



Policy XDM Specification

Candidate Version 1.1 – 24 Aug 2010

Open Mobile Alliance
OMA-TS-XDM_Policy-V1_1-20100824-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.

© 2010 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	7
3.1 CONVENTIONS	7
3.2 DEFINITIONS	7
3.3 ABBREVIATIONS	8
4. INTRODUCTION	9
4.1 VERSION 1.0	9
4.2 VERSION 1.1	9
5. POLICY XDM APPLICATION USAGES	10
5.1 USER ACCESS POLICY	10
5.1.1 Structure	10
5.1.2 Application Unique ID	11
5.1.3 XML Schema	11
5.1.4 Default Namespace	11
5.1.5 MIME Type	11
5.1.6 Validation Constraints	11
5.1.7 Data Semantics	12
5.1.8 Naming Conventions	16
5.1.9 Global Documents	16
5.1.10 Resource Interdependencies	16
5.1.11 Authorization Policies	16
5.1.12 Subscription to Changes	16
5.1.13 Search Capabilities	16
5.1.14 XDM Preferences Document	16
5.1.15 History Information Documents	17
5.1.16 Forwarding	17
5.1.17 Restore	17
5.1.18 Document Reference	17
5.1.19 Differential Read and Write	17
5.2 SUBSCRIBER DEFINED USER ACCESS POLICY	17
5.2.1 Structure	17
5.2.2 Application Unique ID	18
5.2.3 XML Schema	18
5.2.4 Default Namespace	18
5.2.5 MIME Type	18
5.2.6 Validation Constraints	18
5.2.7 Data Semantics	18
5.2.8 Naming Conventions	19
5.2.9 Global Documents	19
5.2.10 Resource Interdependencies	19
5.2.11 Authorization Policies	19
5.2.12 Subscription to Changes	19
5.2.13 Search Capabilities	19
5.2.14 XDM Preferences Document	19
5.2.15 History Information Documents	20
5.2.16 Forwarding	20
5.2.17 Restore	20
5.2.18 Document Reference	20
5.2.19 Differential Read and Write	20

6. SUBSCRIBING TO CHANGES IN THE XML DOCUMENTS.....21

7. BACKWARD COMPATIBILITY TOWARDS THE POC USER ACCESS POLICY APPLICATION USAGE.22

 7.1 PROCEDURES AT THE POLICY XDMS22

 7.2 PROCEDURES AT THE AGGREGATION PROXY.....23

APPENDIX A. CHANGE HISTORY (INFORMATIVE).....24

 A.1 APPROVED VERSION HISTORY24

 A.2 DRAFT/CANDIDATE VERSION 1.1 HISTORY24

APPENDIX B. STATIC CONFORMANCE REQUIREMENTS (NORMATIVE).....25

 B.1 POLICY XDM APPLICATION USAGES (XDMS)25

 B.2 POLICY XDM APPLICATION USAGES (XDMS).....27

 B.3 POLICY XDM APPLICATION USAGES (XDM AGENT)29

 B.4 AGGREGATION PROXY.....31

APPENDIX C. EXAMPLES (INFORMATIVE).....32

 C.1 USER ACCESS POLICY DOCUMENT STRUCTURE.....32

Figures

No table of figures entries found.

1. Scope

This specification describes the data format and Application Usage for the User Access Policy Document, which is a common user access policy definition that can be used by all OMA enablers (e.g. PoC, IM, CPM). It also defines an optional Application Usage for the Subscriber defined User Access Policy.

2. References

2.1 Normative References

OMA

- [Dict] “Dictionary for OMA Specifications”, Version 2.4, Open Mobile Alliance™, OMA-ORG-Dictionary-V2_4,
URL: <http://www.openmobilealliance.org/>
- [SCR RULES] “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 2.1, Open Mobile Alliance™, OMA-TS-XDM_Core-V2_1,
URL: <http://www.openmobilealliance.org/>
- [XSD_commPol] “XML Schema Definition: XDM – Common Policy”, Version 1.0, Open Mobile Alliance™, OMA-SUP-XSD_xdm_commonPolicy-V1_0,
URL: <http://www.openmobilealliance.org/>
- [XSD_ext] “XML Schema Definition: XDM2 Extensions ”, Version 1.0, Open Mobile Alliance™, OMA-SUP-XSD_xdm_extensions-V1_0,
URL: <http://www.openmobilealliance.org/>
- [XSD_ext_2_1] “XML Schema Definition: “XDM 2.1 – Extensions”, Version 1.0, Open Mobile Alliance™, OMA-SUP-XSD_xdm2_1extensions-V1_0,
URL: <http://www.openmobilealliance.org/>

IETF

- [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>
- [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>

2.2 Informative References

OMA

- [PoC_DocMgmt] “OMA PoC Document Management”, Version 2.0. Open Mobile Alliance™, OMA-TS-PoC_Document_Management-V2_0,
URL: <http://www.openmobilealliance.org/>
- [PoC_XDM] “PoC XDM Specification”, Version 1.0, Open Mobile Alliance™, OMA-TS-PoC_XDM-V1_0,
URL: <http://www.openmobilealliance.org/>
- [XDM_AD] “XML Document Management Architecture”, Version 2.1, Open Mobile Alliance™, OMA-AD-XDM-V2_1,
URL: <http://www.openmobilealliance.org/>

3. Terminology and Conventions

3.1 Conventions

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

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

3.2 Definitions

Access Permissions	Use definition from [XDM_RD].
Access Permissions Document	Use definition from [XDM_Core].
Aggregation Proxy	Use definition from [XDM_AD].
Alias Principal	Use definition from [XDM_RD].
Application Server	Use definition from [XDM_Core].
Application Unique ID	Use definition from [XDM_Core].
Application Usage	Use definition from [XDM_Core].
Automatic Answer Mode	A mode of operation in which the client accepts a communication request without manual intervention from the User; Media is immediately played when received.
Document Reference	Use definition from [XDM_AD].
Document URI	Use definition from [XDM_Core].
Enabler	Use definition from [Dict].
Global Document	Use definition from [XDM_Core].
History Information	Use definition from [XDM_AD].
Manual Answer Mode	A mode of operation in which the client requires the User to manually accept the communication request before the communication session is established.
Modification History Information Document	Use definition from [XDM_Core].
Node URI	Use definition from [XDM_Core].
Offline Communication Storage	A data storage where communication sessions can be stored when User is offline e.g. User has not registered to the communication service.
Principal	Use definition from [Dict].
Request History Information Document	Use definition from [XDM_Core].
Subscriber	Use definition from [Dict].
URI List	Use definition from [XDM_RD].
User	A User is any entity that uses the described features through the User Equipment.
User Access Policy	Use definition from [XDM_RD].
User Access Policy Document	An XDM Document containing User Access Policy information.
XCAP Resource	Use definition from [XDM_Core].
XCAP Root	Use definition from [XDM_Core].

XCAP Server	Use definition from [XDM_Core].
XCAP User Identifier	Use definition from [XDM_Core].
XDM Agent	Use definition from [XDM_AD].
XDMC	Use definition from [XDM_AD].
XDM Document	Use definition from [XDM_RD].
XDM Preferences	Use definition from [XDM_Core].
XDM Preferences Document	Use definition from [XDM_Core].
XDMS	Use definition from [XDM_AD].

3.3 Abbreviations

ABNF	Augmented Backus-Naur Form
AUID	Application Unique ID
CPM	Converged IP Messaging
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IM	Instant Messaging
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 User Access Policy Document. It reuses the PoC User Access Policy Document structure described in [PoC_XDM].

The Policy XDMS (see [XDM_AD]) is the logical repository for User Access Policy Documents. The common protocol specified in [XDM_Core] is used for access and manipulation of such policies by authorized Principals.

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

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]).

4.1 Version 1.0

The version 1.0 is called “Shared Policy XDMS” and specifies:

- Application Usage for user access policy;
- its naming conventions, data semantics, schema and validation constraints; and
- subscription to changes in XDM Documents.

4.2 Version 1.1

The version 1.1 is renamed to “Policy XDMS”. It includes the functionality of version 1.0 and in addition specifies:

- Application Usage for subscriber defined user access policy; and
- its naming conventions, data semantics, schema and validation constraints.

