



Enabler Test Specification for Smartcard Web Server

Candidate Version 1.2 – 11 Oct 2011

Open Mobile Alliance
OMA-ETS-Smartcard_Web_Server-V1_2-20111011-C

Use of this document is subject to all of the terms and conditions of the Use Agreement located at <http://www.openmobilealliance.org/UseAgreement.html>.

Unless this document is clearly designated as an approved specification, this document is a work in process, is not an approved Open Mobile Alliance™ specification, and is subject to revision or removal without notice.

You may use this document or any part of the document for internal or educational purposes only, provided you do not modify, edit or take out of context the information in this document in any manner. Information contained in this document may be used, at your sole risk, for any purposes. You may not use this document in any other manner without the prior written permission of the Open Mobile Alliance. The Open Mobile Alliance authorizes you to copy this document, provided that you retain all copyright and other proprietary notices contained in the original materials on any copies of the materials and that you comply strictly with these terms. This copyright permission does not constitute an endorsement of the products or services. The Open Mobile Alliance assumes no responsibility for errors or omissions in this document.

Each Open Mobile Alliance member has agreed to use reasonable endeavors to inform the Open Mobile Alliance in a timely manner of Essential IPR as it becomes aware that the Essential IPR is related to the prepared or published specification. However, the members do not have an obligation to conduct IPR searches. The declared Essential IPR is publicly available to members and non-members of the Open Mobile Alliance and may be found on the “OMA IPR Declarations” list at <http://www.openmobilealliance.org/ipr.html>. The Open Mobile Alliance has not conducted an independent IPR review of this document and the information contained herein, and makes no representations or warranties regarding third party IPR, including without limitation patents, copyrights or trade secret rights. This document may contain inventions for which you must obtain licenses from third parties before making, using or selling the inventions. Defined terms above are set forth in the schedule to the Open Mobile Alliance Application Form.

NO REPRESENTATIONS OR WARRANTIES (WHETHER EXPRESS OR IMPLIED) ARE MADE BY THE OPEN MOBILE ALLIANCE OR ANY OPEN MOBILE ALLIANCE MEMBER OR ITS AFFILIATES REGARDING ANY OF THE IPR'S REPRESENTED ON THE “OMA IPR DECLARATIONS” LIST, INCLUDING, BUT NOT LIMITED TO THE ACCURACY, COMPLETENESS, VALIDITY OR RELEVANCE OF THE INFORMATION OR WHETHER OR NOT SUCH RIGHTS ARE ESSENTIAL OR NON-ESSENTIAL.

THE OPEN MOBILE ALLIANCE IS NOT LIABLE FOR AND HEREBY DISCLAIMS ANY DIRECT, INDIRECT, PUNITIVE, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES ARISING OUT OF OR IN CONNECTION WITH THE USE OF DOCUMENTS AND THE INFORMATION CONTAINED IN THE DOCUMENTS.

© 2011 Open Mobile Alliance Ltd. All Rights Reserved.

Used with the permission of the Open Mobile Alliance Ltd. under the terms set forth above.

Contents

1. SCOPE	4
2. REFERENCES	5
2.1 NORMATIVE REFERENCES	5
2.2 INFORMATIVE REFERENCES	6
3. TERMINOLOGY AND CONVENTIONS	7
3.1 CONVENTIONS	7
3.2 DEFINITIONS	7
3.3 ABBREVIATIONS	8
4. INTRODUCTION	9
5. SMARTCARD WEB SERVER CONFORMANCE TEST CASES	10
6. SMARTCARD WEB SERVER INTEROPERABILITY TEST CASES	11
6.1 SCWS CLIENT TO SCWS SERVER	11
6.1.1 Content typ and content length test group.....	11
6.1.2 Connectivity test group.....	14
6.1.3 URI test group.....	21
6.1.4 Protection test group.....	26
6.1.5 Dynamic content test group.....	28
6.1.6 Transport protocol test group.....	32
6.1.7 Access Control Policy test group.....	34
6.2 REMOTE ADMINISTRATION OF SCWS	37
6.2.1 Portal administration test group.....	37
6.2.2 Connectivity test group.....	48
6.2.3 TLS test group.....	54
6.2.4 Administration using lightweight protocol.....	65
6.2.5 Transport protocol test group.....	66
6.2.6 Backward Compatibility.....	68
6.2.7 Administration Triggering test group.....	70
APPENDIX A. CHANGE HISTORY (INFORMATIVE)	75
A.1 APPROVED VERSION HISTORY	75
A.2 DRAFT/CANDIDATE VERSION 1.2 HISTORY	75
APPENDIX B. SETTINGS FOR THE REMOTE ADMINISTRATION TESTS (INFORMATIVE)	76
B.1 REMOTE ADMIN SERVER SETTINGS	76
B.2 NETWORK OPERATOR SETTINGS	76
B.3 SCWS ADMIN CLIENT CONFIGURATION	78

1. Scope

This document describes in detail available test cases for Smartcard Web Server 1.2, <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 implementations of the specifications work satisfactory.

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

2. References

2.1 Normative References

- [3GPP 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/
- [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 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/
- [3GPP 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/
- [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] “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/>
- [3GPP2 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
- [3GPP2 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
- [ASN.1] Abstract Syntax Notation One, URL: <http://www.itu.int/ITU-T/studygroups/com17/languages>
- [ETSI TR 102 216] “TR 102 216 Technical Report Smart Cards; Vocabulary for Smart Card Platform specifications”, v3.0.0, European Telecommunications Standards Institute (ETSI), URL: <http://www.etsi.org>
- [ETSI 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>
- [ETSI TS 102 223] “TS 102 223 Technical Specification Smart cards; Card Application Toolkit (CAT)”, R7 or higher, European Telecommunications Standards Institute (ETSI), URL: <http://www.etsi.org>
- [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 1.6, Open Mobile Alliance™, OMA-IOP-Process-V1_6, 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, 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/rfc3546.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
[SCWS-AD]	“SCWS Architecture”, Version 1.2, Open Mobile Alliance™, OMA-AD-Smartcard_Web_Server-V1_2, URL: http://www.openmobilealliance.org/
[SCWS-ETR]	“SCWS Enabler Test Requirements” Version 1.2, Open Mobile Alliance™, OMA-ETR-Smartcard_Web_Server-V1_2, URL: http://www.openmobilealliance.org/
[SCWS-RD]	“SCWS Requirements”, Version 1.2, Open Mobile Alliance™, OMA-RD-Smartcard_Web_Server-V1_2, URL: http://www.openmobilealliance.org/
[SCWS-TS]	“SCWS Technical Specification”, Version 1.2, Open Mobile Alliance™, OMA-TS-Smartcard-Web-Server-V1_2, URL: http://www.openmobilealliance.org/
[SCWS-TFP]	“SCWS Test Files Package”, Version 1.2, Open Mobile Alliance™, OMA-TFP-Smartcard-Web-Server-V1_2, URL: http://www.openmobilealliance.org/
[TLS]	“Security Transport Protocol”, RFC 2246, January 1999, URL: http://www.ietf.org/rfc/rfc2246.txt
[WAPCert]	“WAP Certificate and CRL Profiles”, WAP Forum™, WAP-211-WAPCert, URL: http://www.openmobilealliance.org/
[WAPWAE]	“Wireless Application Environment Specification”, Version 2.3, 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/

2.2 Informative References

[OMADICT]	“Dictionary for OMA Specifications”, Version 2.7, Open Mobile Alliance™, OMA-ORG-Dictionary-V2_7, URL: http://www.openmobilealliance.org/
[SCWS WID]	Smartcard web server work item (WID 0196)

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 [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.
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 [ETSI 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). In addition, the Smart Card refers to the smart card definition of [ETSI TR 102 216].

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 [ETSI 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 1.2.

The implementation of some features is optional for the SCWS Clients and/or the SCWS Servers and/or the SCWS Remote Admin Servers in the Smartcard Web Server Enabler. The tests associated with these optional features are marked as "(Includes Optional Features)" in the test specification.

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 typ and content length test group

6.1.1.1 SCWS-1.2-int-001: gif image of small size

Test Case Id	SCWS-1.2-int-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-M SCWS-S-003-M, SCWS-S-008-M, SCWS-S-009-M SCWS-ME-001-M
ETR Reference	C_M_01, S_M_01, S_M_03, S_M_05, S_M_06, D_M_01, D_O_01.
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, §6.1.2, [TEST_CONTENT]
Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server • Prerequisite for this test: <ul style="list-style-type: none"> ○ SCWS server is provisioned with test portal.
Test Procedure	<ol style="list-style-type: none"> 1. In the Terminal select the browser. 2. Select the SCWS test portal link (e.g. 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-1.2-int-002: gif image of large size

Test Case Id	SCWS-1.2-int-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-M SCWS-S-003-M, SCWS-S-008-M, SCWS-S-009-M SCWS-ME-001-M

ETR Reference	C_M_01, S_M_01, S_M_03, S_M_05, S_M_06, D_M_01, D_O_01.
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, §6.1.2, [TEST_CONTENT]
Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server • Prerequisite for this test: <ul style="list-style-type: none"> ○ SCWS server is provisioned with the test content.
Test Procedure	<ol style="list-style-type: none"> 1. In the Terminal select the browser. 2. Select the SCWS test portal link (e.g. 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-1.2-int-003: jpeg image larger than open channel buffer size

Test Case Id	SCWS-1.2-int-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-M SCWS-S-003-M, SCWS-S-008-M, SCWS-S-009-M SCWS-ME-001-M
ETR Reference	C_M_01, S_M_01, S_M_03, S_M_05, S_M_06, D_M_01, D_O_01.
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, §6.1.2, [TEST_CONTENT]
Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server • Prerequisite for this test: <ul style="list-style-type: none"> ○ SCWS server is provisioned with the test content.

Test Procedure	<ol style="list-style-type: none"> 1. In the Terminal select the browser. 2. Select the SCWS test portal link (e.g. 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-1.2-int-004: midi file larger than 32Kb

Test Case Id	SCWS-1.2-int-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-M SCWS-S-003-M, SCWS-S-008-M, SCWS-S-009-M SCWS-ME-001-M
ETR Reference	C_M_01, S_M_01, S_M_03, S_M_05, S_M_06, D_M_01, D_O_01.
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, §6.1.2, [TEST_CONTENT]
Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server • Prerequisite for this test: <ul style="list-style-type: none"> ○ SCWS server is provisioned with the test content.
Test Procedure	<ol style="list-style-type: none"> 1. In the Terminal select the browser. 2. Select the SCWS test portal link (e.g. http://localhost:3516/index.html) 3. Select “Test resources type and length” link. 4. Select “audio.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-1.2-int-005: jpeg file of very big size

Test Case Id	SCWS-1.2-int-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-M SCWS-S-003-M, SCWS-S-008-M, SCWS-S-009-M SCWS-ME-001-M
ETR Reference	C_M_01, S_M_01, S_M_03, S_M_05, S_M_06, D_M_01, D_O_01.
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, §6.1.2, [TEST_CONTENT]
Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server • Prerequisite for this test: <ul style="list-style-type: none"> ○ SCWS server is provisioned with the test content.
Test Procedure	<ol style="list-style-type: none"> 1. In the Terminal select the browser. 2. Select the SCWS test portal link (e.g. 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-1.2-int-100 Access to server Off-line

Test Case Id	SCWS-1.2-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-M SCWS-S-003-M, SCWS-S-008-M, SCWS-S-009-M SCWS-ME-001-M
ETR Reference	C_M_01, S_M_01, S_M_03, S_M_05, S_M_06, D_M_01, D_O_01.
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, [TEST_CONTENT]
Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server • Prerequisite for this test: <ul style="list-style-type: none"> ○ SCWS server is provisioned with the test content.

Test Procedure	<ol style="list-style-type: none"> 1. Terminal is in off-line mode (no network connection). 2. In the Terminal select the browser. 3. Select the SCWS test portal link (e.g. 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-1.2-int-101 html pages with many resources

Test Case Id	SCWS-1.2-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 and 1 stylesheet) is correctly sent from server to client.
Specification Reference	[SCWS-TS] Chapter 7
SCR Reference	SCWS-C-001-M SCWS-S-003-M, SCWS-S-008-M, SCWS-S-009-M SCWS-ME-001-M
ETR Reference	C_M_01, S_M_01, S_M_03, S_M_05, S_M_06, D_M_01, D_O_01.
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1 §6.1.3, [TEST_CONTENT]
Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server • Prerequisite for this test: <ul style="list-style-type: none"> ○ SCWS server is provisioned with the test content.
Test Procedure	<ol style="list-style-type: none"> 1. In the Terminal select the browser. 2. Select the SCWS test portal link (e.g. 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-1.2-int-102 multiple http connection

Test Case Id	SCWS-1.2-int-102
Test Object	Device, SCWS Client and SCWS Server.
Test Case Description	This test case will test multiple http connection in parallel.
Specification Reference	[SCWS-TS] Chapter 7
SCR Reference	SCWS-C-001-M SCWS-S-003-M, SCWS-S-008-M, SCWS-S-009-M SCWS-ME-001-M, SCWS-ME-006-O

ETR Reference	C_M_01, S_M_01, S_M_03, S_M_05, S_M_06, D_M_01, D_O_01, D_M_02.
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1 §6.1.3, [TEST_CONTENT]
Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal that used multiple http connection. ○ Smart Card with SCWS server • Prerequisite for this test: <ul style="list-style-type: none"> ○ SCWS server is provisioned with the test content.
Test Procedure	<ol style="list-style-type: none"> 1. In the Terminal select the browser. 2. Select the SCWS test portal link (e.g. 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-1.2-int-103 Browsing cancelled

Test Case Id	SCWS-1.2-int-103
Test Object	Device, SCWS Client and SCWS Server.
Test Case Description	<p>The purpose is to verify that client/server connection cancelled is correctly managed.</p> <p>This test case will test http message exchange interruption by BIP event channel status ESTABLISHED, LISTEN.</p>
Specification Reference	[SCWS-TS] Chapter 7
SCR Reference	SCWS-C-001-M SCWS-S-003-M, SCWS-S-008-M, SCWS-S-009-M SCWS-ME-001-M
ETR Reference	C_M_01, S_M_01, S_M_03, S_M_05, S_M_06, D_M_01, D_O_01.
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, §6.1.2, [TEST_CONTENT]
Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server • Prerequisite for this test: <ul style="list-style-type: none"> ○ SCWS server is provisioned with the test content.

