DM Smart Card Requirements

Candidate Version 1.0 – 04 Sep 2007

Open Mobile Alliance

OMA-RD-DM_SC-V1_0-20070904-C

Contents

Tables

1. Scope (Informative)

This document defines the requirements for Device Management Smart Card (DM_SC) work stream, enhancing the role of the Smart Card started in the OMA DM v1.2 specifications (as defined in [ERELDDM]: [DMBOOT], [DMDDFDTD], [DMNOTI], [DMPRO], [DMREPU], [DMRD], [DMSEC], [DMSTDOBJ], [DMTND] and [DMTNDS]) and also making use of the functionalities provided by these latter specifications.

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

[ERELDDM] “Enabler Release Definition for OMA Device Management Specifications, version 1.2”. Open Mobile Alliance™. OMA-ERELD-DM-V1_2. URL:http//:www.openmobilealliance.org

[DMBOOT] “OMA Device Management Bootstrap, Version 1.2”. Open Mobile Alliance™. OMA-TS-DM-Bootstrap-V1_2_0. URL:http://www.openmobilealliance.org

[DMDDFDTD] “OMA DM Device Description Framework, Version 1.2”. Open Mobile Alliance™. OMA-TS-DM-DDF-V1_2_0. URL:http://www.openmobilealliance.org

[DMNOTI] “OMA Device Management Notification Initiated Session, Version 1.2”. Open Mobile Alliance™. OMA-DM-Notification-V1_2_0. URL:http://www.openmobilealliance.org

[DMPRO] “OMA Device Management Protocol, Version 1.2”. Open Mobile Alliance™. OMA-TS-DM-Protocol-V1_2_0. URL:http://www.openmobilealliance.org

[DMRD] “OMA Device Management Requirements Document, Version 1.2”. Open Mobile Alliance™. OMA-RD-DM-V1_2_0. URL:http://www.openmobilealliance.org

[DMREPU] “OMA Device Management Representation Protocol, Version 1.2”. Open Mobile Alliance™. OMA-TS-DM-RepPro-V1_2_0. URL:http://www.openmobilealliance.org

[DMSEC] “OMA Device Management Security, Version 1.2”. Open Mobile Alliance™. OMA-TS-DM-Security-V1_2_0. URL:http://www.openmobilealliance.org

[DMSTDOBJ] “OMA Device Management Standardized Objects, Version 1.2”. Open Mobile Alliance™. OMA-TS-DM-StdObj-V1_2_0. URL:http://www.openmobilealliance.org

[DMTND] “OMA Device Management Tree and Description, Version 1.2”. Open Mobile Alliance™. OMA-TS-DM-TND-V1_2_0. URL:http://www.openmobilealliance.org

[DMTNDS] “OMA Device Management Tree and Description Serialization, Version 1.2”. Open Mobile Alliance™. OMA-TS-DM-TNDS-V1_2_0. URL:http://www.openmobilealliance.org

[OMADIC] “Dictionary for OMA Specifications”. Open Mobile Alliance™. OMA-ORG-Dictionary-V2. 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 Issues to its customers smart cards. Telecommunications Network Operators can be card issuers, a service(s) provider and a Management Authority at the same time.

DM Message Clear-text data string or binary WBXML representation of an atomic unit in the OMA DM Protocol [DMPRO]. It can be, for example, a bootstrap message, a firmware update package or a replace command.

Smart Card Management Object Management Object (as defined [DMTND] and [DMSTDOBJ]) describing part of the Smart Card content.

Provisioning data Provisioning data is the information that will be instantiated as Management Objects.

Smart Card Also known as UICC (consult [OMADIC]). A Smart Card is a portable tamper resistant device with an embedded microprocessor chip. It can store data and applications along with security functions and mechanisms.

Service Provider Entity that provides a (several) service(s)/application(s) (e.g. IMPS, Email, …) to users.

3.3 Abbreviations

DM	Device Management
DMS	Device Management Server
MO	Management Object
OMA	Open Mobile Alliance
OTA	Over The Air
RD	Requirement Document
SC	Smart Card

4. Introduction (Informative)

As differentiation between Device (i.e. any User terminal) types grows and Device functionality broadens, the difficulty in provisioning these Devices with service-specific parameters and software increases.

