XML Document Management Requirements

Approved Version 2.2 – 03 May 2016

Open Mobile Alliance

OMA-RD-XDM-V2_2-20160503-A

Contents

Tables

1. Scope (Informative)

This document describes use cases and requirements for the XDM 2.2 Enabler, taking into consideration the demands of end-users, service providers, and system implementers.

2. References

2.1 Normative References

[CPM_RD] "Converged IP Messaging Requirements", Version 1.0, Open Mobile Alliance™, OMA-RD-CPM-V1_0, URL:http://www.openmobilealliance.org

[Dict] "Dictionary for OMA Specifications", Open Mobile Alliance™, OMA-ORG-Dictionary-V2_9, URL:http://www.openmobilealliance.org

[Privacy_RD] "Privacy Requirements for Mobile Services", Open Mobile Alliance™, OMA-RD-Privacy-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

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

[RFC3986] IETF RFC 3986 "Uniform Resource Identifier (URI): Generic Syntax", T. Berners-Lee, R. Fielding, L. Masinter, January 2005, URL: http://www.ietf.org/rfc/rfc3986.txt

IETF

OMA

2.2 Informative References

[CAB_RD] "Converged Address Book Requirements", Version 1.0, Open Mobile Alliance™, OMA-RD-CAB-V1_0, URL:http://www.openmobilealliance.org

[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_1] "Push to Talk over Cellular 2 Requirements", Version 2.1, Open Mobile Alliance™, OMA-RD-PoC-V2_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

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

[XDM_RD-V2_0] "XML Document Management Requirements", Version 2.0, Open Mobile Alliance™, OMA-RD-XDM-V2_0, URL:http://www.openmobilealliance.org

OMA

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	A set of rules that defines which Principals have rights to perform which document management operations on a specific document.
Active Session	An ongoing session of a communications service.
Active User Preferences Profile	The User Preferences Profile selected by the device from a set of User Preferences Profiles of a User which has to be used by network entities when performing a procedure involving that device.
Admin Principal	A Principal which is authorized to modify Access Permissions associated with a document. A Principal may be both Admin Principal and Primary Principal of a particular document.
Alias Principal	A Principal is an alias of another Principal if the treatment of their XCAP User Identities is identical (e.g. they are logically identical).
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.
Client	Use definition from [Dict].
Crisis Event	An unplanned event having potentially significant impact on the safety or well-being of the community (local, regional or national). Examples of a Crisis Event include natural or man-made disasters.
Default User Preferences Profile	The User Preferences Profile to be used by network entities when the network entities have no knowledge about any Active User Preferences Profile.
Document Reference	A function to access content in an XDM Document by a reference.
Enabler	Use definition from [Dict].
Extended Group Advertisements	A function to inform group members about e.g. membership in a Group.
Group	A set of User Addresses and/or Group Identities together with its policies and attributes, which is identified by a Group Identity.
Group Document	An XDM Document containing a Group.
Group Identity	The SIP URI of the Pre-arranged Group or Join-in Group.
Group Usage List	A list of group names or service URIs that are known by an XCAP Client.
Group Usage List Document	An XDM Document containing Group Usage Lists.
Join-in Group	A persistent Group in which a User individually joins to have a Group Session with other joined Users, i.e., the establishment of a Group Session to a Join-in Group does not result in other Users being invited. A Join-in Group optionally has an associated set of Group Members.
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.
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.

Media Burst Control	A mechanism that arbitrates requests from Clients for the right to send media in half-duplex communication.
Offline Communication Storage	A data storage where communication sessions can be stored when the User is offline (e.g. User has not registered to the communication service).
Pre-arranged Group	A persistent Group that has an associated set of Group Members. The establishment of a Group Session to a Pre-arranged Group results in all Group Members being invited.
Primary Principal	The Primary Principal is the User associated with the XCAP User Identity, which defines where the document resides.
Principal	Use definition from [Dict].
Quality of Experience	A communications session property associated with a set of well-defined QoS and prioritization parameters and overload behaviours.
Service Provider	Use definition from [Dict].
Session Control for Crisis Handling	A service providing the means to enforce high enough priority in the network to serve a session for end user groups with more mission critical requirements in applications such as public safety, private safety and national security
Subscriber	Use definition from [Dict].
UPP Directory	A UPP Directory as described in section 6.3.6.
UPP Directory Document	An XDM Document containing a UPP Directory.
URI List	A collection of URIs put together for convenience.
URI List Document	An XDM Document containing URI Lists.
User	Use definition from [Dict].
User Access Policy	A User Access Policy as described in section 6.3.5.
User Address	Use definition from [PoC_CP].
User Preferences Profile	Use definition from [CPM_RD].
User Preferences Profile Identifier	An identifier (e.g. “work”, “home”) associated with a particular User Preferences Profile that is unique within the scope of a Primary Principal.
User Profile	A set of personal information provided by a User and made available to other Users for e.g. search for new contacts. NOTE: this definition differs from the definition in [Dict].
XDM Document	A resource representing an XML document.
XDM Document Part	A resource representing an element within an XML document, or an attribute of an element within an XML document.
XDM Resource	A term used to refer to both XDM Document and XDM Document part.

3.3 Abbreviations

CAB	Converged Address Book
CPM	Converged IP Messaging
IM	Instant Messaging
IP	Internet Protocol
LI	Lawful Interception
OMA	Open Mobile Alliance
P2P	Peer to Peer
PoC	Push to Talk over Cellular
RD	Requirements Document

RFC	Request For Comments
SIMPLE	SIP for Instant Messaging and Presence Leveraging Extensions
SIP	Session Initiation Protocol
UPP	User Preferences Profile
UPPID	User Preferences Profile Identifier
URI	Uniform Resource Identifier
XDM	XML Document Management
XML	eXtensible Markup Language

4. Introduction (Informative)

Various OMA Enablers such as Presence SIMPLE, PoC, SIMPLE IM, CPM, CAB, etc. need support for access to and manipulation of certain information that is needed by these Enablers. One example of such information (whose semantics and syntax are outside the scope of the XDM Enabler) is Presence Subscription Rules, which define the Users who are allowed to subscribe for presence information of a particular User, and the subset of the particular User's presence information they are allowed to receive.

The XDM requirements derive to some extent from the requirement documents of Presence SIMPLE ([PRS_RD-V2_0]), PoC ([PoC_RD-V2_1]), SIMPLE IM ([IM_RD]), CPM ([CPM_RD]) and CAB ([CAB_RD]). Please refer to the appropriate documentation for more information.

To make information accessible to the Enablers that need it, the information is stored in the network where it can be located, accessed and manipulated (e.g. created, changed deleted) by authorized Principals. The XDM Enabler defines how such information is represented in XML format and also defines the common protocol for access and manipulation of such information by authorized Principals.

The XDM Enabler specifies XDM Documents that can be re-used 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.

