Software Component Management Object Requirements

Candidate Version 1.0 – 18 Sep 2007

Open Mobile Alliance

OMA-RD-SCOMO-V1_0-20070918-C

Contents

Tables

1. Scope (Informative)

This document defines the requirements for Software Component Management functionality, which leverage OMA DM enabler and makes use of the functionalities provided by OMA DM protocol [DMPRO] to define special capabilities to manage software components 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/

[OMADICT] "Dictionary for OMA Specifications", Version 2.5, Open Mobile Alliance™, OMA-ORG-Dictionary-V2.5, 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	In this context, a Device is a voice and/or data terminal that uses a Wireless Bearer for data transfer. Device types may include (but are not limited to): mobile phones (GSM, CDMA, 3GSM, etc.), data-only terminals, PDAs, laptop computers, PCMCIA cards for data communication, unattended data-only Devices (e.g., vending machines), and smart cards if associated with these Devices. If within a particular context an associated smart card should not be regarded as part of a Device this is marked explicitly.
Device Reporting	The process that a Device sends specific information to a Device Management System in the network. This can occur as a response to a query (pull) or it can occur autonomously in response to a state change in the Device (push). The information that is sent may either be parameters, configuration capabilities of the Device, or data that has been collected, stored, and assembled for later processing (e.g., performance metrics).
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
Network Operator	An entity that is licensed and allocated frequency to operate a public mobile wireless telecommunications network for the purpose of providing publicly available commercial services.
Service Provider	An entity that provides and administers a service to a Subscriber and/or User. The Network Operator is often a Service Provider.
Subscriber	A Subscriber is an entity (e.g. a user) that is engaged in a Subscription with a service provider. [OMADICT]
Software Component Management Object	A management tree object defined for software components which will be used for delivering and managing software components within client device.
Software Component Activation	The process which results in services or resources a software component embodies to be made accessible to other entities or resources (including the end-user).
Software Component Deactivation	The process which results in services or resources a software component embodies to be made inaccessible to other entities or resources (including the end-user). .
SCOMO Operations	Download, Install, Update, Remove, Activate and Deactivate operations which may be invoked on a Software Component MO as well as inventory queries.
User	An entity which uses services. Example: a person using a device as a portable telephone.[OMADICT]

3.3 Abbreviations

SCOMO	Software Component Management Object
DM	Device Management
OMA	Open Mobile Alliance
MO	Management Object

4. Introduction (Informative)

Software Component Management aims to enable remote operations, such as install, update or remove for software components in the Device.

The objective of this document is to develop a standardized solution for managing Software Components and its requirements. Whereas the idea of Firmware Update is to manage the firmware of the device, the Software Component Management Object is meant to manage any other type of software asset than firmware. Examples of software components are applications, executables, libraries, UI-elements, certificates, licenses etc.

5. Use Cases (Informative)

5.1 Software Component Installation

5.1.1 Short Description

Arnold is a device User and very interested in the latest mobile applications.

He is subscribed to "Fun Applications Co." and this service provider installs always the newest applications on his phone as soon as they are available.

5.1.2 Actors

- **End User**
- **Device**
- **Service Provider** (Fun Applications Co. in this example)
- **Device Management System**

5.1.2.1 Actor Specific Issues

- **End User:** The End User wants to have the newest applications on his device.
- **Service Provider:** The Service Provider assigns what application software should be installed by default on a specific Device type. The provider is authorised to define and change the default software on a Device type.
- **Device ManagementSystem:** The Device Management System issues and handles the commands in the service. Note that the Device Management System can reside under different authorities, such as service provider itself or network operator, depending on the infrastructure.

5.1.2.2 Actor Specific Benefits

- **End User:** End User is able to use the latest version of services.
- **Device:** Device receives the latest software component/s.
- **Service Provider:** The Service Provider is able to deliver the software components into the Device.
- **Device ManagementSystem:** The Device Management System is able to manage the application in the Device.

5.1.3 Pre-conditions

- Device is capable of interfacing with the Device Management System.
- Security constraints imposed by Device Management System and the Device are met.

5.1.4 Post-conditions

- The software component targeted at the device has been delivered and installed.

