



Device Management Architecture

Candidate Version 2.0 – 20 Jul 2010

Open Mobile Alliance
OMA-AD-DM-V2_0-20100720-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.

© 2010 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)4
- 2. REFERENCES5
 - 2.1 NORMATIVE REFERENCES5
 - 2.2 INFORMATIVE REFERENCES5
- 3. TERMINOLOGY AND CONVENTIONS6
 - 3.1 CONVENTIONS6
 - 3.2 DEFINITIONS6
 - 3.3 ABBREVIATIONS6
- 4. INTRODUCTION (INFORMATIVE)7
 - 4.1 VERSION 1.37
 - 4.2 VERSION 2.07
- 5. ARCHITECTURAL MODEL8
 - 5.1 DEPENDENCIES8
 - 5.2 ARCHITECTURAL DIAGRAM8
 - 5.3 FUNCTIONAL COMPONENTS AND INTERFACES/REFERENCE POINTS DEFINITION8
 - 5.3.1 Protocol Endpoints8
 - 5.3.2 Interfaces9
 - 5.4 SECURITY CONSIDERATIONS9
- APPENDIX A. CHANGE HISTORY (INFORMATIVE)10
 - A.1 APPROVED VERSION HISTORY10
 - A.2 DRAFT/CANDIDATE VERSION 2.0 HISTORY10
- APPENDIX B. MANAGEMENT AUTHORITY DIAGRAM AND TEXT (INFORMATIVE)11
 - B.2.1 DM-5 DM Exposes Management Objects11
 - B.2.2 DM-Func DM Functions11
 - B.2.3 DMA-DMS Interface11
 - B.2.4 DM Bootstrapping Request12
 - B.2.5 DM-7 Client-App Registration12
 - B.2.6 DM-8 Client-App Notification12
 - B.2.7 DM-9 Client-App Interaction12
 - B.2.8 DM-10 Exposes Standards MOs12

Figures

- Figure 1: Device Management Architecture using interfaces8
- Figure 2: Device Management Architecture using interfaces11

Tables

No table of figures entries found.

1. Scope

(Informative)

The scope of the Device Management architecture document is to define the architecture for the Device Management v2.0 enabler. This document fulfils the functional capabilities and information flows needed to support this enabler as described in the Device Management requirements document [DM-RD].

2. References

2.1 Normative References

- [DM-RD] “Device Management Requirements”, Open Mobile Alliance™, OMA-RD-DM-V2_0, URL:<http://www.openmobilealliance.org/>
- [RFC2119] “Key words for use in RFCs to Indicate Requirement Levels”, S. Bradner, March 1997, URL:<http://www.ietf.org/rfc/rfc2119.txt>

2.2 Informative References

- [ARCH-PRINC] “OMA Architecture Principles”, OMA-ArchitecturePrinciples-V1_2,, URL:<http://www.openmobilealliance.org/>
- [DM-DICT] “Device Management Dictionary”, Version 1.0, Open Mobile Alliance™, OMA-SUP-DM-DM_Dictionary-V2_0, URL:<http://www.openmobilealliance.org/>
- [OMADICT] “Dictionary for OMA Specifications”, Version 2.7, Open Mobile Alliance™, OMA-ORG-Dictionary-V2_7, URL:<http://www.openmobilealliance.org/>

3. Terminology and Conventions

3.1 Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC2119].

All sections and appendixes, except “Scope” and “Introduction”, are normative, unless they are explicitly indicated to be informative.

3.2 Definitions

| | |
|---------------------------------|-----------------|
| Device | See [OMA-DICT] |
| Device Management Client | See [DM-DICT]. |
| Device Management Server | See [DM-DICT]. |
| Interface | See [OMADICT]. |
| Management Object | See [OMA-DICT]. |

3.3 Abbreviations

| | |
|------------|----------------------|
| DM | Device Management |
| MO | Management Object |
| OMA | Open Mobile Alliance |

4. Introduction

(Informative)

Device Management refers to the management of Device configuration and other managed objects of Devices from the point of view of the 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, execute primitives on Devices, and processing events and alarms generated by Devices. In addition the Device Management v2.0 enabler brings Multiple Management Authority mechanisms.

Device management allows wireless operators, service providers or corporate information management departments to carry out the procedures of configuring devices on behalf of the end user (customer).

4.1 Version 1.3

OMA DM Version 1.3 makes no change to the architecture from OMA DM 1.2, but does introduce new notification and transport protocols.

