Presence XDM Specification
Approved Version 1.0 – 25 Jul 2006

Open Mobile Alliance
OMA-TS-Presence_SIMPLE_XDM-V1_0-20060725-A
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. PRESENCE XDM APPLICATION USAGES ................................................................... 8
   5.1 PRESENCE AUTHORISATION RULES ..................................................................... 8
      5.1.1 Subscription Authorisation Rules ................................................................. 8
      5.1.2 Presence Content Rules ............................................................................... 9
      5.1.3 Default Namespace ..................................................................................... 10
      5.1.4 XML Schema .............................................................................................. 10
      5.1.5 MIME Type .................................................................................................. 11
      5.1.6 Validation constraints ................................................................................ 11
      5.1.7 Data Semantics ........................................................................................... 12
      5.1.8 Naming conventions .................................................................................... 12
      5.1.9 Global documents ....................................................................................... 12
      5.1.10 Resource interdependencies ................................................................. 12
      5.1.11 Authorisation policies ............................................................................... 12
   5.1.2 Presence Content Rules ............................................................................... 9
      5.1.2.1 Structure .................................................................................................. 9
      5.1.2.2 Application Unique ID ........................................................................... 10
      5.1.2.3 Default Namespace .............................................................................. 10
      5.1.2.4 XML Schema .......................................................................................... 10
      5.1.2.5 MIME Type ............................................................................................ 11
      5.1.2.6 Validation constraints ........................................................................... 11
      5.1.2.7 Data Semantics ...................................................................................... 12
      5.1.2.8 Naming conventions ............................................................................. 12
      5.1.2.9 Global documents ................................................................................... 12
      5.1.2.10 Resource interdependencies .............................................................. 12
      5.1.2.11 Authorisation policies ................................................................. 12
6. SUBSCRIBING TO CHANGES IN THE XML DOCUMENTS ........................................ 13
APPENDIX A. STATIC CONFORMANCE REQUIREMENTS (NORMATIVE) ................. 14
   A.1 PRESENCE XDM SERVER APPLICATION USAGES ............................................. 14
   A.2 PRESENCE XDM CLIENT APPLICATION USAGES ........................................... 15
   A.3 SUBSCRIBING TO CHANGES IN THE XML DOCUMENTS ................................ 16
APPENDIX B. EXAMPLES (INFORMATIVE) ................................................................. 17
   B.1 MANIPULATING PRESENCE AUTHORISATION RULES ................................ 17
      B.1.1 Obtaining Presence Authorisation Rules ............................................... 17
APPENDIX C. CHANGE HISTORY (INFORMATIVE) .................................................... 19
   C.1 APPROVED VERSION HISTORY ........................................................................ 19

Figures

Figure B.1- XDM Client obtains Presence Authorisation Rules ...................................... 17
1. **Scope**

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

2.1 Normative References


Note: IETF Draft work in progress


Note: IETF Draft work in progress


Note: IETF Draft work in progress


2.2 Informative References


[PRESAD] “Stage 2 - Presence using SIMPLE”, Version 1.0, Open Mobile Alliance™, OMA-AD-Presence_SIMPLE-V1_0, 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 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 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
- **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 [PRESAUTH].

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 a set of rules which determine:

- who is authorised to subscribe to a presentity’s presence information (subscription authorisation rules), and
- the content of notifications sent to each watcher (presence content rules)

These rules SHALL be described in one single XML document.

The authorisation decision in the Presence Server SHALL be determined based on authorisation policies defined by the service provider (local policy) and the Presence Authorisation Rules document stored in the Presence XDMS.

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 [PRESAUTH] and extended in [XDMSPEC] section 6.6.2, with the extensions and constraints given in this sub-clause.

As described in [PRESAUTH] 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 [COMMONPOL];
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 [PRESAUTH] section 3.2.1.

Other child elements of the <conditions> and <actions> elements described in [PRESAUTH] are not defined by this specification.

