# Enabler Validation Plan for Smartcard-Web-Server

Approved Version 1.1 – 12 May 2009

**Open Mobile Alliance**

OMA-EVP-Smartcard_Web_Server-V1_1-20090512-A

# Contents

1. SCOPE ..... 5
1.1 ASSUMPTIONS ..... 5
1.2 EXCLUSIONS ..... 5
2. REFERENCES ..... 6
2.1 NORMATIVE REFERENCES ..... 6
2.2 INFORMATIVE REFERENCES ..... 6
3. TERMINOLOGY AND CONVENTIONS ..... 7
3.1 CONVENTIONS ..... 7
3.2 DEFINITIONS ..... 7
3.3 ABBREVIATIONS ..... 8
4. ENABLER VALIDATION DESCRIPTION ..... 9
5. TESTFEST ACTIVITIES ..... 10
5.1 ENABLER TEST GUIDELINES ..... 10
5.1.1 Minimal Test Configuration ..... 10
5.1.2 Minimal Participation Guidelines ..... 10
5.1.3 Optimal TestFest Achievement Guidelines ..... 10
5.2 ENABLER TEST REQUIREMENTS ..... 12
5.2.1 Test Infrastructure Requirements ..... 12
5.2.2 Enabler Execution Flow ..... 12
5.2.3 Test Content Requirements ..... 16
5.2.4 Test Limitations ..... 16
5.2.5 Test Restrictions ..... 16
5.2.6 Test Tools ..... 16
5.2.7 Resources Required ..... 16
5.3 TESTS TO BE PERFORMED ..... 16
5.3.1 Entry Criteria for TestFest ..... 16
5.3.2 Testing to be Performed at TestFest ..... 17
5.4 ENABLER TEST REPORTING ..... 18
5.4.1 Problem Reporting Requirements ..... 18
5.4.2 Enabler Test Requirements ..... 18
6. ALTERNATIVE VALIDATION ACTIVITIES ..... 19
7. APPROVAL CRITERIA ..... 20
APPENDIX A. CHANGE HISTORY (INFORMATIVE) ..... 21
A.1 APPROVED VERSION HISTORY ..... 21

# Figures

Figure 1: Example Browsing Flow ..... 12
Figure 2: Example Full Administration Flow ..... 13
Figure 3: Example Lightweight Administration Flow ..... 14

# Tables

**Table 1: Listing of Tests for Entry Criteria for TestFest** ..... **17**

**Table 2: Listing of Tests to be Performed at TestFest** ..... **18**

# 1. Scope

This document details the Validation plan for the Smartcard-Web-Server 1.1 Enabler Release. The successful accomplishment of the validation activities will be required for the Enabler to be considered for Approved status.

The validation plan for the Smartcard-Web-Server 1.1 Enabler Release specifications is based on testing expectations in the Enabler Test Requirements (ETR). While the specific test activities to be performed are described in the Enabler Test Specification (ETS) the test environment is described in this plan. This test environment details infrastructure, operational and participation requirements identified for the needed testing activities.

## 1.1 Assumptions

None.

## 1.2 Exclusions

None.

# 2. References

## 2.1 Normative References


**[IOPPROC]** "OMA Interoperability Policy and Process", Version 1.6, Open Mobile Alliance™, OMA-ORG-IOP_Process-V1_6, 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

**[RFC2119]** "Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, March 1997, URL:http://www.ietf.org/rfc/rfc2119.txt

**[SCWS-AD]** "SCWS Architecture", Version 1.0, Open Mobile Alliance™, OMA-AD-Smartcard_Web_Server-V1_0, URL: http://www.openmobilealliance.org/

**[SCWS-EICS-AD]** 'Enabler Implementation Conformance Statement Admin Server Implementation of Smartcard-Web-Server' Version 1.0, Open Mobile Alliance™, OMA-EICS-Smartcard_Web_Server_AdminServer-V1_0, URL: http://www.openmobilealliance.org/

**[SCWS-EICS-D]** 'Enabler Implementation Conformance Statement Device Implementation of Smartcard-Web-Server', Version 1.0, Open Mobile Alliance™, OMA-EICS-Smartcard_Web_Server_Device-V1_0, URL: http://www.openmobilealliance.org/

**[SCWS-EICS-SC]** 'Enabler Implementation Conformance Statement Smartcard Implementation of Smartcard-Web-Server', Version 1.0, Open Mobile Alliance™, OMA-EICS-Smartcard_Web_Server_Smartcard-V1_0, URL: http://www.openmobilealliance.org/

**[SCWS-ETR]** 'SCWS Enabler Test Requirements" Version 1.1, Open Mobile Alliance™,, OMA-ETR-Smartcard_Web_Server-V1_1, URL: http://www.openmobilealliance.org/