5.1.5 Normal Flow

1. The Service Provider sends via Device Management System a command to the Device to install a software component.
2. The Device issues a request to the User for authorization to install upgrades.
3. Upon confirmation by the User, the Device sends the response to the Device Management System.
4. The Device Management System initiates the software component download, install, and execution.
5. The Device sends a confirmation back to the Device Management System.

5.1.6 Alternative Flow

The device initiates a session with the Device Management System to request software component installation.

The device informs the user of the SW characteristics before download and installation.(price, providers, compatibility, QoS, characteristics...)

The device Management system may interact with an external management authority in order to coordinate the procedures with other software components.

5.2 Software Component Update

5.2.1 Short Description

Bernard is a device User and very interested in keeping his phone free of viruses.

He is subscribed to "Mobile Security Forces Co." and this service provider installs always the latest antivirus software upgrades on his phone as soon as they are available. This way Bernard has better protection against malicious mobile device viruses.

5.2.2 Actors

- **End User**
- **Device**
- **Service Provider** (Mobile Security Forces Co. in this example)
- **Device Management System**

5.2.2.1 Actor Specific Issues

- **End User:** The End User wants to have the newest release of antivirus software.
- **Service Provider:** The Service Provider assigns what software component should be installed by default on a specific Device type. The provider is authorised to define and change the default software on a Device type.
- **Device Management System:** The Device Management System issues and handles the commands in the service.

5.2.2.2 Actor Specific Benefits

- **End User:** End User has good protection against malicious mobile device viruses.
- **Service Provider:** The Service Provider is able to deliver the software component updates into the Device.
- **Device Management System:** The Device Management System is able to manage the software component in the Device.

5.2.3 Pre-conditions

- Installed software component on a Device is to have added functionality applied or is to be enhanced for security or performance reasons.
- Device is capable of interfacing with the Device Management system.
- Security constraints imposed by Device Management System and any DM Client are met.

5.2.4 Post-conditions

- All software component updates targeted at the device have been delivered and installed.
- Device and all purchased services are fully operational.

5.2.5 Normal Flow

1. The Device Management System issues a request to the Device to install software component updates.
2. The Device issues a request to the User for authorization to install updates.
3. Upon confirmation by the User, the Device sends the response to the Device Management System.
4. The Device Management System initiates software component download and update..
5. The Device sends a confirmation back to the Device Management System.

5.2.6 Alternative Flow 1

1. The device initiates a session with the Device Management System to request software component update.

2. The Device Management System has detailed information of the software component available in the device, e.g. whether each software component has been installed/removed, what version the software component is, whether updates should be done promptly or later on.

3. The Device Management System will selectively issue a request to the Device that has outdated software component version.

5.2.7 Alternative Flow II

1. In the Normal Flow above it turns out that component of antivirus software (that are about to be updated) requires an update of another component (e.g. a special version of Application X).
2. The Device Management System signals to the device that these components must either be both successfully installed or none of them should.
3. The Device respects the signal and treats both updates as if they were one. Unless update of both components succeeds – the operation is canceled and an error status is sent back to the server, indicating the problem.

5.3 Software Component Removal

5.3.1 Short Description

Arnold is a device User and subscribes to "Fun Applications Co." applications bundle. This service provider removes software components from his phone when his subscription plan expires.

5.3.2 Actors

- **End User**
- **Device**
- **Service Provider** (Fun Applications Co. in this example)
- **Device Management System**

5.3.2.1 Actor Specific Issues

- **End User:** The End User wants to have applications installed on his device in accordance with the subscription plan..
- **Service Provider:** The Service Provider wants to ensure only subscribed applications are installed on the device.
- **Device ManagementSystem:** The Device Management System issues and handles the commands in the service. Note that the Device Management System can reside under different authorities, such as service provider itself or network operator.

5.3.2.2 Actor Specific Benefits

- **End User:** End User gets unsubscribed applications removed from the device.
- **Device:** Unnecessary applications are removed from the device.

- **Service Provider:** The Service Provider is able to manage the applications on the device.
- **Device Management System:** The Device Management System is able to manage the application in the Device.

5.3.3 Pre-conditions

- Device is capable of interfacing with the Device Management System.
- Security constraints imposed by Device Management System and the Device are met.
- The software component to be removed is installed on the device.

5.3.4 Post-conditions

- The software component has been successfully removed.

