XML Document Management Requirements

Approved Version 2.0 – 03 Apr 2012

Open Mobile Alliance

OMA-RD-XDM-V2_0-20120403-A

Contents

Tables

1. Scope (Informative)

This document describes use cases and requirements for the management of information (e.g., URI Lists) that are stored as documents using an extensible and platform-neutral format that could be used by other OMA service enablers. Therefore, the requirements contained in this document are limited to these aspects (i.e., the storage, management and re-use of such documents containing information by other applications).

The privacy of personal data, such as, principal identity is protected according to privacy regulations. However, mechanisms to obtain the permission of principal (e.g., before they are included in lists that are managed by the XDM enabler) are out of scope.

The XDM enabler provides mechanisms for principals to specify who can access the data they have stored.

In addition, the owner of a XDM enabler deployment has full access to this data (overriding any principal preferences) for purposes, such as, administration and maintenance. The application of those administrative rights in relation to principal preferences may be described in legal or contractual policies, and as such is out of scope for this enabler.

The XDM enabler is designed to support other OMA service enablers and applications. It is envisioned that there will be multiple enabler specifications to satisfy the requirements in this document.

2. References

2.1 Normative References

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

[Privacy_Req] "OMA Privacy Requirements for Mobile Services", Open Mobile Alliance™, 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

[RFC2396] IETF RFC 2396 "Uniform Resource Identifiers (URI): Generic Syntax", T. Berners-Lee et al, August 1998, URL: http://www.ietf.org/rfc/rfc2396.txt

[RFC3261] IETF RFC 3261 "SIP: Session Initiation Protocol", J. Rosenberg, et al, June 2002, URL: http://www.ietf.org/rfc/rfc3261.txt

[XDM_RD-V1_1] "XML Document Management Requirements", Version 1.1, Open Mobile Alliance™, OMA-RD-XDM-V1_1, URL: http://www.openmobilealliance.org/

2.2 Informative References

[IM_RD] "Instant Messaging using SIMPLE Requirements", Version 1.0, Open Mobile Alliance™, OMA-RD-IM-V1_0, URL: http://www.openmobilealliance.org/

[PoC_RD-V1_0] "Push to Talk over Cellular Requirements, Version 1.0, Open Mobile Alliance™, OMA-RD-PoC-V1_0, URL: http://www.openmobilealliance.org/

[PoC_RD-V2_0] "Push to Talk over Cellular 2 Requirements", Version 2.0, Open Mobile Alliance™, OMA-RD-PoC-V2_0, URL: http://www.openmobilealliance.org/

[PRS_RD-V1_1] "Presence SIMPLE Requirements", Version 1.1, Open Mobile Alliance™, OMA-RD-Presence_SIMPLE-V1_1, URL: http://www.openmobilealliance.org/

[PRS_RD-V2_0] "OMA Presence SIMPLE 2.0 Requirements", Version 2.0, Open Mobile Alliance™, OMA-RD-Presence_SIMPLE-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

Access Control Policy	A set of lists (e.g., access control lists, such as, accept/reject lists) and associated rules on how they apply to incoming requests.
Access Permissions	A set of rules that defines which Principals have rights to perform which XDM functions on a specific document
Client	A device, user agent, or other entity that acts as the receiver of a service. (Source: [Dict])
Group	A Group is a predefined set of Users together with its policies and attributes. A Group is identified by a SIP URI.
Group Usage List	A list of group names or service URIs that are known by an XCAP Client
Law Enforcement Agency	A lawfully authorized organization conducting lawful interception.
Lawful Interception	The legal authorization, process, and associated technical capabilities and activities of Law Enforcement Agencies related to the timely interception of signalling and content of wire, oral, or electronic communications.
Primary Principal	The Primary Principal is the user associated with the XCAP User Identity, which defines where the document resides.
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])
Service Provider	A legal or administrative entity that provides a service to its clients or customers. Typically it is (but is not restricted to) a network operator
Shared Group	A Group which can be used by multiple service enablers/applications.
Shared URI List	A URI List that can be used by multiple service enablers/applications.
Shared User Profile	A User Profile that can be used by multiple service enablers/applications.
Subscription Authorisation Policy	An example of access control policy for Presence, which specifies whether a particular watcher (i.e. principal) is authorised to subscribe to a certain set of events.
URI List	A collection of URIs put together for convenience.
User	An entity which uses services. Example: a person using a device as a portable telephone. (Source [Dict])

3.3 Abbreviations

CS	Circuit Switched
GUI	Graphical User Interface
IM	Instant Messaging
LI	Lawful Interception
MSISDN	Mobile Subscriber ISDN number (as defined by the E.164 numbering plan).
OMA	Open Mobile Alliance
P2P	Peer to Peer
PoC	Push to Talk over Cellular
PSL	Presence Subscription List
RD	Requirements Document
RFC	Request For Comments
SIP	Session Initiation Protocol.
SMS	Short Messaging Service
UE	User Equipment
UI	User Interface
URI	Uniform Resource Identifier.
VoIP	Voice Over IP
XDM	XML Document Management
XML	Extensible Markup Language.

4. Introduction (Informative)

Various OMA enablers such as, Presence, Push to Talk Over Cellular (PoC), Instant Messaging (IM), etc. need support for access to and manipulation of certain information that are needed by these enablers. Some examples of such information (whose semantics and syntax are outside the scope of the XDM enabler) include:

- *PoC Group*: the list of PoC participants who can take part in a PoC session as well as additional PoC-specific properties such as auto-answering incoming PoC call requests, etc.
- *PoC Accept/Reject List*: the lists of PoC callers who are allowed/not allowed to call a given user
- *Presence List*: a list of users who are potential presentities, so that this list can be used to collectively subscribe to the presence status of each member in that list
- *Subscription Authorisation Policy*: An example of an access control policy for Presence, which specifies whether a particular watcher (i.e., principal) is authorized to subscribe to a certain set of events.
- *IM Contact List*: the list of individuals which are grouped together by an end user for IM, e.g. Friends, Family, Business, also referred to as 'buddy list',
- *IM Group*: a defined set of IM participants amongst whom an IM session may take place or who may participate in a chat session
- *IM Access Control*: IM user specified rules that restrict the set of other users that may establish IM conversations to the user

The XDM requirements derive to some extent from the Requirement Documents of Presence ([PRS_RD-V1_1] and [PRS_RD-V2_0]), Push-to-Talk ([PoC_RD-V1_0] and [PoC_RD-V2_0]) and Instant Messaging ([IM_RD]). Please refer to the appropriate documentation for more information.

