



Resource List Server (RLS) Specification

Candidate Version 1.0 – 17 Sep 2009

Open Mobile Alliance
OMA-TS-Presence_SIMPLE_RLS-V1_0-20090917-C

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

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

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

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

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

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

© 2009 Open Mobile Alliance Ltd. All Rights Reserved.

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

Contents

1.	SCOPE	4
2.	REFERENCES	5
2.1	NORMATIVE REFERENCES	5
2.2	INFORMATIVE REFERENCES	6
3.	TERMINOLOGY AND CONVENTIONS	7
3.1	CONVENTIONS	7
3.2	DEFINITIONS	7
3.3	ABBREVIATIONS	8
4.	INTRODUCTION	9
4.1	VERSION 1.0	9
5.	FUNCTIONAL DESCRIPTION OF THE RESOURCE LIST SERVER	10
5.1	GENERAL	10
5.2	BACK-END SUBSCRIPTIONS	10
5.3	EVENT NOTIFICATION FILTERING	11
5.4	CONDITIONAL EVENT NOTIFICATIONS	11
5.4.1	Generating Entity Tags	11
5.4.2	Generation of Notifications	12
5.5	HANDLING OF EVENT NOTIFICATION SUPPRESSION	12
5.6	XDM FUNCTIONS	12
5.7	APPLYING EVENT NOTIFICATION THROTTLING	13
5.8	COMPRESSION OF THE BODY IN A NOTIFY REQUEST	13
6.	SECURITY	13
6.1	PRIVACY	13
6.1.1	Anonymous SIP Request	13
6.2	AUTHENTICATION OF SIP REQUESTS	13
6.3	INTEGRITY AND CONFIDENTIALITY PROTECTION	14
APPENDIX A.	CHANGE HISTORY (INFORMATIVE)	15
A.1	APPROVED VERSION HISTORY	15
A.2	DRAFT/CANDIDATE VERSION 1.0 HISTORY	15
APPENDIX B.	STATIC CONFORMANCE REQUIREMENTS (NORMATIVE)	16
B.1	RLS	16

1. Scope

This document provides the specification for the Resource List Server in the OMA Presence SIMPLE 2.0 enabler.

2. References

2.1 Normative References

OMA

- [PRS_AD] “Presence SIMPLE Architecture”, Version 2.0, Open Mobile Alliance™, OMA-AD-Presence_SIMPLE-V2_0, URL: <http://www.openmobilealliance.org/>
- [PRS_RLSXDM] “Resource List Server (RLS) XDM Specification”, Version 2.0, Open Mobile Alliance™, OMA-TS-Presence_SIMPLE_RLS_XDM-V2_0, 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/>
- [XDM_Core] “XML Document Management Specification”, Version 2.0, Open Mobile Alliance™, OMA-TS-XDM_Core-V2_0, URL: <http://www.openmobilealliance.org/>
- [XDM_List] “Shared List XDM Specification”, Version 2.0, Open Mobile Alliance™, OMA-TS-XDM_Shared-V2_0, URL: <http://www.openmobilealliance.org/>

