OMA Device Management Dictionary

Candidate Version 1.0 – 06 Mar 2012

Open Mobile Alliance

OMA-SUP-DM_Dictionary-V1_0-20120306-C

© 2012 Open Mobile Alliance Ltd. All Rights Reserved.

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.

© 2012 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms set forth above.

Contents

© 2012 Open Mobile Alliance Ltd. All Rights Reserved.

Figures

No table of figures entries found.

Tables

No table of figures entries found.

© 2012 Open Mobile Alliance Ltd. All Rights Reserved.

1. Scope

The purpose of this document is to identify specific terms and abbreviations used across the various OMA-DM specifications. Having a common collection of definitions and abbreviations related to the OMA-DM documents will

- ensure that the terminology is used in a consistent manner across OMA-DM documents
- provide the reader a friendly tool explaining the technical terms that are used across multiple documents
- help the editors in using the terminology in a consistent manner across OMA specifications.

The definitions and abbreviations as given in this document are

- created by the OMA DM WG, when the need for precise definition is identified
- imported from existing documentation (e.g. ITU, 3GPP, 3GPP2).

This document will be enhanced and maintained per the following general process.

- In general, only terms used in OMA DM specifications will be included in the dictionary, including terms related to MO Enablers, as long as it makes sense that these terms can be reused in the context of at least another MO or DM spec.
- Terms created by other SDO may be included if used in OMA DM or MO specifications, but other terms supporting/clarifying the external forum terms will not be included, if not used in these specifications; instead, the source forum will be identified so the reader can consult it for further information. If multiple competing definitions with valid application in the OMA DM or MO context exist, they MAY be included.
- Multiple definitions will be included for terms that have different meanings in different OMA DM or MO specifications. While the goal is to align terms across the documents, some documents may have valid reasons for using the same term with different meanings.

© 2012 Open Mobile Alliance Ltd. All Rights Reserved.

2. References

2.1 Normative References

[DM1.3AD] "OMA Device Management Architecture, Version 1.3". Open Mobile Alliance™. OMA-AD-DM -V1_3. URL:http://www.openmobilealliance.org/

[ETSI TR 102 216] "TR 102 216 Technical Report Smart Cards; Vocabulary for Smart Card Platform specifications", v3.0.0, European Telecommunications Standards Institute (ETSI), URL:http://www.etsi.org/

[ISO7816-4] ISO/IEC 7816-4 (1995): "Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 4: Inter-industry commands for interchange".

[OMADICT] "Dictionary for OMA Specifications", Version 2.8, Open Mobile Alliance™, OMA-ORG-Dictionary-V2_8, URL:http://www.openmobilealliance.org/

[PKCS#15] PKCS #15 v1.1: Cryptographic Token Information Syntax Standard", RSA Laboratories, June 6, 2000. URL: ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-15/pkcs-15v1_1.pdf

[RFC2119] "Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, March 1997, URL:http://www.ietf.org/rfc/rfc2119.txt

[RFC2616] "Hypertext Transfer Protocol – HTTP/1.1", R. Fielding, et al., June 1999, URL:http://www.ietf.org/rfc/rfc2616.txt

[SSL] "The SSL 3.0 Protocol", A. Frier, P. Karlton, and P. Kocher, Nov 1996

[TS102.221] "Smart Cards; UICC-Terminal interface; Physical and logical characteristics", (ETSI TS 102 221 release 6), URL:http://www.etsi.org/

[TS151.011] "Specification of the Subscriber Identity Module - Mobile Equipment (SIM-ME) interface", (ETSI TS 151 011), URL:http://www.etsi.org/

2.2 Informative References

None.

© 2012 Open Mobile Alliance Ltd. All Rights Reserved.

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

For definitions not present in the following list, please refer to [OMADICT].

3.2.1 0-9

2G UICC

UICC activated in a 2G mode that has physical characteristics of UICC [TS102.221] but logical characteristics of SIM [TS151.011].

3G UICC

UICC activated in a 3G mode that has physical and logical characteristics of the UICC [TS102.221].

