Enabler Test Specification for OMA DM Smart Card

Candidate Version 1.0 – 18 OCT 2011

Open Mobile Alliance

OMA-ETS-DM_SC-V1_0-20111018-C

Contents

Figures

No table of figures entries found.

Tables

1. Scope

This document describes in detail available test cases for OMA Device Management Smart Card Release 1.0, http://www.openmobilealliance.org/Technical/release_program/DM_SC_v1_0.aspx.

The test cases are split in two categories, conformance and interoperability test cases.

The conformance test cases are aimed to verify the adherence to normative requirements described in the technical specifications.

The interoperability test cases are aimed to verify that implementations of the specifications work satisfactory.

If either conformance or interoperability tests do not exists at the creation of the test specification this part should be marked not available.

2. References

2.1 Normative References

[3GPP TS 31.111] “TS 31.111” Technical Specification Group Terminals; USIM Application Toolkit (USAT). R7 or higher, 3rd Generation Partnership Project (3GPP); URL: http://www.3gpp.org

[3GPP TS 31.124] “ TS 31.124” Technical Specification Group Core Network and Terminals; Mobile Equipment (ME) conformance test specification; Universal Subscriber Identity Module; Application Toolkit (USAT) conformance test specification, R10 or higher.

[3GPP TS 51.014] “TS 51.014” Technical Specification Group Terminals; Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface.
3rd Generation Partnership Project (3GPP); URL: http://www.3gpp.org

[3GPP2 C.S0035] “C.S0035” Technical Specification Group C; CDMA Card Application Toolkit (CCAT). R2, 3rd Generation Partnership Project 2 (3GPP2); URL: http://www.3gpp2.org

[DMERELD] “Enabler Release Definition for DM 1.2”, Version 1.2, Open Mobile Alliance™. OMA-ERELD-DM-V1_2_1. URL:http://www.openmobilealliance.org/

[DMETS] “Enabler Test Specification for Device Management”, Version 1.2, Open Mobile Alliance™. OMA-ETS-DM-V1_2. URL:http://www.openmobilealliance.org/

[DMSCERELD] “Enabler Release Definition for OMA Device Management Smart Card”, Version 1.0, Open Mobile Alliance™. OMA-ERELD-DM_SC-V1_0. URL:http://www.openmobilealliance.org/

[DMSCETR] “Enabler Test Requirements for OMA DM Smart Card”, Version 1.0, Open Mobile Alliance™. OMA-ETR-DM_SC-V1_0. URL:http://www.openmobilealliance.org/

[DMSCETS] “Enabler Test Specification for OMA DM Smart Card”, Version 1.0, Open Mobile Alliance™. OMA-ETS-DM_SC-V1_0. URL:http://www.openmobilealliance.org/

[DMSCTS] “DM Smart Card Technical Specification”, Version 1.0, Open Mobile Alliance™. OMA-TS-DM_SC_V1_0. URL:http://www.openmobilealliance.org/

[ETSI TS 102 223] “TS 102 223”, Technical Specification Smart cards; Card Application Toolkit (CAT)”, R7 or higher, European Telecommunications Standards Institute (ETSI), URL: http://www.etsi.org

[ETSI TS 102 384] “TS 102 384”, Smartcards; UICC-Terminal Interface; Card Application Toolkit (CAT) conformance specification”, V7.3.0 or higher, European Telecommunications Standards Institute (ETSI), URL: http://www.etsi.org

[ETSI TS 102 483] “TS 201 483”, Smart cards; UICC-Terminal interface; Internet Protocol connectivity between UICC and terminal), URL: http://www.etsi.org

[ETSI TS 102 600] “TS 102 600”, Smart Cards; UICC-Terminal interface; Characteristics of the USB interface, URL: http://www.etsi.org

[IOPPROC] “OMA Interoperability Policy and Process”, Version 1.9, Open Mobile Alliance™, OMA-ORG-IOP_Process-V1_9, 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

[SCWSETS] “Enabler Test Specification for Smartcard-Web-Server”, Version 1.0, Open Mobile Alliance™. OMA-ETS-Smartcard_Web_Server-V1_0. URL:http://www.openmobilealliance.org/

2.2 Informative References

[OMADICT] “Dictionary for OMA Specifications”, Version 2.8, Open Mobile Alliance™, OMA-ORG-Dictionary-V2_8, 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”, are normative, unless they are explicitly indicated to be informative.

