Security Common Functions Architecture

Candidate Version 1.0 – 06 May 2008

Open Mobile Alliance

OMA-AD-SEC_CF-V1_0-20080506-C

Contents

Figures

1. Scope (Informative)

Common Security Functions Architecture provides common security architecture for OMA Enablers. SEC_CF also describes a common way to implement security functionality for OMA Enablers and provides various architectures for different enabler deployment scenarios. Ultimately, it should be possible for all types of OMA enablers to use this architecture to provide security.

SEC_CF will be accompanied with several Technical Specifications (TS). This specification (Architecture Document) intends to describe the high level architecture of the SEC_CF and provide architecture guidance for different enabler deployment options. Details of the security implementations will be provided in separate technical specifications. The list of the technical specifications can be found in this document.

2. References

2.1 Normative References

[GBA] 3GPP TS 33.220 "3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Generic Authentication Architecture (GAA); Generic bootstrapping architecture", URL: http://www.3gpp.org/ftp/Specs/html-info/33220.htm

[GBA2] 3GPP2 S.S0109-0 "Generic Boostrapping Architecture (GBA) Framework", Version 1.0, 3rd Generation Partnership Project 2 (3GPP2), April 2006, URL: http://www.3gpp2.org/

[OMA-TS-GBA] "OMA GBA profile", Version 1.0, Open Mobile Alliance™, OMA-TS-GBA_Profile-V1_0, URL: http://www.openmobilealliance.org/

[OMA-SEC-CERT_MO] "OMA SEC-CERT Management Objects ", Open Mobile Alliance™, OMA-DDS-SEC_CERT_MO-V1URL: http://www.openmobilealliance.org/

[OMA-TS-TLS] "OMA TLS Profile", Version 1.0, Open Mobile Alliance™, OMA-TS-TLS-V1_0, URL: http://www.openmobilealliance.org/

[OSE] "OMA Service Environment", Version 1.0, Open Mobile Alliance™, OMA-RRP-OSE-V1_0, URL: http://www.openmobilealliance.org/

[RFC2119] IETF, RFC 2119, "Key words for use in RFCs to Indicate Requirement Levels", S. Bradner, March 1997, URL: http://www.ietf.org/rfc/rfc2119.txt

[RFC2406] IETF, RFC 2406, "IP Encapsulating Security Payload (ESP) ", S. Kent, R. Atkinson, November 1998, URL: http://www.ietf.org/rfc/rfc2406.txt

[RFC2617] IETF, RFC2617, "HTTP Authentication: Basic and Digest Access Authentication", Franks J., et al, June 1999, URL: http://www.ietf.org/rfc/rfc2617.txt

[RFC4279] IETF, RFC 4279, "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)", P. Eronen, H. Tschofenig, December 2005, URL: http://www.ietf.org/rfc/rfc4279.txt

[RFC4301] IETF, RFC 4301, "Security Architecture for the Internet Protocol", S. Kent, K. Seo, December 2005, URL: http://www.ietf.org/rfc/rfc2401.txt

[RFC4346] IETF, RFC 4346, "Transport Layer Security (TLS) Version 1.1", T. Dierks, et al, Apr 2006, URL: http://www.ietf.org/rfc/rfc4346.txt

[SEC_CF-RD] "Security Common Functions Requirements", Open Mobile Alliance™, OMA-RD-SEC_CF-V1_0, URL: http://www.openmobilealliance.org/

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

2.2 Informative References

[ARCH-PRINC] "OMA Architecture Principles", URL: http://www.openmobilealliance.org/

[ARCH-REVIEW] "OMA Architecture Review Process", URL: http://www.openmobilealliance.org/

[OMA-DICT] "OMA Dictionary", 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 [**Error! Reference source not found.**].

All sections and appendixes, except “Scope” and “Introduction”, are normative, unless they are explicitly indicated to be informative.

3.2 Definitions

Communication channel A communication channel is the mean by which two entities can exchange messages.

