Enabler Test Report

Smartcard Web Server v1.0

OMA TestFest (January 2008)
Version 1st February 2008

Open Mobile Alliance
OMA-Enabler_Test_Report-SCWS-V1_0-20080201

This document is a work in process and is not an approved Open Mobile Alliance™ specification. This document is subject to revision or removal without notice. No part of this document may be used to claim conformance or interoperability with the Open Mobile Alliance specifications.

Contents

1. Scope

This report describes the results from the testing carried out at OMA TestFest-22 (January 2008) concerning the Smartcard Web Server Version 1.0 Enabler.

2. References

2.1 Normative References

[IOPPROC] OMA Interoperability Policy and Process, http://www.openmobilealliance.org/

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

[ERELD] Enabler Release Definition for Smartcard Web Server, OMA-ERELD-Smartcard_Web_Server-V1_0-20071002-C.pdf , http://www.openmobilealliance.org/

[SCWS_SPEC] Enabler Release Package for Smartcard Web Server, OMA-ERP-Smartcard_Web_Server-V1_0-20071002-C, http://www.openmobilealliance.org/

[EVP] Enabler Validation Plan for Smartcard Web Server, OMA-EVP-Smartcard_Web_Server-V1_0-20071106-C, http://www.openmobilealliance.org/

[ETS] Enabler Test Specification for Smartcard Web Server (Interoperability), OMA-ETS-Smartcard_Web_Server-V1_0-20071106-C, http://www.openmobilealliance.org/

[SCWS_EICS] Enabler Implementation Conformance Statements, OMA-EICS-Smartcard_Web_Server_AdminServer-V1_0-20070405-A, OMA-EICS-Smartcard_Web_Server_Device-V1_0-20070405-A, OMA-EICS-Smartcard_Web_Server_Smartcard-V1_0-20070405-A; URL:http://www.openmobilealliance.org/

2.2 Informative References

[OMADICT] Dictionary for OMA Specification, OMA-Dictionary http://www.openmobilealliance.org/

[SCWS WID] Smartcard web server work item (WID 92)

3. Terminology and Conventions

3.1 Conventions

This is an informative document, i.e. the document does not intend to contain normative statements.

3.2 Definitions

Application authentication An application that is invoked by the SCWS and that may generate dynamic content can implement its own user or principal authentication scheme. We call this authentication “Application authentication”.

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

BIP gateway BIP implementation in the terminal as defined in [TS 102 223].

Browser A program used to view (x) HTML or other media type documents.

CSIM A Cdma2000 Subscriber Identify Module is an application defined in [3GPP2 C.S0065] residing on the UICC to register services provided by 3GPP2 mobile networks with the appropriate security.

HTTPS A short term for HTTP over TLS.

ISIM An IP Multimedia Services Identity Module is an application defined in [3GPP TS 31.103] residing in the memory of the UICC, providing IP service identification, authentication and ability to set up Multimedia IP Services.

Network Operator An entity that is licensed and allocated frequency to operate a public mobile wireless telecommunications network for the purpose of providing publicly available commercial services.

Proactive UICC session A “Proactive UICC session” is a sequence of related CAT commands and responses which start with the status response '91XX' (proactive command pending) and ends with a status response of '90 00' (normal ending of command) after Terminal Response as defined in [TS 102223].

ProactiveHandler A ProactiveHandler is a smart card entity that is in charge of managing Proactive UICC sessions. Only one Proactive UICC session can be active at a given time.

R-UIM A Removable User Identity Module is a standalone module defined in [3GPP2 C.S0023] to register services provided by 3GPP2 mobile networks with the appropriate security.

SCWS proactive session A “SCWS proactive session” is a proactive UICC session that has been opened by a SCWS and is maintained by a SCWS.

SIM A Subscriber Identity Module is a standalone module defined in [3GPP TS 51.011] to register services provided by 2G mobile networks with the appropriate security.

Smart card This is a portable tamper resistant device with an embedded microprocessor chip. A smart card is used for storing data (e.g. access codes, user subscription information, secret keys etc.) and performing typically security related operations like encryption and authentication. A smart card may contain one or more network authentication applications like the SIM (Subscriber Identification Module), USIM, R-UIM (Removable – User Identification Module), CSIM (CDMA SIM).

Smart card application An application that executes in the smart card.

Smart card issuer The entity that gives/sales the smart card to the user (e.g. network operator for a SIM card).

