DM Smart Card Technical Specification

Approved Version 1.0 – 30 Oct 2012

Open Mobile Alliance

OMA-TS-DM_SC-V1_0-20121030-A

Contents

Figures

Tables

1. Scope

This document covers the technical aspects for implementing the Device Management Smart card requirements [DMSCRD] according to the corresponding Device Management Smart Card architecture [DMSCAD].

The technical solutions depicted in the following chapters leverage the Device Management v1.2 protocol [DM1.2] (or any later compatible release). Its use can enhance deployments of DM-based solutions as well as the wireless ecosystem with improved security where the Smart cards are used.

The following areas are in the scope of this specification:

- Dynamic provisioning through DM sessions between the DM Client and the DM_SC Server.

2. References

2.1 Normative References

[C.S0035] “CDMA Card Application Toolkit (CCAT)”, C.S0035-A v2.0 or higher release, 3GPP2,
URL:http://www.3gpp2.org/

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

[DMNOTI1.2] “OMA Device Management Notification Initiated Session”, OMA-TS-DM_Notification-V1_2, Open Mobile Alliance™,
URL:http://www.openmobilealliance.org/

[DMPRO1.2] “OMA Device Management Protocol”, OMA-TS-DM_Protocol-V1_2, Open Mobile Alliance™,
URL:http://www.openmobilealliance.org/

[DMSEC1.2] “OMA Device Management Security”, OMA-TS-DM_Security-V1_2, 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

[SCRRULES] “SCR Rules and Procedures”, Open Mobile Alliance™, OMA-ORG-SCR_Rules_and_Procedures,
URL:http://www.openmobilealliance.org/

[SCWS1.1] “Enabler Release Definition for Smartcard-Web-Server”, Open Mobile Alliance™, OMA-ERELD-Smartcard_Web_Server-V1_1,
URL:http://www.openmobilealliance.org/

[SYNCMLHTTP] “SyncML HTTP Binding”, OMA-TS-SyncML_HTTPBinding-V1_2, Open Mobile Alliance™,
URL:http://www.openmobilealliance.org/

[TS102221] “UICC-Terminal interface; Physical and logical characteristics”, Rel-7 or higher release,
URL: http://portal.etsi.org/

[TS102223] “Smart Cards; Card Application Toolkit (CAT)”, Latest Release,
URL: http://portal.etsi.org/

[TS102483] “Internet Protocol connectivity between UICC and terminal”, Rel-7 or higher release,
URL: http://portal.etsi.org/

[TS102600] “UICC-Terminal interface; Characteristics of the USB interface”, Rel-7 or higher release,
URL: http://portal.etsi.org/

[TS31.111] “Universal Subscriber Identity Module (USIM) Application Toolkit (USAT)”, Rel-7 or higher release,
URL: http://www.3gpp.org/

[WiMAXSIM] “Architecture, detailed Protocols and Procedures WiMAX-SIM Application on UICC”, DRAFT-T33-114-R015v01-C,
URL: http://www.wimaxforum.org/

2.2 Informative References

[ACMOWP] “White Paper on Provisioning Objects”, OMA-WP-AC_MO, Open Mobile Alliance™,
URL:http://www.openmobilealliance.org/

[DMSCAD] “DM Smart Card Architecture”, Open Mobile Alliance™, OMA-AD-DM_SC-V1_0,
URL:http://www.openmobilealliance.org/

[DMSCRD] “DM Smart Card Requirements”, Open Mobile Alliance™, OMA-RD-DM_SC-V1_0,
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

DM_SC Server	Application residing on the UICC as defined in [TS102221] that acts as an OMA DM server for the DM Client.
Management Authority	Consult [ACMOWP]

3.3 Abbreviations

BIP	Bearer Independent Protocol
CAT	Card Application Toolkit
CCAT	CDMA Card Application Toolkit
CSIM	CDMA Subscriber Identification Module
EEM	Ethernet Emulation Model
IP	Internet Protocol
OMA	Open Mobile Alliance
SC	Smart card
SCWS	Smartcard Web Server
UICC	Universal Integrated Circuit Card
USIM	Universal Subscriber Identity Module or User Services Identity Module
WiMAX-SIM	WiMAX Subscriber Identification Module

