Enabler Test Specification for

Smartcard Web Server

Candidate Version 1.0 – 06 Nov 2007

Open Mobile Alliance

OMA-ETS-Smartcard_Web_Server-V1_0-20071106-C

© 2007 Open Mobile Alliance Ltd. All Rights Reserved.

Used with the permission of the Open Mobile Alliance Ltd. under the terms as stated in this document. [OMA-Template-EnablerTestSpec-20070101-I]

Contents

1. Scope

This document describes in detail available test cases for Smartcard-Web-Server 1.0 http://www.openmobilealliance.org/.

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 the specifications can be imnplemented in an interoperable manner.

2. References

2.1　Normative References

[3GPP TS 31.103]	"TS 31.103 Technical Specification Group Core Network and Terminals; Characteristics of the IP Multimedia Services Identity Module (ISIM) application", 3rd Generation Partnership Project (3GPP), URL: http://www.3gpp.org/ftp/Specs/archive/31_series/31.103/
[3GPP TS 51.011]	"TS 51.011 Technical Specification Group Terminals; Specification of the Subscriber Identity Module-Mobile Equipment (SIM - ME) interface", 3rd Generation Partnership Project (3GPP), URL: http://www.3gpp.org/ftp/Specs/archive/51_series/51.011/
[3GPP2 C.S0023-C]	"Removable User Identity Module for Spread Spectrum Systems", 3rd Generation Partnership Project 2 (3GPP2), Technical Specification 3GPP2 C.S0023, URL: http://www.3gpp2.org/
[3GPP2 C.S0065]	"cdma2000 Application on UICC for Spread Spectrum Systems", 3rd Generation Partnership Project 2 (3GPP2), Technical Specification 3GPP2 C.S0065, URL: http://www.3gpp2.org/
[ASN.1]	Abstract Syntax Notation One, URL: http://www.itu.int/ITU-T/studygroups/com17/languages
[C.S0078]	3GPP2 Common Security Algorithms, "Secured Packet Structure for CDMA Card Application Toolkit (CCAT) Applications", 3rd Generation Partnership Project 2 (3GPP2), Technical Specification 3GPP2 C.S0078, URL: http://www.3gpp2.org/Public_html/specs/alltsgscfm.cfm
[C.S0079]	"Remote APDU Structure for CDMA Card Application Toolkit (CCAT) Applications", 3rd Generation Partnership Project 2 (3GPP2), Technical Specification 3GPP2 C.S0079, URL: http://www.3gpp2.org/Public_html/specs/alltsgscfm.cfm
[HTML 4.0.1]	HyperText Markup Language, HTML 4.01 Specification W3C Recommendation, URL: http://www.w3.org/TR/1999/REC-html401-19991224/
[HTTP over TLS]	"Hypertext Transfer Protocol over TLS protocol", RFC 2818, May 2000, URL: http://www.ietf.org/rfc/rfc2818.txt
[HTTP/1.1]	"Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999, URL: http://www.ietf.org/rfc/rfc2616.txt
[IOPPROC]	"OMA Interoperability Policy and Process", Version 1.5, Open Mobile Alliance™, OMA-IOP-Process-V1_5, URL: http://www.openmobilealliance.org/
[ISO7816-4]	"Information technology -Identification cards -Integrated circuit(s) cards with contacts- Part 4: Interindustry commands for interchange"
[OMA-TLS-Profile]	"OMA TLS Profile", Version 1.0, Open Mobile Alliance™, OMA-TS-TLS-V1_0-20051017-D, URL: http://www.openmobilealliance.org/
[PSK-TLS]	"Pre-Shared Key Cipher suites for Transport Layer Security (TLS)", RFC 4279, URL: http://www.ietf.org/rfc/rfc4279.txt?number=
[RFC 1630]	"Universal Resource Identifiers in WWW: A Unifying Syntax for the Expression of Names and Addresses of Objects on the Network as used in the World-Wide Web", URL: http://www.ietf.org/rfc/rfc1630.txt
[RFC 3546]	"Transport Layer Security (TLS) Extensions", URL: http://www.ietf.org/rfc/rfc2119.txt
[RFC 3986]	"Uniform Resource Identifier (URI): Generic Syntax", URL: http://www.ietf.org/rfc/rfc3986.txt
[RFC2119]	"Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, March 1997, URL: http://www.ietf.org/rfc/rfc2119.txt
[RFC2234]	"Augmented BNF for Syntax Specifications: ABNF". D. Crocker, Ed., P. Overell. November 1997, URL: http://www.ietf.org/rfc/rfc2234.txt
[RFC2617]	"HTTP Authentication: Basic and Digest Access Authentication", URL: http://www.ietf.org/rfc/rfc2617.txt?number=2617
[SCWS-AD]	"SCWS Architecture", Open Mobile Alliance™, OMA-AD-Smartcard_Web_Server-V1_0, URL: http://www.openmobilealliance.org/
[SCWS-ETR]	'SCWS Enabler Test Requirements" Open Mobile Alliance™, OMA-ETR-Smartcard_Web_Server-V1_0, 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", Open Mobile Alliance™, OMA-TS-Smartcard-Web-Server-V1_0, URL: http://www.openmobilealliance.org/
[TEST_CONTENT]	"Enabler Test Specification for Smartcard Web Server Content" Open Mobile Alliance™, OMA-ETS-Smartcard_Web_Server_CONTENT_V1_0-20071106-C.zip, URL: http://www.openmobilealliance.org/
[TEST_CONTENT_D ESC]	"Enabler Test Specification for Smartcard Web Server Content" Open Mobile Alliance™, OMA-ETS-Smartcard_Web_Server_CONTENT_V1_0-20071106-C.doc, URL: http://www.openmobilealliance.org/
[TLS]	"Security Transport Protcol", RFC 2246, January 1999, URL: http://www.ietf.org/rfc/rfc2246.txt
[TS 102 221]	"TS 102 221 Smart Cards; UICC-Terminal interface; Physical and logical characteristics", European Telecommunications Standards Institute (ETSI), URL: http://www.etsi.org
[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
[TS 31.102]	"TS 31.102 Technical Specification Smart cards; Characteristics of the Universal Subscriber Identity Module (USIM) application", 3rd Generation Partnership Project (3GPP), URL: http://www.3gpp.org/ftp/Specs/archive/31_series/31.102/
[TS 31.115]	3GPP TS 31.115: "Secured packet structure for (U)SIM Toolkit applications", 3rd Generation Partnership Project (3GPP), URL: http://www.3gpp.org/ftp/Specs/archive/31_series/31.115/
[TS 31.116]	3GPP TS 31.116: "Remote APDU Structure for (U)SIM Toolkit applications", 3rd Generation Partnership Project (3GPP), URL: http://www.3gpp.org/ftp/Specs/archive/31_series/31.116/
[WAPCert]	"WAP Certificate and CRL Profiles", WAP Forum™, WAP-211-WAPCert, URL: http://www.openmobilealliance.org/

2.2 Informative References

[OMADICT]	"Dictionary for OMA Specifications", Version x.y, Open Mobile Alliance™, OMA-ORG-Dictionary-Vx_y, URL:http://www.openmobilealliance.org/
[SCWS WID]	Smartcard web server work item (WID 92)
[WAPWAE]	"Wireless Application Environment Specification", Open Mobile Alliance™, OMA-WAP-WAESpec-V2_3, URL: http://www.openmobilealliance.org/
[WP HTTP]	"Wireless Profiled HTTP", WAP Forum™, WAP-229-HTTP-20010329-a, 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, e.g. MMS or Browsing |
> | y.z | Version of enabler release, e.g. 1.2 or 1.2.1 |
> | '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, e.g. MMS or Browsing |
> | y.z | Version of enabler release, e.g. 1.2 or 1.2.1 |
> | 'int' | Indicating this test is a interoperability test case |
> | number | Leap number for the test case |

3.2   Definitions

Application authentication	An application that is invoked by the SCWS and that may generate dynamic content can implement its own user or principal authentication scheme. We call this authentication "Application authentication".
BIP	Bearer Independent Protocol as defined in ETSI [TS 102 223].
BIP gateway	BIP implementation in the terminal as defined in [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.
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.
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.
Proactive UICC session	A "Proactive UICC session" is a sequence of related CAT commands and responses which start with the status response '91XX' (proactive command pending) and ends with a status response of '90 00' (normal ending of command) after Terminal Response as defined in [TS 102223].
ProactiveHandler	A ProactiveHandler is a smart card entity that is in charge of managing Proactive UICC sessions. Only one Proactive UICC session can be active at a given time.
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.
SCWS proactive session	A "SCWS proactive session" is a proactive UICC session that has been opened by a SCWS and is maintained by a SCWS.
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).
Terminal (or device)	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).
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

ACP	Access Control Policy
AD	Architecture Document
APDU	Application Protocol Data Units
CAT	Card Application Toolkit
CSIM	CDMA SIM
IP	Internet Protocol
OMA	Open Mobile Alliance
PSK-TLS	Pre-Shared Key TLS
RD	Requirements Document
R-UIM	Removable User Identity Module
SCWS	Smart Card Web Server
TCP	Transmission Control Protocol
TLS	Transport Layer Security
USIM	Universal Subscriber Identity Module

4. Introduction

The purpose of this document is to provide test cases for Smartcard-Web-Server Enabler Release 1.0.

