Device Management Requirements

Candidate Version 2.0 – 09 Mar 2010

Open Mobile Alliance

OMA-RD-DM-V2_0-20100309-C

Contents

1. SCOPE (INFORMATIVE) 4
2. REFERENCES 5
2.1 NORMATIVE REFERENCES 5
2.2 INFORMATIVE REFERENCES 5
3. TERMINOLOGY AND CONVENTIONS 6
3.1 CONVENTIONS 6
3.2 DEFINITIONS 6
3.3 ABBREVIATIONS 6
4. INTRODUCTION (INFORMATIVE) 7
5. DEVICE MANAGEMENT RELEASE DESCRIPTION (INFORMATIVE) 8
5.1 VERSION 1.2 8
5.2 VERSION 1.3 8
5.3 VERSION 2.0 8
6. REQUIREMENTS (NORMATIVE) 9
6.1 MODULARISATION 9
6.2 HIGH-LEVEL FUNCTIONAL REQUIREMENTS 9
6.2.1 Security 11
6.2.2 Charging 12
6.2.3 Administration and Configuration 12
6.2.4 Usability 12
6.2.5 Interoperability 12
6.2.6 Privacy 12
6.3 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 QUERY DEVICE MOS FOR ENHANCED CUSTOMER SUPPORT 14
B.1.1 Short Description 14
B.1.2 Market benefits 14
B.2 A NEWLY INSTALLED APPLICATION RETRIEVES SPECIFIC SETTINGS SECURELY FROM A MANAGEMENT OBJECT 14
B.2.1 Short Description 14
B.2.2 Market benefits 14
B.3 CONTINUOUS PROVISIONING OF NOMADIC DEVICES 14
B.3.1 Short Description 14
B.3.2 Market Benefits 14

Figures

N/A

Tables

Table 1: High-Level Functional Requirements 11

1. Scope (Informative)

This document contains use cases and requirements for OMA Device Management version 2.0. It describes a set of enhanced and new functional requirements for the management of a Device. DM 2.0 is the next major release of OMA's protocol for remote management of Devices. Being a major release of the OMA-DM protocol, backward compatibility with DM 1.2 and other minor releases under DM 1.0 is not assured.

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

[ConnMO] " Reference Release Definition for ConnMO", Version 1.0, Open Mobile Alliance™, OMA-RRELD-ConnMO-V1_0, URL:http://www.openmobilealliance.org/

[DMDICT] " OMA Device Management Dictionary", Draft Version 1.0, , Open Mobile Alliance™, 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/

[OMAPROC] "OMA Organization and Process", Version 1.4, Open Mobile Alliance™, 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

Kindly consult [DMDICT] and [OMADICT] for all definitions used in this document.

3.3 Abbreviations

Kindly consult [DMDICT] and [OMADICT] for all abbreviations used in this document.

4. Introduction (Informative)

The motivation for DM 2.0 stems from two considerations: One is a general desire to address some of the shortcomings of the previous DM releases and theother is to enhance the OMA DM protocol to for converged devices.

Many of the perceived shortcomings of DM 1.2 are being addressed in DM 1.3. Unfortunately some of the shortcomings or enhancements of DM 1.2 cannot be addressed while maintaining backward compatibility and therefore they are not being addressed in DM 1.3, as per OMA guidelines [OMAPROC], thus are expected to be addressed in DM 2.0. The major push for DM 2.0 is to tackle issues related to CDM (Converged Device Management).

Up until DM 2.0, OMA DM has been used for the remote management of single-mode wireless devices. However, in this age of device and service convergence, as multi-mode devices are coming out in the market in increasing numbers and the strict delineation between wireless and wireline devices is getting increasingly blurred, it seems inevitable that OMA DM 2.0 has to address both the existing and a completely new set of market requirements.