5.3.5 Normal Flow

1. The Service Provider sends via Device Management System command(s) to the Device to remove a software component.
2. The Device notifies the User about pending software component removal. [A1][A2]
3. The Device removes the software component. if the software component is active, the Device deactivates it internally
4. The Device sends a confirmation back to the Device Management System
5. The Service Provider is notified of the software component removal

5.3.6 Alternative Flow 1 (A1)

User does not want the action to be performed. The use case ends

5.3.7 Alternative Flow 2 (A2)

Service Provider does not want User permission. Proceed to step 3 of normal flow.

5.4 Inventory Check

5.4.1 Short Description

Bernard is a User who has subscribed to Game Co Inc. software bundle. Game Co Inc. wants to periodically check the software inventory on the device in order to ensure the appropriate versions of required software components are installed on the device.

5.4.2 Actors

- **End User**
- **Device**
- **Service Provider**
- **Device Management System**

5.4.2.1 Actor Specific Issues

- **Service Provider:** The Service Provider wants to ensure (i) required software components are installed on the device, and (ii) deployed software components are at the appropriate version.
- **Device Management System:** The Device Management System issues and handles the commands in the service.

5.4.2.2 Actor Specific Benefits

- **End User:** End User would be able to access latest features/ services that are dependent on the software components
- **Device:** Device receives the latest software components
- **Service Provider:** (i) Operational complexity is reduced by ensuring software components on the managed devices are at the appropriate version (ii) New software components which are not on the device can be downloaded.
- **Device Management System:** The Device Management System is able to manage the application in the Device.

5.4.3 Pre-conditions

- Device is capable of interfacing with the Device Management System.
- Security constraints imposed by Device Management System and any DM Client are met.

5.4.4 Post-conditions

- The Management Authority (Service Provider) obtains the desired list of software components available on the device.

5.4.5 Normal Flow

1. The Service Provider sends via Device Management System command(s) to the Device to perform remote inventory check.
2. The Device sends the requested inventory of software components and related information to the Service Provider via the Device Management System

5.5 Activate/ Deactivate a Software Component

5.5.1 Short Description

Service Provider wants to activate or deactivate a software component.

5.5.2 Actors

- **End User**
- **Device**
- **Service Provider**
- **Device Management System**

5.5.2.1 Actor Specific Issues

- **Service Provider:** The Service Provider wants to activate/ deactivate an application.
- **Device Management System:** The Device Management System issues and handles the commands in the service.

5.5.2.2 Actor Specific Benefits

- **Service Provider:** The Service Provider can OTA activate/ deactivate an installed software component.
- **Device Management System:** The Device Management System is able to manage the software component in the Device.

5.5.3 Pre-conditions

- Device is capable of interfacing with the Device Management system.
- Security constraints imposed by Device Management System and any DM Client are met.

5.5.4 Post-conditions

- Software component is in desired state.

5.5.5 Normal Flow

1. The Service Provider sends via Device Management System command(s) to the Device to activate or deactivate the software component.
2. The Device issues a request to the User for authorization for the necessary action [A1] [A2]

3. Upon confirmation by the User, the Device sends the response to the Device Management System
4. The Device Management System performs the necessary action
5. The Device sends a confirmation back to the Device Management System

5.5.6 Alternative Flow 1 (A1)

User does not want the action to be performed

5.5.7 Alternative Flow 2 (A2)

Service Provider does not want User permission. Proceed to step 4 of normal flow.

6. Requirements (Normative)

6.1 High-Level Functional Requirements

Label	Description	Enabler Release
SCOMO-HLFR-1	The SCOMO enabler SHALL support the download of software components to the device.	SCOMO 1.0
SCOMO-HLFR-2	The SCOMO enabler SHALL support the installation of software components on the Device	SCOMO 1.0
SCOMO-HLFR-3	The SCOMO enabler SHALL support the update of software components on the device.	SCOMO 1.0
SCOMO-HLFR-4	The SCOMO enabler SHALL support the activate/deactivate of software components on the device	SCOMO 1.0
SCOMO-HLFR-5	The SCOMO enabler SHALL support the removal of software components from the device	SCOMO 1.0
SCOMO-HLFR-6	The SCOMO enabler SHALL support the inventory of software components on the device	SCOMO 1.0
SCOMO-HLFR-7	The SCOMO enabler SHALL provide a mechanism that allows the Device to indicate the result of SCOMO Operations.	SCOMO 1.0
SCOMO-HLFR-8	The SCOMO enabler SHALL support a mechanism to bind related Software Components so that they can be installed using a single operation. A failure of such operation SHALL leave the related Software Components in their original state.	SCOMO 1.0