**[SCWS-ETS]** 'SCWS Enabler Test Specification" Version 1.1, Open Mobile Alliance™,, OMA-ETS-Smartcard_Web_Server-V1_1, URL: http://www.openmobilealliance.org/

**[SCWS-RD]** "SCWS Requirements", Version 1.0, Open Mobile Alliance™,, OMA-RD_Smartcard_Web_Server-V1_0, URL: http://www.openmobilealliance.org/

**[SCWS-TS]** "SCWS Technical Specification", Version 1.1, Open Mobile Alliance™,, OMA-TS-Smartcard-Web-Server-V1_1, URL: http://www.openmobilealliance.org/

**[TS 102.223]** "TS 102.223 Technical Specification Smart cards; Card Application Toolkit (CAT)", R7 or higher, URL: http://www.etsi.org


## 2.2 Informative References


**[OMADICT]** "Dictionary for OMA Specifications", Version 2.6, Open Mobile Alliance™, OMA-ORG-Dictionary-V2.6, 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.

## 3.2 Definitions

| | |
|---|---|
| **BIP** | Bearer Independent Protocol as defined in ETSI [TS 102.223] |
| **Browser** | A program used to view (x) HTML or other media type documents. |
| **CSIM** | A Cdma2000 Subscriber Identify Module is an application defined in [3GPP2 C.S0065] residing on the UICC to register services provided by 3GPP2 mobile networks with the appropriate security. |
| **Device (or Terminal)** | A voice and/or data terminal that uses a Wireless Bearer for data transfer. Terminal types may include (but are not limited to): mobile phones (GSM, CDMA, 3GSM, etc.), data-only terminals, PDAs, laptop computers, PCMCIA cards for data communication and unattended data-only terminals (e.g., vending machines). |
| **Enabler Release** | Collection of specifications that combined together form an enabler for a service area, e.g. a download enabler, a browsing enabler, a messaging enabler, a location enabler, etc. The specifications that are forming an enabler should combined fulfil a number of related market requirements. |
| **HTTPS** | A short term for HTTP over TLS |
| **ISIM** | An IP Multimedia Services Identity Module is an application defined in [3GPP TS 31.103] residing in the memory of the UICC, providing IP service identification, authentication and ability to set up Multimedia IP Services. |
| **Minimum Functionality Description** | Description of the guaranteed features and functionality that will be enabled by implementing the minimum mandatory part of the Enabler Release. |
| **Network Operator** | An entity that is licensed and allocated frequency to operate a public mobile wireless telecommunications network for the purpose of providing publicly available commercial services. |
| **R-UIM** | A Removable User Identity Module is a standalone module defined in [3GPP2 C.S0023] to register services provided by 3GPP2 mobile networks with the appropriate security. |
| **SIM** | A Subscriber Identity Module is a standalone module defined in [3GPP TS 51.011] to register services provided by 2G mobile networks with the appropriate security. |
| **Smart card** | This is a portable tamper resistant device with an embedded microprocessor chip. A smart card is used for storing data (e.g. access codes, user subscription information, secret keys etc.) and performing typically security related operations like encryption and authentication. A smart card may contain one or more network authentication applications like the SIM (Subscriber Identification Module), USIM, R-UIM (Removable – User Identification Module), CSIM (CDMA SIM). |
| **Smart card application** | An application that executes in the smart card |
| **Smart card issuer** | The entity that gives/sales the smart card to the user (e.g. network operator for a SIM card) |
| **Smart Card Web Server** | A Web server running in the smart card |
| **UICC** | UICC is the smart card defined for the ETSI standard [TS 102.221]. It is a platform to resident applications (e.g. USIM, CSIM or ISIM). |
| **URI** | Uniform Resource Identifiers (URI, see [RFC1630]) provides a simple and extensible means for identifying a resource. URI syntax is widely used to address Internet resources over the web but is also adapted to local resources over a wide variety of protocols and interfaces. |
| **URL** | The specification is derived from concepts introduced by the World-Wide Web global information initiative, whose use of such objects dates from 1990 and is described in "Universal Resource Identifiers in WWW", RFC 1630. The specification of URLs (see [RFC1738]) is designed to meet the requirements |

| | |
|---|---|
| | laid out in "Functional Requirements for Internet Resource Locators". |
| **User** | Person who interacts with a user agent to view, hear or otherwise use a resource |
| **USIM** | A Universal Subscriber Identity Module is an application defined in [3GPP TS 31.102] residing in the memory of the UICC to register services provided by 3GPP mobile networks with the appropriate security. |
| **Web Page** | A document viewable by using a web browser or client application which is connected to the page server |
| **Web server** | A server process running on a processor, which sends out web pages in response to HTTP requests from browsers. |