IETF

- [IETF-EventThrottle] IETF draft-niemi-sipping-event-throttle-07 “Session Initiation Protocol (SIP) Event Notification Extension for Notification Throttling”, A. Niemi et al., Oct 22, 2008, URL: <http://www.ietf.org/internet-drafts/draft-niemi-sipping-event-throttle-07.txt>
Note: IETF Draft work in progress
- [IETF-SubNotEtag] IETF draft-ietf-sip-subnot-etags-03 “An Extension to Session Initiation Protocol (SIP) Events for Conditional Event Notification”, A. Niemi, Jul 14, 2008, URL: <http://www.ietf.org/internet-drafts/draft-ietf-sip-subnot-etags-03.txt>
Note: IETF Draft work in progress
- [RFC1952] IETF RFC 1952 “GZIP file format specification version 4.3”, P. Deutsch, May 1996, URL: <http://www.ietf.org/rfc/rfc1952.txt>
- [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>
- [RFC2119] IETF RFC 2119 “Key words for use in RFCs to Indicate Requirement Levels”, S. Bradner, Mar 1997, URL: <http://www.ietf.org/rfc/rfc2119.txt>
- [RFC3265] IETF RFC 3265 “Session Initiation Protocol (SIP)-Specific Event Notification”, A. B. Roach, Jun 2002, URL: <http://www.ietf.org/rfc/rfc3265.txt>
- [RFC3323] IETF RFC 3323 “A Privacy Mechanism for the Session Initiation Protocol (SIP)”, J. Peterson, Nov 2002, URL: <http://www.ietf.org/rfc/rfc3323.txt>
- [RFC4474] IETF RFC 4474 “Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)”, J. Peterson et al., Aug 2006, URL: <http://www.ietf.org/rfc/rfc4474.txt>
- [RFC4662] IETF RFC 4662 “A Session Initiation Protocol (SIP) Event Notification Extension for Resource Lists”, A. B. Roach et al., Aug 2006, URL: <http://www.ietf.org/rfc/rfc4662.txt>
- [RFC5367] IETF RFC 5367 “Subscriptions to Request-Contained Resource Lists in the Session Initiation Protocol (SIP)”, G. Camarillo et al., Oct 2008, URL: <http://www.ietf.org/rfc/rfc5367.txt>
- 3GPP/3GPP2
- [3GPP-TS_23.228] 3GPP TS 23.228 “IP Multimedia Subsystem (IMS); Stage 2”, URL: http://www.3gpp.org/ftp/Specs/archive/23_series/23.228/

- [3GPP-TS_24.109] 3GPP TS 24.109 “Bootstrapping interface (Ub) and network application function interface (Ua); Protocol details ; Stage 3”,
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/
- [3GPP-TS_33.203] 3GPP TS 33.203 “Access Security for IP-based services”,
URL: http://www.3gpp.org/ftp/Specs/archive/33_series/33.203/
- [3GPP2-S.R0086] 3GPP2 S.R0086 “IMS Security Framework”,
URL: http://www.3gpp2.org/Public_html/specs/index.cfm
- [3GPP2-X.S0013-002] 3GPP2 X.S0013-002 “All-IP Core Network Multimedia Domain: IP Multimedia Subsystem - Stage 2”,
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

2.2 Informative References

Void.

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

Application Usage	Use definition from [XDM_Core].
Event Package	An additional specification, which defines a set of state information to be reported by a notifier to a subscriber. Event packages also define further syntax and semantics based on the framework defined by this document required to convey such state information. Source: [RFC3265]
Global Tree	Use definition from [XDM_Core].
Request-contained Resource List	Use definition from [PRS_AD].
Resource List	Use definition from [PRS_AD].
Resource List Server (RLS)	Use definition from [PRS_AD].
Subscriber	Use definition from [PRS_AD].

3.3 Abbreviations

AD	Architecture Document
AS	Application Server
IETF	Internet Engineering Task Force
IMS	IP Multimedia Subsystem
IP	Internet Protocol
MIME	Multipurpose Internet Mail Extensions
MMD	Multimedia Domain
OMA	Open Mobile Alliance
PRS	Presence SIMPLE
RD	Requirement Document
RFC	Request For Comments
RLMI	Resource List Meta-Information
RLS	Resource List Server
SIMPLE	SIP for Instant Messaging and Presence Leveraging Extensions
SIP	Session Initiation Protocol
UA	User Agent
UE	User Equipment
URI	Uniform Resource Identifier
XCAP	XML Configuration Access Protocol
XDM	XML Document Management
XDMC	XML Document Management Client
XDMS	XML Document Management Server
XML	eXtensible Markup Language
XUI	XCAP User Identifier

4. Introduction

This document provides the specification for the Resource List Server in the OMA Presence SIMPLE 2.0 enabler.

