РУТОКЕН

конференция
РусКрипто
17-20 марта 2015

# Криптография на мобильных платформах: чтим традиции в новой реальности


Иванов Владимир
Директор по развитию

Мещеряков Кирилл
Менеджер по продуктам


Компания Актив

# О чем поговорим

- История вопроса
- О криптографических модулях
- О регуляторах
- О ключевых носителях
- Об архитектуре
- Как жить дальше?

# И сотворил Apple iPad

- **Устройства для массового рынка**
  - Досуг и развлечения
  - Учеба
  - Работа?
- **Pax Americana**
  - Без региональной криптоспецифики
  - Без легальной возможности её встроить

# Чего хотят пользователи

- Криптография? Что это?
- Сохранение традиционно хорошего UX/UI
- Котики

# Приложения

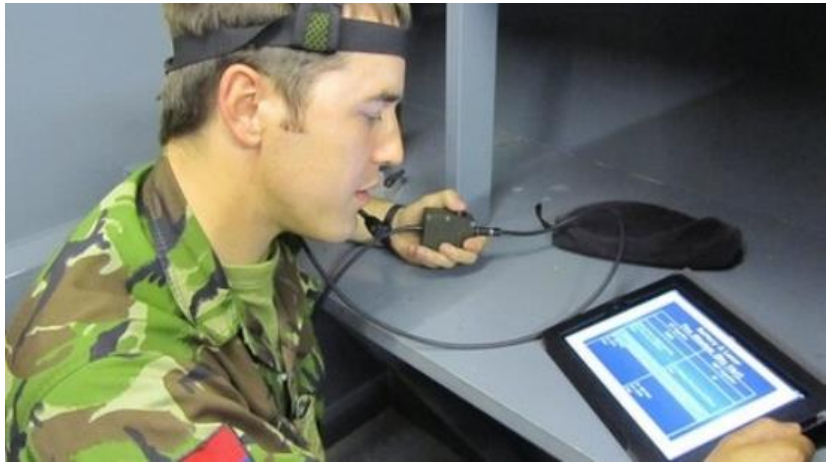
## Общесистемные


- Почта, Контакты, Календарь
- VPN клиент
- RDP клиент

## Клиенты прикладных систем

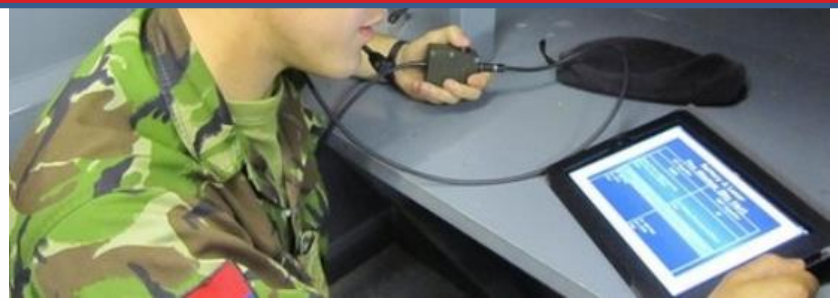
- Клиент ЭДО
- Клиент ERP
- Клиент ДБО

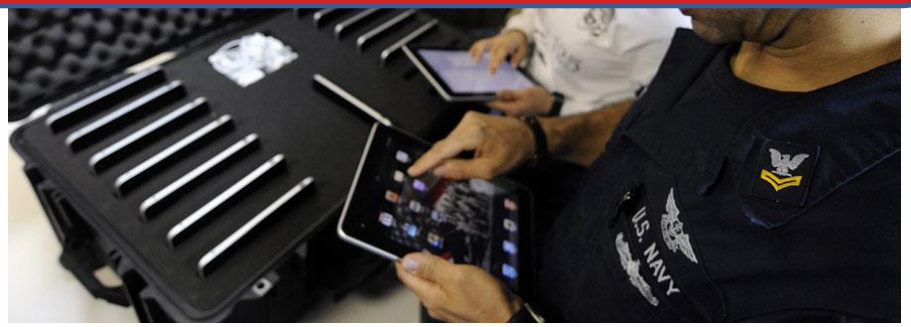
# Лучшее – детям!