Test Procedure	<ol style="list-style-type: none"> 1. In the Terminal select the browser. 2. Select the SCWS test portal link (e.g. 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-1.2-int-104 Browsing interruption

Test Case Id	SCWS-1.2-int-104
Test Object	Device, SCWS Client and SCWS Server.
Test Case Description	<p>The purpose is to verify that client/server connection interruption is correctly managed.</p> <p>This test case will test http message exchange interruption by BIP event channel status ESTABLISHED, LISTEN in multiple connections mode.</p>
Specification Reference	[SCWS-TS] Chapter 7
SCR Reference	SCWS-C-001-M SCWS-S-003-M, SCWS-S-008-M, SCWS-S-009-M SCWS-ME-001-M
ETR Reference	C_M_01, S_M_01, S_M_03, S_M_05, S_M_06, D_M_01, D_O_01.
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, §6.1.3; [TEST_CONTENT]
Preconditions	<ol style="list-style-type: none"> 1. Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server 2. Prerequisite for this test: <ul style="list-style-type: none"> ○ SCWS server is provisioned with the test content.
Test Procedure	<ol style="list-style-type: none"> 1. In the Terminal select the browser. 2. Select the SCWS test portal link (e.g. 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-1.2-int-105 Browsing and server administration

Test Case Id	SCWS-1.2-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-M SCWS-S-003-M, SCWS-S-008-M, SCWS-S-009-M SCWS-ME-001-M
ETR Reference	C_M_01, S_M_01, S_M_03, S_M_05, S_M_06, D_M_01, D_O_01.
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, §6.1.2, [TEST_CONTENT]
Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server and SCWS admin client ○ Remote admin SCWS Server. • Prerequisite for this test: <ul style="list-style-type: none"> ○ SCWS server is provisioned with the test content. ○ Smart Card card administration agent is configured with remote admin SCWS Server parameters (ip-address, port...).
Test Procedure	<ol style="list-style-type: none"> 1. In the Terminal select the browser. 2. In the browser, select the SCWS test portal link (e.g. http://localhost:3516/index.html) 3. In the 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 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	<p>Verify that the download portal of 32kb is present on the Smart Card Web Server.</p> <ol style="list-style-type: none"> 1. In the browser, select page 1 verifies that 4 images are displayed. 2. In the browser, select page 2 verifies that 6 images are displayed.

6.1.2.7 SCWS-1.2-int-106 CAT applications concurrency

Test Case Id	SCWS-1.2-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-M SCWS-S-003-M, SCWS-S-007-M, SCWS-S-008-M, SCWS-S-009-M SCWS-ME-001-M
ETR Reference	C_M_01, S_M_01, S_M_03, S_M_04, S_M_05, S_M_06, D_M_01, D_O_01.
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, §6.1.2, §6.3 [TEST_CONTENT]
Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal A, Terminal B ○ Smart Card with SCWS server and SCWS admin client • Prerequisite for this test: <ul style="list-style-type: none"> ○ SCWS server is provisioned with the test content. ○ CAT concurrency application is loaded and installed in the Smart Card. This CAT application is registered on MT call event and sends a DISPLAY_TEXT proactive command, when triggered by this event.
Test Procedure	<ol style="list-style-type: none"> 1. In the Terminal A select the browser. 2. In the browser, select the SCWS test portal link (e.g. http://localhost:3516/index.html) 3. In the 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. <p>Remark: Synchronize step 5 in order that event MT call is received by the Smart Card before the complete client/server messages exchange</p>
Pass-Criteria	In the Terminal A, “Hello World” is displayed.

6.1.2.8 SCWS-1.2-int-107 GET_WITH_ENVELOPE

Test Case Id	SCWS-1.2-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-M, SCWS-AC-004-M, SCWS-AC-007-M, SCWS-AC-010-M SCWS-AS-001-M, SCWS-AS-005-M SCWS-S-012-M, SCWS-S-022-M
ETR Reference	ADM_C_M_01, ADM_C_M_02, ADM_C_M_03, ADM_C_M_06, ADM_S_M_01, ADM_S_M_03, S_M_13.
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	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal A, Terminal B. ○ Smart Card with SCWS server, CAT application registered on the UNFORMATTED_SMS_PP Event • Prerequisite for this test: <ul style="list-style-type: none"> ○ SCWS server is provisioned with the test content. ○ SIM with a special CAT application executing a SET UP CALL when triggered by a UNFORMATTED_SMS_PP event.
Test Procedure	<ol style="list-style-type: none"> 1. In the Terminal A select the browser. 2. Select the SCWS test portal link (e.g. 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

6.1.2.9 SCWS-1.2-int-108 Browsing and CAT DISPLAY-TEXT user-confirmation

Test Case Id	SCWS-1.2-int-108
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 DISPLAY_TEXT with user-confirmation is triggered by a SMS.
Specification Reference	[SCWS-TS] Chapter 8.1.1.1 SCWS and other CAT applications concurrency
SCR Reference	SCWS-AC-001-M, SCWS-AC-004-M, SCWS-AC-007-M, SCWS-AC-010-M SCWS-AS-001-M, SCWS-AS-005-M SCWS-S-012-M, SCWS-S-022-M
ETR Reference	ADM_C_M_01, ADM_C_M_02, ADM_C_M_03, ADM_C_M_06, ADM_S_M_01, ADM_S_M_03, S_M_13.
Tool	
Test code	CAT application on a SMS_PP i.e. on this event the Applet performs a DISPLAY_TEXT with User-Confirmation proactive command.

Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server, CAT application registered on the SMS_PP Event • Prerequisite for this test: <ul style="list-style-type: none"> ○ SCWS server is provisioned with the test content. ○ SIM with a special CAT application executing a DISPLAY_TEXT SET UP CALL when triggered by a SMS_PP event.
Test Procedure	<ol style="list-style-type: none"> 1. In the Terminal <ul style="list-style-type: none"> • Select the browser. • Select the SCWS test portal link • Select “Test resources type and length” link. • Select “Mer-d-Iroise.jpg” link to start download • SMS is received during resource download. • Verify the pass criteria [1][2] • Press OK button to confirm DISPLAY-TEXT then switch to the browser. • Verify the pass criteria [3] [4] [5]
Pass-Criteria	<ol style="list-style-type: none"> 1. Smart Card emit CAT cmd DISLAY-TEXT (“Hello”) with user-confirm. 2. Terminal display the CAT cmd DISPLAY-TEST (“Hello”). 3. Terminal sent TERMINAL-RESPONSE OK to the Smart Card 4. Smart Card finished SCWS ressource download. 5. The browser displayed the new dowload resource (Mer-d-Iroise.jpg).

6.1.3 URI test group

6.1.3.1 SCWS-1.2-int-200 long file name

Test Case Id	SCWS-1.2-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-M SCWS-S-003-M, SCWS-S-008-M, SCWS-S-009-M SCWS-ME-001-M
ETR Reference	C_M_01, S_M_01, S_M_03, S_M_05, S_M_06, D_M_01, D_O_01.
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, §6.1.4, [TEST_CONTENT]

Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server • Prerequisite for this test: <ul style="list-style-type: none"> ○ SCWS server is provisioned with the test content.
Test Procedure	<ol style="list-style-type: none"> 1. In the Terminal select the browser. 2. Select the SCWS test portal link (e.g. 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-1.2-int-201 long directory name

Test Case Id	SCWS-1.2-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-M SCWS-S-003-M, SCWS-S-008-M, SCWS-S-009-M SCWS-ME-001-M
ETR Reference	C_M_01, S_M_01, S_M_03, S_M_05, S_M_06, D_M_01, D_O_01.
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, §6.1.4, [TEST_CONTENT]
Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server 1. Prerequisite for this test: <ul style="list-style-type: none"> ○ SCWS server is provisioned with the test content.
Test Procedure	<ol style="list-style-type: none"> 1. In the Terminal select the browser. 2. Select the SCWS test portal link (e.g. 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-1.2-int-202 escaped char

Test Case Id	SCWS-1.2-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-M SCWS-S-003-M, SCWS-S-008-M, SCWS-S-009-M SCWS-ME-001-M
ETR Reference	C_M_01, S_M_01, S_M_03, S_M_05, S_M_06, D_M_01, D_O_01.
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, §6.1.4, [TEST_CONTENT]
Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server • Prerequisite for this test: <ul style="list-style-type: none"> ○ SCWS server is provisioned with the test content.
Test Procedure	<ol style="list-style-type: none"> 1. In the Terminal select the browser. 2. Select the SCWS test portal link (e.g. 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-1.2-int-203 query string

Test Case Id	SCWS-1.2-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-M SCWS-S-003-M, SCWS-S-008-M, SCWS-S-009-M SCWS-ME-001-M
ETR Reference	C_M_01, S_M_01, S_M_03, S_M_05, S_M_06, D_M_01, D_O_01.
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, §6.1.4, [TEST_CONTENT]
Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server • Prerequisite for this test: <ul style="list-style-type: none"> ○ SCWS server is provisioned with the test content.

Test Procedure	<ol style="list-style-type: none"> 1. In the Terminal select the browser. 2. Select the SCWS test portal link (e.g. 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-1.2-int-204 uri long (1024 bytes)

Test Case Id	SCWS-1.2-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-M SCWS-S-001-M, SCWS-S-003-M, SCWS-S-008-M, SCWS-S-009-M SCWS-ME-001-M
ETR Reference	C_M_01, S_M_01, S_M_03, S_M_05, S_M_06, D_M_01, D_O_01.
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, §6.1.4, [TEST_CONTENT]
Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server • Prerequisite for this test: <ul style="list-style-type: none"> ○ SCWS server is provisioned with the test content.
Test Procedure	<ol style="list-style-type: none"> 1. In the Terminal select the browser. 2. Select the SCWS test portal link (e.g. 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-1.2-int-205 Uri Not Found

Test Case Id	SCWS-1.2-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-M SCWS-S-003-M, SCWS-S-008-M, SCWS-S-009-M SCWS-ME-001-M

ETR Reference	C_M_01, S_M_01, S_M_03, S_M_05, S_M_06, D_M_01, D_O_01.
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, §6.1.4, [TEST_CONTENT]
Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server • Prerequisite for this test: <ul style="list-style-type: none"> ○ SCWS server is provisioned with the test content.
Test Procedure	<ol style="list-style-type: none"> 1. In the Terminal select the browser. 2. Select the SCWS test portal link (e.g. 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-1.2-int-206 5 directory levels

Test Case Id	SCWS-1.2-int-206
Test Object	Device, SCWS Client and SCWS Server.
Test Case Description	The purpose is to verify that an uri 5 levels of directory is correctly handled by server.
Specification Reference	[SCWS-TS] Chapter 5
SCR Reference	SCWS-C-001-M SCWS-S-001-M, SCWS-S-003-M, SCWS-S-008-M, SCWS-S-009-M SCWS-ME-001-M
ETR Reference	C_M_01, S_M_01, S_M_03, S_M_05, S_M_06, D_M_01, D_O_01.
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, §6.1.4, [TEST_CONTENT]
Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server • Prerequisite for this test: <ul style="list-style-type: none"> ○ SCWS server is provisioned with the test content.
Test Procedure	<ol style="list-style-type: none"> 1. In the Terminal select the browser. 2. Select the SCWS test portal link (e.g. 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.
----------------------	--

6.1.3.8 SCWS-1.2-int-207 default path

Test Case Id	SCWS-1.2-int-207
Test Object	Device, SCWS Client and SCWS Server.
Test Case Description	The purpose is to verify the default path “/” mapping.
Specification Reference	[SCWS-TS] Chapter 5
SCR Reference	SCWS-C-001-M SCWS-S-001-M, SCWS-S-003-M, SCWS-S-008-M, SCWS-S-009-M SCWS-ME-001-M
ETR Reference	C_M_01, S_M_01, S_M_03, S_M_05, S_M_06, D_M_01, D_O_01.
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, §6.1.4, [TEST_CONTENT]
Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server • Prerequisite for this test: <ul style="list-style-type: none"> ○ SCWS server is provisioned with the test content. ○ Default path “/” is mapped on “/index.html”
Test Procedure	<ol style="list-style-type: none"> 1. In the Terminal select the browser. 2. Select the SCWS test portal link (e.g. http://localhost:3516/) 3. Verify the pass criteria below.
Pass-Criteria	The test home page index.html is displayed.

6.1.4 Protection test group

6.1.4.1 SCWS-1.2-int-250 http basic authentication

Test Case Id	SCWS-1.2-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-M, SCWS-C-004-M SCWS-S-003-M, SCWS-S-008-M, SCWS-S-009-M, SCWS-S-013-M, SCWS-S-014-M, SCWS-S-015-M SCWS-ME-001-M

ETR Reference	C_M_01, S_M_01, S_M_03, S_M_05, S_M_06, S_M_09, S_M_10, S_M_11, D_M_01, D_O_01, C_O_03.
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, §6.1.5, [TEST_CONTENT]
Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server • Prerequisite for this test: <ul style="list-style-type: none"> ○ SCWS server is provisioned with the test content. ○ SCWS server is configured with security rules.
Test Procedure	<ol style="list-style-type: none"> 1. In the Terminal select the browser. 2. Select the SCWS test portal link (e.g. 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. Authentication 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	<ol style="list-style-type: none"> 1. Resources basic.html is NOT displayed. 2. Resources basic.html is displayed.

6.1.4.2 SCWS-1.2-int-251 admin protection

Test Case Id	SCWS-1.2-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 through the Browser. This test case will test HTTP status-code ‘403 Forbidden’.
Specification Reference	[SCWS-TS] Chapter 13.5.1.2
SCR Reference	SCWS-C-001-M SCWS-S-003-M, SCWS-S-008-M, SCWS-S-009-M SCWS-ME-001-M
ETR Reference	C_M_01, S_M_01, S_M_03, S_M_05, S_M_06, D_M_01, D_O_01.
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, §6.1.5, [TEST_CONTENT]

Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server • Prerequisite for this test: <ul style="list-style-type: none"> ○ SCWS server is provisioned with the test content. ○ SCWS server is configured with security rules.
Test Procedure	<ul style="list-style-type: none"> ▪ In the Terminal select the browser. ▪ Select the SCWS test portal link (e.g. http://localhost:3516/index.html) ▪ Select link “Test protection (basic auth, admin)” ▪ Select link “admin protocol” ▪ Verify the pass criteria below.
Pass-Criteria	403 Forbidden error message is displayed.

6.1.5 Dynamic content test group

6.1.5.1 SCWS-1.2-int-300 form post method

Test Case Id	SCWS-1.2-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 HTTP POST message with content-body handle by dynamic content application.
Specification Reference	[SCWS-TS] Chapter 6
SCR Reference	SCWS-C-001-M SCWS-S-002-M, SCWS-S-003-M, SCWS-S-008-M, SCWS-S-009-M, SCWS-S-011-M SCWS-ME-001-M
ETR Reference	C_M_01, S_M_01, S_M_02, S_M_03, S_M_05, S_M_06, S_M_08 , D_M_01, D_O_01.
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, §6.1.6, §6.3.2 [TEST_CONTENT]
Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server • Prerequisite for this test: <ul style="list-style-type: none"> ○ SCWS server is provisioned with the test content. ○ Dynamic content application is loaded / installed on the Smart Card.