## 3.3 Abbreviations

| | |
|---|---|
| **(U)SIM** | (Universal) Subscriber Identity Module |
| **APDU** | Application Protocol Data Units |
| **CAT** | Card Application Toolkit |
| **CSIM** | CDMA SIM |
| **EICS** | Enabler Implementation Conformance Statement |
| **ERDEF** | Enabler Requirement Definition |
| **ERELD** | Enabler Release Definition |
| **IP** | Internet Protocol |
| **OMA** | Open Mobile Alliance |
| **PPS** | Protocol and Parameters Selection |
| **R-UIM** | Removable User Identity Module |
| **SCWS** | Smart Card Web Server |
| **SMPP** | Short Message Peer-to-Peer protocol |
| **TCP** | Transmission Control Protocol |
| **TLS** | Transport Layer Security |

# 4. Enabler Validation Description

It is intended that TestFests will be the primary validation method for Smartcard-Web-Server 1.1. Please refer to section 5 for further information.

# 5. TestFest Activities

## 5.1 Enabler Test Guidelines

### 5.1.1 Minimal Test Configuration

The requirements for testing interoperability of the Smartcard-Web-Server enabler are:

1. A Smartcard with SCWS implementation
2. A Mobile Device with SCWS client implementation, that includes:
    - Support of the Bearer Independent Protocol (BIP) ETSI TS 102 223 release 4 & higher, class 'e' (initially standardized in 3GPP TS 11.14, class 'e', release 99)
    - Support of the BIP TCP server mode, ETSI TS 102 223, release 7 and higher.
    - Support of at least 3 channels to enable multiple applications working with the (U)SIM card (http + https + BIP classical download).
3. A Mobile Device must support Support of the Timer Management, Timer Expiration ETSI TS 102 223 release 4 & higher (initially standardized in 3GPP TS 11.14, release 99)
4. A SCWS Remote Admin Server
5. The SCWS Remote Admin Server implementation SHALL provide a way to change the settings of the Remote Administration requests included in the triggering SMS as define in the chapter 13.3.2.4 of the [SCWS-TS].
6. A SMS-C supporting the protocol SMPP 3.4 or higher.

### 5.1.2 Minimal Participation Guidelines

Minimum

- 3 different Smartcards with SCWS implementations
- 2 different SCWS Remote Admin Servers implementations
- 2 Device implementations.

### 5.1.3 Optimal TestFest Achievement Guidelines

The ETS Test Cases listed below represent a subset of all the Test Cases for the Enabler that it is thought can be executed in a test session at an OMA TestFest. This list is intended to facilitate maximum test coverage of the functionality of the enabler within a test session. It is not intended to be the only tests executed at a TestFest, and teams are encouraged to execute more tests if they are able to do in the time allowed.

The list includes:

| Test Case Id | Special Conditions |
|---|---|
| SCWS-1.0-int-001 | gif image of small size |
| SCWS-1.0-int-002 | gif image of large size |
| SCWS-1.0-int-003 | jpeg image larger than open channel buffer size |
| SCWS-1.0-int-100 | Access to server Off-line |
| SCWS-1.0-int-101 | html pages with many resources |
| SCWS-1.0-int-102 | multiple http connection |

