Enabler Release Definition for On-board Key Generation
Candidate Version 1.0 – 22 Mar 2005

Open Mobile Alliance
OMA-ERELD-OBKG-V1_0-20050322-C
Contents

1. SCOPE ............................................................................................................................................................................ 4

2. REFERENCES ............................................................................................................................................................... 5
   2.1 NORMATIVE REFERENCES ...................................................................................................................................... 5
   2.2 INFORMATIVE REFERENCES ................................................................................................................................... 5

3. TERMINOLOGY AND CONVENTIONS .................................................................................................................. 6
   3.1 CONVENTIONS ......................................................................................................................................................... 6
   3.2 DEFINITIONS ............................................................................................................................................................ 6
   3.3 ABBREVIATIONS ...................................................................................................................................................... 6

4. INTRODUCTION ......................................................................................................................................................... 7
   4.1 ARCHITECTURE ........................................................................................................................................................ 7
   4.2 EXAMPLE USE CASE .................................................................................................................................................... 7
       4.2.1 Use case 1 : Deploying Public Key product......................................................................................................... 7
       4.2.2 Use case 2 : Third party usage of PK product...................................................................................................... 8

5. ENABLER RELEASE SPECIFICATION BASELINE............................................................................................. 9

6. MINIMUM FUNCTIONALITY DESCRIPTION FOR OBKG .................................................................................. 10
   6.1 MINIMAL FUNCTIONALITY DESCRIPTION FOR KEY ENROLMENT ............................................................ 10
   6.2 MINIMAL FUNCTIONALITY DESCRIPTION FOR ON-BOARD KEY GENERATION .................................................... 10

7. CONFORMANCE REQUIREMENTS NOTATION DETAILS ............................................................................ 11

8. ERDEF FOR OBKG - CLIENT REQUIREMENTS .......................................................................................... 12

9. ERDEF FOR OBKG - SERVER REQUIREMENTS .............................................................................................. 13

10. ERDEF FOR OBKG - ICC REQUIREMENTS ....................................................................................................... 14

APPENDIX A. CHANGE HISTORY (INFORMATIVE) .......................................................................................... 15
   A.1 APPROVED VERSION HISTORY ............................................................................................................................. 15
   A.2 DRAFT/CANDIDATE VERSION V1.0 HISTORY ...................................................................................................... 15

Tables

Table 1 ERDEF for OBKG Client-side Requirements ......................................................................................................... 12
Table 2 ERDEF for OBKG Server-side Requirements ........................................................................................................ 13
Table 3 ERDEF for OBKG ICC Requirements .................................................................................................................... 14
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


[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/]


[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

<table>
<thead>
<tr>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Enabler Release</strong></td>
</tr>
<tr>
<td>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.</td>
</tr>
<tr>
<td><strong>Minimum Functionality</strong></td>
</tr>
<tr>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Description of the guaranteed features and functionality that will be enabled by implementing the minimum mandatory part of the Enabler Release.</td>
</tr>
</tbody>
</table>

3.3 Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ECMA</td>
<td>European Computer Manufacturer Association</td>
</tr>
<tr>
<td>ERDEF</td>
<td>Enabler Requirement Definition</td>
</tr>
<tr>
<td>ERELD</td>
<td>Enabler Release Definition</td>
</tr>
<tr>
<td>GKA</td>
<td>Generate Key Assurance</td>
</tr>
<tr>
<td>ICC</td>
<td>Integrated Circuit Card</td>
</tr>
<tr>
<td>KEYGEN</td>
<td>Key Generation</td>
</tr>
<tr>
<td>OBKG</td>
<td>On Board Key Generation</td>
</tr>
<tr>
<td>OMA</td>
<td>Open Mobile Alliance</td>
</tr>
<tr>
<td>RKE</td>
<td>Remote Key Enrolment</td>
</tr>
<tr>
<td>ME</td>
<td>Mobile Equipment</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>SE</td>
<td>Security Element</td>
</tr>
<tr>
<td>WAP</td>
<td>Wireless Application Protocol</td>
</tr>
<tr>
<td>WIM</td>
<td>Wireless Identity Module</td>
</tr>
</tbody>
</table>
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.

![Architecture Diagram]

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, i.e. 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. Enabler Release Specification Baseline

This section is normative.