Test Procedure	<ol style="list-style-type: none"> 1. In the Terminal select the browser. 2. Select the SCWS test portal link (e.g. 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-1.2-int-301 form get method

Test Case Id	SCWS-1.2-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-M SCWS-S-002-M, SCWS-S-003-M, SCWS-S-008-M, SCWS-S-009-M SCWS-ME-001-M
ETR Reference	C_M_01, S_M_01, S_M_02, S_M_03, S_M_05, S_M_06, D_M_01, D_O_01.
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, §6.1.6, §6.3.2, [TEST_CONTENT]
Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server • Prerequisite for this test: <ul style="list-style-type: none"> ○ SCWS server is provisioned with the test content. ○ Dynamic content application is loaded / installed on the Smart Card.
Test Procedure	<ol style="list-style-type: none"> 1. In the Terminal select the browser. 2. Select the SCWS test portal link (e.g. 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-1.2-int-302 post inexistent resource

Test Case Id	SCWS-1.2-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 inexistent uri.
Specification Reference	[SCWS-TS] Chapter 6

SCR Reference	SCWS-C-001-M SCWS-S-003-M, SCWS-S-008-M, SCWS-S-009-M, SCWS-S-011-M SCWS-ME-001-M
ETR Reference	C_M_01, S_M_01, S_M_03, S_M_05, S_M_06, S_M_08, D_M_01, D_O_01.
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, §6.1.6, §6.3.2, [TEST_CONTENT]
Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server • Prerequisite for this test: <ul style="list-style-type: none"> ○ SCWS server is provisioned with the test content.
Test Procedure	<ol style="list-style-type: none"> 1. In the Terminal select the browser. 2. Select the SCWS test portal link (e.g. http://localhost:3516/index.html) 3. Select link “Test Dynamic Content” 4. Select link “Test post unexistent 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-1.2-int-303 chunked response

Test Case Id	SCWS-1.2-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: chunked” is correctly processed by Device, SCWS Client.
Specification Reference	[SCWS-TS] Chapter 6
SCR Reference	SCWS-C-001-M SCWS-S-002-M, SCWS-S-003-M, SCWS-S-008-M, SCWS-S-009-M, SCWS-S-011-M SCWS-ME-001-M
ETR Reference	C_M_01, S_M_01, S_M_02, S_M_03, S_M_05, S_M_06, S_M_08, D_M_01, D_O_01.
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, §6.1.6, §6.3.2, [TEST_CONTENT]

Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server • Prerequisite for this test: <ul style="list-style-type: none"> ○ SCWS server is provisioned with the test content. ○ Dynamic content application is loaded/ installed on the Smart Card.
Test Procedure	<ol style="list-style-type: none"> 1. In the Terminal select the browser. 2. Select the SCWS test portal link (e.g. http://localhost:3516/index.html) 3. Select link “Test Dynamic Content” 4. Select link “Test chunked response” 5. Select button “ok”. 6. Verify the pass criteria below.
Pass-Criteria	“Hello World” is displayed.

6.1.5.5 SCWS-1.2-int-304 form get method with special char in query string

Test Case Id	SCWS-1.2-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-M SCWS-S-002-M, SCWS-S-003-M, SCWS-S-008-M, SCWS-S-009-M SCWS-ME-001-M
ETR Reference	C_M_01, S_M_01, S_M_02, S_M_03, S_M_05, S_M_06 D_M_01, D_O_01.
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, §6.1.6, §6.3.2, [TEST_CONTENT]
Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server • Prerequisite for this test: <ul style="list-style-type: none"> ○ SCWS server is provisioned with the test content. ○ Dynamic content application is loaded / installed on the Smart Card.
Test Procedure	<ol style="list-style-type: none"> 1. In the Terminal select the browser. 2. Select the SCWS test portal link (e.g. http://localhost:3516/index.html) 3. Select link “Test Dynamic Content” 4. Select link “Test form get method” 5. Enter ‘/a?2&a=b’ in the form then select button “do get”. 6. Verify the pass criteria below.

Pass-Criteria	“Hello /a?2&a=b” is displayed.
----------------------	--------------------------------

6.1.5.6 SCWS-1.2-int-305 get send SMS

Test Case Id	SCWS-1.2-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-M SCWS-S-002-M, SCWS-S-003-M, SCWS-S-008-M, SCWS-S-009-M, SCWS-S-011-M SCWS-ME-001-M
ETR Reference	C_M_01, S_M_01, S_M_02, S_M_03, S_M_05, S_M_06, S_M_08, D_M_01, D_O_01.
Tool	
Test code	
Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ 2 Terminals A&B ○ Smart Card with SCWS server • Prerequisite for this test: <ul style="list-style-type: none"> ○ SCWS server is provisioned with test portal. ○ Dynamic content application is loaded/ installed on the Smart Card.
Test Procedure	<ol style="list-style-type: none"> 1. In the Terminal A select the browser. 2. Select the SCWS test portal link (e.g. http://localhost:3516/index.html) 3. Select link “Test Dynamic Content” 4. Select link “Test send SMS” 5. Fill up form with the phone number of the Terminal B. 6. Fill up form with the text message to send. 7. Select button “ok”. 8. Verify the pass criteria below.
Pass-Criteria	The SMS content is displayed in Terminal B.

6.1.6 Transport protocol test group

6.1.6.1 SCWS-1.2-int-400 Browsing session using BIP server mode

Test Case Id	SCWS-1.2-int-400
Test Object	Device, SCWS Client and SCWS Server.
Test Case Description	The purpose is to verify that the BIP server mode protocol is correctly handled by client and server.
Specification Reference	[SCWS-TS] Chapter 8.1

SCR Reference	SCWS-C-001-M SCWS-S-003-M, SCWS-S-004-O, SCWS-S-006-O, SCWS-S-008-M, SCWS-S-009-M SCWS-ME-001-M, SCWS-ME-002-O, SCWS-ME-003-O, SCWS-ME-005-O
ETR Reference	C_M_01, S_M_01, S_M_03, S_M_05, S_M_06, S_M_24, D_M_01, D_M_02, D_O_01.
Tool	Smart Card protocol analyser
Test code	[TEST_CONTENT_DESC] §6.1.1, §6.1.2, [TEST_CONTENT]
Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal implementing the BIP protocol ○ Smart Card with SCWS server implementing the BIP protocol • Prerequisite for this test: <ul style="list-style-type: none"> ○ SCWS server is provisioned with the test content.
Test Procedure	<ol style="list-style-type: none"> 1. In the Terminal select the browser. 2. Select the SCWS test portal link (e.g. 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 is displayed. The BIP server mode protocol has been used (check using a transport protocol analyser).

6.1.6.1 SCWS-1.2-int-401 Browsing session using TCP/IP

Test Case Id	SCWS-1.2-int-401
Test Object	Device, SCWS Client and SCWS Server.
Test Case Description	The purpose is to verify that the TCP/IP protocol using the Ethernet Emulation Model (EEM) subclass (i.e. not using BIP server mode protocol) is correctly handled by client and server.
Specification Reference	[SCWS-TS] Chapter 8.2
SCR Reference	SCWS-C-001-M SCWS-S-003-M, SCWS-S-005-O, SCWS-S-008-M, SCWS-S-009-M, SCWS-S-035-O SCWS-ME-001-M, SCWS-ME-004-O, SCWS-ME-013-O, SCWS-ME-014-O
ETR Reference	C_M_01, S_M_01, S_M_03, S_M_05, S_M_06, S_M_25, D_M_01, D_M_04.
Tool	Smart Card protocol analyser
Test code	[TEST_CONTENT_DESC] §6.1.1, §6.1.2, [TEST_CONTENT]

Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal implementing the TCP/IP protocol and EEM subclass ○ Smart Card with SCWS server implementing the TCP/IP protocol and EEM subclass • Prerequisite for this test: <ul style="list-style-type: none"> ○ SCWS server is provisioned with the test content.
Test Procedure	<ol style="list-style-type: none"> 1. In the Terminal select the browser. 2. Select the SCWS test portal link (e.g. http://localuicc: 80/index.html) 3. Select “Test resources type and length” link. 4. Select “Bullet.gif” link. 5. Verify the pass criteria below.
Pass-Criteria	<p>The image “Bullet.gif” is displayed.</p> <p>The TCP/IP protocol has been used using the Ethernet Emulation Model (EEM) subclass (check using a transport protocol analyser).</p>

6.1.7 Access Control Policy test group

6.1.7.1 SCWS-1.2-int-1100 Trusted terminal application

Test Case Id	SCWS-1.2-int-1100
Test Object	Device, SCWS Client and SCWS Server.
Test Case Description	When an Access Control Policy file is present in SCWS server, check that the terminal retrieves this file from the SCWS and enforces access restrictions to the SCWS: a terminal test application considered as trusted will have access to the SCWS.
Specification Reference	[SCWS-TS] Chapter 13
SCR Reference	SCWS-C-001-M SCWS-S-003-M, SCWS-S-008-M, SCWS-S-021-O SCWS-ME-001-M, SCWS-ME-008-O, SCWS-ME-009-M, SCWS-ME-010-M
ETR Reference	C_M_01, S_M_01, S_M_03, S_M_05, S_O_03, D_M_01, D_M_06, D_M_07, D_O_01.
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.7, [TEST_CONTENT]

Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server ○ Terminal test application “Application A” with the following behaviour: <ul style="list-style-type: none"> ▪ This application tries to access the SCWS resource ‘mobile_tv.gif’ ▪ An error message is displayed if the access is rejected; otherwise the image ‘mobile_tv.gif’ is displayed. • Prerequisite for this test: <ul style="list-style-type: none"> ○ Terminal implementing an ACP Enforcer ○ The terminal test application “Application A” is installed in the terminal. ○ SCWS server is provisioned with the portal ‘oma-500’ ○ SCWS server is provisioned with an ACP file /config/acp ○ The terminal test application “Application A” is signed, the device and the ACP file are provisioned, so that the test application “Application A” is considered as a trusted application having access to the SCWS
Test Procedure	<ol style="list-style-type: none"> 1. In Terminal, launch the test application “Application A” <ul style="list-style-type: none"> • The application tries to access the SCWS resource ‘mobile_tv.gif’ 2. Verify the pass criteria below.
Pass-Criteria	<ol style="list-style-type: none"> 1. The Terminal retrieves correctly the ACP file /config/acp 2. The image ‘mobile_tv.gif’ is displayed by the terminal test application “Application A” (i.e. access to the SCWS resources has been granted).

6.1.7.2 SCWS-1.2-int-1101 Untrusted terminal application

Test Case Id	SCWS-1.2-int-1101
Test Object	Device, SCWS Client and SCWS Server.
Test Case Description	When an Access Control Policy file is present in SCWS server, check that the terminal retrieves this file from the SCWS and enforces access restrictions to the SCWS: a terminal test application considered as untrusted will not have access to the SCWS.
Specification Reference	[SCWS-TS] Chapter 13
SCR Reference	SCWS-C-001-M SCWS-S-003-M, SCWS-S-008-M, SCWS-S-021-O SCWS-ME-001-M, SCWS-ME-008-O, SCWS-ME-009-M, SCWS-ME-010-M
ETR Reference	C_M_01, S_M_01, S_M_03, S_M_05, S_O_03, D_M_01, D_M_06, D_M_07, D_O_01.
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.7, [TEST_CONTENT]

Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server ○ Terminal test application “Application B” with the following behaviour: <ul style="list-style-type: none"> ▪ This application tries to access the SCWS resource ‘mobile_tv.gif’ ▪ An error message is displayed if the access is rejected; otherwise the image ‘mobile_tv.gif’ is displayed. • Prerequisite for this test: <ul style="list-style-type: none"> ○ Terminal implementing an ACP Enforcer ○ The terminal test application “Application B” is installed in the terminal. ○ SCWS server is provisioned with the portal ‘oma-500’ ○ SCWS server is provisioned with an ACP file /config/acp ○ The terminal application “Application B” is signed, the device and the ACP file are provisioned, so that the test application “Application B” is considered as an untrusted application i.e. not having access to the SCWS
Test Procedure	<ol style="list-style-type: none"> 1. In Terminal, launch the test application “Application B” <ul style="list-style-type: none"> • The application tries to access the SCWS resource ‘mobile_tv.gif’ 2. Verify the pass criteria below.
Pass-Criteria	<ol style="list-style-type: none"> 1. The Terminal retrieves correctly the ACP file /config/acp 2. An error message is displayed by the terminal test application “Application B” (i.e. the application cannot access to the SCWS resources ‘oma-500/mobile_tv.gif’).

6.1.7.3 SCWS-1.2-int-1102 No ACP file

Test Case Id	SCWS-1.2-int-1102
Test Object	Device, SCWS Client and SCWS Server.
Test Case Description	When an Access Control Policy file is not present in SCWS server, check that the terminal allows any terminal application to access to the SCWS.
Specification Reference	[SCWS-TS] Chapter 13
SCR Reference	SCWS-C-001-M SCWS-S-003-M, SCWS-S-008-M, SCWS-S-021-O SCWS-ME-001-M, SCWS-ME-008-O, SCWS-ME-009-M, SCWS-ME-010-M
ETR Reference	C_M_01, S_M_01, S_M_03, S_M_05, S_O_03, D_M_01, D_M_06, D_M_07, D_O_01.
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.7, [TEST_CONTENT]

Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server ○ Terminal test application “Application B” with the following behaviour: <ul style="list-style-type: none"> ▪ This application tries to access the SCWS resource ‘mobile_tv.gif’ ▪ An error message is displayed if the access is rejected; otherwise the image ‘mobile_tv.gif’ is displayed. • Prerequisite for this test: <ul style="list-style-type: none"> ○ Terminal implementing an ACP Enforcer ○ The terminal test application “Application B” is installed in the terminal. ○ SCWS server is provisioned with the portal ‘oma-500’ ○ The terminal application “Application B” is signed, the device is provisioned, so that the test application “Application B” is considered as an untrusted application i.e. not having access to the SCWS ○ There is no ACP file /config/acp provisioned in the SCWS
Test Procedure	<ol style="list-style-type: none"> 1. In Terminal, launch the test application “Application B” <ul style="list-style-type: none"> • The application tries to access the SCWS resource ‘mobile_tv.gif’ 2. Verify the pass criteria below.
Pass-Criteria	<ol style="list-style-type: none"> 1. The Terminal tries to access the ACP file /config/acp 2. The image ‘mobile_tv.gif’ is displayed by the terminal test application “Application B” (i.e. access to the SCWS resources has been granted).

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-1.2-int-500 single resource small size

Test Case Id	SCWS-1.2-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 through full admin protocol.
Specification Reference	[SCWS-TS] Chapter 13.3.2 [SCWS-TS] Chapter 13.1
SCR Reference	SCWS-AC-001-M, SCWS-AC-004-M, SCWS-AC-007-M, SCWS-AC-010-M, SCWS-AC-017-M, SCWS-S-028-M SCWS-AS-001-M, SCWS-AS-005-M SCWS-S-012-M, SCWS-S-022-M

ETR Reference	ADM_C_M_01, ADM_C_02, ADM_C_M_03, ADM_C_M_06, ADM_C_M_07, ADM_C_M_08, ADM_C_M_11, ADM_S_M_01, ADM_S_M_03, ADM_S_M_07, ADM_S_M_08, S_M_05, S_M_12, S_M_13, S_M_17, D_M_01.
Tool	
Test code	[TEST_CONTENT_DESC], [TEST_CONTENT]
Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server and SCWS admin client ○ Remote admin SCWS Server • Prerequisite for this test: <ul style="list-style-type: none"> ○ Smart Card card administration agent is configured with remote admin SCWS Server parameters (ip-address, port...).
Test Procedure	<ol style="list-style-type: none"> 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 the browser. 5. Select the SCWS test portal link (e.g. http://localhost:3516/index.html) 6. Verify the pass criteria below.
Pass-Criteria	In Terminal browser, the new download resource (portal 'oma-500') is displayed.