| Test Case Id | Special Conditions |
|---|---|
| SCWS-1.0-int-103 | Browsing cancelled |
| SCWS-1.0-int-104 | Browsing interruption |
| SCWS-1.0-int-105 | Browsing and server administration |
| SCWS-1.0-int-106 | CAT applications concurrency |
| SCWS-1.0-int-107 | GET_WITH_ENVELOPE |
| SCWS-1.0-int-108 | Browsing and CAT DISPLAY-TEXT user-confirmation |
| SCWS-1.0-int-200 | long file name |
| SCWS-1.0-int-201 | long directory name |
| SCWS-1.0-int-202 | escaped char |
| SCWS-1.0-int-203 | query string |
| SCWS-1.0-int-204 | Uri long (1024 bytes) |
| SCWS-1.0-int-205 | Uri Not Found |
| SCWS-1.0-int-206 | 5 directory levels |
| SCWS-1.1-int-207 | default path |
| SCWS-1.0-int-250 | http basic authentication |
| SCWS-1.0-int-251 | admin protection |
| SCWS-1.0-int-300 | form post method |
| SCWS-1.0-int-301 | form get method |
| SCWS-1.0-int-302 | post unexistant ressource |
| SCWS-1.0-int-303 | chuncked response |
| SCWS-1.0-int-304 | form get method with special char in query string |
| SCWS-1.0-int-400 | Browsing session using BIP server mode protocol |
| SCWS-1.0-int-401 | Browsing session using TCP/IP protocol |
| SCWS-1.0-int-500 | single resource small size |
| SCWS-1.0-int-501 | single resource large size |
| SCWS-1.0-int-502 | multiple resources total size 32kb |
| SCWS-1.0-int-503 | multiple resources total size 100kb |
| SCWS-1.1-int-504 | directory deletion |
| SCWS-1.1-int-505 | resources gzipped |
| SCWS-1.1-int-506 | administration and Cache mechanism |
| SCWS-1.1-int-507 | authorized entities |
| SCWS-1.1-int-508 | memory full |
| SCWS-1.0-int-551 | administration session with terminal switched-off |
| SCWS-1.0-int-552 | administration session with network coverage loss |
| SCWS-1.0-int-553 | administration session is abandoned |
| SCWS-1.0-int-554 | administration session and browsing |
| SCWS-1.0-int-555 | admin session and other CAT application |
| SCWS-1.0-int-556 | PUT_WITH_ENVELOPE |
| SCWS-1.0-int-600 | TLS_PSK_WITH_3DES_EDE_CBC_SHA |
| SCWS-1.0-int-601 | TLS_PSK_WITH_AES_128_CBC_SHA |
| SCWS-1.0-int-602 | TLS_PSK_WITH_NULL_SHA |
| SCWS-1.0-int-701 | LIGHTWEIGHT and deactivation of the SCWS application |
| SCWS-1.0-int-800 | Admin session using BIP server mode protocol |
| SCWS-1.0-int-801 | Admin session using TCP/IP protocol |
| SCWS-1.1-int-900 | back RemoteAdmin1.0 / AdminClient 1.1 |
| SCWS-1.1-int-901 | back RemoteAdmin1.1 / AdminClient 1.0 |

## 5.2 Enabler Test Requirements

### 5.2.1 Test Infrastructure Requirements

Test infrastructure will include Smartcard with SCWS, SCWS Admin Server, SMS-C, and Device.