Devices equipped with a smart card may use this latter element in order to provide efficient, secure and swift provisioning information of some of its services and/or application.

This document presents use cases and requirements for Smart Card functionalities in the scope of Device Management in the following areas:

- Defining a secure dynamic provisioning of Management Objects available on the Smart Card;
- Definition and description of Smart Card Management Objects;
- Security extension for DM enablers using Smart Cards
- Secure management of Management Objects (including private and sensitive data) in the Smart Card. It would include: MO's update in the SC over-the-air, MO's update in the DM-client and synchronization with the SC, new MO's storage in the SC after manufacturing, etc.

5. Use Cases (Informative)

The use cases are classified into the following categories:

- **Provisioning. Including the following cases:**
  - **Immediate Provisioning of services and applications parameters**
  - **Copying MO from device to SC**
- **DM Enablers Security. Including the following cases:**
  - **Portable Enterprise Policy**
  - **Firmware / Software approval**

5.1 Immediate Provisioning of services and applications parameters

5.1.1 Short Description

Alice has been using the IMPS and Email services on her device of model X for a while, using the Service Provider's configuration stored by the Card Issuer in a Smart Card. She receives as a gift another device of model Y in which the IMPS service and Email application are still available. As soon as Alice inserts the Smart Card inside model Y, she is instantly able to use the IMPS service and Email application without any manual configuration.

5.1.2 Actors

- **User**
- **Device**
- **Service Provider**
- **Card Issuer**
- **Smart Card**

5.1.2.1 Actor Specific Issues

- **User** wants to continue using a(several) service(s) even when changing the device.
- **Device** needs to refresh the configuration parameters of its services/applications when a new smart card is inserted and is providing a new configuration; or when the current smart card is updated with a new configuration.
- **Service Provider** wants that their services/applications remain available when the User changes her device or when the configuration of the services/applications changes
- **Card Issuer**
- **Smart Card**

5.1.2.2 Actor Specific Benefits

- **User**: flexibility in device renewal, immediate configuration and usage of services and applications
- **Service Provider**: immediate access to services and applications offered, reduced helpdesk costs
- **Card Issuer**: optimize resource usage, reduced customer care costs

5.1.3 Pre-Conditions

- Service/application configuration parameters are stored or updated in the Smart Card.

5.1.4 Post-Conditions

- Service/application is configured with the appropriate parameters; or re-configured with new parameters.

5.1.5 Normal Flow

1. User inserts Smart Card with service/application configuration parameters in a different device
2. Device reads service/application configuration parameters from the Smart Card
3. Device refreshes service/application configuration using parameters read from the Smart Card

5.1.6 Alternative Flow

1. Service/application configuration parameters are updated in the Smart Card using over-the-air mechanisms

5.1.7 Operational and Quality of Experience Requirements

- There shall be a business-relationship between the Service Provider and the Card Issuer.

5.2 Copying MO from device to SC

5.2.1 Short Description

Nuria is using on her device an application “Great Application A” from Management Authority. This application stores a MO on the device including some personalised data from Nuria and from the Management Authority.

Management Authority decides that it would be convenient to also store the MO or part of the MO in the SC to allow for example the device to be changed.

5.2.2 Actors

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

5.2.2.1 Actor Specific Issues

- **User:** The User would like to be able to continue using the application even in case of change of the device.
- **Management Authority:** The Management Authority is interested in being able to create a MO or a copy of the MO in the SC.

5.2.2.2 Actor Specific Benefits

- **User:** The User is able to continue using the application even in case of change of the device.
- **Management Authority**: The Management Authority is able create an MO or a copy of the MO in the SC.

5.2.3 Pre-conditions

- The device has already the application on the device.

- The application has already a specific MO in the DM tree.
- The SC is able to receive information from the device.

5.2.4 Post-conditions

- The user is able to continue using the application even in case of change of the device.
- The MO is copied in the SC.

5.2.5 Normal Flow

1. The Management Authority decides to copy a MO or part of a MO in the SC.
2. The Management Authority sends the device an order to copy a MO or part of a MO at the SC.
3. The device creates a MO or a copy of a MO in the SC.

5.2.6 Alternative Flow

- The device may check the MOs existing in a SC and compare them with the MOs currently available in the device.
- The device may keep the current MOs in the device even if there is a copy stored in the SC.
- The DM Server may decide to erase the MO of the Device and only use the copy stored on the SC.

