Resource List Server (RLS) XDM Specification

Candidate Version 1.0 – 28 Jun 2005

Open Mobile Alliance

OMA-TS-Presence_SIMPLE_RLS_XDM-V1_0-20050628-C

Contents

1. SCOPE 4
2. REFERENCES 5
2.1 NORMATIVE REFERENCES 5
2.2 INFORMATIVE REFERENCES 5
3. TERMINOLOGY AND CONVENTIONS 6
3.1 CONVENTIONS 6
3.2 DEFINITIONS 6
3.3 ABBREVIATIONS 6
4. INTRODUCTION 7
5. RLS XDM APPLICATION USAGES 8
5.1 PRESENCE LIST 8
5.1.1 Structure 8
5.1.2 Application Unique ID 8
5.1.3 Default Namespace 8
5.1.4 XML Schema 8
5.1.5 MIME Type 8
5.1.6 Validation constraints 8
5.1.7 Data Semantics 8
5.1.8 Naming conventions 9
5.1.9 Global documents 9
5.1.10 Resource interdependencies 9
5.1.11 Authorization policies 9
6. SUBSCRIBING TO CHANGES IN THE XML DOCUMENTS 9
APPENDIX A. STATIC CONFORMANCE REQUIREMENTS (NORMATIVE) 10
A.1 RLS XDM SERVER APPLICATION USAGES 10
A.2 XDM CLIENT FOR RLS APPLICATION USAGES 11
A.3 SUBSCRIBING TO CHANGES IN THE XML DOCUMENTS 12
APPENDIX B. EXAMPLES (INFORMATIVE) 13
B.1 MANIPULATING PRESENCE LISTS 13
B.1.1 Obtaining Presence Lists 13
B.1.2 Service URI negotiation 14
APPENDIX C. CHANGE HISTORY (INFORMATIVE) 16
C.1 APPROVED VERSION HISTORY 16
C.2 CANDIDATE VERSION 1.0 HISTORY 16

Figures

Figure B.1- XDM Client obtains Presence Lists 13
Figure B.2 - RLS XDMS negotiates a Service URI 14

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

[IOPPROC] "OMA Interoperability Policy and Process", Version 1.1, Open Mobile Alliance™, OMA-IOP-Process-V1_1, URL: http://www.openmobilealliance.org/

[XDMRD] "XML Document Management Requirements", Version 1.0, Open Mobile Alliance™, OMA-RD-XDM-V1_0, URL: http://www.openmobilealliance.org/

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

[RFC2234] "Augmented BNF for Syntax Specifications: ABNF". D. Crocker, Ed., P. Overell. November 1997, URL: http://www.ietf.org/rfc/rfc2234.txt

[XCAP] "The Extensible Markup Language (XML) Configuration Access protocol (XCAP)", J. Rosenberg, June 11, 2005, URL: http://www.ietf.org/internet-drafts/draft-ietf-simple-xcap-07.txt

Note: IETF Draft work in progress

[XCAP_List] "Extensible Markup Language (XML) Formats for Representing Resource Lists", J. Rosenberg, February 7, 2005, URL: http://www.ietf.org/internet-drafts/draft-ietf-simple-xcap-list-usage-05.txt

Note: IETF Draft work in progress

[XDM_Spec] "XML Document Management (XDM) Specification", Version 1.0, Open Mobile Alliance™, OMA-TS-XDM_Core-V1_0, URL: http://www.openmobilealliance.org/

2.2 Informative References

[XDMAD] "XML Document Management Architecture", Version 1.0, Open Mobile Alliance™, OMA-XDM-AD-V1_0, URL: http://www.openmobilealliance.org/

[PRES_Spec] "Presence SIMPLE Specification", Version 1.0, Open Mobile Alliance™, OMA-TS-Presence_SIMPLE-V1_0, 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 that differentiates XCAP resources accessed by one application from XCAP resources accessed by another. (Source: [XCAP])
Global Document	A document placed under the XCAP global tree that applies to all users of that application usage.
Global Tree	A URL that represents the parent for all global documents for a particular application usage within a particular XCAP root. (Source: [XCAP])
XCAP Application Usage	Detailed information on the interaction of an application with an XCAP server. (Source: [XCAP])
XCAP Client	An HTTP client that understands how to follow the naming and validation constraints defined in [XCAP]. (Source: [XCAP])
XCAP Server	An HTTP server that understands how to follow the naming and validation constraints defined in [XCAP]. (Source: [XCAP])

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 [XCAP_List] 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 [XCAP_List] 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 [XCAP_List] section 4.4.4.

5.1.4 XML Schema

A Presence List document SHALL conform to the XML schema described in [XCAP_List] 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 [XCAP_List] 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 [XCAP_List] section 4.4.5, with the following clarifications:

The value of the "uri" attribute of 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_Spec]), which is stored in the RLS XDMS and provisioned to the XDM Client.

NOT violate the "uniqueness constraint" defined in [XCAP_List] 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 [XCAP].

If the <uniqueness-failure> element in the received HTTP "409 Conflict" response includes an "alt-value" element, the XDM Client SHOULD repeat the XCAP request using one of the Service URI provided in the received "alt-value" element.

5.1.7 Data Semantics

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

5.1.8 Naming conventions

The naming conventions of a Presence List document SHALL conform to those described in [XCAP_List] 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 Present List documents that exist in the XCAP user tree, this application usage defines a single global document, “index”, created by the RLS XDMS in the XCAP global tree, as described in [XCAP_List] section 4.4.8.

5.1.10 Resource interdependencies

The RLS XDMS SHALL conform to the resource interdependencies described in [XCAP_List] 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 [XDMSPEC] 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.

6. Subscribing to Changes in the XML Documents

The RLS XDMS SHALL support subscriptions to changes in the XML documents as defined by the procedures in section 6.2.2 of [XDM_Spec].

