



PoC XDM Specification

Approved Version 1.0.2 – 05 Sep 2007

Open Mobile Alliance
OMA-TS-PoC_XDM-V1_0_2-20070905-A

Use of this document is subject to all of the terms and conditions of the Use Agreement located at <http://www.openmobilealliance.org/UseAgreement.html>.

Unless this document is clearly designated as an approved specification, this document is a work in process, is not an approved Open Mobile Alliance™ specification, and is subject to revision or removal without notice.

You may use this document or any part of the document for internal or educational purposes only, provided you do not modify, edit or take out of context the information in this document in any manner. Information contained in this document may be used, at your sole risk, for any purposes. You may not use this document in any other manner without the prior written permission of the Open Mobile Alliance. The Open Mobile Alliance authorizes you to copy this document, provided that you retain all copyright and other proprietary notices contained in the original materials on any copies of the materials and that you comply strictly with these terms. This copyright permission does not constitute an endorsement of the products or services. The Open Mobile Alliance assumes no responsibility for errors or omissions in this document.

Each Open Mobile Alliance member has agreed to use reasonable endeavors to inform the Open Mobile Alliance in a timely manner of Essential IPR as it becomes aware that the Essential IPR is related to the prepared or published specification. However, the members do not have an obligation to conduct IPR searches. The declared Essential IPR is publicly available to members and non-members of the Open Mobile Alliance and may be found on the "OMA IPR Declarations" list at <http://www.openmobilealliance.org/ipr.html>. The Open Mobile Alliance has not conducted an independent IPR review of this document and the information contained herein, and makes no representations or warranties regarding third party IPR, including without limitation patents, copyrights or trade secret rights. This document may contain inventions for which you must obtain licenses from third parties before making, using or selling the inventions. Defined terms above are set forth in the schedule to the Open Mobile Alliance Application Form.

NO REPRESENTATIONS OR WARRANTIES (WHETHER EXPRESS OR IMPLIED) ARE MADE BY THE OPEN MOBILE ALLIANCE OR ANY OPEN MOBILE ALLIANCE MEMBER OR ITS AFFILIATES REGARDING ANY OF THE IPR'S REPRESENTED ON THE "OMA IPR DECLARATIONS" LIST, INCLUDING, BUT NOT LIMITED TO THE ACCURACY, COMPLETENESS, VALIDITY OR RELEVANCE OF THE INFORMATION OR WHETHER OR NOT SUCH RIGHTS ARE ESSENTIAL OR NON-ESSENTIAL.

THE OPEN MOBILE ALLIANCE IS NOT LIABLE FOR AND HEREBY DISCLAIMS ANY DIRECT, INDIRECT, PUNITIVE, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES ARISING OUT OF OR IN CONNECTION WITH THE USE OF DOCUMENTS AND THE INFORMATION CONTAINED IN THE DOCUMENTS.

© 2007 Open Mobile Alliance Ltd. All Rights Reserved.

Used with the permission of the Open Mobile Alliance Ltd. under the terms set forth above.

