Presence XDM Specification

Approved Version 1.1.1 – 25 Feb 2010

Open Mobile Alliance

OMA-TS-Presence_SIMPLE_XDM-V1_1_1-20100225-A

Contents

Figures

1. Scope

The Presence XDMS specific data formats and XCAP application usages are described in this specification.

2. References

2.1 Normative References

[PRESDDS] "Presence SIMPLE Data Specification", Version 1_0, Open Mobile Alliance™, OMA-DDS-Presence_SIMPLE-V1_0,
URL: http://www.openmobilealliance.org/

[PRESSPEC] "Presence SIMPLE Specification", Version 1_1, Open Mobile Alliance™, OMA-TS-Presence_SIMPLE-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

[RFC4745] IETF RFC 4745 "Common Policy: A Document Format for Expressing Privacy Preferences", H. Schulzrinne, J. Morris, H. Tschofenig, J. Cuellar, J. Polk, J. Rosenberg, February 2007,
URL: http://www.ietf.org/rfc/rfc4745.txt

[RFC5025] "Presence Authorization Rules", J. Rosenberg, December 2007, RFC 5025,
URL: http://www.ietf.org/rfc/rfc5025.txt

[XDMSPEC] "XML Document Management (XDM) Specification", Version 1_1, Open Mobile Alliance™, OMA-TS-XDM_Core-V1_1,
URL: http://www.openmobilealliance.org/

[XSD-PRESRULES] "Presence SIMPLE – Presrules", Version 1.0, Open Mobile Alliance™, OMA-SUP-XSD_prs_presrules-V1_0,
URL: http://www.openmobilealliance.org/Technical/schemas.aspx

2.2 Informative References

[PRESAD] "Stage 2 - Presence using SIMPLE", Version 1_1, Open Mobile Alliance™, OMA-AD-Presence_SIMPLE-V1_1,
URL: http://www.openmobilealliance.org/

3. Terminology and Conventions

3.1 Conventions

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

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

3.2 Definitions

Application Unique ID	A unique identifier within the namespace of application unique IDs created by this specification 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])
Presence Content Rules	Presence Content Rules determine which Presence Information is disseminated to Watchers that have been accepted by Subscription Authorisation Rules. A Presentity can define Presence Content Rules that apply to one or more Watchers. (Source: [PRESAD])
Subscription Authorisation Rules	Subscription Authorisation Rules determine those Watchers who are allowed to subscribe to the Presence Information of a Presentity and those who are not allowed. The Subscription Authorisation Rules may include lists that can be stored in the Presence XDMS or the Shared XDMS. (Source: [PRESAD])
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
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

This specification describes the structure of a particular type of XML document used for watcher authorisation in the Presence service. As stated in [PRESAD] there are two different “levels” of a watcher authorisation: subscription authorisation and presence content authorisation. The former defines if a watcher is allowed to subscribe to a presentity’s presence information, and the latter the limitations in presence information that the watcher can get.

This specification provides the XCAP application usage of the Presence Authorisation Rules. It reuses the document structure described in [RFC5025].

The Presence XDMS (see [PRESAD]) is the logical repository for Presence Authorisation Rules documents. The common protocol specified in [XDMSPEC] is used for access and manipulation of such Presence Authorisation Rules by authorized principals.

5. Presence XDM Application Usages

5.1 Presence Authorisation Rules

The Presence Authorisation Rules document contains the following set of rules:

- Subscription Authorisation Rules, which determine if a Watcher is allowed to subscribe to the Presentity's Presence Information; and
- Presence Content Rules, which determine the subset of the Presentity's Presence Information the Watcher is allowed to receive.

These rules SHALL be described in one single XML document.

The application usage of the Presence Authorisation Rules document is described in the subsections below.

5.1.1 Subscription Authorisation Rules

5.1.1.1 Structure

The Subscription Authorization Rules SHALL conform to the structure of the "pres-rules" document described in [RFC5025] and extended in [XDMSPEC] section 6.6.2, with the extensions and constraints given in this sub-clause.

