Location in SIP/IP core Specification

Candidate Version 1.0 – 14 Nov 2011

Open Mobile Alliance

OMA-TS-LOCSIP-V1_0-20111114-C

Contents

Figures

Tables

1. Scope

This document provides the specifications for the OMA Location in SIP/IP core (LOCSIP) enabler.

2. References

2.1 Normative References

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

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

[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_32.240] 3GPP TS 32.240 "Charging management; Charging architecture and principles", URL: http://www.3gpp.org/ftp/Specs/archive/32_series/32.240/

[3GPP TS_32.260] 3GPP TS 32.260 "Charging Management; IP Multimedia Subsystem (IMS) Charging", URL: http://www.3gpp.org/ftp/Specs/archive/32_series/32.260/

[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

[3GPP-TS_24.109] 3GPP TS 24.109, "Bootstrapping interface (Ub) and network application function interface (Ua); Protocol details", URL: http://www.3gpp.org/ftp/Specs/archive/24_series/24.109/

[3GPP TS 24.229] 3GPP TS 24.229 "Internet Protocol (IP) multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3", URL: http://www.3gpp.org/ftp/Specs/archive/24_series/24.229/

[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

[3GPP2-X.S0013-004] 3GPP2 X.S0013-004 "All-IP Core Network Multimedia Domain: IP Multimedia Call Control Protocol Based on SIP and SDP Stage 3", URL: http://www.3gpp2.org/Public_html/specs/index.cfm

[3GPP2-X.S0013-007] 3GPP2 X.S0013-007 "All-IP Core Network Multimedia Domain: IP Multimedia Subsystem – Charging Architecture", URL: http://www.3gpp2.org/Public_html/specs/index.cfm

[3GPP2-X.S0013-008] 3GPP2 X.S0013-008 "All-IP Core Network Multimedia Domain: IP Multimedia Subsystem – Offline Accounting, Information Flows and Protocol", URL: http://www.3gpp2.org/Public_html/specs/index.cfm

[IETF-EventRate] IETF draft-ietf-sipcore-event-rate-control-09 "Session Initiation Protocol (SIP) Event Notification Extension for Notification Rate Control", A.Niemi, Aug 31 2011, URL: http://tools.ietf.org/id/draft-ietf-sipcore-event-rate-control-09.txt
Note: IETF Draft work in progress

[LOCSIP-RD] "Location in SIP/IP core Requirements", Open Mobile Alliance™, Version 1.0, OMA-RD-LOCSIP-V1_0, URL: http://www.openmobilealliance.org/

[OMA SEC CF] "Security Common Functions Architecture," Open Mobile Alliance™, Version 1.0, OMA-AD-SEC_CF-V1_0, URL: http://www.openmobilealliance.org/

[GeoPriv_Policy] "Geolocation Policy: A Document Format for Expressing Privacy Preferences for Location Information," H. Schulzrinne, et al, Oct 14 2011, URL: URL: http://tools.ietf.org/id/draft-ietf-geopriv-policy-25.txt

Note: IETF Draft work in progress

[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

[RFC4479] "A Data Model for Presence", J. Rosenberg, July 2006, URL: http://www.ietf.org/rfc/rfc4479.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
[RFC5025]	"Presence Authorization Rules", J. Rosenberg, December 2007, URL: http://www.ietf.org/rfc/rfc5025.txt
[RFC5139]	IETF RFC 5139, "Revised Civic Location Format for Presence Information Data Format Location Object (PIDF-LO)", M. Thomson etc, 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]	IETF RFC 5491, "GEOPRIV Presence Information Data Format Location Object (PIDF-LO) Usage Clarification, Considerations, and Recommendations", J. Winterbottom etc, March 2009, URL http://tools.ietf.org/html/rfc5491
[RFC5839]	IETF RFC 5839, "An Extension to Session Initiation Protocol (SIP) Events for Conditional Event Notification", A. Niemi, May, 2010, URL: http://tools.ietf.org/html/rfc5839
[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/
[GeoShape]	"GML 3.1.1 PIDF-LO Shape Application Schema for use by the Internet Engineering Task Force (IETF)", Thomson, M. and C. Reed, Candidate OpenGIS Implementation Specification 06-142r1, Version: 1.0, April 2007. URL: http://www.opengeospatial.org/standards/gml
[RFC2046]	IETF RFC 2046 "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types", N. Freed et. al., Nov 1996, URL: http://www.ietf.org/rfc/rfc2046.txt
[RFC2387]	IETF RFC 2387 "The MIME Multipart/Related Content-type", E. Levinson, Aug 1998, URL: http://www.ietf.org/rfc/rfc2387.txt
[RFC3856]	IETF RFC 3856 "A Presence Event Package for the Session Initiation Protocol (SIP)", J. Rosenberg, Jan. 2003, URL: http://www.ietf.org/rfc/rfc3856.txt
[XDM_List]	Shared List XDM Specification", Version 2.0, Open Mobile Alliance™, OMA-TS-XDM_Shared-V2_0, URL: http://www.openmobilealliance.org/
[PRS_RLSXDM]	"RLS XDM Specification", Version 2.0, Open Mobile Alliance□, OMA-TS-Presence_SIMPLE_RLS_XDM-V2_0, URL: http://www.openmobilealliance.org/
[OMA GPMTS]	"Global Permissions Management Technical Specification", OMA-TS-GPM-V1_0, Open Mobile Alliance™, URL: http://www.openmobilealliance.org/
[PRS_SPEC]	"Presence SIMPLE Specification", Version 2.0, Open Mobile Alliance™, OMA-TS-Presence_SIMPLE-V2_0, URL: http://www.openmobilealliance.org/
[XSD-locFilter]	"LOCSIP - Location Filter", Version 1.0, Open Mobile Alliance□, OMA-SUP-XSD_locsip_filter-V1_0, URL: http://www.openmobilealliance.org/tech/profiles/
[XSD-locQoS]	"LOCSIP – Location QoS", Version 1.0, Open Mobile Alliance□, OMA-SUP-XSD_locsip_qos-V1_0, URL: http://www.openmobilealliance.org/tech/profiles/
[XSD-locGPMExt]	"LOCSIP – Extension of GMP PEM1 output template", Version 1.0, Open Mobile Alliance□, OMA-SUP-XSD_ locsip_gpmpem1outputext-V1_0, URL: http://www.openmobilealliance.org/tech/profiles/
[XSD-locGBAKeyid]	"LOCSIP – GBA key identifier", Version 1.0, Open Mobile Alliance□, OMA-SUP-XSD_ locsip_gbakeyid-V1_0, URL: http://www.openmobilealliance.org/tech/profiles/
[GPM INPUT TEMPLATE XSD]	XSD definition file for GPM Input Template, Open Mobile Alliance™, OMA-SUP-XSD_GPM_PEM1InputTemplate-V1_0, URL: http://www.openmobilealliance.org/
[GPM OUTPUT TEMPLATE XSD]	XSD definition file for GPM Output Template, Open Mobile Alliance™, OMA-SUP-XSD_GPM_PEM1OutputTemplate-V1_0, URL: http://www.openmobilealliance.org/
[OMA-PRS_HSA]	"Home Subscription Agent (HSA) Specification", Open Mobile Alliance™, Version 1.0, OMA-TS-Presence_SIMPLE_HSA-V1_0, , URL: http://www.openmobilealliance.org/

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/

[3GPP-TS_23.218] 3GPP TS 23.218 "IP Multimedia (IM) session handling; IM call model; Stage 2", URL: http://www.3gpp.org/ftp/Specs/archive/23_series/23.218/

[3GPP-TS_29.228] 3GPP TS 29.228 "IP Multimedia (IM) Subsystem Cx and Dx Interfaces; Signalling flows and message contents", URL: http://www.3gpp.org/ftp/Specs/archive/29_series/29.228/

[3GPP2-X.S0013-003] 3GPP2 X.S0013-003 "All-IP Core Network Multimedia Domain: IP Multimedia (IMS) session handling; IP Multimedia (IM) call model; Stage 2", URL: http://www.3gpp2.org/Public_html/specs/index.cfm

[3GPP2-X.S0013-006] 3GPP2 X.S0013-006 "All-IP Core Network Multimedia Domain: Cx Interface based on the Diameter Protocol; Protocol Details", URL: http://www.3gpp2.org/Public_html/specs/index.cfm

[3GPP2-X.S0027-001] 3GPP2 X.S0027-001 "Presence Service; Architecture and functional description", URL: http://www.3gpp2.org/Public_html/specs/index.cfm

[I.D.thomson-location-quality] "Specifying Location Quality Constraints in Location Protocols", M. Thomson, J. Winterbottom, June 28 2011, URL: http://tools.ietf.org/id/draft-thomson-geopriv-location-quality-08.txt
Note: IETF Draft work in progress

[3GPP.22.071] 3GPP TS 22.071 : "Location Services (LCS); Service description, Stage 1". URL: http://www.3gpp.org/ftp/Specs/latest/Rel-7/22_series/

[W3C.REC-xpath-19991116] "XML Path Language (XPath) 2.0", Boag, S., Chamberlin, D., Berglund, A., Robie, J., Kay, M., Simeon, J., and M. Fernandez, World Wide Web Consortium, Recommendation REC-xpath20-20070123, January 2007, URL: http://www.w3.org/TR/2007/REC-xpath20-20070123

[3GPP TS 33.220] 3GPP TS 33.220 "Generic Authentication Architecture (GAA); Generic bootstrapping architecture", URL: http://www.3gpp.org/ftp/Specs/archive/23_series/33.220/

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

Back-end Subscription	A Subscription submitted by an RLS or Home Subscription Agent on behalf of the Location Client.
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.

3.3 Abbreviations

AS	Application Server
OMA	Open Mobile Alliance
3GPP	Third Generation Partnership Project
CRS	Coordinate Reference Systems
EPSG	European Petroleum Survey Group
GML	Geography Markup Language
HSA	Home Subscription Agent
IANA	Internet Assigned Numbers Authority
LOCSIP	Location in SIP/IP core
MLP	Mobile Location Protocol
MMD	Multimedia Domain
PIDF	Presence Information Data Format
PIDF-LO	Presence Information Data Format, Location Object
RLS	Resource List Server
UoM	Unit of Measurement
URN	Uniform Resource Namespace

4. Introduction

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.

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. LOCSIP Functional Entities

5.1 Location client

A Location Client is an entity that requests Location Information about one or multiple Targets.

When the SIP/IP Core corresponds with 3GPP IMS or 3GPP2 MMD networks, the Location Client MAY be implemented in a UE or an AS as defined in [3GPP-TS_23.228] and [3GPP2-X.S0013-002] respectively.

5.1.1 Location Information Processing

The Location Client SHALL support location information format and processing procedures as described in Section 9.

5.1.2 Emergency Location Subscription

In case of emergency location subscription, the Location Client SHALL include a "Priority" header field parameter with value “emergency” in the SUBSCRIBE request, indicating the importance of the request to the Location Server.

The use of other header field parameters (e.g. “resource-priority”) to gain priority in the SIP/IP core is out of scope of this specification.

5.1.3 Subscription to Location Information

A Location Client SHALL support subscription and notification of Location Information, according to the subscriber procedures described in [RFC3265] and [RFC3856] with the following clarifications:

The Location Client SHALL include a Feature tag for location service (Appendix D) in the SUBSCRIBE request to allow SIP/IP Core to route the request directly to Home Subscription Agent (HSA) or Location Server. This mechanism is used to distinguish location service requests from presence service requests.

Location subscription MAY include location event notification filter in the body of a SUBSCRIBE request. The subscription MAY also include the required location QoS parameter in the body of a SUBSCRIBE request.

In case of a one-time location request, the subscription duration SHOULD be set to zero. This means that the value of Expires header in SUBSCRIBE request SHOULD be 0.

If the Location Client is aware of the SIP URI of the Target, the Location Client SHOULD insert the SIP URI in the Request-URI of the SUBSCRIBE request rather than a tel URI.

If the Location Client only knows the tel URI of the Target, the tel URI may get translated to a SIP URI by the SIP/IP Core. In this case, the Location Client MAY learn the translated URI from the “entity” attribute of the <presence> element [RFC4119] included in the NOTIFY request and use it for future subscriptions.

5.1.3.1 Subscription to a URI List

Subscription to a URI List (described in [RFC5367]) enables a Location Client to subscribe to multiple Targets using a single SUBSCRIBE request.

