Device Management Requirements

Candidate Version 2.0 – 20 Dec 2011

Open Mobile Alliance

OMA-RD-DM-V2_0-20111220-C

© 2011 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

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 endeavours 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.

© 2011 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 NORMATIVE REFERENCES 6
2.2 INFORMATIVE REFERENCES 6
3. TERMINOLOGY AND CONVENTIONS 7
3.1 CONVENTIONS 7
3.2 DEFINITIONS 7
3.3 ABBREVIATIONS 7
4. INTRODUCTION (INFORMATIVE) 8
4.1 VERSION 1.2 8
4.2 VERSION 1.3 8
4.3 VERSION 2.0 9
5. DEVICE MANAGEMENT RELEASE DESCRIPTION (INFORMATIVE) 10
5.1 END-TO-END SERVICE DESCRIPTION 10
6. REQUIREMENTS (NORMATIVE) 11
6.1 HIGH-LEVEL FUNCTIONAL REQUIREMENTS 11
6.1.1 Security 11
6.1.2 Administration and Configuration 12
6.1.3 Interoperability 12
6.2 OVERALL SYSTEM REQUIREMENTS 12
APPENDIX A. CHANGE HISTORY (INFORMATIVE) 13
A.1 APPROVED VERSION HISTORY 13
A.2 DRAFT/CANDIDATE VERSION 2.0 HISTORY 13
APPENDIX B. USE CASES (INFORMATIVE) 14
B.1 STARTING DEVICE MANAGEMENT BY USER 14
B.1.1 Short Description 14
B.1.2 Market benefits 14
B.2 LOADING CONFIGURATION SETTING 14
B.2.1 Short Description 14
B.2.2 Market benefits 14
B.3 DEVICE MANAGEMENT TRIGGERED BY ERROR REPORTING 14
B.3.1 Short Description 14
B.3.2 Market benefits 14

Figures

Figure 1: Device Management 10

Tables

Table 1: High-Level Functional Requirements 11
Table 2: High-Level Functional Requirements – Security Items 11
Table 3: High-Level Functional Requirements – Authentication Items 11
Table 4: High-Level Functional Requirements – Authorization Items 12
Table 5: High-Level Functional Requirements – Administration and Configuration Items 12

© 2011 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

Table 6: High-Level Functional Requirements – Interoperability Items 12

Table 7: High-Level System Requirements 12

© 2011 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

1. Scope (Informative)

This document contains use cases and requirements for Device Management 2.0. It describes a set of functional requirements for the management of a Device. These functional requirements MAY be overlapped with the requirements for DM 1.x Enabler.

Management of a Device includes:

- Setting initial configuration information in devices
- Subsequent installation and updates of persistent information in devices
- Retrieval of management information from devices
- Processing events and alarms generated by devices

© 2011 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

2. References

2.1 Normative References

[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 Principle", Open Mobile Alliance™, URL:http://www.openmobilealliance.org/

[DM_1.x] "OMA Device Management Protocol", Version 1.3, Open Mobile Alliance™, URL:http://www.openmobilealliance.org/

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

© 2011 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

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

3.3 Abbreviations

OMA Open Mobile Alliance

© 2011 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

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.

Device Management allows network 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 1.2

Device management is the generic term used for technology that allows third parties to carry out the difficult procedures of configuring devices on behalf of the end user (customer). Third parties would typically be operators, service providers or corporate information management departments.

Through device management, an external party can remotely set parameters, conduct troubleshooting servicing of terminals, install or upgrade software. In broad terms, device management consists of three parts:

- Protocol and mechanism: The protocol used between a management server and a device
- Data model: The data made available for remote manipulation, for example browser and mail settings
- Policy: The policy decides who can manipulate a particular parameter, or update a particular object in the device

The specifications in the Device Management enabler Version 1.2 address the first part of device management above, the protocol and mechanism. More particularly, this enabler release addresses the management of devices by specifying a protocol and management mechanism that may be exposed by an OMA DM client and targeted by an OMA DM server.

The architecture of the Device Management enabler anticipates the needs of the market actors to differentiate their products through vendor-specific extensions while providing a core parameter set that can be relied upon in all terminals exposing this standardized interface.

The design of the architecture follows the OMA architecture principle [ARCH-PRINC] of Network Technology Independence by separating the bearer-neutral requirements from bearer-specific bindings. The described architecture also anticipates additional bearer and proxy types, as any are identified, without requiring a respecification of previously released documents. This preserves vendor and customer investment while supporting the scaling required by future innovations.

There are three parts to the object schema that provide break-points between more general and more specific parameters:

- A top level management object which is bearer-neutral;
- A set of bearer-specific parameters;
- Sub-tree(s) for exposing vendor-specific parameters.

