Enabler Release Definition for **Smartcard-Web-Server**

Candidate Version1.2 – 19 Apr 2011

Open Mobile Alliance

OMA-ERELD-Smartcard_Web_Server-V1_2-20110419-C

Contents

Tables

1. Scope

The scope of this document is limited to the Enabler Release Definition of Smart Card Web Server (SCWS) v1.2 according to OMA Release process and the Enabler Release specification baseline listed in section 5.

2. References

2.1 Normative References

[3GPP TS 31.102] "Characteristics of the Universal Subscriber Identity Module (USIM) application", 3rd Generation Partnership Project (3GPP), TS 31.102, URL: http://www.3gpp.org

[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] "Smart Cards; UICC-Terminal interface; Physical and logical characteristics", European Telecommunications Standards Institute (ETSI), TS 102 221,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

[HTTP/1.1] "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, June 1999, URL:http://www.ietf.org/rfc/rfc2616.txt

[HTTP over TLS] "Hypertext Transfer Protocol over TLS protocol", RFC 2818, May 2000, URL:http://www.ietf.org/rfc/rfc2818.txt

[ISO7816-4] "Information technology - Identification cards - Integrated circuit(s) cards with contacts – Part 4: Interindustry commands for interchange"

[OMA Push] "OMA Push", Open Mobile Alliance™, OMA-Push-V2_2, URL: http://www.openmobilealliance.org/

[OMA SIP Push] "OMA SIP Push", Open Mobile Alliance™, OMA-SIP-Push-V1_0, URL: http://www.openmobilealliance.org/

[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", URL: http://www.ietf.org/rfc/rfc1630.txt

[RFC1738] "Uniform Resource Locators (URL)", URL: http://www.ietf.org/rfc/rfc1738.txt

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

[RFC2617] "HTTP Authentication: Basic and Digest Access Authentication", URL: http://www.ietf.org/rfc/rfc2617.txt?number=2617

[SCRRULES] "SCR Rules and Procedures", Open Mobile Alliance™, OMA-ORG-SCR_Rules_and_Procedures, URL:http://www.openmobilealliance.org/

[SCWS_AD] "Smartcard Web Server Architecture", Open Mobile Alliance™, OMA-AD-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_2,

[SCWS_TS] "Smartcard Web Server", Open Mobile Alliance™, OMA-TS-Smartcard_Web_Server-V1_2, 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

[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,

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”, "Release Version Overview" and “Conformance Requirements Notation Details”, are normative, unless they are explicitly indicated to be informative.

The formal notation convention used in sections 8 and 9 to formally express the structure and internal dependencies between specifications in the Enabler Release specification baseline is detailed in [SCRRULES].

3.2 Definitions

Application	The implementation of a well-defined and related set of functions that perform useful work on behalf of the user. It may consist of software and or hardware elements and associated user interfaces.
BIP	Bearer Independent Protocol as defined in [ETSI TS 102 223].
Browser	A program used to view (x) HTML or other media type documents.
Content Provider	An entity that provides data that forms the basis of a service.
Device	In this context, a Device is a voice and/or data terminal that uses a Wireless Bearer for data transfer. Device 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 Devices (e.g., vending machines). Smart Cards are not considered as part of the device within the context of the Smart Card Web Server.
Enabler Release	Collection of specifications that combined together form an enabler for a service area, e.g. a download enabler, a browsing enabler, a messaging enabler, a location enabler, etc. The specifications that are forming an enabler should combined fulfil a number of related market requirements.
Minimum Functionality Description	Description of the guaranteed features and functionality that will be enabled by implementing the minimum mandatory part of the Enabler Release.
Network Operator	An entity that is licensed and allocated frequency to operate a public mobile wireless telecommunications network for the purpose of providing publicly available commercial services.
Smart Card	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). 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).
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 all 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.
Web Page	A document viewable by anyone connected to the page server who has a web browser.

