



XML Document Management Architecture

Candidate Version 1.0 – 28 Jun 2005

Open Mobile Alliance
OMA-AD-XDM-V1_0-20050628-C

Use of this document is subject to all of the terms and conditions of the Use Agreement located at <http://www.openmobilealliance.org/UseAgreement.html>.

Unless this document is clearly designated as an approved specification, this document is a work in process, is not an approved Open Mobile Alliance™ specification, and is subject to revision or removal without notice.

You may use this document or any part of the document for internal or educational purposes only, provided you do not modify, edit or take out of context the information in this document in any manner. Information contained in this document may be used, at your sole risk, for any purposes. You may not use this document in any other manner without the prior written permission of the Open Mobile Alliance. The Open Mobile Alliance authorizes you to copy this document, provided that you retain all copyright and other proprietary notices contained in the original materials on any copies of the materials and that you comply strictly with these terms. This copyright permission does not constitute an endorsement of the products or services. The Open Mobile Alliance assumes no responsibility for errors or omissions in this document.

Each Open Mobile Alliance member has agreed to use reasonable endeavors to inform the Open Mobile Alliance in a timely manner of Essential IPR as it becomes aware that the Essential IPR is related to the prepared or published specification. However, the members do not have an obligation to conduct IPR searches. The declared Essential IPR is publicly available to members and non-members of the Open Mobile Alliance and may be found on the “OMA IPR Declarations” list at <http://www.openmobilealliance.org/ipr.html>. The Open Mobile Alliance has not conducted an independent IPR review of this document and the information contained herein, and makes no representations or warranties regarding third party IPR, including without limitation patents, copyrights or trade secret rights. This document may contain inventions for which you must obtain licenses from third parties before making, using or selling the inventions. Defined terms above are set forth in the schedule to the Open Mobile Alliance Application Form.

NO REPRESENTATIONS OR WARRANTIES (WHETHER EXPRESS OR IMPLIED) ARE MADE BY THE OPEN MOBILE ALLIANCE OR ANY OPEN MOBILE ALLIANCE MEMBER OR ITS AFFILIATES REGARDING ANY OF THE IPR'S REPRESENTED ON THE “OMA IPR DECLARATIONS” LIST, INCLUDING, BUT NOT LIMITED TO THE ACCURACY, COMPLETENESS, VALIDITY OR RELEVANCE OF THE INFORMATION OR WHETHER OR NOT SUCH RIGHTS ARE ESSENTIAL OR NON-ESSENTIAL.

THE OPEN MOBILE ALLIANCE IS NOT LIABLE FOR AND HEREBY DISCLAIMS ANY DIRECT, INDIRECT, PUNITIVE, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES ARISING OUT OF OR IN CONNECTION WITH THE USE OF DOCUMENTS AND THE INFORMATION CONTAINED IN THE DOCUMENTS.

© 2005 Open Mobile Alliance Ltd. All Rights Reserved.

Used with the permission of the Open Mobile Alliance Ltd. under the terms set forth above.

