Enabler Release Definition for On-board Key Generation

Candidate Version 1.0 – 21 Dec 2005

Open Mobile Alliance

OMA-ERELD-OBKG-V1_0-20051221-C

Contents

Tables

1. Scope

The scope of this document is limited to the Enabler Release Definition of On-Board Key Generation according to OMA Release process and the Enabler Release specification baseline listed in section 5.

2. References

2.1 Normative References

[IOPPROC] "OMA Interoperability Policy and Process", Version 1.1, Open Mobile Alliance™, OMA-IOP-Process-V1_1, 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

[OBKG RD] "On-board Key Generation and Key Enrollment Requirements", OMA-RD-OBKG-V1_0, URL: http://www.openmobilealliance.org/

[ESMPCrypto] "ECMA Script Crypto Library", Open Mobile Alliance™ , OMA-WAP-ECMACR-V1_1, URL:http://www.openmobilealliance.org/

[WIM] "Wireless Identity Module Part: Security", Open Mobile Alliance™, OMA-TS-WAP-WIM-V1_2, URL:http://www.openmobilealliance.org/

[WPKI] "Wireless Application Protocol Public Key Infrastructure Definition", Open Mobile Alliance™, OMA-WAP-WPKI-V1_1, URL:http://www.openmobilealliance.org/

2.2 Informative References

[OBKG ETR] "Enabler Test Requirements for OBKG", Open Mobile Alliance™ , OMA-ETR-OBKG-V1_0, 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” and “Introduction”, 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 [IOPPROC].

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

ECMA	European Computer Manufacturer Association
ERDEF	Enabler Requirement Definition
ERELD	Enabler Release Definition
GKA	Generate Key Assurance
ICC	Integrated Circuit Card
KEYGEN	Key Generation
OBKG	On Board Key Generation
OMA	Open Mobile Alliance
RKE	Remote Key Enrolment
ME	Mobile Equipment
PKI	Public Key Infrastructure
SE	Security Element
WAP	Wireless Application Protocol
WIM	Wireless Identity Module

4. Introduction

This document outlines the Enabler Release Definition for "On-Board Key Generation and Remote Key Enrolment" and the respective conformance requirements for clients, smartcards, and servers claiming compliance to it as defined by Open Mobile Alliance across the specification baseline.

This enabler aims to introduce on-board key generation and remote key enrolment functionality by defining additional ECMA Scripts and functions in the WIM. It will enable, first, a remote invocation of on-board key generation in the WIM and, second, remote key enrolment for getting (new) user certificates. Both functions are implemented as ECMA scripts that are embedded in an xHTML page.

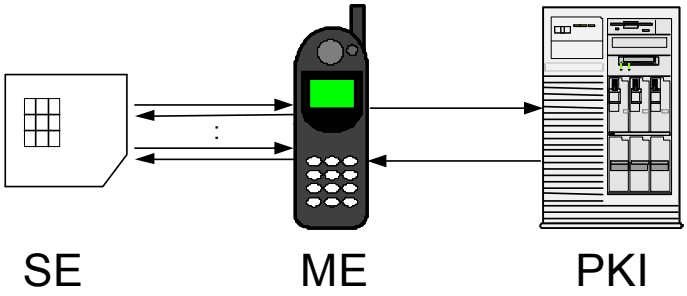
These features answer a requirement for on-board key generation mainly due to the sensitivity of the non-repudiation key pairs. In some legal contexts this requirement is also considered mandatory. Key enrolment functionality is important in order to enable an over the air enrolment of existing, or newly generated keys, and getting new certificates for these keys.

The definition of the ECMA Script crypto functions and the WIM functions allow for the implementation of a mobile PKI model that is more closely aligned with the model currently in wide spread use in wired clients. The use of well known and broadly supported Internet standards allows one to build a Wireless PKI based on existing Public Key Infrastructure.

4.1 Architecture

The architecture is the one defined in [WPKI], with no addition of entity or interface.

The following picture summarizes the three entities and their roles in the on-board key generation and registration process.



The PKI is responsible for issuing certificates and can initiate key generation and certificate enrollment requests. Key generation may occur only once, while a key may be enrolled into multiple PKI

In this model the mobile entity, or device, is responsible for interpreting and acting upon the commands it will receive from a PKI. Mainly this involves the proper generation, signing and formatting of the response that may be required. It also interacts with the SE for cryptographic operations.

The SE will perform, in addition to standard cryptographic functionality operations, the secure generation of new keys inside the SE (KEY GEN) and the signature generation (GKA) providing Proof of Possession and thereby assurance that the was generated by a genuine SE.

4.2 Example Use Case

4.2.1 Use case 1: Deploying Public Key product

The user owns a WIM-enabled mobile phone with a SIM/WIM (SE), issued by its Operator. At that time all SIM/WIM are alike, ie. not yet initialised with user's PKI credentials; Assuming the user wants to use its Operator's m-commerce services s/he asks its Operator to activate the service. The operator will then provide the user with the necessary information to remotely complete this activation with the OBKG services.

Benefits of OBKG for the Operator: facilitated smartcard management as cards are blank until the users configure them ; no need to pre-configure or pre-generate credentials.

4.2.2 Use case 2: Third party usage of PK product

The user owns a WIM enabled mobile phone with a SIM/WIM (SE), issued by its operator. The operator collaborates with a financial institute to provide m-banking services to the user. For this purpose the operator delegates some administrative rights to the financial institute. The financial institute can then apply its own registration policies to generate its own user credentials. The financial institute will provide the user with the necessary information to remotely enroll to the m-banking services.

