# Presence XDM Specification

Candidate Version 2.0 – 17 Sep 2009

## Open Mobile Alliance

OMA-TS-Presence_SIMPLE_XDM-V2_0-20090917-C

# Contents

# Figures

# 1. Scope

The Presence XDMS specific data formats and Application Usages are described in this specification.

# 2. References

## 2.1 Normative References

**OMA**


**[Dict]** "Dictionary for OMA Specifications", Open Mobile Alliance™,
URL: http://www.openmobilealliance.org/

**[PDE_DDS]** "Presence SIMPLE Data Specification", Version 2.0, Open Mobile Alliance™, OMA-DDS-Presence_Data_Ext-V2_0,
URL: http://www.openmobilealliance.org/

**[PRS_AD]** "Presence SIMPLE Architecture", Version 2.0, Open Mobile Alliance™, OMA-AD-Presence_SIMPLE-V2_0,
URL: http://www.openmobilealliance.org/

**[PRS_RD]** "Presence SIMPLE Requirements", Version 2.0, Open Mobile Alliance™, OMA-RD-Presence_SIMPLE-V2_0,
URL: http://www.openmobilealliance.org/

**[SCRRULES]** "SCR Rules and Procedures", Open Mobile Alliance™, OMA-ORG-SCR_Rules_and_Procedures,
URL: http://www.openmobilealliance.org/

**[XDM_Core]** "XML Document Management (XDM) Specification", Version 2.0, Open Mobile Alliance™, OMA-TS-XDM_Core-V2_0,
URL: http://www.openmobilealliance.org/

**[XDM_RD]** "XML Document Management Requirements", Version 2,0, Open Mobile Alliance™, OMA-RD-XDM-V2_0,
URL: http://www.openmobilealliance.org/

**[XSD_presRules]** "PRS – Pres Rules", Version 1.0, Open Mobile Alliance™, OMA-SUP-XSD_prs_presrules-V1_0,
URL: http://www.openmobilealliance.org/tech/profiles/

**[XSD_pubRules]** "PRS – Pres Pub rules", Version 1.0, Open Mobile Alliance™, OMA-SUP-XSD_prs_pubRules-V1_0,
URL: http://www.openmobilealliance.org/tech/profiles/


**IETF**


**[RFC2119]** IETF RFC 2119 "Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, Mar 1997,
URL: http://www.ietf.org/rfc/rfc2119.txt

**[RFC3863]** IETF RFC 3863 "Presence Information Data Format (PIDF)", H.Sugano et al., Aug 2004,
URL: http://www.ietf.org/rfc/rfc3863.txt

**[RFC4745]** IETF RFC 4745 "Common Policy: A Document Format for Expressing Privacy Preferences", H. Schulzrinne et al., Feb 2007,
URL: http://www.ietf.org/rfc/rfc4745.txt

**[RFC4827]** IETF RFC 4827 "An Extensible Markup Language (XML) Configuration Access Protocol (XCAP) Usage for Manipulating Presence Document Contents", M. Isomaki et al, May 2007,
URL: http://www.ietf.org/rfc/rfc4827.txt

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


## 2.2 Informative References

**OMA**


**[PRS_Spec]** "Presence SIMPLE Specification", Version 2.0, Open Mobile Alliance™, OMA-TS-Presence_SIMPLE-V2_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** | Use definition from [XDM_Core]. |
| **Application Usage** | Use definition from [XDM_Core]. |
| **Global Document** | Use definition from [XDM_Core]. |
| **Global Tree** | Use definition from [XDM_Core]. |
| **Permanent Presence State** | Use definition from [PRS_AD]. |
| **Presence Information** | Use definition from [PRS_RD]. |
| **Presence Publication Rules** | Use definition from [PRS_AD]. |
| **Presence Subscription Rules** | Use definition from [PRS_AD]. |
| **Presentity** | Use definition from [PRS_RD]. |
| **Primary Principal** | Use definition from [XDM_RD]. |
| **Principal** | Use definition from [Dict]. |
| **Publication Authorization Rules** | Use definition from [PRS_AD]. |
| **Publication Content Rules** | Use definition from [PRS_AD]. |
| **Subscription Authorization Rules** | Use definition from [PRS_AD]. |
| **Subscription Content Rules** | Use definition from [PRS_AD]. |
| **Watcher** | Use definition from [PRS_RD]. |
| **XCAP Resource** | Use definition from [XDM_Core]. |
| **XCAP Root** | Use definition from [XDM_Core]. |
| **XCAP Server** | Use definition from [XDM_Core]. |
| **XCAP User Identifier** | Use definition from [XDM_Core]. |

## 3.3 Abbreviations

| | |
|---|---|
| **AUID** | Application Unique ID |
| **HTTP** | Hyper Text Transfer Protocol |
| **IETF** | Internet Engineering Task Force |
| **MIME** | Multipurpose Internet Mail Extensions |

| | |
|---|---|
| **OMA** | Open Mobile Alliance |
| **PS** | Presence Server |
| **SIMPLE** | SIP for Messaging and Presence Leveraging Extensions |
| **SIP** | Session Initiation Protocol |
| **URI** | Uniform Resource Identifier |
| **XCAP** | XML Configuration Access Protocol |
| **XDM** | XML Document Management |
| **XDMC** | XML Document Management Client |
| **XDMS** | XML Document Management Server |
| **XML** | eXtensible Markup Language |
| **XUI** | XCAP User Identifier |

# 4. Introduction

This specification provides the Application Usages for the XML documents related to a Presentity. The Presence XDMS (see [PRS_AD]) is the logical repository for these documents. The common protocol specified in [XDM_Core] is used for access and manipulation of the documents by authorized Principals.

## 4.1 Version 1.1

### 4.1.1 Version 1.1.1

The OMA PRS 1.1.1 enabler defines the following Application Usage for XML documents related to a Presentity:

- Presence Subscription Rules, which defines the Watchers who are allowed to subscribe for Presence Information of a Presentity, and the subset of the Presentity's Presence Information they are allowed to receive. The Presence Subscription Rules include:
    - Subscription Authorization Rules; and
    - Subscription Content Rules.

## 4.2 Version 2.0

The OMA PRS 2.0 enabler defines the following additional Application Usage for XML documents related to a Presentity:

- Presence Publication Rules, which defines the identities who are allowed to publish Presence Information on behalf of a Presentity, and the subset of the Presentity's Presence Information they are allowed to publish; The Presence Publication Rules include:
    - Publication Authorization Rules; and
    - Publication Content Rules.
- Publication Content Rules Presence Source View, which is automatically generated by the Presence XDMS based on the Presence Publication Rules and defines the subset of the Presentity's Presence Information a Presence Source is allowed to publish; and
- Permanent Presence State, which is static or semi-static Presence Information pertaining to a Presentity that is an input to composition policy.

# 5. Presence XDM Application Usages

## 5.1 Presence Subscription Rules

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

- Subscription Authorization Rules, which determine if a Watcher is allowed to subscribe to the Presentity's Presence Information; and
- Subscription 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 Subscription Rules document is described in the subsections below.

### 5.1.1 Subscription Authorization 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 [XDM_Core] "*Authorization Rules*", with the clarifications given in this section.

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

a) conditions, defined by the <conditions> element;

b) actions, defined by the <actions> element; and

c) transformations, defined by the <transformations> element.

The Subscription Authorization 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 [XDM_Core] "*Authorization Rules*";

c) the <other-identity> element as defined in [XDM_Core] "*Authorization Rules*";

d) the <anonymous-request> element as defined in [XDM_Core] "*Authorization Rules*".

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 XML Schema

The Subscription Authorization Rules SHALL be composed according to the XML schema detailed in [RFC5025] section 6 and extended in [XDM_Core] "*Authorization Rules*".

#### 5.1.1.4 Default Namespace

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

#### 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 [XDM_Core] "*Authorization Rules*".

#### 5.1.1.8 Naming Conventions

The name of the Presence Subscription Rules document containing the Subscription Authorization 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 Authorization Policies

The authorization policies SHALL be defined according to [XDM_Core] "*Authorization*".