4. Introduction

This specification provides the technical details to implement the Device Management Smart Card enabler in order to mitigate the needs of Management Authorities captured throught the corresponding requirements (see [DMSCRD]). This specification addresses mainly the following areas:

Dynamic provisioning: Extending the provisioning capabilities of the Smart card to cover more of the life cycle of devices in benefit of management authorities and end-users.

The overall technical solution follows architectural guidelines not only by re-using existing specifications such as SCWS (see [SCWS1.1] and [TS102483]), CAT (see [TS102223]) and CCAT (see [C.S0035]), but also by minimizing the number of changes to existing DM 1.2 compliant terminals by re-use of the DM 1.2 protocol (see [DM1.2]). From this point of view, implementations of this specification can fit in systems in a backward compatible fashion.

4.1 Version 1.0

This version is focused on dynamic provisioning of Management Objects through local DM sessions between the SC and the DM Client. These sessions can be triggered through the DM Notification mechanism included in [DM1.2] either remotely by the Management Authority, or locally from a Smart card (typically a UICC-based platform with a telecom application such as USIM / CSIM / WiMAX-SIM).

Dynamic provisioning can only happen if a terminal has been previously bootstrapped. The details of how the bootstrap data is processed and consumed by the device is out of the scope of this specification as it is covered by [DM1.2] or any later release.

5. Global overview

All mandatory features of [SCWS1.1] and all mandatory features of [DM1.2] or any later compatible release MUST be supported. Additional requirements to ensure interoperability and to enable triggering of a DM Session are included in the following sections.

5.1 Physical transport

The following model summarizes the different physical and logical interface layers required to enable DM sessions between a DM_SC Server and a DM Client.

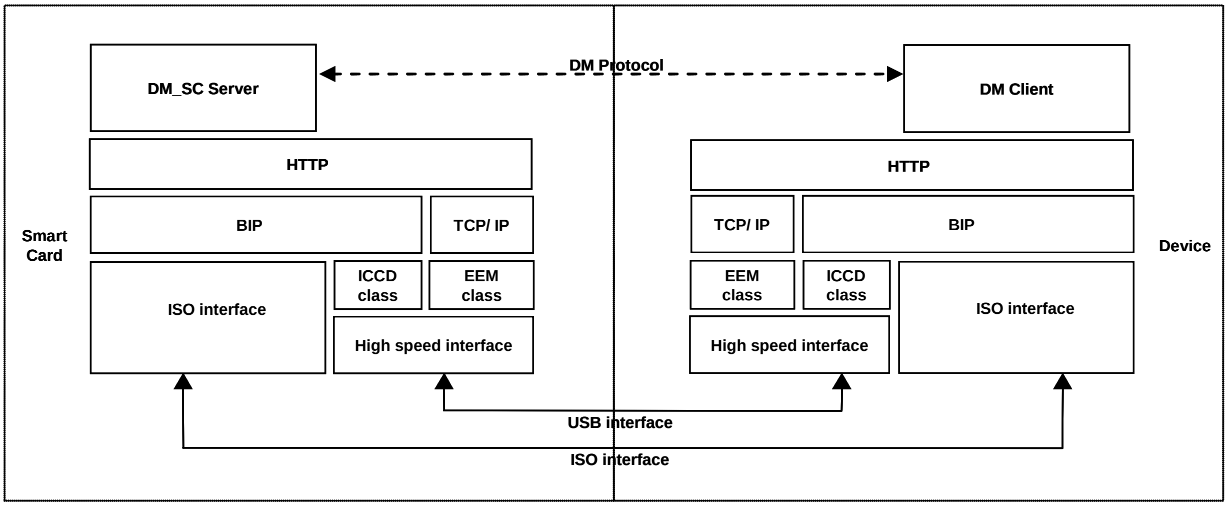

Figure 1: DM_SC Model

The physical layer supported between the SC and the device (i.e. ISO or USB) determines the path followed by the data exchanged between the DM_SC Server and the DM Client. In any case, data exchanges at the DM Protocol level are transparently conveyed through HTTP and the different logical layers are shown for comprehension purposes.