Notice from these examples that such information is not always pure lists (of principals), but can be a combination of lists together with other properties that define an end-user's personalization of the service behaviour. The enablers specify the items that make up the documents representing the information in the examples above, including their semantics and usage. Over time, it is expected that other OMA enablers will define other types of documents needed for their operation.

To make such information accessible to the enablers that need them, the information is expected to be stored in the network where it can be located, accessed and manipulated (created, changed, deleted) by authorised principals. To this end, the OMA is expected to specify the use of an extensible and neutral format (e.g., XML) by which such information will be defined, as well as the common protocol for access and manipulation of such information, represented as XML documents, by authorized principals.

The XDM enabler specifies documents that can be shared by multiple enablers. One such case is a particular type of list, the URI List, which is a convenient way for a principal to group together a number of end users (e.g., "Friends" or "Family) or other resources, where such a list is expected to be reused for a number of different enablers. Such a list can be re-used wherever a principal has a need to collectively refer to a group of other end users or resources.

Thus, it is envisaged that the XDM RD would result in multiple specifications. One specification will define a protocol that could be used by any enabler or end-user to manipulate documents containing information pertaining to that enabler or end-user. Another specification would define certain types of shared information (e.g., URI lists) that can be stored, retrieved, and re-used by multiple enablers. It is expected that other enablers will define the document structure needed for their information as part of their enabler specification.

5. Use Cases (Informative)

The use cases are separated into two parts to identify the generic and the service specific set of XDM functionality.

Functions like "Access Control, Addressing, Copy, Create, Delete, Management of Members and Modify Group Properties" need to be referenced by the use cases.

5.1 Generic Use Cases

The generic use cases define the behaviour, information elements and actors that are common for all services using XDM.

5.1.1 Use Case - URI List

See [XDM_RD-V1_1] "*URI List*".

5.1.2 Use Case - Subscribing for Presence of End-users in a URI List

See [XDM_RD-V1_1] "*Subscribing for Presence of End-users in a URI List*".

5.1.3 Use Case – Groups

See [XDM_RD-V1_1] "*Groups*".

5.1.4 Use Case - P2P Using a Group List

See [XDM_RD-V1_1] "*P2P Using a Group List*".

5.1.5 Use Case – Group Visibility

See [XDM_RD-V1_1] "*Group Visibility*".

5.1.6 Use Case - Assigning Permissions

See [XDM_RD-V1_1] "*Assigning Permissions*".

5.1.7 Use Case - Access Control Policy

See [XDM_RD-V1_1] "*Access Control Policy*".

5.1.8 Use Case - Blocking or Granting communication from different end-users

See [XDM_RD-V1_1] "*Blocking or Granting communication from different end-users*".

5.1.9 Use Case – Retrieving a List of Lists

See [XDM_RD-V1_1] "*Retrieving a List of Lists*".

5.1.10 Use Case – Document History Management

5.1.10.1 Short Description

In this scenario, the general manager of an enterprise creates a group list to communicate with the stakeholders (e.g. development manager, team members, customers, etc.) of a project at various stages of the project. As the Group creator, he is allowed to authorise other members to perform certain management functions on the Group document. This use case shows

the requirements for creation and management of document history information that allows the Group creator to track the operations carried out on the document by him and authorized members during his absence.

5.1.10.2 Actors

Service Provider

John (the general manager), Jeff (the development manager), Alan (quality manager), and Alice (customer) all having devices and added to the group list at various stages.

5.1.10.3 Actor Specific Issues

The Group creator (John) wants to perform some document management functions and refer to that at a later stage.

John wants to authorize another member of the Group to perform certain management functions on the Group document during his absence

John wants to track the changes made to the XML document during his absence at a later time.

John wants to search for the operations carried out on the document by him and the authorized Principal during his absence, at a later stage

5.1.10.4 Actor Specific Benefits

John can track the operations carried out on the document on his group list at a later stage.

5.1.10.5 Pre-conditions

John, Jeff, Alan, and Alice have subscriptions to the service.

John has added Jeff and Alice to the Group.

John and other Group members can use IM service as part of the service subscription owned by them.

As part of the subscription with the Service Provider, the Group creator (John) is allowed to grant permissions to other Group members to perform some document management functions.

5.1.10.6 Post-conditions

The Group creator is able to search and retrieve the document management operations performed by himself and the Principal whom he authorized to perform these operations.

5.1.10.7 Normal Flow

1) John enables the document management history storage option using his document management-capable device.
2) John creates a Group with his development team members and customer so that he can communicate with them for day to day activities and status updates.
3) During a vacation, John authorizes Jeff to perform operations on the Group and coordinate communication.
4) Alice needs to clarify quality audit related aspects from the development team and informs Jeff.
5) Jeff initiates an IM Group conversation.
6) Alice discusses with Jeff and other team members regarding the quality aspects.
7) Jeff wants to get the expert opinion from the quality assurance department of his organization
8) Jeff adds Alan into the Group and invites him to join the conversation

9) Server updates the history information for the document management operation performed by Jeff.

10) Alan joins the conversation and discusses quality related aspects with the Group and clarifies the doubts.

11) John returns back from vacation and searches the history information for documents updates and retrieves the history information.

12) John finds that Alan is still part of the Group and he removes him since he is not required in day to day communication.

13) Server updates the document history information for the operations performed by John.

5.1.10.8 Alternative Flow

None.

5.1.10.9 Operational and Quality of Experience Requirements

End-user is able to activate the history management feature.

Server is able to store the history information for all the document management operations performed by various Principals.

End-user with appropriate rights is able to search and/or retrieve the group management history information stored on the server.

5.1.11 Use Case – Sending Group Information to Members of the Group

5.1.11.1 Short Description

This use case outlines a scenario for extended group advertisement. This includes support for the Primary Principal to enable group advertisement, as well as the automatic notification of all group members, upon initial group creation or additional group members as they are added to an existing group.

5.1.11.2 Actors

John: is the leader for a soccer team and is owner of the Group.

Members of the Group: are team mates of John who play on the soccer team.

Alice: a soccer team mate of John who suffers an injury mid-way through the season.

Bob: a soccer team mate of John who joined the team mid-way through the season.

The group service: a service for storage and modification of end-user's Groups (Group documents).

The communication service: a service (such as PoC, Instant Messaging) that John and members of the Group use to communicate.