Contents

1. SCOPE	5
2. REFERENCES	6
2.1 NORMATIVE REFERENCES	6
2.2 INFORMATIVE REFERENCES	6
3. TERMINOLOGY AND CONVENTIONS	8
3.1 CONVENTIONS	8
3.2 DEFINITIONS	8
3.3 ABBREVIATIONS	9
4. INTRODUCTION	10
5. POC XDM APPLICATION USAGES	11
5.1 PoC GROUP	11
5.1.1 Structure.....	11
5.1.2 Application Unique ID.....	12
5.1.3 XML Schema.....	12
5.1.4 Default Namespace	12
5.1.5 MIME Type	12
5.1.6 Validation constraints	12
5.1.7 Data Semantics	13
5.1.8 Naming conventions	15
5.1.9 Global Documents	15
5.1.10 Resource interdependencies.....	15
5.1.11 Authorization policies.....	15
5.2 POC USER ACCESS POLICY	16
5.2.1 Structure.....	16
5.2.2 Application Unique ID.....	16
5.2.3 XML Schema.....	16
5.2.4 Default Namespace	16
5.2.5 MIME Type	16
5.2.6 Validation constraints	16
5.2.7 Data Semantics	17
5.2.8 Naming conventions	17
5.2.9 Global Documents	17
5.2.10 Resource interdependencies.....	17
5.2.11 Authorization policies.....	17
6. POC EXTENSIONS TO SHARED XDM APPLICATION USAGES	18
6.1 GROUP USAGE LIST	18
6.1.1 Structure.....	18
6.1.2 XML Schema.....	18
APPENDIX A. STATIC CONFORMANCE REQUIREMENTS (NORMATIVE)	19
A.1 PoC XDM APPLICATION USAGES OF XDM SERVER	19
A.2 PoC APPLICATION USAGES OF XDM CLIENT	20
APPENDIX B. EXAMPLES (INFORMATIVE)	21
B.1 MANIPULATING POC GROUP DOCUMENTS	21
B.1.1 Obtaining a PoC Group Document	21
B.1.2 PoC Conference URI negotiation	22
B.2 MANIPULATING POC USER ACCESS POLICY	24
B.2.1 Obtaining PoC User Access Policy rules.....	24
APPENDIX C. CHANGE HISTORY (INFORMATIVE)	26
C.1 APPROVED VERSION HISTORY	26

Figures

Figure B.1 - XDM Client obtains a particular PoC Group document21

Figure B.2 - PoC XDMS negotiates a Conference URI22

Figure B.3 - XDM Client obtains PoC User Access Policy rules.....24

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/](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](http://www.ietf.org/rfc/rfc2119.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](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](http://www.ietf.org/rfc/rfc3966.txt)
- [RFC4234] "Augmented BNF for Syntax Specifications: ABNF". D. Crocker, Ed., P. Overell. October 2005,
[URL:http://www.ietf.org/rfc/rfc4234.txt](http://www.ietf.org/rfc/rfc4234.txt)
- [RFC4745] "Common Policy: A Document Format for Expressing Privacy Preferences", H. Schulzrinne, J. Morris, H. Tschofenig, J. Cuellar, J. Polk, J. Rosenberg, February 2007,
[URL:http://www.ietf.org/rfc/rfc4745.txt](http://www.ietf.org/rfc/rfc4745.txt)
- [RFC4825] IETF RFC 4825: "The Extensible Markup Language (XML) Configuration Access Protocol (XCAP)", J. Rosenberg, May 2007
[URL:http://www.ietf.org/rfc/rfc4825.txt](http://www.ietf.org/rfc/rfc4825.txt)
- [RFC4826] IETF RFC 4826: "Extensible Markup Language (XML) Formats for Representing Resource Lists", J. Rosenberg, May 2007
[URL:http://www.ietf.org/rfc/rfc4826.txt](http://www.ietf.org/rfc/rfc4826.txt)
- [SHAREDXDM] "OMA Shared XDM Specification", Version 1.0, Open Mobile Alliance™, OMA-TS-XDM_Shared-V1_0,
[URL:http://www.openmobilealliance.org/](http://www.openmobilealliance.org/)
- [XDMSPEC] "XML Document Management (XDM) Specification", Version 1.0, Open Mobile Alliance™, OMA-TS-XDM_CORE-V1_0,
[URL:http://www.openmobilealliance.org/](http://www.openmobilealliance.org/)
- [XSD_LISTSERV] "PoC – List Service", Version 1.0, Open Mobile Alliance™, OMA-SUP-XSD_poc_listService-V1_0,
[URL:http://www.openmobilealliance.org/](http://www.openmobilealliance.org/)
- [XSD_POCRULES] "PoC – PoC Rules", Version 1.0, Open Mobile Alliance™, OMA-SUP-XSD_poc_pocRules-V1_0,
[URL:http://www.openmobilealliance.org/](http://www.openmobilealliance.org/)
- [XSD_POCUSAGE] "PoC – PoC Usage", Version 1.0.2, Open Mobile Alliance™, OMA-SUP-XSD_poc_pocusage-V1_0_2,
[URL:http://www.openmobilealliance.org/](http://www.openmobilealliance.org/)