Contents

1.	SCOPE (INFORMATIVE)	5
2.	REFERENCES	6
2.1	INFORMATIVE REFERENCES	6
3.	TERMINOLOGY AND CONVENTIONS	8
3.1	CONVENTIONS	8
3.2	DEFINITIONS	8
3.3	ABBREVIATIONS	8
4.	INTRODUCTION (INFORMATIVE).....	10
4.1	TARGET AUDIENCE	10
4.2	REQUIREMENTS.....	11
5.	FEATURES (INFORMATIVE)	12
5.1	AUTHENTICATION	12
5.2	DOCUMENT MANAGEMENT OPERATIONS.....	12
5.3	NOTIFICATIONS OF CHANGED DATA	12
6.	CONTEXT MODEL (INFORMATIVE).....	13
6.1	CONTEXT COLLABORATION MODEL	13
6.1.1	Functions.....	13
6.1.2	Collaboration with other Service Enablers.....	13
7.	ARCHITECTURAL MODEL (INFORMATIVE)	14
7.1	XML DOCUMENT MANAGEMENT FUNCTIONAL ENTITIES	14
7.1.1	XML Document Management Client.....	14
7.1.2	Aggregation Proxy	14
7.1.3	Shared XML Document Management Server	15
7.2	ENABLER SPECIFIC FUNCTIONAL ENTITIES.....	15
7.2.1	Enabler specific XML Document Management Server	15
7.2.2	Enabler specific Server	15
7.3	EXTERNAL ENTITIES PROVIDING SERVICES TO XML DOCUMENT MANAGEMENT.....	15
7.3.1	SIP/IP Core	15
7.3.2	Device Management Server	16
7.4	DESCRIPTION OF REFERENCE POINTS	16
7.4.1	Reference Point XDM-1: XDM Client – SIP/IP Core	16
7.4.2	Reference Point XDM-2: Shared XDMS – SIP/IP-Core	16
7.4.3	Reference Point XDM-3: XDM Client – Aggregation Proxy	16
7.4.4	Reference Point XDM-4: Aggregation Proxy – Shared XDMS	16
7.4.5	Reference Point DM-1: DM Client – DM Serve.....	17
7.4.6	Reference Points: “Enabler specific XDMS” - SIP/IP Core	17
7.4.7	Reference Points: “Enabler specific Server” - SIP/IP Core	17
7.4.8	Reference Points: Aggregation Proxy – “Enabler specific XDMS”	17
7.4.9	Reference Points : Shared XDMS – “Enabler specific Server”	17
7.4.10	Reference Points: “Enabler specific XDMS” – “Enabler specific Server”	17
7.5	ACCESS CONTROL.....	18
7.6	SECURITY	18
7.7	CHARGING.....	18
7.8	XML DOCUMENT MANAGEMENT SERVICE PROVISIONING.....	18
APPENDIX A.	CHANGE HISTORY (INFORMATIVE).....	19
A.1	APPROVED VERSION HISTORY	19
A.2	DRAFT/CANDIDATE VERSION 1.0 HISTORY	19

Figures

Figure 1: XML Document Management Architecture 14

1. Scope (Informative)

This document presents an overview of the XML Document Management (XDM) enabler. Specifically, it serves as an introduction to the functionality and architecture (i.e. logical entities and reference points between them) of the XDM enabler.

2. References

2.1 Informative References

IETF References

- [RFC2119] "Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, March 1997, [URL:http://www.ietf.org/rfc/rfc2119.txt](http://www.ietf.org/rfc/rfc2119.txt)
- [RFC2617] "HTTP Authentication: Basic and Digest Access Authentication", Franks, J., Hallam-Baker, P., Hostetler, J., Lawrence, S., Leach, P., Luotonen, A. and L. Stewart, June 1999, RFC 2617, (<http://www.ietf.org/rfc/rfc2617.txt>)
- [RFC2818] "HTTP Over TLS", Rescorla, E., May 2000, RFC 2818, (<http://www.ietf.org/rfc/rfc2818.txt>)
- [RFC3261] "[SIP: Session Initiation Protocol](http://www.ietf.org/rfc/rfc3261.txt)", Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M. and E. Schooler, June 2002, RFC 3261, (<http://www.ietf.org/rfc/rfc3261.txt>)
- [RFC3546] Transport Layer Security (TLS) Extensions S. Blake-Wilson, M. Nystrom, D. Hopwood, J. Mikkelsen, T. Wright [June 2003], (<http://www.ietf.org/rfc/rfc3546.txt>)