A device supporting this specification MUST comply with the mandatory local transport requirements indicated in [SCWS1.1]. A Smart card supporting this specification MUST also comply with [SCWS1.1] local transport requirements.

If a device implements a USB interface the EEM class MUST be supported in addition to the ICCD class as indicated in [TS102600].

NOTE: Support of [TS102600] also provides priority between USB and ISO interfaces.

5.2 Data Encapsulation

The DM_SC Server is responsible of the DM protocol encapsulation (see [DMPRO1.2]) including signature and/or encryption supported by the Device as needed (see [DMSEC1.2]); while the SCWS (see [SCWS1.1]) is in charge of the HTTP encapsulation (see [SYNCMLHTTP]) as indicated in the following figure:

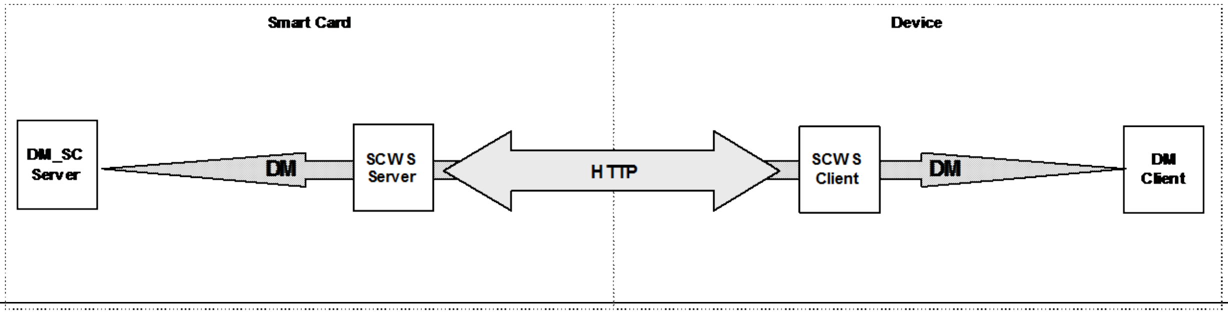

Figure 2: Data Encapsulation

The DM Client and the Smart card MUST support all mandatory requirements of HTTP as indicated in [SYNCMLHTTP] and [DMSEC1.2]. As the level of trust for authentication during DM sessions requires the use of the HTTP protocol over TLS, then it MUST be compliant with [DMSEC1.2] and [SCWS1.1].

5.3 Smart card *wake-up* versus DM Session trigger

A Management Authority (see [ACMOWP]) with corresponding rights can initiate a DM session in different ways. It can be either via a remote DM Server, it can also be as a result of an action from the user, or it can be via the DM_SC Server. In the case of a DM_SC Server, the first condition is to *wake-up* the Smart card; then the DM_SC Server will be able to send a DM Notification message (see [DMNOTI12]) to *trigger* a DM Session.

The Smart card *wake-up* relies on Card Application Toolkit commands and events as defined in [TS102223]. These commands and events provide flexibility to configure different *wake-up* scenarios.

After the Smart card *wake-up* the DM Session can be triggered. The DM Session trigger is considered *on-line* if the network is involved (i.e. to convey the DM notification to the DM Client over-the-air); otherwise it is considered to be *off-line*. The following table summarizes the different DM Session trigger scenarios available and its relationship with the Smart card *wake-up* scenarios:

SCENARIOS		**Network Use**
DM Session *trigger* **(Note 1)**	**Smart card** *wake-up* **(Note 2)**	
User Initiated	Actions made explicitly by the end user, such as calling a “Tech Support” entry in the Phone Book.	Off-line
		On-line
Client Initiated	*Out of the scope of this specification*	Not Applicable
Server Initiated	Events to which the Smart card is registered in the device (e.g. a timer expiration, a location change; etc), a Smart card web server event, or DM Notifications messages reaching the device over-the-air.	Off-line
		On-line

Table 1: DM Session trigger scenarios

NOTE 1: For further details on the different Smart card wake-up scenarios consult chapter 6.