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 [COMMONPOL].
5.1.1.4 XML Schema

The Subscription Authorisation Rules SHALL be composed according to the XML Schema detailed in [PRESAUTH] 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 [COMMONPOL].

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 child element of <identity>, <external-list>, <other-identity> or <anonymous-request>.

5.1.1.7 Data Semantics

The data semantics SHALL conform to the semantics defined in [PRESAUTH] 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 [PRESAUTH] 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 [PRESAUTH] 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 [PRESAUTH] section 3.3.1.2;

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

c. the <provide-services> element as described in [PRESAUTH] 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 [PRESAUTH] section 3.3.2.1;

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

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

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

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

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

m. the <provide-note> element as described in [PRESAUTH] 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 [PRESAUTH] 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 [PRESAUTH] section 3.3.2.14.

Other types of <transformations> elements described in [PRESAUTH] 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 [PRESAUTH] 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 [PRESAUTH] 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 [PRESAUTH] 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 [COMMONPOL].

### 5.1.2.4 XML Schema

The Presence Content Rules SHALL be composed according to the XML Schema detailed in [PRESAUTH] 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 [COMMONPOL].

5.1.2.6 Validation constraints

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

5.1.2.7 Data Semantics

The data semantics SHALL conform to the semantics defined in [PRESAUTH] 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 defined in [PRESSPEC]. 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 defined in [PRESSPEC]. 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 defined in [PRESSPEC]. 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 defined in [PRESSPEC]. 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 defined in [PRESSPEC]. 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 defined in [RFC4119]. 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 0. 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 1.

The `<service-id>` identifies service by its service ID defined in [PRESSPEC].

### 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.
6. Subscribing to changes in the XML documents

The Presence XDMS SHALL support subscriptions to changes in the XML documents as defined by the procedures in section 6.2.2.1 step 2 to step 6, and 6.2.2.2 of [XDMSPEC].
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 [RFC2234].

\[
\text{TerminalExpression} = \text{ScrReference} / \text{NOT TerminalExpression} / \text{TerminalExpression LogicalOperator TerminalExpression} / \text{(" TerminalExpression ")}
\]

\[
\text{ScrReference} = \text{ScrItem} / \text{ScrGroup}
\]

\[
\text{ScrItem} = \text{SpecScrName "–" GroupType "–" DeviceType "–" NumericId} / \text{SpecScrName "–" DeviceType "–" NumericId}
\]

\[
\text{ScrGroup} = \text{SpecScrName ":" FeatureType} / \text{SpecScrName "– " GroupType "–" DeviceType "–" FeatureType}
\]

\[
\text{SpecScrName} = 1*\text{Character};
\]

\[
\text{GroupType} = 1*\text{Character};
\]

\[
\text{DeviceType} = "C" / "S"; C – client, S – server
\]

\[
\text{NumericId} = \text{Number Number Number}
\]

\[
\text{LogicalOperator} = "AND" / "OR"; AND has higher precedence than OR and OR is inclusive
\]

\[
\text{FeatureType} = "MCF" / "OCF" / "MSF" / "OSF"; \text{See Section A.1.6}
\]

\[
\text{Character} = %x41-5A ; A-Z
\]

\[
\text{Number} = %x30-39 ; 0-9
\]