IETF - Drafts

- [XCAP] The Extensible Markup Language (XML) Configuration Access protocol (XCAP)
<http://www.ietf.org/internet-drafts/draft-ietf-simple-xcap-07.txt>
Note: work in progress
- [xcap-package] An Extensible Markup Language (XML) Document Format for Indicating Changes in XML Configuration Access Protocol (XCAP) Resources
<http://www.ietf.org/internet-drafts/draft-ietf-simple-xcap-package-03.txt>
Note: work in progress
- [xcap-lists] An Extensible Markup Language (XML) Formats for Representing Resource Lists
<http://www.ietf.org/internet-drafts/draft-ietf-simple-xcap-list-usage-04.txt>
Note: work in progress
- [sipping-config-framework] A Framework for Session Initiation Protocol User Agent Profile Delivery
<http://www.ietf.org/internet-drafts/draft-ietf-sipping-config-framework-05.txt>
Note: work in progress

3GPP/3GPP2

References

- [3GPP TS 23.002] 3GPP TS 23.002 Network architecture
Rel-6 current version: 6.5.0 [get it](#)
- [3GPP TS 23.228] 3GPP TS 23.228 IP Multimedia Subsystem (IMS); Stage 2,
Rel-6 current version: 6.6.0 [get it](#)
- [3GPP TS 33.141] 3GPP TS 33.141 Group Services and System Aspects; Presence service; Security
Rel-6 current version: 6.0.0 [get it](#)
- [3GPP TS 33.222] TS 33.222 Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)
Rel-6 current version: 6.0.0 [get it](#)
- [3GPP2 X.S0027-003-0] 3GPP2 X.S0027-003-0 Group Services and System Aspects; Presence service; Security

[3GPP2 X.S0013-002-A] 3GPP2 X.S0013 -002-A

OMA References

[ARCH-INVENT]	“Inventory of Architectures and Services”, URL: OMA-Inventory-of-Architectures-and-Services-V1_0
[ARCH-PRINC]	“OMA Architecture Principles”, URL: OMA-ArchitecturePrinciples-V1_2
[ARCH-REVIEW]	“OMA Architecture Review Process”, URL: OMA-ARCH_Review_Process-V1_0_0
[OMA-DICT]	“OMA Dictionary”, URL: OMA-Dictionary-V2_1
[OMA-DM]	OMA Device Management, V1.1.2 (based on SyncML DM)
[OMA-ERDCP]	OMA Enabler Release Definition for Client Provisioning V1.1
[OMA-RD-XDM]	“XML Document Management Requirements”, OMA-RD-XDM-V1_0
[OMA-PRO-AD]	OMA – Provisioning Architecture Overview V1.1
[OMA-PRO-CONT]	OMA – Provisioning Content V1.1
[OMA-PRO-UA]	OMA – Provisioning User Agent Behaviour V1.1
[OMA-PRO-SEC]	OMA - Provisioning Bootstrap V1.1
[OMA-POC-AD]	“Push to talk Over Cellular (PoC) Architecture”, URL: OMA-AD-PoC-V1_0
[OMA-AD- Presence_SIMPLE]	“Stage 2 - Presence using SIMPLE “, URL: OMA-PAG-SIMPLE-AD-V1_1_0
[OMA-RD- Presence_SIMPLE]	“Presence Requirements”, URL: OMA-RD-Presence_SIMPLE-V1_0
[OMA-TS-XDM_Core]	“XML Document Management (XDM) Specification”, URL: OMA-TS-XDM_Core-V1_0
[OMA-TS- XDM_Shared]	“Shared XDM Specification ”, URL: OMA-TS-XDM_Shared-V1_0

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.

This is an informative document, which is not intended to provide testable requirements to implementations.

