Location in SIP/IP core Architecture

Approved Version 1.0 – 17 Jan 2012

Open Mobile Alliance

OMA-AD-LOCSIP-V1_0-20120117-A

Contents

Figures

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_23.002] "Network architecture", 3GPP TS 23.002,
URL: http://www.3gpp.org/ftp/Specs/archive/23_series/23.002/

[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
URL: http://www.3gpp.org/ftp/specs/html-info/33203.htm

[3GPP2 S.R0086-A] "IMS Security Framework", Revision A, Version 1.0
URL: 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

[IMSARCH] IMS in OMA

[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/

[OMA-CHG_AD] "Charging Architecture", Version 1.0, OMA-AD-Charging-V1_0, Open Mobile Alliance™,
URL: http://www.openmobilealliance.org/

[OMA-GSSM_AD] "General Service Subscription Management Architecture", Version 1.0, OMA-AD-GSSM-V1_0, Open Mobile Alliance™,
URL: http://www.openmobilealliance.org/

[OMA-GPM_AD] "Global Permissions Management Architecture", OMA-AD-GPM-V1_0, Open Mobile Alliance™,
URL:http://www.openmobilealliance.org/

[OMA-PRS_AD] "OMA Presence SIMPLE Architecture", OMA-AD-Presence-SIMPLE-V2_0,
URL:http://www.openmobilealliance.org/

[OMA-PRS_HSA] "Home Subscription Agent (HSA) Specification", OMA-TS-Presence_SIMPLE_HSA-V1_0, Open Mobile Alliance™, URL:http://www.openmobilealliance.org/

[OMA-PRS_RLS] "Resource List Server Specification", OMA-TS-Presence-SIMPLE-RLS-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/

[RFC2119] RFC 2119, "Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, March 1997,
URL:http://www.ietf.org/rfc/rfc2119.txt

[RFC3261] RFC 3261, "SIP: Session Initiation Protocol", Rosenberg et al., June 2002,
URL: http://www.ietf.org/rfc/rfc3261.txt

[RFC3265] RFC 3265, "Session Initiation Protocol (SIP)-Specific Event Notification", A.B. Roach, June 2002, RFC 3265,
URL: http://www.ietf.org/rfc/rfc3265.txt

[RFC4119] RFC 4119, "A Presence-based GEOPRIV Location Object Format", SJ. Peterson, December 2005,
URL:http://www.ietf.org/rfc/rfc4119.txt

[RFC4662] RFC 4662, "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,
URL: http://www.ietf.org/rfc/rfc4825.txt

[RFC4826] RFC 4826, "Extensible Markup Language (XML) Formats for Representing Resource Lists", J. Rosenberg, May 2007,
URL: 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,
URL: http://www.ietf.org/rfc/rfc5139.txt

[RFC5367] "Subscriptions to Request-Contained Resource Lists in the Session Initiation Protocol (SIP)", G. Camarillo, A. Roach, O. Levin, October 2008,

URL: http://www.ietf.org/rfc/rfc5367.txt

[RFC5491] "GEOPRIV Presence Information Data Format Location Object (PIDF-LO) Usage Clarification, Considerations and Recommendations", J. Winterbottom, M. Thomson, H. Tschofenig, March 2009

URL: http://tools.ietf.org/html/rfc5491

[RFC5874] RFC 5874, "An Extensible Markup Language (XML) Document Format for Indicating Changes in XML Configuration Access Protocol (XCAP) Resources", J. Rosenberg, May 2010,

URL: http://www.ietf.org/rfc/rfc5874.txt

[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/

[XMLSIG] "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 2.8, Open Mobile Alliance™,
OMA-ORG-Dictionary-V2_8,
URL:http://www.openmobilealliance.org/

3. Terminology and Conventions

3.1 Conventions

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

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

3.2 Definitions

Location Client	Functional entity that subscribes to a Location Server in order to obtain location information for one or more Targets.
Location Information	Information of the physical position of the target. In LOCSIP the allowed formats are restricted to what is defined in section 5.3.4
Location Server	Functional entity that handles location service subscription request and retrieves the location information of the Target.
Target	The device or the user associated with a device whose location is requested.
Home Subscription Agent	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
HSA	Home Subscription Agent
LOCSIP	Location in SIP/IP Core
OMA	Open Mobile Alliance
PKI	Public Key Infrastructure
PoC	Push-to-talk over Cellular
QoS	Quality of Service
RLMI	Resource List Meta-Information
RLS	Resource List Server
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 Presence SIMPLE [OMA-PRS_AD], 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

LOCSIP V1.0 enables a Location Client to subscribe to location information from a Location Server. The subscription may include filters defining temporal or spatial criteria for when location information shall be delivered. The subscription may also include a list of targets either as a resource list included in the subscription or as a reference to resource list stored in Shared List XDMS.

5. Architectural Model

5.1 Dependencies

LOCSIP depends on:

- OMA Presence SIMPLE Architecture [OMA-PRS_AD] as LOCSIP reuses the Home Subscription Agent and the Resource List Server functional entities in the OMA Presence SIMPLE Enabler.
- OMA XML Document Management (XDM) Architecture [OMA XDMAD] for management of the Location Policy XDMS
- IMS in OMA Architecture [IMSARCH] for definition of services provided by SIP/IP Core.
- OMA Global Permission Management (GPM) Architecture [OMA-GPM_AD] to provide the option to evaluate permission in the GPM enabler.

