WPKI Main Specification

Table of Contents

Appendices

1 Requirements Key Pair Generation

2 Requirements SIM card with WPKI functionality

3 Support

10 Terminology and Definitions

11 RP Interface by Adoption of ETSI WPKI Specification

12 WPKI Specification – Dsearch Interface

14 WPKI Specification – CAMO Interface

7 Design Considerations (Informative only)

1 Purpose and Scope

This document describes the WPKI infrastructure and specifies the requirements for the WPKI infrastructure to be functional.

2 Document History

Version	Date	Content
1.0	20 Dec 2004	First version
2.0	31 March 2006	- Adopted for SIM Toolkit - added RP Support Interface - added On-board key-generation, - added PUK and changed definitions around PIN, - minor changes in CAMO and Dsearch interfaces
2.2	14 May 2009	–new appendices for the interfaces CAMO and DSEARCH - minor changes

3 Terminology and Definitions

For complete terminology and definitions, see Appendix 10.

4 Introduction (Informative)

The following roles are mandatory for the WPKI infrastructure to be functional:

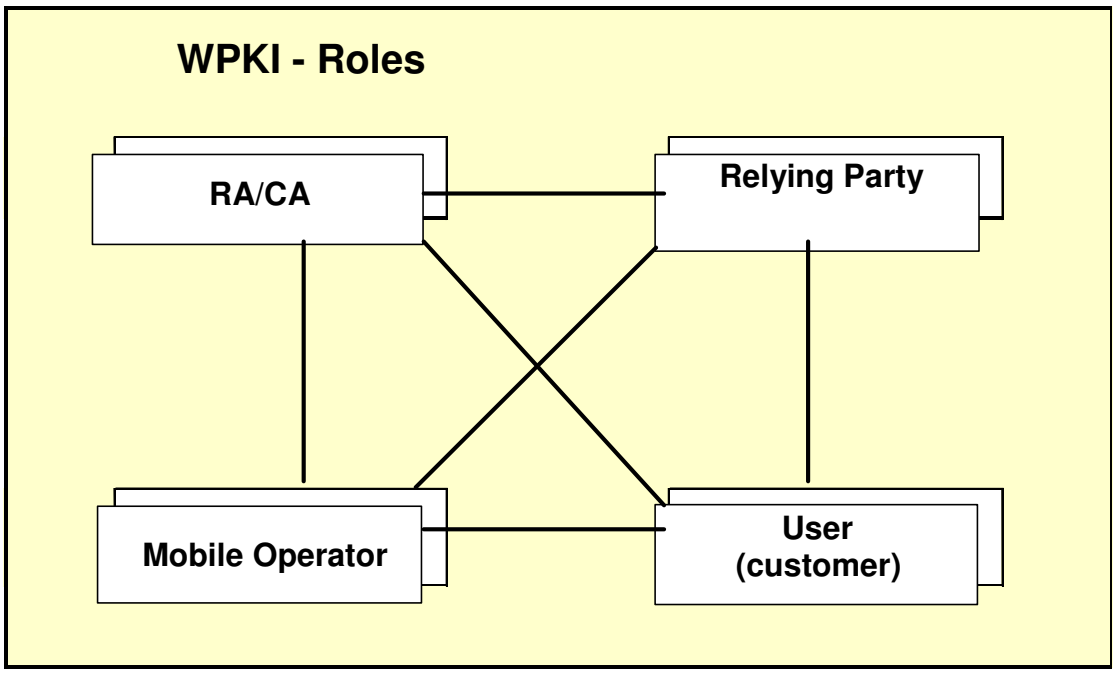

Figure 1WPKI Roles

Mobile Operator (MO):

The Mobile Operator offers mobile access, issues the SIM card with WPKI functionality and is responsible for distributing signature requests to the User and receiving signature responses from the User.

Registration Authority/Certificate Authority (RA/CA):

The RA/CA identifies the User and issues the mobile e-ID.

Relying Party (RP):

The Relying Party offers the actual service that uses the WPKI infrastructure, to the User.

User:

The User uses the service offered by the Relying Party and is the holder of the mobile e-ID.