### 5.2.2 Enabler Execution Flow

#### 5.2.2.1 Browsing Execution Flow

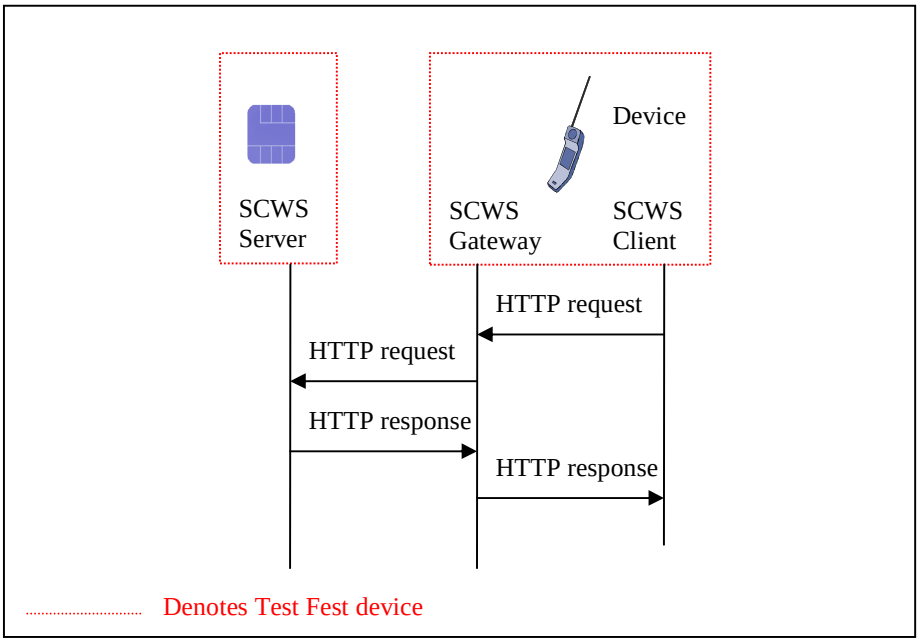



**Figure 1: Example Browsing Flow**

### 5.2.2.2 Full Administration Execution Flow

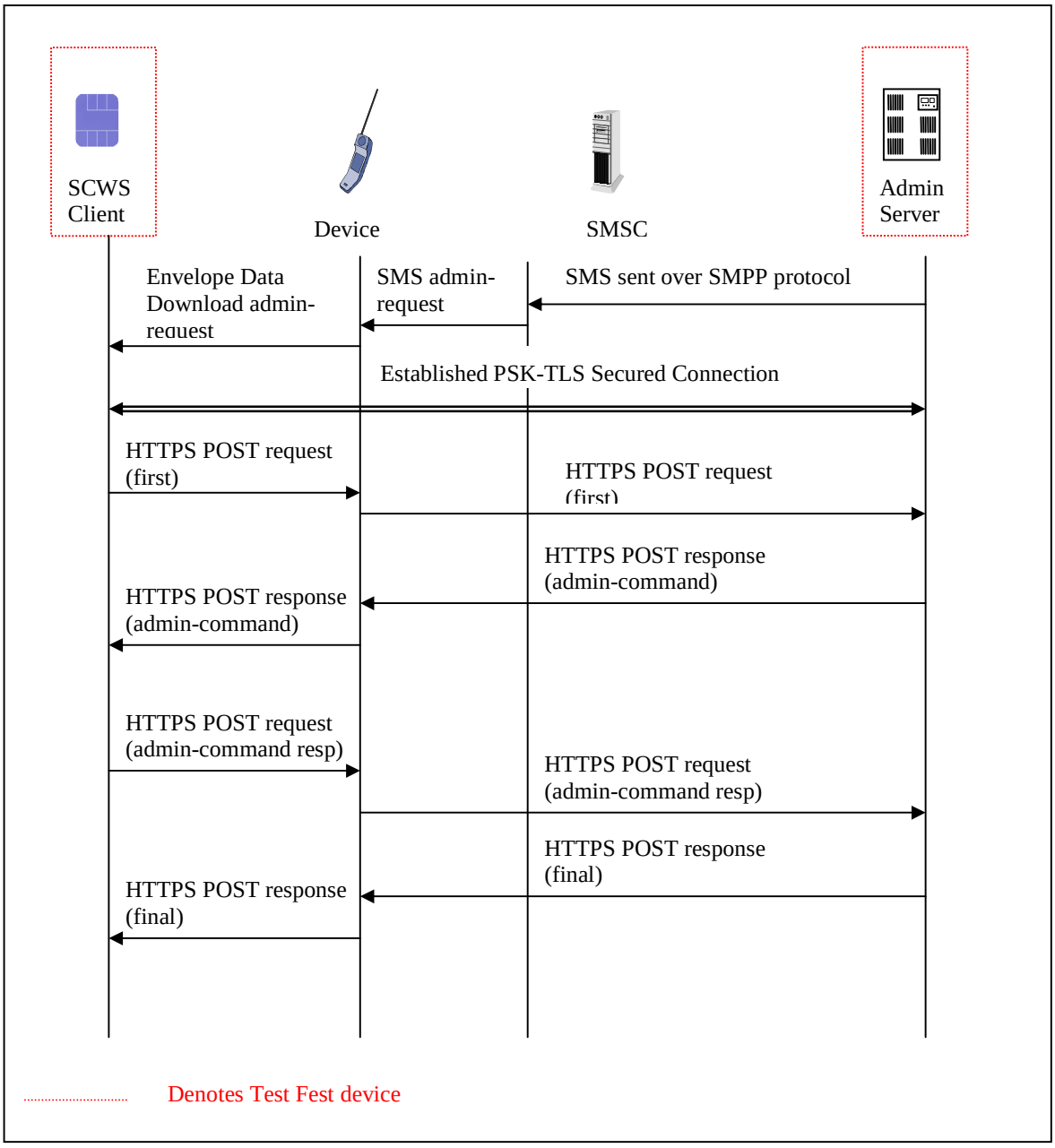



