# Smartcard Web Server Requirements

Approved Version 1.0 – 21 Apr 2008

**Open Mobile Alliance**

OMA-RD_Smartcard_Web_Server-V1_0-20080421-A

# Contents

# Tables

# 1. Scope (Informative)

Network operators aim to improve the user experience when using network operator services in the smart card. The OMA-SEC Smart Card Technology sub-working group (SEC-SCT) has identified these requirements and proposes a solution with the Smart Card Web Server (SCWS).

The SCWS enables smart card issuers to offer static or dynamic web pages. One network operator centric example could be pages generated by applications running in the smart card (e.g. SIM, UICC or R-UIM), enabling access to content (e.g. questionnaires, FAQs) or security-oriented services requiring keys that are stored in the smart card.
All these services will be accessible via a web browser in the device.

This document is a requirement document for the work item presented in [SCWS WID].

# 2. References

## 2.1 Normative References


**[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

**[HTTPS]** "Secure Hypertext Transfer Protocol", RFC 2660, August 1999, URL:http://www.ietf.org/rfc/rfc2660.txt

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

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

**[WAPWAE]** Wireless Application Environment Specification, Open Mobile Alliance™, OMA-WAP-WAESpec-V2_3-20040815 {-Candidate}, URL:http://www.openmobilealliance.org/

**[WP HTTP]** Wireless Profiled HTTP, Open Mobile Alliance™, WAP-229-HTTP-20010329-a, URL:http://www.openmobilealliance.org/


## 2.2 Informative References


**[SCWS WID]** Smart card web server work item (WID 92)

# 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

| | |
|---|---|
| **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. |
| **Local services** | Services that reside in the smart card web server |
| **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, USIM, R-UIM. |
| **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. mobile operator for a SIM card) |
| **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’s server who has a web browser |
| **Web server** | A server process running at a web site, which sends out web pages in response to HTTP requests from remote browsers. |
| **Web site** | A computer connected to the internet that maintains a series of web pages |

## 3.3 Abbreviations

| | |
|---|---|
| **ME** | Mobile Equipment |
| **OMA** | Open Mobile Alliance |
| **SCWS** | Smart Card Web Server |

# 4. Introduction (Informative)

The [SCWS WID] proposes to identify requirements, architecture and specifications for the mechanisms to access the smart card via a WAP/xHTML browser.

This document discusses the use cases and requirements for this WID. The main benefits from this work item are:

- Allow for quick and simple access via the WAP Browser to the SIM based Operators' services
- Allow SIM applications to benefit from WAP browser's rich user interface
- Allow Operators services to benefit from SIM security features

Having identified requirements, specification work will be coordinated with external fora (e.g. 3GPP, 3GPP2, ETSI…) in order to allow a smart card (e.g. SIM, UICC, R-UIM, WIM…) to behave like a web server, offering both static and dynamic web pages.

# 5. Use Cases (Informative)

This section describes, in the form of user scenarios, the benefits that users and mobile communication operators will have by the SCWS providing rich-content and operator's services hosted in the Smart card.

The purpose of this section is:

* To provide a better understanding of the functionality that the OMA Smart card Web Server solution should provide.
* To offer high level descriptions of different OMA scenarios against which the formal requirements for OMA-Smart card Web Server can be checked
* To be a public document that can help to explain what OMA Smart card Web Server is about.

## 5.1 Use Case I&E, Quick and simple access to operator's services

### 5.1.1 Short Description

Martin is now used to browse the Web with his handset; he's got his favourite links to a news site and a weather-forecasting site that are stored within his handset browser.

Unfortunately, he does not really understand the difference between accessing a web service and one of his network operator's services. Thus his operator has implemented Martin's accessible services on a Web Server Smart card in order gives him the same access method to these services as he accesses his internet sites. This way it is transparent for Martin whether his operator's services are smart card based or not.

### 5.1.2 Actors

- The user
- The network operator

#### 5.1.2.1 Actor Specific Issues

The operator is responsible for implementing services in the Smart Card Web Server.

#### 5.1.2.2 Actor Specific Benefits

The operator can provide local services to the user using the same browser like for any remote web application.

### 5.1.3 Pre-conditions

The operator has issued applications and content in the Smart Card Web Server.

