



Location in SIP/IP core Architecture

Candidate Version 1.0 – 23 Dec 2008

Open Mobile Alliance
OMA-AD-LOCSIP-V1_0-20081223-C

Use of this document is subject to all of the terms and conditions of the Use Agreement located at <http://www.openmobilealliance.org/UseAgreement.html>.

Unless this document is clearly designated as an approved specification, this document is a work in process, is not an approved Open Mobile Alliance™ specification, and is subject to revision or removal without notice.

You may use this document or any part of the document for internal or educational purposes only, provided you do not modify, edit or take out of context the information in this document in any manner. Information contained in this document may be used, at your sole risk, for any purposes. You may not use this document in any other manner without the prior written permission of the Open Mobile Alliance. The Open Mobile Alliance authorizes you to copy this document, provided that you retain all copyright and other proprietary notices contained in the original materials on any copies of the materials and that you comply strictly with these terms. This copyright permission does not constitute an endorsement of the products or services. The Open Mobile Alliance assumes no responsibility for errors or omissions in this document.

Each Open Mobile Alliance member has agreed to use reasonable endeavors to inform the Open Mobile Alliance in a timely manner of Essential IPR as it becomes aware that the Essential IPR is related to the prepared or published specification. However, the members do not have an obligation to conduct IPR searches. The declared Essential IPR is publicly available to members and non-members of the Open Mobile Alliance and may be found on the “OMA IPR Declarations” list at <http://www.openmobilealliance.org/ipr.html>. The Open Mobile Alliance has not conducted an independent IPR review of this document and the information contained herein, and makes no representations or warranties regarding third party IPR, including without limitation patents, copyrights or trade secret rights. This document may contain inventions for which you must obtain licenses from third parties before making, using or selling the inventions. Defined terms above are set forth in the schedule to the Open Mobile Alliance Application Form.

NO REPRESENTATIONS OR WARRANTIES (WHETHER EXPRESS OR IMPLIED) ARE MADE BY THE OPEN MOBILE ALLIANCE OR ANY OPEN MOBILE ALLIANCE MEMBER OR ITS AFFILIATES REGARDING ANY OF THE IPR'S REPRESENTED ON THE “OMA IPR DECLARATIONS” LIST, INCLUDING, BUT NOT LIMITED TO THE ACCURACY, COMPLETENESS, VALIDITY OR RELEVANCE OF THE INFORMATION OR WHETHER OR NOT SUCH RIGHTS ARE ESSENTIAL OR NON-ESSENTIAL.

THE OPEN MOBILE ALLIANCE IS NOT LIABLE FOR AND HEREBY DISCLAIMS ANY DIRECT, INDIRECT, PUNITIVE, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES ARISING OUT OF OR IN CONNECTION WITH THE USE OF DOCUMENTS AND THE INFORMATION CONTAINED IN THE DOCUMENTS.

© 2008 Open Mobile Alliance Ltd. All Rights Reserved.

Used with the permission of the Open Mobile Alliance Ltd. under the terms set forth above.

Contents

- 1. SCOPE (INFORMATIVE)5
- 2. REFERENCES6
 - 2.1 NORMATIVE REFERENCES.....6
 - 2.2 INFORMATIVE REFERENCES.....7
- 3. TERMINOLOGY AND CONVENTIONS8
 - 3.1 CONVENTIONS.....8
 - 3.2 DEFINITIONS.....8
 - 3.3 ABBREVIATIONS8
- 4. INTRODUCTION (INFORMATIVE).....9
 - 4.1 VERSION 1.09
- 5. ARCHITECTURAL MODEL10
 - 5.1 DEPENDENCIES.....10
 - 5.2 ARCHITECTURAL DIAGRAM10
 - 5.3 FUNCTIONAL COMPONENTS AND INTERFACES/REFERENCE POINTS DEFINITION.....12
 - 5.3.1 LOCSIP Functional Entities.....12
 - 5.3.2 External Entities Providing Services to LOCSIP13
 - 5.3.3 Description of the Reference Points.....14
 - 5.3.4 Location Information Format.....16
 - 5.3.5 Location Policies.....16
 - 5.3.6 Charging.....16
 - 5.3.7 Registration17
 - 5.4 FLOWS17
 - 5.4.1 Subscribing to Location Notification.....18
 - 5.4.2 Subscribing to Location for a List of Targets25
 - 5.4.3 Canceling/Refreshing a Location Subscription.....26
 - 5.4.4 Subscribing to Changes of XDMS.....29
 - 5.4.5 Authorization using GPM.....30
 - 5.5 SECURITY CONSIDERATIONS.....31
 - 5.5.1 SIP Signaling Security31
 - 5.5.2 User Plane Security.....31
 - 5.5.3 XDM Security.....31
- APPENDIX A. CHANGE HISTORY (INFORMATIVE).....32
 - A.1 APPROVED VERSION HISTORY32
 - A.2 DRAFT/CANDIDATE VERSION 1.0 HISTORY32

Figures

- Figure 1: LOCSIP Architectural Model11
- Figure 2: Support of Charging Through the OMA Charging Enabler.....17
- Figure 3: Subscribing to Location Notification of Single Target.....19
- Figure 4: Flow for Subscribing to the Notification of Periodic Trigger21
- Figure 5: Flow for Subscribing to the Notification of Area Event Trigger.....22
- Figure 6: Flow for Subscription Expiry Notification.....24
- Figure 7: Flow for Subscription Authorization Failure24
- Figure 8: Flow for Subscribing to Location for a List of Targets.....25

Figure 9: Flow for Location Client Initiated Subscription Cancellation/Refreshing.....27

Figure 10: Flow for Location Server Initiated Subscription Cancellation/Refreshing.....28

Figure 11: Subscribing to Changes in Location Policy Data.....29

Figure 12: Flow for permissions checking with GPM30

Tables

1. Scope

(Informative)

The scope of the Location in SIP/IP core (LOCSIP) architecture document is to define the architecture for the LOCSIP Enabler.

The architecture of the SIP/IP Core and the underlying access networks is out of scope of this document.

2. References

2.1 Normative References

- [3GPP TS 23.228] “IP Multimedia Subsystem (IMS); Stage 2”, 3GPP TS 23.228,
URL: http://www.3gpp.org/ftp/Specs/archive/23_series/23.228/
- [3GPP TS 33.203] ”Access Security for IP-based Services”, 3GPP TS 33.203
<http://www.3gpp.org/ftp/specs/html-info/33203.htm>
- [3GPP2 S.R0086-A] ”IMS Security Framework”, Revision A, Version 1.0
http://www.3gpp2.org/public_html/specs/tsgs.cfm
- [3GPP2 X.S0013-002-B] “All-IP Core Network Multimedia Domain: IP Multimedia Subsystem - Stage 2”, Revision B, Version 1.0, 3GPP2,
URL: http://www.3gpp2.org/Public_html/specs/index.cfm
- [CHG_AD] “Charging Architecture”, Version 1.0, Open Mobile Alliance™, OMA-AD-Charging-V1_0, URL:
<http://www.openmobilealliance.org/>
- [RFC2119] “Key words for use in RFCs to Indicate Requirement Levels”, S. Bradner, March 1997,
URL:<http://www.ietf.org/rfc/rfc2119.txt>
- [RFC3265] “Session Initiation Protocol (SIP)-Specific Event Notification”, A.B. Roach, June 2002, RFC 3265,
URL: <http://www.ietf.org/rfc/rfc3265.txt>
- [RFC4119] “A Presence-based GEOPRIV Location Object Format”, SJ. Peterson, December 2005,
URL:<http://www.ietf.org/rfc/rfc4119.txt>
- [RFC4662] “A Session Initiation Protocol (SIP) Event Notification Extension for Resource Lists”, A. B. Roach et al,
August 2006, RFC 4662,
URL: <http://www.ietf.org/rfc/rfc4662.txt>
- [RFC4825] RFC 4825, “Extensible Markup Language (XML) Configuration Access Protocol (XCAP)”, J. Rosenberg,
May 2007, <http://www.ietf.org/rfc/rfc4825.txt>
- [RFC4826] RFC 4826, “Extensible Markup Language (XML) Formats for Representing Resource Lists”, J.
Rosenberg, May 2007, <http://www.ietf.org/rfc/rfc4826.txt>
- [RFC5139] RFC 5139, "Revised Civic Location Format for Presence Information Data Format Location Object
(PIDF-LO)", M. Thomson J. Winterbottom February 2008, <http://www.ietf.org/rfc/rfc5139.txt>
- [LOCSIP-RD] “Location in SIP/IP core Requirements”, Open Mobile Alliance™, OMA-RD-LOCSIP-V1_0,
URL:<http://www.openmobilealliance.org/>
- [LOCSIP-TS] “Location in SIP/IP core Technical Specification”, Open Mobile Alliance™, OMA-TS-LOCSIP-V1_0,
URL:<http://www.openmobilealliance.org/>
- [IMSARCH] IMS in OMA Architecture Document: Open Mobile Alliance™, OMA-AD-IMS-V1_0,
[URL:http://www.openmobilealliance.org/](http://www.openmobilealliance.org/)
- [OMA GPMAD] "Global Permissions Management Architecture", OMA-AD-GPM-V1_0, Open Mobile Alliance™,
URL:<http://www.openmobilealliance.org/>
- [OMA SEC CF] “Security Common Functions Architecture, V1.0”, OMA-AD-SEC_CF-V1_0, Open Mobile Alliance™,
URL: <http://www.openmobilealliance.org/>
- [OMA XDMAD] “OMA XML Document Management (XDM) Architecture, V2.0”, OMA-AD-XDM-V2_0, Open Mobile
Alliance™,
URL: <http://www.openmobilealliance.org/>
- [PIDF-LO Profile] Internet-Draft, GEOPRIV PIDF-LO Usage Clarification, Considerations and Recommendations, J.
Winterbottom, M. Thomson, H. Tschofenig, <http://www.ietf.org/internet-drafts/draft-ietf-geopriv-pdif-lo-profile-13>
- [URILISTSUB] “Subscriptions to Request-Contained Resource Lists in the Session Initiation Protocol (SIP)”,
G. Camarillo, A. Roach, O. Levin, November 2007,
URL: <http://www.ietf.org/internet-drafts/draft-ietf-sip-uri-list-subscribe-02.txt>