Some features in the Smartcard-Web-Server enabler may optionally be implemented in mobile devices.

The interoperability test cases are split in two categories, SCWS Client to SCWS Server and Remote Admin Server to Admin Client test cases.

These two categories are split in several test groups.

5. Smartcard-Web-Server Conformance Test Cases

There are no conformance cases identified at this time. Mandatory SCR items will be covered in the interoperability test case

6. Smartcard-Web-Server Interoperability Test Cases

6.1 SCWS Client to SCWS Server

6.1.1 Content type and content length test group

6.1.1.1 SCWS-1.0-int-001: gif image of small size

Test Case Id	SCWS-1.0int-001
Test Object	Device, SCWS Client and SCWS Server.
Test Case Description	The purpose is to verify that gif image of size 117 bytes is correctly sent from server to client.
Specification Reference	[SCWS-TS] Chapter 9
SCR Reference	SCWS-C-001 SCWS-S-003, SCWS-S-008, SCWS-S-009 SCWS-ME-001
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, §6.1.2, [TEST_CONTENT]

Preconditions	• Equipment:
	    o Terminal
	    o Smartcard with SCWS server
	• Prerequisite for this test:
	    o SCWS server is provisioned with test portal.

Test Procedure	1. In the Terminal select WAP browser. 2. Select the SCWS test portal link (eg http:/localhost:3516/index.html) 3. Select "Test resources type and length" link. 4. Select "Bullet.gif" link. 5. Verify the pass criteria below.
Pass-Criteria	The image "Bullet.gif" is displayed.

6.1.1.2 SCWS-1.0-int-002: gif image of large size

Test Case Id	SCWS-1.0int-002
Test Object	Device, SCWS Client and SCWS Server.
Test Case Description	The purpose is to verify that gif image of size 1519 bytes is correctly sent from server to client. This test case will test segmentation on BIP commands
Specification Reference	[SCWS-TS] Chapter 9
SCR Reference	SCWS-C-001 SCWS-S-003, SCWS-S-008, SCWS-S-009 SCWS-ME-001
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, §6.1.2, [TEST_CONTENT]

Preconditions	- Equipment: ○ Terminal ○ Smartcard with SCWS server - Prerequisite for this test: ○ SCWS server is provisionned with the test content.
Test Procedure	1. In the Terminal select WAP browser. 2. Select the SCWS test portal link (eg http:/localhost:3516/index.html) 3. Select "Test resources type and length" link. 4. Select "mobile tv.gif" link. 5. Verify the pass criteria below.
Pass-Criteria	The image "mobile tv.gif" is displayed.

6.1.1.3   SCWS-1.0-int-003: jpeg image larger than open channel buffer size

Test Case Id	SCWS-1.0int-003
Test Object	Device, SCWS Client and SCWS Server.
Test Case Description	The purpose is to verify that jpeg image of size 11.3 KB bytes is correctly sent from server to client. This test case will test ability to exchange http message larger than BIP OPEN_CHANNEL buffer size.
Specification Reference	[SCWS-TS] Chapter 9
SCR Reference	SCWS-C-001 SCWS-S-003, SCWS-S-008, SCWS-S-009 SCWS-ME-001
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, §6.1.2, [TEST_CONTENT]
Preconditions	- Equipment: ○ Terminal ○ Smartcard with SCWS server - Prerequisite for this test: ○ SCWS server is provisionned with the test content.
Test Procedure	1. In the Terminal select WAP browser. 2. Select the SCWS test portal link (eg http:/localhost:3516/index.html) 3. Select "Test resources type and length" link. 4. Select "Mer-d-Iroise.jpg" link. 5. Verify the pass criteria below.
Pass-Criteria	The image "Mer-d-Iroise.jpg" is displayed.

6.1.1.4   SCWS-1.0-int-003: midi file larger than 32Kb

Test Case Id	SCWS-1.0int-004
Test Object	Device, SCWS Client and SCWS Server.
Test Case Description	The purpose is to verify that midi file of size 41 KB bytes is correctly sent from server to client. This test case will test server ability to host resource bigger than 32Kb.

Specification Reference	[SCWS-TS] Chapter 9
SCR Reference	SCWS-C-001 SCWS-S-003, SCWS-S-008, SCWS-S-009 SCWS-ME-001
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, §6.1.2, [TEST_CONTENT]

Preconditions	• Equipment:
	    o Terminal
	    o Smartcard with SCWS server
	 • Prerequisite for this test:
	    o SCWS server is provisionned with the test content.

Test Procedure	1. In the Terminal select WAP browser. 2. Select the SCWS test portal link (eg http:/localhost:3516/index.html) 3. Select "Test resources type and length" link. 4. Select "audi.mid" link. 5. Verify the pass criteria below.
Pass-Criteria	The file "audio.mid" is downloaded to the Terminal. According to the Terminal capabilities the midi file is played.

6.1.1.5 SCWS-1.0-int-004: jpeg file of very big size

Test Case Id	SCWS-1.0int-005
Test Object	Device, SCWS Client and SCWS Server.
Test Case Description	The purpose is to verify that jpeg file of size 136 KB bytes is correctly sent from server to client. This test case will test long exchange between client and server, during this exchange client time-out can occurred or over flow client capabilities.
Specification Reference	[SCWS-TS] Chapter 9
SCR Reference	SCWS-C-001 SCWS-S-003, SCWS-S-008, SCWS-S-009 SCWS-ME-001
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, §6.1.2, [TEST_CONTENT]

Preconditions	• Equipment:
	    o Terminal
	    o Smartcard with SCWS server
	 • Prerequisite for this test:
	    o SCWS server is provisionned with the test content.

Test Procedure	1. In the Terminal select WAP browser. 2. Select the SCWS test portal link (eg http:/localhost:3516/index.html) 3. Select "Test resources type and length" link. 4. Select "Malaga bench.jpg" link. 5. Verify the pass criteria below.

Pass-Criteria	According to the terminal capabilities the image "Malaga bench.jpg" is displayed.

6.1.2   Connectivity test group

6.1.2.1   SCWS-1.0-int-100 Access to server Off-line

Test Case Id	SCWS-1.0-int-100
Test Object	Device, SCWS Client and SCWS Server.
Test Case Description	The purpose is to verify that server is accessible in off-line mode (no network connection).
Specification Reference	[SCWS-TS] Chapter 7
SCR Reference	SCWS-C-001 SCWS-S-003, SCWS-S-008, SCWS-S-009 SCWS-ME-001
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, [TEST_CONTENT]

Preconditions	• Equipment:
	     o Terminal
	     o Smartcard with SCWS server
	 • Prerequisite for this test:
	     o SCWS server is provisionned with the test content.

Test Procedure	1. Terminal is in off-line mode (no network connection). 2. In the Terminal select WAP browser. 3. Select the SCWS test portal link (eg http:/localhost:3516/index.html) 4. Verify the pass criteria below.
Pass-Criteria	The test portal home page is displayed.

6.1.2.2   SCWS-1.0-int-101 html pages with many resources

Test Case Id	SCWS-1.0-int-101
Test Object	Device, SCWS Client and SCWS Server.
Test Case Description	The purpose is to verify that html page with many resources (9 gif anf 1 stylesheet) is correctly sent from server to client.
Specification Reference	[SCWS-TS] Chapter 7
SCR Reference	SCWS-C-001 SCWS-S-003, SCWS-S-008, SCWS-S-009 SCWS-ME-001
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1 §6.1.3, [TEST_CONTENT]

Preconditions	• Equipment:
	     o Terminal
	     o Smartcard with SCWS server
	• Prerequisite for this test:
	     o SCWS server is provisionned with the test content.

Test Procedure	1. In the Terminal select WAP browser. 2. Select the SCWS test portal link (eg http:/localhost:3516/index.html) 3. Select "Test pages with many resources" link. 4. Verify the pass criteria below.
Pass-Criteria	The testpages.html is displayed.

6.1.2.3   SCWS-1.0-int-102 multiple http connection

Test Case Id	SCWS-1.0-int-102
Test Object	Device, SCWS Client and SCWS Server.
Test Case Description	This test case will test mutiple http connection in parallele.
Specification Reference	[SCWS-TS] Chapter 7
SCR Reference	SCWS-C-001 SCWS-S-003, SCWS-S-008, SCWS-S-009 SCWS-ME-001
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1 §6.1.3, [TEST_CONTENT]

Preconditions	• Equipment:
	     o Terminal that used multiple http connection.
	     o Smartcard with SCWS server
	• Prerequisite for this test:
	     o SCWS server is provisionned with the test content.

Test Procedure	1. In the Terminal select WAP browser. 2. Select the SCWS test portal link (eg http:/localhost:3516/index.html) 3. Select "Test pages with many resources" link. 4. Verify the pass criteria below.
Pass-Criteria	The testpages.html is displayed.

