

Baltic WPKI Forum

WPKI mobile transactions: implementation recommendations

PUBLIC

VERSION 0.3

Date	Author	Version	Changes
11.05.2007	Jürgen Niinre	DRAFT	New document
15.05.2007	Ramūnas Šablinskas	0.1	Update regarding LT situation
28.05.2007	Ramūnas Šablinskas	0.2	Tarvi's remarks
06.08.2007	Jürgen Niinre	0.3	Notes in WPKI forum

WPKI Forum	PUBLIC	VERSION 0.3	WPKI mobile transactions	6.08.2007
------------	--------	----------------	--------------------------	-----------

Table of contents

1. References.....	2
2. Terms and abbreviations.....	2
3. General WPKI overview.....	3
4. Scope.....	4
5. SIM card.....	5
5.1. Technical requirements.....	5
5.2. Cryptographic Keys.....	5
5.3. Personalisation.....	6
5.4. Interface to SIM functions.....	6
5.5. Authentication procedure.....	7
5.6. Signing procedure.....	7
5.7. Changing PIN and Unblocking PIN.....	7
5.8. Localisation.....	8
6. Phone.....	8
7. SMSC.....	8
8. OTA Server.....	8
9. Transaction interface.....	8
10. Mobile phone user interface.....	9

WPKI Forum	PUBLIC	VERSION 0.3	WPKI mobile transactions	6.08.2007
------------	--------	----------------	--------------------------	-----------

1. References

1. GSM 11.11: Digital cellular telecommunications system (Phase 2+);Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface
2. ETSI 102 221: Smart cards; UICC - Terminal interface; Physical and logical characteristics;
3. 3GPP 31.102: 3rd Generation Partnership Project; Technical Specification Group Terminals; Characteristics of the USIM Application;
4. GSM 11.14: Digital cellular telecommunications system (Phase 2+);Specification of the SIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface;
5. ETSI 102 223: Smart Cards; Card Application Toolkit (CAT) ;
6. 3GPP 31.111: Universal Mobile Telecommunications System (UMTS);Universal Subscriber Identity Module (USIM) Application Toolkit (USAT);
7. GSM 03.48: Digital cellular telecommunications system (Phase 2+);Security Mechanisms for the SIM application toolkit;
8. 3GPP 23.048: Security mechanisms for the (U)SIM application toolkit ;
9. PKCS#1: RSA Cryptography Standard, Version 2.1.
10. DIRECTIVE 1999/93 EC – European community framework for electronic signatures

2. Terms and abbreviations

PKI - Public Key Infrastructure, information system to support user authentication and digital signatures;

CA - Certification Authority;

RA - Registration Authority;

TSP - Trust Service Provider;

MO - Mobile operator;

WPKI - PKI over Wireless medium;

SIM - Subscriber Identity Module, used in GSM phones to identify the subscriber, according to [GSM 11.11];

USIM - Universal SIM, used in 3G (and in dual mode also GSM) phones to identify the subscriber, according to [ETSI 102 221], [3GPP 31.102];

STK - SIM Toolkit standard for applications on SIM card by [GSM 11.14], [ETSI 102 223] and [3GPP 31.111];

OTA - Over The Air communication with SIM card by [GSM 03.48] and [3GPP 23.048];

SMS, OTA SMS - Short Message, used for OTA sending to SIM card;

Application, SIM Application, WPKI Application - Application that is added to SIM card and that can handle the WPKI requests;

PIN - Personal Identification Number, to identify the user that is using the application;

PUK - Personal Unblocking Key, used to unblock PIN;

WPKI Forum	PUBLIC	VERSION 0.3	WPKI mobile transactions	6.08.2007
------------	--------	----------------	--------------------------	-----------

OTA server - server application that can format and send SMS for SIM application in a secure way;

WPKI request - request that is issued by TSP to get the signature or authentication data for the mobile user.

challenge code, hash code - binary data that is input for the digital encryption/signature function

verification code – data that is a number derived from hash – or challenge code and is shown to the user to ensure the authenticity of the transaction. Currently there are following formats defined:

1. challenge - or hash code hexadecimal representation;
2. decimal number in range 0-8192, calculated by taking 6 (highest or most significant) bits from the beginning of hash – or challenge code and 7 (lowest or least significant) bits from the end of hash - or challenge code:

$[H^N H^{N-1} H^{N-2} H^{N-3} H^{N-4} H^{N-5}] H^{N-6} \dots H^9 H^8 H^7 [H^6 H^5 H^4 H^3 H^2 H^1 H^0]$

SSCD – Secure signature creation device [DIRECTIVE 1999/93 EC]

3. General WPKI overview

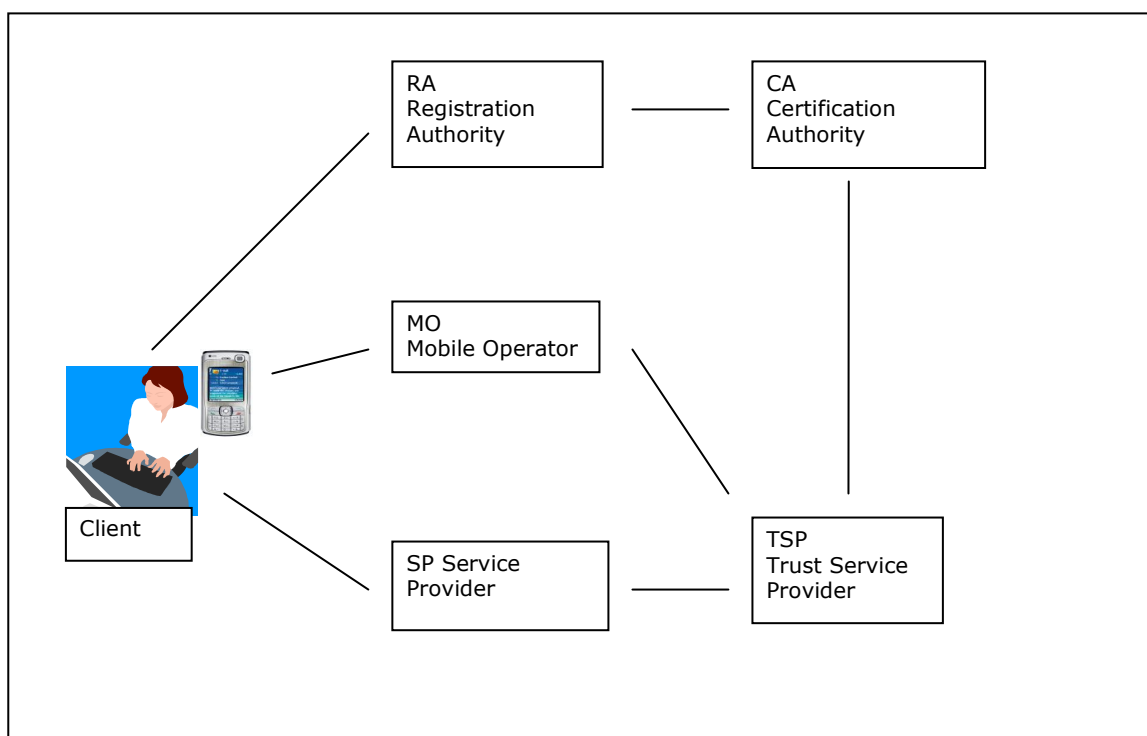


Figure 1. General overview of roles in WPKI

The WPKI organizational structure can be divided into following roles:

- Registration Authority - manages the user registration and customer care, usually acts on behalf of a Certification Authority;
- Certification Authority - manages activation, suspension and revoking of certificates;

WPKI Forum	PUBLIC	VERSION 0.3	WPKI mobile transactions	6.08.2007
------------	--------	----------------	--------------------------	-----------

- Trust Service Provider - acts as a central interface in WPKI infrastructure; main tasks include accepting authentication and signing transactions from Service Providers, passing requests to Mobile Operators and certificate and signature validity check;
- Service Provider - third party that is interested in authentication and/or digital signature of the user.