Note: IETF Draft work in progress

- [XDM_Core] “XML Document Management Specification”, Version 2.0, Open Mobile Alliance™, OMA-TS-XDM_Core-V2_0, URL: <http://www.openmobilealliance.org/>
- [XMLENC] “XML Encryption Syntax and Processing”, W3C Recommendation 10 December 2002, URL: <http://www.w3.org/TR/xmlenc-core/>
- [XMSIG] “XML Signature Syntax and Processing”, W3C Recommendation 12 February 2002, URL: <http://www.w3.org/TR/xmldsig-core/>

2.2 Informative References

- [OMADICT] “Dictionary for OMA Specifications”, Version 2.6, Open Mobile Alliance™, OMA-ORG-Dictionary-V2_6, URL: <http://www.openmobilealliance.org/>
- [RFC3261] “SIP: Session Initiation Protocol”, Rosenberg et al., June 2002, URL: <http://www.ietf.org/rfc/rfc3261.txt>

3. Terminology and Conventions

3.1 Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC2119].

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

3.2 Definitions

Location Server	Functional entity that handles location service subscription request and retrieves the location information of the Target.
Location Client	Functional entity that subscribes to a Location Server in order to obtain location information for one or more Targets.
Target	The device or the user associated with a device whose location is requested.
Requesting Location Server	Functional entity that performs back-end subscription on behalf of the Location Client and handles location service subscription request per local policy.

3.3 Abbreviations

GBA	See [OMADICT]
GPM	Global Permission Management
L-RLS	Location Resource List Server
OMA	Open Mobile Alliance
PKI	Public Key Infrastructure
PoC	Push-to-talk over Cellular
QoS	Quality of Service
RLMI	Resource List Meta-Information
SIP	Session Initiation Protocol
URI	Uniform Resource Identifier
XCAP	XML Configuration Access Protocol
XDM	XML Document Management
XDMC	XML Document Management Client
XDMS	XML Document Management Server
XML	Extensible Markup Language

4. Introduction

(Informative)

The Location in SIP/IP core network (LOCSIP) provides a SIP based interface to expose the location information of Targets. The location information may be processed and utilized by other applications or services in the SIP/IP core network to enrich the end user experience. Examples of services that may utilize location information are Presence and PoC.

LOCSIP does not constitute any position determination functionality. It is assumed that positioning determination is performed by another enabler such as OMA SUPL.

The LOCSIP architecture is reusing the OMA XDM [OMA XDMAD] and IMS in OMA Architecture [IMSARCH] enablers. The architecture has significant similarities with the OMA Presence enabler and shares several IETF specifications used in the Presence enabler. The characteristics of location information have created a number of additional requirements on e.g., Location QoS per subscription, complex spatial filter criteria and enhanced integrity. Realizing the additional requirements as an extended Presence enabler has not been seen as possible as it would jeopardize the Presence service due to increased load and complexity. Furthermore a deployment exposing location information would become unnecessarily complex. The selected solution is instead to define a separate enabler reusing parts of framework and concepts from the Presence enabler.

4.1 Version 1.0

No additional phases are planned beyond this architecture.

5. Architectural Model

5.1 Dependencies

LOCSIP depends on:

- OMA XML Document Management (XDM) Architecture [OMA XDMAD]
- IMS in OMA Architecture [IMSARCH]
- Session Initiation Protocol (SIP)-Specific Event Notification [RFC3265]
- A Session Initiation Protocol (SIP) Event Notification Extension for Resource Lists [RFC4662]
- Subscriptions to Request-Contained Resource Lists in the Session Initiation Protocol (SIP) [URILISTSUB]
- IP Multimedia Subsystem (IMS); Stage 2 [3GPP TS 23.228]
- All-IP Core Network Multimedia Domain: IP Multimedia Subsystem - Stage 2 [3GPP2 X.S0013-002-B]
- OMA Global Permission Management (GPM) Architecture [OAM GPMAD]
- Access Security for IP-based Services [3GPP TS 33.203]
- IMS Security Framework [3GPP2 S.R0086-A]
- A Presence-based GEOPRIV Location Object Format [RFC4119]
- XML Encryption Syntax and Processing [XMLENC]
- XML Signature Syntax and Processing [XMLSIG]

5.2 Architectural Diagram

Figure 1 illustrates the OMA LOCSIP architecture.

The GPM element is optional in the LOCSIP 1.0 architecture.

5.3 Functional Components and Interfaces/reference points definition

5.3.1 LOCSIP Functional Entities

5.3.1.1 Location Client

A Location Client is an entity that requests Location Information about one or multiple Targets. For this, a Location Client supports the following:

- Subscribes to Location Information using [**Error! Reference source not found.**], [**Error! Reference source not found.**], [URILISTSUB] and [LOCSIP-TS].

5.3.1.2 Requesting Location Server

The Requesting Location Server is a functional entity that resides in the same domain as the Location Client. The Requesting Location Server is only needed if the Location Client needs to subscribe to a Location Server in a different domain than the Location Client. The Requesting Location Server supports the following:

- Authorizes Location Service subscriptions per local policy.
- Performs back-end subscriptions on behalf of the Location Client.

NOTE: The method how the SUBSCRIBE request is routed to the Requesting Location Server depends on the underlying SIP/IP Core network and is out of scope of this specification.

5.3.1.3 Location Server

The Location Server is the functional entity that accepts and manages location subscriptions of individual Targets applying policies retrieved from the XDMS.

The Location Server supports the following:

- Receives and authorizes subscriptions from a Location Client and L-RLS and distributes Location Information using [**Error! Reference source not found.**] and [LOCSIP-TS];
- Subscribes to changes to documents stored in the XDMS;
- Fetches documents from the XDMS.

The Location Server has two options to communicate with Location Policy XDMS:

- Communicating with GPM for location policy and GPM provides the results,
- Access Location Policy XDMS for obtaining the documents.

5.3.1.4 Location Resource List Server (L-RLS)

The L-RLS is the functional entity that accepts and manages location subscriptions of predefined groups and Request-Contained Resource Lists, which enables a Location Client application to subscribe to the Location Information of multiple Targets using a single subscription transaction. The L-RLS supports the following:

- Receives and authorizes Location Server subscriptions to predefined groups and Request-Contained Resource Lists from a Location Client, and distributes Location Information using [URILISTSUB], [Error! Reference source not found.], [Error! Reference source not found.] and [LOCSIP-TS];
- Performs back-end subscriptions to the Location Server on behalf of the Location Client [Error! Reference source not found.], [Error! Reference source not found.] and [LOCSIP-TS].

5.3.2 External Entities Providing Services to LOCSIP

5.3.2.1 SIP IP/Core

The SIP/IP Core is a network of servers, such as proxies and/or registrars that perform a variety of services in support of LOCSIP (e.g., routing, authentication). The SIP/IP Core includes a number of [RFC3261] compliant SIP proxies and SIP registrars. The SIP/IP Core performs the following functions that are needed to support the LOCSIP Enabler:

- Routes the SIP signalling between the LOCSIP functional entities;
- Provides discovery and address resolution services;
- Supports SIP compression/decompression;
- Performs authentication and authorization of the LOCSIP functional entities;
- Maintains the registration state;
- Provides charging information.

The specific features offered by different types of SIP/IP Core networks will depend on the particulars of those networks. When LOCSIP is realized using IMS or MMD, it will utilize the capabilities of IMS as specified in 3GPP [3GPP TS 23.228] and 3GPP2 [3GPP2 X.S0013-002-B], respectively

Alternatively, other SIP/IP Core networks may be utilized as long as they perform at least the aforementioned functionality.

5.3.2.2 XML Document Management Server (XDMS)

The functionality of the XDMS is described in [OMA XDMAD].

5.3.2.2.1 Shared List XDMS

The Shared List XDMS documents format and usage are specified in [RFC4826] section 3 Resource Lists Document.

5.3.2.2.2 RLS XDMS

The RLS XDMS document format and usage are specified in [RFC4826] section 4 RLS Services Document.

5.3.2.3 Aggregation Proxy

The functionality of the Aggregation Proxy is described in [OMA XDMAD].

5.3.2.4 XML Document Management Client (XDMC)

The XDMC is defined in [OMA XDMAD] and supports the following functions:

- Manages XML documents;
- Subscribes to changes to documents stored in any XDMS.