A Location Client MAY subscribe to a URI List. If a Location Client subscribes to a URI List, it SHALL support the SIP event notification extension for resource lists, according to the subscriber procedures described in [RFC4662].

Note: As described in section 5.3, the RLS can enforce a limit on the number of back-end subscriptions allowed for a single URI List subscription, in which case the Location Client will not receive <instance> elements for those <resource> elements corresponding to Targets that could not be subscribed by the RLS.

5.1.3.2 Subscription to a Request-contained URI List

Subscription to a Request-contained URI List enables a Location Client to subscribe to multiple Targets using a single SUBSCRIBE request.

A Location Client MAY support subscription to a Request-contained URI List. If supported, the Location Client SHALL follow User Agent Client procedures as described in [RFC5367] sections "User Agent Client Procedures" and "URI-List Document Format" with the following clarifications:

- The Location Client SHOULD NOT use hierarchical lists, <entry-ref> elements, and <external> elements when listing the Targets in the SUBSCRIBE request.

The Location Client MAY be provisioned with the SIP URI of the RLS. Provisioning can be done with local configuration.

Note: As described in section 5.3, the RLS can enforce a limit on the number of back-end subscriptions allowed for a single URI List subscription, in which case the Location Client will not receive <instance> elements for those <resource> elements corresponding to Targets that could not be subscribed by the RLS.

5.1.4 Event Notification Filtering

Event notification filtering is a mechanism for the Location Client to control the content and triggers of notifications.

A Location Client subscribing to Location Information MAY request event notification filtering. If requesting event notification filtering, the Location Client SHALL support the movedHoriz, movedVert, enter and exit filter events location filter document formats described in section 10 and MAY support the remaining filter events filter document formats described in section 10

If requesting event notification filtering, a Location Client SHALL use the "application/location-delta-filter+xml" content type. If the subscription uses a Request-contained Location List as described in Section 5.1.3.2, the Location Client SHALL implement the 'multipart/mixed' content type as described in [RFC2046], in order to aggregate the 'application/location-delta-filter+xml" and 'application/resource-lists+xml' content types in the SUBSCRIBE request.

NOTE: The notification does not identify which filter condition initiated the notification.

5.1.5 Specifying required location QoS parameters

The location QoS parameters that define the expected quality of location information are used by a Location Client to indicate the desired constraints on the quality of the location information provided. Required quality of location information is expressed with:

- location type,
- maximum uncertainty,
- maximum response time,
- maximum age,
- required civic elements, and
- QoS class.

If applicable, the Location Server is able to use this information to control how location information is determined.

A Location Client subscribing to Location Information MAY include location QoS parameters in the form of a Location QoS Document in the body of a SUBSCRIBE request. Content of the Location QoS Document is described in Section 11. The MIME type for Location QoS document is application/location-qos+xml. The location QoS parameters MAY be sent together with a Location Filter document and/or a Request-Contained Resource List in the body of SUBSCRIBE request. In this case, the Location Client SHALL implement the 'multipart/mixed' content type as described in [RFC2046].

5.1.5.1 Location Type

The indication of a location type in the request allows Location Client to specify desired type of the location information in a response: geospatial, civic, or both.

The Location Client MAY include location type parameter in location request.

5.1.5.2 Maximum uncertainty

The maximum uncertainty defines the wanted uncertainty at a certain confidence. There are horizontal and vertical components to the uncertainty parameter. As described in [I.D.thomson-location-quality] horizontal uncertainty is the maximum distance from the centroid of the area to the point in the shape furthest from the centroid on the horizontal plane. Vertical uncertainty is the difference in altitude from the centroid to the point in the shape furthest from the centroid on the vertical axis.

5.1.5.3 Maximum response time

Response time is defined as the time needed for the Location Server to send an initial response with the Location Information after having received a location request. Different Location Clients may have different requirements for the response time. In some cases the response time may depend on the positioning uncertainty and on age of the Location Information. This relation may be dependent on the positioning measurement technique that is used to determine a Target's position. The Location Server may need to make trade-offs between these three parameters.

5.1.5.4 Maximum age

The maximum age parameter states the maximum allowable age of the Location Information that is being sent in a response to a Location Client. This Location Information may have been cached in the system from a previous location query.

5.1.5.5 Required civic elements

The specification of required civic elements in location request allows Location Client to control the quality of Location Information provided in civic format. The specification of required civic element in Location QoS Document uses required civic element specification in [I.D.thomson-location-quality], Section 3.1.2. “Required Civic Elements”.

5.1.5.6 QoS class

The QoS class defines the degree of adherence of the location service to given QoS parameters: location type, maximum uncertainty, maximum response time, maximum age, and required civic elements of Location Information. There are three location QoS classes defined: "Assured", "Best effort" (which are based on definition in [3GPP.22.071]), and “Emergency”:

The "Assured" location QoS class presumes strict adherence to given QoS parameters. The Location Server must obtain Location Information while fulfilling the requirements set by the other QoS parameters.

The "Best effort" location QoS class presumes that QoS parameters are not adhered to strictly. The Location Server shall obtain Location Information while trying to fulfill the requirements set by the other QoS parameters, but it will not discard the response if other QoS parameters are not satisfied. This class is used to allow Location Server to choose proper location determination function (or positioning technique) to invoke (for example, the one which is more accurate but it takes more time to determine, or less accurate but faster).

The “Emergency” location QoS class does not define any adherence to given QoS parameters. Any location QoS parameter included in the request with “Emergency” class has no influence on Location Server behavior. The “Emergency” class is used to indicate to Location Server that location is being retrieved for a Target that is involved in an emergency call or have initiated an emergency service in some other way.

5.1.6 Signaling Compression

When the SIP/IP Core corresponds with 3GPP IMS or 3GPP2 MMD networks, the signaling compression procedures as defined in [3GPP-TS_24.229] / [3GPP2-X.S0013-004] SHALL be used.

5.1.7 Handling of Large MIME Objects

A Location Client MAY implement the 'multipart/related' content type as described in [RFC2387], in order to extract different MIME objects from the body of the SIP NOTIFY request. In this case, the Location Client SHALL indicate its support for the 'multipart/related' content type by using the Accept header field in the SUBSCRIBE request.

5.1.8 Conditional Event Notification

Conditional event notification is a mechanism that allows the Location Client to condition the subscription request to whether the state has changed since the previous notification was received. When such a condition is met, either the body of the location event notification or the entire notification message is suppressed.

A Location Client MAY issue a conditional SUBSCRIBE request according to the subscriber procedures defined in [RFC5839]. If supported, the SUBSCRIBE request SHALL include a Suppress-If-Match header field to indicate the conditional subscription.

5.1.9 Event Notification Rate Control

A Location Client MAY support event notification rate control. If event notification rate control is supported, the Location Client SHALL follow the subscriber maximum and minimum rate procedures for event notification as described in [IETF-EventRate].

Event notification maximum rate is a mechanism for limiting the rate of SIP event notifications. Event notification minimum rate is a mechanism for sending the notifications at a minimum interval regardless of movement.

The Location Client MAY include a Event header parameter "max-rate" in a SIP SUBSCRIBE request, indicating the minimum time period between two consecutive notifications in a subscription. It MAY also include an Event header parameter "min-rate" to specify the maximum time period allowed between two notifications.

The Location Client SHOULD choose a "min-rate" value equivalent or higher than the "max-rate" value.

5.2 Location Server

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

When the SIP/IP Core corresponds with 3GPP IMS or 3GPP2 MMD networks, the Location Server SHALL be implemented in an AS as defined in [3GPP TS 23.228] and [3GPP2 X.S0013-002-B] respectively.

Location Server does not constitute any position determination functionality. It is assumed that positioning determination is performed by another enabler such as OMA SUPL. How Location Server interacts with such position determination functionality to obtain Location Information about particular Target is out of the scope in this specification.

5.2.1 Handling of location subscriptions

Before accepting a SUBSCRIBE request, the Location Server SHALL perform authorization of the subscription attempt of the Location Client per Target's Location Information policy. If the Location Server accepts the SUBSCRIBE request, the Location Server SHALL process the SUBSCRIBE request in accordance with [RFC3265] and [RFC3856] with the following clarification:

The location conditions SHALL be excluded when evaluating the authorization rules. This allows a Location Client to subscribe to the Target when the Location Information doesn't exist and receive notifications later whenever the Location Information is available.

If the Target is identified by a SIP URI and also a tel URI, the Location Server SHALL consider these URIs equivalent for the purposes of event package subscriptions.

The Location Server SHALL accept only SUBSCRIBE requests which include a Feature tag for location service (as described in Appendix D).

The Location Server MAY have a local policy to limit the maximum number of simultaneous subscriptions to a Location Information. The local policy MAY be on a per-Target basis. If the Location Server determines to reject an initial subscription due to the current number of active subscriptions to the Target being equal to or greater than the maximum, the Location Server SHALL send a 503 (Maximum number of subscriptions exceeded) response. The response SHOULD include the Retry-After header field (e.g. based on the expiry of active subscriptions), in order to suggest to the Location Client not to retry the subscription prior to the Retry-After time.

If the Location Client requests a force notification in a subscription, the Location Server SHALL skip the filter evaluation and generate notifications with the current location of the Target whenever the specified time is reached.

The Location Server processes the Location Information before delivering it to the Location Clients by applying the following steps in this order:

1) Location Rules (see section 5.2.1.1)
2) Event notification suppression (see section 5.2.1.2)
3) Location QoS handling (see section 5.2.1.3)
4) Location event notification filtering (see section 5.2.1.4)
5) Event notification rate control (see section 5.2.1.6)
6) Generating Entity Tags (see section 5.2.1.5)
7) Notification generation (see section 5.2.1.7)

Before applying Location Rules, LOCSIP MAY either:

- Evaluate and apply Location Rules itself or
- Delegate the evaluation of Location Rules to GPM

The policies to authorize the Location Client's subscription request are described in Appendix C "LOCSIP XDMS Application Usages". Rules handling with GPM is described in chapter 5.9.

The Location Server SHALL be able to detect an emergency session when the value of "Priority" header in the SUBSCRIBE request is "emergency". The Location Server SHALL handle emergency subscription with higher priority level. The Location Server MAY, based on local configuration, skip the location rules enforcement.

5.2.1.1 Applying Location Rules

The Location Rules (described in Appendix C "LOCSIP XDMS Application Usages") in the Location Policy XDMS consist of two parts:

- Subscription Authorization Rules which determine if a Location Client is allowed to subscribe to the Target's Location Information; and
- Location Privacy Rules which determine the subset of the Target's Location Information the Location Client is allowed to receive. The Location Privacy Rules MAY contain location specific conditions.

The authorization decision in the Location Server SHALL be determined based on authorization policies defined by the service provider (local policy) and the Subscription Authorization Rules document stored in the Location Policy XDMS.

The Location Server SHALL apply the Subscription Authorization Rules to all authenticated SUBSCRIBE requests. The Location Server SHALL apply the Location Privacy Rules for all outgoing NOTIFY requests to Location Client.

When the Target changes the Location Rules, the Location Server SHALL ensure it applies the Location Rules with those most recent changes.

When a SUBSCRIBE request is received, the Location Server SHALL fetch the Target's Location Rules document stored in the Location Policy XDMS according to the procedures defined in [XDM_Core] "Document Management". When constructing the HTTP GET request, the Location Server:

- SHALL set the XCAP Root URI as defined in [XDM_Core];
- SHALL set the AUID to "org.openmobilealliance.loc-rules" as defined in Appendix C;
- SHALL set the XUI to the SIP URI or tel URI of the Target;
- SHALL set the document name to "loc-rules" as defined in Appendix C; and
- SHALL set the X-3GPP-Asserted-Identity header field as defined in [3GPP-TS_24.109] or the X-XCAP-Asserted-Identity header field as defined in [XDM_Core] to the SIP URI or tel URI of the Target.

For example, the HTTP URI of the Location Rules document for a Target with a SIP URI of sip:user@domain.com would be "http://xcap.example.com/org.openmobilealliance.loc-rules/users/sip:user@domain.com/loc-rules", if the XCAP Root URI is "http://xcap.example.com".

