



Software and Application Control Management Object Requirements

Candidate Version 1.0 – 27 Jul 2010

Open Mobile Alliance
OMA-RD-SACMO-V1_0-20100727-C

Use of this document is subject to all of the terms and conditions of the Use Agreement located at <http://www.openmobilealliance.org/UseAgreement.html>.

Unless this document is clearly designated as an approved specification, this document is a work in process, is not an approved Open Mobile Alliance™ specification, and is subject to revision or removal without notice.

You may use this document or any part of the document for internal or educational purposes only, provided you do not modify, edit or take out of context the information in this document in any manner. Information contained in this document may be used, at your sole risk, for any purposes. You may not use this document in any other manner without the prior written permission of the Open Mobile Alliance. The Open Mobile Alliance authorizes you to copy this document, provided that you retain all copyright and other proprietary notices contained in the original materials on any copies of the materials and that you comply strictly with these terms. This copyright permission does not constitute an endorsement of the products or services. The Open Mobile Alliance assumes no responsibility for errors or omissions in this document.

Each Open Mobile Alliance member has agreed to use reasonable endeavours to inform the Open Mobile Alliance in a timely manner of Essential IPR as it becomes aware that the Essential IPR is related to the prepared or published specification. However, the members do not have an obligation to conduct IPR searches. The declared Essential IPR is publicly available to members and non-members of the Open Mobile Alliance and may be found on the "OMA IPR Declarations" list at <http://www.openmobilealliance.org/ipr.html>. The Open Mobile Alliance has not conducted an independent IPR review of this document and the information contained herein, and makes no representations or warranties regarding third party IPR, including without limitation patents, copyrights or trade secret rights. This document may contain inventions for which you must obtain licenses from third parties before making, using or selling the inventions. Defined terms above are set forth in the schedule to the Open Mobile Alliance Application Form.

NO REPRESENTATIONS OR WARRANTIES (WHETHER EXPRESS OR IMPLIED) ARE MADE BY THE OPEN MOBILE ALLIANCE OR ANY OPEN MOBILE ALLIANCE MEMBER OR ITS AFFILIATES REGARDING ANY OF THE IPR'S REPRESENTED ON THE "OMA IPR DECLARATIONS" LIST, INCLUDING, BUT NOT LIMITED TO THE ACCURACY, COMPLETENESS, VALIDITY OR RELEVANCE OF THE INFORMATION OR WHETHER OR NOT SUCH RIGHTS ARE ESSENTIAL OR NON-ESSENTIAL.

THE OPEN MOBILE ALLIANCE IS NOT LIABLE FOR AND HEREBY DISCLAIMS ANY DIRECT, INDIRECT, PUNITIVE, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES ARISING OUT OF OR IN CONNECTION WITH THE USE OF DOCUMENTS AND THE INFORMATION CONTAINED IN THE DOCUMENTS.

© 2010 Open Mobile Alliance Ltd. All Rights Reserved.

Used with the permission of the Open Mobile Alliance Ltd. under the terms set forth above.

Contents

- 1. SCOPE (INFORMATIVE)5
- 2. REFERENCES6
 - 2.1 NORMATIVE REFERENCES6
 - 2.2 INFORMATIVE REFERENCES6
- 3. TERMINOLOGY AND CONVENTIONS7
 - 3.1 CONVENTIONS7
 - 3.2 DEFINITIONS7
 - 3.3 ABBREVIATIONS7
- 4. INTRODUCTION (INFORMATIVE).....8
 - 4.1 VERSION 1.08
- 5. SACMO RELEASE DESCRIPTION (INFORMATIVE).....9
 - 5.1 END-TO-END SERVICE DESCRIPTION9
- 6. REQUIREMENTS (NORMATIVE).....10
 - 6.1 HIGH-LEVEL FUNCTIONAL REQUIREMENTS10
 - 6.1.1 Security10
 - 6.1.2 Charging Events.....11
 - 6.1.3 Administration and Configuration11
 - 6.1.4 Usability.....11
 - 6.1.5 Interoperability.....11
 - 6.1.6 Privacy12
 - 6.2 OVERALL SYSTEM REQUIREMENTS12
 - 6.2.1 Device Management Server.....12
 - 6.2.2 Device12
- APPENDIX A. CHANGE HISTORY (INFORMATIVE).....13
 - A.1 APPROVED VERSION HISTORY13
 - A.2 DRAFT/CANDIDATE VERSION 1.0 HISTORY13
- APPENDIX B. USE CASES (INFORMATIVE)14
 - B.1 APPLICATION PROBLEM RESOLUTION BY CUSTOMER CARE14
 - B.1.1 Short Description14
 - B.1.2 Market benefits14
 - B.2 ENHANCED MAINTENANCE14
 - B.2.1 Short Description14
 - B.2.2 Market benefits15
 - B.3 NEW DEVICE INSTALLATION.....15
 - B.3.1 Short Description15
 - B.3.2 Market benefits15
 - B.4 SIDEBAND DEVICE UPDATE15
 - B.4.1 Short Description15
 - B.4.2 Market Benefits.....15

Figures

No table of figures entries found.