6.2.1.2 SCWS-1.2-int-501 single resource large size

Test Case Id	SCWS-1.2-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 through full admin protocol. This test case will test POST response of remote admin server with HTTP header 'Transfer-Encoding: chunked'.
Specification Reference	[SCWS-TS] Chapter 13.3.2 [SCWS-TS] Chapter 13.1
SCR Reference	SCWS-AC-001-M, SCWS-AC-004-M, SCWS-AC-007-M, SCWS-AC-010-M, SCWS-AC-017-M, SCWS-S-028-M SCWS-AS-001-M, SCWS-AS-005-M SCWS-S-012-M, SCWS-S-022-M
ETR Reference	ADM_C_M_01, ADM_C_02, ADM_C_M_03, ADM_C_M_06, ADM_C_M_07, ADM_C_M_08, ADM_C_M_11, ADM_S_M_01, ADM_S_M_03, ADM_S_M_07, ADM_S_M_08, S_M_05, S_M_12, S_M_13, S_M_17, D_M_01.
Tool	
Test code	[TEST_CONTENT_DESC], [TEST_CONTENT]

Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server and SCWS admin client ○ Remote admin SCWS Server • Prerequisite for this test: Smart Card card administration agent is configured with remote admin SCWS Server parameters (ip-address, port...).
Test Procedure	<ol style="list-style-type: none"> 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 the browser. 5. Select the SCWS test portal link (e.g. http://localhost:3516/index.html) 6. Verify the pass criteria below.
Pass-Criteria	In Terminal browser, the new download resource (portal 'oma-501') is displayed.

6.2.1.3 SCWS-1.2-int-502 multiple resources total size 32kb

Test Case Id	SCWS-1.2-int-502
Test Object	Remote admin SCWS Server, SCWS admin client.
Test Case Description	<p>The purpose is to verify that portal of 32kb (portal 'oma-502') with multiple resources can be sent, received through full admin protocol. This portal contains 2 different pages:</p> <ul style="list-style-type: none"> - Page 1 with 4 images of 5kb. - Page 2 with 6 images of 2kb. <p>This test case will test POST response of remote admin server with pipelined administration command.</p>
Specification Reference	[SCWS-TS] Chapter 13.3.2 [SCWS-TS] Chapter 13.1
SCR Reference	SCWS-AC-001-M, SCWS-AC-004-M, SCWS-AC-007-M, SCWS-AC-010-M, SCWS-AC-017-M, SCWS-S-028-M SCWS-AS-001-M, SCWS-AS-005-M SCWS-S-012-M, SCWS-S-022-M, SCWS-S-027-O
ETR Reference	ADM_C_M_01, ADM_C_02, ADM_C_M_03, ADM_C_M_06, ADM_C_M_07, ADM_C_M_08, ADM_C_M_11, ADM_S_M_01, ADM_S_M_03, ADM_S_M_07, ADM_S_M_08, S_M_05, S_M_12, S_M_13, S_M_17, S_O_10, D_M_01.
Tool	
Test code	[TEST_CONTENT_DESC] §6.2.1, [TEST_CONTENT]

Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server and SCWS admin client ○ Remote admin SCWS Server • Prerequisite for this test: <ul style="list-style-type: none"> ○ Smart Card card administration agent is configured with remote admin SCWS Server parameters (ip-address, port...).
Test Procedure	<ol style="list-style-type: none"> 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 browser. 5. In the browser, select the SCWS test portal link (e.g. http://localhost:3516/index.html) 6. Verify the pass criteria below.
Pass-Criteria	<p>In Terminal browser, the new download resource (portal 'oma-502') is displayed.</p> <p>In the browser, select page 1, verify that 4 images are displayed.</p> <p>In the browser, select page 2, verify that 6 images are displayed.</p>

6.2.1.4 SCWS-1.2-int-503 multiple resources total size 100kb

Test Case Id	SCWS-1.2-int-503
Test Object	Remote admin SCWS Server, SCWS admin client.
Test Case Description	<p>The purpose is to verify that portal of 100kb (portal 'oma-503') with multiple resources can be sent, received through full admin protocol. This portal contains 3 different pages:</p> <ul style="list-style-type: none"> - Page 1 with 2 images of 18kb. - Page 2 with 8 images of 5kb. - Page 3 with 12 images of 2kb. <p>This test case will test POST response of remote admin server with pipelined administration command and and with HTTP header 'Transfert-Encoding: chunked'.</p>
Specification Reference	<p>[SCWS-TS] Chapter 13.3.2</p> <p>[SCWS-TS] Chapter 13.1</p>
SCR Reference	<p>SCWS-AC-001-M, SCWS-AC-004-M, SCWS-AC-007-M, SCWS-AC-010-M, SCWS-AC-017-M, SCWS-S-028-M</p> <p>SCWS-AS-001-M, SCWS-AS-005-M</p> <p>SCWS-S-012-M, SCWS-S-022-M</p>
ETR Reference	<p>ADM_C_M_01, ADM_C_02, ADM_C_M_03, ADM_C_M_06, ADM_C_M_07, ADM_C_M_08, ADM_C_M_11,</p> <p>ADM_S_M_01, ADM_S_M_03, ADM_S_M_07, ADM_S_M_08, S_M_05, S_M_12, S_M_13, S_M_17,</p> <p>D_M_01.</p>
Tool	
Test code	[TEST_CONTENT_DESC] §6.2.2, [TEST_CONTENT]

Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server and SCWS admin client ○ Remote admin SCWS Server • Prerequisite for this test: <ul style="list-style-type: none"> ○ Smart Card card administration agent is configured with remote admin SCWS Server parameters (ip-address, port...).
Test Procedure	<ol style="list-style-type: none"> 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 the browser. 5. In the browser, select the SCWS test portal link (e.g. http://localhost:3516/index.html) 6. Verify the pass criteria below.
Pass-Criteria	<p>In Terminal browser, the new download resource (portal 'oma-503') is displayed.</p> <p>In the browser, select page 1, verify that 2 images are displayed.</p> <p>In the browser, select page 2, verify that 8 images are displayed.</p> <p>In the browser, select page 3, verify that 12 images are displayed.</p>

6.2.1.5 SCWS-1.2-int-504 directory deletion

Test Case Id	SCWS-1.2-int-504
Test Object	Remote admin SCWS Server, SCWS admin client.
Test Case Description	The purpose is to validate portal deletion using directory deletion command.
Specification Reference	[SCWS-TS] Chapter 13.3.2 [SCWS-TS] Chapter 13.1
SCR Reference	SCWS-AC-001-M, SCWS-AC-004-M, SCWS-AC-007-M, SCWS-AC-010-M, SCWS-AC-017-M, SCWS-S-028-M, SCWS-S-029-M SCWS-AS-001-M, SCWS-AS-005-M SCWS-S-012-M, SCWS-S-022-M
ETR Reference	ADM_C_M_01, ADM_C_02, ADM_C_M_03, ADM_C_M_06, ADM_C_M_07, ADM_C_M_08, ADM_C_M_11, ADM_S_M_01, ADM_S_M_03, ADM_S_M_07, ADM_S_M_08, S_M_05, S_M_12, S_M_13, S_M_17, S_M_19 D_M_01.
Tool	
Test code	[TEST_CONTENT_DESC] §6.2.1, [TEST_CONTENT]
Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server and SCWS admin client ○ Remote admin SCWS Server • Prerequisite for this test: <ul style="list-style-type: none"> ○ Smart Card card administration agent is configured with remote admin SCWS Server parameters (ip-address, port...).

Test Procedure	<ol style="list-style-type: none"> 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 the browser. 5. In the browser, select the SCWS test portal link (/index.html) 6. In Terminal browser, the new download resource ('oma-502') is displayed 7. In Remote admin SCWS Server, launch remote admin session to delete directory /img then wait administration finished. 8. In the browser, select the SCWS test portal link (e.g. http://localhost:3516/index.html) 9. Verify the pass criteria below.
Pass-Criteria	In Terminal browser, the new download resource (portal 'oma-502') is displayed with all images not found.

6.2.1.6 SCWS-1.2-int-505 resources gzipped

Test Case Id	SCWS-1.2-int-505
Test Object	Remote admin SCWS Server, SCWS admin client.
Test Case Description	The purpose is to verify that portal with gzip resources can be sent, received through full admin protocol, and properly displayed by the Terminal.
Specification Reference	[SCWS-TS] Chapter 13.3.2 [SCWS-TS] Chapter 13.1
SCR Reference	SCWS-AC-001-M, SCWS-AC-004-M, SCWS-AC-007-M, SCWS-AC-010-M, SCWS-AC-017-M, SCWS-S-028-M, SCWS-S-030-M SCWS-AS-001-M, SCWS-AS-005-M SCWS-S-012-M, SCWS-S-022-M
ETR Reference	ADM_C_M_01, ADM_C_02, ADM_C_M_03, ADM_C_M_06, ADM_C_M_07, ADM_C_M_08, ADM_C_M_11, ADM_S_M_01, ADM_S_M_03, ADM_S_M_07, ADM_S_M_08, S_M_05, S_M_12, S_M_13, S_M_17, S_M_21, C_M_04, D_M_01.
Tool	
Test code	[TEST_CONTENT_DESC] §6.2.1, [TEST_CONTENT]

Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server and SCWS admin client ○ Remote admin SCWS Server • Prerequisite for this test: <ul style="list-style-type: none"> ○ Smart Card card administration agent is configured with remote admin SCWS Server parameters (ip-address, port...). ○ The Remote admin SCWS Server is configured to gzip the html resources. ○ The browser support Transfer-Encoding: gzip.
Test Procedure	<ol style="list-style-type: none"> 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 the browser. 5. In the browser, select the SCWS test portal link (e.g. http://localhost:3516/index.html) 6. In Terminal browser, the new download resource (portal 'oma-502') is displayed 7. In the browser, select the SCWS test portal link (e.g. http://localhost:3516/index.html) 8. Verify the pass criteria below.
Pass-Criteria	In Terminal browser, the new download gzipped resource (portal 'oma-502') is displayed.

6.2.1.7 SCWS-1.2-int-506 Administration and Cache mechanism

Test Case Id	SCWS-1.2-int-506
Test Object	Remote admin SCWS Server, SCWS admin client.
Test Case Description	The purpose is to verify SCWS administration using Cache-Control header in the admin command and browsing cache mechanism based on Entity-Tag validator.
Specification Reference	[SCWS-TS] Chapter 13.3.2 [SCWS-TS] Chapter 9.5.1
SCR Reference	SCWS-S-031-M, SCWS-S-032-M SCWS-ME-011-M, SCWS-ME-012-M
ETR Reference	S_M_20, S_M_22, C_M_02, C_M_03.
Tool	
Test code	[TEST_CONTENT_DESC] §6.2.1, [TEST_CONTENT]

<p>Preconditions</p>	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server and SCWS admin client ○ Remote admin SCWS Server • Prerequisite for this test: <ul style="list-style-type: none"> ○ Smart Card card administration agent is configured with remote admin SCWS Server parameters (ip-address, port...). ○ The Remote admin SCWS Server is configured to gzip the html resources. ○ The browser support Transfer-Encoding: gzip.
<p>Test Procedure</p>	<ol style="list-style-type: none"> 1. In Remote admin SCWS Server: <ul style="list-style-type: none"> • Select Terminal destination address. • Select portal 'oma-506-A'. • Start then wait download finished. • Verify Pass Criteria 1 2. In Terminal, select the browser. <ul style="list-style-type: none"> • Select the SCWS link (/index.html) • Verify Pass Criteria 2 • Return to Terminal idle mode. • Select the SCWS link (/index.html) • Verify Pass Criteria 3 3. In Remote admin SCWS Server: <ul style="list-style-type: none"> • Select Terminal destination address. • Select portal 'oma-506-B'. • Start then wait download finished. • Verify Pass Criteria 4 4. In Terminal, select the browser. <ul style="list-style-type: none"> • Select the SCWS link (/index.html) • Verify Pass Criteria 5

Pass-Criteria	<ol style="list-style-type: none"> 1. The administration session is terminated successfully. <ul style="list-style-type: none"> • The Header Cache-Control is present on each administrative command HTTP PUT. 2. The oma-506-A portal is displayed. <ul style="list-style-type: none"> • HTTP Header Cache-Control is present on each SCWS HTTP response with the same value than Pass-Criteria 1. • HTTP Header Etag is present on each SCWS HTTP response. 3. The oma-506-A portal is displayed (Faster than in Pass-Criteria 2, thanks to the cache mechanism) <ul style="list-style-type: none"> • Conditional HTTP GET request is sent by the WAP-Browser based on Header If-None-Match. • SCWS HTTP response is 304 Not-Modified. 4. The administration session is terminated successfully. 5. The oma-506-B portal is displayed. <ul style="list-style-type: none"> • Conditional HTTP GET request is sent by the WAP-Browser based on Header If-None-Match. • SCWS HTTP response is 200 OK.
----------------------	--

6.2.1.8 SCWS-1.2-int-507 Authorized entities

Test Case Id	SCWS-1.2-int-507
Test Object	Remote admin SCWS Server, SCWS admin client.
Test Case Description	The purpose is to verify that a given authorized entitie (ex: bank) is able to manage its URI and not able to manage other entities URI (ex: transport).
Specification Reference	[SCWS-TS] Chapter 13.3.2 [SCWS-TS] Chapter 13.1
SCR Reference	SCWS-AC-001-M, SCWS-AC-004-M, SCWS-AC-007-M, SCWS-AC-010-M, SCWS-AC-017-M, SCWS-S-028-M, SCWS-AC-013-M, SCWS-AS-001-M, SCWS-AS-005-M SCWS-S-012-M, SCWS-S-022-M, SCWS-S-030-M
ETR Reference	ADM_C_M_01, ADM_C_02, ADM_C_M_03, ADM_C_M_06, ADM_C_M_07, ADM_C_M_08, ADM_C_M_11, ADM_S_M_01, ADM_S_M_03, ADM_S_M_07, ADM_S_M_08, S_M_05, S_M_12, S_M_13, S_M_17, S_M_23, D_M_01.
Tool	
Test code	[TEST_CONTENT_DESC] §6.2.1, [TEST_CONTENT]

<p>Preconditions</p>	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server and SCWS admin client ○ Remote admin SCWS Server • Prerequisite for this test: <ul style="list-style-type: none"> ○ Smart Card card administration agent is configured with remote admin SCWS Server parameters (ip-address, port...). ○ The Remote admin SCWS Server is configured with two authorized entities, one for the bank and one for the transport. ○ Smart Card card administration agent is configured with two authorized entities: bank with URI “/bank/*” and transport with URI “/transport/*”
<p>Test Procedure</p>	<ol style="list-style-type: none"> 1. In Remote admin SCWS Server: <ul style="list-style-type: none"> • Select the bank authorized entity • Select Terminal destination address. • Select the bank portal 'oma-507-bank'. • Start then wait download finished. • Verify Pass Criteria 1 2. In Terminal, select the browser. <ul style="list-style-type: none"> • Select the SCWS link (/bank/index.html) • Verify Pass Criteria 2 3. In Remote admin SCWS Server: <ul style="list-style-type: none"> • Select the bank authorized entity • Select Terminal destination address. • Select the transport portal 'oma-507-transport'. • Start then wait download finished • Verify Pass Criteria 3 4. In Terminal, select the browser. <ul style="list-style-type: none"> • Select the SCWS link (/transport/index.html) • Verify Pass Criteria 4 5. In Remote admin SCWS Server: <ul style="list-style-type: none"> • Select the transport authorized entity • Select Terminal destination address. • Select the transport portal 'oma-507-transport'. • Start then wait download finished • Verify Pass Criteria 5 4. In Terminal, select the browser. <ul style="list-style-type: none"> • Select the SCWS test portal link (/transport/index.html) • Verify Pass Criteria 6