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 [RFC2234].

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	

A.3 Subscribing to changes in the XML documents

Item	Function	Reference	Status	Requirement
RLS_XDM-SU-S-001	Generating a NOTIFY request	[XDM_Spec] 6.2.2.2	M	

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.

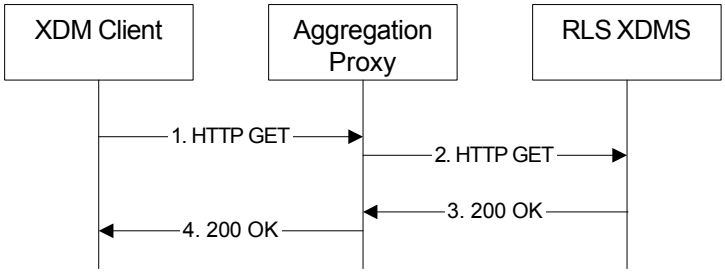

Figure B.1- XDM Client obtains Presence Lists

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 http://xcap.example.com/services/rls-services/users/sip:ronald.underwood@example.com/index/
   HTTP/1.1
...
Content-Length: 0
```

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"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <service uri="sip:mysociety@example.com">
    <resource-list>http://xcap.example.com/services/resource-
   lists/users/sip:hermione.blossom@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>
```

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.

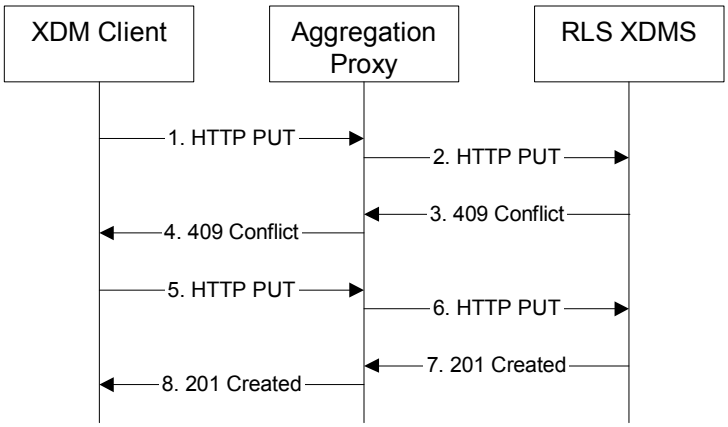

Figure B.2 - RLS XDMS negotiates a Service URI

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 http://xcap.example.com/services/rls-services/users/sip:ronald.underwood@example.com/index/~~
   /rls-services/service HTTP/1.1
...
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 http://xcap.example.com/services/rls-services/users/sip:ronald.underwood@example.com/index/~~
   /rls-services/service HTTP/1.1
...
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
n/a	n/a	No prior version

C.2 Candidate Version 1.0 History

Document Identifier	Date	Sections	Description
Draft Version OMA-RLS_XDM_Specification-V1_0	27 Sept 2004	All	Initial version created.
	15 Oct 2004	All	Incorporates input to committee: OMA-PAG-2004-0544R02-RLS-XDM-Specification OMA-PAG-2004-0547-RLS-XDMS-MessageFlowExample
	22 Oct 2004	5.2.1, 5.3.5, Appendix B	Incorporates input to committee: OMA-PAG-2004-0559-RLS-XDMS-ServiceURINegotiation
	26 Oct 2004	5.2.1, 5.3.5	Incorporates input to committee: OMA-PAG-2004-0588R02-RLS-XDM-Specification
	1 Nov 2004	Appendix A	Incorporates input to committee: OMA-PAG-2004-0618R01-RLS-XDM-SCR
	12 Nov 2004	5.3.5	Incorporates OMA-PAG-2004-0649R02- RLS-XDMS-Uniqueness-of-URI-attribute-value
		5.1, 5.2	Incorporates OMA-PAG-2004-0686R02-RLS-XDM-functional-entity-description
	15 Nov 2004	Appendix A	Incorporates OMA-PAG-2004-0727-RLS-XDM-Spec-SCR-changes
	17 Nov 2004	2, 3	Editor cleanup of references, definitions, and abbreviations
OMA-TS-Presence_SIMPLE_RLS_XDM-V1_0	21 Feb 2005	Various	Incorporates resolutions to CONRR RLS XDM comments 3, 4, 5, 6, 7, 10, 11, 13, 14, 15, and editorials. Also incorporates OMA-PAG-2005-0015R01.
	3 Mar 2005	Various	Incorporates OMA-PAG-2005-0194.
	4 Mar 2005	5.1.11, 6, A.3	Incorporates OMA-PAG-2005-0085R01 and -0252R01.
	8 Mar 2005	Appendix A	Editor cleanup of section references.
Candidate Versions OMA-TS-Presence_SIMPLE_RSL_XDM-V1_0	17 Mar 2005		Status changed to Candidate by TP: OMA ref# OMA-TP-2005-0093R01-Presence-SIMPLE-V1_0-for-Candidate-approval
Candidate Versions OMA-TS-Presence_SIMPLE_RSL_XDM-V1_0	15 Apr 2005	2.1	Incorporates OMA-PAG-2005-0194.R01
Candidate Versions OMA-TS-Presence_SIMPLE_RSL_XDM-V1_0	24 May 2005	5.1.6	Incorporates OMA-PAG-2005-0328
Candidate Versions OMA-TS-Presence_SIMPLE_RSL_XDM-V1_0	14 Jun 2005	A.2	Incorporates OMA-PAG-2005-0372
Candidate Versions OMA-TS-Presence_SIMPLE_RSL_XDM-V1_0	28 Jun 2005	2.1	Incorporate OMA-PAG-2005-0366