



Shared Group XDM Specification

Candidate Version 1.0 – 24 Jul 2007

Open Mobile Alliance
OMA-TS-XDM_Shared_Group-V1_0-20070724-C

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	7
3. TERMINOLOGY AND CONVENTIONS	8
3.1 CONVENTIONS	8
3.2 DEFINITIONS	8
3.3 ABBREVIATIONS	9
4. INTRODUCTION	10
5. SHARED GROUP XDM APPLICATION USAGES	11
5.1 GROUP	11
5.1.1 Structure.....	11
5.1.2 Application Unique ID.....	13
5.1.3 XML Schema.....	13
5.1.4 Default Namespace	13
5.1.5 MIME Type	13
5.1.6 Validation Constraints	13
5.1.7 Data Semantics	15
5.1.8 Naming conventions	19
5.1.9 Global Documents	19
5.1.10 Resource interdependencies.....	19
5.1.11 Authorization policies.....	19
5.1.12 Search Capabilities.....	20
6. SUBSCRIBING TO CHANGES IN THE XML DOCUMENTS	21
7. EXTENDED GROUP ADVERTISEMENTS	22
7.1 EXTENDED GROUP ADVERTISEMENT	22
7.1.1 Structure and Data Semantics	22
7.1.2 XML Schema.....	22
7.1.3 MIME Type	22
7.1.4 Media Element Description	23
7.2 SHARED GROUP XDMS GENERATED EXTENDED GROUP ADVERTISEMENT	23
7.2.1 Procedures at Shared Group XDMS	23
7.2.2 Structure and Data Constraints	24
8. BACKWARD COMPATIBILITY TOWARDS THE POC GROUP APPLICATION USAGE	25
8.1 PROCEDURES AT THE SHARED GROUP XDMS	25
8.2 PROCEDURES AT THE AGGREGATION PROXY	25
APPENDIX A. CHANGE HISTORY (INFORMATIVE)	26
A.1 APPROVED VERSION HISTORY	26
A.2 DRAFT/CANDIDATE VERSION 1.0 HISTORY	26
APPENDIX B. STATIC CONFORMANCE REQUIREMENTS (NORMATIVE)	29
B.1 SHARED GROUP APPLICATION USAGES OF XDMS	30
B.2 SHARED GROUP APPLICATION USAGES OF XDMS	31
B.3 AGGREGATION PROXY	32
APPENDIX C. EXAMPLES (INFORMATIVE)	33
C.1 MANIPULATING GROUP DOCUMENTS	33
C.1.1 Obtaining a Group Document.....	33
C.1.2 Conference URI Negotiation	34
C.2 EXAMPLE XML SCHEMAS	36
C.2.1 Extended Group Advertisement.....	36

C.3 EXAMPLE GROUP DOCUMENT.....37
C.3.1 Open public chat group with the age control and a session activity policy.....37
C.3.2 Prearranged group supporting all service and media types.....37
**APPENDIX D. GUIDELINES FOR THE SPECIFICATION OF ENABLER SPECIFIC <ACTIONS> CHILD
ELEMENTS (INFORMATIVE)39**

Figures

Figure C.1- XDMC obtains a particular Group document.....33
Figure C.2- Shared Group XDMS negotiates a Conference URI.....34

1. Scope

This specification describes the data format and Application Usage for the Group document, which is a common group definition that can be used by all OMA enablers (e.g. PoC and IM). It also defines the data format for the Extended Group Advertisement and procedures for the Shared Group XDMS to send Extended Group Advertisements.

2. References

2.1 Normative References

- [3GPP2-X.S0013-004] 3GPP2 X.S0013-004 “All-IP Core Network Multimedia Domain: IP Multimedia Call Control Protocol Based on SIP and SDP, Stage 3”, URL: http://3gpp2.org/Public_html/specs/index.cfm
- [3GPP-TS_24.229] 3GPP TS 24.229 “IP Multimedia Call Control Protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP)”; Stage 3”, URL: http://www.3gpp.org/ftp/Specs/archive/24_series/24.229/
- [Dict] “Dictionary for OMA Specifications”, Version 2.4, Open Mobile Alliance™, OMA-ORG-Dictionary-V2_4, URL: <http://www.openmobilealliance.org/>
- [PoC_CP] “Push to talk Over Cellular (PoC) - Control Plane Specification”, Draft Version 2.0, Open Mobile Alliance™, OMA-TS-PoC-ControlPlane-V2_0, URL: <http://www.openmobilealliance.org/>
- [PoC_CP-V1_0] “OMA PoC Control Plane”, Version 1.0, Open Mobile Alliance™, OMA-TS-PoC-ControlPlane-V1_0, URL: <http://www.openmobilealliance.org/>
- [PoC_XDM-V1_0] “OMA PoC XDM Specification”, Version 1.0, Open Mobile Alliance™, OMA-TS-PoC-XDM-V1_0, URL: <http://www.openmobilealliance.org/>
- [RFC2119] IETF RFC 2119 “Key words for use in RFCs to Indicate Requirement Levels”, S. Bradner, March 1997, URL: <http://www.ietf.org/rfc/rfc2119.txt>
- [RFC2234] IETF RFC 2234 “Augmented BNF for Syntax Specifications: ABNF”. D. Crocker, Ed., P. Overell. November 1997, URL: <http://www.ietf.org/rfc/rfc2234.txt>
- [RFC3261] IETF RFC 3261 “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>
- [RFC3428] IETF RFC 3428 “Session Initiation Protocol (SIP) Extension for Instant Messaging”, B. Campbell, Ed., J. Rosenberg, H. Schulzrinne, C. Huitema, D. Gurle, December 2002, URL: <http://www.ietf.org/rfc/rfc3428.txt>
- [RFC3966] IETF RFC 3966 “The tel URI for Telephone Numbers”, H. Schulzrinne, December 2004, URL: <http://www.ietf.org/rfc/rfc3966.txt>
- [RFC4745] IETF RFC 4745 “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>
- [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>
- [RFC4826] IETF RFC 4826 “The Extensible Markup Language (XML) Formats for Representing Resource Lists”, J. Rosenberg, May 2007, URL: <http://www.ietf.org/rfc/rfc4826.txt>
- [SCRRULES] “SCR Rules and Procedures”, Version 1.0, Open Mobile Alliance™, OMA-ORG-SCR_Rules_and_Procedures-V1_0, 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_ERELD-V1_0] “Enabler Release Document for XDM”, Version 1.0, Open Mobile Alliance™, OMA-ERELD-XDM-V1_0, URL: <http://www.openmobilealliance.org/>
- [XDM_ERELD-V2_0] “Enabler Release Document for XDM”, Version 2.0, Open Mobile Alliance™, OMA-ERELD-XDM-V2_0, URL: <http://www.openmobilealliance.org/>
- [XDM_List] “Shared List XDM Specification”, Version 2.0, Open Mobile Alliance™, OMA-TS-XDM_Shared_List-V2_0, URL: <http://www.openmobilealliance.org/>
- [XSD_ext] “XML Schema Definition: XDM Extensions”, Version 1.0, Open Mobile Alliance™, OMA-SUP-XSD_xdm_extensions-V1_0, URL: <http://www.openmobilealliance.org/>
- [XSD_listServ] “XML Schema Definition: PoC – List Service”, Version 1.0, Open Mobile Alliance™, OMA-SUP-XSD_poc_listService-V1_0, URL: <http://www.openmobilealliance.org/>

[XSD_poc_group_ad] “XML Schema Definition: PoC – Group Advertisement”, Version 1.0, Open Mobile Alliance™, OMA-SUP-XSD_poc_group_advertisement-V1_0, URL: <http://www.openmobilealliance.org/>

2.2 Informative References

[IM_TS] “SIP/SIMPLE Instant Messaging Specification Document”, Draft Version 1.0, Open Mobile Alliance™, OMA-TS-IM_SIMPLE-V1_0, URL: <http://www.openmobilealliance.org/>

[PoC_DocMgmt] “OMA PoC Document Management”, Draft Version 2.0. Open Mobile Alliance™, OMA-TS-PoC_Document_Management-V2_0, URL: <http://www.openmobilealliance.org/>