In addition LOCSIP depends on following specifications:

- 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) [RFC5367]
- 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]
- 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.

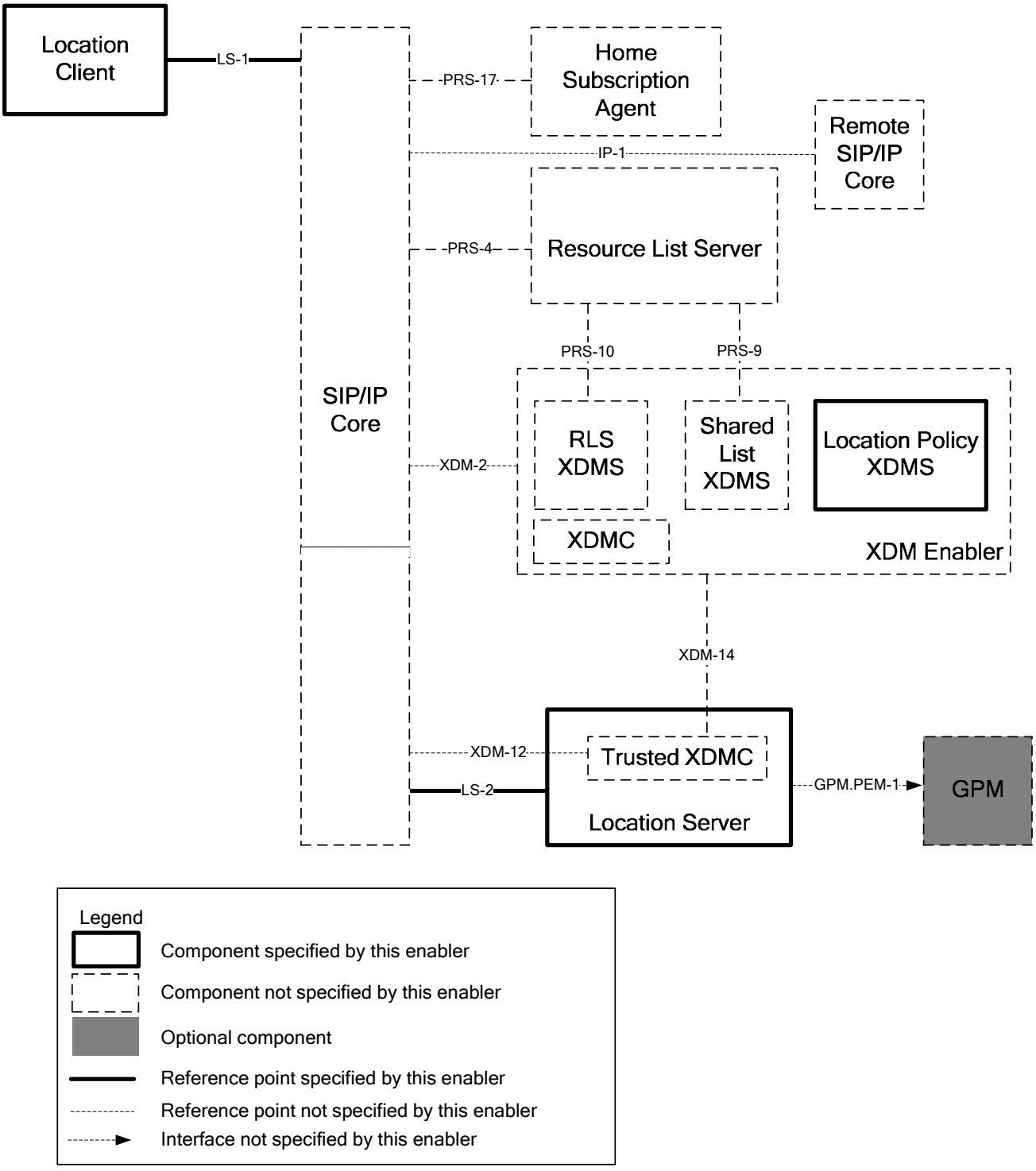

Figure 1: LOCSIP Architectural Model

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 [RFC3265] [RFC4662], [RFC5367] and [LOCSIP-TS].

5.3.1.2 Location Server

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

The Location Server supports the following:

- Receives and authorizes subscriptions from a Location Client and RLS and distributes Location Information using [RFC3265]and [LOCSIP-TS];
- Subscribes to changes to documents stored in the Location Policy XDMS and Shared List XDMS;
- Fetches documents from the XDMS. Two types of document are retrieved, location policy documents from Location Policy XDMS and URI list information from the Shared List XDMS. URI list information is needed when lists of user identities in policy documents are defined using URI lists.

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.

5.3.1.3 Location Policy XDMS

The Location Policy XDMS supports XDMS procedures as described in [XDM_Core]. It stores location policy documents as described in [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 Home Subscription Agent

Home Subscription Agent (HSA) functionality is specified in [OMA-PRS_HSA]. The HSA is located in the domain of the Location Client and controls its LOCSIP service use.

