Shared Policy XDM Specification

Candidate Version 1.0 – 24 Jul 2007

Open Mobile Alliance

OMA-TS-XDM_Shared_Policy-V1_0-20070724-C

Contents

Figures

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 and IM).

2. References

2.1 Normative References

[Dict] "Dictionary for OMA Specifications", Version 2.4, Open Mobile Alliance™, OMA-ORG-Dictionary-V2_4, URL: http://www.openmobilealliance.org

[PoC_XDM-V1_0] "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

[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

[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/

[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/

2.2 Informative References

[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 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])
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 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])
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.
Node Selector	A sequence of path segments, with each segment being separated by a "/", that identify the XML node (element or attribute) being selected within a document. (Source: [RFC4825])
Node Selector Separator	A single path segment equal to two tilde characters "~~" that is used to separate the document selector from the Node Selector within an HTTP URI. (Source: [RFC4825])
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])
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	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])
URI List	A list of URIs.
User	A User is any entity that uses the described features through the User Equipment.
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 this specification. (Source: [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 Engireering Task Force
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-V1_0].

The Shared 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 Shared 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]).

5. Shared Policy XDM Application Usages

5.1 User Access Policy

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 <anonymous-request> element, as defined in [XDM_Core] "*Common Extensions*" ;

e) MAY include the <media-list> element, as defined in [XDM_Core] "*Common Extensions*";

f) MAY include the <service-list> element, as defined in [XDM_Core] "*Common Extensions*" and

g) 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 and

e) 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] 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 Shared 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 shared 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, the Shared 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 shared 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.

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.

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 be defined according to [XDM_Core] *“Authorization”*.

6. Subscribing to changes in the XML documents

The Shared Policy 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. Backward Compatibility towards the PoC User Access Policy Application Usage

7.1 Procedures at the Shared Policy XDMS

If the Shared Policy XDMS allows access by PoCv1.0 Clients, the Shared 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 Shared 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 syncronized as described below.

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

The Shared 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:

1) 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:

   a. SHALL contain the <allow-reject-invite> action set to "true"; and

   b. SHALL NOT contain the <allow-auto-answermode> action.

2) 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:

   a. SHALL contain the <allow-auto-answermode> action set to "true"; and

   b. SHALL NOT contain the <allow-reject-invite> action.

3) 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

   a. SHALL NOT contain the <allow-auto-answermode> action; and

   b. SHALL NOT contain the <allow-reject-invite> action.

The Shared 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:

1) 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;

2) 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";

3) 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";

4) 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 Shared 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 Shared 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 Shared Policy XDMS based on local configuration.

NOTE: An Aggregation Proxy forwards XCAP requests for the PoC User Access Policy AUID to the Shared 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 1.0 History

Document Identifier	Date	Sections	Description
Draft Versions OMA-TS-Shared_Policy_XDM-V1_0	13 Dec 2006	First draft	
	05 Feb 2007	various	Incorporated CRs: OMA-PAG-2007-0025 OMA-PAG-2007-0045R01
	15 Feb 2007	5.1.1, 5.1.5, 5.1.7, 5.1.8, 5.1.11, 6	Incorporated CRs: OMA-PAG-2007-0094 OMA-PAG-2007-0096
	04 Apr 2007	2.1, 6, B, B.1, B.2	Incorporated CRs: OMA-PAG-2007-0147R02 OMA-PAG-2007-0178
	25 Apr 2007	2.1, 3.2, 4, 5.1.1, 5.1.3, 5.1.4, 5.1.5, 5.1.7, 7, 7.1, 7.2, B.1, B.3, C	Incorporated CRs: OMA-PAG-2007-0109R06 OMA-PAG-2007-0171R02 OMA-PAG-2007-0201R01 OMA-PAG-2007-0230R01 OMA-PAG-2007-0275
	10 May 2007	5.1.1, 5.1.3, 5.1.7, 7.1, C.1.1	Incorporated CRs: OMA-PAG-2007-0288R03 OMA-PAG-2007-0303R01
	06 Jun 2007	2.1, 5.1.1, 5.1.3, 5.1.7	Incorporated CRs: OMA-PAG-2007-0333R02 OMA-PAG-2007-0325R01 OMA-PAG-2007-0342 OMA-PAG-2007-0347R01
	14 Jun 2007	2.2, 4, B.1, B.2, B.3, C.1.1	Incorporated CRs: OMA-PAG-2007-0403 OMA-PAG-2007-0460R01 OMA-PAG-2007-0476
Candidate Version OMA-TS-Shared_Policy-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 SCRs [SCRRULES] defined in the following tables include SCRs for:

- Shared User Access XDM Application Usage

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 Policy XDM Application Usages (Server)