6.1.2.4   SCWS-1.0-int-103 Browsing cancelled

Test Case Id	SCWS-1.0-int-103
Test Object	Device, SCWS Client and SCWS Server.
Test Case Description	The purpose is to verify that client/server connection cancelled is correctly managed. This test case will test http message exhange interruption by BIP event channel status ESTABLISHED, LISTEN.
Specification Reference	[SCWS-TS] Chapter 7

SCR Reference	SCWS-C-001 SCWS-S-003, SCWS-S-008, SCWS-S-009 SCWS-ME-001
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, §6.1.2, [TEST_CONTENT]

Preconditions	• Equipment:
	    o Terminal
	    o Smartcard with SCWS server
	• Prerequisite for this test:
	    o SCWS server is provisionned with the test content.

Test Procedure	1. In the Terminal select WAP browser. 2. Select the SCWS test portal link (eg http:/localhost:3516/index.html) 3. Select "Test resources type and length" link. 4. Select "Mer-d-Iroise.jpg" link. 5. Do cancel before the complete image is displayed. 6. Select "Mer-d-Iroise.jpg" link. 7. Verify the pass criteria below.
Pass-Criteria	The image "Mer-d-Iroise.jpg" is displayed.

6.1.2.5   SCWS-1.0-int-104 Browsing interruption

Test Case Id	SCWS-1.0-int-104
Test Object	Device, SCWS Client and SCWS Server.
Test Case Description	The purpose is to verify that client/server connection interruption is correctly managed. This test case will test http message exhange interruption by BIP event channel status ESTABLISHED, LISTEN in multiple connection mode.
Specification Reference	[SCWS-TS] Chapter 7
SCR Reference	SCWS-C-001 SCWS-S-003, SCWS-S-008, SCWS-S-009 SCWS-ME-001
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, §6.1.3; [TEST_CONTENT]

Preconditions	• Equipment:
	    o Terminal
	    o Smartcard with SCWS server
	• Prerequisite for this test:
	    o SCWS server is provisionned with the test content.

Test Procedure	1. In the Terminal select WAP browser.
	2. Select the SCWS test portal link (eg http:/localhost:3516/index.html)
	3. Select "Test pages with many resources" link.
	4. Select first link (image 1) as soon as this link is available.
	5. Verify that "1" is displayed
	6. Select back link.
	7. Verify the pass criteria below.
Pass-Criteria	The "Test pages with many resources" is displayed (testpages.html).

6.1.2.6   SCWS-1.0-int-105 Browsing and server administration

Test Case Id	SCWS-1.0-int-105
Test Object	Device, SCWS Client, SCWS Server, Remote admin SCWS Server, and SCWS admin client.
Test Case Description	The purpose is to verify that admin client connection is taken into account when receiving during client / server exchange.
Specification Reference	[SCWS-TS] Chapter 7
SCR Reference	SCWS-C-001
	SCWS-S-003, SCWS-S-008, SCWS-S-009
	SCWS-ME-001
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, §6.1.2, [TEST_CONTENT]
Preconditions	• Equipment:
	o Terminal
	o Smartcard with SCWS server and SCWS admin client
	o Remote admin SCWS Server.
	• Prerequisite for this test:
	o SCWS server is provisionned with the test content.
	o Smartcard card administration agent is configured with remote admin SCWS Server parameters (ip-address, port...).
Test Procedure	1. In the Terminal select WAP browser.
	2. In the WAP browser, select the SCWS test portal link (eg http:/localhost:3516/index.html)
	3. In the WAP browser, select "Test resources type and length" link.
	4. On the remote admin server interface, select portal of 32kb, and download.1
	5. In the WAP browser, select "audi.mid" link.
	6. The file "audio.mid" is downloaded to the Terminal.
	7. On the remote admin server interface, wait then verify that download portal of 32kb is successful finished.
	8. Verify the pass criteria below.

Pass-Criteria	Verify that the download portal of 32kb is present on the Smartcard Web Server.
	1. In WAP browser, select page 1 verifies that 4 images are displayed.
	2. In WAP browser, select page 2 verifies that 6 images are displayed.

6.1.2.7 SCWS-1.0-int-106 CAT applications concurrency

Test Case Id	SCWS-1.0-int-106
Test Object	Device, SCWS Client, SCWS Server
Test Case Description	The purpose is to verify that the SCWS doesn't modify the behaviour of CAT applications
Specification Reference	[SCWS-TS] Chapter 8.1.1.1
SCR Reference	SCWS-C-001
	SCWS-S-003, SCWS-S-007, SCWS-S-008, SCWS-S-009
	SCWS-ME-001
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1,§6.1.2, §6.3 [TEST_CONTENT]
Preconditions	• Equipment:
	o Terminal A, Terminal B
	o Smartcard with SCWS server and SCWS admin client
	• Prerequisite for this test:
	o SCWS server is provisionned with the test content.
	o CAT concurrency application is loaded and installed in the smartcard. This CAT application is registered on MT call event and send a DISPLAY_TEXT proactive command.when triggered by this event.
Test Procedure	1. In the Terminal A select WAP browser.
	2. In the WAP browser, select the SCWS test portal link (eg http:/localhost:3516/index.html)
	3. In the WAP browser, select "Test resources type and length" link.
	4. Select "Mer-d-Iroise.jpg" link.
	5. Make a call from Terminal B to Terminal A.
	6. Verify the pass criteria below.
	Rmq: Synchronize step 5 in order that event MT call is received by the smartcard before the complete client/server messages exchange
Pass-Criteria	In the Terminal A, "Hello World" is displayed.

6.1.2.8 SCWS-1.0-int-107 GET_WITH_ENVELOPE

Test Case Id	SCWS-1.0-int-107
Test Object	Device, SCWS Client, SCWS Server
Test Case Description	The purpose is to verify that a SCWS browsing session is correctly processed while the execution of the proactive command SET UP CALL is triggered by a SMS from the second terminal.
Specification Reference	[SCWS-TS] Chapter 8.1.1.1 SCWS and other CAT applications concurrency

SCR Reference	SCWS-AC-001, SCWS-AC-004, SCWS-AC-005, SCWS-AC-007, SCWS-AC-010
	SCWS-AS-001, SCWS-AS-004, SCWS-AS-005
	SCWS-S-012, SCWS-S-022
Tool	
Test code	CAT application on a UNFORMATTED_SMS_PP i.e. on this event the Applet performs a SET UP CALL proactive command.

Preconditions	• Equipment:
	     o Terminal A, Terminal B.
	     o Smartcard with SCWS server, CAT application registered on the UNFORMATTED_SMS_PP Event
	 • Prerequisite for this test:
	     o SCWS server is provisioned with the test content.
	     o SIM with a special CAT application executing a SET UP CALL when triggered by a UNFORMATTED_SMS_PP event.

Test Procedure	1. In the Terminal A select WAP browser. 2. Select the SCWS test portal link (eg http:/localhost:3516/index.html) 3. Select "Test resources type and length" link. 4. Select "Mer-d-Iroise.jpg" link to start download 5. . Send SMS from Terminal B to Terminal A. 6. Verify the pass criteria below.
Pass-Criteria	Verify that the SET UP CALL is executed and verify that browsing session is not aborted

6.1.3   URI test group

6.1.3.1   SCWS-1.0-int-200 long file name

Test Case Id	SCWS-1.0-int-200
Test Object	Device, SCWS Client and SCWS Server.
Test Case Description	The purpose is to verify that uri with a long file name is correctly handled by server.
Specification Reference	[SCWS-TS] Chapter 5
SCR Reference	SCWS-C-001
	SCWS-S-003, SCWS-S-008, SCWS-S-009
	SCWS-ME-001
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, §6.1.4, [TEST_CONTENT]

Preconditions	• Equipment:
	o Terminal
	o Smartcard with SCWS server
	• Prerequisite for this test:
	o SCWS server is provisionned with the test content.
Test Procedure	1. In the Terminal select WAP browser.
	2. Select the SCWS test portal link (eg http:/localhost:3516/index.html)
	3. Select link "Test uri (length, escaped, …)"
	4. Select link "long file name"
	5. Verify the pass criteria below.
Pass-Criteria	The "Hello long file name" is displayed.

6.1.3.2 SCWS-1.0-int-201 long directory name

Test Case Id	SCWS-1.0-int-201
Test Object	Device, SCWS Client and SCWS Server.
Test Case Description	The purpose is to verify that uri with a long directory name is correctly handled by server.
Specification Reference	[SCWS-TS] Chapter 5
SCR Reference	SCWS-C-001
	SCWS-S-003, SCWS-S-008, SCWS-S-009
	SCWS-ME-001
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, §6.1.4, [TEST_CONTENT]
Preconditions	• Equipment:
	o Terminal
	o Smartcard with SCWS server
	• Prerequisite for this test:
	o SCWS server is provisionned with the test content.
Test Procedure	1. In the Terminal select WAP browser.
	2. Select the SCWS test portal link (eg http:/localhost:3516/index.html)
	3. Select link "Test uri (length, escaped, …)"
	4. Select link "long directory name"
	5. Verify the pass criteria below.
Pass-Criteria	The "Hello long directory name" is displayed.

