Персональный электронный идентификатор на основе микроконтроллера смарт карты

Докладчик: Зырин Николай Владимирович

ПрограмПарк

7 мая 2009 г., Московский офис Всемирного банка

Росинформтехнологии

Персональный электронный идентификатор на основе микроконтроллера смарт карты

Докладчик: Зырин Николай Владимирович

ПрограмПарк

7 мая 2009 г., Московский офис Всемирного банка

Росинформтехнологии

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
- Учет национальных особенностей

Росинформтехнологии

Персональный электронный идентификатор – носитель информации
(инженерные требования)

- Универсальность
- Защищенность
- Надежность

ПрограмПарк

Росинформтехнологии

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

Росинформтехнологии

Защищенность носителя информации

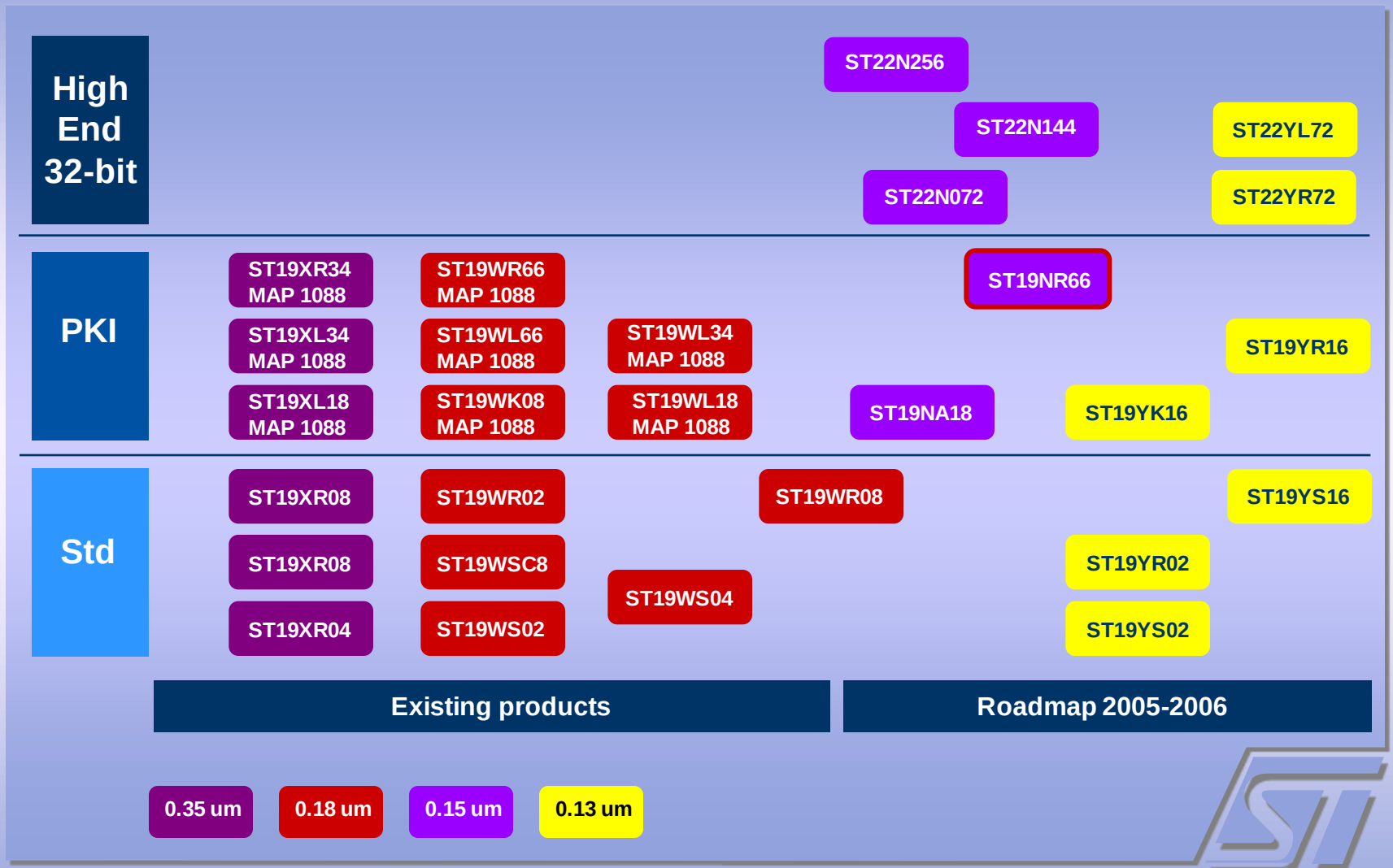
- **Защита информации криптографическими методами по российским стандартам**
  - Криптоалгоритм ЭЦП в соответствии с ГОСТ Р34.10-2001
  - ХЭШ - алгоритм в соответствии с ГОСТ Р34.11-94
  - Криптоалгоритм симметричной криптографии в соответствии с ГОСТ 28147-89
- **Физическая защищенность микроконтроллера**
  - 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)**