5.3.2.5 Global Permission Management (GPM)

The GPM is defined in [OMA GPMAD]. It is optional in the LOCSIP architecture. In case it is implemented, it provides the following functions:

- Evaluate and process permissions rules
- Return to the Location Server a decision on the release of location information

Note: the permission rules are stored on a XDMS. How GPM obtains the permissions rules is out of scope of this specification.

5.3.3 Description of the Reference Points

The Reference Points named as LS are in scope of this Architecture.

5.3.3.1 Reference Point LS-1

The LS-1 reference point supports the communication between the Location Client and the SIP/IP Core network. The protocol for the LS-1 reference point is SIP and the traffic is routed to (and from) the Location Server and the Location Resource List Server via the SIP/IP Core.

LS-1 reference point provides the following functions:

- Subscribe to Targets' Location Information and receive notifications;
- Subscribe to Location Information and receive notifications for Resource lists [**Error! Reference source not found.**] and for Request-Contained Resource List, based on [URILISTSUB];
- Include Location Client preferences in subscription requests;
- SIP compression/decompression when the Location Client resides in a terminal.

5.3.3.2 Reference Point LS-2

The LS-2 reference point supports the communication between the SIP/IP Core network and the L-RLS. The protocol for the LS-2 reference point is SIP.

LS-2 reference point is used to route the SIP messages from the SIP/IP Core to and from the appropriate L-RLS in order to:

- Receive a subscription and send aggregated notifications for Resource lists [**Error! Reference source not found.**] and for Request-Contained Resource List, based on [URILISTSUB];
- Subscribe to Location Information and receive notifications for each Target in a List;
- Regulate the aggregated notifications of a List, as requested by Location Clients;
- Propagate the Location Clients' request to regulate the distribution of Location Information in the back-end subscriptions;
- Subscribe to changes to documents stored in the XDMS and receive notifications.

5.3.3.3 Reference Ppoint LS-3

The LS-3 reference point supports the communication between the SIP/IP Core network and the Location Server. The protocol for the LS-3 reference point is SIP.

LS-3 reference point provides the following functions:

- Receive subscriptions to a single Target's Location Information and send notifications pertaining to this Target;
- Subscribe to changes to documents stored in the XDMS and receive notifications.

5.3.3.4 Reference Point LS-4

The LS-4 reference point supports the communication between the Location Server and both the Shared List XDMS and Location Policy XDMS. The protocol for the LS-4 reference point is XCAP [RFC4825].

The LS-4 reference point supports the following function:

- Retrieval of LOCSIP Policy Documents in the XDMS.
- Retrieval of URI list information from the XDMS. URI list information is needed when lists of user identities in policy documents are defined using URI lists.

5.3.3.5 Reference Point LS-5

The LS-5 reference point supports the communication between the Location Resource List Server and both Shared List XDMS and RLS XDMS. The protocol for the LS-5 reference point is XCAP.

The LS-5 reference point supports the following function:

- Retrieval of XML documents in the XDMS.

Group information is retrieved from the XDMS when location has been requested for members of a group addressed with a Service URI. URI list information from the XDMS is retrieved when members in a group documents are defined using URI lists.

5.3.3.6 Reference Point LS-6

The LS-6 reference point supports the communication between a Location Policy XDMS and the SIP/IP Core network. The protocol for this reference point is SIP.

The reference point provides the following functions:

- Subscription to the modification of the location XML documents,
- Notification of the modification of location XML documents.

5.3.3.7 Reference Point LS-7

The LS-7 reference point supports the communication between the Location Policy XDMS and Aggregation Server. The protocol for this reference point is XCAP.

The reference point provides the following functions:

- Location Policy document management (e.g. create, modify, retrieve, delete).

5.3.3.8 Reference point LS-8

The LS-8 reference point supports the communication between the SIP/IP Core network and the Requesting Location Server. The protocol for the LS-8 reference point is SIP.

The LS-8 reference point provides the following functions:

- Receiving subscriptions to Location Information and sending notifications;
- Authorizing and controlling the Location Client's access to the LOCSIP Service;
- Sending back-end subscriptions on behalf of the Location Client and receiving notifications;

5.3.4 Location Information Format

LOCSIP uses the Presence Information Data Format – Location Object (PIDF-LO) as specified in [RFC4119], [RFC5139] and [PIDF-LO Profile] as the base format through which Location Information is represented.

5.3.5 Location Policies

The following sections describe the Location Policies that control the dissemination of the Target Location Information. The Location Policies consist of Subscription Authorization Rules and Location Content Rules.

5.3.5.1 Subscription Authorization Rules

Subscription Authorization Rules determine how incoming subscriptions are handled.

Subscription Authorization Rules determine those Location Clients who are allowed to subscribe to the Location Information of a Target and those who are not allowed. The Subscription Authorization Rules may include lists that can be stored in the XDMS.

The Subscription Authorization Rules support the following actions:

- Accept
- Reject.

5.3.5.2 Location Content Rules

The Location Content Rules determine which Location Information is disseminated to Location Clients that have been accepted by Subscription Authorization Rules.

The document containing the Location Content Rules is stored in the XDMS.

5.3.6 Charging

Appropriate charging mechanisms may need to be provided by the underlying network or other suitable entities in order to support the charging requirements described in [LOCSIP-RD]. One such mechanism is through the OMA Charging Enabler, described in the following section.

Description of how charging is performed is beyond the scope of the present specification.

5.3.6.1 Support of Charging through the OMA Charging Enabler

The OMA Charging Enabler [CHG_AD] coordinates charging data triggers and flow from OMA enablers into an underlying charging infrastructure, supporting online and offline charging. LOCSIP entities that may optionally report Chargeable Events are:

- Location Server
- Requesting Location Server
- Location Resource List Server

The above entities act as Charging Enabler Users as defined in [CHG_AD]. In addition, the XDMS and the Aggregation Proxy may act as Charging Enabler Users as described in [OMA XDMAD].

Figure 2 shows the reference points between the Charging Enabler and the Location Server, the Requesting Location Server, and the Location Resource List Server entities. These reference points are currently supported by the Charging Enabler, CH-1 for offline charging and CH-2 for online charging. These are described in [CHG_AD].

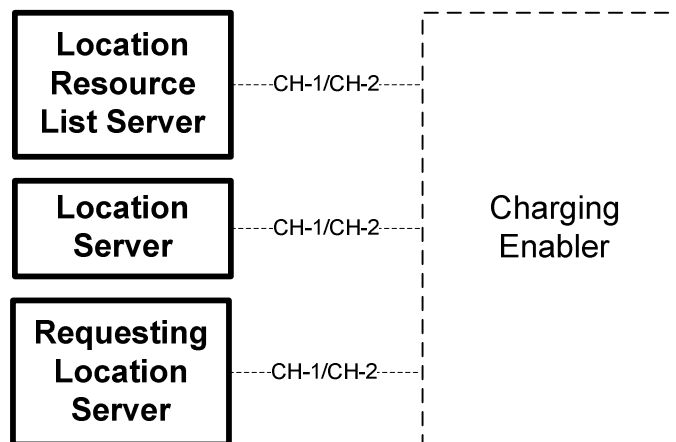


Figure 2: Support of Charging Through the OMA Charging Enabler

Elements shown in bold are defined in this architecture document. The remaining elements are external to this specification.

5.3.7 Registration

When the SIP/IP Core corresponds with 3GPP IMS or 3GPP2 MMD networks, a UE that contains a Location Client functionality uses the registration mechanisms as specified in [3GPP TS 23.228]/[3GPP2 X.S0013-002-B].

5.4 Flows

The flows in the following subchapters describe the logical flows that involve LOCSIP architectural functional entities but do not necessarily fully conform to all the details of protocols that will be used.

The procedure of XDM handling is not described in the high level procedure but can be assumed to take place depending on implementation either prior to or during the flow.

The Location Policy stored in the XDMS is needed when location authorization is performed.

The information stored in the XDMS is needed when:

- Retrieving the location for a group of users
- Performing access control and policy control in location data.

5.4.1 Subscribing to Location Notification

5.4.1.1 Subscribing to Location Notification of a Single Target

The Figure 3 shows the flow when a LOCSIP Location Client subscribes to the location information of the Target.