[XDM_AD] “XML Document Management Architecture”, Version 2.0. Open Mobile Alliance™, OMA-AD-XDM-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 Server	A functional entity that implements the service logic for SIP Sessions (e.g. PoC Server or IM Server).
Application Unique ID	A unique identifier within the namespace of Application Unique IDs created by this specification that differentiates XCAP Resources accessed by one application from XCAP Resources accessed by another application. (Source: [RFC4825])
Application Usage	Detailed information on the interaction of an application with an XCAP Server. (Source: [RFC4825])
Document Selector	A sequence of path segments, with each segment being separated by a “/”, that identify the XML document within an XCAP Root that is being selected. (Source: [RFC4825])
Document URI	The HTTP URI containing the XCAP Root and Document Selector, resulting in the selection of a specific document. As a result, performing a GET against the Document URI would retrieve the document. (Source: [RFC4825])
Global Document	A document placed under the Global Tree that applies to all users of that Application Usage.
Global Tree	A URI that represents the parent for all Global Documents for a particular Application Usage within a particular XCAP Root. (Source: [RFC4825])
Group	A Group is a predefined set of Users together with its policies and attributes. A Group is identified by a SIP URI.
Group Identity	The SIP URI of the Pre-arranged Group or Join-in Group.
Group Member	A User on the predefined list of Users associated with a Pre-arranged Group or Join-in Group.
Group Session	A Group Session is a Pre-arranged Group, Ad-hoc Group or Join-in Group Session.
Group Session Controlling Function	The Group Session Controlling Function is implemented in an Application Server and provides centralized Group Session handling, which includes Group policy enforcement.
Join-in Group	A persistent Group in which a User individually joins to have a Group Session with other joined Users, i.e., the establishment of a Group Session to a Join-in Group does not result in other Users being invited. A Join-in Group optionally has an associated set of Group Members.
Node URI	The HTTP URI containing the XCAP Root, Document Selector, Node Selector Separator and Node Selector, resulting in the selection of a specific XML node. (Source: [RFC4825])
Participant	A Participant is a User in an “active” Session.
Pre-arranged Group	A persistent Group that has an associated set of Group Members. The establishment of a Group Session to a Pre-arranged Group results in all Group Members being invited.
Principal	An entity that has an identity, that is capable of providing consent and other data, and to which authenticated actions are done on its behalf. Examples of principals include an individual user, a group of individuals, a corporation, service enablers/applications, system entities and other legal entities (Source: [Dict])
Quality of Experience Profile	Defines how the end-user experience should be for the Group Session. The service infrastructure will differentiate the end-user experience provided to the Group based on QoE Profile defined for the Group.
Search Request	A request to perform a search operation towards XCAP Resources.
URI List	A list of URIs.
User	A User is any entity that uses the described features through the User Equipment.

User Address	A User Address identifies a User. The User Address can be used by one User to request communication with other Users. (Source: [PoC_CP])
Users Tree	A URI that represents the parent for all user documents for a particular Application Usage within a particular XCAP Root.
XCAP Resource	An HTTP resource representing an XML document, an element within an XML document, or an attribute of an element within an XML document that follows the naming and validation constraints of XCAP. (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 Server	An HTTP server that understands how to follow the naming and validation constraints defined in [RFC4825].
XCAP User Identifier	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

ABNF	Augmented Backus-Naur Form
AUID	Application Unique ID
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IM	Instant Messaging
IP	Internet Protocol
MIME	Multipurpose Internet Mail Extensions
OMA	Open Mobile Alliance
PoC	Push-to-talk over Cellular
SCR	Static Conformance Requirements
SIP	Session Initiation Protocol
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
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 Application Usage for the Group document. It reuses the PoC Group document structure described in [PoC_XDM-V1_0] to make the syntax backward compatible with that of the PoC Group document.

The Shared Group XDMS (see [XDM_AD]) is the logical repository for Group documents. The common protocol specified in [XDM_Core] is used for access and manipulation of such Groups by authorized Principals.

This specification defines how to handle backwards compatibility with the PoC V1.0 enabler when the Shared Group XDMS is introduced in the network.

This specification also defines the Extended Group Advertisement, which is an extension of the PoC Group Advertisement [PoC_CP-V1_0] and is therefore backward compatible with it.

This specification also defines procedures for the Shared Group XDMS to send the Extended Group Advertisement.

The enabler specific extensions to this specification are defined in the corresponding enabler specification (e.g., PoC extensions in PoC Document Management specification [PoC_DocMgmt]).

5. Shared Group XDM Application Usages

5.1 Group

5.1.1 Structure

The Group document SHALL conform to the structure of the “group” document described in this section. The schema definition is provided in section 5.1.3 “XML Schema”.

The <list-service> element:

- a) SHALL include a “uri” attribute representing the Group Identity;
- b) MAY include any other attributes from any other namespaces for the purpose 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 a <subject> element containing a topic or description of the Group;
- i) MAY include one or more <age-restrictions> elements indicating the allowed age or age-range(s) of a Participant;
- j) MAY include a <session-active-policy> element describing the rules for determining whether a Group Session is allowed to become active or remain active;
- k) MAY include an <automatic-group-advertisement> element indicating automatic sending of an Extended Group Advertisement message to Group Members;
- l) MAY include a <supported-services> element containing supported services of the Group.
- m) MAY include a <qoe> element indicating the Quality of Experience Profile assigned to the Group. The element SHALL include one child element defining the Quality of Experience Profile and one “must-understand” attribute from the “urn:oma:xml:xdm:extensions” namespace;
- n) MAY include a <searchable> element indicating that the Group Identity can be retrieved using a Search Request and
- o) MAY include any other elements from any other namespaces for the purposes of extensibility. Such an element MAY include the “must-understand” attribute from the “urn:oma:xml:xdm:-extensions” namespace.

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

- a) an <entry> element, which SHALL contain the “uri” attribute set to a valid User Address, i.e. a SIP URI (as defined in [RFC3261]) or a TEL URI (as defined in [RFC3966]), and MAY contain the <display-name> child element, containing a human readable name of each Group Member, as defined in [RFC4826]; or
- b) an <external> element pointing to a URI List in the Shared List XDMS as defined in [XDM_List].

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:

- a) MAY include the <identity> element as described in [RFC4745], except the sub-elements that are prohibited in [XDM_Core] “*Common Extensions*”;
- b) MAY include the <external-list> element as defined in [XDM_Core] “*Common Extensions*”;
- c) MAY include the <other-identity> element as defined in [XDM_Core] “*Common Extensions*”;
- d) MAY include the <is-list-member> element;
- e) MAY include the <media-list> element as defined in [XDM_Spec] “*Common Extensions*”; and
- f) MAY include other elements from other namespaces for the purposes of extensibility.

Other types of <conditions> child elements described in [RFC4745] are not supported by this specification.

The <actions> child element of any <rule> element:

- a) MAY include the <allow-conference-state> element;
- b) MAY include the <allow-invite-users-dynamically> element;
- c) MAY include the <join-handling> element;
- d) MAY include the <allow-initiate-conference> element;
- e) MAY include the <allow-anonymity> element;
- f) MAY include the <is-key-participant> element;
- g) MAY include the <allow-subconf> element;
- h) MAY include the <allow-private-message> element;
- i) MAY include the <allow-media-handling> element;
- j) MAY include the <remove-media-handling> element;
- k) MAY include the <allow-expelling> element;
- l) MAY include the <block-group-advertisement-sending> element; and
- m) MAY include other elements from other namespaces for the purposes of extensibility..

NOTE: Enablers can define enabler-specific <actions> child elements (Appendix D).

The <age-restrictions> element SHALL include zero or more <age> child elements and the “must-understand” attribute from the “urn:oma+xml:xdm:extensions” namespace. Each <age> child element MAY contain the combination of the “from” and “until” attributes to specify an age or age interval.

The <session-active-policy> element:

- a) SHALL include a “must-understand” attribute from the “urn:oma+xml:xdm:extensions” namespace;
- b) MAY include a <max-duration> element representing the maximum allowed time duration of a Group Session;
- c) MAY include a <required-participants> element representing who must participate for a Group Session to become active or remain active;
- d) MAY include a <min-participant-count> element representing the minimum number of participants needed for a Group Session to become active or remain active;
- e) MAY include a <schedule> element representing the allowed range of time for a Group Session to become active or remain active;

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

The <required-participants> element SHALL contain a sequence of zero or more child elements, each of which is:

- a) an <entry> element, which SHALL contain the "uri" attribute set to a valid User Address, i.e. a SIP URI (as defined in [RFC3261]) or a TEL URI (as defined in [RFC3966]), and MAY contain the <display-name> child element containing the user's human readable name, as defined in [RFC4826]; or
- b) an <external> element pointing to a URI List in the Shared List XDMS as defined in [XDM_List].

The <schedule> element SHALL include zero or more <time-range> child elements. Each <time-range> child element MAY contain the combination of the <start-time> and <end-time> elements to specify a time range.