3.2 Definitions

Context Collaboration Model	An extension of the Context Model. It expands on the Context Model by describing the interactions (collaborations) between the entities of this architecture and external entities (e.g. entities in other architectures).
Contextual Item	A logical entity in an architecture
Context Model	A model that identifies all contextual items relevant to understanding architecture.
Group Management	A generic list of URIs that can be used by different enablers to address all list members at once. They are stored and managed by the Shared XDM. Additional service specific semantics are defined by the using service itself with service specific extensions on the basis of additional XML documents. Due to the overloaded meaning of “Group Management”, it was decided to use “XML Document Management” (short form is XDM) to describe the service enabler that was defined.
Presence	Defined in [OMA-RD-Presence_SIMPLE]
Presence Authorization Policies	Defined in [OMA-RD-Presence_SIMPLE].
Presence Information	Defined in [OMA-RD-Presence_SIMPLE].
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. [OMA-DICT]
Subscription	See [RFC3265]
XDM Client	The XDMC is a client entity that provides access to the various XDMS features. [See also 7.1.1]
XCAP Server	The XCAP Server manages XML documents. [See also 7.2.1]

3.3 Abbreviations

GAA	Generic Authentication Architecture
OMA	Open Mobile Alliance
IETF	Internet Engineering Task Force
PoC	Push to talk over Cellular
RLS	Resource List Server
SIP	Session Initiation Protocol
TLS	Transport Layer Security

UE	User Equipment
XCAP	Extensible Markup Language (XML) Configuration Access Protocol
XDM	XML Document Management
XDMC	XML Document Management Client
XDMS	XML Document Management Server

4. Introduction (Informative)

This Architecture Document describes the features and architecture of the OMA XML Document Management enabler.

The XML Document Management defines a common mechanism that makes user-specific service-related information accessible to the service enablers that need them. Such information is expected to be stored in the network where it can be located, accessed and manipulated (created, changed, deleted, etc.). XDM specifies how such information will be defined in well-structured XML documents, as well as the common protocol for access and manipulation of such XML documents. The XML Configuration Access Protocol (XCAP) [XCAP], as defined by IETF, has been chosen as the common XML Document Management protocol.

The XDM Specification [OMA-TS-XDM_Core] defines two main features:

- The common protocol, XML Configuration Access Protocol (XCAP), by which principals can store and manipulate their service-related data, stored in a network as XML documents.
- The SIP subscription/notification mechanism by which principals can be notified of changes to such documents

Documents accessed and manipulated via XCAP are stored in logical repositories in the network, called XML Document Management Servers (XDMS). Each repository may be associated with a functional entity which uses its data to perform its functions. (For example, a POC server accesses a POC XDMS to obtain a particular type of user document, a POC Group document, which provides the member list for a POC group session, and uses this information to invite such members for a POC session.)

The Shared XDM Specification [OMA-TS-XDM_Shared] specifies a specific type of repository, called a Shared XDMS, which stores documents which can be reused by other enablers. This enabler specifies one such document: the URI List. This is a convenient way for a principal to group together a number of end user identities (e.g., “Friends” or “Family) or other resources, where such a list is expected to be reused by a number of different enablers.

Due to the reusable nature of the XDM enabler, there will be interactions with other service enablers, and therefore, the architectural design of the XDM enabler accommodates the needs of those enablers.

4.1 Target Audience

The target audience for this document includes but is not limited to the following:

- The Working Group(s) that will create specifications based on this subject matter
- Working Groups that need to understand this subject matter
 - OMA - POC WG
 - OMA - MWG
 - OMA – GS WG
 - OMA – DM WG
 - OMA – BAC WG
 - OMA – LOC WG
 - OMA – DS WG
 - OMA – MWS WG
- Architecture Working Group (e.g. during Architecture Reviews as defined in [ARCH-REVIEW], to determine compliance of [ARCH-PRINC], etc.)
- Interoperability Working Group (e.g. for early analysis of interoperability requirements)

4.2 Requirements

All the requirements as defined in the [OMA-RD-XDM] are met with this document.

5. Features

(Informative)

Documents accessed and manipulated via XCAP are stored in (logical) repositories in the network, called generically XML Document Management Servers (XDMS), each repository being associated with a functional entity which uses the data in its associated repository to perform its functions. For example, a POC server accesses a POC XDMS to obtain a particular type of user document, a POC Group document, which provides the member list for a POC group session, and uses this information to invite such members for a POC session.

