Device Management Requirements

Approved Version 1.3 – 24 May 2016

Open Mobile Alliance

OMA-RD-DM-V1_3-20160524-A

Contents

Figures

Tables

1. Scope (Informative)

This document contains use cases and requirements for Device Management 1.3. It describes a set of enhanced or new functional requirements for the management of a Device. These functional requirements will maintain the backward compatibility with DM 1.2.

2. References

2.1 Normative References

[DM12RD] "OMA Device Management Requirements Document", Version 1.2, Open Mobile Alliance™, OMA-RD-DM-V1_2, URL:http://www.openmobilealliance.org/

[DMDICT] "OMA Device Management Dictionary, Version 1.0". Open Mobile Alliance™. OMA-SUP-DM_Dictionary-v1_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

None.

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] for all definitions used in this document.

3.3 Abbreviations

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

4. Introduction (Informative)

Currently, DM technology allows a device to present the information stored on the device to an external server, in case the external server has sufficient rights to do this. This can be seen in the following picture:

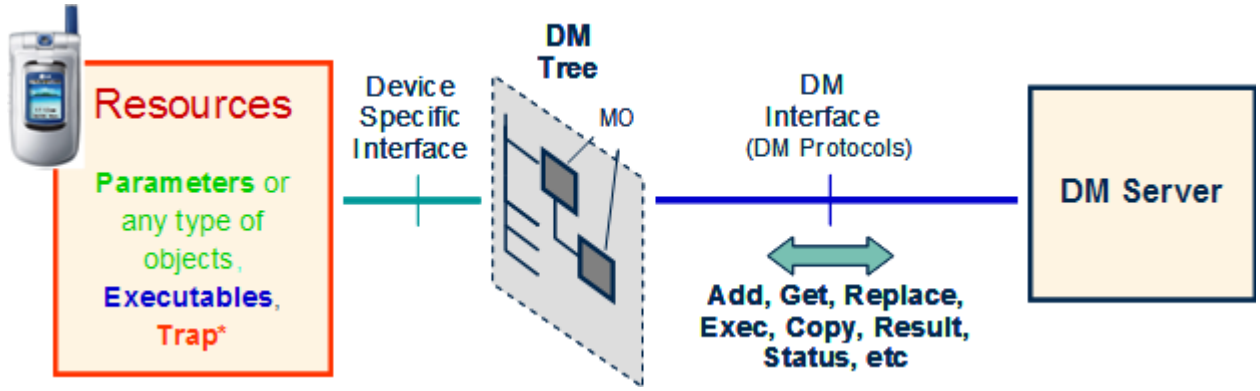

Figure 1: Device management

At the left side of the picture we can find the device, with its internal resources. The device presents part of this information to the server that is on the right part. The way to do this is through Management Objects at the DM Tree.

Along with the emergence of advanced Devices and new services, the device management framework already defined in DM 1.2 [DM12RD] is enhanced in release 1.3 to address more market needs. The objective of this document is to collect additional use cases, a set of enhanced and/or new functional requirements for the management of a Device to cover those needs in release 1.3.

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 functionality:

- Enhanced security
- DM Profile bootstrap
- TNDS
- Inbox
- DM Account
- XML Encryption
- Generic Alert
- Connectivity settings moved to ConnMO Reference Release
- Nonce Resynchronization

5.2 Version 1.3

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

- Sessionless DM
- Support for rich information in notification message including expiration, reason for session, etc.
- Support for notification to contain server request for specific management objects to be sent in package 1
- SIP Push and HTTP Push binding for DM Notification
- Enhancement on existing bootstrap mechanism in DM 1.2
- Support Client to request bootstrap using HTTPS GET
- Clarification regarding Inbox and TNDS Usage
- Support for the discovery of optional DM features supported by the DM client
- Mandating support for TLS 1.1 and recommending support for TLS 1.2 for HTTP Binding
- Virtual URI based addressing
- Enhanced DM structural query
- Indication of the roaming status and bearer for the current DM session
- Server to server delegation

The DM V1.3 enabler merged the OMA SyncML Common V1.2 into its own release.

6. Requirements (Normative)

6.1 Modularisation

The requirements for DM 1.3 are in addition to the requirements for DM 1.2 [DM12RD].