By composing the management objects in this way, it becomes possible for a device management authority to:

- Target generic requirements that span all implementations;
- Focus on bearer-specific idiosyncrasies of a given networking environment;
- Activate terminal-specific behaviour by adjusting vendor-specific parameters.

In a wireless environment, the crucial element for device management protocol is the need to efficiently and effectively address the characteristics of devices including low bandwidth and high latency and to provide for support of these management operations remotely, over-the-air.

4.2 Version 1.3

OMA DM Version 1.3 reused the architecture from OMA DM Version 1.2. It does introduce new notification, transport protocols and a new DM Server to DM Server interface for delegation.

© 2011 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document. [OMA-Template-ReqDoc-20110101-I]

4.3 Version 2.0

OMA DM Version 2.0 reuses Management Objects which are designed for DM Version 1.3 or earlier DM Protocols.OMA DM Version 2.0 introduces new Client-Server DM protocol.

OMA DM Version 2.0 also introduces new user interaction method on Device Management using Web Browser Component.

© 2011 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

5. Device Management release description (Informative)

The Device Management (DM) 2.0 Enabler provides a platform neutral protocol to allow servers to remotely manage devices. DM is intended to operate over a HTTP transport protocol and notification protocols in a platform neutral format.

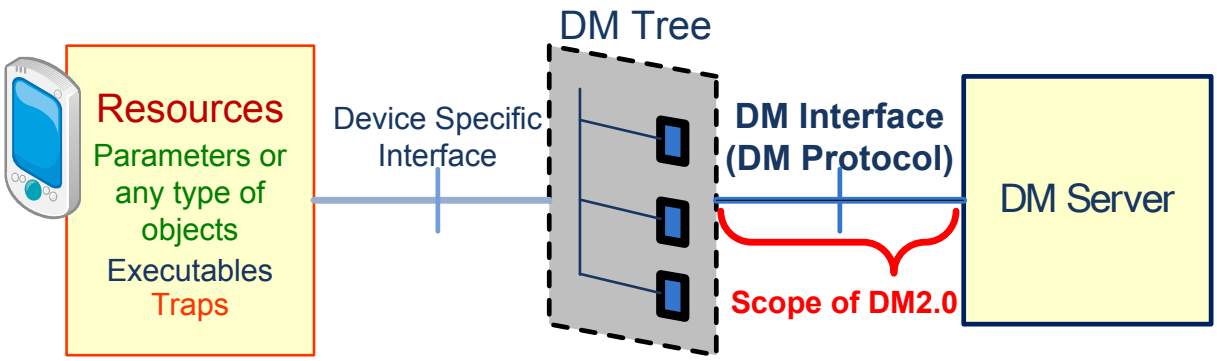

Figure 1: Device Management

5.1 End-to-end Service Description

The DM 2.0 Enabler is based on RESTful architecture. This protocol allows simpler implementations of both DM clients and DM servers by reusing widely deployed standard base technologies, such as HTTP, and JSON data representation.The DM 2.0 Enabler can handle existing Management Objects (MO) which are designed for working with DM 1.x Enabler.

© 2011 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

6. Requirements (Normative)

6.1 High-Level Functional Requirements

Functional Requirements regarding Device Management are described below:

Label	Description	Release
DM-HLF-001	The DM enabler SHALL specify a mechanism for the DM Client to expose supported MO types.	2.0
DM-HLF-002	The DM enabler SHALL support web browser or web browser component for the UI functionality.	2.0
DM-HLF-003	The DM enabler SHALL support a mechanism for delivering the management data and management commands separately.	2.0
DM-HLF-004	The DM enabler SHALL support delivery of management commands and management data in the same message.	2.0
DM-HLF-005	The DM enabler SHALL support HTTP GET, POST, and PUT operations for device management.	2.0
DM-HLF-006	The DM enabler SHALL support a mechanism for delivering information required for bootstrapping.	2.0
DM-HLF-007	The DM enabler SHALL support interface to manipulate DM Management Tree	2.0
DM-HLF-008	The DM enabler SHALL provide a mechanism for the discovery of optional DM features supported by the client	2.0

Table 1: High-Level Functional Requirements

6.1.1 Security

Security requirements are described below:

Label	Description	Release
DM-SEC-001	The DM enabler SHALL support authentication, authorization, integrity and confidentiality.	2.0
DM-SEC-002	DM Enabler SHALL provide secure communication channel between DM Server and DM Client	2.0
DM-SEC-003	DM Enabler SHALL support secure communication channel between Data Repository and DM Client	2.0

Table 2: High-Level Functional Requirements – Security Items

6.1.1.1 Authentication

Label	Description	Release
DM-AT-001	DM Enabler SHALL provide mutual authentication between DM Server and DM Client	2.0
DM-AT-002	DM Enabler SHALL support mutual authentication between Data Repository and DM Client	2.0