Tables

- Table 1: High-Level Functional Requirements10
- Table 2: High-Level Functional Requirements – Security Items10

| | |
|---|-----------|
| Table 3: High-Level Functional Requirements – Authentication Items | 10 |
| Table 4: High-Level Functional Requirements – Authorization Items..... | 10 |
| Table 5: High-Level Functional Requirements – Data Integrity Items | 11 |
| Table 6: High-Level Functional Requirements – Confidentiality Items | 11 |
| Table 7: High-Level Functional Requirements – Charging Items | 11 |
| Table 8: High-Level Functional Requirements – Administration and Configuration Items | 11 |
| Table 9: High-Level Functional Requirements – Usability Items | 11 |
| Table 10: High-Level Functional Requirements – Interoperability Items..... | 12 |
| Table 11: High-Level Functional Requirements – Privacy Items..... | 12 |
| Table 12: High-Level System Requirements | 12 |
| Table 13: DMS Requirements..... | 12 |
| Table 14: Device Requirements | 12 |

1. Scope

(Informative)

This document defines requirements for the SACMO enabler.

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/>
- [DMRD] “Device Management Requirements”, Version 1.2, Open Mobile Alliance™, OMA-RD-DM-V1_2,
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/>

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 | See [OMADICT] |
| Device Management | See [DMRD] |
| Device Management System | See [DMRD] |
| Network Operator | See [OMADICT] |
| SACMO Operations | Any operation which may be invoked on a MO. |
| User | See [OMADICT] |

3.3 Abbreviations

| | |
|--------------|--|
| CCA | Customer Care Agent |
| DM | Device Management |
| DMS | Device Management Server |
| MO | Management Object |
| OMA | Open Mobile Alliance |
| SACMO | Software and Application Control Management Object |

4. Introduction

(Informative)

To address scenarios such as device initiation, or customer care resolution of application issues, Device Management workflows are sometimes applied today, whereby the DM server requests a DM operation to be executed in the device, the result is reported to the DM server, then logic is applied in the DM server to determine which subsequent DM operation to apply and so on.

This can be inefficient for some workflows, leading to a slow execution time and high network load.

The goal of SACMO is to enable DM operations to be applied according to workflow scripts in the device, whereby any combination of operations on existing Management Objects can be applied and conditionally executed, with just the combined result being reported back to the DM server.

This avoids a series of individual client-server interactions, thereby optimising the network traffic and reducing the workflow execution time.

4.1 Version 1.0

SACMO V1.0 covers:

- Download, installation, update, activation, deactivation & removal of SACMO in the device
- Reporting the results of a SACMO workflow
- User confirmation before execution of SACMO workflow operations

Out of scope is:

- Interface between the DM server and a requester such as the Customer Care Agent

5. SACMO release description (Informative)

The SACMO enabler involves the download of a SACMO workflow to a SACMO agent on the device. The SACMO agent may apply conditional logic to execute any combination of DM MOs to lead to the desired result, e.g. initiation of the device or resolution of a known problem with an application.

5.1 End-to-end Service Description

SACMO is intended to build upon existing DM MOs, to allow known tasks involving sequences of DM operations to be applied in a more efficient way to minimise network communication and allow for faster execution. Minimising network communication addresses the need to efficiently use network resources, whereas fast execution will improve user experience.

6. Requirements (Normative)

6.1 High-Level Functional Requirements

| Label | Description | Release |
|--------------|--|-----------|
| SACMO-HLF-1 | The SACMO enabler SHALL support the download of SACMO(s) to the device. | SACMO 1.0 |
| SACMO-HLF-2 | The SACMO enabler SHALL support the installation of SACMO(s) on the device | SACMO 1.0 |
| SACMO-HLF-3 | The SACMO enabler SHALL support the update of SACMO(s) on the device. | SACMO 1.0 |
| SACMO-HLF-4 | The SACMO enabler SHALL support the activation/deactivation of SACMO(s) on the device. | SACMO 1.0 |
| SACMO-HLF-5 | The SACMO enabler SHALL support the removal of SACMO(s) from the device. | SACMO 1.0 |
| SACMO-HLF-6 | The SACMO enabler SHALL provide a mechanism that allows the Device to indicate the result of SACMO operations to the DMS. | SACMO 1.0 |
| SACMO-HLF-7 | The SACMO enabler SHALL support a mechanism to bind related Management Objects so that they can be processed using a single operation. | SACMO 1.0 |
| SACMO-HLF-8 | A failure of a SACMO operation SHALL leave the related Management Object in its original state. | SACMO 1.0 |
| SACMO-HLF-9 | The SACMO enabler SHALL support the conditional execution of operations on Management Objects. | SACMO 1.0 |
| SACMO-HLF-10 | The SACMO enabler SHALL support the definition of workflows. | SACMO 1.0 |