# Лучшее – детям!


## А вот FIPS 140-2 вам!





# Чего не хватает для FIPS 140-2?

- Сертифицированные (доверенные) криптосредства
- Носители ключевой информации

# Криптографический модуль

# Носители ключевой информации

- **Условно отчуждаемые**
  - microSD
  - SIM
- **Отчуждаемые на контактном интерфейсе**
  - USB-токены
  - Смарт-карты
- **Отчуждаемые бесконтактные**
  - Смарт-карты с беспроводным считывателем
  - Bluetooth-токены
  - NFC

# Ключевые носители




# Ключевые носители

Made for iPad


Case iPad mini / Retina (TSS-PK11)
Case iPad 2/3 (TSS-PK12)
Case iPad Air (TSS-PK13)

Made for iPod iPhone iPad



Plug-in – Lightning (TSS-PK7)

Plug-in – 30-pin (TSS-PK8)

FEITIAN
WE BUILD SECURITY

# Ключевые носители



# Ключевые носители

Made for iPhone

# Мобильное устройство в качестве ключевого носителя

- **Изоляция приложений и данных**
- **Шифрование данных приложений**
- **Хранение ключей и сертификатов**
  - iOS Keychain
  - Защищенное хранилище Android
- **Виртуальная смарт-карта?**
  - Charismatics Enigma
  - Indeed AirKey

# Аутентификация пользователя мобильного устройства

- Slide to unlock
- Цифровой код
- Графический код
- «Сильный» пароль
- Распознавание лица
- Отпечаток пальца

следующий уровень

- Отчуждаемый ключевой носитель

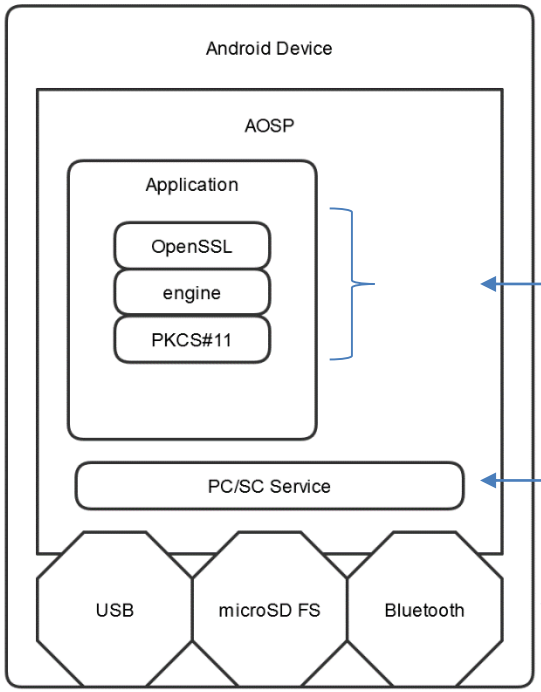
# Биометрическая аутентификация

-Как же можно с человека снять FIPS незаметно?
- Можно. Я не знаю, как они будут действовать, но человека можно оглушить, напоить, усыпить.
**В общем - с бесчувственного тела**.
Наконец, с трупа!
- С чьего... трупа?
- Но я уверен, что до этого не дойдёт!

# Зачем отчуждать ключевые носители?

- Больше риск лишиться устройства
- Меньше копий ключей и сертификатов
- Ключи могут быть неизвлекаемыми
- Соблюдение требований регулятора
- Ощущение безопасности у пользователя