The following numbering scheme is used:

xxx-y.z-con-number where:

xxx	Name of enabler: **DMSC**
y.z	Version of enabler release: **1.0**
’con’	Indicating this test is a conformance test case
number	Leap number for the test case.

Or

xxx-y.z-int-number where:

xxx	Name of enabler: **DMSC**
y.z	Version of enabler release: **1.0**
’int’	Indicating this test is a interoperability test case
number	Leap number for the test case. Numbering ranges are defined as follows: 500-999 for Interoperability tests with all components interacting (i.e. DM Client, DM_SC Gateway and DM_SC Server).

3.2 Definitions

BIP Bearer Independent Protocol as defined in [ETSI TS 102 223].

DM_SC Gateway BIP implementation in the terminal compliant to [DMSCTS].

Test Object It refers to the implementation under test (i.e. DM Client and/or DM_SC Gateway; or DM_SC Server).

Test Case Individual description of operations and expected results that lead to verification of the conformance of the Test Object to a particular mandatory feature of the OMA Enabler Release.

Test Group See Test Suite in [IOPPROC].

Toolkit Applet A Java Card™ applet which is triggered at a toolkit event sent from the Device to the SmartCard. The definition of the toolkit commands are described in [ETSI TS 102 223], [3GPP TS 51.014], [3GPP TS 31.111] and [3GPP2 C.S0035].

<Node> Path from the root to the interior node that is configured before the testing is done (e.g.. ‘./SyncML/DMAcc’ or ‘./DevDetail’). Test case is driven to this configured interior node. The <Node> can be different between different Test Cases.

<Leaf> or <Leaf#n> Leaf node(s) that is configured before the testing is done (e.g.. ‘SwV’ and/or ‘Name’). Test case is driven to this configured interior node. The <Leaf> can be different between different Test Cases.

3.3 Abbreviations

DM_SC	Device Management Smart Card
OMA	Open Mobile Alliance
STK	SIM ToolKit
ME	Mobile Equipment

4. Introduction

The purpose of this document is to provide test cases for OMA DM Smart Card Enabler Release 1.0.

The implementation of some OMA DM Smart Card features is optional for the DM Client and/or the DM_SC Server in the OMA DM Smart Card Enabler 1.0. The tests associated with these optional features are marked as "(Includes Optional Features)" in the test specification.

In general, the following items are needed to adequately test the OMA DM Smart Card enabler 1.0:

- A Smart Card implementing [DMSCTS].
- A device with a DM Client implementing [DMSCTS].
    - As a prerequisite the device must be initialized (i.e. bootstraped) according to [DMBOOT], or any later compatible release.
- A mobile network to allow testing the on-line trigger method.

While OMA DM v1.2 and later compatible releases allow the use of different communication protocols between DM Clients and DM Servers, OMA DM Smart Card Enabler 1.0 is based on the HTTP binding transport.

5. Conformance Test Cases

Re-use of OMA DM 1.2 and SCWS 1.1 requires successful pass of their respective Conformance Test Cases prior to the execution of Interoperability Test Cases depicted in this document. Test Objects shall comply with Conformance Test Cases defined in the correspoinding specifications, respectively in [DMETS], [SCWSETS] and with the tests defined in the specifications listed in the following table:

Command	Test Specification
OPEN CHANNEL (Terminal Server Mode)	**[ETSI TS 102 384]**
GET CHANNEL STATUS	**[ETSI TS 102 384]**
DATA AVAILABLE	**[ETSI TS 102 384]**
CHANNEL STATUS	**[ETSI TS 102 384]**
CLOSE CHANNEL	**[ETSI TS 102 384]**
SEND SHORT MESSAGE	**[3GPP TS 31.124]**
SEND DATA	**[ETSI TS 102 384]**
RECEIVE DATA	**[ETSI TS 102 384]**
PROFILE DOWNLOAD	**[ETSI TS 102 384]**
STATUS	**[3GPP TS 31.124]**

6. Interoperability Test Cases

The following Test Cases aim to cover all Mandatory and Optional Static Conformance Requirements as defined in [DMSCTS], and the corresponding Test Requirements as defined in [DMSCETR].