5.2.7 Operational and Quality of Experience Requirements

n/a.

5.3 Portable Enterprise Policy

5.3.1 Short Description

In order to protect the enterprise, the B Company sets up a policy to limit in a secure way the use of some functions/resources on the employee's mobile device according to the enterprise procedures (e.g. during working hours or specific locations the use of Bluetooth, IR, USB, camera, etc may be forbidden.

The B Company defines, for example, the enterprise security policy including associated credentials that are used to establish the trust between the employee's mobile device and the enterprise administrator. This policy is stored in the Smart Cards. The B Company delivers the Smart Cards to its employees. When the employee inserts the smart card into his device, the device is configured with the corresponding enterprise policy

The B company administrator could manage the use of some functions/resources on the employee's mobile device (e.g. enable/disable, etc) based on the enterprise policy.

5.3.2 Actors

- **Device**
- **Management Authority: The B Company.**
- **User**: The employee of the B Company.

5.3.2.1 Actor Specific Issues

- **Management Authority**: The B Company wants to provide a policy to automatically limit the use of some functions/resources on the employee's mobile device.
- **User**: **U**ser can choose any kind of device he likes, and will not offend the policy of the Management Authority.

5.3.2.2 Actor Specific Benefits

- **Management Authority**: The B Company can manage the use of some functions/resources on the employee's device to protect the enterprise.
- **User**: User can easily follow the rules of the Management Authority.

5.3.3 Pre-conditions

- Enterprise policy shall be available in the Smart Card.
- Target functions/resources in the device can be enabled and disabled.

5.3.4 Post-conditions

The enterprise policy is permanently active after the association between the Smart Card and the Device; or after successful changes in the Smart Card performed by the Management Authority.

5.3.5 Normal Flow

1. The Management Authority defines the enterprise policy and associated credentials used to enable the enterprise administrator to manage the use of some specific functions/resources.
2. This policy is stored in the Smart Card, and then the Management Authority delivers the Smart Card to its employees.
3. The employee inserts the Smart card to his mobile device. The mobile device is configured using the enterprise policy and associated credentials in the Smart Card. Then the policy is valid.
4. According to the policy the device automatically executes the operation of enabling or disabling some specific functions/resources.
5. The device reports the result of the operation to the DM Server, the enterprise administrator obtains the information from the DM Server.

5.3.6 Alternative Flow

5.3.6.1 Alternative Flow1

Steps 1, 2, 3 and 5 are the same as in the Normal Flow.

4. The Management Authority sends an operation of enabling or disabling a resource through the Device Management Server to his employee's mobile device.

5.3.6.2 Alternative Flow 2

Steps 1, 2, 3 and 5 are the same as in the Normal Flow.

4. The operation can be executed as a scheduled task.

5.3.6.3 Alternative Flow 3

The following step occurs between step 3 and 4 of the normal flow.

3bis. The Management Authority decides to make changes over-the-air to the policy stored in the smart card.

5.3.7 Operational and Quality of Experience Requirements

- There shall be a business-relationship between the Management Authority and the Card Issuer.

5.4 Firmware / Software approval

5.4.1 Short description

At Juan's request a DM server initiates an operation such as a firmware update or software installation process in his device. To perform this operation the DM server sends one or several DM messages with a signature. Once the data has been downloaded and before installation starts, the device checks, using a cryptographic mechanism stored in the SC, if the operation and/or the data has been approved by the Management Authority.

After this verification is performed the update or installation process continues.

5.4.2 Actors

- **User**
- **Device**
- **Device Management Server**
- **Smart Card**
- **Management Authority**

5.4.2.1 Actor Specific Issues

- **User:** The User does not want operations such as firmware or software updates that could cause incorrect device operation to be performed in the device.
- **Management Authority**: Management Authority does not want users and devices being affected by inappropriate and/or unauthorized operations.

5.4.2.2 Actor Specific Benefits

- **User:** The User's device operation is not affected by inappropriate and/or unauthorized operations.
- **Management Authority**: Management Authority reduces Customer Care operations necessary to repair devices affected by inappropriate and/or unauthorized operations.

