PoC XDM Specification

Candidate Version 1.0 – 28 April 2005

Open Mobile Alliance

OMA-TS-PoC_XDM-V1_0-20050428-C

Contents

Figures

1. Scope

The PoC enabler specific data formats and XCAP application usages are described in this specification.

2. References

2.1 Normative References

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

[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

[RFC3261] "SIP: Session Initiation Protocol", J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler, June 2002, URL:http://www.ietf.org/rfc/rfc3261.txt

[RFC3966] "The tel URI for Telephone Numbers", H. Schulzrinne, December 2004, URL:http://www.ietf.org/rfc/rfc3966.txt

[XCAP] "The Extensible Markup Language (XML) Configuration Access protocol (XCAP)", J. Rosenberg, November 2004, URL:http://www.ietf.org/internet-drafts/draft-ietf-simple-xcap-05.txt

Note: IETF Draft work in progress.

[COMMONPOL] "A Document Format for Expressing Privacy Preferences", H. Schulzrinne, J. Morris, H. Tschofenig, J. Cuellar, J. Polk, J. Rosenberg, February. 2005, URL:http://www.ietf.org/internet-drafts/draft-ietf-geopriv-common-policy-04.txt

Note: IETF Draft work in progress.

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

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

Note: IETF Draft work in progress.

[SHAREDXDM] "OMA Shared XDM Specification", Version 1.0, Open Mobile Alliance™, OMA-TS-XDM_Shared-V1_0, URL:http://www.openmobilealliance.org/

2.2 Informative References

[XDMAD] "XML Document Management Architecture", Version 1.0. Open Mobile Alliance™. OMA-AD-XDM-V1_0

[OMA-POC-AD] "Push to talk over Cellular (PoC) - Architecture", Version 1.0, Open Mobile Alliance™, OMA-AD-PoC-V1_0, URL:http://www.openmobilealliance.org/

[OMA-POC-CP] "OMA PoC Control Plane", Version 1.0, Open Mobile Alliance™, OMA-TS-PoC_ControlPlane-V1_0, URL:http://www.openmobilealliance.org/

3. Terminology and Conventions

3.1 Conventions

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

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

3.2 Definitions

Application Unique ID (AUID)	A unique identifier that differentiates XCAP resources accessed by one application from XCAP resources accessed by another application. (Source: [XCAP])
Global document	A document placed under the XCAP global tree that applies to all users of that application usage.
Global tree	A URL that represents the parent for all global documents for a particular application usage within a particular XCAP root. (Source: [XCAP])
PoC Group Identity	SIP URI of the Pre-arranged PoC Group or Chat PoC Group. (Source: [PoC-CP])
PoC Group Member	A PoC User on the predefined list of those who are to be invited during initial session establishment (in the case of Pre-arranged PoC Group), or allowed to join the session (in the case of Restricted Chat PoC Group). (Source: [PoC-CP])
XCAP Application Usage	Detailed information on the interaction of an XCAP Client with an XCAP server. (Source: [XCAP])
XCAP Client	An HTTP client that understands how to follow the naming and validation constraints defined in this specification. (Source: [XCAP])
XCAP Root	A context that includes all of the documents across all application usages and users that are managed by a server. [Source: XCAP]
XCAP Root URI	An HTTP URI that represents the XCAP root. Although a valid URI, the XCAP Root URI does not correspond to an actual resource. [Source: XCAP]
XCAP Server	An HTTP server that understands how to follow the naming and validation constraints defined in this specification. (Source: [XCAP])
XCAP User Identifier (XUI)	The XUI is a string, valid as a path element in an HTTP URI, that is associated with each user served by the XCAP server. [Source: XCAP]

3.3 Abbreviations

AUID	Application Unique ID
HTTP	Hypertext Transfer Protocol
OMA	Open Mobile Alliance
PoC	Push-to-Talk Over Cellular
URI	Uniform Resource Identifier
XCAP	XML Configuration Access Protocol
XDM	XML Document Management
XDMC	XDM Client
XDMS	XDM Server
XML	Extensible Markup Language
XUI	XCAP User Identifier

4. Introduction

This specification provides the data schema and application usages for PoC-specific documents. PoC XDM Application Usages include that for PoC Groups and PoC User Acess Policy.

5. PoC XDM Application Usages

5.1 PoC Group

5.1.1 Structure

The PoC Group document SHALL conform to the structure of the “group” document described in this sub-clause. The schema definition is provided in section 5.1.3.

The <list-service> element

a) SHALL include a “uri” attribute representing the PoC Group Identity;

b) MAY include any other attributes from any other namespaces for the purposes of extensibility;

c) MAY include a <display-name> element containing a human readable name of the group;

d) MAY include a <list> element containing the group members;

e) MAY include an <invite-members> element indicating whether the group members will be invited;

f) MAY include a <max-participant-count> element;

g) MAY include a <ruleset> element representing the authorization policy associated with this group;

h) MAY include any other elements from any other namespaces for the purposes of extensibility.

Each <list> element SHALL be composed of a sequence of zero or more elements, each of which is

a) an <entry> element containing an attribute "uri" that conforms with SIP URI (as defined in [RFC3261]) or a TEL URI (as defined in [RFC3966]) identifying a single user, and an optional child element <display-name> associated with each element <entry>, containing a human readable name of each group member, as defined in [XCAP_List]; or

b) an <external> element pointing to a URI List in the Shared XDMS as defined in[SHAREDXDM].

