*posresult*) to the H-SLP.

5.1.2.3 Single Fix – 3rd Party Location Request

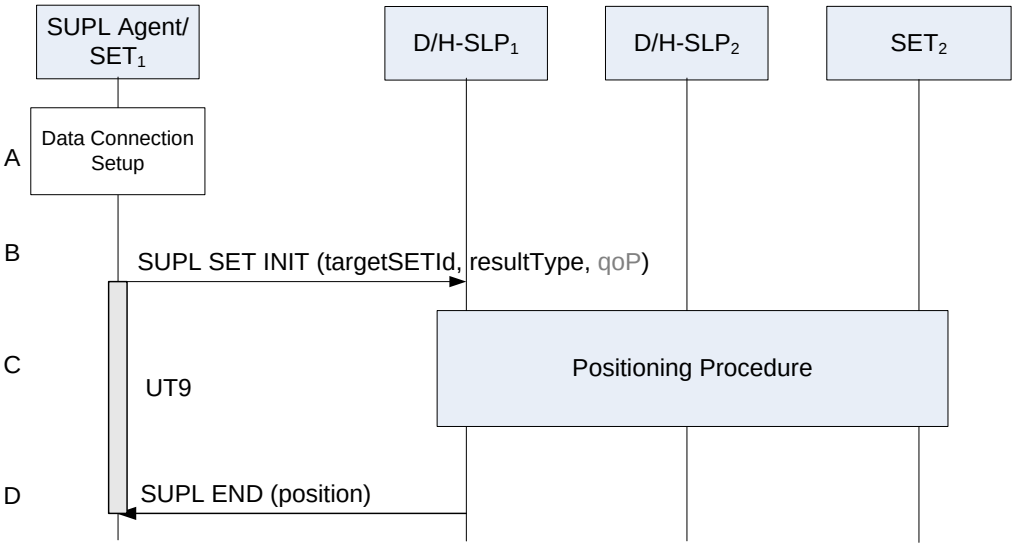

Figure 6: Single Fix - 3rd Party Location Request

A. SET_1 receives a request for position of Target SET_2 from a SUPL Agent (e.g., an application) on SET_1. SET_1 takes appropriate action to establish a secure TLS connection to the $D/H\text{-}SLP_1$.

B. SET_1 SHALL use either the default address provisioned by the Home Network for an H-SLP or the address provided or verified by the H-SLP or by a Proxy D-SLP authorized by the H-SLP for a D-SLP to establish a secure TLS connection to the $D/H\text{-}SLP_1$ and send a SUPL SET INIT message to start a positioning session of the Target SET_2. The SUPL SET INIT message contains an Identity of the Target SET_2 (*targetSETId*) that will be used by the $D/H\text{-}SLP_1$ to identify either the home network ($H\text{-}SLP_2$) or a current D-SLP ($D\text{-}SLP_2$) of the Target SET_2. The SUPL SET INIT message also contains the result type (*resultType*) which indicates whether an absolute position estimate is required (*resultType='absoluteposition'*) or whether a position relative to a reference point is required (*resultType='positionrelativetoreferencepoint'*). It MAY also contain the desired QoP. Note that SET_1 may use either its H-SLP ($H\text{-}SLP_1$) or a currently authorized D-SLP ($D\text{-}SLP_1$) to request the location of Target SET_2. Likewise, $D/H\text{-}SLP_1$ may use either the H-SLP ($H\text{-}SLP_2$) or a currently authorized D-SLP ($D\text{-}SLP_2$) of Target SET_2 to obtain the location of Target SET_2. For example, a D-SLP could be used in both cases if the same D-SLP serves both SETs.

C. The $D/H\text{-}SLP_1$ determines the location of the Target SET_2. This may involve the use of other SLPs. The MLS enabler, LOCSIP enabler and SUPL procedures for Network Initiated queries may be used.

D. The $D/H\text{-}SLP_1$ sends a SUPL END message containing the position estimate of the Target SET_2 to the SET_1. The SET_1 sends the position estimate back to the SUPL Agent. The SET_1 SHALL release the TLS connection to the $D/H\text{-}SLP_1$ and release all resources related to this session. The $D/H\text{-}SLP_1$ SHALL releases all resources related to this session.

NOTE: SET_1 and $D/H\text{-}SLP_1$ MUST NOT release the secure TLS connection between steps B and D.

5.1.2.4 Single Fix – 3rd Party Relative Location Request

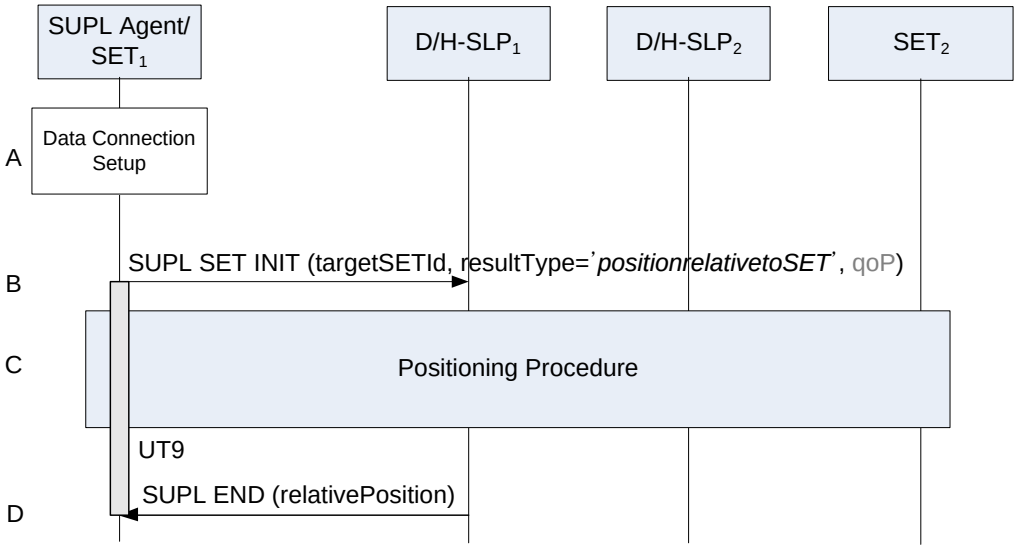

Figure 7: Single Fix - 3rd Party Relative Location Request

A. SET_1 receives a request for a relative position of Target SET_2 from a SUPL Agent (e.g., an application) on SET_1. The SET_1 takes appropriate action to establish a secure TLS connection to the D/H-SLP_1.

B. SET_1 SHALL use either the default address provisioned by the Home Network for an H-SLP or the address provided or verified by the H-SLP or by a Proxy D-SLP authorized by the H-SLP for a D-SLP to establish a secure TLS connection to the D/H-SLP_1 and send a SUPL SET INIT message to start a relative positioning session of the Target SET_2. The SUPL SET INIT message contains the identity of Target SET_2 (*targetSETId*) and the result type. In this case the result type indicates that a position estimate relative to the SET (SET_2) is required (*resultType='positionrelativetoSET'*). The identity of Target SET_2 (*targetSETId*) is used by the D/H-SLP_1 to identify either the home network (H-SLP_2) or a current D-SLP (D-SLP_2) of the Target SET_2. The result type (*resultType*) indicates that the relative position of SET_1 and target SET_2 is to be calculated. It MAY also contain the desired QoP. Note that SET_1 may use either its H-SLP (H-SLP_1) or a currently authorized D-SLP (D-SLP_1) to request the relative location of Target SET_2. Likewise, D/H-SLP_1 may use either the H-SLP (H-SLP_2) or a currently authorized D-SLP (D-SLP_2) of Target SET_2 to obtain the location of Target SET_2.

C. The D/H-SLP_1 determines the relative location of SET_1 and Target SET_2. This may involve the use of other SLPs. The MLS enabler, LOCSIP enabler and SUPL procedures may be used for acquiring positions of SET_1 and Target SET_2.

D. The D/H-SLP_1 sends the SUPL END message containing the relative position of Target SET_2 and SET_1. SET_1 SHALL release the TLS connection to the D/H-SLP_1 and release all resources related to this session. The D/H-SLP_1 SHALL release all resources related to this session.

NOTE: SET_1 and D/H-SLP_1 MUST NOT release the secure TLS connection between steps B and D.

5.1.2.5 Single Fix with Transfer to 3rd Party

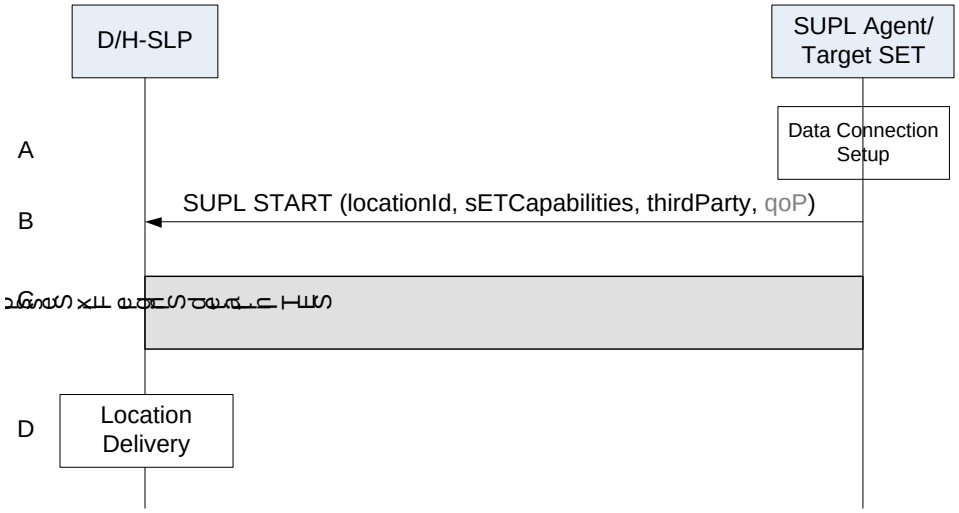

Figure 8: Single Fix with Transfer to 3rd Party

A. The SET receives a position request with transfer to 3rd party from a SUPL Agent (e.g. An application) on the SET. The SET takes appropriate action to establish a secure TLS connection to the D/H-SLP.

B. The SET SHALL use either the default address provisioned by the Home Network for an H-SLP or the address provided or verified by the H-SLP or by a Proxy D-SLP authorized by the H-SLP for a D-SLP to establish a secure TLS connection to the D/H-SLP and send a SUPL START message to start a positioning session with the D/H-SLP. The SUPL START message contains the Location ID (*locationId*), SET capabilities (*sETCapabilities*), identity of 3rd party (*thirdParty*) and optionally the desired QoP.

C. The D/H-SLP and Target SET performs the remaining procedures to determine the location of the Target SET, i.e. step C to step F described in the section 5.1.2.1 are performed.

D. The D/H-SLP transfers the position result to the 3rd party and releases all resources related to the session.

5.1.2.6 Location URI Request

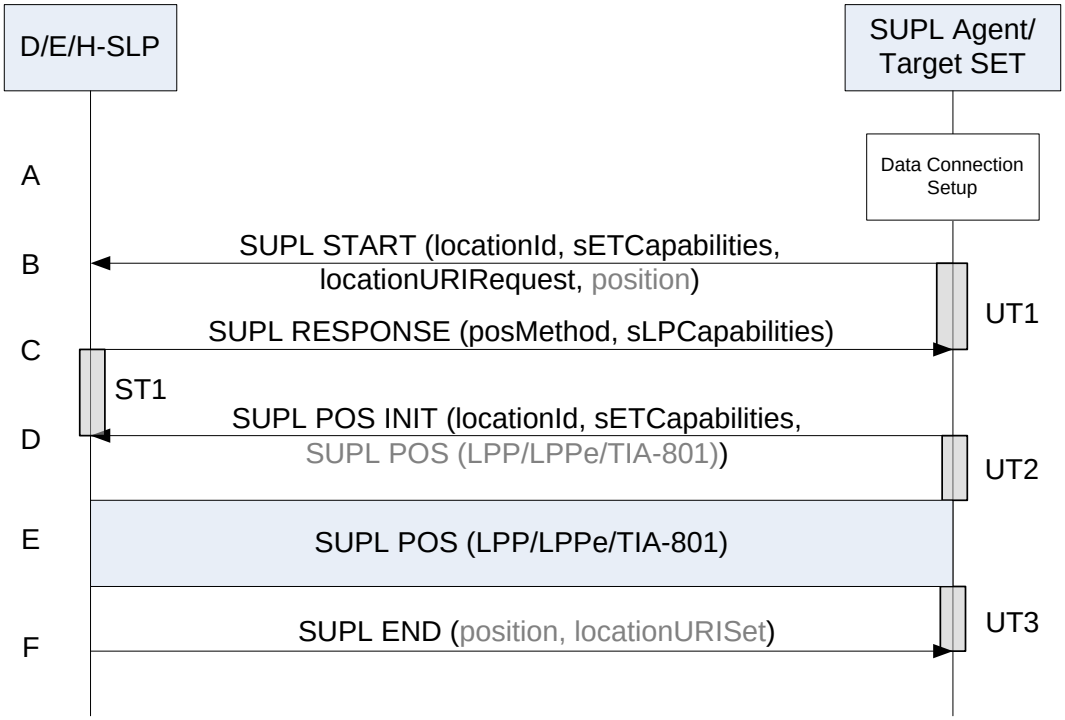

Figure 9: SET Initiated Location URI Request

A. The SET receives a request for a Location URI from a SUPL Agent (e.g., an application) on the SET. The SET takes appropriate action to establish a secure TLS connection to the D/H-SLP in the case of a normal SUPL Agent or to an E-SLP in the case of a SUPL Agent known to support only emergency services.

B. The SET SHALL use the default address provisioned by the Home Network for an H-SLP or the address provided or verified by the H-SLP or a Proxy D-SLP for a D-SLP or E-SLP to establish a secure TLS connection to the D/E/H-SLP and send a SUPL START message to start a positioning session with the D/E/H-SLP. The SUPL START message contains the the Location ID (*locationId*), SET capabilities (*sETCapabilities*) and a location URI Request (*locationURIRequest*). For a request to an E-SLP, the SUPL START message also contains the Emergency Services Indication (*emergencyServicesIndication*). The SET also includes its current position estimate if it is available.

C. The D/E/H-SLP proceeds to step F if it does not need to obtain the position of the SET or verify any position provided in step B. Otherwise, the D/E/H-SLP sends a SUPL RESPONSE message to the SET. The SUPL RESPONSE message contains the intended positioning method (*posMethod*) and the SLP Capabilities (sLPCapabilities).

D. The SET sends a SUPL POS INIT message to the D/E/H-SLP. The SET SHALL send the SUPL POS INIT message even if the SET does not support the intended positioning method indicated in SUPL RESPONSE. The SUPL POS INIT message contains the Location ID (*locationId*), SET capabilities (*sETCapabilities*) and optionally a SUPL POS message carrying LPP and/or TIA-801 positioning protocol messages in line with the D/E/H-SLP's positioning protocol capabilities (indicated in step C in *sLPCapabilities*). The SET MAY also provide its position, if this is supported (as part of LPP/LPPe/TIA-801 or explicitly through the optional position parameter). If a position retrieved in - or calculated based on information received in - the SUPL POS INIT message is available that meets the required QoP, the D/E/H-SLP MAY directly proceed to step F and not engage in a SUPL POS session.

E. SET and D/E/H-SLP engage in a SUPL POS message exchange to calculate a position. The positioning methods used for this session are determined based on the capabilities exchanged by the SET and the D/E/H-SLP during the SUPL POS message exchange or optionally in step D. The D/E/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 D/E/H-SLP (SET-Based).

F. Once any position calculation is complete, the D/E/H-SLP sends a SUPL END message to the SET indicating that the location session has ended and includes a Location URI Set (*locationURISet*). If the D/E/H-SLP cannot return a Location URI Set due to conditions such as location URIs not available, location URI not supported, SET not authorized to receive Location URI, etc,, the D/E/H-SLP SHALL send the SUPL END message containing appropriate status code to the SET. The D/E/H-SLP may also provide any position estimate computed in step E. The SET SHALL release the TLS connection to the D/E/H-SLP and release all resources related to this session. The D/E/H-SLP SHALL release all resources related to this session

5.1.2.7 D-SLP and E-SLP Authorization by the H-SLP

This procedure may be invoked by a SET to obtain authorization from the H-SLP for D-SLPs and/or E-SLPs discovered by the SET that are able to provide location services to the SET at or in the vicinity of its current location and/or to receive addresses of other authorized D-SLPs and/or E-SLPs from the H-SLP that are able to provide location services to the SET at or in the vicinity of its current location. The procedure may also be invoked by a SET to obtain authorization from the H-SLP for D-SLPs and/or E-SLPs discovered by the SET that provide location services at some location remote from the SET – e.g. a location that the SET's user expects to visit at some later time. The H-SLP is not compelled to provide authorization in such cases but may nevertheless chose to do so in order to improve location support. Note that there may be an arrangement between the provider of an H-SLP and the provider of a D-SLP or E-SLP to avoid service overload to the D/E-SLP. The arrangement may limit the number of SETs for which the D/E-SLP can be simultaneously authorized. Such an arrangement and the manner of its support (e.g. realtime versus non-realtime) are outside the scope of this specification.

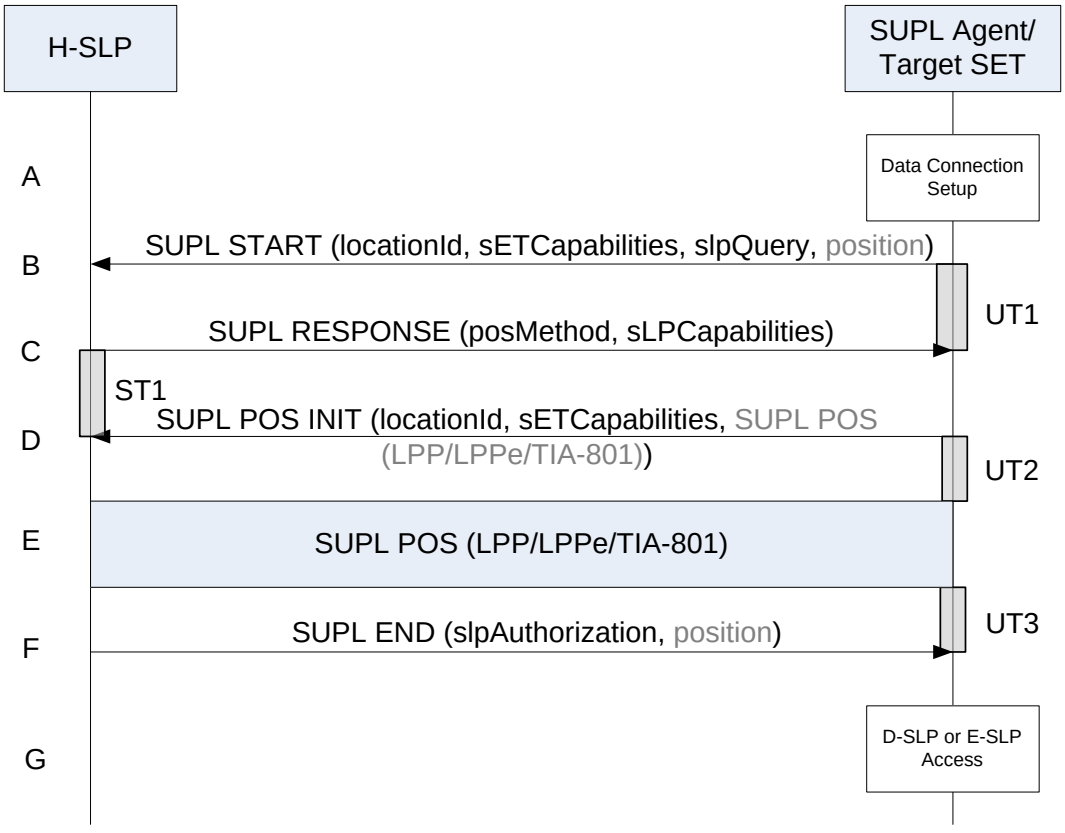

Figure 10: D-SLP and E-SLP Authorization by the H-SLP

A. The SET invokes the procedure to obtain the addresses of up to 10 authorized D-SLPs and/or up to 10 authorized E-SLPs from the H-SLP that are able to provide location services to the SET at or in the vicinity of its current location or, in some cases, at some remote location. The procedure MAY be invoked under any of the following conditions once any minimum retry period for any previous invocation of this procedure has expired:

a. The SET discovers a D-SLP or E-SLP address applicable to its current location or to a remote location that it would like to have authorized. Note that discovery of a D-SLP or E-SLP address is outside the scope of SUPL

b. In the case of D-SLP authorization, the SET is unable to obtain adequate positioning service from the H-SLP and either has no currently authorized D-SLPs or has currently authorized D-SLPs, access to which is forbidden due to geographic area or access network restrictions. Note that a D-SLP remains authorized until the associated service duration has expired.

c. In the case of E-SLP authorization, the SET is accessing a network that is not the home network, needs access to an E-SLP and either has no currently authorized E-SLPs or has currently authorized E-SLPs, access to which is forbidden due to geographic area or access network restrictions. Note that an E-SLP remains authorized until the associated service duration has expired.

The SET SHALL take appropriate action to establish a secure TLS connection to the H-SLP.

B. The SET SHALL use the default address provisioned by the Home Network to establish a secure TLS connection to the H-SLP and send a SUPL START message to start a positioning session with the H-SLP. The SUPL START message contains the Location ID (*locationId*) and the SET capabilities (*sETCapabilities*). The SUPL START message also contains an SLP Query parameter (*slpQuery*) indicating whether the SET requests D-SLP and/or E-SLP addresses. For a D-SLP request, the SET SHALL include a list of any D-SLP addresses currently authorized by the H-SLP and MAY include a list of preferred D-SLP addresses (e.g. discovered D-SLP addresses) and/or a list of not preferred D-SLP addresses (e.g. D-SLPs the SET could not previously obtain service from). An address on the first list MAY appear on the second or third list (but not on both). For an E-SLP request, the SET MAY include three lists of E-SLP addresses corresponding exactly to those for a D-SLP request. In the case of a request for a D-SLP address, the SET MAY also provide the QoP desired from the D-SLP. The SET SHALL also include its current position estimate if it is available.

C. The H-SLP proceeds to step F if it does not need to obtain the position of the SET or verify any position provided in step B. Otherwise, the H-SLP sends a SUPL RESPONSE message to the SET. The SUPL RESPONSE message contains the intended positioning method (*posMethod*) and the SLP Capabilities (sLPCapabilities).

D. The SET sends a SUPL POS INIT message to the H-SLP. The SET SHALL send the SUPL POS INIT message even if the SET does not support the intended positioning method indicated in SUPL RESPONSE. The SUPL POS INIT message contains the Location ID (*locationId*), SET capabilities (*sETCapabilities*) and optionally a SUPL POS message carrying LPP and/or TIA-801 positioning protocol messages in line with the H-SLP's positioning protocol capabilities (indicated in step C in *sLPCapabilities*). The SET MAY also provide its position, if this is supported (as part of LPP/LPPe/TIA-801 or explicitly through the optional position parameter). If a position retrieved in - or calculated based on information received in - the SUPL POS INIT message is available that meets the required QoP, the D/H-SLP MAY directly proceed to step F and not engage in a SUPL POS session.

E. SET and H-SLP engage in a SUPL POS message exchange to calculate a position. The positioning methods used for this session are determined based on the capabilities exchanged by the SET and the H-SLP during the SUPL POS message exchange or optionally in step D. 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).

F. Once any position calculation is complete, the H-SLP determines a new set of authorized D-SLP addresses if D-SLP addresses were requested and/or a new set of authorized E-SLP addresses if E-SLP addresses were requested. If the SET requested a D-SLP address and provided a QoP associated with this request in step B, the H-SLP MAY take the QoP into account as one factor in determining whether to provide any D-SLP addresses. The H-SLP sends a SUPL END message to the SET with an SLP Authorization parameter (*slpAuthorization*) containing a list of authorized D-SLP addresses if D-SLP addresses were requested and/or a list of authorized E-SLP addresses if E-SLP addresses were requested. The addresses in each list are included in priority order, highest priority first, and SHALL replace any previous list of authorized D-SLPs or E-SLPs that the SET may have received previously from the H-SLP. The lack of such a list or a list containing no addresses for a particular requested SLP type means that no addresses for this requested SLP type were authorized and the SET SHALL remove any SLPs of this type previously authorized by the H-SLP. Note that when a previous authorization for a Proxy D-SLP or Proxy E-SLP is removed, any authorizations for D-SLPs or E-SLPs received from the Proxy D-SLP or Proxy E-SLP SHALL also be removed. For

each provided D-SLP or E-SLP address, the H-SLP MAY include the service duration for which the SLP address shall be considered valid, the service area within which the SLP may be accessed, a list of serving access networks from which the SLP may be accessed and a combination type that defines how the service area and access network restrictions are to be combined. In the case of an authorized D-SLP address, the H-SLP MAY also provide a list of services that the SET is permitted to engage in with this D-SLP and MAY provide a preference for accessing a D-SLP versus accessing the H-SLP for any SET initiated location request. The H-SLP MAY also indicate if a D-SLP or E-SLP is a Proxy D-SLP or Proxy E-SLP, respectively, that is allowed to act as a proxy for the H-SLP and provide local D-SLP or E-SLP addresses, respectively, itself to the SET as described in the procedure for Figure 11. When D-SLP addresses are authorized by the H-SLP, the H-SLP MAY indicate whether it wishes to receive a notification from the SET whenever the SET changes access to a different D-SLP. The H-SLP MAY also indicate whether it wishes to receive such notifications only for SET access to D-SLPs that are authorized to provide network initiated services and/or for SET access to D-SLPs authorized by a Proxy D-SLP. Whether or not the H-SLP is able to return any authorized D-SLP and/or E-SLP addresses, the H-SLP may return a minimum retry period for repeating the D-SLP and E-SLP Authorization procedure. The absence of a minimum retry period SHALL be treated the same as a zero retry period. The H-SLP MAY also provide any position estimate computed in step E. The SET SHALL release the TLS connection to the H-SLP and release all resources related to this session. The H-SLP SHALL release all resources related to this session.

G. The SET MAY subsequently access for SET initiated location services any E-SLP or D-SLP authorized by the H-SLP in step F according to the following rules:

   a. D-SLPs and E-SLPs SHALL be accessed in priority order – where a lower priority address is accessed only when all higher priority addresses are precluded by some other condition or cannot provide service.

   b. A D-SLP or E-SLP MAY only be accessed so long as any service duration for the D-SLP or E-SLP has not expired.

      NOTE: A SET SHALL terminate any session in progress with a D-SLP or E-SLP when the service duration expires unless regulatory requirements in the case of an E-SLP require otherwise. In order to avoid loss of service, it is recommended that a SET request reauthorization from the H-SLP of a D/E-SLP that is currently being used some time (e.g. 5 to 10 minutes) before the service duration expires.

   c. A D-SLP or E-SLP MAY only be accessed if the SET satisfies any provided service area and access network restrictions. If the combination type is “AND”, the SET MUST be within the service area and using an access network provided for the D/E-SLP. If the combination type is “OR”, the SET MUST be within the service area or using an access network provided for the D/E-SLP. If the combination type is “Conditional OR”, the SET MUST be within the service area or if the SET cannot deteremine whether it is within the service area then the SET MUST be using an access network provided for the D/E-SLP.

      NOTE: A SET SHOULD use its most recent location estimate (current or previous) to determine any service area condition. The determination may be probabilistic (i.e. determining location within the service area with some probability). Before the conditions for accessing a D/E-SLP are fulfilled, the SET SHOULD NOT access the D/E-SLP to help verify a service area condition. After the access conditions are fulfilled, the SET SHOULD periodically re-verify them. If re-verification fails i.e. if the SET is no longer within the service area, the SET SHOULD cease access and terminate any ongoing sessions. Exact details of how these requirements are supported are implementation dependent.

   d. In the case of D-SLP access, a SET may only request an authorized service. This condition MAY be ignored when the H-SLP did not provide a list of authorized services.

   e. In the case of D-SLP access, the SET SHALL follow any preference provided for H-SLP access. If H-SLP access is indicated as “not allowed”, the SET SHALL NOT access the H-SLP (and thus must access a D-SLP) whenever the conditions for accessing at least one D-SLP are fulfilled. Note that this means the H-SLP will not be accessed even when no D-SLP can provide the required service if the SET has already attempted access to at least one D-SLP. If H-SLP access is indicated as “not preferred”, the SET SHALL only access the H-SLP if no D-SLP could provide the service. If H-SLP access is indicated as “preferred”, the SET shall only access a D-SLP after attempting (and failing) to obtain service from the H-SLP. If no preference is provided, the SET MAY decide its own preference for accessing a D-SLP versus the H-SLP.

f. If access to a D-SLP, E-SLP or the H-SLP fails (e.g. the SET cannot establish a secure IP connection or the D-SLP, E-SLP or H-SLP cannot provide the required service), a SET may access another D-SLP. E-SLP or the H-SLP according to the above rules.

For an Network Initiated service request from an authorized D-SLP, the SET MAY ignore the above restrictions as long as the D-SLP was authorized to support the particular Network Initiated service requested. Note that this means that a SET can accept a Network Initiated session request from an authorized D-SLP or E-SLP even when outside the service area of the D-SLP or E-SLP and/or when not using an allowed access network. For an Network Initiated service request from an E-SLP, whether authorized or not, the SET SHOULD first follow any local regulations regarding support. A D-SLP or E-SLP authorization SHALL be considered to be terminated once any service duration has expired. The SET may then remove any internal data associated with this D-SLP or E-SLP. Authorizations are also considered to expire for any D-SLPs or E-SLPs authorized by a Proxy D-SLP or Proxy E-SLP whose service duration has expired.

5.1.2.8 D-SLP or E-SLP Authorization by a Proxy D-SLP or Proxy E-SLP

This procedure may be invoked by a SET to obtain authorization from a Proxy D-SLP or Proxy E-SLP for D-SLPs or E-SLPs, respectively, that were discovered by the SET that are able to provide location services to the SET at or in the vicinity of its current location. The procedure may also be invoked to receive addresses of other authorized D-SLPs from a Proxy D-SLP that are able to provide location services to the SET at or in the vicinity of its current location. Authorization of D-SLPs or E-SLPs with a service area remote from the SET need not be supported by a Proxy D-SLP or Proxy E-SLP and such authorization should not be expected by the SET. A Proxy D-SLP or Proxy E-SLP is initially authorized by the H-SLP using the procedure for Figure 10. The H-SLP may also provide the serving area for the Proxy D/E-SLP and/or a list of access networks. When a SET satisfies all the conditions defined in step G in Figure 10 for accessing a particular Proxy D/E-SLP it may either access the Proxy D/E-SLP for location services or request authorization of other D-SLPs or E-SLPs by the Proxy D/E-SLP if these may provide better location services. Any D-SLPs or E-SLPs authorized by a Proxy D/E-SLP will be effectively restricted to providing location services for the SET within the service area for the Proxy D/E-SLP and/or from an access network authorized for the Proxy D/E-SLP according to how these restrictions are required to be combined. This is because the rules on D-SLP and E-SLP access (described further on) initially require the SET to verify access to the Proxy D/E-SLP before obtaining access to a D-SLP or E-SLP authorized by this Proxy SLP. The benefit to the H-SLP is that the H-SLP need not be aware of all D-SLPs and E-SLPs (e.g. serving small areas like shopping malls, airports, railway stations etc.) within the service area of a Proxy D/E-SLP. This benefit may be significant when the Proxy SLP is located in a different country to the H-SLP. Instead, the Proxy D/E-SLP can act as a proxy for the H-SLP in authorizing such additional D-SLPs or E-SLPs. Note that there may be an arrangement between the provider of a Proxy D/E-SLP and the provider of a D-SLP or E-SLP authorized by the Proxy D/E-SLP to avoid service overload to the D/E-SLP. The arrangement may limit the number of SETs for which the D/E-SLP can be simultaneously authorized. Such an arrangement and the manner of its support (e.g. realtime versus non-realtime) are outside the scope of this specification. A SET that supports D-SLP or E-SLP authorization from a Proxy D/E-SLP should make use of this in preference to obtaining authorization from the H-SLP whenever authorization of previously unauthorized D-SLPs or E-SLPs is needed and provided the SET also satisfies any service area or access network conditions for accessing a Proxy D/E-SLP.

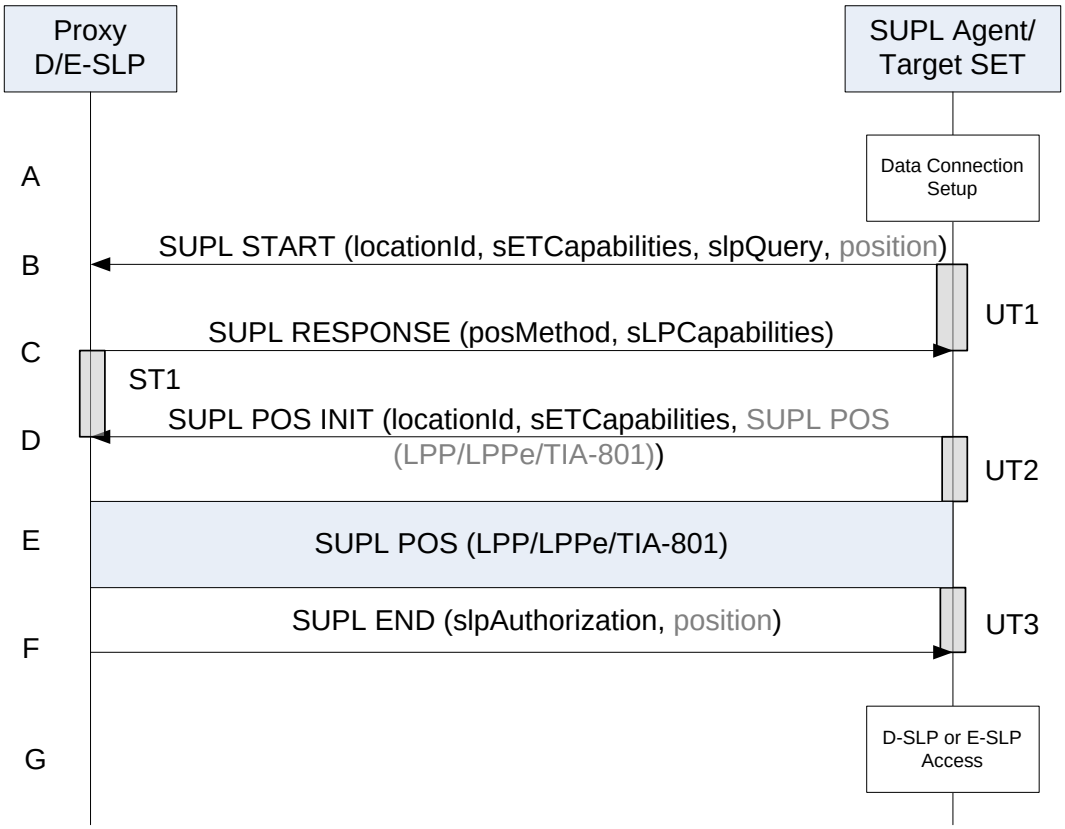

Figure 11: D-SLP or E-SLP Authorization by a Proxy D-SLP or E-SLP

A. The SET invokes the procedure to obtain the addresses of up to 10 authorized D-SLPs or up to 10 authorized E-SLPs from an authorized Proxy D-SLP or E-SLP, respectively. The Proxy D/E-SLP acts as a proxy for the H-SLP by authorizing D-SLPs or E-SLPs in its own serving area (e.g. D-SLPs or E-SLPs that are unknown to the H-SLP). The procedure MAY only be invoked when the SET is currently able to access the Proxy D/E-SLP due to being within any associated service area and/or using any associated access network and provided any minimum retry period for a previous invocation of the procedure to the Proxy D/E-SLP has expired. When these conditions are satisfied, the SET may invoke the procedure when any of the following additional conditions apply.

    a. The SET discovers a D-SLP or E-SLP address within the Proxy D/E-SLP service area and/or from an access network authorized for the Proxy D/E-SLP (according to how these conditions are required to be combined) that it would like to have authorized.

    b. In the case of D-SLP authorization, the SET is unable to obtain adequate positioning service from either the H-SLP or any authorized D-SLP (including the Proxy D-SLP and any D-SLPs currently authorized by the Proxy D-SLP).

    The SET SHALL take appropriate action to establish a secure TLS connection to the Proxy D/E-SLP.

B. The SET SHALL use the address provided by the H-SLP for the Proxy D/E-SLP to establish a secure TLS connection to the Proxy D/E-SLP and send a SUPL START message to start a positioning session with the Proxy D/E-SLP. The SUPL START message contains the Location ID (*locationId*) and the SET capabilities (*sETCapabilities*). The SUPL START message also contains an SLP Query parameter (*slpQuery*) indicating whether the SET requests D-SLP or E-SLP addresses. For a D-SLP request, the SET SHALL include a list of any D-SLP addresses currently authorized by the Proxy D-SLP and MAY include a list of any preferred D-SLP addresses (e.g. discovered D-SLP addresses) and/or a list of any not preferred D-SLP addresses. An address on the first list MAY appear on the second or third list (but not on both). For an E-SLP request, the SET MAY include three lists of E-SLP addresses corresponding exactly to those for a D-SLP request. In the case of a request for D-SLP addresses,

the SET MAY also provide the QoP desired from the D-SLP. The SET SHALL also include its current position estimate if it is available.

C. The Proxy D/E-SLP proceeds to step F if it does not need to obtain the position of the SET or verify any position provided in step B. Otherwise, the Proxy D/E-SLP sends a SUPL RESPONSE message to the SET. The SUPL RESPONSE contains the intended positioning method (*posMethod*) and the SLP Capabilities (sLPCapabilities).

D. The SET sends a SUPL POS INIT message to the Proxy D/E-SLP. The SET SHALL send the SUPL POS INIT message even if the SET does not support the intended positioning method indicated in SUPL RESPONSE. The SUPL POS INIT message contains the Location ID (*locationId*), SET capabilities (*sETCapabilities*) and optionally a SUPL POS message carrying LPP and/or TIA-801 positioning protocol messages in line with the Proxy D/E-SLP's positioning protocol capabilities (indicated in step C in *sLPCapabilities*). The SET MAY also provide its position, if this is supported (as part of LPP/LPPe/TIA-801 or explicitly through the optional position parameter). If a position retrieved in - or calculated based on information received in - the SUPL POS INIT message is available that meets the required QoP, the D/H-SLP MAY directly proceed to step F and not engage in a SUPL POS session.

E. SET and Proxy D/E-SLP engage in a SUPL POS message exchange to calculate a position. The positioning methods used for this session are determined based on the capabilities exchanged by the SET and the Proxy D/E-SLP during the SUPL POS message exchange or optionally in step D. The Proxy D/E-SLP calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance obtained from the Proxy D/E-SLP (SET-Based).

F. Once any position calculation is complete, the Proxy D/E-SLP determines a new set of authorized D-SLP addresses if D-SLP addresses were requested or a new set of authorized E-SLP addresses if E-SLP addresses were requested. If the SET requested D-SLP addresses and provided a QoP associated with this request in step B, a Proxy D-SLP MAY take the QoP into account as one factor in determining whether to provide any D-SLP address. The Proxy D/E-SLP sends a SUPL END message to the SET with an SLP Authorization parameter (*slpAuthorization*) containing a list of authorized D-SLP addresses if D-SLP addresses were requested or a list of authorized E-SLP addresses if E-SLP addresses were requested. The addresses in each list are included in priority order, highest priority first, and SHALL replace any previous list of authorized D-SLPs or E-SLPs that the SET may have received from the same Proxy D/E-SLP. D-SLPs and E-SLPs that were provided by the H-SLP or by another Proxy D/E-SLP are not affected and remain authorized according to the parameters provided by the H-SLP or other Proxy D/E-SLP. The lack of such a list from the Proxy D/E-SLP being queried or a list containing no addresses for a particular requested SLP type means that no addresses for this requested SLP type were authorized by the Proxy D/E-SLP and the SET SHALL remove any addresses previously authorized by the Proxy D/E-SLP. For each provided D-SLP or E-SLP address, the Proxy D/E-SLP MAY include the service duration for which the SLP address shall be considered valid, the service area within which the SLP address may be accessed, a list of serving access networks from which the SLP address may be accessed and a combination type that defines how the service area and access network restrictions are to be combined. In the case of a provided D-SLP address, the Proxy D-SLP SHOULD not provide a list of services that the SET is permitted to engage in with this D-SLP as this may conflict with the services authorized by the H-SLP for the Proxy D-SLP. Instead, the SET SHALL assume the same services that were previously authorized by the H-SLP for the Proxy D-SLP. The proxy D-SLP SHALL NOT provide a preference for accessing the H-SLP or provide a request for notifying the H-SLP when a D-SLP is accessed and the SET SHALL ignore any such indications if received. Whether or not the Proxy D/E-SLP is able to return authorized D-SLP and/or E-SLP addresses, the Proxy D/E MAY return a minimum retry period for repeating the D-SLP or E-SLP Authorization procedure to the same Proxy D/E-SLP. The absence of a minimum retry period is treated the same as a zero retry period. The SET SHALL release the TLS connection to the Proxy D/E-SLP and release all resources related to this session. The Proxy D/E-SLP SHALL release all resources related to this session. The SET shall ignore and not act upon (as specified in step G) any D-SLP or E-SLP authorized by a Proxy D/E-SLP so long as the same D-SLP or E-SLP is authorized by the H-SLP. The SET may retain and act separately upon (as specified in step G) any authorizations from different Proxy D/E-SLPs for the same D-SLP or E-SLP.

G. The SET MAY subsequently access any E-SLP or D-SLP provided by the Proxy D/E-SLP in step F for SET initiated location services according to the following rules which employ two levels of recursion:

    a. The SET SHALL initially follow the rules defined in step G of Figure 10 to determine whether to access the H-SLP or a D-SLP or E-SLP directly authorized by the H-SLP. If the SET determines that a Proxy D-SLP or Proxy E-SLP should be accessed and the Proxy D/E-SLP has itself authorized one or more other

SLPs, the SET SHALL follow the rules below to determine whether to access the Proxy D/E-SLP or an SLP authorized by the Proxy D/E-SLP.

b. D-SLPs or E-SLPs provided by the Proxy D/E-SLP SHALL be accessed in priority order – where a lower priority address is accessed only when all higher priority addresses are precluded by some other condition or cannot provide service.

c. A D-SLP or E-SLP MAY only be accessed so long as any service duration for the D-SLP or E-SLP has not expired.

NOTE: A SET SHALL terminate any session in progress with a D-SLP or E-SLP when the service duration expires unless regulatory requirements in the case of an E-SLP require otherwise. In order to avoid loss of service, it is recommended that a SET request reauthorization from the authorizing Proxy D/E-SLP of a D/E-SLP that is currently being used some time (e.g. 5 to 10 minutes) before the service duration expires.

d. A D-SLP or E-SLP provided by the Proxy D/E-SLP may only be accessed if the SET satisfies any service area and access network restrictions provided by the Proxy D/E-SLP. If the combination type is “AND”, the SET must be within the service area and using an access network provided for the D/E-SLP. If the combination type is “OR”, the SET must be within the service area or using an access network provided for the D/E-SLP. If the combination type is “Conditional OR”, the SET must be within the service area or if the SET cannot deteremine whether it is within the service area then the SET must be using an access network provided for the D/E-SLP.

NOTE: A SET SHOULD use its most recent location estimate (current or previous) to determine any service area condition. The determination may be probabilistic (i.e. determining location within the service area with some probability). Before the conditions for accessing a D/E-SLP are fulfilled, the SET SHOULD NOT access the D/E-SLP to help verify a service area condition. After the access conditions are fulfilled, the SET SHOULD periodically re-verify them. If re-verification fails, i.e.,if the SET is no longer within the service area, the SET SHOULD cease access and terminate any ongoing sessions. Exact details of how these requirements are supported are implementation dependent. In the case of D-SLP access, a SET SHALL only request a service authorized by the H-SLP for the Proxy D-SLP.

e. Preference SHOULD normally be given to accessing a D-SLP or E-SLP authorized by the Proxy D/E-SLP, provided this meets the previous conditions, rather than accessing the Proxy D/E-SLP.

f. If access to a D-SLP, E-SLP or the H-SLP fails (e.g. the SET cannot establish a secure IP connection or the D-SLP, E-SLP or H-SLP cannot provide the required service), a SET may access another D-SLP, E-SLP or the H-SLP according to the above rules.

For an Network Initiated service request from a D-SLP authorized by a Proxy D-SLP, the SET MAY ignore the above restrictions as long as the Proxy D-SLP was authorized by the H-SLP to support the particular Network Initiated service requested. Note that this means that a SET can accept an Network Initiated session request from a D/E-SLP authorized by an authorized Proxy D/E-SLP even when outside the service area of the former and/or when not using an allowed access network. However, privacy requirements (e.g. as defined for each Network Initiated service) should still be followed. For a Network Initiated service request from an E-SLP, whether authorized or not, the SET SHOULD first follow any local regulations regarding support. A D-SLP or E-SLP authorization from a Proxy D/E-SLP SHALL be considered to be terminated once any associated service duration for the D-SLP or E-SLP or for the parent Proxy D/E-SLP has expired. The SET may then remove any internal data associated with this D-SLP or E-SLP.

5.1.2.9 Unsolicited Authorization of D-SLPs and E-SLPs

This procedure may be invoked by the H-SLP or by a Proxy D-SLP or Proxy E-SLP to provide authorized D-SLP and/or E-SLP addresses to a SET. The procedure is only applicable when a SUPL END is sent by the D/E/H-SLP to normally terminate a SUPL session.

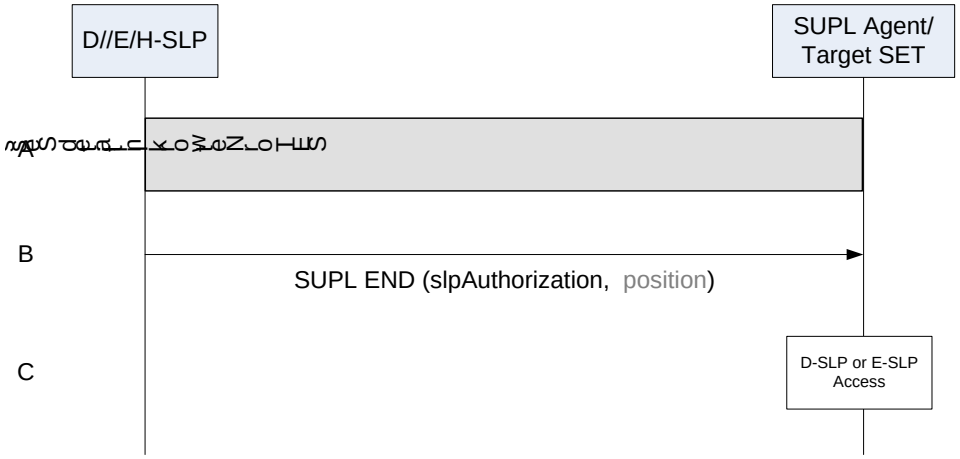

Figure 12: Unsolicited Authorization of D-SLPs and E-SLPs by a an H-SLP, Proxy D-SLP or Proxy E-SLP

A. The SET and D/E/H-SLP engage in an immediate or deferred SUPL session that may be initiated by the SET or by the D/E/H-SLP.

B. Once the SUPL session is complete, the D/E/H-SLP determines a set of authorized D-SLP addresses and/or E-SLP addresses which may be based on the current SET location and current access network(s) used by the SET – e.g. as obtained by the D/E/H-SLP in step A. The D/E/H-SLP sends a SUPL END message to the SET with an SLP Authorization parameter (*slpAuthorization*) containing a list of authorized D-SLP and/or E-SLP addresses. The addresses in each list are included in priority order, highest priority first, and replace any previous list of authorized D-SLPs or E-SLPs that the SET may have received from the same D/E/H-SLP. D-SLPs and E-SLPs that were provided by a different Proxy D/E-SLP are not affected unless the Proxy D/E-SLP has been replaced by other SLPs provided in the SUPL END by the H-SLP. In the latter case, any SLPs provided by such a replaced Proxy D/E-SLP are also removed.. For each provided D-SLP or E-SLP address, the D/E/H-SLP may include the service duration for which the SLP address shall be considered valid, the service area within which the SLP address may be accessed, a list of serving access networks from which the SLP address may be accessed and a combination type that defines how the service area and access network restrictions are to be combined. In the case of a provided D-SLP address, an H-SLP but not a Proxy D-SLP may provide a list of services that the SET is permitted to engage in with this D-SLP. An H-SLP but not a Proxy D-SLP may also provide a preference for accessing the H-SLP versus accessing a D-SLP and/or may provide a request for notifying the H-SLP when a D-SLP is accessed. The H/D/E-SLP may also return a minimum retry period for querying the same D/E/H-SLP for a further D-SLP amd/or E-SLP Authorization. The absence of a minimum retry period is treated the same as a zero retry period. The SET SHALL release the TLS connection to the D/E/H-SLP and release all resources related to the session. The D/E/H-SLP SHALL release all resources related to the session.

C. The SET may subsequently access any E-SLP or D-SLP provided by the D/E/H-SLP in step B for SET initiated location services and/or may accept network iniated location requests from any such D-SLP or E-SLP. The rules for such access are the same as those defined either in step G of Figure 10 in the case of a D-SLP or E-SLP authorized by the H-SLP or in step G of Figure 11 in the case of a D-SLP or E-SLP authorized by a Proxy D-SLP or Proxy E-SLP.

5.1.2.10 D-SLP Access Notification to the H-SLP

This procedure is invoked by a SET to notify the H-SLP about change of D-SLP access by the SET. This enables the H-SLP to track which D-SLP will have access to the SET to perform an Network Initiated location service – e.g. if a location request from an external LCS Agent sent to the H-SLP needs to be forwarded or redirected to the D-SLP. In the event that the H-SLP cannot be reached, the SET may reattempt the procedure at a later time and shall only notify the H-SLP of the most recently accessed D-SLP. To avoid being notified about D-SLPs that are not allowed to perform network initiated services, the H-SLP can restrict this procedure only to D-SLPs that are authorized to perform network initiated services. The H-SLP can also include or exclude notification of SET access to a D-SLP authorized by a Proxy D-SLP.

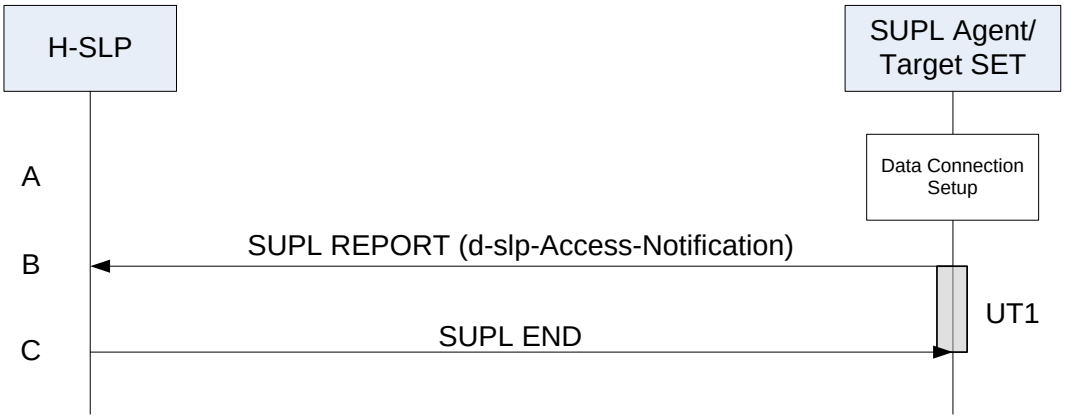

Figure 13: D-SLP Access Notification to the H-SLP

A. The SET accesses a D-SLP either for the first time or for the first time after it has accessed one or more other D-SLPs that were notified to the H-SLP. If the D-SLP was not authorized to perform network initiated services and the H-SLP requested notification only for D-SLPs authorized to perform network initiated services or if the D-SLP was authorized by a Proxy D-SLP and the H-SLP did not request notification of a D-SLPs authorized by a Proxy D-SLP, the SET takes no action. Otherwise, the SET takes appropriate action to establish a secure TLS connection to the H-SLP.

B. The SET SHALL use the default address provisioned by the Home Network for an H-SLP to establish a secure TLS connection to the H-SLP and send a SUPL REPORT message to the H-SLP. The SUPL REPORT message contains the address of the accessed D-SLP.

C. The H-SLP sends a SUPL END message to the SET indicating that the location session has ended. The H-SLP SHALL release all resources related to this session.

5.1.3 Session Info Query

The Session Info Query service is applicable to an H-SLP or D-SLP and enables the D/H-SLP to perform one or more of the following operations:

1. Query the SET for active SUPL session information.
2. Perform re-notification or re-notification and verification for active Network Initiated sessions.
3. Terminate any ongoing Triggered sessions without waiting for the next report interval.
4. Query the SET regarding currently authorized D-SLPs and/or E-SLPs (only applicable to an H-SLP or Proxy D-SLP).
5. Provide new D-SLP and/or E-SLP addresses (only permitted from an H-SLP or Proxy D-SLP).

Note that procedures 2, 3, 4 and 5 above may not work in all SET implementations. Thus, if one of these procedures is attempted and the SET does not support the service, the SET SHALL send the SUPL END message containing the session-id of the Session Info Query service and the status code "serviceNotSupported" to the D/H-SLP.

5.1.3.1 Session Info Query with Re-notification

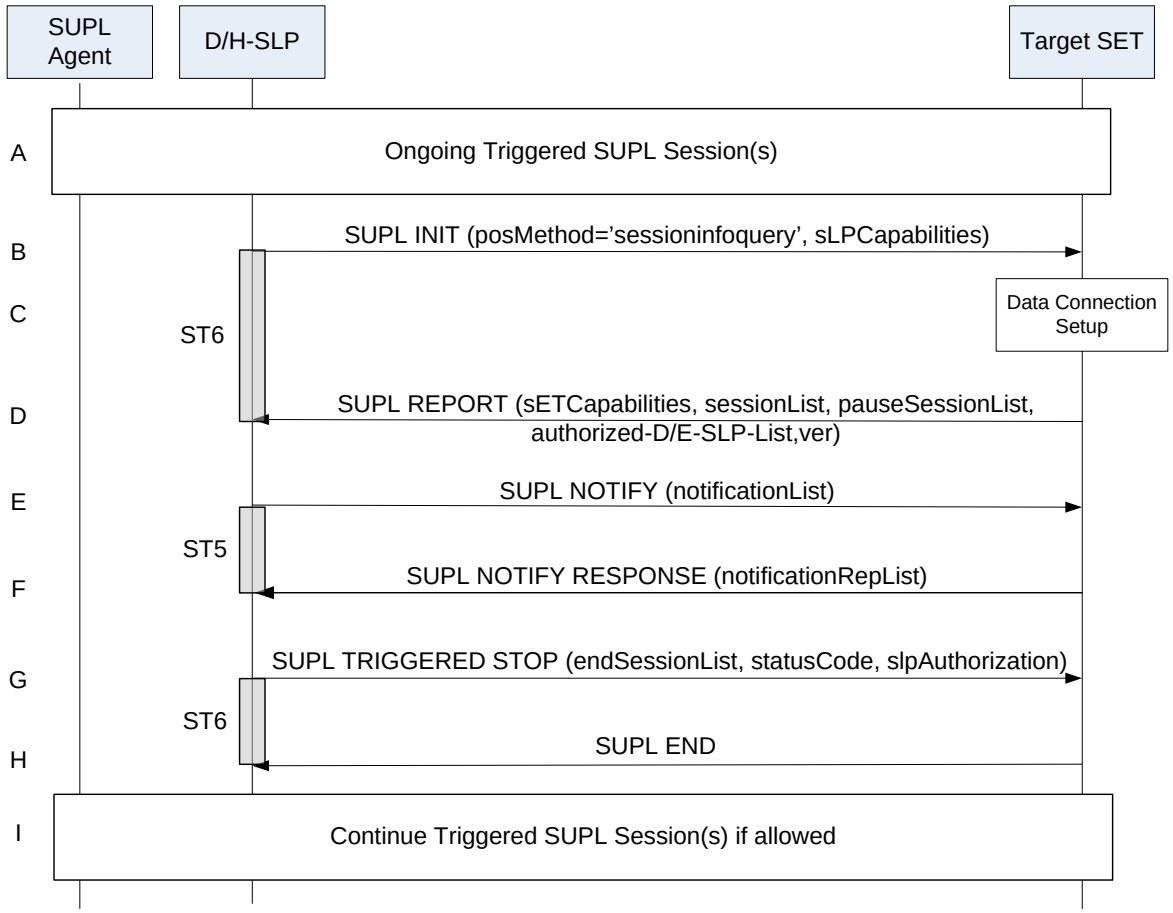

Figure 14: Session Info Query with Re-notification

A. One or more triggered SUPL sessions may be in progress.

B. The D/H-SLP initiates the "query for session info" session with the SET using the SUPL INIT message. The SUPL INIT message contains the positioning method (*posMethod*) and SLP Capabilities (*sLPCapabilities*). Query for session information is indicated by the positioning method (*posMethod*): *sessioninfoquery*. Before the SUPL INIT message is sent, the D/H-SLP also computes and stores a hash of the message.

C. The SET analyses the received SUPL INIT message. If found to be non authentic, the SET takes no further actions. Otherwise the SET takes needed action preparing for the establishment of a TLS connection with the D/H-SLP.

D. The SET returns the SUPL REPORT message to the D/H-SLP including a list of session-ids (*sessionList*) of all currently active sessions with the requesting D/H-SLP. For a request from an H-SLP, the SET SHALL also include a list of the addresses of currently authorized D-SLPs and/or E-SLPs (*Authorized-D/E-SLP-List*) including the addresses of any D-SLPs or E-SLPs currently authorized by a currently authorized Proxy D-SLP or Proxy E-SLP. For a request from a Proxy D-SLP, the SET SHALL include a list of the addresses of all D-SLPs (*Authorized-D-SLP-List*) currently authorized by this Proxy D-SLP. Currently authorized in this context means that any service duration provided earlier by the H-SLP or Proxy D-SLP for a D-SLP or E-SLP has not yet expired. The SET MAY also send the SET Capabilities (*sETCapabilities*) in the SUPL REPORT message. If any sessions are paused, the SET SHALL also include a list of session-ids (*pauseSessionList*) of all currently paused session. The SUPL REPORT message also contains a hash of the received SUPL INIT message (ver).

NOTE: The *sessionList* also includes any paused session(s) because the paused session is considered as an active session.

E. If re-notification or re-notification and verification is needed based upon a check of the subscriber privacy and the elapsed time since notification/verification last occurred for any active triggered sessions as indicated in the *sessionList* parameter, the SUPL NOTIFY message is sent to the SET including a list of session-ids of all sessions that needs re-notification or re-notification and verification (*notificationList*). The *notificationList* parameter also includes a notification type of each session. If there is no session that needs re-notification or re-notification and verification, the D/H-SLP SHALL directly send the SUPL END message to the SET. In the case of an H-SLP or Proxy D-SLP, the SUPL END MAY include an SLP Authorization that includes a list of authorized D-SLP addresses and/or, in the case of an H-SLP, a list of authorized E-SLP addresses. The contents and treatment of these lists SHALL be the same as that described in steps F and G of Figure 10 for an H-SLP Query or steps F and G of Figure 11 for a Proxy D-SLP Query except that if a list is not provided for a particular SLP type, the SET MAY continue to use the previous authorization for this SLP type. Note that if a list is provided that contains no SLP addresses, then the previous authorized list SHALL be removed. If the previous list contained any Proxy D/E-SLPs, then any authorization lists these provided SHALL also be removed.

F. The SET SHALL send the SUPL NOTIFY RESPONSE message to the D/H-SLP. If notification and verification was required in step E then the SUPL NOTIFY RESPONSE message includes a list of verification responses (*NotificationRespList*) from the user.

G. If the *NotificationRespList* received in step F contains one or more response types of "*Not Allowed*" to deny consent for the re-verification, the D/H-SLP sends the SUPL TRIGGERED STOP message to the SET including a list of session-ids of all sessions to cancel (*endSessionList*). The SUPL TRIGGERED STOP also contains a *statusCode* of "*consentDeniedByUser*" and may include an SLP Authorization. The SET SHALL release all resources related to sessions indicated in the *endSessionList* parameter and SHALL treat any SLP Authorization the same as in step E. If there is no session to cancel, the D/H-SLP SHALL directly sends the SUPL END message to the SET and may include an SLP Authorization which SHALL be treated by the SET the same as in step E.

H. If Step G is performed, the SET acknowledges that it has cancelled triggered sessions and interpreted any SLP Authorization with the SUPL END message sent back to the D/H-SLP. The SET SHALL release the TLS connection to the D/H-SLP and release all resources related to the Session Info Query session. The D/H-SLP SHALL release all resources related to the Session Info Query session.

I. Other remaining triggered SUPL session(s) may continue if applicable.

5.1.3.2 Session Info Query with Session Termination

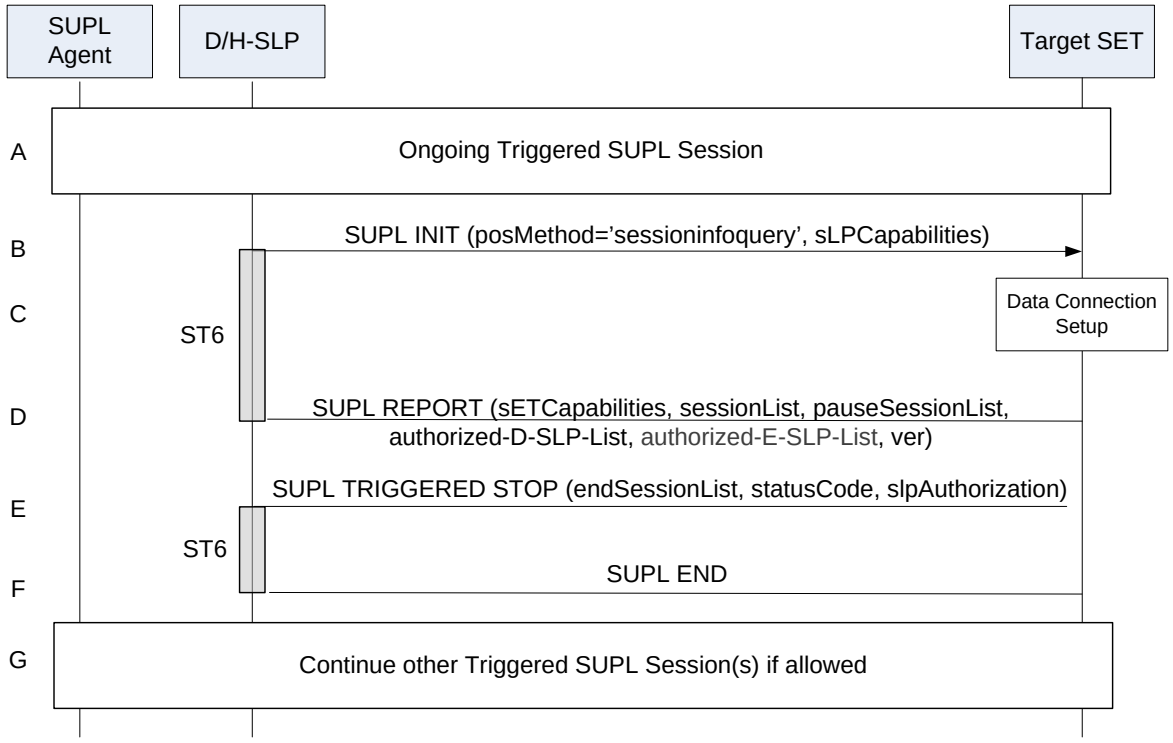

Figure 15: Session Info Query with Session Termination

A. One or more triggered SUPL sessions may be in progress.

B. The D/H-SLP initiates the "query for session info" session with the SET using the SUPL INIT message. The SUPL INIT message contains the positioning method (*posMethod*) and SLP Capabilities (*sLPCapabilities*). Query for session information is indicated by the positioning method (*posMethod*): *sessioninfoquery*. Before the SUPL INIT message is sent, the D/H-SLP also computes and stores a hash of the message.

C. The SET analyses the received SUPL INIT message. If found to be non authentic, the SET takes no further actions. Otherwise the SET takes needed action preparing for the establishment of a TLS connection with the D/H-SLP.

D. The SET returns the SUPL REPORT message to the D/H-SLP including a list of session-ids (*sessionList*) of all currently active sessions with the requesting D/H-SLP. For a request from an H-SLP, the SET SHALL also include a list of the addresses of currently authorized D-SLPs and/or E-SLPs including the addresses of any D-SLPs or E-SLPs currently authorized by a currently authorized Proxy D-SLP or Proxy E-SLP. For a request from a Proxy D-SLP, the SET SHALL include a list of the addresses of all D-SLPs currently authorized by this Proxy D-SLP. The SET MAY also send the SET Capabilities (*sETCapabilities*) in the SUPL REPORT message. If any sessions are paused, the SET SHALL also include a list of session-ids (*pauseSessionList*) of all currently paused session. The SUPL REPORT message also contains a hash of the received SUPL INIT message (ver).

E. The D/H-SLP sends the SUPL TRIGGERED STOP message to the SET to cancel any active and/or paused triggered session without waiting for the next periodic or area event trigger and in the case of an H-SLP it MAY include an SLP Authorization. The SUPL TRIGGERED STOP message contains a list of session-ids of all sessions to cancel (*endSessionList*) and a status code (*statusCode*) of "*sessionStopped*". The SET SHALL release all resources related to sessions indicated in the *endSessionList* parameter and SHALL treat any SLP Authorization from an H-SLP or Proxy D-SLP the same as in step E in Figure 14. If there is no session to cancel, the D/H-SLP SHALL directly send the SUPL END message to the SET and in the case of an H-SLP or Proxy D-SLP MAY include an SLP Authorization which SHALL be treated by the SET the same as in step E in Figure 14.

F. The SET acknowledges that it has cancelled triggered sessions and interpreted any SLP Authorization with the SUPL END message sent back to the D/H-SLP. The SET SHALL release the TLS connection to the D/H-SLP and release all resources related to the Session Info Query session. The D/H-SLP SHALL release all resources related to the Session Info Query session.

G. Triggered SUPL session(s) MAY continue if applicable.

5.1.4 Exception Procedures

5.1.4.1 SET does not allow Positioning

After receiving a SUPL INIT message the SET executes the notification/verification procedure. In this scenario, the subscriber rejects the location request. The call flow shown in Figure 16 applies to both roaming and non-roaming scenarios.

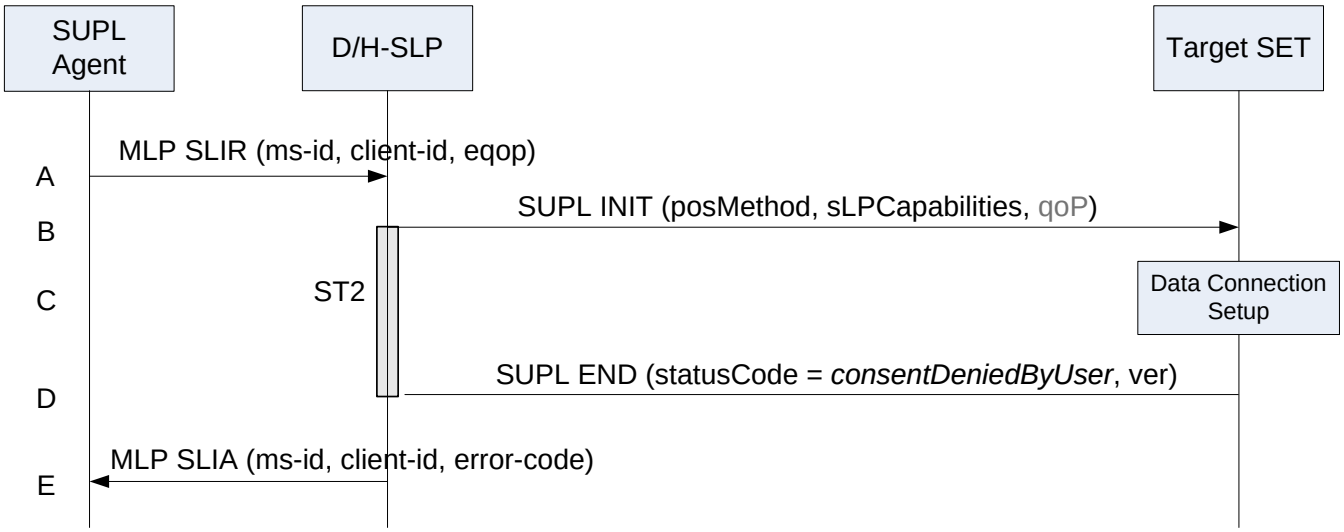

Figure 16: Network Initiated SET User denies Positioning for non roaming

A. SUPL Agent sends an MLP SLIR message to the D/H-SLP, with which the SUPL Agent is associated. The D/H-SLP SHALL authenticate the SUPL Agent and check if the SUPL Agent is authorized for the service it requested, based on the client-id received. Further, based on the received ms-id the D/H-SLP SHALL apply subscriber privacy against the client-id.

B. The D/H-SLP initiates the location session with the SET using the SUPL INIT message. The SUPL INIT message contains the intended positioning method (*posMethod*). In this case the result of the privacy check in Step A indicated that notification or verification to the target subscriber is needed, and the D/H-SLP therefore includes the Notification element in the SUPL INIT message.

C. The SET analyses the received SUPL INIT message. If found to be non authentic, the SET takes no further action. Otherwise the SET takes needed action for establishing or resuming a secure TLS connection.

D. The SET SHALL establish a secure connection to the D/H-SLP. The SET evaluates the notification rules and alerts the subscriber of the position request. In this case the user rejects the location request, either by explicit action or implicitly by not responding to the notification, and the SET returns to the D/H-SLP a SUPL END message containing the hash of the received SUPL INIT message (ver) and the status code *consentDeniedByUser*.

E. The D/H-SLP sends the position response, containing the ms-id, client-id, and the appropriate error-code back to the SUPL Agent in an MLP SLIA message.

5.1.4.2 SUPL Protocol Error

When during a SUPL session the D/H-SLP or the SET receive 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 the protocol error (Figure 17).

Possible protocol error cases are

- 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 used by the SUPL session. When an invalid session-id has been received, the invalid session-id shall be returned to the sending entity along with the appropriate 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.

After the SUPL END message has been sent, D/H-SLP and SET release the resources related to the aborted session.

A SUPL INIT message that is found to be non-authentic (see section 6.3.3) does not constitute a protocol error and no SUPL END message shall be sent.

For network initiated scenarios, the D/H-SLP notifies the SUPL Agent of the error if no position estimate could be calculated based on available information (e.g. previously computed position which meets the QoP, etc.). If a position estimate is available and the privacy check (notification and/or verification) has been passed successfully, the D/H-SLP sends the position estimate to the SUPL Agent.

The described procedure only applies to protocol errors on the SUPL ULP layer. If protocol errors are encountered on the positioning protocol layer (LPP and/or TIA-801), the protocol errors are handled by the positioning protocols.

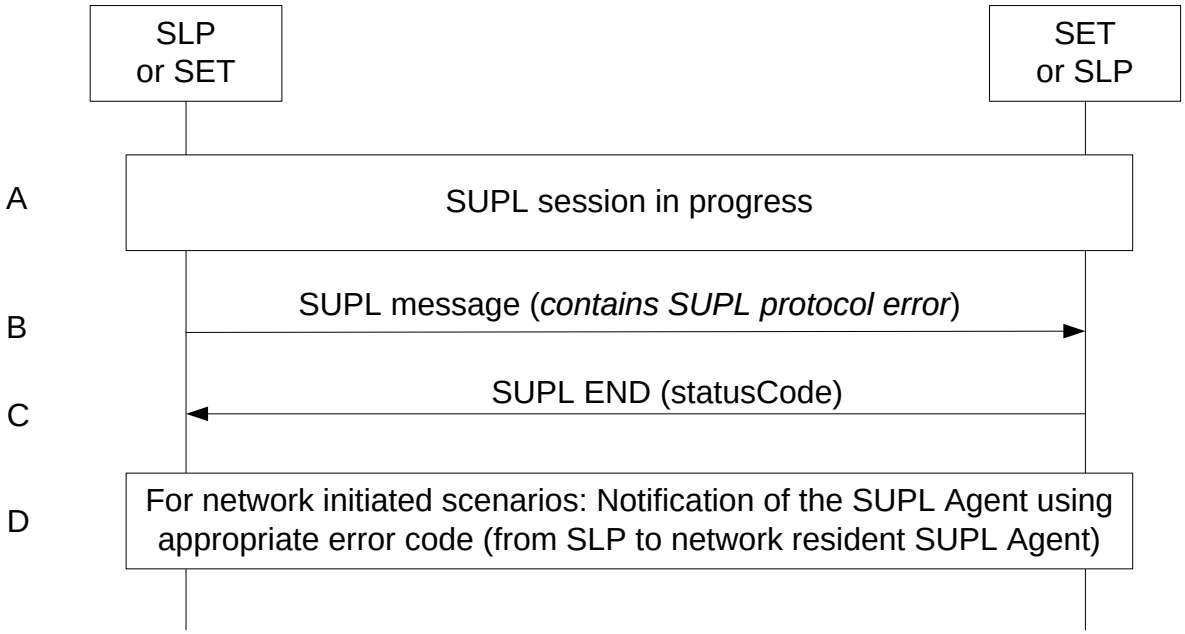

Figure 17: SUPL Protocol Error

A. A SUPL session is in progress.

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).

C. The recipient (either the SLP or SET) of the SUPL message containing the protocol error responds with a SUPL END message including the status code for the specific protocol error. Both sides release all resources related to this session.

D. For network initiated applications: the SLP notifies the SUPL Agent using an appropriate error code.

5.1.4.3 SUPL timer expiration

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

5.1.4.4 Notification based on current location – SET denies permission

During a Network Initiated SUPL session when the SET is asked for verification based on current location, if the SET returns a SUPL NOTIFY RESPONSE with a response type of Not Allowed, the D/H-SLP SHALL respond with a SUPL END with status code “consentDeniedByUser”.

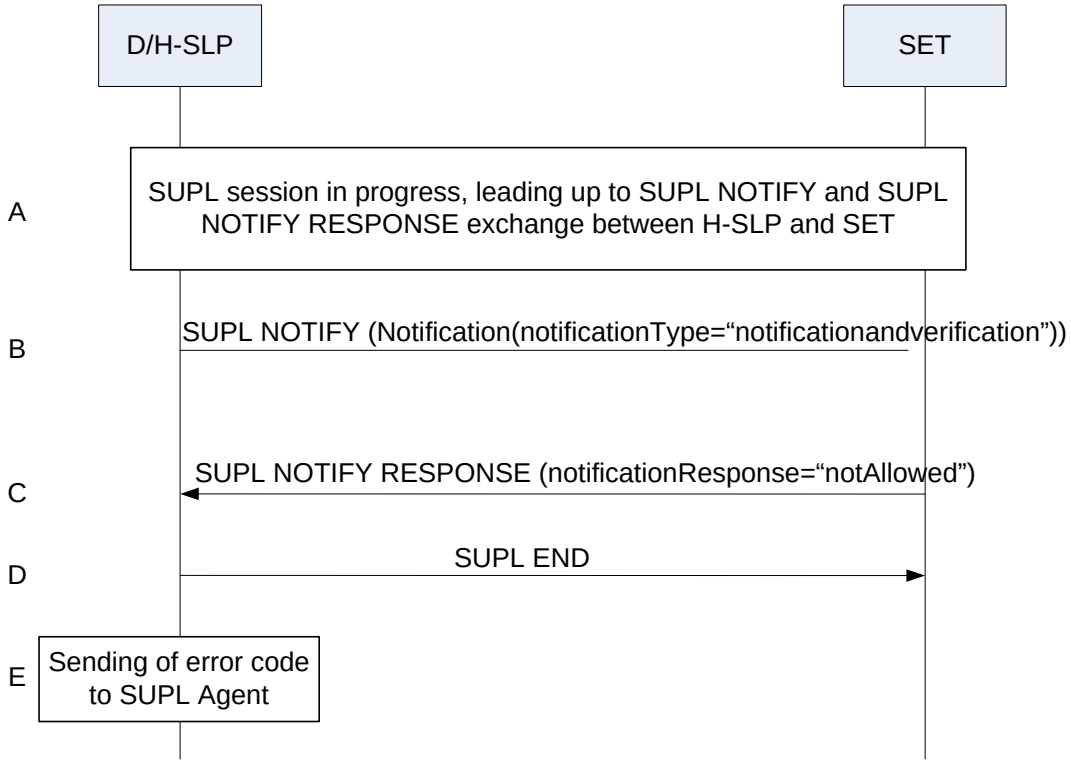

Figure 18: Notification based on current location – SET denies permission

NOTE: If the SUPL NOTIFY message contains notification type "notification only", the contents of the SUPL NOTIFY RESPONSE message SHALL be ignored by the D/H-SLP and the SUPL session SHALL continue.

A. A Network Initiated immediate fix session is in progress (either roaming or non-roaming) and has progressed to the point where a SUPL NOTIFY message with Notification Type of "notification and verification" is sent from the D/H-SLP to the SET.

B. The D/H-SLP sends a SUPL NOTIFY message with notification type of "notification and verification" to the SET.

C. The SET responds with a SUPL NOTIFY RESPONSE containing a notification response of "not allowed" indicating that the location determination has been denied.

D. The D/H-SLP SHALL send a SUPL END with statusCode "consentDeniedByUser" to the SET. The SET SHALL release all resources related to this session.

E. The D/H-SLP then notifies the SUPL Agent of the failed location session using the appropriate error code.

5.1.4.5 Invalid SET Access to a D/E-SLP

The following procedure is used when a SET attempts to access a D-SLP or E-SLP for which access is not authorized – e.g. if the H-SLP had not authorized the D/E-SLP or if the SET is not within service area for the D/E-SLP or is not using an allowed access network.

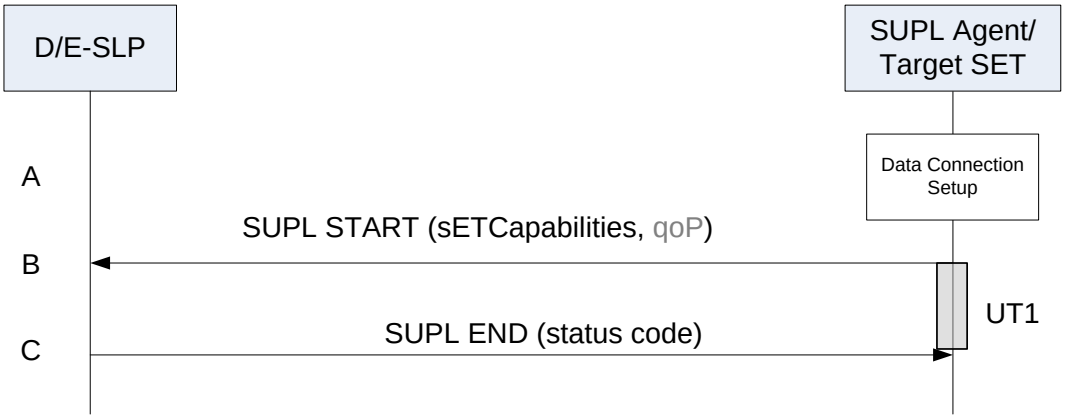

Figure 19: Invalid SET Access to a D/E-SLP

A. The SET receives a position request from a SUPL Agent (e.g., an application) on the SET. The SET takes appropriate action to establish a secure TLS connection to the D-SLP or E-SLP.

B. The SET establishes a secure TLS connection to the D/E-SLP and sends a SUPL START message to start a positioning session with the D/E-SLP. The SUPL START message contains the SET capabilities (*sETCapabilities*) and optionally the desired QoP.

NOTE: If the D/E-SLP cannot authenticate the SET, the procedure will terminate after step B.

C. If the D/E-SLP verifies that the SET is not allowed to access the D/E-SLP, the D/E-SLP returns a SUPL END containing a status code indicating whether access is not authorized or whether access is authorized but not allowed from the SET's current location or current access network.

NOTE: A D/E-SLP may use information received in or associated with the SUPL START to determine whether access is allowed (e.g. a position estimate or the SET IP address). However, it is possible that the D/E-SLP may not determine that access is not allowed until after certain positioning information has been received from the SET (e.g. in a SUPL POS INIT and/or SUPL POS message). In that case, step C may be deferred until after certain additional SUPL messages have been exchanged between the D/E-SLP and the SET.

5.1.4.6 Non supported result type or reference point

When during initiation of a SUPL session the D/H-SLP receive a request for a result type or reference point that is not supported, the D/H-SLP shall send a SUPL END message to the sending entity including a status code indicating the cause.

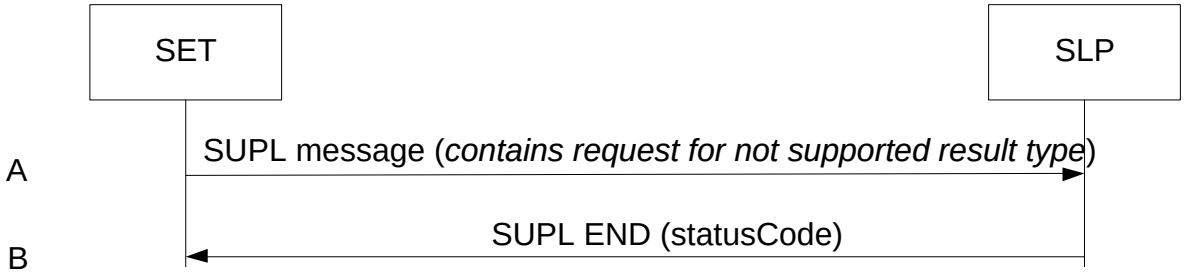

Figure 20: Not supported result type

A. A SUPL message sent from a SET contains a request for not supported result type (i.e. position relative SET) or a not supported reference point.

B. The SLP responds with a SUPL END message including the status code for the specific cause. Both sides release all resources related to this session.

5.2 Emergency Services

Regulatory requirements will dictate the conditions under which the SET should accept emergency SUPL INIT messages. For example, in many cases, the regulatory requirements only require the SET to process emergency SUPL INIT messages if the SET is currently engaged in an emergency call. Consequently, the conditions (under which the SET should accept emergency SUPL INIT messages) are outside the scope of this document.

5.2.1 Network Initiated Non-Roaming

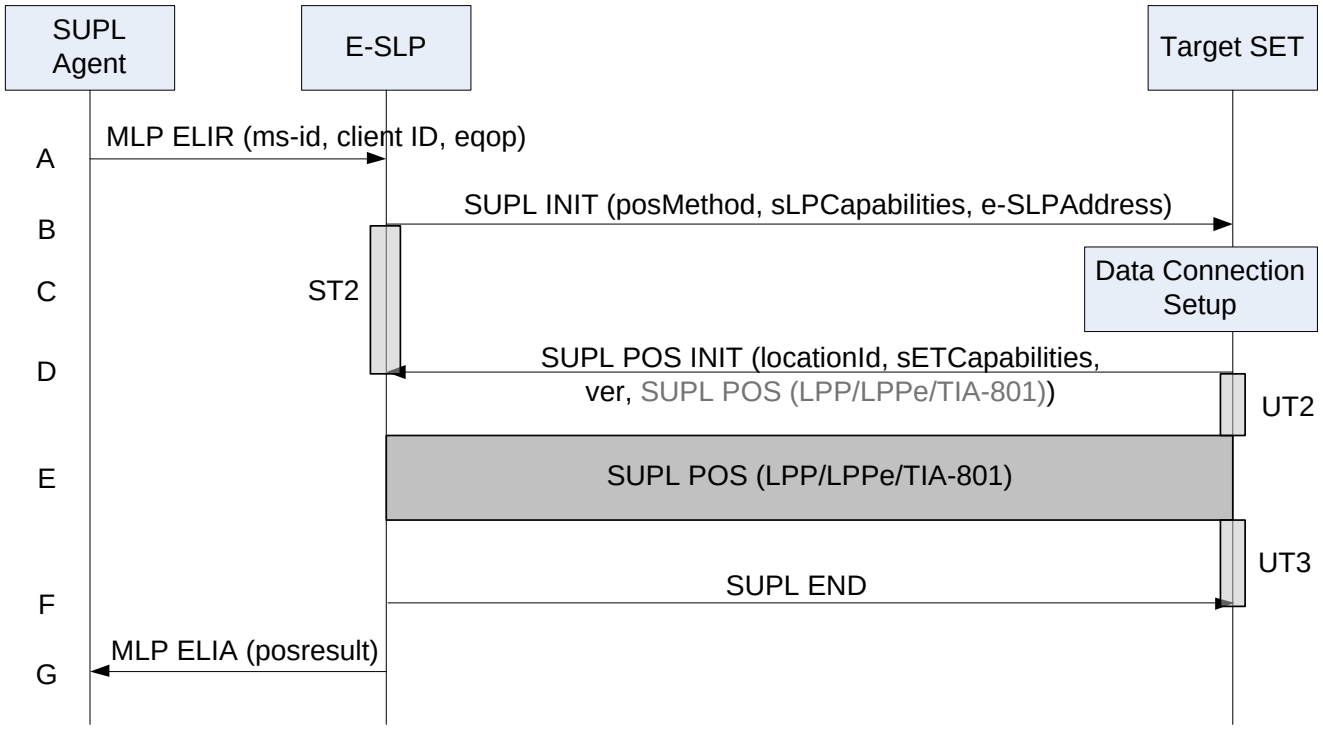

Figure 21: Network Initiated Emergency Services Non-Roaming

A. SUPL Agent issues an MLP ELIR message to the E-SLP, with which SUPL Agent is associated. The MLP ELIR message may include the SET IP address and location data. The E-SLP shall authenticate the SUPL Agent and check if the SUPL Agent is authorized for the service it requested, based on the client-id received.
If a previously computed position which meets the requested QoP is available at the E-SLP and no notification and verification is required according to local regulatory requirements, the E-SLP SHALL directly proceed to step G. If notification and verification or notification only is required, the E-SLP SHALL proceed to step B.