4.1 Version 1.0

The OMA Presence SIMPLE 2.0 enabler separates the functions for the Resource List Server into a specification of its own to simplify reuse by other enablers. The functions included in this specification are:

- Handling of back-end subscriptions;
- Filtering of event notifications;
- Conditional event notifications;
- Suppression of event notifications;
- Support of XDM functions;
- Applying event notification throttling; and
- Compression of information in NOTIFY requests.

5. Functional Description of the Resource List Server

The Resource List Server (RLS) accepts and manages subscriptions to Resource Lists and Request-contained Resource Lists, which enable a Subscriber to subscribe to a list of resource URIs using a single subscription. The RLS may be re-used by Services that make use of the SIP event notification mechanism defined in [RFC3265] and the SIP event notification extension for resource lists defined in [RFC4662].

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

5.1 General

The RLS:

- SHALL support subscriptions to Resource Lists according to the RLS procedures described in [RFC4662];
- MAY support subscriptions to Request-contained Resource Lists according to the RLS procedures described in [RFC5367] sections “*URI-List Document Format*” and “*Resource List Server Behavior*”; and

If subscriptions to Request-contained Resource Lists are supported, the RLS SHALL support “multipart/mixed” content type in SUBSCRIBE requests as described in [RFC2046].

The RLS SHALL, before accepting a subscription to a Resource List, perform authorization of the usage of the Resource List by the Subscriber, per local policy. If the Resource List subscription is authorized, the RLS SHALL resolve the Resource List into individual resource URIs according to section 5.6.

5.2 Back-end Subscriptions

For back-end subscriptions using SIP, the RLS:

- SHALL the subscriber procedures described in [RFC3265];
- SHALL support conditional subscriptions according to the subscriber procedures described in [IETF-SubNotEtag];
- SHALL support event notification suppression according to the procedures in described in section 5.3; and
- MAY indicate that it supports that the body of a NOTIFY request is compressed by the GZIP algorithm [RFC1952] by including an Accept-Encoding header field with the value ‘gzip’ in the SUBSCRIBE request. An RLS indicating support for GZIP compression SHALL, when receiving a NOTIFY request with the Content-Encoding header field with the value ‘gzip’, decompress the received body as defined by [RFC1952] before processing the body of the SIP NOTIFY request.

When the SIP/IP Core corresponds to 3GPP IMS or 3GPP2 MMD networks, the RLS SHALL follow the procedures described in section 5.7.3 of [3GPP-TS_24.229] and [3GPP2-X.S0013-004] and insert a URI value from the P-Asserted-Identity header field of the incoming SUBSCRIBE request (as defined in [3GPP-TS_24.229] and [3GPP2-X.S0013-004]) to the SUBSCRIBE request of the back-end subscription, as opposed to acting as an authentication service (as defined in [RFC4474]) as required by [RFC4662].

If the Resource List subscription is identified as anonymous (see section 6.1.1), the RLS SHALL generate back-end subscriptions as anonymous using the procedures as defined in [PRS_Spec] “*Watcher Privacy*”.

If a service specific OTA Provisioning parameter or local policy instructs, the RLS SHALL limit the number of back-end subscriptions. The RLS:

- SHALL initiate no more back-end subscriptions as instructed by the provisioning parameter or local policy; and
- SHALL return no <instance> element for those <resource> elements that could not be subscribed from the Resource List document or Request-contained Resource List due to this limitation. The <instance> and <resource> elements are part of the Resource List Meta-Information (RLMI) document as defined in [RFC4662].

When the Subscriber adds additional resource URIs to the Resource List while the subscription is active, the RLS SHALL generate back-end subscriptions for the newly added resource URIs, and SHALL include the newly added resource URIs in the next list notification. This procedure SHALL NOT require the Subscriber to re-subscribe to the Resource List.