# Архитектура на Android

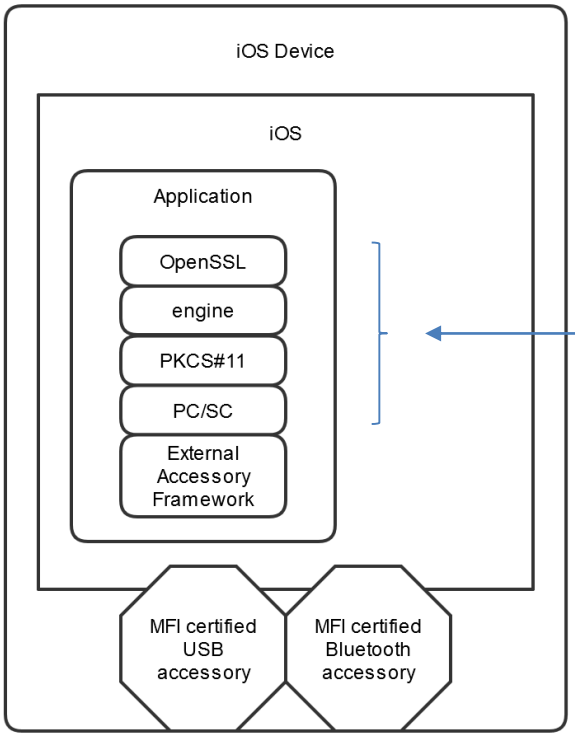



Проверяемый криптомодуль

PC/SC стек или аналог

Системные компоненты

# Архитектура на iOS




Проверяемый криптомодуль

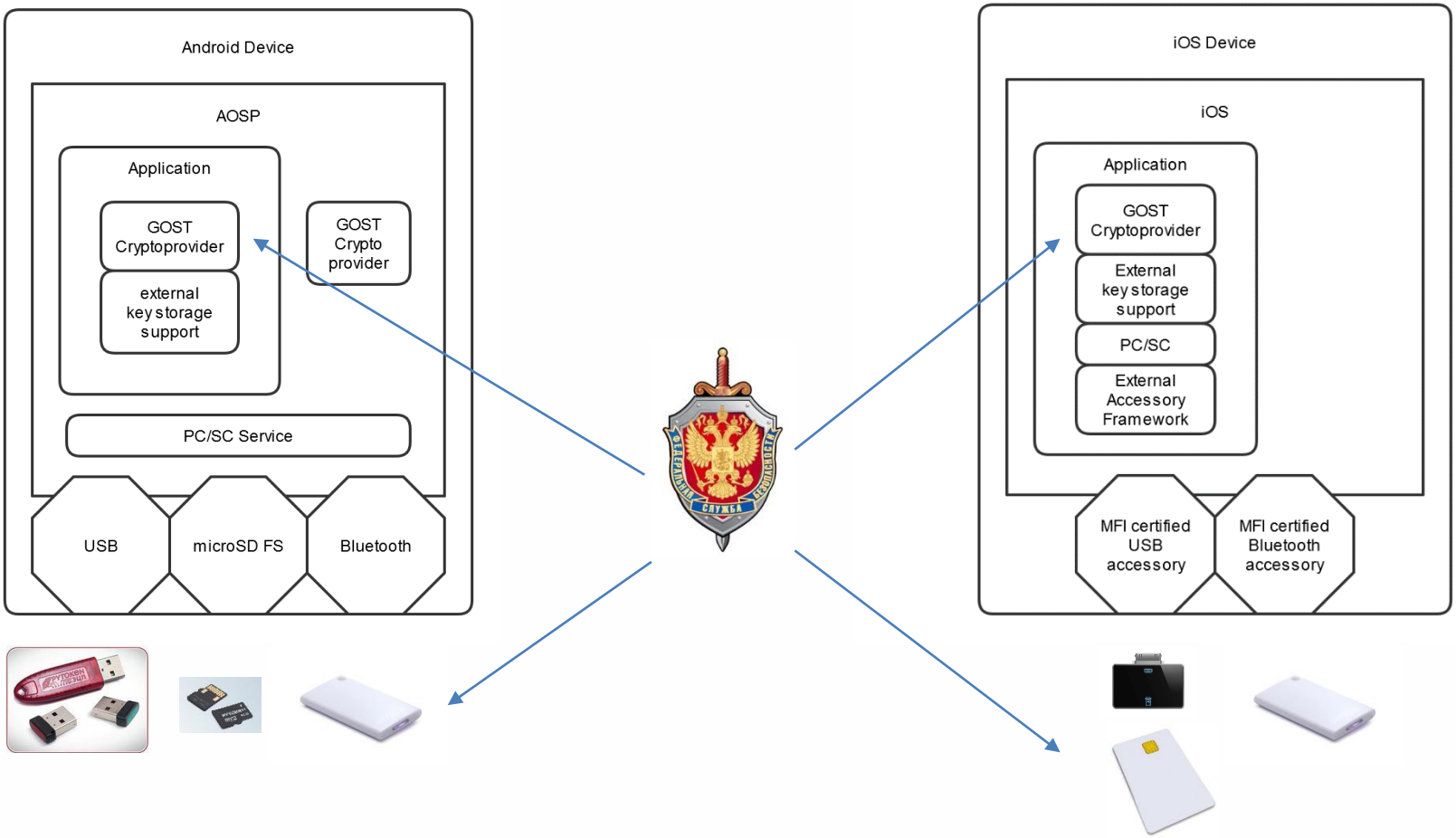
Системные компоненты


# ГОСТ-алгоритмы на Android и iOS

Пока противник рисует карту наступления, мы меняем ландшафты, причем вручную!

