Resource List Server (RLS) XDM Specification

Candidate Version 1.1 – 28 Jan 2008

Open Mobile Alliance

OMA-TS-Presence_SIMPLE_RLS_XDM-V1_1-20080128-C

Contents

Figures

1. Scope

The Resource List Server XDMS (RLS XDMS) specific data formats and XCAP application usages are described in this specification.

2. References

2.1 Normative References

[PRES_Spec] "Presence SIMPLE Specification", Version 1.1, Open Mobile Alliance™, OMA-TS-XDM_Core-V1_1, URL: http://www.openmobilealliance.org/

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

[RFC4234] "Augmented BNF for Syntax Specifications: ABNF". D. Crocker, Ed., P. Overell. October 2005, URL: http://www.ietf.org/rfc/rfc4234.txt

[RFC4825] "The Extensible Markup Language (XML) Configuration Access protocol (XCAP)", J. Rosenberg, May, 2007, URL: http://www.ietf.org/rfc/rfc4825.txt

[RFC4826] "Extensible Markup Language (XML) Formats for Representing Resource Lists", J. Rosenberg, May, 2007, URL: http://www.ietf.org/rfc/rfc4826.txt

[XDM_Spec] "XML Document Management (XDM) Specification", Version 1.1, Open Mobile Alliance™, OMA-TS-XDM_Core-V1_1, URL: http://www.openmobilealliance.org/

2.2 Informative References

[PRES_MO] "OMA Management Object for SIMPLE Presence", Version 1.1, Open Mobile Alliance™, OMA-TS-Presence_SIMPLE_MO-V1_1, URL: http://www.openmobilealliance.org/

[RFC3856] "A Presence Event Package for the Session Initiation Protocol", IETF RFC, August 2004, URL: http://www.ietf.org/rfc/rfc3856.txt

3. Terminology and Conventions

3.1 Conventions

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

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

3.2 Definitions

Application Unique ID	A unique identifier within the namespace of application unique IDs created by [RFC4825] that differentiates XCAP resources accessed by one application from XCAP resources accessed by another. (Source: [RFC4825])
Global Document	A document placed under the XCAP global tree that applies to all users of that application usage.
Global Tree	A URI that represents the parent for all global documents for a particular application usage within a particular XCAP root. (Source: [RFC4825])
XCAP Application Usage	Detailed information on the interaction of an application with an XCAP server. (Source: [RFC4825])
XCAP Client	An HTTP client that understands how to follow the naming and validation constraints defined in [RFC4825]. (Source: [RFC4825])
XCAP Server	An HTTP server that understands how to follow the naming and validation constraints defined in [RFC4825]. (Source: [RFC4825])

3.3 Abbreviations

AUID	Application Unique ID
HTTP	Hyper Text Transfer Protocol
IETF	Internet Engineering Task Force
OMA	Open Mobile Alliance
RLS	Resource List Server
SIP	Session Initiation Protocol
URI	Uniform Resource Identifier
XCAP	XML Configuration Access Protocol
XDM	XML Document Management
XDMS	XML Document Management Server
XML	Extensible Markup Language

4. Introduction

The RLS XDMS is the repository for XML documents that define services which are associated with a list of resources. An example of such a service document is a Presence List, which is used by a RLS (see [PRES_Spec]) to subscribe, on behalf of a watcher, to the presence status of a list of presentities.

The protocol used to access and manipulate such documents is based on the XML Configuration Access Protocol (XCAP), and described in [XDM_Spec].

This specification provides the XCAP application usage for one type of RLS-specific XML document, the Presence List.

5. RLS XDM Application Usages

5.1 Presence List

5.1.1 Structure

The Presence List document SHALL conform to the structure of the "rls-services" document described in [RFC4826] section 4.1, with the following clarifications:

a. Each <service> element SHALL include the <packages> element.

b. Each <packages> element SHALL specify at least the presence event package as defined in [RFC3856].

5.1.2 Application Unique ID

The application unique ID (AUID) of a Presence List document SHALL be "rls-services" within the IETF tree, as specified in [RFC4826] section 4.4.1.

5.1.3 Default Namespace

The default namespace SHALL conform to the default namespace "urn:ietf:params:xml:ns:rls-services" for the "rls-services" document described in [RFC4826] section 4.4.4.

5.1.4 XML Schema

A Presence List document SHALL conform to the XML schema described in [RFC4826] section 4.2.

5.1.5 MIME Type

The MIME type of a Presence List document SHALL be "application/rls-services+xml", as specified in [RFC4826] section 4.4.2.