When the Subscriber removes resource URIs from the Resource List while the subscription is active, the RLS SHALL terminate back-end subscriptions to the recently removed resource URIs, and SHALL indicate that the back-end subscriptions have been terminated in the next list notification. This procedure SHALL NOT require the Subscriber to re-subscribe to the Resource List.

The Resource List can be changed either directly, when the RLS-services document stored in RLS XDMS is updated, or indirectly, when the URI List stored in the Shared List XDMS and referenced in the RLS-services document is updated.

When the Subscriber refreshes the subscription, the RLS SHOULD refresh the back-end subscriptions accordingly. The RLS SHOULD try to re-generate the back-end subscriptions for those resource URIs whose corresponding <resource> element in the last list notification:

- did not include an <instance> element if the omission was not caused by a limit to the maximum number of back-end subscriptions; or
- included an <instance> element whose “state” attribute was set to “terminated”.

5.3 Event Notification Filtering

The RLS SHOULD support event notification filtering according to the following procedures:

- Event notification filtering, according to the RLS and notifier procedures described in [RFC4660] with the clarifications described in this section; and
- Content type ‘application/simple-filter+xml’, according to [RFC4661].

If the RLS supports event notification filtering and

- understands the particular filter included in the payload of the SUBSCRIBE request, the RLS:
 - SHALL, if the filter element contains a “uri” attribute and its value matches with the URI of a resource in the Resource List or Request-contained Resource List, supply the filter document in the back-end subscription to the matching Presentity;
 - SHALL, if the filter element contains a “domain” attribute and its value matches with the domain of a set of resource URIs in the Resource List, Request-contained Resource List, supply the filter document in the back-end subscriptions to the resources matching the “domain” attribute, but not matching the “uri” attribute in other filters in the filter-set; and
 - SHALL, if the filter element does not contain a “uri” or “domain” attribute, supply the filter document in the back-end subscriptions to all resources in the Resource List or Request-contained Resource List not matching a “uri” or a “domain” attribute in other filters in the filter-set.
- does not understand the particular filter included in the payload of the SUBSCRIBE request as requested by the Subscriber, the RLS SHALL indicate it to the Subscriber as specified in [RFC4660].

For every filter propagated in a back-end subscription targeted to a resource, the RLS SHALL remove the “uri” or “domain” attribute if included in the RLS filter obtained from the Subscriber.

5.4 Conditional Event Notifications

The RLS SHALL support the notifier procedures defined in [IETF-SubNotEtag].

5.4.1 Generating Entity Tags

The RLS:

- SHALL generate entity tags for the full Resource List state including the RLMI and the list of individual documents specific to the Event Package as described in [IETF-SubNotEtag] “*List Subscriptions*”; and
- SHALL include the entity tag in all NOTIFY requests as described in [IETF-SubNotEtag].

5.4.2 Generation of Notifications

If the Subscriber requested condition for suppressing a NOTIFY request or a NOTIFY request body evaluates to true, the RLS SHALL suppress the NOTIFY request or the NOTIFY request body appropriately as described in [IETF-SubNotEtag].

5.5 Handling of Event Notification Suppression

The RLS SHALL support event notification suppression according to the procedures described in this section.

If the RLS receives a SUBSCRIBE request including:

- a wildcarded Suppress-If-Match header field using the special "*" entity-tag value as described in [IETF-SubNotEtag] “*Generating SUBSCRIBE Requests*”; or
- a throttle parameter set to the remaining subscription expiration value as described in [IETF-EventThrottle] “*Selecting the Throttle Interval*”,

the RLS SHALL suppress the generation of event notifications until the Subscriber cancels the suppression with a re-SUBSCRIBE request or the subscription state changes.