6.1.3.3 SCWS-1.0-int-202 escaped char

Test Case Id	SCWS-1.0-int-202
Test Object	Device, SCWS Client and SCWS Server.
Test Case Description	The purpose is to verify that uri with escaped char is correctly handled by server.
Specification Reference	[SCWS-TS] Chapter 5

SCR Reference	SCWS-C-001
	SCWS-S-003, SCWS-S-008, SCWS-S-009
	SCWS-ME-001
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, §6.1.4, [TEST_CONTENT]

Preconditions	• Equipment:
	  o Terminal
	  o Smartcard with SCWS server
	• Prerequisite for this test:
	  o SCWS server is provisionned with the test content.

Test Procedure	1. In the Terminal select WAP browser. 2. Select the SCWS test portal link (eg http:/localhost:3516/index.html) 3. Select link "Test uri (length, escaped, …)" 4. Select link "escaped char" 5. Verify the pass criteria below.
Pass-Criteria	The "Hello escaped char" is displayed.

6.1.3.4 SCWS-1.0-int-203 query string

Test Case Id	SCWS-1.0-int-203
Test Object	Device, SCWS Client and SCWS Server.
Test Case Description	The purpose is to verify that uri with query string is correctly handled by server.
Specification Reference	[SCWS-TS] Chapter 5
SCR Reference	SCWS-C-001
	SCWS-S-003, SCWS-S-008, SCWS-S-009
	SCWS-ME-001
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, §6.1.4, [TEST_CONTENT]

Preconditions	• Equipment:
	  o Terminal
	  o Smartcard with SCWS server
	• Prerequisite for this test:
	  o SCWS server is provisionned with the test content.

Test Procedure	1. In the Terminal select WAP browser. 2. Select the SCWS test portal link (eg http:/localhost:3516/index.html) 3. Select link "Test uri (length, escaped, …)" 4. Select link "query string" 5. Verify the pass criteria below.
Pass-Criteria	The "Hello query string" is displayed.

6.1.3.5 SCWS-1.0-int-204 uri long (1024 bytes)

Test Case Id	SCWS-1.0-int-204
Test Object	Device, SCWS Client and SCWS Server.

Test Case Description	The purpose is to verify that uri of 1024 bytes is correctly handled by server.
Specification Reference	[SCWS-TS] Chapter 5
SCR Reference	SCWS-C-001
	SCWS-S-001, SCWS-S-003, SCWS-S-008, SCWS-S-009
	SCWS-ME-001
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, §6.1.4, [TEST_CONTENT]

Preconditions	• Equipment:
	    o Terminal
	    o Smartcard with SCWS server
	• Prerequisite for this test:
	    o SCWS server is provisionned with the test content.

Test Procedure	1. In the Terminal select WAP browser. 2. Select the SCWS test portal link (eg http:/localhost:3516/index.html) 3. Select link "Test uri (length, escaped, …)" 4. Select link "uri long (1024 bytes)" 5. Verify the pass criteria below.
Pass-Criteria	The "Hello uri long" is displayed.

6.1.3.6 SCWS-1.0-int-205 Uri Not Found

Test Case Id	SCWS-1.0-int-205
Test Object	Device, SCWS Client and SCWS Server.
Test Case Description	The purpose is to verify that not found uri is correctly handled by client and server.
Specification Reference	[SCWS-TS] Chapter 5
SCR Reference	SCWS-C-001
	SCWS-S-003, SCWS-S-008, SCWS-S-009
	SCWS-ME-001
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, §6.1.4, [TEST_CONTENT]

Preconditions	• Equipment:
	    o Terminal
	    o Smartcard with SCWS server
	• Prerequisite for this test:
	    o SCWS server is provisioned with the test content.

Test Procedure	1. In the Terminal select WAP browser. 2. Select the SCWS test portal link (eg http:/localhost:3516/index.html) 3. Select link "Test uri (length, escaped, …)" 4. Select link "not found" 5. Verify the pass criteria below.
Pass-Criteria	404 Not Found error message is displayed.

6.1.3.7   SCWS-1.0-int-206 5 directory levels

Test Case Id	SCWS-1.0-int-206
Test Object	Device, SCWS Client and SCWS Server.
Test Case Description	The purpose is to verify that uri 5 levels of directory is correctly handled by server.
Specification Reference	[SCWS-TS] Chapter 5
SCR Reference	SCWS-C-001 SCWS-S-001, SCWS-S-003, SCWS-S-008, SCWS-S-009 SCWS-ME-001
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, §6.1.4, [TEST_CONTENT]

Preconditions	• Equipment:
	  o Terminal
	  o Smartcard with SCWS server
	• Prerequisite for this test:
	  o SCWS server is provisionned with the test content.

Test Procedure	1. In the Terminal select WAP browser. 2. Select the SCWS test portal link (eg http:/localhost:3516/index.html) 3. Select link "Test uri (length, escaped, …)" 4. Select link "5 levels directory" 5. Verify the pass criteria below.
Pass-Criteria	The "Hello 5 directory levels" is displayed.

6.1.4   Protection test group

6.1.4.1   SCWS-1.0-int-250 http basic authentication

Test Case Id	SCWS-1.0-int-250
Test Object	Device, SCWS Client and SCWS Server.
Test Case Description	The purpose is to verify that http basic authentication is correctly handled by client and server. This test case will test HTTP status-code '401 Unauthorized', HTTP response header 'WWW-Authenticate' and HTTP request header 'Authorization'.
Specification Reference	[SCWS-TS] Chapter 9.3 [SCWS-TS] Chapter 10
SCR Reference	SCWS-C-001 SCWS-S-003, SCWS-S-008, SCWS-S-009, SCWS-S-013, SCWS-S-014, SCWS-S-015 SCWS-ME-001
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, §6.1.5, [TEST_CONTENT]

Preconditions	• Equipment:
	o Terminal
	o Smartcard with SCWS server
	• Prerequisite for this test:
	o SCWS server is provisionned with the test content.
	o SCWS server is configured with security rules.
Test Procedure	1. In the Terminal select WAP browser.
	2. Select the SCWS test portal link (eg http:/localhost:3516/index.html)
	3. Select link "Test protection (basic auth, admin)"
	4. Select link "http basic authentication"
	5. User is asked to enter login and password.
	6. Enter wrong credential.
	7. Authentcation failed, resource basic.html is not accessible.
	8. Verify the pass criteria 1.
	9. Enter valid credential login "omauser" password "omapwdr".
	10. Verify the pass criteria 2.
Pass-Criteria	
	1. Ressources basic.html is NOT displayed.
	2. Ressources basic.html is displayed.

6.1.4.2   SCWS-1.0-int-251 admin protection

Test Case Id	SCWS-1.0-int-251
Test Object	Device, SCWS Client and SCWS Server.
Test Case Description	The purpose is to verify that resource protected by admin protection is not accessible throught WAP Browser. This test case will test HTTP status-code '403 Forbiden'.
Specification Reference	[SCWS-TS] Chapter 13.5.1.2
SCR Reference	SCWS-C-001
	SCWS-S-003, SCWS-S-008, SCWS-S-009
	SCWS-ME-001
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, §6.1.5, [TEST_CONTENT]
Preconditions	• Equipment:
	o Terminal
	o Smartcard with SCWS server
	• Prerequisite for this test:
	o SCWS server is provisionned with the test content.
	o SCWS server is configured with security rules.

Test Procedure	1. In the Terminal select WAP browser.
	2. Select the SCWS test portal link (eg http:/localhost:3516/index.html)
	3. Select link "Test protection (basic auth, admin)"
	4. Select link "admin protocol"
	5. Verify the pass criteria below.
Pass-Criteria	403 Forbiden error message is displayed.

6.1.5   Dynamic content test group

6.1.5.1   SCWS-1.0-int-300 form post method

Test Case Id	SCWS-1.0-int-300
Test Object	Device, SCWS Client and SCWS Server.
Test Case Description	The purpose is to verify that server dynamic content application is correctly triggered on HTTP POST method. This test case will test htpp POST message with content-body handle by dynamic content application.
Specification Reference	[SCWS-TS] Chapter 6
SCR Reference	SCWS-C-001
	SCWS-S-002, SCWS-S-003, SCWS-S-008, SCWS-S-009, SCWS-S-011
	SCWS-ME-001
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, §6.1.6, §6.3.2 [TEST_CONTENT]
Preconditions	• Equipment:
	o Terminal
	o Smartcard with SCWS server
	• Prerequisite for this test:
	o SCWS server is provisionned with the test content.
	o Dynamic content application is loaded / installed on the Smartcard.
Test Procedure	1. In the Terminal select WAP browser.
	2. Select the SCWS test portal link (eg http:/localhost:3516/index.html)
	3. Select link "Test Dynamic Content"
	4. Select link "Test form post method"
	5. Enter your name in the form then select button "do post"
	6. Verify the pass criteria below.
Pass-Criteria	"Hello" + name that you have entered are displayed.