4. Scope

The scope of this document is to define recommendations for WPKI transactions implementation to ensure:

- adequate security level (in order to achieve interoperability among applications);
- uniform look and feel for users (in order to simplify user education and support);
- flawless operation.

This document sets recommendations for:

1. SIM card (subroutines related to cryptographic functionality);
2. mobile phone (compatibility with GSM/UMTS standards);
3. SMSC;
4. OTA server;
5. mobile phone user interface (UI);
6. transaction interface (TI).

The recommendations in this document are grouped in two categories: Mandatory and Optional. The implementations that conform to all mandatory recommendations are considered to be potentially interoperable.

The current document considers that only qualified certificates are used in WPKI implementations, therefore CA's are in charge of supervising RA's registration services conformance to local legal requirements.

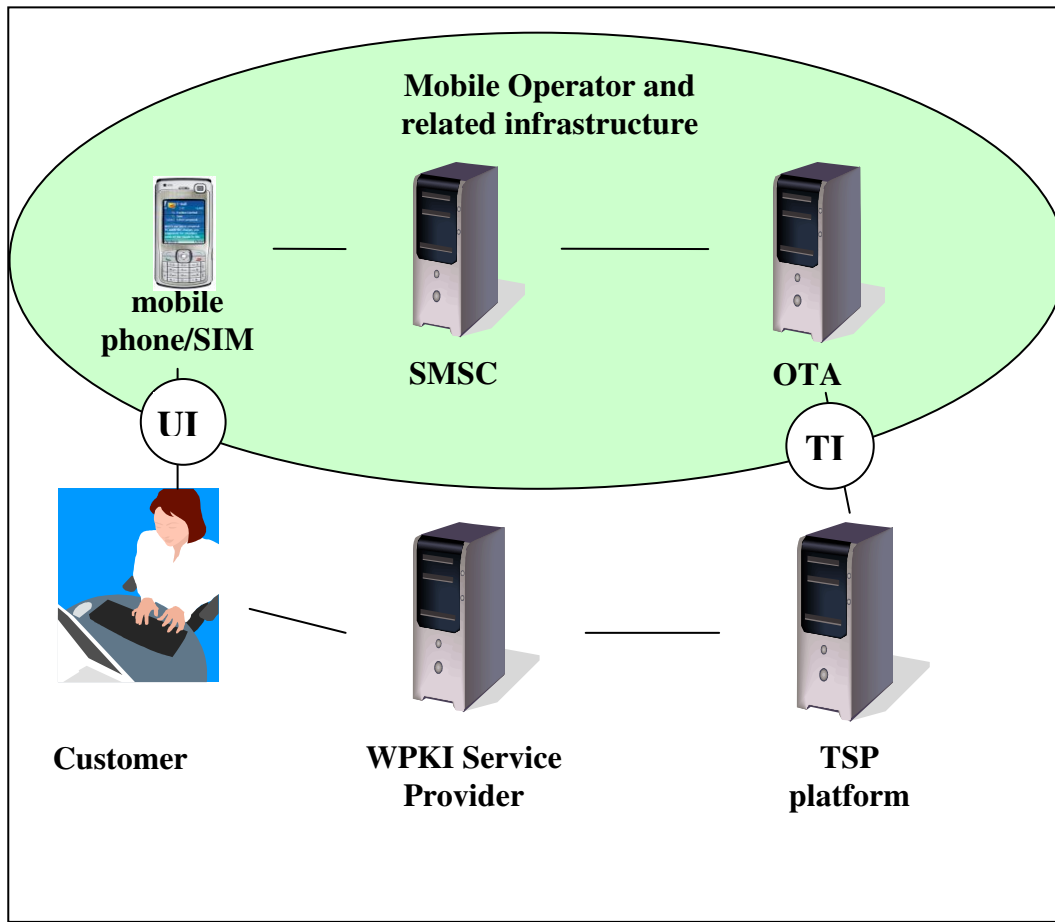


Figure 2. The diagram about the scope of this document

5. SIM card

5.1. Technical requirements

Id	Description	Mandatory
TR1	Application and SIM card must support RSA encryption (i.e. RSA encryption-based signature and authentication) functionality with RSA cryptographic keys at least of 1024 bits (The SIM cards have to comply to SSCD requirements)	Yes
TR2	SIM card must support counter, ciphering and cryptographic checksum of OTA SMS-s sent by the OTA server	Yes