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.
- **Authentication**: 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.
- **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	The DM enabler SHALL specify SIP transport. **Informational Note:** DM 1.2 already supports HTTP, WSP and OBEX.	Future	Transports
DM-HLF-002	The DM enabler SHALL specify UDP transport. **Informational Note:** DM 1.2 already supports HTTP, WSP and OBEX.	Future	Transports
DM-HLF-003	The DM enabler SHALL specify SIP notification method. **Informational Note:** DM 1.2 already supports the WAP PUSH method.	1.3	Notification
DM-HLF-004	The DM enabler SHALL specify UDP notification method. **Informational Note:** DM 1.2 already supports the WAP PUSH method.	Future	Notification
DM-HLF-005	The DM enabler SHALL specify mandatory bootstrap functionality. **Informational Note:** DM 1.2 already supports optional bootstrap.	1.3	Bootstrap
DM-HLF-006	The DM enabler notification SHALL provide expiration for the notification message. **Informational Note:** DM 1.2 notification does not provide for expiration, reason for session or recommended protocol version. The new notification MUST be backward compatible with the DM 1.2 version.	1.3	Notification

DM-HLF-007	The DM enabler notification SHALL convey reason for session information in the notification message. **Informational Note:** DM 1.2 notification does not provide for expiration, reason for session or recommended protocol version. The new notification MUST be backward compatible with the DM 1.2 version.	1.3	Notification
DM-HLF-008	The reason for session information SHALL be made available to the end user as additional information before establishing the management session if user interaction is required.	1.3	Notification
DM-HLF-009	The DM enabler SHALL provide a mechanism for the discovery of optional DM features supported by the client. **Informational Note:** DM 1.2 already provides an indication of Large Object delivery. Optional features to be indicated are Large Object, Nonce Synchronization, TNDS, Inbox object, User Interaction Commands, asynchronous data via Client initiated Alert, Generic Alert, Correlator, Client Event Alert.	1.3	General
DM-HLF-010	The DM enabler SHALL specify mandatory TNDS support. **Informational Note:** DM 1.2 already supports optional support for TNDS.	1.3	Bootstrap
DM-HLF-011	The DM account information SHOULD include highest protocol version supported by the server. **Informational Note**: DM 1.2 account does not provide highest protocol version. The new account information MUST be backward compatible with DM 1.2	Future	General
DM-HLF-012	The DM Enabler SHALL provide a mechanism to obtain the list of locations of all occurrences of an MO within the Device tree, given the MO Identifier.	1.3	General
DM-HLF-013	The DM enabler SHOULD provide a mechanism that allows a DM Client to read bootstrap data larger than 32KB from a smartcard	1.3	Bootstrap
DM-HLF-014	The DM enabler notification SHOULD indicate which transport binding and authentication type are required by the DM Server in the succedent DM session.	1.3	General
DM-HLF-015	The DM enabler notification SHOULD indicate if some specific information in the DevDetail is desired by the DM server.	1.3	General
DM-HLF-016	The DM enabler SHALL specify HTTP Push notification method. **Informational Note:** DM 1.2 already supports the WAP PUSH method.	1.3	Notification
DM-HLF-017	The DM Client SHALL support multiple Management Authorities	1.3	Management Authority
DM-HLF-018	The DM Client SHALL support multiple Management Authorities managing different instances of the same Management Object.	1.3	Management Authority
DM-HLF-019	The DM Client SHALL support the delegation of a Management Authority's control to other Management Authorities.	1.3	Management Authority
DM-HLF-020	The DM Enabler SHALL support a mechanism to prioritize Management Authorities that access the same instance of a management object.	1.3	Management Authority
DM-HLF-021	The DM Enabler SHALL support Partial Delegation.	1.3	Management Authority
DM-HLF-022	The DM Enabler SHALL support Full Delegation.	1.3	Management Authority
DM-HLF-023	The DM Enabler SHALL support Temporary Delegation.	1.3	Management Authority

DM-HLF-024	The DM enabler SHALL provide a mechanism for a Device to discover the URL of the DM Bootstrap Server.	1.3	Bootstrap
DM-HLF-025	The DM enabler SHALL provide a mechanism for the DM Server to allow automatic discovery of the URL of the DM Bootstrap Server.	1.3	Bootstrap
DM-HLF-026	The DM enabler SHALL provide a mechanism for the DM Server to inhibit automatic discovery of the URL of the DM Bootstrap Server.	1.3	Bootstrap
DM-HLF-027	The DM enabler SHALL provide a mechanism for delivery of the DM Bootstrap Server URL to a Device over OMA Push.	1.3	Bootstrap
DM-HLF-028	The DM enabler SHALL provide a mechanism for the DM Server to allow delivery of the DM Bootstrap Server URL to a Device over OMA Push.	1.3	Bootstrap
DM-HLF-029	The DM enabler SHALL provide a mechanism for the DM Server to inhibit delivery of the DM Bootstrap Server URL to a Device over OMA Push.	1.3	Bootstrap
DM-HLF-030	The DM enabler SHALL define a Management Object for the DM Server to manage the URLs of the DM Bootstrap Servers for a Device.	1.3	Bootstrap
DM-HLF-031	The DM enabler SHALL provide a mechanism for devices that support a smartcard to retrieve the Bootstrap Server URL from the smartcard.	1.3	Bootstrap