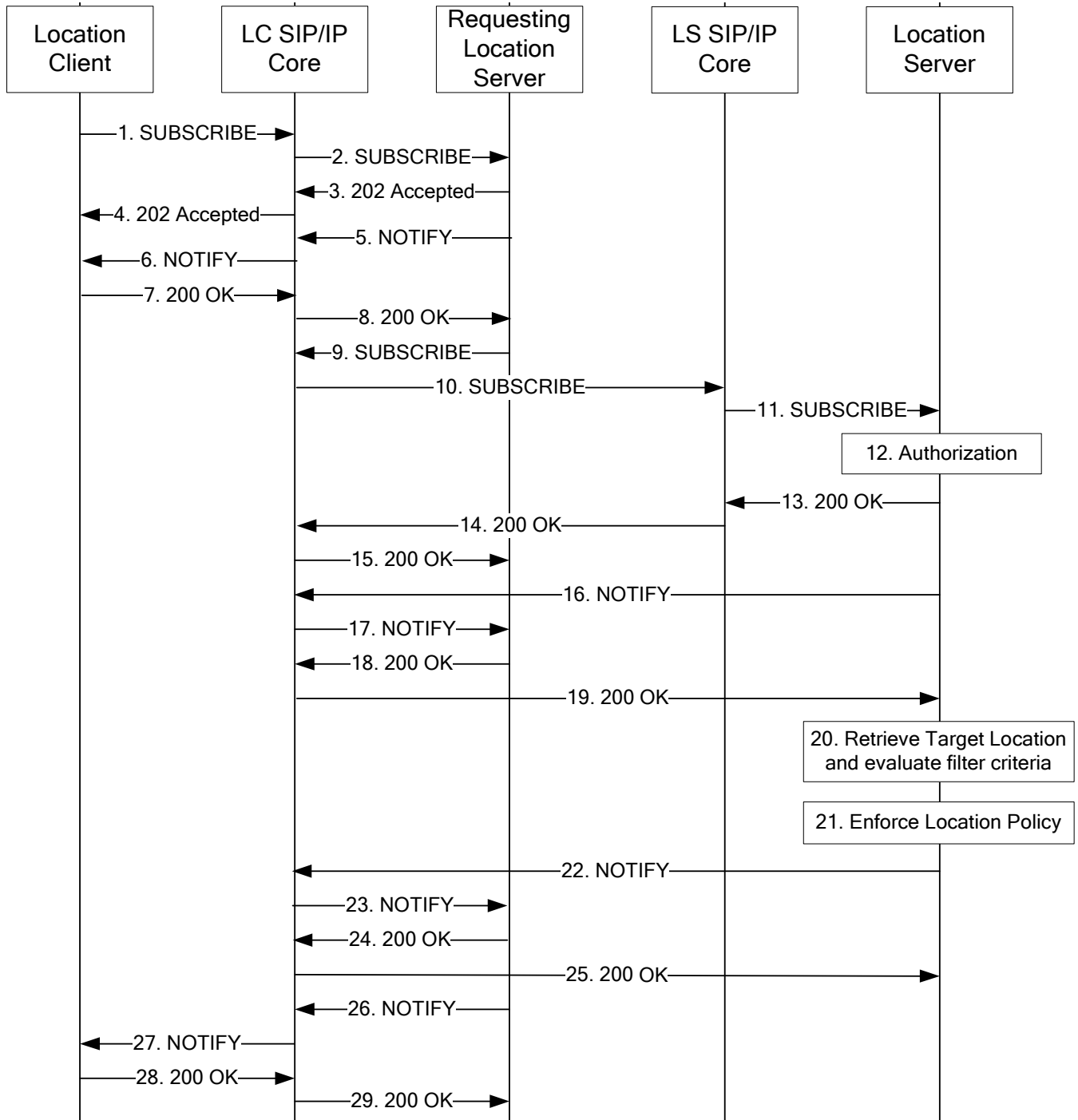


Figure 3: Subscribing to Location Notification of Single Target

1. A Location Client that wants to retrieve the location information of a Target, sends a SIP SUBSCRIBE request which contains the SIP URI of the Target, the duration of the subscription and the feature tag for location service. The duration of the subscription should be set to zero if it's a one-time request instead of persistent subscription. The SIP SUBSCRIBE request may include the required QoS parameters and filter criteria for when notifications are to be sent.
 2. The SIP/IP Core of the Location Client routes the request to the Requesting Location Server.
 3. The Requesting Location Server performs the necessary authorisation checks per local policy. Once authorisation checks are passed the Requesting Location Server issues a SIP 202 Accepted to the SIP/IP Core network.
 4. The SIP/IP Core network forwards the response to the Location Client.
- Steps 5 to 8 are optional and do not have to be performed if step 26 can be performed directly after step 3.
5. The Requesting Location Server sends a SIP NOTIFY with an empty or neutral body to the SIP/IP Core network.
 6. The SIP/IP Core network of the Location Client forwards the SIP NOTIFY request to the Location Client.
 7. The Location Client acknowledges the receipt of the SIP NOTIFY request with a SIP 200 OK response.
 8. The SIP/IP Core network of the Location Client forwards the SIP 200 OK response to the Requesting Location Server.
 9. The Requesting Location Server sends a SIP SUBSCRIBE request on behalf of the Location Client.
 10. The SIP/IP Core network of the Location Client resolves the address of the Target and routes the request to the SIP/IP Core network of the Location Server.
 11. The SIP/IP Core network routes the SIP SUBSCRIBE request to the correct Location Server, based on the address of the Target and the feature tag for location service.
 12. The Location Server performs the necessary authorisation checks on the originator to ensure it is allowed to request the location information of the Target.
 13. Once authorisation checks are fully passed, the Location Server issues a SIP 200 OK to the SIP/IP Core network. If the authorization is pending a Target user interaction, the Location Server returns a SIP 202 Accepted response, which means the request has been accepted and understood, but does not necessarily imply that the subscription has been authorized yet.
 14. The SIP/IP Core network of the Location Server forwards the response to the SIP/IP Core network of the Location Client.
 15. The SIP/IP Core network forwards the response to the Requesting Location Server.
- Steps 16 to 19 are optional and do not have to be performed if step 22 can be performed directly after step 13.
16. As soon as the Location Server sends a SIP 200 OK or a SIP 202 (Accepted) response to accept the subscription, it sends a SIP NOTIFY request as mandated by [RFC3265]. If the Location Information is not available or if the request is not yet authorized, it sends a SIP NOTIFY request with an empty or neutral body.
 17. The SIP/IP Core network of the Location Client forwards the SIP NOTIFY request to the Requesting Location Server.
 18. The Requesting Location Server acknowledges the receipt of the SIP NOTIFY request with a SIP 200 OK response.

19. The SIP/IP Core network forwards the SIP 200 OK response to Location Server.
20. The Location Server retrieves needed location information. The Location Server then determines that a notification is to be sent. The determination is based on the filter criteria, requested QoS and available location information.
21. The Location Server enforces the policy control function. It may perform the appropriate actions and/or transformations before delivering the location information to the Location Client.
22. The Location Server sends a SIP NOTIFY request along the path of the SIP SUBSCRIBE dialog to the SIP/IP Core network of the Location Client. The SIP NOTIFY request contains location estimate, a feature tag for location service, and possibly an indication of subscription termination if it is the last notification. The SIP NOTIFY request may also contain the QoS information and/or some location policies applicable to the Location Client.

NOTE: If the positioning attempt fails or is rejected due to privacy control, the SIP NOTIFY request includes proper failure reason and the indication of subscription termination.

23. The SIP/IP Core network of the Location Client forwards the SIP NOTIFY request to the Requesting Location Server.
24. The Requesting Location Server acknowledges the receipt of the SIP NOTIFY request with a SIP 200 OK response.
25. The SIP/IP Core network of the Location Client forwards the SIP 200 OK response to the Location Server.
26. The Requesting Location Server sends a SIP NOTIFY to the SIP/IP Core network.
27. The SIP/IP Core network of the Location Client forwards the SIP NOTIFY request to the Location Client.
28. The Location Client acknowledges the receipt of the SIP NOTIFY request with a SIP 200 OK response.
29. The SIP/IP Core network of the Location Client forwards the SIP 200 OK response to the Requesting Location Server.

NOTE: Steps 22 to 29 may be repeated during the subscription period whenever the location filter condition is fulfilled.

NOTE: When the Location Client and the Location Server are in the same domain, the Requesting Location Server is not needed. For the remaining flows illustrated in this document, the Location Client and Location Server are assumed to be associated with the same SIP/IP Core network. Thus, only a single SIP/IP Core network, without a Requesting Location Server, is shown in the remaining figures.

