Enabler Release Definition for Application Layer Security Common Functions

Candidate Version 1.1 – 30 Mar 2010

Open Mobile Alliance

OMA-ERELD-SEC_CF-V1_1-20100330-C

Contents

Tables

1. Scope

The scope of this document is limited to the Enabler Release Definition of Application Layer Security Common Functions (SEC_CF) according to OMA Release process and the Enabler Release specification baseline listed in section **Error! Reference source not found.**.

2. References

2.1 Normative References

[RFC793] "Transmission Control Protocol", IETF, RFC 793, J. Postel, September 1981, URL:http://www.ietf.org/rfc/rfc793.txt

[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/

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/

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

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.

3.3 Abbreviations

ERDEF	Enabler Requirement Definition
ERELD	Enabler Release Definition
GBA	Generic Bootstrapping Architecture
KMC	Key Management Center
OMA	Open Mobile Alliance
OSG	OMA Security Gateway
SEC_CF	Security Common Functions
TCP	Transmission Control Protocol
TLS	Transport Layer Security

4. Release Version Overview

Security Common Functions (SEC_CF) aims at providing a common security architecture for OMA Enablers. The common security architecture provides a common way to implement security functionality for OMA Enablers in a flexible way and it is adaptable to the requirements of different enabler deployment scenarios. Ultimately, it should be possible for all types of OMA enablers to use this architecture to provide security.

4.1 Version 1.0 Functionality

This version of the SEC_CF aims to provide security functionality for OMA Enablers that are based on a Client-Server operational model and operate over TCP [RFC793] as the transport protocol.

A Client-Server operational model in the SEC_CF context requires a functional entity denoted Security Agent (SECA), requesting services from an application server. Security Agents are generally implemented on a mobile terminal whereas the application server is likely to be the part of an OMA Enabler such as location servers, charging elements, etc. that resides in a fixed network.

SEC_CF defines another functional entity, OMA security gateway (OSG), which can be integrated into other entities (e.g. mobile terminal, application server, etc) of the OMA Enabler architecture to provide security services to resources that are connected to it. The OSG MAY provide DoS protection. As an implementation option, the functional entity Key Management Center (KMC) is introduced to provide key management support to the OSG (in Home or Visited domains) and key management to the Security Agent. KMC can also be integrated into the OSG.

The interfaces defined between SEC_CF functional entities can be implemented using industry standard security protocols. In some cases SEC_CF functional entities might be integrated into the enablers own functional entities to avoid creating new interfaces and simplify the solution.

SEC_CF defines several security functions such as authentication, confidentiality protection and integrity protection to be re-used by other OMA enablers. Security considerations for each security function are detailed in the relevant SEC_CF technical specifications. The SEC_CF architecture also permits various deployment models to reflect the current established deployment models (Home domain only, visited domain, etc) of service providers.

In a summary, OMA SEC_CF 1.0 Enabler supports for the following functionality.

- Support for OMA Enablers that are based on a Client-Server operational model
- Support for OMA Enablers over TCP protocol
- GBA Profile
- TLS/PSK-TLS Profile
- SEC-CERT Management Object (MO)

4.2 Version 1.1 Functionality

OMA SEC_CF 1.1 Enabler supports for the following additional functionality.

- Support for OMA Push services
- Support for OMA Enablers over SIP protocol
- Support for OMA Enablers over UDP protocol
- Support for Delegated Authentication for Web Services
- DTLS profile
- GBA Push profile
- IPSec profile

5. Document Listing for SEC_CF

This section is normative.

Doc Ref	Permanent Document Reference	Description
Requirement Document		
[SEC_CF_RD]	OMA-RD-SEC_CF-V1_1-20091208-C	Requirement Document for SEC_CF Enabler
Architecture Document		
[SEC_CF_AD]	OMA-AD-SEC_CF-V1_1-20100330- C	Architecture Document for SEC_CF Enabler
Technical Specifications		
[TLS_Profile]	OMA-TS-TLS_Profile-V1_1-20100203-D	Specification that defines an OMA profile of TLS, DTLS and related IETF specifications. The profling amounts to stating which features, in referenced specifications, that must or should be supported.
[GBA_Profile]	OMA-TS-GBA_Profile-V1_0-20091225-D	Specification that defines an OMA profile of GBA, as defined by 3GPP and 3GPP2. GBA specifies how operator controlled smart cards can be used to bootstrap a short term security association between a client and a server. The profling amounts to stating which features, in referenced specifications, that must or should be supported.
[IPSec_Profile]	OMA-TS-IPSec_Profile-V1_1-20091225-D	Specification that defines an OMA profile of IPSec and related IETF specifications. The profling amounts to stating which features, in referenced specifications, that must or should be supported.
Supporting Files		
[SEC_CERT_MO]	OMA-DDS-SEC_CERT_MO-V1_0-20080902-A	Using the OMA DM protocol and its data formats, this data definition specification defines Management Objects required for management of security properties (SEC CERT MOs). To be used as one option to initialize a device in context of the SEC_CF enabler, or in other contexts.
[SEC_CERT_DDF]	OMA-SUP-MO_SEC_CERT-V1_0-20080902-A	DDF for the MO in [SEC_CERT_MO]. Working file in Schema directory: file: SEC_CERT_MO-v1_0.ddf path: http://www.openmobilealliance.org/tech/omna/dm-mo/