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

3.3 Abbreviations

APDU	Application Protocol Data Units
ERDEF	Enabler Requirement Definition
ERELD	Enabler Release Definition
OMA	Open Mobile Alliance
OMNA	Open Mobile Naming Authority
R-UIM	Removable User Identity Module
SCWS	Smart Card Web Server
TCP	Transmission Control Protocol
(U)SIM	(Universal) Subscriber Identity Module

4. Release Version Overview

The Smart Card Web Server enabler defines the interfaces to an HTTP server in a smart card (i.e. Smart Card Web Server) that is embedded in a mobile device (e.g. SIM, (U)SIM, UICC, R-UIM, CSIM).

The main interfaces cover the following aspects:

- The URL to access the Smart Card Web Server (SCWS)
- The transport protocol that is used to enable the communication between HTTP applications in the device and the Smart Card Web Server
- The HTTP profile that the Smart Card Web Server needs to implement
- A secure remote administration protocol for the Smart Card Web Server
- User, or principal, authentication with the Smart Card Web Server and related security protocols

It is important to note that the Smart Card Web Server can be administrated only by the smart card issuer (e.g. Mobile Network Operator) or a delegated authorized entity. This clearly sets the scope of ownership and roles for the remote administration and services that are deployed via the Smart Card Web Server.

4.1 Version 1.0 Functionality

The Smart Card Web Server v1.0 enabler defines all the main requirements of an HTTP server implemented in a smart card, allowing an HTTP client running in the terminal (e.g. the browser) to access resources stored in the smart card. The content delivered by the SCWS can be static resources but also be generated by a smart card application. The SCWS 1.0 also defines the remote administration of the Smart Card Web Server by an authorized entity.

4.2 Version 1.1 Functionality

The Smart Card Web Server 1.1 enabler is a set of optimisations of the Smart Card Web Server 1.0 enabler and therefore does not introduce any new requirement or any change into the architecture. This enabler therefore refers to the requirements and architecture documents of the Smart Card Web Server 1.0 enabler.

The Smart Card Web Server v1.1 enabler improves the Smart Card Web Server v1.0 enabler mainly to optimise the remote management of the SCWS from different trusted entities. Each authorized entity is able to control what content and which smart card applications can be accessed under a given URI.

The Smart Card Web Server v1.1 also clarifies the cache management to improve the efficiency of the exchanges with the HTTP application in the terminal.

The Smart Card Web Server v1.1 has been updated to manage any type of resources allowing a SCWS implementation to be future proof using the `Content-Type`, `Content-Encoding` and `Content-Language` headers defined by the administration server.

The following other optimizations have been included:

- Deletion of a whole directory
- Management of multiple audit commands in the same administration request
- Addition of a cipher suite for PSK-TLS requesting only a signature
- Management of a default page when "`abs_path`" is "/"

The following clarifications have been added:

- Behaviour when the card memory is full

- Behaviour when the SCWS doesn't support persistent connections

Finally the Smart Card Web Server v1.1 enabler clarifies the expected behaviour of the SCWS and of the Remote Administration server to ensure compatibility with former versions of the SCWS enabler.

4.2.1 Version 1.1.1 Functionality

The Smart Card Web Server 1.1.1 enabler provides corrections and clarifications on the Smart Card Web Server 1.1.

4.3 Version 1.2 Functionality

The Smart Card Web Server 1.2 enabler introduces the references to latest versions of TLS (i.e. [TLS 1.1] and [TLS 1.2]) and a new requirement confirming that another removable web server operating in the same terminal can be accessed.

The Smart Card Web Server 1.2 enabler also provides clarification on the implementation of the Smart Card Web Server when using TCP/IP transport Protocol.

The Smart Card Web Server 1.2 enabler introduces the notion of Granted Memory associated to a card administration agent. It allows restricting the amount of content associated to an authorized entity administrating the SCWS content.

To trigger a remote administration session, the Smart Card Web Server already defines the use of a secure SMS sent to a card administration agent. With the Smart Card Web Server 1.2 it is now possible to send this triggering message thanks to the OMA SIP Push Enabler.

With the increase of opened device operating systems, the Smart Card Web Server 1.2 sets the implementation of the Access Control Policy (ACP) mechanism as mandatory for the device.

5. Document Listing for SCWS

This section is normative.