5.1.11.3 Actor Specific Issues

John wants to set up a Group to enable communication with his fellow soccer team mates. The Group (named "Our Soccer Team") has one or more media properties (e.g., "poc", "im") that establish the rules for communication.

5.1.11.4 Actor Specific Benefits

John is able to set up a Group for some specific purpose and he may not need to send group advertisement messages manually after creation of the Group.

5.1.11.5 Pre-conditions

All members of the Group have subscription and devices enabled for the communication service.

5.1.11.6 Post-conditions

A group communication service has been setup between members of the group.

5.1.11.7 Normal Flow

1) John creates a Group document (named "Our Soccer Team") and sets the supported media of the Group to "poc" and "im". John also sets the automatic Group advertisement feature on.

2) After John has created the Group, The group service sends a group advertisement message automatically to all members of the group.

3) All members of the Group receives a group advertisement message and they can save the received Group "Our Soccer Team" to their UEs.

4) A Group communication session can now be established among members of the Group using the communication service and one of the supported media properties.

5.1.11.8 Alternative Flows

If some members of the advertised Group are not online in time when group service sends group advertisement message and thus they don't get this message, group service will notice this and it will resend group advertisement message later to those members (e.g. when they are online again).

5.1.11.8.1 Group Members Unavailable

If some members of the advertised Group "Our Soccer Team" are not online in time when the group service sends the group advertisement message, and thus they don't get the advertisementis message, the group service will notice this and it will try and resend a group advertisement message later to those members (e.g. when they are online again).

5.1.11.8.2 Group Members Added After Initial Group Creation

1) Mid-way through the season a member of "Our Soccer Team" (Alice) goes down with a season ending injury. John finds a replacement (Bob) to join the team.

2) John makes appropriate changes to the Group by adding Bob.

3) Bob receives a group advertisement message and saves the received Group "Our Soccer Team" to his UE.

5.1.11.9 Operational and Quality of Experience Requirements

- Owner of the Group may not need to send group advertisement messages manually when the Group is created.

5.1.12 Use Case – Forwarding XML Documents

5.1.12.1 Short Description

In this scenario, the project management officer of an enterprise creates different Groups on project basis, each Group containing the members of one project. The members of the Group include the development team members, the project lead, the project manager and the program manager. The project manager is supposed to execute the project and communicate with team members and other stakeholders like vendors and customer. The project leader is supposed to lead the team in technical aspects.

As the Group creator, the project management officer is allowed to authorise other members of the Group to perform certain management functions. This use case shows the requirements for forwarding the Group documents by the Group creator to other members of the Group.

5.1.12.2 Actors

Service Provider

David (project management officer), John (program manager), Bob (project manager), Jeff (project lead) all having mobile devices and added to the group list.

Group Service: A service for storage and modification of end-user's groups.

5.1.12.3 Actor Specific Issues

The Group creator (David) wants to forward some Group document(s) to John and Bob, who are newly appointed as the program manager and project manager respectively.

Bob wants to forward one Group XML document related to the project which Jeff handles after filtering some Group properties at the time of forwarding to Jeff.

John, Bob and Jeff wanted to become the owner of the Group document(s) received by them.

5.1.12.4 Actor Specific Benefits

David can send Group document to recipients.

Bob can filter some properties of Group that is not relevant for Jeff

John, Bob and Jeff can become owner of the document(s) received by them.

5.1.12.5 Pre-conditions

David has different Groups related to various projects.

David, John, Bob, Jeff and other members can use an IM service as part of the mobile service subscription owned by them

As part of the subscription with the Service Provider, the Group creator (David) is allowed to forward Group(s) to other subscribers.

5.1.12.6 Post-conditions

The Group creator is able to forward Group document to multiple recipients

The member who forwards the Group document can filter out some properties of the Group and then forward the resulting Group document.

The actors who received the Group document(s) become the owners of their respective copy(ies) of the document(s).

5.1.12.7 Normal Flow

1) David created various Groups based on projects, one group per project.
2) David selects the Group document and forwards to John and Bob.
3) John and Bob are prompted to add the copy of the Group document to their respective user's tree.
4) John and Bob accepts the addition
5) The group service adds the document in the respective user trees.
6) Bob selects the Group document related to the project which Jeff handles and removes the contacts of the Vendor and Customer and forwards the document to Jeff
7) Jeff is prompted to add the Group document to his user tree.

8) Jeff accepts the addition

9) The group service adds the document in the respective user's tree.

5.1.12.8 Alternative Flow

None.

5.1.12.9 Operational and Quality of Experience Requirements

Principals with appropriate rights should be able to forward XML documents to other Principals

Principals forwarding the XML documents should be able to forward documents to multiple Principals

Principals forwarding the XML documents should be able to filter some properties of the XML documents before forwarding them

Recipient Principals should be able to accept or reject the forwarded XML documents

Recipient Principals should be the owners of the documents added to their users trees by the forward operation

5.1.13 Use Case – Exchange of Shared User Profile data

5.1.13.1 Short Description

This use case describes how to enhance the use of the Shared User Profile, through both a better organization of the data it contains and the ease of use of privacy on this data.

The Shared User Profile can be used to build personal contact lists with contact data entered by the contacts themselves. It avoids errors in entering contact information, and it also enables to keep data consistent when it changes.

5.1.13.2 Actors

Roger: An individual, whishing to keep contact with his friends and colleagues

Leo: A friend of Roger's

Martin: A colleague of Roger's

5.1.13.3 Actor specific issues

- Leo moves very often. His address changes every year
- Martin's top management comes up with a different organization twice a year. His work information changes as often

5.1.13.4 Actor specific benefits

- Roger always has an updated profile of his contacts whenever he needs it
- Roger doesn't need to enter the information about Leo and Martin by himself
- Leo and Martin can set the privacy on their information thanks to Groups of attributes

5.1.13.5 Pre-conditions

- Roger's terminal has the ability to read Shared User Profiles (like a messaging Client for instance or a Shared User Profile enabled address book)
- Leo and Martin's terminals have the ability to setup their profile and perform the adequate privacy settings

5.1.13.6 Post-conditions

- Roger always has a fresh view of Leo's and Martin's Shared User Profiles
- Leo's and Martin's privacy settings are respected

5.1.13.7 Normal flow

1) Roger obtains Leo and Martin identifiers for their Shared User Profile (e.g. through search or any external means)
2) Roger subscribes to the changes of Leo and Martin's Shared User Profiles
3) Leo being a friend of Roger's, he grants him the right to see all his personal information (home address, home phone…), but not his professional information
4) Martin being a colleague of Roger's he grants him the right to see all his work-related information (work address, work phone…)
5) Roger receives for the first time data from Leo and Martin. Of course, he receives only the data to which they have granted him access
6) Martin is promoted and changes his work information. Roger is notified of the update about Martin's job position
7) Leo changes his professional telephone number. Roger is not notified of the update, since Leo's privacy does not let him see this information

5.1.13.8 Alternative flow

Roger can update the information about Leo and Martin through periodic requests instead of a subscription

5.1.13.9 Operational and Quality of Experience Requirements

The organization of data into categories will encourage the use of the Shared User Profile. As a User of the service, the privacy settings will be eased by this feature, making it more attractive to the User to share personal information.