3.2.2 A

Access Control List

A list of identifiers and access rights associated with each identifier.

ADM

Access condition to an EF which is under the control of the authority which creates this file.

Application Identifier

A data element that identifies an application in a smartcard. An application identifier may contain a registered application provider number in which case it is a unique identification for the application. If it contains no application provider number, then this identification may be ambiguous.

Authentication

Authentication is the process of ascertaining the validity of either the Device or the Device Management Server’s identity.

3.2.3 B

Binary Files

Binary Files are equivalent to transparent files as described in [TS102.221].

Bootstrap

The process of provisioning the DM Client to a state where it is able to initiate a management session to a DM Server.

Bootstrap Message

A message that is from a Management Authority to the DM Client outside the context of a DM Session.

© 2012 Open Mobile Alliance Ltd. All Rights Reserved.

Bootstrap Process

See Bootstrap.

Built-in Device Test

The functionality of the Device to test itself.

3.2.4 C

Cache

A program's local store of response messages and the subsystem that controls its message storage, retrieval, and deletion. A cache stores cacheable responses in order to reduce the response time and network bandwidth consumption on future, equivalent requests. Any client or server can include a cache, though a cache cannot be used by a server that is acting as a tunnel.

Cacheable

A response is cacheable if a cache is allowed to store a copy of the response message for use in answering subsequent requests. The rules for determining the cacheability of HTTP responses are defined in section 13 of [RFC2616]. Even if a resource is cacheable, there can be additional constraints on whether a cache can use the cached copy for a particular request.

Cardholder Verification

Also called the PIN. Typically a 4 to 8 digit number entered by the cardholder to verify that the cardholder is authorized to use the card.

Command

A DM Command is a protocol primitive. Each DM Command specifies to a recipient an individual operation that is to be performed.

Confidentiality

Confidentiality is the ability to keep contents secret from all but the two entities exchanging a message. It does not limit the visibility of the message (being able to eavesdrop), but it does prevent the interpretation of the data being transmitted. Effectively this prevents the contents of a message being understood by anybody but the intended sender and intended recipient.

Connection

A transport layer virtual circuit established between two programs for the purpose of communication.

Connectionless Session Service

Connectionless session service is an unreliable session service. In this mode, only the request primitive is available to service users, and only the indication primitive is available to the service provider.

Connection-Mode Session Service

Connection-mode session service is a reliable session service. In this mode, both request and response primitives are available to service users, and both indication and confirm primitives are available to the service provider.

Content Negotiation

Content negotiation is the mechanism the server uses to select the appropriate type and encoding of content when servicing a request. The type and encoding of content in any response can be negotiated. Content negotiation allows a server application to decide whether a client can support a certain form of content.

© 2012 Open Mobile Alliance Ltd. All Rights Reserved.

3.2.5 D

Data Object Directory Files

Contain directories of data objects (not keys or certificates) ([PKCS#15]) known to the PKCS#15 application.

Dedicated File

A file containing access conditions and, optionally, Elementary Files (EFs) or other Dedicated Files.

Delegation

The delegating MA delegates either the entire or the partial management control of an end device to the delegated MA. If not Full Delegation, the delegating MA can revoke its management control back.

Delegation Process

A process by which one Management Authority (the delegating MA) delegates the management control to another MA (the delegated MA).

Description Framework

A machine readable specification for how to partly describe the management syntax for a particular Management Object or management tree.

Device Description Framework

A specification for how to describe the management syntax and semantics for a particular device type.

Device Management

Management of the Device configuration and other managed objects of Devices from the point of view of the various Management Authorities. Device Management includes, but is not restricted to setting initial configuration information in Devices, subsequent updates of persistent information in Devices, retrieval of management information from Devices and processing events and alarms generated by Devices.

Device Management Authority

Any legal entity authorized, either directly or through delegation, to perform management operations on a Device using the OMA Device Management protocol through a set of Management Objects

Device Management Gateway

An entity that facilitates interaction between a management server and a management client, at least one of which runs OMA-DM, in situations where direct and unaided interaction between the management server and the management client is not possible.

