DM Smart Card Architecture

Candidate Version 1.0 – 05 Nov 2010

Open Mobile Alliance

OMA-AD-DM_SC-V1_0-20101105-C

Contents

Figures

Tables

No table of figures entries found.

1. Scope (Informative)

This document describes how the Device Management Smart Card enabler fits with the other OMA Device Management Enablers, starting with the DM 1.2 Enabler that it complements using the smart card features for better immediacy of service provisioning, portability of device configuration and security of Device Management operations.

2. References

2.1 Normative References

[DM_SC-RD] "DM Smart Card Requirements", Open Mobile Alliance™, OMA-RD-DM_SC-V1_0, URL:http://www.openmobilealliance.org/

[DM1.2] "Enabler Release Definition for OMA Device Management", Open Mobile Alliance™, OMA-ERELD-DM-V1_2, URL:http://www.openmobilealliance.org/URL: http://www.openmobilealliance.org/

[DMBOOT] "OMA Device Management Bootstrap", OMA-TS-DM-Bootstrap-V1_2, Open Mobile Alliance™, URL:http://www.openmobilealliance.org/

[DMNOTI] "OMA Device Management Notification Initiated Session", OMA-TS-DM_Notification-V1_2, Open Mobile Alliance™, URL:http://www.openmobilealliance.org/

[DMSTDOBJ] "OMA Device Management Standardized Objects", OMA-TS-DM-StdObj-V1_2, Open Mobile Alliance™, URL:http://www.openmobilealliance.org/

[DMTND] "OMA Device Management Tree and Description", OMA-TS-DM-TND-V1_2, Open Mobile Alliance™, URL:http://www.openmobilealliance.org/

[DMTNDS] "OMA Device Management Tree and Description Serialization", OMA-TS-DM-TNDS-V1_2, Open Mobile Alliance™, URL:http://www.openmobilealliance.org/

[OMA-DICT] "OMA Dictionary", OMA-ORG-Dictionary-V2_7, Open Mobile Alliance™, URL:http://www.openmobilealliance.org/

[PROVSC] "Provisioning Smartcard Candidate Version 1.1", OMA-WAP-TS-ProvSC-V1_1, Open Mobile Alliance™, 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

[SCWS] "Enabler Release Definition for Smartcard-Web-Server", Open Mobile Alliance, OMA-ERELD_Smartcard_Web_Server-V1_1, URL:http://www.openmobilealliance.org/URL: http://www.openmobilealliance.org/

2.2 Informative References

[ARCH-PRINC] "OMA Architecture Principles", OMA-ArchitecturePrinciples-V1_2, ", 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

Card Issuer See [DM_SC-RD].

Interface See [OMA-DICT].

Management Tree See [DMTND].

3.3 Abbreviations

CI Card Issuer

CSIM CDMA2000 Subscriber Identity Module

DM Device Management

OMA Open Mobile Alliance

OTA Over-the-air

R-UIM Removable User Identity Module

SC Smart Card

SIM Subscriber Identity Module

USIM Universal Subscriber Identity Module

4. Introduction (Informative)

The Device Management technology provides an infrastructure to perform remote operations of configuration and servicing of devices on behalf of the end-user. In the scope of the DM SC enabler, these operations can be seen under two perspectives:

- Life Cycle: As they can be performed during the initialization phase of the device (when limited or no configuration is present) or after that initialization during the rest of the life cycle of the device.

- Security: As they can involve the use of end-user identities, credentials or data, which, by nature, must be securely administrated.

In the context of wireless networks, a Smart Card (e.g. SIM, USIM, R-UIM, CSIM) provides added value to management authorities and end-users (e.g. portability, authentication, non-repudiation, etc) and is the central element of this enabler that aims to describe an architecture that:

- Extend the provisioning capabilities of the Smart Card to cover more of the life cycle of devices in benefit of management authorities and end-users.

- Enforce the security of Device Management related operations

4.1 Version 1.0

The OMA Principles [ARCH-PRINC] are considered in order to produce a broad, secure, scalable and bearer agnostic architecture in which existent technologies are re-used as much as possible.

4.2 Security Considerations

This enabler addresses the following security threats:

- Network Operators and Enterprise Administrators protection from malicious remote servers trying to “inject” faulty configuration into devices.