Test Objects implementing OMA DM 1.2 shall successfully pass all the mandatory Interoperability Test Cases defined in [DMETS] prior to execution of the Test Cases included in this section. Similarly, Test Objects implementing OMA SCWS 1.1 shall successfully pass all the mandatory Interoperability Test Cases described in [SCWSETS] as pre-requisite.

6.1 Test Group #1: HTTPS Support

The Test Strategy choosen aims to optimize time and resources by cross-testing as much requirements as possible.

SCR coverage of this Test Group is as follows:

N/A = Not Applicable
I = Implicit Coverage
X = Covered by Test Case

SCR / Interoperability Test Case	DM Client				DM_SC Server				DM_SC Gateway				
	DM_SC-C-001-M	DM_SC-C-002-M	DM_SC-C-003-M	DM_SC-C-004-M	DM_SC-S-001-M	DM_SC-S-002-M	DM_SC-S-003-M	DM_SC-S-004-M	DM_SC-D-001-M	DM_SC-D-002-O	DM_SC-D-003-M	DM_SC-D-004-O	DM_SC-D-005-M
DMSC-1.0-int-001	**X**	I	I	**X**	**X**	**X**	I	**X**	I	N/A	**X**	N/A	I
DMSC-1.0-int-002	**X**	N/A	I	**X**	**X**	**X**	I	**X**	I	**X**	N/A	**X**	N/A
DMSC-1.0-int-101	**X**	I	I	**X**	**X**	**X**	I	**X**	I	**N/A**	X	**N/A**	I
DMSC-1.0-int-102	**X**	N/A	I	**X**	**X**	**X**	I	**X**	I	**X**	N/A	**X**	N/A

Table 1: SCR coverage for Test Group #1

Test Requirements coverage of this Test Group is as follows:

Test Requirements / Interoperability Test Case	DM Client		DM_SC Server		DM_SC Gateway				
	Normal Flow		Normal Flow		Normal Flow				Error Flow
	NOTI_C_M_01	HTTPS_C_M_02	NOTI_S_M_01	HTTPS_S_M_02	OFTCFG_D_M_01	WUP_D_M_02	TRIG_D_M_03	TRNS_D_M_04	TERR_D_M_01
DMSC-1.0-int-001	**X**	**X**	**X**	**X**	**X**	I	I	I	I
DMSC-1.0-int-002	**X**	**X**	**X**	**X**	N/A	**X**	I	I	I
DMSC-1.0-int-101	**X**	**X**	**X**	**X**	X	**I**	I	I	I
DMSC-1.0-int-102	**X**	**X**	**X**	**X**	N/A	**X**	I	I	I

Table 2: Test Requirements coverage for Test Group #1

NOTE: All the commands described in this specification in bold are defined in [ETSI TS 102 223], [3GPP TS 51.014], [3GPP TS 31.111] and [3GPP2 C.S0035].