Table 1: High-Level Functional Requirements

6.1.1 Security

| Label | Description | Release |
|-------|-------------|---------|
| N/A | N/A | N/A |

Table 2: High-Level Functional Requirements – Security Items

6.1.1.1 Authentication

| Label | Description | Release |
|---------------|---|-----------|
| SACMO-ATHEN-1 | Only authenticated DMS SHALL be able to perform SACMO operations on the device. | SACMO 1.0 |

Table 3: High-Level Functional Requirements – Authentication Items

6.1.1.2 Authorization

| Label | Description | Release |
|---------------|--|-----------|
| SACMO-ATHOR-1 | Only authorized DMS SHALL be able to perform SACMO operations on the device. | SACMO 1.0 |

Table 4: High-Level Functional Requirements – Authorization Items

6.1.1.3 Data Integrity

| Label | Description | Release |
|-------|-------------|---------|
| N/A | N/A | N/A |

Table 5: High-Level Functional Requirements – Data Integrity Items

6.1.1.4 Confidentiality

| Label | Description | Release |
|-------|-------------|---------|
| N/A | N/A | N/A |

Table 6: High-Level Functional Requirements – Confidentiality Items

6.1.2 Charging Events

| Label | Description | Release |
|-------|-------------|---------|
| N/A | N/A | N/A |

Table 7: High-Level Functional Requirements – Charging Items

6.1.3 Administration and Configuration

| Label | Description | Release |
|-------|-------------|---------|
| N/A | N/A | N/A |

Table 8: High-Level Functional Requirements – Administration and Configuration Items

6.1.4 Usability

| Label | Description | Release |
|-------------|--|-----------|
| SACMO-USE-1 | The SACMO enabler SHALL support a mechanism to inform the user about SACMO operations and any other related information. | SACMO 1.0 |
| SACMO-USE-2 | The SACMO SHALL be able to indicate specific operations in a workflow which need user confirmation or action, and specific operations in a workflow which do not need user confirmation or action. | SACMO 1.0 |
| SACMO-USE-3 | The SACMO enabler SHALL support a mechanism that requests user confirmation before the indicated operations are conducted on the device. | SACMO 1.0 |
| SACMO-USE-4 | The SACMO enabler SHOULD support a mechanism to inform the user that the SACMO operation has been completed successfully or unsuccessfully. | SACMO 1.0 |

Table 9: High-Level Functional Requirements – Usability Items

6.1.5 Interoperability

| Label | Description | Release |
|-------|-------------|---------|
| N/A | N/A | N/A |

Table 10: High-Level Functional Requirements – Interoperability Items

6.1.6 Privacy

| Label | Description | Release |
|-------|-------------|---------|
| N/A | N/A | N/A |

Table 11: High-Level Functional Requirements – Privacy Items

6.2 Overall System Requirements

| Label | Description | Release |
|--------------|--|-----------|
| SACMO-OSR-01 | The SACMO enabler SHALL rely on features as described in OMA DM v1.2 specifications [DMPRO] or higher. | SACMO 1.0 |
| SACMO-OSR-02 | The SACMO enabler SHALL support implementation specific extensions. | SACMO 1.0 |

Table 12: High-Level System Requirements

6.2.1 Device Management Server

| Label | Description | Release |
|--------------|--|-----------|
| SACMO-DMS-01 | The DMS SHALL support download of SACMO(s) using OMA DM and/or at least one Alternate Download protocol. | SACMO 1.0 |
| SACMO-DMS-02 | The DMS SHALL be able to install SACMO(s) on the device. | SACMO 1.0 |
| SACMO-DMS-03 | The DMS SHALL be able to update SACMO(s) on the device. | SACMO 1.0 |
| SACMO-DMS-04 | The DMS SHALL be able to activate/deactivate SACMO(s) on the device. | SACMO 1.0 |
| SACMO-DMS-05 | The DMS SHALL be able to remove SACMO(s) from the device. | SACMO 1.0 |
| SACMO-DMS-06 | The DMS SHALL be able to query the inventory of SACMO(s) on the device. | SACMO 1.0 |
| SACMO-DMS-07 | The DMS SHALL be able to receive notifications about the result of SACMO operations from the device. | SACMO 1.0 |