5. Device Management release description (Informative)

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

5.1 Version 1.2

The DM V1.2 Enabler added or improved the following functionalities:

- Enhanced security
- DM Profile bootstrap
- TNDS
- Inbox
- DM Account
- XML Encryption
- Generic Alert
- Excluded "Con" object which provided rudimentary connectivity configuration and which as since been replaced by the ConnMO Reference Release [ConnMO]
- Nonce Resynchronization

5.2 Version 1.3

The DM V1.3 Enabler supports the following additional functionalities:

- Support for SIP Push for sending notification message,
- Specify for mandatory support for bootstrap/TNDS
- Support for rich information in notification message including expiration, reason for session, etc.
- Improved discovery of optional DM functionalities supported by the DM Client.

5.3 Version 2.0

The DM V2.0 Enabler provides the following functionalities:

- Improved mechanism or requirements for multiple management authorities dealing with a single client.
- Management of devices that do not have DM Clients..
- An application interface for device applications to interact with the DM Client's management objects.
- Support DM functionality on virtualized platforms (i.e. devices with more than one access technology/operating system/environment).
- Improved protocol and representation from DM 1.3.

6. Requirements (Normative)

6.1 Modularisation

This section depicts the whole release as a collection of different functional modules where each one is a group of requirements identified as related with the offering of functionality. Functional modules will be described as mandatory functionality (core functionality) or optional functionality (value-added functionality).

The defined functional modules are as follows:

- **Bootstrap**: this functional module supports the process of installing parameters and/or applications on a DM Client to establish a given service for the first time, or for the purposes of resetting a DM Client to initial settings. This is a mandatory functional module.
- **Notification**: this functional module provides for out-of-band notification from a DM Server to a DM Client, indicating that a session is desired. This is a mandatory functional module.
- **Security**: this functional module provides secure management sessions between a DM Server and a DM Client. This is a mandatory functional module.
- **Transports**: this functional module supports multiple transports for communication between a DM Server and a DM Client. This is a mandatory functional module.
- **Management Authority**: this functional module provides requirements for supporting multiple Management Authorities and delegation functionalities. This is a mandatory functional module.
- **General:** Some requirements are intended to affect all the functional modules, and therefore are marked in the functional module column of the requirement's table as “General”.

6.2 High-Level Functional Requirements

Label	Description	Release	Functional module
DM-HLF-001	DM Protocol and Representation SHALL be access technology agnostic.	2.0	General
DM-HLF-002	DM Enabler SHOULD support a mechanism to allow DM sessions against a device placed behind a firewall or NAT (“Network Address Translator”).	2.0	General
DM-HLF-003	DM Enabler SHOULD support a mechanism to manage devices without user interface.	2.0	General
DM-HLF-004	DM Enabler SHALL support a mechanism allowing a server to retrieve the value of a DM Client’s MOs (all or subset) with a focus on the query and response consuming minimum bandwidth and processing resources.	2.0	General
DM-HLF-005	The DM Client SHALL allow local device’s applications to interact with it’s Management Objects.	2.0	General
DM-HLF-006	DM Enabler SHALL support a mechanism to manage the device with more than one operating system/environment.	2.0	General
DM-HLF-007	DM Enabler SHALL support a mechanism to manage the device with more than one access technologies.	2.0	General