NOTE 2: For further details on the DM Session trigger consult chapter 7.

6. DM_SC Server wake-up

The CAT and CCAT provide multiple events and commands (see [TS102223] and [C.S0035]) that can be used to *wake-up* the Smart card prior to the DM Session *trigger*. Some examples of possible *wake-up* scenarios are:

- **Power On wake-up:**

  The Smart card receives a Profile Download event just after the device is powered on.

- **Regular interval wake-up**

  The Smart card receives either a timer expiration event, or a Status command.

- **User customer care call wake-up**

  The Smart card receives a Call Control event.

- **Roaming wake-up**

  The Smart card receives a Location Status event to optimize radio resources when in roaming.

Devices supporting [SCWS1.1] and the Bearer Independent Protocol, or the USB interface according to section 5.1, support already implicitly several of the above scenarios.

The device MAY support additional events and commands according to [TS31.111] (for 3GPP devices), [C.S0035] (for 3GPP2 devices), or [WiMAXSIM] (for WiMAX devices).

7. DM Session triggering

After the Smart card *wake-up* (see chapter 6) the DM Session can be triggered making use of either an *off-line* trigger, or an *on-line* trigger method. In both cases, the DM_SC Server MUST send a DM Notification message to the DM Client. The following sections provide further details.

A DM Client implementing this specification MUST support receiving DM Notifications as defined in [DMNOTI1.2].

A Smart card implementing this specification MUST support sending DM Notifications as defined in [DMNOTI1.2].

In general, the DM Client and the Smart card MUST support DM Sessions as defined in [DM1.2].

7.1 Off-line Trigger method

As the DM protocol is encapsulated in HTTP, a connection needs to be established. This HTTP connection depends on the physical transport layer as follows:

- If the device supports ISO interface and/or USB ICCD class then the device MUST support the class “e” of [TS102223] to establish and manage the HTTP connection as indicated in [SCWS1.1] using the BIP transport protocol.
- If the device supports USB with EEM class as indicated in [TS102600], the device MUST also support [TS102483] and manage the HTTP connection as indicated in [SCWS1.1] using the TCP/IP transport protocol.

The DM Client MUST be registered in the Card Application Toolkit framework as a launchable application according to [TS102223].

The steps required for this method are:

1. The device MUST support the class “k” of [TS102223] (over ISO interface if the device supports the ISO interface or over USB ICCD class if the device supports the USB interface or finally over TCP/IP over USB EEM once [TS102223] will be available over TCP/IP) in order to communicate, through the *Registry application* data object of an ENVELOPE Terminal Applications, the following information:

    - The *port number* assigned to the DM Client.
      This value MUST be any hexadecimal number assigned by the device to the DM Client.
      The port number MUST be unique for the DM Client.
    - The *type of application* linked to the port number.
      This value MUST be a ‘07’ byte for the DM Client.
    - The *coding scheme* used on the name of the DM Client.
      This value SHOULD correspond to the GSM 7-bit default alphabet.
    - The *name* of the DM Client.
      This value MUST be a character string coded according to the *coding scheme*.

2. With this information, the DM_SC Server opens a BIP channel using the OPEN CHANNEL command in Terminal Server Mode. Using the BIP channel, the DM_SC Server sends the DM Notification message through the *channel data* of a Send Data command. The application data MUST be a General Notification Initiated Session Alert (or Package#0) as described in [DMNOTI1.2]. The device MUST convey this application data contained in the Send Data to the DM Client. If for any reason the application data can not reach the DM Client, the DM_SC Gateway MUST inform the DM_SC Server through a consequent TERMINAL RESPONSE value “Bearer Independent Protocol error”. In this case the device MUST provide additional information explaining the cause using the appropriate code as defined in [TS102223]. Afterwards, the DM_SC Server concludes this step by closing the BIP Channel.