Росинформтехнологии

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 уполномоченных российских компетентных органах

Аппаратная платформа



Микроконтроллер ST19NR66

Росинформтехнологии

- 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
- 1088 – битовый криптографический сопроцессор для криптографии с открытым ключом
- Аппаратный ускоритель DES

Росинформтехнологии

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 2009г.)
3. Доверенная операционная система + спроектированный в России и производимый в России микроконтроллер (появится в 2010г.)

ПрограмПарк

Росинформтехнологии

Функциональные возможности
доверенной операционной системы «Магистра»

- **Набор команд ОС:**
  - **Набор команд фазы инициализации**
  - **Набор команд в соответствии с ISO 7816:**
    - **Включает 27 команд соответствующих ISO 7816-4 разделы 8.2-8.6 (работа с данными), ISO 7816-8 (криптографические команды), ISO 7816-8 (команды управления картой и файлами)**
  - **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.**

Росинформтехнологии

Функциональные требования
к носителю информации

- Обеспечение идентификации держателей карт в Системе
- Обеспечение юридически значимой аутентификации СК в Системе
- Обеспечение подтверждения целостности и достоверности данных, хранящихся в памяти СК
- Обеспечение подтверждения операций на основе применения юридически значимой ЭЦП
- Обеспечение осуществления безналичных электронных платежей
- Реализация функций корпоративных и региональных систем
- Обеспечение защищенной эмиссии СК

Платформа унификации

Росинформтехнологии

- 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"

Росинформтехнологии

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

Проекты

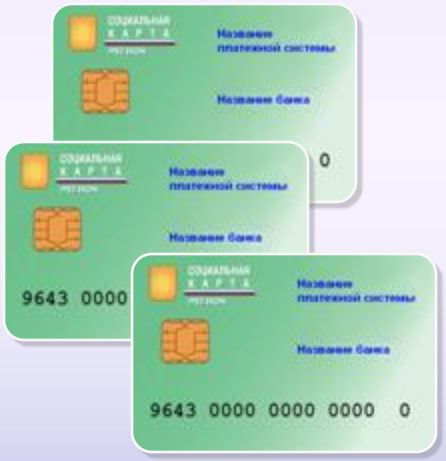
- Социальная карта
- Электронный идентификатор Общероссийского государственного информационного центра (ОГИЦ)
- Ключевой носитель в инфраструктуре удостоверяющих центров

Росинформтехнологии

Приложения социальной карты

Обязательные приложения

- Социальное идентификационное приложение
  - Аутентификация СК в системе
  - Аутентификация персональных идентификационных и социальных данных
  - Идентификация держателя СК в Системе
- Приложение ЭЦП
  - Идентификация и аутентификация владельца
  - Юридически значимое подтверждение операций



Дополнительные приложения

- Платежное приложение
- Транспортное приложение
- Медицинское приложение
- Ведомственные (корпоративные) приложения
- ...

ПрограмПарк

Спасибо за внимание!

Росинформтехнологии

ПрограмПарк

Адрес: Москва, ул. Сущевский вал, д. 16, стр. 5.

Тел./факс: +7 (495) 660-3295

E-mail: z@programpark.ru

Докладчик: Зырин Николай Владимирович

Директор ООО «ПрограмПарк»