Table 1: Listing of Documents in SEC_CF Enabler

6. OMNA Considerations

<< This section is to be used to describe any OMNA items included in the release. This would include, among others:

- Usage of OMA-based Uniform Resource Names (URNs) (including those used as namespace identifiers in Schemas)
- AppiDs for Application Characteristics (AC)
- Managed Object (MO) information for the MO registry
- ISO Object IDs
- PUSH Application Ids
- WAP Wireless Session Protocol (WSP) Content Types
- Presence <service-description> assignments
- Uniform Resource Identifier (URI)-List Registered Usage Names (for XDM)

The format of this section will be left up to the release owners to account for the particular needs they may run into. It should be clear from the written material, though, as to the set of OMNA items needed.

If a new OMNA registry is needed to support the release – clearly this should have been worked with the REL Committee before submitting a Release Document. Failure to do so may result in delays as the required tables are worked up and made publicly available. Another risk is that the table desired is not supported by OMNA (is not a registry type table) and the group will need to re-think how they intend to resolve their needs.

Through the normal development process the OMNA entries or support registries should be accommodated. This should not be trigger to remove the linkage from this section. Thus, if an entry is added to OMNA after the initial Candidate version described the need – the material should stay in this section. It may be useful in subsequent releases to add some text to indicate that the needed items have been accommodated (e.g. add a comment regarding its availability or support as appropriate).

If the release has absolutely no OMNA items to be accommodated – then it should indicate that explicitly with a short description (e.g. this release does not have any OMNA items for handling). This determination probably can not be made until the end of the development phases and editors are encouraged to keep this advisory in place until the Consistency Review.

DELETE THIS COMMENT >>

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 SEC_CF - Client Requirements

This section is normative.

Item	Feature / Application	Requirement
OMA-ERDEF-SEC_CF-C-001-<<M/O>>	SEC_CF Client	

Table 2: ERDEF for SEC_CF Client-side Requirements

9. ERDEF for SEC_CF - Server Requirements

This section is normative.

Item	Feature / Application	Requirement
OMA-ERDEF-SEC_CF-S-001-<<M/O>>	SEC_CF Server	

Table 3: ERDEF for SEC_CF Server-side Requirements

Appendix A. Change History (Informative)

A.1 Approved Version 1.0 History

Reference	Date	Description
Approved versions: OMA-ERELD-SEC_CF-V1_0	02 Sep 2008	Status changed to Approved by TP OMA-TP-2008-0321-INP_SEC_CF_V1_0_ERP_for_Final_Approval

A.2 Draft/Candidate Version 1.1 History

Document Identifier	Date	Sections	Description
Draft Versions: OMA-ERELD-SEC_CF-V1_1	07 Sep 2009	All	Initial baseline for RD review
	21 Oct 2009	2.2, 4.2, 5	To incorporate agreed CRs which address comments from RD formal review
	04 Nov 2009	5, A.2	Editorial corrections: Styles Document Listing Contents with tables Removal of empty App B
Candidate Version: OMA-ERELD-SEC_CF-V1_1	08 Dec 2009	All	Status changed to Candidate by TP: OMA-TP-2009-0543-INP_SEC_CF_V1_1_RD_for_Candidate_Approval
Draft Version: OMA-ERELD-SEC_CF-V1_1	06 Jan 2010	All	Editorial changes: 2010 template Document listing updated
	08 Jan 2010	5	Document listing updated
	09 Mar 2010	5	Document listing updated
Candidate Version: OMA-ERELD-SEC_CF-V1_1	30 Mar 2010	All	Status changed to Candidate by TP: OMA-TP-2010-0127-INP_SEC_CF_V1_1_AD_for_Candidate_approval