5.2. Cryptographic Keys

Id	Description	Mandatory
KR1	There must be at least one keypair for authentication	Yes
KR2	There must be at least one keypair for non-repudiation	Yes
KR3	Non-repudiation private key must be protected by a PIN code	Yes

WPKI Forum	PUBLIC	VERSION 0.3	WPKI mobile transactions	6.08.2007
------------	--------	----------------	--------------------------	-----------

KR4	Authentication private key must support (but not entitled to) PIN protection	Yes
KR5	PIN code for authentication private key should be 4-12 digits long	No
KR6	PIN code for non-repudiation private key should be 5-12 digits long	No
KR7	There should be check on the SIM to not accept PIN codes where: <ol style="list-style-type: none"> 1. all digits are equal; 2. incremental from first digit to the last (for example 12345, 2345, etc); 3. incremental from last digit to the first (for example 9876, 43210, etc). 	No
KR8	Usage of private keys must be blocked at least after 5 th incorrect PIN code entry that is protecting the respective key	Yes
KR9	There must be unblocking mechanism for the PIN codes. After 3 rd incorrect entry of the unblocking code the card should be blocked	No
KR10	It must be possible to change PIN codes later during application life cycle	Yes
KR11	It must be possible to unblock the private keys with unblocking key during application life cycle	No

5.3. Personalisation

Id	Description	Mandatory
PR1	Cryptographic keys must be personalised by SIM card manufacturer	Yes
PR2	The PIN values and private key values must be destroyed in SIM manufacturer's equipment, after completion of a SIM personalisation process	Yes
PR3	SIM manufacturer must deliver non-repudiation public keys to Mobile Operator or to CA in encrypted form (e.g. as certificates)	No

5.4. Interface to SIM functions

Id	Description	Mandatory
IR1	Application must support at least OTA SMS interface for authentication.transaction;	Yes
IR2	Application must support at least OTA SMS interface for digital signature transaction;	Yes
IR3	Application must support changing of PIN codes;	Yes
IR4	Application must support unblocking private keys with PUK code	No
IR5	Application must support decryption of encrypted data	No
IR6	Application must support decryption and display of a text message	No

WPKI Forum	PUBLIC	VERSION 0.3	WPKI mobile transactions	6.08.2007
------------	--------	----------------	--------------------------	-----------

5.5. Authentication procedure

Id	Description	Mandatory
AR1	<p>During authentication procedure, the hash - or challenge code sent by OTA server must be signed with authentication private key, according to following procedure:</p> <ol style="list-style-type: none"> 1. EM is calculated, according to EMSA-PKCS1-v1_5-Encode in PKCS#1 2. Signature is calculated, according to RSASSA-PKCS1-v1_5 in PKCS#1 3. Resulting signature is sent back to OTA server 	Yes
AR2	Application must show the verification code to user during authentication procedure	No

5.6. Signing procedure

Id	Description	Mandatory
SR1	<p>During signing procedure, the hash code sent by OTA server must be signed with non-repudiation private key, according to following procedure:</p> <ol style="list-style-type: none"> 1. EM is calculated, according to EMSA-PKCS1-v1_5-Encode in PKCS#1 2. Signature is calculated, according to RSASSA-PKCS1-v1_5 in PKCS#1 3. Resulting signature is sent back to OTA server 	Yes
SR2	Application must show the verification code to user during signing procedure	Yes

5.7. Changing PIN and Unblocking PIN

Id	Description	Mandatory
CR1	Old PIN or PUK code should be validated before initiating the PIN changing or PIN unblocking procedure	Yes
CR2	The new PIN code must be entered twice by the user	Yes

WPKI Forum	PUBLIC	VERSION 0.3	WPKI mobile transactions	6.08.2007
------------	--------	----------------	--------------------------	-----------

5.8. Localisation

Id	Description	Mandatory
LR1	It should be possible to have user interface in at least three languages (local, russian, english)	No