2.2 Informative References

- [OMA-PoC-AD] "Push to talk over Cellular (PoC) - Architecture", Version 1.0.2, Open Mobile Alliance™, OMA-AD-PoC-V1_0_2,
[URL:http://www.openmobilealliance.org/](http://www.openmobilealliance.org/)
- [OMA-PoC-CP] "OMA PoC Control Plane", Version 1.0.2, Open Mobile Alliance™, OMA-TS-PoC_ControlPlane-V1_0_2,
[URL:http://www.openmobilealliance.org/](http://www.openmobilealliance.org/)

[XDMAD] "XML Document Management Architecture", Version 1.0. Open Mobile Alliance™,
OMA-AD-XDM-V1_0,
[URL:http://www.openmobilealliance.org/](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

1-many-1 PoC Session	A PoC Group Session for a Pre-arranged PoC Group in which one Participant is a Distinguished Participant and each other Participant is an Ordinary Participant. (Source: [PoC-AD])
Application Unique ID (AUID)	A unique identifier that differentiates XCAP resources accessed by one application from XCAP resources accessed by another application. (Source: [RFC4825])
Chat PoC Group	A Chat PoC Group is a persistent Group in which a PoC User individually joins to have a PoC Session with other joined PoC Users, i.e., the establishment of a PoC Session to a Chat PoC Group does not result in other members of the Chat PoC Group being invited. (Source: [PoC-CP])
Chat PoC Group Session	A Chat PoC Group Session is a PoC Session established to a Chat PoC Group. (Source: [PoC-CP])
Controlling PoC Function	The Controlling PoC Function is implemented in a PoC Server and provides centralized PoC Session handling, which includes RTP Media distribution, Talk Burst Control, policy enforcement for participation in Group Sessions, and the Participant information. (Source: [PoC-CP])
Distinguished Participant	The Distinguished Participant is a Participant in a 1-many-1 PoC Session that sends RTP Media to all Ordinary Participants, and that receives RTP Media from any Ordinary Participant. (Source: [PoC-AD])
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: [RFC4825])
Instant Personal Alert	A feature in which a PoC User sends a SIP based instant message to a PoC User requesting a 1-1 PoC Session
Ordinary Participant	An Ordinary Participant is a Participant in a 1-many-1 PoC Session that is only able to send media to the Distinguished Participant, and that likewise is only able to receive media from the Distinguished Participant. (Source: [PoC-AD])
Participant	A Participant is a PoC User in a PoC Session. (Source: [PoC-CP])
PoC Address	A PoC Address identifies a PoC User. The PoC Address can be used by one PoC User to request communication with other PoC Users. (Source: [PoC-CP])
PoC Group	A PoC Group is a predefined set of PoC Users together with its attributes. A PoC Group is identified by a SIP URI. (Source: [PoC-CP])
PoC Group Session	A PoC Group Session is a Pre-arranged PoC Group, Ad-hoc PoC Group or Chat PoC Group Session. (Source: [PoC-CP])
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 PoC Session establishment (in the case of Pre-arranged PoC Group), or allowed to join the PoC Session (in the case of Restricted Chat PoC Group). (Source: [PoC-CP])
PoC Server	The PoC Server implements the 3GPP/3GPP2 IMS application level network functionality for the PoC service. A PoC Server may perform the role of the Controlling PoC Function or Participating PoC Function, or both at the same time. (Source: [PoC-CP])
Pre-arranged PoC Group	A Pre-arranged PoC Group is a persistent PoC Session Identity that has an associated set of PoC members. The establishment of a PoC Session to a Pre-arranged PoC Group results in all members being invited. (Source: [PoC-CP])