4.1 Overview of functionality

The Mobile Operator issues SIM cards with WPKI functionality. The cards are distributed to Users that ask for this functionality. Alternatively this functionality exists on all the SIM cards that the Mobile Operator distributes.

As an alternative to the above, the Mobile Operator may issue SIM cards without cryptographic keys. In this case an on-board key-generation process can be initiated after the card has been delivered to the User, but before or in conjunction with enrolment.

The Mobile Operator defines the distribution process for SIM cards. That distribution process is not in scope for this specification and should be specified by the MO.

The Mobile Operator offers an interface for the RA/CA to obtain the public keys that correspond to the private keys and to check preconditions for enrollment. The MO also offers the RA/CA the interface to obtain information about which key pairs that have been revoked.

The User can, after receiving a SIM card with WPKI functionality, apply for a user certificate from the RA/CA. The RA/CA executes an identification process to verify the User's identity and provides the User with an enrolment activation code. The identification process is not in scope for this specification and should be specified by the RA/CA.

To prove his/her identity the User enters the enrolment activation code provided in the identification process above and signs it on the mobile terminal to prove his/her possession of the Private key.

Based on this information, the RA/CA issues a pair of user certificates.

The RA/CA is also responsible for the functionality of revoking the user certificates.

The RA/CA enters into agreements with relying parties that buy authentication and signature services from the RA/CA.

Depending on the Relying Party, the information channel can be handled by a PC or the mobile phone itself, either through mobile internet or even voice. Other

information channels are also possible. The security channel is always the mobile phone. The User connects to the Relying Party's service on the information channel and logs on using the mobile phone as a security channel to prove his/her identity.

If the functionality of the Relying Party's services contains features for signatures the User can use the mobile phone to create a signature.

4.2 Use of ETSI WPKI 102 204 and 102 207 in this specification

Version 2.0 of the WPKI specification introduced a new interface between the RP and the MO and RA/CA and MO, called RP Support Interface, RPSI. The RPSI is based on the ETSI WPKI specifications 102 204 and 102 207. The RPSI is specified in Appendix 11. No other parts of the infrastructure are specified using the ETSI WPKI specifications.

4.3 Conceptual Description

The WPKI concept is described in the four processes: Pre-Enrolment, Enrolment, Usage and Termination. The following descriptions are provided to give the reader the overview picture of the different roles and general flow in the system. Details are given in the requirements and the referenced Appendixes.

4.3.1 Pre-Enrolment

The purpose of pre-enrolment is to create the conditions necessary to perform enrolment. Pre-enrolment involves distributing the SIM cards with wpki functionality and generating an enrolment activation code that shall be used at enrolment.