5.3.2.3 Resource List Server (RLS)

The RLS functionality is specified in [OMA-PRS_AD] and [OMA-PRS_RLS].

5.3.2.4 XML Document Management Server (XDMS)

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

5.3.2.4.1 Shared List XDMS

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

5.3.2.4.2 RLS XDMS

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

5.3.2.5 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.

5.3.2.6 Global Permission Management (GPM)

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

- Evaluate and process permissions rules for the specific Target

- Return to the Location Server a decision on the release of location information

Note: the permission rules are stored on a Location Policy 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 with prefix LS and IP are in scope of this Architecture. Reference Points named with prefix PRS are specified in the [OMA-PRS_AD], named with prefix XDM are specified in [OMA XDMAD] and named with prefix GPM are specified in [OMA-GPM_AD], they are out 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, the Home Subscription Agent and the 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 [RFC4662] and for Request-Contained Resource List, based on [RFC5367];
- 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 Location Server. The protocol for the LS-2 reference point is SIP.

LS-2 reference point provides the following functions:

- Receive subscriptions to a single Target's Location Information and send notifications pertaining to this Target;

5.3.3.3 Reference Point IP-1

The IP-1 Reference Point [3GPP TS_23.002] supports the communication between the SIP/IP Core and a Remote Network that contains a SIP/IP Core to which remote LOCSIP Enablers connect. The protocol for the IP-1 Reference Point is SIP.

The IP-1 Reference Point provides the following functions:

- Forwarding of SIP signalling messages between SIP/IP Cores.

When the SIP/IP Core corresponds to 3GPP IMS or 3GPP2 MMD networks, the IP-1 Reference Point conforms to the Mw Reference Point as specified in [3GPP TS 23.002] and [3GPP2 X.S0013-002-B].

5.3.4 Location Information Format

LOCSIP uses the Presence Information Data Format – Location Object (PIDF-LO) as specified in [RFC4119], [RFC5139] and [RFC5491] 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 privacy 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 Shared List XDMS.

The subscription authorization rules support the following actions:

- Accept
- Reject.

5.3.5.2 Location Privacy Rules

The location privacy rules determine which Location Information is disseminated to Location Clients that have been accepted by subscription authorization rules.

The document containing the location privacy rules is stored in the Location Policy XDMS.

5.3.6 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 Location Policy XDMS is needed when location authorization is performed.

The information stored in the Location Policy 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 of a Single Target

5.4.1.1 Fetching the Current Location of a Single Target

The Figure 2 shows the flow when a LOCSIP Location Client fetches the current location of a single Target.