3. The DM Client receives the DM Notification and if the DM Notification contains the ServerID of the DM_SC Server, then the DM Client will be able to start a DM session with the DM_SC Server. For this purpose, the DM Client MUST use an initialization from client to server message (or Package#1) as described in [DMPRO1.2] or any compatible version. The DM_SC Server completes the setup phase sending an initialization from server to client message (or Package#2) as described in [DMPRO1.2] or any compatible version.

4. Once the DM session has been started the data exchanges between the DM Client and the DM_SC Server MUST comply with the management phase described in [DMPRO1.2] or any compatible version.

The device MUST support the off-line trigger method.

7.2 On-line Trigger method

In this case, the DM Notification reaches the device within the payload of an SMS and the DM Setup and Management phases are performed as indicated in steps 3 and 4 of the off-line trigger method.

If the SMS bearer is supported then the device MUST support the Send Short Message proactive command as indicated in [C.S0035] (for 3GPP2 devices) and [TS31.111] (for 3GPP devices).

8. DM_SC Server

8.1 DM Account configuration

A DM Account compliant with this specification MUST have the AppAddr parameter associated to the DM_SC ServerID set to the following absolute address: "https://{SCWS@}/OMA/DM", where {SCWS@} depends on the transport and IP version supported as shown in the following table:

Transport	IP version	{SCWS@}
BIP (Note 1)	IPv4	127.0.0.1:4116
	IPv6	[::1]:4116
TCP/IP	IPv4	localuicc:443
	IPv6	localuicc:443

Table 2: DM_SC Server address

NOTE: The DM Client MAY use "localhost" host name instead of loopback address "127.0.0.1" for IPv4 or "[::1]" for IPv6.

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
OMA-TS-DM_SC-V1_0-20121030-A	30 Oct 2012	Approved by TP Ref TP Doc# OMA-TP-2012-0380-INP_DM_Smart_Card_V1_0_ERP_for_Final_Approval

Appendix B. Static Conformance Requirements (Normative)

The notation used in this appendix is specified in [SCRRULES].

B.1 SCR for DM Client

Item	Function	Reference	Requirement
DM_SC-C-001-M	Notification (Support of Server-Alerted Management Session)	Section 7	
DM_SC-C-002-M	Registration to the Card Application Toolkit framework	Section 7	
DM_SC-C-003-M	SyncML HTTP support	Section 5.2	[SYNCMLHTTP]:MCF
DM_SC-C-004-M	HTTPS support	Section 5.2	[DMSEC1.2]:DM-SEC-C-004 AND [SCWS1.1]: SCWS-C-002

B.2 SCR for DM_SC Server

Item	Function	Reference	Requirement
DM_SC-S-001-M	Notification Message	Section 7	
DM_SC-S-002-M	Notification (Support of Server-Alerted Management Session)	Section 7	
DM_SC-S-003-M	SyncML HTTP support	Section 5.2	[SYNCMLHTTP]:MSF
DM_SC-S-004-M	HTTPS support	Section 5.2	[DMSEC1.2]:DM-SEC-S-015 AND [SCWS1.1]:SCWS-S-017

B.3 SCR for DM_SC Gateway

Item	Function	Reference	Requirement
DM_SC-D-001-M	Local Transport	Section 5.1	
DM_SC-D-002-O	SMS Bearer	Section 7.2	
DM_SC-D-003-M	Off-line Trigger	Section 7.1	
DM_SC-D-004-O	On-line Trigger	Section 7.2	DM_SC-D-002-O
DM_SC-D-005-M	Registration to the Card Application Toolkit framework	Section 7.2	