The user has an ME that allows him to access the Smart Card Web Server URL.

### 5.1.4 Post-conditions

The user will be able to browse the Smart Card Web Server content and use the implemented services in the browser window.

### 5.1.5 Normal Flow

- The user open the ME Web browser, type in or select the Smart Card Web Server URL and access the home page that propses the list of services and content to browse.

# 5.2 Use Case I&E, Access to operator's services Off-line

## 5.2.1 Short Description

Thomas has got problems using his brand new handset; actually he's got problems establishing a data connection for his Internet browsing.

Fortunately for Thomas and his operator, there is a Frequently Asked Question web page stored on his Smart card and it is accessible off-line when he launches his browser. This will probably make Thomas and his operator save a lot of time and money as he's got a way to go forward before calling his operator's hotline…

## 5.2.2 Actors

- The user
- The network operator

### 5.2.2.1 Actor Specific Issues

The operator is responsible for implementing services in the Smart Card Web Server.

### 5.2.2.2 Actor Specific Benefits

The operator can provide local services to the user like any remote web application even if there is no connection to the network.

## 5.2.3 Pre-conditions

The operator has issued applications and content in the Smart Card Web Server.

The user has an ME that allows him to access the Smart Card Web Server URL.

## 5.2.4 Post-conditions

The user will be able to browse the Smart Card Web Server content and use the implemented services in the browser window.

## 5.2.5 Normal Flow

- The user open the ME Web browser, type in or select the Smart Card Web Server URL and access the home page that propses the list of services and content to browse.
- The user selects the FAQ link
- The FAQ is displayed formatted for an easy navigation

# 5.3 Use Case I&E, Enhanced operator's services Interface

## 5.3.1 Short Description

Ana most specially enjoys the nice high-resolution screen she's got on her handset. That's what makes her feel she's really got a nice phone, a device she enjoys to use.

Having rich content interface when accessing operator's services in the smart card definitely counts for her.

### 5.3.2 Actors

- The user
- The network operator

#### 5.3.2.1 Actor Specific Issues

The operator is responsible for implementing services in the Smart Card Web Server.

#### 5.3.2.2 Actor Specific Benefits

The operator can provide local services to the user using rich and attractive user interface like any remote web application.

### 5.3.3 Pre-conditions

The operator has issued applications and content in the Smart Card Web Server.

The user has an ME that allows him to access the Smart Card Web Server URL.

### 5.3.4 Post-conditions

The user will be able to browse the Smart Card Web Server content and use the implemented services in the browser window.

### 5.3.5 Normal Flow

- The user open the ME Web browser, type in or select the Smart Card Web Server URL and access the home page that propses the list of services and content to browse.
- The content is displayed in the browser window

## 5.4 Use Case I&E, Capture and Secure connection with a remote server

### 5.4.1 Short Description

Jack wants to go shopping this afternoon, but before that he would feel more comfortable if he had checked the balance of his bank account.

In fact, getting the balance of his bank account is a service he's got with his mobile phone operator. The service is based on the security provided by the operator's smart card present in the handset. So Jack connects to his bank web site and goes to his account review service. The bank web site redirects this request by sending a web page containing a link to the smartcard web server page which includss some authentication parameters and encrypted account data. Jack goes to the proposed link and authenticates himself with his PIN code as requested by the smartcard web server. The smartcard authenticates the bank request and returns the authentication data that are then redirected and sent to the bank Web server. Jack can now browse his account data and make some operations on his account.

The bank server can also send encrypted information embedded in the web page which is redirected to the smart card web server, decrypted and displayed to the user.

Jack is happy with his operator's set of security services because he no longer needs to remember a whole list of website passwords. Moreover, he is confident in the physical security provided by his smart card.

## 5.4.2 Actors

- The user
- The network operator
- The bank

### 5.4.2.1 Actor Specific Issues

The operator is responsible for implementing services in the Smart Card Web Server.

The bank implements a web application that does the redirection to the Smart Card Web Server for authentication.

### 5.4.2.2 Actor Specific Benefits

The operator can provide secure and local services to the user.

## 5.4.3 Pre-conditions

The operator has issued applications and content in the Smart Card Web Server.

The user has an ME that allows him to access the Smart Card Web Server URL.

The bank implements a web application that implements redirection to the Smart Card Web Server for authentication.