4.2 Version 2.0

The OMA DM Version 2.0 architecture is based on OMA DM 1.3. It introduces a new DM Server to DM Server interface and two optional DM Client to application interfaces. It also removes the CP-1 interface between the CP Enabler and the DM Client for the CP Bootstrap Profile.

5. Architectural Model

5.1 Dependencies

DM 2.0 has the same dependencies as the Device Management v1.3 enabler.

5.2 Architectural Diagram

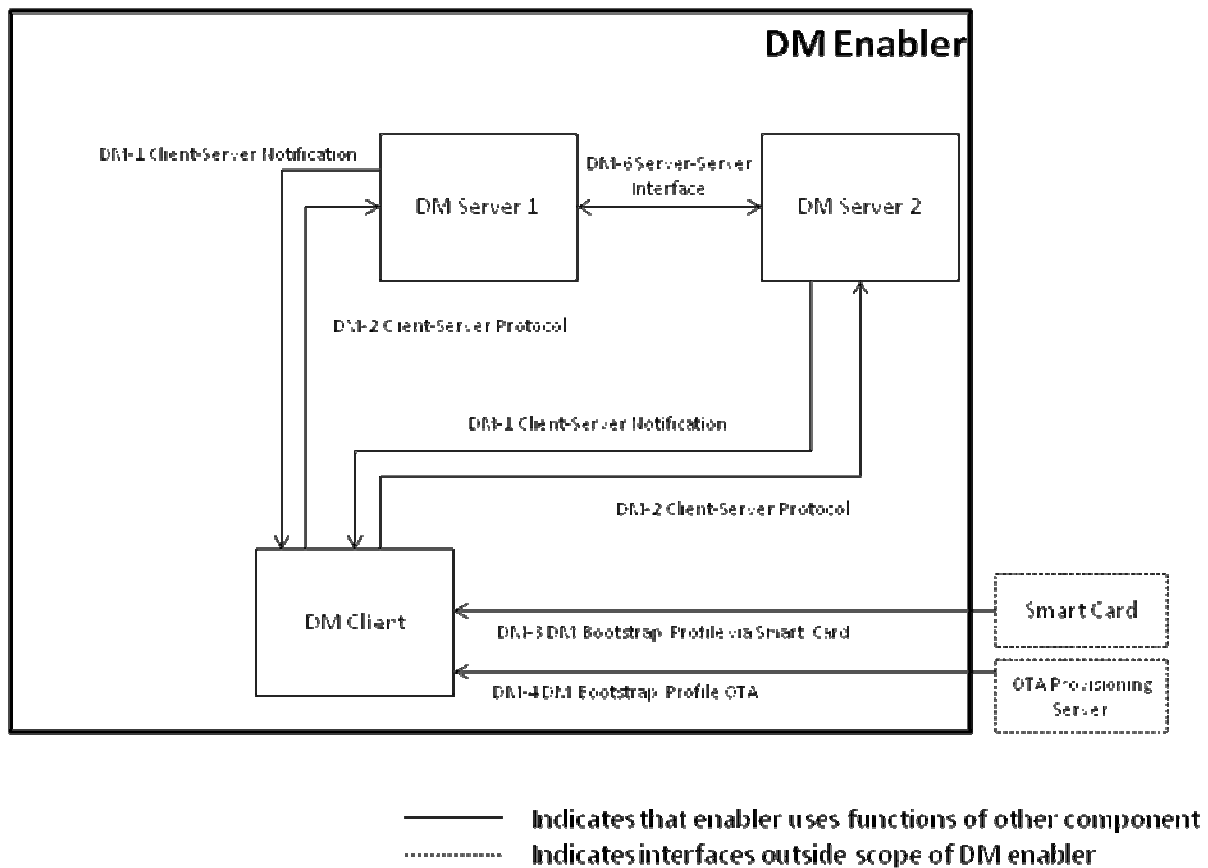


Figure 1: Device Management Architecture using interfaces

5.3 Functional Components and Interfaces/reference points definition

5.3.1 Protocol Endpoints

5.3.1.1 DM Client

The DM Client is the abstract software component that conforms to the requirements for DM Clients specified in the OMA Device Management Enabler.

5.3.1.2 DM Server

The DM Server is the abstract software component that conforms to the requirements for DM Servers specified in the OMA Device Management Enabler.

5.3.2 Interfaces

5.3.2.1 DM-1 Client-Server Notification

This provides an interface over which DM Servers may send device management notification to DM Clients. This is an interface that is bearer neutral and can operate over many protocols such as WAP Push and SIP Push.