Other OMA Enablers can define the XDM Document structure, or define extensions to the XDM Document structure specified in the XDM Enabler needed for their information, as part of their Enabler specification and make use of the protocol defined in the XDM Enabler for access and manipulation of the information.

5. XML Document Management release description (Informative)

5.1 Version 1.1

The XML Document Management (XDM) enabler defines a common mechanism that makes user-specific service-related information accessible to the service enablers that need it. XDM specifies how such information is represented in well-structured XDM Documents, as well as the common protocol for access and manipulation (e.g. created, changed, deleted, etc.) of such XDM Resources.

5.2 Version 2.0

The XDM V2.0 enabler defines new functionality that extends XDM to support the OMA SIMPLE Instant Messaging (IM) V1.0 and Push-to-talk over Cellular (PoC) V2.0 enablers.

To accommodate the needs of these enablers, the following functionality is added in XDM V2.0:

- Search for information in XDM Resources stored in an XDMS;
- Network to Network Interface to enable search and retrieval of information across multiple domains; and
- The SIP subscription/notification mechanism by which Principals can be notified of changes to XDM Resources.

5.3 Version 2.1

The XDM V2.1 Enabler defines new functionality that extends XDM to support the OMA Converged IP Messaging (CPM) and OMA Converged Address Book (CAB) Enablers.

To accommodate the needs of these Enablers, the following functionality is added in XDM V2.1:

- Support for Alias Principal;
- Access permissions
    - Defining which Principals have rights to perform XDM functions to an XDM Resource;
    - Notifying Principals when their Access Permissions to a specific XDM Resource are changed;
- Document history management in order to capture some (or all) changes applied to an XDM Document;
- Restore operation which enables the authorized Principals to restore the XDM Documents to one of its previous versions;
- Forwarding of an XDM Resource by a Principal with appropriate permissions to other Principals;
- User Preferences Profiles which controls aspects of how a User perceives and receives services;
- Support for searching for active sessions;
- Document Reference which enables authorized Principals to share the contents of an XDM Document with other Principals;
- An alternative mechanism to SIP to perform subscription to XDM Resource changes and receive notifications indicating XDM Resource creations, modifications and removals;
- Extensions to User Access Policy and Group Documents; and
- Document Management optimization to allow modifying two or more XDM Document Parts with one modify request.

5.4 Version 2.2

This version adds support for operations on Application Usages with multiple documents.

6. Requirements (Normative)

The following section details requirements for the XDM Enabler.

6.1 Modularisation

The XDM Enabler does not currently include requirements modules.

6.2 High-Level Functional Requirements

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.

Label	Description	Release	Functional module
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 XDM Documents described in an extensible and platform-neutral format.	XDM 1.1	
GEN-003	Each XDM Resource SHALL be identified by at least one globally unique identifier - i.e., a URI according to [RFC3986].	XDM 1.1	
GEN-004	The XDM Enabler SHALL allow an authorized Principal to access and manage stored XDM Resource s from any capable device type over any capable network.	XDM 1.1	
GEN-005	Data consistency of information stored in the XDM Enabler SHALL be ensured, particularly if simultaneous access by multiple authorized end-users and/or multiple devices is allowed.	XDM 1.1	
GEN-006	There SHALL be one and only one Primary Principal of a XDM Document.	XDM 1.1	
GEN-007	The XDM Enabler SHALL allow a Principal to retrieve a list of all stored XDM Documents for which the Principal is the Primary Principal.	XDM 1.1	
GEN-008	The XDM Enabler SHALL allow a Principal to retrieve a list of all stored XDM Documents for which the Principal is the Primary Principal per type of service (e.g., all XDM Documents related to his PoC service).	XDM 1.1	
GEN-009	It SHOULD be possible to provision the XDM Client using existing OMA Device Management and Provisioning Enablers.	XDM 1.1	
GEN-010	XDM Documents SHALL support multiple character sets.	XDM 1.1	
GEN-011	The XDM Enabler SHALL support interfaces that are access technology neutral.	XDM 1.1	
GEN-012	The XDM Enabler SHALL provide a single contact point for all XDM Clients to access XDM Documents managed by the XDM Enabler.	XDM 1.1	
GEN-013	The XDM Enabler SHALL provide a Web Service based interface to manage XDM Documents stored in the XDM Enabler.	Deleted	
GEN-014	The Service Provider SHALL be able to specify that a Principal is an Alias Principal.	XDM 2.1	
GEN-015	The XDM Enabler SHALL support that an Alias Principal shares all XDM Documents associated with the associated Principal.	XDM 2.1	

GEN-016	XML document management operations performed on the Alias Principal's XDM Documents SHALL produce the same result as operations performed on XDM Documents belonging to the associated Principal.	XDM 2.1	
GEN-017	The XDM Enabler MAY be able to include alternative modification hints in an error response when a document modification request fails due to XML schema constraints	Future Release	

Table 1: High-Level Functional Requirements - General

6.2.1 Security

Label	Description	Release	Functional module
	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 2: High-Level Functional Requirements – Security Items

6.2.2 Charging

Label	Description	Release	Functional module
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 an XDM Resource. 2) The number of XDM Documents for which the end-user is the Primary Principal.	Future release	

Table 3: High-Level Functional Requirements – Charging Items

6.2.3 Usability

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

Table 4: High-Level Functional Requirements – Usability Items

6.2.4 Interoperability

Interoperability of the XDM Enabler is provided through the definition of open interfaces and a consistent format of XDM Documents and XDM functions in compliance with the requirements presented in this document.

Label	Description	Release	Functional module
	The XDM functions, open interfaces and XDM Document formats SHALL provide interoperability to include at least the following:		
IOP-001	Administration of XDM Documents.	XDM 1.1	
IOP-002	Transfer of XDM Documents over open interfaces.	XDM 1.1	
IOP-003	Search XDM Documents over open interfaces.	XDM 1.1	
IOP-004	General structure of the XDM Documents transferred over open interfaces.	XDM 1.1	
IOP-005	Collection and general format of charging information.	XDM 1.1	
IOP-006	XDM 2.0 Enabler SHALL support XDM 1.1 Enabler functionality.	XDM 2.0	
IOP-007	While connected to the XDM 1.1 Enabler, XDM 2.0 Clients SHALL support the XDM 1.1 functionality.	XDM 2.0	
IOP-008	XDM 2.1 Enabler SHALL support XDM 2.0 Enabler functionality.	XDM 2.1	
IOP-009	While connected to the XDM 2.0 Enabler, XDM 2.1 Clients SHALL support the XDM 2.0 functionality.	XDM 2.1	

Table 5: High-Level Functional Requirements – Interoperability Items

6.2.5 Privacy

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

Table 6: High-Level Functional Requirements – Privacy Items

6.2.6 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	Release	Functional module
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 7: High-Level Functional Requirements – Lawful Intercept