5.1.6 Validation constraints

In addition to the XML schema, the validation constraints on a Presence List document SHALL conform to those described in [RFC4826] section 4.4.5, with the following clarifications:

Each <service> element SHALL include the <packages> element with a <package> child element with value "presence". If the Presence List document does not conform to this constraint, the RLS XDMS SHALL respond with an HTTP "409 Conflict" response as described in [RFC4825]. The error condition SHALL be described by the <constraint-failure> error element. If included, the "phrase" attribute SHOULD be set to "Presence event package required".

The value of the "uri" attribute proposed by the XDM Client in the <service> element (i.e. the Service URI):

- SHALL be a valid SIP URI.
- SHALL conform to the syntax specified by the Service URI Template (see [PRES_MO]), which is stored in the RLS XDMS and provisioned to the XDM Client.
- SHALL NOT violate the "uniqueness constraint" defined in [RFC4826] section 4.4.5.

If the Service URI does not conform to the local policy or the constraints described above, the RLS XDMS SHALL respond with an HTTP "409 Conflict" response as described in [RFC4825]. The error condition SHALL be described by the <uniqueness-failure> error element. The RLS XDMS SHALL include at least one <alt-value> element in the <uniqueness-failure> error element.

NOTE: The syntax of the <alt-value> element is according to the syntax stored in the RLS XDMS and provisioned to the XDM Client, but may also be a different syntax according to local XDMS policy and not yet provisioned to the XDM Client.

If the XDM Client repeats the XCAP request, it SHOULD use a "uri" attribute chosen from one of the values received in the <alt-value> elements.

5.1.7 Data Semantics

The data semantics of a Presence List document SHALL conform to those described in [RFC4826] section 4.1.

5.1.8 Naming conventions

The naming conventions of a Presence List document SHALL conform to those described in [RFC4826] section 4.4.7.

The document containing the Presence Lists for a particular user SHALL be named "index".

NOTE: Any document in the user's tree without the name "index" will not be accessible by the RLS service.

5.1.9 Global documents

In addition to the Presence List documents that exist in the XCAP user tree, this application usage defines a single global index document, as described in [RFC4826] section 4.4.8.

5.1.10 Resource interdependencies

The RLS XDMS SHALL conform to the resource interdependencies described in [RFC4826] section 4.4.8.

5.1.11 Authorization policies

The authorization policies SHALL conform to those described in [XDM_Spec] section 6.4.3.

The RLS XDMS SHALL check that the identity of the requesting XDMC has been granted access rights to perform requested operations on the global index document

By default, the primary principal of a document in the users tree has permission to perform retrieve operations as defined in [XDM_Spec] section 6.1.1.2 to fetch that part of the global index document that has the same content as the document in the users tree.

Appendix A. Static Conformance Requirements (Normative)

The SCR's defined in the following tables include SCR for:

- RLS XDM Application Usages

Each SCR table identifies a list of supported features as:

Item: Identifier for a feature.

Function: Short description of the feature.

Reference: Section(s) of this specification with more details on the feature.

Status: Whether support for the feature is mandatory or optional. MUST use "M" for mandatory support and "O" for optional support in this column.

Requirement: This column identifies other features required by this feature. If no other features are required, this column is left empty.

This section describes the dependency grammar notation to be used in the Requirement column of the SCR and CCR tables using ABNF [RFC4234].

TerminalExpression = ScrReference / NOT TerminalExpression / TerminalExpression LogicalOperator TerminalExpression / "(" TerminalExpression ")"

ScrReference = ScrItem / ScrGroup

ScrItem = SpecScrName "–" GroupType "–" DeviceType "–" NumericId / SpecScrName "–" DeviceType "–" NumericId

ScrGroup = SpecScrName ":" FeatureType / SpecScrName "– " GroupType "–" DeviceType "–" FeatureType

SpecScrName = 1*Character;

GroupType = 1*Character;

DeviceType = "C" / "S"; C – client, S – server

NumericId = Number Number Number

LogicalOperator = "AND" / "OR"; AND has higher precedence than OR and OR is inclusive

FeatureType = "MCF" / "OCF" / "MSF" / "OSF"; See Section A.1.6

Character = %x41-5A ; A-Z

Number = %x30-39 ; 0-9

A.1 RLS XDM Server Application Usages

Item	Function	Reference	Status	Requirement
RLS_XDM-AU-S-001	Presence list structure	5.1.1	M	
RLS_XDM-AU-S-002	Application Unique ID in presence list	5.1.2	M	
RLS_XDM-AU-S-003	XML schema of presence list	5.1.4	M	
RLS_XDM-AU-S-004	MIME type of presence list	5.1.5	M	

