Enabler Test Requirements for Smartcard-Web-Server

Candidate Version 1.2 – 19 Apr 2011

Open Mobile Alliance

OMA-ETR-Smartcard_Web_Server-V1_2-20110419-C

Contents

Tables

1. Scope

The Enabler Test Requirements (ETR) document for the Enabler under consideration is created and maintained by the Technical Working Group (TWG) responsible for the technical specifications for the corresponding Enabler.

The ETR document is intended to cover at least those requirements collected in the Requirements Document (RD) and the Architecture Document (AD) in addition to any other items the TWG has identified as important enough to warrant attention from interoperability perspective and identify any technical functionalities that should be covered by testing.

2. References

2.1 Normative References

[3GPP TS 31.103] "TS 31.103 Technical Specification Group Core Network and Terminals; Characteristics of the IP Multimedia Services Identity Module (ISIM) application", 3rd Generation Partnership Project (3GPP), URL: http://www.3gpp.org/ftp/Specs/archive/31_series/31.103/

[3GPP TS 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 31.115] 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] "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

[ETSI TS 102 483] "TS 102 483 Technical Specification Smart Cards; UICC-Terminal interface; Internet Protocol connectivity between UICC and terminal" R7 or higher, European Telecommunications Standards Institute (ETSI), URL: http://www.etsi.org

[ETSI TS 102 600] "TS 102 600 Technical Specification Smart Cards; UICC-Terminal interface; Characteristics of the USB interface" 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
[OMA Push Enabler]	"Enabler Release Definition for Push Version 2.2", Open Mobile Alliance™, OMA-ERELD-Push-V2_2, URL: http://www.openmobilealliance.org/
[OMA SIP Push Enabler]	"Session Initiation Protocol (SIP) Push", Open Mobile Alliance™, OMA-ERP-SIP_Push-V1_0, URL: http://www.openmobilealliance.org/
[IOPPROC]	"OMA Interoperability Policy and Process", Version 1.3, Open Mobile Alliance™, OMA-ORG-IOP_Process-V1_3, URL:http://www.openmobilealliance.org/
[ISO7816-4]	"Information technology - Identification cards - Integrated circuit(s) cards with contacts – Part 4: Interindustry commands for interchange"
[PSK-TLS]	"Pre-Shared Key Cipher suites for Transport Layer Security (TLS)", RFC 4279, URL: http://www.ietf.org/rfc/rfc4279.txt
[RFC1630]	"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", RFC1630, URL: http://www.ietf.org/rfc/rfc1630.txt
[RFC2119]	"Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, RFC2119, March 1997, URL: http://www.ietf.org/rfc/rfc2119.txt
[RFC2234]	"Augmented BNF for Syntax Specifications: ABNF", D. Crocker, Ed., P. Overell, RFC2234, November 1997, URL: http://www.ietf.org/rfc/rfc2234.txt
[RFC2617]	"HTTP Authentication: Basic and Digest Access Authentication", RFC2617, June 1999, URL: http://www.ietf.org/rfc/rfc2617.txt
[RFC3546]	"Transport Layer Security (TLS) Extensions", RFC3546, June 2003, URL: http://www.ietf.org/rfc/rfc3546.txt
[RFC3986]	"Uniform Resource Identifier (URI): Generic Syntax", RFC3986, January 2005, URL: http://www.ietf.org/rfc/rfc3986.txt
[RFC4785]	"Pre-Shared Key (PSK) Ciphersuites with NULL Encryption for Transport Layer Security (TLS)", RFC4785, January 2007, URL: http://www.ietf.org/rfc/rfc4785.txt
[RFC5487]	"Pre-Shared Key Cipher Suites for TLS with SHA-256/384 and AES Galois Counter Mode", RFC 5487, March 2009, URL: http://www.ietf.org/rfc/rfc5487.txt
[SCRRULES]	"SCR Rules and Procedures", Open Mobile Alliance™, OMA-ORG-SCR_Rules_and_Procedures, URL: http://www.openmobilealliance.org/
[SCWS-ERELD]	"Enabler Relese Document for Smartcard Web Server", Open Mobile Alliance™, OMA-ERELD-Smartcard_Web_Server-V1_2, URL:http://www.openmobilealliance.org/
[SCWS-RD]	"Smartcard Web Server Requirements", Open Mobile Alliance™, OMA-RD_Smartcard_Web_Server-V1_0, URL: http://www.openmobilealliance.org/
[TLS 1.0]	"Security Transport Protocol", RFC 2246, January 1999, URL: http://www.ietf.org/rfc/rfc2246.txt
[TLS 1.1]	"The Transport Layer Security (TLS) Protocol Version 1.1", RFC 4346, April 2006, URL: http://www.ietf.org/rfc/rfc4346.txt
[TLS 1.2]	"The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008, URL: http://www.ietf.org/rfc/rfc5246.txt
[WAPCert]	"WAP Certificate and CRL Profiles", WAP Forum™, WAP-211-WAPCert, URL: http://www.openmobilealliance.org/