6.2.7 Document Management Functions

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

Label	Description	Release	Functional module
	Document management functions SHALL be controlled by Access Permissions which determine the capabilities available to a Principal wishing to perform a particular function on an XDM Resource. Such Access Permissions SHALL be based on:		
FUNC-DMT-001	A default authorization policy associated with the XDM Document type which cannot be modified by any Principal.	XDM 1.1	
FUNC-DMT-002	Access Permissions associated with each XDM Resource (see section 6.2.8).	XDM 2.1	
FUNC-DMT-003	Principals who try to perform a document management function SHALL first be authenticated.	XDM 1.1	
FUNC-DMT-004	The Primary Principal and the Admin Principal SHALL be assigned to an XDM Document when it is created.	XDM 2.1	

Table 8: Functional Requirements – Document Management

6.2.7.1 Create

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

Table 9: Functional Requirements – Document Management Create

6.2.7.2 Retrieve

Label	Description	Release	Functional module
FUNC-RETR-001	Principals with appropriate permissions SHALL be able to retrieve a XDM Document	XDM 1.1	
FUNC-RETR-002	Principals with appropriate permissions SHALL be able to retrieve information about the difference between the latest XDM Document version and the XDM Document version specified in the retrieve request.	XDM 2.1	
FUNC-RETR-003	When a retrieve operation permits the Principal to access authorized XDM Document Parts of the requested XDM Document, the XDM Enabler SHALL return an XDM Document resulting from the consolidation of those XDM Document Parts.	XDM 2.1	

Table 10: Functional Requirements – Document Management Retrieve

6.2.7.3 Copy

Label	Description	Release	Functional module
FUNC-COPY-001	Principals with appropriate permissions SHALL be able to copy XDM Documents within the same XDMS instance, or to another XDMS instance.	Future Release	
FUNC-COPY-002	Principals with appropriate permissions SHALL be able to copy XDM Documents Parts from one XDM Document to another XDM Document within the same XDMS instance.	Future Release	

Table 11: Functional Requirements – Document Management Copy

6.2.7.4 Delete

Label	Description	Release	Functional module
FUNC-DEL-001	Principals with appropriate permissions SHALL be able to delete a XDM Resource.	XDM 1.1	
FUNC-DEL-002	Principals with appropriate permissions MAY be able to delete multiple XDM Documents within the same Application Usage with one delete request.	XDM 2.2	

Table 12: Functional Requirements – Document Management Delete

6.2.7.5 Modify

Label	Description	Release	Functional module
FUNC-MOD-001	Principals with appropriate permissions SHALL be able to modify an XDM Resource.	XDM 1.1	
FUNC-MOD-002	Principals with appropriate permissions SHALL be able to modify two or more XDM Document Parts with one modify request.	XDM 2.1	

Table 13: Functional Requirements – Document Management Modify

6.2.7.6 Forward

Label	Description	Release	Functional module
FUNC-FWD-001	The XDM Enabler MAY support the forwarding of XDM Documents or XDM Document Parts.	XDM 2.1	
FUNC-FWD-002	If forwarding is supported, the Principals with appropriate permissions SHALL be able to forward XDM Documents or XDM Document Parts to other Principals.	XDM 2.1	
FUNC-FWD-003	If forwarding is supported, the forwarding Principal SHALL be able to filter the contents of an XDM Document or XDM Document Parts without affecting the original XDM Document, before forwarding it.	XDM 2.1	
FUNC-FWD-004	If forwarding is supported, the Principals receiving the forwarded XDM Documents or XDM Document Parts SHALL be able to accept or reject them.	XDM 2.1	
FUNC-FWD-005	If forwarding is supported, the receiving Principals who accept forwarded XDM Documents or XDM Document Parts SHALL own the forwarded XDM Resource and SHALL be regarded as creators of those XDM Resources.	XDM 2.1	
FUNC-FWD-006	If forwarding is supported, the Principals with appropriate permissions MAY be able to forward multiple XDM Documents within same Application Usage to other Principals with one forwarding request.	Future Release	

Table 14: Functional Requirements – Document Management Forward

6.2.7.7 Suspend

Label	Description	Release	Functional module
FUNC-SUSP-001	Principals with appropriate permissions SHALL be able to suspend access to and use of an XDM Document.	Future release	
FUNC-SUSP-002	When access to and use of an XDM Document is suspended, no operation SHALL be permitted on the XDM Document, except to take it out of the suspend state or to delete it.	Future release	

Table 15: Functional Requirements – Document Management Suspend

6.2.7.8 Resume

Label	Description	Release	Functional module
FUNC-RESM-001	Principals with the appropriate permission SHALL be able to resume access to and use of a suspended XDM Document.	Future release	
FUNC-RESM-002	After a resume operation, all operations SHALL be possible to be performed on that XDM Document. A subsequent resume operation SHALL be ignored.	Future release	

Table 16: Functional Requirements – Document Management Resume

6.2.7.9 Search

Label	Description	Release	Functional module
FUNC-SRCH-001	The XDM Enabler MAY support search for information within XDM Documents.	XDM 2.0	
FUNC-SRCH-002	It SHALL be possible to search for the existence of certain content (e.g., the identifier of a User) in an XDM document.	XDM 2.0	
FUNC-SRCH-003	It SHALL be possible to search for the existence of an XDM Document based on meta-data associated with the XDM Document.	Future release	
FUNC-SRCH-004	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	It SHALL be possible to search XDM Documents hosted by the Service Provider.	XDM 2.0	
FUNC-SRCH-006	It MAY be possible to search XDM Documents hosted by other Service Providers.	XDM 2.0	
FUNC-SRCH-007	The content of search results SHALL be subject to Service Provider policy or end-user privacy settings.	Future release	
FUNC-SRCH-008	It SHALL be possible to use wildcards in the search criteria when searching XDM Documents.	XDM 2.0	
FUNC-SRCH-009	Search SHALL be limited to one XDM Document type (e.g. Group XDM Document) at a time.	XDM 2.0	
FUNC-SRCH-010	The XDM Enabler MAY provide a mechanism to limit local User Profile searches to Users who have a searchable User Profile.	Future release	
FUNC-SRCH-011	The XDM Client SHALL be able to use basic logical operations (AND, OR, NOT) when searching XDM Documents.	XDM 2.0	
FUNC-SRCH-012	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	The XDM Enabler MAY combine search responses received from other Service Providers.	XDM 2.0	

FUNC-SRCH-014	The Service Provider SHALL be able to limit the number of logical operations in a search request.	XDM2.0	
FUNC-SRCH-015	A User performing a search MAY specify which information the User wants to receive as a result of the search.	XDM2.0	