B. The E-SLP initiates the location session with the SET using the SUPL INIT message. The SUPL INIT message contains the intended positioning method (*posMethod*), the SLP Capabilities (*sLPCapabilities*) and optionally the *QoP*. The SUPL INIT SHALL contain the E-SLP address if the E-SLP is not the H-SLP for the SET. The E-SLP SHALL also include the Notification element in the SUPL INIT message indicating location for emergency services and, according to local regulatory requirements, whether notification or verification to the target SET is or is not required. Before the SUPL INIT message is sent the E-SLP also computes and stores a hash of the message.
If in step A the E-SLP decided to use a previously computed position, the SUPL INIT message SHALL indicate this in a 'no position' posmethod parameter value and the SET SHALL respond with a SUPL END message carrying the results of the verification process (access granted, or access denied). If no explicit verification is required (notification only) the SET SHALL respond with a SUPL END message. The E-SLP SHALL then directly proceed to step G.

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

C. The SET takes needed action preparing for establishment or resumption of a secure connection.

D. The SET evaluates the Notification rules and takes appropriate action. The SET SHALL establish a TLS connection to the E-SLP using either the provided E-SLP address or, if no E-SLP address was provided in step B, the default E-SLP address. The SET then sends a SUPL POS INIT message to start a positioning session with the E-SLP. The SET SHALL send the SUPL POS INIT message even if the SET supported positioning technologies do not include the intended positioning method indicated in the SUPL INIT message. The SUPL POS INIT message contains the Location ID (*locationId*), SET capabilities (*sETCapabilities*) and the hash (*ver*) of the received SUPL INIT message calculated in step B. The SUPL POS INIT message MAY also include a SUPL POS message carrying LPP and/or TIA-801 positioning protocol messages in line with the E-SLP's positioning protocol capabilities (indicated in step B in *sLPCapabilities*). The SET MAY also provide its position, if this is supported (as part of LPP/LPPe/TIA-801 or explicitly through the optional position parameter). If a position retrieved in - or calculated based on information received in - the SUPL POS INIT message is available that meets the required QoP, the D/H-SLP MAY directly proceed to step F and not engage in a SUPL POS session.

E. SET and E-SLP engage in a SUPL POS message exchange to calculate a position. The positioning methods and positioning protocol used for this session are determined based on the capabilities exchanged by the SET and the E-SLP during the SUPL POS message exchange or optionally in step D. The E-SLP calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance obtained from the E-SLP (SET-Based)

F. Once the position calculation is complete, the E-SLP sends a SUPL END message to the SET indicating that the location session has ended. The SET SHALL release the TLS connection to the E-SLP and release all resources related to this session.

G. The E-SLP sends the position estimate (*posresult*) back to the SUPL Agent in an MLP ELIA message and the E-SLP SHALL release all resources related to this session.

5.2.2 Network Initiated Roaming

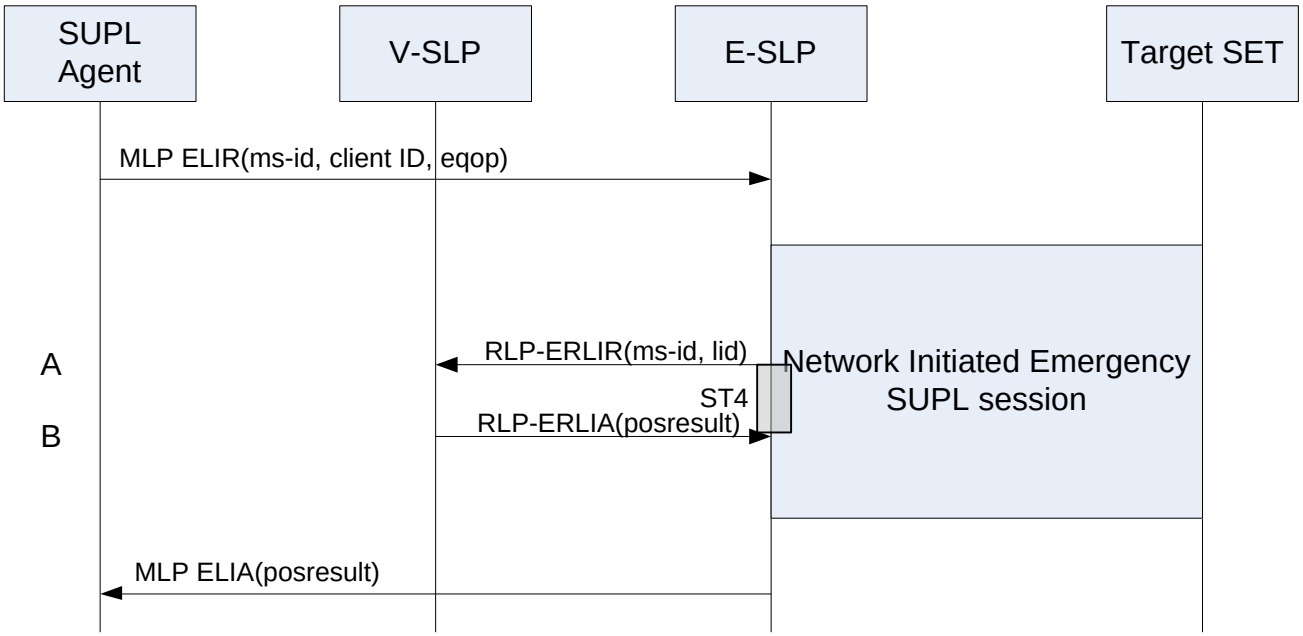

Figure 22: Network Initiated Emergency Services Roaming

For Network Initiated roaming, the ULP message exchange is the same as for non-roaming (see Figure 21). The ULP message exchange between SET and E-SLP is therefore not explicitly shown in Figure 22 but only indicated as "Network Initiated Emergency SUPL session" in the diagram. The V-SLP is invoked if and when the E-SLP requires translation of a cell or access point id into a position estimate.

A. In the course of the emergency SUPL session, the E-SLP requires translation of a cell or access point id into a position estimate. Since the SET is SUPL roaming, the E-SLP is unable to perform the translation on its own. The E-SLP therefore engages the V-SLP by sending an RLP-ERLIR message to the V-SLP including the ms-id and the location id (cell or access point id).

B. The V-SLP translates the received cell or access point id into a position estimate and returns an RLP-ERLIA message including the position (*posresult*) to the E-SLP.

5.2.3 SET Initiated Non-Roaming

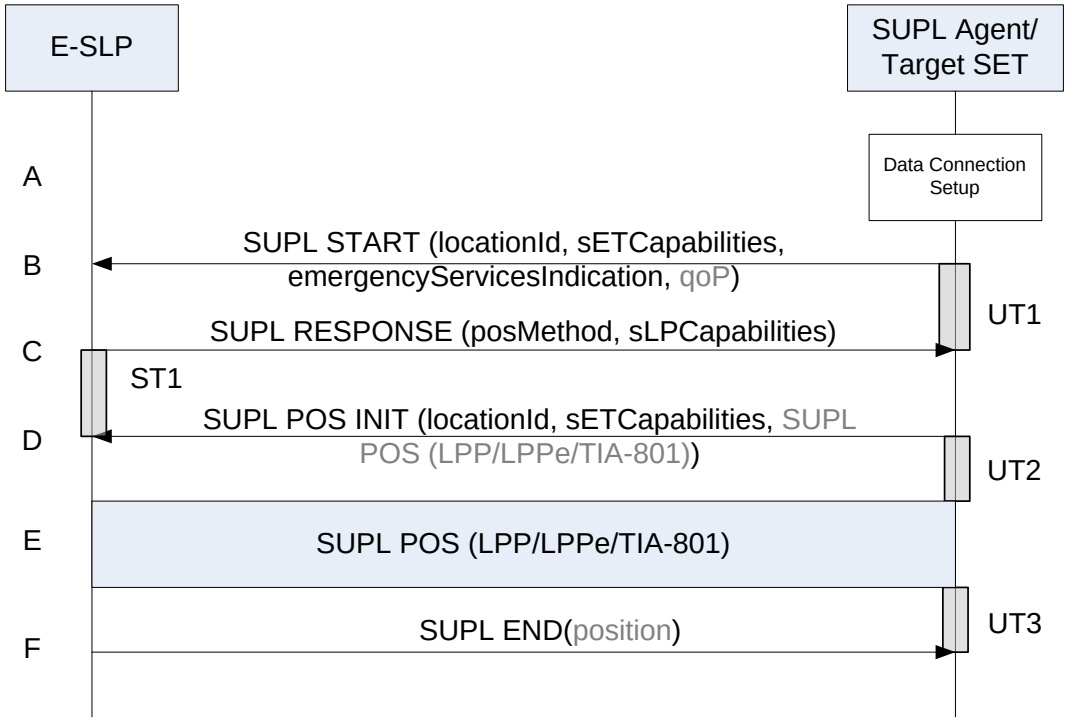

Figure 23: SET Initiated Emergency Services Non-Roaming

A. The SET receives a position request from a SUPL Agent (e.g., an application) on the SET that supports emergency services – e.g. an application invoked following dialling of an emergency call by the SET user. The SET takes appropriate action to establish a secure TLS connection to an E-SLP authorized by either the H-SLP or by a Proxy E-SLP authorized by the H-SLP.

B. The SET SHALL use the E-SLP address provided or verified by the H-SLP or by an authorized Proxy E-SLP to establish a secure TLS connection to the E-SLP and send a SUPL START message to start a positioning session with the E-SLP. The SUPL START message contains the Location ID (*locationId*), SET capabilities (*sETCapabilities*) the Emergency Services Indication (*emergencyServicesIndication*) and optionally the desired QoP.
If a previously computed position which meets the requested QoP is available at the E-SLP, the E-SLP SHALL directly proceed to step F and send a SUPL END message to the SET including the position result (*position*).

C. The E-SLP sends a SUPL RESPONSE message to the SET. The SUPL RESPONSE contains the intended positioning method (*posMethod*) and the SLP Capabilities (sLPCapabilities).

D. The SET sends a SUPL POS INIT message to the E-SLP. The SET SHALL send the SUPL POS INIT message even if the SET does not support the intended positioning method indicated in SUPL RESPONSE. The SUPL POS INIT message contains the Location ID (*locationId*), SET capabilities (*sETCapabilities*) and optionally a SUPL POS message carrying LPP/LPPe and/or TIA-801 positioning protocol messages in line with the E-SLP's positioning protocol capabilities (indicated in step C in *sLPCapabilities*). The SET MAY also provide its position, if this is

supported (as part of LPP/LPPe/TIA-801 or explicitly through the optional position parameter). If a position retrieved in - or calculated based on information received in - the SUPL POS INIT message is available that meets the required QoP, the D/H-SLP MAY directly proceed to step F and not engage in a SUPL POS session.

E. SET and E-SLP engage in a SUPL POS message exchange to calculate a position. The positioning methods used for this session are determined based on the capabilities exchanged by the SET and the E-SLP during the SUPL POS message exchange or optionally in step D. The E-SLP calculates the position estimate based on the received positioning measurements (SET-Assisted) or the SET calculates the position estimate based on assistance obtained from the E-SLP (SET-Based).

F. Once the position calculation is complete, the E-SLP sends a SUPL END message to the SET indicating that the location session has ended. If required, the E-SLP MAY also send the position result (position) in SUPL END. The SET SHALL release the TLS connection to the E-SLP and release all resources related to this session. The E-SLP SHALL release all resources related to this session.

5.2.4 SET Initiated Roaming

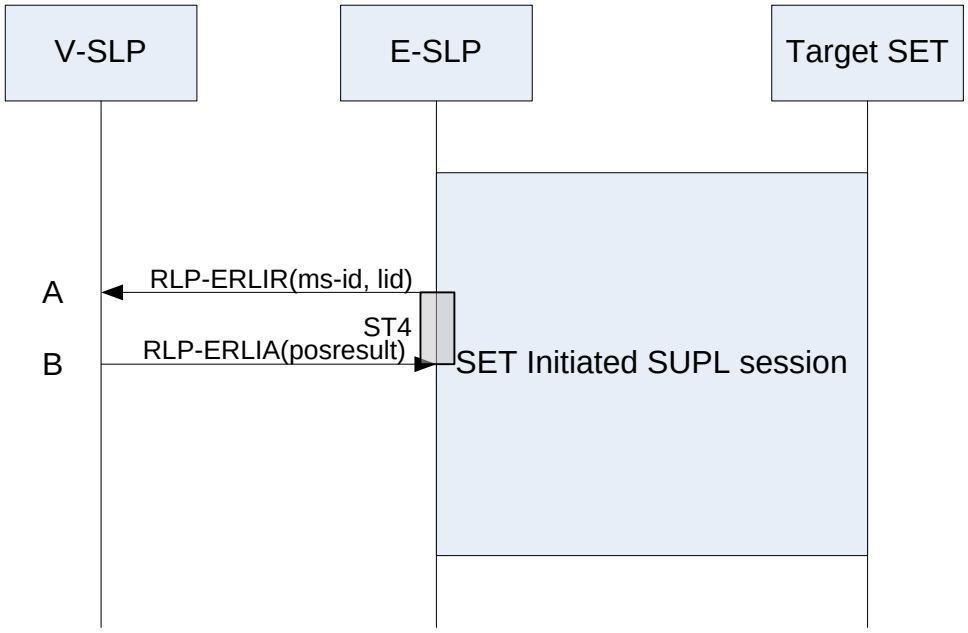

Figure 24: SET Initiated Emergency Services Roaming

For SET Initiated roaming, the ULP message exchange is the same as for non-roaming (see Figure 23). The ULP message exchange between SET and E-SLP is therefore not explicitly shown in Figure 24 but only indicated as “SET Initiated SUPL session” in the diagram. The V-SLP is invoked if and when the E-SLP requires translation of a cell or access point id into a position estimate.

A. In the course of the SUPL session, the E-SLP requires translation of a cell or access point id into a position estimate. Since the SET is SUPL roaming, the E-SLP is unable to perform the translation on its own. The E-SLP therefore engages the V-SLP by sending an RLP-ERLIR message including the ms-id and the location id (cell or access point id).

B. The V-SLP translates the received cell or access point id into a position estimate and returns an RLP-ERLIA message including the position (*posresult*) to the E-SLP.

5.3 Deferred Services

5.3.1 Network Initiated Triggered Periodic

For Network Initiated services, the SUPL Agent resides within the network and the service request is directed at the SLP. This section describes the call flows for Network Initiated Periodic Triggered services. The periodic trigger mechanism resides in the SET which means the SET periodically initiates actions required to determine a position estimate.

Whenever in the course of a Periodic Trigger session the SET needs to send a ULP message to the SLP, the SET SHALL check whether an existing TLS session already exists and – if one exists - reuse that existing TLS session. Otherwise the SET SHALL take appropriate action to resume a suspended TLS session, or establish a new TLS connection. Details of the TLS session (establishment, release, etc.) are not shown in this section.

5.3.1.1 Triggered Periodic – Non Roaming

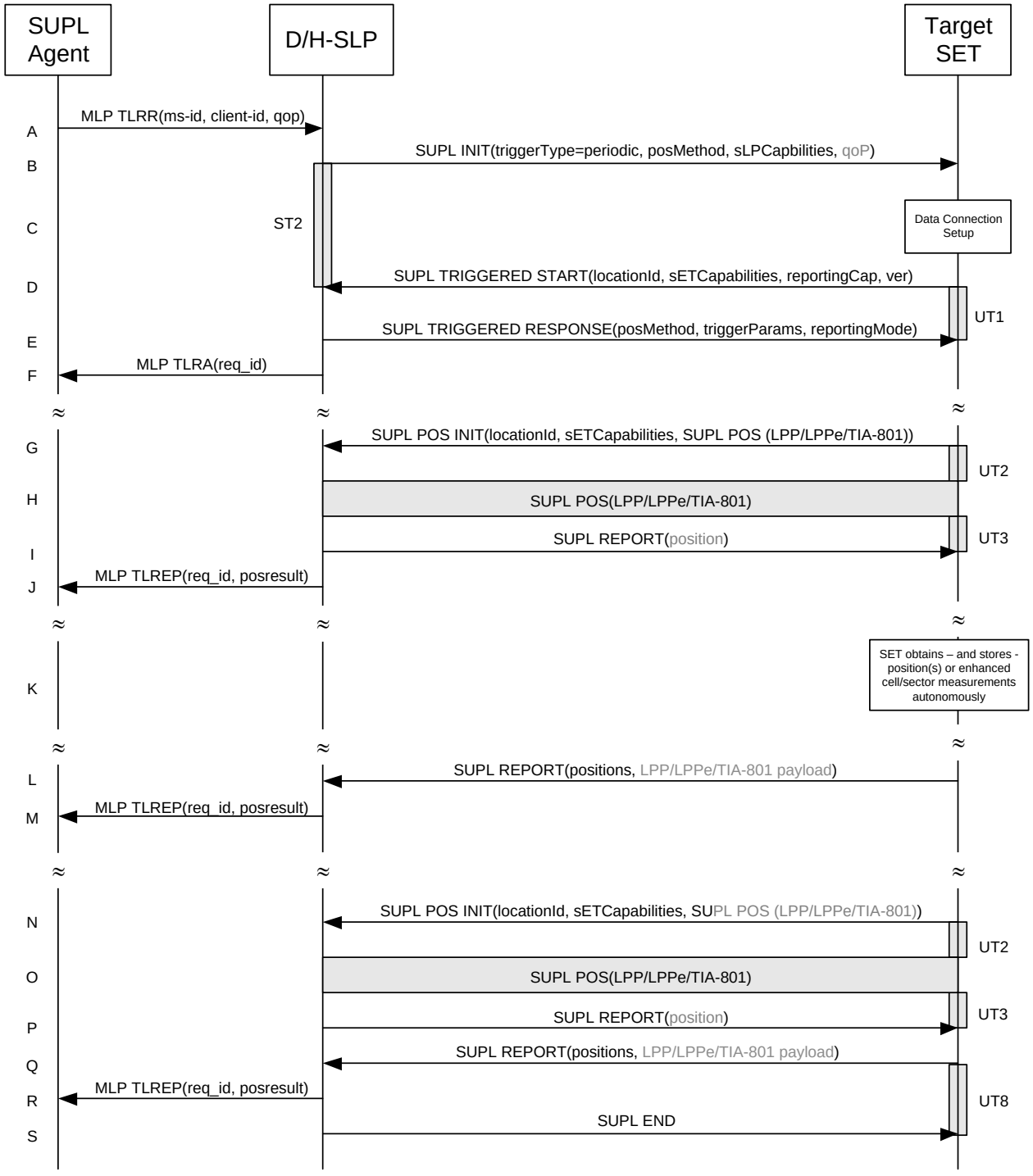

Figure 25: Network Initiated Triggered Periodic Non Roaming

A. The SUPL Agent sends an MLP TLRR message to the D/H-SLP, with which it is associated. The D/H-SLP SHALL authenticate the SUPL Agent and check if the SUPL Agent is authorized for the service it requested based on the *client-id* received. The D/H-SLP shall also provide privacy checking based on *ms-id* and *client-id*. The D/H-SLP MAY also verify that the target SET supports SUPL. The TLRR message may indicate that batch reporting or quasi-real time reporting is to be used instead of real time reporting. In the case of batch reporting, the TLRR indicates the

conditions for sending batch reports to the D/H-SLP and any criteria, when the conditions for sending arise, for including or excluding particular stored position estimates (e.g. QoP, time window).

NOTE: The specifics for determining if the SET supports SUPL are beyond the scope of SUPL 3.0.

B. The D/H-SLP initiates the periodic trigger session with the SET using the SUPL INIT message. The SUPL INIT message contains the intended positioning method (*posMethod*), the SLP Capabilities (*sLPCapabilities*), trigger type indicator (*triggerType*) - in this case periodic - and optionally 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 D/H-SLP SHALL also include the Notification element in the SUPL INIT message. Before the SUPL INIT message is sent, the D/H-SLP also computes and stores a hash of the message.

C. The SET analyses the received SUPL INIT message. If found not to be authentic, the SET takes no further action. Otherwise the SET takes required action to prepare for the establishment of a TLS connection with the D/H-SLP. The SET also calculates the hash of the received SUPL INIT message.

D. The SET evaluates the Notification rules and takes appropriate action. The SET SHALL establish a TLS connection to the D/H-SLP using the D/H-SLP address which is either the H-SLP address provisioned by the Home Network or the D-SLP address provided or verified by the H-SLP or by a Proxy D-SLP authorized by the H-SLP. The SET then sends a SUPL TRIGGERED START message to start a periodic triggered session with the D/H-SLP. The SET SHALL send the SUPL TRIGGERED START message even if the SET does not support the intended positioning method indicated in SUPL INIT (step B). The SUPL TRIGGERED START message contains the Location ID (*locationId*), SET capabilities (*sETCapabilities*), reporting capabilities (*reportingCap*) and the hash of the received SUPL INIT message (*ver*) calculated in step C. The *reportingCap* parameter indicates whether the SET is capable of batch reporting, real time reporting and/or quasi-real time reporting.

E. The D/H-SLP sends a SUPL TRIGGERED RESPONSE message to the SET. The SUPL TRIGGERED RESPONSE message contains the intended positioning method (*posMethod*) and the trigger parameters (*triggerParams*). Consistent with the reporting capabilities of the SET (sent in *reportingCap* in step D), the D/H-SLP also indicates the reporting mode (*reportingMode*) to be used by the SET: real time reporting, quasi-real time reporting or batch reporting. In the case of batch reporting, the SUPL TRIGGERED RESPONSE message indicates the conditions for sending batch reports to the D/H-SLP and any criteria, when the conditions for sending arise, for including or excluding particular stored position estimates and/or (if allowed) particular stored enhanced cell/sector/AP measurements. In the case of quasi-real time reporting, the SUPL TRIGGERED RESPONSE message indicates whether the SET is allowed to send enhanced cell/sector/AP measurements in lieu of or in addition to position estimates. If enhanced cell/sector/AP positioning was selected for batch or quasi-real time reporting, the SUPL TRIGGERED RESPONSE message indicates if the SET is permitted to send stored enhanced cell/sector/AP measurements. In this case, if batch reporting was selected, the SET MAY skip steps G, H and I.

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

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

G. When the periodic trigger in the SET indicates that a position fix has to be performed or at any time the SET decides it requires assistance data, the SET establishes a TLS connection to the D/H-SLP. The SET sends a SUPL POS INIT message to the D/H-SLP. The SUPL POS INIT message contains the Location ID (*locationId*), SET capabilities (*sETCapabilities*) and optionally a SUPL POS message carrying LPP/LPPe and/or TIA-801 positioning protocol messages in line with the D/H-SLP's positioning protocol capabilities (indicated in step B in *sLPCapabilities*). The SET MAY also provide its position, if this is supported (as part of LPP/LPPe/TIA-801 or explicitly through the optional position parameter).
If a position retrieved in - or calculated based on information received in - the SUPL POS INIT message is available that meets the required QoP, the D/H-SLP MAY directly proceed to step I and not engage in a SUPL POS session.

H. SET and D/H-SLP engage in a SUPL POS message exchange in order to calculate a position (or to obtain assistance data). The positioning methods used for this session are determined based on the capabilities exchanged by the SET and the D/H-SLP during that SUPL POS message exchange or optionally in step G.

I. Once the position calculation (or assistance data delivery) is complete, the D/H-SLP sends a SUPL REPORT message to the SET. If the reporting mode is batch reporting, the SET stores all calculated position estimates. In SET Assisted mode the position is calculated by the D/H-SLP and therefore is included in the SUPL REPORT message for batch reporting mode. The SET MAY release the secure connection to the D/H-SLP.

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

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

K. This step is optional: If the SET cannot communicate with the D/H-SLP and quasi-real time reporting is used or if batch reporting is used, the SET MAY – if supported - perform SET Based position fixes (e.g. autonomous GNSS or SET Based A-GNSS where the SET has current assistance data) and/or, if allowed by the D/H-SLP, enhanced cell/sector/AP measurements. In the case of batch reporting, and if explicitly allowed by the D/H-SLP, enhanced cell/sector/AP measurements are permitted even when the SET can communicate with the D/H-SLP.

L. This step is optional and is executed if batch reporting is used and if any of the conditions for sending batch reports have occurred. It is also executed, once the SET is able to re-establish communication with the D/H-SLP, if quasi-real time reporting is used and if one or more previous reports have been missed. The SET sends the stored position estimates and/or, if allowed, the stored enhanced cell/sector/AP measurements in an unsolicited SUPL REPORT message to the D/H-SLP. The SUPL REPORT message contains the position result(s) including date and time information for each position result and optionally the position method used. In the case of batch reporting, the stored position estimates and/or enhanced cell/sector/AP measurements included in the SUPL REPORT message may be chosen according to criteria received in step E. If no criteria are received in step E, the SET shall include all stored position estimates and/or enhanced cell/sector/AP measurements not previously reported. If applicable, enhanced cell/sector/AP measurements are sent in unsolicited LPP/LPPe/TIA-801 messages.

M. If enhanced cell/sector/AP measurements are received in step L, the D/H-SLP calculates corresponding position estimates.

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

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

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

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

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

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

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

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

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

5.3.1.2 Triggered Periodic – Roaming

The ULP message exchange for roaming is the same as for non-roaming (see Figure 25). However, the V-SLP is invoked each time the H-SLP requires translation of enhanced cell/sector/AP information into a position estimate due to SUPL roaming of the SET (see Figure 2).

5.3.2 Network Initiated Area and Velocity Events

For Network Initiated services, the SUPL Agent resides within the network and the service request is directed at the SLP. This section describes the call flows for Network Initiated Triggered Area and Velocity Event services. The trigger resides in the SET i.e., the SET decides if an area event or velocity event occurred.

Whenever in the course of an Area or Velocity Event Trigger session the SET needs to send a ULP message to the SLP, the SET SHALL check whether an existing TLS session already exists and – if one exists - reuse that existing TLS session. Otherwise the SET SHALL take appropriate action to resume a suspended TLS session, or establish a new TLS connection. Details of the TLS session (establishment, release, etc.) are not shown in this section.

5.3.2.1 Triggered Area and Velocity Event – Non Roaming

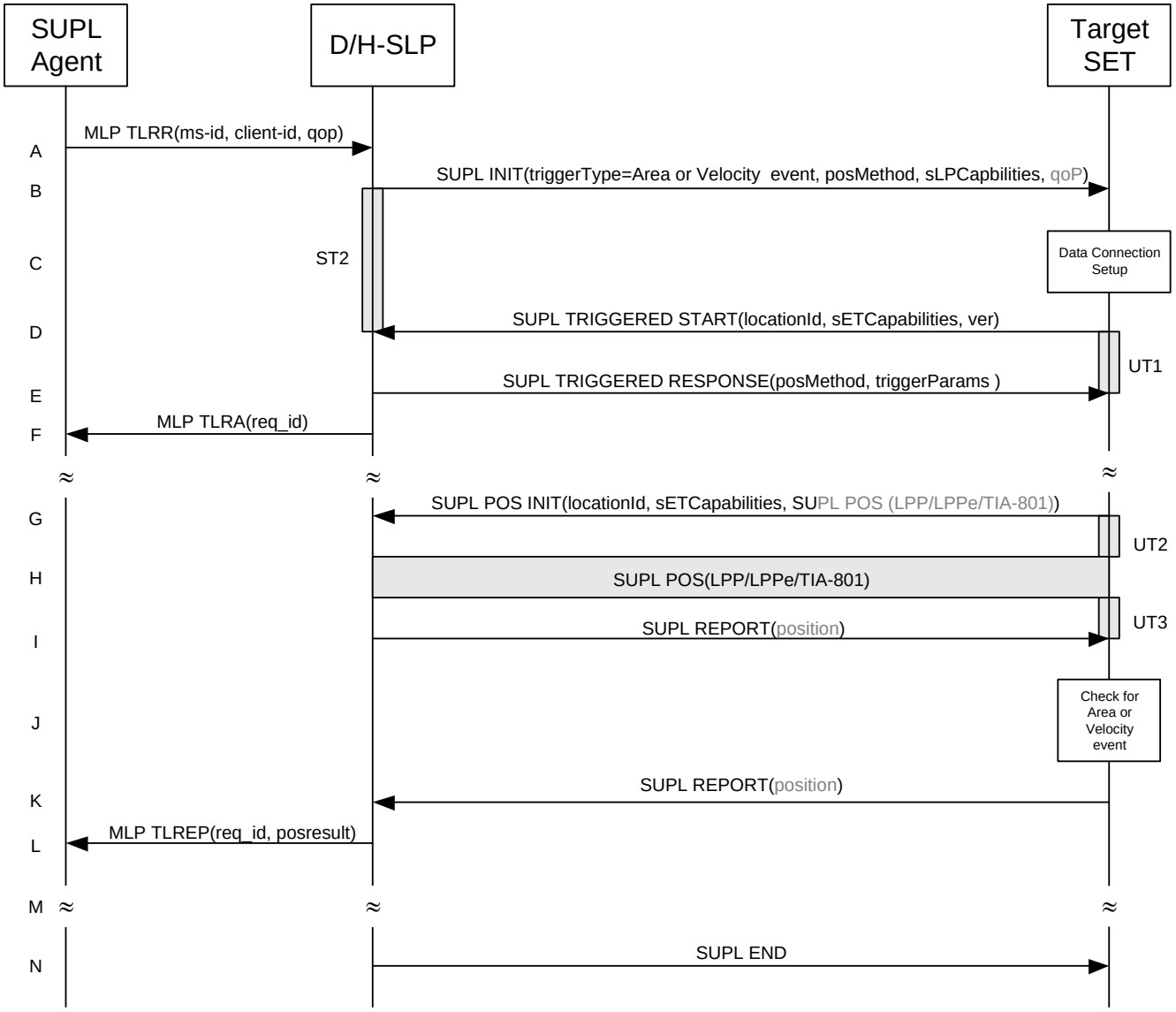

Figure 26: Network Initiated Triggered Area or Velocity Event Non Roaming

A. The SUPL Agent sends an MLP TLRR message to the D/H-SLP, with which it is associated. The D/H-SLP SHALL authenticate the SUPL Agent and check if the SUPL Agent is authorized for the service it requested based on the *client-id* received. The D/H-SLP shall also provide privacy checking based on *ms-id* and *client-id*.

In the case of an area event triggered session: The MLP TLRR message contains all parameters required for the area event trigger session (e.g., geographic target area, trigger criteria, etc.).

In the case of a velocity event triggered session: The MLP TLRR message contains all parameters required for the velocity event trigger session (e.g., target velocity, start time, stop time, number of reports, etc.).

The D/H-SLP MAY also verify that the target SET supports SUPL.

NOTE: The specifics for determining if the SET supports SUPL are beyond the scope of SUPL 3.0.

B. The D/H-SLP initiates the area or velocity event trigger session with the SET using the SUPL INIT message. The SUPL INIT message contains the intended positioning method (*posMethod*), the SLP Capabilities (*sLPCapabilities*),

trigger type indicator (*triggerType*) - area event or velocity event - and optionally 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 D/H-SLP SHALL also include the Notification element in the SUPL INIT message. Before the SUPL INIT message is sent, the D/H-SLP also computes and stores a hash of the SUPL INIT message.

C. The SET analyses the received SUPL INIT message. If found not to be authentic, the SET takes no further action. Otherwise the SET takes required action to prepare for the establishment of a TLS connection with the D/H-SLP. The SET also calculates the hash of the received SUPL INIT message.

D. The SET evaluates the Notification rules and takes appropriate action. The SET SHALL establish a TLS connection to the D/H-SLP using the D/H-SLP address which is either the H-SLP address provisioned by the Home Network or the D-SLP address provided or verified by the H-SLP or by a Proxy D-SLP authorized by the H-SLP. The SET then sends a SUPL TRIGGERED START message to start a triggered area or velocity event session with the D/H-SLP. The SET SHALL send the SUPL TRIGGERED START message even if the SET does not support the intended positioning method indicated in SUPL INIT (step B). The SUPL TRIGGERED START message contains the Location ID (*locationId*), SET capabilities (*sETCapabilities*) and the hash of the received SUPL INIT message (*ver*) calculated in step C.

E. The D/H-SLP sends a SUPLTRIGGERED RESPONSE message to the SET. The SUPL TRIGGERED RESPONSE message contains the intended positioning method (*posMethod*) and the trigger parameters (*triggerParams*).

In the case of an area event triggered session the SUPL TRIGGERED RESPONSE message may also contain the area ids of the specified area for the area event triggered session (in *triggerParams*).

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

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

G. If the area ids are downloaded in step E, the SET SHALL compare the current area id to the downloaded area ids. When the area or velocity event trigger mechanism in the SET indicates that a network assisted position fix is to be executed or assistance data is required, the SET establishes a TLS connection with the D/H-SLP. The SET then sends a SUPL POS INIT message to the D/H-SLP. The SUPL POS INIT message contains the Location ID (*locationId*), SET capabilities (*sETCapabilities*) and optionally a SUPL POS message carrying LPP/LPPe and/or TIA-801 pos protocol payload in line with the D/H-SLP's positioning protocol capabilities (indicated in step B in *sLPCapabilities*). The SET MAY also provide its position, if this is supported (as part of LPP/LPPe/TIA-801 or explicitly through the optional position parameter). If a position retrieved in - or calculated based on information received in - the SUPL POS INIT message is available that meets the required QoP, the D/H-SLP MAY directly proceed to step I and not engage in a SUPL POS session.

H. SET and D/H-SLP engage in a SUPL POS message exchange in order to calculate a position – which may include the velocity - or to obtain assistance data. The positioning methods used for this session are determined based on the capabilities exchanged by the SET and the D/H-SLP during that SUPL POS message exchange or optionally in step G.

I. Once the position calculation (or assistance data delivery) is complete, the D/H-SLP sends a SUPL REPORT message to the SET. The SUPL REPORT message may include the position result (*position*) – which may include the velocity - if the position result was calculated at the D/H-SLP. The SET MAY release the secure connection to the D/H-SLP.

J. In the case of an area event triggered session: The SET compares the calculated position estimate with the target area to check if the event trigger condition has been met.

In the case of a velocity event triggered session: The SET compares the calculated velocity with the target velocity to check if the event trigger condition has been met.

If no area or velocity event is triggered, the SET SHALL return to step G. If an area or velocity event is triggered, the SET SHALL proceed to step K.

K. In the case of an area event triggered session: The SET sends a SUPL REPORT message including the position estimate to the D/H-SLP unless the Location Estimate parameter is set to “false” in which case no position estimate is included.

   In the case of a velocity event triggered session: The SET sends a SUPL REPORT message including the velocity to the D/H-SLP unless the Velocity Estimate parameter is set to “false”. Since velocity estimate is always sent as part of a position estimate, the position estimate is also included whenever a velocity estimate is sent.

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

M. If the SUPL Agent has requested several reports and more reports are to be sent, the SET repeats step G to L or step G to J depending on whether or not a trigger event (area or velocity) has occurred. Note that in this case, step K occurs only after the minimum time between reports has elapsed.

N. When the maximum number of reports for the SUPL triggered session has been reached, the D/H-SLP sends a SUPL END message to the SET.

The message flow described in Figure 26 is applicable to all positioning methods. However, individual steps within the call flows are optional:

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

When the stop time is reached, the SET initiates the ending of the triggered area or velocity event session as shown in Figure 27.

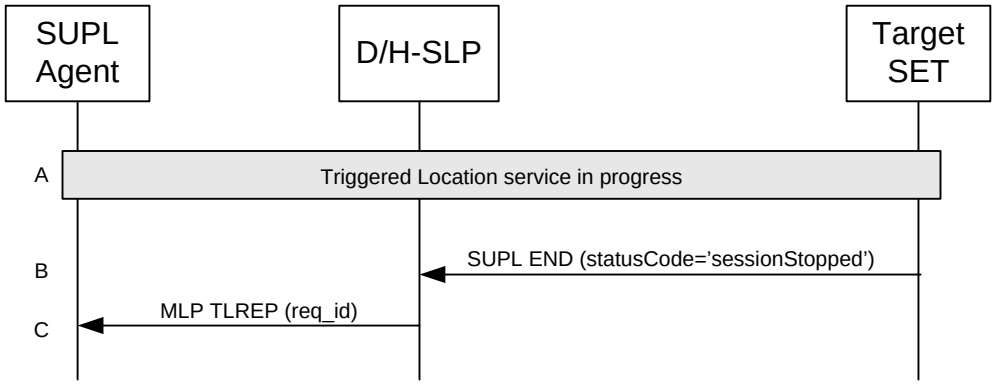

Figure 27: Ending of a triggered area or velocity event session when the stop time has been reached.

A. The area or velocity event triggered session is in progress.

B. When the StopTime of the event trigger is reached, the SET sends a SUPL END message with status code “sessionStopped” to the D/H-SLP . The SET releases all resources related to the session.

C. The D/H-SLP MAY send an MLP TLREP message to the SUPL Agent to indicate the end of the triggered area or velocity event session. The D/H-SLP releases all resources related to the session.

NOTE: If the SET does not send a SUPL END message within a configured time interval after the Stop Time was reached (i.e. step B did not occur), the D/H-SLP MAY proceed directly to step C and discard all resources for the session.

5.3.2.2 Triggered Area and Velocity Event – Roaming

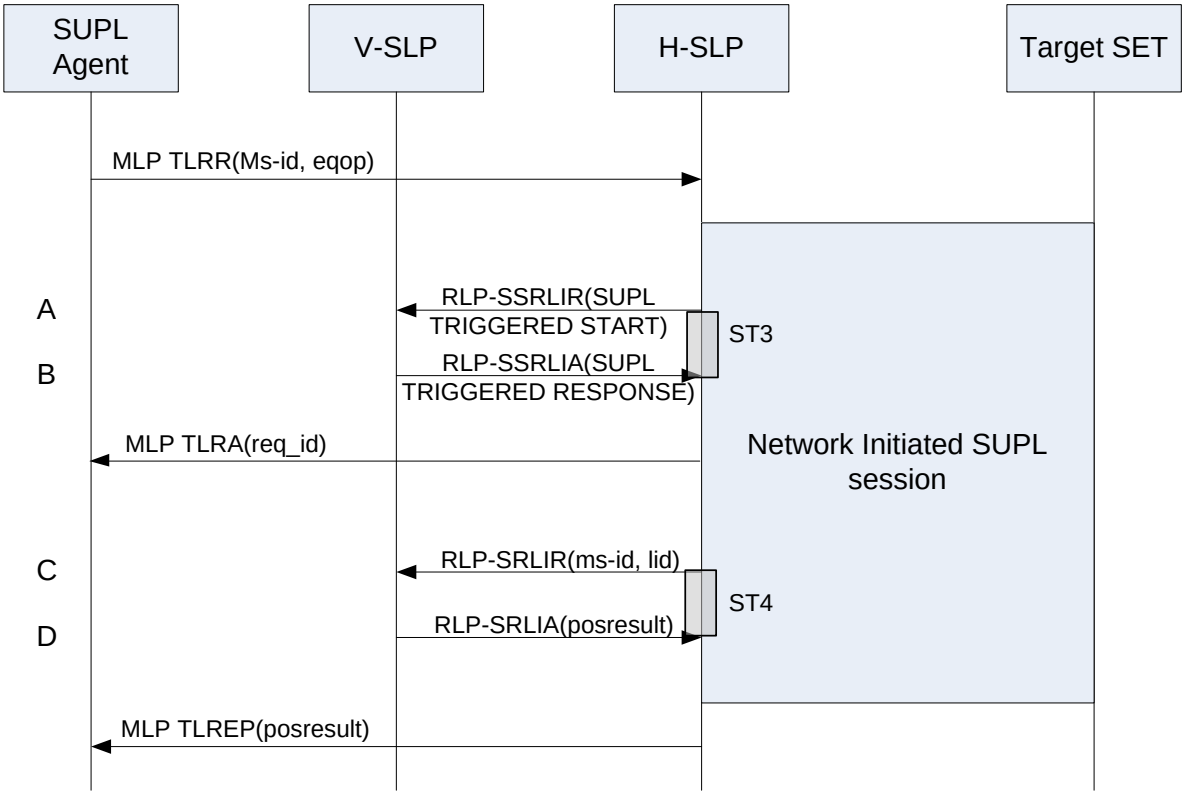

Figure 28: Network Initiated Triggered Area or Velocity Event Roaming

For Network Initiated roaming, the ULP message exchange is the same as for non-roaming (see Figure 26). The ULP message exchange between SET and H-SLP is therefore not explicitly shown in Figure 28 but only indicated as "Network Initiated SUPL session" in the diagram. The V-SLP is invoked:

A. If, after receiving a SUPL TRIGGERED START message from the SET, the H-SLP cannot provide area id information for the selected geographical target area, it forwards the SUPL TRIGGERED START message encapsulated in an RLP-SSRLIR message to the V-SLP.

B. In response to step A and if supported (and if the V-SLP is able to provide this information) by the V-SLP, the V-SLP returns the area ids in a SUPL TRIGGERED RESPONSE message encapsulated in an RLP-SSRLIA message to the H-SLP.

C. When the H-SLP requires translation of a cell/sector/access point id into a position estimate but is unable to perform the translation on its own, the H-SLP engages the V-SLP by sending an RLP-SRLIR message to the V-SLP including the ms-id and the location id (cell or access point id).

D. In response to step C, the V-SLP translates the received cell or access point id into a position estimate and returns an RLP-SRLIA message including the position (*posresult*) to the H-SLP.

Steps C and D may be repeated as required.

5.3.3 SET Initiated Triggered Periodic

For SET Initiated services, the SUPL Agent resides within the SET.

Whenever in the course of a Periodic Trigger session the SET needs to send a ULP message to the SLP, the SET SHALL check whether an existing TLS session already exists and – if one exists - reuse that existing TLS session. Otherwise the SET

SHALL take appropriate action to resume a suspended TLS session, or establish a new TLS connection. Details of the TLS session (establishment, release, etc.) are not shown in this section.

5.3.3.1 Triggered Periodic – Non Roaming

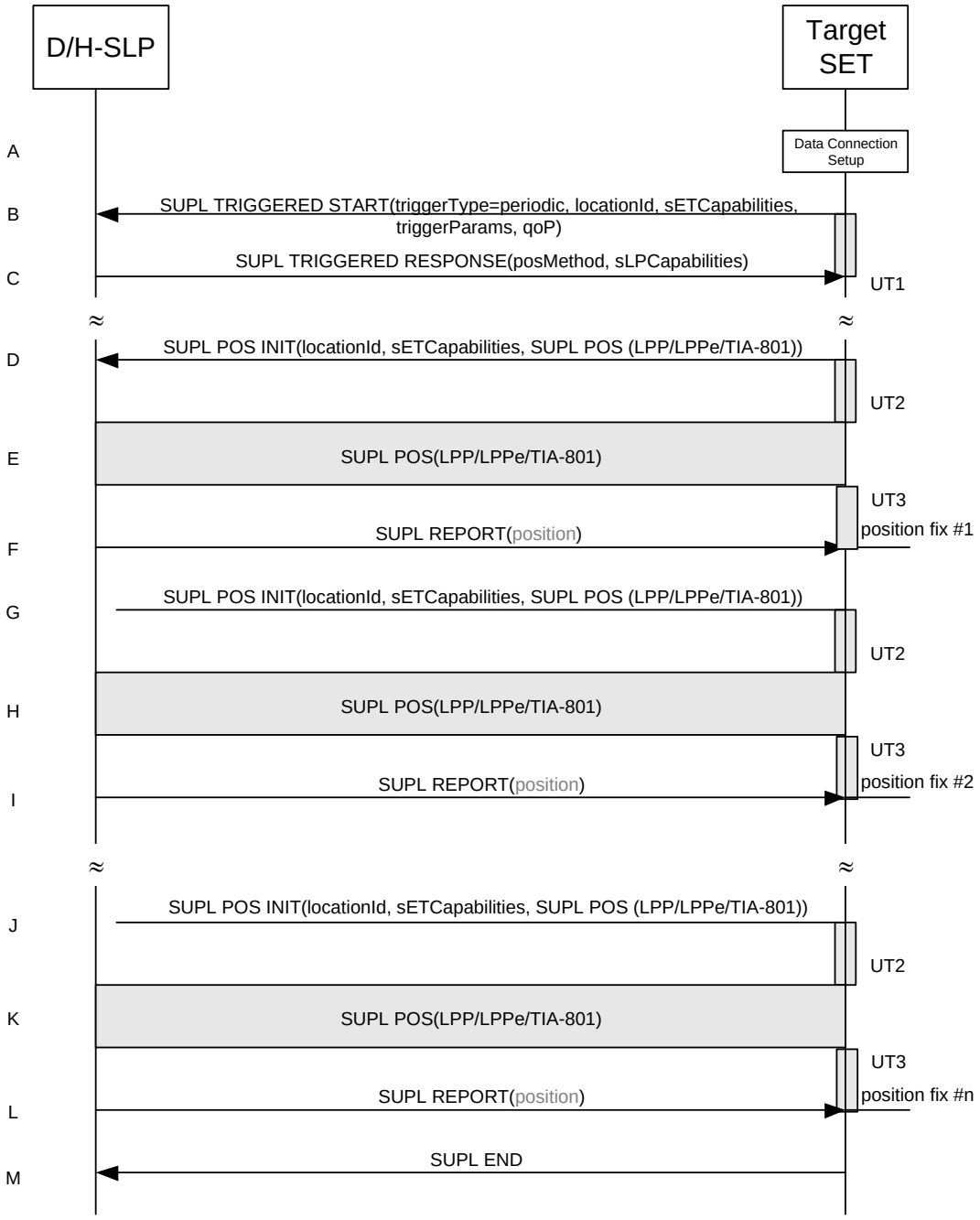

Figure 29: SET Initiated Triggered Periodic Non Roaming

A. The SET receives a position request from a SUPL Agent (e.g., an application) on the SET. The SET takes appropriate action to establish a secure TLS connection to the D/H-SLP.

B. The SET SHALL use either the default address provisioned by the Home Network for an H-SLP or the address provided or verified by the H-SLP or by a Proxy D-SLP authorized by the H-SLP for a D-SLP to establish a TLS connection to the D/H-SLP and send a SUPL TRIGGERED START message to start a positioning session with the

D/H-SLP. The SUPL TRIGGERED START message contains SET capabilities (*sETCapabilities*), trigger type indicator (*triggerType*) - in this case periodic -, periodic trigger parameters (*triggerParams*) and optionally the QoP .

C. The D/H-SLP sends a SUPLTRIGGERED RESPONSE message to the SET. The SUPL TRIGGERED RESPONSE message contains the intended positioning method (*posMethod*) and the SLP Capabilities (*sLPCapabilities*). SET and D/H-SLP MAY release the TLS connection.

D. When the periodic trigger in the SET indicates that a position fix has to be performed or at any time the SET decides it requires assistance data, the SET establishes a TLS connection to the D/H-SLP. The SET sends a SUPL POS INIT message to the D/H-SLP. The SUPL POS INIT message contains the Location ID (*locationId*), SET capabilities (*sETCapabilities*) and optionally a SUPL POS message carrying LPP/LPPe and/or TIA-801 pos protocol payload in line with the D/H-SLP's positioning protocol capabilities (indicated in step C in *sLPCapabilities*). The SET MAY also provide its position, if this is supported (as part of LPP/LPPe/TIA-801 or explicitly through the optional position parameter).
If a position retrieved in - or calculated based on information received in - the SUPL POS INIT message is available that meets the required QoP, the D/H-SLP MAY directly proceed to step F and not engage in a SUPL POS session.

E. SET and D/H-SLP engage in a SUPL POS message exchange in order to calculate a position (or to obtain assistance data). The positioning methods used for this session are determined based on the capabilities exchanged by the SET and the D/H-SLP during that SUPL POS message exchange or optionally in step D.

F. Once the position calculation (or assistance data delivery) is complete, the D/H-SLP sends a SUPL REPORT message to the SET. In SET Assisted mode the position is calculated by the D/H-SLP and may be included in the SUPL REPORT message. The SET MAY release the secure connection to the D/H-SLP.

NOTE: If a SET Based positioning method was chosen which allows the SET to autonomously calculate a position estimate (e.g. autonomous GNSS or A-GNSS SET Based mode where the SET has current GNSS assistance data and does not require an assistance data update from the D/H-SLP), steps D to F are not performed.

Steps G to I (i.e., the second position fix/assistance data delivery) and steps J to L (i.e., the last position fix/assistance data delivery) are a repeat of steps D to F.

G. After the last position result was calculated, the SET ends the periodic triggered session by sending a SUPL END message to the D/H-SLP

5.3.3.2 Triggered Periodic Roaming

The ULP message exchange for roaming is the same as for non-roaming (see Figure 29). However, the V-SLP is invoked each time the H-SLP requires translation of enhanced cell/sector/AP information into a position estimate due to SUPL roaming of the SET (see Figure 2).

5.3.3.3 Triggered Periodic with Transfer to 3rd Party – Non Roaming

5.3.3.4 Triggered Periodic with Transfer to 3rd Party - Roaming

5.3.4 SET Initiated Area and Velocity Events

For SET Initiated services, the SUPL Agent resides within the SET. The trigger also resides in the SET i.e., the SET decides if an area or velocity event occurred.

Whenever in the course of a Trigger Area or Velocity Event session the SET needs to send a ULP message to the SLP, the SET SHALL check whether an existing TLS session already exists and – if one exists - reuse that existing TLS session. Otherwise the SET SHALL take appropriate action to resume a suspended TLS session, or establish a new TLS connection. Details of the TLS session (establishment, release, etc.) are not shown in this section.

5.3.4.1 Triggered Area and Velocity Event – Non Roaming

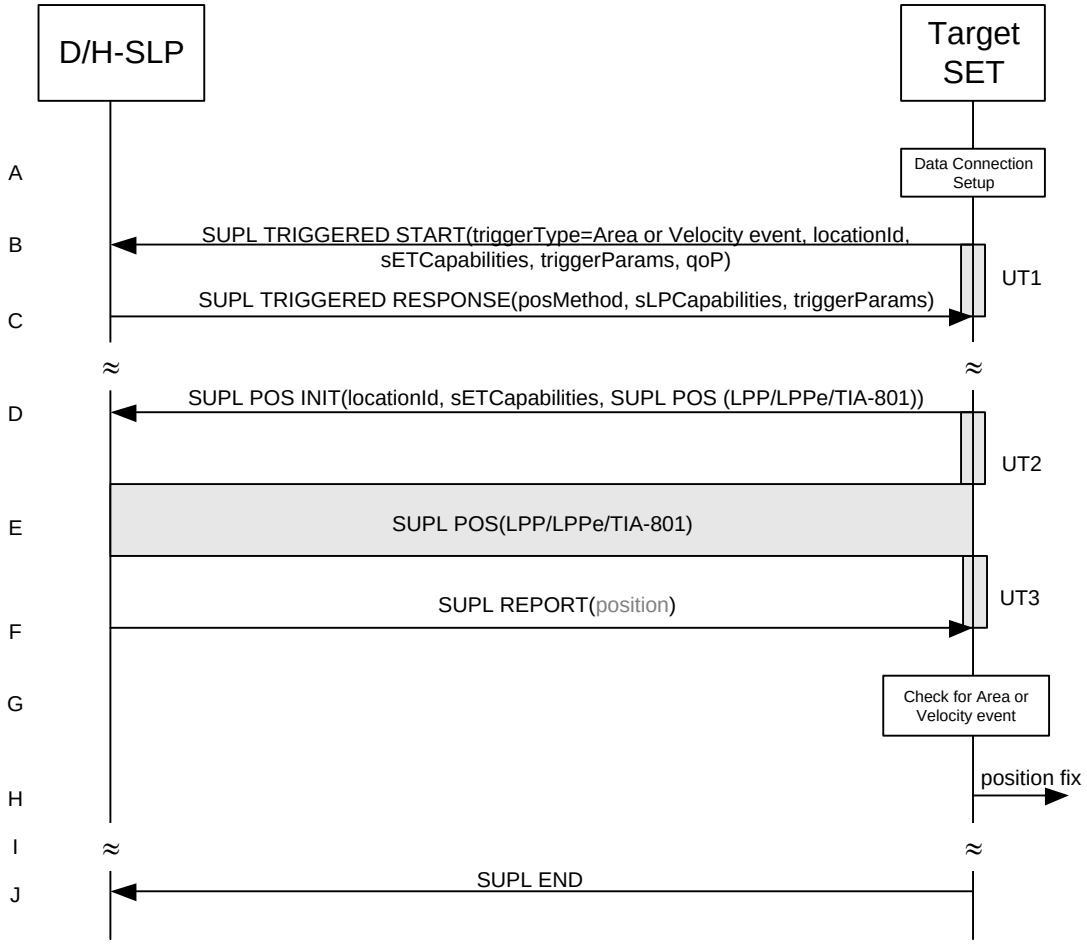

Figure 30: SET Initiated Triggered Area or Velocity Event Non Roaming

A. The SET receives a position request from a SUPL Agent (e.g., an application) on the SET. The SET takes appropriate action to establish a secure TLS connection to the D/H-SLP.

B. The SET SHALL use either the default address provisioned by the Home Network for an H-SLP or the address provided or verified by the H-SLP or by a Proxy D-SLP authorized by the H-SLP for a D-SLP to establish a TLS connection to the D/H-SLP and send a SUPL TRIGGERED START message to start a positioning session with the D/H-SLP. The SUPL TRIGGERED START message contains Location ID (*locationId*), SET capabilities (*sETCapabilities*), trigger type indicator (*triggerType*) - area event or velocity event -, area or velocity event trigger parameters (*triggerParams*) and optionally the QoP.

C. The D/H-SLP sends a SUPLTRIGGERED RESPONSE message to the SET. The SUPL TRIGGERED RESPONSE message contains the intended positioning method (*posMethod*), the SLP Capabilities (*sLPCapabilities*) and the trigger parameters (*triggerParams*). It may also contain the area ids of the specified area for the area event triggered session (in *triggerParams*). SET and D/H-SLP MAY release the TLS connection.

D. If the area ids are downloaded in step C, the SET SHALL compare the current area id to the downloaded area ids. When the area or velocity event trigger mechanism in the SET or the comparison of the current area id to the downloaded area ids indicates that a position fix is to be executed, the SET establishes a TLS connection with the D/H-SLP. A TLS connection with the D/H-SLP is also established by the SET, whenever the area or velocity event trigger in the SET indicates that a position fix has to be performed or at any time the SET decides it requires assistance data. The SET then sends a SUPL POS INIT message to the D/H-SLP. The SUPL POS INIT message contains the Location ID (*locationId*), SET capabilities (*sETCapabilities*) and optionally a SUPL POS message

carrying LPP/LPPe and/or TIA-801 pos protocol payload in line with the D/H-SLP's positioning protocol capabilities (indicated in step C in *sLPCapabilities*). The SET MAY also provide its position, if this is supported (as part of LPP/LPPe/TIA-801 or explicitly through the optional position parameter).
If a position retrieved in - or calculated based on information received in - the SUPL POS INIT message is available that meets the required QoP, the D/H-SLP MAY directly proceed to step F and not engage in a SUPL POS session.

E. SET and D/H-SLP engage in a SUPL POS message exchange in order to calculate a position – which may include the velocity - (or to obtain assistance data). The positioning methods used for this session are determined based on the capabilities exchanged by the SET and the D/H-SLP during that SUPL POS message exchange or optionally in step D.

F. Once the position calculation (or assistance data delivery) is complete, the D/H-SLP sends a SUPL REPORT message to the SET. In SET Assisted mode the position – which may include the velocity - is calculated by the D/H-SLP and may be included in the SUPL REPORT message. The SET MAY release the secure connection to the D/H-SLP.

G. In the case of an area event triggered session: The SET compares the calculated position estimate with the target area to check if the event trigger condition has been met.

In the case of a velocity event triggered session: The SET compares the calculated velocity with the target velocity to check if the event trigger condition has been met.

If no area or velocity event is triggered, the SET SHALL return to step D. If an area or velocity event is triggered, the SET SHALL proceed to step H.

H. If an area or velocity event was triggered, the SET forwards the calculated position and/or velocity estimate to the internal SUPL Agent.

I. If the SUPL Agent has requested several reports and more reports are to be sent, the SET repeats step D to G or step D to H depending on whether or not an area or velocity event occurred. Note that in this case, step H occurs only after the minimum time between reports has elapsed.

J. When the maximum number of reports for the SUPL triggered session has been reached, the SET sends a SUPL END message to the D/H-SLP.

The call flow described in Figure 30 is applicable to all positioning methods, however, individual steps within the call flows are optional:

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

When the stop time is reached, the SET initiates the ending of the triggered area or velocity event session as shown in Figure 31.

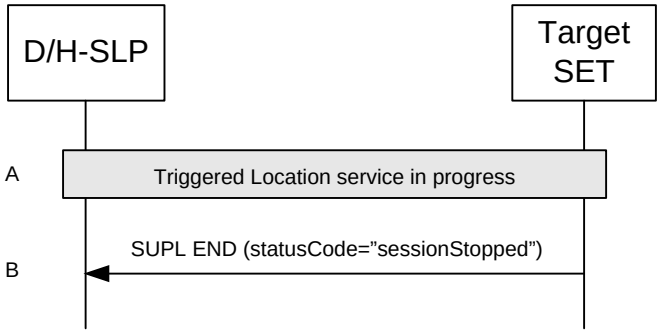

Figure 31: Ending of a triggered area or velocity event session when the stop time has been reached.

A. An area or velocity triggered event session is in progress.

B. When the StopTime of the event trigger is reached, the SET sends a SUPL END message with status code "sessionStopped" to the D/H-SLP. The SET releases all resources related to this session.

NOTE: If the SET does not send a SUPL END message within a configured time interval after the Stop Time was reached (i.e. step B did not occur), the D/H-SLP MAY release all resources for the session.

5.3.4.2 Triggered Area and Velocity Event – Roaming

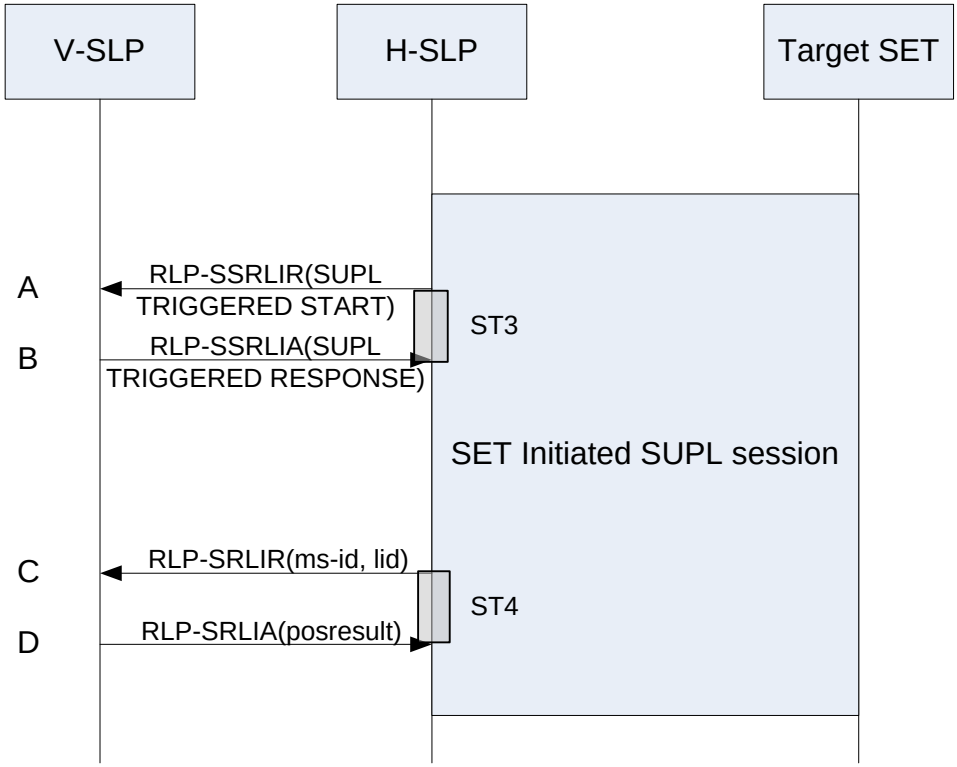

Figure 32: SET Initiated Triggered Area or Velocity Event Roaming

For SET Initiated roaming, the ULP message exchange is the same as for non-roaming (see Figure 30). The ULP message exchange between SET and H-SLP is therefore not explicitly shown in Figure 32 but only indicated as "SET Initiated SUPL session" in the diagram. The V-SLP is invoked:

A. If, after receiving a SUPL TRIGGERED START message from the SET, the H-SLP cannot provide area id information for the selected geographical target area, it forwards the SUPL TRIGGERED START message encapsulated in an RLP-SSRLIR message to the V-SLP.

B. In response to step A and if supported (and if the V-SLP is able to provide this information) by the V-SLP, the V-SLP returns the area ids in a SUPL TRIGGERED RESPONSE message encapsulated in an RLP-SSRLIA message to the H-SLP.

C. When the H-SLP requires translation of a cell/sector/access point id into a position estimate but is unable to perform the translation on its own, the H-SLP engages the V-SLP by sending an RLP-SRLIR message to the V-SLP including the ms-id and the location id (cell or access point id).

D. In response to step C, the V-SLP translates the received cell or access point id into a position estimate and returns an RLP-SRLIA message including the position (*posresult*) to the H-SLP.

Steps C and D may be repeated as required.

5.3.5 Generic SUPL Session

A Generic SUPL Session (GSS) is a SUPL session created to provide a SUPL session framework for positioning activities (exchange of SUPL POS messages which carry LPP/LPPe or TIA-801 payload) between a SET and an SLP. The “generic” in GSS refers to the fact that a GSS constitutes an open SUPL session i.e., a SUPL session without any directly associated SUPL service request.

A GSS can either be Network Initiated or SET Initiated. SET Initiated GSS establishment shall be subject to policy settings in the D/H-SLP. For SET Initiated sessions D/H-SLP may also choose to set up GSS without an explicit request for GSS from the SET. Once established, the D/H-SLP or the SET may invoke positioning activities without the need for formal SUPL session establishment or session termination during the entire lifetime of the GSS. GSS and non-GSS SUPL sessions may be executed simultaneously but some restrictions may apply.

The following sections define the call flows for Network and SET Initiated GSS.

5.3.5.1 Network Initiated GSS – Non Roaming

Figure 33 shows the non roaming call flow of a Network Initiated GSS. MLP messages exchanged between the SUPL Agent and the D/H-SLP are only shown to illustrate possible interactions between SUPL Agents and the D/H-SLP during a GSS. The GSS may be established as a result of an MLP location service request by the SUPL Agent or may be established by the D/H-SLP based on some other event or condition and in the absence of any MLP location requests by the SUPL Agent.

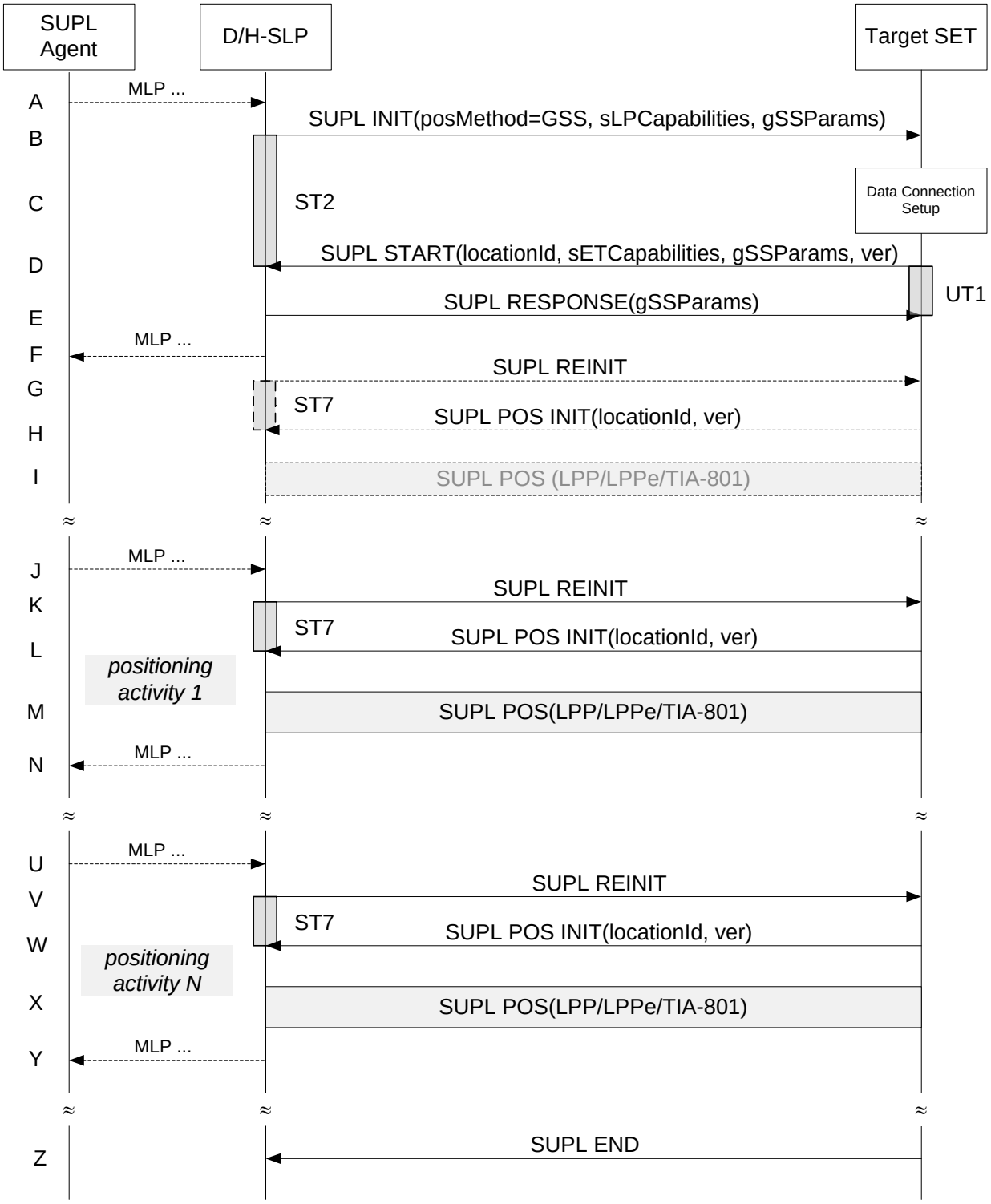

Figure 33: **Network Initiated GSS**

A. This step is optional: the SUPL Agent may send an MLP request for location service to the D/H-SLP, with which it is associated. The D/H-SLP SHALL authenticate the SUPL Agent and check if the SUPL Agent is authorized for the service requested. The D/H-SLP SHALL also provide privacy checking. The D/H-SLP MAY also verify that the target SET supports SUPL. This step is only shown as an example to illustrate that a GSS may be established as a

result of an MLP location request by the SUPL Agent. A GSS may also be established by the D/H-SLP based on some other event or condition and in the absence of any MLP location requests by the SUPL Agent.

NOTE: The specifics for determining if the SET supports SUPL are beyond the scope of SUPL 3.0.

NOTE: The session id used when establishing GSS must remain the same throughout the life time of the GSS.

B. As a result of the request in step A (which is optional) or some other condition, the D/H-SLP initiates a GSS with the SET using a SUPL INIT message. The SUPL INIT message contains a positioning method (*posMethod*) of "GSS". The SLP also includes the SLP Capabilities (*sLPCapabilities*) which are used to indicate the supported positioning protocol (LPP/LPPe or TIA-801) and the GSS Parameter (*gSSParams*). The GSS Parameter defines the desired duration of the GSS. If the result of the privacy check in step A indicates that notification and/or verification of the target subscriber is needed, the D/H-SLP SHALL also include the Notification parameter in the SUPL INIT message otherwise, the Notification parameter SHALL be omitted. Before the SUPL INIT message is sent, the D/H-SLP also computes and stores the hash of the SUPL INIT message.

C. The SET analyses the received SUPL INIT message. If found not to be authentic, the SET takes no further action. Otherwise, the SET takes required action to prepare for the establishment of a TLS connection with the D/H-SLP. The SET also calculates the hash of the received SUPL INIT message.

D. The SET evaluates the Notification rules and takes the appropriate action. The SET SHALL establish a TLS connection to the D/H-SLP using the D/H-SLP address which is either the H-SLP address provisioned by the Home Network or the D-SLP address provided or verified by the H-SLP or by a Proxy D-SLP authorized by the H-SLP. The SET then sends a SUPL START message to the D/H-SLP. The SUPL START message includes the Location ID (*locationId*), SET Capabilities (*sETCapabilities*), GSS Parameter (*gSSParams*) and the hash (*ver*) of the received SUPL INIT message. The SET Capabilities are used to indicate to the D/H-SLP which positioning protocol(s) is/are supported by the SET. The GSS Parameter is used to indicate to the D/H-SLP which duration of GSS the SET is willing and able to support.

E. The D/H-SLP sends a SUPL RESPONSE message to the SET including the GSS Parameter. In line with the GSS Parameter exchange in steps B and D, the GSS Parameter is used to determine the final duration of the GSS.

F. This step is optional and may be performed by the D/H-SLP to acknowledge the MLP location request by the SUPL Agent in step A, if step A was performed.

The GSS is now established with a pre-defined lifetime (*duration*). The D/H-SLP may at any time request a position activity such as assistance data provisioning, measurement and/or position request, etc. based on some condition or event. This is shown in the remainder of the call flow.

Steps G, H and I are optional and should be performed by the SET and the SLP in order to exchange their positioning capabilities unless both entities already know each other's positioning capabilities. The capabilities exchange may be initiated either by the D/H-SLP or the SET. In the case of the D/H-SLP, the D/H-SLP SHALL send a SUPL REINIT as in step G. In the case of the SET, the SET SHALL send a SUPL POS INIT as in step H and step G is omitted.

G. The D/H-SLP SHALL send a SUPL REINIT message to the SET if the capabilities exchange is initiated by the D/H-SLP. The SUPL REINIT message SHALL contain the same session id as that of the GSS. Before the SUPL REINIT message is sent, the D/H-SLP computes and stores the hash of the SUPL REINIT message.

H. The SET analyses the received SUPL REINIT message if received. If found not to be authentic, the SET takes no further action. Otherwise, the SET takes required action to prepare for the establishment of a TLS connection with the D/H-SLP if it is not already established. The SET also calculates the hash of the received SUPL REINIT message. The SET SHALL send a SUPL POS INIT message to the D/H-SLP including the Location ID (*locationId*) and hash of the SUPL REINIT message (*ver*).

I. The positioning capabilities exchanged in this step are those which the SET and the D/H-SLP are willing and able to use for the GSS. If the exchange of positioning capabilities reveals that no suitable match exists, the D/H-SLP SHALL end the GSS by sending a SUPL END message to the SET with status code '*gssCapabilityMismatch*'. The SET and the D/H-SLP MAY release the secure connection after positioning capabilities exchange is complete.

J. This step is optional: a SUPL Agent (which may or may not be the same as the SUPL Agent of step A) sends an MLP request for location service to the D/H-SLP. The D/H-SLP SHALL authenticate the SUPL Agent and check if the SUPL Agent is authorized for the service requested. This step is only shown as an example to illustrate that an MLP location service request may lead to a positioning activity.

K. When the D/H-SLP decides to initiate a positioning activity (which may be the result of step J or some other condition or event), the D/H-SLP SHALL send a SUPL REINIT message to the SET. The SUPL REINIT message SHALL contain the same session id as that of the GSS. Before the SUPL REINIT message is sent, the D/H-SLP computes and stores the hash of the SUPL REINIT message.

L. The SET analyses the received SUPL REINIT message. If found not to be authentic, the SET takes no further action. Otherwise, the SET takes required action to prepare for the establishment of a TLS connection with the D/H-SLP if it is not already established.. The SET also calculates the hash of the received SUPL REINIT message. The SET SHALL send a SUPL POS INIT message to the D/H-SLP including the Location ID (*locationId*) and hash of the SUPL REINIT message (*ver*).

M. SET and D/H-SLP exchange SUPL POS messages to execute the requested positioning activity. Initial SUPL POS messages may be used if needed to provide the D/H-SLP with the access network type for the SET which may then be used to select the most appropriate positioning protocol (LPP/LPPe or TIA-801) and positioning methods. The SET and the D/H-SLP MAY release the secure connection after positioning activity is complete.

N. This step is optional and may be performed by the D/H-SLP to provide a response to the SUPL Agent's request for location service and may include the results of the positioning activity in step J – if step J took place.

Steps J to N may be repeated as required and at any time during the lifetime of the GSS (this is illustrated in steps U to Y).

O. When the end of the GSS is reached, the SET sends a SUPL END message to the D/H-SLP. SET and D/H-SLP release all resources related to the GSS.

5.3.5.2 SET Initiated GSS - Non Roaming

Figure 34 shows the call flow of a SET Initiated GSS.

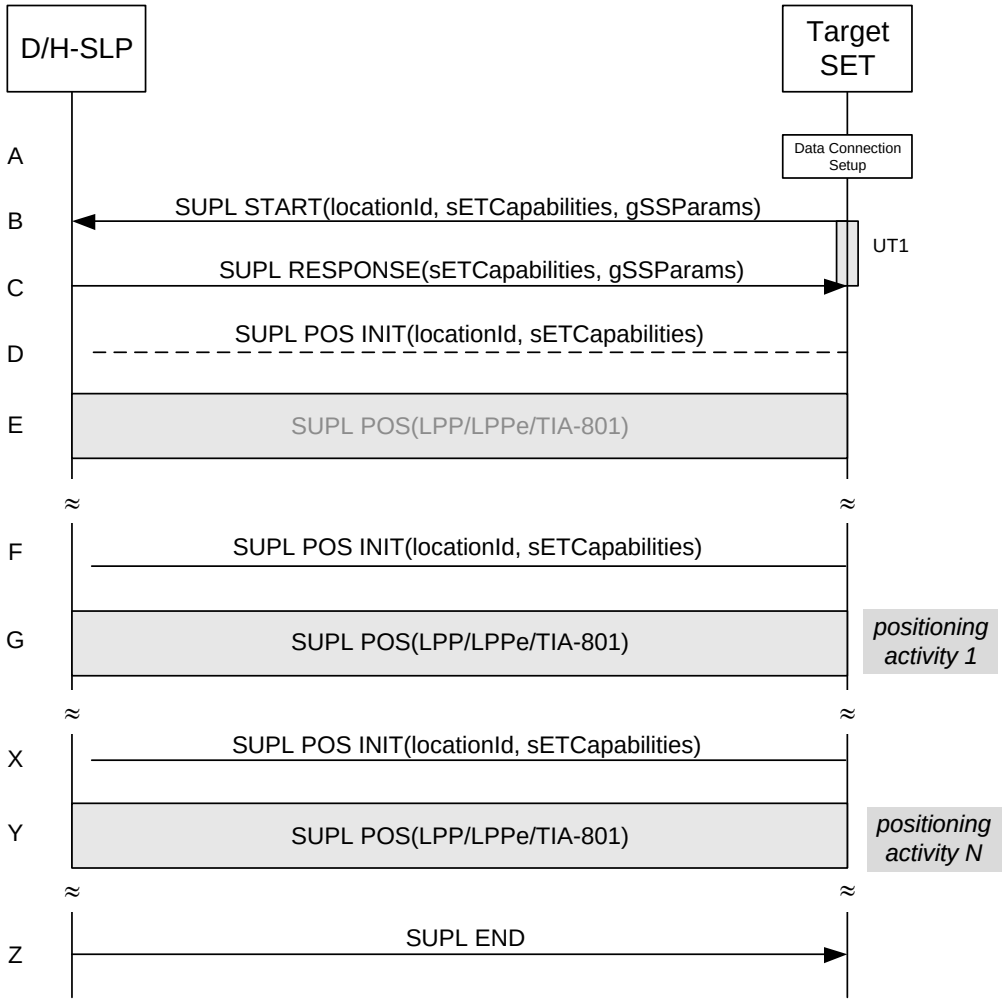

Figure 34: SET Initiated GSS

NOTE: The session id used when establishing GSS must remain the same throughout the life time of the GSS.

A. The SET requests the establishment of a GSS. The SET takes appropriate action to establish a secure TLS connection to the D/H-SLP.

B. The SET SHALL use either the default address provisioned by the Home Network for an H-SLP or the address provided or verified by the H-SLP or by a Proxy D-SLP authorized by the H-SLP for a D-SLP to establish a secure TLS connection to the D/H-SLP and send a SUPL START message to start a GSS with the D/H-SLP. The SUPL START message contains the Location ID (*locationId*), SET capabilities (*sETCapabilities*) and GSS Parameters (*gSSParams*). The SET Capabilities are used to indicate to the D/H-SLP which positioning protocols are supported by the SET (LPP/LPPe or TIA-801). The GSS Parameter is used to indicate the desired duration of the GSS.

C. The D/H-SLP sends a SUPL RESPONSE message to the SET including the SLP Capabilities and the GSS Parameter. In line with the GSS Parameter exchanged in step B, the GSS Parameter in this step is used to determine the final duration of the GSS.

The GSS is now established with a pre-defined lifetime (*duration*). The SET which initiated the GSS may at any time request a position activity such as assistance data provisioning, measurement and/or position request, etc. This is shown in the remainder of the call flow.

Steps D and E are optional and should be performed by the SET and the SLP in order to exchange their positioning capabilities unless both entities already know each other's positioning capabilities. This diagram shows the SET

initiated capabilities exchange. The D/H-SLP may also initiate the set capabilities exchange as shown in Figure 33 steps G, H and I.

D. The SET sends a SUPL POS INIT message to start a positioning session with the H-SLP to exchange their positioning capabilities .

E. The positioning capabilities exchanged in this step are those which the SET and the D/H-SLP are willing (based on user profile, SUPL Agent Id, etc.) and able to use for the GSS. If the exchange of positioning capabilities reveals that no suitable match exists, the SETSHALL end the GSS by sending a SUPL END message to the D/H-SLP with status code '*gssCapabilityMismatch*'. The SET and the D/H-SLP MAY release the secure connection after positioning capabilities exchange is complete.

F. When the SET decides to initiate a positioning activity, the SET establishes a secure connection to the D/H-SLP if it is not already established and then sends a SUPL POS INIT message to start a positioning session with the D/H-SLP.

G. The SET and the D/H-SLP exchange SUPL POS messages to execute the requested positioning activity. The SET and the D/H-SLP MAY release the secure connection after positioning activity is complete.

Steps F and G may be repeated as required and at any time during the lifetime of the GSS (this is illustrated in steps X and Y).

H. When the end of the GSS is reached, the D/H-SLP sends a SUPL END message to the SET. SET and D/H-SLP release all resources related to the GSS.

5.3.5.3 Network Initiated GSS – Roaming

The ULP message exchange for roaming is the same as for non-roaming (see Figure 33). However, the V-SLP is invoked each time the D/H-SLP requires translation of enhanced cell/sector/AP information into a position estimate due to SUPL roaming of the SET (see Figure 2).

5.3.5.4 SET Initiated GSS – Roaming

The ULP message exchange for roaming is the same as for non-roaming (see Figure 34). However, the V-SLP is invoked each time the D/H-SLP requires translation of enhanced cell/sector/AP information into a position estimate due to SUPL roaming of the SET (see Figure 5).

5.3.6 Exception Procedures

5.3.6.1 Triggered Session Pause/Resume Procedure – Network Initiated

This section describes the call flows to pause and resume the network initiated triggered session. In this call scenario, it is assumed that SET is not roaming, however this case will also be applicable if the SET is roaming. Figure 35 illustrates the triggered session pause/resume procedure.

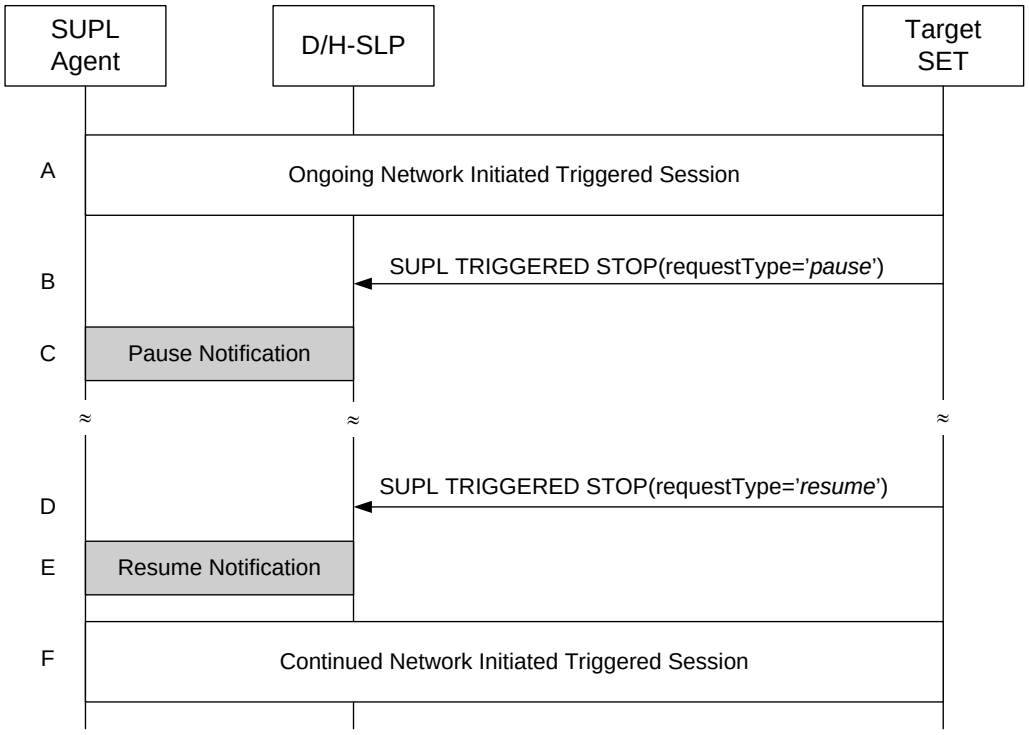

Figure 35: Network Initiated Triggered Session Pause/Resume Procedure Successful Case

A. A triggered session is ongoing.

B. The SET sends a SUPL TRIGGERED STOP message to inform the D/H-SLP that the triggered session in the SET is paused. The SUPL TRIGGERED STOP message SHALL contain the request type parameter (*requestType="pause"*) to indicate that this message is sent in order to pause the current triggered session. Being paused in this context means that the triggered session is still active but that the SET SHALL NOT perform positioning and/or store enhanced cell/section measurements. In case of area event triggered services, the SET SHALL also not perform the Area ID comparison.

C. This step is optional. The D/H-SLP informs the SUPL Agent that the triggered session is paused.

NOTE: The implementation of this step is optional and the presence of this step depends on the D/H-SLP Policy and an implementation.

D. The SET sends a SUPL TRIGGERED STOP message to inform the D/H-SLP that the triggered session in the SET is resumed. The SUPL TRIGGERED STOP message SHALL contain the request type parameter (*requestType="resume"*) to indicate that this message is sent in order to resume the paused triggered session. The SET then SHALL resume the triggered session.

E. This step is optional. The D/H-SLP informs the SUPL Agent that the triggered session is resumed.

NOTE: The implementation of this step is optional hence the presence of this step depends on the D/H-SLP Policy and an implementation.

F. The triggered session is continued.

5.3.6.2 Triggered Session Expires while the Triggered Session is paused – Network Initiated

This section describes the scenario where the stop time of the triggered session expires while the triggered session is paused.

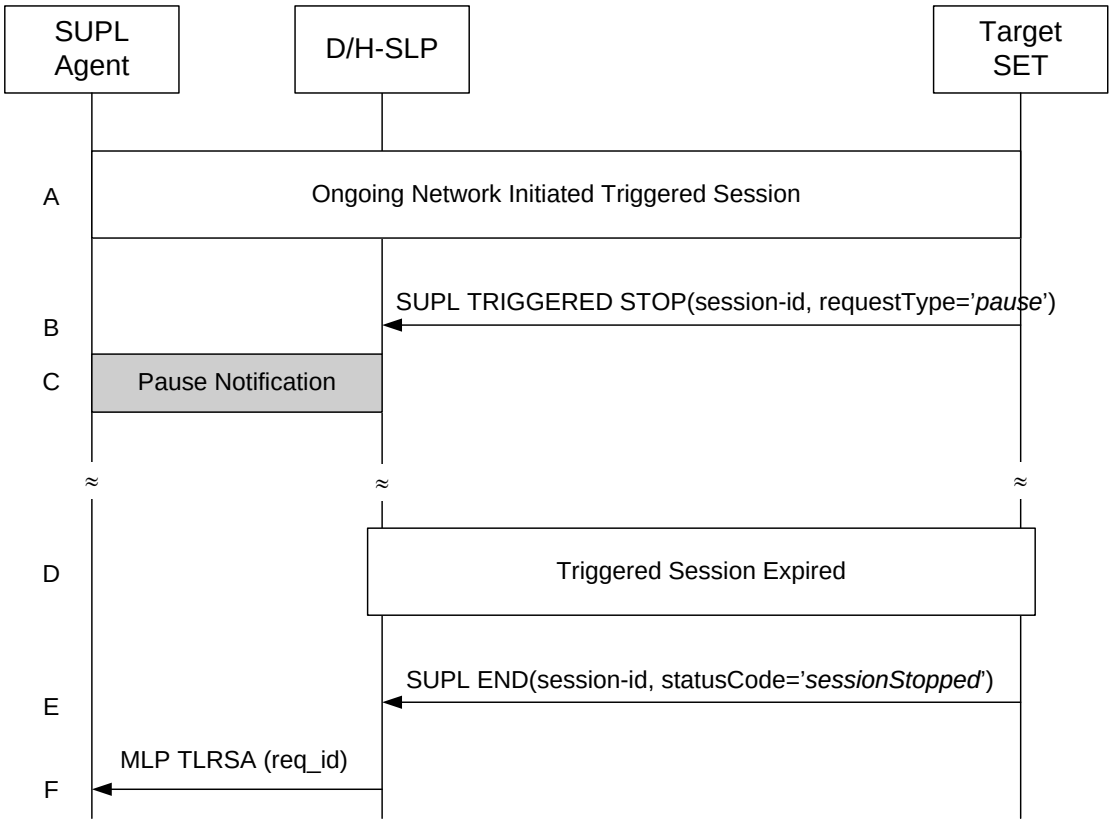

Figure 36: Network Initiated Triggered Session, triggered session expires while the triggered session is paused

A. A triggered session is ongoing.

B. The SET sends a SUPL TRIGGERED STOP message to inform the D/H-SLP that the triggered session in the SET is paused. The SUPL TRIGGERED STOP message SHALL contain the request type parameter (*requestType="pause"*) to indicate that this message is sent in order to pause the current triggered session. Being paused in this context means that the triggered session is still active but that the SET SHALL NOT perform positioning and/or store enhanced cell/section measurements. In case of area event triggered services, the SET SHALL also not perform the Area ID comparison.