Editors' Note: The AUID string “subscriber-defined-access-rules “ needs to be registered

Editor's note: This list needs to be updated when TS text is complete

5. Policy XDM Application Usages

5.1 User Access Policy

This section specifies an Application Usage called User Access Policy, which is used to control incoming and outgoing communication of the User in the Application Server (e.g. PoC Server, IM Server and CPM Server).

5.1.1 Structure

The User Access Policy Document SHALL conform to the structure of the “ruleset” document described in [RFC4745], with the extensions and constraints given in this section.

The User Access Policy Document makes use of the following two elements defined for the <rule> element in [RFC4745]:

- <conditions>
- <actions>

The <transformations> child element defined for the <rule> element in [RFC4745] SHALL be ignored, if present.

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

- a) MAY include the <identity> element, as defined in [RFC4745], except the sub-elements that are ignored as defined 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 <sphere> element, as defined in [RFC4745];
- e) MAY include the <anonymous-request> element, as defined in [XDM_Core] “Common Extensions”;
- f) MAY include the <media-list> element, as defined in [XDM_Core] “Common Extensions”;
- g) MAY include the <service-list> element, as defined in [XDM_Core] “Common Extensions”;
- h) MAY include the <validity> element, as defined in [RFC4745];
- i) MAY include the <invited-identities> element, as defined in [XDM_Core] “Common Extensions”;
- j) MAY include the <activities> element, as defined in [XDM_Core] “Common Extensions”;
- k) MAY include the <qoe-list> element, as defined in [XDM_Core] “Common Extensions”;
- l) MAY include the <country-region-list> element, as defined in [XDM_Core] “Common Extensions”;
- m) MAY include the <location-list> element, as defined in [XDM_Core] “Common Extensions”;
- n) MAY include the <upp-list> element, as defined in [XDM_Core] “Common Extensions”;
- o) MAY include the <expired> element as defined in [XDM_Core] “Common Extensions”;
- p) MAY include the <deferred-messages> element as defined in [XDM_Core] “Common Extensions”; and
- q) MAY include other elements from other namespaces for the purposes of extensibility.

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

- a) MAY include the <allow-reject-invite> element;
- b) MAY include the <allow-offline-storage> element;
- c) MAY include the <allow-auto-answermode> element;
- d) MAY include the <allow-manual-answer-override> element;
- e) MAY include the <allow-barring-media-content> element;
- f) MAY include the <allow-barring-media-stream> element;
- g) MAY include the <allow-remove-text-content> element;
- h) MAY include the <allow-remove-reference-content> element;
- i) MAY include the <allow-add-text-content> element;
- j) MAY include the <allow-add-reference-content> element;
- k) MAY include the <allow-reject-outgoing-invite> element;
- l) MAY include the <allow-defer-and-notify> element;
- m) MAY include the <allow-defer-without-notify> element;
- n) MAY include the <allow-store> element;
- o) MAY include the <allow-forward> element;
- p) MAY include the <allow-interwork> element;
- q) MAY include the <allow-deliver-and-interwork> element;
- r) MAY include the <allow-push> element;
- s) MAY include the <allow-deliver-reference-media> element; and
- t) MAY include other elements from other namespaces for the purposes of extensibility.

5.1.2 Application Unique ID

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

5.1.3 XML Schema

The User Access Policy Document SHALL conform to the XML schema described in [RFC4745], with extensions described in [XSD_commPol], [XSD_ext_2_1] and [XSD_ext] and with extensions described in enabler defined XML schemas.

5.1.4 Default Namespace

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

5.1.5 MIME Type

The MIME type for the User Access Policy Document SHALL be “application/auth-policy+xml” defined in [RFC4745].

5.1.6 Validation Constraints

The User Access Policy Document SHALL conform to the XML Schema described in section 5.1.3 “XML Schema”, with the additional validation constraints described below.

The “id” attribute of the <one> element SHALL contain a SIP URI or a tel URI.

If present, the “id” attribute of the <except> element SHALL contain a SIP URI or a tel URI.

If the AUID value of the Document URI or Node URI proposed in an <external-list> element is other than “resource-lists”, the Policy 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 list”.

If the XUI value of the Document URI or Node URI proposed in an <external-list> element does not match the XUI of the User Access Policy Document URI and if the Policy XDMS determines that the Primary Principal or an associated Alias Principal is not allowed to retrieve the referenced XDM Resource, the Policy 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 list”.

5.1.7 Data Semantics

The User Access Policy Document SHALL conform to the semantics for the “conditions” and “actions” described in [RFC4745] and [XDM_Core] “*Common Extensions*”, with the additional extensions and clarifications described below.

The <allow-reject-invite> element defines the action the Application Server is to take when processing a communication request for a particular User. This element instructs the Application Server performing the terminating participant function to reject an incoming communication request. The value is of a Boolean type:

- “false” instructs the Application Server performing the terminating participant function to not to reject the communication request. This SHALL be the default value taken in the absence of the element;
- “true” instructs the Application Server performing the terminating participant function to reject the communication request using procedures as defined by the enabler.

The <allow-auto-answermode> element defines the action the Application Server performing the terminating participant function is to take when processing an Automatic Answer Mode procedure for a particular User. The value is of a Boolean type:

- “false” instructs the Application Server performing the terminating participant function not to perform the Automatic Answer Mode procedures as defined by the enabler. This SHALL be the default value taken in the absence of the element;
- “true” instructs the Application Server performing the terminating participant function to perform the Automatic Answer Mode procedure as defined by the enabler.

The <allow-offline-storage> element defines the action the Application Server performing the terminating participant function is to take when processing a communication request for a particular User who is offline, and the type of Offline Communication Storage to be connected when the communication request is to be routed to an Offline Communication Storage. The <allow-offline-storage> element:

- a) SHALL include the “allow” attribute to define the action the Application Server is to take when processing a communication request for a particular User who is offline. The value is of a Boolean type:
 - “false” instructs the Application Server not to route the communication request to the Offline Communication Storage when the User is offline. This SHALL be the default value of the attribute.
 - “true” instructs the Application Server to route the communication request to the Offline Communication Storage when the User is offline. The type of Offline Communication Storage to be routed to is defined as a child element of the <allow-offline-storage> element.
- b) MAY contain one or more elements from other namespaces defined by the enabler, which indicate the Offline Communication Storage types.
- c) MAY contain attributes from any other namespaces for the purpose of extensibility.

The <allow-manual-answer-override> element defines the action the Application Server is to take when processing a communication request for a particular User and when the communication request contains a request to override the Manual Answer Mode procedure. The value is of a Boolean type:

"false" instructs the Application Server to reject the communication request. This SHALL be the default value taken in the absence of the element.

"true" instructs the Application Server to process the communication request using Automatic Answer Mode.

The <allow-barring-media-content> element defines the action the Application Server performing the terminating participant function is to take when processing a communication request for a particular User when the communication request contains media content as specified in the <media-list> element. The value is of a Boolean type:

"false" instructs the Application Server to not bar the media content contained in the communication request. This SHALL be the default value taken in the absence of the element.

"true" instructs the Application Server to bar the media content contained in the communication request.

The <allow-barring-media-stream> element defines the action the Application Server performing the terminating participant function is to take when processing a communication request for a particular User when the communication request contains a media stream as specified in the <media-list> element. The value is of a Boolean type:

"false" instructs the Application Server to not bar the media stream contained in the communication request. This SHALL be the default value taken in the absence of the element.

"true" instructs the Application Server to bar the media stream contained in the communication request.

The <allow-remove-text-content> element defines the action the Application Server is to take when processing a communication request for a particular User. The value is of a Boolean type:

"false" instructs the Application Server to allow text content included in particular header fields (e.g. Subject header of SIP invitation request) of communication request. This SHALL be the default value taken in the absence of the element.

"true" instructs the Application Server to remove text content included in particular header fields (e.g. Subject header of SIP invitation request) of communication request.

The <allow-remove-reference-content> element defines the action the Application Server is to take when processing a communication request for a particular User. The value is of a Boolean type:

"false" instructs the Application Server to allow referenced media content included in particular header fields (e.g. Call-info or Alert-info header of SIP invitation request) of communication request. This SHALL be the default value taken in the absence of the element.

"true" instructs the Application Server to remove referenced media content included in particular header fields (e.g. Call-info or Alert-info header of SIP invitation request) of communication request.