Table 17: Functional Requirements – Document Management Search

6.2.7.10 Subscription to Changes

Label	Description	Release	Functional module
FUNC-SUBCHG-001	Principals with appropriate permissions SHALL be able to subscribe to and receive notifications regarding updates to XDM Resources.	XDM 2.0	
	The XDM Enabler SHALL support a mechanism to perform subscription to XDM Resource changes and receive notifications:		
FUNC-SUBCHG-002	1) Indicating XDM Resource creations, modifications and removals; OR	XDM 2.0	
FUNC-SUBCHG-003	2) Containing all individual updates performed on the XDM Resource.	XDM 2.0	
FUNC-SUBCHG-004	The XDM Enabler SHALL support an alternative mechanism to SIP to perform subscription to XDM Resource changes and receive notifications indicating XDM Resource creations, modifications and removals.	XDM 2.1	
FUNC-SUBCHG-005	A Principal SHALL with a single subscription be able to subscribe to notifications regarding changes to multiple XDM Resources.	XDM 2.0	
FUNC-SUBCHG-006	During a subscription to XDM Resource changes a Principal SHALL be able to suppress and resume the sending of notifications. Note: For SIP-based subscriptions, RFC 5839 Sections 5.5, 6.2, and 6.3 are referenced here.	XDM 2.2	
FUNC-SUBCHG-007	When refreshing the subscription's expiration time a Principal SHALL be able to request suppression of the initial notification if the information has not been changed. Note: For SIP-based subscriptions, RFC 5839 Section 5.6 is referenced here.	XDM 2.2	
FUNC-SUBCHG-008	When terminating a subscription a Principal SHALL be able to request suppression of the final notification. Note: For SIP-based subscriptions, RFC 5839 Section 5.7 is referenced here.	XDM 2.2	
FUNC-SUBCHG-009	A Principal SHALL be able to request a minimum time interval between two consecutive notifications.	Future Release	

Table 18: Functional Requirements –Subscription to Changes

6.2.7.11 Document Reference

Label	Description	Release	Functional module
FUNC-SHARE-001	A Principal with appropriate permissions SHALL be able to refer another Principal's XDM Document.	XDM 2.1	
FUNC-SHARE-002	A Principal with appropriate permissions SHALL be able to refer a particular XDM Document Part of the other Principal's XDM Document.	Future Release	
FUNC-SHARE-003	A Principal with appropriate permissions SHALL be able to update the content in a XDM Document that is being referred.	XDM 2.1	

FUNC-SHARE-004	Access Permission rights associated with the referenced XDM Document SHALL also apply for the reference.	XDM 2.1	
FUNC-SHARE-005	The XDM enabler SHALL support that all document management operations towards an XDM Document referencing another XDM Document or XDM Document Part is handled as an operation towards the referenced XDM Document.	XDM 2.1	
FUNC-SHARE-006	A Principal with appropriate permissions SHALL be able to refer to another Principal's XDM Document and be able to select which XDM Document Parts of the referred XDM Document to be included.	XDM 2.2	

Table 19: Functional Requirements – Document Reference

6.2.7.12 Restore

Label	Description	Release	Functional module
FUNC-RES-001	XDM Enabler MAY support an XDM Document restore function.	XDM 2.1	
FUNC-RES-002	Authorized Principals SHALL be able to restore an XDM Document to one of its previous versions when the XDM Document is associated with XDM history information. Note: The Service Provider may limit use of the XDM Document restore function.	XDM 2.1	

Table 20: Functional Requirements –Restore

6.2.8 Access Permissions

Access Permissions define which Principals have rights to perform which XDM functions on the associated XDM Resource.

Label	Description	Release	Functional module
	Access Permissions SHALL include the following data:		
ACP-001	1) Identities of the Principals who have Access Permissions to the associated XDM Document.	XDM 2.1	
	2) Operations these Principals are allowed to perform on the associated XDM Document. Operations SHALL include the following:		
ACP-002	a) Retrieve NOTE: Access Permission for subscription to changes is dependent on having Access Permission for the Retrieve operation.	XDM 2.1	
ACP-003	b) Search	XDM 2.1	
ACP-004	c) Modify	XDM 2.1	
ACP-005	d) Delete	XDM 2.1	
ACP-006	e) Create	XDM 2.1	
ACP-007	f) Restore	XDM 2.1	
ACP-008	g) Copy	Future Release	
ACP-009	h) Forward	XDM 2.1	
ACP-010	i) Suspend	Future release	
ACP-011	j) Resume	Future release	

ACP-012	k) Document reference	XDM 2.1	
	3) Operations these Principals are allowed to perform on the associated XDM Document Parts. Operations SHALL include the following:		
ACP-013	a) Retrieve NOTE: Access Permission for subscription to changes is dependent on having Access Permission for the Retrieve operation.	XDM 2.1	
ACP-014	b) Add or Modify	XDM 2.1	
ACP-015	c) Delete	XDM 2.1	
ACP-016	d) Copy	Future release	
ACP-017	e) Forward	XDM 2.1	
ACP-018	f) Partial document reference	Future release	
	Access Permissions MAY include the following data:		
ACP-019	1) Rule to be applied to all identities not explicitly listed within identities of the Principals who have Access Permissions to the associated XDM Document.	XDM 2.1	
ACP-019A	2) Rule to be applied to multiple XDM Documents.	XDM 2.2	
ACP-020	The Admin Principal of the associated XDM Document SHALL be the only one who has rights to modify the Access Permissions.	XDM 2.1	
ACP-021	The Access Permissions SHALL be managed with the same underlying mechanisms as defined in section 6.2.7.	XDM 2.1	
ACP-022	At the creation of a document, the default Access Permissions SHALL be generated automatically and prevent all Principals, except the Primary Principal, to perform any document management operations.	XDM 2.1	
ACP-023	An Admin Principal SHALL be able to authorize other Principals to perform selected document management operations on an XDM Document or XDM Document Part.	XDM 2.1	
ACP-024	It SHALL be possible to modify the Access Permissions at any time, from creation to deletion of the associated XDM Resource.	XDM 2.1	
ACP-025	It SHOULD be possible for Principals to retrieve their own Access Permissions applied to a specific XDM Resource.	XDM 2.1	
ACP-026	The Access Permissions associated with an XDM Document SHALL be deleted upon deletion of the XDM Document.	XDM 2.1	
ACP-027	It SHALL be possible to notify Principals when their Access Permissions to a specific XDM Resource are changed based on the Primary Principal's User setting, Service Provider policy, type of document and/or type of Access Permission(s).	XDM 2.1	
ACP-028	The XDM Enabler SHALL provide means to enable an authorized Principal to be notified about any Principal's subscription or retrieval operation of an XDM Resource.	XDM 2.1	
ACP-029	An Admin Principal SHALL be able to retrieve Access Permissions associated with an XDM Resource.	XDM 2.1	

Table 21: Functional Requirements – Access Permissions

6.2.9 XDM History

The XDM history contains a history of XDM operations performed on the associated XDM Document.