5.6 XDM Functions

In order to resolve Resource Lists into individual resource URIs, the RLS:

- SHALL support retrieval of XML documents stored in the RLS XDMS and Shared List XDMS, according to [XDM_Core] “*Document Management*” (via the PRS-10 and PRS-9 reference points, respectively);
- SHALL support the Resource List Application Usage as specified in [PRS_RLSXDM] “*Resource List*”; and
- SHALL support the URI List Application Usage as specified in [XDM_List] “*URI List*”.

On receiving a SUBSCRIBE request directed at a Resource List identified by a Request-URI, the RLS either:

- SHALL access the “index” document in the Global Tree using the XCAP path [XCAP Root URI]/rls-services/global/index; or
- SHALL access the “index” document in the Users Tree using the XCAP path [XCAP Root URI]/rls-services/users/[XUI]/index, if the RLS has knowledge about the XUI of the Primary Principal of the Resource List.

NOTE: The latter procedure may be preferred when the RLS has a need to handle multiple Resource Lists owned by a single Primary Principal (i.e. contained in the same “index” document) and the XUI is known (e.g. included as part of the Resource List URI in the Request-URI of the SUBSCRIBE request as defined by the URI template in [XDM_Core] “*Provisioned XDMC Parameters*”).

The RLS SHALL retrieve the Resource List from the contents of the <service> element within the index document whose “uri” attribute value matches the Request-URI of the received SUBSCRIBE request. If the RLS is unable to retrieve the Resource List from the RLS XDMS, the RLS SHALL reject the SUBSCRIBE request with a 404 (Not Found) response.

The Resource List can contain references to URI Lists stored in the Shared List XDMS. If the RLS is unable to retrieve a URI List from the Shared List XDMS, then that URI List SHOULD be ignored; if so, the Subscriber is made aware of this when the URIs which could not be de-referenced are omitted from the list notification.

The RLS MAY subscribe to changes made to XML documents stored in the RLS XDMS and Shared List XDMS. If so, the RLS SHALL follow the procedures defined in [XDM_Core] “*Subscribing to Changes in the XML Documents*” (via the PRS-4 reference point).

When realized in 3GPP IMS or 3GPP2 MMD networks, the RLS SHALL insert a URI from the received P-Asserted-Identity header field (as defined in [3GPP-TS_24.229] and [3GPP2-X.S0013-004]) from the SUBSCRIBE request in 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], of the HTTP GET request.

5.7 Applying Event Notification Throttling

Subject to rate limitations described below, the RLS SHALL generate notifications when it receives updated resource state information from back-end subscriptions.

The RLS MAY have local throttling configuration settings that limit the rate at which notification are generated (i.e. the shortest time period between two NOTIFY requests). In this case, the RLS SHALL NOT generate NOTIFY requests more often than the throttling configuration dictates, except when generating the notification either upon receipt of a SUBSCRIBE request or upon subscription state changes.

The RLS SHALL support Subscriber requested event notification throttling. The RLS SHALL follow the notifier procedures described in [IETF-EventThrottle].

If the RLS has a local throttling configuration setting and it is lower than the Subscriber proposed throttle value, the RLS SHALL accept the Subscriber proposed throttle value.

If the local throttling configuration setting is higher than the Subscriber proposed throttle value, the RLS SHALL adjust the Subscriber proposed throttle value to the local throttling configuration setting and send it back to the Subscriber as described in [IETF-EventThrottle].

If multiple back-end notifications arrive while rate control restrictions apply, the RLS MAY aggregate those notifications (i.e. combine the resource states into a single NOTIFY request) and transmit them when those restrictions expire. The mechanism by which multiple notifications are aggregated is described in [RFC4662].

5.8 Compression of the Body in a NOTIFY Request

If the RLS receives a SUBSCRIBE request containing an Accept-Encoding header field with the value 'gzip', the RLS SHALL, dependent on local policy, compress the NOTIFY request body using the GZIP algorithm [RFC1952] and add a Content-Encoding header field with the value 'gzip' to the NOTIFY request before sending the NOTIFY request to the SIP/IP Core.