Terminal (or device) A voice and/or data terminal that uses a Wireless Bearer for data transfer. Terminal types may include (but are not limited to): mobile phones (GSM, CDMA, 3GSM, etc.), data-only terminals, PDAs, laptop computers, PCMCIA cards for data communication and unattended data-only terminals (e.g., vending machines).

UICC UICC is the smart card defined for the ETSI standard [TS 102 221]. It is a platform to resident applications (e.g. USIM, CSIM or ISIM).

URI Uniform Resource Identifiers (URI, see [RFC1630]) provides a simple and extensible means for identifying a resource. URI syntax is widely used to address Internet resources over the web but is also adapted to local resources over a wide variety of protocols and interfaces.

URL The specification is derived from concepts introduced by the World-Wide Web global information initiative, whose use of such objects dates from 1990 and is described in "Universal Resource Identifiers in WWW", RFC 1630. The specification of URLs (see [RFC1738]) is designed to meet the requirements laid out in "Functional Requirements for Internet Resource Locators".

User Person who interacts with a user agent to view, hear or otherwise use a resource

USIM A Universal Subscriber Identity Module is an application defined in [3GPP TS 31.102] residing in the memory of the UICC to register services provided by 3GPP mobile networks with the appropriate security.

Web Page A document viewable by using a web browser or client application which is connected to the page server.

Web server A server process running on a processor, which sends out web pages in response to HTTP requests from browsers.

3.3 Abbreviations

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

4. Summary

This report gives details of the testing carried out during the OMA TestFest-22 (January 2008) for Smartcard-Web-Server (SCWS) v1.0.

The report is compiled on behalf of OMA by the OMA Trusted Zone.

The work and reporting has followed the OMA IOP processes and policies [IOPPROC].

5. Test Details

5.1 Documentation

This chapter lists the details of the enabler and any documentation, tools or test suites used to prove the enabler.

Date:	18th to 25th January 2008
Location:	Montréal, Canada
Enabler:	Smartcard Web Server v1.0
Process:	OMA Interoperability Policy and Process [OMAIOPPROC]
Type of Testing	Interoperability Testing
Products tested:	Device-Smartcard-Admin Server
Test Guidlines:	SCWS Enabler Validation Plan - OMA-EVP-Smartcard_Web_Server-V1_0-20071106-C [EVP]
Test Specification:	SCWS Enabler Test Specification - OMA-ETS-Smartcard_Web_Server-V1_0-20071106-C OMA-ETS-Smartcard_Web_Server_CONTENT_V1_0-20071106-C [ETS]
Test Tool:	None
Test Code:	None
Type of Test event:	TestFest
Participants:	gemalto N.V. and 4other companies
Number of Client Implementations:	2
Participating Technology Providers for clients:	2 companies
Implementation IDs for each client:	2 clients
Number of Smartcard Implementations:	3
Participating Technology Providers for Smartcards:	gemalto N.V. and 2 other companies
Implementation IDs for each Smartcard:	gemalto SCWS smartcard and 2 other smartcards.
Number of Admin Server Implementations:	2
Participating Technology Providers for Admin servers:	gemalto N.V. and 1 other company.

Implementation IDs for each Admin server:	gemalto SCWS admin server and 1 other admin server
Number of test sessions completed:	18

Table 1. Test Information

5.2 Test Case Statistics

5.2.1 Test Case Summary

This chapter gives an overview of the result for all test cases included in [ETS].

The following status is used in the tables below:

- Total number of TCs: Used in the summary to indicate how many test cases there are in total.
- Number of passed: Used in the summary to indicate how many of the total testcases that successfully has been passed.
- Number of failed: Used in the summary to indicate how many of the total testcases that has failed.
- Number of N/A: Used in the summary to indicate how many of the total testcases that has not be run due to that the implementation(s) do not support the functionality required to run this test case.
- Number of OT: Used in the summary to indicate how many of the total testcases that has not be run due to no time to run the test case.
- Number of INC: Used in the summary to indicate how many of the total testcases that has not been run due to that the functionality could not be tested due to an error in the implementation in another functionality that is required to run this test case.

Test Section:	Number of test sessions:	Total number of TCs:	Number of Passed:	Number of Failed:	Number of N/A:	Number of OT:	Number of INC:	Total:
Device to Smartcard TCs	6	27	156	0	6	0	0	162
Smartcard to Admin Server	12	14	125	0	43	0	0	168
Total	**18**	**41**	**281**	**0**	**49**	**0**	**0**	**330**

Table 2. Test Summary Table

5.2.2 Test Case List

This chapter lists the statistics for all all interoperability test cases included in [ETS].