The <allow-add-text-content> element defines the action the Application Server is to take when processing a communication request for a particular User. The value is of a Boolean type:

"false" instructs the Application Server not to handle text content included in particular header fields (e.g. Subject header of SIP invitation request) of communication request. This SHALL be the default value taken in the absence of the element.

"true" instructs the Application Server to add or replace text content included in particular header fields (e.g. Subject header of SIP invitation request) of communication request.

The <allow-add-reference-content> element defines the action the Application Server is to take when processing a communication request for a particular User. The value is of a Boolean type:

- "false" instructs the Application Server not to handle referenced media content included in particular header fields (e.g. Call-info or Alert-info header of SIP invitation request) of communication request. This SHALL be the default value taken in the absence of the element.
- "true" instructs the Application Server to add or replace referenced media content included in particular header fields (e.g. Call-info or Alert-info header of SIP invitation request) of communication request.

The <allow-reject-outgoing-invite> element defines the action the Application Server is to take when processing a communication request for a particular User. This element instructs the Application Server performing the originating participant function to reject an outgoing communication request. The value is of a Boolean type:

- "false" instructs the Application Server performing the originating participant function not to reject the communication request. This SHALL be the default value taken in the absence of the element;
- "true" instructs the Application Server performing the originating participant function to reject the communication request using procedures as defined by the enabler.

The <allow-defer-and-notify> element defines the action the Application Server is to take when processing a communication request for a particular User. This element instructs the Application Server performing the terminating participant function to defer an incoming communication request and to notify the User. The value is of a Boolean type:

- "false" instructs the Application Server performing the terminating participant function to not defer the communication request nor to notify the User. This SHALL be the default value taken in the absence of the element;
- "true" instructs the Application Server performing the terminating participant function to defer the communication request using procedures as defined by the Enabler and to notify the User.

The <allow-defer-without-notify> element defines the action the Application Server is to take when processing a communication request for a particular User. This element instructs the Application Server performing the terminating participant function to defer an incoming communication request. The value is of a Boolean type:

- "false" instructs the Application Server performing the terminating participant function to not defer the communication request. This SHALL be the default value taken in the absence of the element;
- "true" instructs the Application Server performing the terminating participant function to defer the communication request using procedures as defined by the Enabler.

The <allow-store> element defines the action the Application Server is to take when processing a communication request for a particular User. This element instructs the Application Server performing the terminating participant function to store an incoming communication request in the User's Message Store. The value is of a Boolean type:

- "false" instructs the Application Server performing the terminating participant function to not store the communication request. This SHALL be the default value taken in the absence of the element;
- "true" instructs the Application Server performing the terminating participant function to store the communication request using procedures as defined by the enabler.

The <allow-forward> element defines the action the Application Server is to take when processing a communication request for a particular User. This element instructs the Application Server performing the terminating participant function to forward an incoming communication request to a different address. The <allow-forward> element:

- a) SHALL include the "execute" attribute. The value is of a Boolean type:

"false" instructs the Application Server performing the terminating participant function to not forward the communication request. This SHALL be the default value taken in the absence of the element;

"true" instructs the Application Server performing the terminating participant function to forward the communication request using procedures as defined by the Enabler. A child element <forward-to> of the <allow-forward> element is used to store the address to which the communication is to be forwarded.

- b) MAY contain one or more elements from other namespaces defined by the Enabler; and.

- c) MAY contain attributes from any other namespaces for the purpose of extensibility.

The <allow-interwork> element defines the action the Application Server is to take when processing a communication request for a particular User. This element instructs the Application Server performing the terminating participant function to deliver an incoming communication request using a different communication service. The <allow-interwork> element:

- a) SHALL include the “execute” attribute. The value is of a Boolean type:

“false” instructs the Application Server performing the terminating participant function to not inter-work the communication request. This SHALL be the default value taken in the absence of the element;

“true” instructs the Application Server performing the terminating participant function to inter-work the communication request using procedures as defined by the Enabler. A child element <methods-list> of the <allow-interwork> element is used to store a list of preferred communication services.

The <methods-list> element:

- a) SHALL include one or more <method> element

The <method> element:

- a) SHALL include a priority attribute whose value means a relative priority of this communication method over others. The value of the attribute SHALL be decimal number between 0 and 1 with utmost 3 digits after the decimal point. Higher value indicates higher priority; and
- b) SHALL include a value which indicates the type of the communication methods (e.g. SMS, MMS and email) to be used to interwork.

The <allow-deliver-and-interwork> element defines the action the Application Server is to take when processing a communication request for a particular User. This element instructs the Application Server performing the terminating participant function to deliver an incoming communication request to the User and to send the incoming communication using a different communication service. The <allow-deliver-and-interwork> element:

- a) SHALL include the “execute” attribute. The value is of a Boolean type:

“false” instructs the Application Server performing the terminating participant function to not deliver the communication request nor to send it to an interworking selection function. This SHALL be the default value taken in the absence of the element;

“true” instructs the Application Server performing the terminating participant function to deliver the communication request using procedures as defined by the Enabler and to send the incoming communication request using a different communication service. A child element <methods-list> of the <allow-deliver-and-interwork> element is used to store a list of preferred communication services and the syntax of this element is as described above.

The <allow-push> element defines the action the Application Server is to take when processing deferred communication requests for a particular User. This element instructs the Application Server performing the terminating participant function to push all the deferred communication requests to the User. The value is of a Boolean type:

“false” instructs the Application Server performing the terminating participant function to not push the deferred communication requests. This SHALL be the default value taken in the absence of the element;

“true” instructs the Application Server performing the terminating participant function to push the deferred communication requests using procedures as defined by the enabler.

The <allow-deliver-reference-media> element defines the action the Application Server is to take when processing a communication requests for a particular User. This element instructs the Application Server performing the terminating participant function to store media contained in an incoming communication request and deliver the communication request to the User with a link to the stored media. The value is of a Boolean type:

- “false” instructs the Application Server performing the terminating participant function to not store the media contained in the incoming communication requests nor to include a reference in the communication request. This SHALL be the default value taken in the absence of the element;
- “true” instructs the Application Server performing the terminating participant function to store media contained in an incoming communication request and deliver the communication request to the User with a link to the stored media using procedures as defined by the enabler.

5.1.8 Naming Conventions

The name of the User Access Policy Document SHALL be “access-rules”.

5.1.9 Global Documents

This Application Usage defines no Global Documents.

5.1.10 Resource Interdependencies

This Application Usage defines no additional resource interdependencies.

5.1.11 Authorization Policies

The authorization policies SHALL conform to the default authorization policy as described in [XDM_Core] section “*Authorization*”.

The User Access Application Usage MAY support an Access Permissions Document as described in [XDM_Core] sections “*Authorization*” and “*Access Permissions Document*” with the following clarifications:

- a) An <allow-operation-own-data> element SHALL NOT be included in an <actions> element; and
- b) An <external-list> element SHALL, if such element is included in a <conditions> element, reference a URI List in List XDMS.

5.1.12 Subscription to Changes

The User Access Policy Application Usage SHALL support suscription to changes as specified in [XDM_Core] sections “*Subscriptions to changes in the XDM Resources*”.

5.1.13 Search Capabilities

Not applicable for searching User Access Policy Document.

The User Access Policy Application Usage MAY support search capability for searching:

- The Modification History Information Document as described in [XDM_Core] section “*Modification History Information Document*”; and
- The Request History Information Document as described in [XDM_Core] section “*Request History Information Document*”.

5.1.14 XDM Preferences Document

The User Access Policy Application Usage SHALL support an XDM Preferences Document as described in [XDM_Core] section “*XDM Preferences Document*” if it supports History Information XDM Documents as described in section 5.1.15 or Forwarding as described in section 5.1.16.

5.1.15 History Information Documents

The User Access Policy Application Usage MAY support Modification History Information Document as described in [XDM_Core] section “*Modification History Information Document*”.

The User Access Policy Application Usage MAY support a Request History Information Document as described in [XDM_Core] section “*Request History Information Document*”.

5.1.16 Forwarding

The User Access Policy Application Usage MAY support forwarding of User Access Policy Document as described in [XDM_Core] section “*XDM Resource Forwarding Operations*”.

5.1.17 Restore

The User Access Policy Application Usage MAY support restore of a User Access Policy Document as described in [XDM_Core] section “*XDM Restore*”.

5.1.18 Document Reference

The User Access Policy Application Usage MAY support Document Reference of a User Access Policy Document as described in [XDM_Core] section “*Document Reference*”.

