Device Capability Management Object Requirements

Candidate Version 1.0 – 29 May 2007

Open Mobile Alliance

OMA-RD-DCMO-V1_0-20070529-C

Contents

Tables

1. Scope (Informative)

A number of Device Management specifications have been defined within OMA. These specifications, referred to as OMA DM v1.2 specifications, define protocol and mechanism to be used between a Device Management Server and a mobile device, data model made available for remote manipulation of a mobile device, security and policy to control the access to a particular resource in the mobile device.

This document defines the requirements for Device Capability Management functionality, which is based on OMA DM v1.2 specifications and makes use of the functionalities provided by OMA DM protocol **Error! Reference source not found.** to define special functionalities to manage device capabilities in the client device.

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

[DMPRO] "OMA Device Management Protocol", Version 1.2, Open Mobile Alliance, OMA-TS-DM_Protocol-V1_2, 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 Capability	Physical characteristics and related parameters supported by a device.
Device Management	Management of the Device configuration and other managed objects of Devices from the point of view of the various Management Authorities. Device Management includes: - Setting initial configuration information in Devices - Subsequent updates of persistent information in Devices - Retrieval of management information from Devices - Processing events and alarms generated by Devices
Device Management System	A background system capable to interact with a (set of) Device(s) for the purpose of Device Management.
Enterprise	A business with deployment and Management Authority for WLAN Bearers, Local Wired Bearers, computers, Devices, software, and employees.
Management Authority	An entity that has the right to perform a specific Device Management function on a Device or manipulate a given data element or parameter. For example, the Network Operator, handset manufacturer, enterprise, or Device owner may be the authority or share authority for managing the Device. One Management Authority may own all Device resources or may share or delegate all or parts of these with/to other Management Authorities
Enterprise Management Authority	An enterprise entity that has the right to perform a specific Device Management function on a Device or manipulate a given data element or parameter.
Enterprise Device Management Server	Part of the Device Management System that is under administration of an Enterprise Management Authority.
DCMO Operations	Operations (e.g. enable, disable) which may be invoked on a Device Capability MO.

3.3 Abbreviations

OMA	Open Mobile Alliance
DCMO	Device Capability Management Object
DM	Device Management

4. Introduction (Informative)

Mobile devices are becoming more and more advanced with many features, such as Cameras, Bluetooth, USB, Keyboard and more. In many circumstances, Enterprises, regulations and others have policies against the usage of some features but allow the use of other features available on mobile devices. Device Capability Management aims to specify the mechanisms required for the remote management of device capabilities. In particular, Device Capability Management will address the ability of remote enablement and disablement of device capabilities.

The objective of this document is to develop a standardized approach to Device Capability Management and its requirements.

5. Use Cases (Informative)

The following basic device capability management use case categories can be considered:

1. Device capability disabled/enabled
2. Expose removable hardware capability

5.1 Device Capability Disabled/Enabled Use Case

5.1.1 Short Description

In order to protect the enterprise secret information, the Enterprise sets policy to limit the use of some capabilities on the employee's device during work time, e.g., the Bluetooth, IR, USB, cameras are forbidden in the office.

When the employee enters the R&D centre, the Enterprise Management Authority detects the presence of the device and sends via Device Management System a command to disable the Camera capability on the employee's device with an indication that user is not allowed to enable it manually namely 'keep-disabled'. Only Device Management System can enable the Camera capability on employee's device when the employee goes out of the R&D centre or the Enterprise Management Authority requests the Device Management System to do so.

5.1.2 Actors

- **Device Management System**
- **Enterprise Management Authority**
- **User: the employee of the Enterprise**

5.1.2.1 Actor Specific Issues

- **Enterprise Management Authority**: Enterprise wants to limit the use of some capabilities on the employee's device automatically.
- **Device Management System:** Device Management System performs the required device management operations.
- **User:** User can not take adventure to offend the enterprise security policy.

5.1.2.2 Actor Specific Benefits

- **Enterprise Management Authority:** Enterprise can manage the use of the device capabilities to protect the security of the enterprise's information.
- **User:** User can easily follow the security rule of the enterprise.

5.1.3 Pre-conditions

- Enterprise Management Authority can detect the presence of the device when the employee has gone into or out of the R&D centre.
- Device is capable of interfacing with the Device Management System.
- The device capability can be enabled and keep-disabled.