[XML 1.0] Extensible Markup Language (XML) 1.0 (Third Edition),
URL: http://www.w3.org/TR/2004/REC-xml-20040204/

[XML Media Type] XML Media Types, RFC3023,
URL: http://www.rfc-editor.org/rfc/rfc3023.txt

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)

[WAPWAE] "Wireless Application Environment Specification", Open Mobile Alliance™,
OMA-WAP-WAESpec-V2_3,
URL: http://www.openmobilealliance.org/

[WP HTTP] "Wireless Profiled HTTP", WAP Forum™, WAP-229-HTTP-20010329-a,
URL: http://www.openmobilealliance.org/

3. Terminology and Conventions

3.1 Conventions

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in [RFC2119].

All sections and appendixes, except “Scope” and “Introduction”, are normative, unless they are explicitly indicated to be informative.

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.
IC USB interface	see [ETSI TS 102 600]
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.
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).
TestFest	Multi-lateral interoperability testing event
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", [RFC1630]. 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
EEM	Ethernet Emulation Model
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
(U)SIM	(Universal) Subscriber Identity Module

4. Introduction

The purpose of this Enabler Test Requirements document is to help guide the testing effort for the Enabler Smart Card Web Server V 1.2, documenting those areas where testing is most important to ensure interoperability of implementations.

A Smart Card Web Server (SCWS) is an HTTP server that is implemented in a smart card, embedded in the mobile device (e.g. SIM, (U)SIM, UICC, R-UIM, CSIM). It allows network operators to offer state of the art smart card based services to their customers by using the widely deployed [HTTP/1.1] protocol.

This solution integrates well in the Internet and the OMA architecture. The main scope of the specification is to allow a local communication between a WEB browser running in the terminal and a Web Server running in the smart card. It also covers remote administration of the smart card web server by authorized entities (i.e. card issuer or a delegated entity). This new HTTP interface is a logically separated communication channel from those that already exist today between the terminal and the smart card (e.g. using protocols that are defined in [ISO7616-4], [ETSI TS 102 221] and [ETSI TS 102 223]). It enables HTTP applications in the terminal to communicate with the smart card independently from the current telecom based communication between these two entities.

A Smart card-URI is used in order to communicate with the web server that is embedded in the smartcard (SCWS). We limit our discussion to smart card platforms such as (U)SIM (Subscriber Identification Module), UICC and R-UIM (Removable – User Identification Module), CSIM in a mobile phone.

The Enabler under consideration comprises the following specifications:

- OMA Smart Card Web Server Version 1.2 Requirement Document: Specifying the requirements for the SCWS
- OMA Smart Card Web Server Version 1.2 Enabler Architecture: Specifying the architectural details of SCWS
- OMA Smart Card Web Server Version 1.2 Technical Specification: Specifying the technical details of SCWS

Generally, the testing activity should aim at validating the normal working behaviour of the client/server interactions, as well as testing the error conditions whenever it is possible to set up the appropriate scenarios. The following sections provide a more detailed description of the testing requirements for Smart Card Web Server V 1.2.

This document also intends to provide some guidance on the prioritization of the specifications and features to be tested within Enabler Smart Card Web Server V 1.2.

5. Test Requirements

This enabler test requirements is used to test the Smart Card Web Server in devices.

5.1 Enabler Test Requirements

The test requirements collected in this section are related to the Enabler Smart Card Web Server V1.2.