5.4.1.2 Subscribing to the Notification of Periodic Trigger

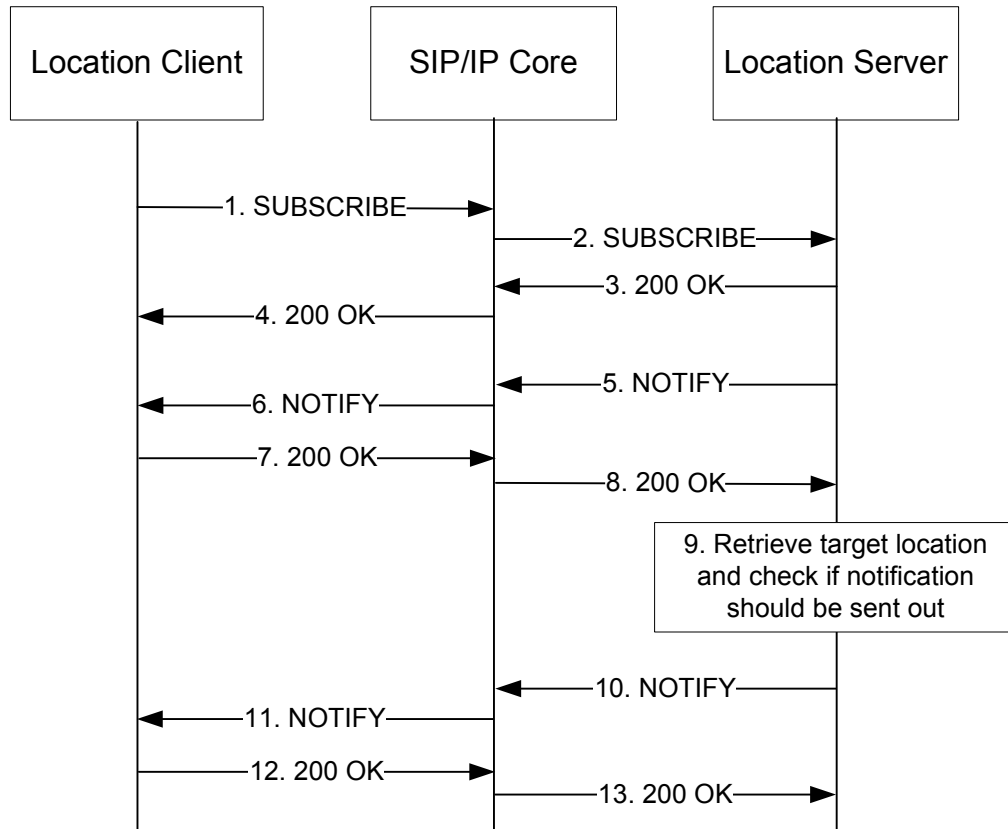


Figure 4: Flow for Subscribing to the Notification of Periodic Trigger

1. A Location Client sends a SIP SUBSCRIBE request to the Location Server requesting the location of the Target to be delivered periodically. This is done by including a filter in the body of the SIP SUBSCRIBE request. The filter indicates the setting of periodic trigger, such as start time, report mode, position interval or the number of fixes.
2. The SIP/IP Core network forwards the SIP SUBSCRIBE request to the Location Server.
3. The Location Server authorizes the subscription and interprets the subscription filter. If the authorization succeeds, the Location Server sends a SIP 200 OK response to the SIP/IP Core network indicating that the subscription has been accepted and the filter is understood.

4. The SIP/IP Core network forwards the SIP 200 OK response to the Location Client.

Steps 5 to 8 are optional and do not have to be performed if step 10 can be performed directly after step 3.

5. The Location Server sends a SIP NOTIFY request with an empty or neutral body to the SIP/IP Core network.
6. The SIP/IP Core network forwards the SIP NOTIFY request to the Location Client.
7. The Location Client acknowledges the SIP NOTIFY request with a SIP 200 OK response.
8. The SIP/IP Core network forwards the SIP 200 OK response to the Location Server.

9. When the time specified by the periodic trigger is reached, the Location Server retrieves, if not already available, the location information of the Target and determines if a notification is to be sent out based on the subscription filter.
10. The Location Server enforces the location policy and generates a SIP NOTIFY request including the location result. The Location Server sends a SIP NOTIFY request along the path of the SIP SUBSCRIBE dialog to the SIP/IP Core network of the Location Client.
11. The SIP/IP Core network forwards the SIP NOTIFY request to the Location Client.
12. The Location Client acknowledges the SIP NOTIFY request with a SIP 200 OK response.
13. The SIP/IP Core network forwards the SIP 200 OK response to the Location Server.

NOTE: Steps 9 to 13 will be repeated during subscription period in order to get location of the Target periodically.

5.4.1.3 Subscribing to the Notification of Area Event Trigger

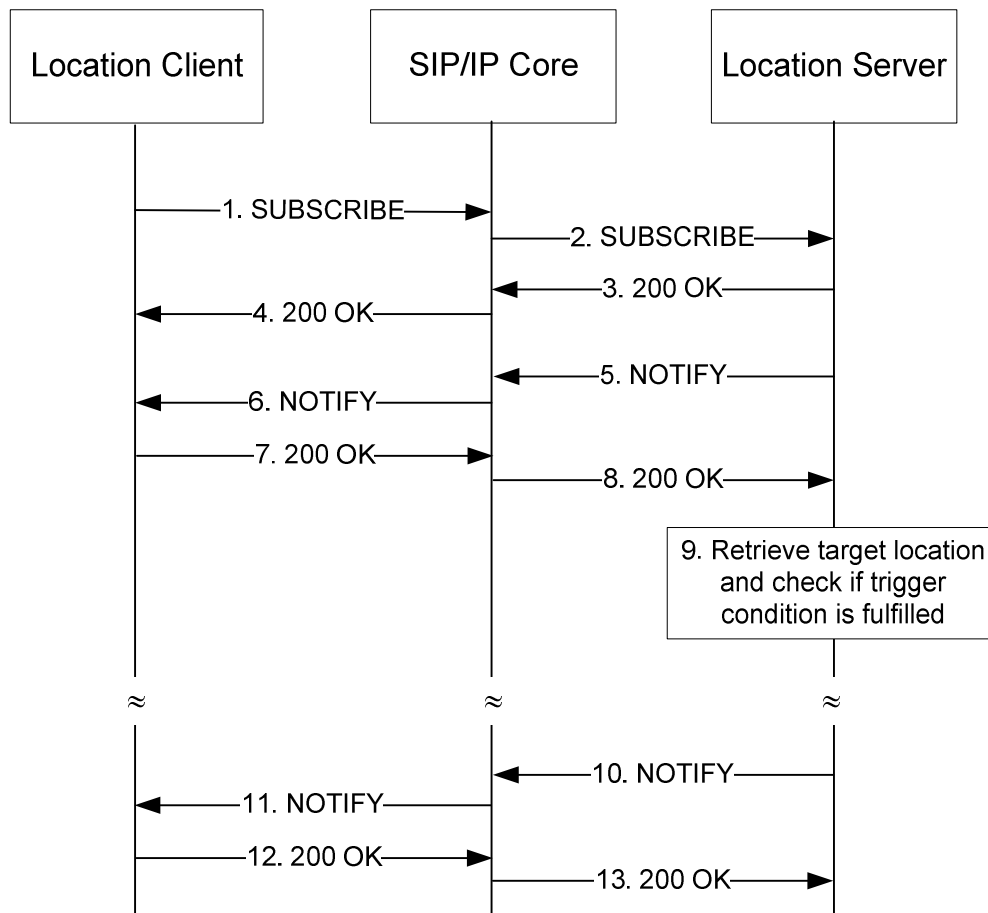


Figure 5: Flow for Subscribing to the Notification of Area Event Trigger

1. The Location Client sends a SIP SUBSCRIBE request to the Location Server in order to start an area event trigger session. This is done by including a filter in the body of the SIP SUBSCRIBE request. The filter indicates the condition for area event trigger. The following types of trigger conditions may be supported:
 - Target enters or exits certain geographical area
 - Target is inside or outside certain geographical area
 - Target has moved a specific distance
 - change of civic address
 2. The SIP/IP Core network forwards the SIP SUBSCRIBE request to the Location Server.
 3. The Location Server authorizes the subscription and interprets the subscription filter. It sends a SIP 200 OK response to the SIP/IP Core network indicating that the subscription has been accepted and the subscription filter is understood.
 4. The SIP/IP Core network forwards the SIP 200 OK response to the Location Client.
- Steps 5 to 8 are optional and do not have to be performed if step 10 can be performed directly after step 3.
5. The Location Server sends a SIP NOTIFY request with an empty or neutral body to the SIP/IP Core network.
 6. The SIP/IP Core network forwards the SIP NOTIFY request to the Location Client.
 7. The Location Client acknowledges the SIP NOTIFY request with a SIP 200 OK response.
 8. The SIP/IP Core network forwards the SIP 200 OK response to the Location Server.
 9. The Location Server monitors the location of the Target and check if the trigger condition is fulfilled. In this case, a notification is triggered.
 10. The Location Server sends a SIP NOTIFY request along the path of the SUBSCRIBE dialog to the SIP/IP Core network of the Location Client. The SIP NOTIFY request may contain the location estimate and a timestamp. If it is the last notification, the SIP NOTIFY request should also contain an indication of subscription termination.
 11. The SIP/IP Core network forwards the SIP NOTIFY request to the Location Client.
 12. The Location Client acknowledges the SIP NOTIFY request with a SIP 200 OK response.
 13. The SIP/IP Core network forwards the SIP 200 OK response to the Location Server.

NOTE 1: Steps 10 to 13 are optional depending on if the trigger condition is met. If the trigger condition has never been met and the stop time is reached, a SIP NOTIFY request will be sent back to the Location Client indicating the subscription is terminated. Please refer to the flow “Expiry of a Subscription”

NOTE 2: Steps 9 to 13 will be repeated during the subscription period if the filter condition indicates repeated reporting is needed.

5.4.1.4 Expiry of a Subscription

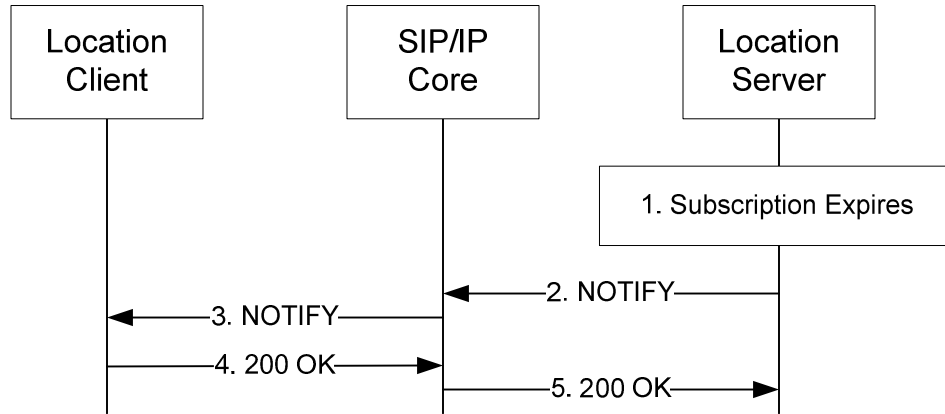


Figure 6: Flow for Subscription Expiry Notification

1. The lifetime of a subscription expires and there is no refreshing transaction to update the subscription.
2. The Location Server issues a SIP NOTIFY request indicating the subscription has expired.
3. The SIP/IP Core network forwards the SIP NOTIFY request to the Location Client.
4. The Location Client sends a SIP 200 OK response to the SIP/IP Core network to acknowledge the SIP NOTIFY request.
5. The SIP/IP Core network forwards the SIP 200 OK response to the Location Server.