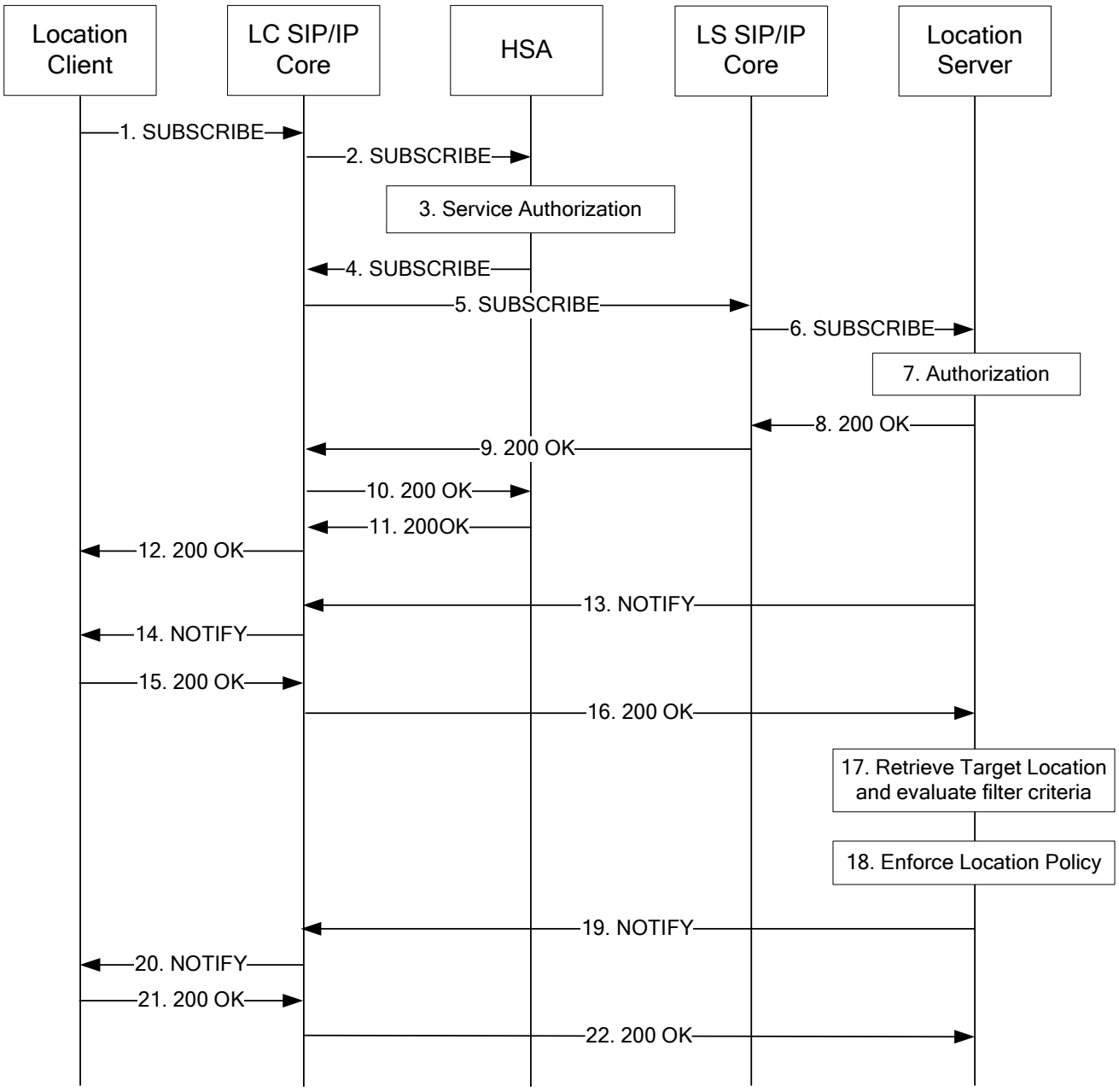

Figure 2: Fetching the Current Location of a Single Target

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 HSA.

3. The HSA performs the necessary authorisation checks per local policy to ensure the Location Client is allowed to use Location Service.

4. Once authorisation checks are passed the HSA forwards the request to the Location Server via SIP/IP Core network.

5. 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.

6. 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.

7. The Location Server performs the necessary authorisation checks on the originator to ensure it is allowed to request the location information of the Target.

8. 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.

9. The SIP/IP Core network of the Location Server forwards the response to the SIP/IP Core network of the Location Client.

10. The SIP/IP Core network of Location Client forwards the response to the HSA.

11. The HSA forwards the response to the SIP/IP Core network of the Location Client.

12. The SIP/IP Core network of the Location Client forwards the response to the Location Client.

Steps 13 to 16 are optional and do not have to be performed if step 22 can be performed directly after step 13.

13. 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. The SIP NOTIFY request is sent to the SIP/IP Core network of the Location Client.

14. The SIP/IP Core network of the Location Client forwards the SIP NOTIFY request to the Location Client.

15. The Location Client acknowledges the receipt of the SIP NOTIFY request with a SIP 200 OK response.

16. The SIP/IP Core network forwards the SIP 200 OK response to Location Server.

17. 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.

18. 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.

19. 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 1: 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.

20. The SIP/IP Core network of the Location Client forwards the SIP NOTIFY request to the Location Client.

21. The Location Client acknowledges the receipt of the SIP NOTIFY request with a SIP 200 OK response.

22. The SIP/IP Core network forwards the SIP 200 OK response to the Location Server.

NOTE 2: The remaining figures in this document only illustrate the simplified case where the Location Client and Location Server are associated with the same SIP/IP Core network, and there is no HSA involved.