5.1.4 Post-conditions

The device capability is enabled or keep-disabled by the Device Management System.

5.1.5 Normal Flow

1. The user tries to enter the R&D center to have a meeting inside and the Enterprise Management Authority detects the presence of the device and sends via Device Management System command to the device to make a specific device capability disabled with the indication that user is not allowed to enable it manually.
2. The device consumes the operations and makes the corresponding capability keep-disabled.
3. The device reports the results to the Device Management System, and the Enterprise Management Authority is notified of the results.
4. After the meeting is finished and the user walks out the R&D center, the Enterprise Management Authority detects this and sends via Device Management System command to the device to enable the capability.
5. The device enables the capability.
6. The device reports the results to the Device Management System, and the Enterprise Management Authority is notified of the results.

5.1.6 Alternative Flow 1

Management Authority detects that a specific capability on the device is abnormal or misbehaving, e.g. by remote diagnostics and monitoring. To protect the user from the effects of a misbehaving device capability (e.g. causing additional charges, degraded performance), Management Authority sends commands via Device Management System to disable that specific capability with an indication that user is allowed to enable it manually namely 'temp-disabled'. If user confirms, the device capability is disabled. When the device capability is recovered to normal state, Management Authority can enable the device capability. Alternatively, user can enable the device capability manually.

The alternative flow illustrates the temp-disable scenario:

1. Management Authority sends via Device Management System command to the device to temporarily disable a specific capability with an indication that user is allowed to enable it manually.
2. The device issues a prompt to the User to confirm this operation.
3. Upon confirmation by the User, the device disables the capability temporarily.
4. The device reports the results to the Device Management System. And Management Authority is notified of the results.

5.1.7 Alternative Flow 2

This alternate flow describes the possibility that the user can enable the capability directly when the device capability is temporarily disabled:

Flow 1~4 are the same as described in alternative flow 1.

5. The user enables a capability on the device.
6. The device enables the capability.
7. The device reports the results to the Device Management System.

5.2 Expose Removable Hardware Capability

5.2.1 Short Description

Several types of removable hardware capabilities may be attached to the device: e.g. camera, keyboard, removable storage.

When a removable hardware is inserted or removed from the device, the device can be aware of this and update the device capability information on the management tree. Then the device capability can be exposed and reported to Management Authority. Management Authority can manage the device capability later.

5.2.2 Actors

- **Management Authority**
- **Device**
- **User**

5.2.2.1 Actor Specific Issues

- **Management Authority:** Management Authority wants to know the short lived capability on the device.
- **Device:** Removable hardware capability on the device needs be exposed to Management Authority.
- **User:** User wants that the removable hardware on his device can be managed by Management Authority.

5.2.2.2 Actor Specific Benefits

- **Management Authority:** Management Authority can know the short lived capability on the device.
- **Device:** Removable hardware capability on the device can be exposed to Management Authority.
- **User:** User can be freed from device capability management.

5.2.3 Pre-conditions

- The device is capable of interfacing with Management Authority.
- The insertion and removal of the removable device capability can be detected by the device.

5.2.4 Post-conditions

The removable hardware capability information can be exposed and reported.

5.2.5 Normal Flow

1. User inserts the removable hardware to the device.
2. The device automatically detects the status of the removable hardware capability and updates the related information on the management tree.

3. The device reports the updated hardware capability information in the case Management Authority has configured a request for notification.

5.2.6 Alternative Flow 1

In the step 1, user removes the removable hardware from the device.

5.2.7 Alternative Flow 2

In the step 2, Management Authority issues command to refresh the device capability information on the device.

6. Requirements (Normative)

6.1 High-Level Functional Requirements

Label	Description	Enabler Release
DCMO-HLFR-1	The DCMO enabler SHALL support a mechanism to enable the device capabilities.	DCMO 1.0
DCMO-HLFR-2	The DCMO enabler SHALL support a mechanism to disable the device capabilities.	DCMO 1.0
DCMO-HLFR-3	The DCMO enabler SHOULD support a mechanism for the Management Authority to specify whether the end-user is informed of DCMO operations performed in the Client.	DCMO 1.0
DCMO-HLFR-4	The DCMO enabler SHALL support a mechanism to indicate whether the user should be allowed to enable or disable specific device capabilities.	DCMO 1.0
DCMO-HLFR-5	The DCMO enabler SHALL support a mechanism to expose the removable device capabilities.	DCMO 1.0
DCMO-HLFR-6	The DCMO enabler SHALL support a mechanism to notify the result of DCMO operations.	DCMO 1.0
DCMO-HLFR-6	The DCMO enabler SHALL support a mechanism for the client initiated DCMO operation.	DCMO 1.0