Pass-Criteria	<ol style="list-style-type: none"> 1. The bank administration session is terminated successfully. 2. The bank portal ('oma-507-bank') is displayed. 3. The bank administration session is terminated with error, check status code error 403 on each HTTP command PUT /transport/... 4. The transport portal ('oma-507-transport') is NOT displayed, the status code 404 not found is returned. 5. The transport administration session is terminated successfully. 6. The transport portal ('oma-507-transport') is displayed.
----------------------	---

6.2.1.9 SCWS-1.2-int-508 memory full

Test Case Id	SCWS-1.2-int-508
Test Object	Remote admin SCWS Server, SCWS admin client.
Test Case Description	The purpose is to verify that http-status code 590 Memory full is returned by SCWS Server on http PUT request when server is currently unable to handle the request because the card memory is full
Specification Reference	[SCWS-TS] Chapter 9.4.1.1 [SCWS-TS] Chapter 13.2.1
SCR Reference	SCWS-AC-001-M, SCWS-AC-004-M, SCWS-AC-007-M, SCWS-AC-010-M, SCWS-AC-017-M, SCWS-S-028-M SCWS-AS-001-M, SCWS-AS-005-M SCWS-S-012-M, SCWS-S-022-M, SCWS-S-027-O
ETR Reference	ADM_C_M_01, ADM_C_02, ADM_C_M_03, ADM_C_M_06, ADM_C_M_07, ADM_C_M_08, ADM_C_M_11, ADM_S_M_01, ADM_S_M_03, ADM_S_M_07, ADM_S_M_08, S_M_05, S_M_12, S_M_13, S_M_17, S_O_10, D_M_01.
Tool	Smart Card protocol analyser
Test code	[TEST_CONTENT_DESC] §6.2.1, [TEST_CONTENT]
Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server and SCWS admin client ○ Remote admin SCWS Server • Prerequisite for this test: <ul style="list-style-type: none"> ○ Smart Card card administration agent is configured with remote admin SCWS Server parameters (ip-address, port...). ○ SCWS Server free memory is less than 32Kbytes.
Test Procedure	<ol style="list-style-type: none"> 1. In Remote admin SCWS Server <ul style="list-style-type: none"> • Select Terminal destination address. • Select portal 'oma-502'. • Start then wait download finished. • Verify Pass criteria.

Pass-Criteria	The administration session finished with an error. In Remote admin SCWS Server or Smart Card protocol analyser log files, the http status-code 590 is returned on an http PUT request.
----------------------	---

6.2.2 Connectivity test group

6.2.2.1 SCWS-1.2-int-551 administration session with terminal switched-off

Test Case Id	SCWS-1.2-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-M, SCWS-AC-004-M, SCWS-AC-007-M, SCWS-AC-010-M, SCWS-AC-008-M SCWS-AS-001-M, SCWS-AS-005-M SCWS-S-012-M, SCWS-S-022-M
ETR Reference	ADM_C_M_01, ADM_C_M_02, ADM_C_M_03, ADM_C_M_04, ADM_C_M_06, ADM_C_M_07, ADM_C_M_08, ADM_C_M_11, ADM_S_M_01, ADM_S_M_03, ADM_S_M_07, ADM_S_M_08, S_M_05, S_M_12, S_M_13, S_M_17, D_M_01.
Tool	
Test code	[TEST_CONTENT_DESC] §6.2.1, [TEST_CONTENT]
Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server and SCWS admin client ○ Remote admin SCWS Server • Prerequisite for this test: <ul style="list-style-type: none"> ○ Smart Card card administration agent is configured with remote admin SCWS Server parameters (ip-address, port...). ○ The Connection parameters (BIP OPEN CHANNEL TLV) must included an Alpha Identifier "open remote connection".

Test Procedure	<ol style="list-style-type: none"> 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 terminal is updated from the suspended command to update the portal. 7. Wait SCWS admin client retry policy expiration delay. 8. In the browser, select the SCWS test portal link (e.g. http://localhost:3516/index.html) 9. Verify the pass criteria below.
Pass-Criteria	<p>The portal 'oma-551' is displayed.</p> <p>On Terminal switch-on the suspended action occurs and the SCWS is updated.</p>

6.2.2.2 SCWS-1.2-int-552 administration session with network coverage loss

Test Case Id	SCWS-1.2-int-552
Test Object	Remote admin SCWS Server, SCWS admin client.
Test Case Description	<p>The purpose is to verify that SCWS admin client retry administration session when the current admin session is interrupted by network coverage loss.</p> <p>This test case will test SCWS admin client resume admin session, BIP event channel status link-dropped, BIP command SEND_DATA, RECEIVED_DATA terminal response temporary-error or permanent-error.</p>
Specification Reference	[SCWS-TS] Chapter 13.3.2.8
SCR Reference	<p>SCWS-AC-001-M, SCWS-AC-004-M, SCWS-AC-007-M, SCWS-AC-010-M, SCWS-AC-008-M</p> <p>SCWS-AS-001-M, SCWS-AS-005-M</p> <p>SCWS-S-012-M, SCWS-S-022-M</p>
ETR Reference	<p>ADM_C_M_01, ADM_C_02, ADM_C_M_03, ADM_C_M_04, ADM_C_M_06, ADM_C_M_07, ADM_C_M_08, ADM_C_M_11, ADM_S_M_01, ADM_S_M_03, ADM_S_M_07, ADM_S_M_08, S_M_05, S_M_12, S_M_13, S_M_17, D_M_01.</p>
Tool	
Test code	[TEST_CONTENT_DESC] §6.2.1, [TEST_CONTENT]

Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server and SCWS admin client ○ Remote admin SCWS Server ○ Anechoic chamber / Faraday cage. • Prerequisite for this test: <ul style="list-style-type: none"> ○ Smart Card card administration agent is configured with remote admin SCWS Server parameters (ip-address, port...). ○ The Connection parameters (BIP OPEN CHANNEL TLV) must included an Alpha Identifier “open remote connection”.
Test Procedure	<ol style="list-style-type: none"> 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 Anechoic chamber / Faraday cage 5. SCWS admin client shall start the retry policy. 6. Network connection is re-established. 7. Wait SCWS admin client retry policy expiration delay. 8. In the browser, select the SCWS test portal link (e.g. 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-1.2-int-553 administration session is abandoned

Test Case Id	SCWS-1.2-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-M, SCWS-AC-004-M, SCWS-AC-007-M, SCWS-AC-010-M, SCWS-AC-008-M, SCWS-AC-009-M SCWS-AS-001-M, SCWS-AS-005-M SCWS-S-012-M
ETR Reference	ADM_C_M_01, ADM_C_02, ADM_C_M_03, ADM_C_M_04, ADM_C_M_05, ADM_C_M_06, ADM_C_M_07, ADM_C_M_08, ADM_C_M_11, ADM_S_M_01, ADM_S_M_03, ADM_S_M_07, ADM_S_M_08, S_M_05, S_M_12, S_M_13, S_M_17, D_M_01.
Tool	
Test code	[TEST_CONTENT_DESC] §6.2.1, [TEST_CONTENT]

Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server and SCWS admin client ○ Remote admin SCWS Server • Prerequisite for this test: <ul style="list-style-type: none"> ○ Smart Card card administration agent is configured with remote admin SCWS Server parameters (ip-address, port...).
Test Procedure	<ol style="list-style-type: none"> 1. In Remote admin SCWS Server, enter wrong connection parameters for the push SMS to the Terminal (e.g wrong tcp-ip address). 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 establishment 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-1.2-int-554 administration session and browsing

Test Case Id	SCWS-1.2-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-M, SCWS-AC-004-M, SCWS-AC-007-M, SCWS-AC-010-M SCWS-AS-001-M, SCWS-AS-005-M SCWS-S-012-M, SCWS-S-022-M
ETR Reference	ADM_C_M_01, ADM_C_02, ADM_C_M_03, ADM_C_M_06, ADM_C_M_07, ADM_C_M_08, ADM_C_M_11, ADM_S_M_01, ADM_S_M_03, ADM_S_M_07, ADM_S_M_08, S_M_05, S_M_12, S_M_13, S_M_17, D_M_01.
Tool	
Test code	[TEST_CONTENT_DESC] §6.2.1 §6.1.1, [TEST_CONTENT]

Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server and SCWS admin client ○ Remote admin SCWS Server • Prerequisite for this test: <ul style="list-style-type: none"> ○ Smart Card card administration agent is configured with remote admin SCWS Server parameters (ip-address, port...). ○ SCWS server is provisioned with test portal.
Test Procedure	<ol style="list-style-type: none"> 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 establishment between remote admin server and admin client. 5. In Terminal, select the browser. 6. Select the SCWS test portal link (e.g. http://localhost:3516/index.html) 7. SCWS server home page is displayed. 8. In Remote admin SCWS Server, wait download finished. 9. In Terminal, select the browser. 10. In the browser, select the SCWS test portal link (e.g. http://localhost:3516/index.html) 11. Verify the pass criteria below.
Pass-Criteria	The portal 'oma-554' is displayed.

6.2.2.5 SCWS-1.2-int-555 admin session and other CAT application

Test Case Id	SCWS-1.2-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 triggering event (push SMS) is received in other card application toolkit context.
Specification Reference	[SCWS-TS] Chapter 13.3.2
SCR Reference	SCWS-AC-001-M, SCWS-AC-004-M, SCWS-AC-007-M, SCWS-AC-010-M SCWS-AS-001-M, SCWS-AS-005-M SCWS-S-012-M, SCWS-S-022-M
ETR Reference	ADM_C_M_01, ADM_C_02, ADM_C_M_03, ADM_C_M_06, ADM_C_M_07, ADM_C_M_08, ADM_C_M_11, ADM_S_M_01, ADM_S_M_03, ADM_S_M_07, ADM_S_M_08, S_M_05, S_M_12, S_M_13, S_M_17, D_M_01.
Tool	
Test code	[TEST_CONTENT_DESC] §6.2.1, §6.3.1 [TEST_CONTENT]

Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server and SCWS admin client ○ Remote admin SCWS Server • Prerequisite for this test: <ul style="list-style-type: none"> ○ Smart Card card administration agent is configured with remote admin SCWS Server parameters (ip-address, port...). ○ SCWS server is provisioned with test portal. ○ Smart Card 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	<ol style="list-style-type: none"> 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 the browser. 9. In the browser, select the SCWS test portal link (e.g. http://localhost:3516/index.html) 10. Verify the pass criteria below.
Pass-Criteria	The portal 'oma-555' is displayed.

6.2.2.6 SCWS-1.2-int-556 PUT_WITH_ENVELOPE

Test Case Id	SCWS-1.2-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-M, SCWS-AC-004-M, SCWS-AC-007-M, SCWS-AC-010-M SCWS-AS-001-M, SCWS-AS-005-M SCWS-S-012-M, SCWS-S-022-M
ETR Reference	ADM_C_M_01, ADM_C_02, ADM_C_M_03, ADM_C_M_06, ADM_C_M_07, ADM_C_M_08, ADM_C_M_11, ADM_S_M_01, ADM_S_M_03, ADM_S_M_07, ADM_S_M_08, S_M_05, S_M_12, S_M_13, S_M_17, D_M_01.
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	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal A and Terminal B capable of sending a SMS to the terminal hosting the SCWS ○ Smart Card 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: <ul style="list-style-type: none"> ○ Smart Card 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	<ol style="list-style-type: none"> 1. In Remote admin SCWS Server , select Terminal A destination address 2. Commanding Remote admin SCWS Server, select portal ‘oma-556’ 3. In Remote admin SCWS Server, start portal update. 4. In the Terminal when “open remote connection” message was displayed, then send SMS from Terminal B to Terminal A. 5. Verify the pass criteria 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-1.2-int-600 TLS 1.0 and TLS_PSK_WITH_3DES_EDE_CBC_SHA

Test Case Id	SCWS-1.2-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 TLS 1.0 and the cipher suite TLS_PSK_WITH_3DES_EDE_CBC_SHA.
Specification Reference	[SCWS-TS] Chapter 11
SCR Reference	<p>SCWS-AC-001-M, SCWS-AC-004-M, SCWS-AC-007-M, SCWS-AC-010-M, SCWS-AC-011-M, SCWS-AC-012-M, SCWS-AC-014-M, SCWS-AC-019-M</p> <p>SCWS-AS-001-M, SCWS-AS-002-M, SCWS-AS-003-M, SCWS-AS-005-M, SCWS-AS-007-M, SCWS-AS-010-M</p> <p>SCWS-S-012-M, SCWS-S-022-M</p>

ETR Reference	ADM_C_M_01, ADM_C_02, ADM_C_M_03, ADM_C_M_06, ADM_C_M_07, ADM_C_M_08, ADM_C_M_08_A, ADM_C_M_09, ADM_C_M_11, ADM_S_M_01, ADM_S_M_03, ADM_S_M_07, ADM_S_M_08, ADM_S_M_06_A, S_M_05, S_M_12, S_M_13, S_M_17, D_M_01.
Tool	
Test code	[TEST_CONTENT_DESC] §6.2.1, [TEST_CONTENT]
Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server and SCWS admin client ○ Remote admin SCWS Server • Prerequisite for this test: <ul style="list-style-type: none"> ○ Smart Card card administration agent is configured with remote admin server parameters (ip-address, port...). ○ Smart Card card administration agent and remote admin server are configured to process admin session through TLS 1.0 and cipher suite TLS_PSK_WITH_3DES_EDE_CBC_SHA.
Test Procedure	<ol style="list-style-type: none"> 1. In Remote admin SCWS Server, <ol style="list-style-type: none"> 1.1 Select Terminal destination address. 1.2 Select portal 'oma-600'. 1.3 Start then wait download finished. 2. In Terminal, select the browser. <ol style="list-style-type: none"> 2.1 Select the SCWS test portal link (e.g. http://localhost:3516/index.html). 2.2 Verify the pass criteria below.
Pass-Criteria	The portal 'oma-600' is displayed.