Device Management Server (DM Server)

An abstract software component in a deployed Device Management infrastructure that conforms to the OMA Device Management Enabler static conformance requirements specified for DM Servers. It serves as an end-point of the DM Client-Server Protocols and DM Server-Server Interface.

Device Management Client (DM Client)

An abstract software component in a Device implementation that conforms to the OMA Device Management Enabler static conformance requirements specified for DM Clients. It serves as an end-point of the DM Client-Server Protocols.

Device Management System

A collection of Device Management Clients, Device Management Servers and Device Management Authority facilities, operating together according to the [DM1.3AD].

© 2012 Open Mobile Alliance Ltd. All Rights Reserved.

DF Path

Concatenation of file identifiers without delimitation. The Path type is defined in [ISO7816-4] sub-clause 5.1.2. If the path starts with the MF identifier (0x3F00), it is an absolute path; otherwise it is a relative path. A relative path must start with the identifier of the current DF (or with the identifier '0x3FFF').

DiagMon Function

Functions in a device that can be remotely invoked by a Diagnostics and Monitoring System, that, when invoked, executes a diagnostics related logic to return results.

DiagMon System

A system that is associated with the Device Management System and is also under the administration of a management authority. It employs the standard Device Management System interaction with a (set of) device(s). The Diagnostics and Monitoring System provides enhancements to the Device Management System to support Diagnostics and Monitoring.

DM Bootstrap Server

A server from which the Bootstrap Message for a Device originates. It may be part of the DM Server or a separate entity.

Dynamic Node

A Node is dynamic if the DDF property Scope is set to Dynamic, or if the Scope property is unspecified.

3.2.6 E

EF Record

A string of bytes within an EF handled as a single entity.

End Device

A Device that is deployed behind a DM Gateway and that is the intended target for an OMA-DM command that is issued by an OMA-DM Server. The Device may or may not have an embedded OMA-DM Client.

Entity

An entity is the information transferred as the payload of a request or response. An entity consists of meta-information in the form of entity-header fields and content in the form of an entity-body.

3.2.7 F

File Identifier

A 2-byte binary value used to address a file on a smartcard.

Full Delegation

The delegating MA delegates the entire management control of an end device to the delegated MA, and remove itself from further participation in the management of the end device. This type of delegation results in the delegating MA deleting its own DM Account from the end device.

Full Device URI

Full path to a device resource specified in the device's context. Three formats are allowed:
1. An absolute URI start from the device root node;
2. A URI relative to the device root node;
3. A URI relative to the parent node of the management object which starts with [x]. The [x] represents The [x] represents the virtual root of the management object.

© 2012 Open Mobile Alliance Ltd. All Rights Reserved.

3.2.8 G

<void>

3.2.9 H

Header

A header contains meta-information. Specifically, a session header contains general information about a session that remains constant over the lifetime of a session; an entity-header contains meta-information about a particular request, response or entity body.

HTTP Client

A program that establishes connections for the purpose of sending HTTP requests.

HTTP Gateway

A HTTP server which acts as an intermediary for some other server. Unlike a proxy, a gateway receives requests as if it were the origin server for the requested resource; the requesting client might not be aware that it is communicating with a gateway.

HTTP Message

The basic unit of HTTP communication, consisting of a structured sequence of octets matching the syntax defined in section 4 of [RFC2616] and transmitted via the connection.

HTTP Proxy

An intermediary program which acts as both a server and a client for the purpose of making requests on behalf of other clients. Requests are serviced internally or by passing them on, with possible translation, to other servers. A proxy MUST implement both the client and server requirements of this specification. A "transparent proxy" is a proxy that does not modify the request or response beyond what is needed for proxy authentication and identification. A "non-transparent proxy" is a proxy that modifies the request or response in order to provide some added service to the user agent, such as group annotation services, media type transformation, protocol reduction, or anonymity filtering. Except where either transparent or non-transparent behavior is explicitly stated, the HTTP proxy requirements apply to both types of proxies.

