sitronics
микроэлектроника

конференция
РусКрипто'2013
http://www.ruscrypto.ru/conference/

Карточная криптография в решениях – от поставщика карточных платформ

Константин Яковлевич Мытник
начальник отдела смарт-карт ОАО «НИИМЭ»

mkron

март 2013

Смарт-карты вокруг нас

sitronics
микроэлектроника

Задачи смарт-технологий

- Обеспечить идентификацию и верификацию владельца
- Обеспечить безопасное хранение, обработку и передачу данных владельца
- Гарантировать соблюдение интересов провайдера приложения в процессе выполнения операции
- Предоставить владельцу криптографические сервисы (генерацию электронной подписи)

Структура универсальной электронной карты

Обязательные приложения

- **Идентификационное приложение УЭК (ИД-приложение)**
- Банковское приложение ПРО-100
- Домен безопасности (служебное приложение)

Дополнительные приложения

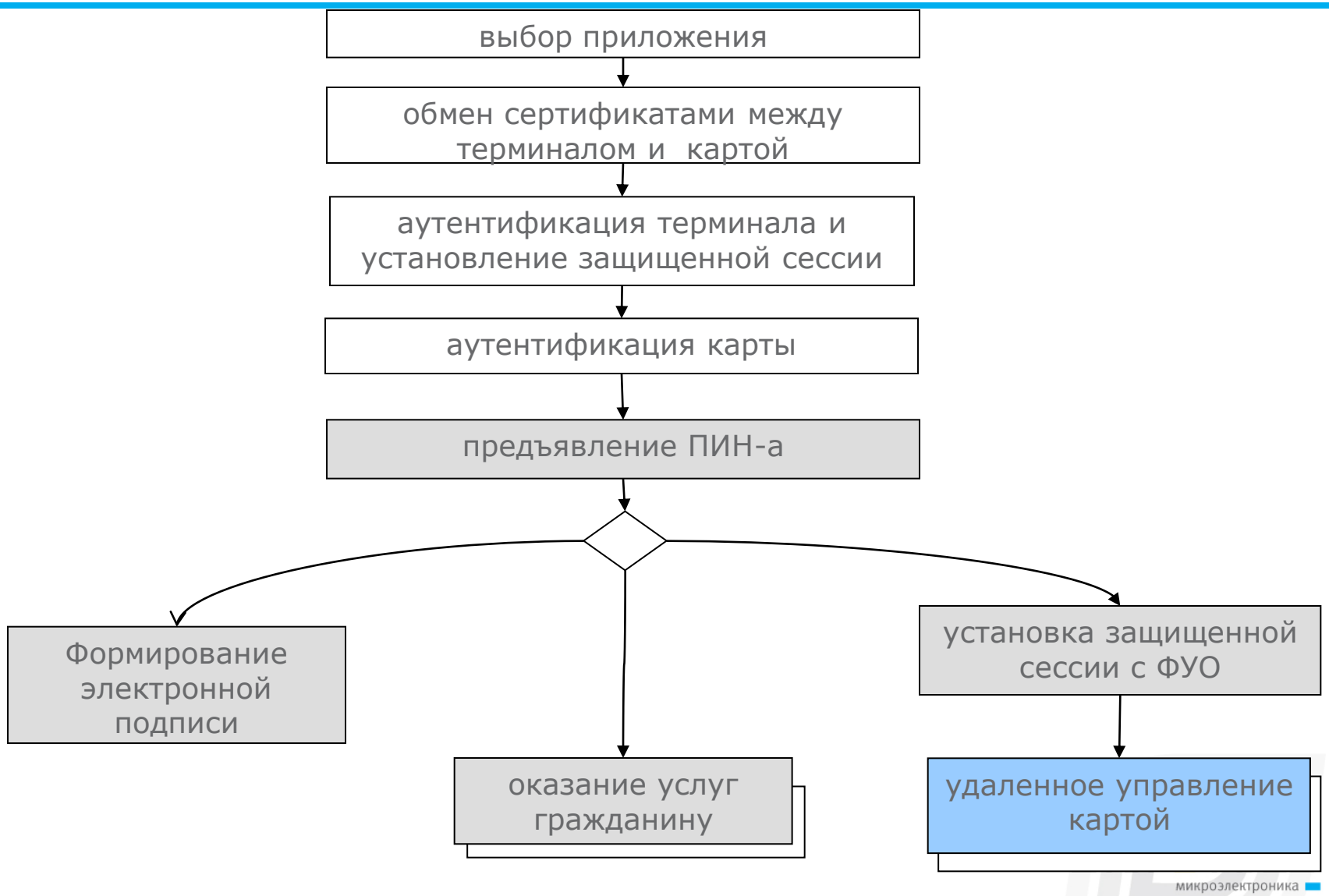
- Транспортное приложение
- Дополнительное банковское приложение (MasterCard)
- Региональные приложения