6.1.1 DMSC-1.0-int-001: Off-line trigger to replace data in the DM Tree over HTTPS using ISO interface

Test Case Id	DMSC-1.0-int-001
Test Object	DM Client and DM_SC Server devices
Test Case Description	After powering on the Device the DM_SC Server in the Smart Card is waken up. Then the DM_SC Server triggers a DM Session with the DM Client in the Device sending a DM Notification via the off-line trigger mechanism. The purpose of the DM Session established over HTTPS is to retrieve the Server ID from the DM Account MO (i.e. ServerID parameter), change the case depending on the current status (i.e. lowercase to uppercase or viceversa) and then write the new name back to the DM Tree.
Specification Reference	[DMSCTS] Chapters 5 to 8.
SCR Reference	**DM_SC-C-001-M** Notification support on DM Client side. **DM_SC-C-004-M** Support for HTTPS transport on DM Client side. **DM_SC-S-001-M** Notification message support on DM_SC Server side. **DM_SC-S-002-M** Notification support on DM_SC Server side. **DM_SC-S-004-M** Support for HTTPS transport on DM_SC Server side. **DM_SC-D-003-M** Off-line Trigger support
ETR Reference	**NOTI_C_M_01** DM Notification support on DM Client side. **HTTPS_C_M_02** HTTPS support on DM Client side. **NOTI_S_M_01** DM Notification support on DM_SC Server side. **HTTPS_S_M_02** HTTPS support on DM_SC Server side. **OFTCFG_D_M_01** Support of off-line trigger. **WUP_D_M_02** Support of wake-up mechanism. **TRIG_D_M_03** Support of trigger method.
Tool	Smart Card Tracer
Test code	TBD

Preconditions	• Equipment: ○ 1 DM Client ○ 1 DM_SC Server ○ Smart Card Reader/Writer ○ Smart Card Tracer • State: ○ DM Account ServerID can either be lowercase or uppercase. • Continuation of / Can be tested at the same time as: ○ None • Prerequisite for this test: ○ DM Client must be bootstrapped with the configuration shown in section C.1, where three DM Account MO configurations are defined. ○ A DM-SC trigger applet must be designed and deployed in the Smart Card. The Toolkit Applet must be able to wake-up the DM-SC by registering in different “events” sent by the device to the smartcard such as **PROFILE DOWNLOAD** and **STATUS**.

Test Procedure	The steps to be followed to execute this test case are: 1. Step 1 – Initialization: a) The test procedure starts with the terminal Power-up. The DM-SC uses BIP in the smartcard architecture to send an **OPEN CHANNEL (UICC Server Mode)** command to the device in order to be able to establish a HTTPS session. b) The UICC receives a **TERMINAL RESPONSE** = "TCP in Listen state" 2. Step 2 – DM Client trigger: a) In the boot-up sequence the wake-up mechanism starts as per [DMSCTS] chapter 6, when the terminal sends a Profile Download Command. b) The DM-SC uses BIP layer in the smartcard architecture to send an **OPEN CHANNEL (Terminal Server Mode)** command to the device in order to trigger the DM Client. c) Once it receives a **TERMINAL RESPONSE** = OK from the ME, indicating that a successful BIP Channel is created, the smartcard uses the **SEND DATA** command to encapsulate package 0 in order to start a DM session. d) The terminal sends a **TERMINAL RESPONS**E = OK to the smartcard which sends a **CLOSE CHANNEL** command back to the terminal in order to close the BIP (Terminal Server Mode) channel. e) The ME finish the trigger process by sending **TERMINAL RESPONSE** = OK to the smartcard. 3. Step 3 – HTTPS session: a) The DM-Client sends the package 1 to the DM-SC (as per defined in DM 1.2 Protocol) with the Server ID from the DM Account MO. b) This message is sent to the address defined in the DM Account (Config #1 or #2) from Appendix C. The DM Client uses a HTTPS POST command encapsulated in the **RECEIVE DATA** command. c) After receiving package 1 with Server ID from DM Account MO, the DM-SC must change the DM Client Server ID font case depending on its current status (i.e. lowercase to uppercase or viceversa). d) The DM-SC sends the package 2 (as per defined in DM 1.2 Protocol) using **SEND DATA** command with the new server authentication data and closes the DM session. f) The ME finish the process by sending **TERMINAL RESPONSE** = OK to the smartcard. 1.

Pass-Criteria	The test case is consider sucessfully exectued only if: 1. After power-up, the Server ID in the ME has its characters changed from lowercase ("dmsc1.0") to uppercase ("DMSC1.0") or vice-versa.