6.2.3.2 SCWS-1.2-int-601 TLS 1.0 and TLS_PSK_WITH_AES_128_CBC_SHA

Test Case Id	SCWS-1.2-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 TLS 1.0 and the cipher suite TLS_PSK_WITH_AES_128_CBC_SHA.
Specification Reference	[SCWS-TS] Chapter 11
SCR Reference	SCWS-AC-001-M, SCWS-AC-004-M, SCWS-AC-007-M, SCWS-AC-010-M, SCWS-AC-011-M, SCWS-AC-012-M, SCWS-AC-015-M, SCWS-AC-019-M SCWS-AS-001-M, SCWS-AS-002-M, SCWS-AS-003-M, SCWS-AS-005-M, SCWS-AS-008-M, SCWS-AS-010-M SCWS-S-012-M, SCWS-S-022-M

ETR Reference	ADM_C_M_01, ADM_C_02, ADM_C_M_03, ADM_C_M_06, ADM_C_M_07, ADM_C_M_08, ADM_C_M_08_B, ADM_C_M_09, ADM_C_M_11, ADM_S_M_01, ADM_S_M_03, ADM_S_M_07, ADM_S_M_08, ADM_S_M_06_B, S_M_05, S_M_12, S_M_13, S_M_17, D_M_01.
Tool	
Test code	[TEST_CONTENT_DESC] §6.2.1, [TEST_CONTENT]
Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server and SCWS admin client ○ Remote admin SCWS Server • Prerequisite for this test: <ul style="list-style-type: none"> ○ Smart Card card administration agent is configured with remote admin SCWS Server parameters (ip-address, port...). ○ Smart Card card administration agent and remote admin server are configured to process admin session through TLS 1.0 and cipher suite TLS_PSK_WITH_AES_128_CBC_SHA.
Test Procedure	<ol style="list-style-type: none"> 1. In Remote admin SCWS Server, <ol style="list-style-type: none"> 1.1 Select Terminal destination address. 1.2 Select portal 'oma-601'. 1.3 Start then wait download finished. 2. In Terminal, select the browser. <ol style="list-style-type: none"> 1.1 Select the SCWS test portal link (e.g. http://localhost:3516/index.html) 1.2 Verify the pass criteria below.
Pass-Criteria	The portal 'oma-601' is displayed.

6.2.3.3 SCWS-1.2-int-602 TLS 1.0 and TLS_PSK_WITH_NULL_SHA

Test Case Id	SCWS-1.2-int-602
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 TLS 1.0 and the cipher suite TLS_PSK_WITH_NULL_SHA.
Specification Reference	[SCWS-TS] Chapter 11
SCR Reference	SCWS-AC-001-M, SCWS-AC-004-M, SCWS-AC-007-M, SCWS-AC-010-M, SCWS-AC-011-M, SCWS-AC-012-M, SCWS-AC-016-M, SCWS-AC-019-M SCWS-AS-001-M, SCWS-AS-002-M, SCWS-AS-003-M, SCWS-AS-005-M, SCWS-AS-008-M, SCWS-AS-009-M, SCWS-AS-010-M SCWS-S-012-M, SCWS-S-022-M

ETR Reference	ADM_C_M_01, ADM_C_02, ADM_C_M_03, ADM_C_M_06, ADM_C_M_07, ADM_C_M_08, ADM_C_M_08_C, ADM_C_M_09, ADM_C_M_11, ADM_S_M_01, ADM_S_M_03, ADM_S_M_07, ADM_S_M_08, ADM_S_M_06_C, S_M_05, S_M_12, S_M_13, S_M_17, D_M_01.
Tool	
Test code	[TEST_CONTENT_DESC] §6.2.1, [TEST_CONTENT]
Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server and SCWS admin client ○ Remote admin SCWS Server • Prerequisite for this test: <ul style="list-style-type: none"> ○ Smart Card card administration agent is configured with remote admin SCWS Server parameters (ip-address, port...). ○ Smart Card card administration agent and remote admin server are configured to process admin session through TLS 1.0 and cipher suite TLS_PSK_WITH_NULL_SHA.
Test Procedure	<ol style="list-style-type: none"> 1. In Remote admin SCWS Server, <ol style="list-style-type: none"> 1.1 Select Terminal destination address. 1.2 Select portal 'oma-601'. 1.3 Start then wait download finished. 1.4 Verify the pass criteria 1. 2. In Terminal, select the browser, <ol style="list-style-type: none"> 1.1 Select the SCWS test portal path (/index.html) 1.2 Verify the pass criteria 2.
Pass-Criteria	<ol style="list-style-type: none"> 1. The portal 'oma-601' correctly downloaded using TLS 1.0 and the TLS cipher suite TLS_PSK_WITH_NULL_SHA. 2. The portal 'oma-601' is displayed.

6.2.3.4 SCWS-1.2-int-603 TLS1.1 and TLS_PSK_WITH_3DES_EDE_CBC_SHA

Test Case Id	SCWS-1.2-int-603
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 TLS 1.1 and the cipher suite TLS_PSK_WITH_3DES_EDE_CBC_SHA.
Specification Reference	[SCWS-TS] Chapter 11
SCR Reference	SCWS-AC-001-M, SCWS-AC-004-M, SCWS-AC-007-M, SCWS-AC-010-M, SCWS-AC-011-M, SCWS-AC-012-M, SCWS-AC-014-M, SCWS-AC-020-O SCWS-AS-001-M, SCWS-AS-002-M, SCWS-AS-003-M, SCWS-AS-005-M, SCWS-AS-007-M, SCWS-AS-011-O SCWS-S-012-M, SCWS-S-022-M

ETR Reference	ADM_C_M_01, ADM_C_02, ADM_C_M_03, ADM_C_M_06, ADM_C_M_08, ADM_C_M_08_A, ADM_C_M_09, ADM_C_M_11, ADM_C_O_04, ADM_S_M_01, ADM_S_M_03, ADM_S_M_08, ADM_S_M_06_A, ADM_S_O_02, S_M_05, S_M_12, S_M_13, S_M_17, D_M_01.
Tool	
Test code	[TEST_CONTENT_DESC] §6.2.1, [TEST_CONTENT]
Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server and SCWS admin client ○ Remote admin SCWS Server • Prerequisite for this test: <ul style="list-style-type: none"> ○ Smart Card card administration agent is configured with remote admin server parameters (ip-address, port...). ○ Smart Card card administration agent and remote admin server are configured to process admin session through TLS 1.1 and cipher suite TLS_PSK_WITH_3DES_EDE_CBC_SHA.
Test Procedure	<ol style="list-style-type: none"> 1. In Remote admin SCWS Server <ol style="list-style-type: none"> 1.1. Select Terminal destination address. 1.2. Select portal 'oma-600'. 1.3. Start then wait download finished. 1.4. Verify the pass criteria 1. 2. In Terminal, select the browser <ol style="list-style-type: none"> 2.1. Select the SCWS test portal path (/index.html) 2.2. Verify the pass criteria 2.
Pass-Criteria	<ol style="list-style-type: none"> 3. The portal 'oma-600' correctly downloaded using the TLS 1.1 with the cipher suite TLS_PSK_WITH_3DES_EDE_CBC_SHA. 4. The portal 'oma-600' is displayed.

6.2.3.5 SCWS-1.2-int-604 TLS 1.1 and TLS_PSK_WITH_AES_128_CBC_SHA

Test Case Id	SCWS-1.2-int-604
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 TLS 1.1 and the cipher suite TLS_PSK_WITH_AES_128_CBC_SHA.
Specification Reference	[SCWS-TS] Chapter 11
SCR Reference	SCWS-AC-001-M, SCWS-AC-004-M, SCWS-AC-007-M, SCWS-AC-010-M, SCWS-AC-011-M, SCWS-AC-012-M, SCWS-AC-015-M, SCWS-AC-020-O SCWS-AS-001-M, SCWS-AS-002-M, SCWS-AS-003-M, SCWS-AS-005-M, SCWS-AS-008-M, SCWS-AS-011-O SCWS-S-012-M, SCWS-S-022-M

ETR Reference	ADM_C_M_01, ADM_C_02, ADM_C_M_03, ADM_C_M_06, ADM_C_M_08, ADM_C_M_08_B, ADM_C_M_09, ADM_C_M_11, ADM_C_O_04, ADM_S_M_01, ADM_S_M_03, ADM_S_M_08, ADM_S_M_06_B, ADM_S_O_02, S_M_05, S_M_12, S_M_13, S_M_17, D_M_01.
Tool	
Test code	[TEST_CONTENT_DESC] §6.2.1, [TEST_CONTENT]
Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server and SCWS admin client ○ Remote admin SCWS Server • Prerequisite for this test: <ul style="list-style-type: none"> ○ Smart Card card administration agent is configured with remote admin server parameters (ip-address, port...). ○ Smart Card card administration agent and remote admin server are configured to process admin session through TLS 1.1 and cipher suite TLS_PSK_WITH_AES_128_CBC_SHA.
Test Procedure	<ol style="list-style-type: none"> 1. In Remote admin SCWS Server <ol style="list-style-type: none"> 1.1. Select Terminal destination address. 1.2. Select portal 'oma-601'. 1.3. Start then wait download finished. 1.4. Verify the pass criteria 1. 2. In Terminal, select the browser <ol style="list-style-type: none"> 2.1. Select the SCWS test portal path (/index.html) 2.2. Verify the pass criteria 2.
Pass-Criteria	<ol style="list-style-type: none"> 1. The portal 'oma-601' correctly downloaded using the TLS 1.1 with the cipher suite TLS_PSK_WITH_AES_128_CBC_SHA. 2. The portal 'oma-601' is displayed.

6.2.3.6 SCWS-1.2-int-605 TLS1.1 and TLS_PSK_WITH_NULL_SHA

Test Case Id	SCWS-1.2-int-605
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 TLS 1.1 and the cipher suite TLS_PSK_WITH_NULL_SHA.
Specification Reference	[SCWS-TS] Chapter 11
SCR Reference	SCWS-AC-001-M, SCWS-AC-004-M, SCWS-AC-007-M, SCWS-AC-010-M, SCWS-AC-011-M, SCWS-AC-012-M, SCWS-AC-016-M, SCWS-AC-020-O SCWS-AS-001-M, SCWS-AS-002-M, SCWS-AS-003-M, SCWS-AS-005-M, SCWS-AS-009-M, SCWS-AS-011-O SCWS-S-012-M, SCWS-S-022-M

ETR Reference	ADM_C_M_01, ADM_C_02, ADM_C_M_03, ADM_C_M_06, ADM_C_M_08, ADM_C_M_08_C, ADM_C_M_09, ADM_C_M_11, ADM_C_O_04, ADM_S_M_01, ADM_S_M_03, ADM_S_M_08, ADM_S_M_06_C, ADM_S_O_02, S_M_05, S_M_12, S_M_13, S_M_17, D_M_01.
Tool	
Test code	[TEST_CONTENT_DESC] §6.2.1, [TEST_CONTENT]
Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server and SCWS admin client ○ Remote admin SCWS Server • Prerequisite for this test: <ul style="list-style-type: none"> ○ Smart Card card administration agent is configured with remote admin server parameters (ip-address, port...). ○ Smart Card card administration agent and remote admin server are configured to process admin session through TLS 1.1 and cipher suite TLS_PSK_WITH_NULL_SHA.
Test Procedure	<ol style="list-style-type: none"> 1. In Remote admin SCWS Server <ol style="list-style-type: none"> 1.1. Select Terminal destination address. 1.2. Select portal 'oma-601'. 1.3. Start then wait download finished. 1.4. Verify the pass criteria 1. 2. In Terminal, select the browser. <ol style="list-style-type: none"> 2.1. Select the SCWS test portal path (/index.html) 2.2. Verify the pass criteria 2.
Pass-Criteria	<ol style="list-style-type: none"> 1. The portal 'oma-601' correctly downloaded using the TLS 1.1 with the cipher suite TLS_PSK_WITH_NULL_SHA. 2. The portal 'oma-601' is displayed.

6.2.3.7 SCWS-1.2-int-606 TLS1.2 and TLS_PSK_WITH_3DES_EDE_CBC_SHA

Test Case Id	SCWS-1.2-int-606
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 TLS 1.2 and the cipher suite TLS_PSK_WITH_3DES_EDE_CBC_SHA.
Specification Reference	[SCWS-TS] Chapter 11
SCR Reference	SCWS-AC-001-M, SCWS-AC-004-M, SCWS-AC-007-M, SCWS-AC-010-M, SCWS-AC-011-M, SCWS-AC-012-M, SCWS-AC-014-M, SCWS-AC-021-O SCWS-AS-001-M, SCWS-AS-002-M, SCWS-AS-003-M, SCWS-AS-005-M, SCWS-AS-007-M, SCWS-AS-012-O SCWS-S-012-M, SCWS-S-022-M

ETR Reference	ADM_C_M_01, ADM_C_02, ADM_C_M_03, ADM_C_M_06, ADM_C_M_08, ADM_C_M_08_A, ADM_C_M_09, ADM_C_M_11, ADM_C_O_05, ADM_S_M_01, ADM_S_M_03, ADM_S_M_08, ADM_S_M_06_A, ADM_S_O_03, S_M_05, S_M_12, S_M_13, S_M_17, D_M_01.
Tool	
Test code	[TEST_CONTENT_DESC] §6.2.1, [TEST_CONTENT]
Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server and SCWS admin client ○ Remote admin SCWS Server • Prerequisite for this test: <ul style="list-style-type: none"> ○ Smart Card card administration agent is configured with remote admin server parameters (ip-address, port...). ○ Smart Card card administration agent and remote admin server are configured to process admin session through TLS 1.2 and cipher suite TLS_PSK_WITH_3DES_EDE_CBC_SHA.
Test Procedure	<ol style="list-style-type: none"> 1. In Remote admin SCWS Server <ol style="list-style-type: none"> 1.1. Select Terminal destination address. 1.2. Select portal 'oma-600'. 1.3. Start then wait download finished. 1.4. Verify the pass criteria 1. 2. In Terminal, select the browser <ol style="list-style-type: none"> 2.1. Select the SCWS test portal path (/index.html) 2.2. Verify the pass criteria 2.
Pass-Criteria	<ol style="list-style-type: none"> 1. The portal 'oma-600' correctly downloaded using the TLS 1.2 with the cipher suite TLS_PSK_WITH_3DES_EDE_CBC_SHA. 2. The portal 'oma-600' is displayed.

6.2.3.8 SCWS-1.2-int-607 TLS 1.2 and TLS_PSK_WITH_AES_128_CBC_SHA

Test Case Id	SCWS-1.2-int-607
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 TLS 1.2 and the cipher suite TLS_PSK_WITH_AES_128_CBC_SHA.
Specification Reference	[SCWS-TS] Chapter 11
SCR Reference	SCWS-AC-001-M, SCWS-AC-004-M, SCWS-AC-007-M, SCWS-AC-010-M, SCWS-AC-011-M, SCWS-AC-012-M, SCWS-AC-015-M SCWS-AC-021-O SCWS-AS-001-M, SCWS-AS-002-M, SCWS-AS-003-M, SCWS-AS-005-M, SCWS-AS-008-M, SCWS-AS-012-O SCWS-S-012-M, SCWS-S-022-M

ETR Reference	ADM_C_M_01, ADM_C_02, ADM_C_M_03, ADM_C_M_06, ADM_C_M_08, ADM_C_M_08_B, ADM_C_M_09, ADM_C_M_11, ADM_C_O_05, ADM_S_M_01, ADM_S_M_03, ADM_S_M_08, ADM_S_M_06_B, ADM_S_O_03, S_M_05, S_M_12, S_M_13, S_M_17, D_M_01.
Tool	
Test code	[TEST_CONTENT_DESC] §6.2.1, [TEST_CONTENT]
Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server and SCWS admin client ○ Remote admin SCWS Server • Prerequisite for this test: <ul style="list-style-type: none"> ○ Smart Card card administration agent is configured with remote admin server parameters (ip-address, port...). ○ Smart Card card administration agent and remote admin server are configured to process admin session through TLS 1.2 and cipher suite TLS_PSK_WITH_AES_128_CBC_SHA.
Test Procedure	<ol style="list-style-type: none"> 1. In Remote admin SCWS Server <ol style="list-style-type: none"> 1.1. Select Terminal destination address. 1.2. Select portal 'oma-601'. 1.3. Start then wait download finished. 1.4. Verify the pass criteria 1. 2. In Terminal, select the browser <ol style="list-style-type: none"> 2.1. Select the SCWS test portal path (/index.html) 2.2. Verify the pass criteria 2.
Pass-Criteria	<ol style="list-style-type: none"> 1. The portal 'oma-601' correctly downloaded using the TLS 1.2 with the cipher suite TLS_PSK_WITH_AES_128_CBC_SHA. 2. The portal 'oma-601' is displayed.