SEC_CF Domain A set of entities for which a common party is responsible for the security functionality.

3.3 Abbreviations

OMA Open Mobile Alliance

SEC_CF Security Common Functions

TCP Transmission Control Protocol

4. Introduction (Informative)

Security Common Functions Architecture aims to provide a common set of security mechanisms with their possible deployment options that can be re-used by OMA Enablers. The rationale behind this specification is to avoid, where possible, duplication of security effort for each OMA Enabler that requires security functionality. SEC_CF offers to re-use both the architectural entities (e.g. Security Gateways, etc) and security specifications (e.g. protocol profiles) when developing new OMA enablers.

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 [TCP] as the transport protocol. A Client-Server operational model in the SEC_CF context requires a Security Agent (e.g. implemented in the Mobile Terminal) requesting services from an application server. Security Agents are generally implemented on a mobile terminal and an 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 functional entities such as security gateways and key management centres that can be integrated into the functional entities (e.g. mobile terminal, application server, etc) of the OMA Enabler architecture in order to provide security services. SEC_CF also permits various deployment models to reflect the current established deployment models (Home domain only, visited domain, etc) of service providers. SEC_CF defines several interfaces between its functional entities that 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.

A successful use of the SEC_CF by other OMA enablers requires an analysis of the security requirements to map the most appropriate SEC_CF options. In most cases SEC_CF cannot be used as a security add-on after the completion of the enabler specification. The development process of the enabler should consider SEC_CF integration as early as possible to avoid any possible architectural inconsistencies.

In this context domain refers to SEC_CF domain, as defined in 3.2.

4.1 Security Considerations

This enabler defines several security features 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.

5. Architectural Model

SEC_CF consists of architectural elements and interfaces between these elements. Detailed specifications of the architecture can be found in sections 5.3 of this document. This section only provides a general overview. Figure 1 illustrates the architectural elements and related interfaces defined for SEC_CF.

Current version of SEC_CF defines the following architectural elements to operate:

- **Security Agent (SECA):** This element is the entity through which an application or a user interacts with a requesting resource. In the case of a user this may be done through a user interface (UI). A Security Agent may be implemented in a Mobile Terminal which may include a removable security token such as a (U)SIM/R-UIM. However, SEC_CF also supports Security Agents that are implemented in application servers without a removable security token. Generally in the SEC_CF the SECA acts on behalf of the user and all identifiers in the SECA are bound to the user (subscriber) identities. Device identifiers for Mobile Terminals are not used within the security context of this version of the SEC_CF.

- **OMA Security Gateway (OSG):** This element provides security services such as authentication, encryption and integrity protection for any requesting resource that makes use of the SEC_CF. OSG can be integrated into the resource utilising SEC_CF or it can deployed as a separate entity that can provide services to a number of resources that can be reached via an OSG.

The following interfaces are defined between the architectural elements in the SEC_CF:

- **SEC-1:** This interface connects a SECA to an OSG. Currently SEC_CF only supports TCP as the transport protocol for SEC-1. If a requesting resource selects an application specific protocol to be implemented over TCP in a Client-Server model, then that protocol can be secured using the security mechanisms implemented by **SEC-1.** Security services for this interface are implemented at the transport and application layers. Security functionality of this interface is defined in section 5.3.2.1 of this document.

- **SEC-2:** This interface securely connects an OSG to another OSG. This interface can be used for distributed enabler deployments where the SECA connects to a requesting resource in a visited domain via the home OSG. Security functionality of this interface is defined in section 5.3.2.2 of this document.

- **SEC-3:** This is an I0 interface that connects an OSG to a requesting resource in cases where the OSG is not fully integrated into the requesting resource. Its definition is out of the scope of the work item as each requesting resource can implement SEC-3 based on the enabler specific protocols. The specific protocol realizations for this interface are out of scope.

