



RemarcSystems OÜ

Mobile-ID

Short description

Presented on

16.03.2014

For free use

Table of Contents

[1 Using mobile signature 3](#_Toc382928079)

[2 Mobile-ID Solution 4](#_Toc382928080)

[2.1 Mobile Signature Service 4](#_Toc382928081)

[2.2 General overview of roles in WPKI 5](#_Toc382928082)

[2.3 Technological connecting 6](#_Toc382928083)

[2.4 Benefits 6](#_Toc382928084)

[3 What we propose 7](#_Toc382928085)

[3.1 USIM Application Toolkit 7](#_Toc382928086)

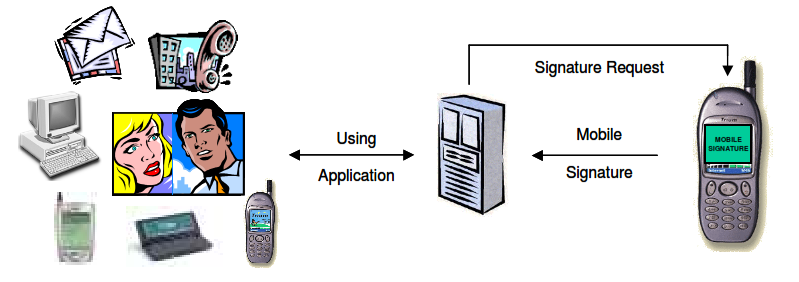
[3.2 MSSP Server 8](#_Toc382928087)

[3.3 Qualifications 9](#_Toc382928088)

[Appendix A: References 10](#_Toc382928089)

[Appendix B: Terms and Abbreviations 11](#_Toc382928090)

# Using mobile signature



Mobile signature is a concept that is applicable to all kinds of "applications" and not just those applications which can be accessed through mobile devices. Its use is appropriate for applications requiring a citizen's permission to proceed with completion of a transaction that may be initiated by a voice-call, via interactive voice response systems, via the internet and other electronic communications channels and even face-to-face situations. In this respect, the mobile device may be considered as a "signing-tool" - the electronic equivalent of a pen.

Mobile-ID provides certain advantages for the end user compared to the ID-card: the user does not need a smartcard reader nor any specific software. Mobile-ID enables you to make electronic transactions, just like an ID-card: it makes it possible for you to log into internet banks and sign various contracts digitally. Personal identification and digital signature functionality are secured by up-to-date security technology and corresponding Personal Identification Numbers (PIN). What makes the solution more convenient is the fact that you no longer need an ID-card reader in your computer - instead, you can access your internet bank from any available computer. A mobile telephone acts as a card and a card reader at the same time.

# Mobile-ID Solution

## Mobile Signature Service

Coordination and management of the mobile signature process represents an opportunity to define a MOBILE SIGNATURE SERVICE for citizens and application providers alike. This approach is implemented by the Remarc MSSP server with the Remarc Mobile-ID USAT application.

The Remarc Mobile-ID server might:

* accelerate adoption of mobile signature by Application providers;
* allow implementation/deployment of a universal API;
* coordinate activation of mobile signature functionality for endusers;
* coordinate the processing of signature requests for application providers;
* reduce service deployment costs;
* minimize duplication of systems and functions;
* aggregate signature traffic.

The Remarc Mobile-ID MSSP server has a standardized interface implemented as an Internet Web Service. In this respect, the Remarc Mobile-ID MSSP server is an intermediary between endusers and APs that provides and implements a Mobile Signature Web Service according to the ETSI TS 102 204 (Mobile Commerce; Mobile Signature Service; Web Service Interface).

## General overview of roles in WPKI

SP...

Teenusepakkuja

SP2 Teenusepakkuja

SP

Service Provider



MO

Mobile Operator

CA

Certification Authority center



TSP

Trusted Service Provider

RA

Registration Authority center

Client

RA and MO

AT&T, T-Mobile …

CA and TSP services provided by

VeriSign,

Verizon, Entrust …

By/Sells Certificates

SLA

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;
* 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. The Trust Service Provider uses MSSP Server for communicate with a Mobile Operator;
* Service Provider - third party that is interested in authentication and/or digital signature of the user.

## Technological connecting C:\Users\Ildar\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\9HE16DSC\MC900435242[1].png

M*SS*P server

with

OTA support

SMSC



TSP

Trust

Service Provider

SP, AP

Service provider

Application provider

CA center

Client

Mobile-ID

USAT applet on USIM



Technology elements:

* USAT applet - USIM card with an application. It supports RSA encryption (the SIM card has to comply with SSCD requirements). It has at least one keypair for authentication and at least one keypair for non-repudiation. It supports OTA SMS interface for authentication and digital signature transactions;
* SMSC – SMS center. It supports priority delivery of OTA SMS-s;
* MSSP Server – Mobile Signature Service Provider server. It supports Mobile Signature Service (ETSI 102.204) and converts it into USAT applet SMS format. It supports counter, ciphering and cryptographic checksum for sending OTA SMS-s to the USAT applet;
* TSP – Trust Service Provider. Trusted security service for Service providers. It links together many Service providers and Mobile operators with its MSSP Servers;
* SP, AP – Service provider or Application provider. It provides some service to a Client and needs authentication or non-repudiation confirmation services.

## Benefits

A Client saves high-level security services to own personal devices. And now the Client may operate with trusted services from other computer with less security level. No need additional devices for increase security level and give access to own trusted services.

It is possibility to develop mobile applications (mobile payment, ticketing, data encryption …) can use trusted key storage and key functions from USAT applet.

# What we propose

## [USIM Application Toolkit](http://en.wikipedia.org/wiki/USIM_Application_Toolkit)

The Remarc Mobile-ID USAT applet this is a JavaCard applet with USIM Application Toolkit menu support.