Table 2: Test Information for DMSC-1.0-int-001 Interoperability Test

6.1.2 DMSC-1.0-int-002: On-line trigger to add data in the DM Tree over HTTPS using ISO interface

Test Case Id	DMSC-1.0-int-002
Test Object	DM Client and DM_SC Server devices
Test Case Description	After a wake-up of the DM_SC Server in the Smart Card, the DM_SC Server triggers a DM Session with the DM Client in the Device sending a DM Notification via the on-line trigger mechanism. The purpose of the DM Session established over HTTPS is to add new server ID in the DM Account.
Specification Reference	[DMSCTS] Chapters 5 to 8.
SCR Reference	**DM_SC-C-001-M** Notification support on DM Client side. **DM_SC-C-004-M** Support for HTTPS transport on DM Client side. **DM_SC-S-001-M** Notification message support on DM_SC Server side. **DM_SC-S-002-M** Notification support on DM_SC Server side. **DM_SC-S-004-M** Support for HTTPS transport on DM_SC Server side. **DM_SC-D-004-O** On-line Trigger support
ETR Reference	**NOTI_C_M_01** DM Notification support on DM Client side. **HTTPS_C_M_02** HTTPS support on DM Client side. **NOTI_S_M_01** DM Notification support on DM_SC Server side. **HTTPS_S_M_02** HTTPS support on DM_SC Server side. **WUP_D_M_02** Support of wake-up mechanism **TRIG_D_M_03** Support of trigger method.
Tool	Smart Card Tracer
Test code	TBD
Preconditions	• Equipment: o 1 DM Client o 1 Smartcard with DM_SC Server and an active subscription o Smart Card Reader/Writer o Smart Card Tracer • State: o DM Account Server ID can either be lowercase or uppercase. • Continuation of / Can be tested at the same time as: o None • Prerequisite for this test: o DM Client must be bootstrapped with the configuration shown in section C.1, where three DM Account MO configurations are defined. o A DM-SC triggering applet must be designed and deployed in the smartcard. The applet must be selectable in the STK Menu. The **SELECT ITEM** command must be also implemented in order to allow the tester/end-user to trigger the DM-SC.

Test Procedure	The steps to be followed to execute this test case are: 1. Step 1 – Initialization: a) The test procedure starts with the terminal Power-up. The DM-SC uses BIP/TCP-IP layer in the smartcard architecture to send an **OPEN CHANNEL (UICC Server Mode)** command to the device in order to be able to establish an HTTPS session. **b)** The UICC receives a **TERMINAL RESPONSE** = “TCP in Listen state”. 2. Step 2 – DM Client trigger: a) The test procedure starts with the DM-SC triggering. This is achieved by the DM-SC triggering applet which must be selectable from the STK menu in the device. b) Once it is launched, the applet issues a **GET INPUT** command to allow the input of the new server ID and sends a **SEND SMS** command to the DM Client in order to trigger the DM-Client. c) The **SEND SMS** command must contain a WAP Push with server initiated request. It must also use a TP-DA value pre-configured in the DM-SC triggering applet. This value should be the tester’s subscription number. The procedure described above corresponds to the DM package 0 as defined in DM 1.2 Notification. 3. Step 3 – HTTPS session: a) The DM-Client sends the package 1 to the DM-SC with device’s Authentication Data, including server ID. b) The DM Client uses a HTTPS POST command encapsulated in the **RECEIVE DATA** command. This command uses HTTPS POST to encapsulate the package 1 information. The message is sent to the address defined in the DM Account (Config #1 or #2) from Appendix C. c) After correct reception of package 1, the DM-SC sends the package 2 to the DM Client with the new server ID provided by the end-user/tester in the Step2 above. This is achieved through the **SEND DATA** command which encapsulates a HTTPS response containing the package 2. d) The ME finish the process by sending **TERMINAL RESPONSE** = OK to the smartcard. 1.
Pass-Criteria	The test case is consider sucessfully exectued only if: 1. After power-up, the Server ID in the ME has its characters changed from lowercase (“dmsc1.0”) to uppercase (“DMSC1.0”) or vice-versa.