In this section, it should be defined what specific functionalities of this Enabler shall or should be tested to ensure adequate operational of the implementations, including any security requirements and constraints on usage if specified (e.g. user can forward a media object but can not visualize it). That means that devices (clients/serves) shall do what they have to do and they shall not do what they are not allowed to do. Both types of test requirements (positive and negative testing) should be included here if so required.

Besides this information, OMA Architecture specifies a "Framework Architecture", consisting of a set of common functions that need to be invoked in most use cases involving the different Service Enablers. The functionality requirements defined in the OMA Framework Architecture, i.e. authentication, authorization, charging, billing, common directory, etc. should also be listed in this table.Use cases are the main input to identify test requirements.

The following test requirements should cover both Conformance test requirements (i.e. functionality to be tested to verify wheter it is implemented either in the client side or in the server side) and Interoperability test requirements (i.e. client/server interactions one with another)

The following sections (Mandatory and Optional test requirements) could also be separated for client and server test requirements.

The tables for the mandatory and optional test requirements include the following columns:

FEATURE KEY: A set of characters uniquely identifying the enabler test requirement to be tested. It is suggested that the Feature Key is no longer than 4 to 5 characters. The purpose of the Feature Key is that when used, it distinctly refers to only one feature to be tested.

FEATURE DESCRIPTION: A description of a technical specification feature to be tested.

FEATURE TEST REQUIREMENTS: A description of what shall be tested for the feature,

5.1.1 Mandatory Test Requirements

Mandatory test requirements should cover those features and use cases that require validation in order to approve the enabler. These include areas with complex interactions between the different functional components of the enabler architecture or where the complexity of the specification(s) is such that there is some uncertainty that they have been correctly specified.

These features and use cases SHOULD cover mandatory and MAY recommend prioritisation of optional implementation features. If testing of some of the mandatory features is not required, then the ETR SHALL contains an explanation for their exclusion.

NOTE: This table needs to be filled out at a level where ambiguity is not present but details are not overwhelming.

Ambiguity means that the details do not have several meanings nor have more than one possible implementation path following.

5.1.1.1 SCWS Admin Client

	Feature Key	Feature Description	Feature Test Requirements
Normal Flow	ADM_C_M_01	Full administration protocol: Using BIP or TCP/IP	Required to test whether Full administration protocol using BIP or TCP/IP is processed properly.

	Feature Key	Feature Description	Feature Test Requirements
	ADM_C_M_12	BIP transport protocol When BIP transport protocol is used, be able to open an additional BIP channel "TCP, UICC in client mode" for SCWS administration	Required to test whether the SCWS admin client can open a connection with a remote administration server using an additional BIP channel "TCP, UICC in client mode". Explicit testing of this transport protocol is not required. Implicit testing thanks to the implementation of the Full administration protocol is sufficient.
	ADM_C_M_13	TCP/IP transport protocol When TCP/IP transport protocol is used, be able to open a remote TCP/IP connection using Ethernet Emulation Model (EEM) subclass for SCWS administration	Required to test whether the SCWS admin client can open a direct TCP/IP connection with a remote administration server using the Ethernet Emulation Model (EEM) subclass. Explicit testing of this transport protocol is not required. Implicit testing thanks to the implementation of the Full administration protocol is sufficient.
	ADM_C_M_02	Admin-server settings: Default configuration resources	Required to test whether the SCWS Admin Client can retrieve default configuration resources.
	ADM_C_M_03	HTTP POST request of card administration agent	Verify that all mandatory fields of HTTP POST request of card administration agent are present and valid.
	ADM_C_M_04	Retry management Resume mode	Required to test whether the resume mode of retry management is processed properly.
	ADM_C_M_05	Retry management SMS-MO emitted if the administration session is abandoned	Required to test whether the SMS-MO of retry management is emitted properly if the administration session is abandoned.
	ADM_C_M_06	Remote administration request tag	Support for all tags used for the remote administration and retry management.
	ADM_C_M_07	TLS 1.0 protocol	Required to test whether TLS 1.0 protocol is processed properly. Implicit testing of TLS 1.0 protocol is sufficient. Explicit testing of TLS 1.0 is not required.
	ADM_C_M_08	PSK-TLS protocol	Required to test whether PSK-TLS protocol is processed properly. Implicit testing of PSK-TLS Protocol is sufficient. Explicit testing of PSK-TLS is not required.
	ADM_C_M_08_A	TLS Cipher-Suite TLS_PSK_WITH_3DES_EDE_CBC_SHA	Required to test whether PSK-TLS using cipher-suite TLS_PSK_WITH_3DES_EDE_CBC_SHA is processed properly. Implicit testing of the cipher-suite is sufficient.
	ADM_C_M_08_B	TLS Cipher-Suite TLS_PSK_WITH_AES_128_CBC_SHA	Required to test whether PSK-TLS using cipher-suite TLS_PSK_WITH_AES_128_CBC_SHA is processed properly. Implicit testing of the cipher-suite is sufficient.
	ADM_C_M_08_C	TLS Cipher-Suite TLS_PSK_WITH_NULL_SHA	Required to test whether PSK-TLS using cipher-suite TLS_PSK_WITH_NULL_SHA is processed properly. Implicit testing of the cipher-suite is sufficient.
	ADM_C_M_09	Fragment Negotiation in TLS	Required to test whether Fragment Negotiation in TLS is processed properly. Implicit testing of Fragment Negotiation in TLS Protocol is sufficient. Explicit testing of Fragment Negotiation in TLS is not required.
	ADM_C_M_10	Trigger the administration session by receiving a secure SMS.	Required to test whether the administration session can be triggered properly by receiving a secure SMS.
	ADM_C_M_11	Ability to process POST response from Remote SCWS admin server implementing the SCWS V1.0	Required to test whether the POST response from Remote SCWS admin server implementing the SCWS V1.0 is processed properly.