### 5.1.2 Subscription Content Rules

#### 5.1.2.1 Structure

The Subscription Content Rules SHALL conform to the structure of the "pres-rules" document described in [RFC5025] and extended in [XDM_Core] "*Authorization Rules*", with the clarifications given below.

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

The <transformations> element SHALL be used to define the visibility a Watcher is granted to a particular component of the presence document 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 and in section 5.1.2.7;

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; and

s) the <provide-deviceID> element as described in [RFC5025] section 3.3.2.3.

Other types of <transformations> elements described in [RFC5025] are not defined by this specification.

NOTE 1: Other OMA Enablers defining Presence Information Elements may also define their own <transformations> child elements.

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 2: 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 was omitted.

### 5.1.2.2 Application Unique ID

The AUID SHALL be “org.openmobilealliance.pres-rules”.

### 5.1.2.3 XML Schema

The Subscription Content Rules SHALL be composed according to the XML schema detailed in [RFC5025] section 6 and extended in [XDM_Core] “*Authorization Rules*”, with the extensions given in [XSD_presRules] and in other OMA Enablers.

### 5.1.2.4 Default Namespace

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

#### 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 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 [XDM_Core] "*Authorization Rules*", together with the clarifications given in this section and in other OMA Enablers.

A <transformations> child element that controls access to a certain Presence Information Element also controls access to the Presence Information Element's attributes and child elements unless otherwise stated in the data semantics for the <transformations> child element.

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

"false" instructs the PS 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 PS 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 [PDE_DDS]. The value is of a Boolean type:

"false" instructs the PS to remove the <network-availability> element if present. This is the default value taken in the absence of the element.

"true" instructs the PS to report the <network-availability> element to the Watcher.

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

"false" instructs the PS to remove the <session-participation> element if present. This is the default value taken in the absence of the element.

"true" instructs the PS to report the <session-participation> element to the Watcher.

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

"false" instructs the PS to remove the <registration-state> element if present. This is the default value taken in the absence of the element.

"true" instructs the PS to report the <registration-state> element to the Watcher.

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

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

“true” instructs the PS to report the <barring-state> element to the Watcher.

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

false instructs the PS 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 PS to report the <geopriv> element and its child elements to the Watcher. It is assigned the numeric value of ten.

The <provide-services> “transformation” controls access to the <tuple> element and some of its child elements as described in [RFC5025]. If the <tuple> element includes a <service-description> child element described in [PDE_DDS], the PS is instructed to report this <service-description> child element to the Watcher in addition to the <contact>, basic <status>, and <timestamp> child elements specified in [RFC5025] section 3.3.2.

The <service-id> identifies a service by its service ID described in [PDE_DDS] and is used to identify a service occurrence in addition to the service occurrence identity elements <class>, <occurrence-id>, <service-uri> and <service-uri-scheme> described in [RFC5025] section 3.3.1.3.

#### 5.1.2.8 Naming Conventions

The name of the Presence Subscription Rules document containing the Subscription 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 Authorization Policies

The authorization policies SHALL be defined according to [XDM_Core] “*Authorization*”.

## 5.2 Permanent Presence State

The Permanent Presence State document contains static or semi-static Presence Information pertaining to a Presentity that is stored in the Presence XDMS and used by the PS as an input to composition policy.

The Application Usage of the Permanent Presence State document is described in the subsections below.

### 5.2.1 Structure

The Permanent Presence State document SHALL conform to the structure of the presence document according to [PDE_DDS] and [RFC3863].

### 5.2.2 Application Unique ID

The AUID SHALL be “pidf-manipulation” as defined in [RFC4827] section 4.

### 5.2.3 XML Schema

The Permanent Presence State document SHALL be composed according to the XML schema detailed in [PDE_DDS] “*Content of the Presence Document*”.

### 5.2.4 Default Namespace

The default namespace SHALL conform to “urn:ietf:params:xml:ns:pidf” as defined in [RFC4827] section 5.

### 5.2.5 MIME Type

The MIME type for this Application Usage SHALL be “application/pidf+xml” defined in [RFC3863].

### 5.2.6 Validation Constraints

There are no validation constraints, other than those imposed by the XML schema.

### 5.2.7 Data Semantics

The data semantics SHALL conform to the semantics defined in [PDE_DDS] “*Content of the Presence Document*”.

### 5.2.8 Naming Conventions

The name of the Permanent Presence State document SHALL be “perm-presence”.

### 5.2.9 Global Documents

This Application Usage defines no Global Documents.

### 5.2.10 Resource Interdependencies

This Application Usage defines no additional resource interdependencies.

### 5.2.11 Authorization Policies

The authorization policies for manipulating a Permanent Presence State document SHALL conform to those described in section 5.3.1.

The Presence XDMS SHALL determine which rules in the Presence Publication Rules document are applicable and evaluate the combined permissions according to the procedures described in [XDM_Core] “*Combining Permissions*” with the following clarifications:

- If an attempt to resolve an <external-list> condition element fails, the Presence XDMS SHALL regard the Presence Publication Rules document as invalid and act according to the default policy.
- If there is no matching rule then the Presence XDMS SHALL further handle the publication according to the default policy.

The default policy SHALL authorize the Presentity, and SHOULD reject all other users.

After evaluating the combined permissions, the Presence XDMS SHALL handle the request based on the value of the <perm-handling> action as follows:

- If the value is “block” or there is no value, then the Presence XDMS SHALL reject the request by responding to the request with an HTTP 403 (Forbidden) error response.

- If the value is “allow”, then the Presence XDMS SHALL accept the request by responding to the request with an HTTP 200 (OK) response.

When handling (i.e. create, modify, delete, etc.) a Permanent Presence State document, the Presence XDMS SHALL also perform authorization of the request by verifying that the XUI matches the value of the “entity” attribute of the <presence> element in the Presence Information document as described in [RFC3863]. In case of no match, the Presence XDMS SHALL reject the request by responding to the request with an HTTP 403 (Forbidden) error response.

# 5.3 Presence Publication Rules

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

- Publication Authorization Rules, which determine the identities authorized to publish a Presentity’s Presence Information; and
- Publication Content Rules, which determine the content of publications allowed for each identity.

These rules SHALL be described in one single XML document.

The Application Usages of the Presence Publication Rules document is described in the subsections below.

## 5.3.1 Publication Authorization Rules

### 5.3.1.1 Structure

The Publication Authorization Rules document SHALL conform to the structure of the “ruleset” document described in [RFC4745] and extended in [XDM_Core] “*Authorization Rules*”, with the clarifications given in this section.

As described in [RFC4745] section 6, the “ruleset” document contains a sequence of <rule> elements, each composed of up to three parts:

a) conditions, defined by the <conditions> element;

b) actions, defined by the <actions> element; and

c) transformations, defined by the <transformations> element.

The Publication Authorization 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 [XDM_Core] “*Authorization Rules*”;

c) the <other-identity> element as defined in [XDM_Core] “*Authorization Rules*”;

d) the <anonymous-request> element as defined in [XDM_Core] “*Authorization Rules*”.

The <actions> child element of any <rule> element MAY include the <pub-handling> element and/or the <perm-handling> element defined in section 5.3.1.7.

### 5.3.1.2 Application Unique ID

The AUID SHALL be “org.openmobilealliance.pub-rules”.

### 5.3.1.3 XML Schema

The Publication Authorization Rules SHALL be composed according to the XML schema described in [RFC4745] section 13 and extended in [XDM_Core] “*Authorization Rules*”, with extensions given in [XSD_pubRules].

#### 5.3.1.4 Default Namespace

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

#### 5.3.1.5 MIME Type

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

#### 5.3.1.6 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.

#### 5.3.1.7 Data Semantics

The data semantics SHALL conform to the semantics defined in [RFC4745] and extended in [XDM_Core] "*Authorization Rules*" with the extensions given in this section.

