On-board Key Generation and Key Enrollment Requirements

Candidate Version 1.0 – 22 Mar 2005

Open Mobile Alliance

OMA-RD-OBKG-V1_0-20050322-C

Contents

1. Scope (Informative)

This document describes the requirements to enhance wireless PKI with on-board key generation and remote key enrollment services.

The Open Mobile Alliance continues the work of the WAP Forum to define a set of specifications to be used by service applications.

2. References

2.1 Normative References

[RFC2119]	"Key words for use in RFCs to Indicate Requirement Levels". S. Bradner. March 1997. URL:http://www.ietf.org/rfc/rfc2119.txt
[ECMACR]	"ECMAScript Crypto Object", OpenMobileAlliance, URL: ???
[PKCS#1]	"PKCS #1: RSA Encryption Standard", version 1.5, RSA Laboratories, November 1993.
[PKCS#7]	"PKCS #7: Cryptographic Message Syntax Standard", version 1.5, RSA Laboratories, November 1993.
[PKCS#10]	"PKCS #10: Certification Request Syntax Version 1.5," IETF RFC 2314, B. Kaliski, March 1998. URL: ftp://ftp.isi.edu/in-notes/rfc2314.txt
[RFC3280]	"Internet X.509 Public Key Infrastructure Certificate and CRL Profile," R. Housley, et al, January 1999. URL: ftp://ftp.isi.edu/in-notes/rfc3280.txt
[WAPCert]	"WAP Cert Profile". WAP Forum. URL: http://www1.wapforum.org/tech/documents/WAP-211-WAPCert-20010522-a.pdf
[WPKI]	"WPKI - Public Key Infrastructure Definition" WAP Forum. URL: http://www1.wapforum.org/tech/documents/WAP-217-WPKI-20010424-a.pdf
[xHTMLMP]	"xHTML Mobile Profile" WAP Forum. URL http://www1.wapforum.org/tech/documents/WAP-277-XHTMLMP-20011029-a.pdf
[WAPWIM]	Wireless Identity Module, OMA-WAP-WIM-v1_1-20021024-C. URL: http://www.openmobilealliance.org/documents.html

2.2 Informative References

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.

3.2 Definitions

Enrolment	Demand for a certificate for a public key pair
On-board Key Generation	Key pair generation that is done internally in the device (e.g. WIM)
Key slot	A place holder for a key that may be generated later
Security Element	A subsystem that provides cryptographic functionality, including private key storage and private key operations. E.g, a WIM as defined by OMA [WAPWIM].

3.3 Abbreviations

CA	Certificate Authority
MAC	Message Authentication Code
ME	Mobile Equipment
OMA	Open Mobile Alliance
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
POP	Proof Of Possession
SE	Security Element
WAP	Wireless Application Protocol
WIM	Wireless Identity Module
OBKG	On-board Key Generation

4. Introduction (Informative)

This document describes the OMA functionality defined to enable the generation and registration of keys into a PKI. Both key generation and key registration (also called enrolment) events may be triggered by the same entity, or they may be triggered by distinct entities; however key registration is always preceded by key generation. A key generation event may be followed by multiple key registration events, allowing for a single key to be enrolled into multiple PKIs. This approach provides a scalable solution and ease of use since a user may only need a single key, and in some cases a single PIN, while having the advantage of enrolling into multiple PKIs and transacting with multiple merchants.

Unlike the WAP model where key pairs were provisioned in a factory and distributed manually, these requirements allow for new key pairs to be generated in the field. In some scenarios the ability to include assurances that the key was generated in a secure manner is required. These assurances may specify that a key was generated per a specific policy and on some approved Security Element (SE), such as a WIM.