The Location Server SHALL determine which rules in the Location Rules document are applicable and evaluate the combined permissions according to the procedures described in [XDM_Core] "Combining Permissions", with the following clarifications:

- The Location Server SHALL use the received P-Asserted-Identity header (as defined in [3GPP TS 24.229] and [3GPP2-X.S0013-004]) in the SUBSCRIBE request to determine the URI value used for matching against a conditions element.
- If an attempt to resolve an <external-list> condition element fails, the Location Server SHALL regard the Subscription Authorization Rules document as invalid and act according to the default policy of the Location Server.
- If there is no matching rule then the Location Server SHALL further handle the subscription according to the default policy of the Location Server. However, it is out of scope of the present specification to define how the default policy is configured.

After evaluating the combined permissions, the Location Server SHALL handle the subscription for this Location Client based on the value of the <sub-handling> action as follows:

- If the value is "block" or there is no value, then the Location Server SHALL reject the subscription by responding to the SUBSCRIBE request according to rules and procedures of [RFC5025], section 3.2;
- If the value is "allow", then the Location Server SHALL place the subscription in the "active" state according to rules and procedures of [RFC5025], section 3.2

While a Location Client's subscription is active, the Location Server SHALL apply Location Privacy Rules for all outgoing NOTIFY requests towards Location Client. The Location Server SHALL evaluate the location conditions based on the current location of the Target. If any rule is matched, the Location Server SHALL apply the Location Privacy Rules defined under the "transformations" element of the matched rule as specified in Appendix C.

While a Location subscription is active, the Subscription Authorization Rules may be modified. After that the Location Server SHALL re-evaluate the subscription state for each Location Client based on the new Subscription Authorization Rules. For example, the Subscription Authorization Rules may be changed to block subscriptions from a Location Client. If the Location Client has an active subscription to the Target's Location Information, the Location Server terminates the subscription and blocks any future subscription requests from this Location Client.

Furthermore, while a Location Client's subscription is active, a Target may update its Location Privacy Rules. The Location Server SHALL re-determine the subset of the Target's Location Information the Location Client is allowed to receive.

The Location Server MAY determine that the Subscription Authorization and/or Location Privacy Rules have been updated by subscribing to changes made to XML documents stored in the Location Policy XDMS.

5.2.1.2 Applying Event Notification Suppression

The Location Server supports event notification suppression according to the procedures described in [RFC5839] and [IETF-EventRate], as summarized in this section.

If the Location Server receives a SUBSCRIBE request within an established dialog that includes a wildcarded Suppress-If-Match header field using the special "*" entity-tag value as described in [RFC5839] “Suppressing NOTIFY Requests”, the Location Server suppresses the generation of event notifications until a Location Client cancels the suppression with a re-SUBSCRIBE request including a Suppress-If-Match header set to other than the special “*” Entity-tag.

If the Location Server receives a SUBSCRIBE request that includes a “max-rate” parameter set to a value that is equal or greater than the remaining subscription expiration value as described in [IETF-EventRate] “Selecting the maximum rate”, the Location Server suppresses the generation of event notifications until the subscription interval elapses or until the Location Client sends a re-SUBSCRIBE request or a 200-class response to a NOTIFY request that does not include a “max-rate” Event header field parameter or that includes a “max-rate” parameter value that is less than the remaining subscription expiration value.

5.2.1.3 Location QoS Handling

The Location Server SHOULD support required location QoS parameters handling according to the following procedures:

- Location QoS validation, according to the procedures described in section 5.1.5,
- Location QoS document described in section 11 and
- Content type ‘application/location-qos+xml’, according to section 5.1.5.

If the Location Server supports location QoS handling and

- understands the location QoS parameters included in the body of the SUBSCRIBE request using the content type ‘application/location-qos+xml’, the Location Server SHALL take the requested location QoS into consideration when determining the location of the Target. E.g, the cached location data shall not be used if the Location Client requests the current location.
- does not understand the particular location QoS parameters included in the body of the SUBSCRIBE request, the Location Server SHALL indicate it to the Location Client with a SIP 488 (Not Acceptable Here) error response.
- the requested QoS class is “Assured”, the Location Server SHALL validate if the available Location Information fulfills the required QoS and
    a. if the available Location Information fulfills the QoS requirements, the Location Server SHALL continue the next step of event notification processing.
    b. if the available Location Information doesn’t fulfill the QoS requirements, the Location Server SHALL discard the Location Information. If the Location Client requires an immediate response (e.g. one-time subscription), the Location Server SHALL generate a NOTIFY request with an empty or neutral body.
- the requested QoS class is not “Assured”, the Location Server SHALL ignore QoS validation procedure and continue event notification handling procedures in order to deliver the Location Information to the Location Client.
- the requested QoS class is “Emergency”, the location requests SHOULD have priority over any other type of location requests. The adherence to other QoS parameters is not defined.
- the location type parameter is not present in Location QoS document, Location Server SHOULD respond with location information in any format: geodetic, civic or both.

- the maximum uncertainty parameter is present in Location QoS document, the Location Server SHALL attempt to satisfy or approach as closely as possible the requested maximum uncertainty when other location QoS parameters are not in conflict.
- the maximum uncertainty parameter is not present in Location QoS document, the Location Server MAY include Location Information with any uncertainty as long as requirements defined with other QoS parameters are fulfilled.
- the maximum response time parameter is present in Location QoS document, the Location Server SHALL attempt to satisfy or approach as closely as possible the requested response time when other location QoS parameters are not in conflict.
- the maximum response time parameter is not present in Location QoS document, the Location Server MAY respond with Location Information at any time as long as requirements defined with other QoS parameters are fulfilled.
- the maximum age parameter is present in Location QoS document, the Location Server SHALL attempt to satisfy or approach as closely as possible the requested age when other location QoS parameters are not in conflict.
- the maximum age parameter is not present in Location QoS document, the Location Server SHOULD include the latest Location Information (of any age) as long as requirements defined with other QoS parameters are fulfilled.

5.2.1.4 Applying Location Event Notification Filtering

Location event notification filtering is a mechanism for the Location Client to control the content and triggers of notifications.

The Location Server SHALL support location event notification filtering document and procedures described in section 10.

If the Location Server understands the particular filter included in the body of the SUBSCRIBE request using the content type ‘application/location-delta-filter+xml’, the Location Server SHALL apply the requested filter. As a result, the authorized Location Clients are notified of the actual Location Information after first applying the privacy filtering procedures as described in section 5.2.1.1, followed by the event notification filtering procedures described in this section. The Location Information used to evaluate the filter criteria SHALL fulfill the maximum uncertainty and maximum age parameters if included in QoS document in the SUBSCRIBE. If the Location Server does not understand the particular filter included in the body of the SUBSCRIBE request, the Location Server SHALL indicate it to the Location Client with response code 488 “Not Acceptable Here”.

5.2.1.5 Generating Entity Tags

The Location Server SHALL support the notifier procedures defined in [RFC5839]. The Location Server:

- SHALL generate entity tags for location documents. The entity tag SHALL be unique to the Presence Information Data Format Location Object (PIDF-LO) document over time, i.e., the Location Server SHALL generate the same entity tag for the same PIDF-LO document in different time samples. The algorithm to generate such entity tags is out of scope of this specification.
  NOTE: The PIDF-LO document here refers to the document generated after “Event Notification Filtering”.
- SHALL include the entity tag in all NOTIFY requests as described in [RFC5839].

5.2.1.6 Applying Event Notification Rate Control

The Location Server SHALL support Location Client requested notification rate control. If supported, the Location Server SHALL follow the notifier procedures for maximum rate and minimum rate as described in [IETF-EventRate].

5.2.1.7 Generation of Notifications

At the last step of subscription to Location Information processing, the Location Server SHALL generate new NOTIFY requests for each Location Client and transmit each of those to the respective Location Client when the content of the new notification is different from the last one that was transmitted to the Location Client.

The Location Server SHALL support the notifier procedures defined in [RFC5839].If the Location Client requested condition for suppressing a NOTIFY request or a NOTIFY request body evaluates to true, the Location Server suppresses the NOTIFY request or the NOTIFY request body appropriately as described in [RFC5839].

The Location Server SHALL set the “entity” attribute of the <presence> element included in the NOTIFY request to the same URI as the one used in the Request-URI of the received SUBSCRIBE request.

The Location Server SHALL reflect back the “Priority" header in the NOTIFY requests, e,g, set the value of “Priority” header to “emergency” for the emergency location subscription.

5.2.1.7.1 Handling of Large MIME Objects

The Location Server MAY generate notifications using the ‘multipart/related’ content type in accordance with [RFC2387], if:

- the Location Information formatted as ‘application/pidf+xml’ includes references to other MIME objects; and
- the Location Client indicates support for the ‘multipart/related’ content type using the Accept header field in the SUBSCRIBE request.

If the Location Client does not indicate support for the ‘multipart/related’ content type or a MIME object cannot be accessed by the Location Server, the Location Server SHOULD exclude the MIME object from the notification.

5.2.2 XDM Functions

Certain Location Server functionality depends on particular XML documents stored in XDMS. In order to provide this functionality the Location Server:

- SHALL support retrieval of XML documents stored in the XDMS, according to [XDM_Core] “Document Management”;
- SHALL support LOCSIP XDMS Application Usage as specified in Appendix C, and the URI List Application Usage specified in [XDM_List] “URI List”;
- MAY subscribe to changes made to XML documents stored in the XDMS. If so, the Location Server SHALL follow the procedure defined in [XDM_Core] “Subscribing to Changes in the XML Documents”.

5.2.3 Handling of PIDF Documents

The PIDF document contained in the SIP Notify message SHALL include the timestamp element indicating the date and time the document is created. The timestamp is the time at the last validated position results included in the document location information.

Note: The error procedures for a missing timestamp are out-of-scope. The Location Client may error or use the location information per implementation.

5.3 Resource List Server

LOCSIP reuses the Resource Location Server (RLS) entity from OMA Presence SIMPLE framework. The RLS enables a Location Client to subscribe the Location Information of multiple Targets using a single subscription.

The RLS in LOCSIP SHALL support all functions and procedures described in [PRS_SPEC] “Resource List Server”, with the following clarifications:

The following functions are supported by Presence RLS but not used in LOCSIP:

1) Request-contained Home Subscription Information Lists as described in section 5.6 in [PRS_SPEC].
2) View Sharing procedures as described in section 5.6.2 in [PRS_SPEC].

3) Partial Notification for Back-end subscription as described in 5.6.2 in [PRS_SPEC].
4) Content indirection mechanism as described in 5.6.2 in [PRS_SPEC].
5) The compression of the Body in a Notify Request as described in section 5.6.7.2 in [PRS_SPEC].

The following functions are LOCSIP specific extensions and SHALL be supported by RLS:

1) Accept the SUBSCRIBE request with feature tag for location service (as described in Appendix D) and include it in the back-end subscription to Location Server.
2) Support content type 'application/location-delta filter+xml" and the event notification filtering procedures, according to the procedures described in section 5.1.3.
3) Support the handling of Location QoS document according to rules in section 5.1.8. The maximum age of Location Information in Location QoS SHOULD be taken into consideration when applying Event Notification Rate Control.

5.4 XDM Client

The XDMC SHALL support the following:

- XDMC procedures described in [XDM_Core] "Procedures at the XDM Client"
- Subscription Authorization Rules and Location Privacy Rules authorization as specified in Appendix C
- URI List Application Usage as specified in [XDM_List] "URI List".

5.5 Location Policy XDMS

The Location Policy XDMS SHALL support the XDMS procedures described in [XDM_Core] *"Procedures at the XDM Server"* and the Application Usages described in Appendix C.

5.6 RLS XDMS

The RLS XDMS SHALL support the XDMS procedures described in [XDM_Core] *"Procedures at the XDM Server"* and the Application Usages described in [PRS_RLSXDM].

5.7 Shared List XDMS

The Shared List XDMS SHALL support the XDMS procedures described in [XDM_Core] *"Procedures at the XDM Server"* and the Shared List XDM Application Usages described in [RFC5367].

5.8 Home Subscription Agent

LOCSIP reuses the Home Subscription Agent (HSA) entity from OMA Presence SIMPLE framework.

The HSA SHALL support the service authorization and traffic optimization for location subscriptions, according to the procedures described in [OMA-PRS_HSA] "Home Subscription Agent", with the following clarifications:

The following functions are supported by Presence HSA but not used in LOCSIP:

1) The event notification suppression as described in section 5.3 in [OMA-PRS_HSA].