C. This step is optional. The D/H-SLP informs the SUPL Agent that the triggered session is paused.

NOTE: The implementation of this step is optional and the presence of this step depends on the D/H-SLP Policy and an implementation.

D. While the triggered session is paused, the stop time of the triggered session is reached.

NOTE: In case of a periodic triggered service, the stop time is defined by the number of fixes, the interval between fixes and the start time.

E. The target SET sends a SUPL END message to the D/H-SLP including the status code "sessionStopped" (*statusCode="sessionStopped")*. The SET releases all resources related to this session.

F. The D/H-SLP sends the MLP TLRSA message to the SUPL Agent confirming cancellation of the triggered session. The D/H-SLP SHALL release all resources related to this session.

5.3.6.3 Triggered Session Pause/Resume Procedure – SET Initiated

This section describes the call flows to pause and resume the SET initiated triggered session. In this call scenario, it is assumed that SET is not roaming, however this case will also be applicable if the SET is roaming. Figure 37 illustrates the triggered session pause/resume procedure.

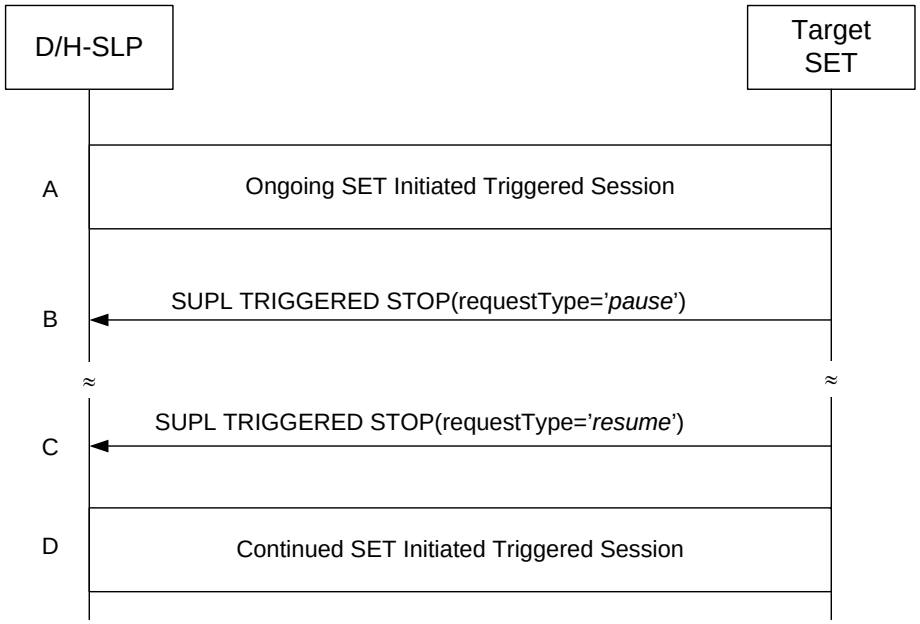

Figure 37: SET Initiated Triggered Session Pause/Resume Procedure Successful Case

A. A triggered session is ongoing.

B. The SET sends a SUPL TRIGGERED STOP message to inform the D/H-SLP that the triggered session in the SET is paused. The SUPL TRIGGERED STOP message SHALL contain the request type parameter (*requestType="pause")* to indicate that this message is sent in order to pause the current triggered session. Being paused in this context means that the triggered session is still active but that the SET SHALL NOT perform positioning and/or store enhanced cell/section measurements. In case of area event triggered services, the SET SHALL also not perform the Area ID comparison.

C. The SET sends a SUPL TRIGGERED STOP message to inform the D/H-SLP that the triggered session in the SET is resumed. The SUPL TRIGGERED STOP message SHALL contain the request type parameter (*requestType="resume")* to indicate that this message is sent in order to resume the paused triggered session. The SET then SHALL resume the triggered session.

D. The triggered session is continued.

5.3.6.4 Triggered Session Expires while the Triggered Session is paused – SET Initiated

This section describes the procedure to handle the case where the stop time of the triggered session expires while the triggered session is paused.

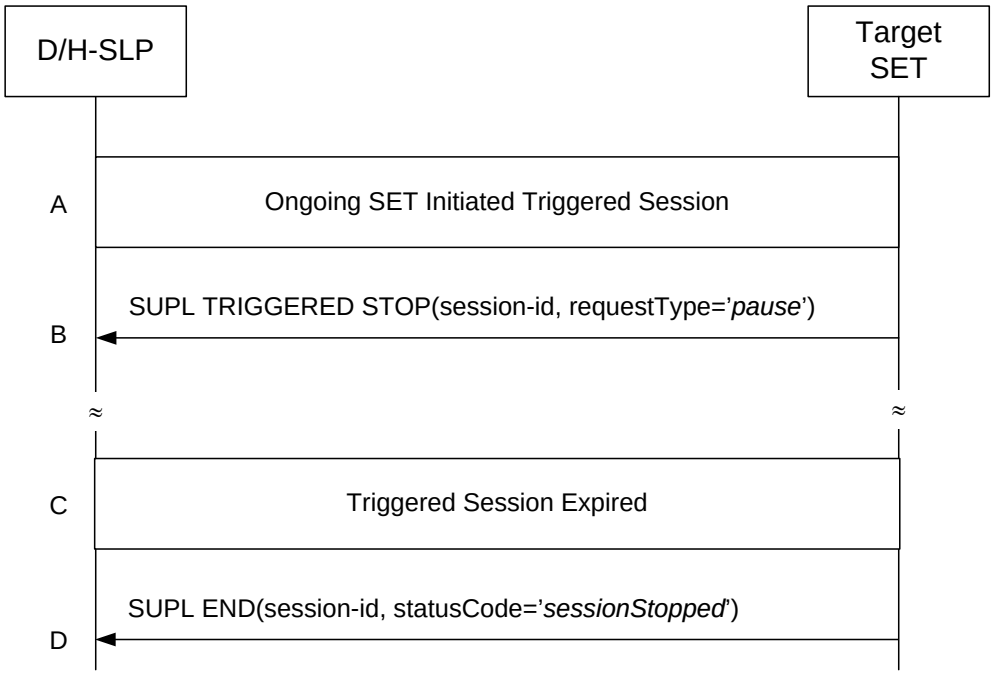

Figure 38: SET Initiated Triggered Session, triggered session expires while the triggered session is paused

A. A triggered session is ongoing.

B. The SET sends a SUPL TRIGGERED STOP message to inform the D/H-SLP that the triggered session in the SET is paused. The SUPL TRIGGERED STOP message SHALL contain the request type parameter (*requestType="pause"*) to indicate that this message is sent in order to pause the current triggered session. Being paused in this context means that the triggered session is still active but that the SET SHALL NOT perform positioning and/or store enhanced cell/section measurements. In case of area event triggered services, the SET SHALL also not perform the Area ID comparison While the triggered session is paused, both triggered sessions paused by the request in the D/H-SLP and the SET SHALL be still active, however the SET SHALL not perform positioning. In case of the area event triggered service, the SET SHALL not also perform the Area ID comparison.

C. While the triggered session is paused, the stop time of the triggered session is reached.

NOTE: In case of a periodic triggered service, the stop time is defined by the number of fixes, the interval between fixes and the start time.

D. The SET sends a SUPL END message to the D/H-SLP including the status code "sessionStopped" (*statusCode="sessionStopped")*. The SET SHALL release all resources related to this session. After receiving the SUPL END message, the D/H-SLP SHALL release all resources related to this session.

5.3.6.5 Network cancels a Triggered SUPL Session

This section describes the scenario where the D/H-SLP cancels an ongoing triggered SUPL session when there is an active TLS connection between the SET and the D/H-SLP.

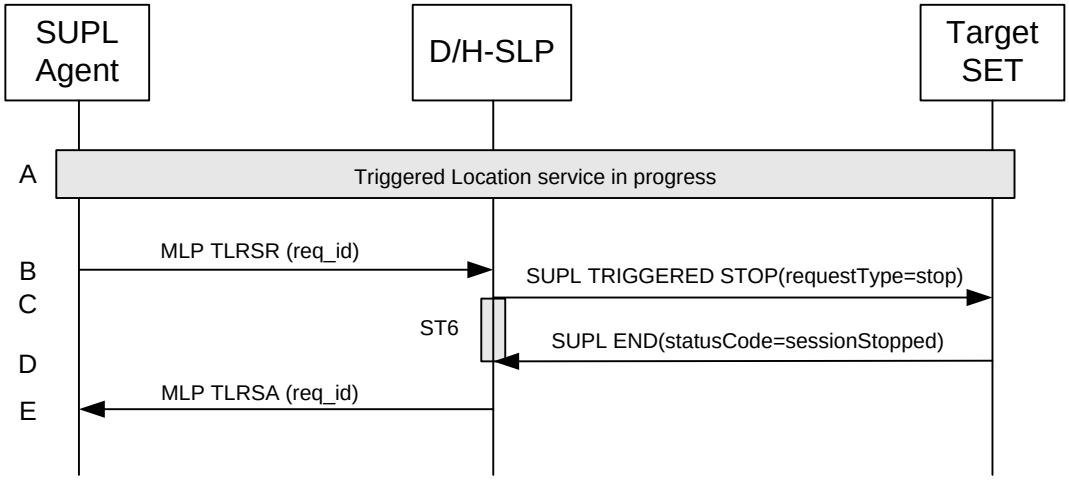

Figure 39: Network cancels the Triggered SUPL session

A. A triggered location session is in progress.

B. The SUPL Agent requests cancellation of the triggered location session by sending an MLP TLRSR message to the D/H-SLP.

NOTE: The cancellation of the triggered location session could have been initiated by the D/H-SLP itself i.e. without the SUPL Agent. In this case the MLP messages shown in steps B and E are superfluous.

C. The D/H-SLP sends a SUPL TRIGGERED STOP message (*requestType=”stop”*) to the target SET to request cancellation of the triggered session. If the D/H-SLP deems the sending of the SUPL TRIGGERED STOP message unsuccessful (i.e. timer ST6 expired with no SUPL END message received), the D/H-SLP considers the triggered session as cancelled and proceeds directly to step E.

D. The target SET acknowledges the cancellation of the triggered session by sending a SUPL END message (statusCode=”sessionStopped”) to the D/H-SLP.

E. The D/H-SLP sends an MLP TLRSA message to the SUPL Agent confirming cancellation of the triggered session.

In scenarios where the D/H-SLP does not have an active TLS connection established with the SET, the D/H-SLP follows the procedure defined in section 5.1.3.2 Session Info Query

5.3.6.6 SET cancels the Triggered SUPL Session

When the SET wishes to cancel a triggered SUPL session, it follows the call flow described in Figure 40.

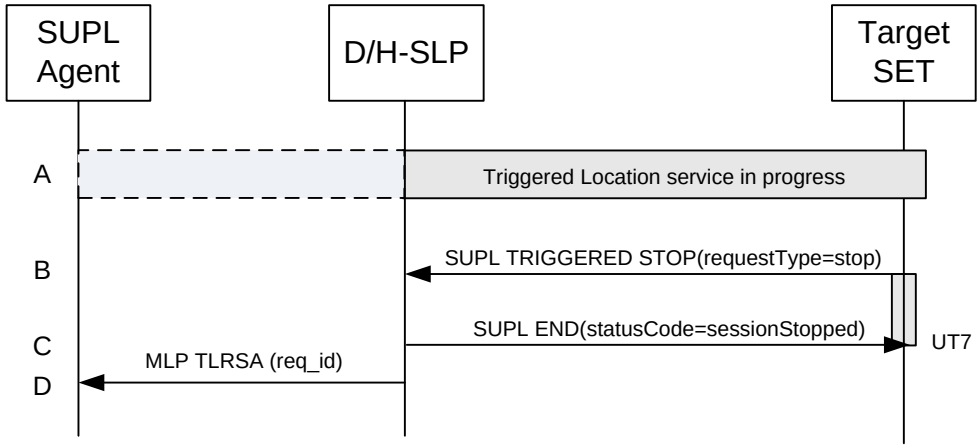

Figure 40: Network cancels the Triggered SUPL session

A. A triggered location session is in progress (applies to both Network and SET Initiated).

B. The SET sends a SUPL TRIGGERED STOP message (requestType=”stop”) to the D/H-SLP to request cancellation of the triggered session.

C. The D/H-SLP sends a SUPL END message (statusCode=”sessionStopped”) to the SET to confirm cancellation of the triggered session. The SET SHALL release the TLS connection and release all resources related to this session.

D. For Network Initiated scenarios: the D/H-SLP MAY notify the SUPL Agent that the triggered session has been cancelled by sending a MLP TLRSA message. The D/H-SLP SHALL release all resources related to this session.

5.3.7 Retrieval of Historic Positions and/or Enhanced Cell Sector Measurements

A SET may store calculated positions and/or network measurements for later retrieval by the network. This section describes the retrieval of stored historic positions and/or enhanced cell/sector measurements.

5.3.7.1 Retrieval of Historic Position Results – Non-Roaming

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

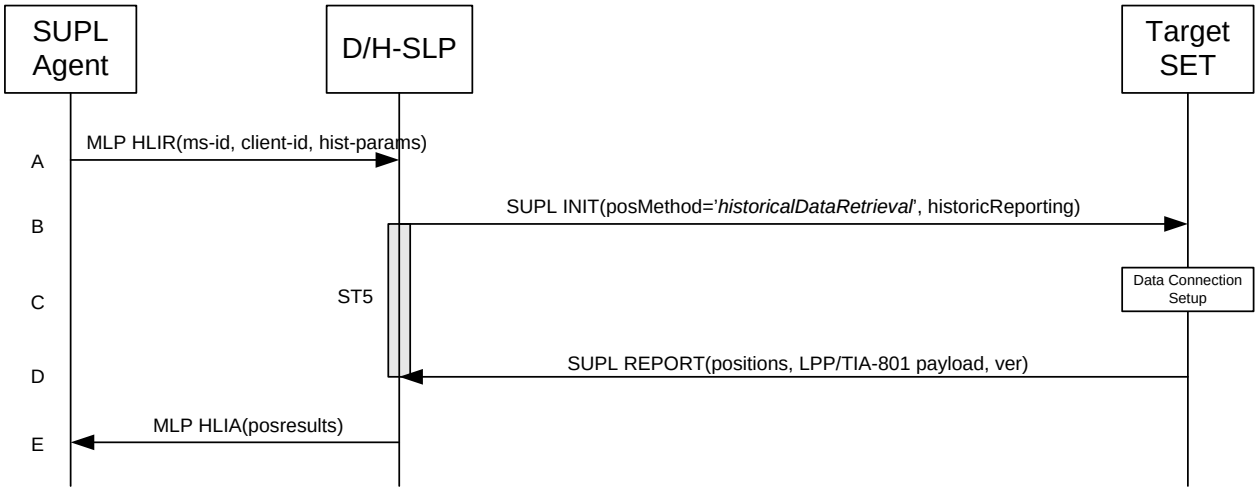

Figure 41: Retrieval of historic positions and/or enhanced cell/sector measurements – non-roaming

A. The SUPL Agent sends an MLP HLIR message to the D/H-SLP, with which SUPL Agent is associated. The D/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 D/H-SLP SHALL apply subscriber privacy against the client-id. The *hist-params* parameter in the HLIR message defines criteria to be applied by the SET when selecting historic positions to be reported to the SUPL Agent (e.g. time window, QoP, etc.).

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

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

D. The SET evaluates the Notification rules and takes appropriate action. The SET SHALL then establish a TLS connection to the D/H-SLP using the D/H-SLP address which is either the H-SLP address provisioned by the Home Network or the D-SLP address provided or verified by the H-SLP or by a Proxy D-SLP authorized by the H-SLP. The SET selects historic position estimates and/or historic enhanced cell/sector measurements based on the criteria received in step B and sends the positions and/or enhanced cell/sector measurements in a SUPL REPORT message to the D/H-SLP. The SUPL REPORT message also contains the hash of the received SUPL INIT message (*ver*). After sending the SUPL REPORT message, the SET SHALL release all resources related to this session.

E. The D/H-SLP converts any enhanced cell/sector measurements received in step D into corresponding position estimates and reports the historic position estimates to the SUPL Agent in a MLP HLIA message.

5.3.7.2 Retrieval of Historic Position Results – Roaming

The following call flow defines the retrieval of historic position results from the SET for roaming. In the context of retrieval of historic position and/or enhanced cell/sector measurements roaming means that enhanced cell/sector measurements reported by the SET were taken while the SET was SUPL roaming.

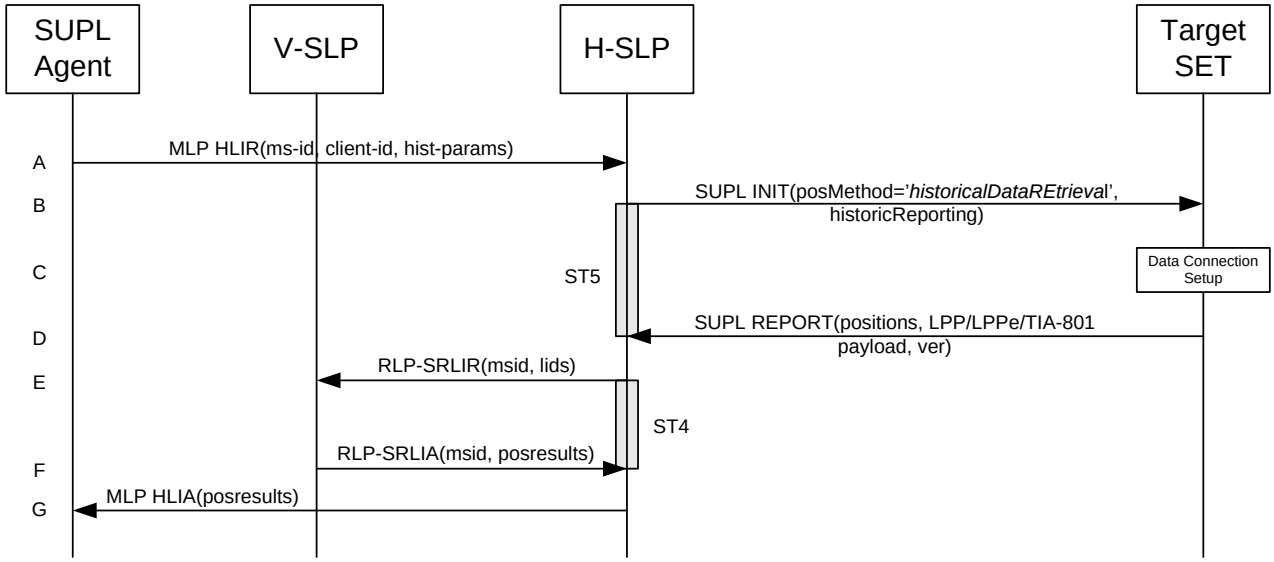

Figure 42: Retrieval of historic positions and/or enhanced cell/sector measurements – roaming

A. The SUPL Agent issues an MLP HLIR 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. The *hist-params* parameter in the HLIR message defines criteria to be applied by the SET when selecting historic positions to be reported to the SUPL Agent (e.g. time window, QoP, etc.).

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

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

D. The SET evaluates the Notification rules and takes appropriate action. The SET SHALL then establish a TLS connection to the H-SLP using an H-SLP address provisioned by the Home Network.

The SET selects historic position estimates and/or historic enhanced cell/sector measurements based on the criteria received in step B and sends the positions and/or enhanced cell/sector measurements in a SUPL REPORT message to the H-SLP. The SUPL REPORT message also contains the hash of the received SUPL INIT message (*ver*). After sending the SUPL REPORT message, the SET SHALL release all resources related to this session.

E. If in step D the H-SLP received enhanced cell/sector measurements, the H-SLP converts them into position estimates. However, enhanced cell/sector measurements taken while the SET was SUPL roaming, cannot to be converted into position estimates by the H-SLP itself. These measurements are instead forwarded to the respective V-SLP in a RLP-SRLIR message.

F. The V-SLP converts the enhanced cell/sector measurements into position estimates and returns the results to the H-SLP in a RLP-SRLIA message.

G. The H-SLP reports the historic position estimates to the SUPL Agent in an MLP HLIA message.

5.3.8 Network/SET capabilities Change for Area Event Triggered Scenarios

Area Event trigger scenarios which rely on area-ids to determine the trigger condition require updating of trigger parameters after network change since area-ids are network dependent. This assumes that a V-SLP exists which is able to update the area id parameters which are part of the trigger parameters. The described mechanism applies to Network Initiated and SET Initiated.

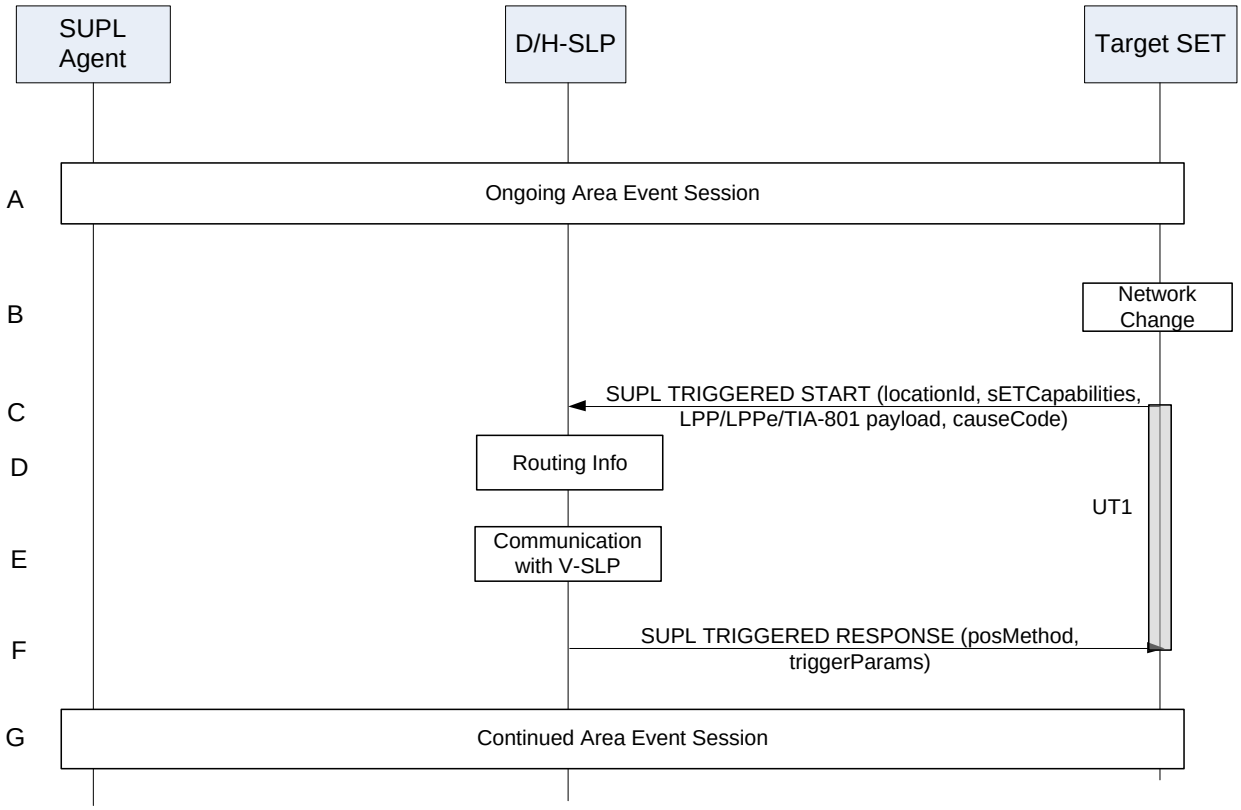

Figure 43: Network/SET capabilities change for Area Event Trigger Scenarios

A. An Area Event session is ongoing.

B. The SET monitors serving network identity and SET capabilities. If the SET detects that it has changed networks and the new serving network is not part of any downloaded area id lists or if the SET detects that the SET capabilities have changed, the SET continues to step C.

C. The SET SHALL establish a TLS connection with the D/H-SLP and send a SUPL TRIGGERED START message to request new event trigger parameters and/or positioning methods. The SUPL TRIGGERED START message contains the Location ID (*locationId*), SET capabilities, cell/sector/AP information carried within LPP/LPPe/TIA-801 payload and the cause for re-sending the SUPL TRIGGERED START message. The SET capabilities include the supported positioning methods and positioning protocols (e.g., LPP/LPPe or TIA-801).

D. This step is optional and only applies to an H-SLP and if a network change was detected by the SET (as opposed to a change in SET capabilities only). Based on information received in the SUPL TRIGGERED START message of step C, the H-SLP determines whether a V-SLP exists which is able to update the area-id parameters.

E. This step is optional and only applies if step D was performed: if in step D the H-SLP was able to determine a V-SLP capable of updating the area-id parameters, the H-SLP communicates with that V-SLP in order to obtain the updated area-id parameters.

F. The D/H-SLP sends a SUPL TRIGGERED RESPONSE message to the SET including the positioning method and area event trigger parameters to be used. If a network change occurred and steps D and E were executed successfully, the SUPL TRIGGERED RESPONSE message may contain the updated area ids. If the D/H-SLP does not provide new trigger parameters in the SUPL TRIGGERED RESPONSE then the SET SHALL maintain the previous trigger parameters.

G. The Area Event session continues.

6. Security Considerations

This section describes the SUPL Security function that enables the SUPL network to authenticate and authorize the SET and enables the SET to authenticate and authorize the SUPL network.

NOTE: Unless otherwise specified, the use of the acronym TLS refers to any session that can be negotiated using a TLS handshake: this includes both TLS 1.1 ciphersuites and TLS-PSK ciphersuites.

NOTE: In this section, the following definitions apply. A *3GPP bearer network* is one for which the standards are maintained by 3GPP; these include GSM, GPRS, EDGE, WCDMA/TD-SCDMA, LTE and LTE-A bearer networks. A *3GPP2 bearer network* is one for which the standards are maintained by 3GPP2; these include cdmaOne, cdma2000 1x and cdma2000 EV-DO bearer networks. An *alternative access network* is any technology other than 3GPP, 3GPP2 and WiMAX.

NOTE: H-SLP operators should note that the authentication methods described herein remain valid for SET handover between access networks belonging to the same operator or where the SET IP address is not changed. The procedures do not take into account scenarios where the SET moves from one access network to another belonging to different operators or where the IP address changes. It is assumed in these scenarios, that after the handover to another access system, the security context may not be available in the terminal and the network and the level of trust between the network and terminal may change.

On powering up and shutting down, detection of a new UICC or removal of a UICC, the SET handset MUST delete any keys (aside from long-term keys) on the SET handset associated with SUPL 3.0, including

- **GBA Keys:** such as Ks, Ks_NAF, Ks_ext_NAF
- **WIMAX Keys:** such as SEK
- **TLS Keys**: such as pre_master_secret, master_secret, and PSK values (aside from long-term keys).
- **SUPL Specific Keys**: such as keys associated with protection of SUPL INIT and SUPL REINIT messages.

6.1 SUPL Authentication Methods

Authentication support requirements for SUPL 3.0 are as follows:

- Mutual authentication SHALL be supported between a SET and an H-SLP.
- Mutual authentication SHALL be supported between a SET and a D-SLP.
- Server authentication SHALL be supported between a SET and an E-SLP, and mutual authentication MAY be supported between a SET and E-SLP.

SUPL 3.0 supports two classes of SET authentication methods

- AN-Dependent method, where the credentials are bound to the Access Network subscription of the SET User.
- AN-Independent methods, where the credentials are bound to the SET, but not directly bound to the Access Network subscription of the SET User. Binding such credentials to the Access Network subscription of the SET User may be achieved using out-of-scope procedures. See Section 6.6 for more discussion of out-of-scope procedures.

When mutual authentication is performed, the SET SHALL act on behalf of the SET User.

- For AN-Dependent methods, the SET uses the security credentials associated with the SET User.
- For AN-Independent methods, the SET uses the security credentials associated with the SET.

Note that a successful authentication of the SET User MUST result in a successful identification of the SET User's ID (e.g., MSISDN, WIMAX user ID or AN-independent user identity).

Note that when MSISDN is used for identification, the SLP MUST perform an IMSI to MSISDN binding before the MSISDN of the authenticated SET User is securely identified.

The details of Key Management can be found in section 6.1.2.

6.1.1 Authentication Methods

Section 6.1.1.1 lists the authentication methods supported in this specification. An informative overview of these methods is provided in section 6.1.1.2. Section 6.1.1.3 describes which methods are mandatory or optional in the various SUPL 3.0 entities, and lists the protocols required in each entity if it is to support a given mutual-authentication method.

6.1.1.1 List of Supported Mutual-Authentication Methods

The SUPL Authentication model requires establishing shared secret keys between the SLP and the SET, bound to either a removable token such as an R-UIM/UICC/SIM/USIM or the SET handset.

There are two classes of authentication methods specified in this document:

- PSK-based methods, consisting of the following methods:
    - AN-Dependent Generic Bootstrapping Architecture (GBA)-based method, providing mutual authentication;
    - AN-Dependent SEK based method (only applicable to a WIMAX SLP), providing mutual authentication;
- Certificate based methods, consisting of the following methods:
    - AN-Independent Device-Certificate based (DCert) Method, providing mutual authentication;
    - AN-Dependent Alternative Client authentication (ACA)-based method, providing mutual authentication;
    - AN-Independent SLP-only method (only applicable in emergency cases), providing SLP authentication only.

6.1.1.2 Overview of Supported Authentication Methods (Informative)

(1) Generic Bootstrapping Architecture (GBA)-Based. TLS-PSK with Generic Bootstrapping Architecture (GBA) [3GPP 33.220], [3GPP 33.222], [3GPP2 S.S0114], [3GPP 24.109]. GBA provides mutual authentication capability based on shared secret that is derived using existing 3GPP/3GPP2 authentication mechanisms.

- SET and SLP are mutually authenticated using TLS-PSK with Generic Bootstrapping Architecture (GBA).

(2) SEK based (only applicable to WIMAX SLP).

- SET and SLP are mutually authenticated using TLS-PSK with SEK. The details of SEK method can be found in section 6.1.2.1.2.

(3) Device Certificate (DCert)-based. This AN-Independent method uses TLS with

- RSA server certificate to authenticate the SLP to the SET,
- RSA client certificate to authenticate the SET to the SLP.

(4) Alternative Client authentication (ACA)-based. This uses TLS with

- RSA certificate to authenticate the SLP to the SET,
- Alternative Client authentication of the SET to the SLP (see section 6.1.4). In this case, the SLP authenticates the SET by getting the bearer network to confirm the IP address associated with the SET Identifier (MSISDN etc.).

(5) SLP-only. This is used in scenarios where it is not possible for the SLP to authenticate the SET. This method SHALL NOT be used for non-emergency cases. The SET cannot distinguish between this method and ACA-based. This uses TLS with

- An RSA certificate to authenticate the SLP to the SET,

- The SET is not authenticated.

6.1.1.3 Support for Mutual-Authentication Methods and Protocols by Entity

Table 1, Table 2, Table 3 and Table 4 describe what is optional and mandatory to support for SUPL 3.0 in SETs supporting various technologies and SLP's supporting those SETs:

- Table 1, indicates those methods that are mandatory and those methods that are optional to implement for SUPL 3.0 in
  - SETs supporting 3GPP and or 3GPP2,
  - SET (R-)UIM/ SIM/USIM in those SETs, and
  - SLPs supporting those SETs;
- Table 2 indicates those methods that are mandatory and those methods that are optional to implement for SUPL 3.0 in
  - SETs supporting WiMAX, and
  - SLPs supporting those SETs;
- Table 3 indicate those methods that are mandatory and those methods that are optional to implement for SUPL 3.0 in
  - SETs that support an alternative access network, and
  - SLPs supporting those SETS.
- Table 4 lists the required protocols for the SLP, SET Handset and (where applicable) SET (R-)UIM/ SIM/USIM for supporting each of the various authentication methods.

For SETs supporting more than one type of access networks (3GPP/3GPP2, WiMAX and alternative access networks), the requirement status should be aggregated from the corresponding tables., using the following rules:

- A requirement status of "Mandatory" over-rides all other requirement status.
- A requirement status of "Optional" over-rides any requirement status other than "Mandatory".

Entity	Requirement Status for SUPL Authentication Method for SETs supporting 3GPP and/or 3GPP2, SET (R-)UIM/ SIM/USIM and SLPs supporting these SETs			
	PSK-based methods	Certificate Based Methods		
	GBA-based	ACA-based	DCert	SLP-only (E-SLP only)
SET Handset	**Optional**	**Mandatory.** The ACA-based method from the SET perspective is identical to SLP-only method. SET Handset support for ACA can thus be mandatory due to mandatory support for SLP-only	**Optional**	**Mandatory.** SET Handset support for SLP-only is required for emergency cases
SET SIM/USIM/ (R)-UIM	SIM/USIM/(R)-UIM is involved in this method, but it already supports the necessary algorithm	This entity is not involved in this method	This entity is not involved in this method	This entity is not involved in this method
D/H-SLP	**Mandatory** to support one of these two methods		**Optional**	**Not supported**
E-SLP	**Optional**	**Optional**	**Optional**	**Mandatory**

Table 1: Requirement status (mandatory or optional) of the various authentication methods for SETs supporting 3GPP and/or 3GPP2 and SLPs supporting these SETs.

Entity	Requirement Status for SUPL Authentication Method for SETs supporting WiMAX, and SLPs supporting these SETs			
	PSK-based methods	Certificate Based Methods		
	SEK based	ACA-based	DCert	SLP-only (E-SLP only)
SET Handset	**Mandatory**	**Not Supported**	**Optional**	**Mandatory**
D/H-SLP	**Mandatory**	**Not Supported**	**Optional**	**Not Supported**
E-SLP	**Optional**	**Not Supported**	**Optional**	**Mandatory**

Table 2: Requirement status (mandatory or optional) of the various authentication methods for WiMAX SETs supporting WiMAX, and SLPs supporting these SETs .

Entity	Requirement Status for SUPL Authentication Method for SETs not supporting 3GPP, 3GPP2 or WiMAX but supporting at least one alternative access network, and SLPs supporting these SETs			
	PSK-based methods	Certificate Based Methods		
	SEK /GBA based	ACA-based	DCert	SLP-only (E-SLP only)
SET Handset	**Not Supported**	**Not Supported**	**Mandatory**	**Mandatory**
D/H-SLP	**Not Supported**	**Not Supported**	**Mandatory**	**Not Supported**
E-SLP	**Not Supported**	**Not Supported**	**Optional**	**Mandatory**

Table 3: Requirement status (mandatory or optional) of the various authentication methods for SETs not supporting 3GPP, 3GPP2 or WiMAX but supporting at least one alternative access network and SLPs supporting these SETs

Entity	Algorithms required to support the Authentication Method between SET and SLP				
	PSK-based methods		Certificate Based Methods		
	GBA-based (3GPP/3GPP2 only)	SEK-based (WiMAX only)	ACA-based (3GPP & 3GPP2 only)	DCert	SLP-only (E-SLP only)
SLP	GBA & TLS-PSK	SEK & TLS-PSK	TLS using server certificates & IP Address/SET ID binding	TLS using server certificates and client certificates	TLS using server certificates
SET Handset	GBA & TLS-PSK	SEK & TLS-PSK	TLS using server certificates	TLS using server certificates and client certificates. Certificates must be provisioned in the SET Handset	TLS using server certificates
SET R-UIM/UICC/ SIM/USIM	No additional algorithms required	Not applicable	No additional algorithms required	Not applicable	Not applicable

Table 4: Required protocols for the SLP, SET Handset and SET R-UIM/UICC/SIM/USIM for supporting the various mutual authentication methods.

NOTE: Where the GBA-based method is supported, the BSF retrieves (from the HSS or AAA) user security settings (USS) associated with the H-SLP applications.

When the H-SLP requests the USS, the BSF MUST include a SET user identity (e.g. IMPI, IMSI or MSISDN) in the USS.

NOTE: The GBA-based method is not dependent on using a 3GPP or 3GPP2 bearer network to transport the SUPL sessions. However, the SET must have a 3GPP or 3GPP2 home network operator in order to have the necessary credentials for performing GBA.

6.1.1.4 Techniques for Minimizing the TLS Handshake Workload

The procedures in this section minimize the workload associated with establishing TLS sessions between the SLP and SET. Where there is a conflict with [TLS], [TLS] takes precedence.

If a SET and SLP are communicating SUPL messages associated with more than one SUPL sessions simultaneously, then the SET and SLP SHOULD use a single TLS sessions to secure these messages; that is, the SET and SLP SHOULD NOT establish distinct TLS sessions if SUPL sessions are simultaneous.

If the SET and the SLP establish a TLS session, then the SLP MAY allow the session to be resumed using the abbreviated handshake shown in Figure 1 of [TLS]. The advantage of resuming a TLS session is that resuming a TLS session based on server certificates does not require the public-key operations: only symmetric cryptographic algorithms are required (which require significantly less processing).

NOTE: This approach is not recommended for E-SLP's since emergency SUPL sessions occur too occasionally to warrant storing the necessary data.

NOTE: The SLP allows the session to be resumed by allocating a TLS SessionID as described in [TLS].

NOTE: There is no advantage to resuming a TLS-PSK session (as used for GBA and SEK-based authentication), since the same computations are performed. However, an SLP may still allow resuming a TLS-PSK session.

NOTE: A SET indicates the choice to resume a TLS session by including the TLS SessionID (of the TLS session to be resumed) in the TLS SessionID parameter in the ClientHello message of the TLS Handshake. If the SET does not wish to resume a TLS session, then the SET sends the TLS ClientHello message without including the TLS SessionID, in which case the full handshake will be performed. If the TLS SessionID parameter is present in the TLS ClientHello message, the SLP then chooses whether or not to resume the TLS session. If no SessionID parameter is present in the TLS ClientHello message, then the SLP cannot associate the TLS handshake with a previous TLS Session, so the TLS handshake establishes a completely fresh TLS session using a full handshake. The details are specified in [TLS].

The SET chooses whether or not to resume a TLS session, using the following guidelines.

- The SET MUST NOT resume a TLS session if the underlying credentials (Ks(_ext)_NAF or SLP certificate or SEK or Device Certificate) are expired.
- The SET MAY choose to not resume a TLS session earlier than the expiry of the underlying credentials, if desired.
- The SET MUST NOT resume a session that was established prior to power-up or detection of a new R-UIM/ UICC/SIM/USIM.

The SLP chooses whether or not to resume a TLS session, using the following guidelines.

- The SLP MUST NOT resume a TLS session if the underlying credentials (Ks(_ext)_NAF or SLP certificate or SEK or Device Certificate) are expired.
- The SLP MAY choose to not resume a TLS session earlier than the expiry of the underlying credentials if desired.

NOTE: Each SLP must decide for itself whether or not to allow abbreviated handshakes, and this decision can even be made on a SET-by-SET basis. The SLP is taking a small risk when it accepts to resume an existing TLS session. This risk is the possibility of a "naughty" SET distributing the master_secret (established during a full TLS handshake), so that others may resume that TLS session, thus allowing multiple SETs to obtain service that will be charged to a single SET. The "naughty" SET could be doing this without the knowledge of the SET owner (for example, a malicious code could be at fault). Note that

the loss can be easily limited: if a SLP detects (or suspects) that such abuse is occurring, then the SLP can easily (a) end the TLS sessions using that master_secret, (b) identify the "naughty" SET and (c) re-authenticate the "naughty" SET using full handshake to allow the user to continue to have service if required. In summary, the benefit of resuming sessions (in terms of reduced computation) for the DCert method, ACA-based method and SLP-only method is thought to exceed the risk of attack.

6.1.2 Key Management for SUPL Authentication

The SUPL Authentication model requires establishing shared secret keys between the SLP and the SET, bound to either a removable token such as an R-UIM/UICC/SIM/USIM or the SET handset.

6.1.2.1 PSK-Based Methods

6.1.2.1.1 Deployments Supporting the GBA Method

In the case of deployments supporting (GBA [3GPP 33.220], [3GPP2 S.S0109]), the shared keys are established as follows:

- When the SLP requests key material from the BSF (for securing IP communication and for protecting SUPL INIT and/or SUPL REINIT), the SLP MUST also request the USS (User security settings). The USS MUST include a permanent user identity (e.g. IMPI, IMSI or MSISDN).

- For securing IP communication between the SET and SLP, the SET and the SLP MUST derive a shared secret key and operate according to TLS-PSK using GBA ([3GPP 33.220], [3GPP 24.109], [3GPP 33.222], [3GPP2 S.S0109]). The SLP MUST have well defined domain name SLP_Address_FQDN designating the SLP, e.g., slp.operator.com. The GBA Ua security protocol identifier that shall be used for TLS-PSK is defined in OMNA Registry [OMNA]. The SLP MUST confirm that the permanent user identity provided by the BSF corresponds to the SET identity in SUPL messages received by the SLP over the corresponding secured connection.

- For MAC protection of SUPL INIT and/or SUPL REINIT, keys are derived according to GBA ([3GPP 33.220], [3GPP2 S.S0109]). The GBA Ua security protocol identifier that shall be used for SUPL INIT protection is defined in OMNA Registry [OMNA]. The keyIdentifier of the basicMAC included in the SUPL INIT message (or SUPL REINIT message) MUST be the B-TID of the Ks from which the Ks_NAF is generated.

  NOTE: The D/H-SLP request for SUPL INIT protection keys from the BSF would typically occur simultaneously with the D/H-SLP request for the keys securing IP communication.

- The SET MUST ensure that it is always provisioned with a valid Ks. If no valid Ks is present then the SET MUST initiate the GBA Bootstrapping procedure to provision Ks. A new Ks MUST be established each time a new UICC (USIM/SIM/R-UIM) is detected by the SET. Additionally, the SET MUST establish new shared keys when the Ks_NAFs lifetime (set by the Home Network operator) expires.

6.1.2.1.2 Deployments Supporting the SEK Method

In the case of deployments supporting SEK, the shared keys are established as follows:

- For securing IP communication between the SET and SLP, the SET and SLP MUST derive a shared secret key and confirm that the permanent user identity provided by the WiMAX AAA server corresponds to the SET identity in the SUPL messages received by the SLP over the corresponding secured connection. The shared keys are derived in the following way:

  - SEK = the 16 most significant (leftmost) octets of HMAC-SHA256(LSK, "slp.operator.com") where 'operator.com' is the FQDN of the WIMAX operator and LSK is derived as specified in WiMAX Network Protocols and Architecture for Location Based Services.

  - SEK will inherit the Location Key Identifier (LSK-ID) (as defined in WiMAX Network Protocols and Architecture for Location Based Services) associated with the LSK and the key identity will be used as the B-TID for WiMAX deployments.

- For MAC integrity protection of SUPL INIT and/or SUPL REINIT messages, keys are derived the following way:

- SEK_MAC = the 16 most significant (leftmost) octets of HMAC-SHA256(LSK, “mac.slp.operator.com”) where 'operator.com' is the FQDN of the SLP operator and LSK is derived as specified in WiMAX Network Protocols and Architecture for Location Based Services.
- The keyIdentifier of the Mode AMAC included in the SUPL INIT and/or SUPL REINIT message MUST be the B-TID of the LSK from which the SEK_MAC is generated.

  NOTE: The SLP request for SUPL INIT protection keys from the WiMAX AAA would typically occur simultaneously with SLP request for the keys securing IP communication.

The SET MUST ensure that it is always provided with a valid SEK. If no valid SEK is present then the SET MUST derive the SEK as specified above. Additionally, the SET MUST establish new shared keys when the lifetime of the LSK expires. The interface between the SLP and the WiMAX AAA server is out of scope of SUPL 3.0.

6.1.2.2 Server-Certificate Based Methods

6.1.2.2.1 Deployments Supporting the DCert Method

In the case of deployments supporting the DCert method, the shared keys are established as follows:

- For securing IP communication between the SET and SLP, the SET and SLP MUST use TLS-RSA [TLS] with a server-certificate authenticating the SLP and a client certificate authenticating the SET. The client certificate shall provide at least one globally unique SET device identity::
  - SETs supporting 3GPP SHOULD include the IMEI as a globally unique SET device identity.
  - SETs supporting 3GPP2 SHOULD include the MSID as a globally unique SET device identity.
  - SETs supporting WiMAX SHOULD use the SET serial number as a globally unique SET device identity.
  - In all SETs, a globally unique serial number MAY be used as the globally unique SET device identity.
- The client certificate is assumed to be provisioned into the SET Device.
- The SUPL User must securely verify to the SLP that this device should be associated with their subscription. This secure verification is out of scope of this specification. See Section 6.6 for further discussion of this topic.
- For MAC integrity protection of SUPL INIT and SUPL REINIT messages, keys are provided to the SET by the SLP in a ULP message. This is described in Section 6.3.5.

6.1.2.2.2 Deployments Supporting the ACA Method

In the case of deployments supporting the ACA method, the shared keys are established as follows:

- For securing IP communication between the SET and SLP, the SET and SLP MUST use TLS-RSA [TLS] with a server-certificate authenticating the SLP. SET authentication (which binds the resulting shared secret keys to either the removable or integrated token discussed above) is described in section 6.1.4 for non-emergency cases and sections 6.2.5 for emergency cases.
- For MAC integrity protection of SUPL INIT and/or SUPL REINIT messages, keys are provided to the SET by the SLP in a ULP message. This is described in Section 6.3.5.

6.1.2.2.3 Deployments Supporting the SLP-Only Method

In the case of deployments supporting the SLP-Only Method, the shared keys are established as follows:

- For securing IP communication between the SET and SLP, the SET and SLP MUST use TLS-RSA [TLS] with a server-certificate authenticating the SLP. There is no SET authentication (which binds the resulting shared secret keys to either the R-UIM/UICC/SIM/USIM or the SET handset).
- MAC protection of SUPL INIT and/or SUPL REINIT messages is not supported in these cases.

6.1.3 TLS Handshake and Negotiation of Mutual-Authentication Method

The SET and SLP need to agree on a mutually-supported authentication method to be applied.

6.1.3.1 Regarding negotiating a Mutual-Authentication Method (Informative)

When establishing a TLS connection to the H-SLP, the SET first attempts to establish a connection using the mutually-supported authentication mechanism with highest preference, according to the following order of preference:

- PSK-based methods: GBA or SEK-based method first preference (if supported);
- DCert method: second preference (if supported);
- ACA or SLP-only methods: third preference (from the SET's perspective there is no difference between the ACA-based method and the SLP-only method).

If there is no mutually-supported authentication method, then the SET shall be unable to perform SUPL session.

A SET that supports PSK based methods may be unable to use the GBA-based method or SEK-based method at a given point in time due to a BSF or WiMAX AAA experiencing problems. Therefore, an attempt by the SET to establish authentication using GBA or SEK does not guarantee that the SET shall be able to establish GBA or SEK-based keys.

Consequently, the SET may not always be able to use the mutually-supported authentication mechanism with highest preference. The SET may have to revert to a less preferable mutually-supported authentication mechanism if available.

If the SLP supports only GBA or SEK, then the SLP is restricted to providing SUPL 3.0 services to subscribers of carriers that have deployed GBA or SEK. If the SLP supports only ACA, then SUPL 3.0 can only be used in circumstances discussed in detail in section 6.1.4. Note that in such a case, if the SET communicates via an alternative bearer (such as wireless LAN) for which the SLP cannot obtain IP binding, then the SLP will be unable to authenticate the SET.

If the E-SLP supports only ACA, then there are caveats on SET authentication, as discussed in detail in section 6.2.5.

6.1.3.2 Negotiating a Mutual-Authentication Method

This specification does not provide a mechanism for the negotiation of the SEK-based method. If the SLP supports the SEK-based method, then the SLP provides an indication to the SETs that support WiMAX using some out-of-scope mechanism such as pre-configuration. If a SET does not have an indication that an SLP supports the SEK-based method, then the SET assumes that the SLP does not support the SEK-based method.

For all other cases (that is, for SETs that do not support WiMAX, and for SETs that support WiMAX but where the SLP has not indicated support for the SEK-based method), the negotiation of a mutual authentication method for SUPL sessions proceeds as follows:

1. The SET initiates negotiation
   a. If the SET supports GBA, then the SET initiates negotiation according to the relevant GBA specifications (see specifications listed at the end of the call flow)
   b. Otherwise (that is, if the SET does not support GBA) then the SET initiates a TLS handshake with a ClientHello message, with ClientHello.cipher_suites field indicating the supported TLS ciphersuites using RSA encryption for the TLS key exchange algorithm.
2. The SLP processes the received ClientHello message. The SLP examines the ClientHello.ciphersuites list and selects a mutually-supported ciphersuite.
   a. If the SET and SLP both support a TLS-PSK ciphersuite, then this indicates support for GBA. The SLP responds with a ServerHello, ServerKeyExchange and ServerHelloDone message, with ServerHello.cipher_suite indicating a mutually-supported TLS-PSK ciphersuite and ServerKeyExchange formed as in the relevant GBA specifications listed below. The details are outside the scope of this document.
   b. Otherwise, the SET and SLP must support a Certificate based method

i. If the SLP supports the DCert method, then the SLP responds with

1. ServerHello with ServerHello.cipher_suite indicating a mutually-supported TLS ciphersuite using RSA encryption for the TLS key exchange algorithm,
2. Certificate,
3. CertificateRequest and
4. ServerHelloDone message.

ii. Otherwise, if (a) the SET is using a 3GPP/3GPP2 bearer network and the SLP supports the ACA method or (b) the SLP supports the SLP only method, then the SLP responds with

1. ServerHello Certificate, with ServerHello.cipher_suite indicating a mutually-supported TLS ciphersuite using RSA encryption for the TLS key exchange algorithm.
2. Certificate,
3. (No CertificateRequest message is sent)
4. ServerHelloDone message

3. The SET processes the received ServerHello message and other messages:

a. If ServerHello.cipher_suite indicates that GBA has been selected by the SLP (as per the relevant GBA specifications) then the SET and SLP continue the process specified in the relevant GBA specifications listed below. The details are outside the scope of this document.

b. Otherwise, the ServerHello.cipher_suite indicates a mutually-supported TLS ciphersuite using RSA encryption for the TLS key exchange algorithm. The SET first verifies the SLP certificate as in [TLS]. The next steps depend on whether the SET received a CertificateRequest message:

i. If the SET received a CertificateRequest then

1. If the SET supports DCert method, then the SET provides a Device Certificate and the SET and Server complete the TLS handshake as in [TLS]. The Server attempts to identify the SUPL User associated with the globally unique SET device identity in the Device Certificate. *It is presumed that the SUPL User has already securely verified to the SLP that the SET device identity should be associated with their subscription – see Section 6.6 for more details.*

a. If no SUPL User is identified, then the session must be terminated. Since we assume that the TLS handshake has already completed, the Server is capable of communicating at the ULP layer. The Server must send an appropriate ULP error message to terminate the ULP session and then close the TLS session.

b. If a SUPL User is identified, then the Server provides the SET with the same authorizations as the SUPL User.

2. Otherwise, the SET replies to the SLP, including an empty ClientCertificate message to implicitly indicate that it does not support the DCert method.

a. If the SLP supports the ACA, then the SLP and SET continues as per the ACA method. The SLP may continue using the ACA method

b. If the SLP does not support the ACA or SLP-only method (the SLP might have supported only the DCert method) then the SLP terminates the TLS handshake with the appropriate TLS alert message.

ii. If the Server does not send a Certificate.Request then the SET continues as per the ACA method. The SLP may continue using either the ACA method or SLP-only method.

In all cases, authentication failures are handled as they are described in [TLS] and in [RFC 4279].

Regarding the GBA-based method:

- A SET wishing to use the GBA-based method with 3GPP credentials SHALL use the method in Section 5.4 of [3GPP 33.222].
- A SET wishing to use the GBA-based method with 3GPP2 credentials SHALL use the method in Section 5.4 of [3GPP 33.222], with the references "[3GPP 24.109]" and "[3GPP 33.220]" replaced by [3GPP2 S.S0109].

6.1.3.3 Principles for authentication and key re-negotiation for the SEK-based Method (Informative)

The key re-negotiation can happen in two ways:

1. When the Location Rootkey (as defined in WiMAX Network Protocols and Architecture for Location Based Services) expires the SET automatically re-authenticates itself with the wimax network and the SUPL associated root keys will be re-generated by the SET, or
2. SLP notices that SEK or Location Rootkey (as defined in WiMAX Network Protocols and Architecture for Location Based Services) has expired and it will request a new key from the WiMAX AAA-server, or
3. The SLP sends a "psk_identity_unknown" TLS alert message during the TLS handshake. This indicates to the SET that the SET needs to re-authenticates itself with the wimax network and the SUPL associated root keys will be re-generated by the SET.

6.1.3.3.1 Authentication procedure

In WiMAX deployments, the PSK TLS [RFC 4279] handshake shall be used with SEK as follows:

- the ClientHello message shall contain one or more PSK-based ciphersuites;
- the ClientHello message shall contain the server_name TLS extension as specified in [RFC 3546] and it shall contain the hostname of the SLP;
- the ServerHello message shall contain a PSK-based ciphersuite selected by the SLP;
- the ServerKeyExchange shall be sent by the server and it shall contain the psk_identity_hint field and it shall contain the static string "SUPL WIMAX bootstrapping"
- the ClientKeyExchange shall contain the psk_identity field and it shall contain a prefix "SUPL WIMAX bootstrapping", a separator character ";" and the current B-TID as specified in section 6.1.2.1.2;
- the SET shall derive the TLS premaster secret from the SLP specific key material i.e. SEK as specified in [RFC 4279].

6.1.3.3.2 Authentication failures

Authentication failures are handled as they are described in [TLS] and in [RFC 4279].

6.1.3.3.3 Bootstrapping required indication

During TLS handshake, the SLP shall indicate to the SET that the SEK key is required by sending a ServerHello message containing a PSK-based ciphersuite, and a ServerKeyExchange message containing the psk_identity_hint field, which contains a static string "SUPL WIMAX bootstrapping". If the SET does not have a valid SEK this shall trigger the SET to derive a new SEK as defined in section 6.1.2.1.2.

6.1.3.3.4 Bootstrapping renegotiation indication

If the SEK expires, then the SLP applies the following methods to indicate expiry of SEK.

If the SET and SLP have a current TLS session in progress, then the SLP shall indicate to the SET that SEK has expired by sending close_notify alert message to the SET.

If the SET attempts to resume an old TLS session (for which SEK has expired) by sending a ClientHello message containing the old session ID. then the SLP shall refuse to use the old session ID by sending a ServerHello message with a new session ID. This will indicate to the SET that the SEK it used has expired.

During TLS handshake, the SLP shall indicate to the SET that the SEK has expired by sending handshake_failure message as a response to the finished message sent by the SET. This will indicate to the SET that the SEK it used has expired.

6.1.4 Alternative Client Authentication (ACA) Mechanisms

This section applies only to deployments supporting 3GPP and/or 3GPP2 SETs.

NOTE: Throughout this section, SET_ID refers to either the MSISDN (if the SET is on a 3GPP bearer network) or one of the MDN, MIN or IMSI (if the SET is on a 3GPP2 bearer network).

Section 6.1.3 outlines the circumstances under which the ACA-based method may be selected by the SLP. If the SLP selects the ACA-method during the TLS handshake, then an SET_ID/IP Address Mapping based client authentication SHALL be used by the SLPs to authenticate the SET. The rest of this section describes the details of this mechanism, known as the Alternative Client Authentication mechanism. If an SLP implements the Alternative Client Authentication mechanism, then the SLP is recommended to implement the method using PSK-TLS with GBA as well.

Section 6.1.1.3 describes which entities must support the ACA-based method, and the algorithms that must be supported by an entity that supports ACA-based method. For informative purposes, this information is repeated here:

- A bearer network may support the ACA-based method. A bearer network must support the ACA-based method if a SLP wishes to support the ACA-based method for the bearer network's subscribers.
- An SLP MAY support the ACA-based method.
- SET handsets supporting 3GPP and/or 3GPP2 MUST support the ACA-based method. This requirement is fulfilled naturally because the SET handset must support the SLP-only method, and there is no difference (from the SET perspective) between the ACA-method and SLP-only method.
- The ACA-based method does not involve the SET UICC/UIM/SIM/USIM.

SETs that support Alternative Client Authentication MUST also support TLS 1.1 with certificate-based server (SLP) authentication. In addition, the SET MUST be provisioned with a root certificate enabling it to verify SLP server certificates. As various different methods exist for provisioning of root certificates to SETs no particular mechanism is defined by this specification. SUPL operators need to ensure that when TLS 1.1 is used for Alternative Client Authentication the relevant root certificates exist in the SET.

SLPs that support Alternative Client Authentication MUST support TLS 1.1 and MUST have a valid TLS Server Certificate, which can be verified by the SETs that implement Alternative Client Authentication.

The Alternative Client Authentication (ACA) mechanism is a mechanism where the SLP can check the binding of the SET's IP address to the SET_ID assigned to the SET. If the ACA mechanism is implemented, then the SLP MUST be able to map the source IP address of a SUPL message received from the SET to the SET_ID used by the SLP to address the SET. In order for an SLP to use the ACA mechanism, the bearer network MUST prevent IP Address Spoofing at the bearer level. A successful mapping between the source IP address and the SET's SET_ID would imply that the SET is securely identified (i.e., authenticated) on the bearer network. This solution does not require any specific client (SET) authentication implementation on the SET but requires the SLP to support acquiring the correct source IP address for a particular SET_ID from the bearer.

3GPP-Bearer-Specific issues: The acquisition of the source IP address will not be possible in all cases – e.g. for GPRS roaming access using a GGSN in the visited rather than home network. Therefore, the alternative client authentication mechanism should only be relied on when the home network assigns the source IP address or has access to it – e.g. as applies for GPRS access when the SET is required to use a GGSN in the home network.

3GPP2-Bearer-Specific issues: The acquisition of the source IP address will not be possible in all cases – e.g. for roaming HRPD access using simple IP or MIP access within the visited network. Therefore, the alternative client authentication

mechanism should only be relied on when the home network assigns the source IP address or has access to it – e.g. as applies for HRPD access when the SET is required to use MIP to an HA in the home network.

Section 6.1.4.1 describes how this mechanism is used for client authentication in SUPL 3.0.

In the case that UDP/IP is used to transfer a SUPL INIT or SUPL REINIT message, SLP SHALL first verify the IP address by querying the bearer network for the SET IP address using the SET_ID or by querying the bearer network for the SET_ID using the IP address.

6.1.4.1 ACA Procedures

Network-Initiated Scenarios: If, after receiving a SUPL INIT or SUPL REINIT message from the SLP (and after applying the appropriate security mechanisms and notification/verification as described elsewhere in this document), the SET is authorized to continue with the corresponding SUPL sessions, then an existing, open mutually-authenticated TLS session SHOULD be used, or a previous resumable TLS session MAY be resumed as discussed in section 6.1.1.4. If there is no open TLS session, or the SET or SLP choose not to resume a session, then the SET and SLP require a fresh TLS session, and the SET and SLP perform the appropriate steps as described in section 6.1.3 for negotiating an authentication method.

The following steps are used by the SLP when the Alternative Client Authentication Mechanism is to be applied for authenticating the SET in a Network-initiated scenario:

1. Notes on SUPL INIT and SUPL REINIT

    a. Note that the SUPL INIT message was sent in response to an MLP request that supplied a SET_ID. The SLP assigns a SLP Session ID for the MLP request and sends a SUPL INIT. The SLP associates the response from the SET with the request from the MLP using the SLP Session ID.

    b. A SUPL REINIT message is sent within the scope of an existing GSS, and the SLP associates the response from the SET with that GSS using the SessionId provided by the SET.

    However, in both cases the SLP must first verify that the responding SET corresponds to the correct SET_ID. The remaining steps describe this authentication process.

2. The SET establishes a TLS 1.1 session with the SLP. The SET MUST check that the TLS server certificate presented by the SLP is bound to the FQDN of the SLP configured in the SET.

3. The SLP processes the first SUPL message from the SET.

    a. If the SessionID in the first SUPL message from the SET corresponds to the SessionId in a SUPL REINIT message from which the SLP is awaiting a response, then the SLP proceeds to Step 4. If the Session ID in the first SUPL message does not correspond to a valid GSS Session ID, then the SLP ends the SUPL Session with the appropriate message.

    b. The SLP determines if the SLP Session ID in the first SUPL message from the SET (in response to SUPL INIT) corresponds to a currently valid SLP Session ID assigned by the SLP. If the SLP Session ID in the first SUPL message does not correspond to a valid SLP Session ID, then the SLP ends the SUPL Session with the appropriate message. Otherwise, the SLP notes the corresponding SET ID.

4. Prior to responding to the first SUPL Message from the SET (SUPL POS INIT, SUPL START, SUPL TRIGGERED START, SUPL REPORT or SUPL END), the SLP MUST verify the SET_ID of the SET. There are two methods for achieving this.

    a. Requesting the SET_ID.

        i. The SLP queries the underlying bearer network to find out the current SET_ID using the source IP address used by the SET.

            1. If a valid SET_ID is returned from the bearer for the source IP address of the first SUPL message sent by the SET then the SLP checks that the returned Session-id is internally associated with the correct SET_ID (see Step 3). If this check fails, then the SLP ends the

SUPL session with the appropriate message. Otherwise, the SET is considered authentic, and the SLP continues with the SUPL session.

2. If a valid SET_ID cannot be found, then the SLP MUST terminate the SUPL session with the relevant SUPL error messages.

b. Requesting the IP address.

i. The SLP queries the underlying bearer network to find out the source IP address being used by the SET associated with this SET_ID (see Step 3).

1. If the bearer network returns an IP address, then the SLP checks that this IP address corresponds to the Source IP address of the first SUPL message. If this check fails, then the SLP ends the SUPL session with the appropriate SUPL message. Otherwise, the SET is considered authentic and the SLP continues with the SUPL session.

2. If an IP address cannot be found, then the SLP MUST terminate the SUPL session with the relevant SUPL error messages.

NOTE: A bearer network might support only one of the two types of query (requesting IP address or requesting SET_ID) in Step 4 for obtaining an SET_ID/IP address binding. The SLP is responsible for conforming to the method supported by the bearer network.

SET-Initiated Scenarios: When the SET wishes to initiate a SUPL session, an existing, open mutually-authenticated TLS session SHOULD be used, or a previous resumable TLS session MAY be resumed as discussed in section 6.1.1.4. If there is no open TLS session, or the SET or SLP chooses not to resume a session, then the SET and SLP require a fresh TLS session, and the SET and SLP perform the appropriate steps as described in section 6.1.3 for negotiating an authentication method.

The following steps are used by the SLP when the Alternative Client Authentication Mechanism is to be applied for authenticating the SET in a SET-initiated scenario.

1. The SET establishes a TLS 1.1 session with the SLP. The SET MUST check that the TLS server certificate presented by the SLP is bound to the FQDN of the SLP configured in the SET.

2. Prior to responding to the first SUPL Message (e.g. SUPL START, SUPL TRIGGERED START), the SLP MUST verify the SET_ID of the SET. There are two methods for achieving this.

a. Requesting the SET_ID.

i. The SLP queries the underlying bearer network to find out the current SET_ID using the source IP address used by the SET.

1. If a valid SET_ID is returned from the bearer for the source IP address of the first SUPL message sent by the SET then the SLP checks that the returned SET_ID is the same as the SET_ID provided by the SET. If this check fails, then the SLP ends the SUPL session with the appropriate message. Otherwise, the SET is considered authentic, and the SLP continues with the SUPL session.

2. If a valid SET_ID cannot be found the SLP MUST terminate the SUPL session with the relevant SUPL error messages.

b. Requesting the IP address.

i. The SLP queries the underlying bearer network to find out the source IP address being used by the SET associated with this SET_ID.

1. If the bearer network returns an IP address, then the SLP checks that this IP address corresponds to the Source IP address of the first SUPL message. If this check fails, then the SLP ends the SUPL session with the appropriate message. Otherwise, the SET is considered authentic and the SLP continues with the SUPL session.

2. If an IP address cannot be found the SLP MUST terminate the SUPL session with the relevant SUPL error messages.

NOTE: In both the SLP-Initiated and SET-Initiated scenarios, the SLP can re-authenticate the SET by sending an appropriate query to the bearer network to bind the SET_ID to the source IP address currently in use. There are various circumstances where this could be useful, for example: (A) if the IP address of the SET changes during a TLS session, then the SLP can send the appropriate query to the bearer network to ensure that the SET_ID is associated with the new IP address; (B) when resuming a TLS session, the SLP can re-use a previous TLS session as discussed in section 6.1.1.4, thereby saving computation, and simply send the appropriate query to the bearer network to authenticate the SET. Note that re-authenticating the SET in this manner does not involve interaction with the SET itself.

6.2 Authentication Mechanisms applicable to an E-SLP

6.2.1 Regarding Emergency-Services Regulatory Bodies

SUPL 3.0 emergency SUPL session may be either Network-Initiated (using SUPL) or SET Initiated. The appropriate emergency services regulatory bodies will dictate support for these emergency sessions:

- The appropriate emergency services regulatory bodies may not dictate support for either Network-Initiated or SET-Initiated sessions;
- The appropriate emergency services regulatory bodies may dictate only Network-Initiated sessions;
- The appropriate emergency services regulatory bodies may dictate only SET-Initiated sessions;
- The appropriate emergency services regulatory bodies may dictate support for both Network-Initiated and SET-Initiated sessions.

6.2.2 Prioritization of SUPL Resources during Emergency Sessions

For the duration of an emergency SUPL session on a SET, all SUPL resources on the SET MUST be made available for that emergency session. Consequently:

- When a SET begins an emergency SUPL session, any SUPL communication related to non-emergency sessions MUST be terminated immediately by the SET. If non-emergency SUPL INIT and/or SUPL REINIT messages are being processed by the SET at this time (e.g. having MAC verified or obtaining user permission), then those processes SHALL be aborted and the SUPL INIT and/or SUPL REINIT messages SHALL be discarded.
- If a SET receives non-emergency SUPL INIT and/or SUPL REINIT message(s) while in emergency SUPL session, these SUPL INIT and/or SUPL REINIT message(s) SHALL be discarded.

6.2.3 E-SLP FQDN

In Network-Initiated emergency SUPL sessions, the FQDN of the E-SLP shall be:

1. The FQDN provided to the SET as E-SLP address in the SUPL INIT. The E-SLP FQDN shall have format "e-slp.xxx.xxx.xxx.xxx.xxx" where "xxx" can be any valid string.
2. If FQDN is not provided in SUPL INIT, the provisioned H-SLP address shall be used.
3. If FQDN is not available as per 1 or 2 above, the FQDN shall be defaulted to one of the three alternatives below:
   - (if connected to a 3GPP bearer network) “e-slp.mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org” if no FQDN is explicitly provided. In this case, the MCC and MNC correspond to the serving 3GPP network as defined in [3GPP 23.167].
   - (if connected to a 3GPP2 bearer network) “e-slp.mnc<MNC>.mcc<MCC>.pub.3gpp2network.org” if no FQDN is explicitly provided. In this case, the MCC and MNC correspond to the serving 3GPP2 network as defined in [3GPP2 X.S0049-0].

- (if connected to a WiMAX bearer network) "e-slp.operator.com" where operator.com is the FQDN of the H-SLP operator.

In SET-Initiated emergency SUPL sessions, the FQDN of the E-SLP shall be in order of preference:

1. (If applicable) the FQDN dictated by the appropriate emergency services regulatory bodies.
2. An FQDN provided by the local access network or by other means that is verified by the H-SLP or by a Proxy E-SLP.
3. An FQDN provided by the H-SLP or a Proxy E-SLP.

6.2.4 Processing Emergency SUPL INIT messages

SET based integrity verification and message origin authentication of SUPL INIT messages is not used by an E-SLP. Thus, the MAC field in an emergency SUPL INIT MUST NOT be populated.

During an emergency call, a SET SHALL NOT apply end-to-end protection of emergency SUPL INIT messages.

Some protection is offered by the use of E-SLP whitelists. The E-SLP whitelist is based on the current position estimate of the SET (such as CellID and/or NetworkID). The E-SLP whitelist is used by a SET to determine the order in which the SET should process received emergency SUPL INIT messages: the E-SLP whitelist SHALL NOT be used for discarding emergency SUPL INIT messages.

6.2.4.1 E-SLP Whitelist

If an emergency SUPL INIT message is received over a channel that is not secured end-to-end (such as SMS or OMA Push or UDP/IP) then the emergency SUPL INIT message may be fake or altered. The remainder of this section describes the security countermeasures used to ensure that the SET is able to contact the genuine E-SLP server as soon as possible.

NOTE: Regulatory requirements will dictate the conditions under which the SET should accept and process emergency SUPL INIT messages. For example, in many cases, the regulatory requirements only require the SET to accept and process emergency SUPL INIT messages if the SET is currently engaged in an emergency call. Consequently, the conditions (under which the SET should accept and process emergency SUPL INIT messages) are outside the scope of this document.

When a SET receives an emergency SUPL INIT message, the SET MUST first verify that the conditions (under which the SET should accept emergency SUPL INIT messages) are currently satisfied. If the conditions are not satisfied, then the SET SHALL ignore the SUPL INIT message. The description from here on assumes that the conditions were satisfied when the SET received the emergency SUPL INIT message.

NOTE: Attackers could send multiple (fake) emergency messages to the SET at the same time that the SET is expecting a genuine emergency SUPL INIT message. There may be cases where the SET could not be told (in advance) from which Emergency SLP to expect the emergency SUPL INIT message. This attack is motivation for the following procedures.

For the period of time that the "accept and process" conditions are satisfied, the SET MUST NOT delete received emergency SUPL INIT messages even if the emergency SUPL INIT message lists an un-expected address for the E-SLP. Once the SET determines that the conditions are no longer satisfied (for example, once the correct E-SLP has been contacted, or sufficient time has passed after the emergency call) then the SET MUST silently discard any received emergency SUPL INIT messages.

If the SET receives, accepts and processes a fake emergency SUPL INIT message (while the “accept and process” conditions are still satisfied), then the SET might not receive an indication that emergency SUPL INIT message is fake until after attempting to contact the E-SLP indicated in the emergency SUPL INIT message. The indication occurs when the E-SLP rejects the SUPL session. This process is not immediate, so it may be necessary for the SET to queue emergency SUPL INIT messages if it receives more than one emergency SUPL INIT message.

An E-SLP whitelist contains a list of E-SLP FQDNs (see section 6.2.3) that the SET could expect to receive emergency SUPL INIT messages from. The SET uses the E-SLP whitelist to ensure that emergency SUPL INIT messages including an E-SLP FQDN that is on the whitelist SHOULD be processed before emergency SUPL INIT messages including an E-SLP FQDN that is not on the whitelist.

Example: Emergency SUPL INIT messages containing an E-SLP FQDN on the whitelist are pushed forward on the emergency SUPL INIT queue to ensure that the message is processed before emergency SUPL INIT messages containing an E-SLP FQDN that is not on the whitelist. E-SLP Whitelisting should be the first criteria for ordering the Emergency SUPL INIT queue. The second criterion is the arrival time, using the first-in first-out principle:

- If the SET has a current E-SLP whitelist for the SET's current locality, then the SET uses both criteria to order the queue.
- If the SET does not have a current E-SLP whitelist for the SET's current locality, then the SET uses the first-in-first-out principle to order the queue.

6.2.4.2 Obtaining an E-SLP whitelist

An E-SLP address that is provided or authorized by the H-SLP can be used by the SET as the E-SLP whitelist or as part of the E-SLP whitelist so long as the E-SLP address remains valid as defined by the H-SLP. Other than this, SUPL 3.0 does not define how the SET obtains and maintains an E-SLP whitelist. This is considered out of scope for SUPL.

6.2.4.3 Procedures regarding Emergency SUPL INIT Messages

If an emergency SUPL INIT is received over a channel that is secured end-to-end (such as a secure SIP Push) then the emergency SUPL INIT message SHALL be processed immediately. The remaining considerations of this subsection are ignored in this case.

If an emergency SUPL INIT message is received over a channel that is not secured end-to-end (such as SMS or OMA Push or UDP/IP), then the message is queued as in section 6.2.4.1. The SET works its way through the messages in the queue, applying the appropriate verification and notification before attempting to connect to the E-SLP to respond.

In responding to the SUPL INIT message, the SET shall establish a secure TLS session (see sections 6.2.5) with the associated E-SLP (see section 6.2.3), and one of the following takes place:

- If, after authenticating the SET (See section 6.2.5), the E-SLP cannot associate the SET with any outstanding SUPL sessions, then the E-SLP SHALL end the session. If the TLS Handshake is not yet complete, then the E-SLP SHOULD end the session using a TLS error message, in order to save un-necessary computation. If the TLS handshake is complete, then the E-SLP SHALL end the session using a SUPL error message indicating that the SET is not authorized. The SET SHALL interpret either form of error message as indication that the SUPL INIT message was fraudulent. The SET then processed to the next SUPL INIT message in order of priority in the queue.
- If, after authenticating the SET (See section 6.2.5), the E-SLP can associate the SET with an outstanding SUPL session, then the SET and E-SLP continue as normal.

The SET continues responding to emergency SUPL INIT messages until the genuine message is found. The SET MAY discard any new or queued SUPL INIT messages once the correct E-SLP has been identified. New or queued SUPL INIT messages from the correct E-SLP may still be processed.

The following two notes are suggestions that regulatory bodies may wish to consider.

NOTE: Once the correct E-SLP has been identified, then the SET should ensure that it remembers the FQDN of this correct E-SLP until the SUPL session successfully completes. If the TLS session with the E-SLP ends prematurely (for example, if there is a loss of data connectivity), the SET should continue attempting to re-establish a TLS session with the E-SLP until the TLS session is re-established so that the SUPL session can continue to successful completion. In some circumstances, it is conceivable that the SET re-establishes the TLS session several times. If the SET is not having success at reestablishing the TLS session, the SET should continue attempting regardless: since this is an emergency situation, the benefit of success outweighs the cost of a flat battery.

NOTE: If the E-SLP loses contact with SET after authentication, but prior to successful completion of the SUPL session, then the E-SLP SHOULD leave the SUPL session open with the hope that the SET is able to re-establish contact and complete the SUPL session.

6.2.5 Authentication for Emergency Sessions

NOTE: The mutual-authentication methods that may be supported by an E-SLP are specified in section 6.1.1.3. The SET and E-SLP negotiate the mutual-authentication method during the TLS handshake, as specified in section 6.1.3.

The order of preference for emergency sessions is

- GBA or SEK method: first preference
- DCert method: second preference
- ACA method: third preference
- SLP-only method: last preference. The SLP-only method should be seen as a last resort.

The FQDN of the E-SLP for all these cases is discussed in section 6.2.3.

GBA-Based Method (SETs supporting 3GPP/3GPP2): SETs and E-SLPs MAY perform PSK-TLS with GBA as described in section 6.1.3 with the E-SLP acting as the NAF. The Ks_NAF obtained by an E-SLP for a particular SET may be retained in association with the SET identity (e.g. IMSI, MSISDN) for the lifetime set by the home network operator.

SEK Based Method (SETs supporting WiMAX): SET and E-SLPs MAY perform mutual authentication using PSK-TLS with SEK as described in section 6.1.3 with the E-SLP acting in the similar fashion as H-SLP. The FQDN of the E-SLP is discussed in section 6.2.3. The SEK obtained by an E-SLP for a particular SET may be retained in association with the SET identity (e.g. WiMAX user ID) for the lifetime set by the home network operator.

DCert Method (All SETs): SET and E-SLPs MAY perform mutual authentication using the DCert method as described in section 6.1.2.2.1. The SET SHALL authenticate the E-SLP using a root certificate of the E-SLP contained in the SET and the FQDN of the E-SLP as defined in section 6.2.3.

ACA-Based Method (SETs supporting 3GPP/3GPP2 while on corresponding bearer networks): For SUPL 3.0 implementations where both GBA with PSK-TLS and the DCert method ARE NOT supported in the E-SLP, the alternative client authentication mechanism defined in section 6.1.4 SHALL be supported with the following differences. The E-SLP SHALL authenticate the SET by binding the IP address used by the SET with the IP address for the SET provided to the E-SLP by the serving network – e.g. by the LRF or E-CSCF in a 3GPP network [3GPP 23.167], or using [3GPP2 X.S0049-0] in a 3GPP2 network.

- **Notes on Network-Initiated Sessions:** Since the SET IP address is used to initiate any emergency VoIP call and can be verified by the serving network before SUPL is invoked, it may be considered to be reliable by the E-SLP. In the case of an emergency call initiated in circuit mode, the SET IP address may not be known to the serving network (e.g. may be assigned by the home network) in which case the E-SLP cannot be provided with the IP address by the serving network and the SET cannot verify the IP address when received later from the SET.

In order to use the ACA method, the serving bearer network MUST prevent IP Address Spoofing at the bearer level. It should be noted that the ACA method can be applied whether or not the SET is registered an authenticated on the bearer network. This supports cases where there is no activated SIM/USIM/UICC/(R)UIM present in the SET.

SLP-Only Method (All SETS): If no other authentication method can be used, then the SET MAY establish a secure IP connection to an E-SLP using the SLP-only method. The SET SHALL authenticate the E-SLP using a root certificate of the E-SLP contained in the SET and the FQDN of the E-SLP as defined in section 6.2.3. The ability to perform mutual authentication depends on where the session was SET initiated or Network-Initiated

- **Network Initiated Sessions**: If the SUPL Session is Network Initiated, then the E-SLP can weakly authenticate the SET based on (e.g.) the session ID and the received hash of the SUPL INIT as discussed in section 6.2.6.
- **SET Initiated Sessions**: If the SUPL Session is SET Initiated then the E-SLP cannot authenticate the SET.

It should be noted that the SLP-only method can be applied even whether or not the SET is registered an authenticated on the bearer network. This supports cases where there is no activated SIM/USIM/UICC/(R)UIM present in the SET.

6.2.6 Integrity Protection of SUPL INIT for Emergency SUPL Sessions

If the E-SLP is able to authenticate the SET as discussed in section 6.2.5, and the E-SLP can associate the SET with an outstanding SUPL sessions, then the E-SLP checks if the SUPL INIT message was altered. If the E-SLP detects that the SUPL INIT message was altered (for example, if SLP Session ID is wrong or if VER fails verification as described in section 6.3.1) then the E-SLP MUST send SUPL INIT to the SET over the TLS session to ensure that the SET is provided with the correct parameters. In response, the SET will discard the SUPL session initiated using the SUPL INIT it originally received, and the SET shall begin a new SUPL session using the SUPL INIT received over the TLS session. The SET shall then process that SUPL INIT message immediately (that is, the SET does not evaluate the priority using an E-SLP whitelist), performing the appropriate actions for notification and verification, and provided the User does not reject the session, the SET then sends the appropriate message (SUPL POS INIT or SUPL AUTH REQ) to the E-SLP to continue the session.

The ability to resend SUPL INIT is only intended for emergency sessions. In non-emergency sessions, if alteration of SUPL INIT is detected, then the SLP shall end the SUPL session using SUPL END, as specified in the non-emergency call flows.

6.3 Processing of the SUPL INIT and SUPL REINIT Messages

As network initiated SUPL sessions are triggered by a SUPL INIT and SUPL REINIT message, it is essential to protect SUPL INIT and SUPL REINIT messages against masquerading and (in some cases) against re-play attacks. Throughout this section, the processes applicable to both SUPL INIT and SUPL REINIT messages are indicated by referring to SUPL INIT/REINIT messages.

SUPL 3.0 specifies the following protection for SUPL INIT/REINIT messages:

- Network-based security, in which the SLP shall perform checks to ensure authentication (section 6.3.1) and replay protection (section 6.3.2) of SUPL INIT/REINIT messages. This verification occurs after the SET has processed the content of the SUPL INIT/REINIT message and established a secure TLS session with the SLP for the purposes of performing the SUPL session.

- End-to-End security, in which: the SLP may apply a combination of encryption, integrity protection and replay protection to the SUPL INIT/REINIT message; and the SET applies the corresponding combination of decryption, integrity verification and replay detection. The SET applies these security measures before processing the content of the SUPL INIT/REINIT message. This security is applied only to non-emergency SUPL INIT/REINIT messages.

Network-based security is mandatory, while End-to-End security is optional.

6.3.1 Network-Based Authentication of the SUPL INIT/REINIT Message

The SLP always performs network verification of the integrity of the SUPL INIT/REINIT message. The first message sent in response to the SUPL INIT/REINIT message (that is, a SUPL POS INIT, SUPL START, SUPL TRIGGERED START, SUPL REPORT or SUPL END message) MUST contain a verification field (VER). When the SLP receives the first message sent in response to the SUPL INIT/REINIT message the SLP MUST check the received VER field against the corresponding value calculated over the transmitted SUPL INIT/REINIT message. If this verification fails the SLP MUST terminate the session with the SUPL END message that contains status code ‘authSuplinitFailure’.

The value for the verification field MUST be calculated as follows:

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

Where SLP is the FQDN of the SLP address. SHA-256 MUST be used as the hash (H) function, with opad and ipad as specified in [HMAC]. The output of the SHA-256 HASH function MUST be truncated to 64 bits, i.e., the function MUST be implemented as HMAC-SHA256-64. Note that the SLP address is not considered secret. The HMAC construct used here does not provide any data authentication but is only used as an alternative to a HASH function.

6.3.2 Network-Based Re-Play protection of SUPL INIT/REINIT Message

For Network Initiated cases where SUPL INIT has been sent, protection against re-play attacks MUST be provided by the SLPs. SLPs MUST ensure that no SUPL messages are accepted from an authenticated SET unless a previous, non-expired

SUPL INIT message has been sent with an "SLP Session Id" that corresponds to the one received inside the SUPL message. SLPs MUST also ensure that the type of SUPL message (e.g. SUPL POS INIT, SUPL TRIGGERED START) agrees with the parameters sent in the SUPL INIT message. Implementations MUST ensure that an "SLP Session Id" is correctly associated with the SET User ID (e.g., MSISDN, WiMAX user ID or MDN) that has been authenticated.

For Network Initiated GSS where SUPL REINIT has been sent, protection against re-play attacks MUST be provided by the SLPs. SLPs MUST ensure that no SUPL POS INIT messages with SessionId for an existing GSS are accepted from an authenticated SET unless a previous, non-expired SUPL REINIT message has been sent with that GSS's SessionId. Implementations MUST ensure that the GSS SessionId is correctly associated with the SET User ID (e.g., MSISDN, WiMAX user ID or MDN) that has been authenticated.

If the SET User authentication is performed using the Alternative Client Authentication method described in this document then a mapping between the source IP address of the response from the SET (SUPL POS INIT, SUPL AUTH REQ or SUPL TRIGGERED START) and the MSISDN or MDN of the SET User is already established and this MSISDN or MDN MUST be used as the authenticated MSISDN or MDN.

Discarding of an erroneous SUPL POS INIT or SUPL TRIGGERED START MUST NOT generate a chargeable event for the SET.

6.3.3 End-to-End Protection of SUPL INIT/REINIT Messages

NOTE: End-to-End Protection of SUPL INIT Messages applies only to non-emergency SUPL INIT/REINIT messages.

The processes in Section 6.3.3 apply only to SLP that are D-SLP and H-SLP; the processes do not apply to E-SLP.

The procedures for End-to-End protection of SUPL INIT and SUPL REINIT messages make no distinction between SUPL INIT and SUPL REINIT messages – both SUPL INIT and SUPL REINIT messages are processed as though they were the same type of message. For simplicity, we refer to the procedures as SUPL INIT protection procedures - both SUPL INIT and SUPL REINIT messages are processed using the as SUPL INIT protection procedures.

Three options of end-to-end SUPL INIT protection are provided for in this specification: Null, Mode A and Mode B-

- Null SUPL INIT protection provides no end-to-end integrity protection, no end-to-end replay protection and no confidentiality protection. The procedures for Null SUPL INIT protection are described in section 6.3.4.
- Mode A SUPL INIT protection provides end-to-end integrity protection and end-to-end replay protection using default algorithms. Mode A SUPL INIT protection uses a shared key sent to the SET by the SLP during a secured ULP Session. The procedures for Mode A SUPL INIT protection are described in section 6.3.5.
- Mode B SUPL INIT protection provides end-to-end integrity protection and end-to-end replay protection using default algorithms. Mode B SUPL INIT protection uses a shared key derived using the appropriate PSK-based Method (GBA or SEK methods). The procedures for Mode B SUPL INIT protection are described in section 6.3.6.