5.2 Service Enabler Specific Use Cases

The service specific use cases define the behaviour, information elements and actors that are common for all OMA services elements using XDM.

5.2.1 Push to talk over Cellular (PoC)

5.2.1.1 Use Case - Creation and Advertising Group List

See [PoC_RD-V1_0] "*Use Case A, SHOPPING LIKE CRAZY*".

5.2.1.2 Use Case - User Defined Group Call One-to-Many

See [PoC_RD-V1_0] "*Use Case G, User Defined Group Call – One-to-Many*".

5.2.1.3 Use Case - Private Chat Group Support One to Many

See [PoC_RD-V1_0] "*Use Case I, Private Chat Group Support – One-to-Many*".

5.2.1.4 Use Case – Use of Multiple Group Operation

See [PoC_RD-V1_0] "*Use Case K, Use of Multiple Group Operation*".

5.2.1.5 Use Case - Ad-hoc Chat Group Support One-to-Many

See [PoC_RD-V1_0] "*Use Case M, Ad-hoc Chat Group Support – One-to-Many*".

5.2.1.6 Use Case - Corporate Chat

See [PoC_RD-V1_0] "*Use Case O, Corporate Chat*".

5.2.1.7 Use Case - Fleet Dispatch: One-to-Many-to-One

See [PoC_RD-V1_0] "*Use Case N, Fleet Dispatch – One-to-Many-to-One*".

5.2.2 Instant Messaging (IM)

5.2.2.1 Use Case – Use of Group Management

See [IM_RD] "*IM Use of Group Management*".

5.2.2.2 Use Case – Add Contact to Contact List by User-ID or Search

See [IM_RD] "*Add Contact to Contact List by User-ID or Search*".

5.2.2.3 Use Case –Public Chat

See [IM_RD] "*Public Chat*".

5.2.2.4 Use Case – Modify Contract Entry

See [IM_RD] "*Modify Contact Entry*".

6. Requirements (Normative)

6.1 High-Level Functional Requirements

This section describes the functional requirements that are common to all document management functions.

Note: there may be requirements in the form of bullet lists where there is heading text followed by a list of numbered requirements. In those cases, the heading text applies to all subsequent numbered requirements.

6.1.1 General

Label	Description	Enabler Release
GEN-001	The end-user SHALL be able to store his per-user information (e.g., URI Lists) in the network.	XDM 1.1
GEN-002	Such information SHALL be stored as one or more documents described in an extensible and platform-neutral format.	XDM 1.1
GEN-003	Each document SHALL be identified by at least one globally unique identifier (i.e., a URI according to RFC 2396).	XDM 1.1
	Documents SHALL be associated with meta-data which describes certain properties of the document that are not included in its content. Such meta-data SHALL include at least the following:	
GEN-004	1) Timestamp of document creation;	Future release
GEN-005	2) Timestamp of last document access.	Future release
GEN-006	A document SHALL be associated with access permissions.	Future release
GEN-007	The access permissions SHALL be managed with the same underlying mechanisms as defined is section 6.1.3. The type of data denoting the access permissions is described in section 6.2.1	Future release
GEN-008	The XDM enabler SHALL allow an authorized Principal to access and manage stored documents from any capable device type over any capable network.	XDM 1.1
GEN-009	Data consistency of information stored in the XDM enabler SHALL be ensured, particularly if simultaneous access by multiple authorised end-users and/or multiple devices is allowed.	XDM 1.1
GEN-010	The XDM enabler SHALL allow a Principal to retrieve a list of all stored documents for which the Principal is the Primary Principal.	XDM 1.1
GEN-011	The XDM enabler SHALL allow a Principal to retrieve a list of all stored documents for which the Principal is the Primary Principal per type of service (e.g., all documents related to his PoC service).	XDM 1.1
GEN-012	It SHOULD be possible to provision the XDM Client using existing OMA Device Management and Provisioning enablers.	XDM 1.1
GEN-013	XDM documents SHALL support multiple character sets.	XDM 1.1
GEN-014	A document MAY be associated with XDM history information. The type of data contained in the XDM history is described in section 6.2.2.	Future release
GEN-015	The XDM history management SHOULD be supported when the Delegation (section 6.2.1) is supported.	Future release
GEN-016	The XDM enabler SHALL support interfaces that are access technology neutral.	XDM 1.1
GEN-017	The XDM enabler SHALL provide a single contact point for all XDM Clients to access XML documents managed by the XDM enabler.	XDM 1.1

Table 1: Functional Requirements -General

6.1.2 Delegation

Label	Description	Enabler Release
FUNC-DLG-001	A Primary Principal SHALL be able to authorise other Principals to perform document management operations, as listed in section 6.1.3.2, 6.1.3.9 and 6.1.3.10, on their documents.	Future release
FUNC-DLG-002	Principals SHALL be able to authorise other principals to perform document management operations, as listed in section 6.1.3.1 to 6.1.3.10, on their documents.	Future release
FUNC-DLG-003	Principals SHALL be able to authorise other Principals to authorise additional Principals to perform document management operations, as listed in section 6.1.3.1 to 6.1.3.10, on their documents.	Future release

Table 2: Functional Requirements -Delegation

6.1.3 Document Management Functions

The sub-sections below identify the set of available document management functions.