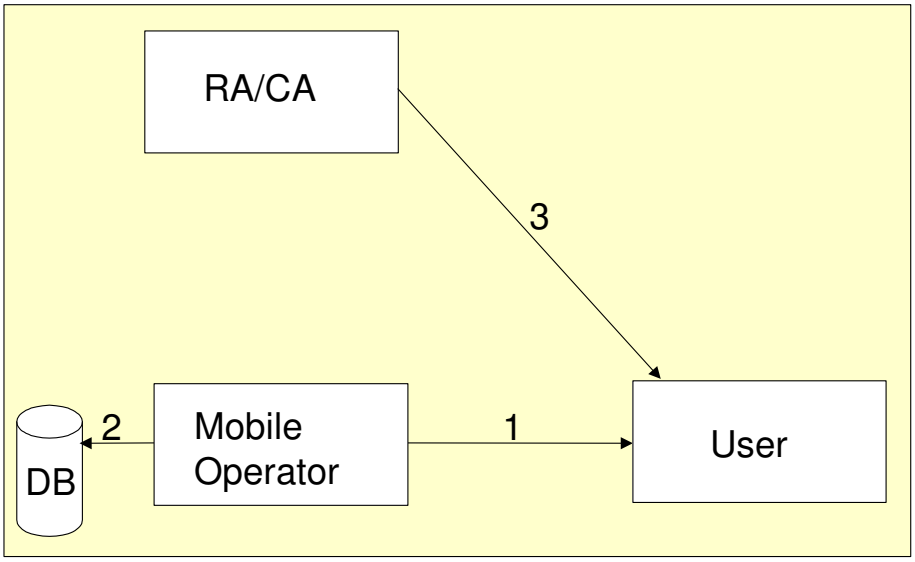

Figure 2Pre-enrolment

1. The SIM card is issued by the mobile operator to the User.
2. If the private keys are already present on the card, the device certificates and PKCS#10 structures that corresponds to the SIM card are placed in a database at the MO premises.
3. The RA/CA performs an original identification process to securely identify the User. The details of this identification process are out of scope from this specification and are defined by each RA/CA combination. The successful completion of the identification process results in the Enrolment Activation Code being issued to the User.

4.3.2 Enrolment

The purpose of enrolment is to generate the user certificates.

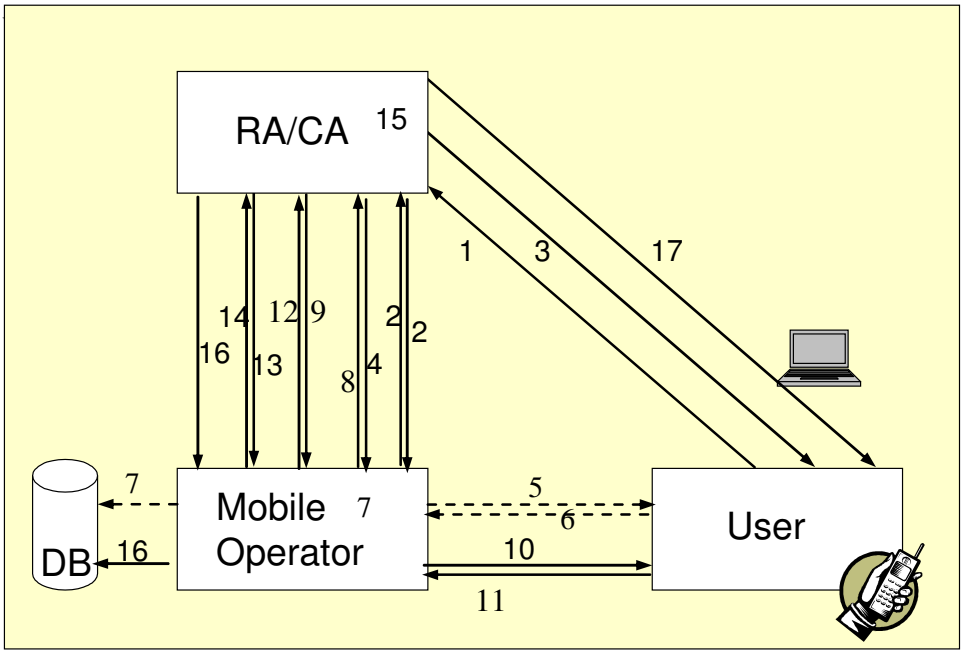

Figure 3Enrolment

The steps below are valid for the case when the User is **using separate information and security channels** as well as when **using the same channel for information and security**.

1. The User contacts the RA/CA over the information channel. The RA/CA requests the User to supply his/her mobile telephone number. The RA/CA identifies which MO the User belongs to. This can be done through a look-up in SNPAC or through a process defined by the RA/CA itself.

2. The RA/CA sends a CAMO.control to the MO to check if the preconditions for the user to proceed with registration are fulfilled. The MO returns result of the check. The different checks that are performed are described in appendix 14.