User	A User is any entity that uses the described features through the User Equipment.
XCAP Application Usage	Detailed information on the interaction of an XCAP Client with an XCAP server. (Source: [RFC4825])
XCAP Client	An HTTP client that understands how to follow the naming and validation constraints defined in this specification. (Source: [RFC4825])
XCAP Root	A context that includes all of the documents across all application usages and users that are managed by a server. (Source: [RFC4825])
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: [RFC4825])
XCAP Server	An HTTP server that understands how to follow the naming and validation constraints defined in this specification. (Source: [RFC4825])
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: [RFC4825])

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 Access 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 PoC Group Members;
- e) MAY include an <invite-members> element indicating whether the PoC 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 PoC 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 PoC Group Member, as defined in [RFC4826]; 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 [RFC4745]. 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 [RFC4745];
- b) the <external-list> element as defined in [XDMSPEC] Section 6.6.2;
- c) the <other-identity> element as defined in [XDMSPEC] Section 6.6.2;
- d) the <is-list-member> element as defined in Section 5.1.3.

Other types of <conditions> elements described in [RFC4745] 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 described in [XSD_LISTSERV].

NOTE: The XML schema is generally applicable to XDMC and XDMS, as well as documents in "users" and "global" tree. For specific validation constraints to either XDMC or XDMS, or both of them, see sub-clause "Validation Constraints" of this specification.

5.1.4 Default Namespace

The default namespace used in expanding URIs SHALL be "urn:oma::xml:poc:list-service" defined in Section 5.1.3.

5.1.5 MIME Type

The MIME type for the PoC Group document SHALL be "application/vnd.oma.poc.groups+xml".

5.1.6 Validation constraints

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

A PoC Group document stored in the "users" tree of PoC XDMS SHALL contain no more than one <list-service> element.

NOTE 1: The "index" document in the "global" tree as specified in subclause 5.1.8 "*Global documents*") can contain multiple <list-service> elements.

The value of the "uri" attribute proposed by the XDM Client 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 [RFC4825]. The error condition SHALL be described by the <uniqueness-failure> error element. The PoC XDMS SHALL include at least one <alt-value> element in the <uniqueness-failure> error element.

NOTE 2: The syntax of the <alt-value> element is according to the syntax, which is stored in the PoC XDMS, and provisioned to the XDM Client but may also be another syntax according to a local XDMS policy and not yet provisioned to the PoC Client.

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

NOTE 3: The rendering of any "phrase" attribute to a human user is a user interface issue, and is not standardized.

NOTE 4: 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 XDM Client repeats the XCAP request it SHOULD use a "uri" attribute chosen from one of the values received in the <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".

NOTE 5: The "phrase" attribute value can be modified to include the highest <max-participant-count> value acceptable for the PoC XDMS.

The value of an <entry> element SHALL contain a syntactically valid PoC Address.

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".

The <entry-ref> element is not defined in the PoC Group schema as specified in the sub-clause "*XML Schema*". As such, if the XDMC uses or adds an <entry-ref> element (as specified in [RFC4826]) under the <list> element, to refer to any storage of a PoC Contact Address in the Shared XDMS, the PoC XDMS complying with this specification SHALL return an error code "409 Conflict" response which includes the XCAP error element <schema-validation-error>.

NOTE 6: The use of <entry-ref> element is avoided in the current version to alleviate possible complexities in resource interdependency.

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".

If the document proposed by the XDM Client contains under the <conditions> element more than one child element of <identity>, <external-list>, <other-identity> or <is-list-member>, the PoC XDMS SHALL return an HTTP "409 Conflict" including the error element <constraint-failure>. If included, the "phrase" attribute SHOULD be set to "Complex rules are not allowed".

5.1.7 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 PoC 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 PoC 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] "*Pre-arranged PoC Group Session setup request*".

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 SHALL be 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> element is defined in [OMA-PoC-CP] section 7.2.1.6. The possible values are:

- "false" 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.
- "true" instructs the PoC Server to accept the access to the PoC Session.

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] "*PoC Session initiation policy*". 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 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.

NOTE: PoC Server can handle the PoC Session as a 1-many-1 PoC Session only in the case that there is one Distinguished Participant.

5.1.8 Naming conventions

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

5.1.9 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.

5.1.10 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.