	Feature Key	Feature Description	Feature Test Requirements
Error Flow	ADM_C_M_99	Triggering of an administration session through a secure SMS: Admin client is not able to store the request and responds SW "9300".	Required to test whether Admin client uses "9300" status word when it is not able to store the administration session triggering request sent using a secure SMS.

Table 1: Applicability Table for Enabler SCWS Admin Client Mandatory Test Requirements

5.1.1.2 Remote SCWS Admin Server

	Feature Key	Feature Description	Feature Test Requirements
Normal Flow	ADM_S_M_01	Implement the "SCWS Full administration protocol"	Required to test whether SCWS Full administration protocol is processed properly.
	ADM_S_M_02	Trigger the administration session by sending a secure SMS to the smart card	Required to test whether the administration session can be triggered properly by sending a secure SMS to the smart card.
	ADM_S_M_03	HTTP POST response of remote administration server	Required to test whether the status code of the HTTP POST response is processed properly.
	ADM_S_M_04	Lightweight administration protocol	Required to test whether the Lightweight administration protocol is supported properly.
	ADM_S_M_07	TLS 1.0 protocol	Required to test whether TLS 1.0 protocol is processed properly. Implicit testing of TLS 1.0 protocol is sufficient. Explicit testing of TLS 1.0 protocol is not required.
	ADM_S_M_08	PSK-TLS protocol	Required to test whether PSK-TLS protocol is processed properly. Implicit testing of PSK-TLS protocol is sufficient. Explicit testing of PSK-TLS protocol is not required.
	ADM_S_M_06_A	TLS Cipher-Suite TLS_PSK_WITH_3DES_EDE_CBC_SHA	Required to test whether PSK-TLS using cipher-suite TLS_PSK_WITH_3DES_EDE_CBC_SHA is processed properly. Implicit testing of the cipher-suite is sufficient
	ADM_S_M_06_B	TLS Cipher-Suite TLS_PSK_WITH_AES_128_CBC_SHA	Required to test whether PSK-TLS using cipher-suite TLS_PSK_WITH_AES_128_CBC_SHA is processed properly. Implicit testing of the cipher-suite is sufficient
	ADM_S_M_06_C	TLS Cipher-Suite TLS_PSK_WITH_NULL_SHA	Required to test whether PSK-TLS using cipher-suite TLS_PSK_WITH_NULL_SHA is processed properly. Implicit testing of the cipher-suite is sufficient
Error Flow			