The order of preference for the level of protection is as follows:

- Null SUPL INIT protection has least preference.
- Mode A SUPL INIT protection has higher preference than Null SUPL INIT protection.
- Mode B SUPL INIT protection has higher preference than Mode A SUPL INIT protection.

In a SUPL INIT message the Protection Level parameter (in the following table) is assigned according to the current level of protection.

NOTE: This specification has been written to allow for more advanced levels of protection to be added in the future revisions. This advanced protection could allow the negotiation of other ways for securing SUPL INIT/REINIT (for example, allowing encryption and allowing the negotiation of algorithms). The Protection Level parameter is included to aid the SET in determining whether it might be able to parse the SUPL INIT/REINIT message or not: the Protection Level parameter is required for extensibility.

A SUPL INIT/REINIT message may have a Protector parameter present for including security parameters: the presence of a Protector parameter is specified in the following table.

Level of End-to-End SUPL INIT Protection	Description	Protector parameter present in SUPL INIT/REINIT?
Null	No end-to-end protection	Optional
Mode A	Integrity protection and replay protection using default algorithms	Mandatory
Mode B	Integrity protection and replay protection using default algorithms	Mandatory

Table 5: SUPL INIT Protection Level parameter values and presence of the Protector parameter in SUPL INIT and SUPL REINIT messages.

A SET or D-SLP or H-SLP that supports the ACA-based method MUST support Null SUPL INIT protection.

All SETs SHOULD support Mode A SUPL INIT protection procedures.

A D-SLP or H-SLP MAY support Mode A SUPL INIT protection procedures.

A SET or D-SLP or H-SLP that supports the PSK-based method MUST support Mode B SUPL INIT protection procedures.

The E-SLP entity is not involved in currently defined SUPL INIT protection.

6.3.3.1 Negotiating the Level of SUPL INIT Protection

The following processes apply only to SLP that are D-SLP and H-SLP; the processes do not apply to E-SLP.

An informal description of how the SUPL INIT protection level is negotiated is as follows:

1. The SET must apply Null SUPL INIT protection when there is no valid SUPL_INIT_ROOT_KEY (e.g. at power-up or when the lifetime of the SUPL_INIT_ROOT_KEY has expired). The initial protection level is always Null SUPL INIT protection. In this state the SET handles all SUPL INIT/REINIT messages, i.e. no messages are silently dropped. If a SUPL INIT/REINIT message is parsed with a failure condition, the SET sends an error message to the SLP.
2. If the SET has a valid SUPL_INIT_ROOT_KEY and valid ReplayCounter already negotiated using Mode A or Mode B SUPL INIT protection for a particular SLP, then the SET processes all SUPL INIT/REINIT messages from that SLP using the negotiated mode (Mode A or Mode B).
3. When the SET establishes a mutually-authenticated secure connection to the SLP,
   a. If a PSK-based method (GBA or SEK) was used for mutual authentication, then Mode B SUPL INIT protection applies and the B-TID exchanged in the PSK-TLS handshake corresponds to the Ks (that will be used as a Ks_NAF in 3GPP and 3GPP2 deployments) or SEK that can be used to derive SUPL_INIT_ROOT_KEY that will be used as a Ks_NAF in 3GPP and 3GPP2 deployments. This Ks_NAF or SEK and the associated B-TID are used in the Mode B SUPL INIT protection until either:
      i. the key expires, in which case the SET and SLP revert to Null SUPL INIT protection
      ii. the SET and SLP use the ACA-method in a non-emergency session, in which case the SET and SLP revert to either Mode A or Null SUPL INIT protection as discussed in step 3b below, or
      iii. the SET and H-SLP use GBA's or SEK's bootstrapping re-negotiation methods to establish TLS using a fresh B-TID, in which case the B-TID and corresponding Ks_NAF or SEK are now used for Mode B SUPL INIT protection.
   b. Otherwise, the SET and SLP established a secure connection using the DCert or ACA method.

i. If the SET does not have a valid SUPL_INIT_ROOT_KEY, it indicates this to the SLP in its SET Capabilities (sUPLINITRootKeyStatus=" invalidSUPLINITRootKey") in the next ULP message carrying the SET Capabilities parameter following the secure session establishment.

1. If the SLP supports Mode A SUPL INIT protection, then the SLP performs the Mode A SUPL_INIT_ROOT_KEY Establishment procedure (Section 6.3.5.2) in the next SUPL END message. A successful Mode A SUPL_INIT_ROOT_KEY Establishment procedure indicates to the SET that Mode A SUPL INIT Protection applies. Until a successful Mode A SUPL_INIT_ROOT_KEY Establishment procedure occurs, the SET SHALL use Null SUPL INIT Protection.

NOTE: The policy for updating SUPL_INIT_ROOT_KEY is a decision of the SLP Operator.

2. If the SLP does not support Mode A SUPL INIT protection (or does not support Mode A SUPL INIT protection at this particular time), then the SLP does not send ModeAKeyIdentifier, TemporaryModeAKeyIdentifier, SUPL_INIT_ROOT_KEY and ModeAKeyLifetime parameters which indicates that the SET SHALL use Null SUPL INIT Protection.

ii. If the SET has a valid SUPL_INIT_ROOT_KEY, but does not have a valid TemporaryModeAKeyIdentifier or has lost synchronization regarding replay protection, it indicates this to the SLP in its SET Capabilities (sUPLINITRootKeyStatus=" outofsyncSUPLINITRootKey") in the next ULP message carrying the SET Capabilities parameter following the secure session establishment.

1. If the SLP support Mode A SUPL INIT protection, then the SLP performs the Mode A Resynchronization procedure (Section 6.3.5.5) in the next SUPL END message. A successful Mode A Resynchronization procedure indicates to the SET that Mode A SUPL INIT Protection applies. Until a successful Mode A Resynchronization procedure occurs, the SET SHALL use Null SUPL INIT Protection.

2. If the SLP does not support Mode A SUPL INIT protection (or does not wish to support Mode A SUPL INIT protection at this particular time), then the SLP does not perform Mode A Resynchronization (Section 6.3.5.5) which indicates that the SET SHALL use Null SUPL INIT Protection.

Note that this means that the protection level is renegotiated every time the SET sets up a fresh TLS connection to the SLP.

6.3.3.2 Negotiation from the SLP Perspective

If the most recent IP session with the SET was authenticated using the GBA or SEK method, and the SLP has a current B-TID and the associated key for the SET, then

- If the B-TID is for a key obtained using GBA, then the SLP assigns SUPL_INIT_ROOT_KEY to be the Ks_(int/ext_)NAF corresponding to the most recent B-TID and generated as follows
  - The FQDN SHALL be the SLP_FQDN
  - The GBA Ua security protocol identifier that shall be used for SUPL_INIT protection is defined in OMNA Registry [OMNA].
- If the B-TID is for a key derived using the SEK-method, then the SUPL_INIT_ROOT_KEY is the SEK as defined in 6.1.2.1.2.
- Assuming no other SUPL INIT protection has been negotiated, then the SLP assigns the Mode B SUPL INIT protection level for that SET.

Otherwise, if the SLP has a valid ModeAKeyIdentifier and associated key for the SET, then the SLP assigns Mode A SUPL INIT protection level for that SET.

If no other level of protection is assigned, then the SLP assigns Null SUPL INIT protection level for that SET.

The SLP applies the procedures (for processing SUPL INIT/REINIT messages prior to delivery) corresponding to the currently assigned level of SUPL INIT/REINIT protection. This includes assigning the appropriate value for the Protection Level parameter in SUPL INIT messages.

6.3.3.3 Negotiation from the SET Perspective

If the most recent IP session with the SLP was authenticated using the GBA or SEK method, and the SET has the current B-TID and associated key used for that IP session, then

- If the B-TID is for a key obtained using GBA, then the SET assigns SUPL_INIT_ROOT_KEY to be the Ks_(int/ext_)NAF corresponding to the most recent B-TID and generated as follows
    - The FQDN SHALL be the SLP_FQDN
    - The GBA Ua security protocol identifier [3GPP 24.109] that shall be used for SUPL_INIT protection is defined in OMNA Registry [OMNA].
- If the B-TID is for a key derived using the SEK-method, then the SUPL_INIT_ROOT_KEY is the SEK as defined in 6.1.2.1.2.
- Assuming no other SUPL INIT protection has been negotiated, then the SET assigns the Mode B SUPL INIT protection level.

Otherwise, if the SET has a valid ModeAKeyIdentifier, TemporaryModeAKeyIdentifier and associated SUPL_INIT_ROOT_KEY for the SLP, then the SET assigns Mode A SUPL INIT protection level for that SLP.

If no other level of protection is assigned, then the SET assigns Null SUPL INIT protection level.

The SET applies the procedures (for processing received SUPL INIT/REINIT messages) corresponding to the currently assigned level of SUPL INIT protection.

6.3.3.4 Exception procedures

If the SET determines that the SET-internal SUPL INIT protection parameters have become corrupted, then the SET must establish a TLS session with the SLP:

- If GBA authentication is used, then the SET must initiate GBA bootstrapping to establish fresh keys;
- For SETs using the SEK method, the SET must initiate SEK bootstrapping to enable fresh keys, as defined in 6.1.2.1.2.
- Otherwise, the SET follows the procedures in Step 3.b of section 6.3.3.1.

If the SLP loses security context (for example, massive loss of data) then the SLP will have no means of initiating positioning activities. The context would be re-established when the Ks_NAF or SEK expires, or the SET connects to the SLP. To prevent this “block out window” the SLP should ensure that all SUPL INIT protection security context information is stored with sufficient redundancy to recover from such a scenario.

6.3.3.5 General Procedure for Processing a SUPL INIT Message at SET

The following procedure is applied by the SET to determine how to process a received SUPL INIT message.

1. The SET identifies the Sending SLP (the SLP that sent the SUPL INIT message).
    a. If a D-SLP FQDN parameter is present in the SUPL INIT message, then the SET SHALL identify the Sending SLP using this parameter.
        i. If the SET has no existing relationship with identified D-SLP, then the SET silently SHALL discard the SUPL INIT message and exits the current procedure.
        ii. Otherwise, the SET proceeds to step 2.

b. If no D-SLP FQDN parameter is present in the SUPL INIT message, then the SET identifies the Sending SLP to be the SET's H-SLP.

2. The SET performs initial filtering based on the SUPL INIT Protection level assigned for the Sending SLP:
   a. If Null SUPL INIT Protection is assigned for the Sending SLP, then the SET performs the Null SUPL INIT Protection procedures, and exits the current procedure.
   b. If Mode A or Mode B SUPL INIT Protection is assigned for the Sending SLP, then
      i. If the SUPL INIT message contains no Protector Parameter, then the SET silently discards the SUPL INIT message and exits the current procedure.
      ii. If the SUPL INIT message contains a Protector Parameter, the SET performs the appropriate Mode A or Mode B SUPL INIT Protection procedures in Section 6.3.5 or Section 6.3.6 respectively. The SET uses the KeyIdentifier parameter in the Protector Parameter to identify which of the SUPL INIT ROOT Keys associated with the Sending SLP is to be used for processing the SUPL INIT message.

6.3.4 Specifications when Null Level of Protection is assigned

NOTE: As noted in Table 5: SUPL INIT Protection Level parameter values and presence of the Protector parameter in SUPL INIT and SUPL REINIT messages., there is no SUPL INIT Protector for Null SUPL INIT protection.

6.3.4.1 SLP Procedures

There are no security procedures for the SLP that are specific to Null SUPL INIT protection.

6.3.4.2 SET Procedures

When Null SUPL INIT protection is assigned and the SET receives a SUPL INIT/REINIT message, then the SET applies the following procedure:

- If the Protection Level parameter is correct, then the SET considers the message to be authentic, and no security related processing is required.
  - Suppose the SLP and SET can support a higher level of protection, but the SET has not yet been in contact with the SLP since being powered up: in this case the SET will have Null SUPL INIT protection assigned. In the period of time until the SET contacts the SLP, the SET will consider any received SUPL INIT/REINIT message (with the correct Protection Level parameter) to be authentic. When the SET first contacts the SLP (which may or may not be in response to a received SUPL INIT/REINIT message), the SET and SLP will transition to a higher level of protection. Once the two entities transition to the higher level of protection, the SET can detect non-authentic SUPL INIT/REINIT messages. In between when the SET is powered up and when the SET first contacts the SLP, there is a period of time when the SET could receive an non-authentic SUPL INIT/REINIT message that is processed by the SET as if the SUPL INIT/REINIT message where authentic. If the SET decides to proceed with the SUPL session associated with the non-authentication SUPL INIT/REINIT message, then the SET will contact the SLP and establish a secure TLS session. The SLP will not allow the SUPL session since it was established using a non-authentic SUPL INIT/REINIT message. If the SET and SLP support a higher level of protection, then this will be established at the same time and the SET will be able to detect non-authentic SUPL INIT /REINIT messages after this time. This means that, if the SET and SLP can support a higher level of protection, then there is a very small window of opportunity for the attacker to get the SET to accept a non-authentic SUPL INIT/REINIT message, and the SET will only attempt to proceed with a SUPL session for at most one non-authentic SUPL INIT/REINIT message.
- If the Protection Level parameter is incorrect (that is, if the Protection Level parameter was anything other than Null), then the SET sends the appropriate error message to the SLP.
  - In the event that the Protection Levels at the SLP and SET lose synchronization, this procedure allows the SET and SLP to resynchronize on a common Protection Level.

6.3.5 Specifications for Mode A SUPL INIT Protection Level

6.3.5.1 Key Identifiers for Mode A SUPL INIT Protection

Mode A SUPL INIT Protection uses two Key Identifiers that may be sent with SUPL INIT/REINIT messages: ModeAKeyIdentifier and TemporaryModeAKeyIdentifier.

- The ModeAKeyIdentifier is a globally-unique, long-term Key Identifier associated with the SUPL_INIT_ROOT_KEY. The SLP provides a new ModeAKeyIdentifer to the SET only when the SLP provisions a new value for SUPL_INIT_ROOT_KEY.
- The TemporaryModeAKeyIdentifier is a short-term identity (pseudonym) associated with the ModeAKeyIdentifier. The TemporaryModeAKeyIdentifier shall be globally unique in the period that the TemporaryModeAKeyIdentifier is valid. The SET and SLP synchronize the value of TemporaryModeAKeyIdentifier as described in Sections 6.3.5.5 and 6.3.5.6.

The SLP will typically use TemporaryModeAKeyIdentifier as the KeyIdentifier in the Basic SUPL INIT Protector. The SET then uses TemporaryModeAKeyIdentifier to determine which SUPL_INIT_ROOT_KEY should be used to verify the Basic SUPL INIT Protector.

The ModeAKeyIdentifier is not typically sent in a SUPL INIT/REINIT message because this would allow an observer to associate multiple SUPL INIT/REINIT messages are associated with a common SET User. The purpose of TemporaryModeAKeyIdentifier to prevent a Threat Agent from using the ModeAKeyIdentifier to associate multiple SUPL INIT/REINIT messages with a SET User. Only the SLP and SET should be able to associate the TemporaryModeAKeyIdentifier with the ModeAKeyIdentifier. The frequency of changing TemporaryModeAKeyIdentifier is primarily a decision of the SET User. An SLP may choose to establish a new value for TemporaryModeAKeyIdentifier based on SLP policy.

However, there are circumstances in which the SLP may wish to use the longer-term ModeAKeyIdentifier as the KeyIdentifier in the Basic SUPL INIT Protector. For example, suppose a SET has not been responding to multiple SUPL INIT/REINIT messages using TemporaryModeAKeyIdentifier in the Basic SUPL INIT Protector. The SLP may be concerned that the SET has lost synchronization regarding TemporaryModeAKeyIdentifier. The SET and SLP are more likely to remain synchronized on the long-term ModeAKeyIdentifier. Hence, the SLP can send a SUPL INIT/REINIT message using ModeAKeyIdentifier in the Basic SUPL INIT Protector to ensure that lack of synchronization does not prevent the SET from verifying the SUPL INIT/REINIT message.

6.3.5.2 Mode A SUPL_INIT_ROOT_KEY Establishment Procedure

A value for the SUPL_INIT_ROOT_KEY is established by the SLP sending (in a SUPL END message to the SET in a secure SUPL session) a new ModeAKeyIdentifier, TemporaryModeAKeyIdentifier, SUPL_INIT_ROOT_KEY and ModeAKeyLifetime parameters. If delivery is successful, then the SLP and SET considers this Mode A SUPL_INIT_ROOT_KEY Establishment Procedure to be a success.

The ModeAKeyLifetime parameter contains the UTC time when the key ceases being valid.

6.3.5.3 Mode A Resynchronization Procedure

A SLP establishes a new value for the TemporaryModeAKeyIdentifier with the SET using the following steps:

1. The SLP sends to the SET (in a SUPL END message to the SET in a secure SUPL session) the current ModeAKeyIdentifier and a new TemporaryModeAKeyIdentifier parameter. If delivery is successful, then the SLP considers this Mode A Resynchronization Procedure to be a success.
2. The SET compares the received ModeAKeyIdentifier against the ModeAKeyIdentifiers of the valid SUPL_INIT_ROOT_KEY values that the SET currently has assigned for that SLP.
    a. If the ModeAkeyIdentifier values differ, then this indicates corruption of the value of ModeAKeyIdentifier assigned on the SET, and the following steps are performed:
        i. The SET discards the TemporaryModeAKeyIdentifier and considers this Mode A Resynchronization to be a failure.

ii. The SET initiates the Exception Procedures in Section 6.3.3.4.

b. If the received ModeAkeyIdentifier is equal to a valid ModeAKeyIdentifier, then:

i. The SET associates the new TemporaryModeAKeyIdentifier with the corresponding ModeAKeyIdentifier,

ii. The SET considers this Mode A Resynchronization Procedure to be a success.

6.3.5.4 Mode A SUPL INIT Protection and the Basic SUPL INIT Protector

Mode A SUPL INIT Protection uses the Basic SUPL INIT Protector and associated procedures as defined in section 6.3.7 with the following additional clarifications:

- KeyIdentifierType: indicates either ModeAKeyIdentifier or a TemporaryModeAKeyIdentifier is used.
- KeyIdentifier: corresponds to either a ModeAKeyIdentifier or a TemporaryModeAKeyIdentifier as appropriate to the ModeAKeyIdentifierType.
- BasicMAC is computed using SUPL_INIT_Basic_IK = HMAC-SHA256-128(SUPL_INIT_ROOT_KEY, “Mode A IK”), using SUPL_INIT_ROOT_KEY associated with the KeyIdentifier above.

6.3.5.5 SLP Procedures

The only Mode-A-specific SLP procedures relate to SUPL INIT ROOT KEY Establishment, expiry of a SUPL_INIT_ROOT_KEY, and maintaining synchronization between the SET and SLP.

The Mode A SUPL_INIT_ROOT_KEY Establishment Procedure is specified in Section 6.3.5.2. An SLP may perform the Mode A SUPL_INIT_ROOT_KEY Establishment Procedure in response to an out of sync indication by the SET (in SET Capabilities (sUPLINITRootKeyStatus=” invalidSUPLINITRootKey”)) or an (out of scope) internal decision of the SLP. That is, the SLP can send a SUPL_INIT_ROOT_KEY (with associated parameters) even when there is no corresponding indication by the SET.

A SUPL_INIT_ROOT_KEY and associated parameters SHALL cease being valid in the SLP after the earlier of

- The lifetime of the associated ModeAKeyIdentifier, and
- The time of a later successful Mode A SUPL_INIT_ROOT_KEY Establishment (Section 6.3.5.2).

The Mode A Resynchronization Procedure is specified in Section 6.3.5.3.An SLP may perform the Mode A Resynchronization Procedure in response to an out of sync indication by the SET (in SET Capabilities (sUPLINITRootKeyStatus=” outofsyncSUPLINITRootKey”)) or an (out of scope) internal decision of the SLP. That is, the SLP can send a TemporaryModeAKeyIdentifier even when there is no corresponding indication by the SET.

Following a successful Mode A SUPL_INIT_ROOT_KEY Establishment Procedure or successful Mode A Resynchronization Procedure, the SLP resets BasicLastReplayCounter to 0x0000.

6.3.5.6 SET Procedures

The only Mode-A-specific SET procedures relate to SUPL INIT ROOT_KEY Establishment, expiry of a SUPL_INIT_ROOT_KEY, and maintaining synchronization between the SET and SLP.

The Mode A SUPL_INIT_ROOT_KEY Establishment Procedure is specified in Section 6.3.5.2. A SET may attempt to trigger a Mode A SUPL_INIT_ROOT_KEY Establishment Procedure by indicating that it does not have a valid SUPL_INIT_ROOT_KEY in the SET (in SET Capabilities (sUPLINITRootKeyStatus=” invalidSUPLINITRootKey”)) in a ULP message carrying the SET Capabilities parameter following a secure session establishment.

An established SUPL_INIT_ROOT_KEY and associated parameters SHALL be considered invalid in the SET after the earlier of the following times.

- The lifetime of the associated ModeAKeyIdentifier.

- Five minutes after the time of a later successful Mode A SUPL_INIT_ROOT_KEY Establishment (Section 6.3.5.2). This time delay allows for delivery of any SUPL INIT messages sent prior to the latest Mode A SUPL_INIT_ROOT_KEY Establishment procedure as such SUPL INIT message would have be protected using the former SUPL_INIT_ROOT_KEY.
- Any time that the SET detects corruption of the values of SUPL_INIT_ROOT_KEY, ModeAKeyIdentifier and ModeAKeyLifetime. If corruption occurs, then the SET shall initiate Exception procedures in Section 6.3.3.4.

Mode A Resynchronization Procedure is specified in Section 6.3.5.3. A SET may attempt to trigger a Mode A Resynchronization Procedure by indicating loss of synchronization in the SET (in SET Capabilities (sUPLINITRootKeyStatus=" outofsyncSUPLINITRootKey")) in a ULP message carrying the SET Capabilities parameter following a secure session establishment.

Upon receipt of the first SUPL INIT messages including the TemporaryModeAKeyIdentifier established in a successful Mode A SUPL_INIT_ROOT_KEY Establishment Procedure or successful Mode A Resynchronization Procedure, the SET clears its cache of used values for BasicReplayCounter (since the SLP will have also reset BasicLastReplayCounter to 0x0000).

6.3.6 Specifications for Mode B SUPL INIT Protection Level

Mode B SUPL INIT Protection uses the Basic SUPL INIT Protector and associated procedures as defined in section 6.3.7, with the following additional clarifications:

- KeyIdentifierType: Only B-TID identifiers are support for Mode B SUPL INIT Protection.
- KeyIdentifier: corresponds to the current B-TID.
- The BasicMAC parameter is computed using SUPL_INIT_Basic_IK = HMAC-SHA256-128(SUPL_INIT_ROOT_KEY, "Mode A IK"), where
    - For GBA-based deployments the SUPL_INIT_ROOT_KEY is the Ks_(int/ext_)NAF corresponding to the most recent B-TID and generated using the GBA Ua security protocol identifier for SUPL INIT protection as defined in OMNA Registry [OMNA],
    - For SEK-based deployments the SUPL_INIT_ROOT_KEY is the SEK_MAC as defined in section 6.1.2.1.2.

6.3.6.1 SLP Procedures

The only Mode-B-specific SLP procedures relate to maintaining synchronization between the SET and SLP.

For Mode B SUPL INIT protection, the BasicReplayCounter in the SLP is reset to zero the first time a key is used and the SET removes all information about "played" SUPL INIT/REINIT messages.

In the unlikely event that the SLP determines that resynchronization is required:

- In the case of deployments supporting the GBA method, the SLP triggers resynchronization by invalidating the GBA B-TID. When that SET next attempts to authenticate to the SLP, then SLP will respond with TLS-PSK alert "psk_identity_unknown". This prompts establishing a new GBA key according to [3GPP 33.220].
- In the case of deployments supporting the SEK method, the SLP triggers resynchronization by invalidating the SEK B-TID. When that SET next attempts to authenticate to the SLP, then SLP will respond with TLS-PSK alert "psk_identity_unknown". This prompts establishing a new SEK as described in section 6.1.3.3

6.3.6.2 SET Procedures

The only Mode-B-specific SET procedures relate to maintaining synchronization between the SET and SLP.

If Mode B SUPL INIT protection is assigned by the SET, then

- Prior to the first time that the SET processes one of a SUPL INIT or SUPL REINIT message with a given SUPL_INIT_ROOT_KEY, the SET clears its cache of used values for BasicReplayCounter.
- The SET can trigger resynchronization by establishing new GBA Ks or new SEK as appropriate. The SLP will continue to use the old GBA Ks (or SEK) until the next successful authentication between the SET and SLP, so the SET should maintain the old GBA Ks (or SEK) until that time.

6.3.7 Specifications for Using the Basic SUPL INIT Protector

A Basic SUPL INIT Protector is used for both Mode A and Mode B SUPL INIT Protection includes the following parameters:

- KeyIdentifierType
- KeyIdentifier: length = 8 octets.
- BasicReplayCounter: length = 2 octets.
- BasicMAC: length = 4 octets.

The BasicMAC parameter is generated as follows:

- BasicMAC = HMAC-SHA256-32(SUPL_INIT_Basic_IK, SUPL_INIT/REINIT'), where
- SUPL_INIT_Basic_IK is derived according to sections 6.3.5 and 6.3.6 for Mode A and Mode B SUPL INIT protection respectively.
- SUPL_INIT/REINIT' corresponding to the SUPL INIT/REINIT message with all parameters except BasicMAC assigned, and with the MAC parameter set to all zeroes, and
- HMAC-SHA256-32 and HMAC-SHA256-128 are specified in [HMAC].

6.3.7.1 SLP Procedures

If Mode A or Mode B SUPL INIT protection is assigned to a SET, then the H-SLP composes the SUPL INIT/REINIT messages as follows:

1. Parameters outside the SUPL INIT Protector are assigned as described elsewhere.
2. KeyIdentifierType is set according to the type of KeyIdentity that the SLP will use for this message.
3. KeyIdentifier is set to a KeyIdentifier associated with the SUPL_INIT_ROOT_KEY.
4. SLP increases the current value of BasicLastReplayCounterValue (associated with this SET and the negotiated SUPL INIT protection Level) by 1, and inserts the new value into the BasicReplayCounter parameter. Note that SUPL INIT and SUPL RE INIT messages use a common BasicLastReplayCounterValue.
5. Finally, after all other parameters are assigned the BasicMAC is calculated from SUPL INIT and SUPL_INIT_ROOT_KEY as specified above.

The SLP is required to store a BasicLastReplayCounterValue of length equal to the length of BasicReplayCounter parameter for each SET for which Mode A or Mode B SUPL INIT protection level is assigned.

If BasicLastReplayCounterValue in the SLP is close to $65535 = 2^{16}-1$ (which is highly unlikely), then the SLP must trigger resynchronization procedures (see sections 6.3.6.1 and 6.3.7.1).

6.3.7.2 SET Procedures

If Mode A or Mode B SUPL INIT protection is assigned, then the SET processes a received SUPL INIT/REINIT message as follows:

1. The SET discards the SUPL INIT/REINIT message if the following parameters fail the appropriate verification:

- Protection Level: must be the assigned value for the negotiated SUPL INIT protection level in Table 5.
- KeyIdentifierType: Must be valid for the assigned SUPL INIT protection level
- KeyIdentifier: Must correspond to the current SUPL_INIT_ROOT_KEY for the negotiated SUPL INIT protection level.
- BasicReplayCounter: the SET uses this value to detect replay of messages. The technique may be implementation specific but must be robust enough to deal with situations where SUPL INIT/REINIT messages are lost or delivered out of order. Note that SUPL INIT and SUPL RE INIT messages use a common BasicReplayCounter.
- BasicMAC: The SET computes an expected BasicMAC from the SUPL INIT/REINIT message and the SUPL_INIT_ROOT_KEY (as described above) and compares this to the received BasicMAC: the values must be equal.
- (Only for SUPL REINIT messages): The SessionId must corresponds to an existing, non-expired GSS.

2. If the SUPL INIT/REINIT message was not discarded in the previous step, then it is considered authentic, and the SET considers the BasicReplayCounterValue to be used. If BasicReplayCounterValue is close to 65535 = 2^{16}-1 (which is highly unlikely), then the SET must establish a new SUPL_INIT_ROOT_KEY with the SLP to reset the counter.

6.4 Providing the H-SLP Address to the SET

The H-SLP address is made available to the SET by the provisioning of the H-SLP address in the UICC, SET or a default H-SLP address is derived as described below. This address MUST be in the form of a FQDN.

The address of an Access-Network dependent H-SLP SHOULD be securely provisioned by the Home Network of the SET. If a SET supports multiple access network technologies (3GPP2, 3GPP, WiMAX or alternative access networks) then an Access-Network dependent H-SLP may apply any of the corresponding mechanisms for provisioning the H-SLP Address.

The mechanisms for provisioning the address of an Access-Network independent H-SLP are outside the scope of this specification.

6.4.1 SETs Supporting 3GPP2

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

6.4.2 SETs Supporting 3GPP

A SETs supporting 3GPP 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 USIM/SIM. If there is no H-SLP address provisioned in the USIM/SIM 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. When a SET uses an H-SLP address provisioned by OMA DM then the SET MUST use the GBA-based authentication method described in section 6.1.2.1.1.

Auto configuration of the H-SLP address: If the H-SLP address cannot be found in the secure storage area of the UICC (USIM/SIM), or in a secure area on the SET, the SET MUST configure the default H-SLP address in the SET based on the IMSI stored in the USIM/SIM.

In the case an H-SLP address has been found in the secure storage area of the UICC (USIM/SIM), or in a secure area on the SET, but its use has resulted in an authentication failure while initiating the SUPL session, the SET MUST configure the default H-SLP address in the SET based on the IMSI stored in the USIM/SIM.

The mechanism to configure a default H-SLP address is defined below.

Please note that the following example has been taken from 3GPP GBA specifications [3GPP 33.220] and adopted for the SUPL use case where an H-SLP address (based on a FQDN) is configured. Implementation of this default configuration mechanism does not require the implementation of the 3GPP GBA specification. The example below is given to illustrate the methodology and can be implemented independent of [3GPP 33.220].

Configuration of H-SLP based on IMSI:

Step 1) Take the first 5 or 6 digits of the IMSI, depending on whether a 2 or 3 digit MNC is used [3GPP 31.102] and separate them into MCC and MNC; if the MNC is 2 digits then a zero SHALL be added at the beginning;

Step 2) Use the MCC and MNC derived in step 1 to create the “mnc<MNC>.mcc<MCC>.pub.3gppnetwork.org” domain name;
add the label “h-slp.” to the beginning of the domain name.

Example 1: If IMSI in use is “234150999999999”, where MCC=234, MNC=15, and MSIN=0999999999, the H-SLP address would be “h-slp.mnc015.mcc234.pub.3gppnetwork.org”.

If a new IMSI is detected by the SET during, or after power on, all previous H-SLP settings MUST be removed from the SET. More specifically, any H-SLP address stored in the SET MUST be removed.

In cases where the IMSI is changed the SET MUST first read the H-SLP address from the UICC (USIM/SIM). If no H-SLP address is stored on the UICC (USIM/SIM) the SET MAY check if the H-SLP address is stored in the SET. If no H-SLP address is found in the UICC or SET, then a default H-SLP address MUST be configured by the SET based on the new IMSI as described above.

Implementations MUST ensure that the address of the H-SLP cannot be changed via applications that are downloaded to the SET after the manufacturer software installation of the SET.

Figure 44 illustrates the flow diagram for the H-SLP address storage.

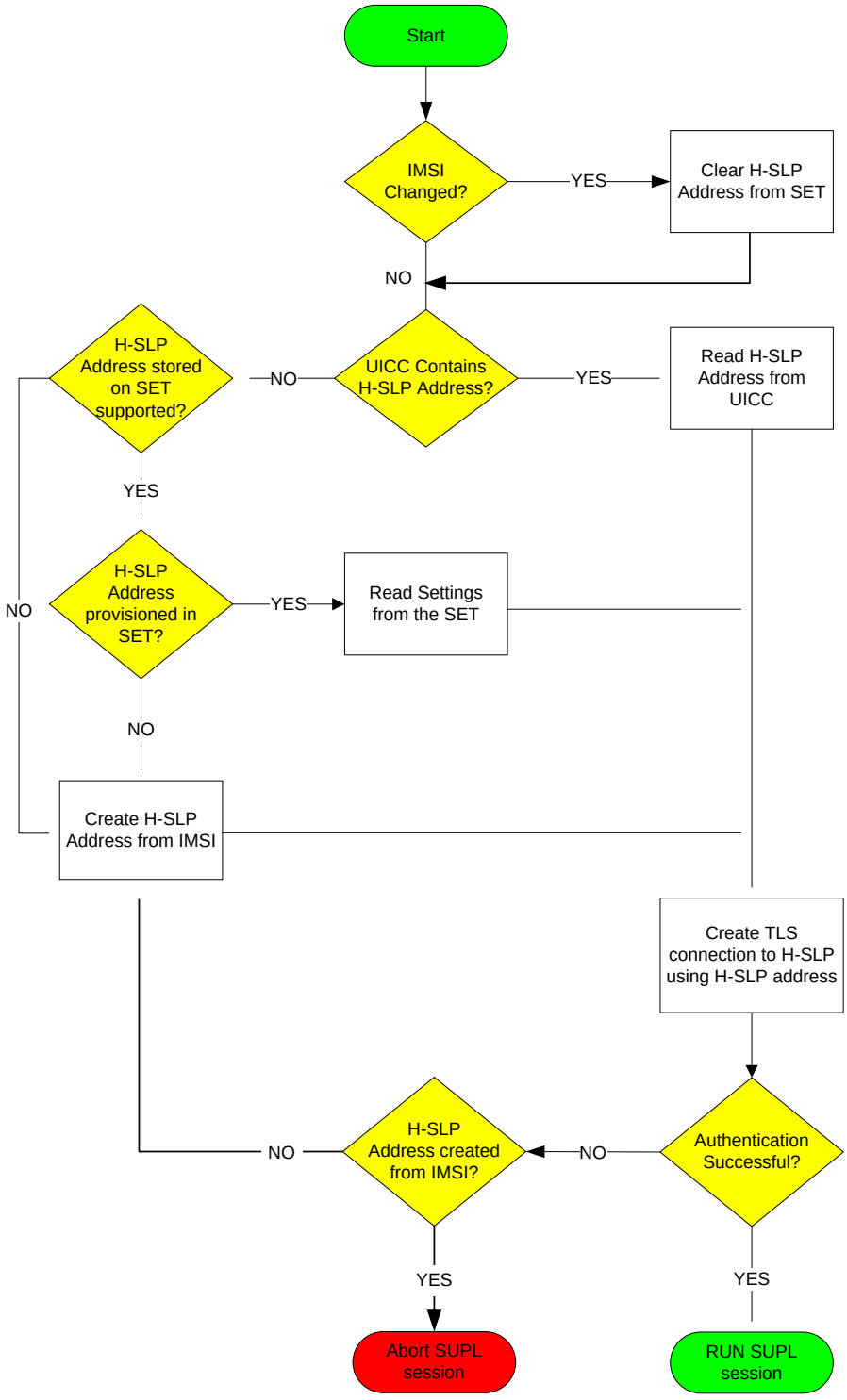

Figure 44: H-SLP address storage flow diagram for SETs supporting 3GPP

6.4.3 WIMAX based deployments

When the SET attaches to the WiMAX network it MAY receive an updated H-SLP address via OMA DM. When the H-SLP address is provisioned in a secure manner to a WiMAX terminal and it must be stored in a protected environment.

6.5 Confidentiality and Data Integrity Protocols

TLS 1.1 [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 “SUPL INIT” and “SUPL REINIT” MUST be delivered within a TLS or PSK-TLS session between a SET and an SLP.

Section 6.1.1.3 provides details for determining which entities in a SUPL 3.0 deployment have TLS with server-certificate authentication and/or TLS-PSK as mandatory or optional.

6.5.1 TLS with Server-Certificates

Implementations of TLS 1.1 with server-certificates shall conform to [TLS] and WAP Profile of TLS 1.1 [WAP TLS] 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.

SLPs supporting TLS 1.1 with server-certificates shall implement the following ciphersuites:

- TLS_RSA_WITH_3DES_EDE_CBC_SHA.
- TLS_RSA_WITH_AES_128_CBC_SHA [TLS-AES].

For SLP implementations supporting TLS 1.1 with server-certificates 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 1.1 SHALL be supported by SLPs supporting TLS 1.1 with server-certificates and SETs.

6.5.2 TLS-PSK

TLS-PSK implementations SHALL conform to PSK-TLS [PSK-TLS] for the TLS Handshake, with Bulk Ciphering as defined for TLS 1.1 [TLS]

SETs supporting TLS-PSK SHALL implement:

- TLS_PSK_WITH_AES_128_CBC_SHA [PSK-TLS].

For SET implementations supporting TLS-PSK that prefer additional cipher suites, the 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 supporting TLS-PSK that prefer additional cipher suites, the SLPs SHOULD implement:

- TLS_PSK_WITH_3DES_EDE_CBC_SHA [PSK-TLS].

6.6 DCert Method and User Binding (Informative)

The DCert method authenticates the SET handset, but (unlike the GBA, SEK and ACA methods) does not perform any authentication tied to Access Network credentials.

If the SLP uses the DCert method for mutual authentication, the SLP Operator is responsible for applying some other mechanism to verify which SUPL User should be associated with the SET. The term "User Binding" is used to describe associating a SUPL User with a SET Identity.

If the SET ownership changes, then is the responsibility of the existing SUPL User to contact the SLP Operator to release the User Binding.

SUPL 3.0 does not specify a User Binding procedure, although one possible procedure is shown in section 6.6.1. Some SLPs may incorporate a User Binding procedure as part of other services provided by the SLP Operator. In other cases, the User Binding may be part of the distribution chain.

The SLP Operator may use any "User Binding" procedure they choose, but the following points should be kept in mind:

- The SUPL User must be authenticated as part of the User Binding procedure.
    - Failure to authenticate the SUPL USER would allow theft of service, and allow the Threat Agent to mislead the SLP regarding the location of the identified SUPL User.
    - We recommend that the SLP Operator apply their existing mechanisms and policies for User Authentication.
- The SET must be authenticated as part of the User Binding procedure.
    - The reasons for this are subtle. Suppose that a Threat Agent wishes to follow the movements of Alice and Alice owns a SET with SET Identity "SET_ID_A". The Threat Agent registers as a legitimate SUPL User and, after authenticating herself, claims to own the SET with SET Identity "SET_ID_A". If the SLP Operator associates this SET with the Threat Agent's account, then the Threat Agent can authorize themselves to obtain periodic location updates from the SLP (via Network Initiated sessions). However, since Alice is using the SET, the Threat Agent is actually getting updates of Alice's location. Since the SLP Operator is expected to keep Alice's location confidential, it is in the SLP Operator's interest to prevent such an attack.

6.6.1 An Example User Binding Procedure

The DCert method is designed primarily for SETs that have web-browsing capabilities: examples include smart-phones, tablets or touch-screen multi-media players.

Such SETs can use the following mechanism:

1. SLP Operator prompts the SUPL User to connect to the URL of an SLP-owned Web Server while using the SET.
2. Subscriber connects to website (possibly WAP) while using the SET.
3. Web Server and SET perform TLS
    a. The Web Server provides a server certificate and requests a client certificate. The Web Server's certificate may be distinct from the certificate for the SLP server certificate used for SUPL service.
    b. The SET authenticates the Web Server
    c. The SET authenticates to the Web Server using the SET's Device Certificate.
    d. The Web-Server has now authenticated that the secure channel is associated with the SET Identity (e.g. IMEI, MEID or serial number) in the Device Certificate.
4. The SUPL User performs some (out of scope) authentication with the website. For example, the Web Server could request an SLP-specific username/password, or federated username/password or other subscriber details such as address, date of birth, etc.

5. The SLP operator has now securely associated the subscriber with the device identity and should store this association in the SLP.

7. ULP Version Negotiation

The ULP Version Negotiation mechanism is based on the assumption that an SLP may support more than one major version of SUPL with supported versions in one contiguous block down from the maximum supported version to the minimum supported version. It is further assumed that a SET only supports one version of SUPL (e.g. a SUPL 3.0 SET only supports SUPL 3.0).

Network Initiated scenarios:

For network initiated scenarios, the SUPL INIT message from the H-SLP or E-SLP to the SET carries the intended SUPL major and minor version M1.m1 (normally the highest version supported by the SLP) in the *version* parameter. The SUPL INIT message also carries the minimum SUPL major version number M2 for which continuation of the session by the SET is possible in the *minimum version* parameter. The value of M2 will depend on the intended SUPL service – e.g. for a single location fix M2 may be one; for triggered location M2 may be two. A SUPL session can be conducted between the SLP and the SET as long as the SET is using a SUPL major version between M2 and M1.

The SET continues the SUPL session normally if it supports a major version M of SUPL between M2 and M1 (i.e. $M2 \leq M \leq M1$) – and indicates this major version and a supported minor version m in the next message (i.e. implicitly in the *version* parameter of the message). The H-SLP or E-SLP then also reverts to the proposed SUPL major version M and the same minor version m if supported (otherwise preferably and if supported to a minor version less than m or less preferably a minor version greater than m). If parameters were included in the SUPL INIT message that are not defined for SUPL version M.m, then the SET will ignore them and the SLP must act as if they had not been sent.

If the SET only supports a major version higher than M1 or a major version lower than M2, it returns a SUPL END.

SET Initiated scenarios:

For SET initiated SUPL sessions, the initial SUPL message from the SET carries the supported SUPL major and minor version M1.m1 (implicitly in the *version* parameter). The H-SLP continues the session if it supports the same major version M1 and otherwise sends a SUPL END and terminates the session.

Version negotiation for SUPL 1.0 is already defined and cannot be changed. Backward compatibility with SUPL 1.0 is achieved as follows:

Exceptions for SUPL 1.0:

For a network initiated SUPL session between an SLP supporting a version of SUPL above 1.0 and a SET that supports only 1.0, the SET will respond to the SUPL INIT message with a SUPL END (implicitly indicating support of SUPL 1.0 in the *version* parameter of SUPL END). The SLP will then restart the session using SUPL 1.0 if supported and if compatible with the intended SUPL service.

For a network initiated SUPL session between an SLP supporting only SUPL 1.0 and a SET that supports only a higher version, the SET will recognize that the SLP only supports SUPL 1.0 and will respond to the SUPL INIT message with SUPL END.

For a SET initiated SUPL session between an SLP supporting a version of SUPL above 1.0 and a SET that supports only 1.0, the SET will indicate SUPL 1.0 in the first SUPL message and the SLP, recognizing this, will either have to continue the session using SUPL 1.0 or reply with a SUPL END thereby terminating the session attempt.

For a SET initiated SUPL session between an SLP supporting only SUPL 1.0 and a SET that supports a higher version, the SLP will respond to the first SET message with a SUPL END and terminate the session.

7.1 Example Call Flows (Informative)

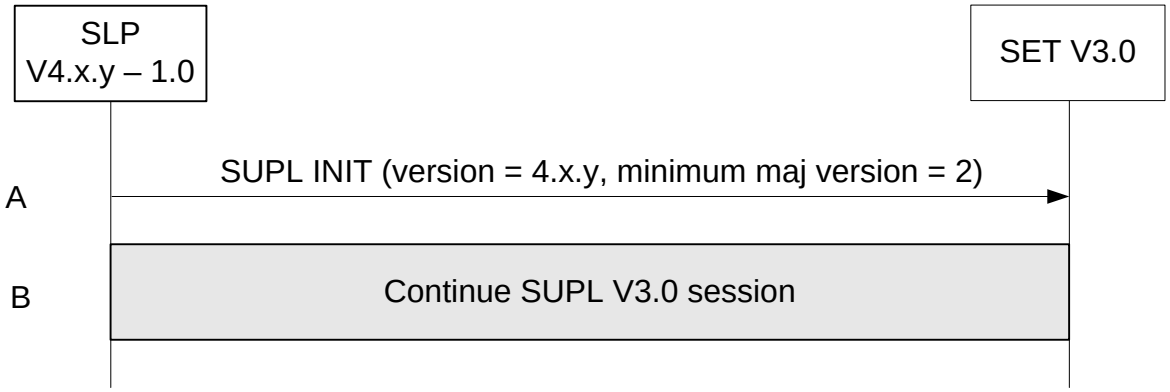

Figure 45: Network Initiated – SLP supports SUPL versions between 1.0 and 4.x.y and the requested service is V3.0 compatible.

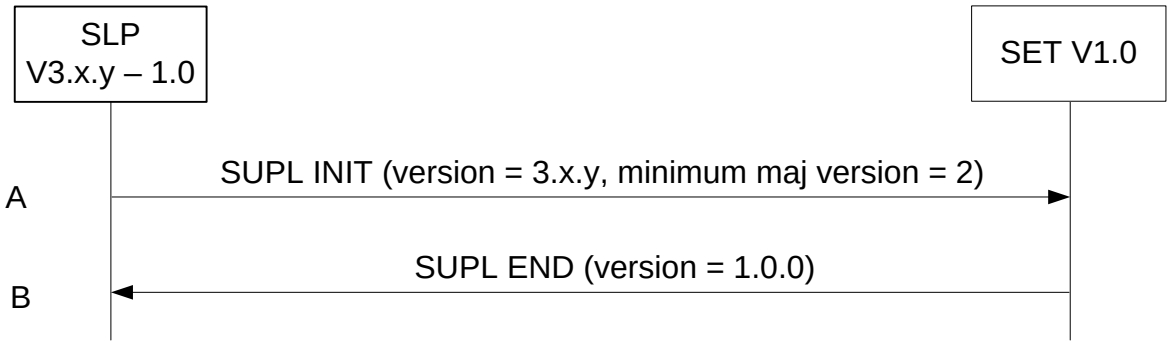

Figure 46: Network Initiated – SLP supports SUPL versions between 1.0 and 3.x.y but the requested service is not V1.0 compatible.

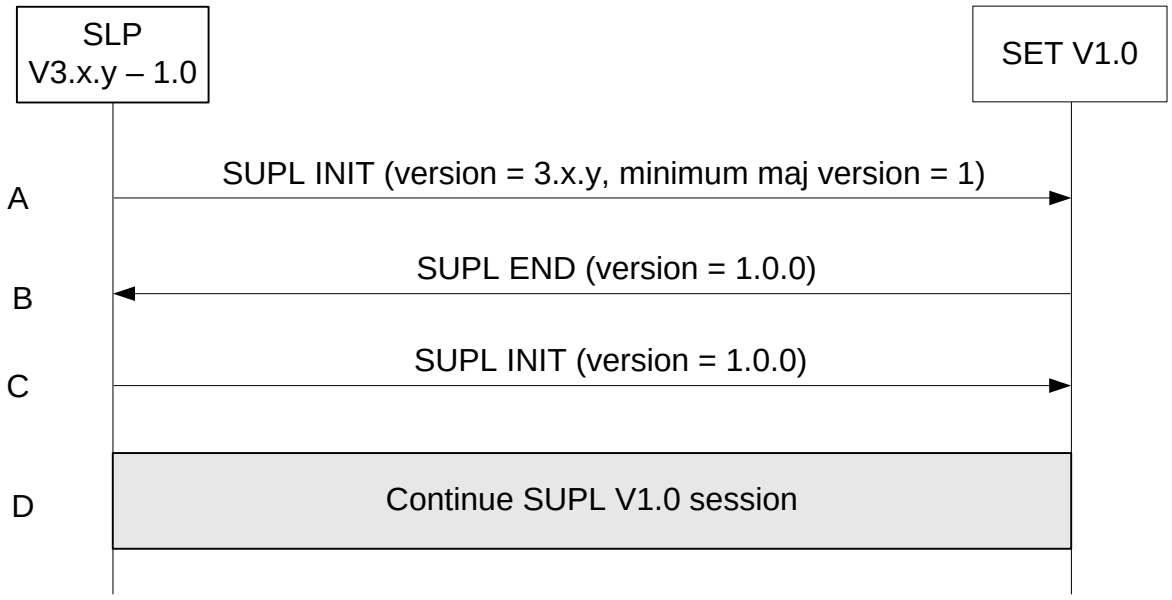

Figure 47: Network Initiated – SLP supports SUPL versions between 1.0 and 3.x.y but the requested service is V1.0 compatible

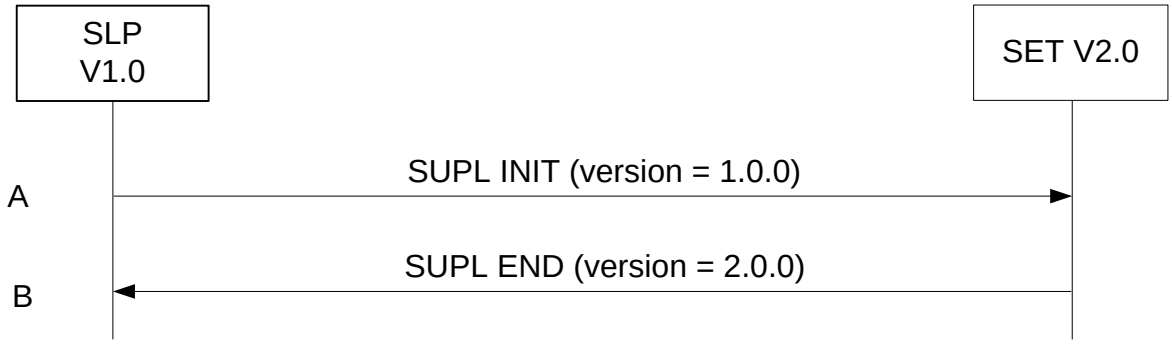

Figure 48: Network Initiated – SLP supports lower version than SET.

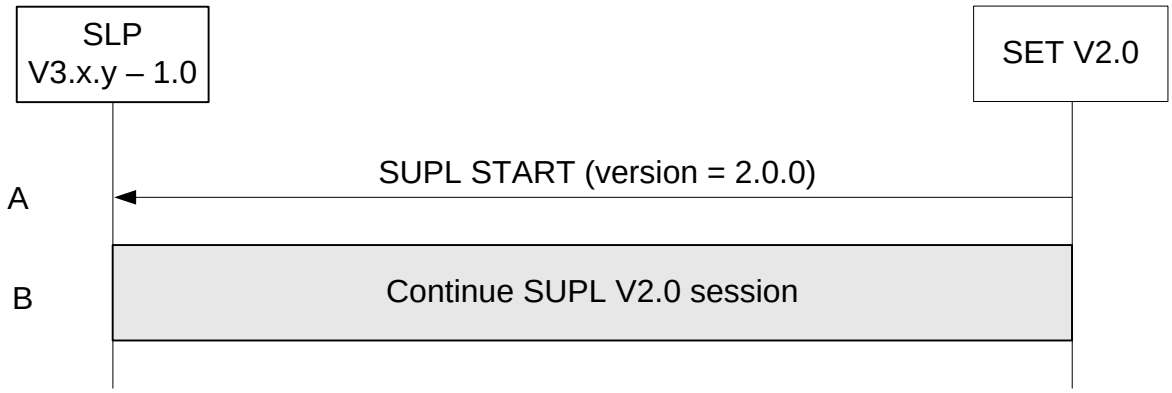

Figure 49: SET Initiated – SLP supports SUPL versions between 1.0 and 3.0 including requested version (V2.0).

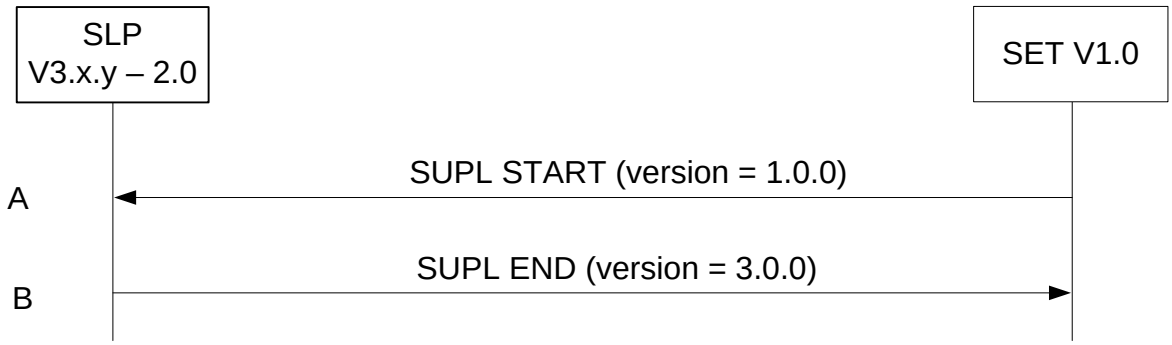

Figure 50: SET Initiated – SLP supports SUPL versions between 2.0 and 3.0 excluding requested version (V1.0).

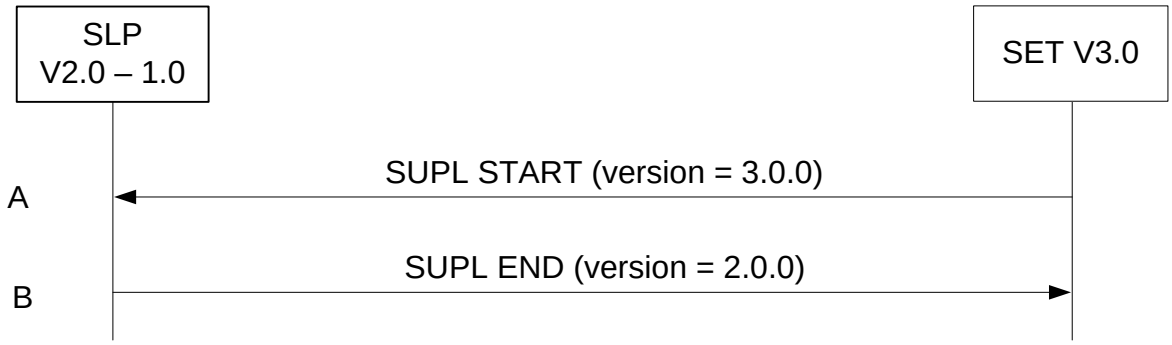

Figure 51: SET Initiated – SLP supports SUPL versions between 1.0 and 2.0 excluding requested version (V3.0).

8. Protocols and Interfaces

The encoding for the ULP protocol SHALL be ASN.1 [ASN.1].

The encoding is BASIC-PER, unaligned encoding [PER].

The transport protocol between SET and SLP SHALL be TCP/IP with the following exception: the initial SUPL INIT/SUPL REINIT message SHALL be transported over OMA Push, SIP Push, Mobile Terminated SMS, UDP/IP or TCP/IP. UDP/IP is applicable if the IP-Address of the SET is known to the SLP or can be retrieved by the SLP. TCP/IP is applicable only for SUPL INIT transport if SET and SLP have an active TLS connection established at the time of sending the SUPL INIT message. In case of OMA Push, the Push message from the PPG or SLP to the SET SHALL follow the OMA Push specifications as per [WAP POTAP]; for SIP Push, the specifications as per [SIP PUSH] with the clarifications given in sections 8.2 and 8.2.1.

For GSM/WCDMA/TD-SCDMA and LTE deployments, SUPL initiation (or re-initiation) using OMA Push, UDP/IP and TCP/IP SHALL be supported by both the SET and the SLP. For CDMA/CDMA2000 deployments, SUPL initiation (or re-initiation) using MT SMS, UDP/IP and TCP/IP SHALL be supported by both the SET and the SLP. For other types of access, SUPL initiation (or re-initiation) using UDP/IP and TCP/IP SHALL be supported by both the SET and the SLP. Support of other transport protocols is optional.

8.1 TCP/IP and UDP/IP

The port number for ULP messages transported over TCP and UDP SHALL be as registered with IANA (Internet Assigned Numbers Authority). The port numbers are:

oma-ulp	7275/tcp	OMA UserPlane Location Protocol
oma-ulp	7275/udp	OMA UserPlane Location Protocol

8.2 SIP Push

SIP Push MESSAGE [SIP PUSH] SHALL be used with the following clarifications:

1. The SIP MESSAGE method SHALL be used to deliver the SUPL INIT/SUPL REINIT message.
2. The Accept-Contact header SHALL include Application Resource Identifier +g.oma.pusheventapp= “ulp.ua”, where the feature tag value “ulp.ua” is derived from the OMNA registered application id “x-oma-application:ulp.ua”.
3. The Content-Type header SHALL be set to OMNA registered content type application/vnd.omaloc-supl-init.
4. The SIP MESSAGE body SHALL contain the PER encoded SUPL INIT/SUPL REINIT message.

An example usage of the MESSAGE method is shown in Appendix G.

8.2.1 SIP Push for IMS Emergency Location Services

In addition to the clarifications given in section 8.2, the following clarifications SHALL apply when the E-SLP uses SIP Push [SIP PUSH] to deliver the SUPL INIT message to the SET via the Emergency IMS Core.

1. The E-SLP SHALL set the Request URI in the SIP MESSAGE to the SET SIP URI or TEL URI received from the Emergency IMS Core or PSAP in the emergency location request.

NOTE: The E-SLP receives the emergency location request from the Emergency IMS Core over 3GPP Ml interface or from the PSAP over the Le interface. The emergency location request contains the SIP URI or TEL URI of the SET which initiated the IMS emergency call. The Emergency IMS Core uses the Request URI to correlate the SIP MESSAGE with the IMS emergency call and routes the SIP MESSAGE to the SET via the signaling path of the IMS emergency call. The specifics of 3GPP Ml interface and Le interface are considered outside scope of SUPL.

An example call flow is shown in Appendix G.

NOTE: 3GPP TS 23.167 mandates SET support for only UDP/IP to support SUPL INIT delivery with SUPL: 2.0 for an IMS Emergency Call from a WCDMA or LTE access network. Therefore, for compatibility, it is recommended that a SUPL 3.0 E-SLP use UDP/IP for any access unless (i) SET support for SIP Push is known in advance or (ii) the E-SLP does not have the SET IP address or (iii) the E-SLP is aware of restrictions to UDP/IP transport such a SET or access network firewall.

8.3 OMA Push

The OMA Push message [OMA PUSH] from an SLP to a PPG SHALL contain the SUPL INIT/SUPL REINIT message and SHALL follow [WAP PAP]. OMA Push over HTTP SHALL be used and SHALL contain the PAP control entity and the PER encoded SUPL INIT/SUPL REINIT message. An example (informative only) is shown in Appendix G. The PPG communicates with the SET over POTAP [WAP POTAP] or SIP Push [SIP PUSH] for an SIP enabled SET with the clarifications given in section 8.2.

The content type SHALL be as registered with IANA (content type: application/vnd.omaloc-supl-init) and OMNA (Open Mobile Naming Authority) (content type's assigned number: 0x312).

The WAP application id SHALL be as registered with OMNA (URN: x-oma-application:ulp.ua) and the assigned code value is (0x10).

8.4 MT SMS

For GSM/WCDMA/TD-SCDMA and LTE, the WDP [WAP WDP] framing SHALL be used for MT SMS. The port number SHALL be as registered with IANA.

This port number is:

oma-ulp 7275/udp OMA User Plane Location Protocol

For CDMA, the SUPL INIT/SUPL REINIT message shall be sent as an MT SMS [TIA-637] using a dedicated Teleservice Identifier [TIA-41]. The dedicated Teleservice Identifier is: 4115.

8.5 SET Provisioning

The SET SHALL be provisioned with the address of the Home SLP in the form of FQDN as described in section 6.4.

8.6 Lup Reference Point

The functions of the Lup reference point are logically separated into Service Management and Position Determination and are described in [SUPLAD3].

8.6.1 Service Management

This interface is used for service management and performs the functions listed in [SUPLAD3].

Table 6 lists Service Management ULP messages.

Message Name	Description
SUPL INIT	The SUPL INIT message is used by the SLP to initiate a SUPL session with the SET. This message is used in Network Initiated SUPL Services.
SUPL REINIT	The SUPL REINIT message is used by the SLP to reinitiate a GSS in situations where the SLP wishes to initiates a positioning activity with the SET in the absence of a secure connection between the SLP and the SET during a GSS.

SUPL SET INIT	The SUPL SET INIT message is used by the SET to initiate a SUPL session in order to locate a 3rd party SET.
SUPL START	The SUPL START message is used by the SET to start a SUPL session with the SLP or as a response to a SUPL INIT message in a Network initiated GSS.
SUPL TRIGGERED START	The SUPL TRIGGERED START message is used by the SET to start a triggered SUPL session with the SLP.
SUPL RESPONSE	The SUPL RESPONSE message is used by the SLP as a response to a SUPL START message in a SET initiated location request.
SUPL TRIGGERED RESPONSE	The SUPL TRIGGERED RESPONSE message is used by the SLP as a response to a SUPL TRIGGERED START message.
SUPL TRIGGERED STOP	The SUPL TRIGGERED STOP message is used by the SLP or SET to end an existing triggered session or to pause/resume an ongoing triggered session.
SUPL END	The SUPL END message is used by the SLP or SET to end an existing SUPL session.
SUPL NOTIFY	The SUPL NOTIFY message is only used by the SLP in notification based on the current location of the SET or for Session Info Query "re-notification" scenarios.
SUPL NOTIFY RESPONSE	The SUPL NOTIFY RESPONSE message is used by the SET as a response to a SUPL NOTIFY message.
SUPL REPORT	The SUPL REPOPRT message is used to report active SET sessions in response to a Session Info Query.

Table 6: Lup Service Management Messages

8.6.2 Position Determination

This interface is used for position calculation. It performs the functions listed in [SUPLAD3].

Table 7 lists Position Determination ULP messages.

Message Name	Description
SUPL POS	The SUPL POS message is used between the SLP and SET to exchange positioning protocol messages (LPP/LPPe or TIA-801) used to calculate the position of the SET. A SUPL POS message MAY include either LPP/LPPe or TIA-801 messages but not both.
SUPL POS INIT	The SUPL POS INIT message is used by the SET to initiate a positioning protocol session (LPP/LPPe/TIA-801) with the SLP.

SUPL REPORT	The SUPL REPORT message is used by the SLP or SET to report position estimate and/or position measurement results and may also be used to indicate the end of a SUPL POS session. Any position measurement results are carried in an LPP, LPP/LPPe or TIA-801 payload.
SUPL END	The SUPL END message is used by the SLP or SET to end an existing SUPL session and may provide a position estimate.

Table 7: Lup Position Determination Messages

A SET and SLP MUST provide support for cell id positioning.

The following requirements apply for a SET or an SLP that supports at least one positioning method standardized for LPP, LPPe or TIA-801. An LTE capable SET and SLP providing support for this SET type SHALL support LPP and MAY support LPPe. A CDMA/HRPD capable SET and SLP providing support for this SET type SHALL support TIA-801. A SET supporting any other bearers and an SLP providing support for this SET SHALL support LPP and LPPe.

A SET or an SLP that supports no positioning method standardized for LPP, LPPe or TIA-801 need not support these positioning protocols although support of SUPL will then be limited.

Table 8 shows a summary of which positioning protocols SHALL be supported and which positioning protocols MAY be supported by SET and an SLP providing support for this SET depending on the bearer and in the case where the SET supports at least one positioning method standardized for LPP, LPPe or TIA-801.

	GSM	WCDMA/TD-SCDMA	LTE	CDMA	HRPD	WLAN	WiMAX	Other
SHALL support	LPP, LPPe	LPP, LPPe	LPP	TIA-801	TIA-801	LPP, LPPe	LPP, LPPe	LPP, LPPe
MAY support			LPPe					

Table 8: Supported positioning protocols by bearer

9. ULP Message Definitions (Normative)

This section contains a normative description of the ULP messages. All messages defined in ULP contain a common part and a message specific part.

9.1 Common Part

The common part contains parameters that are present in all ULP messages.

Parameter	Presence	Description
Message Length	M	The length of the entire ULP Message in octets. NOTE: The first two octets of a PER encoded ULP message contains the length of the entire message. These octets are set to the Message Length when the PER encoding is complete and the entire message length is known.
Version	M	Version of the ULP protocol, in the form major, minor, service indicator
Session ID	M	The unique Session ID
Message Payload	M	This parameter contains one of the messages defined in ULP. Defined messages are: • SUPL INIT • SUPL REINIT • SUPL START • SUPL RESPONSE • SUPL POS INIT • SUPL POS • SUPL END • SUPL SET INIT • SUPL NOTIFY • SUPL NOTIFY RESPONSE • SUPL TRIGGERED START • SUPL TRIGGERED RESPONSE • SUPL TRIGGERED STOP • SUPL REPORT

Table 9: Common Part for all ULP Messages

9.2 Message Specific Part

The message specific part contains further parameters that are unique to each ULP message. The following sub-sections describe the message specific part of ULP messages. To maintain code backwards compatibility with SUPL 2.0, legacy SUPL 2.0 parameters are preserved in SUPL 3.0. Some parameters, however, no longer apply in SUPL 3.0. Parameters which no longer apply are marked as such in the tables of this section.

9.2.1 SUPL INIT

SUPL INIT is the initial message from the H-SLP (or D-SLP or E-SLP) to the SET in Network initiated cases.

Parameter	Presence	Description
Positioning Method	M	This parameter defines the positioning method desired by the SLP for the SUPL session or the action requested for the session. In line with the positioning capabilities of the SET (shared with the SLP on the positioning protocol level) the SLP MAY change the positioning method used in the actual positioning session regardless of the positioning method parameter.
Notification	O	When Notification Mode is Normal Notification /Verification, this field is used to provide instructions to the SET with respect to notification and privacy. If this field is not present the SET SHALL interpret the request as type "No notification & no verification". When Notification Mode is Notification/Verification based on location, this field SHALL NOT be used by the SLP and the SET.
SLP Address	CV	This parameter is not applicable since non-proxy mode is not supported in SUPL 3.0 and is only maintained for code backwards compatibility with SUPL 2.0. This parameter SHALL NOT be used.
QoP	O	Desired Quality of Position. This parameter is also used as reporting criteria for stored historical position estimates. If used in this way, only the spatial components (horacc and veracc) apply and define the accuracy requirements which must be satisfied in order to report any historic position estimate. QoP SHALL NOT be present if High Accuracy QoP is present and vice versa.
SLP Mode	M	This parameter indicates if the SLP uses proxy or non-proxy mode. This parameter SHALL be set to proxy mode since non-proxy mode is not supported in SUPL 3.0.
MAC	O	Not applicable in SUPL 3.0. This parameter SHALL NOT be used.

Key Identity	CV	Not applicable in SUPL 3.0. This parameter SHALL NOT be used.
Notification Mode	O	This parameter indicates whether the notification and verification is based on location or not. If not present, normal notification is assumed.
Supported Network Information	O	This parameter is not applicable in SUPL 3.0. This parameter SHALL NOT be used.
Trigger Type	CV	This parameter indicates network initiated service type: • Periodic • Area event • Velocity event This parameter is conditional and only used if a triggered session is requested in the SUPL INIT message.
E-SLP Address	CV	This parameter provides the E-SLP address. This parameter SHALL be included if the sender of the SUPL INIT is an E-SLP. Use of an FQDN is preferred over an IP address unless the request is associated with an ongoing emergency call.
Historic Reporting	CV	This parameter defines the criteria for reporting of stored historical position estimates and/or enhanced cell/sector measurements. This parameter is conditional and MUST be used if the SUPL INIT message is used to initiate retrieval of stored historical position estimates and/or enhanced cell/sector measurements. Otherwise this parameter is not used.
Protection Level	O	This parameter defines the protection level of the SUPL INIT protection. This parameter is optional. If not present, no protection is implicitly assumed.
GNSS Positioning Technology	O	This parameter is not applicable in SUPL 3.0. This parameter SHALL NOT be used.
Minimum Major Version	O	This parameter defines the minimum major version supported by the SLP which is compatible with the requested service. This parameter is optional. If not present, the only version compatible with the requested service is the *version* parameter (see common part in section 9.1). The *minimum major version* must always be smaller than the *major version*. Range: 0 to 255

SLP Capabilities	O	This parameter defines the SLP capabilities which include the supported positioning protocols (LPP/LPPe and/or TIA-801).
GSS Parameters	CV	This parameter is only used for GSS in which case it is mandatory. The parameter defines the length of the Generic SUPL Session in terms of either duration or number of SUPL POS messages allowed within one GSS.
Extended Notification	O	This parameter provides additional notification information to the SET.
D-SLP Address	CV	This parameter provides the address of a D-SLP and SHALL be included when the sender of the SUPL INIT is a D-SLP.
High Accuracy QoP	O	This parameter is used to specify the desired quality of position for high accuracy positioning. If this parameter is present, high accuracy positioning should be used if supported and applicable. This parameter is also used as reporting criteria for stored historical position estimates. If used in this way, only the spatial components (horacc and veracc) apply and define the accuracy requirements which must be satisfied in order to report any historic position estimate. QoP and High Accuracy QoP are mutually exclusive.

Table 10: SUPL INIT Message

9.2.2 SUPL REINIT

SUPL REINIT is a message from the SLP to the SET. SUPL REINIT is used in Network Initiated GSS scenarios where the SLP initiates a positioning activity with the SET when no secure connection exists. SUPL REINIT only applies to an existing GSS.

Parameter	Presence	Description
Protection Level	O	This parameter defines the protection level of the SUPL REINIT protection. This parameter is optional. If not present, no protection is implicitly assumed.

Table 11: SUPL REINIT Message

9.2.3 SUPL SET INIT

The SUPL SET INIT message is the initial message where a SET can initiate location request to another target SET.

Parameter	Presence	Description

Target SET ID	M	Identifies the 3rd partyTarget SET to be located.
QoP	O	Desired Quality of Position. QoP and High Accuracy QoP are mutually exclusive.
ApplicationID	O	The identifier of the requesting application on the SET.
Result Type	CV	Identify the requested position result type. This parameter can be of type: • Absolute Position • Position relative to Reference Point • Position relative to SET This parameter SHALL be present if the result type is "position relative to reference point" or "position relative to SET". If the position requested is for an absolute position, this parameter MAY be present and if it is present, the result type SHALL be set to "absolute position". If this parameter is not present, it implies that the position requested is for an absolute position. The SLP SHALL reject the request by sending a SUPL END if unable to support the requested result type.
Reference Point Id	CV	This parameter provides a Reference Point Id and is used to indicate that the requested position estimate should be expressed relative to a reference position (relative position). NOTE: The reference point is defined via its unique Id and not via coordinate points. The definition of Reference Point Id is as per [OMA-LPPe]. If the Result Type is *Absolute Position* or *Position relative to SET*, this parameter must not be present. If the Result Type is *Position relative to Reference Point*, this parameter must be present.
High Accuracy QoP	O	This parameter is used to specify the desired quality of position for high accuracy positioning. If this parameter is present, high accuracy positioning should be used if supported and applicable. QoP and High Accuracy QoP are mutually exclusive.

Table 12: SUPL SET INIT Message

9.2.4 SUPL START

SUPL START is the initial message from the SET to the SLP or the response to the SUPL INIT message in Network initiated GSS. Certain parameters in a SUPL START are mutually exclusive and SHALL not be included together. The parameters are as follows listed in priority order, highest priority first.

Mutually exclusive SUPL START Parameters:

- Third Party
- Location URI Request
- SLP Query
- GSS Parameters

When more than one parameter in the above list is included in a SUPL START, the SLP SHALL accept the highest priority parameter and ignore all lower priority parameters. If the result is a badly formed SUPL START message, the SLP SHALL return a SUPL END message and an error code.

Parameter	Presence	Description
SET capabilities	M	Defines the capabilities of the SET
Location ID	M	Defines the current serving cell, current serving WLAN AP or WiMAX BS information of the SET.
QoP	O	Desired Quality of Position. QoP and High Accuracy QoP are mutually exclusive.
Multiple Location IDs	O	This parameter may contain current non-serving cell, current non-serving WLAN AP or current non-serving WiMAX BS information for the SET and/or historic serving or non-serving cell, WLAN AP or WiMAX BS information for the SET.
Third Party	CV	This parameter defines a list of third party identities. For the SET Initiated location request without transfer to Third Party, this parameter SHALL NOT be used. For the SET Initiated location request with transfer of location to Third Party mode, this parameter SHALL be used.

>Third Party ID	M	The identity of the Third Party. There must be at least one Third Party ID. This parameter can be of type • Logical name • MSISDN • Email address • SIP URI • IMS Public Identity • MIN • MDN • URI
ApplicationID	O	The identifier of the requesting application on the SET.
Position	O	Defines the position of the SET.
GSS Parameters	O	This parameter is only used for GSS in which case it is mandatory. The parameter defines the length of the Generic SUPL Session in terms of either duration or number of SUPL POS messages allowed within one GSS.
Location URI Request	CV	This parameter contains a request for a Location URI. This parameter SHALL be included if a Location URI is requested. Location URIs can only be requested in the context of immediate SET Initiated SUPL sessions.
Location URI Set	O	This parameter contains a set of one or more location URIs. The parameter MAY be included if the SET received a Location URI or set of Location URIs from another server that are still valid and if the SET is initiating a location session. The SLP may use the received location URI(s) to obtain a separate location estimate for the SET from the server(s) referenced by the location URI(s). The means for doing this are outside the scope of this specification.
Ver	CV	This parameter contains a hash of the SUPL INIT message. This parameter is only applicable to Network-Initiated GSS.
SLP Query	CV	This parameter is only included for a D-SLP or E-SLP Query to the H-SLP or to a Proxy D-SLP or Proxy E-SLP.

Emergency Services Indication	CV	This parameter indicates whether the SUPL START message is sent to support emergency services (e.g. to support an emergency call). In case of emergency services support, this parameter MUST be sent. Otherwise, this parameter MUST NOT be sent.
Reference Point Id	CV	This parameter provides a Reference Point Id and is used to indicate that the requested position estimate should be expressed relative to a reference position (relative position). This parameter SHALL be included when the SET requests a relative location estimate and SHALL otherwise be absent. The SLP should reject the request by sending a SUPL END if unable to support location relative to the provided reference point. NOTE: The reference point is defined via its unique Id and not via coordinate points. The definition of Reference Point Id is as per [OMA-LPPe].
High Accuracy QoP	O	This parameter is used to specify the desired quality of position for high accuracy positioning. If this parameter is present, high accuracy positioning should be used if supported and applicable. QoP and High Accuracy QoP are mutually exclusive.

Table 13: SUPL START Message

9.2.5 SUPL RESPONSE

SUPL RESPONSE is the response to a SUPL START message.

Parameter	Presence	Description
Positioning Method	M	The positioning method that is desired for the SUPL session. In line with the positioning capabilities of the SET (shared with the SLP on the positioning protocol level) the SLP MAY change the positioning method used in the actual positioning session regardless of the positioning method parameter.

SLP Address	CV	This parameter is not applicable since non-proxy mode is not supported in SUPL 3.0 and is only maintained for code backwards compatibility with SUPL 2.0. This parameter SHALL NOT be used.
SET Auth key	O	This parameter SHALL NOT be used and is only provided for reasons of encoding backwards compatibility with SUPL 1.0.
Key Identity 4	O	This parameter SHALL NOT be used and is only provided for reasons of encoding backwards compatibility with SUPL 1.0.
SPC_SET_Key	O	This parameter defines the authentication key used by the SET for H/V-SPC authentication. This parameter is not applicable in SUPL 3.0. This parameter SHALL NOT be used.
SPC-TID	O	This parameter defines the transaction ID used for H/V-SPC authentication. This parameter is not applicable in SUPL 3.0. This parameter SHALL NOT be used.
SPC_SET_Key_lifetime	O	This parameter defines the lifetime of SPC_SET_Key. This parameter is optional. If not present, a default value of 24 hours is assumed. The units are in hours and the range is from 1 to 24 hours. This parameter is not applicable in SUPL 3.0. This parameter SHALL NOT be used.
Supported Network Information	O	This parameter is not applicable in SUPL 3.0. This parameter SHALL NOT be used. The presence of this parameter is implementation dependent.
Initial Approximate Position	O	Defines the initial approximation for the position of the SET.
GNSS Positioning Technology	O	This parameter is not applicable in SUPL 3.0. This parameter SHALL NOT be used.
SLP Capabilities	O	This parameter defines the SLP capabilities which include the supported positioning protocols (LPP/LPPe and/or TIA-801).
GSS Parameters	CV	This parameter is only used for GSS in which case it is mandatory. The parameter defines the length of the Generic SUPL Session in terms of either duration or number of SUPL POS messages allowed within one GSS.

Initial Approximate Relative Position	O	This parameter defines the initial approximation for a position result relative to a reference point (relative position).
Initial Approximate Civic Position	O	This parameter defines the initial approximation for a position result according to civic address.

Table 14: SUPL RESPONSE Message

9.2.6 SUPL POS INIT

SUPL POS INIT is the message following the SUPL INIT message in Network initiated cases or the SUPL RESPONSE message in SET initiated cases

Parameter	Presence	Description
SET Capabilities	M	Defines the capabilities of the SET.
Requested Assistance Data	O	This parameter is not applicable in SUPL 3.0. This parameter SHALL NOT be used.
Location ID	M	Defines the current serving cell, current serving WLAN AP or current serving WiMAX BS information of the SET.
Position	O	Defines the position of the SET.
SUPLPOS	O	Contains the SUPL POS message. NOTE: Is only used if positioning protocol allows SET to send first message. Any positioning protocol messages in this parameter that are not supported by the SLP SHALL be ignored by that SLP.
Ver	CV	This parameter contains the hash of the SUPL INIT/SUPL REINIT message. In Network Initiated scenarios the SET SHALL calculate the hash of the received SUPL INIT/SUPL/REINIT and include the result of the hash in this parameter.
Multiple Location IDs	O	This parameter may contain current non-serving cell, current non-serving WLAN AP or current non-serving WiMAX BS information for the SET and/or historic serving or non-serving cell, WLAN AP or WiMAX BS information for the SET.
UTRAN GPS Reference Time Result	O	This parameter is not applicable in SUPL 3.0. This parameter SHALL NOT be used.
UTRAN GANSS Reference Time Result	O	This parameter is not applicable in SUPL 3.0. This parameter SHALL NOT be used.

Location URI Set	O	This parameter contains a set of one or more location URIs. The parameter MAY be included if the SET received a Location URI or set of Location URIs from another server that are still valid. The SLP may use the received location URI(s) to obtain a separate location estimate for the SET from the server(s) referenced by the location URI(s). The means for doing this are outside the scope of this specification.

Table 15: SUPL POS INIT Message

9.2.7 SUPL POS

SUPL POS is the message that wraps the underlying TIA-801 or LPP/LPPe positioning protocol payload. A SUPL POS message MAY contain either LPP/LPPe or TIA-801 payload messages but not both.

Parameter	Presence	Description
Positioning Payload	M	The underlying TIA-801 or LPP/LPPe elements. This parameter MAY contain up to three LPP/LPPe or TIA-801 messages, respectively.
Velocity	O	This parameter is not applicable in SUPL 3.0. This parameter SHALL NOT be used.
UTRAN GPS Reference Time Assistance	O	This parameter is not applicable in SUPL 3.0. This parameter SHALL NOT be used.
UTRAN GPS Reference Time Result	O	This parameter is not applicable in SUPL 3.0. This parameter SHALL NOT be used.
UTRAN GANSS Reference Time Assistance	O	This parameter is not applicable in SUPL 3.0. This parameter SHALL NOT be used.
UTRAN GANSS Reference Time Result	O	This parameter is not applicable in SUPL 3.0. This parameter SHALL NOT be used.
More	CV	This parameter is conditional and SHALL be used by the sending entity to indicate to the receiving entity that an additional SUPL POS message will follow and that the receiving entity SHALL wait for this additional SUPL POS message to arrive before proceeding with the SUPL POS exchange. If the more parameter is not present, the receiving entity MAY proceed with the SUPL POS session immediately after receiving the SUPL POS message. More and End parameters are mutually exclusive.

End	CV	This parameter is conditional and SHALL be used by the sending entity to indicate to the receiving entity that the SUPL POS session has ended. More and End parameters are mutually exclusive.

Table 16: SUPL POS Message

9.2.8 SUPL END

SUPL END is the message that ends the SUPL procedure, normally or abnormally.

Parameter	Presence	Description
Position	O	Defines the position result of the SET.
Status Code	O	Defines the Status of the message as either an error indication or an information indication. Error indications have values between 0 and 99, information indications have values between 100 and 199.
Ver	CV	This parameter contains the hash of the SUPL INIT/SUPL REINIT message and is calculated by the SET. This parameter MUST be present in situations where the SUPL END message is sent as a direct response to a SUPL INIT/SUPL REINIT message.
SET Capabilities	O	Defines the SET Capabilities of the SET. This parameter MAY be used if the SUPL END message is sent from the SET to the SLP.
Location URI Set	O	This parameter contains a set of one or more location URIs. This parameter MAY only be included if the SUPL END message is sent from the SLP to the SET and if the SET had previously requested a Location URI from the SLP.

SLP Authorization	CV	This parameter provides one or more authorized D-SLP and/or E-SLP addresses and MAY include limitations on the use of each address. This parameter is included in a response to a D-SLP or E-SLP Query from the SET to the H-SLP, Proxy D-SLP or Proxy E-SLP. The parameter MAY also be included when terminating a Session Info Query from the H-SLP or a Proxy D-SLP. The parameter MAY also be used to support unsolicited provision of D-SLP and/or E-SLP addresses by the H-SLP or by a Proxy D-SLP at the end of any SUPL session. Unsolicited provisioning MAY be used whenever the SET capabilities indicate support for the particular type of D-SLP or E-SLP provision. Any D-SLP addresses or E-SLP addresses provided by an H-SLP or Proxy D-SLP SHALL replace any previous D-SLP or E-SLP addresses, respectively, that were provided earlier by the H-SLP or the same Proxy D-SLP, respectively. Other provided D-SLP and E-SLP addresses are not affected except that removal of a Proxy D/E-SLP address also SHALL remove all D-SLP or E-SLP addresses that may have been provided by the Proxy D/E-SLP.
Relative Position	O	This parameter defines the position result relative to a reference point or another SET (relative position). This parameter is only applicable when sent from the SLP to the SET.
Civic Position	O	This parameter defines the position result as civic address. This parameter is only applicable when sent from the SLP to the SET. The presence of this parameter is implementation dependent.
SUPL INIT Key Response	CV	This parameter is conditional and SHALL only be used for Mode A SUPL_INIT_ROOT_KEY Establishment (see section 6.3.5.2). This parameter SHALL only be used if SUPL END is sent from the SLP to the SET.

Table 17: SUPL END Message

9.2.9 SUPL TRIGGERED START

SUPL TRIGGERED START is the initial message from the SET to the H-SLP or D-SLP for establishing a triggered session.

Parameter	Presence	Description
SET capabilities	M	Defines the capabilities of the SET
Location ID	M	Defines the current serving cell, current serving WLAN AP or WiMAX BS information of the SET.
Ver	CV	This parameter contains a hash of the SUPL INIT message. In Network Initiated mode, the SET SHALL calculate the hash of the received SUPL INIT message and include the result in this parameter. This parameter SHALL NOT be included in a SUPL TRIGGERED START sent to request new trigger parameters.
QoP	O	Desired Quality of Position. QoP and High Accuracy QoP are mutually exclusive.
Multiple Location IDs	O	This parameter may contain current non-serving cell, current non-serving WLAN AP or WiMAX BS information for the SET and/or historic serving or non-serving cell or WLAN AP information for the SET.
Third Party	CV	The identity of the Third Party. This parameter is not applicable in SUPL 3.0 and SHALL NOT be used.
>Third Party ID	M	The identity of the Third Party.
Application ID	O	The identifier of the requesting application on the SET.
Trigger Type	CV	This parameter indicates SET initiated trigger service type: • Periodic • Area event • Velocity event For network initiated trigger service, it MUST not be present.
Trigger Params	CV	This parameter indicates parameters of the trigger session. For network initiated trigger service, this parameter MUST NOT be present. For SET initiated trigger service, this parameter MUST be present.
Position	O	Defines the position of the SET.

Reporting Capability	CV	This parameter defines the reporting capabilities of the SET on a per SUPL session basis (there is a Reporting Capability parameter as part of SET Capabilities -> Service Capabilities which reflects the generic SET Reporting Capabilities). This parameter is conditional and only used for triggered periodic scenarios. The values of this parameter MUST be consistent with the values of Reporting Capability as part of SET Capabilities. For periodic triggered services, this parameter MUST be present. For area or velocity event triggered services, this parameter MUST NOT be present.
>minimum interval between fixes	M	Defines the minimum interval between fixes allowed by the SET. This parameter is used by the H-SLP or D-SLP to avoid conflict between the desired interval between fixes and the SET's capabilities. Range: 1 to 3600, Units in seconds.
>maximum interval between fixes	O	Defines the maximum interval between fixes allowed by the SET. This parameter is used by the H-SLP or D-SLP to avoid conflict between the desired interval between fixes and the SET's capabilities. This parameter is optional. If not present, no maximum interval between fixes is specified. Range: 1 to 1440, Units in minutes.
>Rep Mode	M	This parameter is a bit map indicating the supported reporting mode(s): • Real time • Quasi real time • Batch reporting At least one of the three reporting modes must be supported.

>Batch Report Capability	CV	If batch reporting is supported as reporting mode, this parameter defines the type of reports which are supported: • Position • Measurement data • Position and Measurement data The maximum number of positions and/or measurements the SET is able to store are defined as: • Maximum number of positions • Maximum number of measurements These parameters are optional. If not present, no limit is specified.
Cause Code	O	This parameter indicates the reason for sending this message during an ongoing triggered session. The value could be: • Serving Network not in Area Id list • SET capabilities has changed • No SUPL coverage
Positioning Payload	CV	The LPP/LPPe or TIA-801 payload. In the context of Network Change for Area Event Triggered scenarios (see section 5.3.8); this parameter SHALL be provided by the SET. Otherwise this parameter MUST NOT be used.
Reference Point Id	CV	This parameter provides a Reference Point Id and is used to indicate that the requested position estimate should be expressed relative to a reference position (relative position). This parameter is only used in the context of periodic triggered services. This parameter SHALL be included when the SET requests a relative location estimate and SHALL otherwise be absent. The SLP should reject the request by sending a SUPL END if unable to support location relative to the provided reference point. NOTE: The reference point is defined via its unique Id and not via coordinate points. The definition of Reference Point Id is as per [OMA-LPPe].