The <supported-services> element:

- a) SHALL include a sequence of one or more <service> child elements as defined in [XDM_Core] "Common Extensions" or;
- b) SHALL include an <all-services-except> child element as defined in [XDM_Core] "Common Extensions".

The <all-services-except> element SHALL include zero or more <service> child elements as defined in [XDM_Core] "Common Extensions".

The <service> element MAY include a <group-media> child element.

The <group-media> element MAY include the same child elements as the <media-list> element as defined in [XDM_Core] "Common Extensions".

5.1.2 Application Unique ID

The AUID SHALL be "org.openmobilealliance.groups".

5.1.3 XML Schema

The "group" XML document SHALL be composed according to the XML schema described in [XSD_listServ] and extended with extensions from the XML Schema defined in [XSD_ext] and with extensions from XML Schemas described by other enablers.

5.1.4 Default Namespace

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

5.1.5 MIME Type

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

5.1.6 Validation Constraints

The Group document SHALL conform to the XML Schema described in section 5.1.3 "XML Schema", with the clarifications given below.

A Group document stored in the Users Tree of the Shared Group XDMS SHALL contain no more than one <list-service> element.

NOTE: The "index" document in the Global Tree as specified in section 5.1.9 "Global documents" can contain multiple <list-service> elements.

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

- SHALL be in the format of a SIP URI.

- SHALL be unique amongst *all* Group documents spanning *all* Users Trees stored across all Shared Group XDMS in a service provider's domain. Furthermore, the URI SHALL NOT correspond to an existing resource within the domain of the URI.
- SHALL conform to the syntax specified by the Conference URI Template (see [XDM_Core]), which is stored in the Shared Group XDMS and provisioned to the XDMC.

If this "uri" attribute value does not conform to any local policy or the constraints described above, the Shared Group 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 Shared Group XDMS SHALL include at least one <alt-value> element in the <uniqueness-failure> error element.

NOTE 1: It is out of scope of this specification how the Shared Group XDMS verifies the uniqueness of the Group URI in the "uri" attribute proposed by the XDMC.

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

If the "uri" attribute 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 XDMS uses the "phrase" text as defined in this specification, it will ignore the received HTTP Accept-language header value.

If the XDMC 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 Shared Group 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 User Address.

If the value proposed for the <entry> element does not conform to the syntax of a supported URI, the Shared Group 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 Shared Group 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 schema as specified in section 5.1.3 "XML Schema". As such, if the XDMC adds an <entry-ref> element (as specified in [RFC4826]) under the <list> element, the Shared Group XDMS SHALL return an HTTP "409 Conflict" response which includes the XCAP error element <schema-validation-error>.

NOTE 5: The use of <entry-ref> element is avoided in the current version to alleviate possible complexities in resource interdependency.

If the AUID value of the Document URI or Node URI proposed in an <external> or <external-list> element is other than "resource-lists", the Shared Group XDMS SHALL return 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 URI or Node URI proposed in an <external> or <external-list> element does not match the XUI of the Group document URI, the Shared Group XDMS SHALL return 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 XDMC contains under the <conditions> element more than one child element of <identity>, <external-list>, <anonymous-request>, <other-identity> or <is-list-member>, the Shared Group 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”.

If the XDMC includes the <automatic-group-advertisement> element set to “true” and the Shared Group XDMS does not support automatic sending of Extended Group Advertisements, the Shared Group XDMS SHALL return an HTTP “409 Conflict” response including the <constraint-failure> error element. If included, the “phrase” attribute SHOULD be set to “Automatic group advertisement not supported”.

If the document proposed by the XDMC contains the <searchable> element and search feature is not supported by the Group Application Usage, the Shared Group XDMS SHALL return an HTTP “409 Conflict” response including the error element <constraint-failure>. If included, the “phrase” attribute SHOULD be set to “Search not supported”.

5.1.7 Data Semantics

5.1.7.1 List-service Elements

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

The value of the “must-understand” attribute SHALL be “true”. Any element that includes this attribute must be understood by the Application Server performing the Group Session Controlling Function. If not understood the Application Server performing the Group Session Controlling Function is instructed to reject a request to use the group with an error response according to the procedures of the individual enabler. All elements that contain a mandatory constraint of the usage of a group SHALL contain this attribute.

The <list> element SHALL contain the Group Members.

The <invite-members> element SHALL indicate whether the Group Session Controlling Function will invite the Group Members to the Group Session. The possible values are:

- “false” represents the Join-in Group. The Application Server performing the Group Session Controlling Function will not invite the Group Members to the Group Session. This SHALL be the default value taken in the absence of the element.
- “true” represents the Pre-arranged Group. The Application Server performing the Group Session Controlling Function will invite the Group Members identified by the <list> element.

The <max-participant-count> element SHALL indicate the maximum number of Participants in the Group Session.

The <subject> element SHALL indicate the title or description for the Group.

The <age-restrictions> element SHALL indicate the allowed age or age span of a Participant in a Group Session. Each <age> child element SHALL indicate each of such allowed age or age span by the combination of “from” and “until” attributes. Those attributes represent the boundaries of an age interval. This interval denotes an acceptance of participation (i.e. a user whose age is within the interval is allowed to participate in the Group Session). The boundaries are inclusive (i.e. from 14 until 18 means that people of 14 and 18 are allowed to participate in the Group Session). A missing attribute means “any age”; e.g., <age from=”18”/> means that the age span is from 18 to any. A specific age can be specified by having the same value for both attributes; e.g., <age from=”20” until=”20”>. Multiple <age> child elements under the <age-restrictions> element denote multiple allowed ages or age spans, and SHALL be interpreted as logically ORed.

The <session-active-policy> element SHALL describe the rules for determining whether a Group Session is allowed to become active or remain active. Multiple child elements under the <session-active-policy> element SHALL be interpreted as logically ANDED. The <session-active-policy> has following child elements

- <max-duration> element SHALL indicate the maximum allowed time duration in seconds of a Group Session.
- <required-participants> element SHALL contain a list of the Group Members who must participate for a Group Session to become active or remain active:

- <min-participant-count> element SHALL indicate the minimum number of Participants for a Group Session to become active or remain active.
- <schedule> element SHALL define the allowed range of time for a Group Session to become active or remain active. Each <time-range> child element SHALL indicate each of such allowed range of time by the combination of <start-time> and <end-time> elements. These elements represent the boundaries of the time range during which the Group Session can become active or remain active. A missing element means “any time”; e.g., <time-range> <start-time>“2006-12-01T09:00:00Z” <start-time/> <time-range/> means that the Group Session is allowed to become active at 2006-12-01 09:00:00 UTC and remain active indefinitely. Multiple <time-range> child elements under the <schedule> element denote multiple allowed ranges of time, and SHALL be interpreted as logically ORed.

The <supported-services> element SHALL indicate the supported services of the Group. The data semantics for the child elements to this element SHALL be the same as defined for the child elements to the <service-list> element as defined by [XDM_Core]. A Group document without the <supported-services> element SHALL indicate that the group can not be used by any service “*Common Extensions*” with the following additions:

- a) A <service> element with a <group-media> child element SHALL indicate the supported media types for the service. The data semantic for child elements of the <group-media> element SHALL the same as defined for the child elements to the <media-list> element defined by [XDM_Core] “*Common Extensions*”;
- b) A <service> element without a <group-media> child element SHALL indicate that all media types are supported for the service.

The <automatic-group-advertisement> element indicates automatic sending of an Extended Group Advertisement to Group Members. The possible values are:

- “false” instructs the Shared Group XDMS not to send an Extended Group Advertisement to Group Members. This SHALL be the default value taken in the absence of the element.
- “true” instructs the Shared Group XDMS to send an Extended Group Advertisement to Group Members as described in section 7.

The <qoe> element SHALL indicate the Quality of Experience Profile associated to the Group. The following lists four possible values for the child elements, ordered from the lowest to the highest Quality of Experience Profile:

- <basic> represents the lowest Quality of Experience Profile, intended for Group Sessions with no special quality of experience expectation from its members;
- <premium> represents a Quality of Experience Profile intended for Group Sessions with a quality of experience expectation from its members higher than the basic one;
- <professional> represents a Quality of Experience intended for Group Sessions involved in special applications for professional use that have special and high quality of experience expectation;
- <government> represents the highest Quality of Experience Profile intended for Group Sessions with Group Members with special rights subject to applicable regulations who require priority access to the service and the highest available quality of experience.

NOTE 1: Other values of <qoe> child elements can be described in the future.

NOTE 2: How different applications prioritise different Quality of Experience Group Sessions data traffic is out of the scope of this specification (see [PoC_CP] for an example of how OMA PoC performs this functionality).