5.1.19 Differential Read and Write

User Access Policy Application Usage MAY support Differential Read as described in [XDM_Core] section “*Differential Read*”. A Differential Read request including a <filter-set> element is not supported.

User Access Policy Application Usage MAY support Differential Write as described in [XDM_Core] section “*Differential Write*”. A Differential Write request including a <filter-set> element is not supported.

5.2 Subscriber defined User Access Policy

This section specifies an optional Application Usage for the Policy XDMS, the XDMC and the XDM Agent called Subscriber defined User Access Policy, which overrides User defined User Access Policy described in section 5.1 if needed (e.g. for parental control, control of company paid subscription etc).

5.2.1 Structure

The Subscriber defined User Access Policy Document SHALL conform to the same structure as the User Access Policy Document described in section 5.1.1 “*Structure*”, but using only the elements listed in this section.

The Subscriber defined User Access Policy Document makes use of the following two elements defined for the <rule> element in [RFC4745]:

- <conditions>
- <actions>

The <transformations> child element defined for the <rule> element in [RFC4745] SHALL be ignored, if present.

The <conditions> child element of any <rule> element MAY include the same elements that can be included in the User Access Policy <conditions> child element as defined in section 5.1.1 “*Structure*”.

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

- a) MAY include the <allow-reject-invite> element;

- b) MAY include the <allow-reject-outgoing-invite> element; and
- c) MAY include other elements from other namespaces for the purposes of extensibility.

5.2.2 Application Unique ID

The AUID SHALL be “org.openmobilealliance.subscriber-defined-access-rules”.

5.2.3 XML Schema

The Subscriber defined User Access Policy Document SHALL conform to the XML schema described in [RFC4745], with extensions described in [XSD_commPol], [XSD_ext_2_1] and [XSD_ext] and with extensions described in enabler defined XML schemas.

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 the Subscriber defined User Access Policy Document SHALL be “application/auth-policy+xml” defined in [RFC4745].

5.2.6 Validation Constraints

The Subscriber defined User Access Policy Document SHALL conform to the XML Schema described in section 5.1.3 “XML Schema”, with the additional validation constraints described below.

The “id” attribute of the <one> element SHALL contain a SIP URI or a tel URI.

If present, the “id” attribute of the <except> element SHALL contain a SIP URI or a tel URI.

If the AUID value of the Document URI or Node URI proposed in an <external-list> element is other than “resource-lists”, the Policy 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 list”.

If the XUI value of the Document URI or Node URI proposed in an <external-list> element does not match the XUI of the Subscriber defined User Access Policy Document URI and if the Policy XDMS determines that the Primary Principal or an associated Alias Principal is not allowed to retrieve the referenced XDM Resource, the Policy 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 list”.

5.2.7 Data Semantics

The Subscriber defined User Access Policy Document SHALL conform to the semantics for the “conditions” and “actions” described in [RFC4745] and [XDM_Core] “Common Extensions”, with the additional extensions and clarifications described below.

The <allow-reject-invite> element defines the action the Application Server is to take when processing a communication request for a particular User. This element instructs the Application Server performing the terminating participant function to reject an incoming communication request. The value is of a Boolean type:

- “false” instructs the Application Server performing the terminating participant function not to reject the communication request. This SHALL be the default value taken in the absence of the element;
- “true” instructs the Application Server performing the terminating participant function to reject the communication request using procedures as defined by the enabler.

The <allow-reject-outgoing-invite> element defines the action the Application Server is to take when processing a communication request for a particular User. This element instructs the Application Server performing the originating participant function to reject an outgoing communication request. The value is of a Boolean type:

- “false” instructs the Application Server performing the originating participant function not to reject the communication request. This SHALL be the default value taken in the absence of the element;
- “true” instructs the Application Server performing the originating participant function to reject the communication request using procedures as defined by the enabler.

5.2.8 Naming Conventions

The name of the Subscriber defined User Access Policy Document SHALL be “subscriber-defined-access-rules”.

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 conform to the default authorization policy as described in [XDM_Core] section “*Authorization*”.

The Subscriber defined User Access Application Usage SHALL support an Access Permissions Document as described in [XDM_Core] sections “*Authorization*” and “*Access Permissions Document*” with the following clarifications:

- a) An <allow-operation-own-data> element SHALL NOT be included in an <actions> element; and
- b) An <external-list> element SHALL, if such element is included in a <conditions> element, reference a URI List in List XDMS.

5.2.12 Subscription to Changes

The Subscriber defined User Access Policy Application Usage SHALL support suscription to changes as specified in [XDM_Core] section “*Subscriptions to changes in XDM Resources*”.

5.2.13 Search Capabilities

Not applicable for searching Subscriber defined User Access Policy Document.

The Subscriber defined User Access Policy Application Usage MAY support search capability for searching:

- The Modification History Information Document as described in [XDM_Core] section “*Modification History Information Document*”; and
- The Request History Information Document as described in [XDM_Core] section “*Request History Information Document*”.

5.2.14 XDM Preferences Document

The Subscriber defined User Access Policy Application Usage SHALL support an XDM Preferences Document as described in [XDM_Core] section “*XDM Preferences Document*” if it supports History Information XDM Documents as described in section 5.1.15 or Forwarding as described in section 5.1.16.

5.2.15 History Information Documents

The Subscriber defined User Access Policy Application Usage MAY support Modification History Information Document as described in [XDM_Core] section “*Modification History Information Document*”.

The Subscriber defined User Access Policy Application Usage MAY support a Request History Information Document as described in [XDM_Core] section “*Request History Information Document*”.

5.2.16 Forwarding

The Subscriber defined User Access Policy Application Usage MAY support forwarding of Subscriber defined User Access Policy Document as described in [XDM_Core] section “*XDM Resource Forwarding Operations*”.

5.2.17 Restore

The Subscriber defined User Access Policy Application Usage MAY support restore of a Subscriber defined User Access Policy Document as described in [XDM_Core] section “*XDM Restore*”.

5.2.18 Document Reference

The Subscriber defined User Access Policy Application Usage MAY support Document Reference of a Subscriber defined User Access Policy Document as described in [XDM_Core] section “*Document Reference*”.

5.2.19 Differential Read and Write

The Subscriber defined User Policy Application Usage MAY support Differential Read as described in [XDM_Core] section “*Differential Read*”. A Differential Read request including a <filter-set> element is not supported.

The Subscriber defined User Access Policy Application Usage MAY support Differential Write as described in [XDM_Core] section “*Differential Write*”. A Differential Write request including a <filter-set> element is not supported.

6. Subscribing to changes in the XML documents

Refer to section “Subscription to Changes” in each Application Usage.

7. Backward Compatibility towards the PoC User Access Policy Application Usage

7.1 Procedures at the Policy XDMS

If the Policy XDMS allows access by PoCv1.0 Clients, the Policy XDMS SHALL support the PoC User Access Policy Application Usage defined in [PoC_XDM-V1_0] “*PoC User Access Policy*”, with the clarifications given in this section.

The Policy XDMS SHALL maintain, for each User, both the “pocrules” document of the PoC User Access Policy Application Usage and the “access-rules” document of the User Access Policy Application Usage. There is a one-to-one correspondence between the “pocrules” and “access-rules” documents, and the contents of the documents at any point in time SHALL be synchronized as described below.

NOTE: This does not imply that the Policy XDMS must actually store the “pocrules” document, but must always be prepared to process requests against the “pocrules” document.

The Policy XDMS SHALL, when it receives an XCAP PUT request for the PoC User Access Policy Application Usage, apply the same modifications to the User Access Policy Application Usage with the following exceptions:

- a) If the resulting “pocrules” document contains rule(s) with the <allow-invite> action set to “reject”, the corresponding rule(s) in the “access-rules” document:
 - 1) SHALL contain the <allow-reject-invite> action set to “true”; and
 - 2) SHALL NOT contain the <allow-auto-answermode> action.
- b) If the resulting “pocrules” document contains rule(s) with the <allow-invite> action set to “accept”, the corresponding rule(s) in the “access-rules” document:
 - 1) SHALL contain the <allow-auto-answermode> action set to “true”; and
 - 2) SHALL NOT contain the <allow-reject-invite> action.
- c) If the resulting “pocrules” document contains rule(s) with the <allow-invite> action set to “pass”, the corresponding rule(s) in the “access-rules” document:
 - 1) SHALL NOT contain the <allow-auto-answermode> action; and
 - 2) SHALL NOT contain the <allow-reject-invite> action.