5.1 Dependencies

SEC_CF architecture relies on several IETFspecifications. The lists of dependencies are as follows:

- IETF TLS (Transport Layer Security) [RFC4346]

- IETF PSK-TLS (Pre-Shared Key Ciphersuites for Transport Layer Security) [RFC4279]

- IETF HTTP Digest Authentication [RFC2617]

- IETF IPSec (Internet Security Architecture) [RFC4301]

5.2 Architectural Diagram

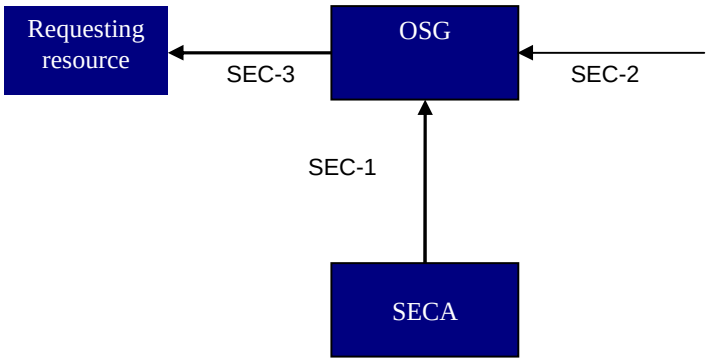

Figure 1: Overview of the SEC_CF Architecture

5.3 Functional Components and Interfaces

Details of the architectural elements and interfaces of SEC_CF can be found in this section.

5.3.1 Functional Elements

5.3.1.1 Security Agent (SECA)

Security Agents is an entity that implements the SEC_CF security functionality. It interfaces with the OSG.

Security Agent provides the following functionality:

- Interfaces with the removable security tokens such as (U)SIM in 3GPP deployments. It MAY interface with R-UIM in 3GPP2 deployments.
- Provides unique identities.
- Uses the necessary key material to perform security services.
- Handles security credentials such as key materials to be used for SEC_CF operations.
- Performs the following security services: Authentication, Confidentiality and Integrity Protection. And MAY provide Denial of Service (DoS) protection.
- It can communicate either with Home or visited OSG.

5.3.1.2 OMA Security Gateway (OSG)

OMA Security Gateway provides the following functionality:

- Provides all the security services defined in the SEC_CF (Authentication, Authorization, Confidentiality and Integrity Protection, Replay Protection) to resources that are connected to it. It MAY provide DoS protection.

5.3.2 Interfaces

5.3.2.1 SEC-1

This interface MUST at least support TLS for transport layer security to provide authentication of the OSG to the SECA. If HTTP is used, HTTP Digest MUST also be used to provide authentication of the SECA to the OSG. If HTTP is not used as transport protocol for this interface, then PSK-TLS and/or client certificates MUST be supported in order to provide mutual authentication between the OSG and SECA in the transport layer.

5.3.2.2 SEC-2

This interface MUST at least support TLS [RFC 4346] and SHOULD also support IPSec [RFC4301] in tunnel mode with confidentiality [RFC 2406] and integrity protection [RFC2406].

5.3.2.3 SEC-3

This interface is not defined by SEC_CF.

Note: OSG initated secure triggers use cases are FFS.

5.3.2.4 Basic flow

The basic SECA initiated flow is indicated in **Error! Reference source not found.**. The first step is that that SECA initiates a setup of a TLS tunnel beetween itself and the OSG. For mutual authentication we have three cases: 1) A shared key is used together with PSK-TLS. 2) The server is authenticated via a server certificate and the SECA via HTTP Digest and 3) The server and the client both use ceretificates for authentication.