The <pub-handling> element SHALL specify the publication authorization decision for PUBLISH requests. The <pub-handling> element is an enumerated Integer type. The defined values are:

"block" This action instructs the PS to reject the publication request. It has the value of zero and it represents the default value taken in the absence of the element.

"allow" This action instructs the PS to accept the publication request. This action has a value of thirty.

The <perm-handling> element SHALL specify the publication authorization decision for Permanent Presence State. The <perm-handling> element is an enumerated Integer type. The defined values are:

"block" This action instructs the Presence XDMS to reject the publication request. It has the value of zero and it represents the default value taken in the absence of the element.

"allow" This action instructs the Presence XDMS to accept the publication request. This action has a value of thirty.

#### 5.3.1.8 Naming Conventions

The name of the Presence Publication Rules document containing the Publication Authorization Rules SHALL be "pub-rules".

#### 5.3.1.9 Global Documents

This Application Usage defines no Global Documents.

#### 5.3.1.10 Resource Interdependencies

This Application Usage defines no additional resource interdependencies.

#### 5.3.1.11 Authorization Policies

The authorization policies SHALL be defined according to [XDM_Core] "*Authorization*".

### 5.3.2 Publication Content Rules

#### 5.3.2.1 Structure

The Publication Content Rules SHALL conform to the structure of the "ruleset" document described in [RFC4745] and extended in [XDM_Core] "*Authorization Rules*", with the clarifications given below.

The <transformations> element SHALL be used to define the content a Presence Source is allowed to publish.

The <transformations> child element of any <rule> element MAY include the following child elements described in section 5.3.2.7:

a) the <allow-persons> element;

b) the <allow-devices> element;

c) the <allow-services> element;

d) the <allow-willingness> element;

e) the <allow-network-availability> element;

f) the <allow-session-participation> element;

g) the <allow-activities> element;

h) the <allow-class> element;

i) the <allow-mood> element;

j) the <allow-place-type> element;

k) the <allow-status-icon> element;

l) the <allow-time-offset> element;

m) the <allow-note> element;

n) the <allow-geopriv> element;

o) the <allow-registration-state> element;

p) the <allow-barring-state> element;

q) the <allow-all-attributes> element;

r) the <allow-unknown-attribute> element.

NOTE: Other OMA Enablers defining Presence Information Elements may also define their own <transformations> child elements.

#### 5.3.2.2 Application Unique ID

The AUID SHALL be “org.openmobilealliance.pub-rules”.

#### 5.3.2.3 XML Schema

The Publication Content Rules SHALL be composed according to the XML schema described in [RFC4745] section 13 and extended in [XDM_Core] “*Authorization Rules*” and with extensions given in [XSD_pubRules] and in other OMA Enablers.

#### 5.3.2.4 Default Namespace

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

#### 5.3.2.5 MIME Type

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

#### 5.3.2.6 Validation Constraints

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

A <rule> element with an <actions> element including a <perm-handling> element with the value "allow" SHALL always contain the following <transformations> child elements: <allow-persons>, <allow-services>, <allow-devices>, and <allow-all-attributes> elements and no others. 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 SHOULD be set to "Invalid set of <transformations> child elements".

A <rule> element with a <pub-handling> or <perm-handling> element with a 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 SHOULD be set to "<transformations> element not allowed".

#### 5.3.2.7 Data Semantics

The data semantics SHALL conform to the semantics defined in this section and in other OMA Enablers defining Presence Information.

A <transformations> child element that controls publication of a certain Presence Information Element also controls publication of the Presence Information Element's attributes and child elements unless otherwise stated in the data semantics for the <transformations> child element.

One group of <transformations> child elements grants coarse-grained publication of person (<allow-persons>), device (<allow-devices>) and tuple (<allow-services>) elements. Once publication authorization is granted to the person, device or tuple elements, publication authorization for specific Presence Information Elements is controlled by another group of <transformations> child elements. These fine-grained publication authorizations address particular well-known Presence Information Elements (e.g. <allow-status-icon> element for the <status-icon> element), a particular but yet unknown Presence Information Element (i.e. <allow-unknown-attribute> element) or all presence attributes (i.e. <allow-all-attributes> element).

The <allow-persons> "transformation" controls publication of the <person> element described in [PDE_DDS]. The value is of a Boolean type:

"false" disallows the Presence Source to publish the <person> element and any of its child elements. This is the default value taken in the absence of the element.

"true" allows the Presence Source to publish the <person> element, a <timestamp> child element, and any child elements that the fine-grained publication authorization allows.

The <allow-devices> "transformation" controls publication of the <device> element described in [PDE_DDS]. The value is of a Boolean type:

"false" disallows the Presence Source to publish the <device> element and any of its child elements. This is the default value taken in the absence of the element.

"true" allows the Presence Source to publish the <device> element, a <timestamp> child element, a <deviceID> child element, and any child elements that the fine-grained publication authorization allows.

The <allow-services> "transformation" controls publication of the <tuple> element described in [PDE_DDS]. The value is of a Boolean type:

"false" disallows the Presence Source to publish the <tuple> element and any of its child elements. This is the default value taken in the absence of the element.

"true" allows the Presence Source to publish the <tuple> element, a <contact> child element, a <service-class> child element, a <status> child element, a <timestamp> child element, a <service-description> child element, a <deviceID> child element, and any child elements that the fine-grained publication authorization allows.

The <allow-willingness> “transformation” controls the fine-grained publication authorization of the <willingness> and <overriding-willingness> elements described in [PDE_DDS]. The value is of a Boolean type:

“false” disallows the Presence Source to publish the <willingness> and <overriding-willingness> elements. This is the default value taken in the absence of the element.

“true” allows the Presence Source to publish the <willingness> and <overriding-willingness> elements.

The <allow-network-availability> “transformation” controls the fine-grained publication authorization of the <network-availability> element described in [PDE_DDS]. The value is of a Boolean type:

“false” disallows the Presence Source to publish the <network-availability> element if present. This is the default value taken in the absence of the element.

“true” allows the Presence Source to publish the <network-availability> element.

The <allow-session-participation> “transformation” controls the fine-grained publication authorization of the <session-participation> element described in [PDE_DDS]. The value is of a Boolean type:

“false” disallows the Presence Source to publish the <session-participation> element if present. This is the default value taken in the absence of the element.

“true” allows the Presence Source to publish the <session-participation> element.

The <allow-activities> “transformation” controls the fine-grained publication authorization of the <activities> element described in [PDE_DDS]. The value is of a Boolean type:

“false” disallows the Presence Source to publish the <activities> element if present. This is the default value taken in the absence of the element.

“true” allows the Presence Source to publish the <activities> element.

The <allow-class> “transformation” controls the fine-grained publication authorization of the <class> element described in [PDE_DDS]. The value is of a Boolean type:

“false” disallows the Presence Source to publish the <class> element if present. This is the default value taken in the absence of the element.

“true” allows the Presence Source to publish the <class> element.

The <allow-mood> “transformation” controls the fine-grained publication authorization of the <mood> element described in [PDE_DDS]. The value is of a Boolean type:

“false” disallows the Presence Source to publish the <mood> element if present. This is the default value taken in the absence of the element.

“true” allows the Presence Source to publish the <mood> element.

The <allow-place-type> “transformation” controls the fine-grained publication authorization of the <place-type> element described in [PDE_DDS]. The value is of a Boolean type:

"false" disallows the Presence Source to publish the <place-type> element if present. This is the default value taken in the absence of the element.

"true" allows the Presence Source to publish the <place-type> element.

The <allow-status-icon> "transformation" controls the fine-grained publication authorization of the <status-icon> element described in [PDE_DDS]. The value is of a Boolean type:

"false" disallows the Presence Source to publish the <status-icon> element if present. This is the default value taken in the absence of the element.

"true" allows the Presence Source to publish the <status-icon> element.