6.2.3.9 SCWS-1.2-int-608 TLS1.2 and TLS_PSK_WITH_NULL_SHA

Test Case Id	SCWS-1.2-int-608
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 TLS 1.2 and the cipher suite TLS_PSK_WITH_NULL_SHA.
Specification Reference	[SCWS-TS] Chapter 11
SCR Reference	SCWS-AC-001-M, SCWS-AC-004-M, SCWS-AC-007-M, SCWS-AC-010-M, SCWS-AC-011-M, SCWS-AC-012-M, SCWS-AC-016-M, SCWS-AC-021-O SCWS-AS-001-M, SCWS-AS-002-M, SCWS-AS-003-M, SCWS-AS-005-M, SCWS-AS-009-M, SCWS-AS-012-O SCWS-S-012-M, SCWS-S-022-M

ETR Reference	ADM_C_M_01, ADM_C_02, ADM_C_M_03, ADM_C_M_06, ADM_C_M_08, ADM_C_M_08_C, ADM_C_M_09, ADM_C_M_11, ADM_C_O_05, ADM_S_M_01, ADM_S_M_03, ADM_S_M_08, ADM_S_M_06_C, ADM_S_O_03, S_M_05, S_M_12, S_M_13, S_M_17, D_M_01.
Tool	
Test code	[TEST_CONTENT_DESC] §6.2.1, [TEST_CONTENT]
Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server and SCWS admin client ○ Remote admin SCWS Server • Prerequisite for this test: <ul style="list-style-type: none"> ○ Smart Card card administration agent is configured with remote admin server parameters (ip-address, port...). ○ Smart Card card administration agent and remote admin server are configured to process admin session through TLS 1.2 and cipher suite TLS_PSK_WITH_NULL_SHA.
Test Procedure	<ol style="list-style-type: none"> 1. In Remote admin SCWS Server <ol style="list-style-type: none"> 1.1. Select Terminal destination address. 1.2. Select portal 'oma-601'. 1.3. Start then wait download finished. 1.4. Verify the pass criteria 1. 2. In Terminal, select the browser <ol style="list-style-type: none"> 2.1. Select the SCWS test portal path (/index.html) 2.2. Verify the pass criteria 2.
Pass-Criteria	<ol style="list-style-type: none"> 1. The portal 'oma-601' correctly downloaded using the TLS 1.2 with the cipher suite TLS_PSK_WITH_NULL_SHA. 2. The portal 'oma-601' is displayed.

6.2.3.10 SCWS-1.2-int-609 TLS 1.2 and TLS_PSK_WITH_AES_128_CBC_SHA256

Test Case Id	SCWS-1.2-int-609
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 TLS 1.2 and the cipher suite TLS_PSK_WITH_AES_128_CBC_SHA256.
Specification Reference	[SCWS-TS] Chapter 11
SCR Reference	SCWS-AC-001-M, SCWS-AC-004-M, SCWS-AC-007-M, SCWS-AC-010-M, SCWS-AC-011-M, SCWS-AC-012-M, SCWS-AC-022-O, SCWS-AC-021-O SCWS-AS-001-M, SCWS-AS-002-M, SCWS-AS-003-M, SCWS-AS-005-M, SCWS-AS-013-O, SCWS-AS-012-O SCWS-S-012-M, SCWS-S-022-M

ETR Reference	ADM_C_M_01, ADM_C_02, ADM_C_M_03, ADM_C_M_06, ADM_C_M_08, ADM_C_M_09, ADM_C_M_11, ADM_C_O_05, ADM_C_O_06, ADM_S_M_01, ADM_S_M_03, ADM_S_M_08, ADM_S_O_03, ADM_S_O_04, S_M_05, S_M_12, S_M_13, S_M_17, D_M_01.
Tool	
Test code	[TEST_CONTENT_DESC] §6.2.1, [TEST_CONTENT]
Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server and SCWS admin client ○ Remote admin SCWS Server • Prerequisite for this test: <ul style="list-style-type: none"> ○ Smart Card card administration agent is configured with remote admin server parameters (ip-address, port...). ○ Smart Card card administration agent and remote admin server are configured to process admin session through TLS 1.2 and cipher suite TLS_PSK_WITH_AES_128_CBC_SHA256.
Test Procedure	<ol style="list-style-type: none"> 1. In Remote admin SCWS Server <ol style="list-style-type: none"> 1.1. Select Terminal destination address. 1.2. Select portal 'oma-601'. 1.3. Start then wait download finished. 1.4. Verify the pass criteria 1. 2. In Terminal, select the browser <ol style="list-style-type: none"> 2.1. Select the SCWS test portal path (/index.html) 2.2. Verify the pass criteria 2.
Pass-Criteria	<ol style="list-style-type: none"> 1. The portal 'oma-601' correctly downloaded using the TLS 1.2 with the cipher suite TLS_PSK_WITH_AES_128_CBC_SHA256. 2. The portal 'oma-601' is displayed.

6.2.3.11 SCWS-1.2-int-610 TLS1.2 and TLS_PSK_WITH_NULL_SHA256

Test Case Id	SCWS-1.2-int-610
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 TLS 1.2 and the cipher suite TLS_PSK_WITH_NULL_SHA256.
Specification Reference	[SCWS-TS] Chapter 11
SCR Reference	SCWS-AC-001-M, SCWS-AC-004-M, SCWS-AC-007-M, SCWS-AC-010-M, SCWS-AC-011-M, SCWS-AC-012-M, SCWS-AC-023-O, SCWS-AC-021-O SCWS-AS-001-M, SCWS-AS-002-M, SCWS-AS-003-M, SCWS-AS-005-M, SCWS-AS-014-O, SCWS-AS-012-O SCWS-S-012-M, SCWS-S-022-M

ETR Reference	ADM_C_M_01, ADM_C_02, ADM_C_M_03, ADM_C_M_06, ADM_C_M_08, ADM_C_M_09, ADM_C_M_11, ADM_C_O_04, ADM_C_O_07, ADM_S_M_01, ADM_S_M_03, ADM_S_M_08, ADM_S_O_02, ADM_S_O_05, S_M_05, S_M_12, S_M_13, S_M_17, D_M_01.
Tool	
Test code	[TEST_CONTENT_DESC] §6.2.1, [TEST_CONTENT]
Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server and SCWS admin client ○ Remote admin SCWS Server • Prerequisite for this test: <ul style="list-style-type: none"> ○ Smart Card card administration agent is configured with remote admin server parameters (ip-address, port...). ○ Smart Card card administration agent and remote admin server are configured to process admin session through TLS 1.2 and cipher suite TLS_PSK_WITH_NULL_SHA256.
Test Procedure	<ol style="list-style-type: none"> 1. In Remote admin SCWS Server <ol style="list-style-type: none"> 1.1. Select Terminal destination address. 1.2. Select portal 'oma-601'. 1.3. Start then wait download finished. 1.4. Verify the pass criteria 1. 2. In Terminal, select the browser <ol style="list-style-type: none"> 2.1. Select the SCWS test portal path (/index.html) 2.2. Verify the pass criteria 2.
Pass-Criteria	<ol style="list-style-type: none"> 1. The portal 'oma-601' correctly downloaded using the TLS 1.2 with the cipher suite TLS_PSK_WITH_NULL_SHA256. 2. The portal 'oma-601' is displayed.

6.2.4 Administration using lightweight protocol

6.2.4.1 SCWS-1.2-int-701 LIGHTWEIGHT and deactivation of the SCWS application

Test Case Id	SCWS-1.2-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-M SCWS-S-011-M, SCWS-S-022-M, SCWS-S-023-M

ETR Reference	ADM_S_M_04, S_M_14, S_M_16, S_M_18.
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, [TEST_CONTENT]
Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server and SCWS admin client ○ Remote admin SCWS Server • Prerequisite for this test: <ul style="list-style-type: none"> ○ SCWS server is provisioned with the test content.
Test Procedure	<ol style="list-style-type: none"> 1. In Remote admin SCWS Server, select Terminal destination address. 2. In Remote admin SCWS Server, send a SMS with admin command to deactivate the SCWS. 3. In Terminal, select the 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 the browser. 7. Verify the pass criteria 2.
Pass-Criteria	<ol style="list-style-type: none"> 1. In the browser, select test portal link (e.g. http://localhost:3516/index.html), verify that a Terminal error is displayed. 2. In the browser, select test portal link (e.g. http://localhost:3516/index.html), verify that portal is displayed.

6.2.5 Transport protocol test group

6.2.5.1 SCWS-1.2-int-800 Admin session using BIP client mode

Test Case Id	SCWS-1.2-int-800
Test Object	Remote admin SCWS Server, SCWS admin client, device.
Test Case Description	The purpose is to verify single resource 1kb (portal 'oma-500') can be sent, received through full admin protocol using the BIP client protocol.
Specification Reference	[SCWS-TS] Chapter 13.3.2 [SCWS-TS] Chapter 13.1
SCR Reference	SCWS-AC-001-M, SCWS-AC-002-O, SCWS-AC-004-M, SCWS-AC-007-M, SCWS-AC-010-M SCWS-AS-001-M, SCWS-AS-005-M SCWS-S-012-M, SCWS-S-022-M SCWS-ME-007-O

ETR Reference	ADM_C_M_01, ADM_C_02, ADM_C_M_03, ADM_C_M_06, ADM_C_M_07, ADM_C_M_08, ADM_C_M_11, ADM_C_M_12, ADM_S_M_01, ADM_S_M_03, ADM_S_M_07, ADM_S_M_08, S_M_05, S_M_12, S_M_13, S_M_17, D_M_01, D_M_03.
Tool	Smart Card protocol analyser
Test code	[TEST_CONTENT_DESC] §6.1.1, §6.1.2, [TEST_CONTENT]
Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal implementing the BIP client protocol ○ Smart Card with SCWS server and SCWS admin client implementing the BIP client protocol ○ Remote admin SCWS Server • Prerequisite for this test: <ul style="list-style-type: none"> ○ Smart Card card administration agent is configured with remote admin SCWS Server parameters (ip-address, port...).
Test Procedure	<ol style="list-style-type: none"> 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 the browser. 5. Select the SCWS test portal link (e.g. http://localhost:3516/index.html) 6. Verify the pass criteria below.
Pass-Criteria	<p>In Terminal browser, the new download resource (portal 'oma-500') is displayed.</p> <p>The BIP client mode protocol has been used (check using a transport protocol analyser).</p>

6.2.5.2 SCWS-1.2-int-801 Admin session using TCP/IP

Test Case Id	SCWS-1.2-int-801
Test Object	Remote admin SCWS Server, SCWS admin client, device.
Test Case Description	The purpose is to verify single resource 1kb (portal 'oma-500') can be sent, received through full admin protocol using the full TCP/IP client protocol using the Ethernet Emulation Model (EEM) subclass (i.e. not using BIP client mode protocol).
Specification Reference	[SCWS-TS] Chapter 13.3.2 [SCWS-TS] Chapter 13.1
SCR Reference	SCWS-AC-001-M, SCWS-AC-003-O, SCWS-AC-004-M, SCWS-AC-007-M, SCWS-AC-010-M, SCWS-AC-024-O SCWS-AS-001-M, SCWS-AS-005-M SCWS-S-012-M, SCWS-S-022-M SCWS-ME-007-O

ETR Reference	ADM_C_M_01, ADM_C_02, ADM_C_M_03, ADM_C_M_06, ADM_C_M_07, ADM_C_M_08, ADM_C_M_11, ADM_C_M_13, ADM_S_M_01, ADM_S_M_03, ADM_S_M_07, ADM_S_M_08, S_M_05, S_M_12, S_M_13, S_M_17, D_M_01, D_M_05.
Tool	Smart Card protocol analyser
Test code	[TEST_CONTENT_DESC] §6.1.1, §6.1.2, [TEST_CONTENT]
Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal implementing the TCP/IP protocol and EEM subclass ○ Smart Card with SCWS server and SCWS admin client implementing the TCP/IP protocol and EEM subclass ○ Remote admin SCWS Server • Prerequisite for this test: <ul style="list-style-type: none"> ○ Smart Card card administration agent is configured with remote admin SCWS Server parameters (ip-address, port...).
Test Procedure	<ol style="list-style-type: none"> 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 the browser. 5. Select the SCWS test portal link (e.g. http://localuicc: 80/index.html) 6. Verify the pass criteria below.
Pass-Criteria	<p>In Terminal browser, the new download resource (portal 'oma-500') is displayed.</p> <p>The TCP/IP protocol has been used using the Ethernet Emulation Model (EEM) subclass (check using a transport protocol analyser).</p>

6.2.6 Backward Compatibility

6.2.6.1 SCWS-1.2-int-900 Back RemoteAdmin1.0 / AdminClient 1.1

Test Case Id	SCWS-1.2-int-900
Test Object	Remote admin server implementing SCWS1.0, SCWS admin client implementing SCWS1.1.
Test Case Description	The purpose is to validate backward compatibility between SCWS Remote Admin 1.0 and Admin Client 1.1
Specification Reference	[SCWS-TS] Chapter 13.3.1 [SCWS-TS] Chapter 13.1
SCR Reference	SCWS-AC-001-M, SCWS-AC-004-M, SCWS-AC-007-M, SCWS-AC-010-M, SCWS-AC-017-M, SCWS-S-028-M SCWS-AS-001-M, SCWS-AS-005-M SCWS-S-012-M, SCWS-S-022-M

ETR Reference	ADM_C_M_01, ADM_C_02, ADM_C_M_03, ADM_C_M_06, ADM_C_M_07, ADM_C_M_08, ADM_C_M_11, ADM_S_M_01, ADM_S_M_03, ADM_S_M_07, ADM_S_M_08, S_M_05, S_M_12, S_M_13, S_M_17, D_M_01, BACK-002.
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, [TEST_CONTENT]
Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS 1.1 server and SCWS 1.1 admin client ○ Remote admin server implementing SCWS 1.0 • Prerequisite for this test: <ul style="list-style-type: none"> ○ SCWS server is provisioned with the test content.
Test Procedure	<ol style="list-style-type: none"> 1. In Remote admin SCWS1.0 Server <ul style="list-style-type: none"> • Select Terminal destination address. • Select portal 'oma-502'. • Start then wait download finished. • Verify Pass Criteria 1 2. In Terminal, select the browser. <ul style="list-style-type: none"> • Select the SCWS test portal link (/index.html) • Verify Pass Criteria 2
Pass-Criteria	<ol style="list-style-type: none"> 1. Administration session is terminated successfully between SCWS 1.1 admin client and Remote admin SCWS 1.0 Server. 2. Portal ('oma-502') is displayed.