5.3.2.2 DM-2 Device Management Client-Server Protocol

This provides an interface over which DM Servers may send device management commands to DM Clients and DM Clients may return status and alerts to DM Servers. This is an interface that is bearer neutral and offers many standardized bindings including HTTP and HTTPS. This interface MAY be exposed over an airlink-based data bearer protocol (e.g. GPRS) to provide over-the-air device management capability.

5.3.2.3 DM-3 DM Bootstrap Profile via Smart Card

The DM Client may be initially provisioned via a file on a Smart Card. This file contains a series of DM Commands to set or replace configuration settings in the DM Client. This is a one-way interface with no feedback from the DM Client. The only expected result is the DM Client connecting to the DM Server at the next practical opportunity.

5.3.2.4 DM-4 DM Bootstrap Profile OTA

The DM Client may be initially provisioned via a file sent by some push protocol. This file contains a series of DM Commands to set or replace configuration settings in the DM Client. This is a one-way interface with no feedback from the DM Client. The only expected result is the DM Client connecting to the DM Server at the next practical opportunity.

5.3.2.5 DM-6 Server-Server Interface

This provides an interface over which DM Servers may send management commands to other DM Servers and receive responses from other DM Servers. This is an interface that is bearer neutral and offers many standardized bindings including HTTP and HTTPS.

Note: The DM-5 interface is an interface described in the appendix B.

5.4 Security Considerations

Since the enabler supports one or more Management Authorities that communicate with a single DM Client, security aspects are very important as described in [DM-RD].

The Device Management enabler v2.0 supports DM Server to DM Client and DM Server to DM Server mutual authentications.

The Management Authority's data access requires authorization and protection.

The DM messages and data will have integrity verification and confidentiality protection mechanisms.

Appendix A. Change History

(Informative)

A.1 Approved Version History

| Protocol Version | Reference | Date | Description |
|------------------|-----------|------|----------------------|
| N/A | N/A | N/A | No prior 2.0 version |

A.2 Draft/Candidate Version 2.0 History

| Document Identifier | Date | Sections | Description |
|----------------------------------|--------------|-------------------------|---|
| Draft versions OMA-AD-DM-V2_0 | 24 Mar 2009 | All | New baseline |
| | 06 Nov 2009 | 5.2, 5.3, Appendix B | Applied the following CRs: OMA-DM-DM20-2009-0039-CR_Architecture_Diagrams OMA-DM-DM13-2009-0087-CR_AD_Diagram_Bug_Fix |
| | 30 Apr. 2010 | 5.2, 5.3, Appendix B | Applied the following CRs: OMA-DM-DM20-2010-0012R01-CR_App_interaction.doc OMA-DM-DM20-2010-0010R01- CR_MMA_Architecture_proposal.doc |
| | 03 May 2010 | 2, App A and B | Editorial clean-up of format by DSO, copyright changed to 2010 Update of figure 2 to show DM-6 |
| | 04 May 2010 | All | Applied the following CR: OMA-DM-DM20-2010-0018R01-CR_AD_addition_and_clean_up Language set to English UK Appendix C deleted (was an example kept from template) |
| | 31 May 2010 | All | Applied the following CRs: OMA-DM-DM20-2010-0020R01-CR_closure_review_updates OMA-DM-DM20-2010-0022-CR_DM_9 Language set to English UK |
| Candidate Version | 20 Jul 2010 | N/A | Status changed to Candidate by TP TP ref#: OMA-TP-2010-0283- INP_DM_V2_0_AD_for_Candidate_Approval |

Appendix B. Management Authority Diagram and Text (informative)