Label	Description	Enabler Release
FUNC-DMT-001	Document management functions SHALL be controlled by permissions which determine the capabilities available to a principal wishing to perform such functions in each document.	XDM 1.1
FUNC-DMT-002	It SHALL be possible to define "roles" that represent a given set of permissions. Assignment of those roles to particular principals is equivalent to assigning the corresponding set of permissions.	Future release
FUNC-DMT-003	Permissions MAY be assigned at any time from creation to deletion of the document.	Future release
FUNC-DMT-004	At the creation of a document, the default permissions of the document SHALL prevent all Principals, except the Primary Principal of the document, to perform any document management functions.	Future release
FUNC-DMT-005	Principals who try to perform a document management function SHALL first be authenticated.	XDM 1.1
FUNC-DMT-006	The creator of a document SHALL become the Primary Principal of the document.	XDM 1.1
FUNC-DMT-007	The Primary Principal SHALL always be allowed to modify the permissions on his/her document.	Future release
FUNC-DMT-008	There SHALL always be one and only one Primary Principal of a document.	XDM 1.1
FUNC-DMT-009	It SHOULD be possible for Principals with the appropriate permission to query the permissions applied to a specific document.	Future release
	The Service Provider SHALL be able to set the expiry time of a document based on one or more of the following:	
FUNC-DMT-010	4) Time-to-live after creation: The expiry time relative to when the document was created.	Future release

FUNC-DMT-011	5) Time-to-live after last access: The expiry time relative to when the document was last accessed.	Future release
FUNC-DMT-012	6) Expiration time: An absolute expiry time.	Future release
FUNC-DMT-013	A Principal with appropriate management permissions MAY be able to set the expiry time of a document to a value that does not exceed the maximum expiry time set by the service provider.	Future release
FUNC-DMT-014	An expired document MAY be deleted automatically.	Future release
FUNC-DMT-015	All permissions associated with a document SHALL be deleted upon deletion of this document.	Future release

Table 3: Functional Requirements –Document Management

6.1.3.1 Create

Label	Description	Enabler Release
FUNC-CREAT-001	Principals with appropriate permissions SHALL be able to create a document	XDM 1.1

Table 4: Functional Requirements –Document Management Create

6.1.3.2 Retrieve

Label	Description	Enabler Release
FUNC-RETR-001	Principals with appropriate permissions SHALL be able to retrieve a document	XDM 1.1

Table 5: Functional Requirements –Document Management Retrieve

6.1.3.3 Copy

Label	Description	Enabler Release
FUNC-COPY-001	Principals with appropriate permissions SHALL be able to copy documents within the same XDMS instance, or to another XDMS instance.	Future release

Table 6: Functional Requirements –Document Management Copy

6.1.3.4 Delete

Label	Description	Enabler Release
FUNC-DEL-001	Principals with appropriate permissions SHALL be able to delete a document.	XDM 1.1

Table 7: Functional Requirements –Document Management Delete

6.1.3.5 Modify

Label	Description	Enabler Release
FUNC-MOD-001	Principals with appropriate permissions SHALL be able to modify a document.	XDM 1.1

Table 8: Functional Requirements –Document Management Modify

6.1.3.6 XDM Forward

Label	Description	Enabler Release
FUNC-FWD-001	The XDM Enabler MAY support the forwarding of documents.	Future release
FUNC-FWD-002	If forwarding is supported the Principals with appropriate permissions SHALL be able to forward a documents to other principals.	Future release
FUNC-FWD-003	If forwarding is supported the forwarding Principal SHALL be able to filter the contents of a document without affecting the original document, before the document is forwarded to other principals so that the receiving Principal(s) receive the filtered document.	Future release
FUNC-FWD-004	If forwarding is supported the Principals receiving the forwarded documents SHALL be able to accept or reject those documents.	Future release
FUNC-FWD-005	If forwarding is supported, the receiving Principals who accept forwarded documents SHALL own the forwarded document and SHALL be regarded as creators of those documents.	Future release

Table 9: XDM Forward

6.1.3.7 Suspend

Label	Description	Enabler Release
FUNC-SUSP-001	Principals with appropriate permissions SHALL be able to suspend access to and use of a document.	Future release
FUNC-SUSP-002	When access to and use of a document is suspended, no operation can be performed on that document, except to take it out of the suspend state or delete it.	Future release

Table 10: Functional Requirements –Document Management Suspend

6.1.3.8 Resume

Label	Description	Enabler Release
FUNC-RESM-001	Principals with the appropriate permission SHALL be able to resume usage of a suspended document.	Future release
FUNC-RESM-002	After a resume operation, all operations SHALL be possible to be performed on that document (except for the resume operation).	Future release

Table 11: Functional Requirements –Document Management Resume

6.1.3.9 Search

Label	Description	Enabler Release
FUNC-SRCH-001	The XDM Enabler MAY support search.	XDM 2.0
FUNC-SRCH-002	If search is supported, it SHALL be possible to search for the existence of certain content (e.g., the identifier of a User) in a document.	XDM 2.0
FUNC-SRCH-003	If search is supported, it SHALL be possible to search for the existence of a document based on meta-data associated with the document.	Future release
FUNC-SRCH-004	If search is supported, it SHALL be possible for a User performing a search and for the Service Provider to limit the number of search results.	XDM 2.0
FUNC-SRCH-005	If search is supported, it SHALL be possible to search documents hosted by the Service Provider.	XDM 2.0
FUNC-SRCH-006	If search is supported, it MAY be possible to search documents hosted by other Service Providers.	XDM 2.0
FUNC-SRCH-007	If search is supported, the content of search results SHALL be subject to Service Provider policy or end-user privacy settings.	Future release
FUNC-SRCH-008	If search is supported, it SHALL be possible to use wildcards in the search criteria when searching documents.	XDM 2.0
FUNC-SRCH-009	If search is supported, search SHALL be limited to one document type (e.g. Shared Group document) at a time.	XDM 2.0
FUNC-SRCH-010	If search is supported, the XDM enabler MAY provide a mechanism to limit local Shared User Profile searches to users who have a searchable Shared User Profile.	Future release
FUNC-SRCH-011	If search is supported, the XDM Client SHALL be able to use basic logical operations (AND, OR, NOT) when searching documents.	XDM 2.0
FUNC-SRCH-012	If search is supported, the XDM Enabler SHALL combine the search results of all the entities in the service provider's domain when sending a response to the XDM Client.	Future release
FUNC-SRCH-013	If search is supported, the XDM enabler MAY combine search responses received from other service providers.	XDM 2.0
FUNC-SRCH-014	If search is supported, the Service Provider SHALL be able to limit the number of logical operations in a search request.	XDM2.0
FUNC-SRCH-015	If search is supported, a User performing a search MAY specify which information the User wants to receive as a result of the search.	XDM2.0