The <searchable> element SHALL indicate whether the Group Identity can be included in a search result. The possible values are:

“false” instructs the Shared Group XDMS that the Group Identity SHALL NOT be included in the search result even if the Group matches to the search criteria. This SHALL be the default value taken in the absence of the element.

“true” instructs the Shared Group XDMS that the Group Identity MAY be included in the search result when the Group matches to the search criteria.

It is RECOMMENDED that only those Join-in Groups where all Users are allowed to join-in be marked as searchable. The operator’s local policy MAY restrict the usage of the <searchable> element.

5.1.7.2 Condition Elements

The <is-list-member> “condition” element SHALL be used to match an identity against the contents of the <list> element.

5.1.7.3 Action Elements

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 possible values are:

“false” instructs the Application Server performing the Group Session Controlling Function 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 Application Server performing the Group Session Controlling Function to accept the subscription to the “conference” event package.

The <allow-invite-users-dynamically> “action” SHALL be used to indicate that the identity matching this rule SHALL be allowed to invite additional participants. The possible values are:

“false” instructs the Application Server performing the Group Session Controlling Function to prevent the user from inviting additional participants. This SHALL be the default value taken in the absence of the element.

“true” instructs the Application Server performing the Group Session Controlling Function to allow the user to invite additional participants.

The <join-handling> element SHALL define the action that the Application Server performing the Group Session Controlling Function is to take when processing a particular request to join a Group Session.

The possible values are:

“false” instructs the Application Server performing the Group Session Controlling Function to block the access to the Group Session. This SHALL be the default value taken in the absence of the element.

“true” instructs the Application Server performing the Group Session Controlling Function to accept the access to the Group 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 Group Session. The possible values are:

“false” instructs the Application Server performing the Group Session Controlling Function to prevent the user from initiating the Pre-arranged Group Session. This SHALL be the default value taken in the absence of the element.

“true” instructs the Application Server performing the Group Session Controlling Function to allow the user to initiate the Pre-arranged Group Session.

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 Application Server performing the Group Session Controlling Function to block an anonymous access to the Group Session. This SHALL be the default value taken in the absence of the element.

“true” instructs the Application Server performing the Group Session Controlling Function to accept an anonymous access to the Group Session.

The <is-key-participant> “action” SHALL be used to indicate that the identity matching this rule is assigned the role of “Distinguished Participant”. The semantics of the “Distinguished Participant” is described in enabler specific specifications, e.g., in case of PoC in [PoC_CP]. The possible values are:

- “false” instructs the Application Server performing the Group Session Controlling Function to treat the User as a normal participant. This SHALL be the default value taken in the absence of the element.
- “true” instructs the Application Server performing the Group Session Controlling Function to treat the User as a Distinguished Participant.

The <allow-subconf> “action” SHALL be used to indicate that the identity matching this rule is allowed to create sub-conferences. The possible values are:

- “false” instructs the Application Server performing the Group Session Controlling Function to block the sub-conferences originated by the User. This SHALL be the default value taken in the absence of the element.
- “true” instructs the Application Server performing the Group Session Controlling Function to accept the subs conferences originated by the User.

The <allow-private-message> “action” SHALL be used to indicate that the identity matching this rule is allowed to use private messages in the conference. The possible values are:

- “false” instructs the Application Server performing the Group Session Controlling Function to deny usage of private messages from the User. This SHALL be the default value taken in the absence of the element.
- “true” instructs the Application Server performing the Group Session Controlling Function to allow usage of private messages to the User.

The <allow-media-handling> “action” SHALL be used to indicate whether the identity matching this rule is allowed to initiate Group Session with media matching this rule and add new media matching this rule in the Group Session.

- “false” instructs the Application Server performing the Group Session Controlling Function to block the request to initiate Group Session or add new media in the Group Session. This SHALL be the default value taken in the absence of the element.
- “true” instructs the Application Server performing the Group Session Controlling Function to accept the request to initiate Group Session or add new media in the Group Session session.

The <remove-media-handling> “action” SHALL be used to indicate that the identity matching this rule is allowed to remove an existing media stream from the active Group Session. The value is of an enumerated integer type, and the lowest value SHALL be the default value taken in the absence of the element. The possible values are:

- “none” instructs the Application Server performing the Group Session Controlling Function NOT to allow the User any media stream removal. This value is assigned the numeric value of 0.
- “own” instructs the Application Server performing the Group Session Controlling Function to allow the User the removal of media stream which were previously initiated or added to the Session by the same User. This value is assigned the numeric value of 100.
- “any” instructs the Application Server performing the Group Session Controlling Function to allow the User any media stream removal. This value is assigned the numeric value of 200.
- “other” for future extensibility.

NOTE 1: This action will apply for all Participants of the active Group Session, not only to the User removing media.

The <allow-expelling> “action” SHALL be used to indicate that the identity matching this rule is allowed to expel other Users from the Group Session. The possible values are:

- “false” instructs the Application Server performing the Group Session Controlling Function to block the request to expel other Users. This SHALL be the default value taken in the absence of the element.

“true” instructs the Application Server performing the Group Session Controlling Function to accept the request to expel other Users.

The <block-group-advertisement-sending> “action” SHALL be used to indicate that Group Advertisements sent by the identity matching this rule are to be blocked by the Application Server. The possible values are:

“false” instructs the Application Server not to block the Group Advertisement sent by the User. This SHALL be the default value taken in the absence of the element.

“true” instructs the Application Server to block the Group Advertisement sent by the User.

NOTE 2: Additional enabler-specific semantics of the above “action” elements may be described in enabler-specific specifications.

5.1.8 Naming conventions

This specification defines no naming conventions.

5.1.9 Global Documents

The Shared Group 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 5.1.6 “*Validation Constraints*”) will ensure that no two <list-service> elements in the Global Document have the same value of that attribute. This allows an Application Server to retrieve a specific <list-service> element in the “index” document using the Group Identity.

As an example, an XCAP GET request targeted at the resource identified by the URI

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

returns the <list-service> element of the Group document.

NOTE: Canonicalization is defined in [RFC4826].

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 XDMS must actually store this “index” document. The XDMS SHALL always be prepared to process requests against this global “index” document and the contents of this document at any point in time SHALL always accurately represent the state of all “group” documents in the Users Tree.

5.1.11 Authorization policies

The authorization policies for XDM operations and subscribing to changes operations of documents in the Users Tree SHALL be defined according to [XDM_Core] “*Authorization*”.

The authorization policies for documents in the Global Tree are as follows:

- 1) Global Documents SHALL be “read-only”
- 2) Access to Global Documents SHALL be restricted based on local policy.

NOTE: It is expected that only an Application Server will access documents in the Global Tree. There is no reason why users should need to access the Global Tree.

The authorization policy for a search operation towards Group documents in the Users Tree is as follows:

- 1) Principals SHALL have permission to perform search.

5.1.12 Search Capabilities

The Group Application Usage MAY support search. If the search feature is supported, it SHALL be possible to search according to the following rules:

The Group Application Usage SHALL support a collection “org.openmobilealliance.groups/users/”, a collection “org.openmobilealliance.groups/users/[XUI]/” and a collection “org.openmobilealliance.groups/users/[XUI]/<document name>” as defined in [XDMSpec].

The basic XQuery expression [XDMSpec] supported by the Shared Group XDMS for this Application Usage SHALL be as follows:

```
xquery version "1.0";
declare default element namespace "urn:oma:xml:poc:list-service";
declare namespace ext="urn:oma:xml:xdm:group";

for $g in collection({Data_Source})/group/list-service/searchable
where [{Condition}]
return <group>{$g/@uri} {$g/display-name} {$g/ext:subject}</group>
```

where:

{Data_Source} represents the collection that SHALL be searched. In case that the value:

- “org.openmobilealliance.groups/users/” is used, the search SHALL be executed over all Group documents stored in the Shared Group XDMS.
- “org.openmobilealliance.groups/users/[XUI]/” is used, the search SHALL be executed over all Group documents stored in the home directory of the User identified by XUI.
- “org.openmobilealliance.groups/users/[XUI]/<document name>” is used, the search SHALL be executed over the Group document identified by <document name>.

{Condition} represents a logical expression defined by an XDMC. An XDMC SHALL be able to use any combination of <subject> element, <display-name> element and “uri” attribute in a {Condition}. All other XML elements/attributes SHALL be forbidden.

An example of a condition is as follows:

```
$g/ext:subject="Football"
```

All Search Requests that do not comply with the basic XQuery expression as defined in this section SHALL be responded to with an HTTP “409 Conflict” error response as defined by [XDM_Core].