6.1.5.2   SCWS-1.0-int-301 form get method

Test Case Id	SCWS-1.0-int-301
Test Object	Device, SCWS Client and SCWS Server.
Test Case Description	The purpose is to verify that server dynamic content application is correctly triggered on HTTP GET method. This test case will test http GET message with query-string handle by dynamic content application.
Specification Reference	[SCWS-TS] Chapter 6

SCR Reference	SCWS-C-001
	SCWS-S-002, SCWS-S-003, SCWS-S-008, SCWS-S-009
	SCWS-ME-001
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, §6.1.6, §6.3.2, [TEST_CONTENT]

Preconditions	• Equipment:
	    o Terminal
	    o Smartcard with SCWS server
	• Prerequisite for this test:
	    o SCWS server is provisionned with the test content.
	    o Dynamic content application is loaded / installed on the Smartcard.

Test Procedure	1. In the Terminal select WAP browser. 2. Select the SCWS test portal link (eg http:/localhost:3516/index.html) 3. Select link "Test Dynamic Content" 4. Select link "Test form get method" 5. Enter your name in the form then select button "do get". 6. Verify the pass criteria below.
Pass-Criteria	"Hello" + name that you have entered are displayed.

6.1.5.3 SCWS-1.0-int-302 post unexistant ressource

Test Case Id	SCWS-1.0-int-302
Test Object	Device, SCWS Client and SCWS Server.
Test Case Description	The purpose is to verify that server response error 404 not found on an http request POST with an unxeistant uri.
Specification Reference	[SCWS-TS] Chapter 6
SCR Reference	SCWS-C-001
	SCWS-S-003, SCWS-S-008, SCWS-S-009, SCWS-S-011
	SCWS-ME-001
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, §6.1.6, §6.3.2, [TEST_CONTENT]

Preconditions	• Equipment:
	    o Terminal
	    o Smartcard with SCWS server
	• Prerequisite for this test:
	    o SCWS server is provisionned with the test content.

Test Procedure	1. In the Terminal select WAP browser. 2. Select the SCWS test portal link (eg http:/localhost:3516/index.html) 3. Select link "Test Dynamic Content" 4. Select link "Test post unexistant ressources" 5. Select button "ok". 6. Verify the pass criteria below.
Pass-Criteria	404 Not Found error message is displayed.

6.1.5.4   SCWS-1.0-int-303 chuncked response

Test Case Id	SCWS-1.0-int-303
Test Object	Device, SCWS Client and SCWS Server.
Test Case Description	The purpose is to verify that dynamic content application response with HTTP Header "Transfert-Encoding: chuncked" is correctly processed by Device, SCWS Client.
Specification Reference	[SCWS-TS] Chapter 6
SCR Reference	SCWS-C-001 SCWS-S-002, SCWS-S-003, SCWS-S-008, SCWS-S-009, SCWS-S-011 SCWS-ME-001
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, §6.1.6, §6.3.2, [TEST_CONTENT]

Preconditions	• Equipment:
	    o Terminal
	    o Smartcard with SCWS server
	 • Prerequisite for this test:
	    o SCWS server is provisionned with the test content.
	    o Dynamic content application is loaded/ installed on the Smartcard.

Test Procedure	1. In the Terminal select WAP browser. 2. Select the SCWS test portal link (eg http:/localhost:3516/index.html) 3. Select link "Test Dynamic Content" 4. Select link "Test chuncked response" 5. Select button "ok". 6. Verify the pass criteria below.
Pass-Criteria	"Hello World" is displayed.

6.1.5.5   SCWS-1.0-int-304 form get method with special char in query string

Test Case Id	SCWS-1.0-int-304
Test Object	Device, SCWS Client and SCWS Server.
Test Case Description	The purpose is to verify that server dynamic content application is correctly triggered on HTTP GET method and query-string with special char is correctly handled by dynamic content application.
Specification Reference	[SCWS-TS] Chapter 6
SCR Reference	SCWS-C-001 SCWS-S-002, SCWS-S-003, SCWS-S-008, SCWS-S-009 SCWS-ME-001
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, §6.1.6, §6.3.2, [TEST_CONTENT]

Preconditions	• Equipment:
	    o Terminal
	    o Smartcard with SCWS server
	• Prerequisite for this test:
	    o SCWS server is provisionned with the test content.
	    o Dynamic content application is loaded / installed on the Smartcard.

Test Procedure	7. In the Terminal select WAP browser. 8. Select the SCWS test portal link (eg http:/localhost:3516/index.html) 9. Select link "Test Dynamic Content" 10. Select link "Test form get method" 11. Enter '/a?2&a=b' in the formulare then select button "do get". 12. Verify the pass criteria below.
Pass-Criteria	"Hello /a?2&a=b" is displayed.

6.1.5.6   SCWS-1.0-int-305 get send SMS

Test Case Id	SCWS-1.0-int-305
Test Object	Device, SCWS Client and SCWS Server.
Test Case Description	The purpose is to verify that server dynamic content application is correctly sending an SMS to another handset.
Specification Reference	[SCWS-TS] Chapter 6
SCR Reference	SCWS-C-001 SCWS-S-002, SCWS-S-003, SCWS-S-008, SCWS-S-009, SCWS-S-011 SCWS-ME-001
Tool	
Test code	

Preconditions	• Equipment:
	    o 2 Terminals A&B
	    o Smartcard with SCWS server
	• Prerequisite for this test:
	    o SCWS server is provisioned with test portal.
	    o Dynamic content application is loaded/ installed on the Smartcard.

Test Procedure	13. In the Terminal A select WAP browser. 14. Select the SCWS test portal link (eg http:/localhost:3516/index.html) 15. Select link "Test Dynamic Content" 16. Select link "Test send SMS" 17. Fill up form with the phone number of the Terminal B. 18. Fill up form with the text message to send. 19. Select button "ok". 8. Verify the pass criteria below.
Pass-Criteria	The SMS content is displayed in Terminal B.

6.2   Remote Administration of SCWS

6.2.1   Portal administration test group

The following tests use the full admin protocol.

6.2.1.1   SCWS-1.0-int-500 single resource small size

Test Case Id	SCWS-1.0-int-500
Test Object	Remote admin SCWS Server, SCWS admin client.
Test Case Description	The purpose is to verify single resource 1kb (portal 'oma-500')can be sent, received throught full admin protocol.
Specification Reference	[SCWS-TS] Chapter 13.3.2 [SCWS-TS] Chapter 13.1
SCR Reference	SCWS-AC-001, SCWS-AC-004, SCWS-AC-005, SCWS-AC-007, SCWS-AC-010 SCWS-AS-001, SCWS-AS-004, SCWS-AS-005 SCWS-S-012, SCWS-S-022
Tool	
Test code	[TEST_CONTENT_DESC §], [TEST_CONTENT]

Preconditions	• Equipment:
	    o Terminal
	    o Smartcard with SCWS server and SCWS admin client
	    o Remote admin SCWS Server
	• Prerequisite for this test:
	    o Smartcard card administration agent is configured with remote admin SCWS Server parameters (ip-address, port...).
	    o

Test Procedure	1. In Remote admin SCWS Server, select Terminal destination address. 2. In Remote admin SCWS Server, select portal 'oma-500'.. 3. In Remote admin SCWS Server, start the download then wait download finished. 4. In Terminal, select WAP browser. 5. Select the SCWS test portal link (eg http:/localhost:3516/index.html) 6. Verify the pass criteria below.
Pass-Criteria	In Terminal WAP browser, the new download resource (portal 'oma-500') is displayed.

6.2.1.2   SCWS-1.0-int-501 single resource large size

Test Case Id	SCWS-1.0-int-501
Test Object	Remote admin SCWS Server, SCWS admin client.
Test Case Description	The purpose is to verify single resource 10kb (portal 'oma-501') can be sent, received throught full admin protocol. This test case will test POST response of remote admin server with HTTP header 'Transfert-Encoding: chuncked'.
Specification Reference	[SCWS-TS] Chapter 13.3.2 [SCWS-TS] Chapter 13.1

SCR Reference	SCWS-AC-001, SCWS-AC-004, SCWS-AC-005, SCWS-AC-007, SCWS-AC-010
	SCWS-AS-001, SCWS-AS-004, SCWS-AS-005
	SCWS-S-012, SCWS-S-022
Tool	
Test code	[TEST_CONTENT_DESC], [TEST_CONTENT]

Preconditions	• Equipment:
	    o Terminal
	    o Smartcard with SCWS server and SCWS admin client
	    o Remote admin SCWS Server
	• Prerequisite for this test:
	    o Smartcard card administration agent is configured with remote admin SCWS Server parameters (ip-address, port...).
	    o

Test Procedure	1. In Remote admin SCWS Server, select Terminal destination address. 2. In Remote admin SCWS Server, select portal 'oma-501'.. 3. In Remote admin SCWS Server, start the download then wait download finished. 4. In Terminal, select WAP browser. 5. Select the SCWS test portal link (eg http:/localhost:3516/index.html) 6. Verify the pass criteria below.
Pass-Criteria	In Terminal WAP browser, the new download resource (portal 'oma-501') is displayed.