Table 1: High-Level Functional Requirements

6.1.1 Security

Label	Description	Enabler Release
DCMO-SEC-1	The DCMO enabler SHALL reuse the security mechanism defined in DM v1.2 **Error! Reference source not found.** or later release.	DCMO 1.0

Table 2: High-Level Functional Requirements – Security Items

6.1.2 Charging

N/A

6.1.3 Administration and Configuration

N/A

6.1.4 Usability

Label	Description	Enabler Release
DCMO-USA-001	The DCMO enabler SHALL support execution of DCMO operations on the device without user notification or permission.	DCMO 1.0
DCMO-USA-002	The DCMO enabler SHALL support a mechanism that request user confirmation before DCMO operations are conducted on the device	DCMO 1.0
DCMO-USA-003	The Client MAY support re-enable the disabled device capabilities with the permission of Management Authority.	DCMO 1.0
DCMO-USA-004	The Client SHOULD support a mechanism to inform the end-user about DCMO operations performed in the Client.	DCMO 1.0

Table 3: High-Level Functional Requirements – Usability Items

6.1.5 Interoperability

N/A

6.1.6 Privacy

N/A

6.2 Overall System Requirements

6.2.1 Device Management System

Label	Description	Enabler Release
DCMO-OSR-DMS -01	The Device Management System SHALL be able to refresh the device capability information.	DCMO 1.0

Table 4: DMS Requirements

6.2.2 Device

Label	Description	Enabler Release
DCMO-OSR-Device -01	The Device SHALL be able to detect the insertion or removal of removable hardware and update the related information on the management tree.	DCMO 1.0
DCMO-OSR-Device -02	The Device SHOULD support the mechanism of HLFR-4 for each device capability.	DCMO 1.0

Table 5: Device Requirements

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
n/a	n/a	No prior version –or- No previous version within OMA

A.2 Draft/Candidate Version 1.0 History

Document Identifier	Date	Sections	Description
Draft Versions OMA-RD-DCMO-V1_0-20060821-D	21 Aug 2006	new draft document	Incorporates input to committee: OMA-DM-DCMO-2006-0001R03-INP_Use_Case_and_Requirements
Draft Versions OMA-RD-DCMO-V1_0-20061004-D	04 Oct 2006	Section 5, 6	Incorporates CR: OMA-DM-DCMO-2006-0002R03-CR_Enable_Disable_Alternative_Flow.doc
Draft Versions OMA-RD-DCMO-V1_0-20061028-D	28 Oct 2006	Section 6	Incorporates CR: OMA-DM-DCMO-2006-0003R01-CR_Usability_Requirements_revision.doc
Draft Versions OMA-RD-DCMO-V1_0-20061121-D	21 Nov 2006	Section 1,4,5,6	Incorporates CR: OMA-DM-DCMO-2006-0005R01-CR_Expose_Removable_Hardware_Capability_Use_Case.doc OMA-DM-DCMO-2006-0008-CR_Scope_Introduction_Update.doc OMA-DM-DCMO-2006-0009R01-CR_Additional_Requirements.doc
Draft Versions OMA-RD-DCMO-V1_0-20070119-D	19 Jan 2006	Section 3.2	Incorporates CR: OMA-DM-DCMO-2006-0011R02-CR_Device_Capability_Definition.doc
Draft Versions OMA-RD-DCMO-V1_0-20070207-D	07 Feb 2007	All	Incorporates CR: OMA-DM-DCMO-2007-0002R01-CR_RD_Closure_Resolution.doc OMA-DM-DCMO-2006-0010R02-CR_Overall_System_Requirements.doc OMA-DM-DCMO-2006-0007R03-CR_Reference_Definition_Abbreviation_Update.doc
	18 Apr 2007	Section 5.1, 6	Incorporates CR: OMA-DM-DCMO-2007-0006-CR_RDRR_Resolutions_UC_HLR OMA-DM-DCMO-2007-0007-CR_Client_Initiated_DCMO
Candidate Versions OMA-RD-DCMO-V1_0	29 May 2007	n/a	Converted to Candidate following TP Approval TP Approval as OMA-TP-2007-0195R01