DM-HLF-008	The DM Enabler SHALL specify a mechanism to allow continuous management of devices, even if the devices are change networks or use different data transports.	2.0	General
DM-HLF-009	The DM Enabler SHALL support a mechanism to control which type of Management Objects can be managed by a specified DM Server.	2.0	Management Authority
DM-HLF-010	The DM Enabler SHOULD support multimedia user interaction methods.	2.0	General
DM-HLF-011	The DM Client SHALL support multiple Management Authorities managing different instances of the same Management Object.	2.0	Management Authority
DM-HLF-012	The DM Client SHALL support multiple Management Authorities.	2.0	Management Authority
DM-HLF-013	The DM Client SHALL support the delegation of a Management Authority's control to other Management Authorities.	2.0	Management Authority
DM-HLF-014	The DM Enabler SHALL support a mechanism to prioritize Management Authorities that access the same instance of a management object.	2.0	Management Authority
DM-HLF-015	The DM Client SHALL process DM messages only from authorized DM Servers.	2.0	Security
DM-HLF-016	The DM enabler SHALL provide a mechanism for local applications in the device to register for notifications to changes to an instance of a registered MO.	2.0	General
DM-HLF-017	The DM enabler SHALL provide a mechanism to notify registered applications in the device for changes to an instance of a registered MO.	2.0	General
DM-HLF-018	The DM Client SHALL be able to choose the appropriate DM Server for a DM Client initiated management session.	2.0	General
DM-HLF-019	The DM enabler SHALL provide a mechanism for the discovery of optional DM features supported by the DM Client	2.0	General
DM-HLF-020	The DM Enabler SHALL support a mechanism to restrict DM Server access to specific types of MOs.	2.0	General
DM-HLF-021	DM Enabler SHALL support the capability to suspend and resume the transfer of large objects	2.0	General
DM-HLF-022	The DM Enabler SHALL support Shared Delegation.	2.0	Management Authority
DM-HLF-023	The DM Enabler SHALL support Full Delegation.	2.0	Management Authority
DM-HLF-024	The DM Enable SHALL support Sub Delegation.	2.0	Management Authority
DM-HLF-025	The DM Enabler SHALL ensure complete confidentiality of data across different Management Authorities in the case of Full Delegation.	2.0	Management Authority

DM-HLF-026	The DM Enabler SHALL allow a Management Authority (MA) to impose restrictions on sub-delegation of management capabilities to other MAs. These restrictions include, but are not limited to, the following: ▪ number of further levels of sub-delegation allowed ▪ prohibited MAs (i.e. MAs to which sub-delegation is not allowed)	2.0	Management Authority
DM-HLF-027	The DM enabler SHALL be backwards compatible with the data structure of existing Management Objects which have been designed to work with OMA DM 1.x.	2.0	General

Table 1: High-Level Functional Requirements

6.2.1 Security

6.2.1.1 Authentication

Label	Description	Release	Functional module
DM-SECACATE-001	The DM Enabler SHALL support a mechanism for mutual authentication between the DM Client and the DM Server.	2.0	Security

6.2.1.2 Authorization

Label	Description	Release	Functional module
DM-SECARIZE-001	The DM Enabler MUST support a mechanism to protect Management Authority's data from unauthorized DM Servers.	2.0	Security
DM-SECARIZE-002	The DM Client MUST protect DM data from unauthorized access.	2.0	Security

6.2.1.3 Data Integrity

Label	Description	Release	Functional module
DM-DI-001	The DM Enabler SHALL provide a mechanism for verifying the integrity of DM messages and DM data transferred.	2.0	Security

6.2.1.4 Confidentiality

Label	Description	Release	Functional module
DM-SECCONF-001	The DM Enabler SHALL ensure confidentiality of DM messages and DM data.	2.0	Security

6.2.2 Charging

N/A

6.2.3 Administration and Configuration

N/A

6.2.4 Usability

N/A

6.2.5 Interoperability

Label	Description	Release	Functional module
DM-IOP-001	The DM Enabler SHALL be interoperable across networks and access technologies.	2.0	General
DM-IOP-002	The DM Enabler SHOULD be interoperable with other OMA enablers.	2.0	General
DM-IOP-003	The DM Enabler SHOULD be interoperable with other remote management protocols.	2.0	General