5.1.11 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 [RFC4745] and extended in sub-clause 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 [RFC4745]:

- <conditions>
- <actions>

NOTE 1: This specification does not define any value for the <transformations> element defined as a child of the <rules> element in [RFC4745]. 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 [RFC4745], except the sub-elements that are prohibited in [XDMSPEC];
- b) the <external-list> element, as defined in [XDMSPEC], sub-clause 6.6 "*Common Extensions*";
- c) the <other-identity> element, as defined in [XDMSPEC], sub-clause 6.6 "*Common Extensions*";

NOTE 2: This specification does not define any value for those elements defined as a part of the <conditions> element in [RFC4745] (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.

- d) the <anonymous-request> element, as defined in [XDMSPEC], sub-clause 6.6 "*Common Extensions*".

The <actions> element supports the <allow-invite> element, as defined in sub-clause 5.2.3 "*XML Schema*" and 5.2.6 "*Data Semantics*".

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 described in [RFC4745] and extended in [XDMSPEC] "*Subscriptions to changes in the XML documents*", with the extensions described in [XSD_POCRULES].

5.2.4 Default Namespace

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

5.2.5 MIME Type

The MIME type for PoC User Access Policy documents SHALL be "application/auth-policy+xml" defined in [RFC4745].

5.2.6 Validation constraints

The PoC User Access Policy document SHALL conform to the XML Schema described in [RFC4745] and extended in subclause 5.2.3 "*XML Schema*", with the additional validation constraints described in this sub-clause.

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

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".

5.2.7 Data Semantics

The PoC User Access Policy document SHALL conform to the semantics for the "conditions" and "actions" described in [RFC4745] and extended in [XDMSPEC] sub-clause 6.6 "*Common Extensions*", together with the clarifications required for the PoC service as given in this subclause.

When evaluating a "rule" against an identity, the value of the "entity" attribute of the <one> element, if present, is compared against that identity to see if the "rule" is applicable.

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 and Instant Personal Alert for a particular PoC User. This element has one of the following three values, whose use is described in [OMA-PoC-CP] "*PoC Session invitation request*" and "*Instant Personal Alert procedure at terminating PoC Server*". 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 PoC User to decide the acceptance), or to process the SIP MESSAGE message in case of the Instant Personal Alert according to [OMA-PoC-CP] "*Instant Personal Alert procedure at terminating PoC Server*". This SHALL be the default value taken in the absence of the element. This value is assigned the numeric value of 0.
- "accept" instructing the PoC Server to accept the invitation according to the User's Answer Mode setting, or to process the SIP MESSAGE message in case of the Instant Personal Alert according to [OMA-PoC-CP] "*Instant Personal Alert procedure at terminating PoC Server*". This value is assigned the numeric value of 1.
- "reject" instructing the PoC Server to reject the invitation or Instant Personal Alert. This value is assigned the numeric value of 2.

NOTE: If there are multiple matching rules containing conflicting values for the <allow-invite> action, then according to the procedures described in [XDMSPEC] sub-clause 6.6.2.3 "*Combining Permissions*", the result is the largest integer value.

5.2.8 Naming conventions

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

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 SHALL be defined according to [XDMSPEC].

6. PoC Extensions to Shared XDM Application Usages

6.1 Group Usage List

6.1.1 Structure

A PoC-specific URI usage shall be used in a Group Usage List stored in the Shared XDMS.

The PoC URI usage, <pocusage>, is defined for the <uriusage> element in [SHAREDXDM]. The <pocusage> element has two values:

- chat
- prearranged.

If present in any <uriusage> element, the <pocusage> element indicates the type of the group URI.

6.1.2 XML Schema

The <pocusage> element SHALL conform to the XML schema described in [XSD_POCUSAGE].

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 [RFC4234].