In order to accommodate this requirement, the ability to include an assurance signature or an assurance message authentication code (MAC) may be included in the registration request. The information that is signed or MACed includes the public key and may include additional information indicating the kind of assertion that is being made. This assurance information is then verified by the PKI to prove that the key was generated in a secure manner. This mechanism currently can indicate not only if the key was generated on-board, but may also be used to indicate if a key was injected into a SE (e.g. WIM). In addition, the registration messages generated by this functionality shall be based on industry standard PKCS#10 message formats, ensuring tight integration with the existing CA and PKI infrastructure.

The ability to invoke the key generation and key registration events through ECMAScript commands in conjunction with the ability to obtain an assurance of the fact that the key was generated on-board allows the link between key generation and key registration to be re-established.

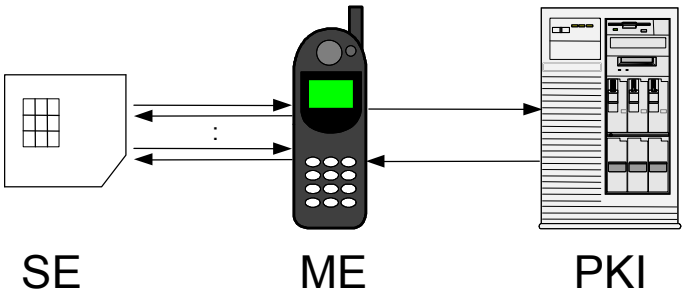
To support the requirement where explicit authorization is needed to perform a key generation or key registration, the functionality should allow for authorization data to be included. Authorization to use the key generation functionality allows the business case where an SE owner (such as an operator) has the ability to charge for the use of empty key slots on its cards to third party vendors. Similarly, authorization to enroll a particular key into a PKI allows the key owner to control who can reuse a particular key in a separate PKI.

4.1 Actors

When considering on-board key generation and key registration it is possible to identify three main participants. These are:

- A PKI
- A Mobile Entity
- A Security Element

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



4.1.1 The PKI

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 PKIs.

4.1.2 Mobile entity

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.

4.1.3 Security Element (SE)

The SE will perform operations triggered by the mobile entity including the generation of new keys in addition to standard cryptographic functionality such as signature generation used for POP (Proof of possession)..

5. Use Cases (Informative)

5.1 Use Case A

5.1.1 Short Description

The user owns a WIM enabled mobile phone with a SIM/WIM, issued by an operator. The WIM is not yet initialised with PKI credentials. The user wants to use m-commerce services and asks her operator to activate the service. The operator will provide the user with the necessary information to remotely complete this activation with the OBKG services.

5.1.2 Actors

These are the actors mentioned in [Actors] and the following:

- The user – the WIM holder
- The operator – WIM issuer

5.1.2.1 Actor Specific Issues

The operator is responsible for the registration of user identity information.

5.1.2.2 Actor Specific Benefits

In some legal contexts the requirement for on-board key generation for Non Repudiation key is considered mandatory.

The WIM is issued without user credentials, which means without user key pairs or user certificates. This allows the WIM issuer to incur the cost of key generation and certificates issuance only when the user really subscribes to a relevant service.

5.1.3 Pre-conditions

The operator has issued a WIM.

The user has a WIM enabled ME.

The operator needs to have a relationship with the PKI to provide user identity information.

5.1.4 Post-conditions

The user will have PKI credentials in the WIM that will allow her to benefit from m-commerce services.

5.1.5 Normal Flow

The normal steps, which describe the actions of the actors and the system behavior, are the following:

- The user contacts the operator to subscribe to m-commerce services
- The operator indicates to the user the URL of the PKI Portal to connect to with a WAP session, and the needed identification means to log-on to this site.
- The user browses the PKI Portal and receives an xHTML page with embedded KeyGen ECMA Script that requires the ME to trigger the key generation in the WIM.
- If the key generation was successful, the user needs to enter her identification information that is used by an embedded Enroll ECMA Script that requires the ME and the WIM to perform the key enrolment. The user may need to enter her PIN code during the Enrolment operation for the WIM to sign the enrolment request.
- The user certificate is delivered to the ME and stored in the WIM.