3. The RA/CA informs the User of how to perform the enrolment process, using the information channel.

4. The RA/CA sends a registration request to the MO of the User through the RPSI.
5. The MO checks if the User's SIM card contains usable keys or not. In the case where no usable keys exist, the MO sends a command to initiate on-board key-generation, which includes a process where the User sets his/her PIN for the generated keys and signs the PKCS#10 structures.
6. If on-board key-generation was initiated, the MO receives the public keys and the self-signed PKCS#10 files from the SIM card.
7. If on-board key-generation was initiated, the MO creates the device certificates and stores them in the device certificate database together with the PKCS#10 files.
8. The MO returns the device certificate for the non-repudiation key.
9. The RA/CA sends a signature request to MO through the RPSI.
10. The MO sends a push message on the security channel to the Users mobile terminal with a signature request where the Enrolment Activation Code shall be input by the User and signed. Before the User can sign the message he/she is asked to set his/her PIN if not already set.
11. The User enters the Enrolment Activation Code on the mobile terminal and signs it using the non-repudiation key by entering the private key PIN. The signed Enrolment Activation Code is returned on the security channel to the MO that sends it to the RA/CA.
12. The RA/CA receives the signed Enrolment Activation Code and verifies it against the one given during pre-enrolment.
13. The RA/CA connects to the Mobile Operator using CAMO.prepare and requests the public keys.
14. The Mobile Operator responds by sending the signed device certificates and PKCS#10 files to the RA/CA.

15. The RA/CA uses this information to produce user certificates that is stored together with information about MSISDN and MO for the User.
16. The RA/CA requests the business relation to be activated by sending a CAMO.subscribe to MO. The MO stores information about which RA/CA that has issued user certificates to the specific SIM card and keys.
17. The RA/CA informs the User that the enrolment was successful using the information channel.

In step 16 the business relation between the RA/CA and the Mobile Operator is activated. For more information about the content and price parameters, see Section 5.

The User can repeat the Enrolment process towards multiple CA:s.

4.3.3 Usage

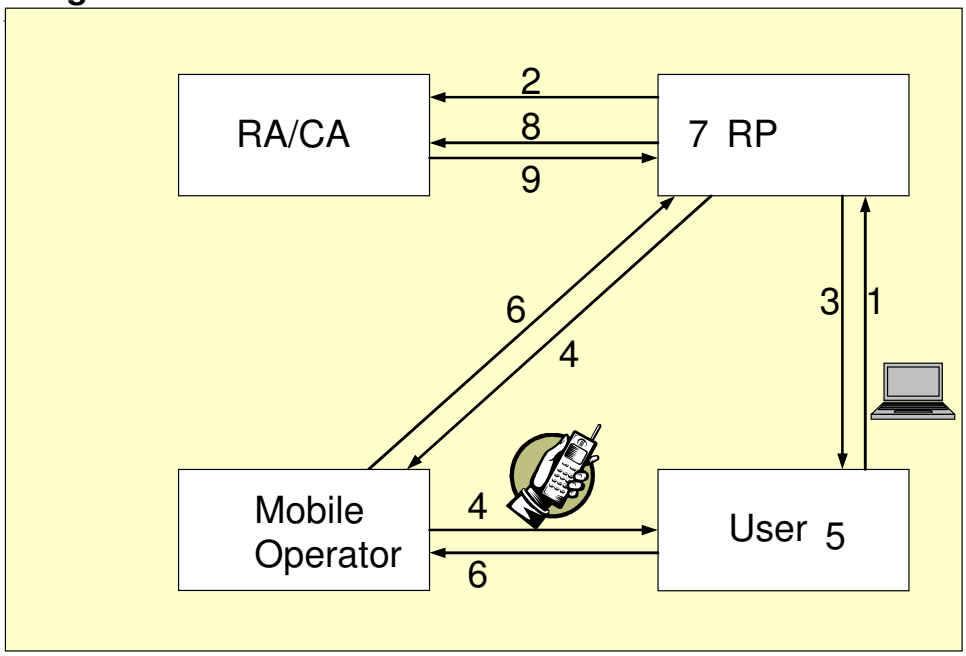

Figure 4Usage

The steps below are valid for the case when the User is **using separate information and security channels** as well as when the User is **using the same channel for information and security.**

1. The User connects to the RP over the information channel. When the User wants to login or to create a signature, the RP requests the User to leave information of his/her mobile telephone number or other information used by the RP to identify the User and retrieve the MSISDN.

2. Using the MSISDN of the User as identifier, the RP retrieves the user certificate to be used for the verification of the signature and the URL to which the signature request shall be sent, by contacting the CAs that are trusted by the RP via the Dsearch interface specified in appendix 12. The RA/CA shall only return valid certificates. If there are multiple user certificates, these are displayed by the RP in the information channel and the User selects which user certificate to use for the transaction.