The structure of the <ruleset> element SHALL conform to [COMMONPOL]. Each <ruleset> element is composed of a sequence of zero or more <rule> elements.

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

a) the <identity> element as described 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 <is-list-member> element as defined in Section 5.1.3.

Other types of <conditions> elements described in [COMMONPOL] are not defined by this specification. This means that, if present, the PoC server ignores such elements.

The <actions> child element of any <rule> element MAY include the following child elements defined in Section 5.1.3:

a) the <allow-conference-state> element

b) the <allow-invite-users-dynamically> element

c) the <join-handling> element

d) the <allow-initiate-conference> element

e) the <allow-anonymity> element

f) the <is-key-participant> element

5.1.2 Application Unique ID

The AUID SHALL be “org.openmobilealliance.poc-groups”.

5.1.3 XML Schema

The “group” document SHALL be composed according to the XML schema detailed in this sub-clause.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
   targetNamespace="urn:oma:params:xml:ns:list-service"
   xmlns:xs=http://www.w3.org/2001/XMLSchema
   xmlns:cr="urn:ietf:params:xml:ns:common-policy"
   xmlns:rl="urn:ietf:params:xml:ns:resource-lists"
   elementFormDefault="qualified" attributeFormDefault="unqualified">

  <!-- This import brings in the IETF common policy -->
  <xs:import namespace="urn:ietf:params:xml:ns:common-policy"/>
  <!-- This import brings in the common extensions for authorization rules in [XDMSPEC]-->
  <xs:import namespace="urn:oma:params:xml:ns:common-policy"/>
  <!-- The root "group" element -->
  <xs:element name="group">
    <xs:complexType>
      <xs:sequence maxOccurs="unbounded">
        <xs:element name="list-service" type="list-service-type"/>
      </xs:sequence>
    </xs:complexType>
  </xs:element>

  <xs:complexType name="list-service-type">
    <xs:sequence>
      <xs:element name="display-name" type=" rl:display-nameType " minOccurs="0"/>
      <xs:element name="list" type="list-type" minOccurs="0"/>
      <xs:element name="invite-members" type="xs:boolean" minOccurs="0"/>
      <xs:element name="max-participant-count" type="xs:nonNegativeInteger"
minOccurs="0"/>
      <xs:element ref="cr:ruleset" minOccurs="0"/>
      <xs:any namespace="##other" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
    </xs:sequence>
    <xs:attribute name="uri" type="xs:anyURI" use="required">
```

```
    <xs:anyAttribute namespace="##other" processContents="lax" minOccurs="0"
maxOccurs="unbounded"/>
  </xs:complexType>

  <xs:complexType name="list-type">
    <xs:sequence>
      <xs:element name="entry" type="rl:entryType" minOccurs="0" maxOccurs="unbounded"/>
      <xs:element name="external" type="rl:externalType" minOccurs="0"
maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

  <xs:simpleType name="join-handling-type">
    <xs:restriction base="xs:string">
      <xs:enumeration value="allow"/>
      <xs:enumeration value="block"/>
    </xs:restriction>
  </xs:simpleType>

  <!-- OMA specific "conditions" child elements -->

  <xs:element name="is-list-member" type="xs:boolean" substitutionGroup="cr:condition"/>

  <!--OMA specific "actions" child elements -->
  <xs:element name="allow-conference-state" type="xs:boolean"
substitutionGroup="cr:action"/>
  <xs:element name="allow-invite-users-dynamically" type="xs:boolean"
substitutionGroup="cr:action"/>
  <xs:element name="join-handling" type="join-handling-type"
substitutionGroup="cr:action"/>
  <xs:element name="allow-initiate-conference" type="xs:boolean"
substitutionGroup="cr:action"/>
  <xs:element name="allow-anonymity" type="xs:boolean" substitutionGroup="cr:action"/>

  <xs:element name="is-key-participant" type="xs:boolean" substitutionGroup="cr:action"/>