6. Security

The security mechanism provides protection to the service environment.

6.1 Privacy

6.1.1 Anonymous SIP Request

The RLS SHALL consider a SIP request as anonymous if it contains a From header indicating an anonymous value as defined in [RFC3323].

When the SIP/IP Core corresponds with 3GPP IMS or 3GPP2 MMD networks, the PS SHALL follow the procedures described in [3GPP-TS_24.229] / [3GPP2-X.S0013-004] section 5.7.1.4 to determine if the SIP request is anonymous.

6.2 Authentication of SIP Requests

The RLS SHALL authenticate all incoming SIP requests. The 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 PS 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
- SHALL, when acting on behalf of the Subscriber, 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.

6.3 Integrity and Confidentiality Protection

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].

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-Presence_SIMPLE_RLS-V1_0	04 Aug 2009	All	First version – based upon contribution OMA-PAG-2009-0058R02-INP_PRS2_new_RLS_TS Application of 2009 template.
	14 Aug 2009	4	CR incorporated: OMA-PAG-2009-0234
Candidate Version OMA-TS-Presence_SIMPLE_RLS-V1_0	17 Sep 2009	N/A	Status changed to Candidate by TP TP ref # OMA-TP-2009-0438- INP_PRS_V2_0_ERP_for_Notification

Appendix B. Static Conformance Requirements (Normative)

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

The SCR's defined in the following table include SCR for the Resource List Server.

The following tags are used in the Function column to identify the release of the Presence SIMPLE enabler that the requirement was introduced:

- PRSv1.1 – Requirement was introduced in Presence SIMPLE 1.1.
- PRSv2.0 – Requirement was introduced in Presence SIMPLE 2.0.

B.1 RLS

Item	Function	Reference	Requirement
PRS-CRLS-S-001-M	Subscriptions to Resource List (PRSv2.0)	5.1	
PRS-CRLS-S-002-O	Subscriptions to Request-contained Resource List according to [RFC5367] (PRSv2.0)	5.1	
PRS-CRLS-S-003-M	List notifications (PRSv1.1)	5.1	
PRS-CRLS-S-004-M	Back-end subscriptions (PRSv1.1)	5.2	
PRS-CRLS-S-005-O	Limiting the number of back-end subscriptions (PRSv1.1)	5.2	
PRS-CRLS-S-006-O	Conditional back-end subscriptions (PRSv2.0)	5.2	
PRS-CRLS-S-007-O	Event notification filtering for the back-end subscriptions (PRSv1.1)	5.2	
PRS-CRLS-S-008-M	Handling of event notification suppression for the back-end subscriptions (PRSv2.0)	5.2	
PRS-CRLS-S-009-O	Apply event notification throttling according to [IETF-Throttle] for the back-end subscriptions (PRSv2.0)	5.2	
PRS-CRLS-S-010-O	Event notification filtering for the list notifications (PRSv1.1)	5.3	
PRS-CRLS-S-011-M	Conditional event notifications for the list notifications (PRSv2.0)	5.4	
PRS-CRLS-S-012-M	Handling of event notification suppression for the list notifications (PRSv2.0)	5.5	
PRS-CRLS-S-013-M	Fetch Resource List from Presence XDMS (PRSv1.1)	5.6	
PRS-CRLS-S-014-O	Subscription to Resource List changes (PRSv2.0)	5.6	

Item	Function	Reference	Requirement
PRS-CRLS-S-015-M	Fetch URI List(s) from Shared List XDMS (PRsv1.1)	5.6	
PRS-CRLS-S-016-O	Subscribe to URI List(s) changes (PRsv2.0)	5.6	
PRS-CRLS-S-017-M	Apply event notification throttling according to [IETF-Throttle] for the list notifications (PRsv2.0)	5.7	
PRS-CRLS-S-018-O	Compression of NOTIFY body using gzip (PRsv2.0)	5.8	