The <allow-time-offset> "transformation" controls the fine-grained publication authorization of the <time-offset> element described in [PDE_DDS]. The value is of a Boolean type:

"false" disallows the Presence Source to publish the <time-offset> element if present. This is the default value taken in the absence of the element.

"true" allows the Presence Source to publish the <time-offset> element.

The <allow-note> "transformation" controls the fine-grained publication authorization of the <note> element described in [PDE_DDS] for <tuple>, <person> and <device> elements. The value is of a Boolean type:

"false" disallows the Presence Source to publish the <note> element if present. This is the default value taken in the absence of the element.

"true" allows the Presence Source to publish the <note> element.

The <allow-geopriv> "transformation" controls the fine-grained publication authorization of the <geopriv> element described in [PDE_DDS]. The <allow-geopriv> element is an enumerated integer type:

"false" disallows the Presence Source to publish 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" allows the Presence Source to publish the <geopriv> element and its child elements. It is assigned the numeric value of ten.

The <allow-registration-state> "transformation" controls the fine-grained publication authorization of the <registration-state> element described in [PDE_DDS]. The value is of a Boolean type:

"false" disallows the Presence Source to publish the <registration-state> element if present. This is the default value taken in the absence of the element.

"true" allows the Presence Source to publish the <registration-state> element.

The <allow-barring-state> "transformation" controls the fine-grained publication authorization of the <barring-state> element described in [PDE_DDS]. The value is of a Boolean type:

"false" disallows the Presence Source to publish the <barring-state> element if present. This is the default value taken in the absence of the element.

"true" allows the Presence Source to publish the <barring-state> element.

The <allow-unknown-attribute> "transformation" controls the fine-grained publication authorization of an unknown presence attribute with the given name and namespace. It also controls the fine-grained publication authorization of presence attributes defined by other OMA Enablers where a dedicated <transformations> child element has not been specified (e.g. the <session-answermode> and the <servcaps> elements described in [PDE_DDS]). The value of the "name" attribute SHALL be an unqualified element name (i.e. namespace prefix SHALL NOT be included), and the value of the "ns" attribute SHALL be a namespace URI. The two are combined to form a qualified element name, which SHALL be matched to all unknown child elements of the <tuple>, <device>, or <person> elements with the same qualified name. The value is of a Boolean type:

"false" disallows the Presence Source to publish the presence attribute with the given name and namespace, if present. This is the default value taken in the absence of the element.

"true" allows the Presence Source to publish the presence attribute with the given name and namespace.

The <allow-all-attributes> "transformation" controls the fine-grained publication authorization of all presence attributes in all <person>, <device>, and <tuple> elements. This implies that, so long as an entire person, service, or device occurrence is allowed, every single presence attribute, including ones not known to the PS and/or defined in future presence document extensions, is granted to be published by the Presence Source.

#### 5.3.2.8 Naming Conventions

The name of the Presence Publication Rules document containing the Publication Content Rules SHALL be "pub-rules".

#### 5.3.2.9 Global Documents

This Application Usage defines no Global Documents.

#### 5.3.2.10 Resource Interdependencies

This Application Usage defines no additional resource interdependencies.

#### 5.3.2.11 Authorization Policies

The authorization policies SHALL be defined according to [XDM_Core] "*Authorization*".

## 5.4 Publication Content Rules Presence Source View

### 5.4.1 Structure

The Publication Content Rules Presence Source View SHALL conform to the structure of the "ruleset" document described in [RFC4745] with the following clarifications:

- A single <rule> element SHALL be included as a child element to the <rule-set> element;
- An <identity> element with a single <one> child element SHALL be included as a child element to the <rule> element. The <one> element SHALL include an "id" attribute as defined in [RFC4745];
- An <actions> element with a single <pub-handling> child element with the value "allow" as defined in sections 5.3.1.1 and 5.3.1.7. SHALL be included as a child element to the <rule> element;
- A <transformations> element SHALL be included as a child element to the <rule> element; and

- Only child elements to a <transformations> element as defined in section 5.3.2.1 MAY be included.

### 5.4.2 Application Unique ID

The AUID SHALL be "org.openmobilealliance.pub-rules-view".

### 5.4.3 XML Schema

The Publication Content Rules Presence Source View SHALL be composed according to the XML schema described in [RFC4745] section 13 with extensions given in [XSD_pubRules].

### 5.4.4 Default Namespace

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

### 5.4.5 MIME Type

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

### 5.4.6 Validation Constraints

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

### 5.4.7 Data Semantics

The data semantics SHALL conform to the semantics defined in [RFC4745] with the extensions defined in this subsection.

The "id" attribute of the <one> element SHALL include the authorized identity of the Principal who retrieves the Publication Content Rules Presence Source View document.

The <transformations> element SHALL define all Presence Information that the Principal who retrieves the Publication Content Rules Presence Source View document is allowed to publish using a PUBLISH request on behalf of the Primary Principal.

The <transformations> element and its child elements SHALL be created combining all permissions that the Primary Principal's Presence Publication Rules defined in sections 5.3.1 and 5.3.2 give to the retrieving Principal.

The data semantics of <transformations> child elements SHALL conform to the semantics defined in section 5.3.2.7.

### 5.4.8 Naming Conventions

The name of the Publication Content Rules Presence Source View document SHALL be "pub-rules-view".

### 5.4.9 Global Documents

This Application Usage defines no Global Documents.

### 5.4.10 Resource Interdependencies

This Application Usage has a resource interdependency towards the "org.openmobilealliance.pub-rules" AUID. A "pub-rules-view" document SHALL contain the Publication Content Rules specifying what Presence Information the retrieving Principal is allowed to publish using a PUBLISH request on behalf of the Primary Principal.

A "pub-rules-view" document exists only during the time it is retrieved and SHALL NOT be included in the "XML Documents Directory" Application Usage document as defined by [XDM_Core] "*XML Document Directory*".

The XDMS SHOULD NOT generate an etag value for the "pub-rules-view" document.

NOTE: This implies that conditional operations are not supported against the "pub-rules-view" document.

## 5.4.11 Authorization Policies

The authorization policies SHALL be defined according to [XDM_Core] "*Authorization*" with the additions defined in this subsection.

Principals SHALL only have permission to perform the "retrieve a document" operation defined in [XDM_Core] "*Retrieve a Document*:

- The Presence XDMS SHALL determine the rules in the Presence Publication Rules document (see sections 5.3.1 and 5.3.2) with regard to the retrieving Principal;
- The Presence XDMS SHALL evaluate the combined permissions according to the procedures described in [XDM_Core] "*Combining Permissions*" with the following clarification:
    - If an attempt to resolve an <external-list> condition element fails, the Presence XDMS SHALL regard the Publication Authorization Rules document as invalid and reject the request by responding to the request with an HTTP 403 (Forbidden) error response.
- If there is no matching rule then the Presence XDMS SHALL reject the request by responding to the request with an HTTP 403 (Forbidden) error response; and
- In case of matching rules, the Presence XDMS SHALL evaluate the <pub-handling> action of the combined permissions:
    - If the value is "block", the Presence XDMS SHALL reject the request by responding to the request with an HTTP 403 (Forbidden) error response; and
    - If the value is "allow", then the Presence XDMS SHALL accept the request by responding to the request with an HTTP 200 (OK) response and return the "pub-rules-view" document with the combined <transformations> element from the matching rules to the Principal.

## 5.4.12 Permanent Presence State Specific Details

This section defines Permanent Presence State details related to specific Presence Information Elements.

### 5.4.12.1 Timestamp

Although the <timestamp> element is an optional element in a <tuple>, <person> or <device> element (see [PDE_DDS] "*Presence Data Model*"), local policy of the service provider MAY mandate a <timestamp> element set by the Presence XDMS.

If such a local policy exists then if either:

- A <timestamp> element exists in a <tuple>, <person> or <device> element, the Presence XDMS SHALL replace the element value with the time when the corresponding HTTP PUT request was received; or
- A <timestamp> element does not exist in a <tuple>, <person> or <device> element, the Presence XDMS SHALL add a <timestamp> element respectively with the time the corresponding HTTP PUT request was received.