Table 1: High-Level Functional Requirements

6.1.1 Security

Label	Description	Enabler Release
SCOMO-SEC-1	Only authenticated Device Management System SHALL be able to perform SCOMO operations on the device.	SCOMO 1.0
SCOMO-SEC-2	Only authorized Device Management System SHALL be able to perform SCOMO operations on the device.	SCOMO 1.0
SCOMO-SEC-3	The SCOMO 1.0 enabler SHALL support confidentiality for software component delivery to the Device.	SCOMO 1.0
SCOMO-SEC-4	The SCOMO 1.0 enabler SHALL support integrity for software component delivery to the Device.	SCOMO 1.0

Table 2: High-Level Functional Requirements – Security Items

6.1.2 Charging

Label	Description	Enabler Release
N/A	N/A	N/A

Table 3: High-Level Functional Requirements – Charging Items

6.1.3 Administration and Configuration

Label	Description	Enabler Release
N/A	N/A	N/A

Table 4: High-Level Functional Requirements – Administration and Configuration Items

6.1.4 Usability

Label	Description	Enabler Release
SCOMO-USA-1	The user SHOULD be asked for confirmation to proceed before SCOMO Operations are conducted on the device.	SCOMO 1.0
SCOMO-USA-2	The user SCOMO enabler SHOULD support a mechanism to be inform the user that the software component installation or update has been completed.	SCOMO 1.0
SCOMO-USA-3	The SCOMO enabler SHALL support a mechanism that requests user confirmation before SCOMO operations are conducted on the device.	SCOMO 1.0
SCOMO-USA-4	The SCOMO enabler SHALL support a mechanism to inform the user about SCOMO operations and any other relevant information.	SCOMO 1.0
SCOMO-USA-5	The SCOMO enabler SHALL support execution of SCOMO Operations on the device with or without user notification or permission.	SCOMO 1.0

Table 5: High-Level Functional Requirements – Usability Items

6.1.5 Interoperability

Label	Description	Enabler Release
SCOMO-IOP-01	The Device SHALL support download of software components using OMA DM and/or at least one Alternate Download protocol.	SCOMO 1.0
SCOMO-IOP-02	The Device Management System SHALL support download of software components using OMA DM and/or at least one Alternate Download protocol.	SCOMO 1.0

Table 6: High-Level Functional Requirements – Interoperability Items

6.1.6 Privacy

Label	Description	Enabler Release
N/A	N/A	N/A

Table 7: High-Level Functional Requirements – Privacy Items

6.2 Overall System Requirements

Label	Description	Enabler Release
SCOMO-OSR-01	When specifying features which rely on OMA DM, the SCOMO 1.0 enabler	SCOMO 1.0

	SHALL reference Enabler Release version 1.2.	
SCOMO-OSR-02	The SCOMO enabler SHALL support vendor extensions.	SCOMO 1.0

Table 8: High-Level System Requirements

6.2.1 Device Management System

Label	Description	Enabler Release
SCOMO-DMS-01	The Device Management System SHALL be able to install software components on the device	SCOMO 1.0
SCOMO-DMS-02	The Device Management System SHALL be able to update software components on the device	SCOMO 1.0
SCOMO-DMS-03	The Device Management System SHOULD be able to activate/deactivate software components on the device	SCOMO 1.0
SCOMO-DMS-04	The Device Management System SHALL be able to removesoftware components on the device	SCOMO 1.0
SCOMO-DMS-05	The Device Management System SHALL be able to query the inventory of software components on the device	SCOMO 1.0
SCOMO-DMS-06	The Device Management System SHALL be able to receive notifications about result of SCOMO operations from the Device	SCOMO 1.0
SCOMO-DMS-07	The Device Management System SHALL support the mechanism of HLFR-8	SCOMO 1.0