As described in [RFC5025] section 1, the Presence Authorisation Rules document contains a sequence of <rule> elements, each composed of up to three parts:

a. "conditions"

b. "actions"

c. "transformations"

The Subscription Authorisation Rules are described from the <conditions> and <actions> 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 [XDMSPEC] Section 6.6.2;

c. the <other-identity> element as defined in [XDMSPEC] Section 6.6.2;

d. the <anonymous-request> element as defined in [XDMSPEC] Section 6.6.2.

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

5.1.1.2 Application Unique ID

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

5.1.1.3 Default Namespace

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

5.1.1.4 XML Schema

The Subscription Authorisation Rules SHALL be composed according to the XML Schema detailed in [RFC5025] section 6 and extended in [XDMSPEC] section 6.6.2.

5.1.1.5 MIME Type

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

5.1.1.6 Validation constraints

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

The <conditions> element SHALL contain no more than one of the <identity>, <external-list>, <other-identity> or <anonymous-request> element. If this constraint is violated, an HTTP 409 (Conflict) response SHALL be returned including the error element <constraint-failure>. If included, the “phrase” attribute of this element SHOULD be set to “Complex rules are not allowed”.

5.1.1.7 Data Semantics

The data semantics SHALL conform to the semantics defined in [RFC5025] and extended in [XDMSPEC] section 6.6.2.

5.1.1.8 Naming conventions

The name of the Presence Authorisation Rules document containing the Subscription Authorisation Rules SHALL be “pres-rules”.

5.1.1.9 Global documents

This application usage defines no global documents.

5.1.1.10 Resource interdependencies

This application usage defines no additional resource interdependencies.

5.1.1.11 Authorisation policies

The authorisation policies SHALL be defined according to [XDMSPEC] section 6.4.3.

5.1.2 Presence Content Rules

5.1.2.1 Structure

The Presence Content Rules SHALL conform to the structure of the “pres-rules” document described in [RFC5025] and extended in [XDMSPEC] section 6.6.2, with the clarifications given below.

The Presence Content Rules are described from the <transformations> element of the Presence Authorisation Rules document.

The <transformations> element SHALL be used to define the visibility a watcher is granted to a particular component of the Presence documents as described in [RFC5025] section 3.3.

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

a. the <provide-persons> element as described in [RFC5025] section 3.3.1.2;

b. the <provide-devices> element as described in [RFC5025] section 3.3.1.1;

c. the <provide-services> element as described in [RFC5025] section 3.3.1.3;

d. the <provide-willingness> element as described in section 5.1.2.7;

e. the <provide-network-availability> element as described in section 5.1.2.7;

f. the <provide-session-participation> element as described in section 5.1.2.7;

g. the <provide-activities> element as described in [RFC5025] section 3.3.2.1;

h. the <provide-class> element as described in [RFC5025] section 3.3.2.2;

i. the <provide-mood> element as described in [RFC5025] section 3.3.2.4;

j. the <provide-place-type> element as described in [RFC5025] section 3.3.2.6;

k. the <provide-status-icon> element as described in [RFC5025] section 3.3.2.10;

l. the <provide-time-offset> element as described in [RFC5025] section 3.3.2.11;

m. the <provide-note> element as described in [RFC5025] section 3.3.2.13;

n. the <provide-geopriv> element as described in section 5.1.2.7;

o. the <provide-all-attributes> element as described in [RFC5025] section 3.3.2.15.

p. the <provide-registration-state> element as described in section 5.1.2.7;

q. the <provide-barring-state> element as described in section 5.1.2.7;

r. the <provide-unknown-attribute> element as described in [RFC5025] section 3.3.2.14.