The HSA SHALL support the following LOCSIP specific extensions:

- Accept the SUBSCRIBE request with the feature tag for location services (as described in Appendix D), and include it in requests towards Location Server.

- Ignore the service authorization and prioritize the incoming subscriptions based on the value of "Priority" header in the SUBSCRIBE request.

5.9 GPM

In order to enforce the privacy of the Location Information, LOCSIP MAY use the Global Permission Management (GPM) enabler as defined in [OMA GPMTS].

5.9.1 Authorization and Privacy Rules

Since GPM does not implement a notification mechanism, LOCSIP SHALL check the authorization and privacy rules at least whenever it:

- receives a subscription or a subscription refresh
- sends a notification with location information

5.9.2 Input template

The request to the GPM must follow the input template defined in [GPM INPUT TEMPLATE XSD] with the following precisions:

The value of the consumerID SHALL convey the identity to be matched to the <identity> element of the Authorization and Privacy Rules document.

The requestedAttributes element SHALL contain only one <targetAttributeName> element. The value of the <targetAttributeName> element SHALL be set to: oma_location.

5.9.3 Output template

The request to the GPM must follow the output template defined in [GPM OUTPUT TEMPLATE XSD] with the following precisions:

In case the "decision" attribute of the <permissionsResult> element returned in the output template is set to "GRANT" , the output template MAY contain additional information.

The additional information MAY contain

- a <location-condition> element, as defined in Appendix C.1.1. In that case, LOCSIP SHALL return the location information only if the condition is met. Data semantics as defined in C.1.7 apply to this element
- a <transformations> element as defined in Appendix C.1.1. Those transformations SHALL be applied before returning location information. Data semantics as defined in C.1.7 apply to this element.

5.9.4 Output template XML Schema

The schema for the additional information in the GPM output template is defined in [XSD-locGPMExt].

6. Security

The security mechanism is divided into SIP signaling security and User Plane security. SIP signaling security relies on mechanisms provided by the underlying SIP/IP Core. User Plane security that is provided by an additional mechanisms to ensure confidentiality. Integrity and message authentication are not needed since they are assumed to be provided by the underlying SIP/IP Core. The mechanism used for User Plane security in LOCSIP is XML symmetric encryption [XMLENC] in combination with two types of key management schemes: symmetric-based and public key-based.

Figure 1 below illustrates the LOCSIP security reference architecture that will be used in the rest of this section.

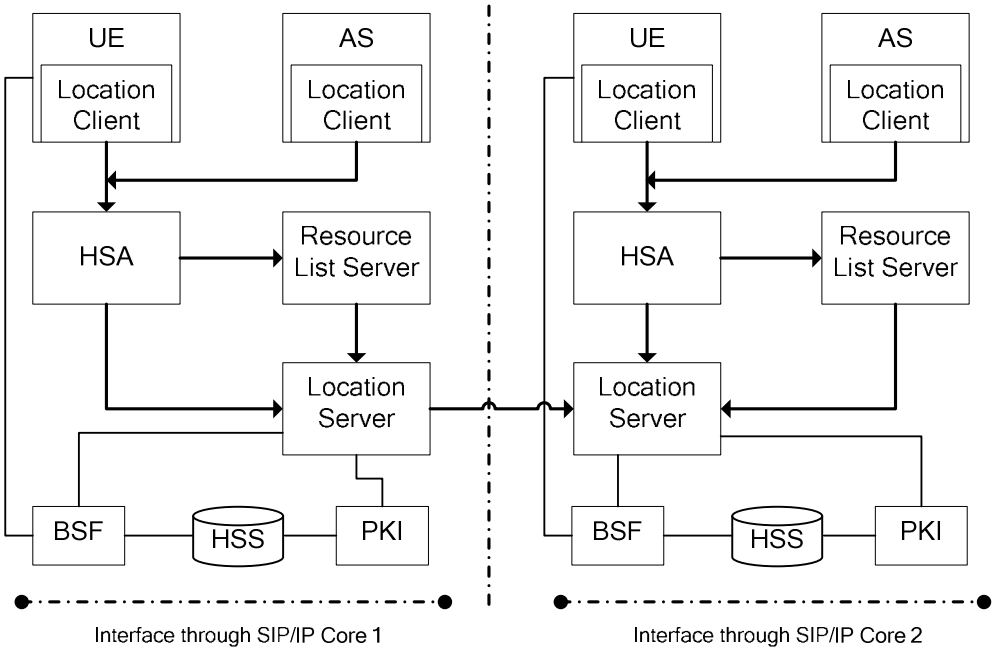

Figure 1: LOCSIP Security Architecture

The right side of the figure shows SUBSCRIBE requests within the same domain, i.e. when the location client (LC) – UE-based or AS-based- subscribes to locate a specific target from the same domain. In such a case, the LC sends the SUBSCRIBE request to the Location Server over SIP/IP core 2. For subscription to a group registered in the same domain as the LC, the SUBSCRIBE request is handled via the RLS. For group Targets in the same domain, the RLS forwards the SUBSCRIBE request to the LS over SIP/IP Core 2.

The left side of the picture shows SUBSCRIBE requests across domains, i.e. when the location client (LC) – UE-based or AS-based- subscribes to locate a specific target from other domain. In such a case, the LC sends the SUBSCRIBE request to its LS over SIP/IP Core 1 that in turn forwards the SUBSCRIBE to the LS in the other domain using a separate security relation. The same procedure applies for subscription to a group Targets registered in another domain, i.e. the RLS sends the subscription request to the LS. The only communication across domains is between the LS in SIP/IP cores 1 and the LS in SIP/IP cores 2.

6.1 SIP Signaling Security

The LS, HSA or RLS SHALL authenticate all incoming SIP requests. The LS, HSA or RLS SHOULD rely on the authentication mechanisms provided by the underlying SIP/IP Core to accomplish user identity verification.

When the SIP/IP Core corresponds with 3GPP IMS or 3GPP2 MMD networks the authentication mechanism SHALL be as specified in [3GPP-TS_33.203] / [3GPP2-S.R0086], and:

- the LS, HSA or RLS SHALL authenticate the SIP request originator as specified in [3GPP-TS_24.229] / [3GPP2-X.S0013-004] section 5.7.1.4 and
- the HSA or RLS SHALL, when acting on behalf of the Location Client, populate security related SIP header fields according to the procedures given in [3GPP-TS_24.229] / [3GPP2-X.S0013-004] section 5.7.3.

An AS acting as originating UA SHALL follow the authentication procedures given in [3GPP-TS_24.229] / [3GPP2-X.S0013-004] section 5.7.3.

The access level security mechanism SHALL be provided by the SIP/IP Core to support integrity and confidentiality protection of SIP signaling.

When the SIP/IP Core corresponds with 3GPP IMS or 3GPP2 MMD networks, the integrity and confidentiality protection mechanism is specified in [3GPP-TS_33.203] / [3GPP2-S.R0086].

6.2 User Plane Security

User Plane security is in LOCSIP applied to the Location Information document as defined in section 9 that is carried in the body of SIP NOTIFY messages.

Confidentiality is achieved by use of XML encryption [XMLENC]. The keys for the XML encryption are managed by two key management schemes, public key-based and GBA-based. The public key–based scheme is used for conveyance of location info from the LS to an AS acting as LC. The GBA-based scheme is used for conveyance of location info from the LS to a terminal acting as LC. The RLS and HSA are not active in the User Plane security function but the Location Information documents are passed transparently through the RLS.

An LC SHOULD be mutually authenticated with any LS sending Location Information to the LC.

A LS SHOULD be mutually authenticated with any LS in another SIP/IP Core sending Location Information to the LS.

The Location documents included in SIP NOTIFY SHOULD be encrypted using XML encryption as specified in [XMLENC]. The encryption shall be performed using keys as specified in section 6.2.1 to 6.2.6.

6.2.1 Terminal acting as Location Client

The SEC-CF [OMA SEC CF] describes how 3GPP GBA/GAA can be used to establish a security association between a client and a server over HTTP. As LOCSIP relies purely on SIP, a SIP-binding for the same procedures is needed. A new GBA Ua Security Protocol Identifier is needed.

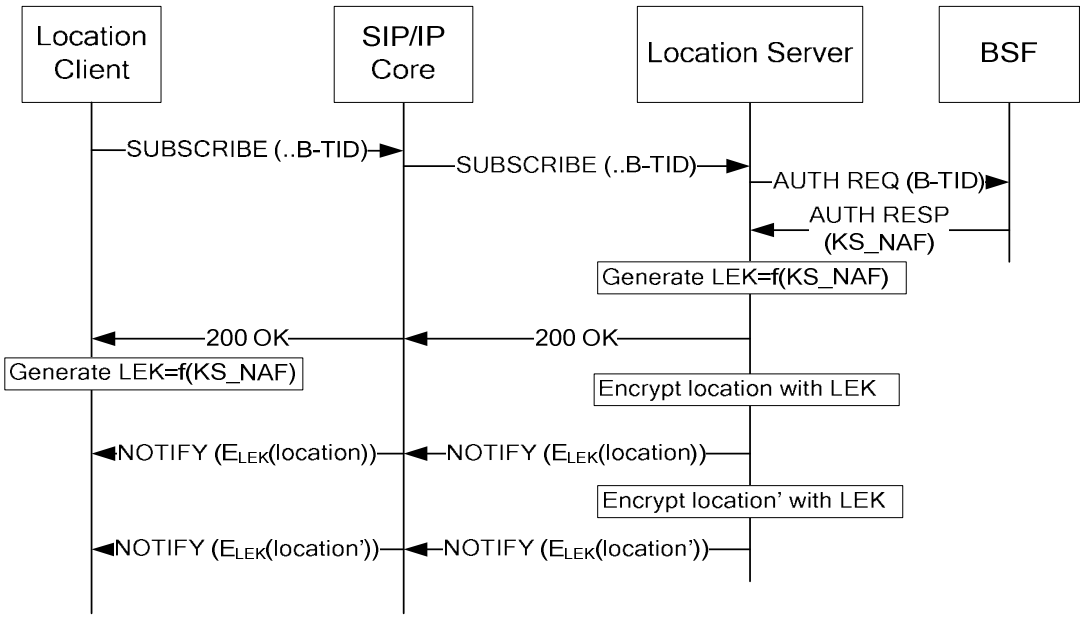

Figure 2: LS initiation with authentication and GBA-based key derivation

Figure 2 describes the security procedures for GBA-based key establishment over SIP. This procedure assumes that both Terminal LC and BSF have previously established a valid Ks and B-TID using GBA according to SEC_CF. The LC SUBSCRIBE contains the corresponding B-TID. The LS authorizes the LC by acquiring the corresponding KS_NAF from the BSF. The KS_NAF is used to derivate the Location Encryption Key (LEK) both on the network-side and on the LC after the SIP 200 OK reply. The LEK is used later to protect the location information including its updates location'.

The function to derivate the LEK using KS_NAF is described in section 6.2.6.2.

For an example of an XML document containing the encrypted location see section 6.2.6.3.

6.2.2 AS acting as Location Client

In this case, we assume that both LC-AS has been provisioned with a public/private key pair or a digital certificate. The LC public key LC_PK or its digital certificate is made known to the LS at subscribe time. The LC_PK or digital certificate is used by the LS to encrypt the LEK and securely transport it to the LC.

Figure 3 shows how the LEK is transported in-bound together with the encrypted location.

For an example of an XML document containing the encrypted location see section 6.2.6.3.