Table 12: Functional Requirements –Document Management – Search

6.1.3.10 Subscription to changes

Label	Description	Enabler Release
FUNC-SUBCHG-001	Principals with appropriate permissions SHALL be able to subscribe to and receive notifications regarding updates to documents.	XDM 2.0

Table 13 : Functional Requirements –Subscription to changes

6.1.3.11 Extended Group Advertisement

Label	Description	Enabler Release
FUNC-GRPAD-001	The XDM Enabler MAY support extended group advertisement.	XDM 2.0
FUNC-GRPAD-002	If the XDM Enabler supports extended group advertisement then it SHALL advertise group automatically to all members of that group when group is created.	XDM 2.0
FUNC-GRPAD-003	If the XDM Enabler supports extended group advertisement then it SHALL advertise group automatically to new member(s) of existing group when new member(s) is added to that group.	XDM 2.0
FUNC-GRPAD-004	Extended group advertisement sent by the XDM Enabler SHALL include information of supported communication means of the group (e.g. audio, message, video).	XDM 2.0
FUNC-GRPAD-005	If the XDM Enabler supports extended group advertisement then it MAY send an extended group advertisement automatically to all members of that group when properties of that group are modified (e.g. new communication mean is added to the group or removed from the group).	XDM 2.0
FUNC-GRPAD-006	Extended group advertisement sent by the XDM Enabler MAY include XCAP URI of corresponding group document.	Future release

Table 14: Functional Requirements –Extended Group Advertisement

6.1.4 Security

Label	Description	Enabler Release
	Mechanisms SHALL be provided to support:	
SEC-001	1) Mutual authentication of the XDM server and XDM client implementations.	XDM 1.1
SEC-002	2) Integrity and confidentiality of XDM message exchanges.	XDM 1.1
SEC-003	If there is a mechanism to perform the security functions mentioned in SEC-001 and SEC-002 in a common way, the XDM protocol SHOULD support the use of such a mechanism instead of duplicating such functionality.	XDM 1.1

Table 15: Security

6.1.5 Charging

Label	Description	Enabler Release
CHA-001	Mechanisms SHALL be provided for the Service Provider to charge for the use of XDM. Examples of charging events include: 1) The creation, modification or deletion of a document. 2) The number of documents for which the end-user is the Primary Principal.	Future release

Table 16: Charging

6.1.6 Usability

Label	Description	Enabler Release
USA-001	The XDM Server SHALL use a version control mechanism to avoid unnecessary document retrievals prior to document manipulation.	XDM 1.1
USA-002	The XDM Client MAY use a version control mechanism to avoid unnecessary document retrievals prior to document manipulation.	XDM 1.1

Table 17: Usability

6.1.7 Interoperability

Label	Description	Enabler Release
	Interoperability of the XDM Enabler is provided through the definition of open interfaces and a consistent format of documents and XDM functions in compliance with the requirements presented in this document.	
	The XDM functions, open interfaces and document formats SHALL provide interoperability to include at least the following:	
IOP-001	1) Administration of documents.	XDM 1.1
IOP-002	2) Transfer of documents over open interfaces.	XDM 1.1
IOP-003	3) Search documents over open interfaces.	XDM 1.1
IOP-004	4) General structure of the documents transferred over open interfaces.	XDM 1.1
IOP-005	5) Collection and general format of charging information.	XDM 1.1
IOP-006	XDM 2.0 Enabler SHALL support XDM 1.0 Enabler functionality (e.g. XDM 2.0 Enabler SHALL be able to manage an XDM 1.0 PoC Group document).	XDM 2.0
IOP-007	While connected to the XDM 1.0 Enabler, XDM 2.0 Clients SHALL support the XDM 1.0 functionality (e.g. an XDM 2.0 client SHALL be able to manage an XDM 1.0 PoC Group Document).	XDM 2.0

Table 18: Interoperability

6.1.8 Privacy

Label	Description	Enabler Release
PRV-001	Access to XDM information SHALL conform to privacy requirements specified in [Privacy_Req].	XDM 1.1

Table 19: Privacy

6.1.9 Lawful Interception

This section specifies the XDM Enabler requirements for lawful interception (LI). The capability to intercept telecommunications traffic and related information for PoC is always implemented in accordance with national or regional (e.g., European Union) laws or technical regulations, where these exist and are applicable to the Service Provider. Nothing in this specification, including the definitions, is intended to supplant such applicable laws or regulations.

Label	Description	Enabler Release
LI-001	The XDM Enabler SHALL support PoC 2.0 LI requirements by providing a single point of interface to a Law Enforcement Agency through which all XDM information for an identified PoC User can be intercepted when appropriate conditions (e.g., in accordance with national or regional laws or regulations) are met.	XDM 2.0
LI-002	The XDM information provided to a Law Enforcement Agency SHALL include Principal Identity, regardless of anonymity or privacy settings.	XDM 2.0

Table 20: Lawful Interception

6.2 Associated Metadata

This section describes a set of metadata that are associated with a document upon its creation, and describes certain properties of the document.

6.2.1 Access Permissions

Access Permissions defines which principals have rights to perform which XDM functions on the associated document.

Label	Description	Enabler Release
	Access Permissions SHALL include the following data, in addition to those properties specified in Section 6.1.1:	
MD-ACP-001	1) Identities of the principals who have access permissions to the associated document, including their human readable name.	Future release
MD-ACP-002	2) Operations these principals are allowed to perform in the associated document. Operations SHALL include following XDM functions:	Future release
MD-ACP-003	a) Retrieve	Future release
MD-ACP-004	b) Search	Future release
MD-ACP-005	c) Subscription for changes	Future release
MD-ACP-006	d) Write	Future release

MD-ACP-007	e) Delete	Future release
MD-ACP-008	f) Create	Future release
MD-ACP-009	g) Copy	Future release
MD-ACP-010	h) Forward	Future release
MD-ACP-011	i) Suspend	Future release
MD-ACP-012	j) Resume	Future release
MD-ACP-013	The Primary Principal of the associated document is the only one, who SHALL have rights to modify the Access Permissions.	Future release

Table 21: Access Permissions Document

6.2.2 XDM History

The XDM History contains a history of XDM operations performed on the associated XML document.