</xs:schema>
```

5.1.4 MIME Type

The MIME type for the PoC Group document SHALL be “application/list-service+xml”.

Editor note: OMNA needs to define the IANA registration procedures for this MIME type.

5.1.5 Validation constraints

The PoC Group document SHALL conform to the XML Schema described in section 5.1.3, with the clarifications given in this sub-clause.

A PoC Group document stored in the “users” tree of PoC XDMS SHALL contain only one <list-service> element.

The value of the "uri" attribute in the <list-service> element:

- SHALL be in the format of a SIP URI.
- SHALL be unique amongst *all* PoC Group documents spanning *all* "users" trees stored across all PoC XDMS in a service provider's domain.
- SHALL conform to the syntax specified by the Conference URI Template (see [OMA-POC-CP] Appendix B), which is stored in the PoC XDMS and provisioned to the XDM Client.

If this "uri" attribute value does not conform to any local policy or the constraintS described above, the PoC XDMS SHALL respond with an HTTP "409 Conflict" response as described in [XCAP]. The error condition SHALL be described by the <uniqueness-failure> error element.

If the Conference URI violated additional constraints imposed by local policy, the "phrase" attribute SHOULD be set to "URI constraint violated".

NOTE 1: The rendering of any "phrase" attribute to a human user is a user interface issue, and is not standardized.

NOTE 2: If the server decides to use the "phrase" text as defined in this specification, it will ignore the received HTTP Accept-language header value.

If the <uniqueness-failure> element in the received HTTP "409 Conflict" response includes an "alt-value" element, the XDM Client SHOULD repeat the XCAP request using a "uri" attribute chosen from one of the values provided in the received "alt-value" elements.

If the value proposed by the XDMC for the <max-participant-count> exceeds the value determined by the PoC XDMS, an HTTP "409 Conflict" response SHALL be returned with the error condition identified by the <constraint-failure> element. If included, the "phrase" attribute of this element SHOULD be set to "Maximum number of participants exceeded".

The value of an <entry> element SHALL contain a syntactically valid PoC Address (see [OMA-POC-CP]).

If the value proposed for the <entry> element does not conform to the syntax of a supported URI, the PoC XDMS SHALL return an HTTP "409 Conflict" response including the XCAP error element <constraint-failure>. If included, the "phrase" attribute SHOULD be set to "URI syntax error".

If the XDMC adds an <entry> element to the <list> element whose "uri" attribute matches that of another <entry> element already present, the PoC XDMS SHALL return an HTTP "409 Conflict" including the error element <constraint-failure>. If included, the "phrase" attribute SHOULD be set to "Duplicate entry".

Any AUID value other than "resource-lists" in the Document URL contained in an <external> or <external-list> element SHALL be a validation error. If so, the <external> or <external-list> insertion SHALL fail with an HTTP "409 Conflict" response which includes the XCAP error element <constraint-failure>. If included, the "phrase" attribute SHOULD be set to "Wrong type of shared list".

If the XUI value of the Document URL proposed in an <external> or <external-list> element does not match the XUI of a PoC group Document URI or a <list> element within a "resource-lists" document, this SHALL be a validation error. If so, the <external> or <external-list> element insertion SHALL fail with an HTTP "409 Conflict" response, which includes the XCAP error element <constraint-failure>. If included, the "phrase" attribute SHOULD be set to "Access denied to shared list".

5.1.6 Data Semantics

The value of the "uri" attribute in the <list-service> element SHALL represent a PoC Group Identity.

The <list> element SHALL contain the PoC Group Members:

- The <list > element MAY contain one or several <entry> child elements. The <entry> element SHALL contain an attribute "uri" which contains a valid PoC Address, i.e., either a SIP URI (as defined in [RFC3261]) or TEL URI (as defined in [RFC3966]) , as well as a <display-name> associated with each of the element <entry>, and

- The <list> element MAY contain one or several<external> child elements. The <external-list> element SHALL referencing URI Lists stored in the Shared XDMS (as defined in [SHAREDXDM]). Such referenced URI lists SHALL belong to the same user as that of the PoC Group document.

The <invite-members> element SHALL indicate whether the PoC Server will invite the group members to the PoC Group Session. The possible values are::

"false" represents the Chat PoC Group (see [OMA-POC-CP]). The PoC Server performing the Controlling PoC Function will not invite the group members to the PoC Group Session. This SHALL be the default value taken in the absence of the element.

"true" represents the Pre-arranged PoC Group (see [OMA-POC-CP]). The PoC Server performing the Controlling PoC Function will invite the members of the <list> element as described in [OMA-POC-CP] section 7.2.1.3.

The <max-participant-count> element SHALL indicate the maximum number of participants allowed by the document owner in the PoC group session. The usage of this parameter is described in [OMA-POC-CP].

The <is-list-member> "condition" element SHALLbe used to match an identity against the contents of the <list> element.

The <join-handling> element SHALL define the action that the PoC Server performing the Controlling PoC Function is to take when processing a particular request to join a PoC Group Session. The semantics of the <join-handling> elemenent is defined in [OMA-POC-CP] section 7.2.1.6. The value SHALL be of an enumerated integer type:

"block" instructs the PoC Server to block the access to the PoC Session. This SHALL be the default value taken in the absence of the element. This value SHALL be assigned the numeric value of 0.

"allow" instructs the PoC Server to accept the access to the PoC Session. This value SHALL be assigned the numeric value of 1.

The <allow-initiate-conference> "action" SHALL be used to indicate that the identity matching this rule SHALL be allowed to initiate a Pre-arranged PoC Group Session. The semantics of the <allow-initiate-conference> is described in [OMA-POC-CP] section 7.2.1.14. The possible values are:

"false" instructs the PoC Server to prevent the user from initiating the Pre-arranged PoC Group Session. This SHALL be the default value taken in the absence of the element.

