![j0305790[1]]()



RemarcSystems OÜ

Mobile-ID

Краткое описание

Представлено

16.03.2013

Для свободного использования

Содержание

[1 В нашей стране 3](#_Toc379881690)

[2 Решение Mobile-ID 3](#_Toc379881691)

[2.1 Цели 3](#_Toc379881692)

[2.2 Общий обзор ролей в WPKI 4](#_Toc379881693)

[2.3 Технологические соединения 5](#_Toc379881694)

[2.4 Преимущества 7](#_Toc379881695)

[3 План реализации 8](#_Toc379881696)

[3.1 Выбор партнеров 8](#_Toc379881697)

[3.2 Что мы предлагаем 8](#_Toc379881698)

[3.3 Квалификация 8](#_Toc379881699)

[4 Стоимость 9](#_Toc379881700)

[Приложение A: Ссылки 10](#_Toc379881701)

[Приложение B: Термины и Сокращения 11](#_Toc379881702)

# В нашей стране

В дополнении к eID, расположенному на национальной ID карте, в мае 2007 года Эстонскому рынку было предложено решение Mobile-ID. В порядке получения Mobile-ID - клиенты должны были поменять свои SIM-карты на карту с PKI-совместимым приложением. В дополнении к функциональности обычной SIM карты - Mobiil-ID SIM карта еще содержит мобильные идентификаторы, которые позволяют поставщикам интернет сервисов идентифицировать пользователя, и дает возможность использовать электронную подпись. Поскольку процесс выпуска карты и ее регистрации, выполняются мобильным оператором, пользователям это может показаться не совсем безопасным. Чтобы избежать недоверия пользователь должен еще “активировать” свое Mobile-ID приложение с помощью своей ID-карты. Таким образом, выдача Mobile-ID привязана к безопасности и качеству ID-карты. Сертификаты Mobile-ID содержат туже самую информацию о личности держателя карты, что и сертификаты ID-карты.

Цель – предоставить альтернативный путь для аутентификации и цифровой подписи в системах Поставщиков Услуг.

# Решение Mobile-ID

## Цели

Mobile-ID предоставляет определенные преимущества для конечного потребителя по сравнению с ID-картой: пользователь не нуждается в считывателе смарт-карт и нет необходимости устанавливать специальное программное обеспечение.

Mobile-ID позволяет делать такие же операции, как и ID-карта: решение дает возможность войти в интернет-банк и подписать различные документы, контракты в цифровом виде.

Идентификация персоны и функциональность цифровой подписи предоставляются по современным технологиям безопасности и защищены соответствующими персональными идентификационными номерами (PIN). Решение делает более удобным то, что больше не нужен считыватель ID-карты в компьютере пользователя - вместо этого, можно получить доступ в интернет-банк из любого доступного компьютера. Мобильный телефон выступает в качестве и карты и устройства чтения карт одновременно.

## Общий обзор ролей в WPKI



Организационная структура WPKI может быть поделена на следующие роли:

* Регистрирующий орган (RA, Registration Authority) - управляет регистрацией пользователя и обслуживает клиентов. Как правило, действует от имени Удостоверяющего центра;
* Удостоверяющий центр (CA, Certification Authority) - управляет выдачей, приостановлением и аннулированием сертификатов;
* Поставщик доверенного сервиса (TSP, Trust Service Provider) - выступает в качестве центрального интерфейса в WPKI инфраструктуре: Основными задачами являются: прием запросов аутентификации; запросов на создание подписи от поставщиков услуг, прохождение заявки на подключение операторов мобильной связи; взаимодействие с приложением Mobile-ID;
* Поставщик услуг (SP, Service Provider) - третья сторона, которая заинтересована в создании подлинной цифровой подписи пользователя, аутентификации и идентификации пользователя.

