Персональный электронный идентификатор на основе микроконтроллера смарт карты

Электронная идентификация при предоставлении услуг
(общие положения)

- Соответствие законодательству РФ
- Национальная безопасность и защита интересов граждан
- Применение мирового опыта
- Использование научно-технического потенциала, имеющегося в России
- Удобство использования
- Учет национальных особенностей

Соответствие законодательству

- ФЗ от 10 января 2002 г. №1 «Об электронной цифровой подписи»
- ФЗ от 27 июля 2006 г. № 149 «Об информации, информационных технологиях и о защите информации»
- ФЗ от 27 июля 2006 г. № 152 «О персональных данных»
- Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (*ПКЗ-2005)*

Зарегистрировано в Минюсте РФ 3 марта 2005 г. N 6382

Персональный электронный идентификатор – носитель информации
(инженерные требования)

- Универсальность

- Защищенность

- Надежность

Универсальность
носителя информации

- Соответствие международным стандартам
- Соответствие российским требованиям в области информационной безопасности
- Различное исполнение – смарт карта, USB-брелок, плата персонального компьютера и др.
- Поддержка контактного и бесконтактного (для смарт карт) интерфейсов

Защищенность
носителя информации

- **Защита информации криптографическими методами по российским стандартам**
  - Криптоалгоритм ЭЦП в соответствии с ГОСТ Р34.10-2001
  - ХЭШ - алгоритм в соответствии с ГОСТ Р34.11-94
  - Криптоалгоритм симметричной криптографии в соответствии с ГОСТ 28147-89
- **Физическая защищенность микроконтроллера**
  - Аппаратные средства контроля целостности данных и разграничения доступа к областям памяти микроконтроллера
  - Аппаратные средства защиты от динамических и статических методов исследования
- **Защита методами полиграфии (для смарт карт)**

Сложности выбора платформы

Особенности применения	Java Card	Native Card	Почему
GSM, EMV приложения	+	+/-	Для GSM необходим сервис по удаленной загрузке приложений, обусловленный особенностями услуг, предоставленных операторами мобильной связи.
Идентификация, аутентификация, системы безопасности	-	+	Надежность и безопасность реализуемых механизмов криптозащиты.
Быстродействие	↓	↑	Прикладные функции в Java-картах реализуются через виртуальный слой, который не имеет прямого доступа к ресурсам процессора (важно для реализации криптографии), что существенно снижает конечное быстродействие приложений.
Использование EEPROM	↓	↑	Java-карты требуют дополнительный объем EEPROM для размещения исполняемого кода как стандартных команд, так и кода приложений. Пример: Объем Java-кода приложения DUET (ОРПС) - 32 Кбайт
Безопасность	-	+	Реализация российской ЭЦП на стандартной Java-карте невозможна, как невозможна и сертификации в ФСБ РФ, требуемая по закону об ЭЦП (Актуально для применения в электронном государстве, проектах федерального уровня).
Надежность	↓	↑	Необходимость разработки программного Java - кода увеличивает вероятность ошибок.
Стоимость карт	↑	↓	Для обеспечения равной функциональности Java-карты требуют применения более производительного микроконтроллера и большего объема памяти (EEPROM), что увеличивает его цену.
Стоимость инициализации	↑	↓	Java-карты требуют дополнительного времени для загрузки исполняемого программного кода приложений, что удлиняет (в разы) время инициализацию, а как следствие – удорожает технологию эмиссии.

Надежность
носителя информации

- Выпускаемый серийно современный микроконтроллер от мирового лидера STMicroelectronics
- Международная сертификация на соответствие стандарту ISO/IEC 15408 (Common criteria) с уровнем доверия EAL 5+
- Сертификация криптомодуля операционной системы «Магистра» в ФСБ РФ по классу КС2

Микроконтроллер ST19NR66

- 8-ми разрядное процессорное ядро
- Внутренний тактовый генератор ~20MHz
- Контактный интерфейс ISO 7816
- RF – интерфейс ISO 14443-B
- RAM – 6 Кбайт
- ROM – 266 Кбайт
- EEPROM – 66 Кбайт *(возможность разместить более 10 независимых приложений)*
- 1088 – битовый криптографический сопроцессор для криптографии с открытым ключом
- Аппаратный ускоритель DES

Три этапа «доверенности» электронного идентификатора

1. Доверенная операционная система + серийно производимый зарубежный микроконтроллер (существует сейчас)
2. Доверенная операционная система + спроектированный в России и производимый за рубежом микроконтроллер (появится в 2010г.)
3. Доверенная операционная система + спроектированный в России и производимый в России микроконтроллер (появится в 2011г.)

Функциональные возможности
доверенной операционной системы «Магистра»

- Набор команд ОС:
  - Набор команд фазы инициализации
  - Набор команд в соответствии с ISO 7816, включает 39 команд соответствующих ISO 7816-4/8
  - Набор сервисных команд ОС:
    - VALIDATE CARD - расширенная диагностика карты
    - HANG CARD - проверка срабатывания защитных механизмов карты
- Возможность реализации независимых приложений.
- Возможность функционального расширения.
- Возможность коммуникации по контактному (ISO 7816) и бесконтактному (ISO 14443 B) интерфейсам.

Функциональные требования

к носителю информации

- Обеспечение персональной идентификации пользователей в Системе
- Обеспечение юридически значимой аутентификации пользователей в Системе
- Обеспечение подтверждения целостности и достоверности данных, хранящихся в памяти носителя
- Обеспечение подтверждения операций на основе применения юридически значимой ЭЦП
- Обеспечение возможности безналичных электронных платежей
- Реализация функций корпоративных и региональных систем
- Обеспечение защищенной эмиссии носителя

Платформа унификации

- Жизненный цикл носителя информации
- Наличие обязательных приложений с возможностью размещения дополнительных
- Состав и форматы данных обязательных приложений
- Система, порядок и протоколы идентификации и аутентификации карты
- Интерфейсы и протоколы обмена данными с терминальным оборудованием
- Конструктивные элементы – дизайн, внешний вид и др. (для смарт карт)

Сферы применения электронного идентификатора с доверенной ОС "Магистра"

- Носитель ключевой и идентификационной информации для систем защищенного документооборота.
- Универсальный электронный идентификационный элемент для пользователей системы.
- Носитель ключевой и идентификационной информации абонентов информационных систем включая системы оказания государственных услуг населению в электронной форме.
- Платежная карта.

Проекты

- Социальная карта
- Электронный идентификатор Общероссийского государственного информационного центра (ОГИЦ)
- Ключевой носитель в инфраструктуре удостоверяющих центров
- Электронный идентификатор и ключевой носитель в АИС ЭТД ОАО «РЖД»