"true" instructs the PoC Server to allow the user to initiate the pre-arranged PoC Group Session.

The <allow-invite-users-dynamically> "action" SHALL be used to indicate to the PoC Server performing the Controlling PoC Function that inviting additional participants is allowed. The semantics of the <allow-invite-users-dynamically> element is defined in [OMA-POC-CP] section 7.2.1.15. The possible values are:

"false" instructs the PoC Server to prevent the user from inviting additional participants. This SHALL be the default value taken in the absence of the element.

"true" instructs the PoC Server to allow the user to invite additional participants.

The <allow-anonymity> “action” SHALL be used to indicate whether anonymity is allowed for a matching identity that is requesting anonymity. The possible values are:

“false” instructs the PoC Server to block an anonymous access to the PoC Session. This SHALL be the default value taken in the absence of the element.

“true” instructs the PoC Server to accept an anonymous access to the PoC Session.

The <allow-conference-state> “action” SHALL be used to indicate that the identity matching this rule is allowed to subscribe to the “conference” event package. The semantics of the <allow-conference-state> element is described in [OMA-POC-CP] section 7.2.1.11.1. The possible values are:

“false” instructs the PoC Server to block the subscription to the “conference” event package. This SHALL be the default value taken in the absence of the element.

“true” instructs the PoC Server to accept the subscription to the “conference” event package.

The <is-key-participant> “action” SHALL be used to indicate that the identity matching this rule is a ” Distinguished Participant”. The semantics of the “Distinguished Participant” is described in [OMA-POC-AD]. The The possible values are:

“false” instructs the PoC Server to treat the user as a normal participant. This SHALL be the default value taken in the absence of the element.

“true” instructs the PoC Server to treat the user as Distinguished Participant if the one-to-many-to-one topology is used.

5.1.7 Naming conventions

The naming conventions SHALL be defined according to [XDMSPEC].

5.1.8 Global documents

For every “list-service” specified in each "group" document created in the “users” tree for a particular user, the PoC XDMS SHALL support a single document in the global tree named “index” representing the union of all of the <list-service> elements across all "group" documents created by all users within the same XCAP root..

The uniqueness constraint on the “uri” attribute in the <list-service> element (see section 5.1.5) will ensure that no two <list-service> elements in the global document have the same value of that attribute. This allows a PoC Server to retrieve a specific <list-service> element in the “index” document using the PoC Group Identity.

Therefore, a XCAP GET targeted at the resource identified by the URI

http://[XCAP Root URL]/org.openmobilealliance.poc-groups/global/index/~~/group/list-service[@uri=”canonicalised value of the Poc Group Identity “]

SHALL return the <list-service> element of the PoC Group.

5.1.9 Resource interdependencies

There is a one-to-one correspondence between each “group” document in the “users” tree for a particular user and a <list-service> element in the “index” document in the global tree.

This correspondence is one-way, which means that a <list-service> element in the "index" document in the global tree is created/deleted/modified if and only if the corresponding document in the “users” tree is created/deleted/modified.

This does not imply that the server must actually store this “index” document. The server MUST always be prepared to process requests against this global “index” document and the contents of this document at any point in time MUST always accurately represent the state of all “group” documents in the “users” tree.

5.1.10 Authorization policies

The authorization policies for documents in the “users” tree SHALL be defined according to [XDMSPEC].

The authorization policies for documents in the “global” tree shall be as follows:

- Global documents SHALL be “read-only”
- Access to global documents SHALL be restricted based on local policy.

NOTE: It is expected that a PoC Server will access documents in the “global” tree. There is no reason why users should need to access the “global” tree

5.2 PoC User Access Policy

5.2.1 Structure

The PoC User Access Policy document SHALL conform to the structure of the “ruleset” document described in [COMMONPOL] and extended in section 5.2.3, with the extensions and constraints given in this sub-clause.

The PoC User Access Policy document makes use of the following two elements defined for the <rules> element in [COMMONPOL]:

- <conditions>
- <actions>

NOTE 1: This specification does not define any value for the <transformations> element defined as a child of the <rules> element in [COMMONPOL]. This means that, if present, the PoC server ignores this element.

The <conditions> element supports the following 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.

NOTE 2: This specification does not define any value for those elements defined as a part of the <conditions> element in [COMMONPOL] (e.g., <sphere>, <validity>) but which are not explicitly identified in the list above. This means that, if present, the PoC server ignores such elements.

The <actions> element supports the <allow-invite> element, as defined in section 5.2.3 and 5.2.6.

5.2.2 Application Unique ID

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

5.2.3 XML Schema

The PoC User Access Policy document SHALL conform to the XML schema detailed in [COMMONPOL] and extended in [XDMSPEC] section 6.6.2, with the extensions given in this sub-clause.

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema targetNamespace="urn:oma:params:xml:ns:poc-rules"
  xmlns:cr="urn:ietf:params:xml:ns:common-policy"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  elementFormDefault="qualified" attributeFormDefault="unqualified">
  elementFormDefault="qualified" attributeFormDefault="unqualified">
 <xs:import namespace="urn:oma:params:xml:ns:common-policy"/>
 <xs:import namespace="urn:ietf:params:xml:ns:common-policy"/>

 <xs:element name="allow-invite" substitutionGroup="cr:action">
  <xs:simpleType>
    <xs:restriction base="xs:string">
      <xs:enumeration value="reject"/>
      <xs:enumeration value="pass"/>
      <xs:enumeration value="accept"/>
    </xs:restriction>
  </xs:simpleType>
 </xs:element>
</xs:schema>
```