## 5.4.4 Post-conditions

The user will be able to browse the Smart Card Web Server security features while accessing the bank server.

## 5.4.5 Normal Flow

- The user open the ME Web browser, type in or select the Smart Card Web Server URL and access the home page that propses the list of services and content to browse.
- He then selects the service to access his bank account.
- The smart card web server returns an xHTML page with an external link to the bank web server which embed origin parameters
- The user selects this link
- The bank server returns an xHTML page that embed a link that is called ‘authentication’ that points to the smart card web server and that also embeds data (e.g. http://smartcard/authApp?data=x06543D8ABC0)
- When the user clicks on the ‘authentication’ link the smart card web server returns an xHTML page that asks the user for his pin code
- When the user enters his pin code the SCWS returns a page that contains a link called ‘Continue’ that embeds the returned authentication data (e.g. http://www.xyzBank.com/verifyAuth?auth=0xC567865AB0954D).
- When the user clicks on this link the data is sent to the bank webserver and the user is authenticated via the sent data
- The user has full access to his bank account

# 5.5 Use Case I&E, Setting preferences for an Operator application in the smart card

## 5.5.1 Short Description

Thomas has an operator application in his smart card that implements some services that require user input.

He can access this application with the smart card URL and the application displays a form with possible configuration parameters. Thomas fills this form and clicks the “Submit” button at the end. The application in the SIM card is now configured with the new parameters.

## 5.5.2 Actors

- The user
- The network operator

### 5.5.2.1 Actor Specific Issues

The operator is responsible for implementing services in the Smart Card Web Server prior to issuing the card to the user.

### 5.5.2.2 Actor Specific Benefits

The operator can provide an easy way of inputting user information for a Network Operator service.

## 5.5.3 Pre-conditions

The operator has issued applications and content in the Smart Card Web Server (prior to issuing the card to the user for example).

The user has an ME that allows him to access the Smart Card Web Server URL.

## 5.5.4 Post-conditions

The user will be able to browse the Smart Card Web Server content and set personal parameters in the implemented services via the browser window.

## 5.5.5 Normal Flow

- The user open the ME Web browser, type in or select the Smart Card Web Server URL and access the home page that propses the list of services and content to browse.
- The user selects an application, which then displays a menu that includes a link called “configure”.
- When clicking on it a form with possible configuration parameters is displayed.
- The user fills this form and clicks the “Submit” button at the end.
- The application in the SIM card is now configured with the new parameters.

## 5.6 Use Case I&E, Managing the smart card web server from a remote trusted application

### 5.6.1 Short Description

Ana uses an e-commerce service that is partially implemented in the smart card web server. She access this service with a URL that points to the smart card web server and gets an xHTML page with some external links to the operator's trusted server to perform some e-commerce operations.

After performing the needed operations the operator's server may detect that there is a need to update her e-commerce application in the smart card web server to upgrade to a new version. In this case it returns an xHTML page that suggests updating her application. When Ana accepts this request the remote server will establish a mutually authenticated HTTPS connection with the smart card web server and update the web application in the smart card web server. This operation can only be done by an authorized remote application since the smart card web server will accept updates only from an authenticated remote application based on credentials that are already provisioned in the smart card.

Ana will now have an upgraded ecommerce application that includes new features.

### 5.6.2 Actors

- The user
- The network operator

### 5.6.3 Actor Specific Issues

The operator is responsible for implementing services in the Smart Card Web Server and the remote application to administer it.

### 5.6.4 Actor Specific Benefits

The operator can provide secure and local services to the user like any remote web application and update it with new versions.

### 5.6.5 Pre-conditions

The operator has issued applications and content in the Smart Card Web Server and the administration remote application to update it.

The user has an ME that allows him to access the Smart Card Web Server URL.

### 5.6.6 Post-conditions

The user will be able to browse the Smart Card Web Server content and use the implemented services in the browser window.

### 5.6.7 Normal Flow

- The user opens the ME Web browser, type in or select the Smart Card Web Server URL and access the home page that propses the list of services and content to browse.
- The returned xHTML page contains an external link that is called "update application version".
- When the user clicks on this link it invokes a remote administration application that establishes a secure HTTPS link with the smart card web server with mutual authentication.
- The authenticated remote application checks the version of internal files and updates them if needed.