5.4.1.5 Subscription Authorization Failure

A (Requesting) Location Server can deny a subscription request from a Location Client if the Service Provider has blocked the Location Client from subscribing to Target’s location. In this case, the (Requesting) Location Server sends a 403 Forbidden message in response to a subscription request.

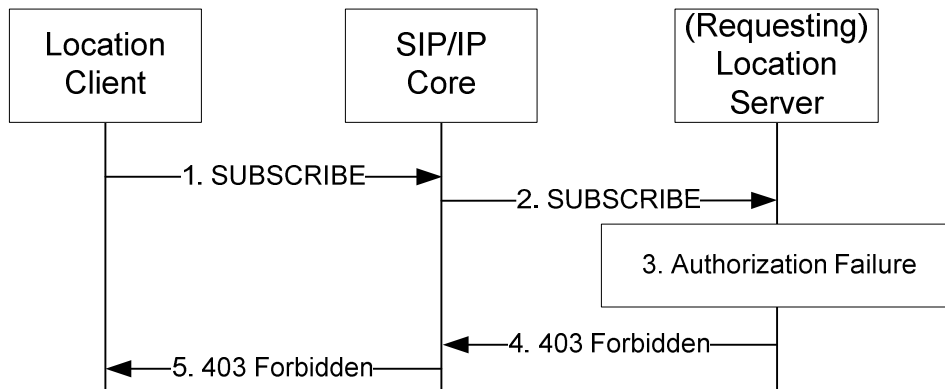


Figure 7: Flow for Subscription Authorization Failure

1. A Location Client that wants to retrieve the location information of a Target sends a SIP SUBSCRIBE request which contains the SIP URI of the Target, the duration of the subscription and the feature tag for location service.

The duration of the subscription should be set to zero if it's a one-time request instead of persistent subscription. The SIP SUBSCRIBE request may include the required QoS parameters and filter criteria for when notifications shall be sent.

2. The SIP/IP Core routes the SIP SUBSCRIBE request to the correct (Requesting) Location Server, based on the address of the Target and the feature tag for location service.
3. The (Requesting) Location Server performs the necessary authorisation checks on the originator to ensure it is allowed to request the location information of Target. In this scenario, the Service Provider has blocked the Location Client from receiving the Target's location information and therefore, the authorization fails.
4. The (Requesting) Location Server sends a SIP 403 Forbidden response to the SIP/IP Core.
5. The SIP/IP Core forwards the response to the Location Client.

5.4.2 Subscribing to Location for a List of Targets

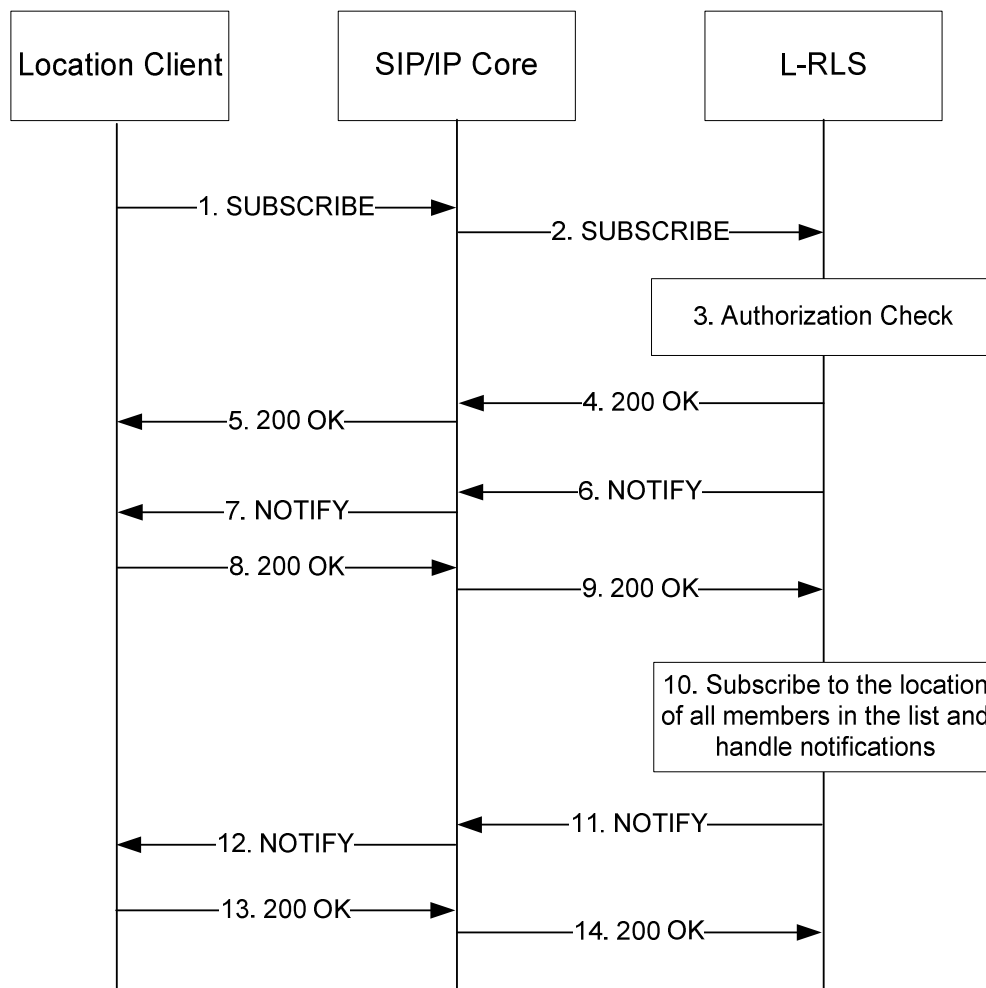


Figure 8: Flow for Subscribing to Location for a List of Targets

1. A Location Client that wants to retrieve the location information of a list of Targets, sends a SIP SUBSCRIBE request containing the Target list, an indication of “eventlist” support and the duration of subscription, according to [RFC3265][RFC4662]. The SIP SUBSCRIBE request may include the required QoS and filter criteria when the notifications are to be sent.
The Target list can be either a pre-defined resource list or a Request-Contained Resource List. The pre-defined resource list refers to existing shared group/list and is identified by the request URI. The Request-Contained Resource List includes a URI-list in the SIP SUBSCRIBE request according to [URILISTSUB].
2. The SIP/IP Core network forwards the request to the correct L-RLS based on the address of Target list and resource list service indication.
3. The L-RLS performs the necessary authorisation checks on the originator to ensure it is allowed to use the resource list.
4. Once authorisation checks are successful, the L-RLS issues a SIP 200 OK to the SIP/IP Core.
5. The SIP/IP Core network forwards the response to the Location Client.
6. The L-RLS generates a SIP NOTIFY request including the RLMI document as a result of the SIP SUBSCRIBE request. The RLMI document describes all the members in the list, as well as the location information for the Targets about which it already knows.
7. The SIP/IP core forwards the SIP NOTIFY request to the Location Client.
8. The Location Client acknowledges the SIP NOTIFY request with a SIP 200 OK response.
9. The SIP/IP Core forwards the SIP 200 OK response to L-RLS.
10. The L-RLS resolves the resource list and generates the necessary SIP SUBSCRIBE requests to the Location Server for each individual Target.

Note: For Resource List, the L-RLS fetches the resource list documents from the XDMS using XCAP, as defined in [XDM_Core]. For Request-Contained Resource List, the L-RLS extracts the URIs in the URI-list directly from the body part of initial SIP SUBSCRIBE request.

11. When the notification condition is fulfilled, the L-RLS generates a SIP NOTIFY request with multipart format. The L-RLS includes the RLMI document, copies/aggregates the body of the received SIP NOTIFY request(s) into the body of the outgoing SIP NOTIFY request and sends it to the Location Client.
12. The SIP/IP Core network forwards the SIP NOTIFY request to the Location Client.
13. The Location Client acknowledges the receipt of the SIP NOTIFY request with a SIP 200 OK response.
14. The SIP/IP Core forwards the SIP 200 OK response to L-RLS.

NOTE: Steps 11 to 14 will be repeated within subscription period whenever the filter condition is fulfilled, for instance when any Target in the list enters the defined trigger area.