## Технологические соединения



Технологические элементы:

* Mobile-ID STK приложение - SIM карта с установленным Mobile-ID приложением. SIM-карта должна соответствовать целому ряду требований: ETSI 102 221, 3GPP 31.102, ETSI 102 223, 3GPP 31.111, GSM 03.48, 3GPP 23.048. Карта поддерживает ассиметричное шифрование, обычно RSA (чтобы создать электронную подпись в формате PKCS#1 для выполнения директивы DIRECTIVE 1999/93 EC). Она имеет, по крайней мере, одну пару ключей для аутентификации и не менее одной пары ключей для обеспечения электронной подписи. Она поддерживает OTA SMS интерфейс для операций аутентификации и цифровой подписи. Карта должна функционировать в аппарате, соответствующем спецификациям GSM 11.11, GSM 11.14;
* SMSC – SMS центр. Он поддерживает приоритетную доставку ОТА SMS;
* MSSP сервер – Mobile Signature Service Provider сервер. Он поддерживает сервис Мобильной подписи (Mobile Signature Service, ETSI 102.204) и конвертирует запросы в SMS формат Mobile-ID STK приложения. Он поддерживает счетчик, шифрование и создание криптографической контрольной суммы для отсылки OTA SMS в Mobile-ID STK приложение в соответствии со спецификацией GSM 03.48;
* Поставщик доверенных услуг (TSP, Trust Service Provider) - Доверенный сервис безопасности для Поставщиков услуг. Он связывает вместе Поставщиков услуг и операторов мобильной связи с помощью своего MSSP сервера;
* Поставщик услуг (SP, Service provider) – Поставщик услуг предоставляет некоторый сервис клиенту и требует аутентификации и идентификации клиента или подтверждения неотрекаемости при получении услуги.

##

## Преимущества

Клиент получает услуги безопасности высокого уровня для своего персонального телефона. И теперь Клиент может получать свои доверенные услуги с любого компьютера, даже не оборудованного специальными устройствами безопасности. Не нужны дополнительные аппараты для увеличения уровня безопасности при получении защищенных услуг.

Цель состоит в том, чтобы предоставлять услуги безопасности высокого уровня без дополнительных устройств - считывателей карт и PIN клавиатур.

Появляется возможность расширять функциональность мобильного аппарата, добавляя мобильные приложения (мобильные платежи, билеты, шифрация данных, …) которые могут использовать хранилище доверенных ключей и операции с ключами с помощью Mobile-ID STK приложения.

# План реализации

Мы хотим предоставить Mobile-ID решение на другие рынки за пределами Эстонии.

## Выбор партнеров

Мы предлагаем найти контакты в государственном Удостоверяющем центре или в уполномоченном государством органе. Эта организация может быть в предлагаемой схеме Поставщиком доверенных услуг, управлять MSSP сервером, представлять Удостоверяющий центр.

Цель состоит в том, чтобы обеспечить надежный хранение ключей с функциями безопасности для мобильных приложений.

Следующая категория партнеров – телекоммуникационные фирмы, мобильные операторы. Это мобильные операторы, которые могут работать с идентификационными модулями в телефоне, базирующимися на спецификации JavaCard. Другими словами – GSM операторы и часть CDMA операторов, которые работают с R-UIM картами (Removable User Identity Module) на базе JavaCard. Эти компании могут играть роль МО в нашей схеме. Так же они могут играть роль RA, если им это доверит УЦ. Эти компании должны будут организовать выпуск карт с Mobile-ID приложением и взаимодействие с MSSP сервером.

## Что мы предлагаем

Помощь в организации Mobile-ID услуги, Mobile-ID STK приложение для USIM карт, MSSP сервер. Мы понимаем, что при другой законодательной базе и других партнерах данные решения должны быть изменены и адоптированы. Мы надеемся, что данные изменения будут минимальны, но мы готовы к анализу реальных требований нового рынка.

## Квалификация

Наш персонал имеет опыт применения eID приложений на смарт-карте. Мы активно участвовали в реализации Универсальной Электронной карты города Москвы. Мы создавали инфраструктуру, работающую с Эстонской eID картой.