5.4.1.2 Subscribing to the Notification of Periodic Trigger

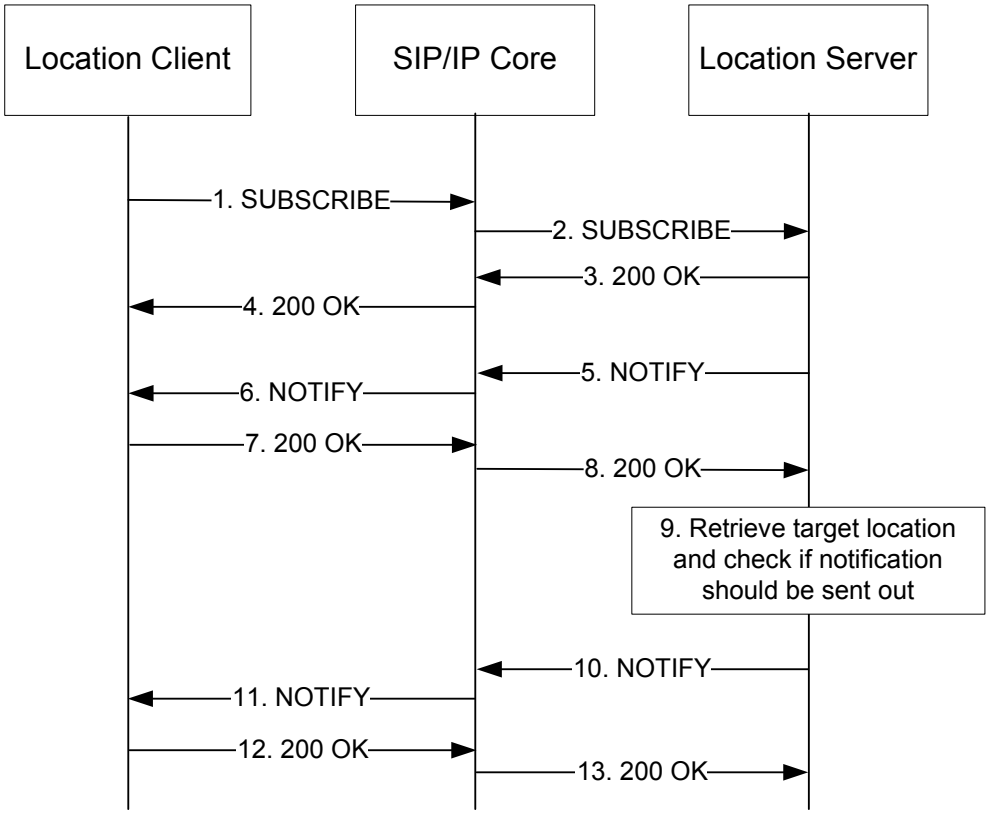

Figure 3: Flow for Subscribing to the Notification of Periodic Trigger

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 an Event header (with min-interval and max-interval set to the same value) in the SIP SUBSCRIBE request.

2. The SIP/IP Core network forwards the SIP SUBSCRIBE request to the Location Server.

3. The Location Server authorizes the subscription. 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.

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. Upon receipt of the SIP SUBSCRIBE request, as well as 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

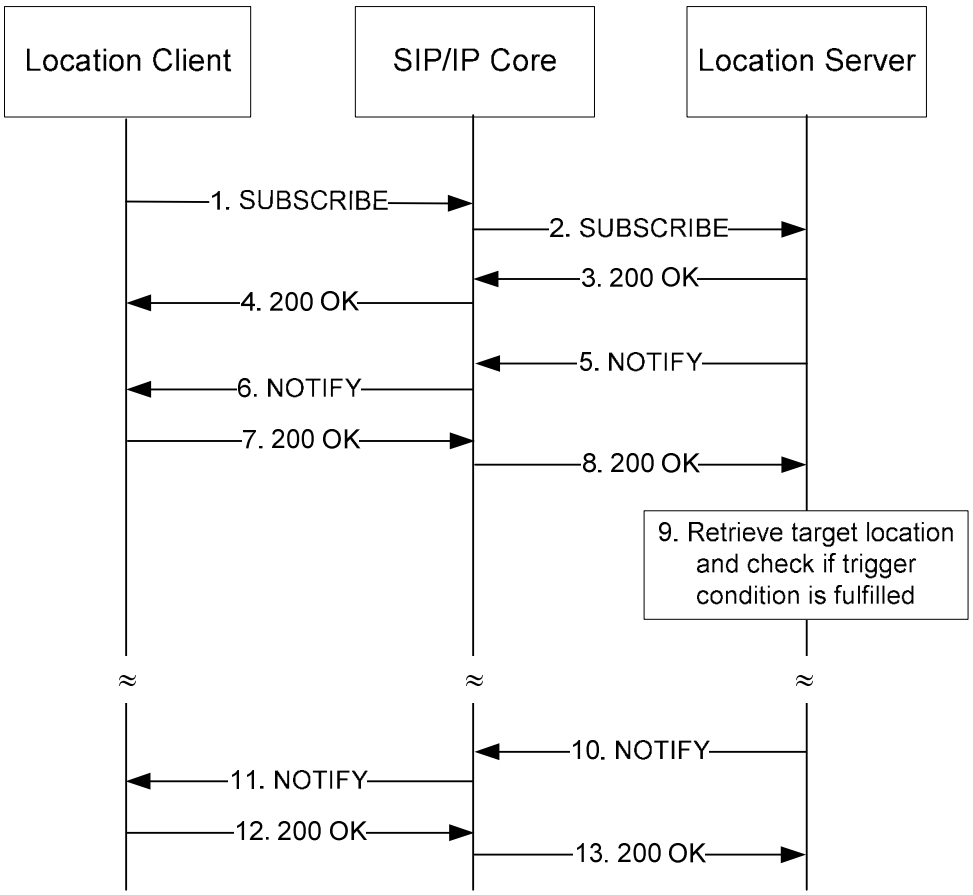

Figure 4: Flow for Subscribing to the Notification of Area Event Trigger

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.

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

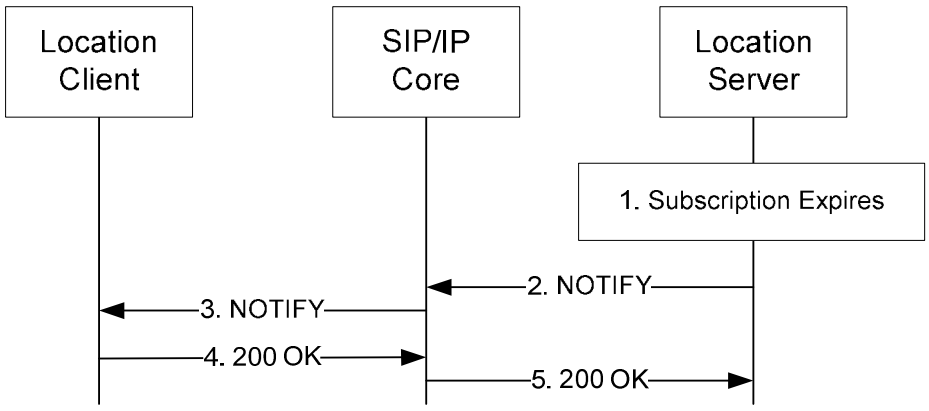

Figure 5: Flow for Subscription Expiry Notification

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 HSA or 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 HSA or Location Server sends a 403 Forbidden message in response to a subcription request.