6.2.6.2 SCWS-1.2-int-901 Back RemoteAdmin1.1 / AdminClient 1.0

Test Case Id	SCWS-1.2-int-901
Test Object	Remote admin server implementing SCWS 1.1, SCWS admin client implementing SCWS 1.0.
Test Case Description	The purpose is to validate backward compatibility between SCWS Remote Admin 1.1 and Admin Client 1.0
Specification Reference	[SCWS-TS] Chapter 13.3.2.6.1 [SCWS-TS] Chapter 13.3.2.7.1
SCR Reference	SCWS-AC-001-M, SCWS-AC-004-M, SCWS-AC-007-M, SCWS-AC-010-M, SCWS-AC-017-M, SCWS-S-028-M SCWS-AS-001-M, SCWS-AS-005-M SCWS-S-012-M, SCWS-S-022-M

ETR Reference	ADM_C_M_01, ADM_C_02, ADM_C_M_03, ADM_C_M_06, ADM_C_M_07, ADM_C_M_08, ADM_C_M_11, ADM_S_M_01, ADM_S_M_03, ADM_S_M_07, ADM_S_M_08, S_M_05, S_M_12, S_M_13, S_M_17, D_M_01, BACK-001.
Tool	
Test code	[TEST_CONTENT_DESC] §6.1.1, [TEST_CONTENT]
Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS 1.0 server and SCWS 1.0 admin client ○ Remote admin server implementing SCWS 1.1 • Prerequisite for this test: <ul style="list-style-type: none"> ○ SCWS server is provisioned with the test content.
Test Procedure	<ol style="list-style-type: none"> 1. In Remote admin SCWS1.1 Server <ul style="list-style-type: none"> • Select Terminal destination address. • Select portal 'oma-502'. • Start then wait download finished. • Verify Pass Criteria 1 2. In Terminal, select the browser. <ul style="list-style-type: none"> • Select the SCWS test portal link (/index.html) • Verify Pass Criteria 2
Pass-Criteria	<ol style="list-style-type: none"> 1. Administration session is terminated successfully between SCWS 1.0 admin client and Remote admin SCWS 1.1 Server. 2. Portal ('oma-502') is displayed.

6.2.7 Administration Triggering test group

6.2.7.1 SCWS-1.2-int-1000 Remote triggering using a SMS

Test Case Id	SCWS-1.2-int-1000
Test Object	Remote admin SCWS Server, SCWS admin client.
Test Case Description	Check if an administration session can be trigger by a secure SMS.
Specification Reference	[SCWS-TS] Chapter 14.3.2.4 [SCWS-TS] Chapter 14.3.2.4.1
SCR Reference	SCWS-AC-001-M, SCWS-AC-004-M, SCWS-AC-005-M, SCWS-AC-007-M, SCWS-AC-010-M, SCWS-AS-001-M, SCWS-AS-004-M, SCWS-AS-005-M SCWS-S-012-M, SCWS-S-022-M

ETR Reference	ADM_C_M_01, ADM_C_02, ADM_C_M_03, ADM_C_M_06, ADM_C_M_07, ADM_C_M_08, ADM_C_M_10, ADM_C_M_11, ADM_S_M_01, ADM_S_M_02, ADM_S_M_03 S_M_05, S_M_12, S_M_13, S_M_17, D_M_01.
Tool	
Test code	[TEST_CONTENT_DESC], [TEST_CONTENT]
Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server and SCWS admin client ○ Remote admin SCWS Server • Prerequisite for this test: <ul style="list-style-type: none"> ○ Remote admin SCWS Server connected to the SMS-C of the network operator. ○ Smart Card card administration agent is configured with remote admin SCWS Server parameters (ip-address, port...).
Test Procedure	<ol style="list-style-type: none"> 3. In Remote admin SCWS Server, <ol style="list-style-type: none"> 3.1. Select Terminal destination address. 3.2. Select the resources to be downloaded by the Smart Card: portal 'oma-500'. 3.3. Send a SMS MT to trigger the administration session 3.4. Wait until the Remote admin SCWS Server notifies that the content has been downloaded by the SCWS admin client. 3.5. Verify the pass criteria 1. 4. In Terminal, select the browser, <ol style="list-style-type: none"> 4.1. Select the SCWS test portal path (/index.html). 4.2. Verify the pass criteria 2.
Pass-Criteria	<ol style="list-style-type: none"> 3. The portal 'oma-500' correctly downloaded by the SCWS admin client when the administration session is triggered by a secure SMS MT. 4. The new download resource (portal 'oma-500') is correctly displayed by the browser.

6.2.7.2 SCWS-1.2-int-1001 Remote triggering using a OMA SIP Push message

Test Case Id	SCWS-1.2-int-1001
Test Object	Remote admin SCWS Server, SCWS admin client.
Test Case Description	Check if an administration session can be trigger by a secure OMA SIP push message.
Specification Reference	[SCWS-TS] Chapter 14.3.2.4 [SCWS-TS] Chapter 14.3.2.4.2

SCR Reference	SCWS-AC-001-M, SCWS-AC-004-M, SCWS-AC-025-O, SCWS-AC-007-M, SCWS-AC-010-M, SCWS-AS-001-M, SCWS-AS-005-M, SCWS-AS-015-O SCWS-S-012-M, SCWS-S-022-M SCWS-ME-015-O, SCWS-ME-016-O
ETR Reference	ADM_C_M_01, ADM_C_02, ADM_C_M_03, ADM_C_M_06, ADM_C_M_07, ADM_C_M_08, ADM_C_M_11, ADM_C_O_03, ADM_S_M_01, ADM_S_M_03, ADM_S_O_06, S_M_05, S_M_12, S_M_13, S_M_17, D_M_01.
Tool	
Test code	[TEST_CONTENT_DESC], [TEST_CONTENT]
Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server and SCWS admin client ○ Remote admin SCWS Server • Prerequisite for this test: <ul style="list-style-type: none"> ○ Remote admin SCWS Server connected to the OMA Push Gateway of the network operator supporting the OTA-SIP Push protocol. ○ Smart Card card administration agent is configured with remote admin SCWS Server parameters (ip-address, port...). ○ The OMA SIP PUSH Client is implemented into the Terminal.
Test Procedure	<ol style="list-style-type: none"> 1. In Remote admin SCWS Server, <ol style="list-style-type: none"> 1.1. Select Terminal destination address. 1.2. Select the resources to be downloaded by the Smart Card: portal 'oma-501'. 1.3. Send a SIP push message to trigger the administration session 1.4. Wait until the Remote admin SCWS Server notifies that the content has been downloaded by the SCWS admin client. 1.5. Verify the pass criteria 1. 2. In Terminal, select the browser, <ol style="list-style-type: none"> 2.1. Select the SCWS test portal path (/index.html). 2.2. Verify the pass criteria 2.
Pass-Criteria	<ol style="list-style-type: none"> 1. The portal 'oma-501' correctly downloaded when the administration session is triggered by SIP push message 2. The new download resource (portal 'oma-501') is correctly displayed by the browser.

6.2.7.3 SCWS-1.2-int-1002 Triggering using an internal event

Test Case Id	SCWS-1.2-int-1002
---------------------	-------------------

Test Object	Remote admin SCWS Server, SCWS admin client.
Test Case Description	Check if an administration session can be trigger by an internal event.
Specification Reference	[SCWS-TS] Chapter 14.3.2.4
SCR Reference	SCWS-AC-001-M, SCWS-AC-004-M, SCWS-AC-006-O, SCWS-AC-007-M, SCWS-AC-010-M, SCWS-AS-001-M, SCWS-AS-005-M SCWS-S-012-M, SCWS-S-022-M
ETR Reference	ADM_C_M_01, ADM_C_02, ADM_C_M_03, ADM_C_M_06, ADM_C_M_07, ADM_C_M_08, ADM_C_M_11, ADM_C_O_01, ADM_S_M_01, ADM_S_M_03 S_M_05, S_M_12, S_M_13, S_M_17, D_M_01.
Tool	
Test code	[TEST_CONTENT_DESC], [TEST_CONTENT]
Preconditions	<ul style="list-style-type: none"> • Equipment: <ul style="list-style-type: none"> ○ Terminal ○ Smart Card with SCWS server and SCWS admin client ○ Remote admin SCWS Server • Prerequisite for this test: <ul style="list-style-type: none"> ○ Smart Card card administration agent is configured with remote admin SCWS Server parameters (ip-address, port...). ○ A CAT application is loaded and installed on the Smart Card. This application registers on the toolkit menu and implements an internal event to trigger the administration session.
Test Procedure	<ol style="list-style-type: none"> 1. In Remote admin SCWS Server, <ol style="list-style-type: none"> 1.1. Select Terminal destination address. 1.2. Select the resources to be downloaded by the Smart Card: portal 'oma-502'. 2. In Terminal, <ol style="list-style-type: none"> 2.1. Select the CAT application in the toolkit menu to send an internal event to trigger an administration session with the Remote admin SCWS Server. 3. In Remote admin SCWS Server, <ol style="list-style-type: none"> 3.1. Wait until the Remote admin SCWS Server notifies that the content has been downloaded by the SCWS admin client. 3.2. Verify the pass criteria 1. 4. In Terminal, select the browser, <ol style="list-style-type: none"> 4.1. Select the SCWS test portal path (/index.html). 4.2. Verify the pass criteria 2.
Pass-Criteria	<ol style="list-style-type: none"> 1. The portal 'oma-502' correctly downloaded when the administration session is triggered by a card internal event. 2. The new download resource (portal 'oma-502') is correctly displayed by the browser.

Appendix A. Change History

(Informative)

A.1 Approved Version History

Reference	Date	Description
n/a	n/a	No prior version

A.2 Draft/Candidate Version 1.2 History

Document Identifier	Date	Sections	Description
Draft Versions OMA-ETS-Smartcard_Web_Server-V1_2	31 Mar 2011	All	Initial version, based on OMA-ETS-Smartcard_Web_Server-V1_2-20100302-C. and 2011 ETS Template OMA-SCT-2007-0063R01-CR_ETIS_Update_RemoteAdminSettings incorporated
	18 Aug 2011	All New sections: 6.1.7, 6.2.3.4 to 6.2.3.11 and 6.2.7	The following CRs are incorporated: OMA-IOP-BRO-2011-0048-CR_SCWS12_ETIS_SCRReferences OMA-IOP-BRO-2011-0049R01-CR_SCWS12_ETIS_ETRReferences OMA-IOP-BRO-2011-0050R01-CR_SCWS12_ETIS_TLS_TestCases OMA-IOP-BRO-2011-0051R01-CR_SCWS12_ETIS_Push_TestCases OMA-IOP-BRO-2011-0052R01-CR_SCWS12_ETIS_ACP_TestCases OMA-IOP-BRO-2011-0053-CR_SCWS12_ETIS_Admin_Settings. The term “WAP browser” is replaced by “browser”. The references to ETR items are aligned with the ones defined in OMA-TS-Smartcard_Web_Server-V1_2.
	01 Sept 2011	6.2.7.2	The following CR is incorporated: OMA-IOP-BRO-2011-0075-CR_SCWS12_ETIS_Push_MissingSCR
Candidate Versions OMA-ETS-Smartcard_Web_Server-V1_2	11 Oct 2011	n/a	Status changed to Candidate by TP TP Ref# OMA-TP-2011-0342- INP_SCWS_1_2_ETIS_for_Candidate_Approval

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

In order to set-up the Remote Administration test, some parameters need to be exchanged between the provider of the Remote Administration server, the network operator and the provider of the SCWS card. The following tables provide an example of the parameters that may be exchanged.

B.1 Remote Admin server settings

The following table may have to 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	Provided by the Admin Server	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	Provided by the Admin Server	
Security Parameters of the full admin protocol session		
PSK identifier	Provided by the Admin Server	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	Provided by the Admin Server	Destination Address of the Remote Admin server used to send the Admin session Failure Report
<i>Agent HTTP post parameters</i>		
administration host	Provided by the Admin Server	Content of the field host in the post request header
agent-ID	Provided by the Admin Server	Content of the field from in the post request header
administration URI	Provided by the Admin Server	URI used to send the post request

B.2 Network operator settings

The following table may have to 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	Provided by Network Host	APN and associated login/password to setup the GSM/GPRS or UMTS/Data packet connection
Login	Provided by Network Host	
Password	Provided by Network Host	
IP addresses coming from the mobile equipment		
(Range of) IP addresses	Provided by Network Host	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. (*): To limit the incoming access rules on the Remote Admin server, the range has to be reduced as much as possible.
Rules applied	Provided by Network Host	
SMSC connection		
Remark: a large account connection is required with the SMSC.		
IP address of the SMSC	Provided by Network Host	IP address and port number used for the large account connection.
Port number of the SMSC	Provided by Network Host	
Login	Provided by Network Host	Login/password if required
Password	Provided by Network Host	
Applicative protocol used (e.g. SMPP3.4)	Provided by Network Host	
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	Provided by Network Host	Service Centre Address of the SMSC Remote Admin server used to send the Admin session Failure Report
Card subscription parameters		
IMSI	Provided by Network Host	Value communicated just before the test fest
Ki	Provided by Network Host	

Authentication Algorithm	Provided by Network Host	
--------------------------	--------------------------	--

B.3 SCWS Admin client configuration

The following table may have to 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
Card subscription parameters		
For each card used during the Remote Administration tests, subscription parameters shall be provided in order to set-up the Remote Admin server.		
Card 1	ICCID= MSISDN= IMSI= Provided by Client/Smart Card vendor	These values may be used by the Remote Admin server to identify the card and the subscription.
Card 2	ICCID= MSISDN= IMSI= Provided by Client/Smart Card vendor	These values may be used by the Remote Admin server to identify the card and the subscription.
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	Value of the TLS Pre-Shared key value used for admin session.

	participants.	The value will be provided to the Test Fest participants once registered.
URI of the default configuration resource	Provided by Client/Smart Card vendor	
Default configuration resource for the full administration protocol		
<i>Connection parameters using the BIP</i>		
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 Provided by Network Host	Depends on the network configuration
Login	See Annex B.2 Provided by Network Host	
Password	See Annex B.2 Provided by Network Host	
Port number of the Remote Admin server	See Annex B.1 Provided by the Admin Server	Depends on the remote admin server configuration
IP Address of the Remote Admin server	See Annex B.1 Provided by the Admin Server	
<i>Security parameters</i>		
PSK Identifier	See Annex B.1 Provided by the Admin Server	Depends on the remote admin server configuration
Card Key Identifier	Provided by Client/Smart Card vendor	
<i>Retry policy parameters</i>		
Retry counter	2	
Retry Delay	20s	
<i>Retry Failure Report SMS MO</i>		
TP Destination address	See Annex B.1 Provided by the Admin Server	Address of the remote admin server configuration
TP Service Center address	See Annex B.2 Provided by Network	Address of the SMSC

	Host	
Alpha identifier	“Error”	
<i>Agent HTTP post parameters</i>		
administration host	See Annex B.1 Provided by the Admin Server	Depends on the remote admin server configuration
agent-ID	See Annex B.1 Provided by the Admin Server	Depends on the remote admin server configuration
administration URI	See Annex B.1 Provided by the Admin Server	Depends on the remote admin server configuration