# 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 [XDM_Core] "*Subscriptions to Changes in the XML Documents*" for the "Presence Subscription Rules", "Permanent Presence State" and "Presence Publication Rules" XML documents. The Presence XDMS SHALL NOT support subscriptions to changes in the "Publication Content Rules Presence Source View" XML document.

# Appendix A. Change History (Informative)

## A.1 Approved Version History

| Reference | Date | Description |
|---|---|---|
| n/a | n/a | No prior version |

## A.2 Draft/Candidate Version 2.0 History

| Document Identifier | Date | Sections | Description |
|---|---|---|---|
| Draft Versions<br>OMA-TS-Presence_SIMPLE_XDM-V2_0 | 20 Jun 2006 | All | Initial version created based on OMA-TS-Presence_SIMPLE_XDM-V1_0-20060620-C (See OMA-PAG-2006-0329) |
| | 02 Aug 2006 | 5.1 | Incorporated CR:<br>OMA-PAG-2006-0400 |
| | 23 Nov 2006 | 2.1, 5.2 | Incorporated CRs:<br>OMA-PAG-2006-0640R02<br>OMA-PAG-2006-0667 |
| | 17 Jan 2007 | B.1.1 | Incorporated CRs:<br>OMA-PAG-2006-0799<br>OMA-PAG-2006-0795 |
| | 01 Jul 2007 | 5.2.5 | Incorporated CR:<br>OMA-PAG-2007-0443 |
| | 03 Sep 2007 | 2.1, 3.2,<br>5.2 | Incorporated CR:<br>OMA-PAG-2007-0549R02 |
| | 11 Oct 2007 | 2.1 | Incorporated CR:<br>OMA-PAG-2007-0593 |
| | 26 Nov 2007 | 5 | Incorporated CR:<br>OMA-PAG-2007-0787 |
| | 18 Jan 2008 | 5 | Incorporated CR:<br>OMA-PAG-2007-0870 |
| | 5 Mar 2008 | 2.1, 4, 5.1,<br>5.3, A.1,<br>A.2, A.3 | Incorporated CR:<br>OMA-PAG-2008-0043<br>OMA-PAG-2008-0059<br>OMA-PAG-2008-0097R03<br>OMA-PAG-2008-0134R01 |
| | 12 Mar 2008 | All | Editorial cleanup based on OMA-PAG-2008-0151<br>Incorporated CR:<br>OMA-PAG-2008-0025 |
| | 28 May 2008 | All | Incorporated CRs:<br>OMA-PAG-2008-0344<br>OMA-PAG-2008-0347R01 + editorial R&A comment |
| | 02 Jul 2008 | 5.1<br>5.2<br>5.3 | Incorporated CRs:<br>OMA-PAG-2008-0484<br>OMA-PAG-2008-0490<br>OMA-PAG-2008-0491R01 |
| | 26 Aug 2008 | 5.1<br>5.3 | Incorporated CRs:<br>OMA-PAG-2008-0421R03<br>OMA-PAG-2008-0489R01 |

| Document Identifier | Date | Sections | Description |
|---|---|---|---|
| | 01 Oct 2008 | All | Incorporated CRs:<br>OMA-PAG-2008-0417R02<br>OMA-PAG-2008-0419R03<br>OMA-PAG-2008-0420R03<br>OMA-PAG-2008-0486R02<br>OMA-PAG-2008-0582R01<br>OMA-PAG-2008-0583<br>OMA-PAG-2008-0599R02<br>OMA-PAG-2008-0601R01<br>OMA-PAG-2008-0602R02 |
| | 14 Oct 2008 | All | Incorporated CRs:<br>OMA-PAG-2008-0659<br>OMA-PAG-2008-0680 |
| | 22 Oct 2008 | 4, 5.1, 5.3., 5.4 | Incorporated CRs:<br>OMA-PAG-2008-0687<br>OMA-PAG-2008-0726 |
| | 27 Oct 2008 | All | Incorporated CRs:<br>OMA-PAG-2008-0694R03<br>OMA-PAG-2008-0725R01<br>OMA-PAG-2008-0757 |
| | 04 Nov 2008 | B.1, B.2, C.4 | Incorporated CRs:<br>OMA-PAG-2008-0768R02<br>OMA-PAG-2008-0775R01 |
| Candidate Version<br>OMA-TS-Presence_SIMPLE_XDM-V2_0 | 23 Dec 2008 | N/A | Status changed to Candidate by TP<br>TP ref # OMA-TP-2008-0490-INP_Presence_SIMPLE_V2_0_ERP_for_Candidate_Approval |
| Draft Versions<br>OMA-TS-Presence_SIMPLE_XDM-V2_0 | 30 Jul 2009 | 2, 4 | Incorporated CR:<br>OMA-PAG-2009-0093<br>OMA-PAG-2009-0198<br>Editorial clean-up |
| | 03 Sep 2009 | 5.4.12 (new) | Incorporated CR:<br>OMA-PAG-2009-0269R03 |
| Candidate Version<br>OMA-TS-Presence_SIMPLE_XDM-V2_0 | 17 Sep 2009 | N/A | Status changed to Candidate by TP<br>TP ref # OMA-TP-2009-0438-INP_PRS_V2_0_ERP_for_Notification |

# Appendix B. Static Conformance Requirements (Normative)

The notation used in this appendix is specified in [SCRRULES].

The following tags are used in the Function column to identify the release of the Presence SIMPLE enabler that the requirement was introduced:

- PRSv1.1 – Requirement was introduced in Presence SIMPLE 1.1.
- PRSv2.0 – Requirement was introduced in Presence SIMPLE 2.0.

## B.1 Presence XDM Application Usages (Server)

| Item | Function | Reference | Requirement |
|---|---|---|---|
| PRS_XDM-XOP-S-001-M | Single Presence Subscription Rules XML document describing who can subscribe to a presentity's presence, and content of notifications (PRSv1.1) | 5.1 | |
| PRS_XDM-XOP-S-002-M | Structure of Presence Subscription Rules (PRSv1.1) | 5.1.1.1<br>5.1.2.1 | |
| PRS_XDM-XOP-S-003-M | Application Unique ID of Presence Subscription Rules (PRSv1.1) | 5.1.1.2<br>5.1.2.2 | |
| PRS_XDM-XOP-S-005-M | XML schema of Presence Subscription Rules (PRSv1.1) | 5.1.1.3<br>5.1.2.3 | |
| PRS_XDM-XOP-S-004-M | Default namespace for Presence Subscription Rules (PRSv1.1) | 5.1.1.4<br>5.1.2.4 | |
| PRS_XDM-XOP-S-006-M | MIME type of Presence Subscription Rules (PRSv1.1) | 5.1.1.5<br>5.1.2.5 | |
| PRS_XDM-XOP-S-007-M | Validation constraints of Presence Subscription Rules, in addition to the XML schema (PRSv1.1) | 5.1.1.6<br>5.1.2.6 | |
| PRS_XDM-XOP-S-008-M | Data semantics of Presence Subscription Rules (PRSv1.1) | 5.1.1.7<br>5.1.2.7 | |
| PRS_XDM-XOP-S-009-M | Naming conventions for Presence Subscription Rules (PRSv1.1) | 5.1.1.8<br>5.1.2.8 | |
| PRS_XDM-XOP-S-010-M | Authorization policies of Presence Subscription Rules (PRSv1.1) | 5.1.1.11<br>5.1.2.11 | |