**Figure 2: Example Full Administration Flow**

### 5.2.2.3 Lightweight Administration Execution Flow

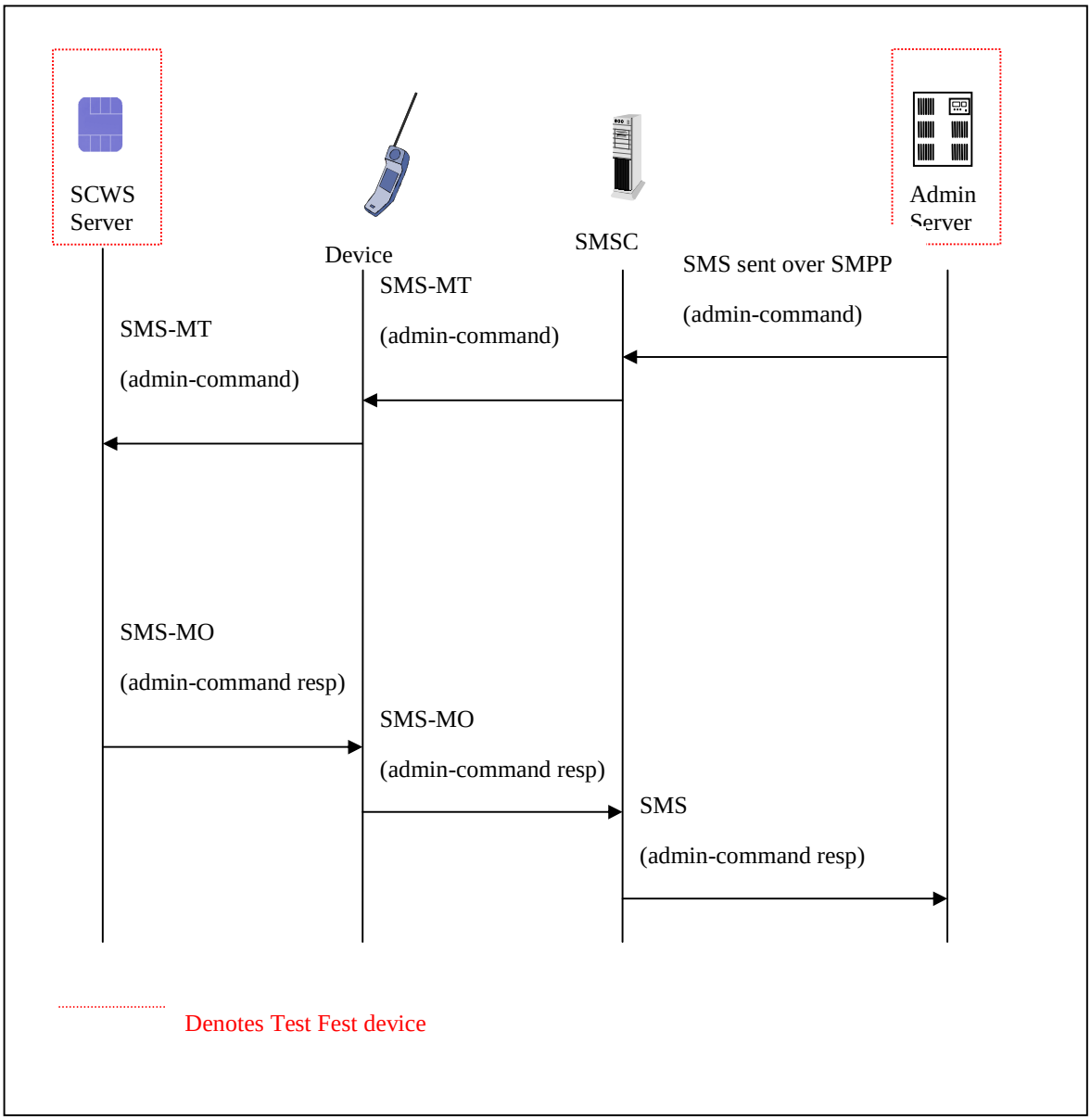
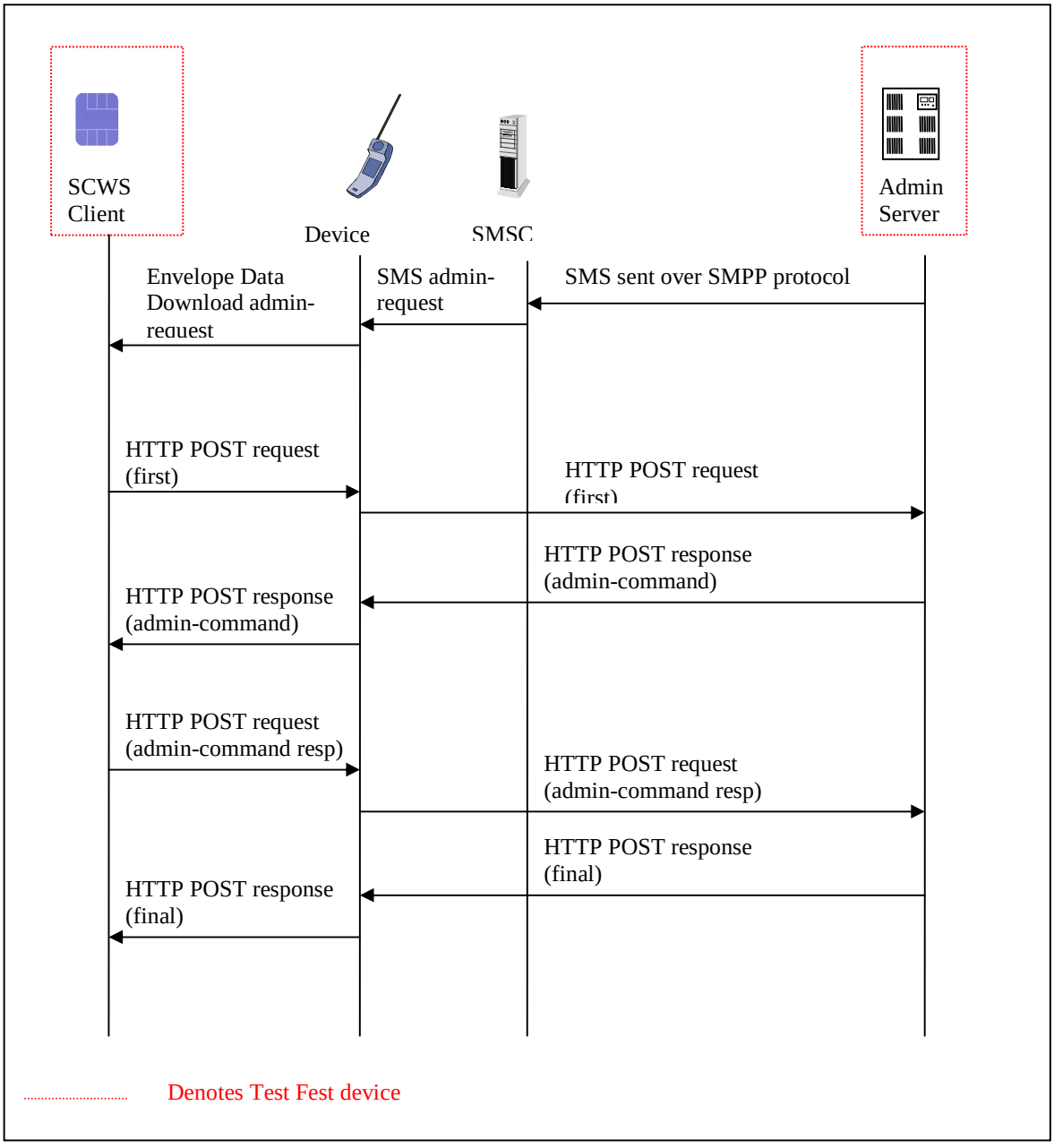