The following sub-sections provide a high level description of the principal features of the XDM enabler.

5.1 Authentication

XDM clients must be authenticated before accessing any XDM services. Depending on the location of the XDMS (e.g terminal or application server), this authentication may occur in multiple levels. For example, an XDMS located in a terminal is authenticated by the Aggregation Proxy using a particular mechanism. Alternatively an XDMS located in application server is authenticated directly by the XDMS using mechanisms outside the scope of the present specification.

5.2 Document Management Operations

This section describes the generic operations that can be performed on documents managed by the XDM enabler. The Document Management Operations should include the XCAP operations against XDMS. The XDM enabler supports the following operations that can be performed on a document:

- Creating or replacing a document
- Deleting a document
- Retrieving a document
- Creating or replacing an XML element
- Deleting an XML element
- Retrieving an XML element
- Creating an XML attribute for an XML element
- Deleting an XML attribute
- Retrieving an XML attribute

Note that some documents might not support all operations.

5.3 Notifications of changed data

This release of XML Document Management uses the SIP subscription/notification mechanism specified by IETF [xcap-package] [sipping-config-framework]. This allows an authorized XDM Client to subscribe to notification of changes to a document in an XDMS.

The XDM Client may subscribe to changes in multiple documents in a single subscription.

Section 7 provides details of the use of this feature across various reference points.

6. Context Model (Informative)

6.1 Context Collaboration Model

6.1.1 Functions

The XDM enabler provides the following functionality:

- 1) Manipulation of XML documents stored in an XDM Server (XDMS) by the XDM Client (XDMC), and
- 2) Change notifications of XML documents, by which an XDMC can learn of any changes made to documents in the XDMS.

Manipulation of XML documents is achieved using the XCAP protocol, between the XDMC and the XDMS storing the data. Authentication is described in Section 5.1. An XDMC may subscribe to the changes done to XML documents using a SIP change event package. When an XDMC subscribes to the changes, it receives notifications from the XDMS whenever an XML document is changed. An XDMC may subscribe to a single or multiple documents with one subscription. The subscription request from the XDMC may be accepted or denied based on authorization decision by the XDMS.

6.1.2 Collaboration with other Service Enablers

The collaboration of the XDM enabler with other enablers has several aspects:

- Terminals use the aggregation proxy to communicate more efficiently with enabler-specific XDMSs as well as the Shared XDMS
- Enabler-specific applications servers directly communicate with the Shared XDMS using both XCAP and SIP-based interfaces.
- Enabler specifications utilize the XDM specifications to define their own XML documents. Enabler-specific applications servers communicate with XDMSs using both XCAP and SIP-based interfaces.

7. Architectural Model

(Informative)