High Accuracy QoP	O	This parameter is used to specify the desired quality of position for high accuracy positioning. If this parameter is present, high accuracy positioning should be used if supported and applicable. QoP and High Accuracy QoP are mutually exclusive.

Table 18: SUPL TRIGGERED START Message

9.2.10 SUPL TRIGGERED RESPONSE

SUPL TRIGGERED RESPONSE is the response to a SUPL TRIGGERED START message from the SLP to the SET

Parameter	Presence	Description
Positioning Method	M	The positioning method desired for the triggered SUPL session. In line with the positioning capabilities of the SET (shared with the SLP on the positioning protocol level) the SLP MAY change the positioning method used in the actual positioning session regardless of the positioning method parameter.
Trigger Params	CV	This parameter indicates triggered session parameters. For network initiated trigger service, this parameter MUST be present. For SET initiated trigger service, this parameter MAY be used to convey an Area Id List to the SET.
SLP Address	CV	This parameter is not applicable since non-proxy mode is not supported in SUPL 3.0 and is only maintained for code backwards compatibility with SUPL 2.0. This parameter SHALL NOT be used.
Supported Network Information	O	This parameter is not applicable in SUPL 3.0. This parameter SHALL NOT be used.
Reporting Mode	O	For periodic triggered sessions this parameter defines the reporting mode requested by the SLP. This parameter is optional. If not present, real time reporting is requested.
>Rep Mode	M	One of the following modes: • Real time • Quasi real time • Batch reporting

>Batch Reporting Conditions	CV	If batch reporting is chosen, the SLP selects one of the following reporting conditions: • Sending of a batch report after every N fixes/measurements • Sending of a batch report after every N minutes • Sending of only one batch report at the end of the session
>Batch Report Type	CV	If batch or quasi-real time reporting is chosen as reporting mode, this parameter defines the type of reports which are allowed to be reported: • Position • Measurement data • Intermediate reporting If set to false, the SET SHALL NOT report any earlier than requested even if it runs out of memory. If not all data could be reported, the SET SHALL indicate this with a result code of outofmemory. If set to true, the SET MAY send intermediate reports earlier than requested if it runs out of memory. The SET SHALL indicate intermediate reports with a result code of outofmemoryintermediatereporting. • Discard Oldest If set to true, the SET SHALL discard the oldest data first in the batch report if it runs out of memory and cannot use intermediate reporting. If set to false, the SET SHALL discard the latest data in the batch report first if it runs out of memory and cannot use intermediate reporting . If not present, it is up to the SET implementation to decide which data to discard first.
SPC_SET_Key	O	This parameter defines the authentication key used by the SET for H/V-SPC authentication. This parameter is not applicable in SUPL 3.0. This parameter SHALL NOT be used.
SPC-TID	O	This parameter defines the transaction ID used for H/V-SPC authentication. This parameter is not applicable in SUPL 3.0. This parameter SHALL NOT be used.

SPC_SET_Key_lifetime	O	This parameter defines the lifetime of SPC_SET_Key. This parameter is optional. If not present, a default value of 24 hours is assumed. The units are in hours and the range is from 1 to 24 hours. This parameter is not applicable in SUPL 3.0. This parameter SHALL NOT be used.
GNSS Positioning Technology	O	This parameter is not applicable in SUPL 3.0. This parameter SHALL NOT be used.
SLP Capabilities	CV	This parameter defines the SLP capabilities which include the supported positioning protocols (LPP/LPPe and/or TIA-801).

Table 19: SUPL TRIGGERED RESPONSE Message

9.2.11 SUPL TRIGGERED STOP

The SUPL TRIGGERED STOP message is used by the SLP or the SET to end an existing triggered session or to pause/resume an ongoing triggered session.

Parameter	Presence	Description
Status Code	O	Defines the status code of the message.
Request Type	CV	Indicates the request type : • Stop • Pause • Resume This parameter SHALL be included when the SUPL TRIGGERED STOP message is sent to stop, pause or resume the triggered session. This parameter SHALL be only sent from the SET to the SLP.
End Session List	CV	A list of session-ids of all sessions to cancel. This parameter SHALL be only used in the “session-info query” session. This parameter SHALL only be sent from the SLP to the SET.
SLP Authorization	O	This parameter may be included only as part of a Session Info Query from the H-SLP or a Proxy D-SLP. The parameter provides new authorized D-SLP and/or E-SLP addresses and may include limitations on the use of these addresses.

Table 20: SUPL TRIGGERED STOP Message

9.2.12 SUPL NOTIFY

SUPL NOTIFY is the message from the SLP to the SET in Network initiated cases.

Parameter	Presence	Description
Notification	M	The purpose of this field is to provide instructions to the SET with respect to notification and privacy. If the Notification List parameter is present, this parameter SHALL be ignored.
Notification List	CV	A list of Notifications to be applied to each session that needs re-notification or re-notification and verification. This parameter SHALL only be used during a *Session Info Query* session.
> **Notification Session**	M	Each Notification Session consists of Session ID and Notification.
>> **Session ID**	M	The Session id that needs re-notification or re-notification and verification.
>> **Notification**	M	Identifies the notification/verification mechanism to be applied.

Table 21: SUPL NOTIFY Message

9.2.13 SUPL NOTIFY RESPONSE

SUPL NOTIFY RESPONSE is the response to a SUPL NOTIFY message.

Parameter	Presence	Description
Notification Response	CV	The purpose of this field is to provide notification response from the user. This field MUST be present in response to a SUPL NOTIFY in which notification and verification was requested.
Notification Resp List	CV	A list of notification responses of each session. This parameter SHALL be only used during a “Session-Info Query” session.
> **Notification Resp Session**	M	Each Notification Resp Session consists of Session ID and Notification Response.
>> **Session ID**	M	The Session id related to the notification response.
>> **Notification Response**	M	The notification response from the user. This parameter can be of type: • Allowed • Not Allowed

Table 22: SUPL NOTIFY RESPONSE Message

9.2.14 SUPL REPORT

The SUPL REPORT message is used in the following instances:

(1) For triggered applications, the SUPL REPORT message is used by the SLP to indicate the end of a positioning procedure (SUPL POS session) to the SET. In this case the SUPL REPORT message may or may not contain a calculated position.

(2) For triggered applications, the SUPL REPORT message may be used to send one or more position result(s) (calculated by the SET) and/or enhanced cell/sector measurement(s) from the SET to the SLP. The enhanced cell/sector/AP measurements are sent in LPP/LPPe/TIA-801 Provide Location Information messages carried within SUPL REPORT. The SUPL REPORT message may be used without a position or velocity result to indicate to the SLP that an Area or Velocity Event has occurred. A result code may optionally be sent to indicate an error condition (e.g. no position available).

(3) As an intermediate report within a continuing batch reporting session, the SUPL REPORT message is used as in triggered applications, but the message should only contain the position result(s). This allows the SET to dynamically manage its memory by lowering the amount of data stored on the SET.

(4) SUPL REPORT is used by the SET in response to a session info query from the H-SLP or D-SLP. In this case the SUPL REPORT message contains a list of session-ids of all active SUPL sessions. The SUPL REPORT message MAY also include the SET Capabilities. For a session info query from the H-SLP, the SUPL REPORT message contains the addresses of all currently authorized D-SLPs and E-SLPs (including D-SLPs and E-SLPs authorized by authorized Proxy D/E-SLPs). For a session info query from a Proxy D-SLP, the SUPL REPORT message contains the addresses of all D-SLPs currently authorized by that Proxy D-SLP.

(5) SUPL REPORT is used by the SET to report change of access to an authorized D-SLP that can support Network Initiated services.

NOTE: For uplink reporting, if the amount of report data to be sent exceeds the maximum ULP message length (64K Octets), the SET SHALL send the report data in multiple SUPL REPORT messages.

Parameter	Presence	Description
SessionList	O	A list of the session-ids of all active SUPL sessions. The list does not contain the session-id of the "session-info query" session which is already included in the session-id parameter of the SUPL REPORT message. This parameter SHALL be only used in the “session-info query” session.
SET capabilities	O	Defines the capabilities of the SET. This parameter may only be used if the SUPL REPORT message is sent in the context of a "session-info query" session.
ReportDataList	O	The Report Data List comprises one up to 1024 occurrences of Report Data.
>Report Data	M	Report Data contains the actual data to be reported: Position Data, Measurement Data, Result Code and Time Stamp.

>>Position Data	O	A calculated position and the respective positioning mode used (optional).
>>>position	M	The calculated position of the SET (including a time stamp).
>>>posmethod	O	Positioning method with which the position was calculated.
>>>GNSS Positioning Technology	O	Defines any GNSSs used to calculate the position. • GPS • Galileo • SBAS • Modernized GPS • QZSS • GLONASS • BDS
>>>GANSS Signals Information	O	This parameter may be included to indicate the GANSS Signals (up to 16) used for calculation of the position. GANSS Signals Information defines a list of GANSS Signals.
>>>>GANSS Id	M	Defines the GANSS. Integer (0..15) 0: Galileo 1: SBAS 2: Modernized GPS 3: QZSS 4: GLONASS 5: BDS 6-15: Reserved for future use

>>>>**GANSS Signals**	M	Bitmap (length 8 bits) defining the supported signals for GNSS indicated by GANSS ID. For Galileo, the bits are interpreted as : Bit 0: E1 Bit 1: E5a Bit 2: E5b Bit 3: E5a+E5b Bit 4: E6 Bits 5-7: Spare For Modernized GPS, the bits are interpreted as: Bit 0: L1 C Bit 1: L2 C Bit 2: L5 Bits 3-7: Spare For QZSS, the bits are interpreted as: Bit 0: L1 C/A Bit 1: L1 C Bit 2: L2 C Bit 3: L5 Bits 4-7: Spare For GLONASS, the bits are interpreted as: Bit 0: G1 Bit 1: G2 Bit 2: G3 Bits 3-7: Spare For SBAS, the bits are interpreted as: Bit 0: L1 Bits 1-7: Spare For BDS, the bits are interpreted as: Bit 0: B1I Bits 1-7: Spare
>>**Multiple Location Ids**	O	Multiple Location Ids.

>>Result Code	O	Result Code describing why no position or measurement could be reported: a. Out of radio coverage b. No position c. No measurement d. No position and no measurement e. Out of memory f. Out of memory, intermediate reporting g. Other
>>Time Stamp	O	Time Stamp in either absolute time (UTC Time) or relative time (relative to "now" i.e. when the SUPL REPORT message is sent. This parameter is only used if Position Data is not present. If Position Data is present, the timestamp parameter within position is used as timestamp.
>>LPP/LPPe/TIA-801 payload	O	This parameter carries LPP/LPPe/TIA-801 payload for sending enhanced cell/sector/AP measurement information.
Ver	CV	This parameter contains a hash of the SUPL INIT message. This parameter MUST be used if the SUPL REPORT message is sent in response to a SUPL INT message. Otherwise this parameter is not applicable.
More Components	CV	This parameter is used if the report data to be sent needs to be segmented into multiple SUPL REPORT messages. If present, this parameter indicates that more SUPL REPORT messages will be sent. The last SUPL REPORT message in a series of segments SHALL omit this parameter.
Pause Session List	O	A list of session-ids of all paused triggered SUPL sessions. This parameter SHALL be only used in the "session-info query" session.

Authorized D-SLP List	O	For a response to a Session Info Query from the H-SLP or a Proxy D-SLP, this parameter carries the addresses of all D-SLPs currently authorized by the H-SLP or Proxy D-SLP. In the case of an H-SLP, the parameter also includes any D-SLPs currently authorized by any authorized Proxy D-SLP. A D-SLP is considered to be currently authorized if its associated service duration has not yet expired.
Authorized E-SLP List	O	For a response to a Session Info Query from the H-SLP, this parameter carries the addresses of all currently authorized E-SLPs including E-SLPs authorized by any authorized Proxy E-SLP. An E-SLP is considered to be currently authorized if its associated service duration has not yet expired.
D-SLP Access Notification	O	This parameter is included to report initial or subsequent access to an authorized D-SLP that can support Network Initiated services. The parameter carries the address of the D-SLP.
Relative Position	O	This parameter defines the position result relative to a reference point (relative position). This parameter is only applicable when sent from the SLP to the SET.
Civic Position	O	This parameter defines the position result according to civic address. This parameter is only applicable when sent from the SLP to the SET. The presence of this parameter is implementation dependent.

Table 23: SUPL REPORT Message

10.Parameter Definitions (Normative)

This section contains descriptions of the parameters used in ULP messages.

10.1 Positioning Payload

Parameter	Presence	Value/Description
Positioning payload		Describes the positioning payload for TIA-801 [TIA-801], LPP [3GPP LPP] and LPPe [OMA-LPPe]. This parameter MAY contain up to three LPP/LPPe messages or up to three TIA801 messages. This parameter MUST NOT contain both LPP/LPPe and TIA-801 messages.

Table 24: Positioning Payload Parameter

10.2 SLP Address

Parameter	Presence	Value/Description
SLP address		The SLP address can be of type: • IPAddress o IPv4 o IPv6 • FQDN

Table 25: SLP Address Parameter

10.3 Velocity

Parameter	Presence	Value/Description
Velocity		Describes the velocity of the SET as per [3GPP GAD]. One of the following four formats are supported: • Horizontal Velocity o Bearing o Horizontal speed • Horizontal and Vertical Velocity o Vertical Direction o Bearing o Horizontal speed o Vertical speed • Horizontal Velocity Uncertainty o Bearing o Horizontal speed o Horizontal speed uncertainty • Horizontal and Vertical Velocity Uncertainty o Vertical direction o Bearing o Horizontal speed o Vertical speed o Horizontal speed uncertainty o Vertical speed uncertainty • High accuracy 3D velocity as per [OMA-LPPe]

Table 26: Velocity Parameter

10.4 Version

Parameter	Presence	Value/Description
Version		Describes the protocol version of ULP. When a SUPL message is received, the receiving entity SHALL determine if the major version part specified in the message is supported by the receiving entity.
>Maj	M	Major version, range: (0..255), MUST be 3 for the version described in this document
>Min	M	Minor version, range: (0..255), MUST be 0 for the version described in this document.
>Serv_ind	M	Service indicator, range: (0..255), MUST be 0 for the version described in this document.

Table 27: Version

10.5 Status Code

Parameter	Presence	Value/Description
Status Code		The different status codes, either error or information indicators, as described in the table below

Table 28: Status Code

Status Code	Description
Error Indicators	Used to indicate errors
unspecified	The error is unknown
systemFailure	System Failure
protocolError	Protocol parsing error
dataMissing	Needed data value is missing
unexpectedDataValue	A datavalue takes a value that cannot be used
posMethodFailure	The underlying positioning method returned a failure
posMethodMismatch	No positioning method could be found matching requested QoP, SET capabilities and positioning method specified by SLP
posProtocolMismatch	No positioning protocol could be found being available at SET and SLP
targetSETnotReachable	The SET was not responding
versionNotSupported	Wrong ULP version
resourceShortage	There were not enough resources available at the SLP to serve the SET or not enough resource available at the SET for the session.
invalidSessionId	Invalid session identity
unexpectedMessage	Unexpected message received
nonProxyModeNotSupported	Non-Proxy mode is no longer supported in SUPL 3.0 and therefore this value is not applicable.
proxyModeNotSupported	Only Proxy-Mode is supported in SUPL 3.0 and therefore this value is not applicable.
positioningNotPermitted	The SET is not authorized by the SLP to obtain a position or assistance data.
authNetFailure	This value is not applicable in SUPL 3.0.
authSuplinitFailure	The SUPL INIT message is not authenticated by the SET or the SLP
serviceNotSupported	Service Capability not supported
incompatibleProtectionLevel	The Protection Level in the SUPL INIT message is not compatible with the protection level of the SET
insufficientInterval	The requested interval between fixes is not compatible with the capabilities of either the SET or the SLP.
noSUPLCoverage	The SET lost SUPL coverage. This status code is used for V-SLP to V-SLP handover to indicate to the H-SLP or D-SLP that the SET lost SUPL coverage.

Information Indicators	Used to indicate information
consentDeniedByUser	User denied consent for location determination session.
consentGrantedByUser	User granted consent for location determination session.
sessionStopped	The triggered session has been stopped by the network or the SET.
appIdDenied	The App Id was not authorized by the SLP and as a result, the requested service was denied.
locationURIUnavailable	The SLP was unable to assign a location URI
locationURINotSupported	The SLP does not support assignment of a location URI
locationURINotAuthorized	The SET is not authorized to receive a location URI
gssCapabilityMismatch	The GSS capabilities of the SET and SLP do not match.
unauthorizedAccessToSLP	The SET is not authorized to access a D-SLP or E-SLP.
invalidAccessToSLP	The SET is authorized to access a D-SLP or E-SLP but is outside the serving area or not using an allowed access network
RelativeLocationNotSupported	Relative location is not supported
ReferencePointNotSupported	The requested reference point is not supported by the SLP.

Table 29: Status Code

10.6 Position

Parameter	Presence	Value/Description
Position		This parameter describes the position of the SET. The parameter also contains a timestamp and optionally the velocity.
>Timestamp	M	Time when position fix was calculated.
>Position Estimate	M	
>>Sign of latitude	M	Indicates North or South.
>>Latitude	M	Integer (0..2^{23}-1). The latitude encoded value (N) is derived from the actual latitude X in degrees (0°..90°) by this formula: $N \leq 2^{23} X /90 < N+1$
>>Longitude	M	Integer (-2^{23}.. 2^{23}-1). The longitude encoded value (N) is derived from the actual longitude X in degrees (-180°..+180°) by this formula: $N \leq 2^{24} X /360 < N+1$

>>Uncertainty ellipse (semi major, semi minor, major axis)	O	Contains the latitude/longitude uncertainty code associated with the major axis, and the uncertainty code associated with the minor axis and the orientation, in degrees, of the major axis with respect to the North. For the correspondence between the latitude/longitude uncertainty code and meters refer to [3GPP GAD] for details.
>>Confidence	O	Represents the confidence by which the position of a target entity is known to be within the shape description (i.e., uncertainty ellipse for 2D-description, uncertainty ellipsoid for 3D-description) and is expressed as a percentage. This is an integer (0..100).
>>Altitude information	O	SHALL be present for a 3D position information; it SHALL remain absent for 2D position information.
>>>Altitude direction	M	Indicates height (above the WGS84 ellipsoid) or depth (below the WGS84 ellipsoid).
>>>Altitude	M	Provides altitude information in meters. Integer (0..2^{15}-1). Refer to [3GPP GAD] for details
>>>Altitude uncertainty	M	Contains the altitude uncertainty code. Refer to [3GPP GAD] for details
>>highAccuracy3Dposition	O	Defines the high accuracy 3D position as defined in [OMA-LPPe]
>Velocity	O	Speed and bearing values as defined by the Velocity type.

Table 30: Position Parameter

The definition and coding of the position estimate parameter (ellipsoid point with altitude, uncertainty ellipse and altitude uncertainty) is based on [3GPP GAD]. The Datum used for all positions are WGS-84.

The definition and coding of the high accuracy 3D position is based on [OMA-LPPe]. If an LPPe version has been selected for the positioning session, then that same version SHALL be used. Otherwise version 1.0 of LPPe SHALL be used.

Since the low accuracy position estimate is mandatory, both low accuracy and high accuracy position estimate SHALL be sent in case of high accuracy position estimate reporting. When both are sent, they SHALL be consistent with each other.

10.7 Positioning Method

Parameter	Presence	Value/Description
Position Method		Describes the desired positioning method or requested action. In line with the positioning capabilities of the SET (shared with the SLP on the positioning protocol level) the SLP MAY change the positioning method used in the actual

		positioning session regardless of the positioning method parameter. Legacy values which are no longer applicable SHALL NOT be used. • A-GPS SET assisted only (not applicable in SUPL 3.0) • A-GPS SET based only (not applicable in SUPL 3.0) • A-GPS SET assisted preferred (A-GPS SET based is the fallback mode) (not applicable in SUPL 3.0) • A-GPS SET based preferred (A-GPS SET assisted is the fallback mode) (not applicable in SUPL 3.0) • A-GNSS SET Assisted only (not applicable in SUPL 3.0) • A-GNSS SET Based only (not applicable in SUPL 3.0) • A-GNSS SET Assisted preferred (A-GNSS SET Based is the fallback mode) (not applicable in SUPL 3.0) • A-GNSS SET Based preferred (A-GNSS SET Assisted is the fallback mode) (not applicable in SUPL 3.0) • Autonomous GPS (not applicable in SUPL 3.0) • Autonomous GNSS (not applicable in SUPL 3.0) • AFLT (not applicable in SUPL 3.0) • Enhanced Cell/sector (not applicable in SUPL 3.0) • EOTD (not applicable in SUPL 3.0) • OTDOA (not applicable in SUPL 3.0) • No position • Historical Data Retrieval • Session-Info Query • SET Assisted Generic (any SET Assisted method or combination of SET assisted methods) • SET Based Generic (any SET based method or combination or SET based methods) • GSS • Other

		For Network Initiated scenarios the positioning method “no position” is used for single fix location requests when no SUPL POS session is to be conducted and the SUPL INIT message was only sent for notification and verification purposes. In this case the SET will respond with a SUPL END message including the appropriate status code (“consentDeniedByUser” or “consentGrantedByUser”). In case no verification was required (“notification only”), the SET will respond with a SUPL END message containing no status code. The positioning method "historical data retrieval" is used to retrieve stored historical position estimates and/or enhanced cell/sector measurements. The Position Method “Session-Info Query” is used to invoke Session Info Query procedure, see section 5.1.3. The positioning method “GSS” is used to initiate a GSS session.

Table 31: Positioning Method Parameter

10.8 SET capabilities

Parameter	Presence	Value/Description
SET capabilities	-	Describes the capabilities of the SET.
>Pos Technology	M	This parameter does not apply to SUPL 3.0. The SLP SHALL ignore this parameter.
>>GANSS Position Methods	O	This parameter is not applicable in SUPL 3.0 and SHALL not be used.
>Pref Method	M	This parameter is not applicable in SUPL 3.0. The SLP SHALL ignore this parameter.
>Pos Protocol	M	Zero or more of the following positioning protocols (bitmap): • TIA-801 • LPP • LPPe Flags for legacy positioning protocols (RRLP and RRC) SHALL be set to FALSE.

>>Pos Protocol Version TIA-801	CV	Describes the protocol version of 3GPP2 C.S0022 (TIA-801) Positioning Protocol. It is required if TIA-801 is identified in the Pos Protocol parameter.
>>>Supported Pos Protocol Version TIA-801	M	Specifies a list of up to 8 different supported 3GPP2 C.S0022 versions. This parameter is required (with at least one entry in the list) if TIA-801 is identified in the Pos Protocol parameter.
>>>>Revision Number	M	Revision part of document number for the specifications of C.S0022 Positioning Protocol. Value: [0,A-Z]
>>>>Point Release Number	M	Point Release number for C.S0022, range: (0..255)
>>>Internal Edit Level	M	Internal Edit Level for C.S0022, range: (0..255)
>>Pos Protocol Version LPP	CV	Describes the protocol version of LPP Positioning Protocol. It is required if LPP is identified in the Pos Protocol parameter.
>>>Major Version Field	M	First (most significant) element of the version number for LPP Positioning Protocol, range: (0..255)
>>>Technical Version Field	M	Second element of the version number for LPP Positioning Protocol, range: (0..255)
>>>Editorial Version Field	M	Third (least significant) element of the version number for LPP Positioning Protocol, range: (0..255)
>>Pos Protocol Version LPPe	CV	Describes the protocol version of LPPe Positioning Protocol. It is required if LPPe is identified in the Pos Protocol parameter.
>>>Major Version Field	M	First (most significant) element of the version number for LPPe Positioning Protocol, range: (0..255)
>>>Minor Version Field	M	Second element of the version number for LPPe Positioning Protocol, range: (0..255)
>Service Capabilities	O	The service capabilities of the SET are described in this parameter. The SET MAY send this parameter in SUPL START, SUPL POS INIT, SUPL TRIGGERED START and SUPL END. The purpose of this parameter is to inform the H-SLP or D-SLP about the service capabilities of the SET

>>services supported	M	Defines the supported services by the SET. Only Network Initiated services are relevant in this context. Zero or more of the following services are supported: • Periodic Trigger • Area Event Trigger • Velocity Event Trigger
>>reporting capabilities	CV	Defines the reporting capabilities of the SET. This parameter is only required if periodic triggers are supported by the SET in which case the parameter is mandatory.
>>>minimum interval between fixes	M	Defines the minimum interval between fixes allowed by the SET. This parameter is used by the H-SLP or D-SLP to avoid conflict between the desired interval between fixes and the SET's capabilities. Range: 1 to 3600, Units in seconds.
>>>maximum interval between fixes	O	Defines the maximum interval between fixes allowed by the SET. This parameter is used by the H-SLP or D-SLP to avoid conflict between the desired interval between fixes and the SET's capabilities. This parameter is optional. If not present, no maximum interval between fixes is specified. Range: 1 to 1440, Units in minutes.
>>>rep mode	M	Supported reporting mode(s): • Real time • Quasi real time • Batch reporting (At least one of the three reporting modes must be supported)
>>>batch rep cap	CV	Defines the type of batch reporting capabilities supported by the SET (only applicable to quasi real time and batch reporting): • Report position (*true* if reporting of position is allowed, *false* otherwise) • Report measurements (*true* if reporting of measurements is supported, *false* otherwise) • Maximum number of positions (range: 1 to 1024) • Maximum number of measurements (range: 1 to 1024)

>>event trigger capabilities	CV	Defines the event trigger capabilities of the SET. This parameter is only required if area event triggers are supported by the SET in which case the parameter is mandatory.
>>> geo area shapes supported	M	This parameter defines the geographic target area shapes supported by the SET in addition to mandatory circular area: • Elliptical • Polygon
>>> max number of geographical target areas supported	O	This parameter defines the maximum number of geographic target areas the SET supports. (range: 1 to 32) This parameter is optional. If not present, the SET does not support geographical target areas.
>>> max number of Area Id Lists supported	O	This parameter defines the maximum number of Area Id Lists the SET supports. (range: 1 to 32) This parameter is optional. If not present, the SET does not support Area Ids.
>>> max number of Area Ids supported per Area Id List	CV	This parameter defines the maximum number of Area Ids per Area Id List the SET supports. (range: 1 to 256) This parameter is conditional: if max number of Area Id Lists is present, then this parameter MUST be present. Otherwise this parameter MUST NOT be present.
>>session capabilities	M	Defines the session capabilities of the SET: • Total number of simultaneous sessions (range: 1 to 128). • Maximum number of simultaneous periodic triggered sessions (only used for periodic triggers) (range: 1 to 32). • Maximum number of simultaneous area event triggered sessions (only used for area event triggers) (range: 1 to 32). • Maximum number of simultaneous velocity event triggered sessions (only used for velocity event triggers) (range: 1 to 32).
> supported bearers	O	This parameter is not applicable in SUPL 3.0. This parameter SHALL NOT be used.

>QoPCapabilities	O	This parameter defines the ability of the SET for reporting and/or receiving high accuracy position and/or velocity results. If parameter is absent capability is not supported.
>Civic Position Capabilities	O	This parameter defines the ability of the SET to support absolute civic positioning. If parameter is absent capability is not supported.
>Relative Position Capabilities	O	This parameter defines the ability of the SET to support relative positioning. If parameter is absent capability is not supported.
> D-SLP Provision from H-SLP	O	This field indicates whether the SET supports provision of authorized D-SLP addresses from the H-SLP. If parameter is absent capability is not supported.
> E-SLP Provision-from-H-SLP	O	This field indicates whether the SET supports provision of authorized E-SLP addresses from the H-SLP. If parameter is absent capability is not supported.
> D-SLP Provision from Proxy D-SLP	O	This field indicates whether the SET supports provision of authorized D-SLP addresses from a Proxy D-SLP. If parameter is absent capability is not supported.
> E-SLP Provision from-Proxy-E-SLP	O	This field indicates whether the SET supports provision of authorized E-SLP addresses from a Proxy E-SLP. If parameter is absent capability is not supported.
> D-SLP Notification to H-SLP	O	This field indicates whether the SET is able to notify the H-SLP when the SET changes access to a D-SLP. If parameter is absent capability is not supported.

> **Sensor Support**	O	Defines whether the SET is able to use sensors to calculate or retrieve location estimates and/or velocity estimates reported in a SUPL REPORT within the session. If parameter is absent capability is not supported. A Sensor is a function in the SET that is not controlled by the positioning protocol (LPP/LPPe or TIA-801) and is able to determine location estimates and/or velocity estimates. A Sensor may get estimates or measurements from entities external to the SET or to the device in which the SET resides. If a Sensor is used to determine position then "Position Method" in SUPL REPORT SHALL be set to "Other". This parameter does not indicate support of a Sensor in LPPe [OMA-LPPe].
SUPL INIT Root Key Status	CV	This parameter is conditional and MAY only be used if Mode A SUPL INIT protection is used. For NULL SUPL INIT Protection and Mode B SUPL INIT Protection, this parameter SHALL NOT be used. This parameter is used by the SET to indicate to the SLP one of the following conditions: • Invalid SUPL INIT Root Key • Out of Sync SUPL INIT Root Key This parameter SHALL be sent and set to "*Invalid SUPL INIT Root Key*" if the SET does not have a valid SUPL INIT Root Key. It SHALL be sent and set to "*Out of Sync SUPL INIT Root Key*" if the SET's SUPL INIT Root Key is out of sync. If the SET has a valid SUPL INIT Root Key which is in sync, this parameter SHALL NOT be sent.

Table 32: SET capabilities Parameter

10.9 Location ID

Parameter	Presence	Value/Description
Location ID	-	Defines the current serving cell, current serving WLAN AP or current serving WiMAX BS information of the SET.
>Cell Info	M	The following cell IDs are supported: • GSM Cell Info • WCDMA/TD-SCDMA Cell Info • CDMA Cell Info • HRPD Cell Info • LTE Cell Info • WLAN AP Info • WiMAX BS Info • No Cell Info - This is to be used for bearers where there is no applicable cell information e.g. Cable Modems.
>Status	M	Describes whether or not the cell, WLAN AP or WiMAX BS info is: • Not Current, last known cell/AP info • Current, the present cell/AP info • Unknown (i.e. not known whether the cell/AP id is current or not current).

Table 33: Location ID Parameter

10.10 GSM Cell Info

The GSM Cell parameter defines the parameter of a GSM radio cell.

Parameter	Presence	Value/Description
Gsm Cell Info	-	GSM Cell ID
>MCC	M	Mobile Country Code, range: (0..999)
>MNC	M	Mobile Network Code, range: (0..999)
>LAC	M	Location Area Code, range: (0..65535)
>CI	M	Cell Identity, range: (0..65535)
>NMR	O	Not applicable in SUPL 3.0. This parameter SHALL NOT be used.
>>ARFCN	M	Not applicable in SUPL 3.0. This parameter SHALL NOT be used.
>>BSIC	M	Not applicable in SUPL 3.0. This parameter SHALL NOT be used.
>>RXLev	M	Not applicable in SUPL 3.0. This parameter SHALL NOT be used.
>TA	O	Not applicable in SUPL 3.0. This parameter SHALL NOT be used.

Table 34: GSM Cell Info Parameter

10.11 WCDMA/TD-SCDMA Cell Info

The WCDMA/TD-SCDMA Cell parameter defines the parameter of a WCDMA/TD-SCDMA radio cell.

Parameter	Presence	Value/Description
Wcdma/TD-SCDMA Cell Info	-	WCDMA/TD-SCDMA Cell ID
>MCC	M	Mobile Country Code, range: (0..999)
>MNC	M	Mobile Network Code, range: (0..999)
>UC-ID	M	Cell Identity, range: (0..268435455). NOTE: This information element contains the Cell Identity sent in SIB3 [3GPP RRC]
>Frequency Info	O	Not applicable in SUPL 3.0. This parameter SHALL NOT be used.
>Primary Scrambling Code	O	Not applicable in SUPL 3.0. This parameter SHALL NOT be used.
>Measured Results List	O	Not applicable in SUPL 3.0. This parameter SHALL NOT be used.
>Cell Parameters ID	O	Not applicable in SUPL 3.0. This parameter SHALL NOT be used.
>Timing Advance	O	Not applicable in SUPL 3.0. This parameter SHALL NOT be used.
>> TA	M	Not applicable in SUPL 3.0. This parameter SHALL NOT be used.
>>TA Resolution	O	Not applicable in SUPL 3.0. This parameter SHALL NOT be used.
>> Chip Rate	O	Not applicable in SUPL 3.0. This parameter SHALL NOT be used.

Table 35: WCDMA/TD-SCDMA Cell Info Parameter

10.12 LTE Cell Info

The LTE Cell Info parameter defines the parameter of a LTE radio cell.

Parameter	Presence	Value/Description
LTE Cell Info	-	LTE Cell ID. Parameter definitions in [3GPP 36.321].
>CellGlobalIdEUTRA	M	
>>PLMN-Identity	M	
>>>MCC	M	Mobile Country Code, range: (0..999)
>>>MNC	M	Mobile Network Code, range: (0..999)
>>CI	M	Cell Identity, length 28 bits.
>PhysCellId	M	Physical Cell ID, range: (0..503)
>TrackingAreaCode	M	Tracking Area Code, length 16 bits
>RSRPResult	O	Not applicable in SUPL 3.0. This parameter SHALL NOT be used.
>RSRQPResult	O	Not applicable in SUPL 3.0. This parameter SHALL NOT be used.

>TA	O	Not applicable in SUPL 3.0. This parameter SHALL NOT be used.
>Measured Results List EUTRA	O	Not applicable in SUPL 3.0. This parameter SHALL NOT be used.

Table 36: LTE Cell Info

10.13 CDMA Cell Info

The CDMA Cell Cell Info parameter defines the parameter of a CDMA radio cell.

Parameter	Presence	Value/Description
Cdma Cell Info	-	CDMA Cell ID
>NID	M	Network ID, range: (0..65535)
>SID	M	System ID, range: (0..32767)
>BASEID	M	Base Station ID, range: (0..65535)
>BASELAT	M	Base Station Latitude, range: (0..4194303)
>BASELONG	M	Base Station Longitude, range: (0..8388607)
>REFPN	M	Base Station PN Number, range: (0..511)
>WeekNumber	M	GPS Week number, range: (0..65535)
>Seconds	M	GPS Seconds, range: (0..4194303)

Table 37: CDMA Cell Info

10.14 HRPD Cell Info

The HRPD Cell Info parameter defines the parameter of a HRPD radio cell.

Parameter	Presence	Value/Description
Hrpd Cell Info	-	HRPD Cell ID
>SECTORID	M	Sector ID, length 128 bits
>BASELAT	M	Base Station Latitude, range: (0..4194303)
>BASELONG	M	Base Station Longitude, range: (0..8388607)
>WeekNumber	M	GPS Week number, range: (0..65535)
>Seconds	M	GPS Seconds, range: (0..4194303)

Table 38: HRPD Cell Info

10.15 WLAN AP Info

The WLAN AP Info parameter defines the parameters of a WLAN access point [IEEE 802.11].

Parameter	Presence	Value/Description
WLAN AP Info	-	WLAN Access Point ID
>AP MAC Address	M	Access Point MAC Address
>AP Transmit Power	O	Not applicable in SUPL 3.0. This parameter SHALL NOT be used.

>AP Antenna Gain	O	Not applicable in SUPL 3.0. This parameter SHALL NOT be used.
>AP S/N	O	Not applicable in SUPL 3.0. This parameter SHALL NOT be used.
> Device Type	O	Not applicable in SUPL 3.0. This parameter SHALL NOT be used.
>AP Signal Strength	O	Not applicable in SUPL 3.0. This parameter SHALL NOT be used.
>AP Channel/Frequency	O	Not applicable in SUPL 3.0. This parameter SHALL NOT be used.
>Round Trip Delay	O	Not applicable in SUPL 3.0. This parameter SHALL NOT be used.
>>RTD Value	M	Not applicable in SUPL 3.0. This parameter SHALL NOT be used.
>>RTD Units	M	Not applicable in SUPL 3.0. This parameter SHALL NOT be used.
>>RTD Accuracy	O	Not applicable in SUPL 3.0. This parameter SHALL NOT be used.
>SET Transmit Power	O	Not applicable in SUPL 3.0. This parameter SHALL NOT be used.
>SET Antenna Gain	O	Not applicable in SUPL 3.0. This parameter SHALL NOT be used.
>SET S/N	O	Not applicable in SUPL 3.0. This parameter SHALL NOT be used.
>SET Signal Strength	O	Not applicable in SUPL 3.0. This parameter SHALL NOT be used.
>AP Reported Location	O	Location of the Access Point as reported by the AP
>>Location Encoding	M	Location encoding description - LCI as per **Error! Reference source not found.** - ASN.1 as per **Error! Reference source not found.**
>>Location Data	M	Location Data
>>>Location Accuracy	O	Location Accuracy in units of 0.1m
>>>Location Value	M	Location value in the format defined in Location Encoding

Table 39: WLAN AP Info

10.16 WiMAX BS Info

The WiMAX BS Info parameter defines the parameters of a WiMAX base station **Error! Reference source not found.**.

Parameter	Presence	Value/Description
WiMAX BS Info	-	WiMAX Base Station Info
>BS ID	M	Base Station Identifier Bit string of fix length of 48
>RTD measurement	O	Not applicable in SUPL 3.0. This parameter SHALL NOT be used.
>>Round Trip Delay	M	Not applicable in SUPL 3.0. This parameter SHALL NOT be used.

>>Round Trip Delay Uncertainty	O	Not applicable in SUPL 3.0. This parameter SHALL NOT be used.
>WiMAX NMR List	O	Not applicable in SUPL 3.0. This parameter SHALL NOT be used.
>> BS ID	M	Not applicable in SUPL 3.0. This parameter SHALL NOT be used.
>> Relative Delay	O	Not applicable in SUPL 3.0. This parameter SHALL NOT be used.
>> Relative Delay uncertainty	O	Not applicable in SUPL 3.0. This parameter SHALL NOT be used.
>>BS Signal Strength	O	Not applicable in SUPL 3.0. This parameter SHALL NOT be used.
>>BS Signal Strength Uncertainty	O	Not applicable in SUPL 3.0. This parameter SHALL NOT be used.
>>BS Tx Power	O	Not applicable in SUPL 3.0. This parameter SHALL NOT be used.
>>BS CINR	O	Not applicable in SUPL 3.0. This parameter SHALL NOT be used.
>>BS CINR Uncertainty	O	Not applicable in SUPL 3.0. This parameter SHALL NOT be used.
>> BS Location	O	Not applicable in SUPL 3.0. This parameter SHALL NOT be used.
>>>Location Encoding	M	Not applicable in SUPL 3.0. This parameter SHALL NOT be used.
>>>>Location Data	M	Not applicable in SUPL 3.0. This parameter SHALL NOT be used.
>>>>>Location Accuracy	O	Not applicable in SUPL 3.0. This parameter SHALL NOT be used.
>>>>>Location Value	M	Not applicable in SUPL 3.0. This parameter SHALL NOT be used.

Table 40: WiMAX BS Info

10.17 Multiple Location Ids

Parameter	Presence	Value/Description
Multiple Location IDs	-	This parameter contains a set of up to MaxLidSize (64) Location ID/Relative Timestamp/Serving Cell Flag data. If Relative Timestamp is present, the associated Location ID represents historical data; if Relative Timestamp is absent, the Location ID represents current data.

>Location ID	M	Describes measured globally unique cell/WLAN AP/WiMAX BS identification of the serving cell/WLAN AP/WiMAX BS or cell/WLAN AP/WiMAX BS identification from any receivable radio network. If this information is historical, the Relative Timestamp parameter must be present. If this data is current, the Relative Timestamp parameter need not be present.
>Relative Timestamp	CV	Time stamp of measured location Id relative to "current Location ID" in units of 0.01 sec. Range from 0 to 65535*0.01 sec. Time stamp for current Location Id if present is 0.
>Serving Cell Flag	M	This flag indicates whether the Location ID data represents a serving cell, WLAN AP or WiMAX BS or idle (i.e. camped-on) cell, WLAN AP or WiMAX BS. If set, the Location ID information represents serving cell, WLAN AP or WiMAX BS information; if not set, the Location ID information represents idle mode information or neighbour cell, WLAN AP or WiMAX BS information.

Table 41: Multiple Location Id Parameter

10.18 Notification

Parameter	Presence	Value/Description
Notification	-	Describes the notification/verification mechanism to be applied.
>Notification type	M	Type of notification: • No notification & no verification • Notification only • Notification and verification o Allowed on no answer (if no answer is received from the SET User, the SET will assume that user consent has been granted and will proceed) o Denied on no answer (if no answer is received from the SET User, the SET will assume that user consent has been denied and will abort) • Privacy override (is used for preventing notification and

		verification without leaving any traces of a performed position fix or position fix attempt in terms of log files etc. on the SET). For "Allowed on no answer" and "Denied on no answer", the SET SHOULD return a response to the H-SLP or D-SLP within 40 seconds of receiving the SUPL INIT. This allows the ST2 timer on the H-SLP or D-SLP to be configured to take user response time into account along with SUPL INIT delivery time, secure session initiation, etc.
>Encoding type	CV	Encoding type is required when Notification type is set to Notification only or Notification and verification and when RequestorID or ClientName is used. • ucs2 • gsm-default • UTF-8 NOTE: gsm-default refers to the 7-bit default alphabet and the SMS packing specified in [3GPP 23.038].
>RequestorID	O	Identity of the Requestor
>RequestorType	CV	Indicates the RequestorID type. It is required if RequestorID is present. The RequestorID type can be one of the following: • Logical name • MSISDN • E-mail address • URL • SIP URI • IMS public identity • MIN • MDN
>ClientName	O	The name of the Location Application.
>ClientNameType	CV	Indicates the type of the client name. It is required if ClientName is present. The type of the client name can be one of the following: • Logical name • MSISDN • E-mail address • URI • SIP URL • IMS public identity • MIN

		• MDN
Emergency Call Location	CV	Indicates location in association with an emergency call. Required in a SUPL INIT for an emergency call.

Table 42: Notification Parameter

10.19 QoP

Parameter	Presence	Value/Description
QoP	-	Describes the desired Quality of Position
>Horizontal accuracy	M	Horizontal accuracy as defined in [3GPP GAD]
>Vertical accuracy	O	Vertical accuracy as defined in [3GPP GAD]
> Maximum Location Age	O	Maximum tolerable age of position estimates used for cached position fixes. Units in seconds from 0 to 65535.
>Delay	O	Values as defined for element Response Time in [3GPP RRLP]: 2^N, N from (0..7), unit is seconds NOTE: The Delay value should be applied to the timer of the used positioning protocol i.e. any positioning protocol specific timers (timers within the SUPL POS block) MUST be equal to the Delay value.

Table 43: QoP

10.20 Session ID

The Session ID SHALL be a unique value, consisting of two parts, a SET value (SET Session ID) (see section 10.20.1) concatenated with an SLP value (SLP Session ID) (see section 10.20.2).

Parameter	Presence	Value/Description
SET Session ID	M	Part of Session ID pertaining to the SET
SLP Session ID	M	Part of Session ID pertaining to the SLP

Table 44: Session ID Parameter

For Network-Initiated flows, when sending a SUPL INIT to the SET, the SLP SHALL assign a value to the SLP Session ID, but to save bandwidth, the SLP SHALL not include the SET Session ID in the message. The SET SHALL then assign a value to the SET Session ID when it receives the message. Any further messages SHALL contain the resultant combined Session ID for the remainder of the session.

For SET-Initiated flows, when sending a SUPL START, SUPL TRIGGERED START or SUPL SET INIT message to the SLP, the SET SHALL assign a value to the SET Session ID. The SET will not send an SLP Session ID in these messages since no SLP Session ID yet exists. The SLP SHALL assign a value to the SLP Session ID when it receives one of these messages. All further messages SHALL contain the resultant combined Session ID for the remainder of the session.

The Session ID SHALL allow for multiple simultaneous sessions on both the SLP and the SET. The main purpose of the Session ID is to allow both SLP and SET to distinguish between multiple simultaneous sessions. Taking advantage of this capability, the SLP SHALL be capable of supporting multiple SUPL sessions with the same SET over any number of one or more secure sockets.

10.20.1 SET Session ID

This section describes the construct of the SET Session ID.

Parameter	Presence	Value/Description
Session ID	M	Session identifier, unique from SET perspective. This value SHALL be unique over all concurrently active ULP sessions on that particular SET. This value may be reused by the SET after the ULP session for which it is being used has ended.
SET ID	M	SET identity value This parameter can be of type • MSISDN • MDN • MIN • IMSI • NAI • IPAddress o IPv4 o IPv6

Table 45: SET Session ID Parameter

10.20.2 SLP Session ID

This section describes the construct of the SLP Session ID.

Parameter	Presence	Value/Description
Session ID	M	Session identifier, unique from SLP perspective. This value SHALL be unique over all concurrently active ULP sessions on that particular SLP. This value may be reused by the SLP after the ULP session for which it is being used has ended. This parameter is written into a 4-octet-string.

SLP ID	M	The identity of the SLP. This parameter can be of type • IPAddress o IPv4 o IPv6 • FQDN. NOTE: SLP ID MAY be of different type and different value compared to the parameter SLP address in the messages SUPL INIT and SUPL RESPONSE.

Table 46: SLP Session ID Parameter

10.21 SLP Mode

Parameter	Presence	Value/Description
SLP Mode	-	Describes the mode that the SLP uses. This parameter can be of type Proxy Mode Non-proxy Mode In SUPL 3.0, only proxy mode is supported and therefore the value of this parameter SHALL be set to "Proxy Mode".

Table 47: SLP Mode Parameter

10.22 MAC

Parameter	Presence	Value/Description
MAC	-	Not used in SUPL 3.0 but empty placeholder remains for SUPL 1.0 backwards compatibility (needed so that a SUPL 3.0 SET can still decode legacy SUPL INIT messages).

Table 48: MAC Parameter

10.23 Key Identity

Parameter	Presence	Value/Description
Key Identity	-	Not used in SUPL 3.0 but empty placeholder remains for SUPL 1.0 backwards compatibility (needed so that a SUPL 3.0 SET can still decode a SUPL 1.0 SUPL INIT message).

Table 49: Key Identity Parameter

10.24 Ver

Parameter	Presence	Value/Description
Ver	-	Describes the hash of the SUPL INIT or SUPL REINIT message.

Table 50: Ver Parameter

10.25 Location Triggers

10.25.1 Trigger Type

Parameter	Presence	Value/Description
Trigger Type	--	This parameter defines the trigger type: • Periodic • Area Event • Velocity Event

Table 51: Trigger Type Parameters

10.25.2 Trigger Params

Parameter	Presence	Value/Description
Trigger Params	--	This parameter can be of type Periodic Params or Area Event Params or Velocity Event Params.

Table 52: Trigger Params Parameters

10.25.2.1 Periodic Params

This section describes the construct of the Periodic Triggers Params. This parameter is required if trigger type is set to Periodic.

Parameter	Presence	Value/Description
Number Of Fixes	M	Describes the number of fixes during the periodic triggered session. (range: 1 to 8639999). For compatibility with MLP and RLP number of fixes * interval between fixes SHALL NOT exceed 8639999 (100 days).
Interval Between Fixes	M	Describes the interval between the start of position fixes for periodic trigger. Units in seconds (range: 1 to 8639999)
StartTime	O	It indicates when the SET is to start the first position fix. Start Time is interpreted relative to the current time i.e. to the time when the message containing the parameter is received by the H-SLP or D-SLP or the SET. Start Time is OPTIONAL. If not present, the SET is to start the first fix immediately. Units in seconds (range: 0 to 2678400).

Table 53: Periodic Params Parameters

10.25.2.2 Area Event Params

This section describes the construction of the Area Event trigger Params. This parameter is required if trigger type is set to Area Event (for more information about Area Event Triggers see Appendix G and Appendix H).

The Area Event trigger can be one of the following types:

- Entering: the SET reports to the SLP when it first detects that it is inside the predefined area. If repeated reporting is present, the SET then reports once more for each time it detects that it has re-entered the predefined area after having left in the meantime.
- Inside: the SET reports to the SLP when it is within the predefined area.
- Outside: the SET reports to the SLP when it is outside the predefined area.
- Leaving: the SET reports to the SLP when it first detects that it is outside the predefined area. If repeated reporting is present, the SET then reports once more for each time it detects that it has exited the predefined area after having been inside again.

Parameter	Presence	Value/Description
Area Event Type	M	Describes the area event trigger type. This parameter describes what kind of event should trigger a report. The valid types are: • Entering event type • Inside event type • Outside event type • Leaving event type
Location estimate	M	The value of this parameter is “true” or “false”. If true, it indicates the location estimates is required. If false, it indicates the location estimates is not required. For SET-Initiated triggered services this parameter is not useful and therefore in this case it SHALL be ignored by the SLP.
Repeated reporting	O	Defines the parameters for repeated reporting. If not present, only one report SHALL be sent. When repeated reporting is used, the SET and the SLP SHALL maintain the triggered event session until the maximum number of reports has been sent, the stop time (if included) has been reached, or either the SET or the SLP has sent a SUPL TRIGGERED STOP or a SUPL END to end the session.
>Minimum Interval Time	M	Defines the minimum time between reports from SET in an Area Event Trigger session. For repeated reporting, an area event trigger cannot be fulfilled unless the minimum time interval has elapsed since the last report. Range: (1..604800). Units in seconds.
>Maximum Number of Reports	M	Defines the maximum number of reports in an Area Event Trigger session. Range: (1..1024)

Start Time	O	Indicates the start of the period when the trigger condition is able to be fulfilled. Start Time is interpreted relative to the current time i.e. to the time when the message containing the parameter is received by the H-SLP or D-SLP or the SET. Start Time is OPTIONAL. If not present, a Start Time of 0 SHALL be used and the trigger condition is allowed to be fulfilled immediately. Units in seconds (range: 0 to 2678400).
Stop Time	O	Stop Time is interpreted relative to the current time i.e. to the time when the message containing the parameter is received by the H-SLP or D-SLP or the SET. It indicates when the SET shall stop the triggered session if it has not already been stopped for other reasons. The SET SHALL use a SUPL END message as defined in section 5.3.2.1, Figure 27 for Network Initiated sessions. For SET Initiated sessions, the SET SHALL use a SUPL END message as defined in section 5.3.4.1, Figure 31 . Stop Time is OPTIONAL. If not present, a Stop Time of 8639999 seconds after the start time SHALL be used. Stop Time SHALL be greater than Start Time (if present). Stop Time – Start Time SHALL NOT be more than 8639999 (100 days in seconds) Units in seconds (range: 0 to 11318399).
Geographic Target Area List	O	Defines a list of geographic target areas. This parameter is OPTIONAL. Maximum number of areas are according to element Max Geo Target Area in SET capabilities. If this parameter is not included in the SUPL TRIGGERED RESPONSE message the SET SHALL NOT use the Geographic Target Area List to check if the event trigger condition has been met.
> Geographic Target Area	M	Defines a geographic target area in terms of either: • CircularArea • EllipticalArea • Polygon

Area Id Lists	CV	This parameter contains one or more Area Id lists. This parameter is REQUIRED when the Geographic Target Area List is NOT present and is OPTIONAL when the Geographic Target Areas are present. The maximum number of Area Id lists to be included is determined by the element "Max Area Id List" in SET capabilities. NOTE: If this parameter is included in the SUPL TRIGGERED START message it is ignored by the SLP.
>Area Id list	M	Each Area Id list consists of a set of Areas Ids. If Geographic Target Area List is present then it may include a Geographic Area Mapping List.
>>Area Id Set	M	A list of area ids. The area ids listed can be any combination of GSM Area Ids, WCDMA/TD-SCDMA Area Ids, CDMA Area Ids, HRPD-Area Ids, LTE-Area Ids, WLAN Area Ids or WiMAX Area Ids. Each set can contain from 1 to [MaxAreaId] area ids. Note that if Area Ids of different bearer networks are provided, Border and Within lists can only be considered complete if the SET monitors each of the bearers.
>>Area Id Set Type	CV	This parameter indicates the position of the Area Id Set relative to the Geographic Target Area, This parameter can be of type • "Border" (of the Geographic Target Area) • "Within" (the Geographic Target Area) This parameter is conditional and may only be present when the Geographic Target Area List parameter is present. The "within" area id list is completely within the geographic target area and the "border" area id list combined with the "within" area id list SHOULD completely cover the geographic target area. Both area id lists are mutually exclusive. Using this parameter the SET may decide whether or not to use high precision positioning. (See Appendix B.7 for additional information).

>> Geographic Area Mapping List	O	Represents the Geographic Target Areas to which the Area Id list applies. (Example: 1,3,7,8). The number of entries can be from 1 to the number of Geographic Target Area elements The value of each entry can be from 1 to the number of Geographic Target Area elements.

Table 54: Area Event Parameters

10.25.2.2.1 GSM Area Id

Parameter	Presence	Value/Description
GSM Area Id	-	Can be of type: • Mobile Country Code • Mobile Country Code + Mobile Network Code • Mobile Country Code + Mobile Network Code +Location Area Code • Cell Global Identity

Table 55: GSM Area Id Parameter

10.25.2.2.2 WCDMA/TD-SCDMA Area Id

Parameter	Presence	Value/Description
WCDMA/TD-SCDMA Area Id	-	Can be of type: • Mobile Country Code • Mobile Country Code + Mobile Network Code • Mobile Country Code + Mobile Network Code +Location Area Code • Mobile Country Code + Mobile Network Code +Location Area Code + Cell Identity • Mobile Country Code + Mobile Network Code + Cell Identity

Table 56: WCDMA/TD-SCDMA Area Id Parameter

10.25.2.2.3 LTE Area Id

Parameter	Presence	Value/Description
LTE Area Id	-	Can be of type: • MCC • MCC+MNC • MCC+MNC+Tracking Area Code • MCC+MNC+Cell-ID

Table 57: LTE Area Id Parameter

10.25.2.2.4 CDMA Area Id

Parameter	Presence	Value/Description
CDMA Area Id	-	Can be of type: • System ID • System ID + Network ID • System ID + Network ID + Base ID

Table 58: CDMA Area Id Parameter

10.25.2.2.5 HRPD Area Id

Parameter	Presence	Value/Description
HRPD Area Id	-	Can be of type: • Sector ID

Table 59: HRPD Area Id Parameter

10.25.2.2.6 WLAN Area Id

Parameter	Presence	Value/Description
WLAN Area Id	-	Can be of type: • AP MAC Address

Table 60: WLAN Area Id Parameter

10.25.2.2.7 WiMAX Area Id

Parameter	Presence	Value/Description
WiMAX Area Id	-	Can be of type: • BS ID

Table 61: WiMAX Area Id Parameter

10.25.2.3 Velocity Event Params

This section describes the Velocity Event trigger Params. This parameter is required if trigger type is set to Velocity Event.

The Velocity Event trigger can be one of the following types:

- Increasing Above: the SET reports to the SLP when its speed increases above the target speed. If repeated reporting is enabled, the SET reports each time its speed increased above the target speed provided the minimum time between reports has elapsed (this implies that in between reports, the speed of the SET has decreased below the target speed).
- Above: the SET reports to the SLP when its speed is above the target speed. If repeated reporting is enabled, the SET reports each time its speed is above the target speed provided the minimum time between reports has elapsed since the last report.
- Decreasing Below: the SET reports to the SLP when its speed decreases below the target speed. If repeated reporting is enabled, the SET reports each time its speed decreases below the target speed provided the minimum time between reports has elapsed (this implies that in between reports, the speed of the SET has increased above the target speed).
- Below: the SET reports to the SLP when its speed is below the target speed. If repeated reporting is enabled, the SET reports each time its speed is below the target speed provided the minimum time between reports has elapsed since the last report.

Parameter	Presence	Value/Description
Velocity Event Type	M	Describes the velocity event trigger type. This parameter describes what kind of event should trigger a report. The valid types are: • Increasing Above • Above • Decreasing Below • Below
Velocity estimate	M	The value of this parameter is "true" or "false". If true, it indicates the velocity estimates is required. If false, it indicates the velocity estimates is not required. For SET-Initiated triggered services this parameter is not useful and therefore in this case it SHALL be ignored by the SLP. NOTE: Velocity is always reported as part of position.
Repeated reporting	O	Defines the parameters for repeated reporting. If not present, only one report SHALL be sent. When repeated reporting is used, the SET and the SLP SHALL maintain the triggered event session until the maximum number of reports has been sent, the stop time (if included) has been reached, or either the SET or the SLP has sent a SUPL TRIGGERED STOP or a SUPL END to end the session.
>Minimum Interval Time	M	Defines the minimum time between reports from the SET in a Velocity Event Trigger session. For repeated reporting, a velocity event trigger cannot occur unless the minimum time interval has elapsed since the last report. Range: (1..604800). Units in seconds.
>Maximum Number of Reports	M	Defines the maximum number of reports in a Velocity Event Trigger session. Range: (1..1024)
Start Time	O	Indicates the time the trigger is armed. Start Time is interpreted relative to the current time i.e. to the time when the message containing the parameter is received by the H-SLP or D-SLP or the SET. Start Time is OPTIONAL. If not present, a Start Time of 0 SHALL be used and the trigger is armed immediately. Units in seconds (range: 0 to 2678400).

Stop Time	O	Stop Time is interpreted relative to the current time i.e. to the time when the message containing the parameter is received by the H-SLP or D-SLP or the SET. It indicates when the SET shall stop the triggered session if it has not already been stopped for other reasons. The SET SHALL use a SUPL END message as defined in section 5.3.2.1, Figure 27 for Network Initiated sessions. For SET Initiated sessions, the SET SHALL use a SUPL END message as defined in section 5.3.4.1, Figure 31. Stop Time is OPTIONAL. If not present, a Stop Time of 8639999 seconds after the start time SHALL be used. Stop Time SHALL be greater than Start Time (if present). Stop Time – Start Time SHALL NOT be more than 8639999 (100 days in seconds) Units in seconds (range: 0 to 11318399).
Target Speed	O	The target speed (speed which triggers a velocity trigger event).

Table 62: Velocity Event Parameters

10.26 Notification Mode

Parameter	Presence	Value/Description
Notification Mode	-	Describes the mode whether the notification and verification is based on location or not. This parameter can be of type Normal Notification/Verification or Notification/Verification based on location

Table 63: Notification Mode Parameter

10.27 Notification Response

Parameter	Presence	Value/Description
Notification Response	-	Describes the notification/verification response from the user. The response can be either "allowed" or "not allowed"

Table 64: Notification Response Parameter

10.28 Third Party ID

Parameter	Presence	Value/Description
Third Party ID	CV	Indicates the identity of the third party. The type of the third party name can be one of the following: • Logical name • MSISDN • E-mail address • SIP URI • IMS public identity • MIN • MDN • URI

Table 65: Third party ID Parameter

10.29 Historic Reporting

Parameter	Presence	Value/Description
Historic Reporting	-	This parameter defines the criteria for reporting of stored historical position estimates and/or enhanced cell/sector measurements.
>Allowed Reporting Type	M	This parameter defines what types of stored historical information the SET is allowed to report: • Position estimates only • Enhanced cell/sector measurements only • Both position estimates and enhanced cell/sector measurements
>Reporting Criteria	O	This parameter defines the criteria used to select stored historical position and/or enhanced cell/sector measurements for reporting. If this parameter is absent, no criteria apply and all stored historical data consistent with *allowed reporting typ* and *QoP* is reported by the SET up to a maximum number of 1024 reports.

>>Time Window	O	The *Time Window* parameter specifies a time window to be applied to all reported position estimates and/or enhanced cell/sector measurements. If present, the SET is only allowed to report stored historical position estimates and/or enhanced cell/sector measurements which fall within the time window. If not present, no time window applies. If no time window is specified, the SET SHALL report all stored data consistent with other selection criteria (*allowed reporting type, QoP, etc.*).
>>>Start Time	M	The time window's start time. The start time is defined as relative time delta to the current time at the SET. Start time is a negative value (historical data) with a range of -525,600 to 1. The unit is in minutes i.e. the start time is up to one year in the past.
>>>Stop Time	O	The time window's stop time. If not present, the SET SHALL send ALL stored historical position estimates and/or enhanced cell/sector measurements (consistent with other selection criteria i.e. *allowed reporting type, QoP*) beginning at Start Time. Stop time is defined as relative time to current time. Stop time must be AFTER start time. Stop time is a negative value (historical data) with a range of -525,599 to 0. The unit is in minutes.
>>Max Number of Reports	O	This parameter defines the maximum number of reports allowed to be reported by the SET. This parameter is optional. If not present, an implicit maximum number of reports of 1024 applies. The data range is 1 to 65536.
>>Minimum Time Interval	O	This parameter defines the minimum time interval between reported positions and/or enhanced cell/sector measurements. This parameter is optional. If not used, no minimum time interval exists. This parameter has a range of 1 to 86,400 in units of one second i.e. the maximum minimum time interval between historical data reports is 24 hours.

Table 66: Historic Reporting Parameter

10.30 Protection Level

The Protection Level parameter defines the level of protection for the SUPL INIT/SUPL REINIT message.

Parameter	Presence	Value/Description
Protection Level	-	This parameter defines the protection level of the SUPL INIT/SUPL REINIT protection. This parameter is optional. If not present, Null protection is assumed.
> Level	M	• Null Protection • Basic Protection (not applicable in SUPL 3.0 i.e., the SLP SHALL NOT select this protection level) • Mode A Protection • Mode B Protection
> Basic Protection Parameters	CV	This parameter is only present if the protection level is *Basic Protection*. • Key-Identifier (= B-TID) • Basic Replay Counter • Basic MAC This parameter SHALL NOT be used since Basic Protection is not supported in SUPL 3.0.
> Protection Parameter	CV	This value is only present if protection level is Mode A Protection or Mode B Protection. • Key Identifier Type o ModeAKeyIdentifier o TemporaryModeAKeyIdentifier o ModeBKeyIdentifier • Key Identifier • Basic Replay Counter • Basic MAC Note that the Key Identifier comes in three different Types (Key Identifier Type): (1) ModeAKeyIdentifier, (2) TemporaryModeAKeyIdentifier and (3) ModeBKeyIdentifier. (1) and (2) apply to Mode A Protection whereas (3) applies to Mode B Protection.

Table 67: Protection Level Parameter

10.31 GNSS Positioning Technology

Parameter	Presence	Value/Description
GNSS Positioning Technology	-	Bitmap of GNSS Positioning Technology. This bitmap indicates the GNSS used or to be used for the positioning computation: • GPS • Galileo • SBAS • Modernized GPS • QZSS • GLONASS When a Bit is set to FALSE: not used, when set to TRUE: used. NOTE: This parameter SHALL NOT be used if posmethod indicates A-GPS or autonomous GPS.

Table 68: GNSS Positioning Technology

10.32 Target SET ID

Parameter	Presence	Value/Description
Target SET ID	-	Target SET identity value. This parameter can be of type • MSISDN • MDN • MIN • IMSI • NAI • IPAddress o IPv4 o IPv6

Table 69: Target SET ID

10.33 Application ID

The Application ID parameter is used to pass information about the end application performing a location request to the SLP. This information is useful for gathering application usage statistical information. Application ID includes the application provider name, application name and optionally the application version. Application ID should only be included on SET Initiated use cases where the SLP is accessed.

Parameter	Presence	Value/Description
Application ID	O	Indicates the application ID for SET initiated call flows.
>App Provider	M	The application provider.
>App Name	M	The application name.
>App Version	O	The application version.

Table 70: Application ID Parameter

10.34 SLP Capabilities

The SLP Capabilities parameter is used to describe the SLP's capabilities to the SET.

Parameter	Presence	Value/Description
SLP Capabilities	-	Indicates the capabilities of the SLP
>Pos Protocol Supported	M	The supported positioning protocol: • LPP • LPPe • TIA-801
>Pos Protocol Version LPP	CV	Describes the protocol version of LPP Positioning Protocol. It is required if LPP is identified in the Pos Protocol parameter.
>>Major Version Field	M	First (most significant) element of the version number for LPP Positioning Protocol, range: (0..255)
>>Technical Version Field	M	Second element of the version number for LPP Positioning Protocol, range: (0..255)
>>Editorial Version Field	M	Third (least significant) element of the version number for LPP Positioning Protocol, range: (0..255)
>Pos Protocol Version LPPe	CV	Describes the protocol version of LPPe Positioning Protocol. It is required if LPPe is identified in the Pos Protocol parameter.
>>Major Version Field	M	First (most significant) element of the version number for LPPe Positioning Protocol, range: (0..255)
>>Minor Version Field	M	Second element of the version number for LPPe Positioning Protocol, range: (0..255)
>Pos Protocol Version TIA-801	CV	Describes the protocol version of 3GPP2 C.S0022 (TIA-801) Positioning Protocol. It is required if TIA-801 is identified in the Pos Protocol parameter.
>>Supported Pos Protocol Version TIA-801	M	Specifies a list of up to 8 different supported 3GPP2 C.S0022 versions. This parameter is required (with at least one entry in the list) if TIA-801 is identified in the Pos Protocol parameter.

>>>Revision Number	M	Revision part of document number for the specifications of C.S0022 Positioning Protocol. Value: [0,A-Z]
>>>Point Release Number	M	Point Release number for C.S0022, range: (0..255)
>>Internal Edit Level	M	Internal Edit Level for C.S0022, range: (0..255)
>QoP Capabilities	O	This parameter defines the ability of the SLP for reporting and/or receiving high accuracy position and/or velocity results.
>Civic Position Capabilities	O	This parameter defines the ability of the SLP to perform civic positioning.
>Relative Position Capabilities	O	This parameter defines the ability of the SLP to perform relative positioning.
>Location URI Capabilities	O	This parameter defines the ability of the SLP to support location URI.

Table 71: SLP Capabilities Parameter

10.35 GSS Parameters

The GSS Parameters parameter is used to describe the parameters used for a GSS.

Parameter	Presence	Value/Description
GSS Parameters	-	Defines the parameters to be used for GSS.
>Duration	M	Defines the duration of a GSS in terms of: (1) Time (2) Number of SUPL POS messages allowed within one GSS as one of the following options a. Uplink b. Downlink c. Uplink + Downlink The duration of a GSS can be defined in terms of (1) Time only, (2) Number of SUPL POS messages only or a combination of (1) and (2) (whichever is reached first).

Table 72: GSS Parameters

10.36 Location URI Set

The Location URI Set parameter provides one or more location URIs each of which is a URI, as defined in [RFC 3986], that references a means to obtain the location of the SET from a particular location server that initially created the location URI. The location server may be a SUPL SLP or some other type of server and is identified within the location URI. The dereferencing protocol used to obtain the SET location using the location URI (e.g. via a query/response operation) is similarly defined within the location URI according to [RFC 3986] and is out of scope of SUPL 3.0. Possible examples include SIP SUBSCRIBE/NOTIFY [RFC 3856] and some extension of HELD [RFC 5985]. In creating a Location URI Set, an SLP MAY include one location URI for each location dereferencing protocol that it supports.

Parameter	Presence	Value/Description
Location URI Set	-	Provides a set of location URIs
> Location URI List	M	Provides a list of one or more location URIs
>> Location URI	M	Provides a single location URI as a visible character string conforming to [RFC 3986].
> Validity Period	O	Provides the length of time (or remaining length of time) in minutes during which each location URI will be valid

Table 73: Location URI Set Parameter

10.37 Location URI Request

The Location URI Request parameter contains a request from a SET for a location URI from an SLP.

Parameter	Presence	Value/Description
Location URI Request	-	Provides a request for a location URI
> Reason	M	Provides the reason for requesting a location URI. Possible values are: a. Location support for an emergency session b. Location support for H-SLP c. Undefined
> Validity Period	O	Provides the requested minimum length of time in minutes during which the location URI will be valid

Table 74: Location URI Request Parameter

10.38 Extended Notification

The Extended Notification parameter provides additional notification information to a SET for a network initiated SUPL session.

Parameter	Presence	Value/Description
Extended Notification	-	

> Location URI	CV	Indicates that SET location is being obtained by the SLP as a consequence of receiving a location request containing the indicated location URI. Required if the same location URI was previously transferred to the SET by the SLP. If the SET had previously forwarded the location URI to another entity in a secure manner (e.g. the H-SLP or an external SUPL Agent), the SET can then know that its location is being requested by this entity.

Table 75: Extended Notification Parameter

10.39 SLP Query

The SLP Query parameter is used to request a list of authorized D-SLP and/or E-SLP addresses, from the H-SLP, a proxy D-SLP or a proxy E-SLP, that are applicable to the current SET location and/or serving access network.

Parameter	Presence	Value/Description
SLP Query	-	Requests provision of one or more D-SLP and/or E-SLP addresses.
> D-SLP Query	O	This parameter SHALL be included in a request for authorized D-SLP addresses.
>> Authorized D-SLP Address List	CV	This parameter provides a list of the addresses of any D-SLPs previously authorized by the SLP to which the SLP Query is sent.
>> Preferred D-SLP Address List	O	This parameter provides a list of any D-SLP addresses preferred by the SET. This list may include addresses of previously authorized D-SLPs and/or addresses of new D-SLPs discovered by the SET.
>> Not preferred D-SLP Addresses	O	This parameter provides a list of any D-SLP addresses not preferred by the SET. This list may include addresses of previously authorized D-SLPs (e.g. that were not able to provide adequate service).
>> QoP	O	This parameter indicates which QoP is requested. This parameter may be used by the SLP to authorize D-SLPs.
> E-SLP Query	O	This parameter SHALL be included in a request for authorized E-SLP addresses.
>> Authorized E-SLP Address List	CV	This parameter provides a list of the addresses of any E-SLPs previously authorized by the SLP to which the SLP Query is sent.

>> Preferred E-SLP Address List	O	This parameter provides a list of any E-SLP addresses preferred by the SET. This list may include addresses of previously authorized E-SLPs and/or addresses of new E-SLPs discovered by the SET.
>> Not preferred E-SLP Addresses	O	This parameter provides a list of any E-SLP addresses not preferred by the SET. This list may include addresses of previously authorized E-SLPs (e.g. that were not able to provide adequate service).

Table 76: SLP Query Parameter

10.40 SLP Authorization

The SLP Authorization parameter is used to provide one or more authorized D-SLP and/or E-SLP addresses and provide optional limitations on the use of these addresses.

Parameter	Presence	Value/Description
SLP Authorization	-	Provides one or more authorized D-SLP and/or E-SLP Addresses.
> D-SLP Authorization List	CV	This parameter is included to provide one or more authorized D-SLP addresses and associated conditions for accessing each address. D-SLP addresses are provided in priority order (highest priority first) where a higher priority D-SLP shall be accessed by the SET in preference to a lower priority D-SLP when associated service area and access network conditions are satisfied. In a response to a SET request for D-SLP addresses, the absence of this parameter or the presence of this parameter containing no D-SLP addresses indicates no D-SLPs are authorized: any D-SLPs previously authorized by the SLP sending the response shall then be considered de-authorized by the SET with any associated SUPL sessions in progress being terminated by the SET with a SUPL END message. If a previously authorized Proxy D-SLP is thereby de-authorized, any D-SLPs authorized by the Proxy D-SLP are also de-authorized.
>> D-SLP List	M	This parameter provides the authorized D-SLP addresses and conditions for accessing each address.
>>> D-SLP Address	M	This field provides an authorized D-SLP address in the form of an FQDN.

>>> **Service Duration**	O	This parameter provides the duration of the D-SLP authorization. If this parameter is absent, the duration is unlimited.
>>> **Service Area**	O	This parameter provides one or more service areas within which the authorized D-SLP may be accessed. The service area consists of the geographic area list, and optionally area ids. If this parameter is absent, no service area is explicitly authorized though access to the D-SLP may still be permitted via the Access Network List.
>>>> **Geographic Area List**	M	Defines a list of geographic areas. Maximum number of areas are according to element Max Geo Target Area in SET capabilities.
>>>>> **Geographic Area**	M	Defines a geographic area in terms of either: • CircularArea • EllipticalArea • Polygon
>>>> **Area Id Area Lists**	O	This parameter contains one or more Area Id lists. This parameter is optional. The maximum number of Area Id lists to be included is determined by the element “Max Area Id List” in SET capabilities.
>>>>> **Area Id list**	M	Each Area Id list consists of a set of Areas Ids. It MAY include a Geographic Area Mapping List.
>>>>>> **Area Id Set**	M	A list of area ids. The area ids listed can be any combination of GSM Area Ids, WCDMA/TD-SCDMA Area Ids, CDMA Area Ids, HRPD-Area Ids, UMB-Area Ids, LTE-Area Ids, WLAN Area Ids or WiMAX Area Ids. Each set can contain from 1 to [MaxAreaId] area ids. Note that if Area Ids of different bearer networks are provided, Border and Within lists can only be considered complete if the SET monitors each of the bearers.

>>>>>> **Area Id Set Type**	O	This parameter indicates the position of the Area Id Set relative to the Geographic Area, This parameter can be of type • "Border" (of the Geographic Area) • "Within" (the Geographic Area) The "within" area id list is completely within the geographic area and the "border" area id list combined with the "within" area id list SHOULD completely cover the geographic area. Both area id lists are mutually exclusive. Using this parameter the SET may decide whether or not to use high precision positioning. (See Appendix H for additional information).
>>>>>> **Geographic Area Mapping List**	O	Represents the Geographic Areas to which the Area Id list applies. (Example: 1,3,7,8). The number of entries can be from 1 to the number of Geographic Area elements. The value of each entry can be from 1 to the number of Geographic Area elements.
>>> **Access Network List**	O	This parameter provides a list of access networks from which the authorized D-SLP address may be accessed. If this parameter is absent, no access networks are explicitly authorized though access to the D-SLP may still be permitted via the Service Area.

>>> **Combination Type**	O	This parameter defines how the Service Area and Access Network List restrictions are combined. The alternatives are: • AND (SET must be within the service area AND using an allowed access network) • OR (SET must be within the service area OR using an allowed access network) • Conditional OR (SET must be within the service area. If the SET cannot determine whether it is within the service area, the SET must use an allowed access network) The default if this parameter is not included is OR.
>>> **Services**	O	This parameter provides a list of services that a SET may engage in with the authorized D-SLP. Allowed services are indicated by a Boolean TRUE value and disallowed services are indicated by FALSE values. A SET SHALL not request or accept a request for any disallowed service. This parameter SHALL NOT be included for a D-SLP authorized by a Proxy D-SLP and SHALL be ignored if included. If this parameter is absent for an authorization received from the H-SLP, all services are allowed. In the case of authorization by a Proxy D-SLP, the services allowed for the D-SLP being authorized are the same as those authorized by the H-SLP for the Proxy D-SLP.
>>> **Proxy D-SLP**	CV	This parameter is conditional and may only be sent by the H-SLP. This presence of this parameter indicates that the D-SLP can act as a proxy for the H-SLP to provide authorized D-SLP addresses to the SET. Any D-SLP addresses provided by a Proxy D-SLP remain associated with the Proxy D-SLP – e.g. the addresses are removed once the duration of the authorization for the Proxy D-SLP (provided by the H-SLP) expires.

>> H-SLP Access Preference	CV	This parameter is conditional and may only be sent by the H-SLP. This parameter indicates whether the H-SLP may be accessed by the SET instead of a D-SLP for SET initiated location services. The following values are supported: • Access to H-SLP not allowed • Access to H-SLP not preferred (H-SLP to be used as a backup) • Access to H-SLP preferred (D-SLP to be used as a backup) Absence of the parameter means there is no preference and the SET may access either the H-SLP or a D-SLP. NOTE: Existing H-SLP sessions SHALL not be affected by this parameter.
>> Report D-SLP Access	CV	This parameter is conditional and may only be sent by the H-SLP. This parameter is included to request notification from the SET to the H-SLP when the SET changes access to a different D-SLP. The notification can be restricted just to D-SLPs authorized to perform network initiated services. The notification can also be extended to D-SLPs authorized by a Proxy D-SLP. The notification can assist the H-SLP to redirect or forward location requests for the SET from external SUPL Agents to the most recently notified D-SLP.
>>> Include Proxy D-SLP Authorized D-SLPs	M	This parameter indicates whether D-SLPs authorized by a Proxy D-SLP that supports Network Initiated services shall be notified to the H-SLP (TRUE) or not (FALSE) in addition to D-SLPs directly authorized by the H-SLP.

> **E-SLP Authorization List**	CV	This parameter is included to provide one or more authorized E-SLP addresses and associated conditions for accessing each address. E-SLP addresses are provided in priority order (highest priority first) where a higher priority E-SLP shall be accessed by the SET in preference to a lower priority E-SLP when associated service area and access network conditions are satisfied. In a response to a SET request for E-SLP addresses, the absence of this parameter or the presence of this parameter containing no E-SLP addresses indicates no E-SLPs are authorized: any E-SLPs previously authorized by the SLP sending the response shall then be considered de-authorized by the SET with any associated SUPL sessions in progress being terminated by the SET by sending a SUPL END. If a previously authorized Proxy E-SLP is thereby deauthorized, any E-SLPs authorized by the Proxy E-SLP are also de-authorized. Exceptions to these rules may exist according to local regulatory requirements – e.g. a SET may accept a Network Initiated request for a single fix from an E-SLP when engaged in an emergency call regardless of whether the E-SLP was or was not authorized by the H-SLP.
>> **E-SLP List**	M	This parameter provides the authorized E-SLP addresses and conditions for accessing each address.
>>> **E-SLP Address**	M	This field provides an authorized E-SLP address in the form of an FQDN.
>>> **Service Duration**	O	This parameter provides the duration of the E-SLP authorization. If this parameter is absent, the duration is unlimited.
>>> **Service Area**	O	This parameter provides a geographic area within which the authorized E-SLP may be accessed. If this parameter is absent, no service area is explicitly authorized though access to the E-SLP may still be permitted via the Access Network List.

>>> **Access Network List**	O	This parameter provides a list of access networks from which the authorized E-SLP address may be accessed. If this parameter is absent, no access networks are explicitly authorized though access to the E-SLP may still be permitted via the Service Area.
>>> **Combination Type**	O	This parameter defines how the Service Area and Access Network List restrictions are combined. The alternatives are: • AND (UE must be within the service area AND using an allowed access network) • OR (UE must be within the service area OR using an allowed access network) • Conditional OR (UE must be within the service area. If the UE cannot determine whether it is within the service area, the UE must use an allowed access network) The default if this parameter is not included is OR.
>>> **Proxy E-SLP**	CV	This parameter is conditional and may only be sent by the H-SLP. This presence of this parameter indicates that the E-SLP can act as a proxy for the H-SLP to provide authorized E-SLP addresses to the SET. Any E-SLP addresses provided by a Proxy E-SLP remain associated with the Proxy E-SLP – e.g. the addresses are removed once the duration of the authorization for the Proxy E-SLP (provided by the H-SLP) expires.
> **Minimum retry period**	O	This parameter provides the minimum time period that the SET must wait before instigating a new D-SLP or E-SLP Authorization request. The parameter is valid in both a response to a SET SLP Authorization request and in an unsolicited SLP Authorization (e.g. for the Session Info Query procedure or in the SUPL END sent by the H-SLP or by a Proxy D-SLP or E-SLP for any SUPL session). The parameter only applies to the SLP that sent it – e.g. the minimum retry period for a Proxy D-SLP does not affect requests to the H-SLP and vice versa.

Table 77: SLP Authorization Parameter

10.41 Authorized D-SLP List

The Authorized D-SLP List parameter is used to provide any currently authorized D-SLP addresses to the H-SLP or to a Proxy D-SLP.

Parameter	Presence	Value/Description
Authorized D-SLP List	-	• Provides currently authorized D-SLP addresses
> Authorized D-SLP	M	• Provides a list of D-SLPs currently authorized by the SLP to which this parameter is sent.
>> D-SLP Address	O	• This parameter provides a D-SLP address in the form of an FQDN.
>> proxy Authorized D-SLP List	O	• This parameter may be sent to an H-SLP when the Authorized D-SLP is a Proxy D-SLP and provides a list of any D-SLPs currently authorized by the Proxy D-SLP.

Table 78: Authorized D-SLP List Parameter

10.42 Authorized E-SLP List

The Authorized E-SLP List parameter is used to provide any currently authorized E-SLP addresses to the H-SLP.

Parameter	Presence	Value/Description
Authorized E-SLP List	-	• Provides currently authorized E-SLP addresses
> Authorized E-SLP	M	• Provides a list of E-SLPs currently authorized by the SLP to which this parameter is sent.
>> E-SLP Address	O	• This parameter provides an E-SLP address in the form of an FQDN.
>> proxy Authorized E-SLP List	O	• This parameter may be sent to an H-SLP when the Authorized E-SLP is a Proxy E-SLP and provides a list of any E-SLPs currently authorized by the Proxy E-SLP.

Table 79: Authorized E-SLP List Parameter

10.43 D-SLP Access Notification

The D-SLP Access Notification parameter is used to provide the address of a recently accessed D-SLP to the H-SLP when the D-SLP is authorized to support Network Initiated services.

Parameter	Presence	Value/Description
D-SLP Access Report	-	• Provides the most recently accessed D-SLP

> D-SLP Address	O	• This parameter provides the D-SLP address in the form of an FQDN.

Table 80: Authorized D-SLP Access Notification Parameter

10.44 Relative Position

The Relative Position Parameter provides a position relative to some known reference position or another SET. The parameter is defined in [OMA-LPPe].

10.45 Reference Point Id

The Reference Point Id provides a unique Id of a reference point as per [OMA-LPPe].

10.46 High Accuracy QoP

Parameter	Presence	Value/Description
High Accuracy QoP	-	Describes the desired High Quality of Position.
>Horizontal accuracy	M	Horizontal accuracy as defined in [OMA LPPe] "*uncertainty-semimajor*"
>Vertical accuracy	O	Vertical accuracy as defined in [OMA LPPe] "*uncertainty-altitude*"
> Maximum Location Age	O	Maximum tolerable age of position estimates used for cached position fixes. Units in seconds from 0 to 65535.
>Delay	O	From (1..256), units in seconds. NOTE: The Delay value should be applied to the timer of the used positioning protocol.
>Requested Velocity	O	Flag, indicating whether velocity estimates shall use the high accuracy format. If set to "true", the high accuracy velocity format shall be used if supported and applicable. If set to "false" the high accuracy velocity format shall not be used.

Table 81: High Accuracy QoP

10.47 Civic Position

The Civic Position Parameter provides a position according to civic address. The parameter is defined in [OMA-LPPe].

10.48 SUPL INIT Key Response

The SUPL INIT Key Response parameter is used in the SUPL_INIT_ROOT_KEY Establishment procedure (see section 6.3.5.2) to send Keys for Mode A SUPL INIT Protection from the SLP to the SET.

Parameter	Presence	Value/Description
SUPL INIT Key Response	-	Used in the Mode A SUPL_INIT_ROOT_KEY Establishment Procedure (section 6.3.5.2) and the Mode A Resynchronization Procedure (section 6.3.5.3)
> Mode A Key Establishment	CV	This parameter is conditional and SHALL be sent in case of Mode A SUPL_INIT_ROOT_KEY Establishment Procedure
> >Mode A Key Identifier	M	This parameter represents the *ModeAKeyIdentifier* (see section 6.3.5.1)
>>Temporary Mode A Key Identifier	M	This parameter represents the *TemporaryModeAKeyIdentifier* (see section 6.3.5.1)
>> SUPL_INIT_ROOT_KEY	M	This parameter represents the SUPL_INIT_ROOT_KEY used for SUPL Init Protection.
>> Mode A Key Lifetime	M	This parameter represents the ModeAKeyLifetime parameter which defines the time when the SUPL_INIT_ROOT_KEY ceases being valid. The lifetime value is expressed in UTC time.
> Mode A Resync	CV	This parameter is conditional and SHALL be sent in case of Mode A Resynchromization Procedure.
>> Mode A Key Identifier	M	This parameter represents the *ModeAKeyIdentifier* (see section 6.3.5.1)
>> Temporary Mode A Key Identifier	M	This parameter represents the *TemporaryModeAKeyIdentifier* (see section 5.3.5.1)

Table 82: SUPL INIT Key Response

11. ASN.1 Encoding of ULP Messages (Normative)

This section defines the ULP messages and common elements with ASN.1 (Normative).

Many ULP parameters used in SUPL 1.0 and/or SUPL 2.0 no longer apply or require setting to a fixed value. For ASN.1 code backwards compatibility, these now superfluous parameters remain in the ASN.1 definitions of the sections in this chapter. Please refer to chapter 10 for the definition of parameter applicability.