HTTP Request

An HTTP request message, as defined in section 5 of [RFC2616].

HTTP Response

An HTTP response message, as defined in section 6 of [RFC2616].

HTTP Server

An application program that accepts connections in order to service HTTP requests by sending back responses. Any given program might be capable of being both an HTTP client and a server; our use of these terms refers only to the role being performed by the program for a particular connection, rather than to the program's capabilities in general. Likewise, any server might act as an HTTP origin server, proxy, gateway, or tunnel, switching behavior based on the nature of each request. NOTE: In this document, when the term "server" appears alone, it refers to a HTTP server, not a DM Server.

3.2.10 I

Inbound/Outbound

Inbound and outbound refer to the request and response paths for messages: "inbound" means "traveling toward the origin server", and "outbound" means "traveling toward the user agent."

Integrity

© 2012 Open Mobile Alliance Ltd. All Rights Reserved.

Integrity is the ability for a message to maintain its content or at a minimum, have the ability to detect modification or corruption of its content.

Interior Node

A Node that may have child Nodes, but cannot store any value. The Format property of an Interior Node is node.

3.2.11 J

<void>

3.2.12 K

<void>

3.2.13 L

Leaf Node

A Node that can store a value, but cannot have child Nodes. The Format property of a Leaf Node is not node.

Loader

Entity that implements the HTTP protocol. The loader is the interface between the WSP layer and the user application.

3.2.14 M

Management Authority (MA)

See definition for Device Management Authority.

Management Object

A Management Object is a subtree of the Management Tree which is intended to be a (possibly singleton) collection of Nodes which are related in some way. For example, the ./DevInfo Nodes form a Management Object. A simple Management Object may consist of one single Node.

Management Object Identifier

A unique identifier of the management object, stored in the “DDFName” property of the root of the Management Object.

Management Session

A continuous connection between the Device and the Device Management Server established for the purpose of carrying out one or more device management operations.

Management Tree

The interface by which the management server interacts with the client, e.g. by storing and retrieving values from it and by manipulating the properties of it, for example the access control lists.

Meta-Information

Parameter or attributes about the representation, state or type or content of an object or property.

Message

Atomic unit in OMA DM Protocol, one packet that the bearer network is able to accept. One OMA DM Protocol package could be divided into many messages. It contains the DM Commands, as well as the related data and meta-information. The DM Message is an XML document.

© 2012 Open Mobile Alliance Ltd. All Rights Reserved.

Message Authentication Code

A value computed based on a message hash and some form of shared secret.

3.2.15 N

Node

A Node is a single element in a Management Tree. There can be two kinds of Nodes in a Management Tree: Interior Nodes and Leaf Nodes. The Format property of a Node provides information about whether a Node is a leaf or an Interior Node.

Notification Message

Message sent from the DM Server to DM Client to alert DM Client to initiate a DM session back for management purpose.

3.2.16 O

OBEX

Objext Exchange Protocol.

Object Directory File

The mandatory Object Directory File ([PKCS#15]) consists of pointers to other EFs, each one containing a directory over PKCS#15 objects of a particular class (here and below, a “directory” means a list of objects).

Originator

The network device that creates a DM request.

Operation

A DM Operation refers to the conceptual transaction achieved by the DM Commands specified by a DM Package.

Origin Server

The HTTP server on which a given resource resides or is to be created.

3.2.17 P

Package

A DM Package is the complete set of commands and related data elements that are transferred between an originator and a recipient. The DM package can consist of one or more DM Messages.

Parser

Refers to an XML parser. An XML parser is not and absolutely needed to support SyncML. However, a SyncML implementation that integrates an XML parser might be easier to enhance.

This document assumes that the reader has some familiarity with XML syntax and terminology.

Permanent Node

A Node is permanent if the DDF property Scope is set to Permanent. If a Node is not permanent, it is dynamic. A permanent Node can never be deleted by the server.

3.2.18 Q

<void>

© 2012 Open Mobile Alliance Ltd. All Rights Reserved.