6. Subscribing to changes in the XML documents

The Shared Group XDMS SHALL support subscriptions to changes in the XML documents as specified in [XDM_Core] “*Subscriptions to changes in the XML documents*”, sections “*Initial subscription*” and “*Generating a SIP NOTIFY request*”.

7. Extended Group Advertisements

7.1 Extended Group Advertisement

The Extended Group Advertisement includes information relevant for the User to know about the advertised Group. It extends the PoC Group Advertisement document defined in [PoC_CP-V1_0] and is therefore backward compatible with the PoC Group Advertisement.

The following subsections define the generic data structure of the Extended Group Advertisement while procedures for generating the Extended Group Advertisement are defined in the Technical Specifications of the Enabler in question.

7.1.1 Structure and Data Semantics

The Extended Group Advertisement document SHALL conform to the structure of the “group-advertisement” document described below in this sub-clause. The schema definition is provided in section 7.1.2 “XML Schema”.

The <group-advertisement> element

- a) SHALL include one or more <group> elements;
- b) MAY include free text in the <note> element indicating some information to be rendered to the User.

The <group> element

- a) MAY include the “type” attribute indicating the type of the Group;
- b) MAY include any other attributes from any other namespaces for the purpose of extensibility;
- c) SHALL include the <uri> element with the value set to the Group Identity of the Group;
- d) MAY include the <display-name> element containing the human readable name of the Group;
- e) MAY include the <supported-services> element from the Group document describing supported services of the Group if present in the Group document;
- f) MAY include any other elements from any other namespaces for the purposes of extensibility.

The “type” attribute SHALL include one of the following values:

- "dialed-in" to indicate the Group is a Join-in Group
- "dialed-out" to indicate the Group is a Pre-arranged Group

"other" is left for future expandability when new types are created that cannot be framed as either dialed-in or dialed-out.

7.1.2 XML Schema

The Extended Group Advertisement document SHALL conform to the XML schema described in [XSD_poc_group_ad] and with extensions described in [XSD_ext].

7.1.3 MIME Type

The MIME type for the Extended Group Advertisement document SHALL be “vnd.poc.group-advertisement+xml”.

7.1.4 Media Element Description

An Extended Group Advertisement SHALL be treated as a media with a media element as defined by [XDM_Core] “Common Extensions”.

NOTE: The <group-advertisement> media element corresponds to a SIP MESSAGE with a body of the MIME-type “vnd.poc.group-advertisement+xml”.

7.2 Shared Group XDMS generated Extended Group Advertisement

The Shared Group XDMS MAY support automatic sending of Extended Group Advertisement. If the Shared Group XDMS supports automatic sending of Extended Group Advertisement, it SHALL send the Extended Group Advertisement upon an indication of the boolean <automatic-group-advertisement> element in the Group document according to procedures defined in this section to:

- 1) all Group Members, when the Group document is created
- 2) all Group Members when any of following elements in the Group document is modified:
 - a. <invite-members>
 - b. <supported-services>
- 3) each new Group Members when added into the <list> element of the Group document. If the <external> element is used within <list> element, the Shared Group XDMS SHALL get information of changes to the URI List by utilizing subscriptions to changes in the XML documents as specified in [XDM_Core] “Subscriptions to changes in the XML documents”.

7.2.1 Procedures at Shared Group XDMS

If an Extended Group Advertisement is to be sent, the Shared Group XDMS:

- 1) SHALL generate, for each enabler identified by an “enabler” attribute of the <supported-services> element’s <service> child element of the Group document, a separate SIP MESSAGE request according to rules and procedures of [RFC3428]; or
- 2) SHALL if the <supported-services> element includes an <all-services-except> element send Extended Group Advertisements as defined by local policy for enablers not being in the list of <service> child elements by generating a separate SIP MESSAGE request according to rules and procedures of [RFC3428] for each type of enabler;
- 3) SHALL include, for each generated SIP MESSAGE request, one media feature tag in an Accept-Contact header to indicate the enabler. For example:
 - a. the media feature tag value '+g.poc.groupad' if the <supported-services> element of the Group document indicates support for the PoC service [PoC_CP].
 - b. the media feature tag value '+g.oma-sip-im' if the <supported-services> element of the Group document indicates support for the IM service[IM_TS].
- 4) SHALL include Group specific content in the MIME body of vnd.poc.group-advertisement+xml as defined in section 7.2.2 “Structure and Data Constraints”.
- 5) SHALL set the Request-URI to the User Address of the Group Member being added to the <list> element, or to the Group Identity if the request is being sent to all Group Members;
- 6) SHALL include the XUI of the Primary Principal of the Group in the Authenticated Originator's Address

NOTE: Anonymity cannot be applied when the Shared Group XDMS sends the Extended Group Advertisement automatically on behalf of the User. If anonymity is required then the <automatic-group-advertisement> element in the Group document should not be set to true.

- 7) SHALL include the User-Agent header to indicate the release version of the XDM Enabler; and,
- 8) SHALL send the SIP MESSAGE according to the procedures of the SIP/IP Core.

When the SIP/IP Core corresponds with 3GPP/3GPP2 IMS, the XDMS SHALL use 3GPP/3GPP2 IMS mechanisms according to rules and procedures of [3GPP-TS_24.229] / [3GPP2-X.S0013-004] with the clarifications given in this section.

7.2.2 Structure and Data Constraints

The Extended Group Advertisement MIME body sent by Shared Group XDMS SHALL conform to the structure of the schema definition in section 7.1.1 “*Structure and Data Semantics*” with following additional data constraints.

The Extended Group Advertisement MIME body sent by the Shared Group XDMS:

- 1) SHALL include only one <group> element with all possible child elements that can be filled with information from the Group document as defined in section 7.1.1 “*Structure and Data Semantics*”;
- 2) SHALL include the <note> element according to the <subject> element of the Group document if present in the Group document;
- 3) SHALL include the <display-name> element according to the <display-name> element of the Group document, if present in the Group document;
- 4) SHALL include the “type” attribute according to the <invite-members> element of the Group document if present in the Group document, and whose value SHALL be:
 - a. "dialed-in" when <invite-members> element has value “false”;
 - b. "dialed-out" when <invite-members> element has value “true”.

8. Backward compatibility towards the PoC Group Application Usage

8.1 Procedures at the Shared Group XDMS

If the Shared Group XDMS is required by local configuration to support PoC V1.0 clients, then the Shared Group XDMS SHALL support the PoC Group Application Usage defined in [PoC_XDM-V1_0] “*PoC Group*” with the clarifications given in this section.

The Shared Group XDMS SHALL maintain, for each PoC Group document, a corresponding Group document whose content at any point in time SHALL be synchronized, with the following extension:

- a) For every PoC Group document created for “org.openmobilealliance.poc-groups” Application Usage, a corresponding Group document SHALL be extended with the <supported-services> element with single <service> child element indicating support of the PoC enabler. Such <service> element indicating support of the PoC enabler SHALL include child element <group-media> with single child element <poc-speech>.

The Shared Group XDMS SHALL maintain, for each Group document, a corresponding PoC Group document whose contents at any point in time SHALL be synchronized with the following exceptions:

- a) A Group Application Usage document that contains an element with a “must-understand” attribute SHALL NOT be regarded as a PoC Group Application Usage document;
- b) A Group Application Usage document that contains a <supported-services> element not indicating support for PoC as defined by [PoC_CP-V1_0] SHALL NOT be regarded as a PoC Group Application Usage document;
- c) A Group Application Usage document without a <supported-services> element SHALL NOT be regarded as a PoC Group Application Usage document.

NOTE: This does not imply that the Shared Group XDMS must actually store the PoC Group documents, but must always be prepared to process requests against PoC Group documents.

The Shared Group XDMS SHALL when it receives an XCAP request for an XML Documents Directory document as defined in [XDM_Core] “*XML Documents Directory*” include all Group documents for the Group Application Usage and all PoC Group documents for the PoC Group Application Usage.

When responding to a request for the XCAP Server Capabilities as defined in [XDM_Core] “*XCAP Server Capabilities*” the Shared Group XDMS SHALL include the XCAP Server capabilities for the Group Application Usage and the XCAP Server capabilities for the PoC Group Application Usage.

8.2 Procedures at the Aggregation Proxy

The Aggregation Proxy SHALL forward XCAP requests for the PoC Group AUID to either the PoC XDMS or the Shared Group XDMS based on local configuration.

NOTE: An Aggregation Proxy forwards XCAP requests for the PoC Group AUID to the Shared Groups XDMS when the network supports PoC V2.0 or the PoC XDMS when the network supports PoC V1.0.