6. Phone

Id	Description	Mandatory
PHONE1	Phone must support at least phase 2+ (SIM toolkit)	Yes

7. SMSC

Id	Description	Mandatory
SMSC1	SMSC should support priority delivery of OTA SMS-s	No
SMSC2	SMSC should support 0 second retry of OTA SMS-s (the time difference between delivery failure and resend should be 0s)	No
SMSC3	SMSC should use no more than two tries to send the OTA SMS-s	No

8. OTA Server

Id	Description	Mandatory
OTA1	OTA server must support counter, ciphering and cryptographic checksum for sending OTA SMS-s to the SIM card	Yes

9. Transaction interface

Id	Description	Mandatory
TI1	OTA server must accept following data in part of WPKI request <ol style="list-style-type: none"> 1. MSISDN 2. language identifier 3. hash code (20, 32, 48 or 64 bytes) 4. Text to be displayed to the user 5. request type (authentication or signing) 	Yes
TI2	OTA server must return following data as to the initiator of WPKI request: <ol style="list-style-type: none"> 1. result code (OK, Cancelled, User timeout, SIM error) 	Yes

WPKI Forum	PUBLIC	VERSION 0.3	WPKI mobile transactions	6.08.2007
------------	--------	----------------	--------------------------	-----------

	2. RSA digital signature if OK	
--	--------------------------------	--

10. Mobile phone user interface

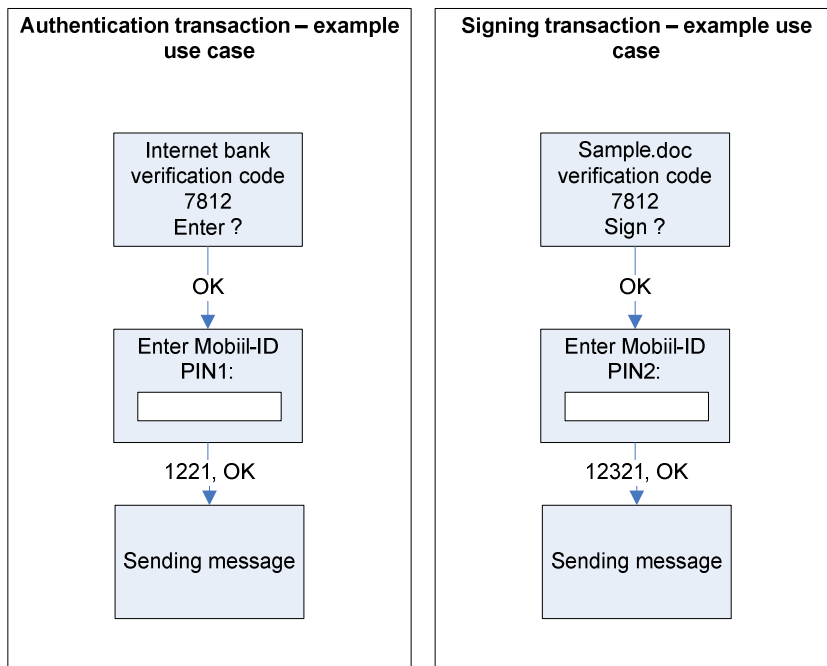


Figure 3. Authentication and signing transaction example use cases

Id	Description	Mandatory
UI1	It must be possible for the OTA server to send text to be displayed on mobile phone screen with the WPKI request (e.g.: "Internet bank or Sample.doc")	Yes
UI2	verification code must be displayed for the signing transactions, and is not mandatory in authentication transaction (e.g.: "verification code 7812")	Yes
UI3	Different text must be displayed to the user, depending on the request type (authentication or signing) (e.g.: Enter? or Sign?)	Yes
UI4	Different PIN code prompts must be displayed, depending on the request type and private key used (authentication or non-repudiation) (e.g: "Enter PIN1:" or "Eneter your signing PIN2:")	Yes

WPKI Forum	PUBLIC	VERSION 0.3	WPKI mobile transactions	6.08.2007
------------	--------	----------------	--------------------------	-----------

- END OF DOCUMENT -