Label	Description	Release	Functional module
HST-001	An XDM Document MAY be associated with XDM history information.	XDM 2.1	
HST-002	The XDM history information SHALL be associated with the XDM Document, when Access Permissions for certain operations (e.g. create, modify, delete, suspend, resume) is granted to other Principals, unless the Primary Principal explicitly disables the XDM history function on this XDM Document.	XDM 2.1	
HST-003	The Admin Principal SHALL be the only one who has rights to enable and disable the XDM history function, on a per-XDM Document basis.	XDM 2.1	
	The XDM history information of the performed operations SHALL include at least:		
HST-004	1) Type of operation;	XDM 2.1	
HST-005	2) Timestamp of operation;	XDM 2.1	
HST-006	3) Identity of the Principal that performed the operation;	XDM 2.1	
HST-007	4) Change details (e.g. modified XDM Resources, deleted XDM Document).	XDM 2.1	
HST-008	If the XDM history function is enabled, the XDM history information of the performed operations SHALL include information about the performed modification on the XDM Resource	XDM 2.1	
HST-009	If the XDM history function is enabled, the XDM history information of the performed operations MAY include information about the performed operations other than modification.	XDM 2.1	
HST-010	The XDM history information SHALL be managed with the same underlying mechanisms as defined in section 6.2.7.	XDM 2.1	
HST-011	An authorized Principal SHALL be able to retrieve the stored XDM history information.	XDM 2.1	
	An authorized Principal MAY be able to:		
HST-012	1) Delete XDM History information;	XDM 2.1	
HST-013	2) Search XDM History information;	XDM 2.1	
HST-014	3) Subscribe for changes in XDM History information.	XDM 2.1	
	Authorized Principals SHALL be able to search, at least, using the following criteria:		
HST-015	1) Type of operation;	XDM 2.1	
HST-016	2) Time range;	XDM 2.1	
HST-017	3) Identity of Principal that performed the operation(s);	XDM 2.1	
HST-018	4) Change details (e.g. modified element/attribute).	Future release	
HST-019	The Service Provider SHALL be able to limit XDM History information. NOTE: The limitation may refer to the number of entries, length of time and/or number of bytes required to save history.	XDM 2.1	
HST-020	The XDM history information SHALL remain stored after deletion of the related XDM Document for the time interval specified by the Service Provider.	XDM 2.1	

	The Admin Principal SHOULD be able to set the XDM history related preferences to specify:		
HST-021	1) Which XDM history information to be stored.	XDM 2.1	
HST-022	2) Conditions upon which the information is stored in XDM history.	XDM 2.1	

Table 22: Functional Requirements – XDM History

6.2.10 XDM Document Properties

Document properties provide meta-data relating to an XDM Document that are not included with its content.

Label	Description	Release	Functional module
DP-001	XDM Documents MAY be associated with meta-data which describes certain properties of the XDM Document that are not included in its content	Future release	
	If XDM Document properties are supported, then they SHALL include the following data:		
DP-002	1) Timestamp of XDM Document creation.	Future release	
DP-003	2) Timestamp of last XDM Document access.	Future release	
	If XDM Document properties are supported, then they MAY include the following data:		
DP-004	1) Time-to-live after creation: The expiry time relative to when the XDM Document was created.	Future release	
DP-005	2) Time-to-live after last access: The expiry time relative to when the XDM Document was last accessed.	Future release	
DP-006	3) Expiration time: An absolute expiry time.	Future release	
DP-007	The Service Provider MAY define maximum possible values for the time-to-live after creation, time-to-live after last access and expiration time XDM Document properties.	Future release	
DP-008	A Principal with appropriate Access Permissions MAY be able to set the value of the time-to-live after creation, time-to-live after last access and expiration time XDM Document properties.	Future release	
DP-009	If the Service Provider defines maximum possible values for the time-to-live after creation, time-to-live after last access and expiration time XDM Document properties, Principal SHALL NOT exceed these values when setting the values of XDM Document properties.	Future release	
DP-010	An expired XDM Document MAY be deleted automatically.	Future release	

Table 23: Functional Requirements – Document Properties

6.2.11 Extended Group Advertisement

Label	Description	Release	Functional module
GRPAD-001	The XDM Enabler MAY support extended group advertisement.	XDM 2.0	

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	
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	
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	
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	
GRPAD-006	Extended group advertisement sent by the XDM Enabler MAY include XCAP URI of corresponding group XDM Document.	XDM 2.1	

Table 24: Functional Requirements – Extended Group Advertisement

6.2.12 User Preferences Profiles

Label	Description	Release	Functional module
UPP-001	The XDM Enabler MAY support User Preferences Profiles.	XDM 2.1	
UPP-002	If User Preferences Profiles are supported, a Primary Principal MAY have one or more User Preferences Profiles.	XDM 2.1	
UPP-003	A User Preferences Profile SHALL be identified by a UPPID which is unique for each User Preferences Profile of a Primary Principal.	XDM 2.1	
UPP-004	The Primary Principal SHALL be able to specify, per relevant User setting, whether that setting is applicable for a particular User Preferences Profile, for a set of User Preferences Profiles, or for all User Preferences Profiles.	XDM 2.1	
UPP-005	If User Preferences Profiles are supported, the Primary Principal SHALL be able to manage User Preferences Profiles.	XDM 2.1	
UPP-006	The XDM Enabler SHALL support that a Primary Principal is able to select one of the User Preferences Profiles as the Active User Preferences Profile for each of his devices.	XDM 2.1	
UPP-007	The XDM Enabler SHALL support that a Primary Principal is able to select one of his User Preferences Profiles as the Default User Preferences Profile from any of his devices.	XDM 2.1	
UPP-008	The Primary Principal SHALL be able to determine which User Preferences Profile is the Active User Preferences Profile for any of his devices.	XDM 2.1	
UPP-009	The Primary Principal SHALL be able to determine which User Preferences Profile is the Default User Preferences Profile from any of the his devices.	XDM 2.1	
UPP-010	The Primary Principal SHALL be able to determine from any of his devices, all applicable User Preference Profiles.	XDM 2.1	

Table 25: Functional Requirements – User Preferences Profiles

6.2.13 Active Sessions

Label	Description	Release	Functional module
ASD-001	If search of Active Sessions is supported, an authorized Principal SHALL be able to search for Active Sessions of another Enabler supporting Active Session search.	XDM 2.1	
ASD-002	Search of Active Sessions SHALL be possible based on session subjects as search criterion.	XDM 2.1	

Table 26: Functional Requirements – Active Sessions

6.2.14 Multiple Devices

Label	Description	Release	Functional module
FUNC-MD-001	XDM Enabler SHALL support usage of multiple devices per Primary Principal.	XDM 1.1	