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 1.0 History

Document Identifier	Date	Sections	Description
Draft Versions OMA-TS-Shared_Group_XDM-V2_0	09 Jan 2006	First draft	OMA-PAG-2005-0612R03
	13 Mar 2006	5.1.1 5.1.1, 5.1.3, 5.1.7	OMA-PAG-2005-0680 OMA-PAG-2005-0004R01
	12 Apr 2006	B.1.1 B.1.2 5.1.3 5.1.7	OMA-PAG-2006-0135R02 OMA-PAG-2006-0136R02 OMA-PAG-2006-0190R02
	26 Jun 2006	2.1, 7 B.1.2 all, 2.1, 5, B Filename	Incorporated CRs: OMA-PAG-2006-0144R03 OMA-PAG-2006-0238R01 OMA-PAG-2006-0258 OMA-PAG-2006-0314R01 OMA-PAG-2006-0315R01 OMA-PAG-2006-0321 Document history moved as Appendix A
	31 Aug 2006	7, 5.1.7, 5.1.11, 5.1.10 5.1.1 2, 5.1.1, C.1.1, C.1.2 5.1.6 7, 7.1.1 5.1.1, 5.1.6, Appendix D	Incorporated CRs: OMA-PAG-2006-0433 OMA-PAG-2006-0434 OMA-PAG-2006-0438 OMA-PAG-2006-0439 OMA-PAG-2006-0427R01 OMA-PAG-2006-0465 OMA-PAG-2006-0474 OMA-PAG-2006-0476 OMA-PAG-2006-0477 OMA-PAG-2006-0475R02 OMA-PAG-2006-0483
	05 Sep 2006	7	Editorial correction
	10 Nov 2006	2.1, 5.1.1, 5.1.6, 5.1.7, 5.1.3, 7.1.6, B.1	Incorporated CRs: OMA-PAG-2006-0437 OMA-PAG-2006-0443R02 OMA-PAG-2006-0510 OMA-PAG-2006-0511R02 OMA-PAG-2006-0583 OMA-PAG-2006-0602 OMA-PAG-2006-0609R02
	24 Nov 2006	B.1, B.2	Incorporated CR: OMA-PAG-2006-0683R01

Document Identifier	Date	Sections	Description
	18 Dec 2006	2.2, 5.1.1, 5.1.7, 7, 7.1.2, 7.1.3, App. C.1,	Incorporated CRs: OMA-PAG-2006-0435R03 OMA-PAG-2006-0675R04 OMA-PAG-2006-0792R01 OMA-PAG-2006-0797 OMA-PAG-2006-0815 OMA-PAG-2006-0816R03 OMA-PAG-2006-0859 Editorial correction of figure numbering in App C.
	05 Feb 2007	Various	Incorporated CRs: OMA-PAG-2007-0047R01
	14 Feb 2006	3.2, 5.1.7	Incorporated CRs: OMA-PAG-2007-0097 OMA-PAG-2007-0108R02
	05 Mar 2007	3.2, 5.1.6	Incorporated CRs: OMA-PAG-2007-0129
	06 Mar 2007	5.1.1, 5.1.7, 5.1.8, 7.1, 7.1.1, 7.1.2, 7.1.3, 7.1.4, 7.1.5	Incorporated CRs: OMA-PAG-2007-0064R02 OMA-PAG-2007-0141
	21 Mar 2007	1, 2.2, 4, 5.1.7	Incorporated CRs: OMA-PAG-2007-0134R01 OMA-PAG-2007-0139R01
	04 Apr 2007	5.1.6, 5.1.7.1, 5.1.7.2, 5.1.7.3, 6, 7.2, 7.2.1, 7.2.2, B.1, B.2	Incorporated CRs: OMA-PAG-2007-0063R03 OMA-PAG-2007-0145R02 OMA-PAG-2007-0175 OMA-PAG-2007-0179 OMA-PAG-2007-0187
	11 Apr 2007	7, C.1.2	Incorporated CR: OMA-PAG-2007-0064R02 (correcting the implementation of the CR) Bullet numbering correction (editorial no CR)
	12 Apr 2007	7.1.1	OMA-PAG-2007-0064R02 (correcting the implementation of the CR)
	23 Apr 2007	5.1.9, App. C, App. D	Incorporated CRs: OMA-PAG-2007-0257R01 OMA-PAG-2007-0273R01
	25 Apr 2007	2.1, 3.2, 4, 5.1.1, 5.1.3, 5.1.6, 5.1.7, 5.1.7.1, 5.1.7.3, 5.1.12, 7.1.1, 7.1.2, 7.2, 7.2.1, 7.2.2, 8 App. B1, B.3 App. C.2.1, App C.3	Incorporated CRs: OMA-PAG-2007-0132R06 OMA-PAG-2007-0287R01 OMA-PAG-2007-0186R01 OMA-PAG-2007-0188R02 OMA-PAG-2007-0197R02 OMA-PAG-2007-0198R02 OMA-PAG-2007-0219R03 OMA-PAG-2007-0223 OMA-PAG-2007-0234 OMA-PAG-2007-0235R01 OMA-PAG-2007-0264 OMA-PAG-2007-0276R01

Document Identifier	Date	Sections	Description
	10 May 2007	5.1.1, 5.1.3, 5.1.7.1, 5.1.7.3, 7.1.4, C.1.1, C.1.2, C.2.1, C.3.2	Incorporated CRs: OMA-PAG-2007-0284R03 OMA-PAG-2007-0308R01
	22 May 2007	7.2, B, B.1, B.2, B.3 5.1.11, 5.1.12, 5.1.7.1	Incorporated CRs: OMA-PAG-2007-0301R02 OMA-PAG-2007-0315R01 OMA-PAG-2007-0320
Draft Versions OMA-TS-Shared_Group_XDM-V1_0	05 Jun 2007	All	Incorporated CRs: OMA-PAG-2007-0324R02 OMA-PAG-2007-0331R03
	14 Jun 2007	2.2, 4, 5.1.1, 5.1.7.1, 5.1.7.3, 7.1.1, 7.1.4, 7.2, 7.2.1, 8.1, B.2, C.1.1, C.1.2, C.2.1, C.3.2,	Incorporated CRs: OMA-PAG-2007-0404 OMA-PAG-2007-0436R01 OMA-PAG-2007-0458R02 OMA-PAG-2007-0459R02 OMA-PAG-2007-0466 OMA-PAG-2007-0475
	30 Jun 2007	7.2.2, 8.1	Incorporated CRs: OMA-PAG-2007-0489R01
Candidate Version OMA-TS-XDM_Shared_Group-V1_0	24 Jul 2007	n/a	Status changed to Candidate by TP (2007-07-11 to 2007-07-24) TP ref # OMA-TP-2007-0284- INP_XDM_V2_0_ERP_for_Candidate_approval

Appendix B. Static Conformance Requirements (Normative)

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

- Shared Group XDM Application Usages

Each SCR table MUST have a title and MUST have only the following columns [SCRRULES]:

- Item: Identifier for a feature. It MUST be of type ScrItem in the dependency grammar described below.
- Function: Short description of the feature.
- Reference: Section(s) of the specification(s) with more details on the feature.
- Requirement: Other features required by this feature, independent of whether those other features are mandatory or optional. The notation in the dependency grammar, as described below, MUST be used for this column when other features are required, else the column MUST be left empty.

The dependency grammar notation to be used in the Requirement column of the SCR and CCR tables using ABNF [RFC2234] is described below [SCRRULES].

```

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

ScrReference =        ScrItem
                      / ScrGroup

ScrItem =             SpecScrName "-" GroupType "-" DeviceType "-" NumericId "-"
                      Status
                      / SpecScrName "-" DeviceType "-" NumericId "-" Status

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

SpecScrName = 1*Character;
GroupType = 1*Character;
DeviceType = "C" / "S"; C - client, S - server
NumericId = Number Number Number
Status = "M" / "O"; M - Mandatory, O - Optional
LogicalOperator = "AND" / "OR"; AND has higher precedence than OR and OR is inclusive
FeatureType = "MCF" / "OCF" / "MSF" / "OSF";
Character = %x41-5A ; A-Z
Number = %x30-39 ; 0-9

```

The following tags are used in the Function column to identify the relationship of the requirements in this enabler release [XDM_ERELD-V2_0] with the requirements of the previous enabler release [XDM_ERELD-V1_0]:

- XDMv1.0 – Requirement that is the same in this enabler release [XDM_ERELD-V2_0], as in the previous enabler release [XDM_ERELD-V1_0].
- XDMv2.0 – Requirement that is new in this enabler release [XDM_ERELD-V2_0].