Benefits of OBKG for the Operator and Third parties: Operators have means to share the PKI features of their cards and, while keeping control of their cards, can provide third parties with control on users' credentials.

5. Document Listing for OBKG V1.0

This section is normative.

Doc Ref	Permanent Document Reference	Description
Requirement Document		
[OBKG_RD]	OMA-RD-OBKG-V1_0-20050322-C	Requirement Document for OBKG Enabler
Architecture Document		
n/a		
Technical Specifications		
[ESMPCrypto]	OMA-WAP-ECMACR-V1_1-20050322-C	This document specifies an object for cryptographic functionality of the ECMAScript Mobile Profile [ESMP].
[WIM]	OMA-TS-WAP-WIM-V1_2-20051221-C	Specification that defines the WAP Identity Module (WIM), which is used in performing WTLS, TLS and application level security functions, and especially, to store and process information needed for user identification and authentication.
[WPKI]	OMA-WAP-WPKI-V1_1-20050322-C	Specification that defines the Public Key Infrastructure and procedures required to enable the trust relationships needed for authentication of servers and clients..
Supporting Files		
n/a		

6. Minimum Functionality Description for OBKG

This section is informative.

Key enrolment might be implemented alone (when keys are generated before the WIM is issued). On board key generation requires the implementation of key enrolment.

6.1 Minimal Functionality Description for Key Enrolment

- PKI portals: support of the enroll function, as specified in [WPKI]
- ME: implementation of the ECMA script 'enroll', as specified in [ESMPCrypto]
- ME: support of the WIM 'gka' function; [WIM]
- WIM: implementation of the 'gka' function; [WIM]

6.2 Minimal Functionality Description for On-Board Key Generation

- PKI portals: support of keyGen an enroll function, as specified in [WPKI]
- ME: implementation of the ECMA script 'keygen', as specified in [ESMPCrypto]
- ME: support of the WIM 'keygen' function; [WIM]
- WIM: implementation of the 'keygen' function. [WIM]
- ME: implementation of the ECMA script 'enrol', as specified in [ESMPCrypto]
- ME: support of the WIM 'gka' function; [WIM]
- WIM: implementation of the 'gka' function; [WIM]

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 [IOPPROC].

Feature/Application: Entry in this column SHOULD be a short descriptive label to the **Item** in question.

Status: Entry in this column MUST accurately reflect the architectural status of the **Item** in question.

- M means the **Item** is mandatory for the class
- O means the **Item** is optional for the class
- NA means the **Item** is not applicable for the class

Requirement: Expression in the column MUST be a valid TerminalExpression according to [IOPPROC] and it MUST accurately reflect the architectural requirement of the **Item** in question.

8. ERDEF for OBKG - Client Requirements

This section is normative.
These tables summarize the ERDEF listed in the specifications, and introduced by the OBKG features. In case of discrepancy, the specifications take precedence.

Item	Feature / Application	Status	Requirement
OMA-ERDEF-OBKG-C-001	ECMA GenEnroll	M	[ESMPCrypto]
OMA-ERDEF-OBKG-C-002	ECMA KeyGen	M	[ESMPCrypto]
OMA-ERDEF-OBKG-C-003	WPKI	M	[WPKI]

Table 1: ERDEF for OBKG Client-side Requirements

9. ERDEF for OBKG - Server Requirements

This section is normative.

Item	Feature / Application	Status	Requirement
OMA-ERDEF-OBKG-S-001	ECMA GenEnroll	M	[ESMPCrypto]
OMA-ERDEF-OBKG-S-002	ECMA KeyGen	M	[ESMPCrypto]
OMA-ERDEF-OBKG-S-003	WPKI	M	[WPKI]

Table 2: ERDEF for OBKG Server-side Requirements

10.ERDEF for OBKG - ICC Requirements

This section is normative.

Item	Feature / Application	Status	Requirement
OMA-ERDEF-OBKG-ICC-001	WIM GenerateKeyAssurance	O	[WIM]
OMA-ERDEF-OBKG-ICC-002	WIM Generate Asymetric Key Pair	O	[WIM]

Table 3: ERDEF for OBKG ICC Requirements

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description
		No previous version within OMA

A.2 Draft/Candidate Version V1.0 History

Document Identifier	Date	Sections	Description
Draft Versions OMA-ERELD-OBKG-V1_0	24 Jul 2003		The initial version of this document.
	09 Sep 2003		New doc references, new ERDEF
	03 Feb 2004		New doc references, new ERDEF, ECMA def, Usecase, Architecture
	01 Apr 2004		Doc references update, sec 5 CR follow up table removed, sec 8 WPKI req,
	10 Nov 2004		References to ETR added
	02 Feb 2005		ETR reference made informative, reference to OBKG RD included, ICC defined, WPKI version changed to 1.1, many editorial changes, (following consistency review comments)
Candidate Versions OMA-ERELD-OBKG-V1_0	22 Mar 2005		Candidate approval as TP ref OMA-TP-2005-0091-OBKG-V1_0-for-Candidate-approval
	21 Dec 2005		Section 5 renamed to "Document Listing for OBKG V 1.0", and new table incorporated. Change to ERP: One class 2 CR agreed against OMA-WAP-WIM-V1_2-20050322-C