wPKI Specification

1 Scope
This document describes requirements for wPKI, it defines in detail the requirements for wireless implementation of PKI, related to qualified signatures.

2 Version history
Versiion 1.0 2005-11-01 Draft
Versiion 1.2 2006-01-05 Revision
Versija 1.3 2007-01-15 Revision
Versija 1.4 2007-01-30 Migration to common terms/definitions
Versija 1.5 2007-03-16 Corrections according to work-group notes
Versija 1.6 2007-05-09 Signed by E3P Coordinating Committee

3 Abbreviations and definitions
All the terms and definitions inside this document are put in italic and are understood exactly as defined in Appendix A to this paper.

4 Introduction (Informative)
The following obligatory roles are defined in wPKI set-ups:
4.1 Functionality overview

RA provisions SIM cards with SSCD function for those customers who express their will in using PKI services (see “PKI specification” section 4.1 for more details).

Service Providers deliver their services to the customers by electronic means (based on special internet, voice and similar applications). The mobile phone is a signing device in authentication and signing applications for wPKI case.

4.2 Conceptual description

In wPKI operation there are 4 main processes: SIM provision, certificate activation, usage and termination.

Description of these services is only informative.

4.2.1 SIM provision

The process of SIM provision is constructed to provide SSCD for physical persons in such a way, that this SSCD could be used for issuing a qualified certificate later on:

1. RA establishes identity of the person and deliver SIM card for GSM subscriber in face-to-face procedure.
2. SSCD’s device certificate is declared active for particular SIM and is made available for all TSP’s.
3. The customer receives the code for activation of qualified certificate.

4.2.2 User registration/certificate activation

The purpose of the certificate activation process is to create and activate a qualified certificate.

1. User issue request to activate their qualified certificate (activation interface - mobile).
2. RA initiates signing request to the user’s mobile device to sign the personal data.
3. The user verifies the data and signs it by inputting their device certificate activation code.
4. RA receives personal data signed.
5. RA adds up additional data (including device certificate) and forwards the request for certificate activation to some CA.
6. CA creates and activates a qualified certificate and publishes it.
7. The user is notified about the operation status, the user is given an opportunity to change their sPIN.
4.2.3 Usage
The usage scheme describes processes initiated by SP and TSP interaction (e.g. usage of authentication service). The scheme does not include user-SP interaction:

1. Service Provider requests some identity service from TSP (the user is identified by personal ID code or by GSM subscriber number).
2. TSP generates the signature request and sends it to the user's mobile phone.
3. User signs the request by entering their sPIN.
4. TSP receives signature data.
5. TSP checks the validity of the signature data and validity of certificate.
6. Service Provider receives identity-related service from TSP.

4.2.4 Termination
It is possible for the user to stop using PKI services in several ways:
- when the user expresses their will to RA to stop using the services,
- when the user informs RA about lost/compromized SSCD,
- the qualified certificate expires,
- RA finds out that the user has violated the user-CA agreement or in situations regulated by law.

In cases of certificate revocation:
1. RA informs CA of certificate revocation, CA immediately revokes certificate, CRL lists are updated.
2. In case of SIM blocking due to loss or SIM damage, the device certificate is taken out of the list of valid SSCD available to all TSP's.
5 Products (Normative)
This section describes services that have to be delivered by participating parties.

5.1 RA products for CA

5.2 CA products for RA
Qualified certificate production/activation service. Qualified certificate revocation service. Qualified certificate publication service.

5.3 RA products for user
User identification, Production and delivery of SSCD (SIM card), Agreement on using SSCD and qualified certificates, Support/helpdesk services, Instruction/informational material, Managing of the certificate lifecycle: activation and revocation.

5.4 RA products to TSP
List of active device certificates, associated to SSCD and MSISDN (phone number). Qualified certificates and associated personal data.

5.5 TSP products to SP
Service Level Agreement for PKI service provision Connection to wPKI (system interface) Monitoring and support, problem resolution (single point of contact for all PKI-related problems)

5.6 Mobile Operator products for TSP
Service level agreement for connection to wPKI Connection to wPKI (system interface).

6 Technical requirements (Normative)
This section describes requirements for wPKI elements.

6.1 General requirements
TR.1 The SIM cards used in wPKI applications have to be produced in secure environment and have to comply to protection profile defined by CEN CWA 14169 with evaluation assurance level EAL4+ according to “Common criteria - security” standard (ISO/IEC15408). The SIM vendor has to provide certificate upon request from CA for a particular SIM product.

TR.2 The SIM card may have two key pairs (Key-s and Key-N) stored in secure SSCD area. The Key-N usage must be protected by signatory PIN code “sPIN”.

wPKI interaction with the user is based on SIM Toolkit [STK], with RSA cryptographic plug-ins for:
i) binary information encryption/signing function (Fingerprint Signature Plugin - FP), capable of using two private keys, (this function may be used in authentication and non-repudiation signing applications)

ii) text decryption function (TD), related to one private key (This function allows to securely send some secret text message to the user; the TD does not produce any reusable output, except showing decrypted text on mobile phone’s display);

iii) binary information decryption function (AD), related to one private key (this function is used for user's data protection in external systems).

TR.3 The usage of the private key Key-N has to be protected by the sPIN code (the sPIN has to be input at every usage of the Key-S). sPIN has to comprise of 4-8 digits. The sPIN has to be blocked after 5 incorrect attempts to input this code.

The picture below indicates relation of cryptographic plug-ins and keys:

```
   AD   BP   TD
    \   /   /
     S N  S
    /   \
   Key-S  Key-N
```

TR.4 The access to plug-in FP should be granted only to TSP's that provide qualified signature-based PKI services (i.e. these TSP declare their signing system to be secure with assurance level EAL4, according to protection profile defined by CEN CWA 14170).

6.2 SIM provision and certificate activation requirements

TR.12 The user is provided with “activation code” used in activation of qualified certificate, it has to be delivered personally with preconditions:

- the user identity has been established according to Registration Policy,
- the user familiarizes themselves with the main principles of usage of qualified certificates and signs the related contract.

TR.15 The user may be provided with a possibility to set their sPIN value before or immediately after activation of their qualified certificate.

6.3 Other requirements

TR.20 Mobile operators have to sign agreements and provide access to wPKI to all the TSP's that comply to TR.4.

TR.24 Mobile Operators must provide list of all active device certificates and revoked certificates to TSPs.

TR.30 RA has to perform the following actions when terminating qualified certificates:

- informs CA of certificate revocation,
- terminates CA-user agreement related to particular SIM card.