- XDMv1.0mod – Requirement that exists in the previous enabler release [XDM_ERELD-V1_0], but is modified in this enabler release [XDM_ERELD-V2_0].

B.1 Shared Group Application Usages of XDMS

Item	Function	Reference	Requirement
XDM_Group-XOP-S-001-M	Support Group document structure (XDMv2.0)	5.1.1	XDM_Core -XCAP-S-001-M
XDM_Group-XOP-S-002-M	Support Application Unique ID of Group document (XDMv2.0)	5.1.2	
XDM_Group-XOP-S-003-M	Support XML schema of Group document (XDMv2.0)	5.1.3	
XDM_Group-XOP-S-004-M	Support validation constraints of Group document (XDMv2.0)	5.1.6	
XDM_Group-XOP-S-005-M	Support MIME type of Group document (XDMv2.0)	5.1.5	
XDM_Group-XOP-S-006-M	Support data semantics of Group document (XDMv2.0)	5.1.7	
XDM_Group-XOP-S-007-M	Support naming conventions for Group document (XDMv2.0)	5.1.8	
XDM_Group-XOP-S-008-M	Support authorization policies for manipulating Group document (XDMv2.0)	5.1.11	
XDM_Group-XOP-S-009-O	Search procedures for Group Application Usage	5.1.12	XDM_Core-SRC-S-001-O AND XDM_Core-SRC-S-002-O
XDM_Group-SRC-S-001-O	Support Search capabilities (XDMv2.0)	5.1.12	
XDM_Group-SUB-S-001-M	Subscribing to changes in XML documents (XDMv2.0)	6	XDM_Core -SUB-S-001-O AND XDM_Core -SUB-S-002-O
XDM_Group-GA-S-001-O	Sending Extended Group Advertisement (XDMv2.0)	7.2	XDM_Group-GA-S-002-O AND XDM_Group-GA-S-003-O
XDM_Group-GA-S-002-O	Procedures of creating an Extended Group Advertisement (XDMv2.0)	7.2.1	XDM_Group-GA-S-001-O
XDM_Group-GA-S-003-O	Support structure and data constraints of Extended Group Advertisement (XDMv2.0)	7.2.2	XDM_Core -XCAP-S-001-M AND XDM_Group-GA-S-001-O
XDM_Group-BC-S-001-M	Backward compatibility PoC Group Application Usage.	8.1	

B.2 Shared Group Application Usages of XDMC

Item	Function	Reference	Requirement
XDM_Group-XOP-C-001-M	Support Group document structure (XDMv2.0)	5.1.1	XDM_Core-XOP-C-003-M
XDM_Group-XOP-C-002-M	Support application Unique ID of Group document (XDMv2.0)	5.1.2	
XDM_Group-XOP-C-003-M	Support XML schema of Group document (XDMv2.0)	5.1.3	
XDM_Group-XOP-C-004-M	Support validation constraints of Group document (XDMv2.0)	5.1.6	
XDM_Group-XOP-C-005-M	Support MIME type of Group document (XDMv2.0)	5.1.5	
XDM_Group-XOP-C-006-M	Support data semantics of Group document (XDMv2.0)	5.1.7	
XDM_Group-ERR-C-001-M	XDMC handling of HTTP “409 Conflict” response from the Shared XDMS (XDMv2.0)	5.1.6	
XDM_Group-XOP-C-007-M	Naming conventions for Group document (XDMv2.0)	5.1.8	
XDM_Group-XOP-C-008-M	Support authorization policies for manipulating Group document (XDMv2.0)	5.1.11	
XDM_Group-XOP-C-010-O	Search procedures for Group Application Usage	5.1.12	XDM_Core-SRC-C-001-O AND XDM_Core-SRC-C-002-O
XDM_Group-SRC-C-001-O	Search capabilities (XDMv2.0)	5.1.12	

B.3 Aggregation Proxy

Item	Function	Reference	Requirement
XDM_Group-BC-S-002-M	Backward compatibility Procedures at the Aggregation Proxy.	8.2	

Appendix C. Examples

(Informative)

C.1 Manipulating Group Documents

C.1.1 Obtaining a Group Document

Figure C.1 describes how XDMC obtains a particular Group document.

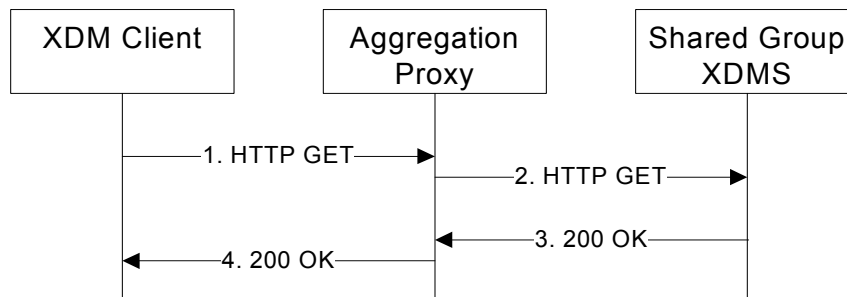


Figure C.1- XDMC obtains a particular Group document

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.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 Shared Group XDMS.

- 3) After the Shared Group XDMS has performed the necessary authorisation checks on the request originator, the Shared Group 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"
  xmlns:ocr="urn:oma:xml:xdm:common-policy"
  xmlns:oxe="urn:oma:xml:xdm:extensions">

  <list-service uri="sip:myconference@example.com">
    <display-name xml:lang="en-us">Friends</display-name>
    <list>
      <entry uri="tel:+1-212-555-1234"/>
      <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>
          <allow-invite-users-dynamically>true</allow-invite-users-dynamically>
          <oxe:allow-subconf>true</oxe:allow-subconf>
        </cr:actions>
      </cr:rule>
    </cr:ruleset>
  </list-service>
</group>
  
```

```

        <oxe:allow-private-message>true</oxe:allow-private-message>
      </cr:actions>
    </cr:rule>
  </cr:ruleset>
  <oxe:subject>My conference</oxe:subject>
  <oxe:supported-services>
    <oxe:service oxe:enabler="poc">
      <oxe:group-media>
        <oxe:poc-speech/>
      </oxe:group-media>
    </oxe:service>
    <oxe:service oxe:enabler="im">
      <oxe:group-media>
        <oxe:all-media-except>
          <oxe:file-transfer/>
          <oxe:audio/>
        </oxe:all-media-except>
      </oxe:group-media>
    </oxe:service>
  </oxe:supported-services>
</list-service>
</group>

```

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

C.1.2 Conference URI Negotiation

Figure C.2 describes how the Shared Group XDMS can negotiate a Conference URI.

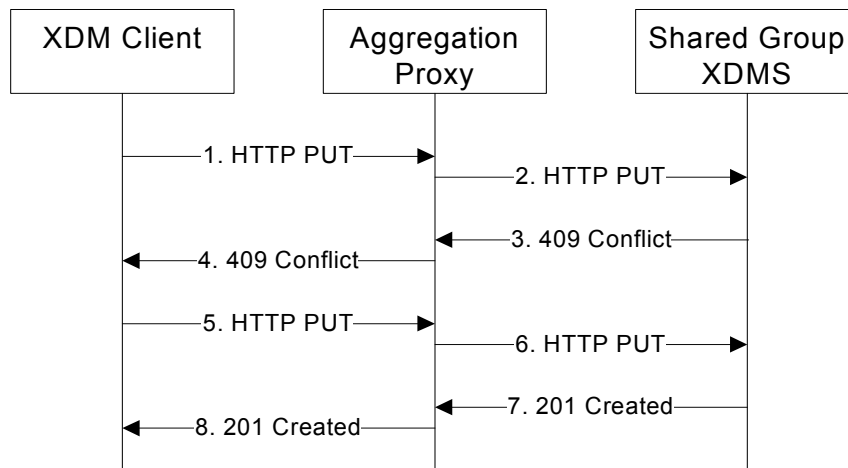


Figure C.2- Shared Group XDMS negotiates a Conference URI

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.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:oxe="urn:oma:xml:xdm:extensions">

```

```

<list-service uri="sip:wrongname@example.com">
  <list>
    <entry uri="tel:+1-212-555-1234"/>
    <entry uri="sip:hermione.blossom@example.com"/>
  </list>
  <invite-members>true</invite-members>

  <cr:ruleset>
    <cr:rule id="a78t">
      <cr:conditions>
        <is-list-member/>
      </cr:conditions>
      <cr:actions>
        <join-handling>true</join-handling>
        <allow-initiate-conference/>
        <oxe:allow-private-message>true</oxe:allow-private-message>
      </cr:actions>
    </cr:rule>
  </cr:ruleset>
  <oxe:subject>My conference</oxe:subject>
</list-service>
</group>