3. The RP uses the information channel to display the information that the User should sign though the security channel. The RP optionally also displays a Control Code on the information channel and requests the User to enter the Control Code on the mobile terminal and sign the information with his/her private key.
4. The RP sends a signature request to the RPSI to reach the security channel to the User's mobile terminal.
5. If a control code is used, the User enters the control code on the mobile terminal. The control code is added to the Data to Be Signed (DTBS). The TTBS is displayed to the User who signs it by entering the six-digit private key PIN.
6. The signed message is returned to the MO. The MO restructures the signature to comply with PKCS#7 [PKCS#7] and forwards it to the RP.
7. The RP can verify the signature and validate the user certificate.
8. The RP validates the user certificate through an OCSP request.
9. The RA/CA returns status.

In step 8, the business relation between the RP and the RA/CA is activated. However, the relation is not handled in this concept and this is left to the market to define.

4.3.4 Termination

The input to terminate a user certificate or user certificate pair can come from different sources:

- The User can contact the RA/CA and order the termination of the user certificates
- The User can contact the Mobile Operator and cancel either the subscription or the device certificate, due to loss of terminal/SIM, change

of operator or other reasons such as blocked PINs, change of phone number, change of SIM (broken) etc.

- The RA/CA can terminate the user certificates due to expired date, misuse or other reason
- The Mobile Operator can terminate the subscription/SIM due to misuse or other reason

When the information about termination of the user certificates is received at the RA/CA the following steps are taken

1. The RA/CA revokes the user certificates.
2. The RA/CA contacts the Mobile Operator with information about the termination by sending a CAMO.unsubscribe.
3. The Mobile Operator removes the information, that was created in step 16 in Enrolment, that the RA/CA has issued user certificates for the keys from the device certificate database and terminates the business relation between the RA/CA and Mobile Operator for the specific User and SIM card.

When the information about termination of the subscription/SIM is received at the Mobile Operator the following steps are taken. Note that the User might have enrolled for user certificates from different RA/CA. The steps below represent what happens in each of the relations.

1. The Mobile Operator may remove the information, that was created in step 16 in Enrolment, that the RA/CA has issued user certificates for the keys from the device certificate database and terminates the business relation between the RA/CA and Mobile Operator for the specific User and SIM card.
2. The Mobile Operator revokes the device certificates and publishes the revocation status as a CRL.

3. The RA/CA revokes the user certificates in the user certificate database
4. The RA/CA terminates the business relation that was created in step 16 in Enrolment by sending a CAMO.unsubscribe.

5 Deliverables (Normative)

This section specifies the mandatory deliverables in the WPKI infrastructure between the roles described in section 4, Introduction (Informative).

5.1 Mobile Operator to RA/CA

Delivery of device certificates, PKCS# 10 file(s) and status information via CAMO Interface according to Appendix 12

Delivery of Root certificates and, if applicable, all intermediate certificates that have been used to sign the device certificates

Revocation service for information that a user certificate should be revoked

Administration support

RP-Support Interface according to Appendix 11 for distribution of signature requests and registration requests

5.2 RA/CA to Mobile Operator

Revocation service for user certificates

Publishing of user certificates

5.3 Mobile Operator to User

SIM card with WPKI functionality

Agreement of SIM card with WPKI functionality

Customer/User support

Information and User training related to WPKI functionality

Revocation service

5.4 Mobile Operator to Relying Party

Optionally - RP-Support Interface according to Annex 11 for distribution of signature requests

5.5 RA/CA to Relying Party

Connection to the WPKI services

Agreement of identification and signature services using WPKI Services

Support

URI to RP-Support Interface according to Annex 11 for distribution of signature requests

Optionally - RP-Support Interface according to Annex 11 for distribution of signature requests

5.6 RA/CA to User

Original identification

Information and sales material to introduce the WPKI service to Users.

WPKI Agreement

Revocation service

Support

Registration services

6 Main Technical Requirements (Normative)

This section specifies the main requirements on the WPKI infrastructure.

6.1 Basic Requirements

MR.1 The WPKI Infrastructure shall be based on the SIM Toolkit-standard [STK], where the SIM contains a SIM Toolkit application capable of performing signatures.