- End-user protection through a mechanism that allows a configurable confirmation request for operations involving charging and/or end-user data manipulation.

- Data protection through a mechanism that allows a configurable ciphering.

- Business protection through a mechanism that provides non-repudiation of Customer Care operations.

5. Architectural Model

5.1 Dependencies

The following dependencies are identified:

Work Item	Short name	Details
Device Management	DM 1.2	See [DM1.2]
Smart Card Web Server	SCWS 1.1	See [SCWS]

5.2 Architectural Diagram

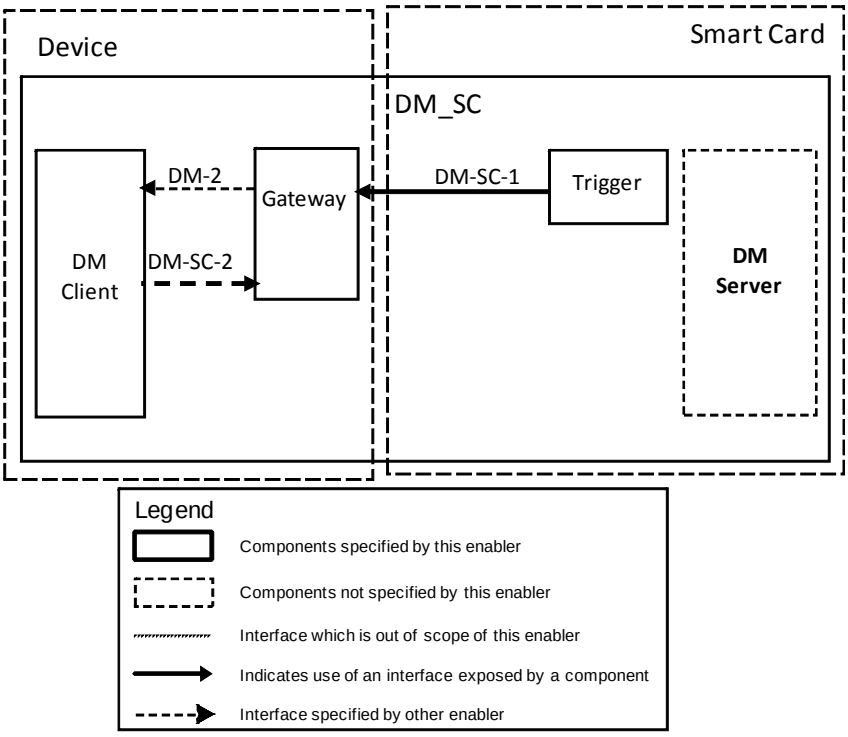

Figure 1: Device Management Smart Card Component Architecture

5.3 Functional Components and Interfaces/reference points definition

5.3.1 Components

5.3.1.1 DM_SC Trigger

This component conveys a DM Notification (see [DM1.2]) from the smart card to the DM Client. For a complete view of the relationship between this component and other DM Enabler (see [DM1.2]) components and interfaces please refer to Appendix B.

5.3.1.2 DM_SC Gateway

This component conveys transparently a DM Notification from the DM_SC Gateway to a DM Client registered as *launchable* in the Card Application Toolkit framework. As the Smart card needs to interact with it to deal with error cases it appears as a bold box in the architecture diagram.

5.3.1.3 DM Client

The DM Client is specified in the OMA Device Management Enabler. As this specification requires the support of the Notification feature, HTTP, as well as the registration of the DM Client in the Card Application Toolkit framework, this component appears as a bold box in the architectural diagram.

5.3.2 Interfaces

5.3.2.1 DM-SC-1: Smartcard triggering Interface

This interface allows the smartcard to trigger the DM Client in order to start a DM session.

5.3.2.2 DM-SC-2: Registration Interface

This interface allows the DM Client to register as *launchable* application in the Card Application Toolkit framework.

5.4 Flows

The Device Management Smart Card architecture relies on the OMA Device Management enabler [DM1.2] but requires particular data flows for interfacing the DM Client with the smartcard as shown in Figure 1. The following logical flows provide a high level view of the exchanges needed to satisfy the DM_SC requirements and use-cases (as described in [DM_SC-RD]). Readers are referred to those documents for further information.

The update of provisioning data in the smartcard is out of the scope of this enabler (see Appendix B).