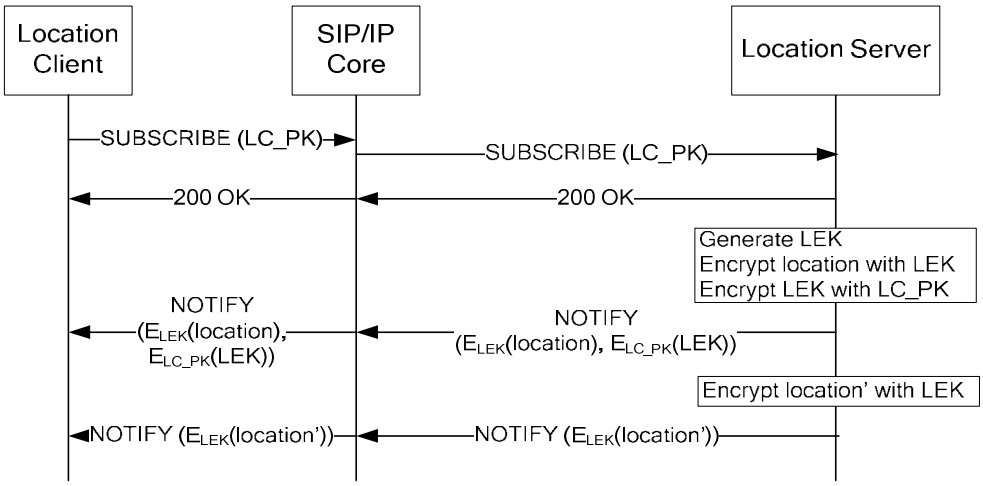

Figure 3 LS initiation with in-bound public key-based key establishment

6.2.3 LS acting as Proxy to other domain

This case covers the scenario that the LSforwards the requests to and from a LS in another domain. In this case, we assume that both the LS have been provisioned with a public/private key pair or digital certificate and the public key/certificate is made known to the LS upon SUBSCRIBE. The LS public key/certificate LS_PK is used by the LS to encrypt the LEK and securely transport it.

Figure 4 shows how the LEK is transported in-bound together with the encrypted location.

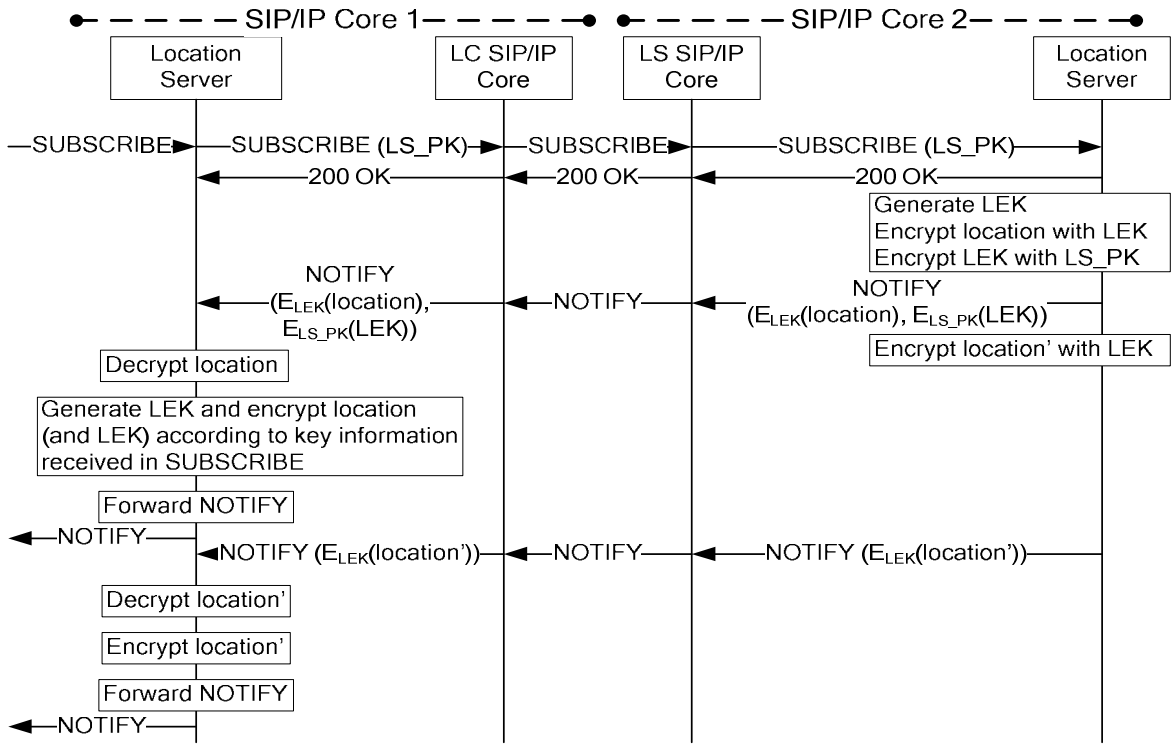

Figure 4 LS initiation with public key in-bound public key-based key establishment

6.2.4 Location List (Group) Subscription

When an LC needs to perform a Location List (group) subscription, the RLS will act on behalf of the LC, sending multiple subscription requests to the corresponding LS routing back the responses, including LEK.

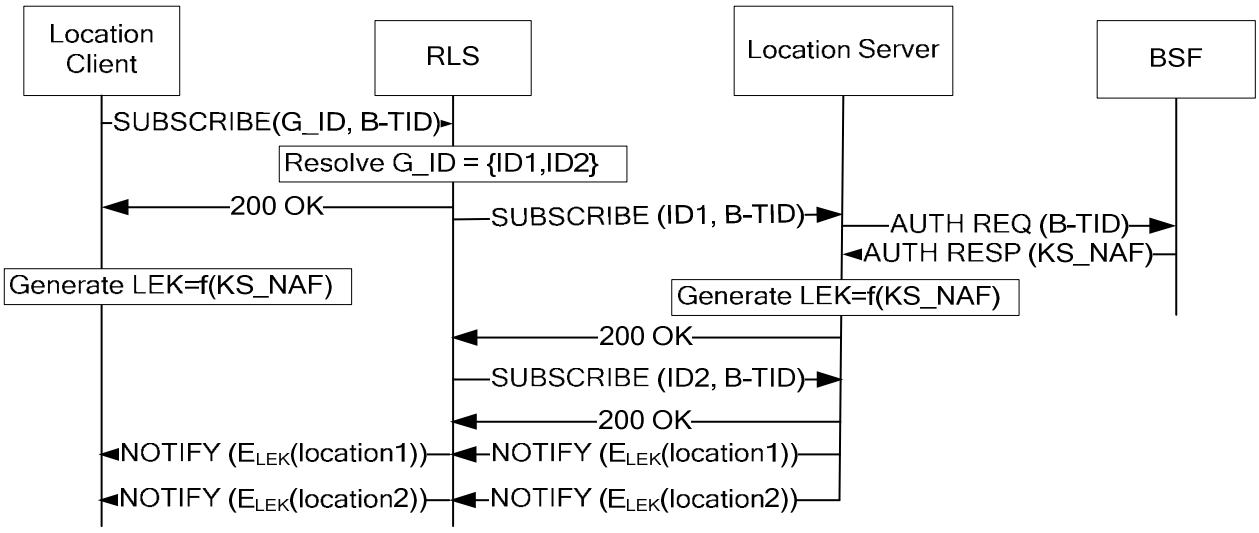

Figure 5 LS initiation with authentication and GBA-based key derivation for Location List Subscription

Figure 5 illustrates the subscription to a group – identified by G_ID consisting of two targets ID1 and ID2- when the LC is a terminal. We assume that the LC has performed a GBA bootstrap. The very first SUBSCRIBE arriving to the LS from a given LC will trigger a contact to the BSF to fetch the corresponding KS_NAF based on the B-TID and LEK derivation from KS_NAF. Further SUBSCRIBE requests to the same LS with the same B-TID would be acknowledged. Note that the LEK is per LC, i.e. it is used for encrypting all locations of Targets to which a given LC has subscribed to. Note also that the RLS is transparent to the security procedures.

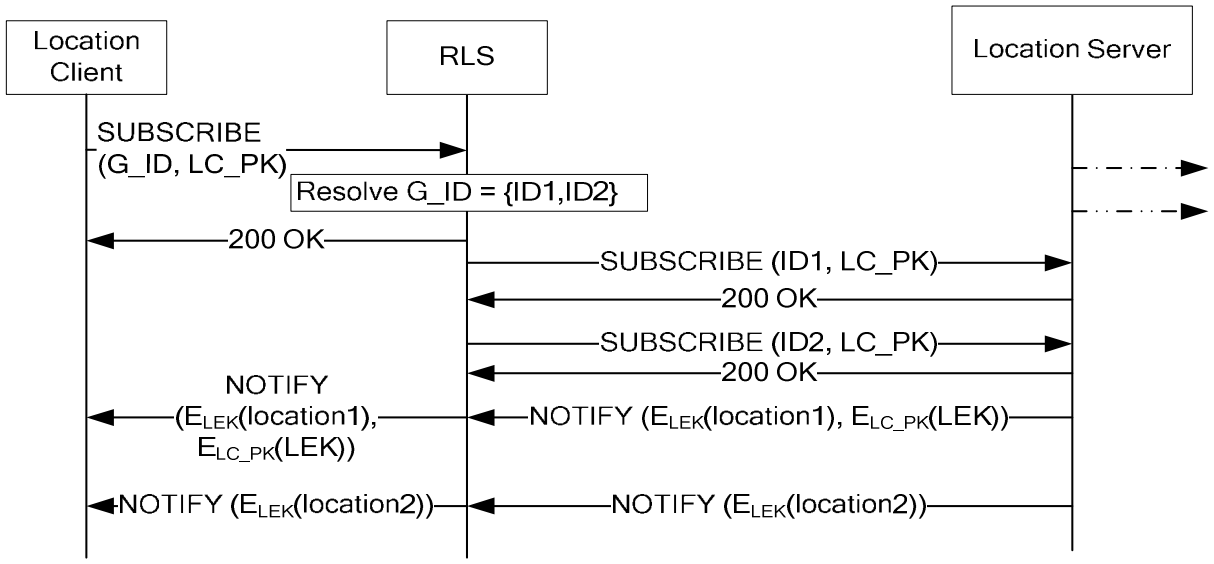

Figure 6 LS initiation with public key and in-bound public key-based key establishment

Figure 6 illustrates the subscription to a group – identified by G_ID consisting of two targets ID1 and ID2- when the LC is an AS. We assume that the LC has made its public key or certificate available to the LS. Only the first NOTIFY message to the same LS from the same LC would be responded with the LEK encrypted under the LC_PK. Further NOTIFY messages would only carry the encrypted location, Note that the RLS is mainly transparent to the security procedures. The same LEK is used for protecting further Location information, for any Target between said LC and LS.

6.2.5 Multiple LC: Terminal-based and AS-based

When the LS needs to send location to both types of LC, terminal- and AS-based, for security reasons, different Location Encryption Keys shall be used for each LC. The reason is that using the same LEK for two different LC would allow one of them to be able to continue decrypting locations after its subscription is finished. The LEK itself is derivated using the KS_NAF or distributed with key transport using public key LC_PK depending on their type, terminal-based or AS-based respectively.

6.2.6 Key Management Considerations

6.2.6.1 LOCSIP GBA Protocol Identifier

The Ua security protocol identifier that shall be used for LOCSIP is declared in OMNA GBA Protocol Identifier Registry [OMNA].

6.2.6.2 LEK Key Derivation and Refreshment

The LEK shall be derived from the key Ks_NAF using the GBA key derivation function (see Annex B of [3GPP TS 33.220]) as follows (see notation style is explained in Annex B of [3GPP TS 33.220]):

- FC = 0x01
- P0 = "locsip-lek" (i.e. 0x6C 0x6F 0x63 0x73 0x69 0x70 0x2D 0x6C 0x65 0x6B), and
- L0 = length of P0 is 10 octets (i.e. 0x00 0xA).

The Key to be used in key derivation shall be:

- Ks_NAF (i.e. NAF specific key) as specified in [3GPP TS 33.220].

In summary, the LEK shall be derived from the Ks_NAF and static string "locsip-lek" as follows:

- LEK = KDF (Ks_NAF, "locsip-lek")

The handling of LEK lifetime and refreshment SHALL follow the GBA procedures specified in [3GPP TS 33.220]

6.2.6.3 Using XML Encryption

If User Plane security is required, the LS SHALL encrypt the Location Information using the keys corresponding to the specific LC. When a LC resides on a terminal, the LC SHALL include B-TID in the SUBSCRIBE requests. The format of key document is defined in [XSD-locGBAKeyid]. The MIME type for this format is “application/location-gbakey-id+xml”.

When an AS acting as a LC, the LS MUST know LC’s public key or its digital certificate before the subscription. It is assumed that the necessary infrastructure for certificate management (e.g. certificate discovery, validation, revocation) is in place and thus it is out of the scope of this specification

The encryption of Location Information SHALL conform to XML encryption [XMLENC] with the following clarifications:

- Only the LEK and Location Information elements contents MUST be encrypted.
- The LEK MUST be protected using the XML EncryptedKey element together with an identifier Id and KeyName in order for the LC to be able to later locate the key corresponding to a received encrypted Location Information.
- Location Information MUST be protected using the XML EncryptedData element.
- For confidentiality the algorithms RSA and AES128 MUST be supported.
- When the LEK is encrypted, it MUST be done by asymmetric key RSA-1_5.