11.1 Common Part

```
ULP DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

IMPORTS
        Version, SessionID
FROM ULP-Components
        SUPLINIT
FROM SUPL-INIT
        SUPLSTART
FROM SUPL-START
        SUPLRESPONSE
FROM SUPL-RESPONSE
        SUPLPOSINIT
FROM SUPL-POS-INIT
        SUPLPOS
FROM SUPL-POS
        SUPLEND
FROM SUPL-END
        SUPLAUTHREQ
FROM SUPL-AUTH-REQ
        SUPLAUTHRESP
FROM SUPL-AUTH-RESP
        Ver2-SUPLTRIGGEREDSTART
FROM SUPL-TRIGGERED-START
        Ver2-SUPLTRIGGEREDRESPONSE
FROM SUPL-TRIGGERED-RESPONSE
        Ver2-SUPLREPORT
FROM SUPL-REPORT
        Ver2-SUPLTRIGGEREDSTOP
FROM SUPL-TRIGGERED-STOP
        Ver2-SUPLSETINIT
FROM SUPL-SET-INIT
        Ver2-SUPLNOTIFY
FROM SUPL-NOTIFY
        Ver2-SUPLNOTIFYRESPONSE
FROM SUPL-NOTIFY-RESPONSE
        Ver3-SUPLREINIT
FROM SUPL-REINIT;

-- general ULP PDU layout;--
ULP-PDU ::= SEQUENCE {
  length     INTEGER(0..65535),
  version    Version,
  sessionID  SessionID,
  message    UlpMessage}

UlpMessage ::= CHOICE {
```

```
  msSUPLINIT      SUPLINIT,
  msSUPLSTART     SUPLSTART,
  msSUPLRESPONSE  SUPLRESPONSE,
  msSUPLPOSINIT   SUPLPOSINIT,
  msSUPLPOS       SUPLPOS,
  msSUPLEND       SUPLEND,
  msSUPLAUTHREQ   SUPLAUTHREQ,
  msSUPLAUTHRESP  SUPLAUTHRESP,
 ...,
  msSUPLTRIGGEREDSTART            Ver2-SUPLTRIGGEREDSTART,
  msSUPLTRIGGEREDRESPONSE         Ver2-SUPLTRIGGEREDRESPONSE,
  msSUPLTRIGGEREDSTOP             Ver2-SUPLTRIGGEREDSTOP,
  msSUPLNOTIFY                    Ver2-SUPLNOTIFY,
  msSUPLNOTIFYRESPONSE            Ver2-SUPLNOTIFYRESPONSE,
  msSUPLSETINIT                   Ver2-SUPLSETINIT,
  msSUPLREPORT                    Ver2-SUPLREPORT,
  msSUPLREINIT                    Ver3-SUPLREINIT}

END
```

11.2 Message Specific Part

11.2.1 SUPL INIT

```
SUPL-INIT DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

EXPORTS SUPLINIT, Notification;

IMPORTS
        SLPAddress, QoP, PosMethod
FROM ULP-Components
        Ver2-SUPL-INIT-extension
FROM ULP-Version-2-message-extensions
        Ver2-Notification-extension
FROM ULP-Version-2-parameter-extensions
        Ver3-SUPL-INIT-extension
FROM ULP-Version-3-message-extensions;

SUPLINIT ::= SEQUENCE {
  posMethod     PosMethod,
  notification  Notification OPTIONAL,
  sLPAddress    SLPAddress OPTIONAL,
  qoP           QoP OPTIONAL,
  sLPMode       SLPMode,
  mAC           MAC OPTIONAL, -- included for backwards compatibility
  keyIdentity   KeyIdentity OPTIONAL, -- included for backwards compatibility
  ...,
-- version 2 extension element
  ver2-SUPL-INIT-extension        Ver2-SUPL-INIT-extension OPTIONAL,
-- version 3 extension element
  ver3-SUPL-INIT-extension        Ver3-SUPL-INIT-extension OPTIONAL}

Notification ::= SEQUENCE {
  notificationType  NotificationType,
  encodingType      EncodingType OPTIONAL,
  requestorId       OCTET STRING(SIZE (1..maxReqLength)) OPTIONAL,
  requestorIdType   FormatIndicator OPTIONAL,
```

```
  clientName        OCTET STRING(SIZE (1..maxClientLength)) OPTIONAL,
  clientNameType    FormatIndicator OPTIONAL,
  ...,
  ver2-Notification-extension      Ver2-Notification-extension OPTIONAL}

NotificationType ::= ENUMERATED {
  noNotificationNoVerification(0), notificationOnly(1),
  notificationAndVerficationAllowedNA(2),
  notificationAndVerficationDeniedNA(3), privacyOverride(4), ...}

EncodingType ::= ENUMERATED {ucs2(0), gsmDefault(1), utf8(2), ...}

maxReqLength INTEGER ::= 50

maxClientLength INTEGER ::= 50

FormatIndicator ::= ENUMERATED {
  logicalName(0), e-mailAddress(1), msisdn(2), url(3), sipUrl(4), min(5),
  mdn(6), iMSPublicidentity(7), ...}

SLPMode ::= ENUMERATED {proxy(0), nonProxy(1)}

MAC ::= BIT STRING(SIZE (64)) -- empty placeholder required for SUPL 1.0
backwards compatibility

KeyIdentity ::= BIT STRING(SIZE (128)) -- empty placeholder required for SUPL
1.0 backwards compatibility

END
```

11.2.2 SUPL START

```
SUPL-START DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

EXPORTS SUPLSTART, SETCapabilities;

IMPORTS
        LocationId, QoP
FROM ULP-Components
        Ver2-SUPL-START-extension
FROM ULP-Version-2-message-extensions
        Ver2-SETCapabilities-extension, Ver2-PosProtocol-extension, Ver2-
PosTechnology-extension
FROM ULP-Version-2-parameter-extensions
        Ver3-SUPL-START-extension
FROM ULP-Version-3-message-extensions
        Ver3-PosProtocol-extension
FROM ULP-Version-3-parameter-extensions
        Ver3-SETCapabilities-extension
FROM ULP-Version-3-parameter-extensions;

SUPLSTART ::= SEQUENCE {
  sETCapabilities  SETCapabilities,
  locationId       LocationId,
  qoP              QoP OPTIONAL,
  ...,
-- version 2 extension element
  ver2-SUPL-START-extension       Ver2-SUPL-START-extension OPTIONAL,
```

```
-- version 3 extension element
  ver3-SUPL-START-extension        Ver3-SUPL-START-extension OPTIONAL}

SETCapabilities ::= SEQUENCE {
  posTechnology  PosTechnology,
  prefMethod     PrefMethod,
  posProtocol    PosProtocol,
  ...,
  ver2-SETCapabilities-extension   Ver2-SETCapabilities-extension OPTIONAL,
  ver3-SETCapabilities-extension   Ver3-SETCapabilities-extension OPTIONAL}

PosTechnology ::= SEQUENCE {
  agpsSETassisted  BOOLEAN,
  agpsSETBased     BOOLEAN,
  autonomousGPS    BOOLEAN,
  aFLT             BOOLEAN,
  eCID             BOOLEAN,
  eOTD             BOOLEAN,
  oTDOA            BOOLEAN,
  ...,
  ver2-PosTechnology-extension     Ver2-PosTechnology-extension OPTIONAL}

PrefMethod ::= ENUMERATED {
  agpsSETassistedPreferred, agpsSETBasedPreferred, noPreference}
-- To achieve compatibility  with ULP V1.0 the names of the enumerations are
-- kept the same as in ULP V1.0. agps shall be interpreted as agnss.

PosProtocol ::= SEQUENCE {
  tia801  BOOLEAN,
  rrlp    BOOLEAN,
  rrc     BOOLEAN,
  ...,
  ver2-PosProtocol-extension       Ver2-PosProtocol-extension OPTIONAL,
  ver3-PosProtocol-extension       Ver3-PosProtocol-extension OPTIONAL}

END
```

11.2.3 SUPL RESPONSE

```
SUPL-RESPONSE DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

EXPORTS SUPLRESPONSE;

IMPORTS
        PosMethod, SLPAddress
FROM ULP-Components
        Ver2-SUPL-RESPONSE-extension
FROM ULP-Version-2-message-extensions
        Ver3-SUPL-RESPONSE-extension
FROM ULP-Version-3-message-extensions;

SUPLRESPONSE ::= SEQUENCE {
  posMethod     PosMethod,
  sLPAddress    SLPAddress OPTIONAL,
  sETAuthKey    SETAuthKey OPTIONAL, -- included for backwards compatibility
  keyIdentity4  KeyIdentity4 OPTIONAL, -- included for backwards compatibility
  ...,
-- version 2 extension element
```

```
  ver2-SUPL-RESPONSE-extension     Ver2-SUPL-RESPONSE-extension OPTIONAL,
-- version 3 extension element
  ver3-SUPL-RESPONSE-extension     Ver3-SUPL-RESPONSE-extension OPTIONAL}

SETAuthKey ::= CHOICE {
  shortKey  BIT STRING(SIZE (128)),
  longKey   BIT STRING(SIZE (256)),
  ...}

KeyIdentity4 ::= BIT STRING(SIZE (128))

END
```

11.2.4 SUPL POS INIT

```
SUPL-POS-INIT DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

EXPORTS SUPLPOSINIT;

IMPORTS
        SUPLPOS
FROM SUPL-POS
        SETCapabilities
FROM SUPL-START
        LocationId, Position, Ver
FROM ULP-Components
        Ver2-SUPL-POS-INIT-extension
FROM ULP-Version-2-message-extensions
        Ver2-RequestedAssistData-extension
FROM ULP-Version-2-parameter-extensions
        Ver3-SUPL-POS-INIT-extension
FROM ULP-Version-3-message-extensions;

SUPLPOSINIT ::= SEQUENCE {
  sETCapabilities      SETCapabilities,
  requestedAssistData  RequestedAssistData OPTIONAL,
  locationId           LocationId,
  position             Position OPTIONAL,
  sUPLPOS              SUPLPOS OPTIONAL,
  ver                  Ver OPTIONAL,
  ...,
-- version 2 extension element
  ver2-SUPL-POS-INIT-extension     Ver2-SUPL-POS-INIT-extension OPTIONAL,
-- version 3 extension element
  ver3-SUPL-POS-INIT-extension     Ver3-SUPL-POS-INIT-extension OPTIONAL}

RequestedAssistData ::= SEQUENCE {
  almanacRequested                BOOLEAN,
  utcModelRequested               BOOLEAN,
  ionosphericModelRequested       BOOLEAN,
  dgpsCorrectionsRequested        BOOLEAN,
  referenceLocationRequested      BOOLEAN, -- Note: Used also for GANSS
  referenceTimeRequested          BOOLEAN,
  acquisitionAssistanceRequested  BOOLEAN,
  realTimeIntegrityRequested      BOOLEAN,
  navigationModelRequested        BOOLEAN,
  navigationModelData             NavigationModel OPTIONAL,
  ...,
```

```
  ver2-RequestedAssistData-extension Ver2-RequestedAssistData-extension
OPTIONAL}

NavigationModel ::= SEQUENCE {
  gpsWeek   INTEGER(0..1023),
  gpsToe    INTEGER(0..167),
  nSAT      INTEGER(0..31),
  toeLimit  INTEGER(0..10),
  satInfo   SatelliteInfo OPTIONAL,
...}

-- Further information on this fields can be found
-- in [3GPP RRLP]and [3GPP 49.031]

SatelliteInfo ::= SEQUENCE (SIZE (1..31)) OF SatelliteInfoElement

SatelliteInfoElement ::= SEQUENCE {
  satId  INTEGER(0..63),
  iODE   INTEGER(0..255),
  ...}

END
```

11.2.5 SUPL POS

```
SUPL-POS DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

EXPORTS SUPLPOS, PosPayLoad;

IMPORTS
        Velocity
FROM ULP-Components
        Ver2-SUPL-POS-extension
FROM ULP-Version-2-message-extensions
        Ver2-PosPayLoad-extension
FROM ULP-Version-2-parameter-extensions
        Ver3-SUPL-POS-extension
FROM ULP-Version-3-message-extensions;

SUPLPOS ::= SEQUENCE {
  posPayLoad  PosPayLoad,
  velocity    Velocity OPTIONAL,
  ...,
-- version 2 extension element
  ver2-SUPL-POS-extension         Ver2-SUPL-POS-extension OPTIONAL,
-- version 3 extension element
  ver3-SUPL-POS-extension         Ver3-SUPL-POS-extension OPTIONAL}

PosPayLoad ::= CHOICE {
  tia801payload  OCTET STRING(SIZE (1..8192)),
  rrcPayload     OCTET STRING(SIZE (1..8192)),
  rrlpPayload    OCTET STRING(SIZE (1..8192)),
  ...,
  ver2-PosPayLoad-extension  Ver2-PosPayLoad-extension}

END
```

11.2.6 SUPL END

```
SUPL-END DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

EXPORTS SUPLEND;

IMPORTS
        StatusCode, Position, Ver
FROM ULP-Components
        Ver2-SUPL-END-extension
FROM ULP-Version-2-message-extensions
        Ver3-SUPL-END-extension
FROM ULP-Version-3-message-extensions;

SUPLEND ::= SEQUENCE {
  position           Position OPTIONAL,
  statusCode         StatusCode OPTIONAL,
  ver                Ver OPTIONAL,
  ...,
-- version 2 extension element
  ver2-SUPL-END-extension         Ver2-SUPL-END-extension OPTIONAL,
-- version 3 extension element
  ver3-SUPL-END-extension         Ver3-SUPL-END-extension OPTIONAL}

END
```

11.2.7 SUPL AUTH REQ

```
SUPL-AUTH-REQ DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

EXPORTS SUPLAUTHREQ;

IMPORTS
        Ver
FROM ULP-Components
        SETCapabilities
FROM SUPL-START;

SUPLAUTHREQ ::= SEQUENCE {
  ver                Ver OPTIONAL,
  sETCapabilities    SETCapabilities OPTIONAL,
  ...}

END
```

11.2.8 SUPL AUTH RESP

```
SUPL-AUTH-RESP DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

EXPORTS SUPLAUTHRESP;

IMPORTS
        SPCSETKey, SPCTID, SPCSETKeylifetime
FROM Ver2-ULP-Components;

SUPLAUTHRESP ::= SEQUENCE {
  sPCSETKey          SPCSETKey,
```

```
  sPCTID              SPCTID,
  sPCSETKeylifetime   SPCSETKeylifetime OPTIONAL,
  ...}

END
```

11.2.9 SUPL NOTIFY

```
SUPL-NOTIFY DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

EXPORTS Ver2-SUPLNOTIFY;

IMPORTS
        Notification
FROM SUPL-INIT
        Ver3-SUPL-NOTIFY-extension
FROM ULP-Version-3-message-extensions;

Ver2-SUPLNOTIFY ::= SEQUENCE {
  notification  Notification,
  ...,
-- version 3 extension element
  ver3-SUPL-NOTIFY-extension       Ver3-SUPL-NOTIFY-extension OPTIONAL}
END
```

11.2.10 SUPL NOTIFY RESPONSE

```
SUPL-NOTIFY-RESPONSE DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

EXPORTS Ver2-SUPLNOTIFYRESPONSE, NotificationResponse;

IMPORTS
        Ver3-SUPL-NOTIFY-RESPONSE-extension
FROM ULP-Version-3-message-extensions;

Ver2-SUPLNOTIFYRESPONSE ::= SEQUENCE {
  notificationResponse  NotificationResponse OPTIONAL,
  ...,
-- version 3 extension element
  ver3-SUPL-NOTIFY-RESPONSE-extension Ver3-SUPL-NOTIFY-RESPONSE-extension
OPTIONAL}

NotificationResponse ::= ENUMERATED {allowed(0), notAllowed(1), ...}

END
```

11.2.11 SUPL SET INIT

```
SUPL-SET-INIT DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

EXPORTS Ver2-SUPLSETINIT;

IMPORTS
        SETId, QoP
FROM ULP-Components
        ApplicationID
FROM Ver2-ULP-Components
```

```
        Ver3-SUPL-SET-INIT-extension
FROM ULP-Version-3-message-extensions;


Ver2-SUPLSETINIT ::= SEQUENCE {
  targetSETID    SETId, --Target SETid identifies the target SET to be located
  qoP            QoP OPTIONAL,
  applicationID  ApplicationID OPTIONAL,
  ...,
-- version 3 extension element
  ver3-SUPL-SET-INIT-extension     Ver3-SUPL-SET-INIT-extension OPTIONAL}

END
```

11.2.12 SUPL TRIGGERED START

```
SUPL-TRIGGERED-START DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

EXPORTS Ver2-SUPLTRIGGEREDSTART, TriggerType, TriggerParams, maxNumGeoArea,
maxAreaId, maxAreaIdList, GeographicTargetArea, GeographicTargetAreaList,
AreaIdList;

IMPORTS
        LocationId, QoP, Ver, Position
FROM ULP-Components
        MultipleLocationIds, CauseCode, ThirdParty, ApplicationID,
ReportingCap, Coordinate, CircularArea, EllipticalArea, PolygonArea
FROM Ver2-ULP-Components
        SETCapabilities
FROM SUPL-START
        Ver3-SUPL-TRIGGERED-START-extension
FROM ULP-Version-3-message-extensions
        Ver3-TriggerParams-extension, Ver3-LTEAreaId-extension
FROM ULP-Version-3-parameter-extensions;

Ver2-SUPLTRIGGEREDSTART ::= SEQUENCE {
  sETCapabilities     SETCapabilities,
  locationId          LocationId,
  ver                 Ver OPTIONAL,
  qoP                 QoP OPTIONAL,
  multipleLocationIds MultipleLocationIds OPTIONAL,
  thirdParty          ThirdParty OPTIONAL,
  applicationID       ApplicationID OPTIONAL,
  triggerType         TriggerType OPTIONAL,
  triggerParams       TriggerParams OPTIONAL,
  position            Position OPTIONAL,
  reportingCap        ReportingCap OPTIONAL,
  causeCode           CauseCode OPTIONAL,
   ...,
-- version 3 extension element
   ver3-SUPL-TRIGGERED-START-extension Ver3-SUPL-TRIGGERED-START-extension
OPTIONAL}

TriggerType ::= ENUMERATED {
  periodic(0), areaEvent(1),
  ..., ver3-velocityEvent(2)}

TriggerParams ::= CHOICE {
```

```
   periodicParams     PeriodicParams,
   areaEventParams    AreaEventParams,
   ...,
  ver3-TriggerParams-extension Ver3-TriggerParams-extension}

PeriodicParams ::= SEQUENCE{
   numberOfFixes                   INTEGER(1.. 8639999),
   intervalBetweenFixes            INTEGER(1.. 8639999),
   startTime                       INTEGER(0..2678400) OPTIONAL,
...}
-- intervalBetweenFixes and startTime are in seconds.
-- numberOfFixes  * intervalBetweenFixes shall not exceed 8639999
-- (100 days in seconds) for compatibility with OMA MLP and RLP
-- startTime is in relative time in units of seconds measured from "now"
-- a value of 0 signifies "now", a value of "startTime" signifies startTime
-- seconds from "now"

AreaEventParams ::= SEQUENCE {
  areaEventType                    AreaEventType,
  locationEstimate                 BOOLEAN,
  repeatedReportingParams          RepeatedReportingParams OPTIONAL,
  startTime                        INTEGER(0..2678400) OPTIONAL,
  stopTime                         INTEGER(0..11318399) OPTIONAL,
  geographicTargetAreaList         GeographicTargetAreaList   OPTIONAL,
  areaIdLists                      SEQUENCE (SIZE (1..maxAreaIdList)) OF
AreaIdList OPTIONAL,
  ...}

-- startTime and stopTime are in seconds.
-- startTime and stop Time are in relative time in units of seconds measured
-- from "now"
-- a value of 0 signifies "now"
-- stopTime must be > startTime
-- stopTime - startTime shall not exceed 8639999
-- (100 days in seconds) for compatibility with OMA MLP and RLP

AreaEventType ::= ENUMERATED {enteringArea(0), insideArea(1), outsideArea(2),
leavingArea(3), ...}

RepeatedReportingParams ::= SEQUENCE {
  minimumIntervalTime      INTEGER (1..604800), -- time in seconds
  maximumNumberOfReports   INTEGER (1..1024),
  ...}

GeographicTargetAreaList ::= SEQUENCE (SIZE (1..maxNumGeoArea)) OF
GeographicTargetArea

GeographicTargetArea ::= CHOICE {
 circularArea         CircularArea,
 ellipticalArea       EllipticalArea,
 polygonArea          PolygonArea,
 ...}

AreaIdList ::= SEQUENCE {
 areaIdSet            AreaIdSet,
 areaIdSetType        AreaIdSetType OPTIONAL,
 geoAreaMappingList                GeoAreaMappingList OPTIONAL}
```

```
AreaIdSet ::= SEQUENCE SIZE (1..maxAreaId) OF AreaId

AreaId ::= CHOICE {
 gSMAreaId            GSMAreaId,
 wCDMAAreaId          WCDMAAreaId, -- For TD-SCDMA networks, this parameter
indicates a TD-SCDMA Area ID
 cDMAAreaId           CDMAAreaId,
 hRPDAreaId           HRPDAreaId,
 uMBAreaId            UMBAreaId,
 lTEAreaId            LTEAreaId,
 wLANAreaId           WLANAreaId,
 wiMAXAreaId          WimaxAreaId,
 ...}

GSMAreaId ::= SEQUENCE {
 refMCC               INTEGER(0..999) OPTIONAL, -- Mobile Country Code
 refMNC               INTEGER(0..999) OPTIONAL, -- Mobile Network Code
 refLAC               INTEGER(0..65535) OPTIONAL, -- Location Area Code
 refCI                INTEGER(0..65535) OPTIONAL, -- Cell Id
 ...}

-- if only CI is present, MCC, MNC and LAC are assumed to be identical to the
current serving or camped on network values
-- if only CI + LAC are present, MCC and MNC are assumed to be identical to the
current serving or camped on network values
-- if only CI + LAC + MNC are present, MCC is assumed to be identical to the
current serving or camped on network values
-- if only LAC is present, MCC and MNC are assumed to be identical to the
current serving or camped on network values
-- if only MNC is present, MCC is assumed to be identical to the current
serving or camped on network value

WCDMAAreaId ::= SEQUENCE {
  refMCC INTEGER(0..999) OPTIONAL, -- Mobile Country Code
  refMNC INTEGER(0..999) OPTIONAL, -- Mobile Network Code
  refLAC INTEGER(0..65535) OPTIONAL, -- Location Area Code
  refUC  INTEGER(0..268435455) OPTIONAL, -- Cell identity
...}

-- if only UC is present, MCC and MNC are assumed to be identical to the
current serving or camped on network values
-- if only LAC is present, MCC and MNC are assumed to be identical to the
current serving or camped on network values
-- if only MNC is present, MCC is assumed to be identical to the current
serving or camped on network value

CDMAAreaId::= SEQUENCE {
  refSID         INTEGER(0..65535) OPTIONAL, -- System Id
  refNID         INTEGER(0..32767) OPTIONAL, -- Network Id
  refBASEID      INTEGER(0..65535) OPTIONAL, -- Base Station Id
...}

-- if only BASEID is present, SID and NID are assumed to be identical to the
current serving or camped on network values
-- if only NID is present, SID is assumed to be identical to the current
serving or camped on network value

HRPDAreaId::= SEQUENCE {
```

```
  refSECTORID    BIT STRING(SIZE (128)), -- HRPD Sector Id
...}

UMBAreaId::= SEQUENCE {
  refMCC              INTEGER(0..999) OPTIONAL, -- Mobile Country Code
  refMNC              INTEGER(0..999) OPTIONAL, -- Mobile Network Code
  refSECTORID         BIT STRING(SIZE (128)) OPTIONAL, -- UMB Sector Id
...}

-- if only SECTORID is present, MCC and MNC are assumed to be identical to the
current serving or camped on network values
-- if only SECTORID + MNC are present, MCC is assumed to be identical to the
current serving or camped on network values
-- if only MNC is present, MCC is assumed to be identical to the current
serving or camped on network value

LTEAreaId::= SEQUENCE {
  refMCC INTEGER(0..999) OPTIONAL, -- Mobile Country Code
  refMNC INTEGER(0..999) OPTIONAL, -- Mobile Network Code
  refCI  BIT STRING(SIZE (29)) OPTIONAL, -- LTE Cell-Id (bit 29 is not valid
and shall be disregarded by the SET)
...,
ver3-LTEAreaID-extension          Ver3-LTEAreaId-extension OPTIONAL}

-- if only CI or TrackingAreaCode is present, MCC and MNC are assumed to be
identical to the current serving or camped on network values
-- if only CI + MNC are present, MCC is assumed to be identical to the current
serving or camped on network values
-- if only MNC is present, MCC is assumed to be identical to the current
serving or camped on network value


WLANAreaId::= SEQUENCE {
  apMACAddress       BIT STRING(SIZE (48)), -- AP MAC Address
...}

WimaxAreaId ::= SEQUENCE {
  bsID-MSB      BIT STRING (SIZE(24)) OPTIONAL,
  bsID-LSB      BIT STRING (SIZE(24)) }
-- if only LSB is present, MSB is assumed to be identical to the current
serving BS or clamped on network value

AreaIdSetType ::=  ENUMERATED {border(0), within(1), ...}

GeoAreaMappingList ::= SEQUENCE (SIZE (1..maxNumGeoArea)) OF GeoAreaIndex

GeoAreaIndex ::= INTEGER (1..maxNumGeoArea)

maxNumGeoArea INTEGER ::= 32

maxAreaId INTEGER ::= 256

maxAreaIdList INTEGER ::= 32

END
```

11.2.13 SUPL TRIGGERED RESPONSE

```
SUPL-TRIGGERED-RESPONSE DEFINITIONS AUTOMATIC TAGS ::=
```

```
BEGIN

EXPORTS Ver2-SUPLTRIGGEREDRESPONSE;

IMPORTS
        PosMethod, SLPAddress
FROM ULP-Components
        SupportedNetworkInformation, SPCSETKey, SPCTID, SPCSETKeylifetime,
GNSSPosTechnology
FROM Ver2-ULP-Components
        TriggerParams
FROM SUPL-TRIGGERED-START
        Ver3-SUPL-TRIGGERED-RESPONSE-extension
FROM ULP-Version-3-message-extensions;

Ver2-SUPLTRIGGEREDRESPONSE::= SEQUENCE{
  posMethod                       PosMethod,
  triggerParams                   TriggerParams  OPTIONAL,
  sLPAddress                      SLPAddress OPTIONAL,
  supportedNetworkInformation     SupportedNetworkInformation OPTIONAL,
  reportingMode                   ReportingMode OPTIONAL,
  sPCSETKey                       SPCSETKey    OPTIONAL,
  sPCTID                          SPCTID       OPTIONAL,
  sPCSETKeylifetime               SPCSETKeylifetime OPTIONAL,
  gnssPosTechnology               GNSSPosTechnology OPTIONAL,
  ...,
-- version 3 extension element
  ver3-SUPL-TRIGGERED-RESPONSE-extension Ver3-SUPL-TRIGGERED-RESPONSE-extension
OPTIONAL}
ReportingMode ::= SEQUENCE {
  repMode             RepModee,
  batchRepConditions  BatchRepConditions OPTIONAL, -- only used for batch
reporting
  batchRepType        BatchRepType OPTIONAL, -- only used for batch reporting
  ...}

RepModee ::= ENUMERATED {realtime(1), quasirealtime(2), batch(3), ...}

BatchRepConditions ::= CHOICE {
 num-interval INTEGER (1..1024), -- number of periodic fixes/measurements after
which the batch report is sent to the SLP
 num-minutes INTEGER (1..2048), -- number of minutes after which the batch
report is sent to the SLP
 endofsession NULL, -- if selected batch report is to be sent at the end of the
session
 ...}

BatchRepType ::= SEQUENCE {
  reportPosition      BOOLEAN, -- set to "true" if reporting of position is
allowed
  reportMeasurements  BOOLEAN, -- set to " true" if reporting of measurements
is allowed
  intermediateReports   BOOLEAN, -- set to "true" if the SET is allowed to send
intermediate reports if it runs out of memory
  discardOldest       BOOLEAN OPTIONAL, -- set to "true" if the SET should
discard the oldest positions or measurements of the batch report in order to
save memory, set to "false" the SET should discard the latest positions or
measurements
```

```
  ...}

END
```

11.2.14 SUPL REPORT

```
SUPL-REPORT DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

EXPORTS Ver2-SUPLREPORT, SessionList, maxnumSessions;

IMPORTS
        SETCapabilities
FROM SUPL-START
        Position, PosMethod, SessionID, Ver
FROM ULP-Components
        MultipleLocationIds, GNSSPosTechnology, GANSSSignals
FROM Ver2-ULP-Components
        maxGANSS
FROM ULP-Version-2-parameter-extensions
        Ver3-SUPL-REPORT-extension
FROM ULP-Version-3-message-extensions
        Ver3-PosPayLoad-rep-extensions
FROM ULP-Version-3-parameter-extensions;

Ver2-SUPLREPORT ::= SEQUENCE {
 sessionList          SessionList OPTIONAL,
 sETCapabilities      SETCapabilities OPTIONAL,
 reportDataList       ReportDataList OPTIONAL,
 ver                  Ver OPTIONAL,
 moreComponents       NULL OPTIONAL,
...,
-- version 3 extension element
 ver3-SUPL-REPORT-extension        Ver3-SUPL-REPORT-extension OPTIONAL}

SessionList ::= SEQUENCE SIZE (1..maxnumSessions) OF SessionInformation

SessionInformation ::= SEQUENCE {
 sessionID            SessionID,
 ...}

maxnumSessions    INTEGER ::= 64

ReportDataList ::= SEQUENCE SIZE (1.. 1024) OF ReportData

ReportData ::= SEQUENCE {
  positionData        PositionData OPTIONAL,
  multipleLocationIds MultipleLocationIds OPTIONAL,
  resultCode          ResultCode OPTIONAL,
  timestamp           TimeStamp OPTIONAL,
  ...,
  posPayLoad          Ver3-PosPayLoad-rep-extensions OPTIONAL} -- this
parameter is used to carry enhanced cell/sector/AP measurements for either LPPe
or TIA-801

PositionData ::= SEQUENCE {
 position                          Position,
 posMethod                         PosMethod OPTIONAL,
 gnssPosTechnology                 GNSSPosTechnology OPTIONAL,
```

```
 ganssSignalsInfo                  GANSSsignalsInfo OPTIONAL,
 ...}

GANSSsignalsInfo ::= SEQUENCE SIZE (1..maxGANSS) OF GANSSSignalsDescription

GANSSSignalsDescription ::= SEQUENCE {
 ganssId             INTEGER(0..15), -- coding according to parameter
definition in section 10.8
 gANSSSignals        GANSSSignals,
 ...}

ResultCode ::= ENUMERATED {outofradiocoverage(1), noposition(2),
nomeasurement(3), nopositionnomeasurement(4), outofmemory(5),
outofmemoryintermediatereporting(6), other(7), ...}

TimeStamp ::= CHOICE {
  absoluteTime  UTCTime,
  relativeTime  INTEGER (0..31536000)} -- relative time to when the SUPL REPORT
message is sent in units of 1 sec, where 0 signifies "now" and n signifies n
seconds in the past

END
```

11.2.15 SUPL TRIGGERED STOP

```
SUPL-TRIGGERED-STOP DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

EXPORTS Ver2-SUPLTRIGGEREDSTOP;

IMPORTS
        StatusCode
FROM ULP-Components
        Ver3-SUPL-TRIGGERED-STOP-extension
FROM ULP-Version-3-message-extensions;

Ver2-SUPLTRIGGEREDSTOP::= SEQUENCE{
  statusCode     StatusCode OPTIONAL,
  ...,
  -- version 3 extension element
  ver3-SUPL-TRIGGERED-STOP-extension Ver3-SUPL-TRIGGERED-STOP-extension
OPTIONAL}

END
```

11.2.16 SUPL REINIT

```
SUPL-REINIT DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

EXPORTS Ver3-SUPLREINIT;

IMPORTS
        ProtectionLevel
FROM ULP-Version-2-message-extensions;


Ver3-SUPLREINIT::= SEQUENCE {
  protectionLevel     ProtectionLevel OPTIONAL,
```

```
...}

END
```

11.3 Message Extensions (SUPL Version 2)

```
ULP-Version-2-message-extensions DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

EXPORTS
Ver2-SUPL-INIT-extension, Ver2-SUPL-START-extension, Ver2-SUPL-RESPONSE-
extension, Ver2-SUPL-POS-INIT-extension, Ver2-SUPL-POS-extension, Ver2-SUPL-
END-extension, ProtectionLevel;

IMPORTS
        SLPAddress, Position, Ver
FROM ULP-Components
        SETCapabilities
FROM SUPL-START
        SupportedNetworkInformation, GNSSPosTechnology, MultipleLocationIds,
UTRAN-GPSReferenceTimeResult, UTRAN-GANSSReferenceTimeResult, UTRAN-
GPSReferenceTimeAssistance, UTRAN-GANSSReferenceTimeAssistance, SPCSETKey,
SPCTID, SPCSETKeylifetime, ThirdParty, ApplicationID
FROM Ver2-ULP-Components
        TriggerType
FROM SUPL-TRIGGERED-START
        Ver3-ProtectionLevel-extension
FROM ULP-Version-3-parameter-extensions;

Ver2-SUPL-INIT-extension ::= SEQUENCE {
  notificationMode                NotificationMode OPTIONAL,
  supportedNetworkInformation     SupportedNetworkInformation OPTIONAL,
  triggerType                     TriggerType OPTIONAL,
  e-SLPAddress                    SLPAddress OPTIONAL,
  historicReporting               HistoricReporting OPTIONAL,
  protectionLevel                 ProtectionLevel OPTIONAL,
  gnssPosTechnology               GNSSPosTechnology OPTIONAL,
  minimumMajorVersion             INTEGER (0..255) OPTIONAL,
...}

NotificationMode ::= ENUMERATED {normal(0), basedOnLocation(1), ...}

HistoricReporting ::= SEQUENCE {
  allowedReportingType            AllowedReportingType,
  reportingCriteria               ReportingCriteria OPTIONAL,...}

AllowedReportingType ::= ENUMERATED {
  positionsOnly(0), measurementsOnly(1), positionsAndMeasurements(2),...}

ReportingCriteria ::= SEQUENCE {
  timeWindow          TimeWindow   OPTIONAL,
  maxNumberofReports  INTEGER(1..65536) OPTIONAL,
  minTimeInterval     INTEGER(1..86400) OPTIONAL,
...}

TimeWindow ::= SEQUENCE {
  startTime           INTEGER(-525600..-1), -- Time in minutes
  stopTime            INTEGER(-525599..0)} -- Time in minutes
```

```
ProtectionLevel ::= SEQUENCE {
 protlevel                          ProtLevel,
 basicProtectionParams              BasicProtectionParams     OPTIONAL, -- not
applicable in SUPL 3.0
...,
ver3-ProtectionLevel-extension      Ver3-ProtectionLevel-extension OPTIONAL}

ProtLevel ::= ENUMERATED {
 nullProtection(0), basicProtection(1), ..., ver3-modeAProtection(2), ver3-
modeBProtection(3)} -- basicProtection(1) is not applicable in SUPL 3.0

BasicProtectionParams ::= SEQUENCE {
 keyIdentifier                      OCTET STRING(SIZE (8)),
 basicReplayCounter                 INTEGER(0..65535),
 basicMAC                           BIT STRING(SIZE (32)),
...}

Ver2-SUPL-START-extension ::= SEQUENCE {
  multipleLocationIds MultipleLocationIds OPTIONAL,
  thirdParty          ThirdParty OPTIONAL,
  applicationID       ApplicationID OPTIONAL,
  position            Position OPTIONAL,
...}

Ver2-SUPL-RESPONSE-extension ::= SEQUENCE {
  supportedNetworkInformation      SupportedNetworkInformation OPTIONAL,
  sPCSETKey                        SPCSETKey    OPTIONAL,
  sPCTID                           SPCTID       OPTIONAL,
  sPCSETKeylifetime                SPCSETKeylifetime OPTIONAL,
  initialApproximateposition       Position     OPTIONAL,
  gnssPosTechnology                GNSSPosTechnology OPTIONAL,
...}

Ver2-SUPL-POS-INIT-extension ::= SEQUENCE {
  multipleLocationIds              MultipleLocationIds OPTIONAL,
  utran-GPSReferenceTimeResult     UTRAN-GPSReferenceTimeResult OPTIONAL,
  utran-GANSSReferenceTimeResult   UTRAN-GANSSReferenceTimeResult OPTIONAL,
...}

Ver2-SUPL-POS-extension ::= SEQUENCE {
utran-GPSReferenceTimeAssistance   UTRAN-GPSReferenceTimeAssistance OPTIONAL,
utran-GPSReferenceTimeResult       UTRAN-GPSReferenceTimeResult OPTIONAL,
utran-GANSSReferenceTimeAssistance UTRAN-GANSSReferenceTimeAssistance OPTIONAL,
utran-GANSSReferenceTimeResult     UTRAN-GANSSReferenceTimeResult OPTIONAL,
...}

Ver2-SUPL-END-extension ::= SEQUENCE {
  sETCapabilities     SETCapabilities OPTIONAL,
...}

END
```

11.4 Message Extensions (SUPL Version 3)

```
ULP-Version-3-message-extensions DEFINITIONS AUTOMATIC TAGS ::=
BEGIN
```

```
EXPORTS
Ver3-SUPL-INIT-extension, Ver3-SUPL-START-extension, Ver3-SUPL-POS-INIT-
extension, Ver3-SUPL-END-extension, Ver3-SUPL-RESPONSE-extension, Ver3-SUPL-
TRIGGERED-RESPONSE-extension, Ver3-SUPL-TRIGGERED-START-extension, Ver3-SUPL-
TRIGGERED-STOP-extension, Ver3-SUPL-SET-INIT-extension, Ver3-SUPL-NOTIFY-
extension, Ver3-SUPL-NOTIFY-RESPONSE-extension, Ver3-SUPL-REPORT-extension,
QoPCapabilities, RelativePositioningCapabilities, CivicPositioningCapabilities,
LocationURICapabilities, Ver3-SUPL-POS-extension;

IMPORTS
  Ver, QoP, FQDN
FROM ULP-Components
 PosProtocolVersion3GPP, PosProtocolVersion3GPP2
FROM ULP-Version-2-parameter-extensions
 PosProtocolVersionOMA
FROM ULP-Version-3-parameter-extensions
 PosPayLoad
FROM SUPL-POS
 Notification
FROM SUPL-INIT
 SessionID
FROM ULP-Components
 NotificationResponse
FROM SUPL-NOTIFY-RESPONSE
 maxnumSessions, SessionList
FROM SUPL-REPORT
 OMA-LPPe-RelativeLocation, OMA-LPPe-ReferencePointUniqueID, OMA-LPPe-
CivicLocation
FROM OMA-LPPE
GeographicTargetArea, GeographicTargetAreaList, AreaIdList, maxAreaIdList
FROM SUPL-TRIGGERED-START;


Ver3-SUPL-INIT-extension ::= SEQUENCE {
  sLPCapabilities     SLPCapabilities OPTIONAL,
  gSSParameters       GSSParameters OPTIONAL,
  extendedNotification            ExtendedNotification      OPTIONAL,
  d-slp-Address                   SLP-Address               OPTIONAL,
  highAccuracyQoP                 HighAccuracyQoP           OPTIONAL,
...}

SLPCapabilities ::= SEQUENCE {
  supportedPosProtocols           SupportedPosProtocols,
  supportedProtocolVersions       SupportedProtocolVersions,
  qoPCapabilities                 QoPCapabilities OPTIONAL,
  civicPositioningCapabilities    CivicPositioningCapabilities OPTIONAL,
  relativePositioningCapabilities RelativePositioningCapabilities OPTIONAL,
  locationURICapabilities         LocationURICapabilities   OPTIONAL,
...}

QoPCapabilities ::= SEQUENCE {
  highQualityPositionRX           BOOLEAN,
  highQualityPositionTX           BOOLEAN,
  highQualityVelocityRX           BOOLEAN,
  highQualityVelocityTX           BOOLEAN,
...}

CivicPositioningCapabilities ::= SEQUENCE {
```

```
  positioningAbsoluteCivicAddress  BOOLEAN,
...}

RelativePositioningCapabilities ::= SEQUENCE {
  positioningRelativeToReferencePoint           BOOLEAN,
...}

LocationURICapabilities ::= SEQUENCE {
  locationURISupport  BOOLEAN,
...}

SupportedPosProtocols ::= BIT STRING {
  lpp                (0),
  lppe               (1),
  tia-801            (2)} (SIZE (1..8))

SupportedProtocolVersions ::= SEQUENCE {
  posProtocolVersionLPP           PosProtocolVersion3GPP    OPTIONAL,
  posProtocolVersionLPPe          PosProtocolVersionOMA     OPTIONAL,
  posProtocolVersionTIA801        PosProtocolVersion3GPP2   OPTIONAL,
...}

GSSParameters ::= SEQUENCE {
  duration           Duration,
...}

Duration ::= SEQUENCE {
  timeDuration       INTEGER (1..44640) OPTIONAL, -- time duration in minutes
(maximum time duration is 31 days)
  messageCountDuration            MessageCountDuration OPTIONAL,
...} -- either timeDuration or messageCountDuration or both SHALL be included

MessageCountDuration ::= SEQUENCE {
  numUplinkMessages   INTEGER (1..4096) OPTIONAL, -- max number of SUPL POS
messages on uplink
  numDownlinkMessages INTEGER (1..4096) OPTIONAL, -- max number of SUPL POS
messages on downlink
  numTotalMessages    INTEGER (1..8192) OPTIONAL, -- max number of uplink +
downlink SUPL POS messages
...}

ExtendedNotification ::= SEQUENCE {
  locationURI        URI          OPTIONAL,
...}

URI ::= VisibleString (FROM ( "a".."z" | "A".."Z" | "0".."9" | ":" | "/" | "?"
| "#" | "[" | "]" | "@" | "!" | "$" | "&" | "'" | "(" | ")" | "*" | "+" | "," |
";" | "=" | "-" | "." | "_" | "~" | "%"))

Ver3-SUPL-START-extension ::= SEQUENCE {
  gSSParameters       GSSParameters             OPTIONAL,
  locationURISet      LocationURISet            OPTIONAL,
  locationURIRequest  LocationURIRequest        OPTIONAL,
  ver                 Ver                       OPTIONAL,
  slpQuery            SLPQuery                  OPTIONAL,
  emergencyServicesIndication     EmergencyServicesIndication OPTIONAL,
  referencePointId                OMA-LPPe-ReferencePointUniqueID OPTIONAL,
  highAccuracyQoP                 HighAccuracyQoP OPTIONAL,
```

```
...}

EmergencyServicesIndication ::= SEQUENCE {
...}

LocationURISet ::= SEQUENCE {
  locationURIList     LocationURIList,
  validity            LocationURIValidity,
...}

LocationURIList ::= SEQUENCE (SIZE(1..maxLocationURI)) OF URI

maxLocationURI INTEGER ::= 5

LocationURIValidity ::= INTEGER (1..1440) -- in units of minutes

LocationURIRequest ::= SEQUENCE {
  reason              LocationURIReason,
  validity            LocationURIValidity,
...}

LocationURIReason ::= ENUMERATED {emergencysession, h-SLP, undefined, ...}

SLPQuery ::= SEQUENCE {
  d-SLP-Query         D-SLP-Query               OPTIONAL,
  e-SLP-Query         E-SLP-Query               OPTIONAL,
...}

D-SLP-Query ::= SEQUENCE {
  authorized-D-SLP-Address-List    SLP-Address-List OPTIONAL,
  preferred-D-SLP-Address-List     SLP-Address-List OPTIONAL,
  not-preferred-D-SLP-Address-List SLP-Address-List OPTIONAL,
  qop                              QoP              OPTIONAL,
...}

E-SLP-Query ::= SEQUENCE {
  authorized-E-SLP-Address-List    SLP-Address-List OPTIONAL,
  preferred-E-SLP-Address-List     SLP-Address-List OPTIONAL,
  not-preferred-E-SLP-Address-List SLP-Address-List OPTIONAL,
...}

SLP-Address-List ::= SEQUENCE (SIZE(1..maxSLP)) OF SLP-Address

maxSLP INTEGER ::= 10

SLP-Address ::= SEQUENCE {
  fqdn   FQDN,
...}

AccessNetwork ::= CHOICE {
 gSMAccess            MCC-MNC,
 wCDMAAccess          MCC-MNC,
 lTEAccess            MCC-MNC,
 eHRPDAccess          MCC-MNC,
 cDMAAccess           SID-NID,
 hRPDAccess           Sector-ID,
 wiMaxAccess          BSID,
 wLANAccess           WLAN-ID,
```

```
 fixedAccess          Fixed-Access,
...}

MCC-MNC ::= SEQUENCE {
 mcc     SEQUENCE (SIZE (3))       OF INTEGER (0..9),
 mnc     SEQUENCE (SIZE (2..3))    OF INTEGER (0..9) OPTIONAL}


SID-NID ::= SEQUENCE {
  sid         INTEGER(0..65535),                -- System Id
  nid         INTEGER(0..32767)    OPTIONAL}    -- Network Id

Sector-ID ::= BIT STRING(SIZE (128)) -- HRPD Sector Id

BSID ::= SEQUENCE {
  bsID-MSB      BIT STRING (SIZE(24)),
  bsID-LSB      BIT STRING (SIZE(24)) OPTIONAL}

WLAN-ID ::= SEQUENCE {
  apMACAddress        BIT STRING(SIZE (48)) OPTIONAL, -- AP MAC Address
  ssid                OCTET STRING (SIZE (1..32)) OPTIONAL, -- WLAN SSID
...}
-- at least one of apMACAddress and ssid must be included

Fixed-Access ::= SEQUENCE {
 ipV4Address          BIT STRING (SIZE (32))    OPTIONAL,
 ipV6Address          BIT STRING (SIZE (128))   OPTIONAL,
... }

Ver3-SUPL-POS-INIT-extension ::= SEQUENCE {
  locationURISet      LocationURISet            OPTIONAL,
...}

Ver3-SUPL-END-extension ::= SEQUENCE {
  locationURISet      LocationURISet            OPTIONAL,
  slpAuthorization    SLPAuthorization          OPTIONAL,
  relativePosition    OMA-LPPe-RelativeLocation OPTIONAL,
  civicPosition       OMA-LPPe-CivicLocation OPTIONAL,
  sULPINITKeyResponse SULPINITKeyResponse OPTIONAL,
...}

SLPAuthorization ::= SEQUENCE {
  d-SLP-Authorization-List         D-SLP-Authorization-List  OPTIONAL,
  e-SLP-Authorization-List         E-SLP-Authorization-List  OPTIONAL,
  minimum-retry-period             INTEGER (0..1440)         OPTIONAL,    --
units are minutes
...}

D-SLP-Authorization-List ::= SEQUENCE {
  d-slp-List                       D-SLP-List,
  h-SLP-Access-Preference          H-SLP-Access-Preference OPTIONAL,
  report-D-SLP-Access              Report-D-SLP-Access OPTIONAL,
...}
-- h-SLP-Access-Preference and report-D-SLP-Access shall not be included when
the sender is a Proxy D-SLP and shall be ignored if received

D-SLP-List ::= SEQUENCE (SIZE(0..maxSLP)) OF D-SLP-Authorization
```

```
D-SLP-Authorization ::= SEQUENCE {
  d-SLP-Address       SLP-Address,
  serviceDuration     ServiceDuration OPTIONAL,
  serviceArea         ServiceArea  OPTIONAL,
  accessNetworkList   AccessNetworkList OPTIONAL,
  combinationtype     CombinationType OPTIONAL,
  services            D-SLP-Services OPTIONAL,
  proxy-d-slp         Proxy-D-SLP  OPTIONAL,
...}
-- accessNetworkList and proxy-d-slp are mutually exclusive and when both are
present, a receiver shall ignore accessNetworkList
-- services and proxy-d-slp shall not be included when the sender is a Proxy D-
SLP and shall be ignore if received

E-SLP-Authorization-List ::= SEQUENCE {
  e-slp-List          E-SLP-List,
...}

E-SLP-List ::= SEQUENCE (SIZE(0..maxSLP)) OF E-SLP-Authorization

E-SLP-Authorization ::= SEQUENCE {
  e-SLP-Address       SLP-Address,
  serviceDuration     ServiceDuration OPTIONAL,
  serviceArea         GeographicTargetArea      OPTIONAL,
  accessNetworkList   AccessNetworkList OPTIONAL,
  combinationType     CombinationType OPTIONAL,
  proxy-e-slp         Proxy-E-SLP  OPTIONAL,
...}
-- accessNetworkList and proxy-e-slp are mutually exclusive
-- when both are present, a receiver shall ignore accessNetworkList

ServiceDuration ::= INTEGER (1..1024)           -- units are hours

ServiceArea ::= SEQUENCE {
 geographicArea      GeographicTargetAreaList,
 areaIdLists         SEQUENCE (SIZE (1..maxAreaIdList)) OF AreaIdList
OPTIONAL,
...}

maxArea INTEGER ::= 32 -- maximum number of service areas of D-SLP

AccessNetworkList ::= SEQUENCE (SIZE (1..maxAccessNetwork)) OF AccessNetwork

maxAccessNetwork INTEGER ::= 1024

CombinationType ::= ENUMERATED {and, or, conditional-or, ...}

D-SLP-Services ::= SEQUENCE {
  nI-SingleFix                    BOOLEAN,
  nI-SessionInfoQuery             BOOLEAN,
  nI-TriggeredPeriodic            BOOLEAN,
  nI-TriggeredAreaEvent           BOOLEAN,
  nI-VelocityEvent                BOOLEAN,
  nI-RetrievalHistoricPosition    BOOLEAN,
  nI-GSS                          BOOLEAN,
  sI-SingleFix                    BOOLEAN,
  sI-SingleFixThirdParty          BOOLEAN,
  sI-SingleFixThirdPartyRelative  BOOLEAN,
```

```
  sI-SingleFixTransferThirdParty   BOOLEAN,
  sI-TriggeredPeriodic             BOOLEAN,
  sI-TriggeredAreaEvent            BOOLEAN,
  sI-VelocityEvent                 BOOLEAN,
  sI-GSS                           BOOLEAN,
  nI-LocationURIRequest            BOOLEAN,
...}

H-SLP-Access-Preference ::= ENUMERATED {no-access, access-not-preferred,
access-preferred, ...}

Report-D-SLP-Access ::= SEQUENCE {
  only-Notify-D-SLPs-Authorized-For-NI-Service  BOOLEAN,
  include-Proxy-D-SLP-Authorized-D-SLPs         BOOLEAN,
...}

Proxy-D-SLP ::= SEQUENCE {
...}

Proxy-E-SLP ::= SEQUENCE {
...}

Ver3-SUPL-REPORT-extension ::= SEQUENCE {
  pauseSessionList                SessionList  OPTIONAL,
  authorized-D-SLP-List           Authorized-D-SLP-List OPTIONAL,
  authorized-E-SLP-List           Authorized-E-SLP-List OPTIONAL,
  d-slp-Access-Notification       D-SLP-Access-Notification  OPTIONAL,
  relativePosition                OMA-LPPe-RelativeLocation OPTIONAL,
  civicPosition                   OMA-LPPe-CivicLocation OPTIONAL,
...}

Authorized-D-SLP-List ::= SEQUENCE (SIZE(1..maxSLP)) OF Authorized-D-SLP

Authorized-D-SLP ::= SEQUENCE {
  d-SLP-Address                                 SLP-Address,
  proxy-Authorized-D-SLP-List     SLP-Address-List OPTIONAL,
...}
-- proxy-Authorized-D-SLP-List may only be included in a response to an H-SLP
Session Info Query when d-SLP-Address refers to a Proxy D-SLP

Authorized-E-SLP-List ::= SEQUENCE (SIZE(1..maxSLP)) OF Authorized-E-SLP

Authorized-E-SLP ::= SEQUENCE {
  e-SLP-Address                                 SLP-Address,
  proxy-Authorized-E-SLP-List     SLP-Address-List OPTIONAL,
...}
-- proxy-Authorized-E-SLP-List may only be included in a response to an H-SLP
Session Info Query when e-SLP-Address refers to a Proxy E-SLP

D-SLP-Access-Notification ::= SEQUENCE {
  d-SLP-Address      SLP-Address,
...}

Ver3-SUPL-TRIGGERED-STOP-extension ::= SEQUENCE {
  requestType        RequestType  OPTIONAL,
  endSessionList     SessionList  OPTIONAL,
  slpAuthorization   SLPAuthorization OPTIONAL,
...}
```

```
Ver3-SUPL-RESPONSE-extension ::= SEQUENCE {
  sLPCapabilities     SLPCapabilities OPTIONAL,
  gSSParameters       GSSParameters OPTIONAL,
  relativePosition    OMA-LPPe-RelativeLocation OPTIONAL,
  civicPosition       OMA-LPPe-CivicLocation OPTIONAL,
...}

Ver3-SUPL-TRIGGERED-RESPONSE-extension ::= SEQUENCE {
  sLPCapabilities     SLPCapabilities OPTIONAL,
...}

Ver3-SUPL-TRIGGERED-START-extension ::= SEQUENCE {
 posPayLoad           PosPayLoad,
 referencePointId     OMA-LPPe-ReferencePointUniqueID OPTIONAL,
 highAccuracyQoP      HighAccuracyQoP OPTIONAL,
...}

RequestType ::= ENUMERATED {stop, pause, resume, ...}

Ver3-SUPL-SET-INIT-extension ::= SEQUENCE {
  resultType          ResultType   OPTIONAL,
  referencePointId    OMA-LPPe-ReferencePointUniqueID OPTIONAL,
  highAccuracyQoP     HighAccuracyQoP OPTIONAL,
...}

ResultType ::= ENUMERATED {absoluteposition, positionrelativetoreferencepoint,
positionrelativetoSET, ...}

Ver3-SUPL-NOTIFY-extension ::= SEQUENCE {
  notificationList    SEQUENCE (SIZE (1..maxnumSessions)) OF
NotificationSession   OPTIONAL,
...}

NotificationSession ::= SEQUENCE {
  sessionID           SessionID,
  notification        Notification,
...}

Ver3-SUPL-NOTIFY-RESPONSE-extension ::= SEQUENCE {
  notificationRepList SEQUENCE (SIZE (1.. maxnumSessions)) OF
NotificationRepSession             OPTIONAL,
...}

NotificationRepSession ::= SEQUENCE {
  sessionID                        SessionID,
  notificationResponse             NotificationResponse,
...}

HighAccuracyQoP ::= SEQUENCE {
  horacc     INTEGER(0..255), -- as defined in [OMA LPPe] "uncertainty-semimajor" for
OMA-LPPe-HighAccuracy3Dposition
  veracc     INTEGER(0..255) OPTIONAL, -- as defined in [OMA LPPe] "uncertainty-
altitude" for OMA-LPPe-HighAccuracy3Dposition
  maxLocAge  INTEGER(0..65535) OPTIONAL, -- in units of seconds
  delay      INTEGER(1..256) OPTIONAL, -- in units of seconds
  requestVelocity     BOOLEAN, -- used to request high accuracy velocity
  ...}
```

```
SULPINITKeyResponse ::= CHOICE {
  modeAKeyEstablishment                          ModeAKeyEstablishment,
  modeAResynch                                   ModeAResynch,
...}

ModeAKeyEstablishment ::= SEQUENCE {
  modeAKeyIdentifier                             OCTET STRING(SIZE (8)),
  temporaryModeAKeyIdentifier                    OCTET STRING(SIZE (8)),
  sUPLINITROOTKEY                                          BIT STRING(SIZE
(128)),
  modeAKeyLifetime                                         UTCTime,
...}

ModeAResynch ::= SEQUENCE {
  modeAKeyIdentifier                             OCTET STRING(SIZE (8)),
  temporaryModeAKeyIdentifier                    OCTET STRING(SIZE (8)),
...}

Ver3-SUPL-POS-extension ::= SEQUENCE {
  more               BOOLEAN,
  end                BOOLEAN,
...} -- the 'more' and 'end' flag are mutually exclusive

END
```

11.5 Parameter Extensions (SUPL Version 2)

```
ULP-Version-2-parameter-extensions DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

EXPORTS
maxGANSS, Ver2-Notification-extension, Ver2-SETCapabilities-extension, Ver2-
PosProtocol-extension, Ver2-PosTechnology-extension, Ver2-RequestedAssistData-
extension, Ver2-PosPayLoad-extension, PosProtocolVersion3GPP,
PosProtocolVersion3GPP2;

IMPORTS
        GANSSSignals, ReportingCap
FROM Ver2-ULP-Components
        maxNumGeoArea, maxAreaId, maxAreaIdList
FROM SUPL-TRIGGERED-START
        Ver3-ServiceSupported-extensions
FROM ULP-Version-3-parameter-extensions;

Ver2-Notification-extension ::= SEQUENCE {
  emergencyCallLocation  NULL OPTIONAL,
  ...}

Ver2-SETCapabilities-extension ::= SEQUENCE {
  serviceCapabilities          ServiceCapabilities OPTIONAL,
...,
  supportedBearers SupportedBearers OPTIONAL}


ServiceCapabilities ::= SEQUENCE {
  servicesSupported               ServicesSupported,
  reportingCapabilities           ReportingCap OPTIONAL,
```

```
  eventTriggerCapabilities         EventTriggerCapabilities OPTIONAL,
  sessionCapabilities              SessionCapabilities,
...}

ServicesSupported ::= SEQUENCE {
  periodicTrigger     BOOLEAN,
  areaEventTrigger    BOOLEAN,
...,
ver3-ServiceSupported-extensions Ver3-ServiceSupported-extensions OPTIONAL}

EventTriggerCapabilities ::= SEQUENCE {
  geoAreaShapesSupported           GeoAreaShapesSupported,
  maxNumGeoAreaSupported           INTEGER (0..maxNumGeoArea) OPTIONAL,
  maxAreaIdListSupported           INTEGER (0..maxAreaIdList) OPTIONAL,
  maxAreaIdSupportedPerList        INTEGER (0..maxAreaId) OPTIONAL,
...}

GeoAreaShapesSupported ::= SEQUENCE {
  ellipticalArea   BOOLEAN,
  polygonArea      BOOLEAN,
...}

SessionCapabilities ::= SEQUENCE {
  maxNumberTotalSessions           INTEGER (1..128),
  maxNumberPeriodicSessions        INTEGER (1..32),
  maxNumberTriggeredSessions       INTEGER (1..32),
...}

SupportedBearers ::= SEQUENCE {
  gsm                BOOLEAN,
  wcdma              BOOLEAN,
  lte                BOOLEAN,
  cdma               BOOLEAN,
  hprd               BOOLEAN,
  umb                BOOLEAN,
  wlan               BOOLEAN,
  wiMAX              BOOLEAN,
...}

Ver2-PosProtocol-extension ::= SEQUENCE {
  lpp     BOOLEAN,
  posProtocolVersionRRLP           PosProtocolVersion3GPP OPTIONAL,
  posProtocolVersionRRC            PosProtocolVersion3GPP OPTIONAL,
  posProtocolVersionTIA801         PosProtocolVersion3GPP2 OPTIONAL,
  posProtocolVersionLPP  PosProtocolVersion3GPP OPTIONAL,
...}

PosProtocolVersion3GPP ::= SEQUENCE {
  majorVersionField      INTEGER(0..255),
  technicalVersionField  INTEGER(0..255),
  editorialVersionField  INTEGER(0..255),
...}

PosProtocolVersion3GPP2 ::= SEQUENCE (SIZE(1..8)) OF
Supported3GPP2PosProtocolVersion

Supported3GPP2PosProtocolVersion ::= SEQUENCE {
```

```
  revisionNumber                    BIT STRING(SIZE (6)), -- the location
standard revision number the SET supports coded according to 3GPP2 C.S0022
  pointReleaseNumber                INTEGER(0..255),
  internalEditLevel                 INTEGER(0..255),
...}

Ver2-PosTechnology-extension ::= SEQUENCE {
  gANSSPositionMethods  GANSSPositionMethods OPTIONAL,
...}

GANSSPositionMethods ::= SEQUENCE (SIZE(1..16)) OF GANSSPositionMethod

GANSSPositionMethod ::= SEQUENCE {
 ganssId                            INTEGER(0..15), -- coding according to
parameter definition in section 10.8
 ganssSBASid                        BIT STRING(SIZE(3)) OPTIONAL, --coding
according to parameter definition in section 10.8
 gANSSPositioningMethodTypes        GANSSPositioningMethodTypes,
 gANSSSignals                       GANSSSignals,
...}

GANSSPositioningMethodTypes ::= SEQUENCE {
  setAssisted         BOOLEAN,
  setBased            BOOLEAN,
  autonomous          BOOLEAN,
...}

Ver2-RequestedAssistData-extension ::= SEQUENCE {
  ganssRequestedCommonAssistanceDataList
GanssRequestedCommonAssistanceDataList OPTIONAL,
  ganssRequestedGenericAssistanceDataList
GanssRequestedGenericAssistanceDataList OPTIONAL,
  extendedEphemeris                 ExtendedEphemeris OPTIONAL,
  extendedEphemerisCheck            ExtendedEphCheck OPTIONAL,
...}

GanssRequestedCommonAssistanceDataList ::= SEQUENCE {
  ganssReferenceTime                            BOOLEAN,
  ganssIonosphericModel                         BOOLEAN,
  ganssAdditionalIonosphericModelForDataID00    BOOLEAN,
  ganssAdditionalIonosphericModelForDataID11    BOOLEAN,
  ganssEarthOrientationParameters               BOOLEAN,
...,
  ganssAdditionalIonosphericModelForDataID01    BOOLEAN OPTIONAL}

GanssRequestedGenericAssistanceDataList ::= SEQUENCE(SIZE(1..maxGANSS)) OF
GanssReqGenericData

GanssReqGenericData ::= SEQUENCE {
  ganssId   INTEGER(0..15), -- coding according to parameter definition in
section 10.8
  ganssSBASid BIT STRING(SIZE(3)) OPTIONAL, --coding according to parameter
definition in section 10.8
  ganssRealTimeIntegrity            BOOLEAN,
  ganssDifferentialCorrection       DGANSS-Sig-Id-Req OPTIONAL,
  ganssAlmanac                      BOOLEAN,
  ganssNavigationModelData          GanssNavigationModelData OPTIONAL,
  ganssTimeModels                   BIT STRING(SIZE(16)) OPTIONAL,
```

```
  ganssReferenceMeasurementInfo    BOOLEAN,
  ganssDataBits                    GanssDataBits OPTIONAL,
  ganssUTCModel                    BOOLEAN,
  ganssAdditionalDataChoices GanssAdditionalDataChoices OPTIONAL,
  ganssAuxiliaryInformation        BOOLEAN,
  ganssExtendedEphemeris           ExtendedEphemeris OPTIONAL,
  ganssExtendedEphemerisCheck      GanssExtendedEphCheck OPTIONAL,
...,
  bds-DifferentialCorrection       BDS-Sig-Id-Req OPTIONAL,
  bds-GridModelReq    BOOLEAN OPTIONAL}

DGANSS-Sig-Id-Req ::= BIT STRING (SIZE(8))

BDS-Sig-Id-Req ::= BIT STRING (SIZE(8))

GanssNavigationModelData ::= SEQUENCE {
ganssWeek                          INTEGER(0..4095),
ganssToe                           INTEGER(0..167),
t-toeLimit                         INTEGER(0..15),
satellitesListRelatedDataList      SatellitesListRelatedDataList OPTIONAL,
...}

SatellitesListRelatedDataList ::= SEQUENCE(SIZE(0..maxGANSSSat)) OF
SatellitesListRelatedData

SatellitesListRelatedData ::= SEQUENCE {
  satId  INTEGER(0..63),
  iod    INTEGER(0..1023),
...}

maxGANSS    INTEGER ::= 16
maxGANSSSat INTEGER ::= 32

GanssDataBits ::= SEQUENCE {
  ganssTODmin                      INTEGER (0..59),
  reqDataBitAssistanceList         ReqDataBitAssistanceList,
...}

ReqDataBitAssistanceList ::= SEQUENCE {
  gnssSignals                      GANSSSignals,
  ganssDataBitInterval             INTEGER (0..15),
  ganssDataBitSatList              SEQUENCE (SIZE(1..maxGANSSSat)) OF INTEGER
(0..63) OPTIONAL,
...}

GanssAdditionalDataChoices ::= SEQUENCE {
  orbitModelID       INTEGER(0..7) OPTIONAL,
  clockModelID       INTEGER(0..7) OPTIONAL,
  utcModelID         INTEGER(0..7) OPTIONAL,
  almanacModelID     INTEGER(0..7) OPTIONAL,
...}

ExtendedEphemeris ::= SEQUENCE {
  validity        INTEGER (1..256), -- Requested validity in 4 hour steps
  ...}

ExtendedEphCheck ::= SEQUENCE {
  beginTime       GPSTime, -- Begin time of ephemeris extension held by SET
```

```
  endTime         GPSTime, -- End time of ephemeris extension held by SET
  ...}

GanssExtendedEphCheck ::= SEQUENCE {
  beginTime  GANSSextEphTime, -- Begin time of ephemeris extension held by SET
  endTime    GANSSextEphTime, -- End time of ephemeris extension held by SET
  ...}

GPSTime ::= SEQUENCE {
  gPSWeek    INTEGER (0..1023),
  gPSTOWhour INTEGER (0..167),
...}

GANSSextEphTime ::= SEQUENCE {
  gANSSday       INTEGER (0..8191),
  gANSSTODhour   INTEGER (0..23),
...}

Ver2-PosPayLoad-extension ::= SEQUENCE {
   lPPPayload SEQUENCE (SIZE (1..3)) OF OCTET STRING(SIZE (1..60000)) OPTIONAL,
   tIA801Payload SEQUENCE (SIZE(1..3)) OF OCTET STRING(SIZE (1..60000))
OPTIONAL,
...} -- a combination of both lPPPayload and tIA801Payload messages within a
-- single Ver2-PosPayLoad-extension message SHALL NOT be used


END
```

11.6 Parameter Extensions (SUPL Version 3)

```
ULP-Version-3-parameter-extensions DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

EXPORTS
Ver3-PosProtocol-extension, Ver3-SETCapabilities-extension, Ver3-TriggerParams-
extension, Ver3-ServiceSupported-extensions, Ver3-ProtectionLevel-extension,
Ver3-PosPayLoad-rep-extensions;

IMPORTS
  QoPCapabilities, RelativePositioningCapabilities,
CivicPositioningCapabilities
FROM ULP-Version-3-message-extensions
  TrackingAreaCode
FROM Ver2-ULP-Components;

Ver3-PosProtocol-extension ::= SEQUENCE {
  posProtocolVersionLPPe           PosProtocolVersionOMA OPTIONAL,
...}

Ver3-SETCapabilities-extension ::= SEQUENCE {
  qoPCapabilities              QoPCapabilities OPTIONAL,
  civicPositioningCapabilities CivicPositioningCapabilities OPTIONAL,
  relativePositioningCapabilities
                               RelativePositioningCapabilities OPTIONAL,
  d-SLP-Provision-from-H-SLP                                    BOOLEAN,
  e-SLP-Provision-from-H-SLP                                    BOOLEAN,
  d-SLP-Provision-from-Proxy-D-SLP                              BOOLEAN,
  e-SLP-Provision-from-Proxy-E-SLP                              BOOLEAN,
```

```
  d-SLP-Notification-to-H-SLP                                    BOOLEAN,
  sensorSupport                                                  BOOLEAN,
  sUPLINITRootKeyStatus        SUPLINITRootKeyStatus OPTIONAL,
...}

SUPLINITRootKeyStatus ::= ENUMERATED {invalidSUPLINITRootKey(0),
outofsyncSUPLINITRootKey(1), ...}

PosProtocolVersionOMA ::= SEQUENCE {
  majorVersionField      INTEGER(0..255),
  minorVersionField      INTEGER(0..255),
...}

Ver3-TriggerParams-extension::= CHOICE {
        velocityEventParams       VelocityEventParams,
...}

VelocityEventParams ::= SEQUENCE {
  velocityEventType               VelocityEventType,
  velocityEstimate                BOOLEAN,
  repeatedReportingParams         RepeatedReportingParams OPTIONAL,
  startTime                       INTEGER(0..2678400) OPTIONAL,
  stopTime                        INTEGER(0..11318399) OPTIONAL,
  targetSpeed                     TargetSpeed  OPTIONAL,
  ...}

-- startTime and stopTime are in seconds.
-- startTime and stop Time are in relative time in units of seconds measured
-- from "now"
-- a value of 0 signifies "now"
-- stopTime must be > startTime
-- stopTime - startTime shall not exceed 8639999
-- (100 days in seconds) for compatibility with OMA MLP and RLP

RepeatedReportingParams ::= SEQUENCE {
  minimumIntervalTime             INTEGER (1..604800), -- time in seconds
  maximumNumberOfReports          INTEGER (1..1024),
  ...}

VelocityEventType ::= ENUMERATED {increasingAbove(0),
above(1),decreasingBelow(2),below(3), ...}

TargetSpeed ::= INTEGER(1..65536) -- in units of km/hour

Ver3-ServiceSupported-extensions ::= SEQUENCE {
  velocityTrigger     BOOLEAN,
...}

Ver3-LTEAreaId-extension ::= SEQUENCE {
  trackingAreaCode    TrackingAreaCode OPTIONAL,
...}

Ver3-ProtectionLevel-extension ::= SEQUENCE {
  keyIdentifierType               KeyIdentifierType,
  keyIdentifier                   OCTET STRING(SIZE (8)),
  basicReplayCounter  INTEGER(0..65535),
  basicMAC                                  BIT STRING(SIZE (32)),
...}
```

```
KeyIdentifierType ::= ENUMERATED {
 modeAKeyIdentifier(0), temporaryModeAKeyIdentifier(1), modeBKeyIdentifier(2),
...}

Ver3-PosPayload-rep-extensions ::= SEQUENCE {
  posPayload-rep PosPayload-rep,
...}

PosPayload-rep ::= CHOICE {
  lPPpayload  OCTET STRING(SIZE (1..60000)),
  tia801payload  OCTET STRING(SIZE (1..600000)),
...}

END
```

11.7 Common elements (SUPL Version 1)

```
ULP-Components DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

EXPORTS Version, SessionID, IPAddress, SLPAddress, LocationId, Position,
StatusCode, Velocity, QoP, PosMethod, Ver, SETId, PrimaryCPICH-Info,
CellParametersID, FQDN;

IMPORTS
        Ver2-CellInfo-extension
FROM Ver2-ULP-Components
        Ver3-CellInfo-extension, Ver3-PositionEstimate-extension, Ver3-
Velocity-extension
FROM Ver3-ULP-Components;

-- protocol version expressed as x.y.z (e.g., 5.1.0)--
Version ::= SEQUENCE {
  maj      INTEGER(0..255),
  min      INTEGER(0..255),
  servind  INTEGER(0..255)}

SessionID ::= SEQUENCE {
  setSessionID  SetSessionID OPTIONAL, -- the semantics of OPTIONAL applies to
the encoding only. The parameter itself is MANDATORY. This is introduced only
to minimize bandwidth for the SUPL INIT message. Since the setSessionID is
allocated by the SET, there is no setSessionID to be transmitted in the SUPL
INIT message.
  slpSessionID  SlpSessionID OPTIONAL -- the semantics of OPTIONAL applies to
the encoding only. The parameter itself is MANDATORY. This is introduced only
to minimize bandwidth for the SUPL START, SUPL TRIGGERED START and SUPL SET
INIT messages. Since the slpSessionID is allocated by the SLP, there is no
slpSessionID to be transmitted in these messages (with the exception described
in section 10.14).--
}

SetSessionID ::= SEQUENCE {sessionId  INTEGER(0..65535),
                           setId      SETId}

SETId ::= CHOICE {
  msisdn     OCTET STRING(SIZE (8)),
  mdn        OCTET STRING(SIZE (8)),
```

```
  min        BIT STRING(SIZE (34)), -- coded according to [TIA-553]
  imsi       OCTET STRING(SIZE (8)),
  nai        IA5String(SIZE (1..1000)),
  iPAddress  IPAddress,
  ...}
-- msisdn, mnd and imsi are a BCD (Binary Coded Decimal) string
-- represent digits from 0 through 9,
-- two digits per octet, each digit encoded 0000 to 1001 (0 to 9)
-- bits 8765 of octet n encoding digit 2n
-- bits 4321 of octet n encoding digit 2(n-1) +1
-- not used digits in the string shall be filled with 1111

SlpSessionID ::= SEQUENCE {
  sessionID  OCTET STRING(SIZE (4)),
  slpId      SLPAddress}

IPAddress ::= CHOICE {
  ipv4Address  OCTET STRING(SIZE (4)),
  ipv6Address  OCTET STRING(SIZE (16))}

SLPAddress ::= CHOICE {iPAddress  IPAddress,
                       fQDN       FQDN,
                       ...}

FQDN ::=
  VisibleString(FROM ("a".."z" | "A".."Z" | "0".."9" |".-"))(SIZE (1..255))

Ver ::= BIT STRING(SIZE (64))

LocationId ::= SEQUENCE {cellInfo  CellInfo,
                         status    Status,
                         ...}

Status ::= ENUMERATED {stale(0), current(1), unknown(2), ...}

CellInfo ::= CHOICE {
  gsmCell    GsmCellInformation,
  wcdmaCell  WcdmaCellInformation, --WCDMA Cell Information/TD-SCDMA Cell
Information
  cdmaCell   CdmaCellInformation,
  ...,
  ver2-CellInfo-extension          Ver2-CellInfo-extension,
  ver3-CellInfo-extension          Ver3-CellInfo-extension}

Position ::= SEQUENCE {
  timestamp         UTCTime, -- shall include seconds and shall use UTC time.
  positionEstimate  PositionEstimate,
  velocity          Velocity OPTIONAL,
  ...}

PositionEstimate ::= SEQUENCE {
  latitudeSign  ENUMERATED {north, south},
  latitude      INTEGER(0..8388607),
  longitude     INTEGER(-8388608..8388607),
  uncertainty
    SEQUENCE {uncertaintySemiMajor  INTEGER(0..127),
              uncertaintySemiMinor  INTEGER(0..127),
```

```
              orientationMajorAxis  INTEGER(0..180)} OPTIONAL, -- angle in
degree between major axis and North
  confidence    INTEGER(0..100) OPTIONAL,
  altitudeInfo  AltitudeInfo OPTIONAL,
  ..., -- Coding as in [3GPP GAD]
  ver3-PositionEstimate-extension  Ver3-PositionEstimate-extension OPTIONAL}
-- this extension defines high accuracy 3D position as defined in [OMA-LPPe]

AltitudeInfo ::= SEQUENCE {
  altitudeDirection  ENUMERATED {height, depth},
  altitude           INTEGER(0..32767),
  altUncertainty     INTEGER(0..127),
  ... } -- based on [3GPP GAD]

CdmaCellInformation ::= SEQUENCE {
  refNID         INTEGER(0..65535), -- Network Id
  refSID         INTEGER(0..32767), -- System Id
  refBASEID      INTEGER(0..65535), -- Base Station Id
  refBASELAT     INTEGER(0..4194303), -- Base Station Latitude
  reBASELONG     INTEGER(0..8388607), -- Base Station Longitude
  refREFPN       INTEGER(0..511), -- Base Station PN Code
  refWeekNumber  INTEGER(0..65535), -- GPS Week Number
  refSeconds     INTEGER(0..4194303), -- GPS Seconds --
  ...}

GsmCellInformation ::= SEQUENCE {
  refMCC  INTEGER(0..999), -- Mobile Country Code
  refMNC  INTEGER(0..999), -- Mobile Network Code
  refLAC  INTEGER(0..65535), -- Location area code
  refCI   INTEGER(0..65535), -- Cell identity
  nMR     NMR OPTIONAL,
  tA      INTEGER(0..255) OPTIONAL, --Timing Advance
  ...}

WcdmaCellInformation ::= SEQUENCE {
  refMCC                 INTEGER(0..999), -- Mobile Country Code
  refMNC                 INTEGER(0..999), -- Mobile Network Code
  refUC                  INTEGER(0..268435455), -- Cell identity
  frequencyInfo          FrequencyInfo OPTIONAL,
  primaryScramblingCode  INTEGER(0..511) OPTIONAL, -- Not applicable for TDD
  measuredResultsList    MeasuredResultsList OPTIONAL,
  ...,
  cellParametersId       INTEGER(0..127) OPTIONAL, -- Not applicable for FDD
  timingAdvance          TimingAdvance OPTIONAL -- Not applicable for FDD
}

TimingAdvance ::= SEQUENCE {
 tA     INTEGER (0..8191),
 tAResolution    TAResolution OPTIONAL, -- If missing, resolution is 0.125
chips
 chipRate        ChipRate OPTIONAL, -- If missing, chip rate is 1.28 Mchip/s
...}

TAResolution ::= ENUMERATED {res10chip(0),res05chip(1),res0125chip(2), ...} --
Corresponding to 1.0-chip, 0.5-chip and 0.125-chip resolutions, respectively

ChipRate ::= ENUMERATED {tdd128(0),tdd384(1), tdd768(2), ...} -- Corresponding
to 1.28-Mchips/s, 3.84-Mchips/s and 7.68-Mchips/s chip rates, respectively
```

```
FrequencyInfo ::= SEQUENCE {
  modeSpecificInfo  CHOICE {fdd  FrequencyInfoFDD,
                            tdd  FrequencyInfoTDD,
                            ...},
  ...}

FrequencyInfoFDD ::= SEQUENCE {
  uarfcn-UL  UARFCN OPTIONAL,
  uarfcn-DL  UARFCN,
  ...}

FrequencyInfoTDD ::= SEQUENCE {uarfcn-Nt  UARFCN,
                               ...}

UARFCN ::= INTEGER(0..16383)

NMR ::= SEQUENCE (SIZE (1..15)) OF NMRelement

NMRelement ::= SEQUENCE {
  aRFCN  INTEGER(0..1023),
  bSIC   INTEGER(0..63),
  rxLev  INTEGER(0..63),
  ...}

MeasuredResultsList ::= SEQUENCE (SIZE (1..maxFreq)) OF MeasuredResults

MeasuredResults ::= SEQUENCE {
  frequencyInfo            FrequencyInfo OPTIONAL,
  utra-CarrierRSSI         UTRA-CarrierRSSI OPTIONAL,
  cellMeasuredResultsList  CellMeasuredResultsList OPTIONAL}

CellMeasuredResultsList ::=
  SEQUENCE (SIZE (1..maxCellMeas)) OF CellMeasuredResults

-- SPARE: UTRA-CarrierRSSI, Max = 76
-- Values above Max are spare
UTRA-CarrierRSSI ::= INTEGER(0..127)

CellMeasuredResults ::= SEQUENCE {
  cellIdentity      INTEGER(0..268435455) OPTIONAL,
  modeSpecificInfo
    CHOICE {fdd
              SEQUENCE {primaryCPICH-Info  PrimaryCPICH-Info,
                        cpich-Ec-N0        CPICH-Ec-N0 OPTIONAL,
                        cpich-RSCP         CPICH-RSCP OPTIONAL,
                        pathloss           Pathloss OPTIONAL},
            tdd
              SEQUENCE {cellParametersID   CellParametersID,
                        proposedTGSN       TGSN OPTIONAL,
                        primaryCCPCH-RSCP  PrimaryCCPCH-RSCP OPTIONAL,
                        pathloss           Pathloss OPTIONAL,
                        timeslotISCP-List  TimeslotISCP-List OPTIONAL -- NOTE:
TimeSlotISCP measurement list cannot be interpreted without the knowledge of
Cell Info as defined in [3GPP RRC]
}}}
```

```
CellParametersID ::= INTEGER(0..127)

TGSN ::= INTEGER(0..14)

PrimaryCCPCH-RSCP ::= INTEGER(0..127)

-- SPARE: TimeslotISCP, Max = 91
-- Values above Max are spare
TimeslotISCP ::= INTEGER(0..127)

TimeslotISCP-List ::= SEQUENCE (SIZE (1..maxTS)) OF TimeslotISCP

PrimaryCPICH-Info ::= SEQUENCE {primaryScramblingCode  INTEGER(0..511)}

-- SPARE: CPICH-Ec-No, Max = 49
-- Values above Max are spare
CPICH-Ec-N0 ::= INTEGER(0..63)

-- SPARE: CPICH- RSCP, data range from 0 to 91 and from 123 to 127.
-- Values from 92 to 122 are spare
-- the encoding of cpich-RSCP is (as per [3GPP RRC] V5.11.0)

-- cpich-RSCP = 123    CPICH RSCP <-120 dBm
-- cpich-RSCP = 124    -120 ≤ CPICH RSCP < -119 dBm
-- cpich-RSCP = 125    -119 ≤ CPICH RSCP < -118 dBm
-- cpich-RSCP = 126    -118 ≤ CPICH RSCP < -117 dBm
-- cpich-RSCP = 127    -117 ≤ CPICH RSCP < -116 dBm
-- cpich-RSCP = 0      -116 ≤ CPICH RSCP < -115 dBm
-- cpich-RSCP = 1      -115 ≤ CPICH RSCP < -114 dBm
-- …       …      …
-- cpich-RSCP = 89     -27 ≤ CPICH RSCP < -26 dBm
-- cpich-RSCP = 90     -26 ≤ CPICH RSCP < -25 dBm
-- cpich-RSCP = 91     -25 ≤ CPICH RSCP       dBm

CPICH-RSCP ::= INTEGER(0..127)

-- SPARE: Pathloss, Max = 158
-- Values above Max are spare
Pathloss ::= INTEGER(46..173)

maxCellMeas INTEGER ::= 32

maxFreq INTEGER ::= 8

maxTS INTEGER ::= 14

StatusCode ::= ENUMERATED {
  unspecified(0), systemFailure(1), unexpectedMessage(2), protocolError(3),
  dataMissing(4), unexpectedDataValue(5), posMethodFailure(6),
  posMethodMismatch(7), posProtocolMismatch(8), targetSETnotReachable(9),
  versionNotSupported(10), resourceShortage(11), invalidSessionId(12),
  nonProxyModeNotSupported(13), proxyModeNotSupported(14),
  positioningNotPermitted(15), authNetFailure(16), authSuplinitFailure(17),
consentDeniedByUser(100), consentGrantedByUser(101), ..., ver2-
incompatibleProtectionLevel(18), ver2-serviceNotSupported(19), ver2-
insufficientInterval(20), ver2-noSUPLCoverage(21), ver2-sessionStopped(102),
ver2-appIdDenied(103), ver3-locationURIUnavailable (130), ver3-
locationURINotSupported (131), ver3-locationURINotAuthorized (132), ver3-
```

```
gssCapabilityMismatch(133), ver3-unauthorizedAccessToSLP (134), ver3-
invalidAccessToSLP (135), ver3-RelativeLocationNotSupported(136), ver3-
ReferencePointNotSupported(137)}

QoP ::= SEQUENCE {
  horacc     INTEGER(0..127),
  veracc     INTEGER(0..127) OPTIONAL, -- as defined in [3GPP GAD] "uncertainty
altitude"
  maxLocAge  INTEGER(0..65535) OPTIONAL,
  delay      INTEGER(0..7) OPTIONAL, -- as defined in [3GPP RRLP]
  ...}

Velocity ::= CHOICE {
  horvel           Horvel,
  horandvervel     Horandvervel,
  horveluncert     Horveluncert,
  horandveruncert  Horandveruncert,
  ..., -- velocity definition as per [3GPP GAD]
  ver3-Velocity-extension          Ver3-Velocity-extension} -- this extension
defines high accuracy 3D velocity as defined in [OMA-LPPe]

Horvel ::= SEQUENCE {
  bearing   BIT STRING(SIZE (9)),
  horspeed  BIT STRING(SIZE (16)),
  ...}

Horandvervel ::= SEQUENCE {
  verdirect  BIT STRING(SIZE (1)),
  bearing    BIT STRING(SIZE (9)),
  horspeed   BIT STRING(SIZE (16)),
  verspeed   BIT STRING(SIZE (8)),
  ...}

Horveluncert ::= SEQUENCE {
  bearing      BIT STRING(SIZE (9)),
  horspeed     BIT STRING(SIZE (16)),
  uncertspeed  BIT STRING(SIZE (8)),
  ...}

Horandveruncert ::= SEQUENCE {
  verdirect       BIT STRING(SIZE (1)),
  bearing         BIT STRING(SIZE (9)),
  horspeed        BIT STRING(SIZE (16)),
  verspeed        BIT STRING(SIZE (8)),
  horuncertspeed  BIT STRING(SIZE (8)),
  veruncertspeed  BIT STRING(SIZE (8)),
  ...}

PosMethod ::= ENUMERATED {
agpsSETassisted(0), agpsSETbased(1), agpsSETassistedpref(2),
agpsSETbasedpref(3), autonomousGPS(4), aFLT(5), eCID(6), eOTD(7), oTDOA(8),
noPosition(9), ..., ver2-historicalDataRetrieval(10), ver2-
agnssSETassisted(11), ver2-agnssSETbased(12), ver2-agnssSETassistedpref(13),
ver2-agnssSETbasedpref(14), ver2-autonomousGNSS(15), ver2-sessioninfoquery(16),
ver3-genericSETassisted(17), ver3-genericSETbased(18), ver3-gss(19), ver3-
other(20)}

END
```