5.4.3 Pre-conditions

There is a cryptographic mechanism stored in the SC and shared with the Management Authority.

The device is able to check if a signed DM message has been approved using a cryptographic mechanism stored in the SC.

5.4.4 Post-conditions

n/a

5.4.5 Normal Flow

1. The DM server initiates an operation such as a Firmware Update or a Software Component installation or update process.

2. The Device downloads the associated data.
3. Before installation, the Device checks, using the cryptographic mechanism stored in the Smart Card, if the operation and/or data has been approved by the Management Authority. If approved then the installation proceeds normally.
4. If the operation and/or the data is not approved then the Device (depending on its policy)

   a) rejects the operation, or

   b) asks the user for confirmation before proceeding.
5. In the latter case (b), if the user accepts, the operation is performed in the device.

5.4.6 Alternative Flow

1. The Firmware Update or Software Component is not downloaded from the DM server but obtained from a different source (e.g. memory card or PC connection)

5.4.7 Operational and Quality of Experience Requirements

n/a.

6. Requirements (Normative)

6.1 High-Level Functional Requirements

Label	Description	Enabler Release
DM-SC-GEN-1	The Smart Card SHALL be capable of storing Management Objects and provisioning data.	DM_SC 1.0
DM-SC-GEN-2	The Device Management Smart Card Enabler SHALL allow the Device to determine if provisioning data is available on an installed activated Smart Card.	DM_SC 1.0
DM-SC-GEN-3	The Device Management Smart Card Enabler MAY provide a mechanism to allow authorized applications in the Device to manipulate their own provisioning data available in the smart card.	DM_SC 1.0
DM-SC-GEN-4	The Device Management Smart Card Enabler SHALL provide a mechanism based on the Smart Card to be used to ensure authenticity, integrity and non-repudiation of session between Device and Device Management Server.	DM_SC 1.0
DM-SC-GEN-5	The Device MAY be capable of comparing MOs in the SC with the MOs installed in the device.	DM_SC 1.0
DM-SC-GEN-6	The Device Management Smart Card Enabler SHALL define a mechanism to allow retrieval and incorporation of provisioning data stored on the Smart Card into the Device configuration.	DM_SC 1.0
DM-SC-GEN-7	The Device Management Smart Card Enabler SHALL provide a mechanism that allows Device Management Server to indicate the Device to store Management Objects in the Smart Card.	DM_SC 1.0
DM-SC-GEN-8	The Device Management Smart Card Enabler SHALL provide a mechanism to allow the Device to request information from the Smart Card.	DM_SC 1.0
DM-SC-GEN-9	The Device Management Smart Card Enabler SHALL allow Devices to use cryptographic mechanisms in the SC to support verification and/or signing of DM messages and, other operative data.	DM_SC 1.0
DM-SC-GEN-10	The Device Management Smart Card enabler SHALL allow to group a selection of Management Objects that have some relation between them	DM_SC 1.0
DM-SC-GEN-11	The Device Management Smart Card enabler SHALL allow a Device to request the selection of a specific group of Management Objects in the Smart Card	DM_SC 1.0
DM-SC-GEN-12	A mechanism SHALL allow the Smart Cards to store Management Objects containing large blocks of data.	DM_SC 1.0
DM-SC-GEN-13	The Device Management Smart Card Enabler SHALL provide a discovery mechanism to allow Smart Cards and Devices to identify the support of this enabler.	DM_SC 1.0
DM-SC-GEN-14	The Device Management Smart Card Enabler SHALL provide a mechanism to allow Smart Card to indicate the Device to initiate a session with the Smart Card.	DM_SC 1.0
DM-SC-GEN-15	The Device Management Smart Card Enabler SHALL provide a mechanism to indicate to the Smart Card changes in the Device's configuration data.	DM_SC 1.0
DM-SC-GEN-16	The Device Management Smart Card Enabler SHALL provide an error handling mechanism.	DM_SC 1.0
DM-SC-GEN-17	The Device Management Smart Card Enabler SHALL define a mechanism that allows the Device to consume data directly from the Smart Card.	DM_SC 1.0
DM-SC-GEN-18	The Device Management Smart Card Enabler SHALL provide a mechanism to be used to verify cryptographically signed data.	DM_SC 1.0
DM-SC-GEN-19	The Device Management Smart Card Enabler SHALL define a mechanism that allows Management Authorities to provide policies in the Smart Card.	DM_SC 1.0