The Policy XDMS SHALL, when it receives an XCAP PUT request for the User Access Policy Application Usage, apply the same modifications to the PoC User Access Policy Application Usage with the following exceptions:

- a) If the resulting “access-rules” document contains rule(s) with the <service-list > condition and <media-list> condition not specifying a PoC v1.0 service the rule(s) SHALL be omitted from the “pocrules” document;
- b) If the resulting “access-rules” document contains rule(s) with the <allow-reject-invite> action set to “true”, the corresponding rule(s) in the “pocrules” document SHALL contain the <allow-invite> action set to “reject”;
- c) If the resulting “access-rules” document contains rule(s) with the <allow-auto-answermode> action set to “false”, the corresponding rule(s) in the “pocrules” document SHALL contain the <allow-invite> action set to “pass”;
- d) If the resulting “access-rules” document contains rule(s) with the <allow-auto-answermode> action set to “true”, the corresponding rule(s) in the “pocrules” document SHALL contain the <allow-invite> action set to “accept”.

The Policy XDMS SHALL, when it receives an XCAP request for an XML Documents Directory document as defined in [XDM_Core] “XML Documents Directory”, include the “pocrules” document in addition to the “access-rules” document.

When responding to a request for the XCAP Server Capabilities as defined in [XDM_Core] “XCAP Server Capabilities”, the Policy XDMS SHALL include the XCAP Server Capabilities for the PoC User Access Policy Application Usage, in addition to the User Access Policy Application Usage.

7.2 Procedures at the Aggregation Proxy

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

NOTE: An Aggregation Proxy forwards XCAP requests for the PoC User Access Policy AUID to the Policy 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 1.1 History

Document Identifier	Date	Sections	Description
Draft Version OMA-TS-Shared_Policy_XDM-V1_1	14 Apr 2009	n/a	Baseline created from OMA-TS-XDM_Shared_Policy-V1_0-20080916-C Application of the 2009 template (section 4).
Draft Versions OMA-TS- Policy_XDM-V1_1	24 Apr 2009	All	Incorporated CR: OMA-PAG-2009-0127- CR_XDM2.1_TS_Shared_Policy_Removal_Of_Shared
	03 Sep 2009	5.1.1, 5.1.7, 5.4.1, 5.2	Incorporated CRs: OMA-PAG-2009-0142 OMA-PAG-2009-0186 OMA-PAG-2009-0205 OMA-PAG-2009-0213R01 OMA-PAG-2009-0214R01
	24 Sep 2009	5.1.1	Incorporated CR: OMA-PAG-2009-0271R02
	28 Oct 2009	4	Incorporated CR: OMA-PAG-2009-0364R01
	08 Feb 2010	All	Incorporated CR: OMA-PAG-2010-0057R01
	08 Mar 2010	All	Incorporated CR: OMA-MWG-XDM-2010-0075R01
	10 Mar 2010	1, 2.1, 2.2, 3.2, 3.3, 4, 5.1, 5.2, App B	Incorporated CRs: OMA-MWG-XDM-2010-0106R01 OMA-MWG-XDM-2010-0107R01 OMA-MWG-XDM-2010-0108R01
	21 May 2010	All	Incorporated CR OMA-COM-XDM-2010-0177R01
	08 Jul 2010	All	Incorporated CRs: OMA-COM-XDM-2010-0257R02- CR_XDM2.1_Policy_Fix_Search_History_AI005 OMA-COM-XDM-2010-0281R01- CR_XDM_2_1_Policy_F008_plus_fix_to_accesspermissions OMA-COM-XDM-2010-0286R02-CR_XDM_User_preferences OMA-COM-XDM-2010-0296R04- CR_XDM_2_1_Policy_F023_SCR_table_some_new_items
15 Jul 2010	All	Formatting of bullets	
Candidate Version OMA-TS- Policy_XDM-V1_1	24 Aug 2010	N/A	Status changed to Candidate by TP TP ref # OMA-TP-2010-0368- INP_XDM_V2.1_ERP_and_ETR_for_Candidate_approval

Appendix B. Static Conformance Requirements

(Normative)

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

The SCRs defined in the following tables include SCRs for:

- Policy XDM Application Usages
- Aggregation Proxy

B.1 Policy XDM Application Usages (XDMS)

Item	Function	Reference	Requirement
XDM_UAP-AU-S-001-M	Support User Access Policy Document structure (XDMv2.0)	5.1.1	XDM_Core-XOP-S-001-M
XDM_UAP-AU-S-002-M	Support Application Unique ID of User Access Policy Application Usage (XDMv2.0)	5.1.2	
XDM_UAP-AUP-S-003-M	Support XML schema of User Access Policy Document (XDMv2.0)	5.1.3	
XDM_UAP-AU-S-008-O	Support XML schema of the User Access Policy Document extensions (XDMv2.1)	5.1.3	
XDM_UAP-AU-S-004-M	Support MIME type of User Access Policy Document (XDMv2.0)	5.1.5	
XDM_UAP-AU-S-005-M	Support Validation constraints of the XDM v2.0 User Access Policy Document (XDMv2.0)	5.1.6	
XDM_UAP-AU-S-009-O	Support Validation constraints of the XDM v2.1 User Access Policy Document XDM extensions	5.1.6	
XDM_UAP-AU-S-006-M	Support Data semantics of XDM v2.0 User Access Policy Document (XDMv2.0)	5.1.7	
XDM_UAP-AU-S-010-O	Support Data semantics for of the XDM v2.1 User Access Policy Document XDM extensions	5.1.7	
XDM_UAP-AU-S-007-M	Support Naming conventions for User Access Policy Document (XDMv2.0)	5.1.8	
XDM_UAP-SEC-S-008-M	Support for the default Authorization policy for accessing a User Access Policy Document (XDMv2.0)	5.1.11	XDM_Core-SEC-S-001-M
XDM_UAP-SEC-S-002-O	Support for Authorization policies defined in an Access Permissions Document governing access to a User Access Policy Document (XDMv2.1)	5.1.11	XDM_Core-SEC-S-002-O
XDM_UAP-SUB-S-001-M	Support Subscribing to changes in User Access Policy Document (XDMv2.0)	5.1.12	XDM_Core-SUB-S-001-O AND XDM_Core-SUB-S-002-O
XDM_UAP-SRC-S-001-O	Support Search in Modification History Document (XDMv2.1)	5.1.13	XDM_Core-SRC-S-004-O AND XDM_UAP-MHI-S-001-O
XDM_UAP-SRC-S-002-O	Support Search in Request History Information Document (XDMv2.1)	5.1.13	XDM_Core-SRC-S-005-O AND XDM_UAP-RHI-S-001-O
XDM_UAP-PRF-S-001-O	Support XDM Preferences Document (XDMv2.1)	5.1.14	XDM_Core-PRF-S-001-O AND (XDM_UAP-FWD-S-001-O OR XDM_UAP-MHI-S-001-O OR XDM_UAP-RHI-S-001-O)