B.1 Architectural Diagram

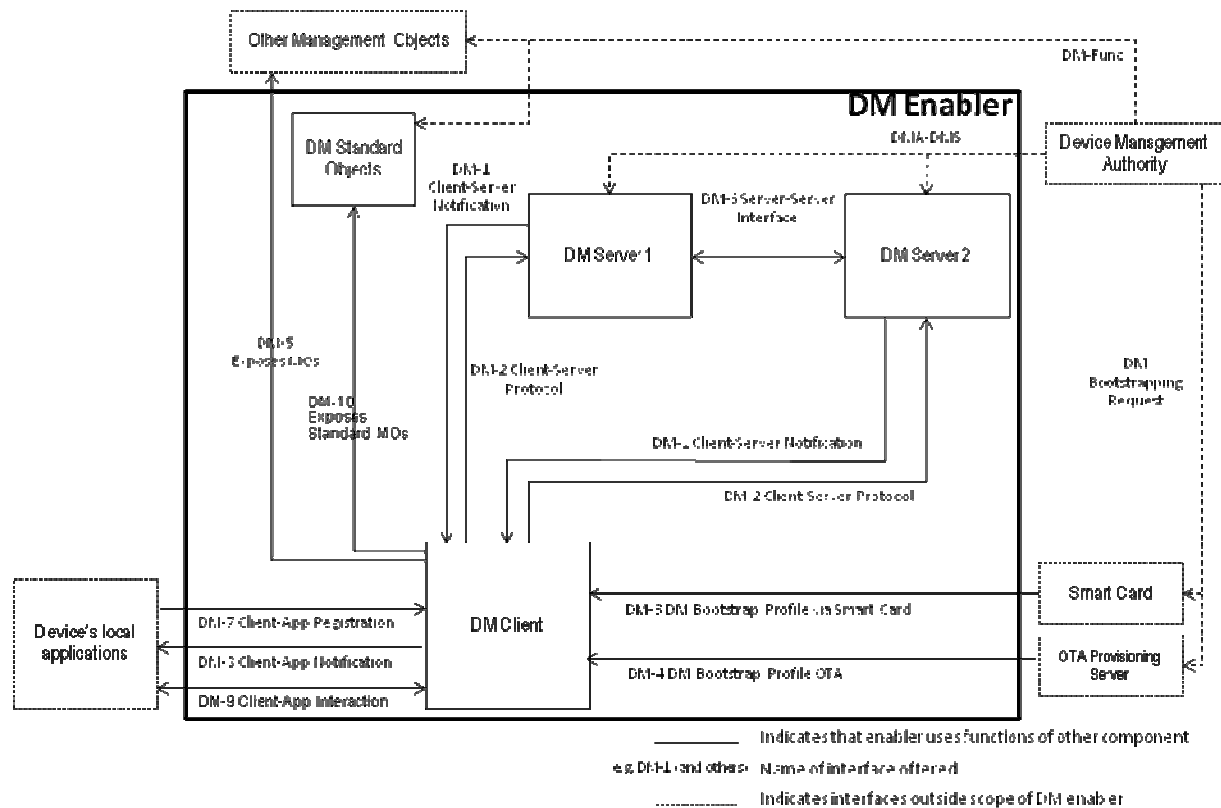


Figure 2: Device Management Architecture using interfaces

B.2 Additional Interfaces

B.2.1 DM-5 DM Exposes Management Objects

The MO schemas are exposed by the DM Client through its device management tree.

B.2.2 DM-Func DM Functions

The Standard Management Objects represent interfaces to the Device’s DM Client configuration and the Device’s DM-related information which may be targeted by a Device Management Authority to perform Device Management Functions. The functions available depend upon the DM Standard Object specifications, the access rights assigned to specific parameters for a given Device Management Authority, and on the specific device implementation.

B.2.3 DMA-DMS Interface

The interfaces between a Device Management Authority’s line-of-business systems and a Device Management Server are out of scope. For purposes of illustration, this interface allows the Device Management Authority to submit device management requests to the DM Server and to be apprised of results and device-generated alerts received by the DM Server from the DM Client. For purposes of this reference architecture description, readers should assume that an implementation-specific

interface to the DM Server is used by the Device Management Authority to submit DM commands and analyze results returned by the DM Client.

B.2.4 DM Bootstrapping Request

The Device Management Authority sets the initial provisioning information into the DM Bootstrapping Request that can then be used by the DM Client. The details of the DM Bootstrapping Request are decided by the Device Management Authority and typically relate to information necessary for the DM Client to connect to the DM Server.

B.2.5 DM-7 Client-App Registration

This provides an interface over which the device's local applications may send Management Object registration or deregistration commands to the DM Client. The device's local application may issue a Management Object retrieval request.

B.2.6 DM-8 Client-App Notification

This provides an interface over which the DM Client may send Management Object update notification to the registered device's local application.

B.2.7 DM-9 Client-App Interaction

This provides an interface over which the device's local applications may send Management Object manipulation and retrieval commands.

B.2.8 DM-10 Exposes Standards MOs

The Standard Management Objects' schemas are exposed by the DM Client through its Device Management Tree. Those Management Objects are DMAcc, DevInfo, DevDetail and Inbox.