DM-SC-GEN-20	The Device Management Smart Card Enabler SHALL enforce continuous provisioning from the smart card providing one or several mechanism(s) that allow the smart card to indicate to the device the presence of provisioning data in the smart card.	DM_SC 1.0
DM-SC-GEN-21	The Device SHALL look for provisioning data in the smart card at each power on.	DM_SC 1.0

Table 1: High-Level Functional Requirements

6.1.1 Security

Label	Description	Enabler Release
DM-SC-SEC-1	The Smart Card SHALL be able to securely store cryptographic parameters and mechanisms.	DM_SC 1.0

Table 2: High-Level Functional Requirements – Security Items

6.1.1.1 Authentication

Label	Description	Enabler Release
DM-SC-AUTH-1	The Device Management Smart Card Enabler SHALL support a transport mechanism that allows a variety of authentication methods to be used between the Smart Card and Device.	DM_SC 1.0
DM-SC-AUTH-2	The Device Management Smart Card Enabler SHALL ensure the successful completion of the authentication process before allowing any operation between Device and Smart Card.	DM_SC 1.0
DM-SC-AUTH-3	The Device Management Smart Card Enabler SHALL allow the Smart Card to indicate that authentication is required between the Smart Card and the Device.	DM_SC 1.0
DM-SC-AUTH-4	The Device Management Smart Card Enabler SHALL provide a mechanism to protect personal data in the Smart Card by authenticating the end-user.	DM_SC 1.0

Table 3: High-Level Functional Requirements – Authentication Items

6.1.1.2 Authorization

Label	Description	Enabler Release
DM-SC-AUT-1	Provisioning data on smart card SHALL be protected against unauthorized modification.	DM_SC 1.0

Table 4: High-Level Functional Requirements – Authorization Items

6.1.1.3 Data Integrity

No requirements identified

6.1.1.4 Confidentiality

No requirements identified

6.1.2 Charging

No requirements identified

6.1.3 Administration and Configuration

Label	Description	Enabler Release
DM-SC-ADM-1	The Device Management Smart Card Enabler SHALL provide a mechanism to allow authorized Device Management Servers to establish a data link with a Smart Card installed in a Device.	DM_SC 1.0
DM-SC-ADM-2	The Device Management Smart Card Enabler SHALL provide a mechanism to allow authorized Device Management Servers to manage provisioning data available in the Smart Card.	DM_SC 1.0

Table 5: High-Level Functional Requirements – Administration and Configuration Items

6.1.4 Usability

Label	Description	Enabler Release
DM-SC-USE-1	If smart card data contains user confirmation indication which explicitly requests user confirmation, the Device SHALL ask for user confirmation before incorporation of provisioning data stored on an installed activated smart card.	DM_SC 1.0
DM-SC-USE-2	If smart card data contains user confirmation indication which explicitly requests no user confirmation, the Device MUST NOT ask for user confirmation before incorporation of provisioning data stored on an installed activated smart card.	DM_SC 1.0
DM-SC-USE-3	If smart card data does not contain any user confirmation indication, the Device MAY ask for user confirmation before incorporation of provisioning data stored on an installed activated smart card.	DM_SC 1.0
DM-SC-USE-4	If the check for Management Authority approval of a signed DM message fails, the Device SHOULD reject the DM message and delete the downloaded data.	DM_SC 1.0
DM-SC-USE-5	If the check for Management Authority approval of a signed DM message fails, the Device MAY ask for user confirmation before processing the DM message.	DM_SC 1.0

Table 6: High-Level Functional Requirements – Usability Items

6.1.5 Interoperability

No requirements identified

6.1.6 Privacy

Label	Description	Enabler Release
DM-SC-PRV-1	The Device Management Smart Card Enabler SHALL define a mechanism to allow the Device to consume data from Smart Card without being copied in the Device.	DM_SC 1.0

Table 7: High-Level Functional Requirements – Privacy Items

6.2 Overall System Requirements

Label	Description	Enabler Release
DM-SC-OSR-1	The Smart Card SHALL decide the allocation and management of space for provisioning data inside the Smart Card.	DM_SC 1.0