Item	Function	Reference	Requirement
XDM_UAP-MHI-S-001-O	Support Modification History Information Document (XDMv2.1)	5.1.15	XDM_Core-MHI-S-001-O AND XDM_UAP-PRF-S-001-O
XDM_UAP-RHI-S-001-O	Support Request History Information Document (XDMv2.1)	5.1.15	XDM_Core-RHI-S-001-O
XDM_UAP-FWD-S-001-O	Support Forwarding of a User Access Policy Document (XDMv2.1)	5.1.16	XDM_Core-FWD-S-001-O
XDM_UAP-RES-S-001-O	Support Restore of User Access Policy Document (XDMv2.1)	5.1.17	XDM_Core-RES-S-001-O
XDM_UAP-REF-S-001-O	Support Document Reference of User Access Policy Document	5.1.18	XDM_Core-REF-S-001-O
XDM_UAP-DIFF-S-001-O	Support Differential Read in User Access Policy Document (XDMv2.1)	5.1.19	XDM_Core-DIFF-S-001-O
XDM_UAP-DIFF-S-001-O	Support Differential Write in User Access Policy Document (XDMv2.1)	5.1.19	XDM_Core-DIFF-S-002-O
XDM_Policy-SUB-S-001-M	Subscribing to changes in Access Policy documents	5.2	XDM_Core -SUB-S-001-O AND XDM_Core -SUB-S-002-O
XDM-UAP-BC-S-001-M	Support Backward compatibility PoC User Access Policy Application Usage (XDMv2.0)	7.1	
XDM_SUAP-AU-S-001-O	Support for Subscriber defined User Access Policy Application Usage (XDMv2.1)	5.2	XDM_Core-XOP-S-001-M AND XDM_SUAP-AU-S-002-O AND XDM_SUAP-AU-S-003-O AND XDM_SUAP-AU-S-004-O AND XDM_SUAP-AU-S-005-O AND XDM_SUAP-AU-S-006-O AND XDM_SUAP-AU-S-007-O AND XDM_SUAP-AU-S-008-O AND XDM_SUAP-AU-S-009-O AND XDM_SUAP-SEC-1-002-O AND XDM_SUAP-SEC-S-002-O
XDM_SUAP-AU-S-002-O	Subscriber defined User Access Policy Document structure (XDMv2.1)	5.2.1	XDM_SUAP-AU-S-001-O
XDM_SUAP-AU-S-003-O	Support Application Unique ID in Subscriber defined User Access Policy Application Usage (XDMv2.1)	5.2.2	XDM_SUAP-AU-S-001-O
XDM_SUAP-AU-S-004-O	Support XML schema of Subscriber defined User Access Policy Document (XDMv2.1)	5.2.3	XDM_SUAP-AU-S-001-O
XDM_SUAP-AU-S-005-O	Support MIME type of Subscriber defined User Access Policy Document (XDMv2.1)	5.2.5	XDM_SUAP-AU-S-001-O
XDM_SUAP-AU-S-006-O	Support validation constraints of Subscriber defined User Access Policy Document User Acce (XDMv2.1)	5.2.6	XDM_SUAP-AU-S-001-O
XDM_SUAP-AU-S-007-O	Support data semantics of Subscriber defined User Access Policy Document (XDMv2.1)	5.2.7	XDM_SUAP-AU-S-001-O
XDM_SUAP-AU-S-008-O	Support naming conventions of Subscriber defined User Access Policy Document (XDMv2.1)	5.2.8	XDM_SUAP-AU-S-001-O
XDM_SUAP-SEC-S-001-O	Support default Authorization policy for accessing a Subscriber defined User Access Policy Document (XDMv2.1)	5.2.11	XDM_SUAP-AU-S-001-O AND XDM_Core-SEC-S-001-M

Item	Function	Reference	Requirement
XDM_SUAP-SEC-S-002-O	Support Authorization policies defined in an Access Permissions Document governing access to a Subscriber defined User Access Policy Document (XDMv2.1)	5.2.11	XDM_SUAP-AU-S-001-O AND XDM_Core-SEC-S-002-O
XDM_SUAP-SUB-S-001-O	Support Subscribing to changes in User Access Policy Document (XDMv2.1)	5.2.12	XDM_SUAP-AU-S-001-O AND XDM_Core-SUB-S-001-O AND XDM_Core-SUB-S-002-O
XDM_SUAP-PRF-S-001-O	Support XDM Preferences Document (XDMv2.1)	5.2.14	XDM_Core-PRF-S-001-O AND XDM_SUAP-AU-S-001-O AND (XDM_SUAP-FWD-S-001-O OR XDM_SUAP-MHI-S-001-O OR XDM_SUAP-RHI-S-001-O)
XDM_SUAP-MHI-S-001-O	Support Modification History Information Document (XDMv2.1)	5.2.15	XDM_SUAP-AU-S-001-O AND XDM_Core-MHI-S-001-M
XDM_SUAP-RHI-S-001-O	Support Request History Information Document (XDMv2.1)	5.2.15	XDM_SUAP-AU-S-001-O AND XDM_Core-RHI-S-001-O
XDM_SUAP-RES-S-001-O	Support Restore of Subscriber defined User Access Policy Document (XDMv2.1)	5.2.17	XDM_SUAP-AU-S-001-O AND XDM_Core-RES-S-001-O
XDM_SUAP-REF-S-001-O	Support Document Reference of Subscriber defined User Access Policy Document (XDMv2.1)	5.2.18	XDM_SUAP-AU-S-001-O AND XDM_Core-REF-S-001-O
XDM_SUAP-DIFF-S-001-O	Support Differential Read in Subscriber defined User Access Policy Document (XDMv2.1)	5.2.19	XDM_SUAP-AU-S-001-O AND XDM_Core-DIFF-S-001-O

B.2 Policy XDM Application Usages (XDMC)

Item	Function	Reference	Requirement
XDM_UAP-AU-C-001-O	Support for User Access Policy Application Usage (XDMv2.0)	5.1	XDM_UAP-AU-C-002-O AND XDM_UAP-AU-C-003-O AND XDM_UAP-AU-C-004-O AND XDM_UAP-AU-C-005-O AND XDM_UAP-AU-C-006-O AND XDM_UAP-AU-C-007-O AND XDM_UAP-AU-C-008-O
XDM_UAP-AU-C-002-O	Support User Access Policy Document structure (XDMv2.0)	5.1.1	XDM_Core-XOP-C-003-M AND XDM_UAP-AU-C-001-O
XDM_UAP-AU-C-003-O	Support Application Unique ID in User Access Policy Application Usage (XDMv2.0)	5.1.2	XDM_UAP-AU-C-001-O
XDM_UAP-AU-C-004-O	Support XML schema User Access Policy Document (XDMv2.0)	5.1.3	XDM_UAP-AU-C-001-O
XDM_UAP-AU-C-005-O	User Access Policy conforms to MIME type	5.1.5	XDM_UAP-AU-C-001-O
XDM_UAP-AU-C-006-O	Validation constraints, in addition to the XML schema	5.1.6	XDM_UAP-AU-C-001-O
XDM_UAP-AU-C-007-O	Data semantics of User Access Policy	5.1.7	XDM_UAP-AU-C-001-O
XDM_UAP-AU-C-008-O	Support Naming conventions of User Access Policy Document (XDMv2.0)	5.1.8	XDM_UAP-AU-C-001-O
XDM_UAP-ERR-C-001-O	Support handling of HTTP "409 Conflict" response from the XDMS (XDMv2.0)	5.1.6	XDM_UAP-AU-C-001-O