sitronics
микроэлектроника

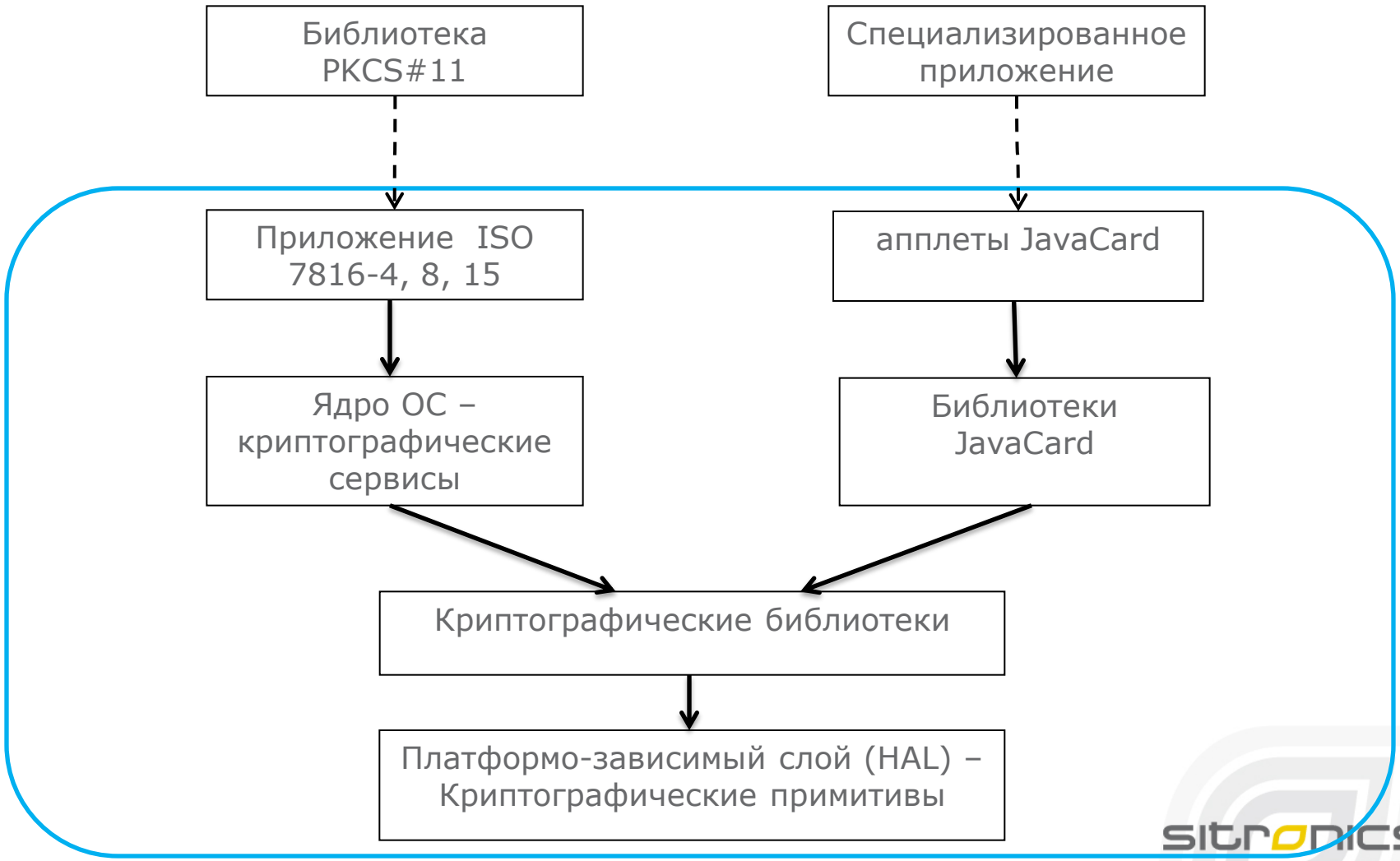
Криптографические механизмы ИД-приложения УЭК

- Взаимная аутентификация и выработка сессионных ключей с использованием PKI.
- Обеспечение защищенного канала передачи информации
- Генерация электронной подписи владельца

Типичный сценарий использования ИД-приложения УЭК



Архитектура криптографического приложения



Сценарий разработки приложения на основе ISO 7816

- Спроектировать приложение
  - Распределить элементы данных по файлам
  - Определить требования к ключам и протоколам
- Определить политику безопасности
  - Настроить систему разграничения доступа к данным и ключам
  - Определить назначение ключей и допустимые режимы работы
  - Настроить среду безопасности (связать протоколы с конкретными ключами)
- Разработать процедуру инициализации приложения (создание файлов данных и ключей)
- Разработать процедуру персонализации приложения
- Разработать приложение для терминала, опирающееся на стандартные библиотеки (PKCS#11 или аналогичные)

Сценарий разработки приложения на Java Card

- Спроектировать интерфейс приложения
- Разработать апплет
  - Реализовать базовые алгоритмы и контейнеры для хранения данных
  - Реализовать систему разграничения доступа
  - Реализовать бизнес-логику
  - Внедрить дополнительные меры защиты от инженерных атак
  - Провести отладку и тестирование
- Разработать процедуру персонализации приложения
- Разработать приложение для терминала согласно спецификации на интерфейс приложения

Перспективы индустрии приложений для смарт-карт

- Стандартизация протоколов
- Расширение и стандартизация API для JavaCard
- Развитие инструментальных средств
- Рост профессионализма разработчиков приложений
- Формирование рынка приложений для смарт-карт

sitronics
микроэлектроника

Спасибо за внимание

mkron