5.1.6 Alternative Flow

If the WIM is configured so that the key generation demands an authentication of the PKI Portal the first attempt to generate the key will return a challenge that must be signed by the invoking party. The second attempt will process normally if the authentication succeeds.

5.1.7 Operational and Quality of Experience Requirements

The user may not be involved in the key generation procedure but must be involved in the key enrolment. The xHTML pages, sent by the PKI Portal, need to be designed to respect the following:

- User experience for the enrolment phase should be similar to current service on the Web
- Number of interactions with the user for key generation phase should be minimized

5.2 Use Case B

5.2.1 Short Description

The user owns a WIM enabled mobile phone with a SIM/WIM, issued by an 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 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.

5.2.2 Actors

These are the actors mentioned in [Actors] and the following:

- The user – the WIM holder
- The operator – WIM issuer
- The financial institute – provides m-banking services and controls its own user credentials in the WIM

5.2.2.1 Actor Specific Issues

- The financial institute is responsible for the registration of user identity information.
- The financial institute needs to have an agreement with the operator.

5.2.2.2 Actor Specific Benefits

In some legal contexts the requirement for on-board key generation for Non Repudiation key is considered mandatory.

The WIM is issued without user credentials, which means without user key pairs nor user certificates. This allows the WIM issuer to incur the cost of key generation and certificates issuance only when the user really subscribes to a relevant service.

The financial institute can apply its own registration policies and control the creation of user credentials.

5.2.3 Pre-conditions

The operator has issued a WIM.

The user has a WIM enabled ME.

The operator delegates rights, to administrate the WIM on OBKG services, to the financial institute.

The financial institute needs to have a relationship with the PKI to provide user identity information.

5.2.4 Post-conditions

The user will have PKI credentials in the WIM that will allow her to benefit from m-banking services.

5.2.5 Normal Flow

The normal steps, which describe the actions of the actors and the system behavior, are the following:

- The user contacts the financial institute to subscribe to m-banking services
- The financial institute indicates to the user the URL of the PKI Portal to connect to with a WAP session, and the needed identification means to log-on to this site.
- The user browses the PKI Portal and receives an xHTML page with embedded KeyGen ECMA Script that requires the ME to trigger the key generation in the WIM.
- If the key generation was successful, the user needs to enter her identification information that is used by an embedded Enroll ECMA Script that requires the ME and the WIM to perform the key enrolment. The user may need to enter her PIN code during the Enrolment operation for the WIM to sign the enrolment request.
- The user certificate is delivered to the ME and stored in the WIM.

5.2.6 Alternative Flow

If the WIM is configured so that the key generation demands an authentication of the PKI Portal the first attempt to generate the key will return a challenge that must be signed by the invoking party. The second attempt will process normally if the authentication succeeds.

5.2.7 Operational and Quality of Experience Requirements

The user may not be involved in the key generation procedure but must be involved for the key enrolment. The xHTML pages, sent by the PKI Portal, need to be designed to respect the following:

- User experience for the enrolment phase should be similar to current service on the Web
- Number of interactions with the user for key generation phase should be minimized

5.3 Open Issues

None.

6. Requirements (Normative)

6.1 High-Level Functional Requirements

1. Interfaces defined for key generation and enrollment functionality SHALL work for any SE implementation
2. It SHALL be possible for the SE issuer to authorize a PKI Portal to remotely invoke the key generation and key enrolment services
3. It SHALL be possible to invoke the key generation functionality separately from the enrollment functionality.
4. The key enrolment SHALL be based on well known and broadly supported Internet standards to allow for the use of existing infrastructure and a flexible PKI
5. There SHALL be a mechanism to provide an assurance to the PKI Portal that the key to enroll for a certificate was generated or is stored in an SE that is acceptable by the PKI Portal policies.
6. It SHALL be possible for the PKI Portal to set sensitive user credential attributes in the SE such as key label and PIN code value.