3.2.19 R

Recipient

The network device that receives a DM request, processes the request and sends any resultant DM response.

Representation

An entity included with a response that is subject to content negotiation, as described in section 12 of [RFC2616]. There can exist multiple representations associated with a particular response status.

Representation protocol

A well-defined format for exchanging a particular form of information. SyncML is a representation protocol for conveying data synchronization and device management operations.

Request

A message or a command sent from a device to another.

Resource

A network data object or service that can be identified by a URI, as defined in Hypertext Transfer Protocol [RFC2616]. Resources may be available in multiple representations (e.g. multiple languages, data formats, size, and resolutions) or vary in other ways.

3.2.20 S

Secure Transport

A transport that provides authentication, integrity and encryption.

Server Identifier

The OMA DM internal name for a DM Server. A DM Server is associated with an existing Server Identifier in a device through OMA DM account.

Sessionless Command Message

A standalone DM Message sent from a DM Server to a DM Client, outside a Management Session, for the configuration or continuous management purposes.

Sessionless Process

The sending and processing of Sessionless Command Messages to a DM client for the purpose of carrying out one or more device management operations outside a Management Session.

Sessionless Report Alert

A specially formatted alert, issued by the DM Client to the DM Server, for which there is no acknowledgement from the DM Server.

Sessionless Report Message

A SyncML message that contains one or more Sessionless Report Alerts in its body.

SIM Message

A message sent by the ME to the smartcard that initiates an action and solicits a response from the smartcard.

Smartcard

© 2012 Open Mobile Alliance Ltd. All Rights Reserved.

The Smartcard refers to the smart card definition of [ETSI TR 102 216].

3.2.21 T

Test Fest

Multi-lateral interoperability testing event

Trap

A mechanism employed by a management authority to enable the Device to capture and report events and other relevant information generated from various components of the Device, such as a protocol stack, device drivers, or applications.

Tunnel

An intermediary program which is acting as a blind relay between two connections. Once active, a tunnel is not considered a party to the HTTP communication, though the tunnel might have been initiated by an HTTP request. The tunnel ceases to exist when both ends of the relayed connections are closed.

3.2.22 U

UICC Message

A message sent by the ME to the smartcard that initiates an action and solicits a response from the smartcard.

User Agent

The client which initiates a request. These are often browsers, editors, spiders (web-traversing robots), or other end user tools.

3.2.23 V

<void>

3.2.24 W

<void>

3.2.25 X

<void>

3.2.26 Y

<void>

3.2.27 Z

<void>

3.3 Abbreviations

For abbreviations not present in the following list, please refer to [OMADICT].

3.3.1 0-9

<void>

© 2012 Open Mobile Alliance Ltd. All Rights Reserved.

3.3.2 A

ADF	Application Dedicated File
ALW	Always. Access condition indicating a given function is always accessible

3.3.3 B

BIP	Bearer Independent Protocol

3.3.4 C

CHV	Cardholder Verification

3.3.5 D

DiagMon	Diagnostics and Monitoring
DiagMonMO	Diagnostics and Monitoring MO
DL	Download
DMBEK	DM Bootstrap Encryption Key
DMBIK	DM Bootstrap Integrity Key
DM_SC	Device Management Smart Card
DSO	Document Support Officer

3.3.6 E

EMI	Experimental Meta Information

3.3.7 F

<void>

3.3.8 G

GwMO	Gateway Management Object
GRUU	Globally Routable User Agent URI

3.3.9 H

<void>

3.3.10 I

IC	Integrated Circuit
IrLAP	Infrared Link Access Protocol
IrLMP	Infrared Link Management Protocol

© 2012 Open Mobile Alliance Ltd. All Rights Reserved.