Table 27: Functional Requirements – Multiple Devices

6.3 XDM Document Types

6.3.1 URI List

Label	Description	Release	Functional module
DOC-URI-001	A URI List SHALL contain a Display name information, representing the human readable name.	XDM 1.1	
DOC-URI-002	A URI List SHALL contain zero or more URI List members.	XDM 1.1	
	The following requirements apply to 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 [RFC3986]).	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 URI List.	XDM 1.1	
DOC-UIR-006	A URI List Document SHALL be able to contain one or more URI Lists	XDM 1.1	

Table 28: URI List

6.3.2 User Profile

Label	Description	Release	Functional module
DOC-USP-001	An XDM Document that 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	This XDM 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 this XDM Document SHALL ensure that all mandatory information elements are also completed.	XDM 2.0	
DOC-USP-004	This XDM Document SHALL support the assignment of permissions to multiple elements in one operation.	Future release	
DOC-USP-005	An XDM Document 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	
	This XDM Document MAY contain the following static information of the User:		
DOC-USP-007	1) User identifier that uniquely identifies the User that this XDM Document 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	There SHALL be two types of XDM Documents: One containing the information [DOC-USP-007 to DOC-USP-036] set by the User; One containing the date of birth of the User [DOC-USP-013 to DOC-USP-016] which is set and locked by the Service Provider.	XDM 2.0	
DOC-USP-038	The authorized Principal of this XDM Document SHALL be able to set the privacy that defines the limitation in searching or accessing the information in this XDM Document.	Future release	

Table 29: User Profile

6.3.3 Group

Label	Description	Release	Functional module
DOC-GRP-001	A Group Document SHALL include a URI attribute to represent a Group Identity.	XDM 2.0	
	A Group Document 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 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 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 Group.	XDM 2.0	
	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:		
DOC-GRP-012	a) Age minimum: This indicates the minimum allowed age of a participant.	XDM 2.0	
DOC-GRP-013	b) Age maximum: This indicates the maximum allowed age of a participant.	XDM 2.0	
	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).		
DOC-GRP-014	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-015	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-016	c) Minimum number of participants: This describes how many must remain participating for the session to remain active.	XDM 2.0	
DOC-GRP-017	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-018	e) Maximum media inactivity timeout: This describes the maximum allowed time of media inactivity (e.g. 40 seconds) for the session to remain active.	Deleted	
DOC-GRP-019	13) Allow sub-conferencing: This describes who may create sub-conferences in a group session.	XDM 2.0	
DOC-GRP-020	14) Allow private messaging: This describes who may send private messages in a group session.	XDM 2.0	
DOC-GRP-021	15) Allowed media: This identifies which media are allowed to be used in a group session e.g. audio, text, video.	XDM 2.0	
DOC-GRP-022	16) Allow conference state: This describes who can see the state of the group session (e.g. who is currently online).	XDM 2.0	
DOC-GRP-023	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-024	18) Dispatcher participant: This identifies who may assume the role of dispatcher (e.g. PoC Dispatcher).	Deleted	
DOC-GRP-025	19) Allow role transfer: This describes who can request the transfer of an active role (e.g. PoC Dispatcher) to another authorized participant.	Deleted	
DOC-GRP-026	20) Allow expelling: This describes who may expel other participants from the group session.	XDM 2.0	
DOC-GRP-027	21) Allow adding media: This describes who may add a media stream to a new or existing group session.	XDM 2.0	
DOC-GRP-028	22) Allow sending media: This describes who is allowed to send media in the group session.	XDM 2.1*	
DOC-GRP-029	23) Allow receiving media: This describes who is allowed to receive media in the group session.	XDM 2.1*	
DOC-GRP-030	24) Allow removing media: This describes who may remove an existing media stream from a group session.	XDM 2.0	
	25) Media add/modify/remove policy: This describes conditions for adding, modifying, or removing a media stream to a particular participant:		
DOC-GRP-031	a) Allow to use multicast bearer service: This describes if a multicast bearer service is allowed to be used in the group session.	Deleted	
DOC-GRP-032	b) Allowed Media Burst Control scheme: This describes what Media Burst Control schemes are allowed to be used in the group session.	Deleted	

DOC-GRP-033	26) Allow to use multicast bearer service: This describes if a multicast bearer service is allowed to be used in the group session.	Deleted	
DOC-GRP-034	27) Allowed Media Burst Control scheme: This describes what Media Burst Control schemes are allowed to be used in the group session.	Deleted	
DOC-GRP-035	28) Moderator: This identifies who is allowed to take the role of moderator (e.g. a PoC Moderator).	Deleted	
	29) Allowed manner to render multiple media streams of same media type: This content describes the allowed manner to render media streams of same media type at in the client of application enabler user equipment (e.g. PoC Client):		
DOC-GRP-036	a) Allow to mix media streams at a partial rate.	XDM 2.1	
DOC-GRP-037	b) Allow one media stream of multiple media streams of the same media type to be mandatory.	XDM 2.1	
	30) Allowed participating information principle: NOTE: This content is used to send session related information to session participants (e.g. participants in a PoC session).		
DOC-GRP-038	a) Allow subscription to limited participating information. NOTE: Limited participant information is a subset of participating information.	XDM 2.1	
DOC-GRP-039	b) Allow subscription to participant information.	XDM 2.1	
DOC-GRP-040	31) Session control for crisis handling: This identifies that Session Control for Crisis Handling SHALL always be used for this group.	Deleted	
DOC-GRP-041	32) Crisis Event handling entity address: This identifies the address of the entity handling Session Control for Crisis Handling (e.g. the address of PoC Session Control for Crisis Handling).	Deleted	
	33) Group specific releasing policy: This describes the conditions under which a group session SHALL or SHALL NOT be released.		
DOC-GRP-042	a) The group session is released or not released when the group session initiator leaves the group session.	Deleted	
DOC-GRP-043	b) The group session is released or not released when the maximum media inactivity timeout expires (e.g. for PoC speech.)	Deleted	
DOC-GRP-044	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-045	Each URI in the Group member list SHALL occur only once.	XDM 1.1	
DOC-GRP-046	Each URI in the Group reject list SHALL occur only once.	XDM 1.1	

DOC-GRP-047	The Service Provider SHALL be able to set the maximum number of participants in a Group Document.	XDM 1.1	
DOC-GRP-048	A Principal with appropriate management permissions MAY be able to set the maximum number of participants in a Group Document to a value that does not exceed the maximum number set by the Service Provider.	XDM 1.1	
DOC-GRP-049	It SHALL be possible to create a Group Document that contains members in the Group member list or Group reject list that belong to different Service Providers.	XDM 1.1	
DOC-GRP-050	If search of Group Documents is supported (see section 6.2.7.9), an authorized Principal SHALL be able to search for Groups based on a given criteria (e.g. display name, session type, subject, Group Identity, etc.).	XDM 2.0	

Table 30: Group

*: Did not require any specific additions in XDM 2.1. Requirement covered in POC using existing XDM 2.0 specifications.