Table 3: Test Information for DMSC-1.0-int-002 Interoperability Test

6.1.3 DMSC-1.0-int-101: Off-line trigger to replace data in the DM Tree over HTTPS using USB interface

Test Case Id	DMSC-1.0-int-101
Test Object	DM Client and DM_SC Server devices
Test Case Description	After powering on the Device the DM_SC Server in the Smart Card is waken up. Then the DM_SC Server triggers a DM Session with the DM Client in the Device sending a DM Notification via the off-line trigger mechanism. The purpose of the DM Session established over HTTPS is to retrieve the Server ID from the DM Account MO (i.e. ServerID parameter), change the case depending on the current status (i.e. lowercase to uppercase or viceversa) and then write the new name back to the DM Tree.
Specification Reference	[DMSCTS] Chapters 5 to 8.
SCR Reference	**DM_SC-C-001-M** Notification support on DM Client side. **DM_SC-C-004-M** Support for HTTPS transport on DM Client side. **DM_SC-S-001-M** Notification message support on DM_SC Server side. **DM_SC-S-002-M** Notification support on DM_SC Server side. **DM_SC-S-004-M** Support for HTTPS transport on DM_SC Server side. **DM_SC-D-003-M** Off-line Trigger support
ETR Reference	**NOTI_C_M_01** DM Notification support on DM Client side. **HTTPS_C_M_02** HTTPS support on DM Client side. **NOTI_S_M_01** DM Notification support on DM_SC Server side. **HTTPS_S_M_02** HTTPS support on DM_SC Server side. **OFTCFG_D_M_01** Support of off-line trigger. **WUP_D_M_02** Support of wake-up mechanism. **TRIG_D_M_03** Support of trigger method.
Tool	Smart Card Tracer
Test code	TBD
Preconditions	• Equipment: ○ 1 DM Client ○ 1 DM_SC Server ○ Smart Card Reader/Writer ○ Smart Card Tracer • State: ○ DM Account Server ID can either be lowercase or uppercase. • Continuation of / Can be tested at the same time as: ○ None • Prerequisite for this test: DM Client must be bootstrapped with the configuration shown in section C.1, where three DM Account MO configurations are defined. A DM-SC trigger applet must be designed and deployed in the Smart Card. The Toolkit Applet must be able to wake-up the DM-SC by registering in different "events" sent by the device to the smartcard such as **PROFILE DOWNLOAD** and **STATUS**.

Test Procedure	The steps to be followed to execute this test case are: 1. Step 1 – Initialization: a) The USB interface case follows [ETSI TS 102 600] for the initialization and [ETSI TS 102 483] for TCP/IP establishment. **2.** Step 2 – DM Client trigger: **a)** In the boot-up sequence the wake-up mechanism starts as per [DMSCTS] chapter 6, when the terminal sends a Profile Download Command. **b)** The DM-SC uses BIP layer in the smartcard architecture to send an **OPEN CHANNEL (Terminal Server Mode)** command to the device in order to trigger the DM Client. **c)** Once it receives a **TERMINAL RESPONSE** = OK from the ME, indicating that a successful BIP Channel is created, the smartcard uses the **SEND DATA** command to encapsulate package 0 in order to start a DM session. **d)** The terminal sends a **TERMINAL RESPONS**E = OK to the smartcard which sends a **CLOSE CHANNEL** command back to the terminal in order to close the BIP (Terminal Server Mode) channel. **e)** The ME finish the trigger process by sending **TERMINAL RESPONSE** = OK to the smartcard. **3.** Step 3 – HTTPS session: **a)** The DM-Client sends the package 1 to the DM-SC (as per defined in DM 1.2 Protocol) with the Server ID from the DM Account MO, as in Annex C. **b)** This message is sent to address defined in Appendix C for DM Account MO (Config. #3) by the use of a HTTPS POST command. c) After receiving package 1 with Server ID from DM Account MO, the DM-SC must change the DM Client Server ID font case depending on its current status (i.e. lowercase to uppercase or viceversa). d) The DM-SC sends the package 2 (as per defined in DM 1.2 Protocol) with the new server authentication data and closes the DM session.