Наши клиентами были финансовые и телекоммуникационные компании, такие как Elion (TeleSoneria), Nasdaq.

Наши Java разработчики и архитекторы имеют сертификаты от SUN, Weblogic, Oracle. Большинство разработчиков имеют сертификацию Oracle Certified Professional.

# Стоимость

Mobile-ID STK приложение для USIM карт, MSSP сервер – все эти продукты должны быть дополнительно адаптированы под нужды клиентов. Стоимость зависит от существующего процесса обмена OTA ключами, типа SIM карты, процесса выпуска карт, процесса выпуска сертификатов.

Один из возможных путей формирования стоимости может быть таким:

* Годовые отчисления для каждого установленного STK приложения – 1 EUR. В этом случае MSSP сервер поставляется бесплатно (оплата производится только за адаптацию продуктов к процессам обмена OTA ключами, типу SIM карты, процессам выпуска карт, процессам выпуска сертификатов);
* Плата за транзакцию. В этом случае STK приложение и MSSP сервер поставляется бесплатно (оплата производится только за адаптацию продуктов к процессам обмена OTA ключами, типу SIM карты, процессам выпуска карт, процессам выпуска сертификатов);
* Разовая плата за лицензию использования STK приложения для мобильного оператора и MSSP сервера в данном регионе.

# Приложение A: Ссылки

1. GSM 11.11: Digital cellular telecommunications system (Phase 2+);Specification of the Subscriber Identity Module - Mobile Equipment (SIM - ME) interface;
2. 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;
3. ETSI 102 221: Smart cards; UICC - Terminal interface; Physical and logical characteritics;
4. 3GPP 31.102: 3rd Generation Partnership Project; Technical Specification Group Terminals; Characteristics of the USIM Application;
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.

# Приложение B: Термины и Сокращения

* **PKI** - Public Key Infrastructure, информационная среда, поддерживающая инфраструктуру ассиметричных ключей для обеспечения возможности аутентификации и идентификации пользователя и создания электронной подписи;
* **CA** - Certification Authority, Удостоверяющий Центр;
* **RA** - Registration Authority, Регистрирующий орган;
* **TSP** - Trust Service Provider, Поставщик доверенных услуг;
* **MO** – Мобильный оператор;
* **WPKI** - PKI over Wireless medium, Инфраструктура ассиметричных ключей в беспроводных сетях;
* **SIM** - Subscriber Identity Module, Идентификационный модуль для применения в GSM телефонах. Идентифицирует аппарат в соответствии с [GSM 11.11];
* **USIM** - Universal SIM, используется в сетях 3G (и в GSM сетях тоже в режиме dual mode) для идентификации аппарата, в соответствии с [ETSI 102 221], [3GPP 31.102];
* **STK** - SIM Toolkit спецификация для приложений на SIM карте в соответствии с [GSM 11.14], [ETSI 102 223] and [3GPP 31.111];
* **OTA** - Over The Air связь с SIM картой в соответствии с [GSM 03.48] и [3GPP 23.048];
* **SMS, OTA SMS** - Short Message, короткие сообщения, использующие OTA для отсылки сообщений SIM карте;
* SIM приложение –приложение, устанавливаемое на SIM карту и которое может обрабатывать WPKI запросы;
* **PIN** - Personal Identification Number, Персональный Идентификационный Номер - число используемое для аутентификации пользователя, использующего приложение на карте;
* **PUK** - Personal Unblocking Key - числовой ключ, используемый для разблокировки PIN;
* **WPKI запрос** – запрос, который посылает TSP, чтобы получить подпись или идентификационные данные для пользователя.
* **challenge code, hash code** – бинарные данные, которые являются параметрами для функций шифрования или создания электронной подписи.
* **verification code** – данные, число, полученное из hash – или challenge code и показываемые пользователю, чтобы убедиться в соответствии запроса в мобильном устройстве и текущей транзакции.

**SSCD** – Secure signature creation device, устройство создания электронной подписи [DIRECTIVE 1999/93 EC].