Item	Function	Reference	Status	Requirement
RLS_XDM-AU-S-005	Validation constraints, in addition to the XML schema	5.1.6	M	
RLS_XDM-AU-S-006	RLS XDMS validates that the Service URI conforms to the additional constraints of local policy.	5.1.6	M	
RLS_XDM-AU-S-007	Data semantics of presence list	5.1.7	M	
RLS_XDM-AU-S-008	Naming conventions for presence list	5.1.8	M	
RLS_XDM-AU-S-009	RLS conforms to resource interdependencies	5.1.10	M	
RLS_XDM-AU-S-010	Authorization policies	5.1.11	M	

A.2 RLS XDM Client Application Usages

Item	Function	Reference	Status	Requirement
RLS_XDM-AU-C-001	Presence list structure	5.1.1	M	
RLS_XDM-AU-C-002	Application Unique ID in presence list	5.1.2	M	
RLS_XDM-AU-C-003	XML schema of presence list	5.1.4	M	
RLS_XDM-AU-C-004	MIME type of presence list	5.1.5	M	
RLS_XDM-AU-C-005	Validation constraints, in addition to the XML schema	5.1.6	M	
RLS_XDM-AU-C-006	Data semantics of presence list	5.1.7	M	
RLS_XDM-AU-C-007	Naming conventions for presence list	5.1.8	M	

Item	Function	Reference	Status	Requirement
RLS_XDM-CAU-C-001	XDM Client handling of HTTP “409 Conflict” response from the RLS XDMS	5.1.6	O	

Appendix B. Examples (Informative)

B.1 Manipulating Presence Lists

B.1.1 Obtaining Presence Lists

Figure B.1 describes how an XDM client obtains Presence Lists.

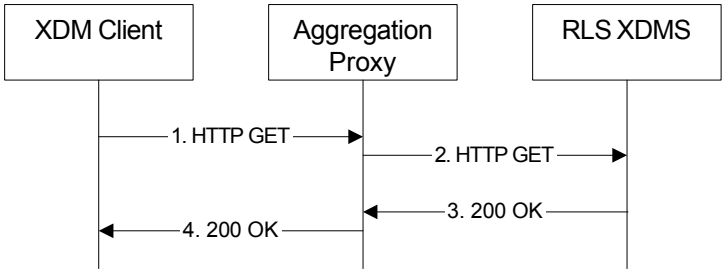

Figure B.1- XDM Client obtains Presence Lists

The details of the flows are as follows:

1) The user "sip:ronald.underwood@example.com" wants to obtain the document describing his Presence Lists. For this purpose the XDMC sends an HTTP GET request to the Aggregation Proxy.

```
GET /rls-services/users/sip:ronald.underwood@example.com/index/ HTTP/1.1
Host: xcap.example.com
...
```

2) Based on the AUID the Aggregation Proxy forwards the request to RLS XDMS.

3) After the RLS XDMS has performed the necessary authorisation checks on the request originator, the RLS XDMS sends an HTTP "200 OK" response including the requested document in the body.

```
HTTP/1.1 200 OK
Etag: "etuk8"
...
Content-Type: application/rls-services+xml

<?xml version="1.0" encoding="UTF-8"?>
<rls-services xmlns="urn:ietf:params:xml:ns:rls-services"
   xmlns:rl="urn:ietf:params:xml:ns:resource-lists">
  <service uri="sip:mysociety@example.com">
    <resource-list>http://xcap.example.com/resource-lists/users/sip:
   ronald.underwood@example.com/~~
/resource-lists/list%5b@name=%22spew%22%5d</resource-list>
    <packages>
      <package>presence</package>
    </packages>
  </service>
  <service uri="sip:friends@example.com">
    <list name="friends">
      <rl:entry uri="sip:hermione.blossom@example.com"/>
      <rl:entry uri="tel:5678;phone-context=+43012349999"/>
    </list>
    <packages>
      <package>presence</package>
    </packages>
  </service>
</rls-services>
```

NOTE: The <resource-list> field represents a pointer to an external list located on the Shared XDMS enabler

4) The Aggregation Proxy routes the response to the XDM Client.

B.1.2 Service URI negotiation

Figure B.2 describes how the RLS XDMS can negotiate a Service URI.