Pass-Criteria	The test case is consider sucessfully executed only if: 2. After power-up, the Server ID in the ME has its characters changed from lowercase (“dmsc1.0”) to uppercase (“DMSC1.0”) or vice-versa.

Table 4: Test Information for DMSC-1.0-int-101 Interoperability Test

6.1.4 DMSC-1.0-int-102: On-line trigger to add data in the DM Tree over HTTPS using USB interface

Test Case Id	DMSC-1.0-int-102
Test Object	DM Client and DM_SC Server devices
Test Case Description	After a wake-up of the DM_SC Server in the Smart Card, the DM_SC Server triggers a DM Session with the DM Client in the Device sending a DM Notification via the on-line trigger mechanism. The purpose of the DM Session established over HTTPS is to add new server ID in the DM Account.
Specification Reference	[DMSCTS] Chapters 5 to 8.
SCR Reference	**DM_SC-C-001-M** Notification support on DM Client side. **DM_SC-C-004-M** Support for HTTPS transport on DM Client side. **DM_SC-S-001-M** Notification message support on DM_SC Server side. **DM_SC-S-002-M** Notification support on DM_SC Server side. **DM_SC-S-004-M** Support for HTTPS transport on DM_SC Server side. **DM_SC-D-004-O** On-line Trigger support
ETR Reference	**NOTI_C_M_01** DM Notification support on DM Client side. **HTTPS_C_M_02** HTTPS support on DM Client side. **NOTI_S_M_01** DM Notification support on DM_SC Server side. **HTTPS_S_M_02** HTTPS support on DM_SC Server side. **WUP_D_M_02** Support of wake-up mechanism **TRIG_D_M_03** Support of trigger method.
Tool	Smart Card Tracer
Test code	TBD
Preconditions	• Equipment: o 1 DM Client o 1 Smartcard with DM_SC Server and an active subscription o Smart Card Reader/Writer o Smart Card Tracer • State: o DM Account Server ID can either be lowercase or uppercase. • Continuation of / Can be tested at the same time as: o None • Prerequisite for this test: o DM Client must be bootstrapped with the configuration shown in section C.1, where three DM Account MO configurations are defined. o A DM-SC triggering applet must be designed and deployed in the smartcard. The applet must be selectable in the STK Menu. The **SELECT ITEM** command must be also implemented in order to allow the tester/end-user to trigger the DM-SC.

Test Procedure	The steps to be followed to execute this test case are: 1. Step 1 – Initialization: a) The USB interface case follows [ETSI TS 102 600] for the initialization and [ETSI TS 102 483] for TCP/IP establishment. 2. Step 2 – DM Client trigger: a) The test procedure starts with the DM-SC triggering. This is achieved by the DM-SC triggering applet which must be selectable from the STK menu in the device. b) Once it is launched, the applet issues a **GET INPUT** command to allow the input a new server ID and sends a **SEND SMS** command to the DM Client in order to trigger the DM-Client. c) The **SEND SMS** command must contain a WAP Push with server initiated request. It must also use a TP-DA value pre-configured in the DM-SC triggering applet. This value should be the tester's subscription number. The procedure described above corresponds to the DM package 0 as defined in DM 1.2 Notification. 3. Step 3 – HTTPS session: a) The DM-Client sends the package 1 to the DM-SC (as per defined in DM 1.2 Protocol) with the Server ID from the DM Account MO. b) This message is sent to address defined in Appendix C for DM Account MO (Config. #3) by the use of a HTTPS POST command. c) After receiving package 1 with Server ID from DM Account MO, the DM-SC must change its font case depending on its current status (i.e. lowercase to uppercase or viceversa). d) The DM-SC sends the package 2 (as per defined in DM 1.2 Protocol) with the new server authentication data and closes the DM session.
Pass-Criteria	The test case is consider sucessfully exectued only if: 1. After power-up, the Server ID in the ME has its characters changed from lowercase ("dmsc1.0") to uppercase ("DMSC1.0") or vice-versa.

Table 5: Test Information for DMSC-1.0-int-102 Interoperability Test

6.2 Test Cases applicability

This section lists the tests to be executed according to the respective interface(s) supported by the device.