Table 3: High-Level Functional Requirements – Authentication Items

6.1.1.2 Authorization

Authorization requirements are described below:

© 2011 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

Label	Description	Release
DM-AZ-001	The DM enabler SHALL support a mechanism to separate the right for managing the access control from managing data. **Informational Note**: DM 1.3 use 'Replace' right for both managing data and the access control.	2.0
DM-AZ-002	DM Enabler SHALL not allow un-authorized access from DM Client to DM Server	2.0
DM-AZ-003	DM Enabler SHALL not allow un-authorized access from DM Server to DM Client	2.0

Table 4: High-Level Functional Requirements – Authorization Items

6.1.2 Administration and Configuration

Administration and Configuration requirements regarding Device Management Service are described below:

Label	Description	Release
DM-ADM-001	DM Enabler SHALL allow the DM Server to use the same DM account across multiple devices.	2.0

Table 5: High-Level Functional Requirements – Administration and Configuration Items

6.1.3 Interoperability

Interoperability requirements hiding difference between implementations:

Label	Description	Release
DM-INT-001	The DM enabler SHALL support the usage of MIME types for identifying the format of the management data.	2.0
DM-INT-002	The DM enabler SHALL specify a JSON format for delivering a MO.	2.0
DM-INT-003	The DM enabler SHALL allow the servers to manage devices without the knowledge of a MO location.	2.0
DM-INT-004	The DM enabler SHALL allow supported MOs to be described in separate DDF files.	2.0
DM-INT-005	The DM enabler SHALL support existing Management Objects which have been designed to work with OMA DM 1.x.	2.0

Table 6: High-Level Functional Requirements – Interoperability Items

6.2 Overall System Requirements

General requirements for DM Enabler are describe below:

Label	Description	Release
DM-SYS-001	The DM enabler SHALL allow state-less implementation of servers.	2.0

Table 7: High-Level System Requirements

© 2011 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

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 2.0 History

Document Identifier	Date	Sections	Description
Draft Versions OMA-RD-DM-V2_0	10 May 2011	All	First template version as baseline, agreed in "OMA-DM-DMNG-2011-0013-INP_Baseline_RD"
	26 May 2011	6.1	Adding lates revision of CR# 2011-0016 ➔ 2011-0023
	10 Aug 2011	1, 5, 6.1, App B	Adding CR 2011-0026R01, 0028R01, 0031, 0032R01
	3 Oct 2011	6.x	Adding CR: OMA-DM-DMNG-2011-0036R01-CR_RD_Cleanup OMA-DM-DMNG-2011-0037R02-CR_Req_Account OMA-DM-DMNG-2011-0043R01-CR_Right_for_Managing_... OMA-DM-DMNG-2011-0048-CR_RD_interop_and_securit... OMA-DM-DMNG-2011-0050R01-CR_MoreReqsForDM20
	17 Oct 2011	4 6	Added CR: OMA-DM-DMNG-2011-0060R01-CR_RD_Intro Editorial updates (renumber requirements)
	26 Oct 2011	All	Editorial updates from the closure review
	2 Dec 2011	2.2 & 6.2	Adding CR OMA-DM-DMNG-2011-0087-CR_RD_RR_Corrections that includes all chages resulting from the consistency review
Candidate Version OMA-RD-DM-V2_0	20 Dec 2011	N/A	Status changed to Candidate by TP Ref # OMA-TP-2011-0440-INP_DMNG_DM_V2_0_RD_for_Candidate_approval

© 2011 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document.

Appendix B. Use Cases (Informative)

Basic use cases are introduced here to clarify the functional requirements for DM 2.0 protocol.

B.1 Starting Device Management by user

B.1.1 Short Description

A subscriber user decided to be managed by the DM Server. The user creates his account for DM service, and registers his Device to be managed. The device will be configured to accept the managements from the DM Server.

B.1.2 Market benefits

The subscriber user may purchase the device without initial contact with any operators. The user may choose one of his/her subscribing operators as the device's Management Authority.

B.2 Loading Configuration Setting

B.2.1 Short Description

A user had a problem to get access on the public wireless network. She wanted to load the configuration setting for the device from the DM Server. The mobile network operator's portal site provides the links to load the setting for various wireless network providers.

B.2.2 Market benefits

The subscriber user can help his/herself using the operator's portal site.

B.3 Device Management triggered by Error Reporting

B.3.1 Short Description

A subscriber user experienced call-drop due to network error. The device report the error event to the DM Server, and the server manage the device to collect further detail information from the log in the device.

B.3.2 Market benefits

The DM Server can collect the log information from the device, only when the error is occurred.

© 2011 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document. [OMA-Template-ReqDoc-20110101-I]