The encrypted data is included in the “location-info” element within a PIDF-LO document defined in [RFC4119]. The format of encrypted data is defined in [XMLENC].

An example of location encryption for a terminal acting as a Location Client:

```
<presence xmlns="urn:ietf:params:xml:ns:pidf"
  xmlns:gp="urn:ietf:params:xml:ns:pidf:geopriv10"
  entity="sip:geotarget@example.com”>
  <person id="chm1345">
      <gp:geopriv>
         <gp:location-info>
            <enc:EncryptedData xmlns:enc="http://www.w3.org/2001/04/xmlenc#"
   Type="http://www.w3.org/2001/04/xmlenc#Element">
               <enc:EncryptionMethod
   Algorithm="http://www.w3.org/2001/04/xmlenc#tripledes-cbc"/>
               <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
```

```
                  <ds:KeyName>Location Encryption Key</ds:KeyName>
               </ds:KeyInfo>
               <enc:CipherData>
                  <enc:CipherValue>abcdefg</enc:CipherValue>
               </enc:CipherData>
            </enc:EncryptedData>
         </gp:location-info>
         <gp:usage-rules>
            <gb:retransmission-allowed>no</gp:retransmission-allowed>
            <gb:retention-expiry>2003-06-23T04:57:29Z</gp:retention-expiry>
         </gp:usage-rules>
      </gp:geopriv>
    <timestamp>2009-01-22T20:58:31Z</timestamp>
  </person>
</presence>
```

An example of location encryption for an AS acting as Location Client:

```
<presence xmlns="urn:ietf:params:xml:ns:pidf"
  xmlns:gp="urn:ietf:params:xml:ns:pidf:geopriv10"
  entity="sip:geotarget@example.com”>
   <person id=" bgt4367">
         <gp:geopriv>
            <gp:location-info>
               <xenc:EncryptedData xmlns:enc="http://www.w3.org/2001/04/xmlenc#
  Type="http://www.w3.org/2001/04/xmlenc#Element" >
                  <enc:EncryptionMethod
  Algorithm="http://www.w3.org/2001/04/xmlenc#aes128-cbc"/>
                  <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                     <enc:EncryptedKey>
                        <enc:EncryptionMethod
  Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-1_5"/>
                           <ds:KeyInfo
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                              <ds:KeyName>LEK Transport</ds:KeyName>
                           </ds:KeyInfo>
                           <enc:CipherData>
                <enc:CipherValue>qZk+NkcGgWq6PiVxeFDCbJzQ2J0=</enc:CipherValue>
                           </enc:CipherData>
                     </enc:EncryptedKey>
                  </ds:KeyInfo>
                  <enc:CipherData>
                    <enc:CipherValue>abcdefg</enc:CipherValue>
                  </enc:CipherData>
               </xenc:EncryptedData>
            </gp:location-info>
```

```
            <gp:usage-rules>
              <gp:retransmission-allowed>no</gp:retransmission-allowed>
              <gp:retention-expiry>2003-06-23T04:57:29Z</gp:retention-expiry>
            </gp:usage-rules>
         </gp:geopriv>
      <timestamp>2009-01-22T20:58:31Z</timestamp>
   </person>
</presence>
```

7. Charging

When the SIP/IP Core network corresponds with 3GPP IMS or 3GPP2 MMD networks, the online or offline charging SHOULD be performed according to [3GPP TS 32.240] [3GPP TS 32.260] for 3GPP and [3GPP2-X.S0013-007] [3GPP2-X.S0013-008] for 3GPP2.

In the context of other realizations of the SIP/IP Core network, similar charging functions SHOULD be provided.

8. Registration

When the SIP/IP Core corresponds with 3GPP IMS or 3GPP2 MMD networks, the Location Client implemented in a Terminal SHALL use the 3GPP IMS or 3GPP2 MMD networks registration mechanisms as defined in [3GPP-TS_24.229] / [3GPP2-X.S0013-004].

In a non-3GPP/3GPP2 network, this document has no requirement regarding the SIP registration procedures.

9. Content of the Location Information Document

9.1 Location Object Definition

The Presence Information Data Format Location Object (PIDF-LO) defined in [RFC4119] is the recommended way of encoding location information and associated privacy rules. The location information in a PIDF-LO may be described in a geospatial manner based on a subset of GMLv3 defined in [GeoShape], or as civic location information defined in [RFC4119] and [RFC5139].

Uses for PIDF-LO are envisioned in the context of numerous location based applications. In order to ensure interoperability, the implementations SHALL comply with the rules and recommendations defined in [RFC4479] and [RFC5491].

9.2 Location Information Element Semantics

The [LOCSIP-RD] specifies a set of building blocks of Location Information that needs to be supported by the LOCSIP enabler and their semantics.

The following sections describe the mapping of those location information building blocks initially to some presence data model components and then to some element of PIDF-LO [RFC4119], or one of its extensions (e.g. geographical location [RFC5491], and civic location [RFC5139]).

The mandatory instance identifier "id" attribute in the <person>, <device> and <tuple> elements of a presence document serves no other purpose than to syntactically distinguish between the elements.

9.2.1 Location Information

9.2.1.1 Description

The "Location Information" building block indicates the Target's location. It could be either a geographical location or civic address.

9.2.1.2 Mapping to presence data model

The "Location Information" is part of the "geopriv" object for "person" and/or "device" components according to the presence data model.

9.2.1.3 Mapping to PIDF

The "Location Information" building block SHALL be mapped to PIDF as follows, based on [RFC4479]:

- <person> →<geopriv> → <location-info> and/or
- <device> →<geopriv> → <location-info>.

The <location-info> element is based on [RFC4119] and is further refined as described in Section 9.1. A <location-info> element may contain one or more chunks of location information.

9.2.1.4 Location Client Processing

The Location Client SHALL follow the rules relating to the <location-info> element defined in [RFC5491].

9.2.1.5 Limitations

None.

9.2.2 Usage Rules

9.2.2.1 Description

The “Usage Rules” building block indicates the privacy preference associated to the Location Information.

9.2.2.2 Mapping to presence data model

The “Usage Rules” is part of the “geopriv” object for “person” and/or “device” components according to the presence data model.

9.2.2.3 Mapping to PIDF

The “Usage Rules” building block SHALL be mapped to PIDF as follows:

- <person> → <geopriv> → <usage-rules> and/or
- <device> → <geopriv> → <usage-rules>.

The <usage-rules> element is defined in [RFC4119].

9.2.2.4 Location Client Processing

The Location Client SHALL follow the privacy rules associated with the Location Information.

9.2.2.5 Limitations

None.

9.2.3 Method

9.2.3.1 Description

The “Method” building block indicates the way that the location information was determined.

9.2.3.2 Mapping to presence data model

The “Method” is part of the “geopriv” component according to PIDF-LO definition.

9.2.3.3 Mapping to PIDF

The “Method” building block SHALL be mapped to PIDF-LO as follows:

- <person> → <geopriv> → <method> and/or
- <device> → <geopriv> → <method>.

The <method> element is defined in [RFC4119].

9.2.3.4 Location Client Processing

Implementations MUST limit the use of this method to the values shepherded by IANA.

9.2.3.5 Limitations

None.

9.2.4 Provided-by

9.2.4.1 Description

The "Provided By" building block indicates the entity or organization that supplied this location information.

9.2.4.2 Mapping to presence data model

The "Provided By" is part of the "geopriv" component according to PIDF-LO definition.

9.2.4.3 Mapping to PIDF

The "Provided By" building block SHALL be mapped to PIDF-LO as follows:

- <person> → <geopriv> → <provided-by> and/or
- <device> → <geopriv> → <provided-by>.

The <provided-by> element is defined in [RFC4119].

9.2.4.4 Location Client Processing

The values for the <provided-by> element MUST be IANA-registered XML namespace. A single XML namespace for <provided-by> is pre-registered in [RFC4119] Appendix A.

9.2.4.5 Limitations

None.

9.3 OMA LOCSIP Specific PIDF Extensions

None

10.Content of the Location Filter Document

10.1 The ‘enter’ and ‘exit’ filter events

The ‘enter’ filter event is satisfied when the Target enters (or re-enters) a 2-dimensional region described by one of the shapes defined in section 5 of [RFC5491]. The ‘exit’ filter event is satisfied when the Target exits (or re-exits) a 2-dimensional region described by one of the shapes defined in section 5 of [RFC5491]. These regions can be defined using inline snippets of GML, or externally referenced using a URI (Uniform Resource Identifier).

Any 2-dimensional region MUST be defined using the EPSG 4326 coordinate reference system. A location-filter document can contain more than one enter or exit filter events.

Following is an example of a ‘enter’ filter which defines that notification is sent when Target enters a 2-dimensional area:

```
<location-filter>
     <enter>
          <gml :extentOf>
            <gml :Polygon srsName= »urn :ogc :def :crs :EPSG ::4326 » xmlns
  :gml= »http ://www.opengis.net/gml »>
              <gml :exterior>
                <gml :LinearRing>
                  <gml :posList>
                       37.41188 -121.93243
                       37.41142 -121.93243
                       37.41142 -121.93132
                       37.41188 -121.93132
                       37.41188 -121.93243
                  </gml :posList>
                </gml :LinearRing>
              </gml :exterior>
            </gml :Polygon>
          </gml:extentOf>
     </enter>
   </location-filter>
```

10.2 The ‘inRange’ and the ‘outOfRange’ filter events

The ‘inRange’ and the ‘outOfRange’ are more advanced location filters where relative distance from specified Target is taken into account. The ‘inRange’ filter event triggers notification when relative distance from the specified Target to any secondary target specified in the filter is less than defined distance. The ‘outOfRange’ filter event triggers notification when distance from specified Target to any secondary target specified in the filter exceeds the defined value. Each secondary target is specified with “uri” attribute value of “entry” element. The distance is specified as a value of “distance” element. The “distance” element has attribute “uom” (for “units of measure”) which indicates the units of the element. The default unit is meters. The Location Server may utilize Location Information determined at different time instances when evaluating this filter condition. In such case, the time difference SHALL be less or equal to the maximum age parameters if included in QoS document in the SUBSCRIBE.

Following example illustrates a ‘inRange’ filter which will send location notification each time a Target distance from the single secondary Target specified in the filter (identified with URI sip:alice@operator.com) is less than 1000 meters:

```
<location-filter>
```

```
    <inRange>
        <entry uri=”sip:alice@operator.com”/>
        <distance uom=”urn:ogc:def:uom:EPSG::9001”>1000</distance>
    </inRange>
  </location-filter>
```

10.3 The ‘movedHoriz’ and the ‘movedVert’ filter events

The ‘movedHoriz’ and ‘movedVert’ filter event are satisfied when the Target has moved the specified horizontal or vertical distance since last notification. The ‘movedHoriz’ and ‘movedVert’ elements have attribute “uom” (for “units of measure”) which indicates the units of the element. The default unit is meters

Following is an example of combined ‘movedHoriz’ and ‘movedVert’ filter which defines that notification is sent when Target has moved 20 meter in horizontal direction or/and has moved 3 meter in vertical direction:

```
<location-filter>
  <movedHoriz uom="urn:ogc:def:uom:EPSG::9001">20</movedHoriz>
  <movedVert uom="urn:ogc:def:uom:EPSG::9001">3</movedVert>
</location-filter>
```

10.4 The ‘speedExceeds’ filter events

The ‘speedExceeds’ filter event is satisfied when the Target exceed the specified horizontal speed. The ‘speedExceeds’ elements has attribute “uom” (for “units of measure”) which indicates the units of the element. The default unit is meters per second.

Following is an example of a ‘speedExceeds’ filter which defines that notification is sent when Target speed exceeds 3 meters per second:

```
<location-filter>
  <speedExceeds uom="http://aurora.regenstrief.org/~ucum/ucum.html
#m/s">3</speedExceeds>
</location-filter>
```

10.5 The ‘valueChanges’ filter events

The valueChanges filter event contains a string which is interpreted as an XPath [W3C.REC-xpath-19991116] expression evaluated within the context of the location-info element of the PIDF-LO document which would be generated by the notification. The XPath expression MUST evaluate to only a single Xpath node. If the value of any of the elements in the resulting node changes then the filter event is triggered. Note that the value of the resulting node changes if any of those nodes or subnodes transitions from having a value to having no value or vice versa.