Table 8: High-Level System 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-DM_SC-V1_0	10 Aug 2005	3.2, 4, 5.5, 6, App A	Alignment to Requirements Document template Alignment to WID and WISPR
	23 Aug 2005	5	Removal of use cases already covered by DM Bootstrap, addition of use case relevant to the scope of the WID
	6 Sep 2005		Baseline document
	22 Sep 2005	5.1	Incorporation of CR: OMA-DM-2005-0238R03
	06 Oct 2005	6.1.4	Incorporation of CRs: OMA-DM-SC-2005-0011R01 OMA-DM-SC-2005-0012
	06 Oct 2005	5.1.3, 6.1, 6.1.4	Incorporation of CR: OMA-DM-SC-2005-0013R02
	23 Nov 2005	5.2, 6.1, 6.1.4	Re-arrangement of section 5 to create section 5.2 Move of use case introduced with CR OMA-DM-2005-0238R03-CR-to-DM-SC-RD-HTTP-Bootstrap-SC-Signature-Use-Case (see 22 September 2005) in section 5.2 Incorporation of CR: OMA-DM-SC-2005-0016R01
	01 Dec 2005	4	Alignment of Introduction to approved WID
	19 Dec 2005	5.1.3, 6.1 2	Incorporation of CR: OMA-DM-SC-2005-0015R06 Cleaning of normative references as commented during informal review with REQ group
	11 Jan 2006	6.1, 6.1.6 6.1.4 3.2	Incorporation of CRs: OMA-DM-SC-2005-0010R03 OMA-DM-SC-2006-0001 OMA-DM-SC-2006-0002R01
	24 Feb 2006	3.2, 6.1, 6.1.x, 6.2 6.1.1, 6.1.3, 6.1.4, 6.1.1.x	Incorporation of CRs: OMA-DM-SC-2006-0004R03 OMA-DM-SC-2006-0005R02- Alignment to Requirements Document template dated 20060207
	08 Mar 2006	6.1 6.1, 6.2	Incorporation of CRs: OMA-DM-SC-2006-0007R02 OMA-DM-SC-2006-0008R01
	05 Apr 2006	6	Editorial changes: Removal of the word ‘the’ in the DM-SC-GEN-2 requirement. Re-shuffling of requirements to move them in the right sections and tables. Usage of consistent naming for the enabler.
	22 Jun 2006	6.1, 6.1.4, 6.2 6.1	Incorporation of CRs: OMA-DM-SC-2006-0015 OMA-DM-SC-2006-0016R01

Document Identifier	Date	Sections	Description
	18 Oct 2006		Incorporation of CRs: OMA-DM-SC-2006-0018R01 OMA-DM-SC-2006-0019 OMA-DM-SC-2006-0020R02 Editorials: a) Correction to add a comma after word "camera" in 1st paragraph of section 5.1.3.1. b) Requirement DM-SC-USE-1 was removed and agreed change was reflected in new HLFR: DM-SC-GEN-19. c) All Usability requirements were re-numbered accordingly. OMA-DM-SC-2006-0024
	17 Jan 2007	5.1.1.2, 5.1.1.2.1, 5.1.1.3, 5.1.1.4, 6.1 6.1.1 6.1, 6.1.1	Incorporation of CRs: OMA-DM-SC-2006-0021R02 OMA-DM-SC-2006-0025 OMA-DM-SC-2006-0026
	07 Jun 2007	Figures, 5.x 6.1.1.1, 6.1.1.3, 6.1.1.4, 6.1.2, 6.1.3, 6.1.5	Incorporation of CRs: OMA-DM-SC-2007-0002 OMA-DM-SC-2007-0003R01
	26 Jul 2007	5, 5.4, 6.1.4	Incorporation of: OMA-DM-SC-2007-0005 Editorials on: Copyright years and year of the previous update
	31 Jul 2007	5.2,5.4, 6.2	Incorporation of: OMA-DM-SC-2007-0004R01
	13 Aug 2007	All	Editorials Update history box
Candidate Versions: OMA-RD-DM_SC-V1_0	04 Sep 2007	n/a	Status changed to Candidate by OMA TP: TP ref #: OMA-TP-2007-0329-INP_DM_Smart_Card_RD_for_Candidate_Approval