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

ScrReference = ScrItem / ScrGroup

ScrItem = SpecScrName “-“ GroupType “-“ DeviceType “-“ NumericId / SpecScrName “-“ DeviceType
“-“ NumericId

ScrGroup = SpecScrName “:” FeatureType / SpecScrName “-“ GroupType “-“ DeviceType “-“
FeatureType

SpecScrName = 1*Character;

GroupType = 1*Character;

DeviceType = “C” / “S”; C – client, S – server

NumericId = Number Number Number

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

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

Character = %x41-5A ; A-Z

Number = %x30-39 ; 0-9

A.1 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 and validation constraints of PoC Group	5.1.3 5.1.6	M	
PoC_XDM-AU-S-004	MIME type of PoC Group and User Access policy documents	5.1.5. 5.2.5	M	
PoC_XDM-AU-S-005	Data semantics of PoC Group document	5.1.7	M	
PoC_XDM-AU-S-006	Naming conventions for PoC Group and User Access policy documents	5.1.8 5.2.8	M	
PoC_XDM-AU-S-007	Authorization policies for manipulating PoC Group and User Access policy documents	5.1.11 5.2.11	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 and validation constraints of PoC User Access Policy document	5.2.3 5.2.6	M	
PoC_XDM-AU-S-010	Data semantics of PoC User Access Policy document	5.2.7	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	5.1.7	M	
PoC_XDM-CAU-C-002	XDM Client handling of HTTP "409 Conflict" response from the PoC XDMS	5.1.6	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.