# 5.7 Use Case I&E, Loading Application from the SCWS to the ME

## 5.7.1 Short Description

James has aquired a new handset and SIM supporting SCWS containing a set of ME applications provided by his Operator. When James installs his SIM in the handset he can immediately start browsing his SCWS and load and install ME applications that he likes. Some time later when he will feel like changing handset, by simply shifting the SIM from the old phone to the new one, he will be able to install his ME applications to his new phone.

## 5.7.2 Actors

- The user
- The network operator

## 5.7.3 Actor Specific Issues

The operator is responsible for providing ME applications to download from the Smart Card Web Server.

## 5.7.4 Actor Specific Benefits

The operator can provide data and ME applications to be downloaded from the smart card web server.

## 5.7.5 Pre-conditions

The operator has issued content in the Smart Card Web Server that includes ME applications that can be downloaded into the ME.

The user has an ME that allows him to access the Smart Card Web Server URL.

## 5.7.6 Post-conditions

The user will be able to download ME applications from the Smart Card Web Server.

## 5.7.7 Normal Flow

- The user opens the ME Web browser, type in or select the Smart Card Web Server URL and access the home page that propses the list of services and content to browse.
- The returned xHTML page contains a list of ME applications to download and install in the ME (e.g. Games, Java MIDlets etc.)
- When the user clicks on a chosen ME application it is downloaded and installed in the ME.
- The user can invoke the ME application in the ME and use it.

# 5.8 Use Case I&E, PIN protected pages in the SCWS

## 5.8.1 Short Description

Bill has stored in his SCWS a set of personal information (Phonebook, contacts, adresses, passwords codes or other private information) to which access is protected by a PIN. At some point he needed to retrieve a password that he uses for accessing his favourite web sites. He starts his browser and enters his private section in the SCWS. The SCWS asks him for a PIN entry prior to displaying the protected information. He will then browse the content of all PIN protected pages at will.

### 5.8.2 Actors

- The user
- The network operator

### 5.8.3 Actor Specific Issues

The operator is responsible for providing applications (e.g. servelets) to mange private sections in the Smart Card Web Server.

### 5.8.4 Actor Specific Benefits

The operator can provide secure smart card services to the user.

### 5.8.5 Pre-conditions

The operator has issued applications and content in the Smart Card Web Server.

The user has an ME that allows him to access the Smart Card Web Server URL.

### 5.8.6 Post-conditions

The user will be able to securely store and retrieve private information in the Smart Card Web Server.

### 5.8.7 Normal Flow

- The user opens the ME Web browser, type in or select the Smart Card Web Server URL and access the home page that propses the list of services and content to browse.
- The returned xHTML page that contains a link to the user's private section
- When the user clicks on the above link the SCWS present a page that asks for user's PIN.
- The user enters his PIN and clicks the 'submit' button.
- The SCWS returns the xHTML pages with the private information

# 6. Requirements (Normative)

## 6.1 High-Level Functional Requirements

| Requirement number | Related Use-case | Requirement | Enabler Release |
|---|---|---|---|
| REQ-FCT-1 | All | A URL to access the SCWS SHALL be defined in this enabler | 1.0 |
| REQ-FCT-2 | All | The solution SHALL aim to minimize modification or adaptation of the web browser in the device | 1.0 |
| REQ-FCT-3 | <Access to card issuer's services Off-line> | It SHALL be possible to access the SCWS when the device is off-line (i.e. when network connection is not available) | 1.0 |
| REQ-FCT-4 | < Quick and simple access to card issuer's services > | The SCWS SHALL be able to serve static and dynamic content to the web browser in the device | 1.0 |
| REQ-FCT-5 | < Quick and simple access to card issuer's services > | The SCWS SHALL implement a default home page that shall be returned when no specific page is given with the URL | 1.0 |
| REQ-FCT-6 | <Setting preferences for a card issuer application in the smart card> | It SHALL be possible to provide data (such as queries, parameters, etc.) in the URL to access smartcard entities or applications | 1.0 |
| REQ-FCT-7 | <Enhanced card issuer's services Interface> | It SHALL be possible for the SCWS to invoke smart card applications. The SCWS shall be able to forward parameters to a smart card application and return the smart card application response. The sent URL SHALL identify the smart card application. | 1.0 |
| REQ-FCT-8 | All | The SCWS architecture SHALL allow the implementation of different mechanisms for the transport of data, in particular HTTP and HTTPS messages, between the SCWS and the device. | 1.0 |