Other types of <transformations> elements described in [RFC5025] are not defined by this specification. The <provide-services> element MAY include either the <all-services> child element, or a sequence of zero or more elements, each of which can be:

a. the <class>, the <service-uri>, or the <service-uri-scheme> element as described in [RFC5025] section 3.3.1.3, or;

b. the <service-id> as described in section 5.1.2.7.

The <provide-persons> element MAY include either the <all-persons> child element, or a sequence of zero or more <class> element(s) as described in [RFC5025] section 3.3.1.2.

The <provide-devices> element MAY include either the <all-devices> child element, or a sequence of zero or more <class> or <deviceID> element(s) as described in [RFC5025] section 3.3.1.1.

NOTE: When the <provide-services>, <provide-persons> or <provide-devices> element is present with no child elements, it has the same meaning as if the element wasn't present at all.

5.1.2.2 Application Unique ID

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

5.1.2.3 Default Namespace

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

5.1.2.4 XML Schema

The Presence Content Rules SHALL be composed according to the XML Schema detailed in [RFC5025] section 6 and extended in [XDMSPEC] section 6.6.2, with the extensions given in [XSD_PRESRULES].

5.1.2.5 MIME Type

The MIME type for this application usage SHALL be "application/auth-policy+xml" defined in [RFC4745].

5.1.2.6 Validation constraints

The validation constraints SHALL conform to those imposed by the XML schema with the following clarification:

A <rule> element with a <sub-handling> element value different than “allow” SHALL NOT contain a <transformations> element. If this constraint is violated, an HTTP “409 Conflict” response 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 “<transformations> element not allowed”.

5.1.2.7 Data Semantics

The data semantics SHALL conform to the semantics defined in [RFC5025] and extended in [XDMSPEC] section 6.6.2, together with the clarifications given in this sub-clause.

The <provide-willingness> “transformation” controls access to <willingness> and <overriding-willingness> elements described in [PRESDDS]. The value is of a Boolean type:

“false” instructs the Presence Server to remove the <willingness> and <overriding-willingness> elements if present. This is the default value taken in the absence of the element.

“true” instructs the Presence Server to report the <willingness> and <overriding-willingness> elements to the watcher.

The <provide-network-availability> “transformation” controls access to the <network-availability> element described in [PRESDDS]. The value is of a Boolean type:

“false” instructs the Presence Server to remove the <network-availability> element if present. This is the default value taken in the absence of the element.

“true” instructs the Presence Server to report the <network-availability> element to the watcher.

The <provide-session-participation> “transformation” controls access to the <session-participation> element described in [PRESDDS]. The value is of a Boolean type:

“false” instructs the Presence Server to remove the <session-participation> element if present. This is the default value taken in the absence of the element.

“true” instructs the Presence Server to report the <session-participation> element to the watcher.

The <provide-registration-state> “transformation” controls access to the <registration-state> element described in [PRESDDS]. The value is of a Boolean type:

“false” instructs the Presence Server to remove the <registration-state> element if present. This is the default value taken in the absence of the element.

“true” instructs the Presence Server to report the <registration-state> element to the watcher.

The <provide-barring-state> “transformation” controls access to the <barring-state> element described in [PRESDDS]. The value is of a Boolean type:

“false” instructs the Presence Server to remove the <barring-state> element if present. This is the default value taken in the absence of the element.

“true” instructs the Presence Server to report the <barring-state> element to the watcher.

The <provide-geopriv> “transformation” controls access to the <geopriv> element described in [PRESDDS]. The <provide-geopriv> element is an enumerated integer type, and its value defines what information is provided to watchers:

false: instructs the Presence Server to remove (if present) the <geopriv> element and its child elements. It is assigned the numeric value of zero. This is the default value taken in the absence of the element.

full: instructs the Presence Server to report the <geopriv> element and its child elements to the watcher. It is assigned the numeric value of ten.

The <service-id> identifies service by its service ID described in [PRESDDS].

5.1.2.8 Naming conventions

The name of the Presence Authorization Rules document containing the Presence Content Rules SHALL be “pres-rules”.