6.2.1.3   SCWS-1.0-int-502 multiple resources total size 32kb

Test Case Id	SCWS-1.0-int-502
Test Object	Remote admin SCWS Server, SCWS admin client.
Test Case Description	The purpose is to verify that portal of 32kb (portal 'oma-502') with multiple resources can be sent, received throught full admin protocol. This portal contains 2 different pages: - Page 1 with 4 images of 5kb. - Page 2 with 6 images of 2kb. This test case will test POST response of remote admin server with pipelined administration command.
Specification Reference	[SCWS-TS] Chapter 13.3.2
	[SCWS-TS] Chapter 13.1
SCR Reference	SCWS-AC-001, SCWS-AC-004, SCWS-AC-005, SCWS-AC-007, SCWS-AC-010
	SCWS-AS-001, SCWS-AS-004, SCWS-AS-005
	SCWS-S-012, SCWS-S-022
Tool	
Test code	[TEST_CONTENT_DESC] §6.2.1, [TEST_CONTENT]

Preconditions	• Equipment:
	     o Terminal
	     o Smartcard with SCWS server and SCWS admin client
	     o Remote admin SCWS Server
	• Prerequisite for this test:
	     o Smartcard card administration agent is configured with remote admin SCWS Server parameters (ip-address, port...).
	     o

Test Procedure	1. In Remote admin SCWS Server, select Terminal destination address. 2. In Remote admin SCWS Server, select portal 'oma-502'. 3. In Remote admin SCWS Server, start then wait download finished. 4. In Terminal, select WAP browser. 5. In WAP browser, select the SCWS test portal link (eg http:/localhost:3516/index.html) 6. Verify the pass criteria below.
Pass-Criteria	In Terminal WAP browser, the new download resource (portal 'oma-502') is displayed. -In WAP browser, select page 1, verify that 4 images are displayed.- In WAP browser, select page 2, verify that 6 images are displayed.

6.2.1.4   SCWS-1.0-int-503 multiple resources total size 100kb

Test Case Id	SCWS-1.0-int-503
Test Object	Remote admin SCWS Server, SCWS admin client.
Test Case Description	The purpose is to verify that portal of 100kb (portal 'oma-503') with multiple resources can be sent, received throught full admin protocol. This portal contains 3 different pages: - Page 1 with 2 images of 18kb. - Page 2 with 8 images of 5kb. - Page 3 with 12 images of 2kb. This test case will test POST response of remote admin server with pipelined administration command and and with HTTP header 'Transfert-Encoding: chuncked'.
Specification Reference	[SCWS-TS] Chapter 13.3.2 [SCWS-TS] Chapter 13.1
SCR Reference	SCWS-AC-001, SCWS-AC-004, SCWS-AC-005, SCWS-AC-007, SCWS-AC-010 SCWS-AS-001, SCWS-AS-004, SCWS-AS-005 SCWS-S-012, SCWS-S-022
Tool	
Test code	[TEST_CONTENT_DESC] §6.2.2, [TEST_CONTENT]

Preconditions	• Equipment:
	    o Terminal
	    o Smartcard with SCWS server and SCWS admin client
	    o Remote admin SCWS Server
	• Prerequisite for this test:
	    o Smartcard card administration agent is configured with remote admin SCWS Server parameters (ip-address, port...).
	    o

Test Procedure	1. In Remote admin SCWS Server, select Terminal destination address. 2. In Remote admin SCWS Server, select portal 'oma-503'. 3. In Remote admin SCWS Server, start then wait download finished. 4. In Terminal, select WAP browser. 5. In WAP browser, select the SCWS test portal link (eg http:/localhost:3516/index.html) 6. Verify the pass criteria below.
Pass-Criteria	In Terminal WAP browser, the new download resource (portal 'oma-503') is displayed. - In WAP browser, select page 1, verify that 2 images are displayed- In WAP browser, select page 2, verify that 8 images are displayed.- In WAP browser, select page 3, verify that 12 images are displayed.

6.2.2   Connectivity test group

6.2.2.1   SCWS-1.0-int-551 administration session with terminal switched-off

Test Case Id	SCWS-1.0-int-551
Test Object	Remote admin SCWS Server, SCWS admin client.
Test Case Description	The purpose is to verify that SCWS admin client retry administration session when the current admin session is interrupted by terminal switch-off. This test case will test admin client POST request with HTTP header 'SCWS-resume: true'.
Specification Reference	[SCWS-TS] Chapter 13.3.2.8
SCR Reference	SCWS-AC-001, SCWS-AC-004, SCWS-AC-005, SCWS-AC-007, SCWS-AC-010, SCWS-AC-008 SCWS-AS-001, SCWS-AS-004, SCWS-AS-005 SCWS-S-012, SCWS-S-022
Tool	
Test code	[TEST_CONTENT_DESC] §6.2.1, [TEST_CONTENT]

Preconditions	• Equipment:
	    o Terminal
	    o Smartcard with SCWS server and SCWS admin client
	    o Remote admin SCWS Server
	• Prerequisite for this test:
	    o Smartcard card administration agent is configured with remote admin SCWS Server parameters (ip-address, port...).
	    o The Connection parameters (BIP OPEN CHANNEL TLV) must included an AlhaIdentifier "open remote connection".

Test Procedure	1. In Remote admin SCWS Server, select Terminal destination address. 2. In Remote admin SCWS Server, select portal 'oma-551'. 3. In Remote admin SCWS Server, start portal update. 4. In the Terminal when "open remote connection" message was displayed switch-off the Terminal. 5. Switch-on the Terminal. 6. SCWS admin client shall start the retry policy. The termial is updated from the suspended command to update the portal. 7. Wait SCWS admin client retry policy expiration delay. 8. In WAP browser, select the SCWS test portal link (eg http:/localhost:3516/index.html) 9. Verify the pass criteria below.
Pass-Criteria	1. The portal 'oma-551' is displayed. On Terminal switch-on the suspended action occurs and the SCWS is updated. . 2.

6.2.2.2 SCWS-1.0-int-552 administration session with network coverage loss

Test Case Id	SCWS-1.0-int-552
Test Object	Remote admin SCWS Server, SCWS admin client.
Test Case Description	The purpose is to verify that SCWS admin client retry administration session when the current admin session is interrupted by network coverage loss. This test case will test SCWS admin client resume admin session, BIP event channel status link-dropped, BIP commad SEND_DATA, RECEIVED_DATA terminal response temporary-error or permanent-error.
Specification Reference	[SCWS-TS] Chapter 13.3.2.8
SCR Reference	SCWS-AC-001, SCWS-AC-004, SCWS-AC-005, SCWS-AC-007, SCWS-AC-010, SCWS-AC-008 SCWS-AS-001, SCWS-AS-004, SCWS-AS-005 SCWS-S-012, SCWS-S-022
Tool	
Test code	[TEST_CONTENT_DESC] §6.2.1, [TEST_CONTENT]

Preconditions	- Equipment: - Terminal - Smartcard with SCWS server and SCWS admin client - Remote admin SCWS Server - Annecoic chamber / Faraday cage. - Prerequisite for this test: - Smartcard card administration agent is configured with remote admin SCWS Server parameters (ip-address, port...). - The Connection parameters (BIP OPEN CHANNEL TLV) must included an AlhaIdentifier "open remote connection".
Test Procedure	1. In Remote admin SCWS Server, select Terminal destination address. 2. In Remote admin SCWS Server, select portal 'oma-552'. 3. In Remote admin SCWS Server, start portal update. 4. In the Terminal when "open remote connection" message was displayed then the network connection is loss using Annecoic chamber / Faraday cage 5. SCWS admin client shall start the retry policy. 6. Netwotk connection is re-established. 7. Wait SCWS admin client retry policy expiration delay. 8. In WAP browser, select the SCWS test portal link (eg http:/localhost:3516/index.html) 9. Verify the pass criteria below.
Pass-Criteria	The portal 'oma-552' is displayed.When the network connection is resumed the suspended action occurs and the SCWS is updated.