- **152 приказ ФАПСИ**
- **Сертификация по КС2**

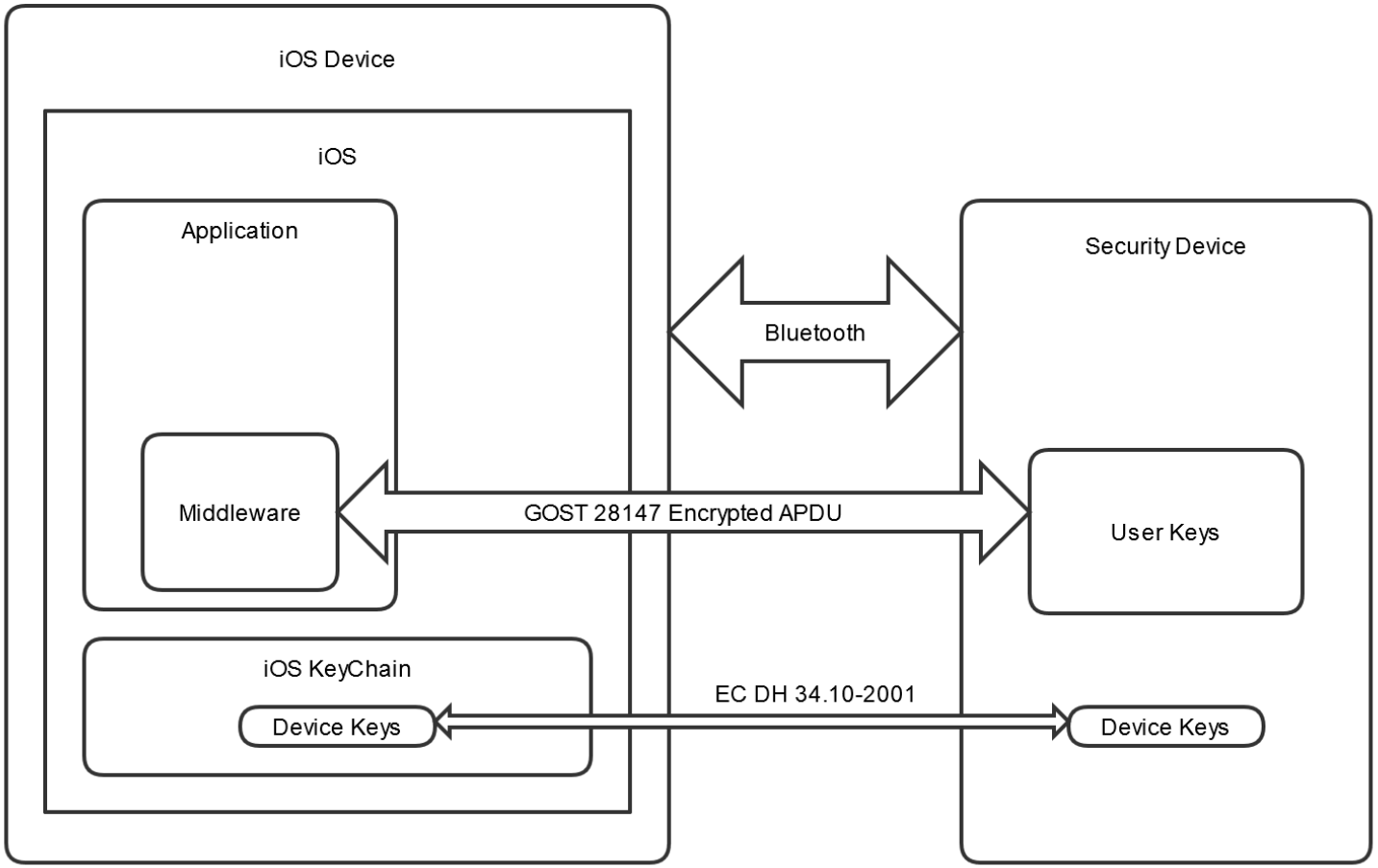
# Архитектура с поддержкой ГОСТ на Android и iOS



# Варианты

- USB неудобно
  - Что-то торчит (легко сломать, портит вид)
  - Громоздкий чехол
  - Трудно вставлять и вынимать
- microSD извлекаемый лишь «условно»
  - к многим устройствам неприменимо, Apple – 100%
- Bluetooth – небезопасно?

# Защита Bluetooth-канала



# Защита Bluetooth-канала

РУТОКЕН

# Приложения

## Общесистемные

- Почта, Контакты, Календарь
- VPN клиент
- Облачное хранилище


## Клиенты прикладных систем

- Клиент ЭДО
- Клиент ERP
- Клиент ДБО


# Разработка защищенных приложений

**Приложение с встроенной «навесной» криптографией обычно выглядит примерно так ☺**

# Приложений мало?!

Искусство по-прежнему в большом долгу!

РУТОКЕН

# Вопросы

# Контактная информация


## Электронная почта:

Общие вопросы – info@rutoken.ru

Тех.поддержка – hotline@rutoken.ru

Отдел продаж – sales@rutoken.ru

## Сайты:

www.rutoken.ru

www.aktiv-company.ru

## Телефон:

(495) 925-77-90