Following is an example of a ‘valueChanges’ filter which defines that notification is sent when any of the elements A1, A2, A3 or PC changes:

```
<location-filter
  xmlns:cl="urn:ietf:params:xml:ns:pidf:geopriv10:civilLoc">
  <valueChanges>cl:civilAddress/cl:A1</valueChanges>
  <valueChanges>cl:civilAddress/cl:A2</valueChanges>
  <valueChanges>cl:civilAddress/cl:A3</valueChanges>
```

```
  <valueChanges>cl:civilAddress/cl:PC</valueChanges>
</location-filter>
```

10.6 The XML Schema of the Location Filter Document

The XML Schema for Location Filter Document is defined in [XSD-locFilter].

11.Content of the Location QoS Document

Location QoS Document specifies parameters which define the expected quality of location information (location QoS parameters). Location QoS parameters are location type, maximum uncertainty, maximum response time, maximum age, required civic elements, and QoS class.

The Location QoS Document starts with a top-level XML element called "location-qos", which contains one or more location QoS parameters. The semantics of multiple elements inside a “location-qos” element is a logical AND.

The "locationType" element defines the type of location information that is requested by the Location Client. Possible values are “geodetic” (to receive location inforamtion in geospatial format based on a subset of GMLv3), “civic” (to receive civic location information) or “all” (to receive location information in both civic and geodetic form). The example is given below.

```
<location-qos>
  <locationType>geodetic</locationType>
</location-qos>
```

The maximum uncertainty parameter is defined with “maxUncertainty” element. This element specifies maximum size of a positioning uncertainty area or volume at a given confidence. The "horizontal" and "vertical" elements are numerical values that contain a decimal value in meters. Maximum uncertainty values MUST be greater than zero. The "confidence" attribute of this element includes the confidence level (expressed as a percentage) that the uncertainty is evaluated at. The default confidence attribute value is 95%.

An example of Location QoS Document which is specified with preferred maximum uncertainty parameter is given below.

```
<location-qos>
  <maxUncertainty confidence=”67”>
           <horizontal>150</horizontal>
  </maxUncertainty>
</location-qos>
```

The “maxResponseTime” element defines maximum allowable time needed for the Location Server to send a response with the Location Information after having received a location request. The value of “maxResponseTime " element is expressed as a non negative integer in units of seconds.

An example of Location QoS Document which specifies maximum preferred horizontal uncertainty of 150 meters and maximum response time of 60 seconds is given below.

```
<location-qos>
  <maxUncertainty confidence=”67”>
           <horizontal>150</horizontal>
  </maxUncertainty>
  <maxResponseTime>60</maxResponseTime>
</location-qos>
```

The “maxAge” element indicates the maximum age of Location Information. The value of “maxAge" element is expressed as a non negative integer in units of seconds. An example given below illustrates the case when Location Client would like to receive current Location Information.

```
<location-qos>
   <maxAge>0</maxAge>
</location-qos>
```

The "requiredCivic" element represents the requirements of a Location Client for civic address information. A Location Client can specify the address elements that need to be present in the civic address in order for the location information to meet their quality requirements.

The "requiredCivic" element contains a whitespace-separated list of element names. These can be interpreted as XPath [W3C.REC-xpath-19991116] expressions that are evaluated in the context of the "civicAddress" element [RFC5139]. These XPath statements are restricted to use of qualified names only (using the response document namespace context) and the "/" separator; that is, the only permitted axis is the "child::" axis. All child nodes of elements (including attributes and textual content) are treated as belonging to an element. (from [I.D.thomson-location-quality])

An example of Location QoS Document which specifies that country, state (or equivalent) and post code civic address elements of Location Information are provided, is given below. This example is based on an example of specifying required civic address fields in [I.D.thomson-location-quality].

```
<location-qos>
       <requiredCivic
           xmlns:ca="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr">
         ca:country ca:A1 ca:PC
       </requiredCivic>
</location-qos>
```

The Location Server SHOULD NOT restrict civic address information to the fields indicated in “requiredCivic” element. Additional fields MAY be provided.

The QoS class is defined with “class” attribute in top element “location-qos”. The attribute may have one of two values: “assured” and “bestEffort”. The "bestEffort" value is considered as the default value in the case that there is no QoS class attribute definition provided in the request. An example of Location QoS Document is given below. Document specifies that the location request should be discarded if Location Server cannot provide Location Information with maximum of 150 meters horizontal uncertainty size at 95% confidence, and the maximum age should not be greater than 600 seconds.

```
<location-qos class=”assured”>
  <maxUncertainty>
           <horizontal>150</horizontal>
  </maxUncertainty>
  <maxAge>600</maxAge>
</location-qos>
```

11.1 The XML Schema for Location QoS Document

The XML Schema for Location QoS Document is defined in [XSD-locQoS].

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-TS-LOCSIP-V1_0	08 Feb 2008	All	Initial Draft
	23 Oct 2008	All	Applied the following CRs • OMA-LOC-2008-0441R01-CR_LOCSIP_1_0_TS_Section_2_References • OMA-LOC-2008-0442-CR_LOCSIP_1_0_TS_Section_3_Terms • OMA-LOC-2008-0443-CR_LOCSIP_1_0_TS_Section_4_Introduction • OMA-LOC-2008-0444R01-CR_LOCSIP_1_0_TS_Section_5_1_LocationClient • OMA-LOC-2008-0445R01-CR_LOCSIP_1_0_TS_Section_5_2_LocationServer • OMA-LOC-2008-0448R01-CR_LOCSIP_1_0_TS_Section_5_4_XDMClient • OMA-LOC-2008-0449R01-CR_LOCSIP_1_0_TS_Section_7_Charging • OMA-LOC-2008-0450-CR_LOCSIP_1_0_TS_Section_8_Registration • OMA-LOC-2008-0451R01-CR_LOCSIP_1_0_TS_Section_9_LocationInfoDocument • OMA-LOC-2008-0453-CR_LOCSIP_1_0_TS_Appendix_D_FeatureTags.doc • OMA-LOC-2008-0446R02-CR_LOCSIP_1_0_TS_Section_5_X_Requesting_LocationServer • OMA-LOC-2008-0447R01-CR_LOCSIP_1_0_TS_Section_5_3_LocationRLS • OMA-LOC-2008-0477-CR_LOCSIP_1_0_TS_more _ReferencesAndTerms
	19 Dec 2008	All	Applied the following CRs • OMA-LOC-2008-0505-CR_LOCSIP_1_0_TS_Sec5_Missing_SubSec • In chapter 5.7, changed [URILISTSUB] to [RFC5367] (reference had disappeared due to contribution 517) • OMA-LOC-2008-0509R02-CR_LOCSIP_1_0_TS_Appendix_C_Policy_XDM • OMA-LOC-2008-0517-CR_LOCSIP_1_0_TS_RFC5367 • OMA-LOC-2008-0518-CR_LOCSIP_1_0_TS_GPM_usage • OMA-LOC-2008-0508R01-CR_LOCSIP_1_0_TS_LocationQoSSections (fixed a numbering issue – section 5.1.9 vs section 5.1) • OMA-LOC-2008-0510R01-CR_LOCSIP_1_0_TS_Security – modified • OMA-LOC-2008-0511R02-CR_LOCSIP_TS_SCR • OMA-LOC-2008-0507R02-CR_LOCSIP_TS_EventNotificationFiltering
	29 Jan 2009	All	Applied the following CRs • OMA-LOC-2009-0003-CR_LOCSIP_TS_Reuse_Presence_RLS_WA • OMA-LOC-2009-0004-CR_LOCSIP_TS_Sigcomp • OMA-LOC-2009-0005R01-CR_LOCSIP_TS_Loc_filter_schema • OMA-LOC-2009-0006R02-CR_LOCSIP_TS_Loc_qos_schema Changed: "the maximum age should not be great than 600 seconds" for "the maximum age should not be greater than 600 seconds" Edited the XML alignment and traded tabs for spaces Suppressed a trailing "or" at the beginning of 6.1

Document Identifier	Date	Sections	Description
	20 Feb 2009	All	Applied the following CRs • OMA-LOC-2009-0018-CR_LOCSIP_TS_Loc_filter_Issues • OMA-LOC-2009-0023R01-CR_LOCSIP_TS_Subscription_Handling_and_Suppression • OMA-LOC-2009-0024R01-CR_LOCSIP_TS_Loc_Qos_Handling • OMA-LOC-2009-0025-CR_LOCSIP_TS_Qos_multipart.doc • OMA-LOC-2009-0026-CR_LOCSIP_TS_XDMS_Access • OMA-LOC-2009-0028R01-CR_LOCSIP_TS_encryption_In_LS • OMA-LOC-2009-0029-CR_LOCSIP_TS_Appendix_B_SCR • OMA-LOC-2009-0034R01-CR_LOCSIP_TS_XML_encryption_examples_rules • OMA-LOC-2009-0035R01-CR_LOCSIP_TS_Complete_Templates Corrected problems in the previous application of CR OMA-LOC-2009-0005R01
	11 May 2009	All	Applied the following CRs • OMA-LOC-2009-0049-CR_LOCSIP_TS_Reuse_PRS2_HSA • OMA-LOC-2009-0078R01-CR_LOCSIP_TS_CONRRC032_Emergency_Service • OMA-LOC-2009-0079R04-CR_LOCSIP_TS_CONRR_C1_C46_Rate_Control • OMA-LOC-2009-0107-CR_LOCSIP_TS_CONRRC43_44_47_References • OMA-LOC-2009-0108-CR_LOCSIP_TS_CONRRC45_FeatureTag • OMA-LOC-2009-0109-CR_LOCSIP_TS_CONRRC51_Authentication
	01 June 2009	All	Applied editorial correction according to CONRR. Applied the following CRs • OMA-LOC-2009-0136-CR_LOCSIP_TS_CONRR_C008_C013 • OMA-LOC-2009-0138-CR_LOCSIP_TS_CONRR_C24_39_50_Schema_OMNA • OMA-LOC-2009-0139-CR_LOCSIP_TS_CONRR_C034_Location_Policy • OMA-LOC-2009-0140-CR_LOCSIP_TS_CONRR_C041_Content_Type 5.1.4 changed “using” to “uses” • OMA-LOC-2009-0141-CR_LOCSIP_TS_CONRR_C052_C053_Key_Handling Replaced another instance of TS 33.220 [6] by the right 3GPP reference Capitalized SHALLs • OMA-LOC-2009-0149-CR_LOCSIP_TS_HSA_Ref
	30 June 2009	2.1, 5, 6.2, 7, 10, 11	Fixed CONRR (OMA-CONRR-LOCSIP-V1_0-20090526-D) issues: C021 Applied the following CRs • OMA-LOC-2009-0153R02-CR_LOCSIP_TS_Notify_Timestamp • OMA-LOC-2009-0166-CR_LOCSIP_TS_CONRR_C25_26_29_30_31_33_35_57_CorrectionsCleanUp • OMA-LOC-2009-0169R01-CR_LOCSIP_TS_CONRR_C27__Restructure_LS_LC • OMA-LOC-2009-0170-CR_TS_CONRR_C037_GPM_Schema_ref Fixed Section numbers Added URL link to referenece [GeoShape]
Candidate Versions OMA-TS-LOCSIP-V1_0	18 Aug 2009	n/a	TP approval: OMA-TP-2009-0356-INP_LOCSIP_1.0_ERP_for_Candidate_approval
Draft Versions OMA-TS-LOCSIP-V1_0	29 Oct 2009	5.2.2, 6	CR incorporated: OMA-LOC-2009-0263
	26 Apr 2010	5.2.1.1 5.2.1.3 5.2.1.5 5.2.1.6	CR incorporated: OMA-LOC-2010-0065

Document Identifier	Date	Sections	Description
	08 Jul 2010	2.1, 5.1.4, 5.2.1.4, 10, 9, 5.1.9, 5.2.1.2, 5.2.1.6, 5.3, B1, 5.1.8, 5.2.1.5, 5.2.1.7,	CR incorporated: OMA-LOC-2010-0124R01 OMA-LOC-2010-0125R01 OMA-LOC-2010-0126 OMA-LOC-2010-0127 OMA-LOC-2010-0128
Candidate Versions OMA-TS-LOCSIP-V1_0	03 Aug 2010	n/a	TP approval: OMA-TP-2010-0326-INP_LOCSIP_1.0_ERP_for_Candidate_reapproval
Draft Versions OMA-TS-LOCSIP-V1_0	02 Sep 2010	9, 6	CR incorporated: OMA-LOC-2010-0186R01
Candidate Versions OMA-TS-LOCSIP-V1_0	25 Nov 2010	n/a	TP approval: OMA-TP-2010-0505-INP_LOCSIP_1.0_ERP_for_notification
Draft Versions OMA-TS-LOCSIP-V1_0	14 Nov 2011	2, 5	Incorporated CR: OMA-LOC-2011-0325-CR_LOCSIP_TS_CR_2009_0050_0312R01
Candidate Versions OMA-TS-LOCSIP-V1_0	14 Nov 2011	n/a	TP approval: OMA-TP-2011-0407-INP_LOCSIP_1.0_ERP_for_notification

Appendix B. Static Conformance Requirements (Normative)

The notation used in this appendix is specified in [SCRRULES].