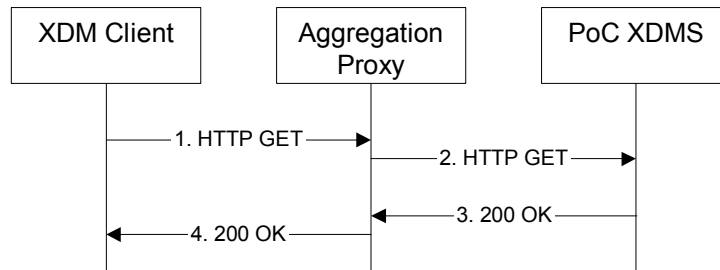


Figure B.1 - XDM Client obtains a particular PoC Group document

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 /org.openmobilealliance.poc-groups/users/sip:ronald.underwood@example.com/gossips.xml HTTP/1.1
Host: xcap.example.com
...
  
```

- 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/vnd.oma.poc.groups+xml

<?xml version="1.0" encoding="UTF-8"?>
<group xmlns="urn:oma:xml:poc:list-service"
  xmlns:rl="urn:ietf:params:xml:ns:resource-lists"
  xmlns:cr="urn:ietf:params:xml:ns:common-policy"
  >

  <list-service uri="sip:myconference@example.com">
    <display-name xml:lang="en-us">Friends</display-name>
    <list>
      <entry uri="tel:+43012345678"/>
      <entry uri="sip:hermione.blossom@example.com"/>
    </list>

    <max-participant-count>10</max-participant-count>
    <cr:ruleset>
      <cr:rule id="a7c">
        <cr:conditions>
          <is-list-member/>
        </cr:conditions>
        <cr:actions>
          <join-handling>true</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.

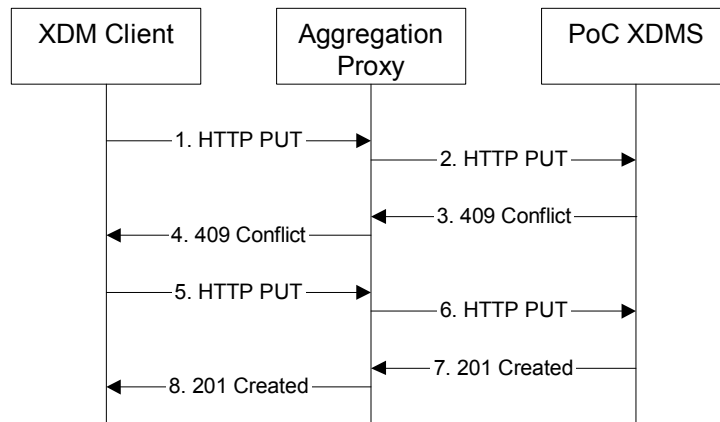


Figure B.2 - PoC XDMS negotiates a Conference URI

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 org.openmobilealliance.poc-groups/users/sip:ronald.underwood@example.com/MyGroup.xml HTTP/1.1
Host: xcap.example.com
...
Content-Type: application/vnd.oma.poc.groups+xml
Content-Length: (...)

<?xml version="1.0" encoding="UTF-8"?>
<group xmlns="urn:oma:xml:poc:list-service"

  xmlns:rl="urn:ietf:params:xml:ns:resource-lists"
  xmlns:cr="urn:ietf:params:xml:ns:common-policy"
  xmlns:ocr="urn:oma:xml:xdm:common-policy">
  <list-service uri="sip:wrongname@example.com">
  <list>
    <entry uri="tel:+43012345678"/>
    <entry uri="sip:hermione.blossom@example.com"/>
  </list>
  <invite-members>true</invite-members>
  <cr:ruleset>
    <cr:rule id="78t">
      <cr:conditions>
        <ocr:other-identity/>
      </cr:conditions>
      <cr:actions>
        <join-handling>true</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 /org.openmobilealliance.poc-groups/users/sip:ronald.underwood@example.com/MyGroup.xml HTTP/1.1
Host: xcap.example.com

...
Content-Type: application/vnd.oma.poc.groups+xml
Content-Length: (...)

<?xml version="1.0" encoding="UTF-8"?>
<group xmlns="urn:oma:xml:poc:list-service"

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

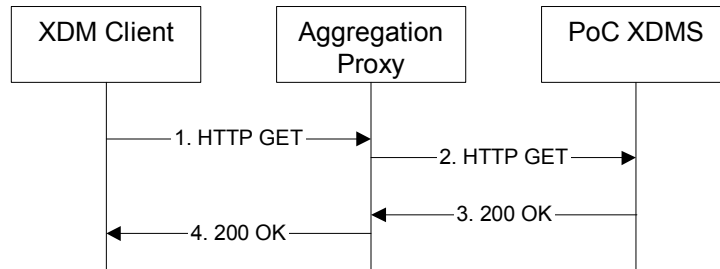


Figure B.3 - XDM Client obtains PoC User Access Policy rules

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

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: "etul5"
...
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:xml:poc:poc-rules"
  xmlns:ocp="urn:oma:xml:xdm:common-policy"
  >
  <rule id="f3g44r1">
    <conditions>
      <identity>
        <one id="tel:5678;phone-context="+43012349999"/>
        <one id="sip:percy.underwood@example.com"/>
      </identity>
    </conditions>
    <actions>
      <poc:allow-invite>accept</poc:allow-invite>
    </actions>
  </rule>
  <rule id="ythk764">
    <conditions>
      <ocp:anonymous-request/>
    </conditions>
    <actions>
      <poc:allow-invite>reject</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
OMA-TS-PoC-XDM-V1_0-20060609-A	09 Jun 2006	Status changed to Approved by TP: OMA-TP-2006-0201R02-ERP_PoCv1_0_for_Final_Approval
OMA-TS-PoC_XDM-V1_0_1-20061128-A	28 Nov 2006	Updated with agreed CRs: OMA-POC-POCv1-2006-0137 OMA-POC-POCv1-2006-0162 OMA-POC-POCv1-2006-0169
OMA-TS-PoC_XDM-V1_0_2-20070905-A	05 Sep 2007	Inclusion of CRs: OMA-POC-POCv1-2005-0017 (correcting erroneous omission of agreed CR from earlier revision) OMA-POC-POCv1-2006-0169R02 OMA-POC-POCv1-2006-0177R01 OMA-POC-POCv1-2007-0006 OMA-POC-POCv1-2007-0019R02 OMA-POC-POCv1-2007-0023 OMA-POC-POCv1-2007-0046R01 OMA-POC-POCv1-2007-0054R01 OMA-POC-POCv1-2007-0064R01 OMA-POC-POCv1-2007-0067 (undoing OMA-POC-POCv1-2005-0017 changes) OMA-POC-POCv1-2007-0068 Editorial changes to References section. Editorial clean-up of styles and formatting.