The following status is used in the tables below:

- **Runs (R)**: Used to indicate the total number of times the test case have been run (R = P + F + I).
- **Pass (P):** Used to indicate how many times the test case have been run and successfully passed.
- **Fail (F):** Used to indicate how many times the test cases have been run and failed (used when the failure reason is known).
- **Inconclusive (I)**: Used to indicate how many times the test cases have been run and did not pass due to other nature than conclusive implementation or specification failure (e.g.: the failure reason cannot be clearly determined).
- **Not Applicable (N/A):** Used to indicate how many times the test cases have not be run due to lack of support for the required functionality to run this test case by one or more involved implementations.
- **Out of Time (O):** Used to indicate how many times the test cases have not been run due to lack of time.
- **Problem Report (PR):** Used to indicate how many PRs have been issued for the test case.
- **Note:** Used to indicate the cause of the Inconclusive or Failed results.

Tests for Smartcard Web Server TestFest Taken From OMA-ETS-Smartcard_Web_Server-V1_0-20071106-C

Test Case id:	Description:	Test Counts						PR:	Note:
		R	P	F	O	I	N/A		
SCWS-1.0-INT-001	The purpose is to verify that gif image of size 117 bytes is correctly sent from server to client.	6	6	0	0	0	0		
SCWS-1.0-INT-002	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	6	6	0	0	0	0		
SCWS-1.0-INT-003	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.	6	6	0	0	0	0		

Test Case id:	Description:	Test Counts						PR:	Note:
		R	P	F	O	I	N/A		
SCWS-1.0-INT-004	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.	4	4	0	0	0	2		
SCWS-1.0-INT-005	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.	2	2	0	0	0	4		
SCWS-1.0-INT-100	The purpose is to verify that server is accessible in off-line mode (no network connection).	6	6	0	0	0	0		
SCWS-1.0-INT-101	The purpose is to verify that html page with many resources (9 gif anf 1 stylesheet) is correctly sent from server to client.	6	6	0	0	0	0		
SCWS-1.0-INT-102	This test case will test mutiple http connection in parallele.	6	6	0	0	0	0		
SCWS-1.0-INT-103	The purpose is to verify that client/server connection cancelled is correctly managed. This test case will test http message exhange interruption by BIP event channel status ESTABLISHED, LISTEN.	6	6	0	0	0	0		
SCWS-1.0-INT-104	The purpose is to verify that client/server connection interruption is correctly managed. This test case will test http message exhange interruption by BIP event channel status ESTABLISHED, LISTEN in multiple connection mode.	6	6	0	0	0	0		
SCWS-1.0-INT-105	The purpose is to verify that admin client connection is taken into account when receiving during client / server exchange.	12	12	0	0	0	0		
SCWS-1.0-INT-106	The purpose is to verify that the SCWS doesn’t modify the behaviour of CAT applications	6	6	0	0	0	0		

Test Case id:	Description:	Test Counts						PR:	Note:
		R	P	F	O	I	N/A		
SCWS-1.0-INT-107	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.	6	6	0	0	0	0		
SCWS-1.0-INT-200	The purpose is to verify that uri with a long file name is correctly handled by server.	6	6	0	0	0	0		
SCWS-1.0-INT-201	The purpose is to verify that uri with a long directory name is correctly handled by server.	6	6	0	0	0	0		
SCWS-1.0-INT-202	The purpose is to verify that uri with escaped char is correctly handled by server.	6	6	0	0	0	0		
SCWS-1.0-INT-203	The purpose is to verify that uri with query string is correctly handled by server.	6	6	0	0	0	0		
SCWS-1.0-INT-204	The purpose is to verify that uri of 1024 bytes is correctly handled by server.	6	6	0	0	0	0		
SCWS-1.0-INT-205	The purpose is to verify that not found uri is correctly handled by client and server.	6	6	0	0	0	0		
SCWS-1.0-INT-206	The purpose is to verify that uri 5 levels of directory is correctly handled by server.	6	6	0	0	0	0		
SCWS-1.0-INT-250	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’.	6	6	0	0	0	0		
SCWS-1.0-INT-251	The purpose is to verify that resource protected by admin protection is not accessible throught WAP Browser. This test case will test HTTP status-code ‘403 Forbiden’.	6	6	0	0	0	0		