| Item | Function | Reference | Requirement |
|---|---|---|---|
| PRS_XDM-XOP-S-011-O | Permanent Presence State Application Usage | 5.2 | PRS-PS-S-008-O AND<br>PRS_XDM-XOP-S-012-O AND PRS_XDM-XOP-S-013-O AND PRS_XDM-XOP-S-014-O AND PRS_XDM-XOP-S-015-O AND PRS_XDM-XOP-S-016-O AND PRS_XDM-XOP-S-017-O AND PRS_XDM-XOP-S-018-O AND PRS_XDM-XOP-S-019-O |
| PRS_XDM-XOP-S-012-O | Structure of Permanent Presence State (PRSv2.0) | 5.2.1 | PRS_XDM-XOP-S-011-O |
| PRS_XDM-XOP-S-013-O | Application Unique ID of Permanent Presence State (PRSv2.0) | 5.2.2 | PRS_XDM-XOP-S-011-O |
| PRS_XDM-XOP-S-014-O | XML schema of Permanent Presence State (PRSv2.0) | 5.2.3 | PRS_XDM-XOP-S-011-O |
| PRS_XDM-XOP-S-015-O | Default namespace for Permanent Presence State (PRSv2.0) | 5.2.4 | PRS_XDM-XOP-S-011-O |
| PRS_XDM-XOP-S-016-O | MIME type of Permanent Presence State (PRSv2.0) | 5.2.5 | PRS_XDM-XOP-S-011-O |
| PRS_XDM-XOP-S-017-O | Data semantics of Permanent Presence State (PRSv2.0) | 5.2.7 | PRS_XDM-XOP-S-011-O |
| PRS_XDM-XOP-S-018-O | Naming conventions for Permanent Presence State (PRSv2.0) | 5.2.8 | PRS_XDM-XOP-S-011-O |
| PRS_XDM-XOP-S-019-O | Authorization policies of Permanent Presence State (PRSv2.0) | 5.2.11 | PRS_XDM-XOP-S-011-O |

| Item | Function | Reference | Requirement |
|---|---|---|---|
| PRS_XDM-XOP-S-020-O | Presence Publication Rules Application Usage (PRSv2.0) | 5.3 | PRS-PS-S-017-O AND<br>PRS_XDM-XOP-S-021-O AND PRS_XDM-XOP-S-022-O AND PRS_XDM-XOP-S-023-O AND PRS_XDM-XOP-S-024-O AND PRS_XDM-XOP-S-025-O AND PRS_XDM-XOP-S-026-O AND PRS_XDM-XOP-S-027-O AND PRS_XDM-XOP-S-028-O AND PRS_XDM-XOP-S-029-O |
| PRS_XDM-XOP-S-021-O | Structure of Presence Publication Rules (PRSv2.0) | 5.3.1.1<br>5.3.2.1 | PRS_XDM-XOP-S-020-O |
| PRS_XDM-XOP-S-022-O | Application Unique ID of Presence Publication Rules (PRSv2.0) | 5.3.1.2<br>5.3.2.2 | PRS_XDM-XOP-S-020-O |
| PRS_XDM-XOP-S-023-O | XML schema of Presence Publication Rules (PRSv2.0) | 5.3.1.3<br>5.3.2.3 | PRS_XDM-XOP-S-020-O |
| PRS_XDM-XOP-S-024-O | Default namespace for Presence Publication Rules (PRSv2.0) | 5.3.1.4<br>5.3.2.4 | PRS_XDM-XOP-S-020-O |
| PRS_XDM-XOP-S-025-O | MIME type of Presence Publication Rules (PRSv2.0) | 5.3.1.5<br>5.3.2.5 | PRS_XDM-XOP-S-020-O |
| PRS_XDM-XOP-S-026-O | Validation constraints of Presence Publication Rules, in addition to the XML schema (PRSv2.0) | 5.3.1.6<br>5.3.2.6 | PRS_XDM-XOP-S-020-O |
| PRS_XDM-XOP-S-027-O | Data semantics of Presence Publication Rules (PRSv2.0) | 5.3.1.7<br>5.3.2.7 | PRS_XDM-XOP-S-020-O |
| PRS_XDM-XOP-S-028-O | Naming conventions for Presence Publication Rules (PRSv2.0) | 5.3.1.8<br>5.3.2.8 | PRS_XDM-XOP-S-020-O |
| PRS_XDM-XOP-S-029-O | Authorization policies of Presence Publication Rules (PRSv2.0) | 5.3.1.11<br>5.3.2.11 | PRS_XDM-XOP-S-020-O |

| Item | Function | Reference | Requirement |
|---|---|---|---|
| PRS_XDM-XOP-S-030-O | Publication Content Rules Presence Source View Application Usage | 5.4 | PRS_XDM_XOP-S-020-O AND<br>PRS_XDM_XOP-S-031-O AND<br>PRS_XDM_XOP-S-032-O AND<br>PRS_XDM_XOP-S-033-O AND<br>PRS_XDM_XOP-S-034-O AND<br>PRS_XDM_XOP-S-035-O AND<br>PRS_XDM_XOP-S-036-O AND<br>PRS_XDM_XOP-S-037-O AND<br>PRS_XDM_XOP-S-038-O AND<br>PRS_XDM_XOP-S-039-O |
| PRS_XDM-XOP-S-031-O | Structure of Publication Content Rules Presence Source View (PRSv2.0) | 5.4.1 | PRS_XDM-XOP-S-030-O |
| PRS_XDM-XOP-S-032-O | Application Unique ID of Publication Content Rules Presence Source View (PRSv2.0) | 5.4.2 | PRS_XDM-XOP-S-030-O |
| PRS_XDM-XOP-S-033-O | XML schema Publication Content Rules Presence Source View (PRSv2.0) | 5.4.3 | PRS_XDM-XOP-S-030-O |
| PRS_XDM-XOP-S-034-O | Default namespace for Publication Content Rules Presence Source View (PRSv2.0) | 5.4.4 | PRS_XDM-XOP-S-030-O |
| PRS_XDM-XOP-S-035-O | MIME type of Publication Content Rules Presence Source View (PRSv2.0) | 5.4.5 | PRS_XDM-XOP-S-030-O |
| PRS_XDM-XOP-S-036-O | Data semantics of Publication Content Rules Presence Source View (PRSv2.0) | 5.4.7 | PRS_XDM-XOP-S-030-O |
| PRS_XDM-XOP-S-037-O | Naming conventions for Publication Content Rules Presence Source View (PRSv2.0) | 5.4.8 | PRS_XDM-XOP-S-030-O |
| PRS_XDM-XOP-S-038-O | Resource Interdependencies for Publication Content Rules Presence Source View (PRSv2.0) | 5.4.10 | PRS_XDM-XOP-S-030-O |

| Item | Function | Reference | Requirement |
|---|---|---|---|
| PRS_XDM-XOP-S-039-O | Authorization policies of Publication Content Rules Presence Source View (PRSv2.0) | 5.4.11 | PRS_XDM-XOP-S-030-O |
| PRS_XDM-SUB-S-001-M | Subscription to XML document changes (PRSv2.0) | 6 | |