**Table 1: High-Level Functional Requirements**

### 6.1.1 Security

| Requirement number | Related Use-case | Requirement | Enabler Release |
|---|---|---|---|
| REQ-SEC-1.1 | <PIN protected pages in the SCWS> | It SHALL be possible to authenticate a user to a smart card application using the SCWS | 1.0 |
| REQ-SEC-1.2 | <Capture and Secure connection with a remote server> | It SHALL be possible to authenticate a principal to a smart card application using the SCWS (principal as defined in OMA dictionary) | 1.0 |
| REQ-SEC-2 | <PIN protected pages in the SCWS><br><br><Capture and Secure connection with a remote server> | The SCWS SHALL support a mechanism so the browser is able to indicate to the user that the SCWS is being used | Future |
| REQ-SEC-3 | <PIN protected pages in the SCWS><br><br><Capture and Secure connection with a remote server> | The SCWS enabler SHALL provide a mechanism to control access of applications to the SCWS | 1.0 |
| REQ-SEC-4 | <PIN protected pages in the SCWS><br><br><Capture and Secure connection with a remote server> | Access control rights to the SCWS SHALL be indicated by the smart card. | 1.0 |

| Requirement number | Related Use-case | Requirement | Enabler Release |
|---|---|---|---|
| REQ-SEC-5 | <PIN protected pages in the SCWS><br><br><Capture and Secure connection with a remote server> | Access control rights to the SCWS SHALL deal with:<br>- preinstalled device browsers and applications (i.e. delivered by the device manufacturer)<br><br>- other device applications (e.g. based on their origin or user decision) | 1.0 |
| REQ-SEC-6.a | <Managing the smart card web server from a remote trusted application> | It SHALL be possible to manage the SCWS by a remote entity that establish an end to end secure session with mutual authentication | 1.0 |
| REQ-SEC-6.b | <Managing the smart card web server from a remote trusted application> | It SHALL be possible to browse the SCWS by a remote entity that establish an end to end secure session with mutual authentication. | Future |
| REQ-SEC-7 | All use cases | There SHALL be a clear separation between the interface to the SCWS and the interface to other applications in the smart card | 1.0 |
| REQ-SEC-8 | All use cases | Denial of service attacks SHOULD be addressed | 1.0 |

**Table 2: High-Level Functional Requirements – Security Items**

### 6.1.2 Content

| Requirement number | Related Use-case | Requirement | Enabler Release |
|---|---|---|---|
| REQ-CONT-1 | <Enhanced card issuer's services Interface> | It SHALL be possible to serve xHTML content from the SCWS | 1.0 |
| REQ-CONT-2 | <Enhanced card issuer's services Interface> | It SHALL be possible to serve all the media content defined in WAPWAE specification from the SCWS | 1.0 |
| REQ-CONT-3 | <Enhanced card issuer's services Interface> | It SHALL be possible for the SCWS to allow browsing of smart card files if authorized by the smart card issuer | 1.0 |

| Requirement number | Related Use-case | Requirement | Enabler Release |
|---|---|---|---|
| REQ-CONT-4 | <Loading Application from the SCWS to the ME> | The SCWS SHALL allow the download of device applications | 1.0 |

**Table 3: High-Level Functional Requirements – Charging Items**

### 6.1.3 Administration and Configuration

| Requirement number | Related Use-case | Requirement | Enabler Release |
|---|---|---|---|
| REQ-ADM-1 | <Managing the smart card web server from a remote trusted application > | The smart card issuer or any 3rd party authorised by the smart card issuer SHALL be able to control what content and smart card applications can be accessed via the SCWS | 1.0 |

**Table 4: High-Level Functional Requirements – Administration and Configuration Items**

### 6.1.4 Usability

| Requirement number | Related Use-case | Requirement | Enabler Release |
|---|---|---|---|
| REQ-USB-1 | <Loading Application from the SCWS to the device> | It SHALL be possible to identify a resource in the SCWS using an URL | 1.0 |