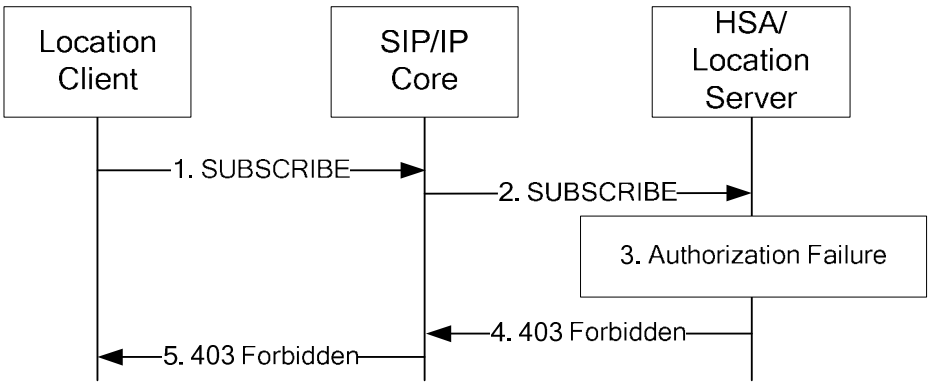

Figure 6: Flow for Subscription Authorization Failure

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 HSA or Location Server, based on the address of the Target and the feature tag for location service.

3. The HSA or 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 HSA or 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

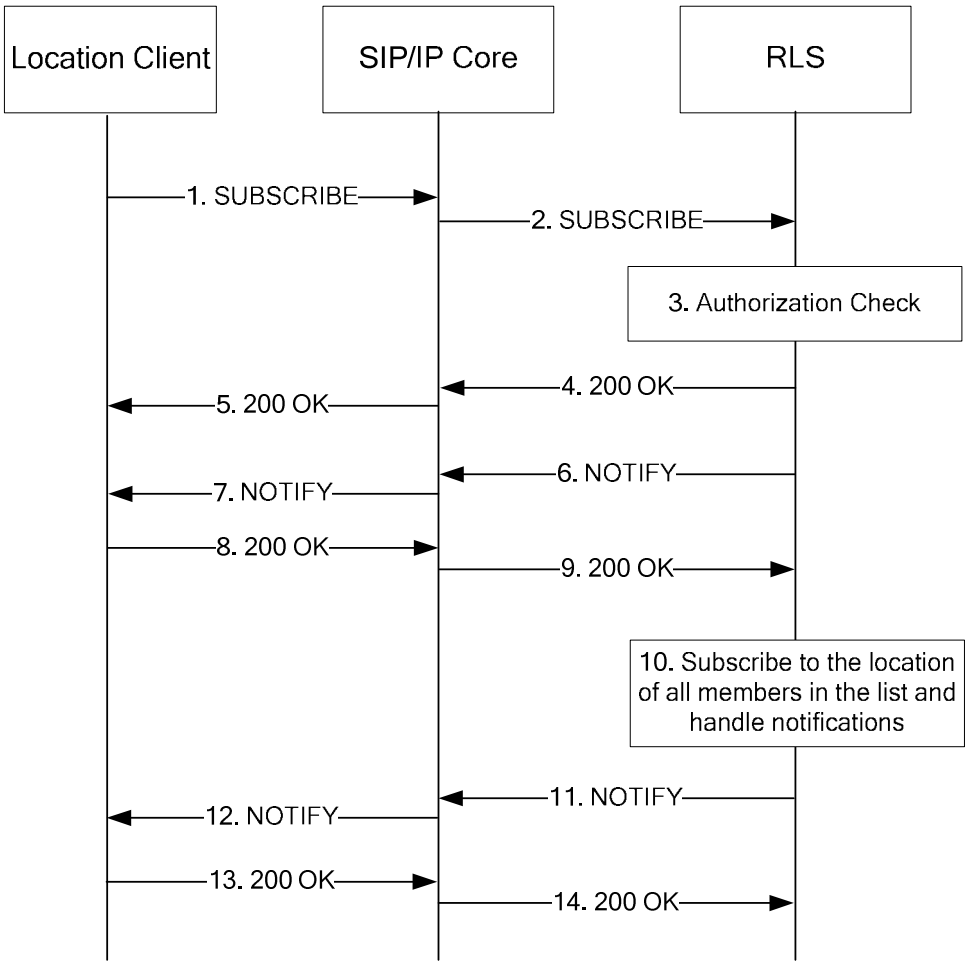

Figure 7: Flow for Subscribing to Location for a List of Targets

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] and [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 list refers to an existing resource list stored in RLS XDMS and is identified by the request URI. The Request-Contained Resource List includes a URI-list in the SIP SUBSCRIBE request according to [RFC5367].