## B.2 Presence XDM Application Usages (Client)

| Item | Function | Reference | Requirement |
|---|---|---|---|
| PRS_XDM-XOP-C-001-O | Single Presence Subscription Rules XML document describing who can subscribe to a presentity's presence, and content of notifications (PRSv1.1) | 5.1 | PRS_XDM_XOP-C-002-O AND<br>PRS_XDM_XOP-C-003-O AND<br>PRS_XDM_XOP-C-004-O AND<br>PRS_XDM_XOP-C-005-O AND<br>PRS_XDM_XOP-C-006-O AND<br>PRS_XDM_XOP-C-007-O AND<br>PRS_XDM_XOP-C-008-O AND<br>PRS_XDM_XOP-C-009-O |
| PRS_XDM-XOP-C-002-O | Structure of Presence Subscription Rules (PRSv1.1) | 5.1.1.1<br>5.1.2.1 | PRS_XDM-XOP-C-001-O |
| PRS_XDM-XOP-C-003-O | Application Unique ID of Presence Subscription Rules (PRSv1.1) | 5.1.1.2<br>5.1.2.2 | PRS_XDM-XOP-C-001-O |
| PRS_XDM-XOP-C-005-O | XML schema of Presence Subscription Rules (PRSv1.1) | 5.1.1.3<br>5.1.2.3 | PRS_XDM-XOP-C-001-O |
| PRS_XDM-XOP-C-004-O | Default namespace for Presence Subscription Rules (PRSv1.1) | 5.1.1.4<br>5.1.2.4 | PRS_XDM-XOP-C-001-O |
| PRS_XDM-XOP-C-006-O | MIME type of Presence Subscription Rules (PRSv1.1) | 5.1.1.5<br>5.1.2.5 | PRS_XDM-XOP-C-001-O |

| Item | Function | Reference | Requirement |
|---|---|---|---|
| PRS_XDM-XOP-C-007-O | Validation constraints of Presence Subscription Rules, in addition to the XML schema (PRSv1.1) | 5.1.1.6<br>5.1.2.6 | PRS_XDM-XOP-C-001-O |
| PRS_XDM-XOP-C-008-O | Data semantics of Presence Subscription Rules (PRSv1.1) | 5.1.1.7<br>5.1.2.7 | PRS_XDM-XOP-C-001-O |
| PRS_XDM-XOP-C-009-O | Naming conventions for Presence Subscription Rules (PRSv1.1) | 5.1.1.8<br>5.1.2.8 | PRS_XDM-XOP-C-001-O |
| PRS_XDM-XOP-C-010-O | Structure of Permanent Presence State (PRSv2.0) | 5.2.1 | PRS-SRC-C-016-O AND<br>PRS_XDM-XOP-C-011-O AND PRS_XDM-XOP-C-012-O AND PRS_XDM-XOP-C-013-O AND PRS_XDM-XOP-C-014-O AND PRS_XDM-XOP-C-015-O AND PRS_XDM-XOP-C-016-O |
| PRS_XDM-XOP-C-011-O | Application Unique ID of Permanent Presence State (PRSv2.0) | 5.2.2 | PRS_XDM-XOP-C-010-O |
| PRS_XDM-XOP-C-012-O | XML schema of Permanent Presence State (PRSv2.0) | 5.2.3 | PRS_XDM-XOP-C-010-O |
| PRS_XDM-XOP-C-013-O | Default namespace for Permanent Presence State (PRSv2.0) | 5.2.4 | PRS_XDM-XOP-C-010-O |
| PRS_XDM-XOP-C-014-O | MIME type of Permanent Presence State (PRSv2.0) | 5.2.5 | PRS_XDM-XOP-C-010-O |
| PRS_XDM-XOP-C-015-O | Data semantics of Permanent Presence State (PRSv2.0) | 5.2.7 | PRS_XDM-XOP-C-010-O |
| PRS_XDM-XOP-C-016-O | Naming conventions for Permanent Presence State (PRSv2.0) | 5.2.8 | PRS_XDM-XOP-C-010-O |

| Item | Function | Reference | Requirement |
|---|---|---|---|
| PRS_XDM-XOP-C-017-O | Presence Publication Rules Application Usages (PRSv2.0) | 5.3 | PRS_XDM-XOP-S-018-O AND PRS_XDM-XOP-S-019-O AND PRS_XDM-XOP-S-020-O AND PRS_XDM-XOP-S-021-O AND PRS_XDM-XOP-S-022-O AND PRS_XDM-XOP-S-023-O AND PRS_XDM-XOP-S-024-O AND PRS_XDM-XOP-S-025-O |
| PRS_XDM-XOP-C-018-O | Structure of Presence Publication Rules (PRSv2.0) | 5.3.1.1<br>5.3.2.1 | PRS_XDM-XOP-C-017-O |
| PRS_XDM-XOP-C-019-O | Application Unique ID of Presence Publication Rules (PRSv2.0) | 5.3.1.2<br>5.3.2.2 | PRS_XDM-XOP-C-017-O |
| PRS_XDM-XOP-C-020-O | XML schema of Presence Publication Rules (PRSv2.0) | 5.3.1.3<br>5.3.2.3 | PRS_XDM-XOP-C-017-O |
| PRS_XDM-XOP-C-021-O | Default namespace for Presence Publication Rules (PRSv2.0) | 5.3.1.4<br>5.3.2.4 | PRS_XDM-XOP-C-017-O |
| PRS_XDM-XOP-C-022-O | MIME type of Presence Publication Rules (PRSv2.0) | 5.3.1.5<br>5.3.2.5 | PRS_XDM-XOP-C-017-O |
| PRS_XDM-XOP-C-023-O | Validation constraints of Presence Publication Rules, in addition to the XML schema (PRSv2.0) | 5.3.1.6<br>5.3.2.6 | PRS_XDM-XOP-C-017-O |
| PRS_XDM-XOP-C-024-O | Data semantics of Presence Publication Rules (PRSv2.0) | 5.3.1.7<br>5.3.2.7 | PRS_XDM-XOP-C-017-O |
| PRS_XDM-XOP-C-025-O | Naming conventions for Presence Publication Rules (PRSv2.0) | 5.3.1.8<br>5.3.2.8 | PRS_XDM-XOP-C-017-O |

| Item | Function | Reference | Requirement |
|---|---|---|---|
| PRS_XDM-XOP-C-026-O | Structure of Publication Content Rules Presence Source View (PRSv2.0) | 5.4.1 | PRS_XDM-XOP-C-017-O AND PRS_XDM-XOP-C-027-O AND PRS_XDM-XOP-C-028-O AND PRS_XDM-XOP-C-029-O AND PRS_XDM-XOP-C-030-O AND PRS_XDM-XOP-C-031-O AND PRS_XDM-XOP-C-032-O |
| PRS_XDM-XOP-C-027-O | Application Unique ID of Publication Content Rules Presence Source View (PRSv2.0) | 5.4.2 | PRS_XDM-XOP-C-026-O |
| PRS_XDM-XOP-C-028-O | XML schema of Publication Content Rules Presence Source View (PRSv2.0) | 5.4.3 | PRS_XDM-XOP-C-026-O |
| PRS_XDM-XOP-C-029-O | Default namespace for Publication Content Rules Presence Source View (PRSv2.0) | 5.4.4 | PRS_XDM-XOP-C-026-O |
| PRS_XDM-XOP-C-030-O | MIME type of Publication Content Rules Presence Source View (PRSv2.0) | 5.4.5 | PRS_XDM-XOP-C-026-O |
| PRS_XDM-XOP-C-031-O | Data semantics of Publication Content Rules Presence Source View (PRSv2.0) | 5.4.7 | PRS_XDM-XOP-C-026-O |
| PRS_XDM-XOP-C-032-O | Naming conventions for Publication Content Rules Presence Source View (PRSv2.0) | 5.4.8 | PRS_XDM-XOP-C-026-O |

# Appendix C. Examples (Informative)

## C.1 Manipulating Presence Subscription Rules

### C.1.1 Obtaining Presence Subscription Rules

Both Subscription Authorization Rules and Subscription Content Rules are stored in one XML document. Figure C.1 describes how the XDMC obtains Presence Subscription Rules.

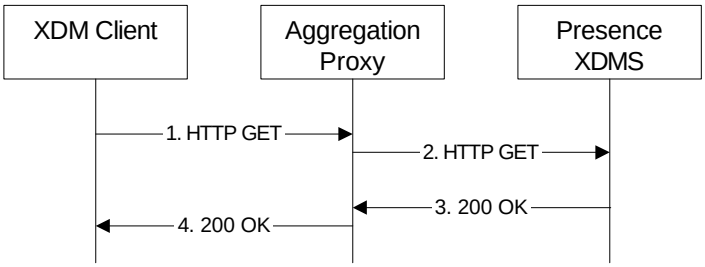


**Figure C.1- XDMC obtains Presence Subscription Rules**

The details of the flows are as follows:

1) The user "sip:ronald.underwood@example.com" wants to obtain the document describing his Presence Subscription Rules. For this purpose the XDMC 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 authorization 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 XDMC.