11.8 Common elements (SUPL Version 2)

```
Ver2-ULP-Components DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

EXPORTS Ver2-CellInfo-extension, MultipleLocationIds,
SupportedNetworkInformation, CauseCode, UTRAN-GPSReferenceTimeAssistance,
UTRAN-GPSReferenceTimeResult, SPCSETKey, SPCTID, SPCSETKeylifetime, UTRAN-
GANSSReferenceTimeAssistance, UTRAN-GANSSReferenceTimeResult,
GNSSPosTechnology, GANSSSignals, ThirdParty, ApplicationID, ReportingCap,
Coordinate, CircularArea, EllipticalArea, PolygonArea;

IMPORTS
        LocationId, PrimaryCPICH-Info, CellParametersID, FQDN
FROM ULP-Components;

MultipleLocationIds ::= SEQUENCE SIZE (1..maxLidSize) OF LocationIdData

LocationIdData ::= SEQUENCE {
locationId           LocationId,
relativetimestamp    RelativeTime OPTIONAL, -- if relativetimestamp is
present, then data represents historical measurement, if absent, data
represents current measurements
servingFlag          BOOLEAN, -- if "true" measurements represent serving cell
...}

RelativeTime ::= INTEGER (0..65535) -- relative time to "current" Location Id
in multiples of 0.01sec

maxLidSize           INTEGER ::= 64

SupportedNetworkInformation ::= SEQUENCE {
  wLAN                          BOOLEAN,
  supportedWLANInfo             SupportedWLANInfo OPTIONAL,
  supportedWLANApsList          SupportedWLANApsList OPTIONAL,
  gSM                           BOOLEAN,
  wCDMA                         BOOLEAN,
  supportedWCDMAInfo            SupportedWCDMAInfo OPTIONAL,
  cDMA                          BOOLEAN,
  hRDP                          BOOLEAN,
  uMB                           BOOLEAN,
  lTE                           BOOLEAN,
  wIMAX                         BOOLEAN,
  historic                      BOOLEAN,
  nonServing                    BOOLEAN,
  uTRANGPSReferenceTime         BOOLEAN,
  uTRANGANSSReferenceTime       BOOLEAN,
  ...}

SupportedWLANInfo ::= SEQUENCE {
  apTP        BOOLEAN, -- AP transmit power
  apAG        BOOLEAN, -- AP antenna gain
  apSN        BOOLEAN, -- AP S/N received at SET
  apDevType   BOOLEAN, -- Device type
  apRSSI      BOOLEAN, -- AP signal strength at SET
  apChanFreq  BOOLEAN, -- AP channel/frequency of Tx/Rx
  apRTD       BOOLEAN, -- Round Trip Delay between SET and AP
  setTP       BOOLEAN, -- SET transmit power
```

```
  setAG       BOOLEAN, -- SET antenna gain
  setSN       BOOLEAN, -- SET S/N received at AP
  setRSSI     BOOLEAN, -- SET signal strength at AP
  apRepLoc    BOOLEAN, -- AP Location as reported by AP
  ...}

maxWLANApDataSize    INTEGER ::= 128

SupportedWLANApsList ::= SEQUENCE {
 supportedWLANApDataList     SEQUENCE (SIZE (1..maxWLANApDataSize)) OF
SupportedWLANApData,
 supportedWLANapsChannel11a  SupportedWLANApsChannel11a  OPTIONAL,
 supportedWLANapsChannel11bg SupportedWLANApsChannel11bg OPTIONAL,
 ...
}

SupportedWLANApsChannel11a ::= SEQUENCE {
 ch34    BOOLEAN,
 ch36    BOOLEAN,
 ch38    BOOLEAN,
 ch40    BOOLEAN,
 ch42    BOOLEAN,
 ch44    BOOLEAN,
 ch46    BOOLEAN,
 ch48    BOOLEAN,
 ch52    BOOLEAN,
 ch56    BOOLEAN,
 ch60    BOOLEAN,
 ch64    BOOLEAN,
 ch149   BOOLEAN,
 ch153   BOOLEAN,
 ch157   BOOLEAN,
 ch161   BOOLEAN
}

SupportedWLANApsChannel11bg ::= SEQUENCE {
 ch1  BOOLEAN,
 ch2  BOOLEAN,
 ch3  BOOLEAN,
 ch4  BOOLEAN,
 ch5  BOOLEAN,
 ch6  BOOLEAN,
 ch7  BOOLEAN,
 ch8  BOOLEAN,
 ch9  BOOLEAN,
 ch10 BOOLEAN,
 ch11 BOOLEAN,
 ch12 BOOLEAN,
 ch13 BOOLEAN,
 ch14 BOOLEAN
}

SupportedWLANApData ::= SEQUENCE {
 apMACAddress  BIT STRING (SIZE (48)),
 apDevType  ENUMERATED {wlan802-11a(0), wlan802-11b(1), wlan802-11g(2), ...},
 ...}

SupportedWCDMAInfo ::= SEQUENCE {
```

```
  mRL    BOOLEAN, -- Measured Results List
  ...}

Ver2-CellInfo-extension ::= CHOICE {
  hrpdCell   HrpdCellInformation,
  umbCell    UmbCellInformation,
  lteCell    LteCellInformation,
  wlanAP     WlanAPInformation,
  wimaxBS    WimaxBSInformation,
  ...}

HrpdCellInformation ::= SEQUENCE {
  refSECTORID    BIT STRING(SIZE (128)) OPTIONAL, -- HRPD Sector Id
  refBASELAT     INTEGER(0..4194303), -- Base Station Latitude
  reBASELONG     INTEGER(0..8388607), -- Base Station Longitude
  refWeekNumber  INTEGER(0..65535), -- GPS Week Number
  refSeconds     INTEGER(0..4194303), -- GPS Seconds --
  ...}

UmbCellInformation ::= SEQUENCE {
  refSECTORID         BIT STRING(SIZE (128)), -- UMB Sector Id
  refMCC              INTEGER(0..999), -- Mobile Country Code
  refMNC              INTEGER(0..999), -- Mobile Network Code
  refBASELAT          INTEGER(0..4194303), -- Base Station Latitude
  reBASELONG          INTEGER(0..8388607), -- Base Station Longitude
  refWeekNumber       INTEGER(0..65535), -- GPS Week Number
  refSeconds          INTEGER(0..4194303), -- GPS Seconds --
  ...}

-- LTE Cell info per [3GPP LTE] --
-- If not otherwise stated info is related to serving cell --

LteCellInformation ::= SEQUENCE {
  cellGlobalIdEUTRA               CellGlobalIdEUTRA,
  physCellId                      PhysCellId,
  trackingAreaCode                TrackingAreaCode,
  rsrpResult                      RSRP-Range   OPTIONAL,
  rsrqResult                      RSRQ-Range   OPTIONAL,
  tA      INTEGER(0..1282) OPTIONAL, -- Timing Advance as per [3GPP 36.321]
  measResultListEUTRA   MeasResultListEUTRA OPTIONAL, --Neighbour measurements
  ...}

-- Measured results of neighbours cells per [3GPP LTE] --

MeasResultListEUTRA ::= SEQUENCE (SIZE (1..maxCellReport)) OF MeasResultEUTRA

MeasResultEUTRA ::=   SEQUENCE {
 physCellId PhysCellId,
 cgi-Info SEQUENCE {
        cellGlobalId CellGlobalIdEUTRA,
        trackingAreaCode TrackingAreaCode
} OPTIONAL,
 measResult SEQUENCE {
        rsrpResult   RSRP-Range   OPTIONAL,  -- Mapping to measured values
        rsrqResult   RSRQ-Range   OPTIONAL,  -- in 3GPP TS 36.133
        ...
 }
}
```

```
PhysCellId ::=         INTEGER (0..503)

TrackingAreaCode ::=  BIT STRING (SIZE (16))

CellGlobalIdEUTRA ::= SEQUENCE {
 plmn-Identity        PLMN-Identity,
 cellIdentity         CellIdentity,
 ...
}

PLMN-Identity ::= SEQUENCE {
 mcc MCC OPTIONAL,
 mnc MNC
}

CellIdentity ::= BIT STRING (SIZE (28))

MCC ::= SEQUENCE (SIZE (3)) OF MCC-MNC-Digit

MNC ::=  SEQUENCE (SIZE (2..3)) OF MCC-MNC-Digit

MCC-MNC-Digit ::= INTEGER (0..9)

RSRP-Range ::= INTEGER(0..97)
RSRQ-Range ::= INTEGER(0..34)
maxCellReport INTEGER ::= 8

WlanAPInformation ::= SEQUENCE { -- as per [IEEE 802.11]
  apMACAddress       BIT STRING(SIZE (48)), -- AP MAC Address
  apTransmitPower    INTEGER(-127..128) OPTIONAL, -- AP transmit power in dbm
  apAntennaGain      INTEGER(-127..128) OPTIONAL, -- AP antenna gain in dBi
  apSignaltoNoise    INTEGER(-127..128) OPTIONAL, -- AP S/N received at SET
  apDeviceType       ENUMERATED {wlan802-11a(0), wlan802-11b(1), wlan802-
11g(2), ...} OPTIONAL,
  apSignalStrength   INTEGER(-127..128) OPTIONAL, -- AP signal strength at SET
  apChannelFrequency INTEGER(0..256) OPTIONAL, -- AP channel/frequency of Tx/Rx
  apRoundTripDelay   RTD OPTIONAL, -- Round Trip Delay between SET and AP
  setTransmitPower   INTEGER(-127..128) OPTIONAL, -- SET transmit power in dBm
  setAntennaGain     INTEGER (-127..128) OPTIONAL, -- SET antenna gain in dBi
  setSignaltoNoise   INTEGER (-127..128) OPTIONAL, -- SET S/N received at AP
  setSignalStrength  INTEGER(-127..128) OPTIONAL, -- SET signal strength at AP
  apReportedLocation ReportedLocation OPTIONAL, -- AP Location reported by AP
  ...}

RTD ::= SEQUENCE { -- as per [IEEE 802.11]
  rTDValue     INTEGER(0..16777216), -- measured RTD value corresponding to
-- about 500km in units of 1/10 of nanoseconds
  rTDUnits     RTDUnits, -- units of RTD
  rTDAccuracy  INTEGER(0..255) OPTIONAL, -- RTD accuracy
  ...}

RTDUnits ::= ENUMERATED {
  microseconds(0), hundredsofnanoseconds(1), tensofnanoseconds(2),
nanoseconds(3), tenthsofnanoseconds(4), ...}

ReportedLocation ::= SEQUENCE { -- as per [IEEE 802.11v]
  locationEncodingDescriptor  LocationEncodingDescriptor,
```

```
  locationData        LocationData, -- location data field
  ...}

LocationEncodingDescriptor ::= ENUMERATED {
  lCI(0), aSN1(1), ...}

LocationData ::= SEQUENCE {
  locationAccuracy   INTEGER(0..4294967295) OPTIONAL,
  locationValue      OCTET STRING (SIZE(1..128)),
  ...}

WimaxBSInformation ::= SEQUENCE {
  wimaxBsID          WimaxBsID,    -- WiMax serving base station ID
  wimaxRTD           WimaxRTD     OPTIONAL, -- Round Trip Delay measurements
  wimaxNMRList       WimaxNMRList OPTIONAL, -- Network measurements
  ...}

WimaxBsID ::= SEQUENCE {
  bsID-MSB           BIT STRING (SIZE(24)) OPTIONAL,
  bsID-LSB           BIT STRING (SIZE(24)),
 ...}
-- if only LSB is present, MSB is assumed to be identical to the current
serving BS or clamped on network value

WimaxRTD ::= SEQUENCE {
  rTD    INTEGER (0..65535), -- Round trip delay of serving BS in units of 10
ns
  rTDstd INTEGER (0..1023) OPTIONAL, -- Standard deviation of round trip delay
in units of 10 ns
...}

WimaxNMRList ::= SEQUENCE  (SIZE (1..maxWimaxBSMeas)) OF WimaxNMR

WimaxNMR ::= SEQUENCE {
  wimaxBsID   WimaxBsID,           -- WiMax BS ID for the measurement
  relDelay    INTEGER (-32768..32767) OPTIONAL, -- Relative delay for this
neighbouring BSs to the serving cell in units of 10 ns
  relDelaystd  INTEGER (0..1023) OPTIONAL, -- Standard deviation of Relative
delay in units of 10 ns
  rSSI        INTEGER (0..255) OPTIONAL, -- RSSI in 0.25 dBm steps, starting
from -103.75 dBm
  rSSIstd     INTEGER (0..63) OPTIONAL, -- Standard deviation of RSSI in dB
  bSTxPower   INTEGER (0..255) OPTIONAL, -- BS transmit power in 0.25 dBm
steps, starting from -103.75 dBm
  cINR        INTEGER (0..255) OPTIONAL, -- in dB
  cINRstd     INTEGER (0..63) OPTIONAL, -- Standard deviation of CINR in dB
  bSLocation  ReportedLocation OPTIONAL, -- Reported location of the BS
...}

maxWimaxBSMeas INTEGER ::= 32

UTRAN-GPSReferenceTimeAssistance ::= SEQUENCE {
utran-GPSReferenceTime             UTRAN-GPSReferenceTime,
gpsReferenceTimeUncertainty        INTEGER (0..127) OPTIONAL,
utranGPSDriftRate                  UTRANGPSDriftRate OPTIONAL}

UTRAN-GPSReferenceTime ::= SEQUENCE {
```

```
-- For utran-GPSTimingOfCell values above 2322431999999 are not used in this
version of the specification. Actual value utran-GPSTimingOfCell = (ms-part *
4294967296) + ls-part used on the downlink i.e. sent from the SLP to the SET
     utran-GPSTimingOfCell         SEQUENCE {
        ms-part       INTEGER (0..1023),
        ls-part       INTEGER (0..4294967295)},
            modeSpecificInfo      CHOICE {
                      fdd         SEQUENCE {
                        referenceIdentity      PrimaryCPICH-Info},
                      tdd         SEQUENCE {
                        referenceIdentity      CellParametersID}} OPTIONAL,
            sfn       INTEGER (0..4095)}

UTRANGPSDriftRate ::= ENUMERATED {
      utran-GPSDrift0, utran-GPSDrift1, utran-GPSDrift2,
      utran-GPSDrift5, utran-GPSDrift10, utran-GPSDrift15,
      utran-GPSDrift25, utran-GPSDrift50, utran-GPSDrift-1,
      utran-GPSDrift-2, utran-GPSDrift-5, utran-GPSDrift-10,
      utran-GPSDrift-15, utran-GPSDrift-25, utran-GPSDrift-50}

UTRAN-GPSReferenceTimeResult ::= SEQUENCE {
-- For ue-GPSTimingOfCell values above 37158911999999 are not used in this
version of the specification. Actual value utran-GPSTimingOfCell = (ms-part *
4294967296) + ls-part used on the uplink i.e. reported by the SET to the SLP
     set-GPSTimingOfCell           SEQUENCE {
        ms-part       INTEGER (0.. 16383),
        ls-part       INTEGER (0..4294967295)},
            modeSpecificInfo      CHOICE {
                      fdd         SEQUENCE {
                        referenceIdentity      PrimaryCPICH-Info},
                      tdd         SEQUENCE {
                        referenceIdentity      CellParametersID}} OPTIONAL,
            sfn       INTEGER (0..4095),
     gpsReferenceTimeUncertainty   INTEGER (0..127) OPTIONAL,
     ...}

UTRAN-GANSSReferenceTimeAssistance ::= SEQUENCE {
ganssDay INTEGER (0..8191) OPTIONAL,
ganssTimeID           INTEGER (0..15),
utran-GANSSReferenceTime           UTRAN-GANSSReferenceTime,
utranGANSSDriftRate   UTRANGANSSDriftRate       OPTIONAL}

UTRAN-GANSSReferenceTime ::= SEQUENCE {

     ganssTOD INTEGER (0..86399),
     utran-GANSSTimingOfCell       INTEGER (0..3999999)OPTIONAL,
            modeSpecificInfo      CHOICE {
                      fdd         SEQUENCE {
                        referenceIdentity      PrimaryCPICH-Info},
                      tdd         SEQUENCE {
                        referenceIdentity      CellParametersID}} OPTIONAL,
            sfn       INTEGER (0..4095),
            ganss-TODUncertainty INTEGER (0..127) OPTIONAL,
...}

UTRANGANSSDriftRate ::= ENUMERATED {
      utran-GANSSDrift0, utran-GANSSDrift1, utran-GANSSDrift2,
      utran-GANSSDrift5, utran-GANSSDrift10, utran-GANSSDrift15,
```

```
      utran-GANSSDrift25, utran-GANSSDrift50, utran-GANSSDrift-1,
      utran-GANSSDrift-2, utran-GANSSDrift-5, utran-GANSSDrift-10,
      utran-GANSSDrift-15, utran-GANSSDrift-25, utran-GANSSDrift-50}

UTRAN-GANSSReferenceTimeResult ::= SEQUENCE {
     ganssTimeID      INTEGER (0..15),
     set-GANSSReferenceTime        SET-GANSSReferenceTime,
            ...}

SET-GANSSReferenceTime ::= SEQUENCE {
-- Actual value [ns] = (ms-Part * 4294967296 + ls-Part) * 250
-- Actual values [ns] > 86399999999750 are reserved and are considered a
-- protocol error
            set-GANSSTimingOfCell  SEQUENCE {
                 ms-part           INTEGER (0..80),
                 ls-part           INTEGER (0..4294967295)} OPTIONAL,
             modeSpecificInfo      CHOICE {
                       fdd         SEQUENCE {
                         referenceIdentity      PrimaryCPICH-Info},
                       tdd         SEQUENCE {
                         referenceIdentity      CellParametersID}} OPTIONAL,
             sfn      INTEGER (0..4095),
             ganss-TODUncertainty INTEGER (0..127) OPTIONAL,
...}

GNSSPosTechnology ::= SEQUENCE {
  gps                BOOLEAN,
  galileo            BOOLEAN,
  sbas               BOOLEAN,
  modernized-gps     BOOLEAN,
  qzss               BOOLEAN,
  glonass            BOOLEAN,
...,
  bds                BOOLEAN      OPTIONAL}

GANSSSignals ::= BIT STRING {
  signal1 (0),
  signal2 (1),
  signal3 (2),
  signal4 (3),
  signal5 (4),
  signal6 (5),
  signal7 (6),
  signal8 (7)} (SIZE (1..8))

SPCSETKey ::= BIT STRING(SIZE (128))

SPCTID ::= SEQUENCE {
  rAND               BIT STRING(SIZE (128)),
  slpFQDN            FQDN,
        ...}

SPCSETKeylifetime ::= INTEGER (1..24) -- units in hours

CauseCode ::= ENUMERATED {
  servingNetWorkNotInAreaIdList(0), sETCapabilitiesChanged(1),
noSUPLCoverage(2), ...}
```

```
ThirdParty ::= SEQUENCE (SIZE (1..64)) OF ThirdPartyID

ThirdPartyID ::= CHOICE {
        logicalName  IA5String(SIZE (1..1000)),
        msisdn       OCTET STRING(SIZE (8)),
        emailaddr    IA5String(SIZE (1..1000)),
        sip-uri      VisibleString(FROM ("a".."z" | "A".."Z" | "0".."9" |
":./-_~%#@?")) (SIZE (1..255)),
        ims-public-identity       VisibleString(FROM ("a".."z" | "A".."Z" |
"0".."9" | ":./-_~%#@?")) (SIZE (1..255)),
        min          BIT STRING(SIZE (34)), -- coded according to [TIA-553]
        mdn          OCTET STRING(SIZE (8)),
        uri          VisibleString(FROM ("a".."z" | "A".."Z" | "0".."9" | "./-
_~%#")) (SIZE (1..255)),
...}

ApplicationID ::= SEQUENCE {
        appProvider IA5String(SIZE (1..24)), -- The application provider
        appName IA5String(SIZE (1..32)), -- The application name
        appVersion IA5String(SIZE (1..8)) OPTIONAL,  -- The application
version
...}

ReportingCap ::= SEQUENCE {
  minInt INTEGER (1..3600), -- units in seconds
  maxInt INTEGER (1..1440) OPTIONAL, -- units in minutes
  repMode            RepMode,
  batchRepCap        BatchRepCap OPTIONAL, -- only used for batch and quasi
real time reporting
  ...}

RepMode ::= SEQUENCE {
  realtime           BOOLEAN,
  quasirealtime      BOOLEAN,
  batch              BOOLEAN,
  ...}

BatchRepCap ::= SEQUENCE {
  report-position    BOOLEAN, -- set to "true" if reporting of position is
supported
  report-measurements BOOLEAN, -- set to "true" if reporting of measurements is
supported
  max-num-positions   INTEGER (1..1024) OPTIONAL,
  max-num-measurements INTEGER (1..1024) OPTIONAL,
  ...}

Coordinate::= SEQUENCE {
 latitudeSign        ENUMERATED {north(0), south(1)},
 latitude            INTEGER(0..8388607),
 longitude           INTEGER(-8388608..8388607)} -- Coding as in [3GPP GAD]

CircularArea ::= SEQUENCE {
 coordinate          Coordinate,
 radius              INTEGER(1..1000000), -- radius in meters
 radius-min          INTEGER(1..1000000) OPTIONAL, -- hysteresis minimum
radius
 radius-max          INTEGER(1..1500000) OPTIONAL} -- hysteresis maximum
radius
```

```
EllipticalArea ::= SEQUENCE {
 coordinate           Coordinate,
 semiMajor            INTEGER(1..1000000), -- units in meters
 semiMajor-min        INTEGER(1..1000000) OPTIONAL, -- hysteresis minimum
semiMajor
 semiMajor-max        INTEGER(1..1500000) OPTIONAL, -- hysteresis maximum
semiMajor
 semiMinor            INTEGER(1..1000000), -- units in meters
 semiMinor-min        INTEGER(1..1000000) OPTIONAL, -- hysteresis minimum
semiMinor
 semiMinor-max        INTEGER(1..1500000) OPTIONAL, -- hysteresis maximum
semiMinor
 angle                INTEGER(0.. 179)} -- units in degrees. The angle is
defined as the angle between the semi-major axis and North, increasing in a
clockwise direction. An angle of 0 represents an ellipse with the semi-major
axis pointing North/South while an angle of 90 represents an ellipse with the
semi-major axis pointing East/West.

PolygonArea ::= SEQUENCE {
 polygonDescription   PolygonDescription,
 polygonHysteresis    INTEGER(1..100000) OPTIONAL} -- units in meters

PolygonDescription ::= SEQUENCE (SIZE (3..15)) OF Coordinate

END
```

11.9 Common elements (SUPL Version 3)

```
Ver3-ULP-Components DEFINITIONS AUTOMATIC TAGS ::=
BEGIN

EXPORTS Ver3-CellInfo-extension, Ver3-PositionEstimate-extension, Ver3-
Velocity-extension;

IMPORTS
OMA-LPPe-HighAccuracy3Dposition, OMA-LPPe-HighAccuracy3Dvelocity
FROM OMA-LPPE;

Ver3-PositionEstimate-extension ::= SEQUENCE {
 highAccuracy3Dposition           OMA-LPPe-HighAccuracy3Dposition OPTIONAL,
...}

Ver3-Velocity-extension ::= SEQUENCE {
 highAccuracy3Dvelocity           OMA-LPPe-HighAccuracy3Dvelocity OPTIONAL,
...}

Ver3-CellInfo-extension ::= CHOICE {
  noCellInfo          NULL,
  ...}

END
```

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
OMA-TS-ULP-V1_0-20070615-A	15 Jun 2007	Status changed to Candidate by TP TP Ref # OMA-TP-2007-0219R01-INP_ERP_SUPL_1_0_for_Final_Approval

A.2 Draft/Candidate Version 3.0 History

Document Identifier	Date	Sections	Description
Draft Versions OMA-TS-UPL-V3_0	28 Jun 2010	n/a	Initial draft based on TS template.
	30 Jun 2010	5.1.1, 5.1.1.1, 5.1.1.2, 5.1.2, 5.1.2.1, 5.1.2.2, 5.3.1, 5.3.1.1, 5.3.1.2, 5.3.2, 5.3.2.1, 5.3.2.2, 5.3.3, 5.3.3.1, 5.3.3.2, 5.3.4, 5.3.4.1, 5.3.4.2, 5.3.5.1, 5.3.5.2	• OMA-LOC-2010-0141R01-CR_SUPL3.0_TS_ULP_legacy_services_I • OMA-LOC-2010-0142R01-CR_SUPL3.0_TS_ULP_legacy_services_II • OMA-LOC-2010-0143R01-CR_SUPL3.0_TS_ULP_legacy_services_III • OMA-LOC-2010-0144R02-CR_SUPL3.0_TS_ULP_legacy_services_IV • OMA-LOC-2010-0145R03-CR_SUPL3.0_TS_ULP_legacy_services_V • OMA-LOC-2010-0146R03-CR_SUPL3.0_TS_ULP_legacy_services_VI • OMA-LOC-2010-0022R03-CR_SUPL3_0_ULP_TS_Triggered_Session_Pause_Resume_NI • OMA-LOC-2010-0023R03-CR_SUPL3_0_ULP_TS_Triggered_Session_Pause_Resume_SI
	6 Sep 2010	2.1, 5.1.1, 5.1.2.3, 5.1.2.4, 5.1.3, 5.3.5, 5.3.6.2, 5.3.6.3, 9, 10, 11, Appendix D, D.1, D.2, D.3	• OMA-LOC-2010-0197-CR_SUPL3.0_TS_ULP_Message_Definitions • OMA-LOC-2010-0198-CR_SUPL3.0_TS_ULP_Parameter_Definitions • OMA-LOC-2010-0199-CR_SUPL3.0_TS_ULP_ASN1_Definitions • OMA-LOC-2010-0205R01-CR_SUPL3_0_ULP_TS_Flows_MLP_Alternatives • OMA-LOC-2010-0206-CR_SUPL3_0_ULP_TS_App_LOCSIP_Single_Fix • OMA-LOC-2010-0207-CR_SUPL3_0_ULP_TS_App_LOCSIP_Periodic • OMA-LOC-2010-0208-CR_SUPL3_0_ULP_TS_App_LOCSIP_Area_Event • OMA-LOC-2010-0224R01-CR_SUPL3_0_ULP_TS_Legacy_Session_Info_Query • OMA-LOC-2010-0225R01-CR_SUPL3_0_ULP_TS_Pauselist_in_SessionInfoQuery • OMA-LOC-2010-0227R01-CR_SUPL3_0_ULP_TS_Legacy_SET_Initiated_Location_Request_of_Another_SET • OMA-LOC-2010-0228R01-CR_SUPL3_0_ULP_TS_Immediate_Relative_Location_Service • OMA-LOC-2010-0210R01-CR_SUPL3.0_TS_ULP_Generic_SUPL_Service • OMA-LOC-2010-0024R04-CR_SUPL3_0_ULP_TS_Triggered_Session_Pause_Resume_Exceptional
	21 Oct 2010	5.1.3.1, 5.1.3.2, 5.3.6.2, 5.3.6.3, Appendix E, Appendix F	• OMA-LOC-2010-0241R03-CR_SUPL3_0_ULP_TS_Re_Notification_Termination_in_Session_Info_Query • OMA-LOC-2010-0252R02-CR_SUPL3_0_ULP_TS_Stop_Time_Triggered_Service • OMA-LOC-2010-0264-CR_SUPL3.0_TS_ULP_LPPe_Call_Flows_for_Legacy_Services • OMA-LOC-2010-0265-CR_SUPL3.0_TS_ULP_LPPe_Call_Flows_for_GSS

Document Identifier	Date	Sections	Description
	22 Nov 2010	5.3.1.1, 5.3.2.1, 5.1.2.3, 5.1.2.4, 5.3.4.1, 5.3.5.1, 5.3.5.2, 9.2.15, 11.2.14	OMA-LOC-2010-0287- CR_SUPL3_0_TS_relative_and_absolute_positioning_bugfix OMA-LOC-2010-0292R01-CR_SUPL3_0_ULP_TS_Editorial_Cleanup OMA-LOC-2010-0279R01- CR_SUPL3.0_TS_ULP_Legacy_Triggered_Services
	14 Feb 2011	9, 10	OMA-LOC-2011-0028R01- CR_SUPL3.0_TS_ULP_Message_Definitions OMA-LOC-2011-0029R01- CR_SUPL3.0_TS_ULP_Parameter_Definitions
	17 Mar 2011	2.1, 3.3, 5.1.2.6, 9.2.1, 9.2.4, 9.2.6, 9.2.8, 10.5, 10.31, 10.32, 10.33, 11.2.1, 11.2.2, 11.2.4, 11.2.6, 11.4, 11.6	OMA-LOC-2011-0030R01-CR_SUPL3.0_TS_ULP_Location_URI

Document Identifier	Date	Sections	Description
	18 Apr 2011	2.1, 3.2, 3.3, 4.2, 4.3, 5, 5.1.1.1, 5.1.2.1, 5.1.2.4, 5.1.3.1, 5.1.4, 5.2, 5.2.1, 5.2.2, 5.2.3, 5.2.4, 5.3.2.1, 5.3.3.1, 5.3.4.1, 5.3.5.1, 5.3.5.2, 5.3.6.1, 5.3.6.2, 5.3.6.3, 5.3.6.4, 5.3.6.5, 5.3.6.6, 5.3.8, 5.3.8.1, 5.3.8.2, 6, 7, 7.1, 8, 9, 9.2, 9.2.1, 9.2.3, 9.2.4, 9.2.5, 9.2.7, 9.2.10, 9.2.11, 9.2.12, 9.2.13, 9.2.14, 10.1, 10.8, 10.29, 11, 11.1, 11.2.2, 11.2.3, 11.2.5, 11.2.12, 11.2.13, 11.2.16, 11.3, 11.4, 11.5, 11.6, 11.6, Appendix D.1, Appendix E, E.1, E.2, E.3, Appendix F, F.1, F.2	OMA-LOC-2011-0042R01-CR_SUPL3.0_TS_ULP_Introduction OMA-LOC-2011-0043R01-CR_SUPL3.0_TS_ULP_Transport_Protocol OMA-LOC-2011-0044-CR_SUPL3.0_TS_ULP_Exception_Procedures OMA-LOC-2011-0045R01-CR_SUPL3.0_TS_ULP_Event_Trigger_Session_End OMA-LOC-2011-0046R01-CR_SUPL3.0_TS_ULP_Emergency_Services OMA-LOC-2011-0047R02-CR_SUPL3.0_TS_ULP_ASN1 OMA-LOC-2011-0048-CR_SUPL3.0_TS_ULP_Removal_of_V_SLP_to_V_SLP_Handover OMA-LOC-2011-0049-CR_SUPL3.0_TS_ULP_Retrieval_of_Historic_Reports OMA-LOC-2011-0051R01-CR_SUPL3.0_TS_ULP_Network_or_SET_Capabilities_Change OMA-LOC-2011-0052-CR_SUPL3.0_TS_ULP_Version_Negotiation OMA-LOC-2011-0054R01-CR_SUPL3.0_TS_ULP_Support_for_LPPe OMA-LOC-2011-0066-CR_SUPL3.0_TS_ULP_Positioning_Payload OMA-LOC-2011-0068R01-CR_SUPL3 0_TS_ULP_Security OMA-LOC-2011-0069R01-CR_SUPL3.0_TS_ULP_Triggered_Pause_Resume_Parameter OMA-LOC-2011-0070R01-CR_SUPL3.0_TS_ULP_3rd_Party_Relative_Location_Parameters OMA-LOC-2011-0071R02-CR_SUPL3.0_TS_ULP_Session_Info_Query_Parameters OMA-LOC-2011-0072R01-CR_SUPL3.0_TS_SUPL_START_parameter

Document Identifier	Date	Sections	Description
	23 May 2011	3.2, 3.3, 4.1, 5, 5.1, 5.1.2.1, 5.1.2.3, 5.1.2.4, 5.1.2.5, 5.1.2.6, 5.3, 5.3.3.1, 5.3.4.1, 5.3.5.1, 6.1, 9.2.2, 9.2.5, 9.2.9, 9.2.10, 9.2.12, 9.2.15, 10.3, 10.5, 10.6, 10.8, 10.17.3.7, 10.29, 10.34, 10.35, 10.36, 10.37, 10.38, 11.2.2, 11.2.3, 11.2.9, 11.2.10, 11.2.11, 11.2.14, 11.2.15, 11.2.16, 11.4, 11.6, 11.7, 11.9, Appendix C	OMA-LOC-2011-0096-CR_SUPL3.0_TS_ULP_GSS_correction OMA-LOC-2011-0094-CR_SUPL3.0_TS_ULP_Timers OMA-LOC-2011-0093-CR_SUPL3.0_TS_ULP_noCellInfo OMA-LOC-2011-0102R01-CR_SUPL3.0_TS_ULP_high_accuracy_position OMA-LOC-2011-0103-CR_SUPL3.0_TS_ULP_SUPL_Agent_correction OMA-LOC-2011-0108-CR_SUPL3_0_TS_Wording_Correction_Positioning_Payload_Section_9_2_9 OMA-LOC-2011-0115-CR_SUPL3.0_TS_ULP_Corrections OMA-LOC-2011-0083R01-CR_SUPL3.0_TS_ULP_Triggered_Pause_Resume_ASN1 OMA-LOC-2011-0084R01-CR_SUPL3.0_TS_ULP_3rd_Party_Relative_Location_ASN1 OMA-LOC-2011-0085R02-CR_SUPL3.0_TS_ULP_Session_Info_Query_ASN1 OMA-LOC-2011-0067R02-CR_SUPL3.0_TS_Addition_of_a_D_SLP OMA-LOC-2011-0116R01-CR_SUPL3.0_TS_ULP_Single_Fix_with_Transfer_to_3rd_Party
	30 Jun 2011	Throughout document	OMA-LOC-2011-0109R02-CR_SUPL3_0_TS_Velocity_Event_Triggered_Service OMA-LOC-2011-0127-CR_SUPL3.0_TS_ULP_SCR OMA-LOC-2011-0129R02-CR_SUPL3.0_TS_D_SLP_and_E_SLP_Revisions OMA-LOC-2011-0132-CR_SUPL3.0_TS_ULP_Notification_based_on_Current_Location OMA-LOC-2011-0135R01-CR_SUPL3.0_TS_ULP_security_update OMA-LOC-2011-0151R01-CR_SUPL3.0_TS_Missing_Emergency_Support OMA-LOC-2011-0155R02-CR_SUPL3.0_TS_Relative_Position OMA-LOC-2011-0159-CR_SUPL3.0_TS_High_Accuracy_QoP OMA-LOC-2011-0166R01-CR_SUPL3.0_TS_ULP_D_SLP_Supported_Service OMA-LOC-2011-0167-CR_SUPL3.0_TS_ULP_Message_Description OMA-LOC-2011-0169-CR_SUPL3.0_TS_ULP_Version_Correction OMA-LOC-2011-0176R03-CR_SUPL3.0_TS_ULP_Velocity_Trigger_Modification OMA-LOC-2011-0178-CR_SUPL3.0_TS_ULP_Absolute_Civic_Location
	9 Aug 2011	Throughout document	OMA-LOC-2011-0186-CR_SUPL3.0_CONRR_Corrections_C001_C002_C003_C004 All ‘assigned to editor’ items in OMA-CONRR-SUPL-V3_0-20110804-D

Document Identifier	Date	Sections	Description
	19 Aug 2011	Throughout document	OMA-LOC-2011-0204-CR_SUPL3.0_CONRR_C066_Connection_rules OMA-LOC-2011-0205-CR_SUPL3.0_CONRR_C079_SUPL_Agent OMA-LOC-2011-0207-CR_SUPL3.0_CONRR_C301_302_unsolicited OMA-LOC-2011-0210-CR_SUPL3.0_CONRR_C354_355_372_AreaId OMA-LOC-2011-0191R01-CR_SUPL3.0_CONRR_Corrections_C083 OMA-LOC-2011-0192R01-CR_SUPL3.0_CONRR_Corrections_C109 OMA-LOC-2011-0193R01-CR_SUPL3.0_CONRR_Corrections_C115 OMA-LOC-2011-0194-CR_SUPL3.0_CONRR_Corrections_C51_C62_C108_C118_C166_C200 OMA-LOC-2011-0195-CR_SUPL3.0_CONRR_Corrections_C068_C072 OMA-LOC-2011-0196-CR_SUPL3.0_CONRR_Corrections_C247_C249_C251 OMA-LOC-2011-0197-CR_SUPL3 0_CONRR_Corrections_C265 OMA-LOC-2011-0198R01-CR_SUPL3.0_CONRR_Corrections_C276 OMA-LOC-2011-0199-CR_SUPL3.0_CONRR_Corrections_C278 OMA-LOC-2011-0200-CR_SUPL3.0_CONRR_Corrections_C325_C330 OMA-LOC-2011-0202-CR_SUPL3.0_CONRR_Corrections_C385_C386_C387_C388 OMA-LOC-2011-0212R01-CR_SUPL3.0_CONRR_Corrections_C371 OMA-LOC-2011-0213-CR_SUPL3.0_CONRR_Corrections_C390 OMA-LOC-2011-0214-CR_SUPL3.0_CONRR_Corrections_C394 OMA-LOC-2011-0215R01-CR_SUPL3.0_CONRR_Corrections_C243 OMA-LOC-2011-0217R01-CR_SUPL3.0_CONRR_Corrections_C117

Document Identifier	Date	Sections	Description
	7 Sep 2011	Throughout document	OMA-LOC-2011-0228-CR_SUPL3.0_CONRR_Corrections_C360 OMA-LOC-2011-0242-CR_SUPL3.0_CONRR_Corrections_C244 OMA-LOC-2011-0227-CR_SUPL3.0_CONRR_Corrections_C267 OMA-LOC-2011-0260R01-CR_SUPL3.0_CONRR_Corrections_C040_C057 OMA-LOC-2011-0203R02-CR_SUPL3.0_CONRR_C048_TLS OMA-LOC-2011-0257-CR_SUPL3.0_CONRR_Corrections_C081_C082 OMA-LOC-2011-0258-CR_SUPL3.0_CONRR_Corrections_C086 OMA-LOC-2011-0259-CR_SUPL3.0_CONRR_Corrections_C087 OMA-LOC-2011-0233R01-CR_SUPL3.0_CONRR_C088_089_RFC2119 OMA-LOC-2011-0263-CR_SUPL3.0_CONRR_Corrections_C090 OMA-LOC-2011-0264-CR_SUPL3.0_CONRR_Corrections_C091 OMA-LOC-2011-0265-CR_SUPL3.0_CONRR_Corrections_C098_C101 OMA-LOC-2011-0241-CR_SUPL3.0_CONRR_Corrections_C228 OMA-LOC-2011-0208R02-CR_SUPL3.0_CONRR_C272_289_313_326_327_328_332_to_C335_337_PosMethods OMA-LOC-2011-0206R01-CR_SUPL3.0_CONRR_C280_ErrorHandling OMA-LOC-2011-0229-CR_SUPL3_0_CONRR_Correction_C362 OMA-LOC-2011-0270-CR_SUPL3.0_CONRR_Corrections_C401 OMA-LOC-2011-0271-CR_SUPL3.0_CONRR_Corrections_C367 OMA-LOC-2011-0216R01-CR_SUPL3.0_CONRR_Corrections_C297 OMA-LOC-2011-0223-CR_SUPL3.0_TS_CONRR_C058 OMA-LOC-2011-0224-CR_SUPL3.0_TS_CONRR_C080 OMA-LOC-2011-0254-CR_SUPL3.0_CONRR_C403 OMA-LOC-2011-0252R04-CR_SUPL3.0_TS_CONRR_C400 OMA-LOC-2011-0222R02-CR_SUPL3.0_CONRR_Corrections_C013_C373_C374_C375_C376 OMA-LOC-2011-0209R03-CR_SUPL3.0_CONRR_C338_Sensor
Candidate Version OMA-TS-UPL-V3_0	20 Sep 2011	All	TP approved via R&A: OMA-TP-2011-0332-INP_SUPL_3.0_ERP_for_Candidate_approval
Draft Versions OMA-TS-UPL-V3_0	26 Apr 2012	10.40, 11.4	OMA-LOC-2012-0116R01-CR__SUPL_3_0_TS_D_SLP_Service_Area
	18 Jul 2012	Appendix I	OMA-LOC-2012-0179-CR_SUPL_3.0_ULP_TS_Area_Event_with_D_SLP_Procedure
	26 Sep 2012	11.2.12, 11.4	Incorporated CR; OMA-LOC-2012-0209-CR_SUPL3_TS_ULP_serviceArea Editorial changes
	20 Nov 2012	10.5, 8.6.2, 10.33, 11.7	OMA-LOC-2012-0247-CR_SUPL_3.0_ULP_TS_App_Id_Status_Code OMA-LOC-2012-0261-CR_SUPL_3.0_ULP_TS_Cell_Id_Positioning_Correction OMA-LOC-2012-0286-CR_SUPL_3.0_ULP_TS_Application_ID_Correction
	16 Jan 2013	10.40, 11.2.12, 11.4	OMA-LOC-2012-0178R05-CR_SUPL_3.0_ULP_TS_Area_ids_for_D_SLP_Service_Area
	05 Feb 2013	B 1.1, B 2.1	OMA-LOC-2012-0189R01-CR_SUPL_3_0_SCR_item_for_Unsolicited_Authorization_of_D_SLPs_and_E_SLPs
	28 Feb 2013	4.4	OMA-LOC-2013-0028-CR_SUPL_3_0_Correction_for_section_reference
	07 Jun 2013	10.25.2.2	Incorporated CR: OMA-LOC-2013-0085-CR_ULP_3_0_ClarificationAbsentGeoTargetArea Editorial changes
	26 Sep 2013	2.1	OMA-LOC-2013-0127R02-CR_SUPL3.0_TS_ULP_WLAN_AP_Info_Corrections

Document Identifier	Date	Sections	Description
	27 Feb 2014	3.3, 9.2.14, 11.5, 11.8,	OMA-LOC-2014-0036-CR_SUPL3.0_TS_ULP_Beidou_Support
	25 Mar 2014	11.5, 11.8	OMA-LOC-2014-0057-CR_SUPL3.0_TS_ULP_ASN.1_correction
	23 Apr 2014	11	OMA-LOC-2014-0076-CR_SUPL_3.0_ULP_ASN.1_Corrections
	03 Sep 2014	11	OMA-LOC-2014-0135-CR_SUPL_3.0_TS_ULP_ASN.1_Corrections
Candidate Version OMA-TS-UPL-V3_0	16 Sep 2014	n/a	Status changed to Candidate by TP TP Ref # OMA-TP-2014-0213-INP_SUPL_V3_0_ERP_for_Candidate_re_approval

Appendix B. Static Conformance Requirements

The notation used in this appendix is specified in [SCRRULES].

B.1 SCR for SUPL Client

B.1.1 SET Procedures

Item	Function	Reference	Requirement
ULP-PRO-C-001-O	SET supporting 3GPP defined system mode		(ULP-PRO-C-009-O OR ULP-PRO-C-010-O) AND (ULP-PRO-C-011-O OR ULP-PRO-C-012-O)
ULP-PRO-C-002-O	SET supporting 3GPP2 defined system mode		(ULP-PRO-C-009-O OR ULP-PRO-C-010-O) AND ULP-PRO-C-013-O
ULP-PRO-C-003-O	SET supporting WiMAX mode		(ULP-PRO-C-009-O OR ULP-PRO-C-010-O) AND (ULP-PRO-C-011-O OR ULP-PRO-C-013-O)
Security modes			
ULP-PRO-C-004-O	Security function, GBA authentication model	ULP 6	ULP-PRO-C-046-O
ULP-PRO-C-005-O	Security function, DCert authentication model	ULP 6	ULP-PRO-C-046-O
ULP-PRO-C-006-M	Security function, ACA authentication model	ULP 6	ULP-PRO-C-045-O
ULP-PRO-C-007-M	Security function, SLP-only authentication model	ULP 6	ULP-PRO-C-045-O
ULP-PRO-C-008-O	Security function, SEK authentication model	ULP 6	ULP-PRO-C-046-O
High-level procedures			
ULP-PRO-C-009-O	Support of network initiated services	ULP 5.1	
ULP-PRO-C-010-O	Support of SET initiated services	ULP 5.1	
Positioning Protocols			
ULP-PRO-C-011-O	Support of LPP positioning protocol		ULP-MES-C-005-O
ULP-PRO-C-012-O	Support of LPPe positioning protocol		ULP-MES-C-005-O AND ULP-PRO-C-011-O
ULP-PRO-C-013-O	Support of TIA-801 positioning protocol		ULP-MES-C-005-O
ULP Version Negotiation			
ULP-PRO-C-014-M	Support of ULP version negotiation	ULP 7	
Detailed procedures			
ULP-PRO-C-015-O	Support of network initiated single fix		ULP-MES-C-001-O AND ULP-MES-C-004-O AND ULP-MES-C-005-O AND ULP-MES-C-006-M
ULP-PRO-C-016-O	Support of SET initiated single fix		ULP-MES-C-002-O AND ULP-MES-C-003-O AND ULP-MES-C-004-O AND ULP-MES-C-005-O AND ULP-MES-C-006-M

Item	Function	Reference	Requirement
ULP-PRO-C-017-O	Support for SET initiated single fix – 3rd party location request		ULP-MES-C-012-O AND ULP-MES-C-006-M
ULP-PRO-C-018-O	Support for SET initiated single fix – 3rd party relative location request		ULP-MES-C-012-O AND ULP-MES-C-006-M
ULP-PRO-C-019-O	Support for SET initiated single fix – transfer to 3rd party		ULP-MES-C-002-O AND ULP-MES-C-003-O AND ULP-MES-C-004-O AND ULP-MES-C-005-O AND ULP-MES-C-006-M
ULP-PRO-C-020-O	Support for Location URI request		ULP-MES-C-002-O AND ULP-MES-C-006-M
ULP-PRO-C-021-O	Support for D-SLP and E-SLP authorization by the H-SLP		ULP-MES-C-002-O AND ULP-MES-C-003-O AND ULP-MES-C-004-O AND ULP-MES-C-005-O AND ULP-MES-C-006-M
ULP-PRO-C-022-O	Support for D-SLP or E-SLP authorization by a proxy D-SLP or proxy E-SLP		ULP-MES-C-002-O AND ULP-MES-C-003-O AND ULP-MES-C-004-O AND ULP-MES-C-005-O AND ULP-MES-C-006-M
ULP-PRO-C-023-O	Support of D-SLP access notification to the H-SLP		ULP-MES-C-013-O AND ULP-MES-C-006-M
ULP-PRO-C-024-O	Support of Session Info Query with re-notification		ULP-MES-C-001-O AND ULP-MES-C-013-O AND ULP-MES-C-010-O AND ULP-MES-C-011-O AND ULP-MES-C-009-O AND ULP-MES-C-006-M
ULP-PRO-C-025-O	Support of Session Info Query with session termination		ULP-MES-C-001-O AND ULP-MES-C-013-O AND ULP-MES-C-009-O AND ULP-MES-C-006-M
ULP-PRO-C-026-O	Support of network initiated triggered periodic		ULP-MES-C-001-O AND ULP-MES-C-007-O AND ULP-MES-C-008-O AND ULP-MES-C-004-O AND ULP-MES-C-005-O AND ULP-MES-C-013-O AND ULP-MES-C-006-M
ULP-PRO-C-027-O	Support of network initiated area event		ULP-MES-C-001-O AND ULP-MES-C-007-O AND ULP-MES-C-008-O AND ULP-MES-C-004-O AND ULP-MES-C-005-O AND ULP-MES-C-013-O AND ULP-MES-C-006-M
ULP-PRO-C-028-O	Support of SET initiated triggered periodic		ULP-MES-C-007-O AND ULP-MES-C-008-O AND ULP-MES-C-004-O AND ULP-MES-C-005-O AND ULP-MES-C-013-O AND ULP-MES-C-006-M
ULP-PRO-C-029-O	Support of SET initiated triggered area event		ULP-MES-C-007-O AND ULP-MES-C-008-O AND ULP-MES-C-004-O AND ULP-MES-C-005-O AND ULP-MES-C-013-O AND ULP-MES-C-006-M
ULP-PRO-C-030-O	Support of network initiated GSS		ULP-MES-C-001-O AND ULP-MES-C-002-O AND ULP-MES-C-003-O AND ULP-MES-C-005-O AND ULP-MES-C-014-O AND ULP-MES-C-004-O AND ULP-MES-C-006-M

Item	Function	Reference	Requirement
ULP-PRO-C-031-O	Support of SET initiated GSS		ULP-MES-C-002-O AND ULP-MES-C-003-O AND ULP-MES-C-005-O AND ULP-MES-C-014-O AND ULP-MES-C-004-O AND ULP-MES-C-006-M
ULP-PRO-C-032-O	Support of Single Fix with Notification based on Location		ULP-MES-C-001-O AND ULP-MES-C-004-O AND ULP-MES-C-005-O AND ULP-MES-C-006-M AND ULP-MES-C-010-M AND ULP-MES-C-011-M
ULP-PRO-C-033-O	Support of network initiated velocity event Triggered Services		ULP-MES-C-001-O AND ULP-MES-C-007-O AND ULP-MES-C-008-O AND ULP-MES-C-004-O AND ULP-MES-C-005-O AND ULP-MES-C-013-O AND ULP-MES-C-006-M
ULP-PRO-C-034-O	Support of SET initiated velocity event Triggered Services		ULP-MES-C-007-O AND ULP-MES-C-008-O AND ULP-MES-C-004-O AND ULP-MES-C-005-O AND ULP-MES-C-013-O AND ULP-MES-C-006-M
ULP-PRO-C-035-O	Support of notification		
ULP-PRO-C-036-O	Support of receiving QoP		
ULP-PRO-C-037-O	Support of sending QoP		
ULP-PRO-C-038-O	Support of initial position		
ULP-PRO-C-039-O	Support of real time reporting		
ULP-PRO-C-040-O	Support of quasi real time reporting		
ULP-PRO-C-041-O	Support of batch reporting		
ULP-PRO-C-042-O	Support of retrieval of historic position results		
ULP-PRO-C-043-O	Support of retrieval of historic enhanced cell/sector measurements		
ULP-PRO-C-044-O	Support of Network/SET capabilities change for area event triggered		
ULP-PRO-C-045-O	Support of Null Level		
ULP-PRO-C-046-O	Support of Mode A Protection		
ULP-PRO-C-047-O	Support of Mode B Protection		
ULP-PRO-C-048-O	Support of Multiple Location IDs		
ULP-PRO-C-049-O	Support of Unsolicited Authorization of D-SLPs and E-SLPs		

B.1.2 ULP Protocol Interface

Item	Function	Reference	Requirement
ULP-PIN-C-001-M	ULP encoding	ULP 8	
ULP-PIN-C-002-M	ULP transport	ULP 8	
ULP-PIN-C-003-M	Support of TCP/IP port number	ULP 8	
ULP-PIN-C-004-M	Support of OMA Push	ULP 8	
ULP-PIN-C-005-M	Support of MT SMS	ULP 8	
ULP-PIN-C-006-O	Support of SIP Push	ULP 8	
ULP-PIN-C-007-O	Support of UDP	ULP 8	

B.1.3 ULP Messages

Item	Function	Reference	Requirement
ULP-MES-C-001-O	Support of SUPL INIT	ULP 9,10,11	
ULP-MES-C-002-O	Support of SUPL START	ULP 9,10,11	
ULP-MES-C-003-O	Support of SUPL RESPONSE	ULP 9,10,11	
ULP-MES-C-004-O	Support of SUPL POS INIT	ULP 9,10,11	
ULP-MES-C-005-O	Support of SUPL POS	ULP 9,10,11	
ULP-MES-C-006-M	Support of SUPL END	ULP 9,10,11	
ULP-MES-C-007-O	Support of SUPL TRIGGERED START	ULP 9,10,11	
ULP-MES-C-008-O	Support of SUPL TRIGGERED RESPONSE	ULP 9,10,11	
ULP-MES-C-009-O	Support of SUPL TRIGGERED STOP	ULP 9,10,11	
ULP-MES-C-010-O	Support of SUPL NOTIFY	ULP 9,10,11	
ULP-MES-C-011-O	Support of SUPL NOTIFY RESPONSE	ULP 9,10,11	
ULP-MES-C-012-O	Support of SUPL SET INIT	ULP 9,10,11	
ULP-MES-C-013-O	Support of SUPL REPORT	ULP 9,10,11	
ULP-MES-C-014-O	Support of SUPL REINIT	ULP 9,10,11	

B.2 SCR for SUPL Server

B.2.1 SLP Procedures

Item	Function	Reference	Requirement
ULP-PRO-S-001-O	SET supporting 3GPP defined system mode		(ULP-PRO-S-009-O OR ULP-PRO-S-010-O) AND ULP-PRO-S-011-O
ULP-PRO-S-002-O	SET supporting 3GPP2 defined system mode		(ULP-PRO-S-009-O OR ULP-PRO-S-010-O) AND ULP-PRO-S-013-O

Item	Function	Reference	Requirement
ULP-PRO-S-003-O	SET supporting WiMAX mode		(ULP-PRO-S-009-O OR ULP-PRO-S-010-O) AND ULP-PRO-S-008-O
Security modes			
ULP-PRO-S-004-O	Security function, GBA authentication model	ULP 6	ULP-PRO-S-046-O
ULP-PRO-S-005-O	Security function, DCert authentication model	ULP 6	ULP-PRO-S-046-O
ULP-PRO-S-006-M	Security function, ACA authentication model	ULP 6	ULP-PRO-S-045-O
ULP-PRO-S-007-M	Security function, SLP-only authentication model	ULP 6	ULP-PRO-S-045-O
ULP-PRO-S-008-O	Security function, SEK authentication model	ULP 6	ULP-PRO-S-046-O
High-level procedures			
ULP-PRO-S-009-O	Support of network initiated services	ULP 5.1	
ULP-PRO-S-010-O	Support of SET initiated services	ULP 5.1	
Positioning Protocols			
ULP-PRO-S-011-O	Support of LPP positioning protocol		ULP-MES-S-005-O
ULP-PRO-S-012-O	Support of LPPe positioning protocol		ULP-MES-S-005-O AND ULP-PRO-S-011-O
ULP-PRO-S-013-O	Support of TIA-801 positioning protocol		ULP-MES-S-005-O
ULP Version Negotiation			
ULP-PRO-S-014-M	Support of ULP version negotiation	ULP 7	
Detailed procedures			
ULP-PRO-S-015-O	Support of network initiated single fix		ULP-MES-S-001-O AND ULP-MES-S-004-O AND ULP-MES-S-005-O AND ULP-MES-S-006-M
ULP-PRO-S-016-O	Support of SET initiated single fix		ULP-MES-S-002-O AND ULP-MES-S-003-O AND ULP-MES-S-004-O AND ULP-MES-S-005-O AND ULP-MES-S-006-M
ULP-PRO-S-017-O	Support for SET initiated single fix – 3rd party location request		ULP-MES-S-012-O AND ULP-MES-S-006-M
ULP-PRO-S-018-O	Support for SET initiated single fix – 3rd party relative location request		ULP-MES-S-012-O AND ULP-MES-S-006-M
ULP-PRO-S-019-O	Support for SET initiated single fix – transfer to 3rd party		ULP-MES-S-002-O AND ULP-MES-S-003-O AND ULP-MES-S-004-O AND ULP-MES-S-005-O AND ULP-MES-S-006-M
ULP-PRO-S-020-O	Support for Location URI request		ULP-MES-S-002-O AND ULP-MES-S-006-M

Item	Function	Reference	Requirement
ULP-PRO-S-021-O	Support for D-SLP and E-SLP authorization by the H-SLP		ULP-MES-S-002-O AND ULP-MES-S-003-O AND ULP-MES-S-004-O AND ULP-MES-S-005-O AND ULP-MES-S-006-M
ULP-PRO-S-022-O	Support for D-SLP or E-SLP authorization by a proxy D-SLP or proxy E-SLP		ULP-MES-S-002-O AND ULP-MES-S-003-O AND ULP-MES-S-004-O AND ULP-MES-S-005-O AND ULP-MES-S-006-M
ULP-PRO-S-023-O	Support of D-SLP access notification to the H-SLP		ULP-MES-S-013-O AND ULP-MES-S-006-M
ULP-PRO-S-024-O	Support of Session Info Query with re-notification		ULP-MES-S-001-O AND ULP-MES-S-013-O AND ULP-MES-S-010-O AND ULP-MES-S-011-O AND ULP-MES-S-009-O AND ULP-MES-S-006-M
ULP-PRO-S-025-O	Support of Session Info Query with session termination		ULP-MES-S-001-O AND ULP-MES-S-013-O AND ULP-MES-S-009-O AND ULP-MES-S-006-M
ULP-PRO-S-026-O	Support of network initiated triggered periodic		ULP-MES-S-001-O AND ULP-MES-S-007-O AND ULP-MES-S-008-O AND ULP-MES-S-004-O AND ULP-MES-S-005-O AND ULP-MES-S-013-O AND ULP-MES-S-006-M
ULP-PRO-S-027-O	Support of network initiated area event		ULP-MES-S-001-O AND ULP-MES-S-007-O AND ULP-MES-S-008-O AND ULP-MES-S-004-O AND ULP-MES-S-005-O AND ULP-MES-S-013-O AND ULP-MES-S-006-M
ULP-PRO-S-028-O	Support of SET initiated triggered periodic		ULP-MES-S-007-O AND ULP-MES-S-008-O AND ULP-MES-S-004-O AND ULP-MES-S-005-O AND ULP-MES-S-013-O AND ULP-MES-S-006-M
ULP-PRO-S-029-O	Support of SET initiated triggered area event		ULP-MES-S-007-O AND ULP-MES-S-008-O AND ULP-MES-S-004-O AND ULP-MES-S-005-O AND ULP-MES-S-013-O AND ULP-MES-S-006-M
ULP-PRO-S-030-O	Support of network initiated GSS		ULP-MES-S-001-O AND ULP-MES-S-002-O AND ULP-MES-S-003-O AND ULP-MES-S-005-O AND ULP-MES-S-014-O AND ULP-MES-S-004-O AND ULP-MES-S-006-M
ULP-PRO-S-031-O	Support of SET initiated GSS		ULP-MES-S-002-O AND ULP-MES-S-003-O AND ULP-MES-S-005-O AND ULP-MES-S-014-O AND ULP-MES-S-004-O AND ULP-MES-S-006-M
ULP-PRO-S-032-O	Support of Single Fix with Notification based on Location		ULP-MES-S-001-O AND ULP-MES-S-004-O AND ULP-MES-S-005-O AND ULP-MES-S-006-M AND ULP-MES-S-010-M AND ULP-MES-S-011-M
ULP-PRO-S-033-O	Support of network initiated velocity event Triggered Services		ULP-MES-S-001-O AND ULP-MES-S-007-O AND ULP-MES-S-008-O AND ULP-MES-S-004-O AND ULP-MES-S-005-O AND ULP-MES-S-013-O AND ULP-MES-S-006-M

Item	Function	Reference	Requirement
ULP-PRO-S-034-O	Support of SET initiated velocity event Triggered Services		ULP-MES-S-007-O AND ULP-MES-S-008-O AND ULP-MES-S-004-O AND ULP-MES-S-005-O AND ULP-MES-S-013-O AND ULP-MES-S-006-M
ULP-PRO-S-035-O	Support of notification		
ULP-PRO-S-036-O	Support of receiving QoP		
ULP-PRO-S-037-O	Support of sending QoP		
ULP-PRO-S-038-O	Support of initial position		
ULP-PRO-S-039-O	Support of real time reporting		
ULP-PRO-S-040-O	Support of quasi real time reporting		
ULP-PRO-S-041-O	Support of batch reporting		
ULP-PRO-S-042-O	Support of retrieval of historic position results		
ULP-PRO-S-043-O	Support of retrieval of historic enhanced cell/sector measurements		
ULP-PRO-S-044-O	Support of Network/SET capabilities change for area event triggered		
ULP-PRO-S-045-O	Support of Null Protection Level		
ULP-PRO-S-046-O	Support of Basic Protection Level		
ULP-PRO-S-047-O	Support of Multiple Location IDs		
ULP-PRO-S-048-O	Support of Unsolicited Authorization of D-SLPs and E-SLPs		

B.2.2 ULP Protocol Interface

Item	Function	Reference	Requirement
ULP-PIN-S-001-M	ULP encoding	ULP 8	
ULP-PIN-S-002-M	ULP transport	ULP 8	
ULP-PIN-S-003-M	Support of TCP/IP port number	ULP 8	
ULP-PIN-S-004-M	Support of OMA Push	ULP 8	
ULP-PIN-S-005-M	Support of MT SMS	ULP 8	
ULP-PIN-S-006-O	Support of SIP Push	ULP 8	
ULP-PIN-S-007-O	Support of UDP	ULP 8	

B.2.3 ULP Messages

Item	Function	Reference	Requirement
ULP-MES-S-001-O	Support of SUPL INIT	ULP 9,10,11	
ULP-MES-S-002-O	Support of SUPL START	ULP 9,10,11	

Item	Function	Reference	Requirement
ULP-MES-S-003-O	Support of SUPL RESPONSE	ULP 9,10,11	
ULP-MES-S-004-O	Support of SUPL POS INIT	ULP 9,10,11	
ULP-MES-S-005-O	Support of SUPL POS	ULP 9,10,11	
ULP-MES-S-006-M	Support of SUPL END	ULP 9,10,11	
ULP-MES-S-007-O	Support of SUPL TRIGGERED START	ULP 9,10,11	
ULP-MES-S-008-O	Support of SUPL TRIGGERED RESPONSE	ULP 9,10,11	
ULP-MES-S-009-O	Support of SUPL TRIGGERED STOP	ULP 9,10,11	
ULP-MES-S-010-O	Support of SUPL NOTIFY	ULP 9,10,11	
ULP-MES-S-011-O	Support of SUPL NOTIFY RESPONSE	ULP 9,10,11	
ULP-MES-S-012-O	Support of SUPL SET INIT	ULP 9,10,11	
ULP-MES-S-013-O	Support of SUPL REPORT	ULP 9,10,11	
ULP-MES-S-014-O	Support of SUPL REINIT	ULP 9,10,11	

Appendix C. Timers

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

Timer	Default value (sec.)	Description	Actions on expiration
UT1	11	For immediate applications, from sending of SUPL START to receipt of SUPL RESPONSE or SUPL END. For trigger applications, from sending of SUPL TRIGGERED START to receipt of SUPL TRIGGERED RESPONSE or SUPL END. For GSS, from sending of SUPL START to receipt of SUPL RESPONSE or SUPL END. For D-SLP Access Notification to the H-SLP (in SUPL REPORT) to receipt of SUPL END.	The SET sends SUPL END to the SLP. The SET clears all session resources at the SET.
UT2	11	From sending of SUPL POS INIT to receipt of first SUPL POS, SUPL REPORT or SUPL END message.	For immediate applications the SET sends SUPL END to the SLP and clears all session resources. For triggered applications, the SET skips the SUPL POS session and continues the triggered session.
UT3	10	From sending of the last SUPL POS message to receipt of SUPL END, SUPL REPORT or SUPL NOTIFY.	For immediate applications, the SET sends SUPL END to the SLP and clears all session resources. For triggered applications, the SET continues the triggered session.
UT5	10	Only applicable to “notification based on location” scenarios. From sending of SUPL NOTIFY RESPONSE to receipt of SUPL END.	The SET sends SUPL END to the SLP. The SET clears all session resources.
UT7	10	Only applicable to triggered scenarios. From sending of SUPL TRIGGERED STOP to receipt of SUPL END.	The SET sends SUPL END to the SLP. The SET clears all session resources.
UT8	10	Only applicable to triggered periodic scenarios. From sending the last SUPL REPORT message to receipt of SUPL END.	The SET sends SUPL END to the SLP. The SET clears all session resources.
UT9	60	Only applicable to SET Initiated 3rd Party Location Request. From sending of SUPL SET INIT to receipt of SUPL END.	The SET sends SUPL END to the SLP. The SET clears all session resources.

Table 83: SET Timer values

Timer	Default value (sec.)	Description	Actions on expiration
ST1	10	From sending of SUPL RESPONSE to receipt of SUPL POS INIT.	Send SUPL END to SET Clear session resources at SLP

Timer	Default value (sec.)	Description	Actions on expiration
ST2	10 NOTE: When user verification is required using "allow on no answer" or "deny on no answer", the H/D-SLP should allow at least 40 seconds for the SET to prompt the user and determine that no answer has been made.	From sending of SUPL INIT to receipt of SUPL POS INIT, SUPL TRIGGERED START, SUPL START or SUPL END. From sending of SUPL REINIT to receipt of SUPL POS or SUPL END.	For non-roaming scenario: For non GSS: inform SUPL agent that the session has ended. For GSS: optionally inform SUPL agent that the session has ended. For roaming scenario: For non GSS: inform SUPL agent or, where applicable, R-SLP that the session has ended. For GSS: Optionally inform SUPL agent or, where applicable, R-SLP that the session has ended. Clear session resources at SLP
ST3	10	From sending of RLP-SRLIR(SUPL START) to receipt of RLP-SRLIA(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) From sending SUPL INIT to receipt of SUPL REPORT.	For network initiated scenario: Send SUPL END to SET Send RLP-SRLIA to R-SLP Clear session resources at SLP For SET initiated scenario: Send SUPL END to SET Clear session resources at SLP
ST5	10 NOTE: When user verification is required using "allow on no answer" or "deny on no answer", the H-SLP should allow at least 40 seconds for the SET to prompt the user and determine that no answer has been made.	From sending SUPL NOTIFY to receipt of SUPL NOTIFY RESPONSE.	Send SUPL END to SET. Clear session resources at SLP.
ST6	10	Only applicable to "session-info query" sessions. From sending SUPL INIT to receipt of SUPL REPORT for Session Info Query session OR from sending SUPL TRIGGERED STOP to receipt of SUPL END for stopped triggered session.	Clear session resources at SLP.

Timer	Default value (sec.)	Description	Actions on expiration
ST7	10	From sending of SUPL REINIT to receipt of SUPL POS INIT or SUPL END. This timer is only applicable to GSS.	Clear session resources at SLP.

Table 84: SLP Timer values

Appendix D. Message Flows – Use of LOCSIP 1.0 for the Le/L1 Reference Point (Informative)

This Appendix describes the use of OMA LOCSIP 1.0 [OMA-LOCSIP] in place of MLP for the Le/L1 Reference Point, for a subset of the network-initiated SUPL 3.0 flows described in Section 5.

For these flows, the SUPL Agent behaves as a LOCSIP Location Client, a Home Subscription Agent (HSA), or a Resource List Server (RLS). The D/H-SLP performs the functionality of the LOCSIP Location Server.

D.1 Network-Initiated Single Fix

This section illustrates the message flow for a network-initiated single fix. It corresponds to the flow as specified in Section 5.1.1.1, but uses LOCSIP messages instead of MLP messages between the SUPL Agent and the D/H-SLP.

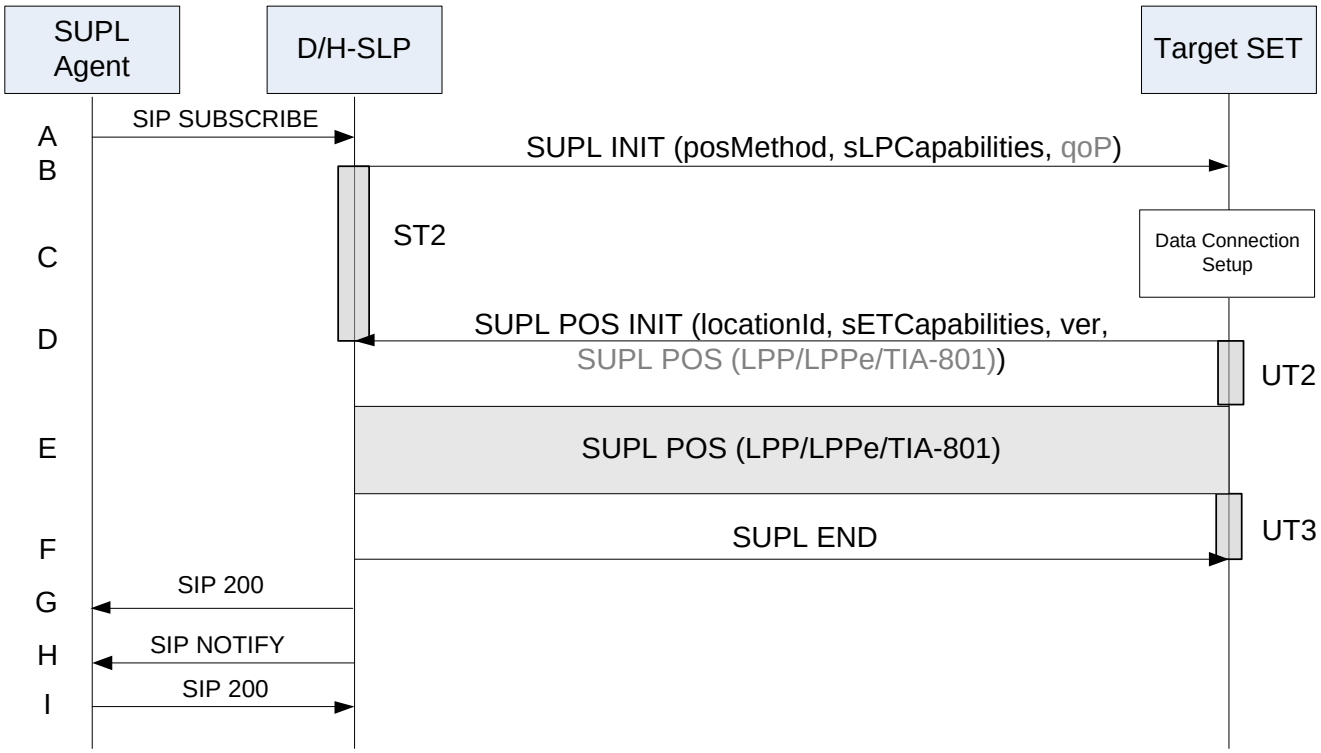

Figure 52: Network-Initiated Single Fix

A. The SUPL Agent sends a SIP SUBSCRIBE message that is directed to the D/H-SLP with which the Target SET is associated. The D/H-SLP performs the necessary authorisation checks to ensure the originator is allowed to request the location information of the Target SET. The D/H-SLP may also verify that the Target SET supports SUPL.
If a previously computed position which meets the requested QoP is available at the D/H-SLP and no notification and verification is required, the D/H-SLP proceeds directly to step G. If notification and verification or notification only is required, the D/H-SLP proceeds to step B.

NOTE: The specifics for determining if the SET supports SUPL are beyond the scope of SUPL 3.0.

B. The D/H-SLP initiates the location session with the SET using the SUPL INIT message. The SUPL INIT message contains the intended positioning method (*posMethod*), the SLP Capabilities (*sLPCapabilities*), and optionally the *QoP*. If the result of the authorization in step A indicates that notification and/or verification of the target subscriber is needed, the D/H-SLP includes the Notification parameter in the SUPL INIT message. Before the SUPL INIT message is sent, the D/H-SLP also computes and stores the hash of the SUPL INIT message.
If in step A the D/H-SLP decided to use a previously computed position, the SUPL INIT message indicates this in a

'no position' *posMethod* parameter value and the SET responds 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 responds with a SUPL END message. The D/H-SLP then proceeds directly to step G.

NOTE: Before sending the SUPL END message, the SET performs the data connection setup procedure of step C and uses the procedures described in step D to establish a TLS connection to the D/H-SLP.

C. The SET analyses the received SUPL INIT message. If found not to be authentic, the SET takes no further action. Otherwise, the SET takes the action required to prepare for the establishment of a TLS connection with the D/H-SLP. The SET also calculates the hash of the received SUPL INIT message.

D. The SET evaluates the Notification rules and takes the appropriate action. The SET establishes a TLS connection to the D/H-SLP using the D/H-SLP address which is either the H-SLP address provisioned by the Home Network or the D-SLP address provided or verified by the H-SLP or by a Proxy D-SLP authorized by the H-SLP. The SET then sends a SUPL POS INIT message to start a positioning session with the D/H-SLP. The SET sends the SUPL POS INIT message even if the SET does not support the intended positioning method indicated in SUPL INIT. The SUPL POS INIT message contains the Location ID (*locationId*), SET capabilities (*sETCapabilities*) and the hash (*ver*) of the received SUPL INIT message calculated in step C. The SUPL POS INIT message may also include a SUPL POS message carrying LPP/LPPe and/or TIA-801 positioning protocol messages in line with the D/H-SLP's positioning protocol capabilities (indicated in step B in *sLPCapabilities*). The SET may also provide its position, if this is supported (as part of LPP/LPPe/TIA-801 or explicitly through the optional position parameter). If a position retrieved in - or calculated based on information received in - the SUPL POS INIT message is available that meets the required QoP, the D/H-SLP MAY directly proceed to step F and not engage in a SUPL POS session.

E. The SET and D/H-SLP engage in a SUPL POS message exchange to calculate a position. The positioning methods used for this session are determined based on the capabilities exchanged by the SET and the D/H-SLP during the SUPL POS message exchange or optionally in step D. The D/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 D/H-SLP (SET-Based).

F. Once the position calculation is complete, the D/H-SLP sends a SUPL END message to the SET indicating that the location session has ended. The SET releases the TLS connection to the D/H-SLP and releases all resources related to this session.

G. The D/H-SLP responds to the SUPL Agent with an appropriate SIP 200 or 202 response.

NOTE: The SIP response may be sent earlier at any time after the D/H-SLP receives the SIP SUBSCRIBE message. A SIP 200 response indicates that the subscription has been accepted and that the SUPL Agent is authorized to subscribe to the requested resource. A SIP 202 response merely indicates that the subscription has been understood, and that authorization may or may not have been granted.

H. The D/H-SLP sends the position estimate back to the SUPL Agent in the body of a SIP NOTIFY message.

I. The SUPL Agent returns a SIP 200 OK response to the D/H-SLP and the D/H-SLP releases all resources related to this session.

D.2 Network-Initiated Triggered Periodic

This section illustrates the message flow for a network-initiated triggered periodic session. It corresponds to the flow as specified in Section 5.3.1.1, but uses LOCSIP messages instead of MLP messages between the SUPL Agent and the D/H-SLP.

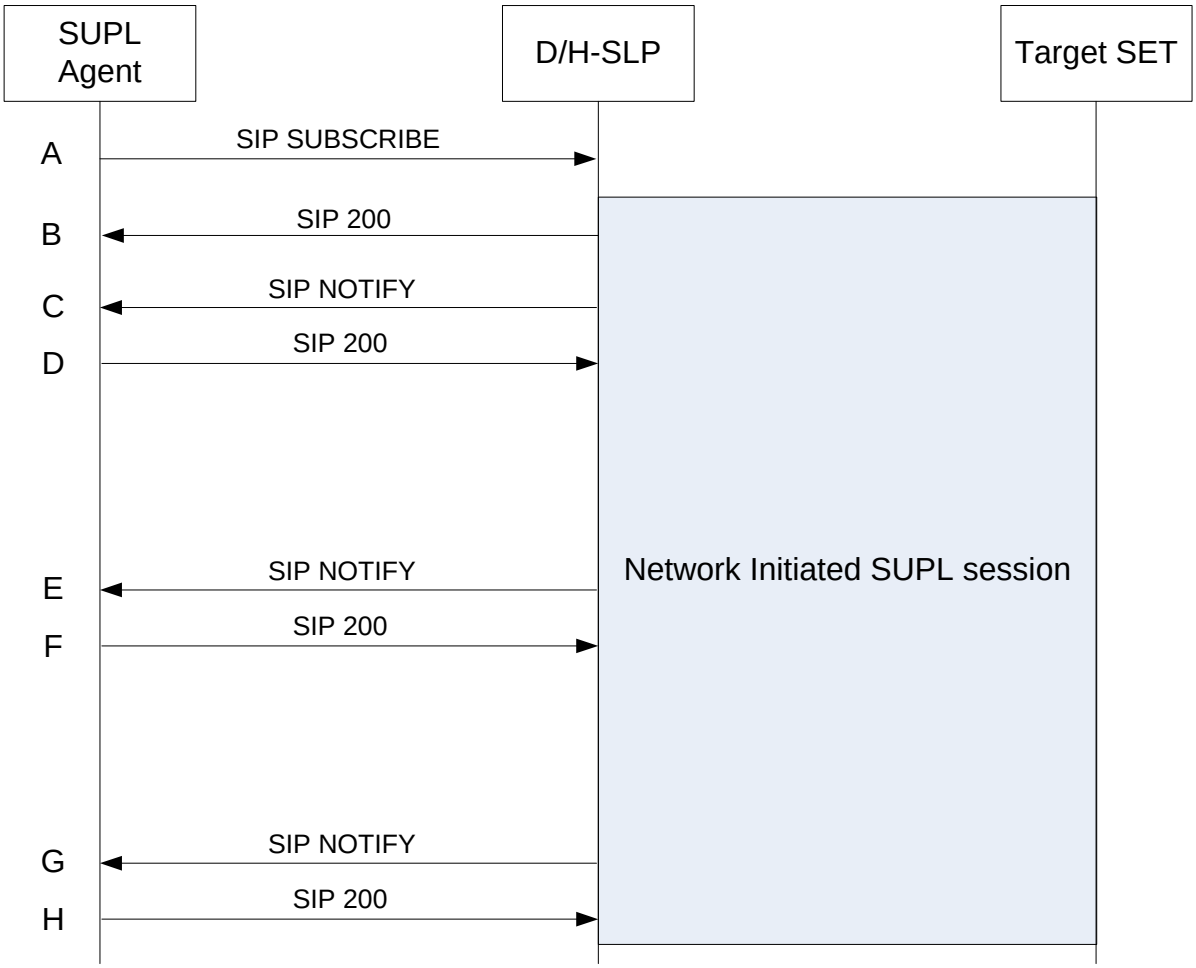

Figure 53: Network-Initiated Triggered Periodic

A. The SUPL Agent sends a SIP SUBSCRIBE message that is directed to the D/H-SLP with which the Target SET is associated. The SIP SUBSCRIBE message includes an Event header (with min-interval and max-interval set to the same value) to request periodic reporting. The D/H-SLP performs the necessary authorisation checks to ensure the originator is allowed to request the location information of the Target SET. The D/H-SLP may also verify that the Target SET supports SUPL.

NOTE: The specifics for determining if the SET supports SUPL are beyond the scope of SUPL 3.0.

The D/H-SLP initiates a SUPL session. For Network Initiated Triggered Periodic reporting, the corresponding ULP message exchange between the SET and D/H-SLP is the same as described in Section 5.3.1.1 (Figure 25), and is therefore not explicitly shown in Figure 53, but only indicated as "Network Initiated SUPL session" in the diagram.

B. The D/H-SLP responds to the SUPL Agent with an appropriate SIP 200 or 202 response.

NOTE: The SIP response may be sent at any time after the D/H-SLP receives the SIP SUBSCRIBE message.

C. Once the position calculation is complete (as described in steps G to I of Section 5.3.1.1), the D/H-SLP sends the initial position estimate back to the SUPL Agent in the body of a SIP NOTIFY message.

D. The SUPL Agent returns a SIP 200 OK response to the D/H-SLP.

Steps C and D are repeated periodically (as illustrated in steps E and F).

When the last position estimate is calculated (i.e., the end of the periodic triggered session has been reached), the D/H-SLP sends the final position estimate back to the SUPL Agent in the body of a SIP NOTIFY message (as illustrated in step G). The SUPL Agent returns a SIP 200 OK response to the D/H-SLP (in step H) and the D/H-SLP releases all resources related to this session.

D.3 Network-Initiated Triggered Area and Velocity Event

This section illustrates the message flow for network-initiated triggered area and velocity event sessions. It corresponds to the flow as specified in Section 5.3.2.1, but uses LOCSIP messages instead of MLP messages between the SUPL Agent and the D/H-SLP.

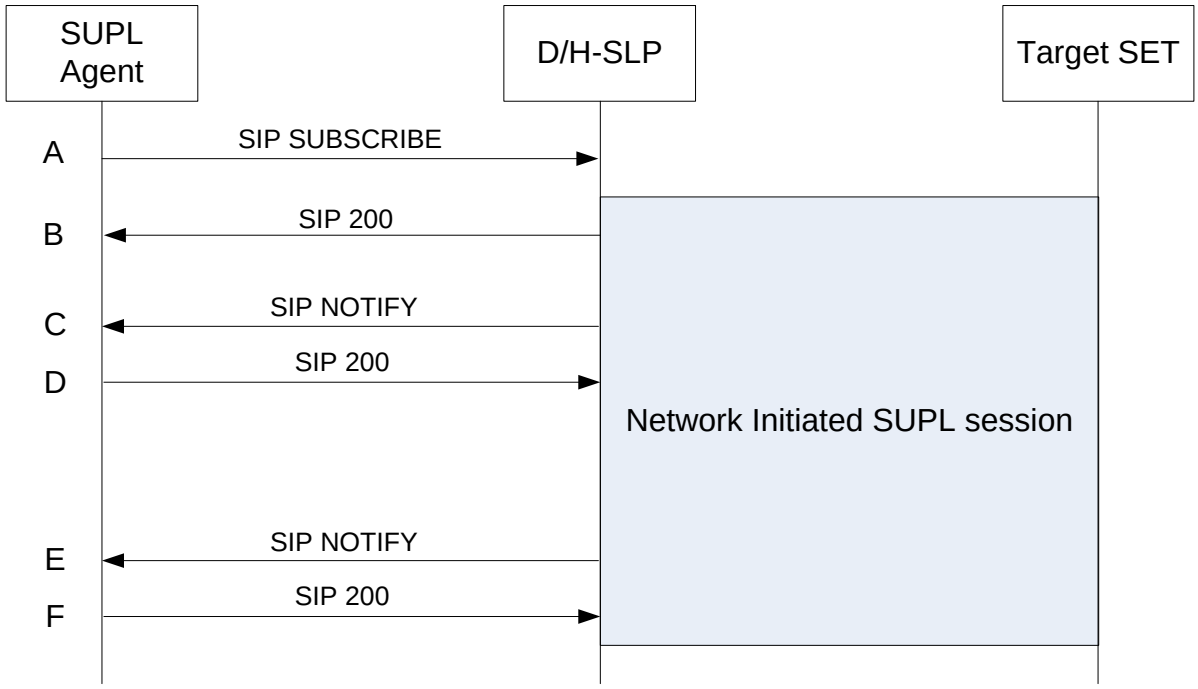

Figure 54: Network-Initiated Triggered Area or Velocity Event

A. The SUPL Agent sends a SIP SUBSCRIBE message that is directed to the D/H-SLP with which the Target SET is associated. The SIP SUBSCRIBE message includes all parameters required for the area or velocity event trigger session (e.g., geographic target area, trigger criteria, etc.). The D/H-SLP performs the necessary authorisation checks to ensure the originator is allowed to request the location information of the Target SET. The D/H-SLP may also verify that the Target SET supports SUPL.

NOTE: The specifics for determining if the SET supports SUPL are beyond the scope of SUPL 3.0.

The D/H-SLP initiates a SUPL session. For Network-Initiated Triggered Area or Velocity Event reporting, the corresponding ULP message exchange between the SET and D/H-SLP is the same as described in Section 5.3.2.1 (Figure 26), and is therefore not explicitly shown in Figure 54, but only indicated as “Network Initiated SUPL session” in the diagram.

B. The D/H-SLP responds to the SUPL Agent with an appropriate SIP 200 or 202 response.

NOTE: The SIP response may be sent at any time after the D/H-SLP receives the SIP SUBSCRIBE message.

C. Once the position or velocity calculation is complete and the area or velocity event trigger is checked (as described in steps G to K of Section 5.3.2.1), the D/H-SLP sends a SIP NOTIFY message to the SUPL Agent. If the area or velocity event trigger condition is satisfied, the D/H-SLP includes the initial position (and/or velocity) estimate in

the body of the SIP NOTIFY message. If the area or velocity event trigger condition is not satisfied, the D/H-SLP includes an empty or neutral body in the SIP NOTIFY message.

D. The SUPL Agent returns a SIP 200 OK response to the D/H-SLP.

If the SUPL Agent has requested several reports and more reports are to be sent, steps C and D are repeated.

E. If an area or velocity event is triggered (as described in steps J and K of Section 5.3.2.1), the D/H-SLP sends the position (and/or velocity) estimate back to the SUPL Agent in the body of a SIP NOTIFY message.

NOTE: Subsequent SIP NOTIFY messages are sent only after the minimum time between reports has elapsed.

F. The SUPL Agent returns a SIP 200 OK response to the D/H-SLP.

When the last requested report is sent, the D/H-SLP releases all resources related to this session.

Appendix E. Use of LPP/LPPe for Legacy Services (Normative)

This Appendix describes the use of LPP/LPPe for Legacy Services. Legacy Services are SUPL services which follow the call flow logic established in previous releases of SUPL and include all services except those using GSS. In the following, the term LPPe is used instead of LPP/LPPe and it is assumed that the call flows apply to both LPP and LPPe.

The LPP/LPPe call flows shown in this appendix are the same for non-roaming and roaming scenarios and only non-roaming scenarios are presented here.

The following sections define a minimum set of LPP/LPPe call flows which SHALL be supported by both the SET and the D/H-SLP. It should be noted that LPP/LPPe allows other message flows that are not defined here. These other flows may be employed by a SET and D/H-SLP but their support is not mandated for SUPL 3.0.

Please note that the order of LPP/LPPe messages received (as shown in the diagrams in this appendix) SHALL also be the order of LPP/LPPe messages processed.

NOTE: All LPP/LPPe messages are encapsulated in SUPL POS. While shown in the diagrams, the encapsulation of LPP/LPPe messages in SUPL POS is not explicitly mentioned in the call flow descriptions.

E.1 Immediate Services

The call flows in this section apply when the first LPP/LPPe message(s) for the session is (are) sent by the SET. Note that the SET decides whether or not to send the first message(s) not the D/H-SLP.

Figure 55 shows the LPP/LPPe call flow for Network Initiated SET-Assisted and SET-Based position determination for immediate services which SHALL be supported by the SET and the D/H-SLP. Only the LPP/LPPe call flow part of the entire call flow diagram is described.

