Enabler Release Definition for Application Layer Security Common Functions

Approved Version 1.1 – 31 Jul 2012

Open Mobile Alliance

OMA-ERELD-SEC_CF-V1_1-20120731-A

Use of this document is subject to all of the terms and conditions of the Use Agreement located at
http://www.openmobilealliance.org/UseAgreement.html.

Unless this document is clearly designated as an approved specification, this document is a work in process, is not an approved Open Mobile Alliance™ specification, and is subject to revision or removal without notice.

You may use this document or any part of the document for internal or educational purposes only, provided you do not modify, edit or take out of context the information in this document in any manner. Information contained in this document may be used, at your sole risk, for any purposes. You may not use this document in any other manner without the prior written permission of the Open Mobile Alliance. The Open Mobile Alliance authorizes you to copy this document, provided that you retain all copyright and other proprietary notices contained in the original materials on any copies of the materials and that you comply strictly with these terms. This copyright permission does not constitute an endorsement of the products or services. The Open Mobile Alliance assumes no responsibility for errors or omissions in this document.

Each Open Mobile Alliance member has agreed to use reasonable endeavors to inform the Open Mobile Alliance in a timely manner of Essential IPR as it becomes aware that the Essential IPR is related to the prepared or published specification. However, the members do not have an obligation to conduct IPR searches. The declared Essential IPR is publicly available to members and non-members of the Open Mobile Alliance and may be found on the "OMA IPR Declarations" list at http://www.openmobilealliance.org/ipr.html. The Open Mobile Alliance has not conducted an independent IPR review of this document and the information contained herein, and makes no representations or warranties regarding third party IPR, including without limitation patents, copyrights or trade secret rights. This document may contain inventions for which you must obtain licenses from third parties before making, using or selling the inventions. Defined terms above are set forth in the schedule to the Open Mobile Alliance Application Form.

NO REPRESENTATIONS OR WARRANTIES (WHETHER EXPRESS OR IMPLIED) ARE MADE BY THE OPEN MOBILE ALLIANCE OR ANY OPEN MOBILE ALLIANCE MEMBER OR ITS AFFILIATES REGARDING ANY OF THE IPR'S REPRESENTED ON THE "OMA IPR DECLARATIONS" LIST, INCLUDING, BUT NOT LIMITED TO THE ACCURACY, COMPLETENESS, VALIDITY OR RELEVANCE OF THE INFORMATION OR WHETHER OR NOT SUCH RIGHTS ARE ESSENTIAL OR NON-ESSENTIAL.

THE OPEN MOBILE ALLIANCE IS NOT LIABLE FOR AND HEREBY DISCLAIMS ANY DIRECT, INDIRECT, PUNITIVE, SPECIAL, INCIDENTAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES ARISING OUT OF OR IN CONNECTION WITH THE USE OF DOCUMENTS AND THE INFORMATION CONTAINED IN THE DOCUMENTS.

© 2012 Open Mobile Alliance Ltd. All Rights Reserved.
Used with the permission of the Open Mobile Alliance Ltd. under the terms set forth above.

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 5.

2. References

2.1 Normative References

[OMNA]	"Open Mobile Naming Authority", URL: http://www.openmobilealliance.org/Tech/OMNA.aspx
[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 2.8, Open Mobile Alliance™, OMA-ORG-Dictionary-V2_8, 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
IPsec	IP Security
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

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_1-20120731-A	Requirement Document for SEC_CF Enabler
Architecture Document		
[SEC_CF_AD]	OMA-AD-SEC_CF-V1_1-20120731-A	Architecture Document for SEC_CF Enabler
Technical Specifications		
[TLS_Profile]	OMA-TS-TLS_Profile-V1_1-20120731-A	Specification that defines an OMA profile of TLS, DTLS and related IETF specifications. The profiling amounts to stating which features, in referenced specifications, that must or should be supported.
[GBA_Profile]	OMA-TS-GBA_Profile-V1_1-20120731-A	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 profiling amounts to stating which features, in referenced specifications, that must or should be supported.
[IPsec_Profile]	OMA-TS-IPSec_Profile-V1_1-20120731-A	Specification that defines an OMA profile of IPsec and related IETF specifications. The profiling amounts to stating which features, in referenced specifications, that must or should be supported.
[Delegated_Authn_Profile]	OMA-TS-Delegated_Authentication_Profile-V1_1-20120731-A	Specificaton that defines an OMA profile of existing mechanisms related to delegated authentication for web service to provide SSO experience for users during accessing web services as well as to allow users to control their public identifiers on the web.
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/
[SEC_CF_GBA_XSD]	OMA-SUP-XSD_seccf_gba-V1_1-20120731-A	XML Schema for GBA in OMA Security Common Functions (SEC_CF) Working file in Schema directory: file: seccf_gba-v1_1.xsd path: http://www.openmobilealliance.org/tech/profiles/

Table 1: Listing of Documents in SEC_CF Enabler

6. OMNA Considerations

6.1 Namespace

The SEC CF enabler introduces the following namespace in the "seccf" domain.

Note that in order to maintain compatibility between minor versions of the same major version, only the major version is reflected in the namespace identifier. Further note that subsequent minor versions of the same XML schema (e.g. 1.2) will be registered against the same namespace identifier.

Description	Registered URN	Schema Links
GBA profile	urn:oma:xml:seccf:gba:1	http://www.openmobilealliance.org/tech/profiles/seccf_gba-v1_1.xsd

6.2 GBA Protocol Identifier

SEC CF declares the following GBA Protocol Identifier registered in [OMNA].

Protocol Description	Octet String	Specification References	OMA Enabler Usage
SIP Digest	0x03, 0x00, 0x00, 0x00, 0x03	SIP RFC3261	SEC CF V1.1

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	SEC_CF Client	[TLS]: MCF
OMA-ERDEF-SEC_CF-C-002-O	SEC_CF Client	[GBA_Profile]: OCF
OMA-ERDEF-SEC_CF-C-003-O	SEC_CF Client	[SEC_CERT_MO]: OCF
OMA-ERDEF-SEC_CF-C-004-O	SEC_CF Client	[Ipsec_Profile]: OCF
OMA-ERDEF-SEC_CF-C-005-O	SEC_CF Client	[Delegated_Authn_Profile]: OCF

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	SEC_CF Server	[TLS]: MSF
OMA-ERDEF-SEC_CF-S-002-O	SEC_CF Server	[GBA_Profile]: OSF
OMA-ERDEF-SEC_CF-S-003-O	SEC_CF Server	[SEC_CERT_MO]: OSF
OMA-ERDEF-SEC_CF-S-004-O	SEC_CF Server	[Ipsec_Profile]: OSF
OMA-ERDEF-SEC_CF-S-005-O	SEC_CF Server	[Delegated_Authn_Profile]: OSF

Table 3: ERDEF for SEC_CF Server-side Requirements

Appendix A.   Change History   (Informative)

A.1   Approved Version 1.0 History

Reference	Date	Description
OMA-ERELD-SEC_CF-V1_0-20080902-A	02 Sep 2008	Status changed to Approved by TP OMA-TP-2008-0321-INP_SEC_CF_V1_0_ERP_for_Final_Approval
OMA-ERELD-SEC_CF-V1_1-20120731-A	31 Jul 2012	Status changed to Approved by TP Ref TP Doc# OMA-TP-2012-0291-INP_SEC_CF_V1_1_for_Final_Approval