6.3.4 Group Usage List

Label	Description	Release	Functional module
DOC-GUL-001	A Group Usage List SHALL have a Display name: A human readable name.	XDM 1.1	
DOC-GUL-002	A Group Usage List SHALL contain usage information about zero or more Groups.	XDM 1.1	
DOC-GUL-003	A Group defined in a Group Usage List SHALL be identified by a globally unique identifier (i.e., a URI as defined in [RFC3986]).	XDM 1.1	
DOC-GUL-004	A Group defined in a Group Usage List MAY have a Display name: A human readable name.	XDM 1.1	
DOC-GUL-005	A Group defined in a 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 Group Usage List.	XDM 1.1	
DOC-GUL-007	A Group Usage List Document SHALL be able to contain one or more Group Usage Lists.	XDM 1.1	

Table 31: Group Usage List

6.3.5 User Access Policy

Label	Description	Release	Functional module
	The User SHALL be able to specify the following preferences, in a User Access Policy Document, for how an Application Server is to handle an incoming session invitation:		
DOC-UAP-001	1) Reject the session invitation.	XDM 2.0	

DOC-UAP-002	2) Accept the session invitation and send immediately to the User.	XDM 2.0	
DOC-UAP-003	3) Store the session in a specified Communication Storage.	XDM 2.0	
	4) Perform Automatic Answer Mode procedures, as follows:		
DOC-UAP-004	a) Auto answer: This indicates whether the Application Server is to perform Automatic Answer Mode procedures.	XDM 2.0	
DOC-UAP-005	b) Allow manual answer override: When the session invitation contains a request to override Manual Answer Mode procedures, this indicates whether the Application Server is to perform Automatic Answer Mode procedures or reject the session invitation.	XDM 2.0	
DOC-UAP-006	5) Route the session invitation to an alternate communication service, via interworking.	XDM 2.1	
DOC-UAP-007	6) Filtering criteria for storing of the session contents in specified communication storage.	XDM 2.1	
	The User SHALL be able to specify the following preferences, in a User Access Policy Document, for how an Application Server is to handle an incoming pager-mode message:		
DOC-UAP-008	1) Reject the message.	XDM 2.0	
DOC-UAP-009	2) Accept the message and send immediately to the User.	XDM 2.0	
DOC-UAP-010	3) Discard the message and provide a notification to the sender based on sender's preferences.	XDM 2.1	
DOC-UAP-011	4) Store the message in a specified Communication Storage.	XDM 2.1	
DOC-UAP-012	5) Defer the message.	XDM 2.1	
DOC-UAP-013	6) Store the media from the message in a network-based Communication Storage, and allow the User to receive the message without the media by including a link to access this media in the Communication Storage.	XDM 2.1	
DOC-UAP-014	7) Route the message to an alternate communication service, via interworking.	XDM 2.1	
DOC-UAP-015	8) Filtering criteria for storing of the message contents in specified communication storage.	XDM 2.1	
	The User SHALL be able to specify different preferences for handling incoming requests, depending on:		
DOC-UAP-016	1) The identity of the request initiator.	XDM 2.0	
DOC-UAP-017	2) Whether the request initiator has requested anonymity.	XDM 2.0	
	3) The message-type associated with the request, which MAY be one of the following:		
DOC-UAP-018	a) Session-based message	XDM 2.0	

DOC-UAP-019	b) Pager mode message	XDM 2.0	
	4) The media-type associated with the request, which MAY be one or more of the following:		
DOC-UAP-020	a) File transfer	XDM 2.0	
DOC-UAP-021	b) Audio	XDM 2.0	
DOC-UAP-022	c) Video	XDM 2.0	
DOC-UAP-023	d) PoC speech	XDM 2.0	
DOC-UAP-024	e) Group advertisement	XDM 2.0	
DOC-UAP-025	f) Text	XDM 2.1	
DOC-UAP-026	g) Image	XDM 2.1	
DOC-UAP-027	h) Binary data	XDM 2.1	
	5) The service-type associated with the request, which MAY be one or more of the following:		
DOC-UAP-028	a) A particular service Enabler defined by OMA (e.g. PoC, IM).	XDM 2.0	
DOC-UAP-029	6) The priority associated with the request (i.e. “non-urgent”, “normal”, “urgent”, and “emergency” as described in [RFC3261])	XDM 2.1	
DOC-UAP-030	7) The User Preferences Profile Identity.	XDM 2.1	
DOC-UAP-031	8) Availability of the User.	XDM 2.1	
DOC-UAP-032	9) Quality of Experience associated with the request.	XDM 2.1	
	The User MAY be able to specify the media content adding, replacement or removing preference for incoming or outgoing invitation requests:		
DOC-UAP-033	1) Removing media content in an incoming invitation request	XDM 2.1	
DOC-UAP-034	2) The media content which adds or replaced media content in an incoming invitation request.	XDM 2.1	
DOC-UAP-035	3) Media content (reference or text based content) to be added in an outgoing invitation request.	XDM 2.1	
	The User MAY be able to specify different preferences for handling incoming requests, depending on:		
DOC-UAP-036	1) The current date and time.	XDM 2.1	
DOC-UAP-037	2) The identities of the invited Users.	XDM 2.1	
DOC-UAP-038	3) The User's presence activity information element.	XDM 2.1	
DOC-UAP-039	The Subscriber MAY be able to specify different preferences for handling incoming communication requests depending on the same attributes as for the User.	XDM 2.1	

	The User and the Subscriber MAY be able to specify different preferences for handling outgoing communication requests, depending on:		
	1) The media-type associated with the request, which MAY be one or more of the following:		
DOC-UAP-040	a) File transfer	XDM 2.1	
DOC-UAP-041	b) Audio	XDM 2.1	
DOC-UAP-042	c) Video	XDM 2.1	
DOC-UAP-043	d) PoC speech	XDM 2.1	
DOC-UAP-044	e) Group advertisement	XDM 2.1	
DOC-UAP-045	f) Text	XDM 2.1	
DOC-UAP-046	g) Image	XDM 2.1	
DOC-UAP-047	h) Binary data	XDM 2.1	
DOC-UAP-048	2) The Quality of Experience associated with the request.	XDM 2.1	
DOC-UAP-049	3) The current date and time.	XDM 2.1	
DOC-UAP-050	4) The identities of the invited Users.	XDM 2.1	
DOC-UAP-051	5) The country or region in which the invited User's home network is located.	XDM 2.1	
DOC-UAP-052	6) The geographical location of the inviting and invited Users.	XDM 2.1	
DOC-UAP-053	7) The invited Users' presence activity information elements.	XDM 2.1	
DOC-UAP-054	It SHALL be possible to determine which preferences for handling incoming or outgoing communication requests have been specified by the User and which preferences have been specified by the Subscriber.	XDM 2.1	