Table 13: DMS Requirements

6.2.2 Device

| Label | Description | Release |
|------------------|---|-----------|
| SACMO-Device-01 | The Device SHALL support download of SACMO(s) using OMA DM and/or at least one Alternate Download protocol. | SACMO 1.0 |
| SACMO-Device -02 | The Device SHALL support installation of SACMO(s). | SACMO 1.0 |
| SACMO-Device -03 | The Device SHALL support updating of SACMO(s). | SACMO 1.0 |
| SACMO-Device -04 | The Device SHALL support activation/deactivation of SACMO(s). | SACMO 1.0 |
| SACMO-Device -05 | The Device SHALL support removal of SACMO(s). | SACMO 1.0 |
| SACMO-Device -06 | The Device SHALL be able to send notifications about the result of SACMO operations to the DMS. | SACMO 1.0 |
| SACMO-Device -07 | The Device SHOULD be able to initiate a session for SACMO operations. | SACMO 1.0 |

Table 14: 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 Versions OMA-RD-SACMO-V1_0 | 22 Apr 2010 | All | Incorporates input to committee: OMA-DM-SACMO-2010-0001-INP_SACMO_RD_baseline |
| | 26 May 2010 | 6.1.1.1 6.1.1.2 6.1.4 B.4 | Incorporates CRs agreed at May 25 telco: OMA-DM-SACMO-2010-0004-CR_Security_Requirement_Corrections OMA-DM-SACMO-2010-0005-CR_Sideband_Update_Usecase OMA-DM-SACMO-2010-0006R01-CR_Usability_Requirement_Addition |
| | 01 June 2010 | All | Incorporates CR agreed at June 1 telco: OMA-DM-SACMO-2010-0007R01-CR_RD_closure_review_updates |
| Candidate Version OMA-RD-SACMO-V1_0 | 27 Jul 2010 | N/A | Status changed to Candidate by TP: OMA-TP-2010-0296-INP_SACMO_V1_0_RD_for_Candidate_Approval |

Appendix B. Use Cases (Informative)

B.1 Application problem resolution by Customer care

B.1.1 Short Description

A Customer Care Agent (CCA) receives a request from a user to fix a problem with an application on the user's device.

The CCA identifies an available control workflow to be processed on the device, which is downloaded & activate via the DM server.

The workflow checks the firmware level needed to run this application, no customer confirmation is needed for this step. The workflow identifies that a firmware update is needed, and updates the firmware following confirmation by the customer.

The workflow confirms that the application version is the current one, however it checks the software components needed to support the application and identifies that the software component for the web runtime environment is not installed. It then installs following confirmation by the customer.

The workflow then initiates a full device restart, after having received customer confirmation.

The overall result of the workflow is then reported back to the CCA.

Alternative flows

- (a) The device itself initiates the DM session, leading to the download & installation of the SACMO workflow.

When the workflow identifies that the software component needed for the web runtime environment is not installed, it rejects the installation and sends the result to the DMS to obtain specialised instructions.

B.1.2 Market benefits

The use of a device workflow avoids a series of individual client-server interactions - thereby optimising the network traffic & the reducing the workflow execution time.

B.2 Enhanced maintenance

B.2.1 Short Description

The user has a device with an enhanced maintenance service. In order to provide the desired enhanced maintenance service a specialised control workflow has been installed and pre-configured.

The customer accidentally deletes a needed software component and changes the email server address & associated APN so that a critical application will no longer work.

The maintenance service workflow executes daily, and identifies that the software components and configuration parameters needed to run the critical application are no longer available, and with customer confirmation re-installs the software component & resets the email server address & associated APN.

B.2.2 Market benefits

The critical application continues to run without the need for customer care intervention.

B.3 New device installation

B.3.1 Short Description

A customer buys a second hand device and wishes to use that device with their network operator.

The network operator downloads a workflow to the device, which installs the latest version of the web runtime environment used by the operator, adds key applications provided by the operator such as their address book, messaging & social networking clients, and sets the configuration settings for SMSC, MMSC, email server, IMS bearer environment, and APNs.

B.3.2 Market benefits

The operator can create and apply a script for each device type to initialise it and provide it with the operator specific key services and applications

B.4 Sideband Device Update

B.4.1 Short Description

A Mobile Network Operator has an agreement with an OEM that firmware updates to devices from that vendor will be processed over the web, using the vendor's proprietary mechanism. The MNO initiates the firmware update process by using the SACMO enabler to download a workflow (script file) to the device that instructs the User to tether her device to her PC for the update. The script file contains the URL of the vendor's server and any additional information necessary to enable the update (such as User confirmation messages, instructions, connection re-try algorithms, etc.). The User tethers her device, the firmware update is installed, and results reported to the SACMO client and then ultimately to the MNO's DM Server.

B.4.2 Market Benefits

Mobile Network Operators can maintain control of firmware update campaigns and configuration awareness of devices in their networks while allowing vendors to employ proprietary update mechanisms where necessary or appropriate. Additionally, out-of-band updates can conserve mobile network resources when dealing with large update packages.