B.1 LOCSIP Client

Item	Function	Reference	Requirement
LOCSIP-LC-C-01-M	Location Information subscriptions	5.1.2	
LOCSIP-LC-C-02-O	URI List Subscription	5.1.2.1	
LOCSIP-LC-C-03-O	Request-contained URI List Subscription	5.1.2.2	
LOCSIP-LC-C-04-M	Location Information notifications	5.1.2	
LOCSIP-LC-C-05-O	URI List notifications	5.1.2.1	
LOCSIP-LC-C-06-M	Location Information Processing	5.1.1	
LOCSIP-LC-C-08-O	Event notification filtering	5.1.3	
LOCSIP-LC-C-09-O	Handling notification of large objects	5.1.6	
LOCSIP-LC-C-10-O	Conditional event notification according to [RFC5839]	5.1.7	
LOCSIP-LC-C-11-O	Event notification rate control according to [IETF-EventRate]	5.1.8	
LOCSIP-LC-C-12-O	QoS Document	5.1.4	
LOCSIP-LC-C-13-O	Location Filter Document	5.1.3	
LOCSIP-LC-C-14-O	Signaling Compression	5.1.5	

B.2 LOCSIP Server

Item	Function	Reference	Requirement
LOCSIP-LS-S-01-M	Location Information Subscriptions	5.2.1	
LOCSIP-LS-S-02-O	Local policy to limit the maximum number of simultaneous subscriptions from Location Client	5.2.1.1	
LOCSIP-LS-S-03-M	Location Information Notifications	5.2.1.6	
LOCSIP-LS-S-04-O	Handling notification of large objects	5.2.1.6.1	
LOCSIP-LS-S-05-O	Fetch Location Policies from Location Policy XDMS	5.2.2	
LOCSIP-LS-S-06-O	Subscription to Location	5.2.2	

Item	Function	Reference	Requirement
	policy changes		
LOCSIP-LS-S-07-O	Apply Location Authorization Rules	5.2.1.1	
LOCSIP-LS-S-08-O	Apply Location Privacy Rules	5.2.1.1	
LOCSIP-LS-S-09-M	Location Information Data Model	5.2	
LOCSIP-LS-S-10-M	Fetch URI List(s) from Shared List XDMS	5.2.2	
LOCSIP-LS-S-11-O	Subscribe to URI List(s) changes	5.2.2	
LOCSIP-LS-S-12-M	Apply event notification suppression	5.2.1.2	
LOCSIP-LS-S-13-O	Apply event notification filtering	5.2.1.4	
LOCSIP-LS-S-14-M	Apply event notification rate control according to [IETF-EventRate]	5.2.1.5	
LOCSIP-LS-S-15-M	Generate entity tag according to [RFC5839]and suppressing notifications	5.2.1.6	
LOCSIP-LS-S-16-M	Location QoS handling	5.2.1.3	
LOCSIP-LS-S-17-M	Generating and suppressing notifications	5.2.1.7	
LOCSIP-LS-S-18-M	Handling of Large MIME Objects	5.2.1.7.1	

B.3 RLS

Item	Function	Reference	Requirement
LOCSIP-RLS-S-01-M	Support needed RLS functions as described in [PRS_SPEC]	5.3	
LOCSIP-RLS-S-02-O	Support feature tag for location service	5.3	
LOCSIP-RLS-S-03-M	Backend subscription	5.3	
LOCSIP-RLS-S-04-M	Support location filter	5.3	
LOCSIP-RLS-S-05-O	Support location QoS	5.3	

B.4 Home Subscription Agent

Item	Function	Reference	Requirement
LOCSIP-REQ-S-01-O	Support needed HSA function as described in [PRS_SPEC]	5.8	
LOCSIP-REQ-S-02-O	Support feature tag for location services	5.8	

B.5 XDM Client

Item	Function	Reference	Requirement
LOCSIP-XC-C-01-M	Mandatory XDMC functions	5.4	
LOCSIP-XC-C-02-O	Optional XDMC functions	5.4	
LOCSIP-XC-C-03-M	Location Rules Application Usage	5.4	
LOCSIP-XC-C-04-M	URI List Application Usage	5.4	

B.6 RLS XDMS

Item	Function	Reference	Requirement
LOCSIP-RX-S-01-M	Mandatory XDMS functions	5.6	
LOCSIP-RX-S-02-O	Optional XDMS functions	5.6	
LOCSIP-RX-S-03-M	Presence List Application Usage	5.6	
LOCSIP-RX-S-04-M	Subscription to XML Document Changes	5.6	

B.7 Location Policy XDMS

Item	Function	Reference	Requirement
LOCSIP-LX-S-01-M	Mandatory XDMS functions	5.5	
LOCSIP-LX-S-02-O	Optional XDMS functions	5.5	
LOCSIP-LX-S-03-M	Location Rules Application Usage	5.5	
LOCSIP-LX-S-04-M	Subscription to XML Document Changes	5.5	

B.8 GPM

Item	Function	Reference	Requirement
LOCSIP-GPM-S-01-M	Mandatory GPM functions	5.9	
LOCSIP-GPM-S-02-O	Optional XDMS functions	5.9	

Appendix C. LOCSIP XDMS Application Usages (Normative)

C.1 Location Rules

The Location Rules consist of two parts: Subscription Authorization Rules which determine if a Location Client is allowed to subscribe to the Target's Location Information; and Location Privacy Rules which determine the accuracy and associated usage policies of the Target's Location Information to be returned.

The Application Usage of the Location Rules document is described in the subsections below.

C.1.1 Structure

The Location Rules document contains a sequence of <rule> elements, each composed of up to three parts:

a) "conditions"

b) "actions"

c) "transformations"

The Subscription Authorization Rules are described by the <conditions> and <actions> elements. The Location Privacy Rules are comprised of the <conditions> and <transformations> elements.

The <conditions> child element of any <rule> element MAY include the following child elements:

a) the <identity> element as defined in [RFC4745];

b) the <external-list> element as defined in [XDM_Core] "*Authorization Rules*";

c) the <other-identity> element as defined in [XDM_Core] "*Authorization Rules*";

d) the <anonymous-request> element as defined in [XDM_Core] "*Authorization Rules*".

e) the <location-condition> element as defined in [GeoPriv_Policy] section 4.

The <actions> child element of any <rule> element MAY include the <sub-handling> element as described in as described in [RFC5025] section 3.2.1.

The <transformations> child element of any <rule> element MAY include the following child elements:

a) the <provide-location> element as described in [GeoPriv_Policy] section 6.5.

b) the <set-retransmission-allowed> element as described in [GeoPriv_Policy] section 6.1

c) the <set-retention-expiry> element as described in [GeoPriv_Policy] section 6.2

d) the <set-note-well> element as described in [GeoPriv_Policy] section 6.3

e) the <keep-rule-reference> element as described in [GeoPriv_Policy] section 6.4

C.1.2 Application Unique ID

The AUID SHALL be "org.openmobilealliance.loc-rules".

C.1.3 XML Schema

The Subscription Authorization Rules SHALL be composed according to the XML schema detailed in [RFC5025] section 6 and extended in [XDM_Core] *"Authorization Rules"*.

The Location Privacy Rules SHALL follow the XML schema defined in [GeoPriv_Policy] section 9

C.1.4 Default Namespace

The default namespace used in expanding URIs SHALL be “urn:ietf:params:xml:ns:common-policy” defined in [RFC4745]

C.1.5 MIME Type

The MIME type for this Application Usage SHALL be “application/auth-policy+xml” defined in [RFC4745].

C.1.6 Validation Constraints

The validation constraints SHALL conform to those imposed by the XML schema.

The <conditions> element SHALL contain no more than one child element of <identity>, <external-list>, <other-identity>, <anonymous-request> or <location-condition>.

The <sub-handling> element is described in [RFC5025]. Only “block” and “allow” are used by this specification. If other value is present an HTTP 409 (Conflict) SHALL be returned with the error condition identified by the <constraint-failure> element. If included, the “phrase” attribute of this element SHOULD be set to “value of <sub-handling> element not allowed”.

C.1.7 Data Semantics

The data semantics for Subscription Authorization Rules SHALL conform to the semantics defined in [RFC5025] and extended in [XDM_Core] “Authorization Rules”.

The <location-condition> in <conditions> element and the <transformations> element SHALL be ignored when evaluating Subscription Authorization Rules.

The data semantics for Location Privacy Rules SHALL conform to the semantics defined in [GeoPriv_Policy] together with the clarifications given in this sub-clause.

The Location Privacy Rules SHALL be ignored if the <sub-handling> child element in a <rule> element has a value different than “allow”.

The <conditions> element SHALL evaluate to TRUE if all contained <location-condition> elements are evaluated to TRUE. The <location-condition> element SHALL evaluate to TRUE if any of its child elements <location> is TRUE. A <location> element SHALL evaluate to TRUE if the current location of the Target is within the described location.

The <actions> element SHALL be ignored when evaluating Location Privacy Rules.

The <provide-location> “transformation” controls the location information to be returned. There are two possible location profiles, namely:

a) the <provide-civic> element, restricts the level of civic location information the Location Server is permitted to disclose. The <provide-civic> child element is described in [GeoPriv_Policy] Section 6.5.1.

b) the <provide-geo> element, restricts the returned geodetic location information based on the specified accuracy. The <provide-geo> child element is described in [GeoPriv_Policy] Section 6.5.2.

The <transformations> element MAY include instructions on the basic authorization policies carried inside the <geopriv> element which are described by the following child elements: <set-retransmission-allowed>, <set-retention-expiry>, <set-note-well> and/or <keep-rule-reference> elements as defined in [GeoPriv_Policy] section 6.

C.1.8 Naming Conventions

The name of the Location Rules document SHALL be “loc-rules”.

C.1.9 Global Documents

This Application Usage defines no Global Documents.

C.1.10 Resource Interdependencies

This application usage defines no additional resource interdependencies.

C.1.11 Authorization Policies

The authorization policies SHALL be defined according to [XDM_Core] “Authorization”.

Appendix D. LOCSIP feature tags

This section describes LOCSIP feature tags.

Media feature tag name: g.oma.locsip.

Summary of the media feature indicated by this tag: This SIP feature tag indicates that the network element supports procedures defined by the OMA Location in SIP/IP core network (LOCSIP) specifications.

Values appropriate for use with this feature tag: Boolean.

The SIP feature tag is intended primarily for use in the following applications, protocols, services, or negotiation mechanisms:

> This feature tag is most useful in services that may utilize location information, such as Presence and PoC.

Examples of typical use:

> Providing this information in SUBSCRIBE request allows SIP/IP Core to route the location request directly to Location Server. This mechanism is used to distinguish location service requests from presence service requests.

Related standards or documents: OMA-TS-LOCSIP-V1_0 published at http://www.openmobilealliance.org/.

Security considerations: Security considerations for this media feature tag are discussed in Section 11.1 of [RFC3840].

Name(s) & email address(es) of person(s) to contact for further information:

1. Name : OMA Location in SIP/IP core network (LOCSIP) Working Group
2. Email : technical-comments@mail.openmobilealliance.org

Intended usage: Common

Author/Change controller: The OMA LOCSIP specifications are a work item of the OMA Location in SIP/IP core network (LOCSIP) Working Group. The Open Mobile Alliance has change control over these specifications, with mailing list address technical-comments@mail.openmobilealliance.org