6.2.6 Privacy

N/A

6.3 Overall System Requirements

N/A

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	16 Dec 2008	All	Initial Baseline document
	24 Feb 2009	All	Incorporated CRs: OMA-DM-DM20-2009-0002R01 OMA-DM-DM20-2009-0003R01 OMA-DM-DM20-2009-0005R01 OMA-DM-DM20-2009-0006R01
	26 Mar 2009	5.1&2	Incorporated CR: OMA-DM-DM20-2009-0008
	07 Apr 2009	6.2.5	Incorporated CR: OMA-DM-DM20-2009-0010
	07 May 2009	6.2&B.3	Incorporated CRs: OMA-DM-DM20-2009-0011R01 OMA-DM-DM20-2009-0012R02 OMA-DM-DM20-2009-0018R01 OMA-DM-DM20-2009-0020R03
	30 May 2009	6	Incorporated CR: OMA-DM-DM20-2009-0015R02
	07 July 2009	6	Incorated CRs: OMA-DM-DM20-2009-0024R01 OMA-DM-DM20-2009-0026R01 OMA-DM-DM20-2009-0027R01
	11 Sep. 2009	6	Incorated CRs: OMA-DM-DM20-2009-0031R01 OMA-DM-DM20-2009-0035R02 OMA-DM-DM20-2009-0038
	21 Oct. 2009	5 & 6	Incorated CRs: OMA-DM-DM20-2009-0042R01 OMA-DM-DM20-2009-0041R01 OMA-DM-DM20-2009-0046
	06 Nov. 2009	All	General editorial clean up
	12 Dec, 2009	5 & 6	Incorated CRs: OMA-DM-DM20-2009-0032R03 OMA-DM-DM20-2009-0069R01
	24 Jan, 2010	6	Incorated CRs: OMA-DM-DM20-2009-0070R01 OMA-DM-DM20-2009-0072R01
	04 Feb, 2010	5&6	Incorated CRs: OMA-DM-DM20-2009-0073R01 OMA-DM-DM20-2010-0002R01 OMA-DM-DM20-2010-0003R01
	05 Feb. 2010	6	Some online changing in Sorrento meeting.
Candidate Version OMA-RD-DM-V2_0	09 Mar 2010	N/A	Status changed to Candidate by TP TP ref#: OMA-TP-2010-0100-INP_DM_V2_0_RD_for_Candidate_Approval

Appendix B. Use Cases (Informative)

B.1 Query Device MOs for Enhanced Customer Support

B.1.1 Short Description

A user calls customer care with a fault on their device. The customer care centre wishes to query the device receiving back the current state of all or a subset of the DM MOs on the device. This needs to be done in some reasonable amount of time to provide good service to the user and reduce costs for the customer care centre.

B.1.2 Market benefits

Fast retrieval of a device's current configuration state information (DM MOs) will allow customer care personnel to more quickly diagnose and resolve customer problems. Obviously good customer service and ensuring devices in the field continue to function well is one of the key purposes of OMA DM.

B.2 A newly installed application retrieves specific settings securely from a Management Object

B.2.1 Short Description

A user installs an application on her device, this application requires specific settings to work correctly. The application once installed registers with the device's DM client. The device's DM client makes the necessary verifications and allows the application to retrieve the requested settings.

B.2.2 Market benefits

The user does not have to call the customer care representative or/and to enter any technical settings. The application setup is quick, easy and totally transparent for the end user. The user experience is enhanced. If, in the future, the parameters used by the application are updated, the application settings will be updated accordingly.

B.3 Continuous Provisioning of nomadic devices

B.3.1 Short Description

Home network deployments are mimicking small and medium business network deployments as users are getting more security conscious. Firewall and NAT functionality is now an integral part of the home gateway device. Users are expecting secure connectivity between the smart gadgets and the outside world irrespective of their physical location.

The following use case elaborates this requirement:

> *Yamada Taro purchases a smart gadget from the operator's outlet store and hooks it up into his home network. The smart gadget gets bootstrapped and is able to establish communication with a DM Server. The DM Server performs initial provisioning on the device. After a few days, he unplugs the gadget from his home network and plugs it into his business network. Even though the smart gadget has moved from one private network to another, the DM Server is able to continue with Continuous Provisioning of the gadget.*

B.3.2 Market Benefits

Service providers will greatly benefit from this requirement since they will be able to satisfy users' expectation of seamless management of nomadic devices, irrespective of the location of the device.