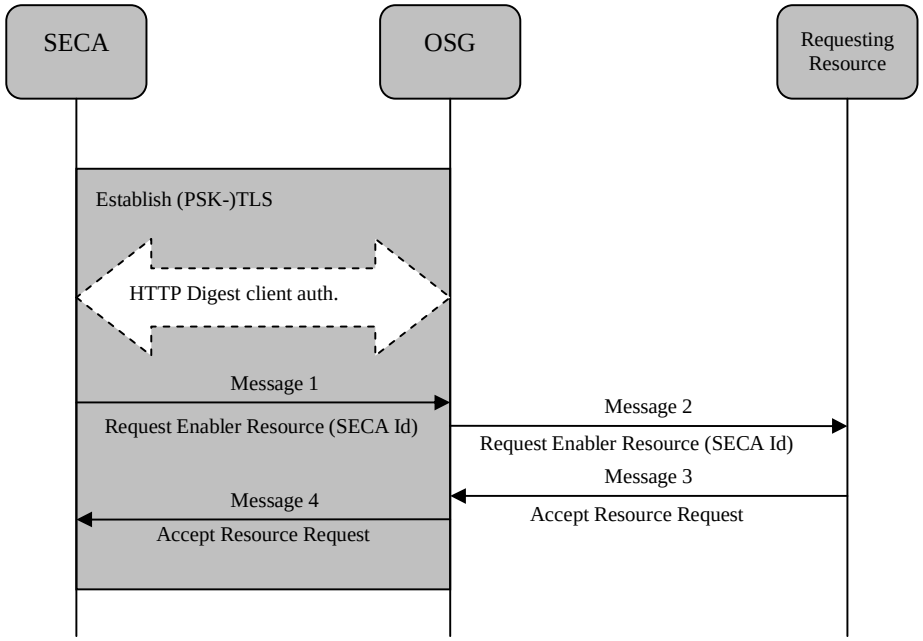

Figure 2: Basic call flow

6. SEC_CF Deployment Options (Informative)

This version of SEC_CF allows SECAs to securely access resources in the visited domains either via the Home OSGs or directly via the visited OSG. The particular deployment of SEC_CF may depend on the specific operational requirements of the OMA Enabler as well as the underlying the IP transport model.

For the following deployment scenarios some additional elements and interfaces are introduced (in addition to the architectural elements and interfaces defined in chapter 5):

Key Management Centre (KMC)

Key Management Centre provides the following functionality:

- Provides the key management support to the OSG (Home and Visited).
- Provides key management to the SECA

KMC can also be integrated into the OSG.

Note: in the case where KMC is not integrated into the OSG, the KMC could be based on the BSF as defined in [GBA][GBA2].

KMC-IF

This interface connects an OSG to a KMC. The interface is not defined by SEC_CF.

Note: For 3GPP based implementations this interface corresponds to the Zn interface defined in Generic Bootstapping Architecutre [GBA] defined in 3GPP specifications.

6.1.1 SEC_CF Direct OSG Access

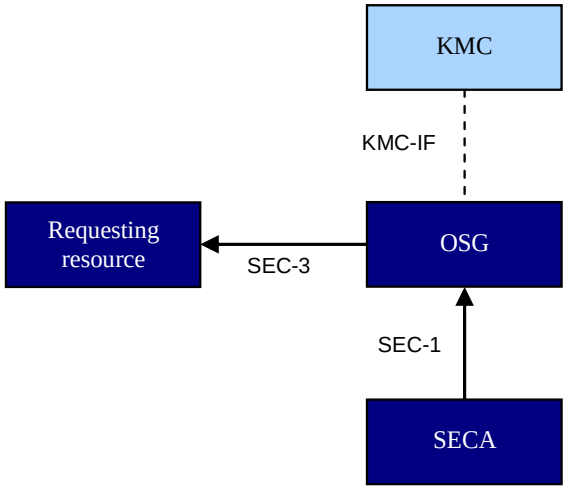

Figure 3: SEC_CF Home Domain Deployment

In the cases where GBA is used for key management SECA will also have additional interfaces to the KMC (BSF in GBA). This interface is defined in 3GPP specifications and it is outside the scope of SEC_CF.

When the SEC-1 interface is GBA-based, a Ua security protocol identifier is needed. For more information see the corresponding section in [OMA-TS-GBA].