6.2.2.3 SCWS-1.0-int-553 administration session is abandoned

Test Case Id	SCWS-1.0-int-553
Test Object	Remote admin SCWS Server, SCWS admin client.
Test Case Description	The purpose is to verify that SCWS admin client sent SMS MO admin-failure-report to the Remote admin SCWS Server when administration session is abandoned.
Specification Reference	[SCWS-TS] Chapter 13.3.2.8
SCR Reference	SCWS-AC-001, SCWS-AC-004, SCWS-AC-005, SCWS-AC-007, SCWS-AC-010, SCWS-AC-008, SCWS-AC-009 SCWS-AS-001, SCWS-AS-004, SCWS-AS-005 SCWS-S-012
Tool	
Test code	[TEST_CONTENT_DESC] §6.2.1, [TEST_CONTENT]

Preconditions	• Equipment:
	    ○ Terminal
	    ○ Smartcard with SCWS server and SCWS admin client
	    ○ Remote admin SCWS Server
	• Prerequisite for this test:
	    ○ Smartcard card administration agent is configured with remote admin SCWS Server parameters (ip-address, port...).
	    ○

Test Procedure	1. In Remote admin SCWS Server, enter wrong connection parameters for the push sms to the Terminal (e.g wrong tcp-ip adress). 2. In Remote admin SCWS Server, select Terminal destination address. 3. In Remote admin SCWS Server, select portal 'oma-553'. 4. In Remote admin SCWS Server, start portal update. 5. SCWS admin client try to establish connection with admin server. 6. This connection establishment should fail due to wrong parameters. 7. SCWS admin client retry X times after waiting delay Y to establish connection with admin server (X and Y is a admin client configuration parameters), the connection establishement failed X times. 8. SCWS admin client abandoned this administration session. 9. SCWS admin client sends SMS-MO admin-failure-report to the remote admin server.
Pass-Criteria	Remote admin SCWS Server received SMS-MO admin-failure-report with format specified in [SCWS-TS] § 13.3.2.9.8 , the error code is '01' open, channel error

6.2.2.4   SCWS-1.0-int-554 administration session and browsing

Test Case Id	SCWS-1.0-int-554
Test Object	Remote admin SCWS Server, SCWS admin client.
Test Case Description	The purpose is to verify that SCWS server connection is taken into account when receiving during admin client / remote admin server exchange. This test case will test reception of the BIP Event-Data-Available (channel http) during BIP admin-channel exchange.
Specification Reference	[SCWS-TS] Chapter 13.3.2
SCR Reference	SCWS-AC-001, SCWS-AC-004, SCWS-AC-005, SCWS-AC-007, SCWS-AC-010 SCWS-AS-001, SCWS-AS-004, SCWS-AS-005 SCWS-S-012, SCWS-S-022
Tool	
Test code	[TEST_CONTENT_DESC] §6.2.1 §6.1.1, [TEST_CONTENT]

Preconditions	• Equipment: 　　○ Terminal 　　○ Smartcard with SCWS server and SCWS admin client 　　○ Remote admin SCWS Server • Prerequisite for this test: 　　○ Smartcard card administration agent is confured with remote admin SCWS Server parameters (ip-address, port...). 　　○ SCWS server is provisionned with test portal.
Test Procedure	1. In Remote admin SCWS Server, select Terminal destination address. 2. In Remote admin SCWS Server, select portal 'oma-554'. 3. In Remote admin SCWS Server, start portal download. 4. Wait until connection establishement beween remote admin server and admin client. 5. In Terminal, select WAP browser. 6. Select the SCWS test portal link (eg http:/localhost:3516/index.html) 7. SCWS server home pages is displayed. 8. In Remote admin SCWS Server, wait download finished. 9. In Terminal, select WAP browser. 10. In WAP browser, select the SCWS test portal link (eg http:/localhost:3516/index.html) 11. Verify the pass criteria below.
Pass-Criteria	1. The portal 'oma-554' is displayed. 2.

6.2.2.5 SCWS-1.0-int-555 admin session and other CAT application

Test Case Id	SCWS-1.0-int-555
Test Object	Remote admin SCWS Server, SCWS admin client.
Test Case Description	The purpose is to verify that administration session is taken into account when card administration agent trigerring event (push sms) is received in other card application toolkit context.
Specification Reference	[SCWS-TS] Chapter 13.3.2
SCR Reference	SCWS-AC-001, SCWS-AC-004, SCWS-AC-005, SCWS-AC-007, SCWS-AC-010 SCWS-AS-001, SCWS-AS-004, SCWS-AS-005 SCWS-S-012, SCWS-S-022
Tool	
Test code	[TEST_CONTENT_DESC] §6.2.1, §6.3.1 [TEST_CONTENT]

Preconditions	- Equipment: - Terminal - Smartcard with SCWS server and SCWS admin client - Remote admin SCWS Server - Prerequisite for this test: - Smartcard card administration agent is configured with remote admin SCWS Server parameters (ip-address, port...). - SCWS server is provisionned with test portal. - Smartcard is provisioned with Card Application Toolkit (CAT) application. This CAT application is register on the SIM services menu and do a DISPLAY_TEXT proactive command on menu selection event.
Test Procedure	1. In the Terminal select SIM Services menu item "Hello". 2. In the Terminal, text "Hello World" is displayed. 3. In Remote admin SCWS Server, select Terminal destination address. 4. In Remote admin SCWS Server, select portal 'oma-555'. 5. In Remote admin SCWS Server, start portal download. 6. In Terminal, select button ok. 7. In Remote admin SCWS Server, wait download finished. 8. In Terminal, select WAP browser. 9. In WAP browser, select the SCWS test portal link (eg http:/localhost:3516/index.html) 10. Verify the pass criteria below.
Pass-Criteria	1. The portal 'oma-555' is displayed. 2.

6.2.2.6   SCWS-1.0-int-556 PUT_WITH_ENVELOPE

Test Case Id	SCWS-1.0-int-556
Test Object	Device, SCWS Client, SCWS Server
Test Case Description	The purpose is to verify that a SCWS admin session with PUT is correctly processed while the execution of the proactive command SET UP CALL is triggered by a SMS from the second terminal.
Specification Reference	[SCWS-TS] Chapter 8.1.1.1 SCWS and other CAT applications concurrency
SCR Reference	SCWS-AC-001, SCWS-AC-004, SCWS-AC-005, SCWS-AC-007, SCWS-AC-010 SCWS-AS-001, SCWS-AS-004, SCWS-AS-005 SCWS-S-012, SCWS-S-022
Tool	
Test code	CAT application on a UNFORMATTED_SMS_PP i.e. on this event the Applet performs a SET UP CALL proactive command.

Preconditions	- Equipment: - Terminal A and Terminal B capable of sending a SMS to the terminal hosting the SCWS - Smartcard with SCWS server, SCWS admin client and a CAT application registered on the SMS PP Data Download Event - Remote admin SCWS Server - Prerequisite for this test: - Smartcard card administration agent is configured with remote admin SCWS Server parameters (ip-address, port...). - SIM with a special CAT application executing SET UP CALL when triggered by a UNFORMATTED_SMS_PP event. - The connection parameters (BIP OPEN CHANNEL TLV) must included an Alpha Identifier "open remote connection".
Test Procedure	- In Remote admin SCWS Server , select Terminal A destination address - commanding Remote admin SCWS Server, select portal 'oma-556' - In Remote admin SCWS Server, start portal update. - In the Teminal when "open remote connection" message was displayed, then send SMS from Terminal B to Terminal A. - Verify the pass critera below.
Pass-Criteria	Verify that the SET UP CALL is performed and verify that the content 'oma-556' has been correctly stored on the SCWS.

6.2.3   TLS test group

6.2.3.1   SCWS-1.0-int-600 TLS_PSK_WITH_3DES_EDE_CBC_SHA

Test Case Id	SCWS-1.0-int-600
Test Object	Remote admin SCWS Server, SCWS admin client.
Test Case Description	The purpose is to verify that administration session is correctly processed using TLS communication channel using cipher suite TLS_PSK_WITH_3DES_EDE_CBC_SHA.
Specification Reference	[SCWS-TS] Chapter 11
SCR Reference	SCWS-AC-001, SCWS-AC-004, SCWS-AC-005, SCWS-AC-007, SCWS-AC-010, SCWS-AC-011, SCWS-AC-012 SCWS-AS-001, SCWS-AS-002, SCWS-AS-003, SCWS-AS-004, SCWS-AS-005 SCWS-S-012, SCWS-S-022
Tool	
Test code	[TEST_CONTENT_DESC] §6.2.1, [TEST_CONTENT]

Preconditions	• Equipment:
	    o Terminal
	    o Smartcard with SCWS server and SCWS admin client
	    o Remote admin SCWS Server
	• Prerequisite for this test:
	    o Smartcard card administration agent is configured with remote admin server parameters (ip-address, port...).
	    o Smartcard card administration agent and remote admin server is configure to process admin session throught TLS and cipher suite TLS_PSK_WITH_3DES_EDE_CBC_SHA.
	    o

Test Procedure	1. In Remote admin SCWS Server, select Terminal destination address. 2. In Remote admin SCWS Server, select portal 'oma-600'. 3. In Remote admin SCWS Server, start then wait download finished. 4. In Terminal, select WAP browser. 5. In WAP browser, select the SCWS test portal link (eg http:/localhost:3516/index.html) 6. Verify the pass criteria below.
Pass-Criteria	1. The portal 'oma-600' is displayed. 2.

6.2.3.2   SCWS-1.0-int-601 TLS_PSK_WITH_AES_128_CBC_SHA

Test Case Id	SCWS-1.0-int-601
Test Object	Remote admin SCWS Server, SCWS admin client.
Test Case Description	The purpose is to verify that administration session is correctly processed using TLS communication channel using cipher suite TLS_PSK_WITH_AES_128_CBC_SHA.
Specification Reference	[SCWS-TS] Chapter 11
SCR Reference	SCWS-AC-001, SCWS-AC-004, SCWS-AC-005, SCWS-AC-007, SCWS-AC-010, SCWS-AC-011, SCWS-AC-012 SCWS-AS-001, SCWS-AS-002, SCWS-AS-003, SCWS-AS-004, SCWS-AS-005 SCWS-S-012, SCWS-S-022
Tool	
Test code	[TEST_CONTENT_DESC] §6.2.1, [TEST_CONTENT]

Preconditions	• Equipment:
	o Terminal
	o Smartcard with SCWS server and SCWS admin client
	o Remote admin SCWS Server
	• Prerequisite for this test:
	o Smartcard card administration agent is configured with remote admin SCWS Server parameters (ip-address, port...).
	o Smartcard card administration agent and remote admin server is configure to process admin session throught TLS and cipher suite TLS_PSK_WITH_AES_128_CBC_SHA.
	o
Test Procedure	1. In Remote admin SCWS Server, select Terminal destination address.
	2. In Remote admin SCWS Server, select portal 'oma-601'.
	3. In Remote admin SCWS Server, start then wait download finished.
	4. In Terminal, select WAP browser.
	5. In WAP browser, select the SCWS test portal link (eg http:/localhost:3516/index.html)
	6. Verify the pass criteria below.
Pass-Criteria	1. The portal 'oma-601' is displayed.
	2.