Table 2: Applicability Table for Enabler Remote SCWS Admin Server Mandatory Test Requirements

5.1.1.3 SCWS Client

	Feature Key	Feature Description	Feature Test Requirements

	Feature Key	Feature Description	Feature Test Requirements
Normal Flow	C_M_01	Use the SCWS URL to access the SCWS	Required to test whether SCWS can be accessed by the SCWS Client.
	C_M_02	Override the default caching algorithms using HTTP 'Cache-Control' general-header.	Required to test whether default caching algorithms can be override using HTTP Cache-Control general-header.
	C_M_03	HTTP cache mechanim base on the Entity-Tag validators.	Required to test whether cache mechanism based on the Entity-Tag validator is processed properly.
	C_M_04	Decode http response entity based on the Content-Encoding header.	Required to test whether compressed entity based on the Content-Encoding header is processed properly.
Error Flow			

Table 3: Applicability Table for Enabler SCWS Client Mandatory Test Requirements

5.1.1.4 SCWS Server

	Feature Key	Feature Description	Feature Test Requirements
Normal Flow	S_M_01	Use the SCWS URL with a length up to 1024 characters to access the SCWS	Required to test whether SCWS supports URLs with a length up to 1024 characters.
	S_M_02	Dynamic Content	Required to test whether SCWS application may dynamically create content.
	S_M_03	Use local transport protocols with the client device (BIP transport protocol or TCP/IP transport protocol)	Required to test whether at least one local transport protocol can be used with the client device (i.e BIP, or TCP/IP).
	S_M_24	BIP transport protocol: When BIP transport protocol is used, be able to open at least 2 BIP channels in "TCP, UICC in server mode"	Required to test whether SCWS can open at least 2 BIP channels in "TCP, UICC in server mode". Explicit testing of this transport protocol is not required. Implicit testing when accessed by the client device is sufficient.
	S_M_25	TCP/IP transport protocol: When TCP/IP transport protocol is used, be able to open a local TCP/IP connection using Ethernet Emulation Model (EEM) subclass	Required to test whether SCWS can open a direct TCP/IP connection with Ethernet Emulation Model (EEM) subclass. Explicit testing of this transport protocol is not required. Implicit testing when accessed by the client device is sufficient.

	Feature Key	Feature Description	Feature Test Requirements
	S_M_04	Concurrency with other CAT application	Required to test whether the concurrency with other CAT application is processed properly.
	S_M_05	Compliance with HTTP 1.1	Required to test whether HTTP 1.1 profile is processed properly. Implicit testing of HTTP 1.1 is sufficient. Explicit testing of HTTP 1.1 is not required other than what is specifically called in ETR.
	S_M_06	HTTP GET Request	Required to test whether HTTP GET Request is processed properly.
	S_M_07	HTTP HEAD Request	Required to test whether HTTP HEAD Request is processed properly.
	S_M_08	HTTP POST Request	Required to test whether HTTP POST Request is processed properly.
	S_M_09	HTTP Authorisation request header	Required to test whether HTTP Authorisation request header is processed properly.
	S_M_10	HTTP WWW-Authenticate response header	Required to test whether HTTP WWW-Authenticate response header is processed properly.
	S_M_11	HTTP Basic authentication	Required to test whether HTTP basic authentication is executed properly.
	S_M_12	Administration commands: PUT HTTP request	Required to test whether PUT administration command is processed properly.
	S_M_13	Administration commands: DELETE HTTP request	Required to test whether DELETE administration command is processed properly.
	S_M_14	Administration commands POST HTTP request	Required to test whether POST administration command is processed properly.
	S_M_15	Administration commands: GET HTTP request	Required to test whether GET administration command is processed properly.
	S_M_26	Administration commands: HEAD HTTP request	Required to test whether HEAD administration command is processed properly.
	S_M_16	Special administration commands	Required to test whether SCWS administration commands are processed properly.
	S_M_17	Response to admin commands within the POST command: Pragma header	Required to test whether Pragma header can be used properly within the POST command.
	S_M_18	Lightweight administration protocol	Required to test whether Lightweight administration protocol is supported properly
	S_M_19	Administration commands: DELETE directory	Required to test whether DELETE directory administration command is processed properly.
	S_M_20	Cache mechanism based on Entity-tag validates	Required to test whether cache mechanism based on Entity-tag validators is processed properly.
	S_M_21	Administration commands: PUT with gzip Content-Encoding	Required to test whether PUT resource with gzip Content-Encoding is processed properly.
	S_M_22	Administration commands: PUT with Cache-Controle information.	Required to test whether PUT resource with Cache-Controle header is processed properly.
	S_M_23	Administration commands not allowed accessing the URI requested in the request.	Required to test that the Administration commands are rejected when access to the requested URI is not allowed