6.1.1 Security

1. It SHALL be possible for the SE to authenticate the PKI Portal to verify authorization for key generation and key enrolment services
2. It SHALL be possible to use symmetric and/or asymmetric authentication methods to verify authorization for key generation and key enrolment services
3. When an SE has the ability to generate more then one key, it SHALL be possible for the SE to protect each key pair with distinct authorization data
4. There SHALL be a mechanism to ensure confidential transport of sensitive user credential attributes associated with a specific key generated by the key generation operation (e.g. key label, PIN code value)

6.1.2 Charging

None Identified. The mechanisms used by SE issuers to charge for key generation is out of the scope of these set of specifications.

6.1.3 Administration and configuration

1. In the case the SE is implemented as a WIM, the WIM SHALL be pre-configured with a pre-defined number of key slots for the storage of internally generated key values

6.1.4 Usability

None identified.

6.1.5 Interoperability

None identified

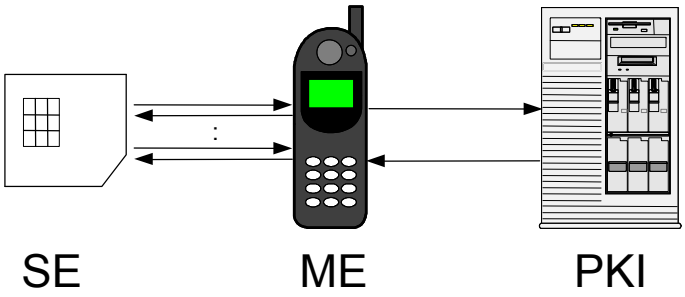
6.1.6 Privacy

None identified

6.2 Overall System Requirements

n/a

6.3 System Elements



6.3.1 System Element PKI

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 PKIs.

The separation of key generation and key registration makes it possible to support a model where it is possible to trigger key generation through another (possibly proprietary) mechanism and still have a standard way to enroll the key in a PKI.

6.3.1.1 Interfaces to System Element ME

The current interface to the ME SHALL be via WAP 2.0 protocols (e.g. HTTP, xHTML, ECMAScript).

6.3.2 System Element ME

The mobile entity 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.

In some cases, the ME is also responsible for interacting with the SE for administrative functionality such as the setting and verifying relevant PINs. When this is the case, such as when a WIM is in use, the ME is also responsible for interacting with the user when necessary. An example of this would be the selecting of a new PIN at key generation time.

The interpretation and implementation of the script commands is part of the browser implementation on the mobile entity.

6.3.2.1 Interfaces to System Element SE

At this stage the only concrete SE interface is to a WIM. The WIM uses the well-known APDU interface as defined by ISO 7816.

6.3.2.2 Interfaces to System Element PKI

Interface to the PKI is via WAP 2.0 protocols (e.g. HTTP, xHTML, ECMAScript)

6.3.3 System Element SE

The SE performs operations triggered by the mobile entity including the generation of new keys in addition to standard cryptographic functionality such as signature generation used for POP (Proof of possession). A SE that supports the key

assurance concept will be responsible for the generation of these assurances values. Other SE functionality may include the management of user PINs and any relevant flags, especially when a SE takes the form of a WIM.

6.3.3.1 Interfaces to System Element ME

At this stage the only concrete SE interface is to a WIM. The WIM uses the well-known APDU interface as defined by ISO 7816.

6.3.4 Network interfaces

None Identified

Appendix A. Change History (Informative)

A.1 Approved Version History

Reference	Date	Description

A.2 Draft/Candidate Version V1.0 History

Version Name	Date	Section	Description
OMA-RD-OBKG-V1_0-20050322-C	22 March 2005		Candidate approval as TP ref OMA-TP-2005-0091-OBKG-V1_0-for-Candidate-approval
0.2	Sep 8, 2003		Requirements clarification. Fleshed out Section 6.3.
0.1.	Sep 5, 2003		Added Additional requirements. Generalized to use SE. Removed implementation specific info from introduction.
0.0	July 24, 2003		initial document