**Figure 3: Example Lightweight Administration Flow**

#### 5.2.2.4 Full Administration Execution Flow for troubleshooting

For troubleshooting analyses it's recommended to be able to deactivated TLS Security:

- Smartcard Full Administration without TLS.
- Admin Server without TLS.



### 5.2.3 Test Content Requirements

The Smartcard shall be personalized with html pages, as define in the ETS.

The Smartcard and the Admin-Server shall be personalized to fulfil the requirement of the TestFest infrastructure (SMS-C address, TLS Pre-Shared-Key value, IP address, etc).

### 5.2.4 Test Limitations

#### 5.2.4.1 Physical

None

#### 5.2.4.2 Resources

None

### 5.2.5 Test Restrictions

None

### 5.2.6 Test Tools

No conformance test tool is available.

#### 5.2.6.1 Existing Tools to be Used

None

#### 5.2.6.2 Test Tool Requirements

It is necessary to have a Smartcard protocol analyser (logging the messages between the Smartcard eg SIM and Mobile Device) to allow for analysis of the SCWS protocol messages sent and received). The Smartcard or the Mobile Device providers can provide this tool.

If order to perform the tests of the different transport protocols (BIP protocol or TCP/IP protocol), if the client doesn't implement the protocol, the server can be tested using a client simulator provided by the Smartcard or the Mobile Device providers.

### 5.2.7 Resources Required

It is expected that Smartcard, Remote Admin Server and Device implementations have at least ONE dedicated person supporting the testing during the entire duration of a test session. This person SHOULD be familiar with the actual implementation of the enabler so that he/she can answer any pertinent questions immediately and if necessary make changes to connection setup and other implementation aspects.

If the Admin Server is tested remotely and no admin interface is available remotely, a dedicated person shall be present near the equipment to perform administration task.

## 5.3 Tests to be Performed

The following sections describe the tests related to the formal TestFest validation activities.

### 5.3.1 Entry Criteria for TestFest

The following tests need to be performed and passed by implementations by members wishing to participate in the TestFest. This ensures minimal requisite capability of the implementations. The tests are defined in the ETS [ETS-SCWS] and any special comments are noted.

| Test Case Id | Special Conditions |
|---|---|
| SCWS-1.0-int-001 | gif image of small size |
| SCWS-1.0-int-101 | html pages with many resources |
| SCWS-1.0-int-103 | Browsing cancelled |
| SCWS-1.0-int-500 | single resource small size |
| SCWS-1.0-int-502 | multiple resources total size 32kb |
| SCWS-1.0-int-600 | TLS_PSK_WITH_3DES_EDE_CBC_SHA |

**Table 1: Listing of Tests for Entry Criteria for TestFest**

### 5.3.2 Testing to be Performed at TestFest

The following tests need to be performed to fully cover the range of capabilities of the enabler and defined protocols. These tests are to be covered in the TestFest. The tests are defined in the ETS [ETS-SCWS] and any special comments are noted.