Editor note: It must be clarified how to register the OMA specific namespace.

5.2.4 MIME Type

The MIME type for PoC User Access Policy documents SHALL be “application/auth-policy+xml” defined in [COMMONPOL].

5.2.5 Validation constraints

The PoC User Access Policy document SHALL conform to the XML Schema described in [COMMONPOL] and extended in sub-clause 5.2.3, with the additional validation constraints described in this sub-clause.

The <id> child element of <identity>, if present, SHALL contain a SIP URI or a TEL URI.

For a given <ruleset>, the same value of an <id> element SHALL NOT occur in two “rules” which have different values for <allow-invite>. If this constraint is violated, the PoC XDMS SHALL return an HTTP “409 Conflict” including the XCAP error element <constraint-failure>. If included, the “phrase” attribute SHOULD be set to “Same user in contradictory rules”.

For a given <ruleset>, the same value of an <external-list> element SHALL NOT occur in two “rules” which have different values for <allow-invite>. If this constraint is violated, the PoC XDMS SHALL return an HTTP “409 Conflict” including the XCAP error element <constraint-failure>. If included, the “phrase” attribute SHOULD be set to “Same users in contradictory rules”.

NOTE: These validation constraints ensure that the end user is alerted to a contradictory choice, and also ensures that the PoC server has an unambiguous way of evaluating the rules.

Any AUID value other than “resource-lists” in the Document URL contained in an <external-list> element SHALL be a validation error. If so, the <external-list> insertion SHALL fail with an HTTP “409 Conflict” response which includes the XCAP error element <constraint-failure>. If included, the “phrase” attribute SHOULD be set to “Wrong type of shared list”.

If the XUI value of the Document URL proposed in an <external-list> element does not match the XUI of the PoC User Access Document URI, this SHALL be a validation error. If so, the <external-list> element insertion SHALL fail with an HTTP “409 Conflict” response, which includes the XCAP error element <constraint-failure>. If included, the “phrase” attribute SHOULD be set to “Access denied to shared list”.

5.2.6 Data Semantics

The PoC User Access Policy document SHALL conform to the semantics for the “conditions” and “actions” described in [COMMONPOL] and extended in [XDMSPEC] section 6.6.2, together with the clarifications required for the PoC service as given in this sub-clause.

When evaluating a “rule” against an identity, the value of an <id> element, if present, is compared against that identity to see if the “rule” is applicable.

If present, the <domain> child element of <identity> is used to create a simple rule matching all identities from a particular domain or only certain identities, using the <except> child element, in that domain.

The PoC User Access Policy document can contain references to URI Lists stored in Shared XDMS (as defined in [SHAREDXDM]).

The <allow-invite> element defines the action the PoC Server is to take when processing a PoC session invitation for a particular user. This element has one of the following three values, whose use is described in [OMA-POC-CP] section 7.3.2.2. The value is of an enumerated integer type:

“pass” instructing the PoC server to process the PoC session invitation using manual answer procedure (i.e. leave it for user to decide the acceptance). This is the lowest value for this action, and also the value used when no match happens, according to [COMMONPOL]. This value is assigned the numeric value of 0.

reject” instructing the PoC server to reject the invitation. This value is assigned the numeric value of 1.

“accept” instructing the PoC server to accept the invitation according to the user's answer mode setting. This value is assigned the numeric value of 2.

5.2.7 Naming conventions

The name of the PoC User Access Policy document SHALL be “pocrules”.

5.2.8 Global documents

This application usage defines no global documents.

5.2.9 Resource interdependencies

This application usage defines no additional resource interdependencies.

5.2.10 Authorization policies

The authorization policies SHALL be defined according to [XDMSPEC].

Appendix A. Static Conformance Requirements (Normative)

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

- PoC XDM Application Usages

Each SCR table identifies a list of supported features as:

Item: Identifier for a feature.

Function: Short description of the feature.

Reference: Section(s) of this specification with more details on the feature.

Status: Whether support for the feature is mandatory or optional. MUST use "M" for mandatory support and "O" for optional support in this column.

Requirement: This column identifies other features required by this feature. If no other features are required, this column is left empty.

This section describes the dependency grammar notation to be used in the Requirement column of the SCR and CCR tables using ABNF [RFC2234].

TerminalExpression = ScrReference / NOT TerminalExpression / TerminalExpression LogicalOperator TerminalExpression / "(" TerminalExpression ")"

ScrReference = ScrItem / ScrGroup

ScrItem = SpecScrName "–" GroupType "–" DeviceType "–" NumericId / SpecScrName "–" DeviceType "–" NumericId

ScrGroup = SpecScrName ":" FeatureType / SpecScrName "– " GroupType "–" DeviceType "–" FeatureType

SpecScrName = 1*Character;

GroupType = 1*Character;

DeviceType = "C" / "S"; C – client, S – server

NumericId = Number Number Number

LogicalOperator = "AND" / "OR"; AND has higher precedence than OR and OR is inclusive

FeatureType = "MCF" / "OCF" / "MSF" / "OSF"; See Section A.1.6

Character = %x41-5A ; A-Z

Number = %x30-39 ; 0-9

A.1 PoC XDM Application Usages of XDM Server

Item	Function	Reference	Status	Requirement
POC_XDM-AU-S-001	PoC Group document structure and elements supported	5.1.1	M	
POC_XDM-AU-S-002	Application Unique ID of PoC document	5.1.2 5.2.2	M	

Item	Function	Reference	Status	Requirement
POC_XDM-AU-S-003	XML schema of PoC Group	5.1.4 5.1.6	M	
POC_XDM-AU-S-004	MIME type of PoC Group and User Access policy documents	5.1.4. 5.2.4	M	
POC_XDM-AU-S-005	Data semantics of PoC Group document	5.1.6	M	
POC_XDM-AU-S-006	Naming conventions for PoC Group and User Access policy documents	5.1.7 5.2.7 s	M	
POC_XDM-AU-S-007	Authorization policies for manipulating PoC Group and User Access policy documents	5.1.10 5.2.10	M	
POC_XDM-AU-S-008	PoC User Access Policy document structure and elements supported	5.2.1	M	
POC_XDM-AU-S-009	XML schema of PoC User Access Policy document	5.2.3 5.2.5	M	
POC_XDM-AU-S-010	Data semantics of PoC User Access Policy document	5.2.6	M	

A.2 PoC Application Usages of XDM Client

Item	Function	Reference	Status	Requirement
PoC_XDM-CAU-C-001	Data semantics of PoC Group document	5.1.6	M	
PoC_XDM-CAU-C-002	XDM Client handling of HTTP “409 Conflict” response from the PoC XDMS	5.1.5	M	

Appendix B. Examples (Informative)

B.1 Manipulating PoC Group Documents

B.1.1 Obtaining a PoC Group Document

Figure B.1 describes how XDM client obtains a particular PoC Group document.