Label	Description	Enabler Release
MD-HST-001	If the XDM history function is supported, the Primary Principal SHALL be able to enable and disable the XDM history function, on a per-document basis.	Future release
MD-HST-002	If the XDM history function is enabled, the XDM history information of the performed operations of Document Management Functions for the modification of the document (i.e. creation/deletion/modification of an element or attribute) SHALL be stored	Future release
MD-HST-003	If the XDM history function is enabled, the XDM history information of the performed operations of other Document Management Functions than that for the modification of the document MAY be stored.	Future release
	The XDM history information of the performed operations SHALL include at least:	
MD-HST-004	1) Type of operation	Future release
MD-HST-005	2) Timestamp of operation	Future release
MD-HST-006	3) Identity of the Principal that performed the operation	Future release
MD-HST-007	The Primary Principal SHALL be able to retrieve the stored XDM History information.	Future release
MD-HST-008	It MAY be possible to search the information on the performed operations through the XDM History Information on a single document.	Future release
	If supported, Primary Principals SHALL be ableto search, at least, using the following criteria:	
MD-HST-009	1) Type of operation.	Future release
MD-HST-010	2) Time range	Future release
MD-HST-011	3) Identity of Principal that performed the operation(s).	Future release
MD-HST-012	The service provider SHALL be able to limit the size of the XDM History information.	Future release

Table 22: XDM History Document

6.3 Document Types

6.3.1 Shared Documents

Label	Description	Enabler Release
DOC-SHD-001	It SHALL be possible to share the following types of documents: URI List, Group Usage List, such that they can be used by multiple enablers (e.g. PoC, Presence, IM, etc.).	XDM 1.1
DOC-SHD-002	It SHALL be possible to share the following types of documents: User Profile, Group, User Access Policy document such that they can be used by multiple enablers (e.g. PoC, Presence, IM, etc.).	XDM 2.0

Table 23: Shared Documents

6.3.1.1 Shared URI List

Label	Description	Enabler Release
DOC-URI-001	A Shared URI List SHALL contain a Display name information, representing the human readable name.	XDM 1.1
DOC-URI-002	A Shared URI List SHALL contain zero or more URI List members.	XDM 1.1
	The following requirements apply to Shared URI List members:	
DOC-URI-003	1) Every URI List member SHALL be identified by a globally unique identifier (i.e., a URI as defined in RFC 2396).	XDM 1.1
DOC-URI-004	2) A URI List member MAY have a human readable display name.	XDM 1.1
DOC-URI-005	The service provider SHALL be able to set the maximum number of URIs in a Shared URI List.	XDM 1.1

Table 24: Shared URI List

6.3.1.2 Shared User Profile

Label	Description	Enabler Release
DOC-USP-001	Shared User Profile document SHALL contain static user information that can be used by other users and applications for means of communication i.e search for a chat partner.	XDM 2.0
DOC-USP-002	The Shared User Profile document contains mandatory information and a user SHALL NOT be able to create a profile unless all the mandatory information elements are completed.	XDM 2.0
DOC-USP-003	Modifications to the Shared User Profile SHALL ensure that all mandatory information elements are also completed.	XDM 2.0
DOC-USP-004	The Shared User Profile SHALL support the assignment of permissions to multiple elements in one operation.	Future release
DOC-USP-005	A Shared User Profile element MAY belong to several groups of elements	XDM 2.0
DOC-USP-006	Each element SHALL be uniquely identifiable to be appropriately computed and used by services	XDM 2.0
	The Shared User Profile document MAY contain the following static information of the user:	
DOC-USP-007	1) User identifier that uniquely identifies the user that the Shared User Profile is meant for.	XDM 2.0
DOC-USP-008	2) Communication address(es). This field MAY contain the following information:	XDM 2.0
DOC-USP-009	a) SIP URI as defined in [RFC3261]	XDM 2.0
DOC-USP-010	b) E.164 number	XDM 2.0

DOC-USP-011	c) E-mail address	XDM 2.0
DOC-USP-012	3) Display name, which is a non-unique and not routable identification of that user that could be displayed to others.	XDM 2.0
DOC-USP-013	4) Date of birth: if supported this information SHALL contain the following information:	XDM 2.0
DOC-USP-014	a) Birth day-of month	XDM 2.0
DOC-USP-015	b) Birth month	XDM 2.0
DOC-USP-016	c) Birth year	XDM 2.0
DOC-USP-017	5) Name, representing the civil identity of the user. This field MAY contain the following information:	XDM 2.0
DOC-USP-018	a) Given name	XDM 2.0
DOC-USP-019	b) Family name	XDM 2.0
DOC-USP-020	c) Middle name	XDM 2.0
DOC-USP-021	d) Name suffix	XDM 2.0
DOC-USP-022	e) Name prefix	XDM 2.0
DOC-USP-023	6) Address, representing one or several of the physical addresses of the user (e.g. home, work…). This field MAY contain the following information:	XDM 2.0
DOC-USP-024	a) Country: the country in which the user is located (for this address)	XDM 2.0
DOC-USP-025	b) Region: the region (i.e. state, province…) in which the user is located	XDM 2.0
DOC-USP-026	c) Locality (i.e town, village, city…)	XDM 2.0
DOC-USP-027	d) Area: the subdivision of the town in which the user is located (i.e. neighbourhood, suburb, district…)	XDM 2.0
DOC-USP-028	e) Street name: the name of the street where the user is located for this address	XDM 2.0
DOC-USP-029	f) Street number: the number in this street where the user is located for this address	XDM 2.0
DOC-USP-030	g) Postal code: the code for postal delivery (e.g ZIP code)	XDM 2.0
DOC-USP-031	7) Gender, indicating whether the user is male or female.	XDM 2.0

DOC-USP-032	8) Free text description.	XDM 2.0
DOC-USP-033	9) Communication abilities, which defines possible means to reach the user e.g. voice, message, video etc..	XDM 2.0
DOC-USP-034	10) Hobbies.	XDM 2.0
DOC-USP-035	11) Favourite links, in the form of a list of URLs.	XDM 2.0
DOC-USP-036	12) QoE Profile subscribed by the user. This information is defined by the Service Provider and can not be modified by the user.	XDM 2.0
DOC-USP-037	The Shared User Profile SHALL contain two kinds of Date of Birth information of the user; one that delivers the real Date of Birth, set and locked by the Service Provider, and the other that delivers the Date of Birth as set by the user.	XDM 2.0
DOC-USP-038	The authorized Principal of the Shared User Profile SHALL be able to set the privacy that defines the limitation in searching or accessing the information in the Shared User Profile.	Future release