Table 1: High-Level Functional Requirements

6.2.1 Security

Label	Description	Release	Functional module
DM-SEC-001	The DM enabler Network Initiated Bootstrapping SHOULD also support a NETWORKID based on a shared secret between device and network provider. **Informational Note:** DM 1.2 suggests IMSI/ESN as shared secret NETWORKID which is a vulnerability, but needs to be kept for backwards compatibility.	1.3	Bootstrap
DM-SEC-002	The mechanism for delivery of the DM Bootstrap Server URL to a Device over OMA Push SHALL be secure.	1.3	Bootstrap

Table 2: High-Level Functional Requirements – Security Items

6.2.1.1 Authentication

N/A

6.2.1.2 Authorization

N/A

6.2.1.3 Data Integrity

N/A

6.2.1.4 Confidentiality

N/A

6.2.2 Charging

N/A

6.2.3 Administration and Configuration

Label	Description	Release	Functional module
DM-ADM-001	The Management Authority SHALL be able to specify that the DM Client connect to the DM Server upon successful processing a DM Profile bootstrap message	1.3	Bootstrap
DM-ADM-002	The DM Client SHOULD be able to securely retrieve a bootstrap message from an URL	1.3	Bootstrap

Table 3: High-Level Functional Requirements – Administration and Configuration Items

6.2.4 Usability

N/A

6.2.5 Interoperability

N/A

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
OMA-RD-DM-V1_3-20160524-A	24 May 2016	Status changed to Approved by TP TP Ref # OMA-TP-2016-0041R01-INP_DM_V1_3_ERP_for_final_Approval

Appendix B. Use Cases (Informative)

B.1 Bootstrap retrieval via URL

B.1.1 Short Description

A DM client will download, authenticate and process a bootstrap message from a URL. This downloaded bootstrap message would be processed just like a normal bootstrap message. The DM client would decide when to download the bootstrap message, and would be allowed to check to see if the bootstrap message had changed from the last download before processing it.

B.1.2 Market benefits

Device can directly retrieve a bootstrap message from a server without having to wait for the server to discover the device.

Devices can retrieve the bootstrap on networks without notification.

B.2 Reason for session

B.2.1 Short Description

A Network Operator changes its platform configuration for its browsing service and initiates a campaign to update the browser settings on devices already in the field. The Device Management Server sends the DM Notification via SMS to the users' devices. The DM Notification is the trigger to perform a DM session but local market policies oblige the Network Operator to provide the user with a legal disclaimer concerning benefits and risks of such session before performing it. For this reason, an informative text is associated to the DM Notification. The DM Client in the users' device receives the DM Notification and displays the informative text in a popup informing, for example, that Network Operators' DM System requests a new session in order to update the browser settings. This text also indicates that if user decides to refuse the connection, he/she won't be able to use the browser, and that Network Operators' DM System is not responsible for any damage suffered by device in consequence of the DM session. Finally, the user confirmation is requested for starting or refusing the connection with the DM Server. If the user accepts, the client initiates the DM session and he/she can use the browser with the new settings.

B.2.2 Market benefits

The Network Operator can inform the user about the reason and legal notice of the request for a DM session using the DM Notification, avoiding the need, for example, of a text SMS sent previously and separately and increasing the users' acceptance for remote configurations.

The user can be informed about the reasons why the DM Session is needed avoiding unnecessary impact on the services he/she consumes regularly (e.g. browser).

B.3 Search for MO instances by MO Identifier

B.3.1 Short Description

A Device may support several kinds of MOs. These MOs may exist during factory bootstrap or may be dynamically created by the DM Server. The DM Server needs to know the location of the MO or its properties since it is Device dependent. Currently structural queries on the management tree to obtain DDF files are used to identify the location of a MO. However DDF files may be static, not provided or out-of-date which cause structural queries insufficient for this purpose. When multiple DM Servers exist, this functionality would also need a convenient way to find MO instances or their properties.

B.3.2 Market Benefits

Adding the ability to dynamically retrieve the location of a specific MO in the tree will simplify the design and implementation of application within the DM Server – instead of hard-coding the location of the MO per specific devices (by make, model, version, etc.), the application only needs to know the MO ID.