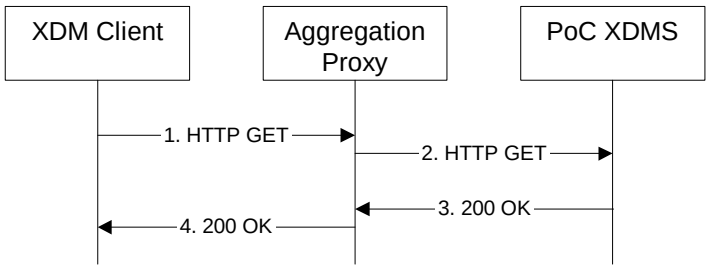

Figure B.1- XDM Client obtains a particular PoC Group document

The details of the flows are as follows:

1) The user "sip:ronald.underwood@example.com" wants to obtain the document, gossips.xml, describing the group "sip:myconference@example.com". For this purpose the XDMC sends an HTTP GET request to the Aggregation Proxy.

```
GET http://xcap.example.com/services
   /org.openmobilealliance.poc-groups/users/sip:ronald.underwood@example.com/gossips.xml HTTP/1.1
...
Content-Length: 0
```

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

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

```
HTTP/1.1 200 OK
Etag: "et53"
...
Content-Type: application/list-service+xml

<?xml version="1.0" encoding="UTF-8"?>
<group xmlns="urn:oma:params:xml:ns:list-service"
   xmlns:rl="urn:ietf:params:xml:ns:resource-lists"
   xmlns:cr="urn:oma:params:xml:ns:common-policy"
   >
  <list-service uri="sip:myconference@example.com">
    <list>
      <rl:entry uri="tel:+43012345678"/>
      <rl:entry uri="sip:hermione.blossom@example.com"/>
    </list>
    <display-name xml:lang="en-us">Friends</display-name>
    <max-participant-count>10</max-participant-count>
    <cr:ruleset>
      <cr:rule id="a7c">
        <cr:conditions>
          <cr:is-list-member/>
        </cr:conditions>
        <cr:actions>
          <join-handling>allow</join-handling>
          <allow-anonymity>true</allow-anonymity>
        </cr:actions>
      </cr:rule>
    </cr:ruleset>
  </list-service>
```

```
</group>
```

4) The Aggregation Proxy routes the response to the XDM Client.

B.1.2 PoC Conference URI negotiation

Figure B.2 describes how the PoC XDMS can negotiate a Conference URI.

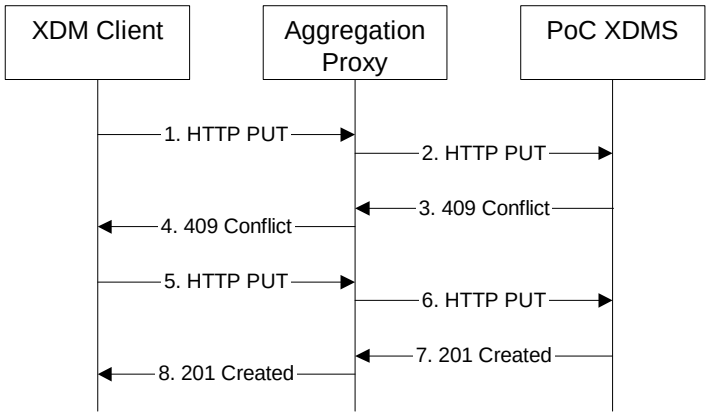

Figure B.2- PoC XDMS negotiates a Conference URI

The details of the flows are as follows:

1) The user "sip:ronald.underwood@example.com" wants to create a document with a conference URI "sip:wrongname@example.com". For this purpose the XDMC sends an HTTP PUT request to the Aggregation Proxy.

```
PUT http://xcap.example.com/services
   /org.openmobilealliance.poc-groups/users/sip:ronald.underwood@example.com/MyGroup.xml HTTP/1.1
...
Content-Type: application/list-service+xml
Content-Length: (...)

<?xml version="1.0" encoding="UTF-8"?>
<group xmlns="urn:oma:params:xml:ns:list-service"
   xmlns:poc="urn:oma:params:xml:ns:poc-group"
   xmlns:rl="urn:ietf:params:xml:ns:resource-lists"
   xmlns:cr="urn:oma:params:xml:ns:common-policy">
  <list-service uri="sip:wrongname@example.com">
    <list>
      <rl:entry uri="tel:+43012345678"/>
      <rl:entry uri="sip:hermione.blossom@example.com"/>
    </list>
    <invite-members>true</invite-members>
    <cr:ruleset>
      <cr:rule id="78t">
        <cr:conditions>
          <cr:other-identity/>
        </cr:conditions>
        <cr:actions>
          <join-handling>allow</join-handling>
        </cr:actions>
      </cr:rule>
    </cr:ruleset>
  <list-service>
</group>
```

creating the file "MyGroup.xml" to describe the pre-arranged PoC Group whose proposed name is "sip:wrongname@example.com".