Doc Ref	Permanent Document Reference	Description
Requirement Document		
[SCWS _RD]	OMA-RD-Smartcard_Web_Server-V1_2-20110419-C	Requirement Document for SCWS v1.2 Enabler
Architecture Document		
[SCWS_AD]	OMA-AD-Smartcard_Web_Server-V1_2-20110419-C	Architecture Document for SCWS v1.2 Enabler
Technical Specifications		
[SCWS_TS]	OMA-TS-Smartcard_Web_Server-V1_2-20110419-C	Specification that defines the protocols for the SCWS that provide control interface between the SCWS Client and SCWS Server and also between the SCWS server and a remote administration server.
Supporting Files		
(none)		

Table 1: Listing of Documents in SCWS Enabler

6. OMNA Considerations

The Smart Card Web Server 1.2 enabler includes the following OMNA item:

- PUSH Application Id:
  a. Number: to be assigned after OMNA registration
  b. URN: x-oma-application:push.scws
  c. Description: Identifier of the SCWS Push Gateway to receive OMA SIP Push messages to trigger a SCWS remote administration session.

7. Conformance Requirements Notation Details

This section is informative

The tables in following chapters use the following notation:

Item: Entry in this column MUST be a valid ScrItem according to [SCRRULES].

Feature/Application: Entry in this column SHOULD be a short descriptive label to the **Item** in question.

Requirement: Expression in the column MUST be a valid TerminalExpression according to [SCRRULES] and it MUST accurately reflect the architectural requirement of the **Item** in question.

8. ERDEF for SCWS - Client Requirements

This section is normative.

The Client is an application running in the Device that connects to the SCWS (Smart Card Web Server).

Item	Feature / Application	Requirement
OMA-ERDEF-SCWS-C-001-M	SCWS Client	[SCWS-TS]: MCF

Table 2: ERDEF for SCWS Client-side Requirements

9. ERDEF for SCWS - Server Requirements

This section is normative.

Item	Feature / Application	Requirement
OMA-ERDEF-SCWS-S-001-M	SCWS Server	[SCWS-TS]: MSF

Table 3: ERDEF for SCWS Server-side Requirements

10.ERDEF for SCWS – Admin Client Requirements

This section is normative.

The Admin Client is an application running in the smart card that connects to a remote administration server in order to receive administration commands that are addressed to the SCWS.

Item	Feature / Application	Requirement
OMA-ERDEF-SCWS-admin-C-001-M	SCWS Admin Client	[SCWS-TS]: MCF (admin)

Table 4: ERDEF for SCWS Admin Client-side Requirements

11. ERDEF for SCWS – Remote Admin Server Requirements

This section is normative.
The Admin Server is a remote administration server that sends administration commands to the SCWS via the Admin Client in the smart card.

Item	Feature / Application	Requirement
OMA-ERDEF-SCWS-admin-S-001-M	SCWS Remote Admin Server	[SCWS-TS]: MSF (admin)

Table 5: ERDEF for SCWS Remote Admin Server-side Requirements

12.ERDEF for SCWS – Device Requirements

This section is normative.

The Device in which the SCWS Client (application that connects to the SCWS) is running.

Item	Feature / Application	Requirement
OMA-ERDEF-SCWS-Device-001-M	Device	[SCWS-TS]: MDF (D-stands for Device)

Table 6: ERDEF for SCWS ME Requirements

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-ERELD-Smartcard_Web_Server-V1_2	09 Nov 2010	All	Initial version, based on OMA-ERELD-Smartcard_Web_Server-V1_1_1-20100910-A.
Candidate Version OMA-ERELD-Smartcard_Web_Server-V1_2	11 Jan 2011	All	Status changed to Candidate by TP: OMA-TP-2010-0529-INP_SCWS_V1_2_AD_and_RD_for_Candidate_Approval
Draft Versions OMA-ERELD-Smartcard_Web_Server-V1_2	01 Feb 2011	Section 4.3, section 5 and section 6	The following CR is integrated: OMA-ARC-SCT-2011-0016R01-CR_ERELD_updates.doc
	11 Feb 2011	5	Document listing updated
	16 Mar 2011	5	Document listing updated before CONR closure
Candidate Version OMA-ERELD-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