Enabler Release Definition for Smartcard-Web-Server

Candidate Version 1.1 – 12 Aug 2008

Open Mobile Alliance

OMA-ERELD- Smartcard_Web_Server-V1_1-20080812-C

Contents

Tables

1. Scope

The scope of this document is limited to the Enabler Release Definition of Smartcard Web Server (SCWS) v1.1 according to OMA Release process and the Enabler Release specification baseline listed in section 5.

2. References

2.1 Normative References

[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-TLS-Profile] "OMA TLS Profile", Open Mobile Alliance™, OMA-TS-TLS-V1_0, URL: 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

[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_0, 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/

[SCWS_TS] "Smartcard Web Server", Open Mobile Alliance™, OMA-TS-Smartcard_Web_Server-V1_1, URL: http://www.openmobilealliance.org/

[TLS] "Security Transport Protcol", RFC 2246, January 1999, URL: http://www.ietf.org/rfc/rfc2246.txt

[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

2.2 Informative References

[OMADICT] "Dictionary for OMA Specifications", Version x.y, Open Mobile Alliance™, OMA-ORG-Dictionary-V2_1, URL:http://www.openmobilealliance.org/

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

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

[WP HTTP] "Wireless Profiled HTTP", WAP Forum™, WAP-229-HTTP, 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”, "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 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.
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.
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.
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.
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", [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

APDU	Application Protocol Data Units
CSIM	CDMA SIM
ERDEF	Enabler Requirement Definition
ERELD	Enabler Release Definition
IP	Internet Protocol
OMA	Open Mobile Alliance
OMNA	Open Mobile Naming Authority
PSK-TLS	Pre-Shared Key TLS
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. 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.

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_0-20080421-A	Requirement Document for SCWS Enabler This document is inherited from SCWS 1.0, since no changes are needed to the requirements in SCWS 1.1.
Architecture Document		
[SCWS_AD]	OMA-AD-Smartcard_Web_Server-V1_0-20080421-A	Architecture Document for SCWS Enabler This document is inherited from SCWS 1.0, since no architectural changes are needed to the requirements in SCWS 1.1.
Technical Specifications		
[SCWS_TS]	OMA-TS-Smartcard_Web_Server-V1_1-20080812-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

This release does not have any OMNA items for handling

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	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	Smart Card Web 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	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	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	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
Approved Version OMA-ERELD-Smartcard_Web_Server-V1_0	21 Apr 2008	Status changed to Approved by TP TP ref # OMA-TP-2008-0139-INP_SCWS_V1_0_ERP_and_IOP_RPT_for_final_approval

A.2 Draft/Candidate Version 1.1 History

Document Identifier	Date	Sections	Description
Draft Versions OMA-ERELD-Smartcard_Web_Server-V1_1	22 May 2008	n/a	Initial - Draft ERELD for the Smartcard Web Server Enabler v1.1
	26 May 2008	4.2	Editorial correction
	26 June 2008	4.2	Editorial correction
Draft Version OMA-ERELD-Smartcard_Web_Server-V1_1	28 Jul 2008	4.2,5	Incorporated Agreed CR: OMA-SCT-2008-0063R04-CR_ERELD_Update.doc
	29 Jul 2008	4.2,5	Corrections to above CR
Candidate Version OMA-ERELD-Smartcard_Web_Server-V1_1	12 Aug 2008	All	Status changed to Candidate by TP TP ref#: OMA-TP-2008-0271R05-INP_Smartcard_Web_Server_V1_1_ERP_for_Candidate_Approval.zip