6.2.4 Administration using lightweight protocol

6.2.4.1 SCWS-1.0-int-701 LIGHTWEIGHT and deactivation of the SCWS application

Test Case Id	SCWS-1.0-int-701
Test Object	Remote admin SCWS Server, SCWS admin client.
Test Case Description	The purpose is to deactivate the SCWS using the lightweight protocol. At the end the SCWS shall be reactivated.
Specification Reference	[SCWS-TS] Chapter 13.3.1 [SCWS-TS] Chapter 13.1
SCR Reference	SCWS-AS-006 SCWS-S-011, SCWS-S-022, SCWS-S-023
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, [TEST_CONTENT]
Preconditions	• Equipment:
	o Terminal
	o Smartcard with SCWS server and SCWS admin client
	o Remote admin SCWS Server
	• Prerequisite for this test:
	o SCWS server is provisioned with the test content.

Test Procedure	1. In Remote admin SCWS Server, select Terminal destination address. 2. In Remote admin SCWS Server, send a SMS with admin command to desactivate the SCWS. 3. In Terminal, select WAP browser. 4. Verify the pass criteria 1. 5. In Remote admin SCWS Server, send a SMS with admin command to reactivate the SCWS. 6. In Terminal, select WAP browser. 7. Verify the pass criteria 2.
Pass-Criteria	1. In WAP browser, select test portal link (eg http:/localhost:3516/index.html), verify that a Terminal error is displayed. 2. In WAP browser, select test portal link (eg http:/localhost:3516/index.html), verify that portal is displayed.

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-Smartcard_Web_Server-V1_0	02 July 2007	-	First draft

	26 July 2007	Appendix B
		Chapter
		6.1..5.6
			Incorporated CRs:
			  OMA-IOP-PRC-2007-0084
			  OMA-IOP-PRC-2007-0086

	26 Sep 2007	6.1.2.8 6.2.2.6	Incorporated CR: OMA-IOP-PRC-2007-0109
	18 Oct 2007	n/a	IOP WG agreed, ref # OMA-IOP-2007-0204R02-INP_SCWS_Candidate_Pending_Docs
Candidate Version OMA-ETS-Smartcard_Web_Server-V1_0	06 Nov 2007	n/a	Status changed to candidate. TP R&A 2007-10-24 to 2007-11-06, TP doc. ref # OMA-TP-2007-0439R01-INP_ETS_SCWS_V1_0_and_ETS_SCWS_Content_V1_0_for_candidate_Approval

Appendix B.   Settings for the Remote Administration tests (Normative)

B.1   Remote Admin server settings

These reference document should be completed according to the specifics of the corresponding Remote Admin server being used substituting the bold text with the appropriate parameters for that server. These values will be used to set up the cards properly or to integrate the Remote Admin server within the infrastructure of the operator.

When filled up by the Remote Admin server provider, this table will be forwarded to the Test Fest participants once they have register.

	Values	Remarks
IP address of the Remote Admin server	**xxx.xxx.xxx.xxx**	The IP address and the TCP port must be reachable by the mobile equipments. This means that the couple IP address and port number shall be recognized by the firewall of the network operator as outgoing traffic
TCP Port number of the Admin server	**xxxxx**	
Security Parameters of the full admin protocol session		
PSK identifier	**xxxxxxxxxxxxxxxx**	Identifier of the TLS Pre-Shared key value used for admin session
TLS Pre-Shared Key value	Key value is commonly shared by all the participants.	Value of the TLS Pre-Shared key value used for admin session. The value will be provided to the Test Fest participants once registered.
SMS-MO Failure Report		
TP-Destination address	**Xxxxxxxxxxxxxxx**	Destination Address of the Remote Admin server used to send the Admin session Failure Report
Agent HTTP post parameters		
administration host	**Xxxxxxxxxxxxxxx**	Content of the field host in the post request header
agent-ID	**Xxxxxxxxxxxxxxx**	Content of the field from in the post request header
administration URI	**Xxxxxxxxxxxxxxx**	URI used to send the post request

B.2   Network operator settings

These reference document should be completed according to the specifics of the corresponding network operator infrastructure being used substituting the bold text with the appropriate parameters for that network. These values will be used to set up the cards and the remote admin servers properly.

When filled up by the Network operator hosting the Test Fest, this table will be forwarded to the Test Fest participants once they have register, except the IMSI/KI values that may required specific delivery rules.

	Values	Remarks

APN of the network operator		
APN	Xxxxxxxxxxxxxxx	APN and associated login/password to setup the GSM/GPRS or UMTS/Data packet connection
Login	Xxxxxxxxxxxxxxx	
Password	Xxxxxxxxxxxxxxx	
IP addresses coming from the mobile equipment		
(Range of) IP addresses	Xxxxxxxxxxxxxxx	IP addresses or range of IP addresses (*) that will be potentially used by the mobile equipment (ME) to connect the Remote Admin server and subsequently the rules applied to allocate the IP addresses (dynamically) to the ME.
Rules applied	Xxxxxxxxxxxxxxx	(*) To limit the incoming access rules on the Remote Admin server, the range has to be reduced as much as possible.
SMSC connection		
Remark: a large account connection is required with the SMSC.		
IP address of the SMSC	Xxxxxxxxxxxxxxx	IP address and port number used for the large account connection.
Port number of the SMSC	Xxxxxxxxxxxxxxx	
Login	Xxxxxxxxxxxxxxx	Login/password if required
Password	Xxxxxxxxxxxxxxx	
Applicative protocol used (e.g. SMPP3.4)	Xxxxxxxxxxxxxxx	
VPN link between the SMSC and the Remote Admin server		
If a VPN is required by the network operator, the configuration of the VPN has to be set up according to the requirement of the Remote Admin Server		
SMS-MO Failure Report		
Service Center address	Xxxxxxxxxxxxxxx	Service Centre Address of the SMSC Remote Admin server used to send the Admin session Failure Report
Card subscription parameters		
IMSI	xxxxxxxxxxx	Value communicated just before the test fest
Ki	xxxxxxxxxxx	
Authentication Algorithm	xxxxxxxxxxx	

B.3 SCWS Admin client configuration

These reference document should be completed according to the specifics of the corresponding SCWS card being used substituting the bold text with the appropriate parameters for that card. These values will be used to set up the Remote Admin servers.

When filled up by the smart card provider, this table will be forwarded to the Test Fest participants once they have register.

	Values	Remarks
Lightweight administration protocol		
SCWS server TAR	TAR value is commonly shared by all the participants.	The TAR value will be provided to the Test Fest participants once registered.
Security settings	SPI='000000' Kic='00' Kid='00'	No security
Full administration protocol		
TAR used for the Push SMS	TAR value is commonly shared by all the participants.	The TAR value will be provided to the Test Fest participants once registered.
Security settings of the Push SMS	SPI='000000' Kic='00' Kid='00'	No security
TLS Pre-Shared key value	Key value is commonly shared by all the participants.	Value of the TLS Pre-Shared key value used for admin session. The value will be provided to the Test Fest participants once registered.
URI of the default configuration resource	**XXXXXXXXXXXX**	
Default configuration resource for the full administration protocol		
Connection parameters using the BIP		
Bearer Description	02 02 04 03 05 1F 02	Value defined according to 3GPP TS 51.010-1 to generate most of PDP-contexts
Buffer size	1422 bytes	
APN	See Annex B.2	Depends on the network configuration
Login	See Annex B.2	
Password	See Annex B.2	
Port number of the Remote Admin server	See Annex B.1	Depends on the remote admin server configuration
IP Address of the Remote Admin server	See Annex B.1	
Security parameters		
PSK Identifier	See Annex B.1	Depends on the remote admin server configuration
Card Key Identifier	**xxxxxxxxxxxx**	

Retry policy parameters		
Retry counter	2	
Retry Delay	20s	
Retry Failure Report SMS MO		
TP Destination address	See Annex B.1	Address of the remote admin server configuration
TP Service Center address	See Annex B.2	Address of the SMSC
Alpha identifier	"Error"	
Agent HTTP post parameters		
administration host	See Annex B.1	Depends on the remote admin server configuration
agent-ID	See Annex B.1	Depends on the remote admin server configuration
administration URI	See Annex B.1	Depends on the remote admin server configuration