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

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
Table 6: High-Level Functional Requirements – Interoperability Items .................................................................12
Table 7: High-Level System Requirements .................................................................................................................12
1. Scope

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
2. References

2.1 Normative References


2.2 Informative References


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
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.
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.
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.

![Device Management Diagram]

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.
6. Requirements

6.1 High-Level Functional Requirements

Functional Requirements regarding Device Management are described below:

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

Table 1: High-Level Functional Requirements

6.1.1 Security

Security requirements are described below:

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>DM-SEC-001</td>
<td>The DM enabler SHALL support authentication, authorization, integrity and confidentiality.</td>
<td>2.0</td>
</tr>
<tr>
<td>DM-SEC-002</td>
<td>DM Enabler SHALL provide secure communication channel between DM Server and DM Client</td>
<td>2.0</td>
</tr>
<tr>
<td>DM-SEC-003</td>
<td>DM Enabler SHALL support secure communication channel between Data Repository and DM Client</td>
<td>2.0</td>
</tr>
</tbody>
</table>

Table 2: High-Level Functional Requirements – Security Items

6.1.1.1 Authentication

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>DM-AT-001</td>
<td>DM Enabler SHALL provide mutual authentication between DM Server and DM Client</td>
<td>2.0</td>
</tr>
<tr>
<td>DM-AT-002</td>
<td>DM Enabler SHALL support mutual authentication between Data Repository and DM Client</td>
<td>2.0</td>
</tr>
</tbody>
</table>

Table 3: High-Level Functional Requirements – Authentication Items
6.1.1.2 Authorization

Authorization requirements are described below:

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>DM-AZ-001</td>
<td>The DM enabler SHALL support a mechanism to separate the right for managing the access control from managing data.</td>
<td>2.0</td>
</tr>
<tr>
<td></td>
<td><strong>Informational Note:</strong> DM 1.3 use ‘Replace’ right for both managing data and the access control.</td>
<td></td>
</tr>
<tr>
<td>DM-AZ-002</td>
<td>DM Enabler SHALL not allow un-authorized access from DM Client to DM Server</td>
<td>2.0</td>
</tr>
<tr>
<td>DM-AZ-003</td>
<td>DM Enabler SHALL not allow un-authorized access from DM Server to DM Client</td>
<td>2.0</td>
</tr>
</tbody>
</table>

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:

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>DM-ADM-001</td>
<td>DM Enabler SHALL allow the DM Server to use the same DM account across multiple devices.</td>
<td>2.0</td>
</tr>
</tbody>
</table>

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

6.1.3 Interoperability

Interoperability requirements hiding difference between implementations:

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

Table 6: High-Level Functional Requirements – Interoperability Items

6.2 Overall System Requirements

General requirements for DM Enabler are describe below:

<table>
<thead>
<tr>
<th>Label</th>
<th>Description</th>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>DM-SYS-001</td>
<td>The DM enabler SHALL allow state-less implementation of servers.</td>
<td>2.0</td>
</tr>
</tbody>
</table>

Table 7: High-Level System Requirements
Appendix A. Change History (Informative)

A.1 Approved Version History

<table>
<thead>
<tr>
<th>Reference</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>N/A</td>
<td>N/A</td>
<td>No prior version</td>
</tr>
</tbody>
</table>

A.2 Draft/Candidate Version 2.0 History

<table>
<thead>
<tr>
<th>Document Identifier</th>
<th>Date</th>
<th>Sections</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Draft Versions</td>
<td>10 May 2011</td>
<td>All</td>
<td>First template version as baseline, agreed in “OMA-DM-DMNG-2011-0013-INP_Baseline_RD”</td>
</tr>
<tr>
<td></td>
<td>26 May 2011</td>
<td>6.1</td>
<td>Adding latest revision of CR# 2011-0016 ➔ 2011-0023</td>
</tr>
<tr>
<td></td>
<td>10 Aug 2011</td>
<td>1, 5, 6.1, App B</td>
<td>Adding CR 2011-0026R01, 0028R01, 0031, 0032R01</td>
</tr>
<tr>
<td></td>
<td>26 Oct 2011</td>
<td>All</td>
<td>Editorial updates from the closure review</td>
</tr>
<tr>
<td></td>
<td>2 Dec 2011</td>
<td>2.2 &amp; 6.2</td>
<td>Adding CR OMA-DM-DMNG-2011-0087-CR_RD_RR_Corrections that includes all changes resulting from the consistency review</td>
</tr>
</tbody>
</table>

Candidate Version

<table>
<thead>
<tr>
<th>Document Identifier</th>
<th>Date</th>
<th>Sections</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OMA-RD-DM-V2_0</td>
<td>20 Dec 2011</td>
<td>N/A</td>
<td>Status changed to Candidate by TP Ref # OMA-TP-2011-0440-INP_DMNG_DM_V2_0_RD_for_Candidate_approval</td>
</tr>
<tr>
<td>Candidate Version</td>
<td>10 Dec 2013</td>
<td>n/a</td>
<td>Status changed to Candidate by TP TP Ref # OMA-TP-2013-0384-INP_DM_V2_0_ERP_and_ETR_for_Candidate_approval</td>
</tr>
</tbody>
</table>
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.