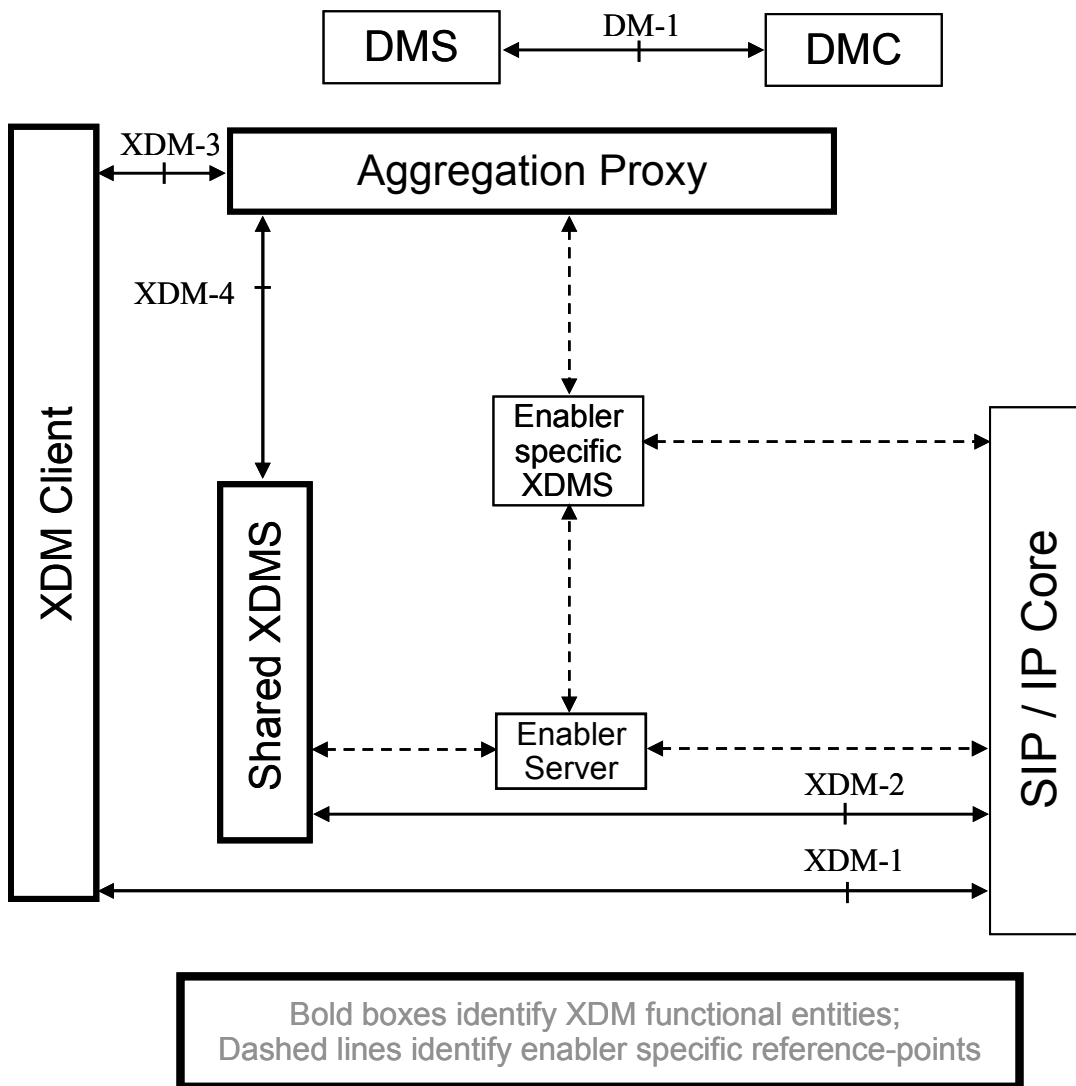


Figure 1: XML Document Management Architecture

7.1 XML Document Management Functional Entities

7.1.1 XML Document Management Client

The XDMC is a client entity that provides access to the various XDMS features as described in Section 5. An application implementing an XDMC may implement various subsets of those features, as required, subject to certain mandatory requirements described in [OMA-TS-XDM_Core].

The XDMC can be implemented in both terminal and server entities.

7.1.2 Aggregation Proxy

The Aggregation Proxy is the contact point for the XDM Client implemented in an UE to access XML documents stored in any XDMS. The Aggregation Proxy performs the following functions:

- Performs authentication of the XDM Client.
- Routes individual XCAP requests to the correct XDMS
- Optionally supports charging
- Optionally performs compression/decompression over the radio interface

7.1.3 Shared XML Document Management Server

The Shared XDMS is a server entity providing the functionality described in Section 5. The Shared XDMS supports only URI Lists as described in [OMA-TS-XDM_Share].

7.2 Enabler specific Functional Entities

Each of these functional entities are defined in the specifications for the enabler in question

7.2.1 Enabler specific XML Document Management Server

The enabler specific XDMSs are XCAP Servers that supports the following functions:

- Performs authorisation of incoming SIP and XCAP requests
- Manages XML documents, which are specific to the service enabler.
- Provides aggregation of notifications of changes to multiple documents stored on the enabler specific XDMS.
- Notifies subscribers of changes to the enabler specific documents stored in the network.

