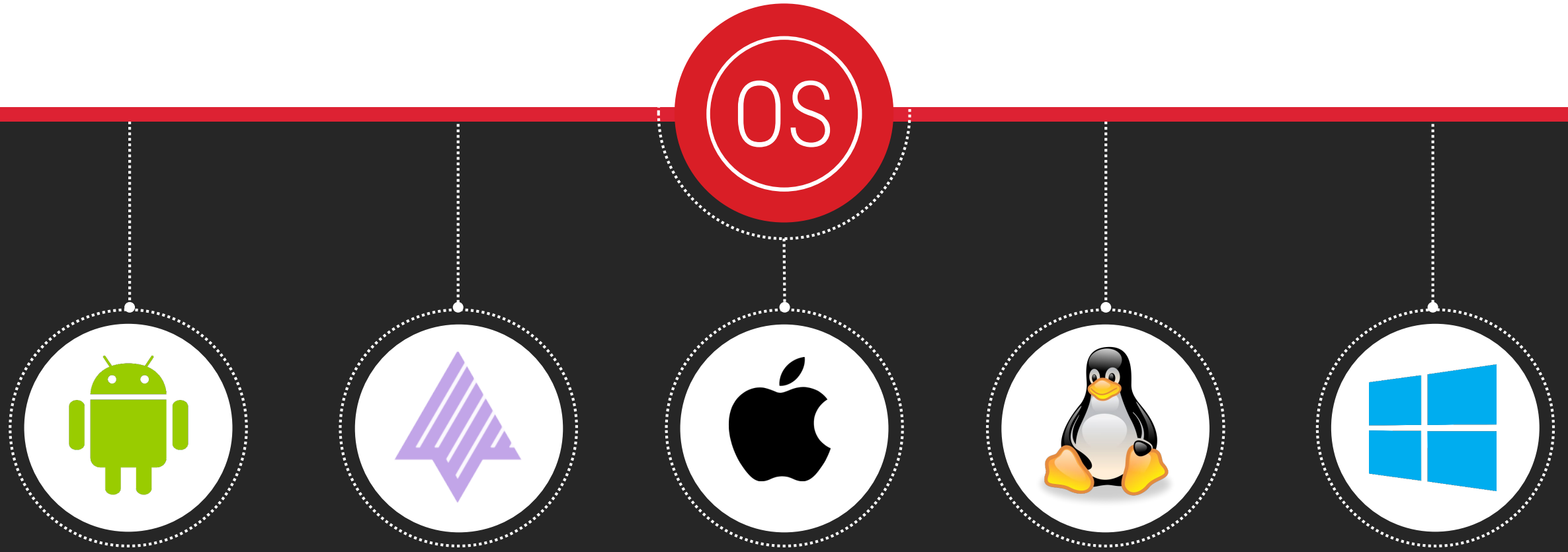
XXIII международная конференция
«РусКрипто'2021»

РУТОКЕН

Программно-аппаратные решения Рутокен для мобильных платформ

Владимир Иванов
Директор по развитию
Компания «Актив»

Операционные системы



Типы мобильных устройств

Смартфоны

Планшеты

Мобильные терминалы

POS-терминалы

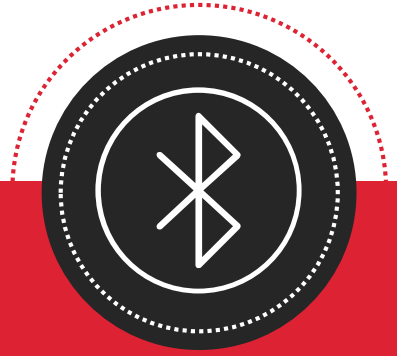
Терминалы сбора данных

Кассовые аппараты

Актуальные задачи для мобильных устройств

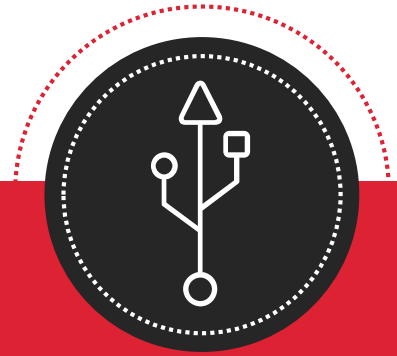
- Подписывать электронные документы вне офиса
- Хранить и использовать ключи подписи и аутентификации безопасным способом
- Подписывать электронные документы в автономном режиме или в условиях ограниченной связи
- Учитывать специфические условия окружающей среды
- Обеспечивать подпись «живым» пользователем
- Обеспечивать возможность работы нескольких пользователей на одном мобильном устройстве

NFC vs...