6.1.2 SEC_CF Proxy OSG Access

For SEC_CF deployment based on GBA, only "Proxy Mode" is feasible. The home OSG will act as a proxy for the OMA enabler in the visited domain. Home OSG MUST provide a secure connection over the SEC-2 between the home and the visited OSG.

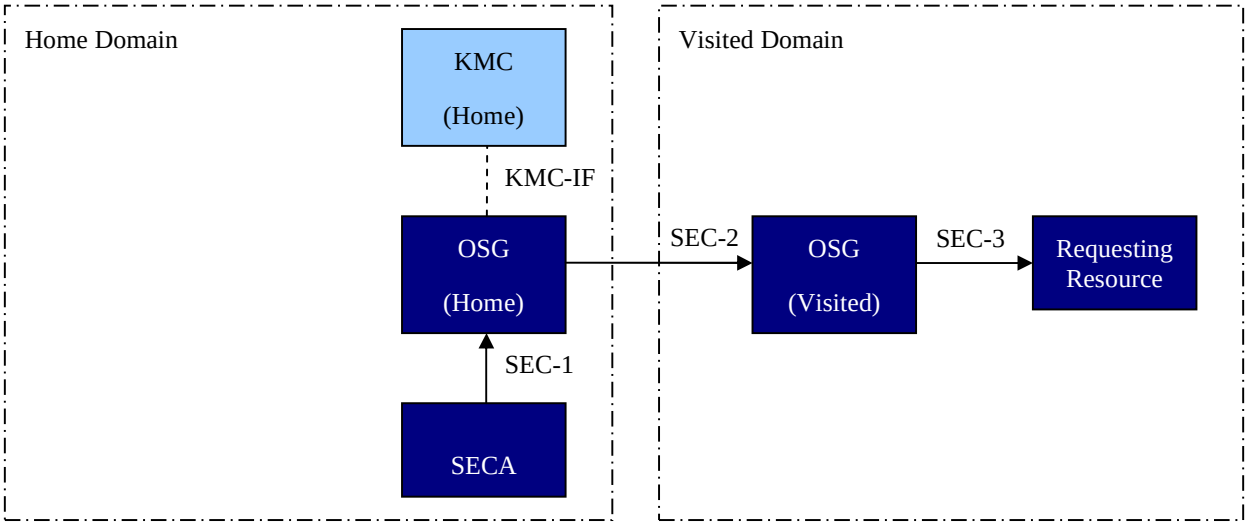

Figure 4: GBA deployment for SEC_CF roaming domain architecture

6.2 Enabler Protocol Requirements

Following requirements are defined for any OMA Enabler deployments that implement this version of the SEC_CF to secure its operations.

- The Enabler protocol MUST be based on the TCP protocol
- The Enabler protocol MUST operate in a Client-Server model.

6.3 Flows

6.3.1 Establishing a secure communication channel using SEC_CF

6.3.1.1 SECA initiated SEC_CF usage

The basic SECA initiated flow is indicated in **Error! Reference source not found.**. The first step is that that SECA initiates a setup of a TLS tunnel beetween itself and the OSG. For mutual authentication we have three cases: 1) A shared key is used together with PSK-TLS. 2) The server is authenticated via a server certificate and the SECA via HTTP Digest and 3) The server and the client both use certificates for authentication. In cases 1) and 2) The OSG requests the credentials to be used from the KMC in Message 1 and receives them in Message 2.