7.2.2 Enabler specific Server

The functionality of the enabler specific Servers are defined in the specifications for the enabler in question.

7.3 External Entities Providing Services to XML Document Management

7.3.1 SIP/IP Core

The SIP/IP Core is a network of servers, such as proxies and/or registrars, that perform a variety of services in support of the XDM Service, such as routing, authentication, compression, etc. The specific features offered by different types of SIP/IP Core networks will depend on the particulars of those networks.

This release of the XDM enabler utilises IMS and MMD networks.

When the XDM Service is realized using IMS, the OMA XDM servers utilizes the capabilities of IMS as specified in 3GPP [3GPP TS 23.228] and 3GPP2 [3GPP2 X.S0013-002-A], respectively. In such cases the IMS network performs the following additional functions in support of the XDM Service:

- Routes the SIP signalling between the XDM Client and the XDM servers
- Provides discovery and address resolution services
- Supports SIP compression
- Performs a certain type of authorization of the XDM Client based on user's service profile
- Maintains the registration state

- Provides charging information

7.3.2 Device Management Server

The Device Management (DM) Server [OMA-DM] performs initialisations and updates of all configuration parameters necessary for XDMC.

7.4 Description of Reference Points

7.4.1 Reference Point XDM-1: XDM Client – SIP/IP Core

The XDM-1 reference point supports the communication between the XDM Client and the SIP/IP Core network. The protocol for the XDM-1 reference point is SIP.

The XDM-1 reference point provides the following functions:

- Subscription to the modification of any XDM documents.
- Notification of the modification of any XDM documents.

When SIP/IP Core corresponds with 3GPP/3GPP2 IMS, the XDM-1 reference point conforms with the ISC reference point [3GPP TS 23.002] [3GPP2 X.S0013.0].

7.4.2 Reference Point XDM-2: Shared XDMS – SIP/IP-Core

The XDM-2 reference point supports the communication between the Shared XDMS and the SIP/IP Core. The protocol for the XDM-2 reference point is SIP.

The XDM-2 reference point provides the following functions:

- Subscription to the modification of shared XML documents.
- Notification of the modification of shared XML documents.

When SIP/IP Core corresponds with 3GPP/3GPP2 IMS, the XDM-2 reference point conforms to the ISC reference point [3GPP TS 23.002] [3GPP2 X.S0013.0].

7.4.3 Reference Point XDM-3: XDM Client – Aggregation Proxy

The XDM-3 reference point is between the XDM Client and the Aggregation Proxy. The protocol for the XDM-3 reference point is XCAP.

The XDM-3 reference point provides the following functions:

- XML document management (e.g. create, modify, retrieve, delete)

When the SIP/IP Core network corresponds with 3GPP/3GPP2 IMS, then the XDM-3 reference point conforms to the Ut reference point [3GPP TS 23.002].

7.4.4 Reference Point XDM-4: Aggregation Proxy – Shared XDMS

The XDM-4 reference point is between the Aggregation Proxy and the Shared XDMS. The protocol for the XDM-4 reference point is XCAP.

The XDM-4 reference point provides the following functions:

Shared XML document management (e.g. create, modify, retrieve, delete)

7.4.5 Reference Point DM-1: DM Client – DM Serve

The DM-1 reference point is described in [OMA-DM]. The XDM enabler will define the XDM configuration object(s).

7.4.6 Reference Points: “Enabler specific XDMS” - SIP/IP Core

Each of these reference points are named by and defined in the specifications for the enabler in question.

They support the communication between an enabler specific XDMS and the SIP/IP Core network. The protocol for the reference points is SIP.