	Feature Key	Feature Description	Feature Test Requirements
Error Flow	S_M_99	Response to admin commands within the POST command: HTTP response status code “403” for non-executed admin commands	Required to test whether HTTP response status code “403” for non-executed admin is interpreted correctly.
	S_M_98	Response to admin commands within the POST command for non-executed admin commands: Error result string: code error	Required to test whether correct Error strings are returned.

Table 4: Applicability Table for Enabler SCWS Server Mandatory Test Requirements

5.1.1.5 Device

	Feature Key	Feature Description	Feature Test Requirements
Normal Flow	D_M_01	Use local transport protocols with the smart card (BIP transport protocol or TCP/IP transport protocol)	Required to test whether local transport protocols can be used with smart card. i.e. BIP protocol or TCP/IP protocol
	D_M_02	BIP transport protocol: When BIP transport protocol is used, be able to open at least 2 BIP channels in “TCP, UICC in server mode”	Required to test whether terminal application can open at least 2 BIP channels in “TCP, UICC in server mode”.
	D_M_03	BIP transport protocol: When BIP transport protocol is used, be able to open an additional BIP channel “TCP, UICC in client mode” for SCWS administration	Required to test whether terminal application can open an additional BIP channel “TCP, UICC in client mode” for SCWS administration.
	D_M_04	TCP/IP transport protocol: When TCP/IP transport protocol is used, be able to open a local TCP/IP connection using Ethernet Emulation Model (EEM) subclass	Required to test whether terminal can open a direct TCP/IP connection with Ethernet Emulation Model (EEM) subclass with SCWS.
	D_M_05	TCP/IP transport protocol: When TCP/IP transport protocol is used, be able to open a remote TCP/IP connection using Ethernet Emulation Model (EEM) subclass	Required to test whether terminal can open a direct TCP/IP connection with a remote administration server using Ethernet Emulation Model (EEM) subclass.
	D_M_06	Retrieve the ACP from the SCWS	Required to test whether the ACP from the SCWS can be retrieved properly.
	D_M_07	SCWS ACP enforcer	Required to test whether the SCWS ACP enforcer is processed properly by the terminal.
Error Flow			

Table 5: Applicability Table for Enabler ME Mandatory Test Requirements

5.1.2 Optional Test Requirements

Optional test requirements should cover those features and use cases that are not mandated to be tested, but it is still felt that their inclusion will enhance the quality of the enabler validation.

Additionally, important conformance test requirements MAY be listed.

These features and use cases SHOULD cover optional and MAY cover mandatory implementation features. In case a mandatory feature is listed here, the Feature Test Requirements column should provide an explanation why testing of this feature is not mandated.

NOTE: This table needs to be filled out at a level where ambiguity is not present but details are not overwhelming.

Ambiguity means that the details do not have several meanings nor have more than one possible implementation path following.