A.1 Presence XDM Server Application Usages

<table>
<thead>
<tr>
<th>Item</th>
<th>Function</th>
<th>Reference</th>
<th>Status</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Presence_XDM-AU-S-001</td>
<td>Single XML document describing who can subscribe to a presentity’s presence, and content of notifications</td>
<td>5.1</td>
<td>M</td>
<td></td>
</tr>
<tr>
<td>Item</td>
<td>Function</td>
<td>Reference</td>
<td>Status</td>
<td>Requirement</td>
</tr>
<tr>
<td>-------------------</td>
<td>---------------------------------------------------------------------------</td>
<td>-----------</td>
<td>--------</td>
<td>-------------</td>
</tr>
<tr>
<td>Presence_XDM-AU-S-002</td>
<td>Structure of Presence Authorisation Rules XML document, and function of Subscription Authorization and Presence Content parts</td>
<td>5.1.1.1</td>
<td></td>
<td>M</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5.1.2.1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Presence_XDM-AU-S-003</td>
<td>Application Unique ID in Presence Authorisation Rules XML document</td>
<td>5.1.1.2</td>
<td></td>
<td>M</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5.1.2.2</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Presence_XDM-AU-S-004</td>
<td>XML schema, including validation constraints, of Presence Authorisation Rules</td>
<td>5.1.1.4</td>
<td></td>
<td>M</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5.1.1.6</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>5.1.2.4</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>5.1.2.6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Presence_XDM-AU-S-005</td>
<td>XML document conforms to MIME type</td>
<td>5.1.1.5</td>
<td></td>
<td>M</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5.1.2.5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Presence_XDM-AU-S-006</td>
<td>Data semantics of Presence Authorisation Rules</td>
<td>5.1.1.7</td>
<td></td>
<td>M</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5.1.2.7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Presence_XDM-AU-S-007</td>
<td>Naming conventions for Presence Authorisation Rules</td>
<td>5.1.1.8</td>
<td></td>
<td>M</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5.1.2.8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Presence_XDM-AU-S-008</td>
<td>Authorization policies</td>
<td>5.1.1.11</td>
<td></td>
<td>M</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5.1.2.11</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### A.2 Presence XDM Client Application Usages

<table>
<thead>
<tr>
<th>Item</th>
<th>Function</th>
<th>Reference</th>
<th>Status</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Presence_XDM-AU-C-001</td>
<td>Single XML document describing who can subscribe to a presentity’s presence, and content of notifications</td>
<td>5.1</td>
<td></td>
<td>M</td>
</tr>
</tbody>
</table>
### A.3 Subscribing to changes in the XML documents

<table>
<thead>
<tr>
<th>Item</th>
<th>Function</th>
<th>Reference</th>
<th>Status</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>Presence_XDM-SU-S-001</td>
<td>Generating a NOTIFY request</td>
<td>[XDM_Spec] 6.2.2.2</td>
<td>M</td>
<td></td>
</tr>
<tr>
<td>Presence_XDM-SU-S-002</td>
<td>Support Initial Subscription when SUBSCRIBE message received</td>
<td>[XDM-Spec] 6.2.2.1</td>
<td>M</td>
<td></td>
</tr>
<tr>
<td>Presence_XDM-SU-S-003</td>
<td>“Not Implemented” Error Handling or SUBSCRIBE request Handling</td>
<td>[XDM-Spec] 6.2.2.1</td>
<td>M</td>
<td></td>
</tr>
</tbody>
</table>
Appendix B. Examples

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](image)

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 http://xcap.example.com/pres-rules/users/sip:ronald.underwood@example.com/pres-rules HTTP/1.1
   Content-Length: 0
   ```

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
   ```

   ```
   <xml version="1.0" encoding="UTF-8"?>
   <cr:ruleset
      xmlns:op="urn:oma:xml:prs:pres-rules"
      xmlns:pr="urn:ietf:params:xml:ns:pres-rules"
      xmlns:cr="urn:ietf:params:xml:ns:common-policy"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
      <cr:rule id="ck81">
      <cr:identity>
         <cr:one id="tel:+43012345678"/>
         <cr:one id="sip:hermione.blossom@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-session</op:service-id>
         </pr:provide-services>
      </cr:transformations>
   </cr:ruleset>
   ```
4) The Aggregation Proxy routes the response to the XDM Client.
Appendix C. Change History

C.1 Approved Version History

<table>
<thead>
<tr>
<th>Reference</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OMA-TS-Presence_SIMPLE_XDM-V1_0</td>
<td>25 Jul 2006</td>
<td>TP approved: OMA-TP-2006-0223R04-INP_Presence_SIMPLE_V1_0_for_final_approval</td>
</tr>
</tbody>
</table>