Item	Function	Reference	Requirement
XDM_UAP-SEC-C-001-O	Support Access Permissions Document (XDMv2.1)	5.1.11	XDM_UAP-AU-C-001-O AND XDM_Core-SEC-C-006-O
XDM_UAP-SUB-C-001-O	Support Subscribing to changes in User Access Policy Document (XDMv2.0)	5.1.12	XDM_UAP-AU-C-001-O AND XDM_Core-SUB-C-001-O AND XDM_Core-SUB-C-002-O
XDM_UAP-SUB-C-002-O	Support Subscribing to changes in User Access Policy Document using XDCP (XDMv2.1)	5.1.12	XDM_UAP-AU-C-001-O AND XDM_Core-SUB-C-003-O
XDM_UAP-SRC-C-001-O	Support Search in Modification History Information (XDMv2.1)	5.1.13	XDM_UAP-AU-C-001-O AND XDM_Core-SRC-C-004-O
XDM_UAP-SRC-C-002-O	Support Search in Request History Information (XDMv2.1)	5.1.13	XDM_UAP-AU-C-001-O AND XDM_Core-SRC-C-005-O
XDM_UAP-PRF-C-001-O	Support XDM Preferences Document(XDMv2.1)	5.1.14	XDM_UAP-AU-C-001-O AND XDM_Core-PRF-C-001-O
XDM_UAP-MHI-C-001-O	Support Modification History Document (XDMv2.1)	5.1.15	XDM_UAP-AU-C-001-O AND XDM_Core-MHI-C-001-O
XDM_UAP-RHI-C-001-O	Support Request History Document (XDMv2.1)	5.1.15	XDM_UAP-AU-C-001-O AND XDM_Core-RHI-C-001-O
XDM_UAP-RES-C-001-O	Support Restore of User Access Policy Document (XDMv2.1)	5.1.17	XDM_UAP-AU-C-001-O AND XDM_Core-RES-C-001-O
XDM_UAP-REF-C-001-O	Support Document Reference of User Access Policy Document (XDMv2.1)	5.1.18	XDM_UAP-AU-C-001-O AND XDM_Core-REF-C-001-O
XDM_UAP-DIFF-C-001-O	Support Differential Read of User Access Policy Document (XDMv2.1)	5.1.19	XDM_UAP-AU-C-001-O AND XDM_Core-DIFF-C-001-O
XDM_UAP-DIFF-C-001-O	Support Differential Write of User Access Policy Document(XDMv2.1)	5.1.19	XDM_UAP-AU-C-001-O AND XDM_Core-DIFF-C-003-O
XDM_SUAP-AU-C-001-O	Support Subscriber defined User Access Policy Application Usage (XDMv2.1)	5.2	XDM_SUAP-AU-S-002-O AND XDM_SUAP-AU-S-003-O AND XDM_SUAP-AU-S-004-O AND XDM_SUAP-AU-S-005-O AND XDM_SUAP-AU-S-006-O AND XDM_SUAP-AU-S-007-O AND XDM_SUAP-AU-S-008-O AND XDM_SUAP-AU-S-009-O
XDM_SUAP-AU-C-002-O	Support Subscriber defined User Access Policy Document structure (XDMv2.1)	5.2.1	XDM_SUAP-AU-S-001-O AND XDM_Core -XCAP-S-001-M
XDM_SUAP-AU-C-003-O	Support Application Unique ID in Subscriber defined User Access Policy Application Usage (XDMv2.1)	5.2.2	XDM_SUAP-AU-S-001-O
XDM_SUAP-AU-C-004-O	Support XML schema of Subscriber defined User Access Policy Document (XDMv2.1)	5.2.3	XDM_SUAP-AU-S-001-O
XDM_SUAP-AU-C-005-O	Support MIME type of Subscriber defined User Access Policy (XDMv2.1)	5.2.5	XDM_SUAP-AU-S-001-O
XDM_SUAP-AU-C-006-O	Support Validation constraints of Subscriber defined User Access Policy Document (XDMv2.1)	5.2.6	XDM_SUAP-AU-S-001-O
XDM_SUAP-AU-C-007-O	Support Data semantics of Subscriber defined User Access Policy Document (XDMv2.1)	5.2.7	XDM_SUAP-AU-S-001-O
XDM_SUAP-AU-C-008-O	Support Naming conventions for Subscriber defined User Access Policy Application Usage (XDMv2.1)	5.2.8	XDM_SUAP-AU-S-001-O

Item	Function	Reference	Requirement
XDM_SUAP-SEC-C-001-O	Support Access Permissions Document (XDMv2.1)	5.2.11	XDM_SUAP-AU-S-001-O
XDM_SUAP-SUB-C-001-O	Support Subscribing to changes in Subscriber defined User Access Policy Document using SIP (XDMv2.1)	5.2.12	XDM_SUAP-AU-C-001-O AND XDM_Core-SUB-C-001-O AND XDM_Core-SUB-C-002-O
XDM_SUAP-SUB-C-002-O	Support Subscribing to changes in Subscriber defined User Access Policy Document using XDCP (XDMv2.1)	5.2.12	XDM_SUAP-AU-C-001-O AND XDM_Core-SUB-C-003-O
XDM_UAP-SRC-C-001-O	Support Search in Modification History Information (XDMv2.1)	5.2.13	XDM_SUAP-AU-C-001-O AND XDM_Core-SRC-C-004-O
XDM_UAP-SRC-C-002-O	Support Search in Request History Information (XDMv2.1)	5.2.13	XDM_SUAP-AU-C-001-O AND XDM_Core-SRC-C-005-O
XDM_SUAP-PRF-C-001-O	Support XDM Preferences Document(XDMv2.1)	5.2.14	XDM_SUAP-AU-C-001-O AND XDM_Core-PRF-C-001-O
XDM_SUAP-MHI-C-001-O	Support Modification History Document (XDMv2.1)	5.2.15	XDM_SUAP-AU-C-001-O AND XDM_Core-MHI-C-001-O
XDM_SUAP-RHI-C-001-O	Support Request History Document (XDMv2.1)	5.2.15	XDM_SUAP-AU-C-001-O AND XDM_Core-RHI-C-001-O
XDM_SUAP-RES-C-001-O	Support Restore of Subscriber defined User Access Policy Document (XDMv2.1)	5.2.17	XDM_SUAP-AU-C-001-O AND XDM_Core-RES-C-001-O
XDM_SUAP-REF-C-001-O	Support Document Reference of Subscriber defined User Access Policy Document (XDMv2.1)	5.2.18	XDM_SUAP-AU-C-001-O AND XDM_Core-REF-C-001-O
XDM_SUAP-DIFF-C-001-O	Support Differential Read of Subscriber defined User Access Policy Document (XDMv2.1)	5.2.19	XDM_SUAP-AU-C-001-O AND XDM_Core-DIFF-C-001-O
XDM_SUAP-DIFF-C-001-O	Support Differential Write of Subscriber defined User Access Policy Document (XDMv2.1)	5.2.19	XDM_SUAP-AU-C-001-O AND XDM_Core-DIFF-C-003-O

B.3 Policy XDM Application Usages (XDM Agent)

Item	Function	Reference	Requirement
XDM_UAP-AU-A-001-O	Support User Access Policy Application Usage (XDMv2.0)	5.1	XDM_UAP-AU-A-002-O AND XDM_UAP-AU-A-003-O AND XDM_UAP-AU-A-004-O AND XDM_UAP-AU-A-005-O AND XDM_UAP-AU-A-006-O AND XDM_UAP-AU-A-007-O AND XDM_UAP-AU-A-008-O
XDM_UAP-AU-A-002-O	Support User Access Policy Document structure (XDMv2.0)	5.1.1	XDM_Core-XOP-A-003-M AND XDM_UAP-AU-A-001-O
XDM_UAP-AU-A-003-O	Support Application Unique ID in User Access Policy Application Usage (XDMv2.0)	5.1.2	XDM_UAP-AU-A-001-O
XDM_UAP-AU-A-004-O	Support XML schema User Access Policy Document (XDMv2.0)	5.1.3	XDM_UAP-AU-A-001-O
XDM_UAP-AU-A-005-O	Support MIME type of User Access Policy Document (XDMv2.0)	5.1.5	XDM_UAP-AU-A-001-O
XDM_UAP-AU-A-006-O	Support Validation constraints of User Access Policy Document (XDMv2.0)	5.1.6	XDM_UAP-AU-A-001-O