MR.2 It shall be possible to communicate with the SIM Toolkit application using SIM Toolkit Messaging [STK-SM].

MR.3 The SIM Toolkit application for signing shall operate according to a what-you-see-is-what-you-sign principle.

MR.4 It will be the responsibility of the MO to convert the output of the SIM Toolkit application to the signature format defined by Appendix 11.

6.2 Pre-enrolment Related Requirements

MR.10 The Mobile Operator shall issue a SIM card with WPKI functionality to the User.

MR.11 The SIM card with WPKI functionality shall fulfill the requirements in appendix 2, “Requirements SIM card with WPKI functionality”.

MR.12 The Authentication and the Non-repudiation key pairs on the SIM card with WPKI functionality shall be generated according to the requirements in appendix 1, “Requirements Key Pair Generation”.

MR.13 After completing the original identification, the RA/CA shall provide the User with an “enrolment activation code” that consists of digits only.

6.3 Enrolment-Related Requirements

MR.20 If the SIM card does not contain keys at time of enrolment, the MO must initiate the on-board key-generation process before the enrolment can proceed.

MR.21 The User shall sign the enrolment activation code with the private key at enrolment. The non-repudiation key shall be used.

MR.22 The RA/CA shall use the registration request as defined in Appendix 11 to retrieve the device certificate corresponding to the non-repudiation key from MO. The device certificate is later used to perform signature request and signature verification during enrolment.

MR.23 The CAMO interface specified in Appendix 14 shall be used between RA/CA and MO during the enrolment phase and termination phase.
During enrolment, RA/CA retrieves not only the particular certificate, but both device certificates in the pair and corresponding self-signed certificate requests, PKCS#10 [PKCS#10].
CAMO.control is used by the RA/CA to initiate a verification performed by the MO with the purpose of checking if all preconditions for the User to enrol for a user certificate are fulfilled. Some verification issues are mandatory. Other ones are optional and the result is delivered as information. More than one status code may be delivered depending on what verifications have been done.
CAMO.prepare is called by the RA/CA during enrolment of an User, before the Subscribe method is called. The purpose of the prepare method is to allow the CA system to retrieve the information necessary to issue user certificates before calling Subscribe.
CAMO.subscribe is called by the RA/CA during enrolment of an User and signifies that the RA/CA from now on subscribes to the mobile signature service of the MO for a single user certificate pair.
CAMO.unsubscribe is called by the RA/CA to end a subscription to the mobile signature service for a user certificate pair for example when the user certificates are revoked.

MR.24 The Mobile Operator shall register and keep track of which RA/CA that have received which device certificates and PKCS#10 [PKCS#10].

MR.25 The Mobile Operator shall offer an interface for RA/CA to send a signature request to the User. See appendix 11 for details.

6.4 Usage-Related Requirements

MR.30 The Mobile Operator must be able to offer a signature request interface according to appendix 11 to RA/CAs and/or RPs that want to distribute signing and authentication requests to the mobile terminal.

MR.31 The use of control code, to ensure that the same User is present at both the information channel and the security channel, is optional.

MR.32 If a control code is used it shall consist of digits only.

MR.33 To reduce the risk of replay attacks, the User should not be requested to sign something that has already been signed by the User. Usage of variable data in DTBS is required, for example use of timestamp. A signature request should not contain a DTBS already signed by the User.

MR.34 If a control code is used, it shall be entered by the User in the security channel. It shall thereafter be displayed to the User in the security channel as DTBS together with varying data. Subsequently, the User shall sign the DTBS with the private key.

MR.35 The RP shall decide which user certificate to use prior to sending the signature request to the security channel.

MR.36 The RP software shall be designed to display only the user certificates for the appropriate use, authentication or signing, to the User.

MR.37 If only one user certificate pair is found in a distributed search, the RP shall select the appropriate user certificate, authentication or signing, without asking the User.

MR.38 If more than one user certificate pair is found in a distributed search, the RP shall present all appropriate user certificates to the User in the information channel to User and the User shall select which one to use.