5.4.1 Data provisioning triggered by the management authority

The following flows describe the exchanges between the DM Client and the smartcard needed to perform data provisioning. The data provisioning in this section does not refer to bootstrap data, which is covered in [DMBOOT] and can be provisioned using different mechanisms.

5.4.1.1 Normal Flow: Remote trigger for data provisioning

As data is stored at an unknown location the provisioning needs the smartcard to temporarily play a role of master in the session.

1. The External Card Management System sends a remote push notification to the DM Client.
2. The DM Client opens a DM session with the smartcard
3. The smartcard sends provisioning data to the DM Client

4. Optionally, end-user interaction messages may be used
5. The DM Client integrates provisioning data into its configuration
6. The DM Client provides results to the smartcard

5.4.1.2 Alternate Flow: Local Trigger for data provisioning

As data is stored at an unknown location the provisioning needs the smartcard to temporarily play a role of master in the session.

1. An event triggers the smartcard (e.g. as a timer expiration)
2. The smartcard informs the DM Client about the need of a DM session
3. Same steps as in Normal Flow (steps 2 to 6)

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-AD-DM_SC-V1_0	23 Oct 2007	All	Editorial full-text migration to the 5th of October 2007 AD template.
	5 Mar 2009	2.1, 5.2 and 5.3	Incorporates: OMA-DM-SC-2008-0001R04-CR_AD_diagram_update
	23 Apr 2009	5.2, 5.3.2, 5.4, and Appendix B	Incorporates: OMA-DM-SC-2009-0001R04-CR_AD_flows
	5 May 2009	All	Incorporates editorial changes raised during the Closure Review conference held on the 5th of May, 2009.
	26 Aug 2009	3.3, 4, 2.1, 5.1, 5.4.1 5.2, 5.3, Appendix B	Incorporates: OMA-DM-SC-2009-0009R02-CR_AD_updates OMA-DM-SC-2009-0012R03-CR_AD_clarification and some editorials
	29 Sep 2009	5.2, Appendix B	Incorporates: OMA-DM-SC-2009- 0014-CR_Interface_direction
	29 Oct 2009	All	General clean-up by DSO (formatting)
Candidate Version OMA-AD-DM_SC-V1_0	17 Nov 2009	N/A	Status changed to Candidate by TP TP ref# OMA-TP-2009-0517-INP_DM_Smart_Card_V1.0_AD_for_Candidate_Approval
Draft Version OMA-AD-DM_SC-V1_0	18 Dec 2009	5.2, 5.3, App B	Incorporates: OMA-DM-SC-2009-0018R02-CR_ArchitectureUpdate
Candidate Version OMA-AD-DM_SC-V1_0	27 Apr 2010	N/A	Status changed to Candidate by TP TP ref# OMA-TP-2010-0190R01-INP_DM_Smart_Card_V1_0_ERP_for_Candidate_Approval
Draft Version OMA-AD-DM_SC-V1_0	30 Sep 2010	5.2, App B	Incorporates: OMA-DM-SC-2010-0006-CR_DM_Interface_Labeling
Candidate Version OMA-AD-DM_SC-V1_0	05 Nov 2010	N/A	Status changed to Candidate by TP TP ref# OMA-TP-2010-0462R01-INP_DM_SmartCard_V1.0_ERP_and_ETR_for_Notification

Appendix B. Management Authority Diagram (Informative)