Item	Function	Reference	Requirement
XDM_UAP-AU-A-007-O	Support Data semantics of User Access Policy Document (XDMv2.0)	5.1.7	XDM_UAP-AU-A-001-O
XDM_UAP-AU-A-008-O	Support Naming conventions for User Access Policy Document (XDMv2.0)	5.1.8	XDM_UAP-AU-A-001-O
XDM_UAP-ERR-A-001-O	Support handling of HTTP "409 Conflict" response from the XDMS (XDMv2.0)	5.1.6	XDM_UAP-AU-A-001-O
XDM_UAP-SEC-A-001-O	Support Access Permissions Document (XDMv2.1)	5.1.11	XDM_UAP-AU-A-001-O AND XDM_Core-SEC-A-006-O
XDM_UAP-SUB-A-001-O	Support Subscribing to changes in User Access Policy Document using SIP (XDMv2.1)	5.1.12	XDM_UAP-AU-A-001-O AND XDM_Core-SUB-A-001-O AND XDM_Core-SUB-A-002-O
XDM_UAP-SRC-A-001-O	Support Search in Modification History Information (XDMv2.1)	5.1.13	XDM_UAP-AU-A-001-O AND XDM_Core-SRC-A-004-O
XDM_UAP-SRC-A-002-O	Support Search in Request History Information (XDMv2.1)	5.1.13	XDM_UAP-AU-A-001-O AND XDM_Core-SRC-A-005-O
XDM_UAP-PRF-A-001-O	Support XDM Preferences Document (XDMv2.1)	5.1.14	XDM_UAP-AU-A-001-O AND XDM_Core-PRF-A-001-O
XDM_UAP-MHI-A-001-O	Support Modification History Document (XDMv2.1)	5.1.15	XDM_UAP-AU-A-001-O AND XDM_Core-MHI-A-001-O
XDM_UAP-RHI-A-001-O	Support Request History Document (XDMv2.1)	5.1.15	XDM_UAP-AU-A-001-O AND XDM_Core-RHI-A-001-O
XDM_UAP-RES-A-001-O	Support Restore of User Access Policy Document (XDMv2.1)	5.1.17	XDM_UAP-AU-A-001-O AND XDM_Core-RES-A-001-O
XDM_UAP-REF-A-001-O	Support Document Reference of User Access Policy Document (XDMv2.1)	5.1.18	XDM_UAP-AU-A-001-O AND XDM_Core-REF-A-001-O
XDM_UAP-DIFF-A-001-O	Support Differential Read of User Access Policy Document (XDMv2.1)	5.1.19	XDM_UAP-AU-A-001-O AND XDM_Core-DIFF-A-001-O
XDM_UAP-DIFF-A-001-O	Support Differential Write of User Access Policy Document (XDMv2.1)	5.1.19	XDM_UAP-AU-A-001-O AND XDM_Core-DIFF-A-003-O
XDM_SUAP-AU-A-001-O	Support for Subscriber defined User Access Policy Application Usage (XDMv2.1)	5.2	XDM_SUAP-AU-S-002-O AND XDM_SUAP-AU-S-003-O AND XDM_SUAP-AU-S-004-O AND XDM_SUAP-AU-S-005-O AND XDM_SUAP-AU-S-006-O AND XDM_SUAP-AU-S-007-O AND XDM_SUAP-AU-S-008-O AND XDM_SUAP-AU-S-009-O
XDM_SUAP-AU-A-002-O	Support Subscriber defined User Access Policy Document structure (XDMv2.1)	5.2.1	XDM_SUAP-AU-S-001-O AND XDM_Core-XOP-S-001-M
XDM_SUAP-AU-A-003-O	Support Application Unique ID in Subscriber defined User Access Policy Application Usage(XDMv2.1)	5.2.2	XDM_SUAP-AU-S-001-O
XDM_SUAP-AU-A-004-O	Support XML schema of Subscriber defined User Access Policy Document (XDMv2.1)	5.2.3	XDM_SUAP-AU-S-001-O
XDM_SUAP-AU-A-005-O	Support Subscriber defined User Access Policy Document(XDMv2.1)	5.2.5	XDM_SUAP-AU-S-001-O
XDM_SUAP-AU-A-006-O	Support Validation constraints of Subscriber defined User Access Policy Document (XDMv2.1)	5.2.6	XDM_SUAP-AU-S-001-O
XDM_SUAP-AU-A-007-O	Support Data semantics of Subscriber defined User Access Policy Document (XDMv2.1)	5.2.7	XDM_SUAP-AU-S-001-O

Item	Function	Reference	Requirement
XDM_SUAP-AU-A-008-O	Support Naming conventions for Subscriber defined User Access Policy Document(XDMv2.1)	5.2.8	XDM_SUAP-AU-S-001-O
XDM_SUAP-SEC-A-001-O	Support Access Permissions Document (XDMv2.1)	5.2.11	XDM_SUAP-AU-A-001-O AND XDM_Core-SEC-A-006-O
XDM_SUAP-SUB-A-001-O	Support Subscribing to changes in Subscriber defined User Access Policy Document using SIP (XDMv2.1)	5.2.12	XDM_SUAP-AU-A-001-O AND XDM_Core-SUB-A-001-O AND XDM_Core-SUB-A-002-O
XDM_SUAP-SRC-A-001-O	Support Search in Modification History Information (XDMv2.1)	5.2.13	XDM_SUAP-AU-A-001-O AND XDM_Core-SRC-A-004-O
XDM_SUAP-SRC-A-002-O	Support Search in Request History Information (XDMv2.1)	5.2.13	XDM_SUAP-AU-A-001-O AND XDM_Core-SRC-A-005-O
XDM_SUAP-PRF-A-001-O	Support XDM Preferences Document (XDMv2.1)	5.2.14	XDM_SUAP-AU-A-001-O AND XDM_Core-PRF-A-001-O
XDM_SUAP-MHI-A-001-O	Support Modification History Document (XDMv2.1)	5.2.15	XDM_SUAP-AU-A-001-O AND XDM_Core-MHI-A-001-O
XDM_SUAP-RHI-A-001-O	Support Request History Document (XDMv2.1)	5.2.15	XDM_SUAP-AU-A-001-O AND XDM_Core-RHI-A-001-O
XDM_SUAP-RES-A-001-O	Support Restore of Subscriber defined User Access Policy Document (XDMv2.1)	5.2.17	XDM_SUAP-AU-A-001-O AND XDM_Core-RES-A-001-O
XDM_SUAP-REF-A-001-O	Support Document Reference of Subscriber defined User Access Policy Document of (XDMv2.1)	5.2.18	XDM_SUAP-AU-A-001-O AND XDM_Core-REF-A-001-O
XDM_SUAP-DIFF-A-001-O	Support Differential Read of Subscriber defined User Access Policy Document (XDMv2.1)	5.2.19	XDM_SUAP-AU-A-001-O AND XDM_Core-DIFF-A-001-O
XDM_SUAP-DIFF-A-001-O	Support Differential Write of Subscriber defined User Access Policy Document (XDMv2.1)	5.2.19	XDM_SUAP-AU-A-001-O AND XDM_Core-DIFF-A-003-O

B.4 Aggregation Proxy

Item	Function	Reference	Requirement
XDM_UAP-BC-S-002-M	Support Backward compatibility Procedures at the Aggregation Proxy (XDMv2.0)	7.2	

Appendix C. Examples

(Informative)

C.1 User Access Policy Document Structure

1) Following table shows the sample structure of a User Access Policy Document of Ronald (“sip:ronald.underwood@example.com”) containing the following policies:

- For the IM Service Ronald wants to reject all the incoming request except for Pager Mode Message from the user whose address is sip:percy.underwood@example.com or “tel:+43012349999”
- Reject all the Anonymous Request
- Reject Group Advertisements
- Route all PoC communication requests from users except Alice to the Offline Storage if Ronald is offline.
- Auto Answer is enabled for the PoC communication requests received from the users listed in PoC Buddy List.

```
<?xml version="1.0" encoding="UTF-8"?>
<ruleset xmlns="urn:ietf:params:xml:ns:common-policy"
  xmlns:ocp="urn:oma:xml:xdm:common-policy"
  xmlns:oxe="urn:oma:xml:xdm:extensions"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <rule id="f3g44r1">
    <conditions>
      <identity>
        <one id="tel:+43012349999"/>
        <one id="sip:percy.underwood@example.com"/>
      </identity>
      <oxe:media-list>
        <oxe:all-media-except>
          <oxe:pager-mode-message/>
        </oxe:all-media-except>
      </oxe:media-list>
      <oxe:service-list>
        <oxe:service enabler="im"/>
      </oxe:service-list>
    </conditions>
    <actions>
      <oxe:allow-reject-invite>true</oxe:allow-reject-invite>
    </actions>
  </rule>
  <rule id="ythk764">
    <conditions>
      <ocp:anonymous-request/>
    </conditions>
    <actions>
      <oxe:allow-reject-invite>true</oxe:allow-reject-invite>
    </actions>
  </rule>
  <rule id="ythk780">
    <conditions>
      <oxe:media-list>
        <oxe:group-advertisement/>
      </oxe:media-list>
    </conditions>
    <actions>
      <oxe:allow-reject-invite>true</oxe:allow-reject-invite>
    </actions>
  </rule>
  <rule id="ythk790">
    <conditions>
      <identity>
        <many>
```



```
        <except id="sip:alice@example.com" />
    </many>
</identity>
<oxe:service-list>
    <oxe:service enabler="poc" />
</oxe:service-list>
</conditions>
<actions>
    <oxe:allow-offline-storage>true</oxe:allow-offline-storage>
</actions>
</rule>
<rule id="ythk7000">
    <conditions>
        <ocp:external-list>
            <ocp:entry anc="http://xcap.example.com/resource-
                lists/users/sip:ronald.underwood@example.com/index/~/resource-
                list/list%5B@name=%22oma_pocbuddylist%22%5D" />
        </ocp:external-list>
        <oxe:service-list>
            <oxe:service enabler="poc" />
        </oxe:service-list>
    </conditions>
    <actions>
        <oxe:allow-auto-answermode>true</oxe:allow-auto-answermode>
    </actions>
</rule>>
</ruleset>
```