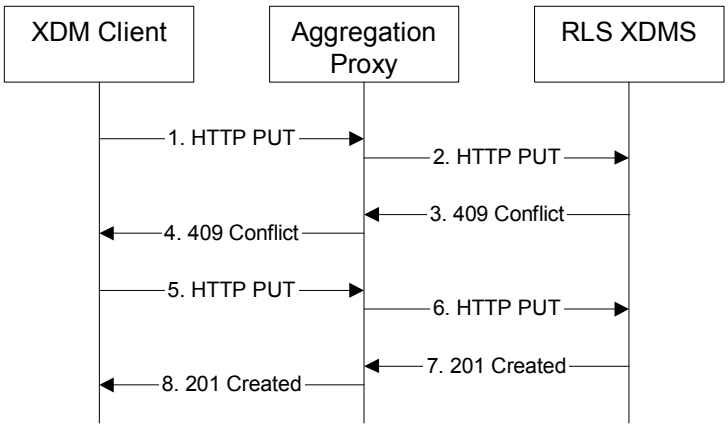

Figure B.2 - RLS XDMS negotiates a Service URI

The details of the flows are as follows:

1) The user "sip:ronald.underwood@example.com" wants to create a Service URI "sip:wrongname@example.com". For this purpose the XDMC sends an HTTP PUT request to the Aggregation Proxy.

```
PUT /rls-services/users/sip:ronald.underwood@example.com/index/~~/rls-services/service HTTP/1.1
Host: xcap.example.com
...
Content-Type: application/xcap-el+xml
Content-Length: (...)

<service uri="sip:wrongname@example.com">
  <list name="family">
    <rl:entry uri="sip:vernon.keel@example.com"/>
  </list>
  <packages>
    <package>presence</package>
  </packages>
</service>
```

2) Based on the AUID the Aggregation Proxy forwards the request to RLS XDMS.

3) The RLS XDMS detects that the Service URI does not conform to the local policy. The RLS XDMS generates a valid Service URI "sip:correctname@example.com" and sends an HTTP "409 Conflict" response including the generated URI.

```
HTTP/1.1 409 Conflict
...
Content-Type: application/xcap-error+xml

<?xml version="1.0" encoding="UTF-8"?>
<xcap-error xmlns="urn:ietf:params:xml:ns:xcap-error">
  <uniqueness-failure>
    <exists field="service/@uri">
      <alt-value>sip:correctname@example.com</alt-value>
    </exists>
  </uniqueness-failure>
</xcap-error>
```

4) The Aggregation Proxy routes the response to the XDM Client.

5) The XDM Client repeats the XCAP request (sent in step 1) using the received Service URI.

```
PUT /rls-services/users/sip:ronald.underwood@example.com/index/~~/rls-services/service HTTP/1.1
Host: xcap.example.com
...
Content-Type: application/xcap-el+xml
Content-Length: (...)

<service uri="sip:correctname@example.com">
  <list name="family">
    <rl:entry uri="sip:vernon.keel@example.com"/>
  </list>
  <packages>
    <package>presence</package>
  </packages>
</service>
```

6) Based on the AUID the Aggregation Proxy forwards the request to RLS XDMS.

7) The RLS XDMS creates the requested Presence List document and sends an HTTP “201 Created” response.

```
HTTP/1.1 201 Created
Etag: "etu65"
...
Content-Length: 0
```

8) The Aggregation Proxy routes the response to the XDM Client.

Appendix C. Change History (Informative)

C.1 Approved Version History

Reference	Date	Description
OMA-TS-Presence_SIMPLE_RLS_XDM-V1_0-20060725-A	25 Jul 2006	TP approved: OMA-TP-2006-0223R04-INP_Presence_SIMPLE_V1_0_for_final_approval
OMA-TS-Presence_SIMPLE_RLS_XDM -V1_0_1-20061128-A	28 Nov 2006	CRs incorporated: OMA-PAG-2006-0664 OMA-PAG-2006-0704R02 OMA-PAG-2006-0747R02

C.2 Draft/Candidate Version 1.1 History

Document Identifier	Date	Sections	Description
Draft Version OMA-TS-Presence_SIMPLE_ RLS_XDM -V1_1	01 Jul 2007	6, A.3	Baseline based on OMA-TS-Presence_SIMPLE_RLS_XDM -V1_0_1-20061128-A, created as per OMA-PAG-2007-0400R01-INP_PRS_1_1_baseline Incorporated CR: OMA-PAG-2007-0345
	30 Aug 2007	2.1, 3.2, 5.1,	Incorporated CRs: OMA-PAG-2007-0514 OMA-PAG-2007-0542
	26 Nov 2007	2, Appendix A	Incorporated CRs: OMA-PAG-2007-0714R01
	11 Dec 2007	All	Editorial changes
	12 Dec	2.1	Editorial changes
Candidate Versions OMA-TS-Presence_SIMPLE_ RLS_XDM -V1_1	28 Jan 2008	n/a	Status changed to Candidate by TP TP ref # OMA-TP-2007-0506R02-INP_Presence_Simple_V1_1_for_Candidate_approval