Table 25: Shared User Profile

6.3.1.3 Shared Group Document

Label	Description	Enabler Release
DOC-GRP-001	A document describing a Shared Group SHALL include a URI attribute to represent a group identity.	XDM 2.0
	A document describing a Shared Group MAY have the following content:	
DOC-GRP-002	1) Display name: This is a human readable name.	XDM 2.0
DOC-GRP-003	2) Session Type: This identifies the nature of the Shared Group e.g. chat, instant. (In an instant group session, end-users are invited during session initiation. In a chat group session, end-users are not invited during session initiation but are instead expected to individually join the session once it is active.)	XDM 2.0
DOC-GRP-004	3) Allow session initiation: This describes who may initiate a group session	XDM 2.0
DOC-GRP-005	4) Group member list: This identifies end-users who are members of the Shared Group. The semantics of group membership may depend on the session type, and may also be enabler-specific.	XDM 2.0
DOC-GRP-006	5) Allow session access: This describes who may join a group session	XDM 2.0
DOC-GRP-007	6) Maximum number of participants: This is the maximum number of end-users who can be active in the session	XDM 2.0
DOC-GRP-008	7) Allow anonymous access: This describes who may join a group session anonymously, if anonymous access is requested	XDM 2.0
DOC-GRP-009	8) Allow dynamic invitation: This describes who may invite additional participants to a group session.	XDM 2.0
DOC-GRP-010	9) Key participant: This describes who may assume the role of a "Key Participant". The semantics of Key Participant may depend on the session type, and may also be enabler-specific (e.g. a "Distinguished Participant" of a 1-many-1 PoC group session).	XDM 2.0
DOC-GRP-011	10) Subject: This contains a topic or description of a Shared Group.	XDM 2.0
DOC-GRP-012	11) Session participation policy: This describes conditions that limit the participation in a group session. The session participation policy MAY be based on the following:	XDM 2.0
DOC-GRP-013	a) Age minimum: This indicates the minimum allowed age of a participant.	XDM 2.0
DOC-GRP-014	b) Age maximum: This indicates the maximum allowed age of a participant.	XDM 2.0
DOC-GRP-015	12) Session active policy: This describes the rules for determining the existence of a group session. The session active policy MAY be based on the following: **NOTE**: How to utilize the session active policy for the actual session initiation or termination is not the scope of XDM enabler but that of the application enabler (e.g., IM or PoC).	XDM 2.0
DOC-GRP-016	a) Maximum duration: This indicates the maximum allowed time duration (e.g., 1 hour) for the session to remain active.	XDM 2.0
DOC-GRP-017	b) Required participant: This describes who (e.g. session initiator) must participate for the session to get or remain active.	XDM 2.0

DOC-GRP-018	c) Minimum number of participants: This describes how many must remain participating for the session to remain active.	XDM 2.0
DOC-GRP-019	d) Allowed range of a time: This describes the allowed range of time (e.g., from 2pm to 4pm) for the session to get or remain active.	XDM 2.0
DOC-GRP-020	13) Allow sub-conferencing: This describes who may create sub-conferences in a group session.	XDM 2.0
DOC-GRP-021	14) Allow Private messaging: This describes who may send private messages in a group session.	XDM 2.0
DOC-GRP-022	15) Allowed medias: This identifies which medias are allowed to use in a group session e.g. audio, text, video, application.	XDM 2.0
DOC-GRP-023	16) Allow to see conference state: This describes who can see the state of the group session (e.g. who is currently online).	XDM 2.0
DOC-GRP-024	17) QoE Profile: This describes the Quality of Experience profile assigned to the group. The profile defines how the end-user experience should be for the group session	XDM 2.0
DOC-GRP-025	18) Dispatcher participant: This identifies who may assume the role of dispatcher (e.g. PoC Dispatcher).	XDM 2.0
DOC-GRP-026	19) Allow role transfer: This describes who can request the transfer of an active role (e.g. PoC Dispatcher) to another authorized participant.	XDM 2.0
DOC-GRP-027	20) Allow expelling: This describes who may expel other participants from the group session.	XDM 2.0
DOC-GRP-028	Each entry in a Group member list or Group reject list SHALL be a tuple consisting of a URI and, optionally, a display name.	XDM 1.1
DOC-GRP-029	Each URI in the Group member list SHALL occur only once.	XDM 1.1
DOC-GRP-030	Each URI in the Group reject list SHALL occur only once.	XDM 1.1
DOC-GRP-031	The Service Provider SHALL be able to set the maximum number of participants in a Shared Group document.	XDM 1.1
DOC-GRP-032	A Principal with appropriate management permissions MAY be able to set the maximum number of participants in a Shared Group document to a value that does not exceed the maximum number set by the Service Provider.	XDM 1.1
DOC-GRP-033	It SHALL be possible to create a Shared Group document that contains members in the Group member list or Group reject list that belong to different Service Providers.	XDM 1.1

Table 26: Shared Group Document

6.3.1.4 Shared Group Usage List

Label	Description	Enabler Release
DOC-GUL-001	A Shared Group Usage List SHALL have a Display name: A human readable name.	XDM 1.1

DOC-GUL-002	A Shared Group Usage List SHALL contain usage information about zero or more Groups.	XDM 1.1
DOC-GUL-003	A Group defined in a Shared Group Usage List SHALL be identified by a globally unique identifier (i.e., a URI as defined in [RFC2396]).	XDM 1.1
DOC-GUL-004	A Group defined in a Shared Group Usage List MAY have a Display name: A human readable name.	XDM 1.1
DOC-GUL-005	A Group defined in a Shared Group Usage List MAY have information about the usage of it.	XDM 1.1
DOC-GUL-006	The Service Provider SHALL be able to set the maximum number of Groups in a Shared Group Usage List.	XDM 1.1

Table 27: Shared Group Usage List

6.3.1.5 Shared User Access Policy Document

Label	Description	Enabler Release
DOC-UAP-001	A document describing Shared User Access Policy SHALL describe user preferences that specify how a user wants to be contacted upon communication requests to the user.	XDM 2.0
DOC-UAP-002	A document describing Shared User Access Policy SHALL contain the action that the Application Server is to take when processing a communication request to the user of concern.	XDM 2.0

Table 28: Shared User Access Policy Document

Appendix A. Change History (Informative)

A.1 Approved Version 2.0 History

Reference	Date	Description
OMA-RD-XDM-V2_0-20120403-A	03 Apr 2012	Status changed to Approved by TP: OMA-TP-2012-0135-INP_XDM_V2_0_ERP_for_Final_Approval