Table 9: DMS Requirements

6.2.2 Device

Label	Description	Enabler Release
SCOMO-Device - 01	The Device SHALL support installation of software components	SCOMO 1.0
SCOMO-Device - 02	The Device SHOULD support updating of software components	SCOMO 1.0
SCOMO-Device - 03	The Device SHOULD support activation/deactivation of software components	SCOMO 1.0
SCOMO-Device - 04	The Device SHALL support removal of software components	SCOMO 1.0
SCOMO-Device - 05	The Device SHALL be able to provide software component inventory information to a Device Management System	SCOMO 1.0
SCOMO-Device - 06	The Device SHALL be able to send notifications about result of SCOMO operations to the Device Management System	SCOMO 1.0
SCOMO-Device - 07	The Device MAY be able to initiate a session for SCOMO operations	SCOMO 1.0
SCOMO-Device- 08	The Device Management System SHALL support the mechanism of HLFR-8	SCOMO 1.0

Table 10: Device Requirements

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 1.0 History

Document Identifier	Date	Sections	Description
Draft Version OMA-RD-Software_Component_Management-V1_0_0	14 Aug 2005	All	New RD
Draft Version OMA-RD-Software_Component_Management-V1_0_1	21 Feb 2006		Agreed Dec 2005 & Jan 2006 CRs included
Draft Version OMA-RD-Software_Component_Management-V1_0_0	12 Apr 2006	5, 6	Applied agreed CRs: OMA-DM-SCOMO-2006-0016 OMA-DM-SCOMO-2006-0014R02 OMA-DM-SCOMO-2006-0012R01 OMA-DM-SCOMO-2006-0011R01 OMA-DM-SCOMO-2006-0010R03 OMA-DM-SCOMO-2006-0003R08 Editorial Changes: Removed repetitious text in section 6 Updated A.1 based on RD template guidelines
Draft Version OMA-RD-SCoMO-V1_0	14 Jun 2006	6	Applied agreed CRs: OMA-DM-SCOMO-2006-0017R01 OMA-DM-SCOMO-2006-0021R02
	07 Jul 2006	All	Applied clerical changes recommended during the SCOMO-RD closure review
	02 Aug 2006	3, 6	Applied following CRs which resulted as a result of the SCOMO RD closure review OMA-DM-SCOMO-2006-0027R01 OMA-DM-SCOMO-2006-0028 OMA-DM-SCOMO-2006-0029 OMA-DM-SCOMO-2006-0031R01 OMA-DM-SCOMO-2006-0032 OMA-DM-SCOMO-2006-0033
	03 Aug 2006	6	Incorporated: OMA-DM-SCOMO-2006-0023R01
	18 Aug 2006	6	Addressed comments raised in closure review of Aug 3, 2006 1. Ensure SCOMO CR#23R01 properly applied 2. Ensure next revision of SCOMO RD has "N/A" added to sections with no requirements 3. Ensure all requirements in the SCOMO RD are numbered properly
	20 Sep 2006	6	Incorporated OMA-DM-SCOMO-2006-0038R01
	30 Nov 2006	5, 6	Incorporated: OMA-DM-SCOMO-2006-0051 OMA-DM-SCOMO-2006-0052 OMA-DM-SCOMO-2006-0053R02-

Document Identifier	Date	Sections	Description
	06 Apr 2007	All	Incorporated: OMA-DM-SCOMO-2006-0056 OMA-DM-SCOMO-2006-0057R04 OMA-DM-SCOMO-2006-0058R03 OMA-DM-SCOMO-2006-0061 OMA-DM-SCOMO-2006-0062 OMA-DM-SCOMO-2007-0004R01 OMA-DM-SCOMO-2007-0005 OMA-DM-SCOMO-2007-0006R01 OMA-DM-SCOMO-2007-0007 OMA-DM-SCOMO-2007-0015 OMA-DM-SCOMO-2007-0016 OMA-DM-SCOMO-2007-0017 OMA-DM-SCOMO-2007-0018R01 OMA-DM-SCOMO-2007-0019
Candidate Versions OMA-RD-SCOMO-V1_0	31 Jul 2007	n/a	Status changed to Candidate by TP TP ref #OMA-TP-2007-0277R02- INP_SCOMO_RD_For_Candidate_Approval
	18 Sep 2007	5	Incorporated: OMA-DM-SCOMO-2007-0064