5.4.3 Canceling/Refreshing a Location Subscription

5.4.3.1 Location Client Initiated Canceling/Refreshing

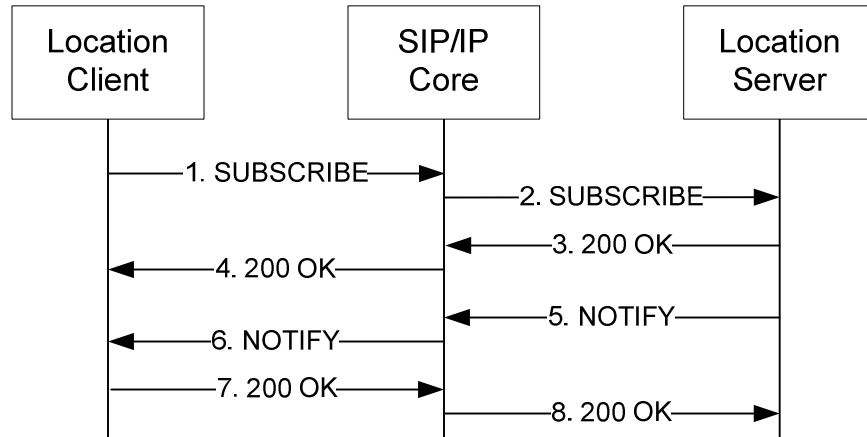


Figure 9: Flow for Location Client Initiated Subscription Cancellation/Refreshing

1. A Location Client sends a SIP SUBSCRIBE request on the same dialog as the existing subscription, with an “Expires” header field indicating the new duration of the subscription, according to [RFC3265]. To refresh the subscription, the “Expires” header field should be set to the new expiration time. To terminate the subscription, the “Expires” header field should be set to 0.
2. The SIP/IP Core routes the SIP SUBSCRIBE request to the correct Location Server, based on the address of the Target and the feature tag for location service.
3. The Location Server accepts the SIP SUBSCRIBE request and updates the duration of subscription to the new expiration time specified by the “Expires” header. If the “Expires” header is set to 0, the subscription will be terminated, indicating the canceling a subscription operation. After that, the Location Server sends a SIP 200 OK response to the SIP/IP Core.
4. The SIP/IP Core forwards the response to the Location Client.
5. Location Server sends a SIP NOTIFY request to the SIP/IP Core network according to [RFC3265]. For refreshing subscription, the SIP NOTIFY request contains a "Subscription-State" header with value "active" together with an "Expires" header indicating the time remaining on the subscription. For cancelling subscription, the SIP NOTIFY request contains a “Subscription-State” header field with value “terminated”.
6. The SIP/IP Core of the Location Client forwards the SIP NOTIFY request to the Location Client.
7. The Location Client acknowledges the receipt of the SIP NOTIFY request with a SIP 200 OK response.
8. The SIP/IP Core forwards the SIP 200 OK response to the Location Server.

5.4.3.2 Location Server Initiated Canceling/Refreshing

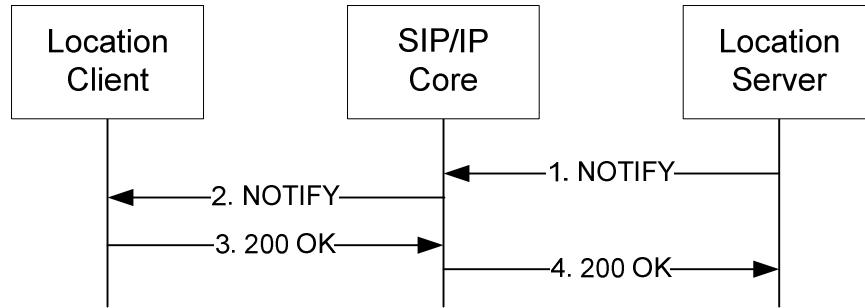


Figure 10: Flow for Location Server Initiated Subscription Cancellation/Refreshing

1. The Location Server sends a SIP NOTIFY request with a “Subscription-State” header field to inform the new state of location subscription according to [RFC 3265]. If the subscription is cancelled, the “Subscription-State” is set to “terminated”. If the subscription is refreshed, the “Subscription-State” header field is set to “active” and the new expiration time is included in the SIP NOTIFY request.
2. The SIP/IP Core network forwards the SIP NOTIFY request to the Location Client.
3. The Location Client sends a SIP 200 OK response to the SIP/IP Core network to acknowledge the SIP NOTIFY request.
4. The SIP/IP Core network forwards the SIP 200 OK to the Location Server.

5.4.4 Subscribing to Changes of XDMS

5.4.4.1 Location Server Subscribing to Changes in Location Policy Data

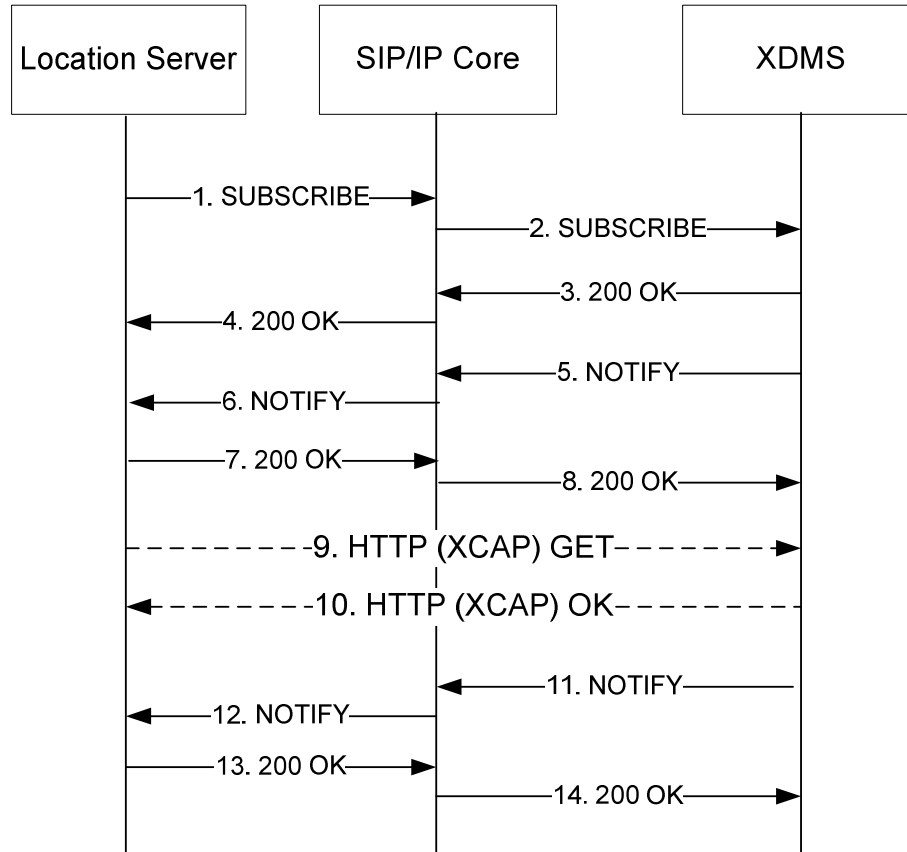


Figure 11: Subscribing to Changes in Location Policy Data

1. A Location Server that wishes to subscribe to the changes made to the Location Authorization/Policy Rules document, sends a SIP SUBSCRIBE request with the “Event” header field set to “xcap-diff” as described in [XDM_Core]. The Request-URI of the SIP SUBSCRIBE request is set to the public user identity of the Target whose documents the Location Server wishes to subscribe to.
2. The SIP/IP Core forwards the request to the appropriate XDMS.
3. The XDMS accepts the subscription and responds with a SIP 200 OK.
4. The SIP/IP Core forwards the response to the Location Server.
5. The XDMS sends the first SIP NOTIFY request, which is used in order to synchronize the XDMS and Location Server on a common “baseline” document as described in [IETF-XCAP_Diff].
6. The SIP/IP Core forwards the SIP NOTIFY request to the Location Server.
7. The Location Server accepts the SIP NOTIFY request with a SIP 200 OK response.
8. The SIP/IP Core forwards the SIP 200 OK response to the XDMS.
9. The Location Server fetches using HTTP (XCAP) GET request the version of the document indicated (with the Etag) in the received SIP NOTIFY request, as defined in [IETF-XCAP_diff] and [XDM_Core].
10. The version of the document requested is provided by the XDMS.

11. When changes occur in the Location Authorization/Policy Rules document, the XDMS informs the Location Server about the changes through a SIP NOTIFY request with the changed data.
12. The SIP/IP Core forwards the SIP NOTIFY request to the Location Server.
13. The Location Server responds to the SIP NOTIFY request with a 200 OK response.
14. The SIP/IP Core forwards the 200 OK response to the XDMS.

5.4.4.2 L-RLS Subscribing to Changes in Group/List

The L-RLS SHALL support subscriptions to changes in the group/list documents stored in XDMS as specified in [XDM_Core] “Subscriptions to Changes in the XML Documents”.