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

3) The PoC XDMS detects that the conference URI does not conform to the local policy. The PoC XDMS generates a valid conference name “sip:correctname@example.com” and sends an HTTP “409 Conflict” response including the generated URI.

```
HTTP/1.1 409 Conflict
...
Content-Type: application/xcap-error+xml

<?xml version="1.0" encoding="UTF-8"?>
<xcap-error xmlns="urn:ietf:params:xml:ns:xcap-error">
  <uniqueness-failure phrase="URI constraint violated">
    <exists field="group/list-service/@uri">
      <alt-value>sip:correctname@example.com</alt-value>
    </exists>
  </uniqueness-failure>
</xcap-error>
```

4) The Aggregation Proxy routes the response to the XDM Client.

5) The XDM Client repeats the XCAP request (sent in step 1) using the received PoC conference URI value.

```
PUT http://xcap.example.com
   /services/org.openmobilealliance.poc-groups/users/sip:ronald.underwood@example.com/MyGroup.xml
   HTTP/1.1
...
Content-Type: application/list-service+xml
Content-Length: (...)

<?xml version="1.0" encoding="UTF-8"?>
<group xmlns="urn:oma:params:xml:ns:list-service"
   xmlns:poc="urn:oma:params:xml:ns:poc-group"
   xmlns:rl="urn:ietf:params:xml:ns:resource-lists"
   xmlns:cr="urn:oma:params:xml:ns:common-policy">
  <list-service uri="sip:correctname@example.com">
    <list>
      <rl:entry uri="tel:+43012345678"/>
      <rl:entry uri="sip:hermione.blossom@example.com"/>
    </list>
    <invite-members>true</invite-members>
    <cr:ruleset>
      <cr:rule id="78t">
        <cr:conditions>
          <cr:other-identity/>
        </cr:conditions>
        <cr:actions>
          <join-handling>allow</join-handling>
        </cr:actions>
      </cr:rule>
    </cr:ruleset>
  <list-service>
</group>
```

where the file “MyGroup.xml” is the document created in step 1)

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

7) The PoC XDMS creates the request PoC conference URI and sends an HTTP “201 Created” response.

```
HTTP/1.1 201 Created
Etag: "et17a"
...
Content-Length: 0
```

8) The Aggregation Proxy routes the response to the XDM Client.

B.2 Manipulating PoC User Access Policy

B.2.1 Obtaining PoC User Access Policy rules

Figure B.3 describes how XDM client obtains PoC User Access Policy rules.

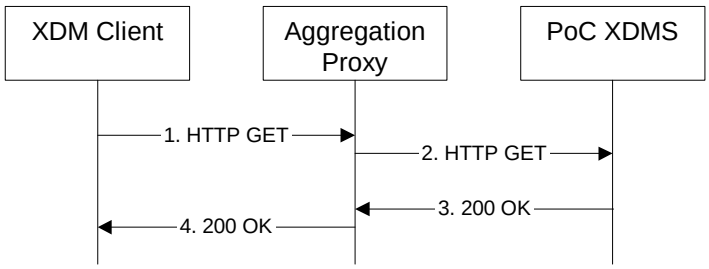

Figure B.3- XDM Client obtains PoC User Access Policy rules

The details of the flows are as follows:

1) The user "sip:ronald.underwood@example.com" wants to obtain the document describing his PoC User Access Policy rules. For this purpose the XDMC sends an HTTP GET request to the Aggregation Proxy.

```
GET http://xcap.example.com
   /services/org.openmobilealliance.poc-rules/users/sip:ronald.underwood@example.com/pocrules
   HTTP/1.1
...
Content-Length: 0
```

where the filename "pocrules" is a standardized naming convention (see section 5.2.7).