Test Case id:	Description:	Test Counts						PR:	Note:
		R	P	F	O	I	N/A		
SCWS-1.0-INT-300	The purpose is to verify that server dynamic content application is correctly triggered on HTTP POST method. This test case will test htpp POST message with content-body handle by dynamic content application.	6	6	0	0	0	0		
SCWS-1.0-INT-301	The purpose is to verify that server dynamic content application is correctly triggered on HTTP GET method. This test case will test htpp GET message with query-string handle by dynamic content application.	6	6	0	0	0	0		
SCWS-1.0-INT-302	The purpose is to verify that server response error 404 not found on an http request POST with an unxeistant uri.	6	6	0	0	0	0		
SCWS-1.0-INT-303	The purpose is to verify that dynamic content application response with HTTP Header “Transfert-Encoding: chuncked” is correctly processed by Device, SCWS Client.	6	6	0	0	0	0		
SCWS-1.0-INT-304	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.	6	6	0	0	0	0		
SCWS-1.0-INT-305	The purpose is to verify that server dynamic content application is correctly sending an SMS to another handset.	6	6	0	0	0	0		
SCWS-1.0-INT-500	The purpose is to verify single resource 1kb (portal ’oma-500’)can be sent, received throught full admin protocol.	12	12	0	0	0	0		

Test Case id:	Description:	Test Counts						PR:	Note:
		R	P	F	O	I	N/A		
SCWS-1.0-INT-501	The purpose is to verify single resource 10kb (portal 'oma-501') can be sent, received throught full admin protocol. This test case will test POST response of remote admin server with HTTP header 'Transfert-Encoding: chuncked'.	12	12	0	0	0	0		
SCWS-1.0-INT-502	The purpose is to verify that portal of 32kb (portal 'oma-502') with multiple resources can be sent, received throught full admin protocol. This portal contains 2 different pages: - Page 1 with 4 images of 5kb. - Page 2 with 6 images of 2kb. This test case will test POST response of remote admin server with pipelined administration command.	12	12	0	0	0	0		
SCWS-1.0-INT-503	The purpose is to verify that portal of 100kb (portal 'oma-503') with multiple resources can be sent, received throught full admin protocol. This portal contains 3 different pages: - Page 1 with 2 images of 18kb. - Page 2 with 8 images of 5kb. - Page 3 with 12 images of 2kb. This test case will test POST response of remote admin server with pipelined administration command and and with HTTP header 'Transfert-Encoding: chuncked'.	12	12	0	0	0	0		
SCWS-1.0-INT-551	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'.	6	6	0	0	0	6		

Test Case id:	Description:	Test Counts						PR:	Note:
		R	P	F	O	I	N/A		
SCWS-1.0-INT-552	The purpose is to verify that SCWS admin client retry administration session when the current admin session is interrupted by network coverage loss. This test case will test SCWS admin client resume admin session, BIP event channel status link-dropped, BIP commad SEND_DATA, RECEIVED_DATA terminal response temporary-error or permanent-error.	5	5	0	0	0	7		
SCWS-1.0-INT-553	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.	8	8	0	0	0	4		
SCWS-1.0-INT-554	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.	12	12	0	0	0	0		
SCWS-1.0-INT-555	The purpose is to verify that administration session is taken into account when card administration agent trigerring event (push sms) is received in other card application toolkit context.	12	12	0	0	0	0		
SCWS-1.0-INT-556	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.	12	12	0	0	0	0		

Test Case id:	Description:	Test Counts						PR:	Note:
		R	P	F	O	I	N/A		
SCWS-1.0-INT-600	The purpose is to verify that administration session is correctly processed using TLS communication channel using cipher suite TLS_PSK_WITH_3DES_EDE_CBC_SHA.	4	4	0	0	0	8		
SCWS-1.0-INT-601	The purpose is to verify that administration session is correctly processed using TLS communication channel using cipher suite TLS_PSK_WITH_AES_128_CBC_SHA.	4	4	0	0	0	8		
SCWS-1.0-INT-701	The purpose is to deactivate the SCWS using the lightweight protocol. At the end the SCWS shall be reactivated.	2	2	0	0	0	10		

Table 3. Test Case Counts

5.3 Problem Reports

During the activities for TestFest-22, the following problem reports were generated relating to the test materials and test process:

PR Number	Affecting	Description	Test Case reference / Specification reference
		None raised from this event	

Table 4. Problem Reports

Full details of the Problem Reports can be found at:

http://www.openmobilealliance.org/TestFests/Problem_Reporting.aspx

6. Confirmation

This signature states that the included information is true and valid.

OMA Trusted Zone

Appendix A. Change History (Informative)

Type of Change	Date	Section	Description
Initial Release	1st February 2008	All	First Version from TestFest-22