3.3.11 J

<void>

3.3.12 K

<void>

3.3.13 L

L2CAP	Logical link control and adaptation protocol
ListMO	List of supported Management Object
LMP	Link Management protocol

3.3.14 M

MD	Message Digest
MF	Master File
MOID	Management Object Identifier

3.3.15 N

<void>

3.3.16 O

OBEX	Object Exchange protocol
ODF	Object Directory File
OID	Object Identifier
OMNA	Open Mobile Naming Authority

3.3.17 P

<void>

3.3.18 Q

<void>

3.3.19 R

RD	Requirements Document
RFCOMM	Radio frequency communication
RRELD	Reference Release Definition
R-UIM	CDMA Removable User Identity Module

3.3.20 S

SACMO	Software and Application Control Management Object

© 2012 Open Mobile Alliance Ltd. All Rights Reserved.

SC	Smart Card
SCOMO	Software Component Management Object
SCR	Static Conformance Requirement
SCWS	Smart Card Web-Server
SDO	Standard Developing Organization
SIM	Subscriber Identity Module
SNTP	Simple Network Time Protocol
SSL	Secure Socket Layer [SSL]
SUP	Support Document

3.3.21 T

Tiny TP	Tiny Transport Protocol
TNDS	Tree and Description Serialization

3.3.22 U

UDP	User Datagram Protocol
UTC	Universal Time Coordinated

3.3.23 V

<void>

3.3.24 W

WiMAX	Worldwide Interoperability for Microwave Access

3.3.25 X

<void>

3.3.26 Y

<void>

3.3.27 Z

<void>

© 2012 Open Mobile Alliance Ltd. All Rights Reserved.

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-SUP-DM_Dictionary-V1_0	29 Jan 2009	3.2.5	Applied OMA-DM-2008-0163R01-CR_DM__Dictionary
	11 Dec 2009	All	Applied OMA-DM-2009-0120-CR_DM_Gateway_Definition, OMA-DM-2009-0143R01-CR_Delegation_related_definitions
	11 Feb 2010	All	Editorial clean-up by DSO
	26 Apr 2010	Cover page, 3.3	Removed automatic update field on cover page Re-numbering of sub sections in 3.3
	27 Apr 2010	3.2.5	Formatting of fonts Deletion of editor's note
Candidate Version OMA-SUP-DM_Dictionary-V1_0	25 May 2010	N/A	Status changed to Candidate by TP Ref # OMA-TP-2010-0221- INP_DM_V1.3_ERP_and_ETR_for_Candidate_approval
Draft Versions OMA-SUP-DM_Dictionary-V1_0	16 Feb 2011	All	Applied OMA-DM-DM13-2010-0132R01- CR_moving_DM20Dict_to_DM13Dict
	25 Mar 2011	3.2.5	Applied OMA-DM-DM13-2011-0023-CR_DM_Bootstrap_Server_Defn
	19 Apr 2011	3.2.17, 3.2.20	Applied OMA-DM-DM13-2011-0030R01- CR_MMA_Delegation_Type_Definition
	02 Sep 2011	3.2.3, 3.2.7	Applied OMA-DM-DM13-2011-0076R04-CR_Dic_BootstrapDefinition OMA-DM-DM13-2011-0088R01-CR_dictionary_clarification
	21 Oct 2011	3.2.5, 3.2.7, 3.2.17	Applied OMA-DM-DM13-2011-0098R01- CR_DM_DICT_Update_for_Delegations
	04 Jan 2012	All	Applied OMA-DM-DM13-2011-0126R02-CR_CONR_DM_Dictionary
	19 Jan 2012	All	Applied OMA-DM-DM13-2012-0006-CR_AP_DM_Dictionary
	02 Feb 2012	All	Restored cross-references in the whole document.
	14 Feb 2012	1, 2.1, 3.2, 3.3	Applied OMA-DM-DM13-2012-0049-CR_Dictionary_editorials OMA-DM-DM13-2012-0050R01-CR_Dictionary
Candidate Version OMA-SUP-DM_Dictionary-V1_0	06 Mar 2012	N/A	Status changed to Candidate by TP Ref # OMA-TP-2012-0084- INP_DM_V1_3_ERP_and_ETR_for_Candidate_re_approval

© 2012 Open Mobile Alliance Ltd. All Rights Reserved.