The following specifications comprise the OMA OBKG enabler release:

“On-board Key Generation and Key Enrollment Requirements, version 1.0” [OBKG RD]
“ECMA Script Crypto Library, Version 1_1” [ESMPCrypto]
“Wireless Application Protocol Public Key Infrastructure Definition, Version 1_1” [WPKI]
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.

<table>
<thead>
<tr>
<th>Item</th>
<th>Feature / Application</th>
<th>Status</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>OMA-ERDEF-OBKG-C-001</td>
<td>ECMA GenEnroll</td>
<td>M</td>
<td>[ESMPCrypto]</td>
</tr>
<tr>
<td>OMA-ERDEF-OBKG-C-002</td>
<td>ECMA KeyGen</td>
<td>M</td>
<td>[ESMPCrypto]</td>
</tr>
<tr>
<td>OMA-ERDEF-OBKG-C-003</td>
<td>WPKI</td>
<td>M</td>
<td>[WPKI]</td>
</tr>
</tbody>
</table>

Table 1 ERDEF for OBKG Client-side Requirements
9. ERDEF for OBKG - Server Requirements

This section is normative.

<table>
<thead>
<tr>
<th>Item</th>
<th>Feature / Application</th>
<th>Status</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>OMA-ERDEF-OBKG-S-001</td>
<td>ECMA GenEnroll</td>
<td>M</td>
<td>[ESMPCrypto]</td>
</tr>
<tr>
<td>OMA-ERDEF-OBKG-S-002</td>
<td>ECMA KeyGen</td>
<td>M</td>
<td>[ESMPCrypto]</td>
</tr>
<tr>
<td>OMA-ERDEF-OBKG-S-003</td>
<td>WPKI</td>
<td>M</td>
<td>[WPKI]</td>
</tr>
</tbody>
</table>

Table 2 ERDEF for OBKG Server-side Requirements
10. ERDEF for OBKG - ICC Requirements

This section is normative.

<table>
<thead>
<tr>
<th>Item</th>
<th>Feature / Application</th>
<th>Status</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>OMA-ERDEF-OBKG-ICC-001</td>
<td>WIM GenerateKeyAssurance</td>
<td>O</td>
<td>[WIM]</td>
</tr>
<tr>
<td>OMA-ERDEF-OBKG-ICC-002</td>
<td>WIM Generate Asymmetric Key Pair</td>
<td>O</td>
<td>[WIM]</td>
</tr>
</tbody>
</table>

Table 3 ERDEF for OBKG ICC Requirements
Appendix A. Change History

A.1 Approved Version History

<table>
<thead>
<tr>
<th>Reference</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

A.2 Draft/Candidate Version V1.0 History

<table>
<thead>
<tr>
<th>Document Identifier</th>
<th>Date</th>
<th>Sections</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Candidate version OMA-ERELD-OBKG-V1_0</td>
<td>22-3-2005</td>
<td></td>
<td>Candidate approval as TP ref OMA-TP-2005-0091-OBKG-V1_0-for-Candidate-approval</td>
</tr>
<tr>
<td>Draft version OMA-ERELD-OBKG-V1_0</td>
<td>2-2-2005</td>
<td></td>
<td>ETR reference made informative, reference to OBKG RD included, ICC defined, WPKI version changed to 1.1, many editorial changes, (following consistency review comments)</td>
</tr>
<tr>
<td>Draft version OMA-ERELD-OBKG-V1_0</td>
<td>10-11-2004</td>
<td></td>
<td>References to ETR added</td>
</tr>
<tr>
<td>Draft version OMA-ERELD-OBKG-V1_0</td>
<td>01-04-2004</td>
<td></td>
<td>Doc references update, sec 5 CR follow up table removed, sec 8 WPKI req.</td>
</tr>
<tr>
<td>Draft version OMA-ERELD-OBKG-V1_0</td>
<td>03-02-2004</td>
<td></td>
<td>New doc references, new ERDEF, ECMA def, Usecase, Architecture</td>
</tr>
<tr>
<td>Draft version OMA-ERELD-OBKG-V1_0</td>
<td>09-09-2003</td>
<td></td>
<td>New doc references, new ERDEF</td>
</tr>
<tr>
<td>Draft version OMA-ERELD-OBKG-V1_0</td>
<td>24-07-2003</td>
<td></td>
<td>The initial version of this document.</td>
</tr>
</tbody>
</table>