Table 32: User Access Policy

6.3.6 UPP Directory

Label	Description	Release	Functional module
DOC-PPD-001	The UPP Directory Document SHALL contain meta data about a Primary Principal's User Preferences Profiles.	XDM 2.1	
	A UPP Directory Document SHALL, per User Preferences Profile, contain the following meta data:		
DOC-PPD-002	1) A User Preferences Profile Identifier.	XDM 2.1	
DOC-PPD-003	2) A Display name representing a human readable name.	XDM 2.1	
DOC-PPD-004	The UPP Directory Document SHALL contain information about which User Preferences Profile is the Active User Preferences Profile per device.	XDM 2.1	

DOC-PPD-005	The UPP Directory Document SHALL contain information about which User Preferences Profile is the Default User Preferences Profile.	XDM 2.1	

Table 33: UPP Directory

6.4 Overall System Requirements

Overall system requirements are not applicable to XDM.

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
OMA-RD-XDM-V2_2-20160503-A	03 May 2016	Status changed to Approved by TP TP Ref # OMA-TP-2016-0052R01-INP_XDM_V2_2_ERP_for_final_Approval

Appendix B. 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.

B.1 Use Case – URI List

See [XDM_RD-V1_1] “URI List”.

B.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*”.

B.3 Use Case – Groups

See [XDM_RD-V1_1] “*Groups*”.

B.4 Use Case – P2P Using a Group List

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

B.5 Use Case – Group Visibility

See [XDM_RD-V1_1] “*Group Visibility*”.

B.6 Use Case – Assigning Permissions

See [XDM_RD-V1_1] “*Assigning Permissions*”.

B.7 Use Case – Access Control Policy

See [XDM_RD-V1_1] “*Access Control Policy*”.

B.8 Use Case – Blocking or Granting communication from different end-users

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

B.9 Use Case – Retrieving a List of Lists

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

B.10 Use Case – Document History Management

B.10.1 Short Description

It is possible for a Primary Principal to assign specific document functions to other authorised Users. As a follow-on to this functionality, it is often desirable for the Primary Principal to be aware of some (or all) of the changes to a document. This

use case demonstrates a scenario for document history management. This includes enabling/disabling the document history function, as well as the review of all or a subset of changes made to a document.

B.10.1.1 Actors

Service Provider

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

B.10.1.2 Normal Flow

1) John enables the document management history storage option on the Group document, using his document management-capable device.
2) During a vacation, John authorizes Jeff to perform specific operations (e.g. modify Group document) on the Group and coordinate communication.
3) Alice needs to clarify quality audit related aspects from the development team and informs Jeff.
4) Jeff initiates an IM Group conversation.
5) Alice discusses with Jeff and Bob regarding the quality aspects.
6) Jeff wants to get the expert opinion from the quality assurance department of his organization
7) Jeff adds Alan into the Group and invites him to join the conversation
8) Server updates the history information for the document management operation performed by Jeff.
9) Alan joins the conversation and discusses quality related aspects with the Group and clarifies the doubts.
10) John returns back from vacation and searches the history information for documents updates and retrieves the history information.
11) John finds that, during his absence, Jeff has modified the Group document by adding Alan. Given Alan is still a member of the Group, John removes him as he is no longer required to participate in day to day communication relating to the project.
12) Server updates the document history information for the operations performed by John.

B.10.2 Market Benefits

End-user is able to activate the history management feature and can track the operations carried out on the document on his group list at a later stage.

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.

B.11 Use Case – Sending Group Information to Members of the Group

See [XDM_RD-V2_0] “Sending Group Information to Members of the Group”.

B.12 Use Case – Forwarding XML Documents

B.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.

B.12.1.1 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.

B.12.1.2 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.

B.12.2 Market Benefits

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 user's tree by the forward operation.

B.13 Use Case – Exchange of User Profile data

B.13.1 Short Description

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

The 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.

B.13.1.1 Actors

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

Leo: A friend of Roger's

Martin: A colleague of Roger's

B.13.1.2 Normal Flow

1) Roger obtains Leo and Martin identifiers for their User Profile (e.g. through search or any external means)
2) Roger subscribes to the changes of Leo and Martin's 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

B.13.1.3 Alternative Flow

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

B.13.2 Market Benefits

The organization of data into categories will encourage the use of the 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. Further, a User will always have an updated profile of his contacts when required, and the User sharing their personal information maintains privacy control on their information thanks to Groups of attributes.

B.14 Use Case – Third-party Service Provider Managing User Service-related Data

B.14.1 Short Description

This use case describes a scenario where a third-party Service Provider application (with appropriate rights) acceses and manages user service-related data stored in the network.

B.14.1.1 Actors

Third-party Service Provider

Network operator

Daniela (the end-user)

B.14.1.2 Normal Flow

1) Third-party Service Provider has an idea on a new and appealing service that needs to use XDM network capabilities.
2) Third-party Service Provider deploys the new service.
3) The new service is offered to end-users.
4) Daniela enjoys the new service.

B.14.2 Market Benefits

The possibility of exposing XDM network capabilities to third-party Service Providers will ease the adoption of the XDM Enabler by network operators. Also, the usage of a common interface will increase the usage of the XDM Enabler by third-party Service Providers and enable new business opportunities. Further, the third-party Service Provider can offer new and appealing services to end-users.

B.15 Service Enabler Specific Use Case – Push to talk over Cellular (PoC) – Creation and Advertising Group List

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

B.16 Service Enabler Specific Use Case – Push to talk over Cellular (PoC) – User Defined Group Call One-to-Many

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

B.17 Service Enabler Specific Use Case – Push to talk over Cellular (PoC) – Private Chat Group Support One to Many

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

B.18 Service Enabler Specific Use Case – Push to talk over Cellular (PoC) – Use of Multiple Group Operation

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

B.19 Service Enabler Specific Use Case – Push to talk over Cellular (PoC) – Ad-hoc Chat Group Support One-to-Many

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

B.20 Service Enabler Specific Use Case – Push to talk over Cellular (PoC) – Corporate Chat

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

B.21 Service Enabler Specific Use Case – Push to talk over Cellular (PoC) – PoC Fleet Dispatch: One-to-Many-to-One

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

B.22 Service Enabler Specific Use Case – Instant Messaging (IM) - Use of Group Management

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

B.23 Service Enabler Specific Use Case – Instant Messaging (IM) - Add Contact to Contact List by User ID or Search

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

B.24 Service Enabler Specific Use Case – Instant Messaging (IM) – Use of Public Chat

See [IM_RD] "*Public Chat*".

B.25 Service Enabler Specific Use Case – Instant Messaging (IM) – Modify Contact Entry

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