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

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

```
HTTP/1.1 200 OK
Etag: "etu15"
...
Content-Type: application/auth-policy+xml

<?xml version="1.0" encoding="UTF-8"?>
<ruleset xmlns="urn:ietf:params:xml:ns:common-policy"
   xmlns:poc="urn:oma:params:xml:ns:poc-rules">
  <rule id="f3g44r1">
    <conditions>
      <identity>
        <id>tel:5678;phone-context=+43012349999</id>
        <id>sip:percy.underwood@example.com</id>
      </identity>
    </conditions>
    <actions>
      <poc:allow-invite>true</poc:allow-invite>
    </actions>
  </rule>
</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
n/a	n/a	No prior version

C.2 Candidate Version 1.0 History

Document Identifier	Date	Sections	Description
Draft Version OMA-PoC_XDM_Specification-V1_0	27 Sept 2004	All	Initial version created.
	26 Oct 2004	All	Incorporates input to committee: OMA-PAG-2004-0534R1-POC-XDMS-InitialContribution OMA-PAG-2004-0557-Changes-to-Section-5-of-the-PoC-XDM-Spec
	02 Nov 2004	All	Incorporates input to committee: OMA-PAG-2004-0580R02-PoC-XDM-Spec-key-participant OMA-PAG-2004-0604R01-XDM-POC-Corrections OMA-PAG-2004-0626-PoC-XDM-SCR OMA-PAG-2004-0643-XDM-PoC-MIME-Type
	11.Nov. 2004		OMA-PAG-2004-0579R01-PoC-XDM-Spec-external-list-in-access-policy.doc OMA-PAG-2004-0675R01-PoC-XDM-Spec-external-list-in-group-policy.doc
OMA-PoC_XDM_Specification-V1_0	12.Nov.2004	5.1. 5.2 and Appendix A - SCR	OMA-PAG-2004-0707-PoC-XDM-Remove-5.1and5.2.doc
		5.3.5 Validation constraints	OMA-PAG-2004-0650R02-PoC-XDMS-Spec-Uniqueness-of-the-Conference-URI-value.doc
	13.Nov.2004	5.4.1 Structure and 5.4.3 XML Schema	OMA-PAG-2004-0709-XDM-PoC-UserAccessPolicy.doc
			OMA-PAG-2004-0714-XDM-PoC-Editorial.doc
	15.Nov.2004	5.1.1, 5.1.3, 5.1.5, 5.2.1, 5.2.3, 5.2.6,	OMA-PAG-2004-0713R02-XDM-PoC-ExternalLists-DefaultPolicy
	15.Nov.2004	5.1.3	OMA-PAG-2004-0732-XDM-PoC-Group-XMLSchema.doc
OMA-PoC_XDM_Specification-V1_0	16.Nov.2004	2.1, 2.2, 3.2, 5.1.6, 5.1.8, 5.1.9, 5.1.10	OMA-PAG-2004-0692R02-PoC-XDMS-Spec-Retrieving-PoC-Group-document.doc
	17.Nov.2004	5.1.1, 5.1.6	OMA-PAG-2004-0750-PoC-XDM-Spec-invite-users.doc
		5.2.1, 5.2.6	OMA-PAG-2004-0746R01-PoC-XDM-Spec-allow-invite-values.doc
		5.1.5, 5.1.6	OMA-PAG-2004-0743R02-PoC-XDMS-Adding-Errors.doc
OMA-TS-PoC_XDM-V1_0_0	19 Jan 2005	B.1	OMA-PAG-2004-0774R01-PoC-XDMS-Correcting-the-Examples
		5.2	OMA-PAG-2004-0775R02-PoC-XDMS-Various-Changes-to-User-Access-Policy
		5.2.7, B.2.1	OMA-PAG-2004-0776-PoC-XDMS-Naming-Convention-for-Access-Control-Policy-Document
		5.2.5	OMA-PAG-2004-0777R01-PoC-XDMS-Validation-Constraints-for-User-Access-Policy
		5.1	OMA-PAG-2004-0809R04-PoC-XDMS-Various-Clarifications-to-PoC-Group-Document
		5.1.1, 5.1.3, 5.1.6	OMA-PAG-2005-0021-PoC-XDM-allow-anonymity
		All	CONRR items 2.002, 2.016, 2.019, 2.024, 2.025, 2.029, 2.042, 2.046, 2.058, 2.059, and editorial comments
OMA-TS-PoC_XDM-V1_0	28 Jan 2005	5.1.5, B.1.2	OMA-PAG-2005-0030-XDM_CONRR_2.022--URI_Negotiation
		All	OMA-PAG-2005-0060R01-XDM-Remove-CPCP

Document Identifier	Date	Sections	Description
OMA-TS-PoC_XDM-V1_0	29 Jan 2005	5.1.1, 5.1.5, 5.1.6, 5.2.6	OMA-PAG-2005-0079-XDM-PoC-AdditionalDescription
		5.1.1, 5.1.6	OMA-PAG-2005-0081R01-XDM-PoC-GroupType
		5.1.1, 5.1.3	OMA-PAG-2005-0076R03-PoC_XDMS_XML_Schema
		2	CONRR items 2.033, 2.034
OMA-TS-PoC_XDM-V1_0	31.Jan. 2005	A.1	A.1.1, A.1.2 were included. This closes CONRR items 2.047; OMA-PAG-2005-0071-XDM-Spec-SCR-Tables-Readjustments.doc
		…	Editorial Bug fixes; OMA-PAG-2005-0080R01-PoC-Group-data-semantics.doc
		B.1.1, B.1.2	A root element “group” , <invite-members> element was introduced. The “poc:” namespace is no more used, The <list> element can be present for chat groups; The TEL URI shown in B.1.2 is not according to [RFC 3966] a valid URI. OMA-PAG-2005-0089-XDM-PoC-CorrectedExamples.doc
		5.1.3, 6.6.1	This document proposes to add in the Section 5.1.3 XML Schema, the OMA specific common extensions for authorization rules as specified in the Section 6.6.1 in XDM Specification. It is also proposed to rename the "external-list" element in "list" element to "external" element, in order to differentiate the "external-list" element in XDMS common-policy. In addition, the subsequence corrections and clarifications of the texts and references are suggested. OMA-PAG-2005-0087R01-PoCXDMS-CR-Adding_auth_rules_common_extensions.doc
OMA-TS-PoC_XDM-V1_0	2.Feb.2005		Change in Section 5.1.6, to be applied after OMA-PAG-2005-0080R01; OMA-PAG-2005-0103-PoC-XDM-consistency-with-POC-CP.doc
OMA-TS-PoC_XDM-V1_0	5.Mar.2005	A.1	Editing mistake corrected.
OMA-TS-PoC_XDM-V1_0	17 Mar 2005		Status changed to Candidate by TP: OMA ref# OMA-TP-2005-0059-PoC-V1_0-for-candidate-approval
OMA-TS-PoC_XDM-V1_0	28 Apr 2005	All	Updated according to CRs agreed during PoC#20 and PoC Conference call on 25th April : 0343, 0399R02, 0420