5.1.2.1 SCWS Admin Client

	Feature Key	Feature Description	Feature Test Requirements
Normal Flow	ADM_C_O_01	Trigger the administration session by a local event	Required to test whether an administration session can be triggered by a local event.
	ADM_C_O_03	Trigger the administration session by receiving an OMA SIP Push message.	Required to test whether the administration session can be triggered properly by receiving an OMA SIP Push message.
	ADM_C_O_02	Trigger several administration sessions.	Required to test whether several administration sessions could be trigerred and processed properly.
	ADM_C_O_04	TLS 1.1 protocol	Required to test whether TLS 1.1 protocol is processed properly. Implicit testing of TLS 1.1 protocol is sufficient. Explicit testing of TLS 1.1 protocol is not required.
	ADM_C_O_05	TLS 1.2 protocol	Required to test whether TLS 1.2 protocol is processed properly. Implicit testing of TLS 1.2 protocol is sufficient. Explicit testing of TLS 1.2 protocol is not required.
	ADM_C_O_06	TLS Cipher-Suite TLS_PSK_WITH_AES_128_CBC_SHA256	When using TLS 1.2 protocol, required to test whether PSK-TLS using cipher-suite. TLS_PSK_WITH_AES_128_CBC_SHA256 is processed properly. Implicit testing of the cipher-suite is sufficient.
	ADM_C_O_07	TLS Cipher-Suite TLS_PSK_WITH_NULL_SHA256	When using TLS 1.2 protocol, required to test whether PSK-TLS using cipher-suite. TLS_PSK_WITH_NULL_SHA256 is processed properly. Implicit testing of the cipher-suite is sufficient.
Error Flow	ADM_C_O_08	Triggering of an administration session through the OMA SIP Push Enabler: Admin client is not able to store the request and responds HTTP response with status code = 503.	Required to test whether Admin client returns a HTTP response with status code = 503 when it is not able to store the administration session triggering request sent using an OMA SIP Push message.

Table 6: Applicability Table for Enabler SCWS Admin Client Optional Test Requirements

5.1.2.2 Remote SCWS Admin Server

	Feature Key	Feature Description	Feature Test Requirements

	Feature Key	Feature Description	Feature Test Requirements
Normal Flow	ADM_S_O_01	TLS extensions supported: Maximum Fragment Length Negotiation	Required to test whether TLS extensions are processed properly.
	ADM_S_O_02	TLS 1.1 protocol	Required to test whether TLS 1.1 protocol is processed properly. Implicit testing of TLS 1.1 protocol is sufficient. Explicit testing of TLS 1.1 protocol is not required.
	ADM_S_O_03	TLS 1.2 protocol	Required to test whether TLS 1.2 protocol is processed properly. Implicit testing of TLS 1.2 protocol is sufficient. Explicit testing of TLS 1.2 protocol is not required.
	ADM_S_O_04	TLS Cipher-Suite TLS_PSK_WITH_AES_128_CBC_SHA256	When using TLS 1.2 protocol, required to test whether PSK-TLS using cipher-suite. TLS_PSK_WITH_AES_128_CBC_SHA256 is processed properly. Implicit testing of the cipher-suite is sufficient.
	ADM_S_O_05	TLS Cipher-Suite TLS_PSK_WITH_NULL_SHA256	When using TLS 1.2 protocol, required to test whether PSK-TLS using cipher-suite. TLS_PSK_WITH_NULL_SHA256 is processed properly. Implicit testing of the cipher-suite is sufficient.
	ADM_S_O_06	Trigger the administration session by sending an OMA SIP Push message to the smart card	Required to test whether the administration session can be triggered properly by sending an OMA SIP Push message to the smart card.
Error Flow			

Table 7: Applicability Table for Enabler Remote SCWS Admin Server Optional Test Requirements

5.1.2.3 SCWS Client

	Feature Key	Feature Description	Feature Test Requirements
Normal Flow	C_O_01	TLS 1.0 protocol	Required to test whether TLS 1.0 protocol is processed properly. Implicit testing of TLS 1.0 protocol is sufficient. Explicit testing of TLS 1.0 protocol is not required.
	C_O_02	PSK-TLS protocol	Required to test whether PSK-TLS protocol is processed properly. Implicit testing of PSK-TLS protocol is sufficient. Explicit testing of PSK-TLS is not required.
	C_O_03	HTTP Basic authentication	Required to test whether HTTP basic authentication is executed properly.
	C_O_04	Support for HTTP Digest authentication	Required to test whether HTTP Digest authentication is executed properly.
Error Flow			

Table 8: Applicability Table for Enabler SCWS Admin Client Optional Test Requirements