# C.2 Manipulating Presence Publication Rules

## C.2.1 Obtaining Presence Publication Rules

Both Publication Authorization Rules and Publication Content Rules are stored in one XML document. Figure C.2 describes how the XDMC obtains Presence Publication Rules.

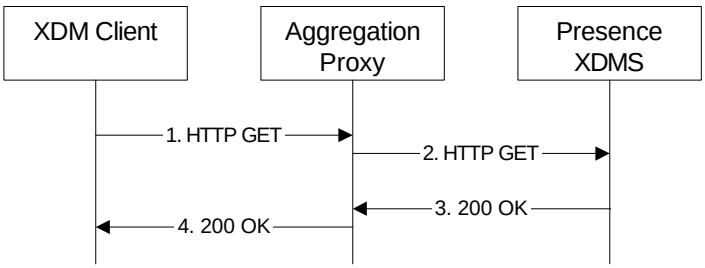


**Figure C.2- XDMC obtains Presence Publication Rules**

The details of the flows are as follows:

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

```
GET / org.openmobilealliance.pub-rules/users/sip:ronald.underwood@example.com/pub-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 authorization checks on the request originator, the Presence XDMS sends an HTTP 200 (OK) response including the requested document in the body. In this document the user "sip:hermione.blosom@example.com" is given the permission to publish any type of presence information using a PUBLISH request or a Permanent Presence State. The user "sip:joe.carter@example.com" is given the permission only to publish the <person> element with one or more <activities> child elements using a PUBLISH request.

```
HTTP/1.1 200 OK
Etag: "ett6e"
...
Content-Type: application/auth-policy+xml; charset="utf-8"

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

```
  <cr:rule id="wp_prs_allow_one_1">
    <cr:conditions>
      <cr:identity>
        <cr:one id="sip:hermione.blosom@example.com"/>
      </cr:identity>
    </cr:conditions>
    <cr:actions>
      <op:pub-handling>allow</op:pub-handling>
      <op:perm-handling>allow</op:perm-handling>
    </cr:actions>
    <cr:transformations>
      <op:allow-services>true</op:allow-services>
      <op:allow-persons>true</op:allow-persons>
      <op:allow-devices>true</op:allow-devices>
      <op:allow-all-attributes/>
    </cr:transformations>
  </cr:rule>
  <cr:rule id="wp_prs_allow_one_2">
    <cr:conditions>
      <cr:identity>
        <cr:one id="sip:joe.carter@example.com"/>
      </cr:identity>
    </cr:conditions>
    <cr:actions>
      <op:pub-handling>allow</op:pub-handling>
    </cr:actions>
    <cr:transformations>
      <op:allow-persons>true</op:allow-persons>
      <op:allow-activities>true</op:allow-activities>
    </cr:transformations>
  </cr:rule>
</cr:ruleset>
```

4) The Aggregation Proxy routes the response to the XDMC.

# C.3 Obtaining a Publication Content Rules Presence Source View Document

In this example, a Presence Source with the identity “sip:joe.carter@example.com” has published a presence document using a SIP PUBLISH request on behalf of a Presentity as described in [PRS_Spec] with the identity sip:ronald.underwood@example.com”. The Presence Information published includes Presence Information that is not a <person> element with an <activities> child element (e.g. a <tuple> element) and the Presence Publication Rules document used by the PS to perform the Publication Content Authorization is the one shown in appendix C.2.1. This means that the PS has returned a 488 response with a Policy-Contact header containing a URI “http:// xcap.example.com/org.openmobilealliance.pub-rules-view/users/sip:ronald.underwood@example.com/pub-rules-view”. The Presence Source retrieves the document via an XDMC in the UE. Figure C.3 describes how the XDMC obtains this Publication Content Rules Presence Source View Document.

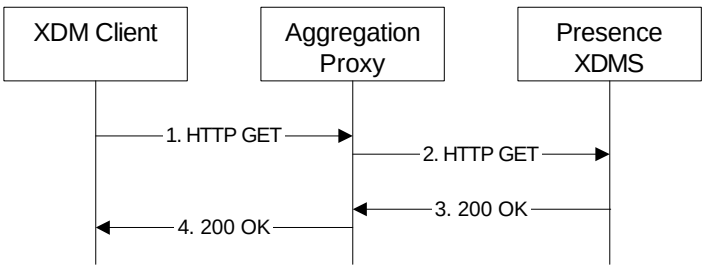


**Figure C.3- XDMC obtains Publication Content Rules Presence Source View**

The details of the flow are as follows:

1) The XDMC sends an HTTP GET request to the Aggregation Proxy.

```
GET / org.openmobilealliance.pub-rules-view/users/sip:ronald.underwood@example.com/pub-rules-view
   HTTP/1.1
Host: xcap.example.com
...
X-3GPP-Intended-Identity: "sip:joe.carter@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 authorization checks on the request originator as described in section 5.3.2.11, the Presence XDMS sends an HTTP 200 (OK) response including the requested document in the body.

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

<?xml version="1.0" encoding="UTF-8"?>
<cr:ruleset
   xmlns:op="urn:oma:xml:prs:pub-rules"
   xmlns:cr="urn:ietf:params:xml:ns:common-policy">
   <cr:rule id="wp_prs_allow_one_2">
    <cr:conditions>
      <cr:identity>
        <cr:one id="sip:joe.carter@example.com"/>
      </cr:identity>
    </cr:conditions>
    <cr:actions>
      <op:pub-handling>allow</op:pub-handling>
    </cr:actions>
    <cr:transformations>
      <op:allow-persons>true</op:allow-persons>
      <op:allow-activities>true</op:allow-activities>
    </cr:transformations>
  </cr:rule>
</cr:ruleset>
```

4) The Aggregation Proxy routes the response to the XDMC.

5) The Presence Source receives this information via the XDMC and makes a decision if it shall send a new SIP PUBLISH request or not.

# C.4 Manipulating Permanent Presence State

## C.4.1 Obtaining Permanent Presence State

Figure C.4 describes how the XDMC obtains the Permanent Presence State document.

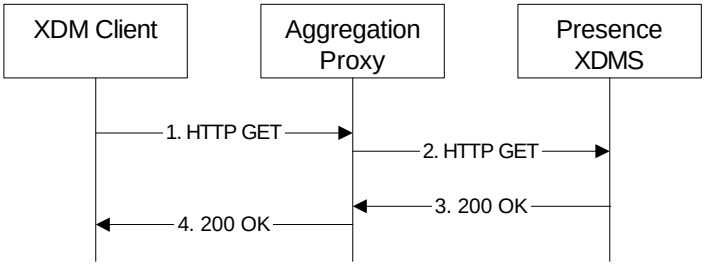

**Figure C.4- XDMC obtains Permanent Presence State**

The details of the flows are as follows:

5) A user “sip:ronald.underwood@example.com” wants to obtain his Permanent Presence State document. For this purpose the XDMC sends an HTTP GET request to the Aggregation Proxy.

```
GET / pidf-manipulation/users/sip:ronald.underwood@example.com/perm-presence HTTP/1.1
Host: xcap.example.com
...
```

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

7) After the Presence XDMS has performed the necessary authorization 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: "ett0f"
...
Content-Type: application/pidf+xml; charset="utf-8"

<?xml version="1.0" encoding="UTF-8"?>
<presence xmlns="urn:ietf:params:xml:ns:pidf"
    xmlns:pdm="urn:ietf:params:xml:ns:pidf:data-model"
    xmlns:rpid="urn:ietf:params:xml:ns:pidf:rpid"
    entity="sip:ronald.underwood@example.com">

    <pdm:person id="a1233">
        <rpid:activities>
            <rpid:vacation/>
        </rpid:activities>
        <pdm:note xml:lang="en">I am skiing in Alps!!!</pdm:note>
    </pdm:person>

</presence>
```

8) The Aggregation Proxy routes the response to the XDMC.