5.1.2.9 Global documents

This application usage defines no global documents.

5.1.2.10 Resource interdependencies

This application usage defines no additional resource interdependencies.

5.1.2.11 Authorisation policies

The authorisation policies SHALL be defined according to [XDMSPEC] section 6.4.3.

Appendix A. Static Conformance Requirements (Normative)

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

- Presence XDM Server Application Usages
- Presence XDM Client 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 Presence XDM Server Application Usages

Item	Function	Reference	Status	Requirement
Presence_XDM-AU-S-001	Single XML document describing who can subscribe to a presentity's presence, and content of notifications	5.1	M	

Item	Function	Reference	Status	Requirement
Presence_XDM-AU-S-002	Structure of Presence Authorisation Rules XML document, and function of Subscription Authorization and Presence Content parts	5.1.1.1 5.1.2.1	M	
Presence_XDM-AU-S-003	Application Unique ID in Presence Authorisation Rules XML document	5.1.1.2 5.1.2.2	M	
Presence_XDM-AU-S-004	XML schema, including validation constraints, of Presence Authorisation Rules	5.1.1.4 5.1.1.6 5.1.2.4 5.1.2.6	M	
Presence_XDM-AU-S-005	XML document conforms to MIME type	5.1.1.5 5.1.2.5	M	
Presence_XDM-AU-S-006	Data semantics of Presence Authorisation Rules	5.1.1.7 5.1.2.7	M	
Presence_XDM-AU-S-007	Naming conventions for Presence Authorisation Rules	5.1.1.8 5.1.2.8	M	
Presence_XDM-AU-S-008	Authorization policies	5.1.1.11 5.1.2.11	M	

A.2 Presence XDM Client Application Usages

Item	Function	Reference	Status	Requirement
Presence_XDM-AU-C-001	Single XML document describing who can subscribe to a presentity's presence, and content of notifications	5.1	M	

Item	Function	Reference	Status	Requirement
Presence_XDM-AU-C-002	Structure of Presence Authorisation Rules XML document, and function of Subscription Authorization and Presence Content parts	5.1.1.1 5.1.2.1	M	
Presence_XDM-AU-C-003	Application Unique ID in Presence Authorisation Rules XML document	5.1.1.2 5.1.2.2	M	
Presence_XDM-AU-C-004	XML schema	5.1.1.4 5.1.2.4	M	
Presence_XDM-AU-C-005	XML document conforms to MIME type	5.1.1.5 5.1.2.5	M	
Presence_XDM-AU-C-006	Data semantics of Presence Authorisation Rules	5.1.1.7 5.1.2.7	M	
Presence_XDM-AU-C-007	Naming conventions for Presence Authorisation Rules	5.1.1.8 5.1.2.8	M	

Appendix B. Examples (Informative)

B.1 Manipulating Presence Authorisation Rules

B.1.1 Obtaining Presence Authorisation Rules

Both Subscription Authorisation Rules and Presence Content Rules are stored in one XML document. Figure B.1 describes how XDM client obtains Presence Authorisation Rules.

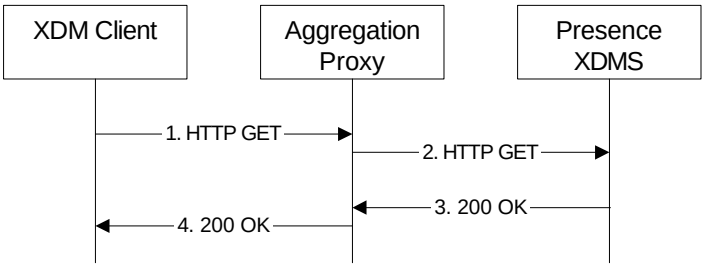

Figure B.1- XDM Client obtains Presence Authorisation Rules

The details of the flows are as follows:

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

```
GET org.openmobilealliance.pres-rules/users/sip:ronald.underwood@example.com/pres-rules HTTP/1.1
Host: xcap.example.com
...
```

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

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

```
HTTP/1.1 200 OK
Etag: "ett5e"
...
Content-Type: application/auth-policy+xml; charset="utf-8"

<?xml version="1.0" encoding="UTF-8"?>
<cr:ruleset
   xmlns:op="urn:oma:xml:prs:pres-rules"
   xmlns:ocp="urn:oma:xml:xdm:common-policy"
   xmlns:pr="urn:ietf:params:xml:ns:pres-rules"
   xmlns:cr="urn:ietf:params:xml:ns:common-policy">
```

```
<cr:rule id="wp_prs_allow_own">
    <cr:conditions>
      <cr:identity>
        <cr:one id="sip:ronald.underwood@example.com"/>
      </cr:identity>
    </cr:conditions>
    <cr:actions>
      <pr:sub-handling>allow</pr:sub-handling>
    </cr:actions>
    <cr:transformations>
      <pr:provide-services>
        <pr:all-services/>
      </pr:provide-services>
      <pr:provide-persons>
        <pr:all-persons/>
      </pr:provide-persons>
      <pr:provide-devices>
        <pr:all-devices/>
      </pr:provide-devices>
      <pr:provide-all-attributes/>
    </cr:transformations>
  </cr:rule>

  <cr:rule id="wp_prs_unlisted">
    <cr:conditions>
      <ocp:other-identity/>
    </cr:conditions>
    <cr:actions>
      <pr:sub-handling>confirm</pr:sub-handling>
    </cr:actions>
  </cr:rule>


  <cr:rule id="wp_prs_allow_one_1">
    <cr:conditions>
      <cr:identity>
        <cr:one id="tel:+43012345678"/>
              </cr:identity>
    </cr:conditions>
    <cr:actions>
      <pr:sub-handling>allow</pr:sub-handling>
    </cr:actions>
    <cr:transformations>
      <pr:provide-services>
        <op:service-id>org.openmobilealliance:PoC-session</op:service-id>
      </pr:provide-services>
      <op:provide-willingness>true</op:provide-willingness>
      <pr:provide-status-icon>true</pr:provide-status-icon>
    </cr:transformations>
  </cr:rule>

<cr:rule id="wp_prs_allow_one_2">
    <cr:conditions>
      <cr:identity>
        <cr:one id="sip:hermione.blosom@example.com"/>
      </cr:identity>
    </cr:conditions>
    <cr:actions>
      <pr:sub-handling>allow</pr:sub-handling>
    </cr:actions>
    <cr:transformations>
      <pr:provide-services>
        <op:service-id>org.openmobilealliance:PoC-alert</op:service-id>
      </pr:provide-services>
      <op:provide-willingness>true</op:provide-willingness>
    </cr:transformations>
  </cr:rule>

</cr:ruleset>
```

4) 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_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_XDM-V1_0_1-20061128-A	28 Nov 2006	Incorporated CRs: OMA-PAG-2006-0404 OMA-PAG-2006-0503 OMA-PAG-2006-0666 OMA-PAG-2006-0746R01
OMA-TS-Presence_SIMPLE_XDM-V1_1-20080627-A	27 Jun 2008	Status changed to Approved by TP TP ref# OMA-TP-2008-0250-INP_Presence_SIMPLE_V1_1_ERP_for_Final_Approval
OMA-TS-Presence_SIMPLE_XDM-V1_1_1-20090310-D	10 Mar 2009	Incorporated CR: OMA-PAG-2008-0825 Updated hyperlink in section 2.1 according to PAG-09-001R&A comment.
OMA-TS-Presence_SIMPLE_XDM-V1_1_1-20100225-A	25 Feb 2010	Status changed to Approved by TP TP ref# OMA-TP-2010-0110-INP_Presence_SIMPLE_V1_1_1_ERP_for_notification