5.1.2.4 SCWS Server

	Feature Key	Feature Description	Feature Test Requirements
Normal Flow	S_O_01	Support for HTTP Digest authentication	Required to test whether HTTP Digest authentication is executed properly.
	S_O_02	Support for server public key pair and certificate over TLS	Required to test whether Public Key Pair and device certificate is processed properly by the server authentication.
	S_O_03	Deliver an ACP data object	Required to test whether ACP data object can be delivered.
	S_O_04	UICC File access with URI	Required to test whether access to UICC files is processed properly.
	S_O_05	Content audit	Required to test whether audit of the SCWS content is processed properly.
	S_O_06	User self-care administration	Required to test whether user self-care administration is processed properly.
	S_O_07	Support of HTTPS with PK TLS	Required to test whether HTTPS with PK TLS protocol using BIP or TCP/IP is processed properly.
	S_O_08	Support of HTTPS with PSK-TLS	Required to test whether HTTPS with PSK-TLS protocol using BIP or TCP/IP is processed properly.
	S_O_09	Fragment Negotiation in TLS	Required to test whether Fragment Negotiation in TLS is processed properly. Implicit testing of Fragment Negotiation in TLS protocol is sufficient. Explicit testing of Fragment Negotiation in TLS is not required.
	S_O_10	Pipelined administrative commands	Required to test whether pipelined administrative commands are processed properly.
	S_O_11	Error flow on the optional features	Required to test error flow for the optional features.
Error Flow			

Table 9: Applicability Table for Enabler SCWS Server Optional Test Requirements

5.1.2.5 Device

	Feature Key	Feature Description	Feature Test Requirements
Normal Flow	D_O_01	Mnemonic names associated to the SCWS	Required to test whether mnemonic names are associated with the SCWS.
	D_O_02	Device implements a “trusted execution environment”	Required to test whether a “trusted execution environment” is processed properly.
	D_O_05	Forward the triggering message received by an OMA SIP Push message to the card administration agent using a HTTP POST request.	Required to test whether the administration session can be triggered properly by sending an OMA SIP Push message.
Error Flow			

Table 10: Applicability Table for Enabler ME Optional Test Requirements

5.2 Backwards Compatibility

OMA Smart Card Web Server version 1.2 is an evolution of OMA Smart Card Web Server version 1.1 and 1.0.

The purpose of Smart Card Web Server version 1.2 is to add functionality that was missing from version 1.1 and version 1.0.

	Feature Key	Feature Description	Feature Test Requirements
Normal Flow	BACK-001	SCWS Remote Admin server version 1.1 ability to process POST request from SCWS admin client implementing the SCWS V1.0	Required to test whether the POST request from SCWS Admin client implementing the SCWS V1.0 is processed properly by SCWS remote admin server version 1.1
	BACK-002	SCWS Admin client ability to process POST response from Remote SCWS admin server implementing the SCWS V1.0	Required to test whether the POST response from Remote SCWS admin server implementing the SCWS V1.0 is processed properly by SCWS admin client version 1.1
Error Flow			

Table 11: Backwards Compatibility Requirements

5.3 Enabler Dependencies

This section should outline what dependencies (if any) Enabler Smart Card Web Server V1.2 has on other Enablers (e.g. underlying protocols needed to support the Enabler)

In addition to the use of a secure SMS to trigger a remote administration session, Smart Card Web Server V1.2 defines the possibility to send this triggering message using an OMA SIP Push message as defined by [OMA SIP Push Enabler].

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 Version OMA-ETR-Smartcard_Web_Server-V1_2	14 Dec 2010	All	First draft based on SCWS 1.1 ETR and last OMA template.
	25 Jan 2011	All	The following CR is incorporated: OMA-ARC-SCT-2011-0008R01-CR_ETR_Updates
	15 Mar 2011	Serctions 2.1, 3.2 and 3.3 Sections 5.1.1.5 and 5.1.2.5	Updates after the SCWS 1.2 Consistency Review. The 2011 OMA Template is applied. The following CRs are incorporated: OMA-ARC-SCT-2011-0025R01-CR_CONR_EditorialComments_ETR OMA-ARC-SCT-2011-0026R01-CR_CONR_TechnicalComments_ETR
Candidate Version OMA-ETR-Smartcard_Web_Server-V1_2	19 Apr 2011	All	Status changed to Candidate by TP: OMA-TP-2011-0138-INP_SCWS_V1_2_ERP_for_Candidate_Approval