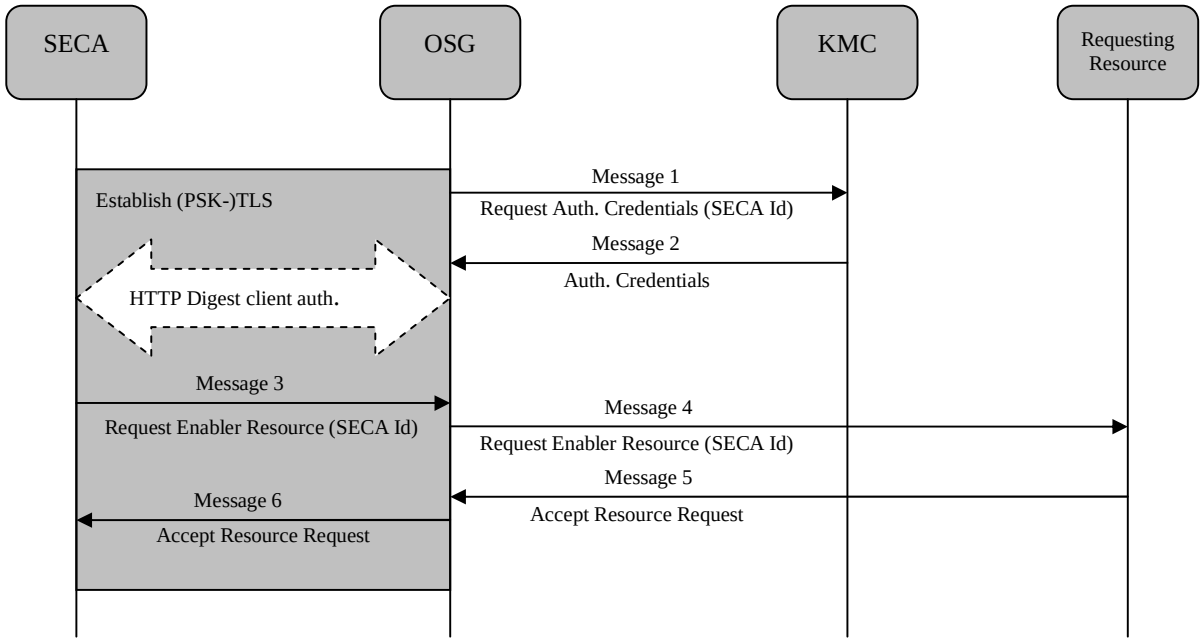

Figure 5: SECA initated call flow

6.4 Related Specifications

Further Details of SEC_CF are defined in the following specifications.

- SEC_CF TS OMA TLS Profile [OMA-TS-TLS]
- SEC_CF TS OMA GBA Profile [OMA-TS-GBA]
- SEC_CF DDS OMA SEC-CERTManagement Objects (MO) [OMA-SEC-CERT-MO]

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
First incomplete version	05 Jul 2005		Document creation.
Draft Versions: OMA-AD-SEC_CF-V1_0	23 Aug 2005	All sections	First draft version of the AD
	22 Aug 2006	All sections	Usage of the new template and several section updates.
	04 Oct2006	Contents, Figures, Section 5.	Updates to the figures and interface descriptions.
	13 Feb 2007	All sections	Applied changes according to ADRR resolved comments
	15 May 2007	All sections	Applied changes according to the comments received on the second round of AD review.
	12 Jun 2007	All sections	Applied changes according to the input received during the SEC face-to-face meeting.
	26 Jun 2007	All sections	Applied changes according to the input received during the SEC-ARC face-to-face meeting.
	08 Aug 2007	All sections	Applied changes according to the input received during the SEC-ARC conference calls and email discussions.
	12 Dec 2007	All	Editorial clean-up of formatting and styles prior to consistency review.
	01 Apr 2008	All	Incorporated Agreed CR: OMA-SEC-2008-0029R01-CR_SEC_CF_AD_editorial
	02 Apr 2008	Section 6	Incorporated Agreed CR: OMA-SEC-2008-0042R01-CR_SEC_CF_AD_Technical
Candidate Versions: OMA-AD-SEC_CF-V1_0	06 May 2008	All	Status changed to Candidate by TP TP ref# OMA-TP-2008-0173-INP_SEC_CF_V1_0_ERP_for_Candidate_Approval