2. The SIP/IP Core network forwards the request to the correct RLS based on the address of Target list and resource list service indication.
3. The 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 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 RLS resolves the Target list into individual targets and 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.

Note 1: For Resource List, the RLS fetches the resource list document from the Shared List XDMS using XCAP, as defined in [XDM_Core]. For Request-Contained Resource List, the RLS extracts the URIs in the URI-list directly from the body part of initial SIP SUBSCRIBE request.

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 RLS.
10. The RLS generates the necessary SIP SUBSCRIBE requests to the Location Server for each individual Target in the list.

11. When the notification condition is fulfilled, the RLS generates a SIP NOTIFY request with multipart format. The RLS includes the RLMI document, copies/aggregates the body of the received SIP NOTIFY request(s) from Location Server 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 RLS.

NOTE 2: 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

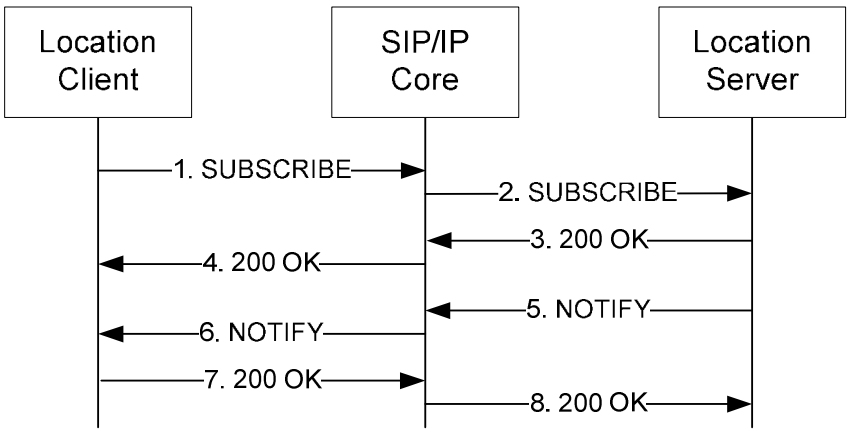

Figure 8: Flow for Location Client Initiated Subscription Cancellation/Refreshing

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, indicating the cancellation of a subscription operation, the subscription will be terminated. 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" and with an "expires" parameter 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

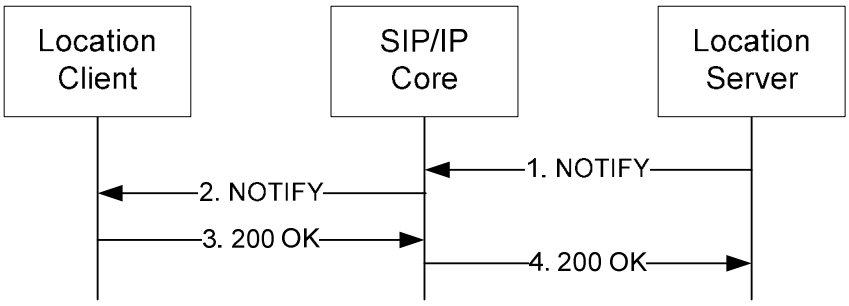

Figure 9: Flow for Location Server Initiated Subscription Cancellation/Refreshing

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 [RFC3265]. 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