**Table 5: High-Level Functional Requirements – Usability Items**

### 6.1.5 Interoperability

| Requirement number | Related Use-case | Requirement | Enabler Release |
|---|---|---|---|
| REQ-IOP-1 | All | The SCWS SHALL support URLs with a length of at least 1024 characters | 1.0 |
| REQ-IOP-2 | <managing the smart card web server> | The SCWS SHALL implement standardised commands to load web pages, or related resources, into the SCWS | 1.0 |

**Table 6: High-Level Functional Requirements – Interoperability Items**

### 6.1.6 Privacy

| Requirement number | Related Use-case | Requirement | Enabler Release |
|---|---|---|---|
| REQ-PRV-1 | <PIN protected pages in the SCWS> | The SCWS SHALL be able to protect access to user data with a user PIN code | 1.0 |

**Table 7: High-Level Functional Requirements – Privacy Items**

## 6.2 System Elements

The following section gives requirements on the communication mechanisms between the different system elements.

| | | |
|---|---|---|
| System Element Browser: | The device's web browser or applications that need to connect to the SCWS | |
| System Element Device: | See the definition section | |
| System Element Smart card: | See the definition section | |
| System Element SCWS: | Web server implemented in the smart card | |

**Table 8: System Elements**

### 6.2.1 System Element Browser

| Requirement number | | Requirement |
|---|---|---|
| REQ-BRW-1 | The browser SHALL be able to connect to the SCWS | |

**Table 9: Requirements for System Element Browser**

### 6.2.2 System Element Device

| Requirement number | | Requirement |
|---|---|---|
| REQ-DEV-1 | The device SHALL provide the interfaces to access the SCWS | |
| REQ-DEV-2 | The device SHOULD support the existing proactive command issued by the smart card to launch the device's web browser. | |

**Table 10: Requirements for System Element Device**

### 6.2.3 System Element Smart card

| Requirement number | | Requirement |
|---|---|---|
| REQ-SC-1 | The smart card SHALL provide the communication channel(s) to access the SCWS | |
| REQ-SC-2 | The smart card SHALL provide the needed resources to execute a SCWS, related applications and needed data storage | |

**Table 11: Requirements for System Element Smart card**

### 6.2.4 System Element SCWS

| Requirement number | | Requirement |
|---|---|---|
| REQ-SCWS-1 | It SHALL be possible to serve content from the SCWS using [HTTP/1.1] and [WP HTTP], or a sub-profiles of these protocols. | |
| REQ-SCWS-2 | It MAY be possible to serve content from the SCWS using [HTTPS] or [HTTP over TLS] | |

**Table 12: Requirements for System Element SCWS**

# 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 1.0 History

| Document Identifier | Date | Sections | Description |
|---|---|---|---|
| Draft Version OMA-RD_Smartcard_Web_Server-V0_2 | 17 Nov. 2004 | | Initial |
| Draft Version OMA-RD_Smartcard_Web_Server-V1_0 | 15 Mar 2005 | | Modifications to Functional, Security, Interoperability, Content and System Elements sections. Updates to the definitions and scenarios. |
| | 22 Jun 2005 | | Modifications to Functional, Security, Usabilty and Interoperability requirements after second RD review. |
| | 14 Jul 2005 | | Approved in third RD review |
| Candidate version OMA-RD_Smartcard_Web_Server-V1_0 | 06 Sep 2005 | | Status changed to Candidate by TP<br>TP ref # OMA-TP-2005-0265-SCWS-RD-for-Approval |
| Draft version OMA-RD_Smartcard_Web_Server-V1_0 | 10 May 2006 | 6.1.1 | Candidate version demoted to Draft status.<br>One Class 1 CR incorporated: OMA-SCT-2006-0054R03. |
| Candidate version OMA-RD_Smartcard_Web_Server-V1_0 | 06 Jun 2006 | all | Status changed to Candidate by TP<br>TP ref # OMA-TP-2006-0198R01-OMA-RD-Smartcard_Web_Server-V1_0_for_re-approval_as_Candidate |
| Approved version OMA-RD_Smartcard_Web_Server-V1_0 | 21 Apr 2008 | All | Status changed to Candidate by TP<br>TP ref # OMA-TP-2008-0139-INP_SCWS_V1_0_ERP_and_IOP_Report_for_Final_Approval |