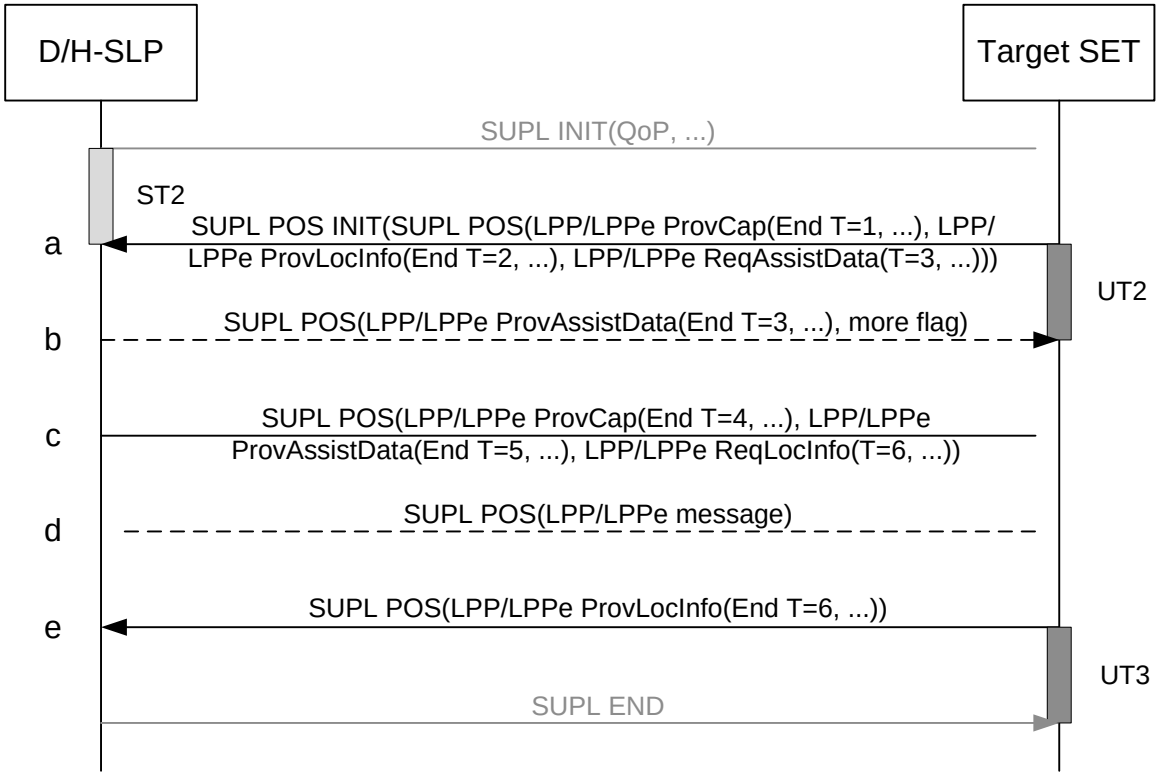

Figure 55: Network Initiated SET-Assisted/SET-Based Position Determination LPP/LPPe Session for Single Fix Service

a. The SET sends a SUPL POS INIT message starting the positioning session with the D/H-SLP. The SET includes a SUPL POS message carrying LPP/LPPe payload. The SET SHALL send an unsolicited LPP/LPPe Provide Capabilities message (transaction id = 1, transaction end flag set) to provide the D/H-SLP with its LPP/LPPe capabilities. The SET SHALL send an unsolicited LPP/LPPe Provide Location Information message (transaction id = 2, transaction end flag set) to provide the D/H-SLP with location information required to obtain assistance data for the SET and/or to enable an initial location estimate. Minimally, this location information SHALL include information on the serving access network – e.g. serving cell ID, serving WiFi AP, SET IP address. The SET MAY start an LPP/LPPe Assistance Data Transfer procedure (transaction id = 3) requesting assistance data by sending an LPP/LPPe Request Assistance Data message (transaction id = 3) to the D/H-SLP. The LPP/LPPe Provide Location Information message need not be sent if the minimal location information is included in the LPP/LPPe Request Assistance Data.

b. If the D/H-SLP is able to obtain a location estimate from the location information provided by the SET in step (a) that satisfies the QoP, it may skip the remaining LPP/LPPe steps. This step is only performed if in step (a) the SET requested assistance data in which case the D/H-SLP SHALL provide the requested assistance data in an LPP/LPPe Provide Assistance Data message (transaction id = 3, transaction end flag set) to the SET. If the requested assistance data in step (a) is identical to the assistance data the D/H-SLP is intending to send based on the selected positioning method, this step is skipped and the assistance data will be sent in step (c) instead. This ends the LPP/LPPe Assistance Data Transfer procedure (transaction id = 3). The D/H-SLP indicates that further SUPL POS messages will follow by setting the *more flag*.

c. If the D/H-SLP has not previously provided its LPP/LPPe capabilities to the SET, the D/H-SLP MAY send an unsolicited LPP/LPPe Provide Capabilities message (transaction id = 4, transaction end flag set) to the SET. The D/H-SLP MAY send an LPP/LPPe Provide Assistance Data message (transaction id = 5, transaction end flag set) providing unsolicited assistance data to the SET (e.g. data additional to anything requested in step (a) and provided in step (b)). However, if step (b) was not performed, the LPP/LPPe Provide Assistance Data message is sent in response to the LPP/LPPe Request Assistance Data message (transaction id = 3) in step (a) and as a result, the LPP Provide Assistance Data message is solicited with transaction id = 3. The D/H-SLP SHALL initiate an LPP/LPPe Location Information Transfer procedure (transaction id = 6) by sending an LPP/LPPe Request Location Information message (transaction id =

6) to the SET. In SET-Assisted mode, the D/H-SLP requests measurements while in SET-Based mode the D/H-SLP requests a position estimate from the SET.

d. The SET may request additional assistance data and the D/H-SLP may request additional location information in accordance with the LPP call flow rules defined in [3GPP LTE] and shown in Appendix E.3.

e. The SET responds with an LPP/LPPe Provide Location Information message (transaction id = 6, transaction end flag set). This ends the LPP/LPPe Location Information procedure (transaction id = 6). In SET-Assisted mode, the SET provides measurements while in SET-Based mode the SET provides a position estimate to the D/H-SLP. If the position result obtained by the D/H-SLP does not meet the QoP, steps (c) to (e) may be repeated as needed. This ends the LPP/LPPe session.

Figure 56 shows the LPP/LPPe call flow for SET Initiated SET-Assisted and SET-Based (with position result being sent back to the D/H-SLP) position determination for immediate services which SHALL be supported by the SET and the D/H-SLP. Only the LPP/LPPe call flow part of the entire call flow diagram is described.

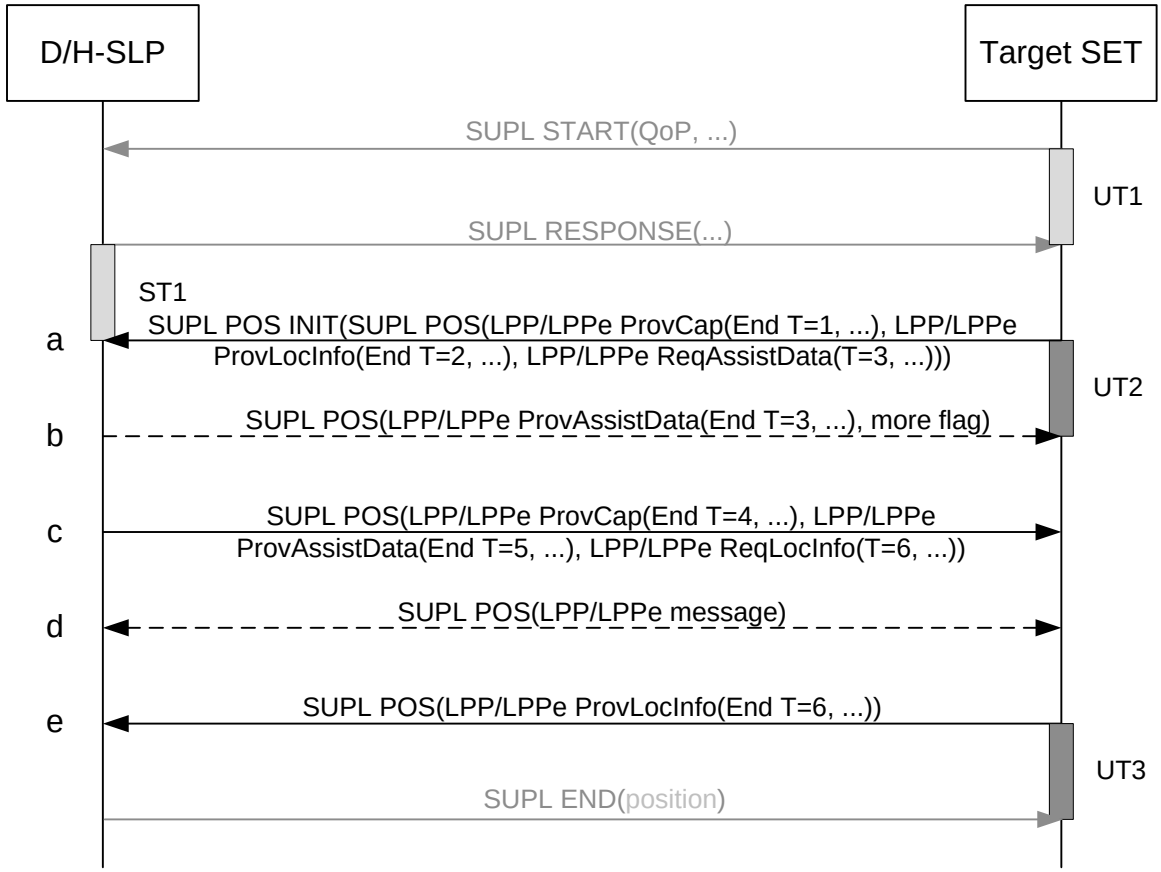

Figure 56: SET Initiated SET-Assisted and SET-Based (with position result being sent back to the D/H-SLP) Position Determination LPP/LPPe Session for Single Fix Service

Steps (a) – (e) in Figure 56 are the same as those in Figure 55. Please note that in SET-Assisted mode, the SUPL END message carries the position result while in SET-Based mode the SUPL END message does not carry a position result.

Figure 57 shows the LPP/LPPe call flow for Assistance Data SET-Based positioning for immediate services which SHALL be supported by the SET and the D/H-SLP. Only the LPP/LPPe call flow part of the entire call flow diagram is described.

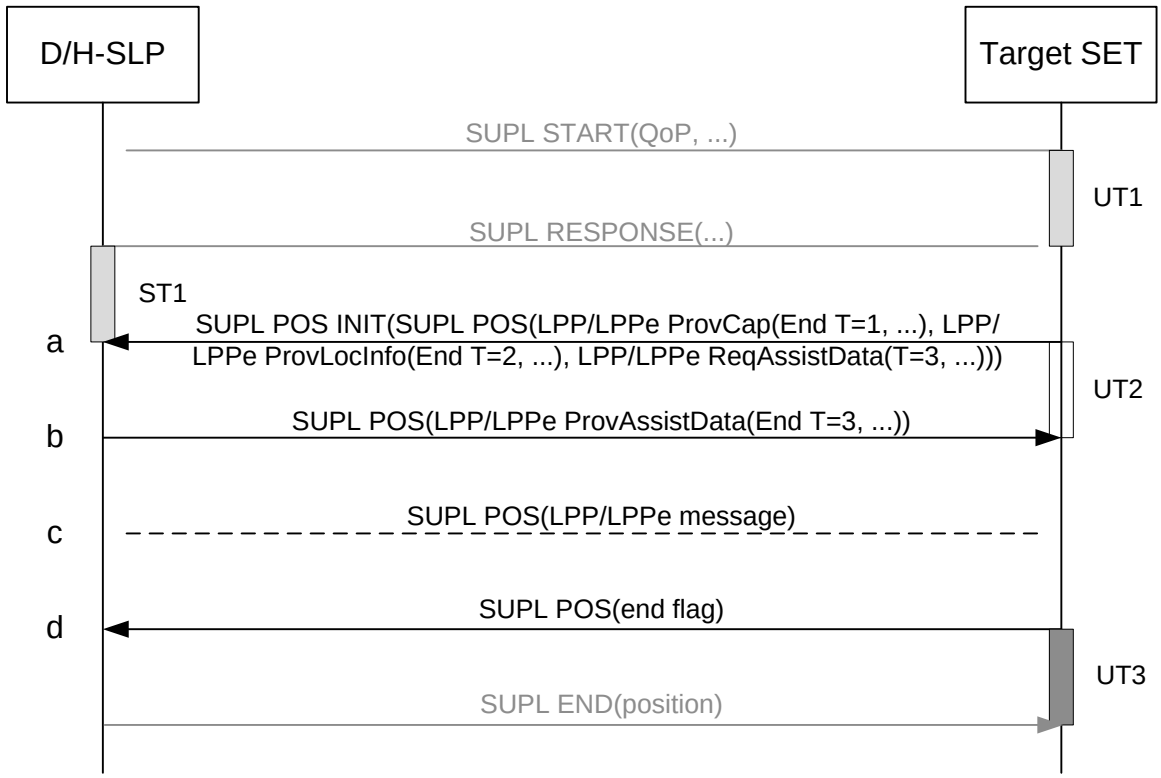

Figure 57: SET Initiated Assistance Data SET-Based Position Determination LPP/LPPe Session for Single Fix Service

a. Same as in Figure 55 except that the assistance data which the SET may request in this step is for SET-Based positioning.

b. If the D/H-SLP is able to obtain a location estimate from the location information provided by the SET in step (a) that satisfies the QoP, it may skip the remaining LPP/LPPe steps and return the position estimate to the SET in the SUPL END message. If the D/H-SLP is able to determine that the requested assistance data is associated with SET-Based rather than SET-Assisted positioning, the D/H-SLP SHALL provide the requested assistance data in an LPP/LPPe Provide Assistance Data message (transaction id = 3, transaction end flag set) to the SET. This ends the LPP/LPPe Assistance Data Transfer procedure (transaction id = 3).

c. The SET may request additional assistance data and the D/H-SLP may request additional location information in order to support this assistance data in accordance with the LPP call flow rules defined in [3GPP LTE] and shown in Appendix E.3.

d. To end the LPP/LPPe session, the SET sends an empty SUPL POS message with the *end flag* set.

E.2 Deferred Services

The call flows in this section apply when the first LPP/LPPe message(s) for the session is(are) sent by the SET. Note that the SET decides whether or not to send the first message(s) not the D/H-SLP.

Figure 58 shows the LPP/LPPe call flow for Network Initiated SET-Assisted and SET-Based position determination for triggered services which SHALL be supported by the SET and the D/H-SLP. Only the LPP/LPPe call flow of the first positioning session is described. The LPP/LPPe call flows for all subsequent positioning sessions are identical.

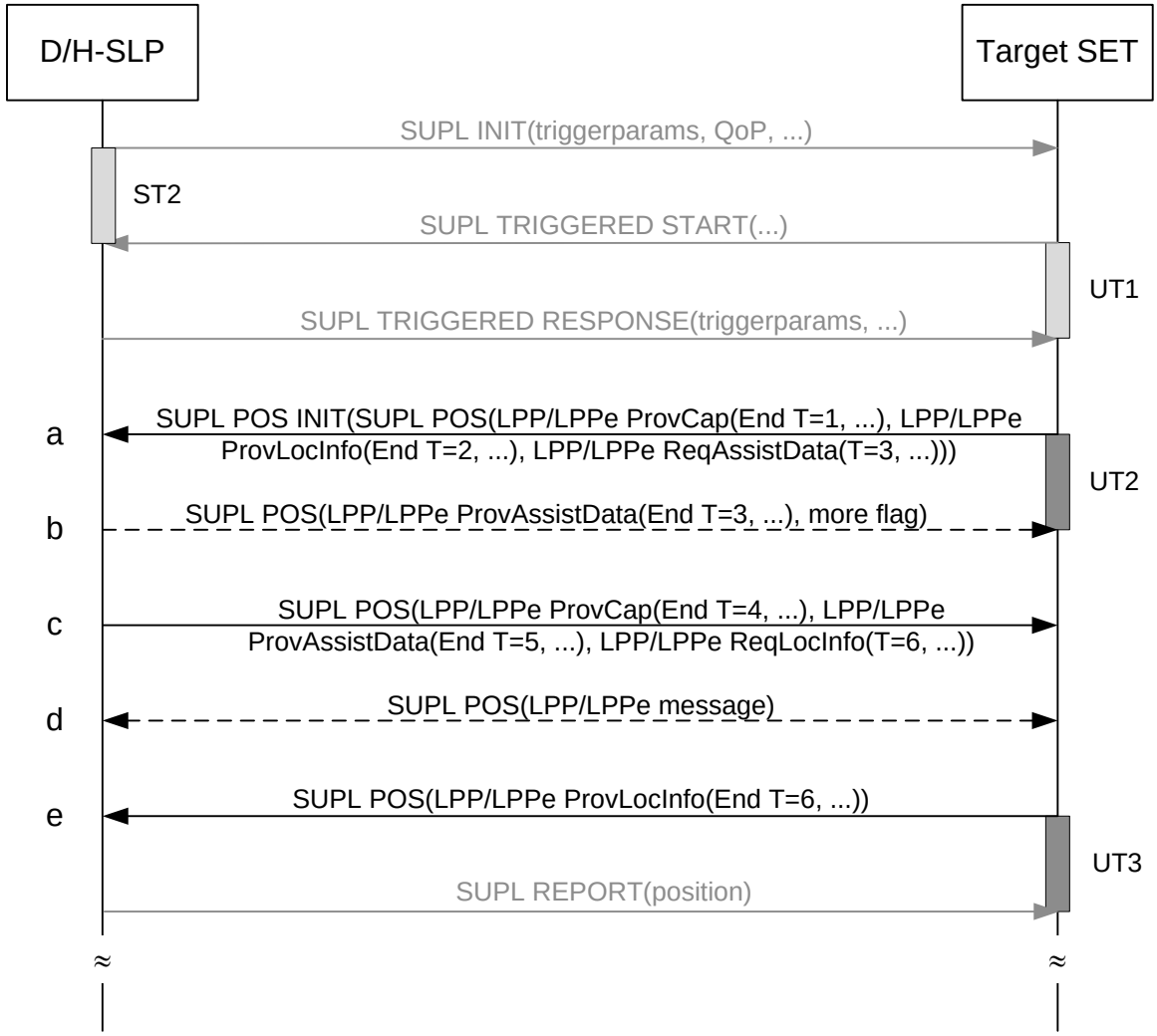

Figure 58: Network Initiated SET-Assisted/SET-Based Position Determination LPP/LPPe Session for Triggered Services

Steps (a) – (e) are the same as those in Figure 55.

Note that in the last step in Figure 58, depending on the reporting mode (real time, quasi real time or batch reporting) the D/H-SLP may include the position estimate result in SUPL REPORT.

Figure 59 shows the LPP/LPPe call flow for SET Initiated SET-Assisted and SET-Based (with position result being sent back to the D/H-SLP) position determination for triggered services which SHALL be supported by the SET and the D/H-SLP. Only the LPP/LPPe call flow of the first positioning session is described. The LPP/LPPe call flows for all subsequent positioning sessions are identical.

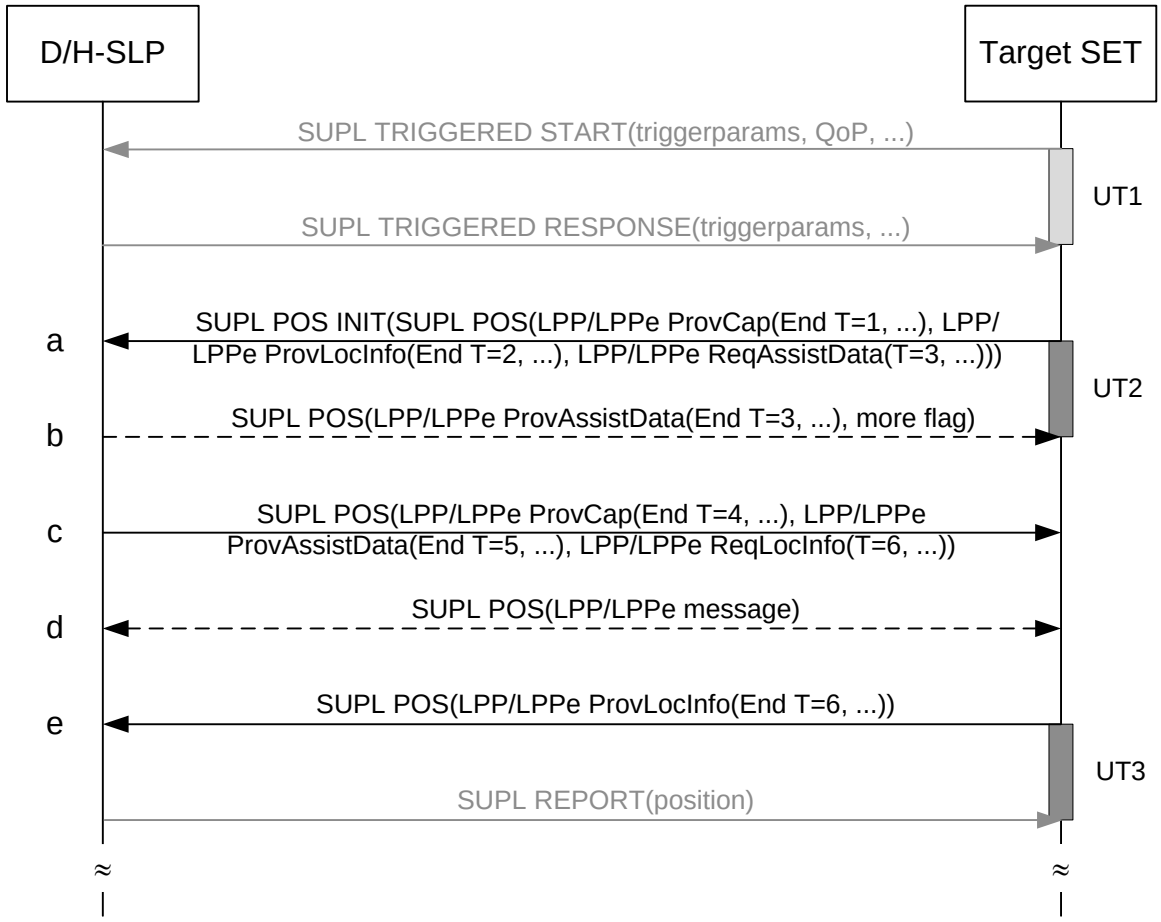

Figure 59: SET Initiated SET-Assisted and SET-Based (with position result being sent back to the D/H-SLP) Position Determination LPP/LPPe Session for Triggered Services

Steps (a) – (e) are the same as those in Figure 55.

Note that in the last step of Figure 59, in SET-Assisted mode the SUPL REPORT message carries the position estimate result, while in SET-Based mode the SUPL REPORT message does not carry the position estimate result.

Figure 60 shows the LPP/LPPe call flow for Assistance Data SET-Based positioning for triggered services which SHALL be supported by the SET and the D/H-SLP. Only the LPP/LPPe call flow of the first positioning session is described. The LPP/LPPe call flows for all subsequent positioning sessions are identical.

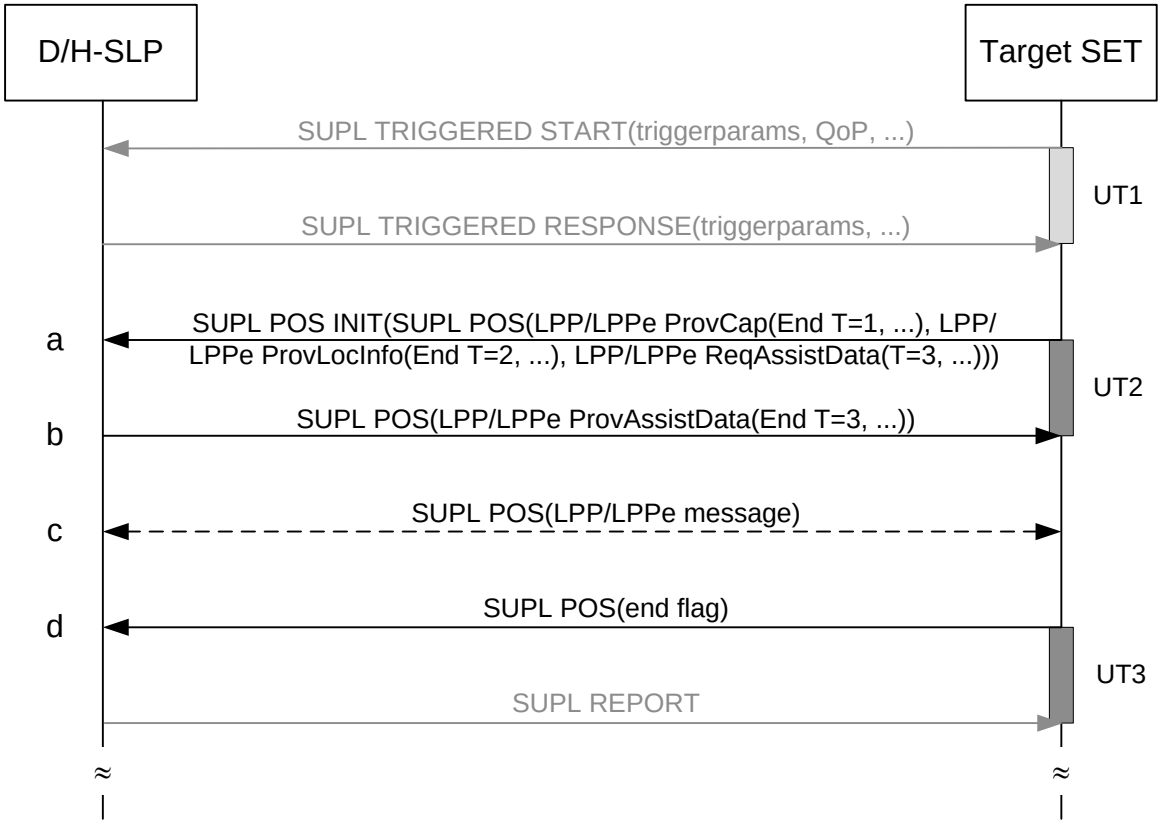

Figure 60: SET Initiated Assistance Data SET-Based Position Determination LPP/LPPe Session for Triggered Services

Steps (a) – (e) are the same as those in Figure 57.

E.3 Additional LPP/LPPe Call Flows

This section shows additional LPP/LPPe call flows for LPP/LPPe Assistance Data and Location Information transfer procedures which SHALL be supported by the SET and the SLP. These call flows are required if in the course of the LPP/LPPe call flows shown in the previous sections of Appendix F the SET requires additional assistance data or the SLP requires additional location information.

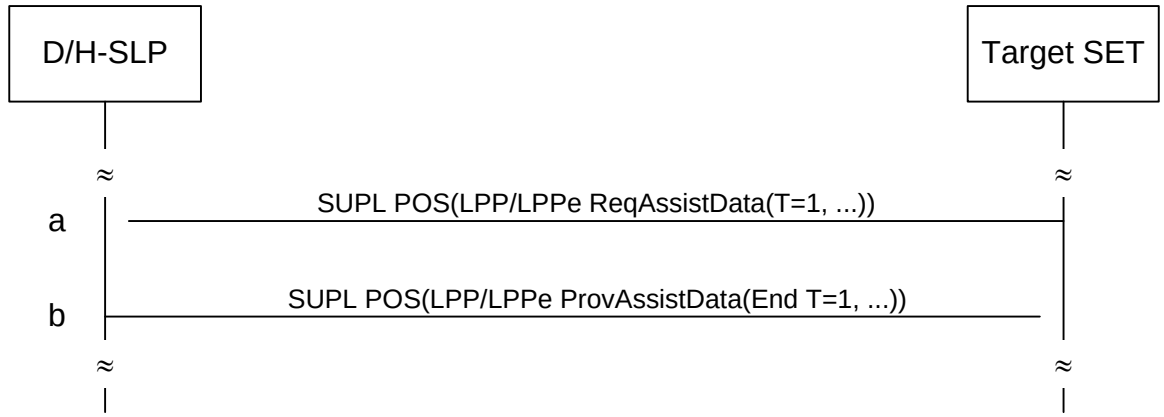

Figure 61: LPP/LPPe Assistance Data Transfer Procedure

a. The SET starts an LPP/LPPe Assistance Data Transfer procedure (transaction id = 1) by sending an LPP/LPPe Request Assistance Data message (transaction id = 1) to the D/H-SLP.

b. The D/H-SLP provides the requested assistance data by sending an LPP/LPPe Provide Assistance Data message (transaction id = 1, transaction end flag set) to the SET. This ends the LPP/LPPe Assistance Data Transfer procedure (transaction id = 1).

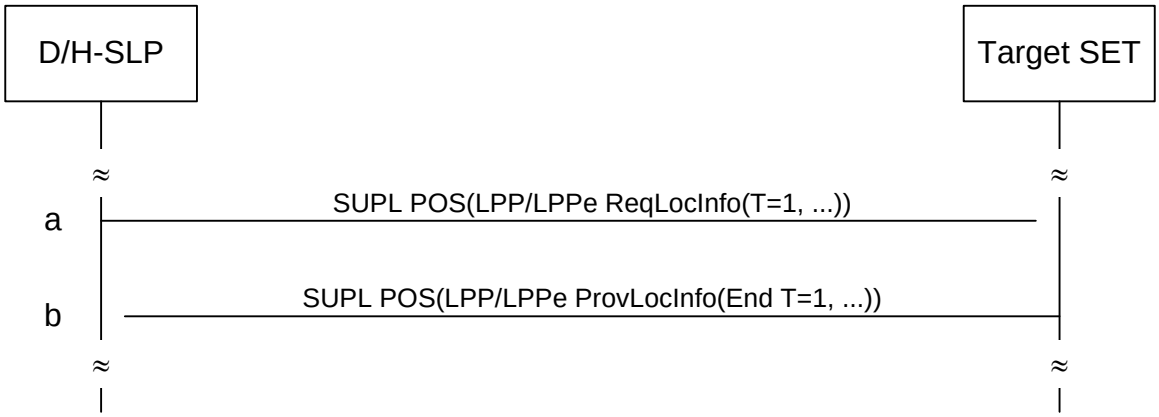

Figure 62: LPP/LPPe Location Information Transfer Procedure

a. The D/H-SLP starts an LPP/LPPe Location Information Transfer procedure (transaction id = 1) by sending an LPP/LPPe Request Location Information message (transaction id = 1) to the SET.

b. The SET provides the requested location information by sending an LPP/LPPe Provide Location Information message (transaction id = 1, transaction end flag set) to the D/H-SLP. This ends the LPP/LPPe Location Information Transfer procedure (transaction id = 1).

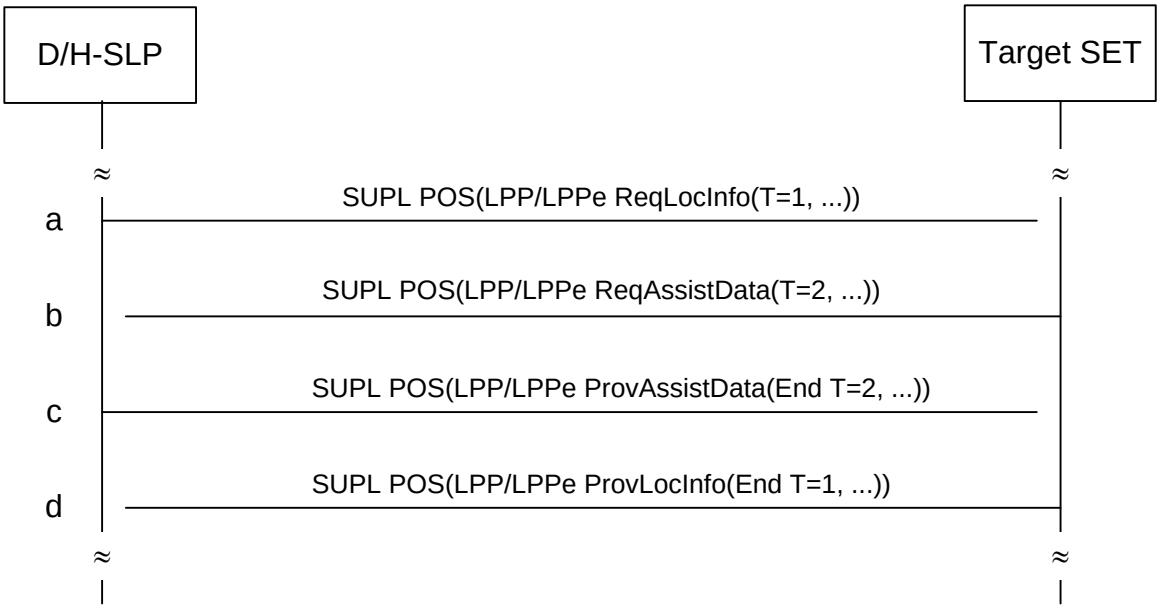

Figure 63: LPP/LPPe Assistance Data Transfer Procedure including LPP/LPPe Location Information Transfer

a. The D/H-SLP starts an LPP/LPPe Location Information Transfer procedure (transaction id = 1) by sending an LPP/LPPe Request Location Information message (transaction id = 1) to the SET.

b. In order to provide the requested location information, the SET requests assistance data from the D/H-SLP. To this end the SET initiates an LPP/LPPe Assistance Data Transfer procedure (transaction id = 2) and sends an LPP/LPPe Request Assistance Data message (transaction id = 2) to the D/H-SLP.

c. The D/H-SLP responds by providing the requested assistance data to the SET by sending an LPP/LPPe Provide Assistance Data message (transaction id = 2, transaction end flag set) to the SET. This ends the LPP/LPPe Assistance Data Transfer procedure (transaction id = 2).

d. The SET provides the location information requested in step (a) by sending an LPP/LPPe Provide Location Information message (transaction id = 1, transaction end flag set) to the D/H-SLP. This ends the LPP/LPPe Location Information Transfer procedure (transaction id = 1).

Appendix F. Use of LPP/LPPe in Positioning Activities in GSS (Normative)

This Appendix describes the use of LPP/LPPe for positioning activities in GSS as defined in chapter 5.3.5.

Within a GSS, positioning activities can be invoked at any time to (1) request assistance data, (2) provide assistance data, (3) request position or measurements and (4) provide position or measurements and combinations thereof. SET and D/H-SLP can also exchange their LPP/LPPe capabilities. Each activity is performed by executing a corresponding LPP/LPPe session. The LPP/LPPe call flows in this appendix are the same for non-roaming and roaming scenarios and only the non-roaming scenarios are presented here.

The following sections define a minimum set of LPP/LPPe call flows which SHALL be supported by both the SET and the D/H-SLP. It should be noted that LPP/LPPe allows other message flows that are not defined here. These other flows may be employed by a SET and D/H-SLP but their support is not mandated for SUPL 3.0.

Please note that the order of LPP/LPPe messages received (as shown in the diagrams in this appendix) SHALL also be the order of LPP/LPPe messages processed.

NOTE: All LPP/LPPe messages are encapsulated in SUPL POS. While shown in the diagrams, the encapsulation of LPP/LPPe messages in SUPL POS is not explicitly mentioned in the call flow descriptions.

F.1 Network Initiated Positioning Activities

Figure 64 shows the LPP/LPPe call flow for Network Initiated SET-Assisted and SET-Based positioning determination.

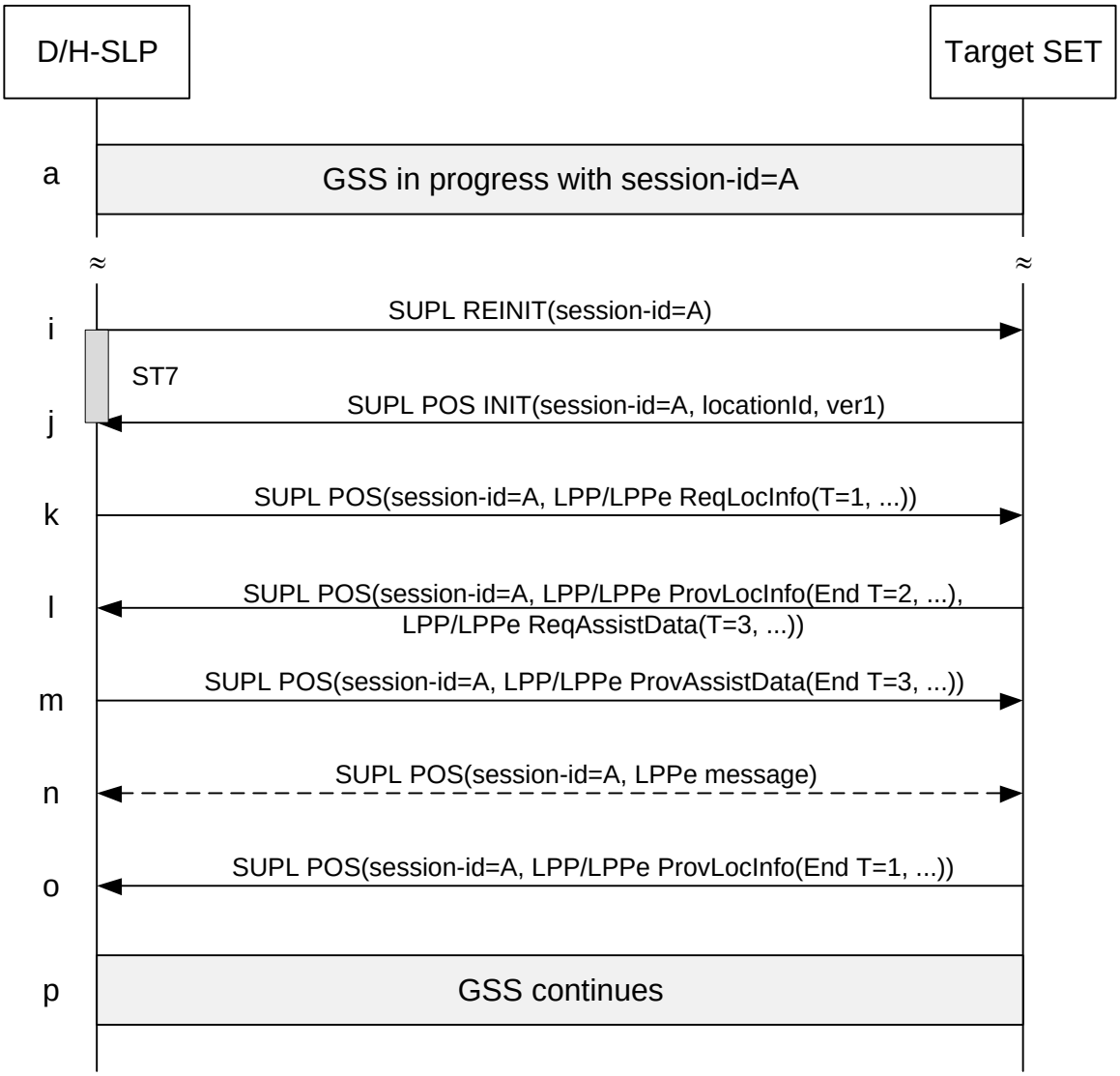

Figure 64: Network Initiated SET-Assisted/SET-Based Positioning Determination LPP/LPPe Session

a. A GSS session is in progress.

b. When the D/H-SLP wants to start a positioning activity with the SET, the D/H-SLP sends a SUPL REINIT message to the SET to initiate the positioning activity. Before the SUPL REINIT message is sent, the D/H-SLP also computes and stores a hash of the message.

c. The SET analyses the received SUPL REINIT message. If found to be non authentic, the SET takes no further action. Otherwise the SET takes needed action to establish or resume a secure connection. The SET responds with a SUPL POS INIT message carrying the Location ID (*locationId*) and hash of the SUPL REINIT message (*ver1*).

d. The D/H-SLP SHALL check that the hash of SUPL REINIT (*ver1*) matches the one it has computed for this particular session. The D/H-SLP starts an LPP/LPPe session with the SET in order to determine the SET's position in either SET-Assisted or SET-Based mode. The D/H-SLP initiates an LPP/LPPe Location Information Transfer procedure (transaction id = 1) with the SET by sending an LPP/LPPe Request Location Information message (transaction id = 1) to the SET. In SET-Assisted mode, the D/H-SLP requests measurements from the SET while in SET-Based mode, the D/H-SLP requests position estimates from the SET.

e. This step is optional and is executed only if the SET requires assistance data from the D/H-SLP. The SET SHALL provide any location information required by the D/H-SLP to provide assistance data in an unsolicited LPP/LPPe

Provide Location Information message to the D/H-SLP (transaction id = 2, transaction end flag set). This message need not be sent if the location information is included in the LPP/LPPe Request Assistance Data or if the SET is aware (e.g. from previous GSS activity) that the D/H-SLP already has recent location information for the SET that is still valid. The SET SHALL initiate an LPP/LPPe Assistance Data Transfer procedure (transaction id = 3) with the D/H-SLP by sending an LPP/LPPe Request Assistance Data message (transaction id = 3) to the D/H-SLP, requesting the required assistance data.

f. This step is optional and only executed if step (l) was performed. The D/H-SLP provides the assistance data requested in step (l) to the SET by sending an LPP/LPPe Provide Assistance Data message (transaction id = 3, transaction end flag set) to the SET. This ends the LPP/LPPe Assistance Data Transfer procedure (transaction id = 3).

g. The SET may request additional assistance data and the D/H-SLP may request additional location information in accordance with the LPP call flow rules defined in [3GPP LTE] (see Appendix E.3).

h. The SET provides the location information requested in step (k) (measurements for SET-Assisted and position estimate for SET-Based mode) to the D/H-SLP by sending an LPP/LPPe Provide Location Information message to the D/H-SLP. This ends the LPP/LPPe Location Information Transfer procedure (transaction id = 1, transaction end flag set). This also ends the LPP/LPPe session.

i. The GSS continues.

Figure 65 shows the LPP/LPPe call flow for Capabilities Request by the D/H-SLP.

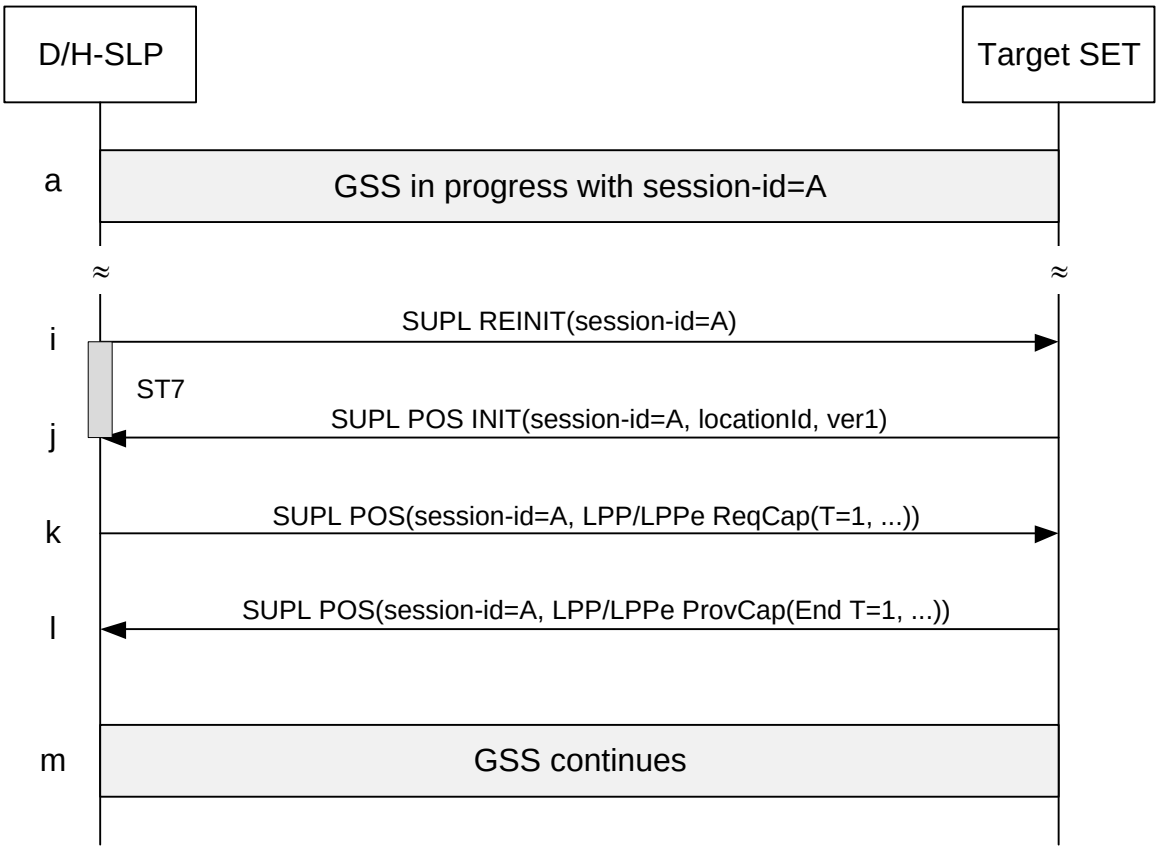

Figure 65: Capabilities Request by the D/H-SLP

a. A GSS session is in progress.

b. When the D/H-SLP wants to start a positioning activity with the SET, the D/H-SLP sends a SUPL REINIT message to the SET to initiate the positioning activity. Before the SUPL REINIT message is sent, the D/H-SLP also computes and stores a hash of the message.

c. The SET analyses the received SUPL REINIT. If found to be non authentic, the SET takes no further action. Otherwise the SET takes needed action to establish or resume a secure connection. The SET responds with a SUPL POS INIT message carrying the Location ID (*locationId*) and hash of the SUPL REINIT message (*ver1*).

d. The D/H-SLP starts an LPP/LPPe Capabilities Transfer procedure (transaction id = 1) by sending an LPP/LPPe Request Capabilities message (transaction id = 1) to the SET.

e. The SET provides its LPP/LPPe capabilities requested in step (k) to the D/H-SLP by sending an LPP/LPPe Provide Capabilities message (transaction id = 1, transaction end flag set) to the SET. This ends the LPP/LPPe Assistance Data Transfer procedure (transaction id = 1).

f. The GSS continues.

Figure 66 shows the LPP/LPPe call flow for unsolicited Capabilities Provide by the D/H-SLP.

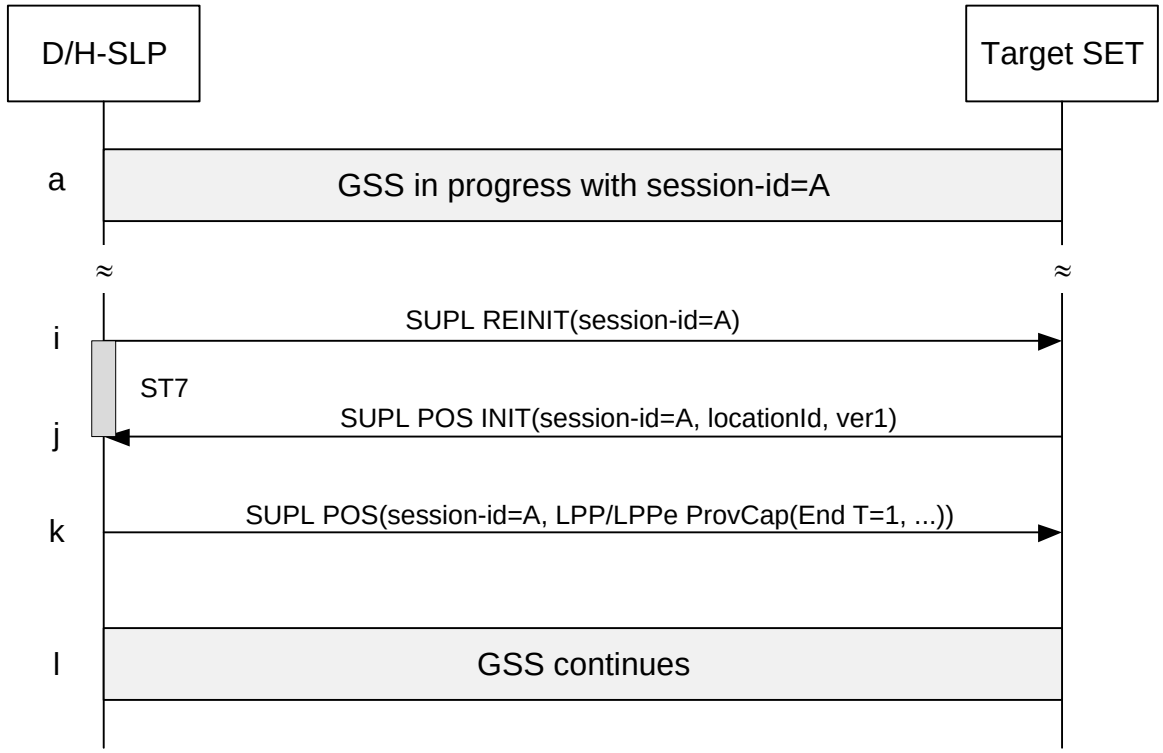

Figure 66: Unsolicited Capabilities Provide by the D/H-SLP

a. A GSS session is in progress.

b. When the D/H-SLP wants to start a positioning activity with the SET, the D/H-SLP sends a SUPL REINIT message to the SET to initiate the positioning activity. Before the SUPL REINIT message is sent, the D/H-SLP also computes and stores a hash of the message.

c. The SET analyses the received SUPL REINIT. If found to be non authentic, the SET takes no further action. Otherwise the SET takes needed action to establish or resume a secure connection. The SET responds with a SUPL POS INIT message carrying the Location ID (*locationId*) and hash of the SUPL REINIT message (*ver1*).

d. The D/H-SLP sends an unsolicited LPP/LPPe Provide Capabilities message (transaction id = 1, transaction end flag set) to the SET.

e. The GSS continues.

Please note that D/H-SLP and SET may also perform a combination of the call flows of Figure 65 and Figure 66 whereby the D/H-SLP requests the SET's LPP/LPPe Capabilities in an LPP/LPPe Request Capabilities message while at the same time providing its own LPP/LPPe Capabilities in an unsolicited LPP/LPPe Provide Capabilities message within the same SUPL POS message.

F.2 SET Initiated Positioning Activities

Figure 67 shows the LPP/LPPe call flow for SET Initiated SET-Assisted positioning determination (option I).

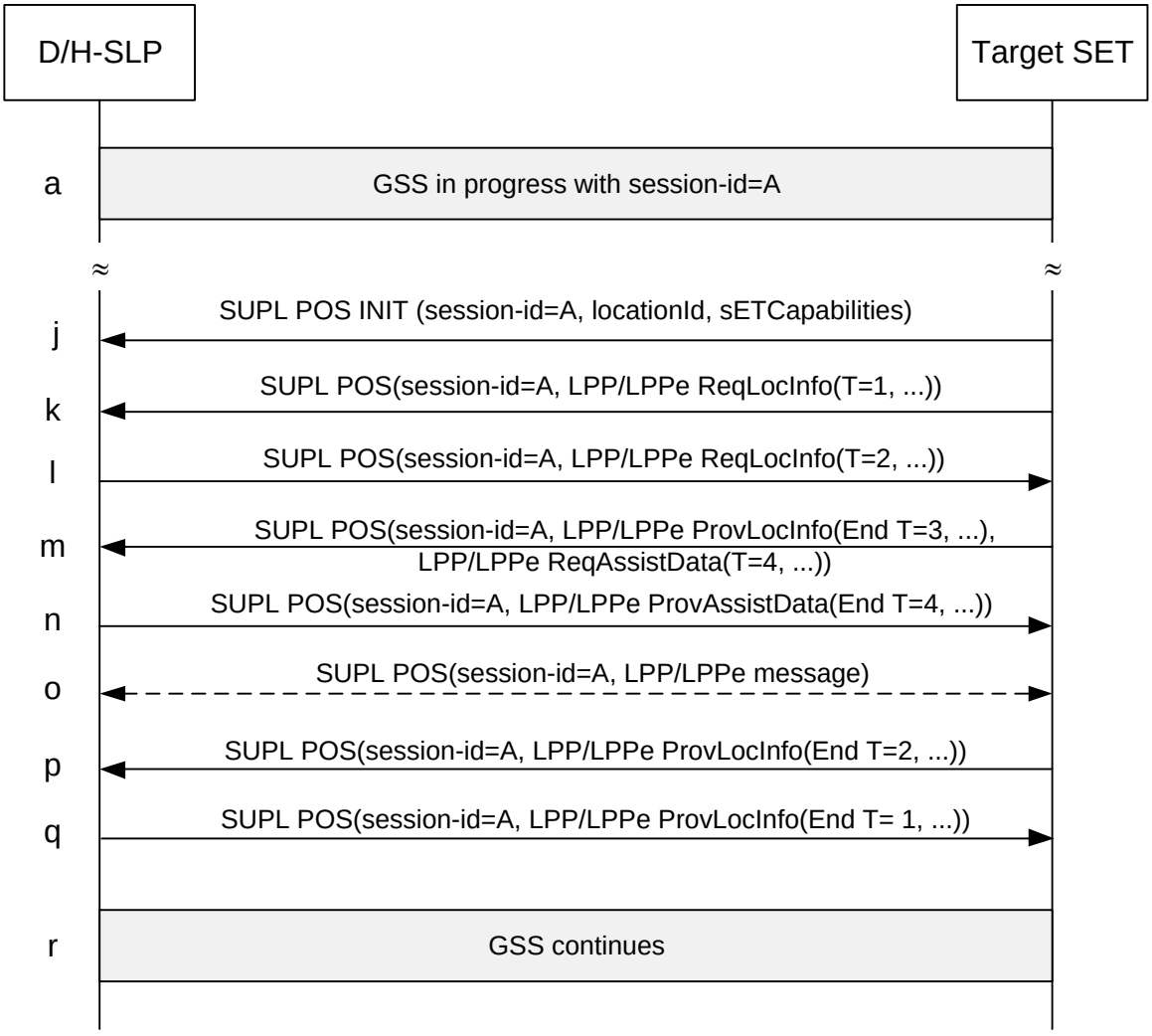

Figure 67: SET Initiated SET-Assisted Positioning Determination LPP/LPPe Session – Option I

a. A GSS session is in progress.

b. The SET starts an LPP/LPPe session with the D/H-SLP in order to determine its position in SET-Assisted mode. If required (i.e., no active secure connection exists between the SET and the D/H-SLP), the SET takes action to establish

or resume a secure connection with the D/H-SLP. The SET sends a SUPL POS INIT message containing the Location ID (*locationId*) and SET capabilities (*sETCapabilities*)

c. The SET initiates an LPP/LPPe Location Information Transfer procedure (transaction id = 1) with the D/H-SLP indicating SET-Assisted mode by sending an LPP/LPPe Request Location Information message (transaction id = 1) to the D/H-SLP.

d. The D/H-SLP starts an LPP/LPPe Location Information Transfer procedure (transaction id = 2) with the SET indicating SET-Assisted mode by sending an LPP/LPPe Request Location Information message (transaction id = 2) requesting measurements to the SET.

e. This step is optional and only executed if the SET requires assistance data from the D/H-SLP. The SET SHALL provide any location information required by the D/H-SLP to obtain assistance data in an unsolicited LPP/LPPe Provide Location Information message (transaction id = 3, transaction end flag set) to the D/H-SLP. This message need not be sent if the location information is included in the LPP/LPPe Request Assistance Data or if the SET is aware (e.g. from previous GSS activity) that the D/H-SLP already has recent location information for the SET that is still valid. The SET initiates an LPP/LPPe Assistance Data Transfer procedure (transaction id = 4) with the D/H-SLP by sending an LPP/LPPe Request Assistance Data message (transaction id = 4) to the D/H-SLP requesting the required assistance data.

f. This step is optional and only executed if step (m) was performed. The D/H-SLP provides the assistance data requested in step (m) to the SET by sending an LPP/LPPe Provide Assistance Data message (transaction id = 4, transaction end flag set) to the SET. This ends the LPP/LPPe Assistance Data Transfer procedure (transaction id = 4).

g. The SET may request additional assistance data and the D/H-SLP may request additional location information in accordance with the LPP call flow rules defined in [3GPP LTE] (see Appendix E.3).

h. The SET obtains the measurements requested in step (l) and sends the measurements to the D/H-SLP in an LPP/LPPe Provide Location Information message. This ends the LPP/LPPe Location Information Transfer procedure (transaction id = 2, transaction end flag set).

i. The D/H-SLP uses the measurements received from the SET in step (p) to calculate a position estimate and returns the position estimate result to the SET in an LPP/LPPe Provide Location Information message. This ends the LPP/LPPe Location Information Transfer procedure (transaction id = 1, transaction end flag set). This also ends the LPP/LPPe session.

j. The GSS continues.

Figure 68 shows the LPP/LPPe call flow for SET Initiated SET-Assisted positioning determination (option II).

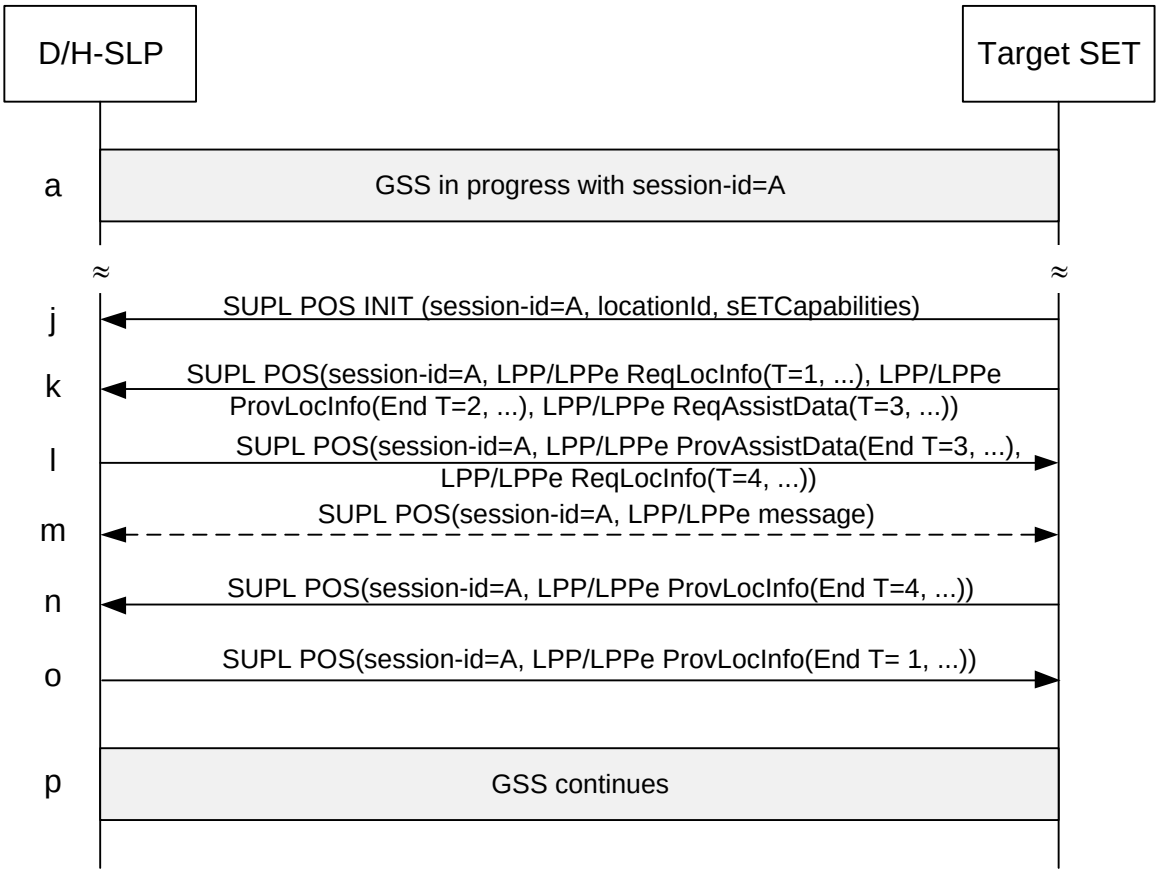

Figure 68: SET Initiated SET-Assisted Positioning Determination LPP/LPPe Session – Option II

a. A GSS session is in progress.

b. The SET starts an LPP/LPPe session with the D/H-SLP in order to determine its position in SET-Assisted mode. If required (i.e., no active secure connection exists between the SET and the D/H-SLP), the SET takes action to establish or resume a secure connection with the D/H-SLP. The SET sends a SUPL POS INIT message containing the Location ID (*locationId*) and SET capabilities (*sETCapabilities*).

c. The SET initiates an LPP/LPPe Location Information Transfer procedure (transaction id = 1) with the D/H-SLP indicating SET-Assisted mode by sending an LPP/LPPe Request Location Information message (transaction id = 1) to the D/H-SLP. The SET provides any location information required by the D/H-SLP to obtain assistance data in an unsolicited LPP/LPPe Provide Location Information message (transaction id = 2, transaction end flag set) to the D/H-SLP. This message need not be sent if the location information is included in the LPP/LPPe Request Assistance Data or if the SET is aware (e.g. from previous GSS activity) that the D/H-SLP already has recent location information for the SET that is still valid. The SET also initiates an LPP/LPPe Assistance Data Transfer procedure (transaction id = 3) with the D/H-SLP by sending an LPP/LPPe Request Assistance Data message (transaction id = 3) to the D/H-SLP requesting assistance data.

d. The D/H-SLP provides the assistance data requested in step (k) to the SET by sending an LPP/LPPe Provide Assistance Data message (transaction id = 3, transaction end flag set) to the SET. This ends the LPP/LPPe Assistance Data Transfer procedure (transaction id = 3). The D/H-SLP starts an LPP/LPPe Location Information Transfer procedure (transaction id = 4) with the SET indicating SET-Assisted mode by sending an LPP/LPPe Request Location Information message (transaction id = 4) requesting measurements to the SET.

e. The SET may request additional assistance data and the D/H-SLP may request additional location information in accordance with the LPP call flow rules defined in [3GPP LTE] (see Appendix E.3).

f. The SET obtains the measurements requested in step (l) and sends the measurements to the D/H-SLP in an LPP/LPPe Provide Location Information message (transaction id = 4, transaction end flag set). This ends the LPP/LPPe Location Information Transfer procedure (transaction id = 4).

g. The D/H-SLP uses the measurements received from the SET in step (n) to calculate a position estimate and returns the position estimate result to the SET in an LPP/LPPe Provide Location Information message (transaction id = 1, transaction end flag set). This ends the LPP/LPPe Location Information Transfer procedure (transaction id = 1). This also ends the LPP/LPPe session.

h. The GSS continues.

Figure 69 shows the LPP/LPPe call flow for SET Initiated SET-Based positioning determination and solicited assistance data transfer.

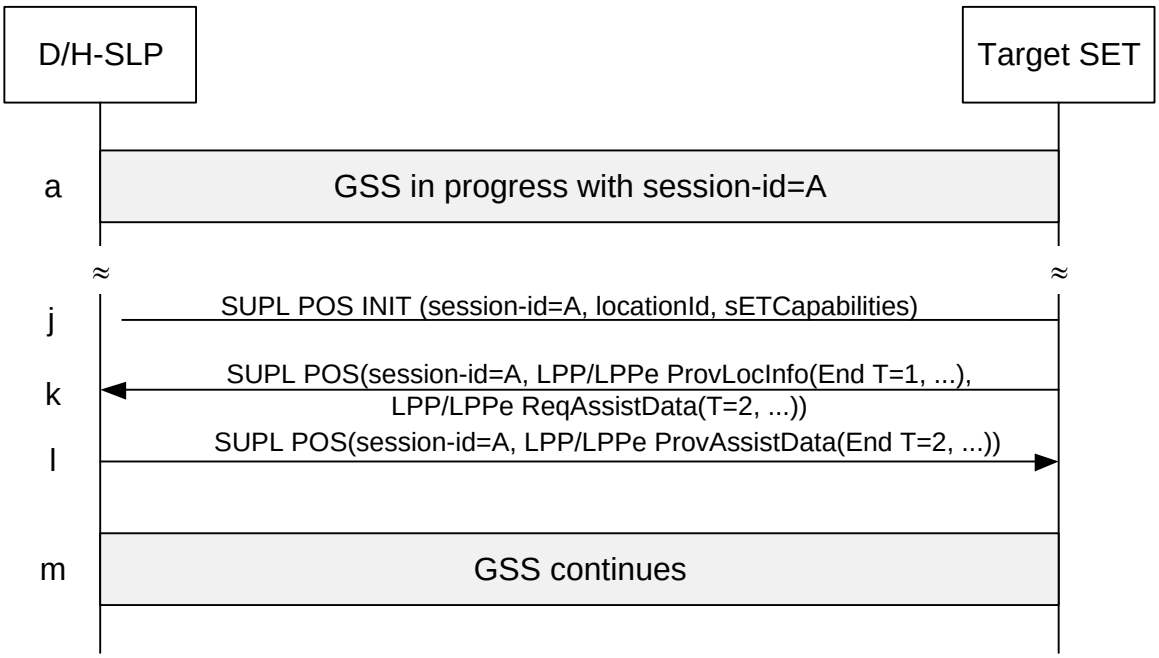

Figure 69: SET Initiated SET-Based Positioning Determination (Solicited Assistance Data Transfer) LPP/LPPe Session

a. A GSS session is in progress.

b. The SET starts a positioning activity with the D/H-SLP. If required (i.e., no active secure connection exists between the SET and the D/H-SLP), the SET takes action to establish or resume a secure connection with the D/H-SLP. The SET sends a SUPL POS INIT message containing the Location ID (*locationId*) and SET capabilities (*sETCapabilities*).

c. The SET provides any location information required by the D/H-SLP to obtain assistance data in an unsolicited LPP/LPPe Provide Location Information message (transaction id = 1, transaction end flag set) to the D/H-SLP. This message need not be sent if the location information is included in the LPP/LPPe Request Assistance Data or if the SET is aware (e.g. from previous GSS activity) that the D/H-SLP already has recent location information for the SET that is still valid. The SET initiates an LPP/LPPe Assistance Data Transfer procedure (transaction id = 2) with the D/H-SLP by sending an LPP/LPPe Request Assistance Data message (transaction id = 2) to the D/H-SLP, requesting the required assistance data.

d. The D/H-SLP provides the assistance data requested in step (k) to the SET by sending an LPP/LPPe Provide Assistance Data message to the SET. This ends the LPP/LPPe Assistance Data Transfer procedure (transaction id = 2, transaction end flag set). This also ends the LPP/LPPe session.

e. The GSS continues.

Figure 70 shows the LPP/LPPe call flow for Capabilities Request by the SET.

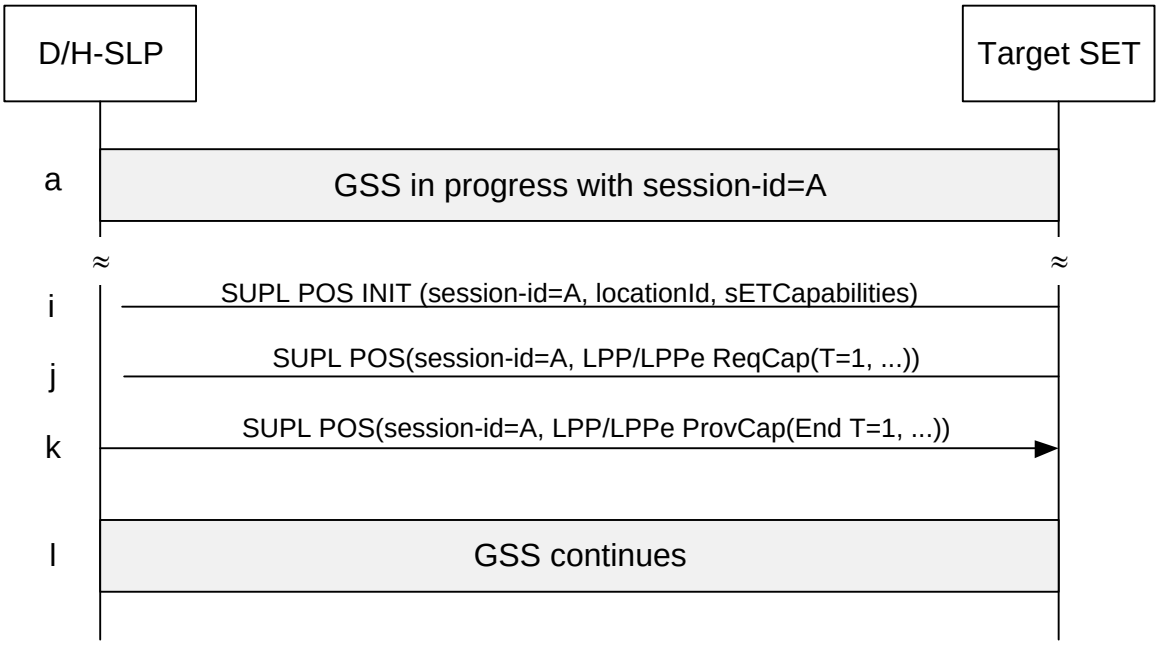

Figure 70: Capabilities Request by the SET

a. A GSS session is in progress.

b. The SET starts a capabilities request procedure with the D/H-SLP. If required (i.e., no active secure connection exists between the SET and the D/H-SLP), the SET takes action to establish or resume a secure connection with the D/H-SLP. The SET sends a SUPL POS INIT message containing the Location ID (*locationId*) and SET capabilities (*sETCapabilities*).

c. The SET starts an LPP/LPPe Capabilities Transfer procedure (transaction id = 1) by sending an LPP/LPPe Request Capabilities message (transaction id = 1) to the SET.

d. The D/H-SLP provides its LPP/LPPe capabilities requested in step (j) to the SET by sending an LPP/LPPe Provide Capabilities message (transaction id = 1, transaction end flag set) to the D/H-SLP. This ends the LPP/LPPe Assistance Data Transfer procedure (transaction id = 1).

e. The GSS continues.

Figure 71 shows the LPP/LPPe call flow for unsolicited Capabilities Provide by the SET.

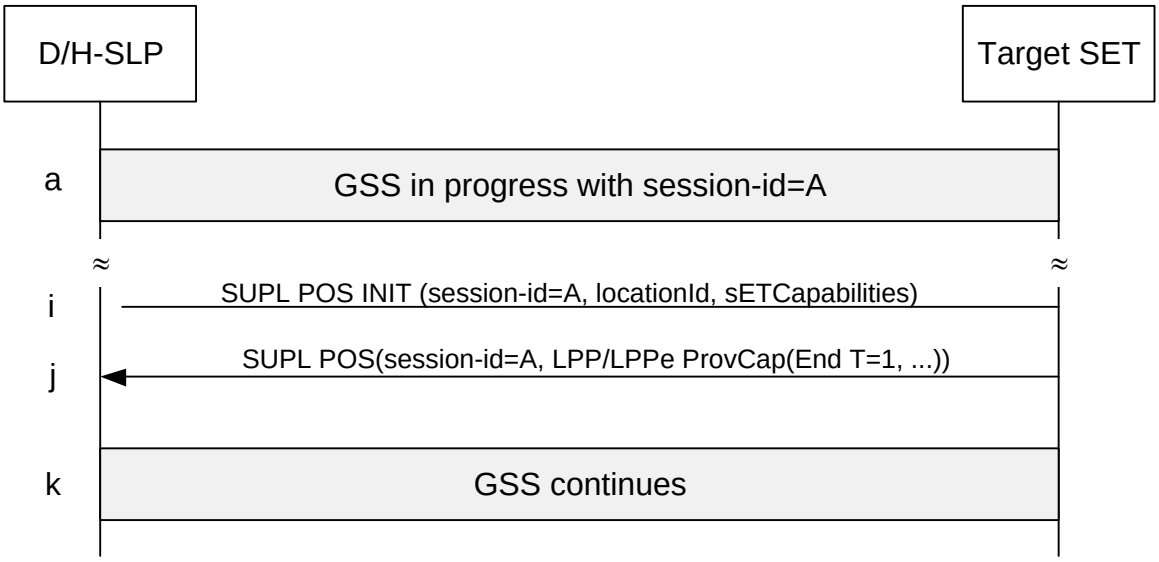

Figure 71: Unsolicited Capabilities Provide by the SET

a. A GSS session is in progress.

b. The SET starts an unsolicited capabilities provide procedure with the D/H-SLP. If required (i.e., no active secure connection exists between the SET and the D/H-SLP), the SET takes action to establish or resume a secure connection with the D/H-SLP. The SET sends a SUPL POS INIT message containing the Location ID (*locationId*) and SET capabilities (*sETCapabilities*).

c. The SET sends an unsolicited LPP/LPPe Provide Capabilities message (transaction id = 1, transaction end flag set) to the D/H-SLP.

d. The GSS continues.

Please note that D/H-SLP and SET may also perform a combination of the call flows of Figure 70 and Figure 71 whereby the SET requests the D/H-SLP's LPP/LPPe Capabilities in an LPP/LPPe Request Capabilities message while at the same time providing its own LPP/LPPe Capabilities in an unsolicited LPP/LPPe Provide Capabilities message within the same SUPL POS message.

Appendix G. Area Event Trigger Examples (informative)

The following section provides examples of how area event triggers can be used singly or combined to support different use cases. These examples can themselves be combined for new use cases.

G.1 Single report when SET is inside target area

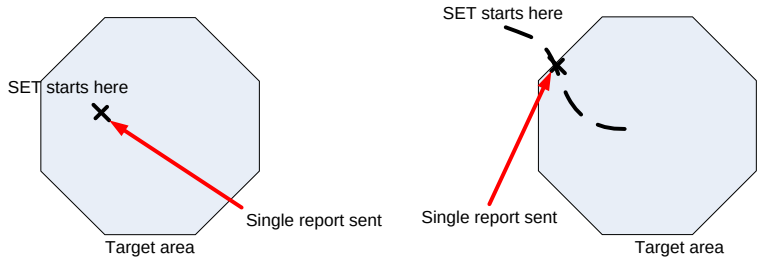

Figure 72: Single report when SET is inside area

Behaviour:	Report once only the first time the SET detects it is inside the target area.
Example use case:	An advertising service is triggered once a user is within a certain area.
Triggers:	“Entering” trigger with no repeated reporting OR “Inside” trigger with no repeated reporting.

G.2 Single report when SET is outside target area

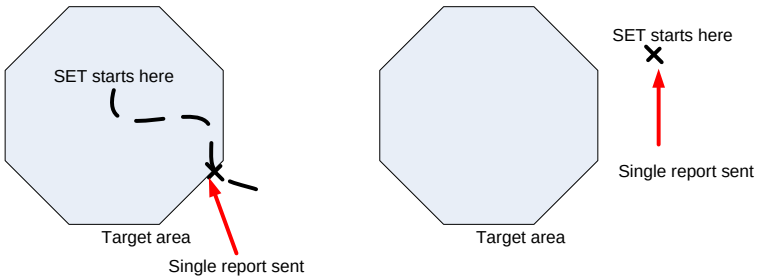

Figure 73: Single report when SET is outside area

Behaviour:	Report once only the first time the SET detects it is outside the target area.
Example use case:	An asset tracking service generates an alert if a vehicle goes outside a predetermined area.
Triggers:	“Leaving” trigger with no repeated reporting OR “Outside” trigger with no repeated reporting.

G.3 Repeated reports whenever SET is inside target area

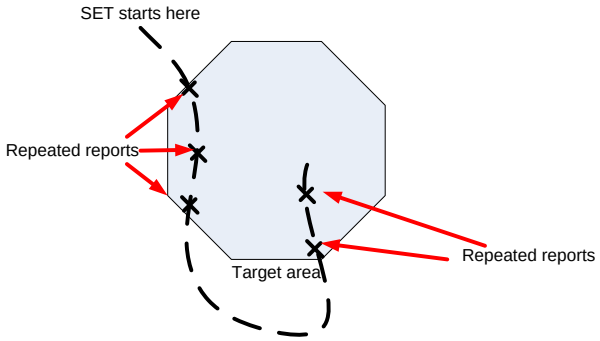

Figure 74: Repeated reports whenever SET is inside target area

Behaviour:	Report at regular intervals while the SET is inside the target area.
Example use case:	A staff locator service tracks the location of employees while they are on campus, but not while they are off-site.
Triggers:	“Inside” trigger with repeated reporting.

G.4 Repeated reports whenever SET is outside target area

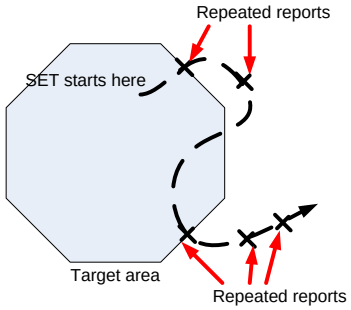

Figure 75: Repeated reports when SET is outside area

Behaviour:	Report at regular intervals while the SET is outside the target area.
Example use case:	An asset tracking service tracks the location of company vehicles while they are on the road, but not while they are within their compound.
Triggers:	“Outside” trigger with repeated reporting.

G.5 Repeated reports each time SET enters target area

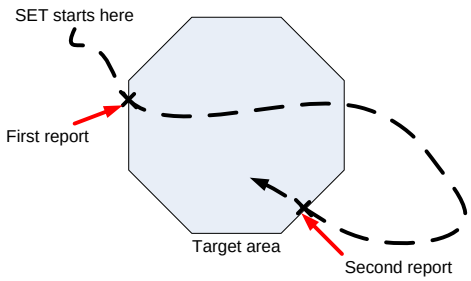

Figure 76: Repeated reports each time SET enters target area

Behaviour:	Report each time SET enters the target area.
Example use case:	A social networking service alerts friends whenever a user enters a predefined area.
Triggers:	“Entering” trigger with repeated reporting.

G.6 Repeated reports each time SET leaves target area

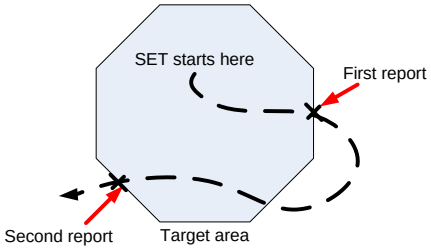

Figure 77: Repeated reports each time SET leaves target area

Behaviour:	Report each time SET enters the target area.
Example use case:	An employee tracking service records each time an employee leaves an assigned region.
Triggers:	“Leaving” trigger with repeated reporting.

G.7 Repeated reports for a fixed period after SET leaves target area

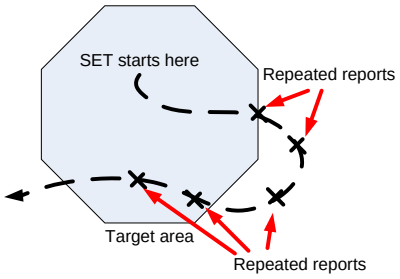

Figure 78: Repeated reports for a fixed period after SET leaves target area

Behaviour:	Report a fixed number of times after SET leaves the target area, regardless of whether it re-enters.
Example use case:	An asset tracking service tracks potentially stolen equipment after it has left an assigned area.
Triggers:	“Leaving” trigger without repeated reporting, followed by periodic trigger.

G.8 Repeated reports for a fixed period after SET enters target area

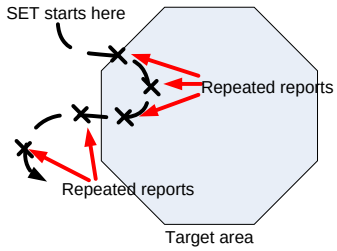

Figure 79: Repeated reports for a fixed period after SET enters target area

Behaviour:	Report a fixed number of times after SET enters the target area, regardless of whether it subsequently exits the target area
Example use case:	A vehicle tracking service generates notifications each time a vehicle enters a predefined area along with an estimated vector calculated by a new of multiple position reports in quick succession.
Triggers:	“Entering” trigger without repeated reporting, followed by periodic trigger.

Appendix H. Interpretation of Geographic Target Areas and Area Id Lists when both are present (informative)

The area id list concept is used to optimize the behaviour of the SET (e.g. minimize battery consumption, save radio bandwidth, reduce the load on the SLP, etc.) and is defined as follows: for each geographic target area there may be two area id lists: (1) one area id list which is *completely* inside the geographic target area called "within" and (2) one area id list which covers the *entire* border area called "border" (refer to Figure 80). The type of the area id list is expressed in the parameter *Area Id Set Type* (part of *Area Event Params*) which can be of type "border" or "within". The following rules apply:

- If a "within" area id list is provided and the SET determines that it is inside the "within" area id list, the SET can assume that it is within the geographic target area.
- If a "border" area id list is provided and the SET determines it is not within either the "border" or the "within" area id list, the SET can assume it is outside the geographic target area. Note that it may be impossible for the H-SLP to completely verify the completeness of area id lists.

Please note that it is up to the SET to decide what action to take after determining that its position is either within or outside the geographic target area.

Depending on the shape and location of the geographic target area, the radio network coverage or the ability of the SLP to generate suitable area id lists, there may or may not be clearly defined "within" or "border" area id lists (examples: (1) one single large radio cell covers the entire geographic target area i.e. there is no "within" area id list but only a "border" area id list; (2) two single large radio cells each partially cover the geographic target area but fail to cover the entire geographic target area i.e. there is no "within" area id list nor is there a "border" area id list).

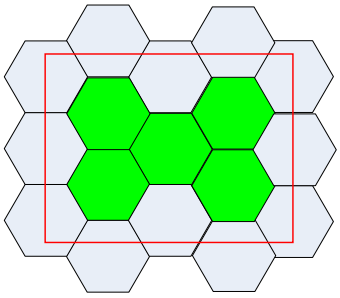

Figure 80: Area ID Lists and Geographic Target Are. The geographic Target Area is shown as bold red line. Note that in this example the green area id list constitutes the "within" area id list while the grey area id list constitutes the "border" area id list.

Appendix I. Area Event Trigger with D-SLP (Informative)

Depending on the D-SLP's service area, the SET's location and the target area's (areas') location when the SET initiates an area event triggered location session (SET Initiated Area Event Triggered Location SUPL session), additional procedures and/or internal actions in the SLP and/or SET may be performed to successfully execute the area event triggered location session. The following sections describe how area event triggers may be performed successfully for different scenarios.

I.1 The target area is outside the D-SLP's service area when the SET is inside the D-SLP's service area

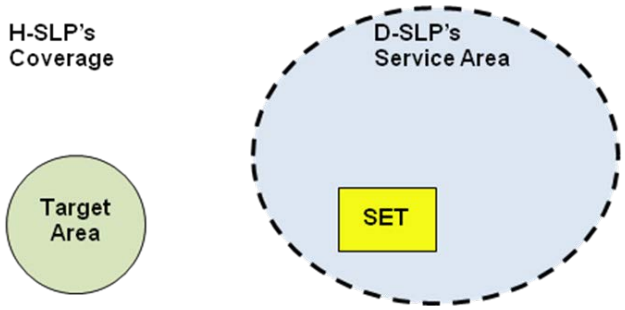

Figure 81: The target area is outside the D-SLP's service area when the SET is inside the D-SLP's service area

The SET initiates the area event triggered location service with the H-SLP immediately, if possible, or the SET initiates the area event triggered location service with the H-SLP when the SET leaves the D-SLP's service area.

I.2 The target area is inside the D-SLP's service area when the SET is outside the D-SLP's service area

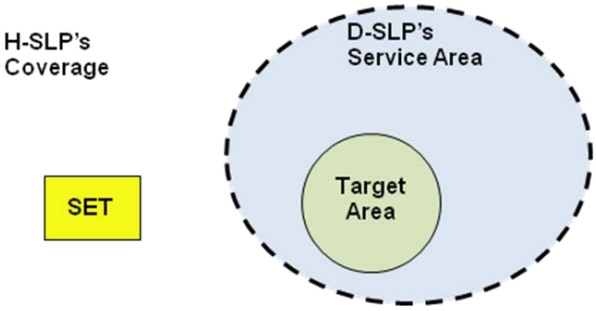

Figure 82: The target area is inside the D-SLP's service area when the SET is outside the D-SLP's service area

The SET initiates the area event triggered location service with the D-SLP when the SET enters the D-SLP's service area.

I.3 The target area is both inside and outside the D-SLP's service areas

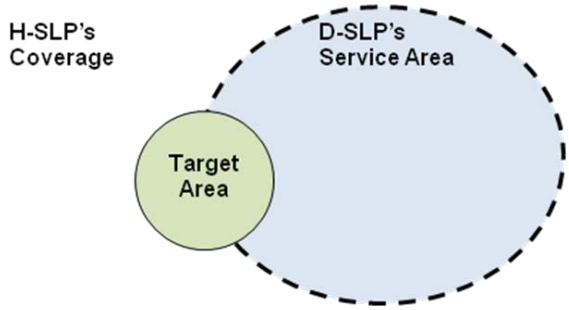

Figure 83: The target area is both inside and outside the D-SLP's service area

The SET splits the target area into two separate target areas. One target area is inside the D-SLP's service area and the other target area is outside the D-SLP's service area. The SET then executes two separate area event trigger session and depending on its location (inside or outside the D-SLP's service area) may act as described in section I.1 and I.2.

I.4 Target areas of the same area event triggered session reside both inside and outside the D-SLP's service area

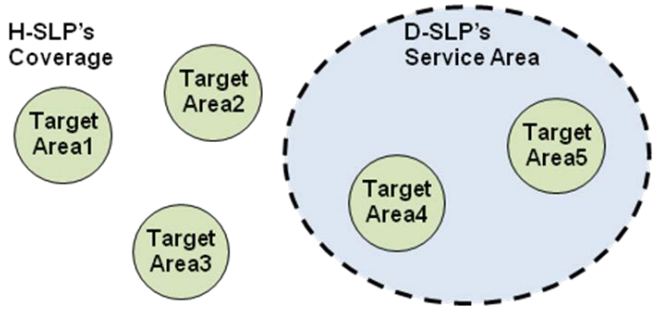

Figure 84: Area event triggered session with target areas that reside both inside and outside the D-SLP's service area

When the SET is inside the D-SLP's service area:

The SET splits the single area event trigger session into two separate area event trigger sessions: one area event trigger session with target areas inside the D-SLP's service area (Target Area 4 and 5), and one area event trigger session with target areas outside the D-SLP's service area (Target Area 1, 2, and 3). The SET then executes two separate area event trigger sessions and depending on its location (inside or outside the D-SLP's service area) may act as described in section I.1 and I.2.

When the SET is outside the D-SLP's service area:

In case that the SET is outside the D-SLP's service area, the SET may execute one of the following two procedures:

Procedure 1: The SET performs the area event trigger session with the H-SLP with all event areas.

Procedure 2: The SET splits the single area event trigger session into two separate area event trigger sessions: one area event trigger session with target areas inside the D-SLP's service area (Target Area 4 and 5), and one area event trigger session with target areas outside the D-SLP's service area (Target Area 1, 2, and 3). The SET then executes two separate area event trigger sessions and depending on its location (inside or outside the D-SLP's service area) may act as described in the section I.1 and I.2.