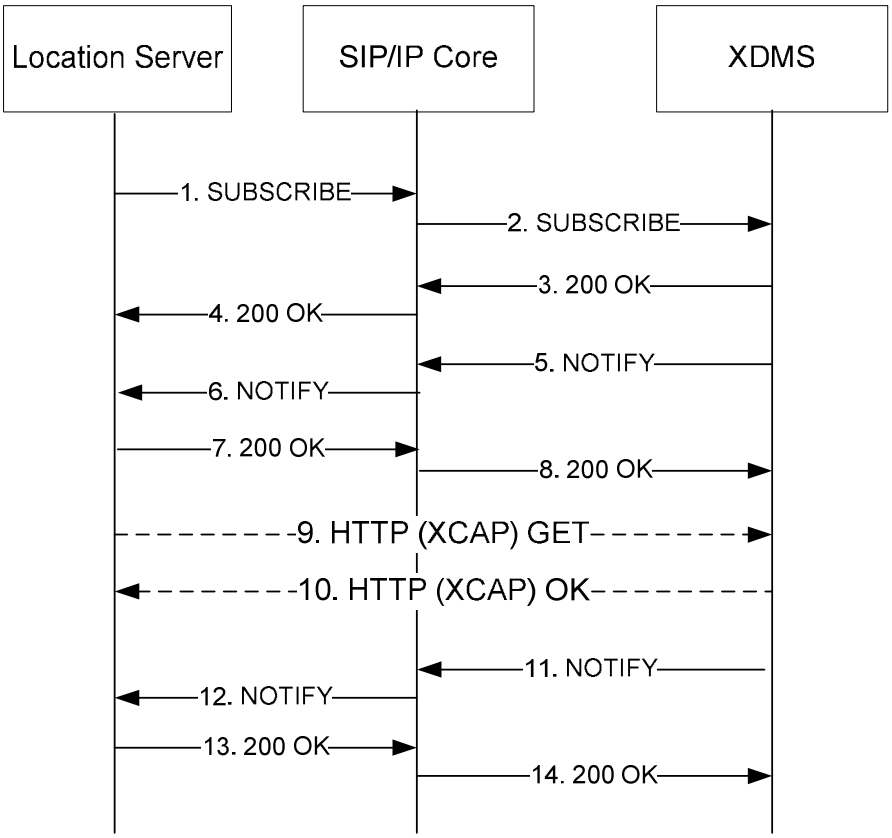

Figure 10: Subscribing to Changes in Location Policy Data

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 Location Policy XDMS.
3. The Location Policy 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 Location Policy XDMS sends the first SIP NOTIFY request, which is used in order to synchronize the Location Policy XDMS and Location Server on a common "baseline" document as described in [RFC5874].
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 Location Policy 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 [RFC5874]. and [XDM_Core].
10. The version of the document requested is provided by the Location Policy XDMS.

11. When changes occur in the Location Authorization/Policy Rules document, the Location Policy 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 Location Policy XDMS.

5.4.4.2 RLS Subscribing to Changes in Group/List

The RLS SHALL support subscriptions to changes in the group/list documents stored in RLS XDMS and Shared List XDMS as specified in [XDM_Core] "*Subscriptions to Changes in the XML Documents*".

5.4.5 Authorization using GPM

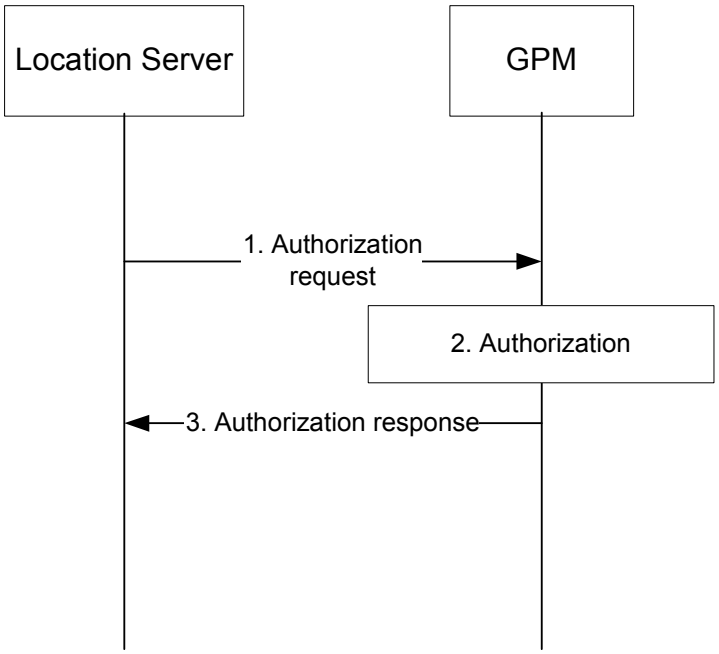

Figure 11: Flow for permissions checking with GPM

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].

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 IMS or 3GPP2 MMD networks, 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. The privacy data for the target shall only be obtained from the home network of the target. Only the home domain deployment model supported by [OMA SEC CF] is applicable to LOCSIP.

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
OMA-AD-LOCSIP-V1_0	17 Jan 2012	No prior version

Appendix B. Charging (Informative)

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.

B.1 Support of Charging through the OMA Charging Enabler

The OMA Charging Enabler [OMA-CHG_AD] coordinates charging data triggers and flow from OMA enablers into an underlying charging infrastructure, supporting online and offline charging. The Location Server is a LOCSIP entity that may optionally report Chargeable Events.

The Location Server acts as a Charging Enabler User as defined in [OMA-CHG_AD]. In addition, the RLS XDMS, the Shared List XDMS, the Location Policy 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. This reference point is currently supported by the Charging Enabler, CH-1 for offline charging and CH-2 for online charging. These are described in [OMA-CHG_AD].

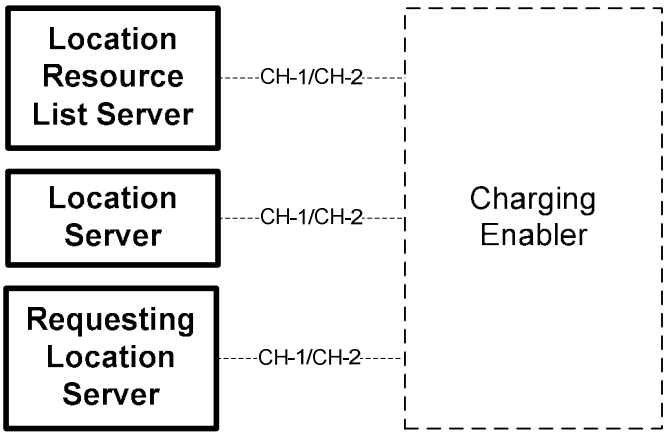

Figure 12: Support of Charging Through the OMA Charging Enabler

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

Appendix C. Service Subscription Management (Informative)

A LOCSIP service provider manages the service subscription of the users based on OMA General Service Subscription Management Architecture [OMA-GSSM_AD]. A LOCSIP user manages the service subscription of the location information through XCAP [RFC4825].