| Test Case Id | Special Conditions |
|---|---|
| SCWS-1.0-int-001 | gif image of small size |
| SCWS-1.0-int-002 | gif image of large size |
| SCWS-1.0-int-003 | jpeg image larger than open channel buffer size |
| SCWS-1.0-int-004 | midi file larger than 32Kb |
| SCWS-1.0-int-005 | jpeg file of very big size |
| SCWS-1.0-int-100 | Access to server Off-line |
| SCWS-1.0-int-101 | html pages with many resources |
| SCWS-1.0-int-102 | multiple http connection |
| SCWS-1.0-int-103 | Browsing cancelled |
| SCWS-1.0-int-104 | Browsing interruption |
| SCWS-1.0-int-105 | Browsing and server administration |
| SCWS-1.0-int-106 | CAT applications concurrency |
| SCWS-1.0-int-107 | GET_WITH_ENVELOPE |
| SCWS-1.0-int-108 | Browsing and CAT DISPLAY-TEXT user-confirmation |
| SCWS-1.0-int-200 | long file name |
| SCWS-1.0-int-201 | long directory name |
| SCWS-1.0-int-202 | escaped char |
| SCWS-1.0-int-203 | query string |
| SCWS-1.0-int-204 | Uri long (1024 bytes) |
| SCWS-1.0-int-205 | Uri Not Found |
| SCWS-1.0-int-206 | 5 directory levels |
| SCWS-1.1-int-207 | default path |
| SCWS-1.0-int-250 | http basic authentication |
| SCWS-1.0-int-251 | admin protection |
| SCWS-1.0-int-300 | form post method |
| SCWS-1.0-int-301 | form get method |
| SCWS-1.0-int-302 | post unexistant ressource |
| SCWS-1.0-int-303 | chuncked response |
| SCWS-1.0-int-304 | form get method with special char in query string |
| SCWS-1.0-int-400 | Browsing session using BIP server mode protocol |
| SCWS-1.0-int-401 | Browsing session using TCP/IP protocol |
| SCWS-1.0-int-500 | single resource small size |
| SCWS-1.0-int-501 | single resource large size |

| Test Case Id | Special Conditions |
|---|---|
| SCWS-1.0-int-502 | multiple resources total size 32kb |
| SCWS-1.0-int-503 | multiple resources total size 100kb |
| SCWS-1.1-int-504 | directory deletion |
| SCWS-1.1-int-505 | resources gzipped |
| SCWS-1.1-int-506 | administration and Cache mechanism |
| SCWS-1.1-int-507 | authorized entities |
| SCWS-1.1-int-508 | memory full |
| SCWS-1.0-int-551 | administration session with terminal switched-off |
| SCWS-1.0-int-552 | administration session with network coverage loss |
| SCWS-1.0-int-553 | administration session is abandoned |
| SCWS-1.0-int-554 | administration session and browsing |
| SCWS-1.0-int-555 | admin session and other CAT application |
| SCWS-1.0-int-556 | PUT_WITH_ENVELOPE |
| SCWS-1.0-int-600 | TLS_PSK_WITH_3DES_EDE_CBC_SHA |
| SCWS-1.0-int-601 | TLS_PSK_WITH_AES_128_CBC_SHA |
| SCWS-1.0-int-602 | TLS_PSK_WITH_NULL_SHA |
| SCWS-1.0-int-701 | LIGHTWEIGHT and deactivation of the SCWS application |
| SCWS-1.0-int-800 | Admin session using BIP server mode protocol |
| SCWS-1.0-int-801 | Admin session using TCP/IP protocol |
| SCWS-1.1-int-900 | back RemoteAdmin1.0 / AdminClient 1.1 |
| SCWS-1.1-int-901 | back RemoteAdmin1.1 / AdminClient 1.0 |

**Table 2: Listing of Tests to be Performed at TestFest**

## 5.4 Enabler Test Reporting

### 5.4.1 Problem Reporting Requirements

Normal Reporting, no special reporting required.

### 5.4.2 Enabler Test Requirements

Normal Reporting, no special reporting required.

# 6. Alternative Validation Activities

No alternative validation activities are specified.

# 7. Approval Criteria

The SCWS 1.1 Enabler can be put in the Approved state when:

- The Enabler has been tested successfully at at least one formal Test Fest
- Whose results can be improved by bi-lateral test sessions that have reported results and any issues to OMA.

No open PRs exist.

# Appendix A. Change History (Informative)

## A.1 Approved Version History

| Reference | Date | Description |
|---|---|---|
| OMA-EVP-Smartcard_Web_Server-V1.1 | 12 May 2009 | Status changed to Approved by TP<br>TP ref # OMA-TP-2009-0190-INP_Smartcard_Web_Server_V1_1_ERP_for_Final_Approval |