```

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

- 2) Based on the AUID the Aggregation Proxy forwards the request to Shared Group XDMS.
- 3) The Shared Group XDMS detects that the conference URI does not conform to the local policy. The Shared Group 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 XDMC.
- 5) The XDMC repeats the XCAP request (sent in step 1) using the received conference URI value.

```

PUT /org.openmobilealliance.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:oxe="urn:oma:xml:xdm:extensions">

  <list-service uri="sip:correctname@example.com">
    <list>
      <entry uri="tel:+1-212-555-1234"/>
      <entry uri="sip:hermione.blossom@example.com"/>
    </list>
    <invite-members>true</invite-members>

    <cr:ruleset>
      <cr:rule id="a78t">
        <cr:conditions>

```

```

    <is-list-member/>
  </cr:conditions>
  <cr:actions>
    <join-handling>true</join-handling>
    <allow-initiate-conference/>
    <oxe:allow-private-message>true</oxe:allow-private-message>
  </cr:actions>
</cr:rule>
</cr:ruleset>
<oxe:subject>My conference</oxe:subject>
</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 Shared Group XDMS.
- 7) The Shared Group XDMS creates the requested conference URI and sends an HTTP “201 Created” response.

```

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

```

- 9) The Aggregation Proxy routes the response to the XDMC.

C.2 Example XML Schemas

C.2.1 Extended Group Advertisement

```

<?xml version="1.0" encoding="UTF-8"?>
  <group-advertisement
    xmlns="urn:oma:xml:poc:group-advertisement"
    xmlns:oxe="urn:oma:xml:xdm:extensions">
    <note>Ice Hockey Discussion</note>
    <group type="dialed-in">
      <display-name>Ice Hockey Club</display-name>
      <uri>sip:ice-hockey-club1@example.com</uri>
      <uri>sip:ice-hockey-club1@example.com</uri>
      <oxe:supported-services>
        <oxe:service enabler="im">
          <oxe:group-media>
            <oxe:poc-speech/>
          </oxe:group-media>
        </oxe:service>
        <oxe:service enabler="poc">
          <oxe:group-media>
            <oxe:message-session>
              <oxe:full-duplex/>
            </oxe:message-session>
            <oxe:pager-mode-message/>
          </oxe:group-media>
        </oxe:service>
      </oxe:supported-services>
    </group>
  </group-advertisement>

```

C.3 Example Group Document

C.3.1 Open public chat group with the age control and a session activity policy

This example describes a group with the service URI “sip:mymusicgroupforyoungpeople” that any authenticated users can join if they are between 8 and 15 years old. It is only possible to join the group between 2008-02-16 9:30:00 UTC and 2008-02-26 9:30:00 UTC. The subject of the group is “Music”.

```
<?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"
  xmlns:oxe="urn:oma:xml:xdm:extensions">

  <list-service uri="sip:mymusicgroupforyoungpeople@example.com">

    <cr:ruleset>
      <cr:rule id="t78">
        <cr:conditions>
          <ocr:other-identity/>
        </cr:conditions>
        <cr:actions>
          <join-handling>true</join-handling>
          <oxe:allow-private-message>true</oxe:allow-private-message>
        </cr:actions>
      </cr:rule>
    </cr:ruleset>

    <oxe:subject>Music</oxe:subject>

    <oxe:age-restrictions oxe:must-understand="true">
      <oxe:age oxe:from="8" oxe:until="15"/>
    </oxe:age-restrictions>
    <oxe:session-activity-policy oxe:must-understand="true">
      <oxe:schedule>
        <oxe:start-time>2008-02-16T09:30:00Z</oxe:start-time>
        <oxe:end-time>2008-02-26T09:30:00Z</oxe:end-time>
      </oxe:schedule>
    </oxe:session-activity-policy>

  </list-service>
</group>
```

C.3.2 Prearranged group supporting all service and media types

This example describes a group with the service URI “sip:mygroup1_hermione.blossom@example.com”. The group is a prearranged group with 4 members. The group is allowed to be used for all types of services and media. The group supports sending of extended group advertisement done by the Shared Group XDMS. All members are allowed to start a group session, rejoin the group, to subscribe for the conference state and to do private messaging with another participant in the group session. The member “sip:hermione.blossom@example.com” is allowed to add the file transfer media type to the group session, to remove any media from the group session, to expel other participants from the group session, to create a sub conference and to invite new participants to an ongoing group session. The member “sip:alice@example.com” is blocked from sending a request to the group to send a group advertisement to all members of the group.

```
<?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"
  xmlns:oxe="urn:oma:xml:xdm:extensions">

  <list-service uri="sip:mygroup1_hermione.blossom@example.com">
    <list>
```

```

<entry uri="tel:+1-212-555-1234"/>
<entry uri="sip:hermione.blossom@example.com"/>
<entry uri="sip:bob@example.com"/>
<entry uri="sip:alice@example.com"/>
</list>
<invite-members>true</invite-members>
<cr:ruleset>
  <cr:rule id="t78">
    <cr:conditions>
      <is-list-member/>
    </cr:conditions>
    <cr:actions>
      <join-handling>true</join-handling>
      <allow-initiate-conference>true</allow-initiate-conference>
      <allow-conference-state>true</allow-conference-state>
      <oxe:allow-private-message>true</oxe:allow-private-message>
    </cr:actions>
  </cr:rule>
  <cr:rule id="t90">
    <cr:conditions>
      <cr:identity>
        <cr:one id="sip:hermione.blossom@example.com"/>
      </cr:identity>
      <oxe:media-list>
        <oxe:file-transfer/>
      </oxe:media-list>
    </cr:conditions>
    <cr:actions>
      <oxe:allow-media-handling>true</oxe:allow-media-handling>
    </cr:actions>
  </cr:rule>
  <cr:rule id="t95">
    <cr:conditions>
      <cr:identity>
        <cr:one id="sip:hermione.blossom@example.com"/>
      </cr:identity>
    </cr:conditions>
    <cr:actions>
      <oxe:remove-media-handling>any</oxe:remove-media-handling>
      <oxe:allow-expelling>true</oxe:allow-expelling>
      <oxe:allow-subconf>true</oxe:allow-subconf>
      <allow-invite-users-dynamically>true</allow-invite-users-dynamically>
    </cr:actions>
  </cr:rule>
  <cr:rule id="t30">
    <cr:conditions>
      <cr:identity>
        <cr:one id="sip:alice@example.com"/>
      </cr:identity>
    </cr:conditions>
    <cr:actions>
      <oxe:block-group-advertisement-sending>true</oxe:block-group-advertisement-sending>
    </cr:actions>
  </cr:rule>
</cr:ruleset>
<oxe:automatic-group-advertisement>true</oxe:automatic-group-advertisement>
</list-service>
</group>

```

Appendix D. Guidelines for the specification of enabler specific <actions> child elements (Informative)

The <actions> child elements in this document describe actions that are applicable across enablers. Any other enabler specific <actions> child element is recommended to be specified in the corresponding enabler specification. That specification should describe at least, XML schema definition under a namespace chosen by the enabler, structure, validation constraints if any, and data semantics.

The following text in the grey marked field provides a recommended template for the specification of enabler specific <actions> child elements and the text should be copied into a normative part the enabler specific specification and numbered according to where it is included.

NOTE 1. Text inside the parenthesis in X.1, X.2, X.3 and X.4 to be replaced.

NOTE 2: The reference [Shared_Group_XDM] must be present in the enabler specification

X Definition of enabler specific <actions> child element.

According to the Shared Group XDM Specification [Shared_Group_XDM], a Group rule that is to be evaluated and applied upon operations to the Group is described under the <rule> element.

A <rule> element consists of:

1. a <conditions> element that specifies in its child elements the matching conditions for the rule to be executed; and
2. an <actions> element that specifies in its child elements the actions to be taken according to this rule.

The <actions> child elements that are applied across enablers are specified and defined in [Shared_Group_XDM]. The <actions> child elements that are applied only for this enabler are specified and defined as follows.

X.1. XML Schema

(Here is defined an enabler specific <actions> child element under a namespace. If the namespace is a new one, it should be OMNA registered. An example of a namespace would be “urn:oma:xml:xdm:group:actions-XXX”, where XXX would be a short name of the enabler, e.g. im, poc2.)

X.2. Structure

(Here is described the structure of the element if necessary)

X.3. Validation Constraints

(Here is described any constraints that cannot be expressed by the schema definition.)

X.4. Data Semantics

(Here is described the semantics of the element value if any.)