Applicability	Test Cases
Device supports ISO interface	DMSC-1.0-int-001 - Off-line trigger to replace data in the DM Tree over HTTPS using ISO interface DMSC-1.0-int-002 - On-line trigger to add data in the DM Tree over HTTPS using ISO interface
Device supports USB interface	DMSC-1.0-int-101- Off-line trigger to replace data in the DM Tree over HTTPS using USB interface DMSC-1.0-int-102 - On-line trigger to add data in the DM Tree over HTTPS using USB interface
Device supports both ISO and USB interfaces	DMSC-1.0-int-001 - Off-line trigger to replace data in the DM Tree over HTTPS using ISO interface DMSC-1.0-int-002 - On-line trigger to add data in the DM Tree over HTTPS using ISO interface DMSC-1.0-int-101- Off-line trigger to replace data in the DM Tree over HTTPS using USB interface DMSC-1.0-int-102 - On-line trigger to add data in the DM Tree over HTTPS using USB interface

Table 4: Applicability of Test Cases

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
n/a	n/a	No prior version –or- No previous version within OMA

A.2 Draft/Candidate Version 1.0 History

Document Identifier	Date	Sections	Description
Draft Versions OMA-ETS-DM_SC-V1_0	13 Sep 2010	All	Incorporates draft baseline trough input contribution: OMA-IOP-MEC-2010-0078-INP_DMSC_ETS_baseline
	28 Sep 2010	Coversheet, Table of content, §6.1.1, §6.1.2	Renumbering Test Case Ids, date update on the coversheet: OMA-IOP-MEC-2010-0078R01-INP_DMSC_ETS_baseline
	26 Sep 2011	All	Incorporates the following CRs: • OMA-IOP-MEC-2011-0077R01-CR_DM_SC_1.0_ETS_Test_Conformance • OMA-IOP-MEC-2011-0076-CR_CR_DM_SC_1.0_ETS_Test_Cases_Applicability • OMA-IOP-MEC-2011-0058R01-CR_ETS_DM_SC_V1_Test_Procedure_and_Pass_Criteria
Candidate Versions OMA-ETS-DM_SC-V1_0	18 Oct 2011	n/a	Status changed to Candidate by TP TP Ref # OMA-TP-2011-0354-INP_DMSC_1_0_ETS_for_Candidate_Approval

Appendix B. Test Configuration

B.1 Bootstrap

B.1.1 DM Account

The DM Account used to initialize the DM Client has to be configured according to the following provisions.

B.1.1.1 Server ID and AppID

Any DM_SC Server subject to testing shall use the following configuration:

B.1.1.1.1 Server ID Configuration

DM Acc Parameter	Value
AppID	"w7"
ServerID	"dmsc1.0"

B.1.1.2 Authentication Settings

The DM Account has to contain authentication settings suitable for Test Group #1. The following configuration shall be used to bootstrap the DM Client under testing:

B.1.1.2.1 Auth Configuration (Test Group #1)

	DM Acc Parameter	Value
	AAuthPref?	TRANSPORT
Transport Layer Configuration	AAuthLevel	HTTP
	AAuthType	TRANSPORT
	AAuthName?	HTTPS Config
	AAuthSecret?	
	AAuthData?	

B.1.1.3 Address Settings

The DM Account has to contain DM_SC Server address settings suitable for Test Group #1. The following configurations shall be used to bootstrap the DM Client under testing:

B.1.1.3.1 Address Configuration (Test Group #1)

	Suggested Name			**DM Acc Parameter**	**Value**
Config. 1	B4HTTPS	BIP	IPv4	Addr	https://localhost:4116/oma/dm
				AddrType	URI
				PortNbr	4116
Config. 2	B6HTTPS		IPv6	Addr	https:// [::1]:4116/oma/dm
				AddrType	URI
				PortNbr	4116
Config. 3	TCPHTTPS	TCP	IPv4 / IPv6	Addr	https://localuicc:443/oma/dm
				AddrType	URI
				PortNbr	443