



# **Presence XDM Specification**

Approved Version 1.0.1 – 28 Nov 2006

---

**Open Mobile Alliance**  
OMA-TS-Presence\_SIMPLE\_XDM-V1\_0\_1-20061128-A

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.

© 2006 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 .....	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
5.1.1.1 Structure .....	8
5.1.1.2 Application Unique ID .....	8
5.1.1.3 Default Namespace .....	8
5.1.1.4 XML Schema .....	9
5.1.1.5 MIME Type .....	9
5.1.1.6 Validation constraints .....	9
5.1.1.7 Data Semantics .....	9
5.1.1.8 Naming conventions .....	9
5.1.1.9 Global documents .....	9
5.1.1.10 Resource interdependencies .....	9
5.1.1.11 Authorisation policies .....	9
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 .....	11
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

- [COMMONPOL] “A Document Format for Expressing Privacy Preferences”, H. Schulzrinne et al., Mar Aug 2006, URL: <http://www.ietf.org/internet-drafts/draft-ietf-geopriv-common-policy-11.txt>  
Note: IETF Draft work in progress
- [PRESAUTH] “Presence Authorization Rules”, J. Rosenberg, October 22, 2006, URL: <http://www.ietf.org/internet-drafts/draft-ietf-simple-presence-rules-08.txt>  
Note: IETF Draft work in progress
- [PRESSPEC] “Presence SIMPLE Specification”, Version 1.0.1, Open Mobile Alliance™, OMA-TS-Presence\_SIMPLE-V1\_0\_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>
- [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, October 13, 2006, URL: <http://www.ietf.org/internet-drafts/draft-ietf-simple-xcap-12.txt>  
Note: IETF Draft work in progress
- [XDMSPEC] “XML Document Management (XDM) Specification”, Version 1.0.1, Open Mobile Alliance™, OMA-TS-XDM\_Core-V1\_0\_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/tech/profiles/>

### 2.2 Informative References

- [RFC4119] “Presence-based GEOPRIV Location Object Format”, J. Peterson, December 2005, URL: <http://www.ietf.org/rfc/rfc4119.txt>
- [PRESAD] “Stage 2 - Presence using SIMPLE”, Version 1.0.1, Open Mobile Alliance™, OMA-AD-Presence\_SIMPLE-V1\_0\_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

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

### 3.3 Abbreviations

<b>AUID</b>	Application Unique ID
<b>HTTP</b>	Hyper Text Transfer Protocol
<b>IETF</b>	Internet Engineering Task Force
<b>OMA</b>	Open Mobile Alliance
<b>SIP</b>	Session Initiation Protocol
<b>URI</b>	Uniform Resource Identifier
<b>XCAP</b>	XML Configuration Access Protocol
<b>XDM</b>	XML Document Management
<b>XDMS</b>	XML Document Management Server
<b>XML</b>	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].

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	

### A.3 Subscribing to changes in the XML documents

Item	Function	Reference	Status	Requirement
Presence_XDM-SU-S-001	Generating a NOTIFY request	[XDM_Spec] 6.2.2.2	M	
Presence_XDM-SU-S-002	Support Initial Subscription when SUBSCRIBE message received	[XDM-Spec] 6.2.2.1	M	
Presence_XDM-SU-S-003	“Not Implemented” Error Handling or SUBSCRIBE request Handling	[XDM-Spec] 6.2.2.1	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.

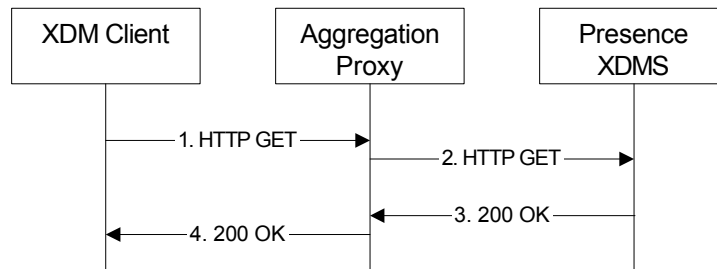


Figure B.1- XDM Client obtains Presence Authorisation Rules

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

<?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">
  <cr:rule id="ck81">
    <cr:conditions>
      <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>
      <op:provide-willingness>true</op:provide-willingness>
      <pr:provide-status-icon>true</pr:provide-status-icon>
    </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