MR.39 The MO shall provide revocation status through CRLs on the device certificates to CAs that have issued user certificates.

MR.40 The RA/CA shall revoke all user certificates corresponding to revoked device certificates.

MR.41 The Interface between MO and RA/CA for providing revocation status shall use CRLs [CRL].

MR.42 The CRLs [CRL] shall be published (ldap, http or https) by the MO and retrieved by the CA periodically, at least once every 24 hour.

MR.43 The CRLs [CRL] shall contain the issuer Distinguished Name and serial numbers of all revoked device certificates.

MR.44 The interface between RP and RA/CA for distributed search is detailed in Appendix 12. The interface is used by the RP to find all user certificates related to a specific MSISDN. In the response all user certificates issued by the RA/CA for the provided MSISDN are included together with the service URL for the RPSI service provider. In the request, the RP may also specify if only certificates with a specific certificate usage as well as the CA certificate chain shall be included in the response or not.

MR.45 The RA/CA may offer an interface for RP to send a signature request to the User. See appendix 11 for details.

6.5 Termination-Related Requirements

MR.50 If the information about termination of a user certificate is received at the RA/CA, the following steps shall be taken

- The RA/CA shall revoke the user certificate in the user certificate database

- The RA/CA shall contact the SIM card issuing Mobile Operator with information about the termination according to the interface specified in Appendix 14
- The Mobile Operator shall be able to receive a termination request from RA/CA according to the interface specified in Appendix 14
- The Mobile Operator, when receiving the termination request, shall terminate the business relation between the RA/CA and Mobile Operator for the specific user certificate

MR.51 If the information about termination of the subscription/SIM is received at the Mobile Operator, the following steps shall be taken for each RA/CA concerned.

- The Mobile Operator shall terminate the business relation between the Parties for the specific user certificate(s)
- The Mobile Operator shall revoke the device certificate and publish the revocation status as a CRL
- The RA/CA shall revoke the user certificate in the user certificate database

7 References

[CRL] Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, rfc3280
Internet Engineering Task Force
http://www.ietf.org/rfc/rfc3280.txt

[WPKI] WAP Public Key Infrastructure Definition, WAP-217-WPKI-20010424-a
WAP Forum
http://www.openmobilealliance.org/tech/affiliates/wap/wapindex.html

[STK] Universal Subscriber Identity Module (USIM) Application Toolkit (USAT), GSM 11.14 / 3GPP TS 31.111
3GPP
http://www.3gpp.org/specs/specs.htm

[STK-SM] Security mechanisms for the (U)SIM application toolkit, GSM 03.48 / 3GPP TS 23.048
3GPP
http://www.3gpp.org/specs/specs.htm

[USAT-INT] Universal Subscriber Identity Module Application Toolkit (USAT) interpreter byte codes, 3GPP TS 31.113
3GPP
http://www.3gpp.org/specs/specs.htm

[Signtext] WMLScript Crypto Library, WAP-161-WMLScriptCrypto-20010620-a
WAP Forum
http://www.openmobilealliance.org/tech/affiliates/wap/wapindex.html

[PKCS#7] PKCS #7 Cryptographic Message Syntax Standard
RSA Laboratories
ftp://ftp.rsasecurity.com/pub/pkcs/doc/pkcs-7.doc

[PKCS#10] PKCS #10 v1.7: Certification Request Syntax Standard
RSA Laboratories
ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-10/pkcs-10v1_7.pdf

[3GPP T3] 3GPP Specifications for group: T3,
http://www.3gpp.org/ftp/Specs/html-info/TSG-WG--T3.htm

[SSL] “The SSL 3.0 Protocol”, Nov 1996
Netscape Communications Corp.
http://wp.netscape.com/eng/ssl3/ssl-toc.html

[TLS] The TLS protocol, rfc 2246, Jan 1999
Internet Engineering Task Force
http://www.ietf.org/rfc/rfc2246.txt

[ETSI 204] Mobile Signature Service, Web Service Interface, ETSI TS 102 204
ETSI
http://www.etsi.org

[ETSI 207] Mobile Signature Service, Roaming in Mobile Signature Services, ETSI TS 102 207
ETSI
http://www.etsi.org