After personalization of the USAT applet on a USIM card a Mobile Operator provide a generated OTA keys to the Remarc MSSP Server.

After that the Remarc MSSP Server can communicated with the Remarc Mobile-ID USAT applet application via Mobile Operator’s SMSC server.

Basic functions of the Remarc Mobile-ID SAT applet:

* Authentication function:
  + During an authentication, a challenge code sent by MSSP server will be signed with an authentication private key;
  + The applet shows a part of a received verification code and a received text to a user during authentication with the USAT applet with an additional prompt "Confirm XXXX?" (this text line depends from selected language);
* Signing function:
  + During signing, a hash code sent by MSSP server will be signed with a non-repudiation private key. Resulting signature is sent back to MSSP server;
  + The applet shows a part of a received verification code and a received text to user during signing with the SAT applet with an additional prompt "Confirm XXXX?" (this text line depends from selected language);
* Changing PIN1/PIN2 - in a USAT menu is present a menu item for access to the PIN changing function;
* Changing PUK - in a USAT menu is present a menu item for access to PUK changing function;
* Unblock PIN1/PIN2 - in a USAT menu is present a menu item for access to the Unblock PIN function;
* View information - in a USAT menu is present a menu item with information of PIN usage.

The specification of the Remarc Mobile-ID SAT applet:

* The application is based on Java Card™ platform, version 2.2.1;
* The application uses USIM Application Toolkit for the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface, defined in [3GPP](http://en.wikipedia.org/wiki/3GPP) 31.111 for 3G;
* The application supports RSA encryption and verification functionality with RSA cryptographic keys in range from 1024 to 2048 bits;
* There is one keypair for authentication;
* There is one keypair for non-repudiation;
* Access to signature function of each keypair is protected by own PIN code;
* PIN can be 4-12 digits long;
* PIN length have to defined during application personalization;
* PIN length have to defined separately for each keypair;
* It is possible to change PIN codes during application life cycle;
* Usage of private keys is blocked after 3th incorrect PIN code entry;
* There is unblocking mechanism for the usage of private keys;
* After 5rd incorrect entry of the unblocking code (PUK) the application is blocked;
* The application has command for each keypair generation;
* The application has command for getting of public key for each keypair;
* The application supports changing of PIN codes via SAT menu;
* Old PIN or PUK code is validated before initiating the PIN changing or PIN unblocking procedure;
* The new PIN code is entered twice by the user;
* The application supports unblocking usage of private keys with PUK code via SAT menu;
* The application counts the number of times the use of each PIN;
* The application has user interface in a three languages.

## [MSSP](http://en.wikipedia.org/wiki/USIM_Application_Toolkit) Server

The Remarc Mobile-ID MSSP Server this is a typical J2EE application that was built with the Spring framework:

* base languages and API: Java JDK 1.6/1.7, J2EE 1.4, Servlet 2.3/2.4, JSP 1.1/1.2;
* framework: Spring3;
* MVC2: Spring MVC, View: Tiles2, JSP;
* DB mapping: Hibernate4;
* web services: The Java API for XML Web Services (JAX-WS).

Basic functions of the Remarc MSSP Server:

* supporting mandatory parts of ETSI TS 102 204 Technical specification V1.1.4 web service protocol:
  + the “Mobile Signature” function with the messaging mode either synchronous mode, or asynchronous ClientServer mode, or asynchronous ServerServer mode;
  + the Mobile Signature status query function;
  + the Mobile Signature profile query function;
  + the Mobile Signature registration function;
  + the Mobile Signature receipt function;
  + the Mobile Signature handshake function;
* supporting of CMS, PKCS#10 and XML-Signature formats;
* supporting of counter, ciphering and cryptographic checksum for sending OTA SMS-s to the Remarc USAT application;
* supporting GSM 03.48 specification during commands exchange with SIM;
* supporting of a OTA key encryption in the database;
* supporting of a private key encryption in the database;
* supporting of the SMPP for connecting to a SMSC;
* supporting of a few database types (Oracle, MS SQL, MySQL) for persist necessary data (will configured before an application build);
* the MSSP server accepts following data in part of WPKI request:
  + 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);
* the MSSP server returns following data as to the initiator of WPKI request:
  + 1. result code (OK, Cancelled, User timeout, SIM error)
  + 2. RSA digital signature if OK;
* the MSSP server can select correct SMSC (a Mobile Operator) by provided MSISDN;
* the MSSP server selects correct keys for GSM 03.48 by provided MSISDN.

## Qualifications

Our personal has experience of implementation of eID on smart card. We actively participated in the implementation of Universal Electronic Card (UEC) of Moscow.

Our clients financial and telecom firms like Elion (TeleSoneria), Nasdaq.

Our Java developers and architects have programmer and architect certification from SUN, Weblogic, Oracle. Most of developers have Oracle Certified Professional certification.

# Appendix A: 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. ETSI 102 223: Smart Cards; Card Application Toolkit (CAT);
5. 3GPP 31.111: Universal Mobile Telecommunications System (UMTS);Universal Subscriber Identity Module (USIM) Application Toolkit (USAT);
6. GSM 03.48: Digital cellular telecommunications system (Phase 2+);Security Mechanisms for the SIM application toolkit;
7. 3GPP 23.048: Security mechanisms for the (U)SIM application toolkit;
8. PKCS#1: RSA Cryptography Standard, Version 2.1;
9. DIRECTIVE 1999/93 EC – European community framework for electronic signatures.

# Appendix B: 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];
* USAT - USIM Application Toolkit standard for applications on SIM card by [3GPP 31.111] and [ETSI 102 223];
* 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 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.
* SSCD – Secure signature creation device [DIRECTIVE 1999/93 EC]