Item	Function	Reference	Requirement
XDM_Policy-XOP-S-001-M	Shared User Access Policy structure (XDMv2.0)	5.1.1	XDM_Core -XCAP-S-001-M
XDM_Policy-XOP-S-002-M	Application Unique ID in Shared User Access Policy (XDMv2.0)	5.1.2	
XDM_Policy-XOP-S-003-M	XML schema of Shared User Access Policy (XDMv2.0)	5.1.3	
XDM_Policy-XOP-S-004-M	Shared User Access Policy conforms to MIME type (XDMv2.0)	5.1.5	
XDM_Policy-XOP-S-005-M	Validation constraints, in addition to the XML schema (XDMv2.0)	5.1.6	
XDM_Policy-XOP-S-006-M	Data semantics of Shared User Access Policy (XDMv2.0)	5.1.7	
XDM_Policy-XOP-S-007-M	Naming conventions for Shared User Access Policy (XDMv2.0)	5.1.8	
XDM_Policy-XOP-S-008-M	Authorization policies (XDMv2.0)	5.1.11	
XDM_Policy-SUB-S-001-M	Subscribing to changes in Shared Access Policy documents (XDMv2.0)	6	XDM_Core -SUB-S-001-O AND XDM_Core -SUB-S-002-O
XDM_Policy-BC-S-001-M	Backward compatibility PoC User Access Policy Application Usage.	7.1	

B.2 Shared Policy XDM Application Usages (Client)

Item	Function	Reference	Requirement
XDM_Policy-XOP-C-001-O	Shared User Access Policy Application Usage (XDMv2.0)	5.1	XDM_Policy-XOP-C-002-O AND XDM_Policy-XOP-C-003-O AND XDM_Policy-XOP-C-004-O AND XDM_Policy-XOP-C-005-O AND XDM_Policy-XOP-C-006-O AND XDM_Policy-XOP-C-007-O AND XDM_Policy-XOP-C-008-O
XDM_Policy-XOP-C-002-O	Shared User Access Policy structure (XDMv2.0)	5.1.1	XDM_Core-XOP-C-003-M AND XDM_Policy-XOP-C-001-O
XDM_Policy-XOP-C-003-O	Application Unique ID in Shared User Access Policy (XDMv2.0)	5.1.2	XDM_Policy-XOP-C-001-O
XDM_Policy-XOP-C-004-O	XML schema Shared User Access Policy (XDMv2.0)	5.1.3	XDM_Policy-XOP-C-001-O

Item	Function	Reference	Requirement
XDM_Policy-XOP-C-005-O	Shared User Access Policy conforms to MIME type (XDMv2.0)	5.1.5	XDM_Policy-XOP-C-001-O
XDM_Policy-XOP-C-006-O	Validation constraints, in addition to the XML schema (XDMv2.0)	5.1.6	XDM_Policy-XOP-C-001-O
XDM_Policy-XOP-C-007-O	Data semantics of Shared User Access Policy (XDMv2.0)	5.1.7	XDM_Policy-XOP-C-001-O
XDM_Policy-XOP-C-008-O	Naming conventions for Shared User Profile (XDMv2.0)	5.1.8	XDM_Policy-XOP-C-001-O
XDM_Policy-ERR-C-001-O	XDM Client handling of HTTP "409 Conflict" response from the XDMS (XDMv2.0)	5.1.6	XDM_Policy-XOP-C-001-O

B.3 Aggregation Proxy

Item	Function	Reference	Requirement
XDM_Policy-BC-S-002-M	Backward compatibility Procedures at the Aggregation Proxy.	7.2	

Appendix C. Examples (Informative)

C.1 Manipulating User Access Policy

C.1.1 Obtaining User Access Policy document

Figure C.1 describes how the XDMC obtains the User Access Policy document. In this example, the XDMC is residing in a UE in the same domain as the Shared Policy XDMS. It is also assumed that the address of the Aggregation Proxy is "xcap.example.com" and the XCAP Root URI is "xcap.example.com/".

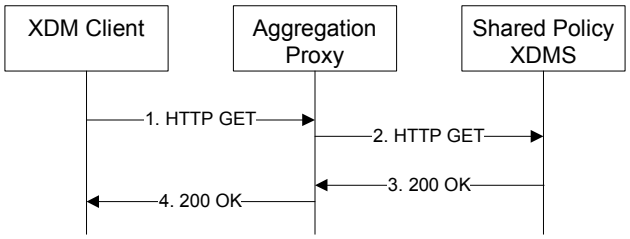

Figure C.1- XDM Client obtains User Access Policy document

The details of the flows are as follows:

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

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

where the filename "access-rules" is a standardized naming convention (see section 5.1.8).

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

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

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

<?xml version="1.0" encoding="UTF-8"?>
<ruleset xmlns="urn:ietf:params:xml:ns:common-policy"
         xmlns:ocp="urn:oma:xml:xdm:common-policy "
         xmlns:oxe="urn:oma:xml:xdm:xdm2-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>
```

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