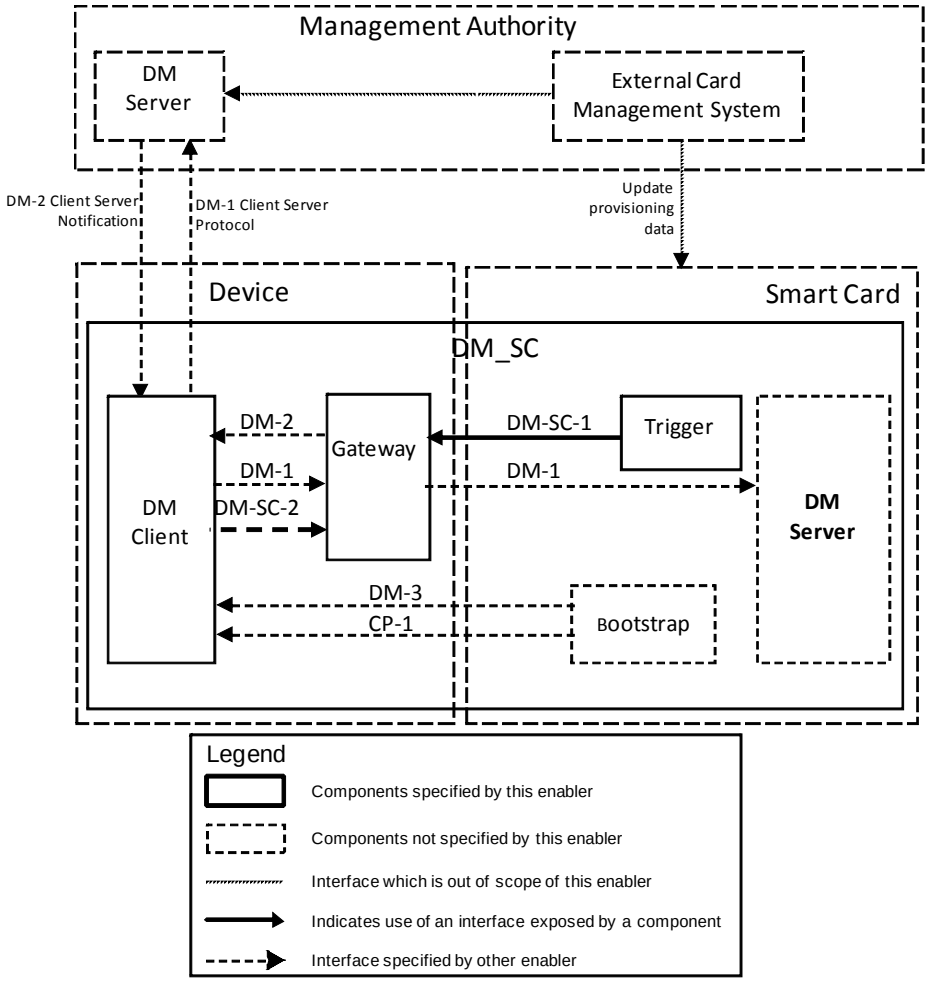

Figure 2: Architecture using interfaces

B.1 Additional Components

B.1.1 DM Client

The DM Enabler allows the Management of the Device configuration and other Managed Objects of Devices from the point of view of the various Management Authorities. DM includes, but is not restricted to setting initial configuration information in Devices, subsequent updates of persistent information in Devices, retrieval of management information from Devices and processing events and alarms generated by Devices (see [DM1.2]).

The DM Client is specified in the OMA Device Management Enabler. As this specification requires the support of the Notification feature, HTTP, as well as the registration of the DM Client in the Card Application Toolkit framework, this component appears as a bold box in the architectural diagram.

B.1.2 DM Server

The DM Server is the component that conforms to the requirements for DM Servers specified in the OMA Device Management Enabler.

B.1.3 DM_SC Gateway

This component conveys transparently a DM Notification from the DM_SC Gateway to a DM Client registered as *launchable* in the Card Application Toolkit framework. As the Smart card needs to interact with it to deal with error cases it appears as a bold box in the architecture diagram.

B.2 Additional Interfaces

B.2.1 DM-3: DM Bootstrap Profile

This interface is defined in the DM enabler (i.e. [DMBOOT]). It enables the SC to convey bootstrap information to the DM Client. The bootstrap information can consist of a single object (i.e. DMAccount as in [DMSTDOBJ] and [DMTND]) or a set of serialized objects (as in [DMTNDS]).

B.2.2 CP-1: CP Bootstrap Profile

Depending on the device implementation, and as indicated in the DM enabler (i.e. [DMBOOT]), the bootstrap information could optionally consist of application characteristics documents (see [PROVSC]). This interface enables the SC to convey bootstrap information to the DM Client.

B.2.3 DM-1: DM Client Server Protocol

This interface allows DM Servers to send device management commands to DM Clients and DM Clients may return status and alerts to DM Servers (see [DM1.2]).

B.2.4 Update Provisioning Data: External Card Management System

It enables a remote and secure updating of the SC. The interaction with the SC and the DMS is out of the scope of this enabler.