They provide the following functions:

- Subscription to the modification of enabler specific XML documents.
- Notification of the modification of enabler specific XML documents

7.4.7 Reference Points: “Enabler specific Server” - SIP/IP Core

Each of these reference points are named by and defined in the specifications for the enabler in question.

They support the communication between an enabler specific Server and the SIP/IP Core network. The protocol for the reference points is SIP.

They provide the following functions:

- Subscription to the modification of enabler specific XML documents.
- Notification of the modification of enabler specific XML documents

7.4.8 Reference Points: Aggregation Proxy – “Enabler specific XDMS”

Each of these reference points are named in the specification for the enabler in question and owned by it. The basic XML Document Management requirements for the reference points are described in the XDM core specification [OMA-TS-XDM_Core].The enabler unique requirements for the reference points are described in the XDM enabler specification"

They provide the following functions:

- “Enabler specific” XML document management (e.g. create, modify, retrieve, delete)

7.4.9 Reference Points : Shared XDMS – “Enabler specific Server”

Each of these reference points are named in the specification for the enabler in question and owned by it. The requirements for the reference points are described in the XDM enabler specification [OMA-TS-XDM_Core] and in the enabler specific specification.

The protocol for the reference points is XCAP

They provide the following function:

- Transfer of URI Lists to the enabler specific server

7.4.10 Reference Points: “Enabler specific XDMS” – “Enabler specific Server”

Each of these reference points are named by and defined in the specifications for the enabler in question.

The protocol for the reference points is defined in the specifications for the enabler in question.

They provide the following function:

- Transfer of enabler specific documents from the enabler specific XDMS to the enabler specific server.

7.5 Access Control

This release of the XDM specifications defines a default access control policy, which is that only the creator of a document is allowed to perform all XDM actions to the document. Also application servers of the trusted networks are allowed to read the document. No other entities are allowed to access the document.

A permissions-based system, in which more elaborate access policies are defined, may be included in future releases of XDM.

7.6 Security

The XDMC is to be authenticated prior to accessing the XDM service as specified in [XCAP]. TLS is used as specified in [XCAP] in order to provide integrity and confidentiality protection to the exchanged messages. HTTP Digest is the default authentication mechanism.

For a 3GPP realisation the Generic Authentication Architecture (GAA) as an underlying network mechanism is used as specified in [3GPP TS 33.222] to provide the XDM service security if GAA is present; otherwise requirements as above applies.

7.7 Charging

Appropriate charging mechanisms may need to be provided by the underlying network or other suitable entities in order to support the charging requirements described in [OMA-RD-XDM].

Description of how charging is performed is beyond the scope of the present specification.

7.8 XML Document Management Service Provisioning

The XML Document Management (XDM) Service provider can set up the XDM Service configurations remotely in the terminal device by using the device management mechanism specified in [OMA-PRO-AD]. The updates of the XDM Service configurations are remotely performed in the terminal device by using [OMA-DM].

A UE running the XDMC, compliant with [OMA-PRO-UA] is able to receive the contents sent by the service provider. The exact syntax and definition of parameters needed for the XDM enabler are specified in [OMA-PRO-CONT]. The bootstrap mechanism defined in [OMA-PRO-SEC] and [OMA-DM] are used to enhance the security of the provisioning.

Appendix A. Change History

(Informative)

A.1 Approved Version History

Reference	Date	Description
n/a	n/a	No prior version

A.2 Draft/Candidate Version 1.0 History

Document Identifier	Date	Sections	Description
Draft Versions OMA-AD_Group-Mgmt-V0_1	18 Apr 2004		
Candidate Version OMA-AD-XDM-V1_0	04 Feb 2005	n/a	Status changed to Candidate by TP: OMA-TP-2005-0060-XDM_1_0--for-candidate-approval
Candidate Version OMA-AD-XDM-V1_0	17 Mar 2005	4.2	CR TP-2005-0095 implemented.
Candidate Version OMA-AD-XDM-V1_0	28 Jun 2005	2.1	Incorporated OMA-PAG-0363