5.4.5 Authorization using GPM

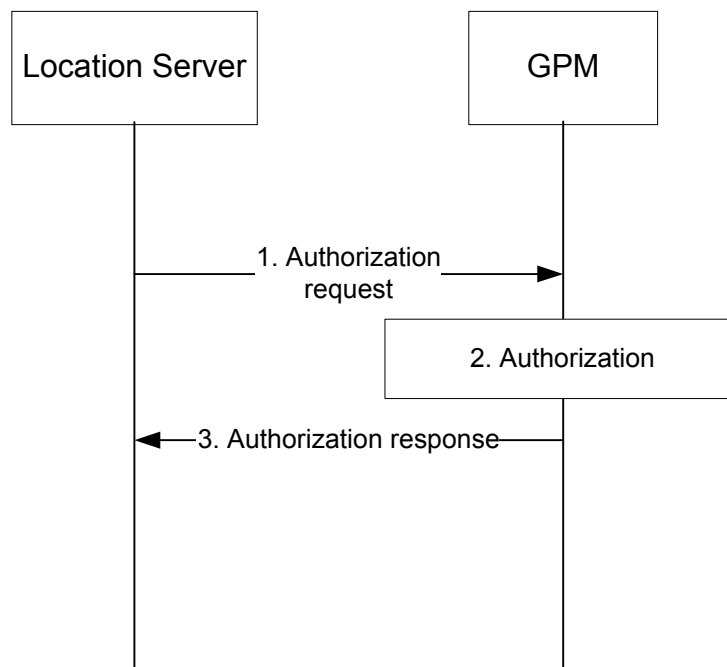


Figure 12: Flow for permissions checking with GPM

1. The Location Server sends an authorization request to the GPM. This request may include parameters such as the identity of the requester, the required QoS, the location of the Target, etc
2. The GPM performs the authorization checks by internal means that are out of scope of this document.
3. The GPM returns an authorization response to the Location Server. The response may contain indications pertaining to what kind of location information the Location Server is allowed to return to the Location Client.

Note: the authorization request should be performed every time the Location Server delivers location information.

5.5 Security Considerations

This section describes the mechanisms required for the secure operation of LOCSIP.

Security mechanisms provide protection to the LOCSIP service environment. The following aspects of security are considered: SIP signalling security, location information security and XDM security.

For SIP signalling security in general, LOCSIP rely on the security mechanisms provided by the SIP/IP Core network. However, location information is particularly sensitive from a privacy perspective and the Location Server cannot always trust that the SIP/IP Core network provides adequate confidentiality and integrity protection of the location information. A mechanism for protection of the location information from Location Server to Location Client is thus defined.

The XDM security is specified in [OMA XDMAD].

The LOCSIP security function is described in Section **Error! Reference source not found.**

5.5.1 SIP Signaling Security

The Location Client SHALL be authenticated prior to accessing the Location Server. The Location Server MAY rely on the security mechanisms provided by the underlying SIP/IP Core, for securing the service environments.

When the SIP/IP Core corresponds with 3GPP/3GPP2 IMS, and the Location Client contains USIM/ISIM or UIM/R-UIM, the mutual authentication SHALL be applied as specified in [3GPP TS 33.203]/[3GPP2 S.R0086-A]. For further SIP signalling, the integrity protection mechanism SHALL be used as specified in [3GPP TS 33.203]/[3GPP2 S.R0086-A].

5.5.2 User Plane Security

There are two aspects to be considered: User Authentication and Location Information protection.

In order to protect User Plane communication Location Client and Location Server SHOULD be mutually authenticated, subject to service provider policies.

The baseline for integrity and confidentiality protection is described in [OMA SEC CF] but it needs to be extended to provide a SIP-binding - instead of the existing HTTP – since the LOCSIP server exposes only a SIP interface.

For Location Information the SIP/IP Core network security is not always sufficient. The Location Server SHOULD thus apply XML encryption as specified in [XMLENC] to ensure confidentiality protection of the location information and XML signature as specified in [XMLSIG] to ensure integrity protection of the location information.

The key management is defined in [LOCSIP-TS]. .

5.5.3 XDM Security

The XDM security is specified in [OMA XDMAD] "*Security Considerations*".

Appendix A. Change History

(Informative)

A.1 Approved Version History

Reference	Date	Description
n/a	n/a	No prior version

A.2 Draft/Candidate Version 1.0 History

Document Identifier	Date	Sections	Description
Draft Versions OMA-AD-LOCSIP-V1_0	02 Dec 2007	All	Initial Draft
	21 Mar 2008	2, 3, 5, (All)	Incorporated the following approved CR: LOC-2008-052-CR_LOCSIP_1_0_AD_ArchModel
	28 Apr 2008	n/a	Incorporated the following approved CR: LOC-2008-0215R01-CR_LOCSIP_1_0_AD_Archmod_Corr LOC-2008-0216R01-CR_LOCSIP_1_0_AD_Initial_Flow LOC-2008-0217-CR_LOCSIP_1_0_AD_Dependencies LOC-2008-0218-CR_LOCSIP_1_0_AD_Phases
	12 May 2008	1, 2, 4, 5	Incorporated the following approved CR: LOC-2008-0280-CR_LOCSIP_1_0_AD_Scope LOC-2008-0281R01-CR_LOCSIP_1_0_AD_ArchDiag_Corr LOC-2008-0282-CR_LOCSIP_1_0_AD_Security LOC-2008-0283-INP_LOCSIP_1_0_AD_Informal_Review LOC-2008-0284- CR_LOCSIP_1_0_AD_Functional_Components_and_Interfaces LOC-2008-0285- CR_LOCSIP_1_0_AD_Subscribing_to_Location_Notification LOC-2008-0286- CR_LOCSIP_1_0_AD_Cancelling_a_Subscription_Notification
	22 May 2008	5	Incorporated the editor note from meeting report: LOC-2008-290R01-MINUTES_07May2008_CC.doc Incorporated CR: LOC-2008-0282-CR_LOCSIP_1_0_AD_Security Change section 3 withdrawn
	07 Jul 2008	2, 3.2, 3.3, 4, 5.2, 5.3.2, 5.3.3.5, 5.4.1, 5.4.2, 5.5.1, 5.5.3, 5.5.4	Incorporated the following approved CR: LOC-2008-0340R01-CR_LOCSIP_1_0_AD_Improve_Intro OMA-LOC-2008-0341-CR_LOCSIP_1_0_AD_Clarify_SIP_IP_Core OMA-LOC-2008-0342R01-CR_LOCSIP_1_0_AD_XML_Security OMA-LOC-2008-0343R01- CR_LOCSIP_1_0_AD_Modify_SingleTarget OMA-LOC-2008-0344-CR_LOCSIP_1_0_AD_Refresh_Subscription OMA-LOC-2008-0345R02- CR_LOCSIP_1_0_AD_Subscription_Group OMA-LOC-2008-0346R02-CR_LOCSIP_1_0_AD_Flows_XDM OMA-LOC-2008-0350- CR_LOCSIP_1.0_AD_Flows_Single_SIP_IP_Core OMA-LOC-2008-0351-CR_LOCSIP_1_0_AD_GeneralCleanup OMA-LOC-2008-0365R01-CR_LOCSIP_1_0_AD_Trigger OMA-LOC-2008-0372R01-CR_LOCSIP_1_0_AD_GPM_addition OMA-LOC-2008-0373-CR_LOCSIP_1_0_XDMS

Document Identifier	Date	Sections	Description
	01 Sep 2008	5.3.1.1, 5.3.1.2	OMA-LOC-2008-0391R01- CR_LOCSIP_1_0_AD_ADRR_005_006_007 OMA-LOC-2008-0392- CR_LOCSIP_1_0_AD_ADRR_10_12_16_Policy OMA-LOC-2008-0393- CR_LOCSIP_1_0_AD_ADRR_51_52_DummyNotify
	03 Oct 2008	2, 5.1, 5.2, 5.3.1.2, 5.3.2.2, 5.3.3.4, 5.3.3.6, 5.3.3.7, 5.3.3.8, 5.3.4, 5.3.5.2, 5.3.6.1, 5.4.1.1, 5.4.1.2, 5.4.1.3, 5.4.2, 5.4.4.1, 5.5.1.1	OMA-LOC-2008-0415-CR_LOCSIP_1_0_AD_ADRR_11_URI_List OMA-LOC-2008-0417- CR_LOCSIP_1_0_AD_ADRR_042_Dependencies OMA-LOC-2008-0377R02- CR_LOCSIP_AD_Arch_Figure_A43_A45_A46_A47_A56 OMA-LOC-2008-0379R01-CR_LOCSIP_1_0_AD_A002_A013 OMA-LOC-2008-0418R01-CR_LOCSIP_1_0_AD_UserPlane_Security OMA-LOC-2008-0422R04- CR_LOCSIP_1_0_AD_ADRR_027_054_Requesting_LS OMA-LOC-2008-0425- CR_LOCSIP_1_0_AD_ADRR_057_Dummy_SIP_NOTIFY OMA-LOC-2008-0426- CR_LOCSIP_1_0_AD_ADRR_013_014_Charging OMA-LOC-2008-0431-CR_LOCSIP_AD_PIDF_LO_Reference
	03 Nov 2008	5.3.6.1, 3.2, 5.4.1.5	OMA-LOC-2008-0470-CR_LOCSIP_1_0_AD_Charging OMA-LOC-2008-0471-CR_LOCSIP_1.0_AD_3.2_Definition OMA-LOC-2008-0472R01- CR_LOCSIP_1.0_AD_5.4.1.5_Subscription_Authorization_Failure
Draft Version OMA-AD-LOCSIP-V1_0	23 Dec 2008	N/A	Status changed to Candidate by TP TP ref#: OMA-TP-2008-0484- INP_LOCSIP_AD_Package_for_Candidate_Approval