- Стоимость
- Оверхед
- Настройка и сопряжение
- Радиус действия
- Питание

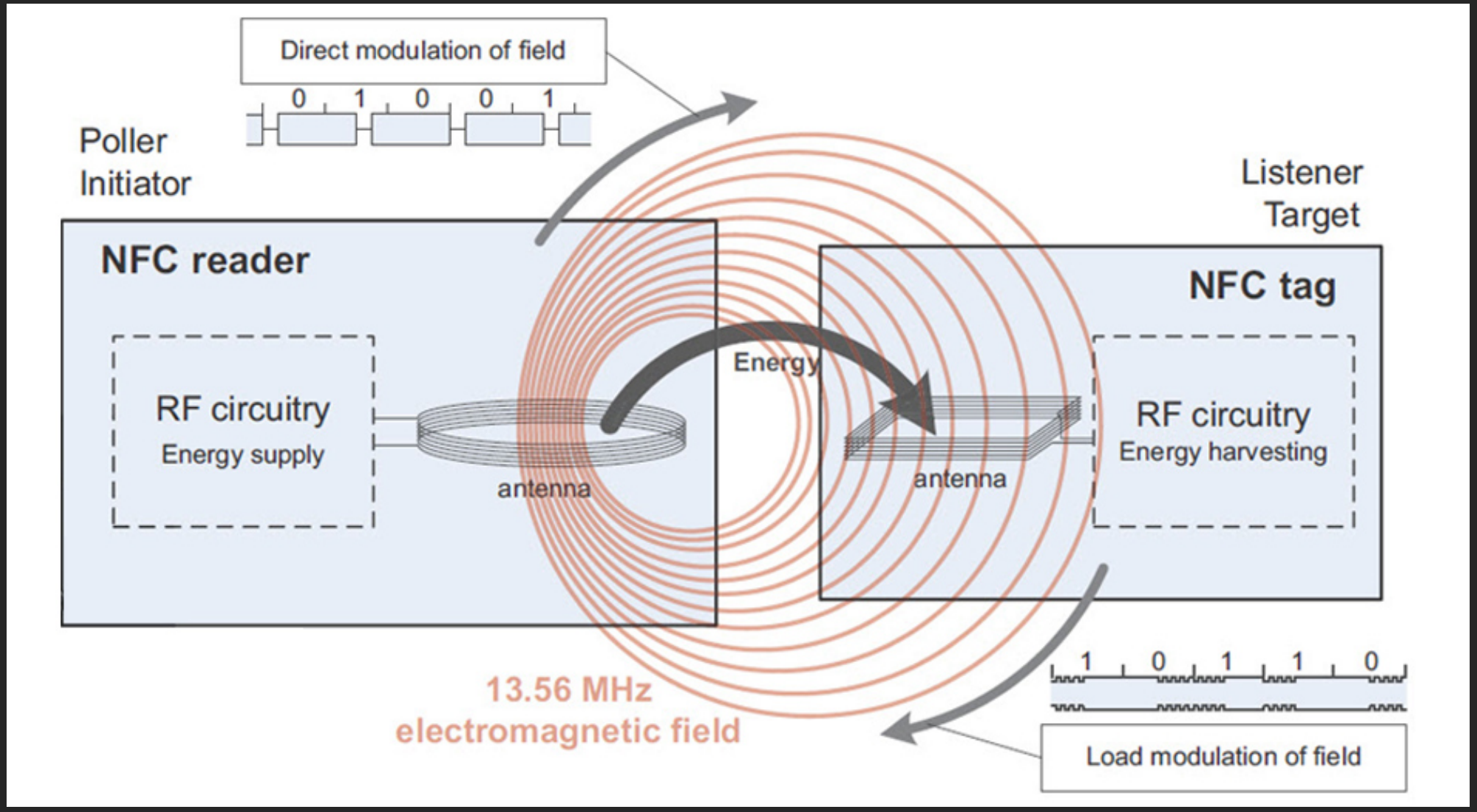
- Стоимость
- Радиус действия
- Питание



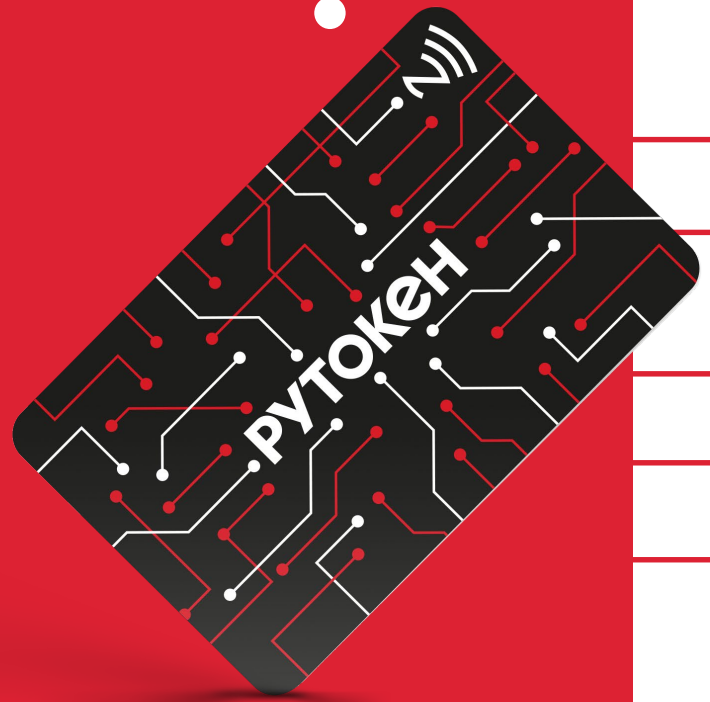
- Бесконтактная работа
- Ничего не торчит и не обламывается

- Не нужна камера (задержки, освещение, заняты руки)
- Много данных, можно менять

NFC — как это работает?



Дуальная смарт-карта
Рутокен ЭЦП 3.0 NFC



- Подпись касанием карты к мобильному устройству или считывателю
- Криптография на борту на неизвлекаемых ключах
- Производительность через NFC канал не хуже, чем через контактный интерфейс
- Не требует процедуры сопряжения
- Питание через интерфейсы
- Использование на мобильных устройствах (Android, iOS, Аврора) бесконтактно
- Использование на ПК бесконтактно и контактно
- Секреты хранятся отдельно от приложений и документов

Как взаимодействовать с NFC-картой

SDK Рутокен

PKCS#11

SDK КриптоПро CSP 5.0 R2

CryptoAPI

Новое в SDK Рутокен для NFC-карт

В комплекте разработчика (Рутокен SDK) рассмотрены и описаны большинство возможных сценариев встраивания устройств и программного обеспечения Рутокен

Приложения в исходных кодах для удобства встраивания:

Мобильный банк

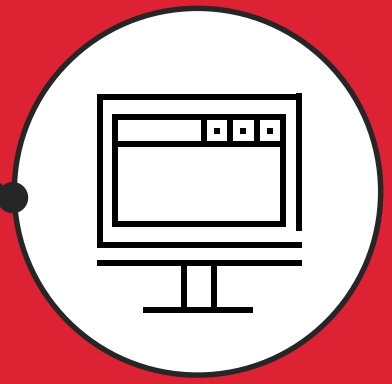
Работа с документами и эл. подписью несколькими людьми на одном устройстве

КриптоПро CSP 5.0 R2

КРИПТОПРО
РУТОКЕН

Мобильные устройства Android 7+, iOS 13+, Аврора, Astra Linux

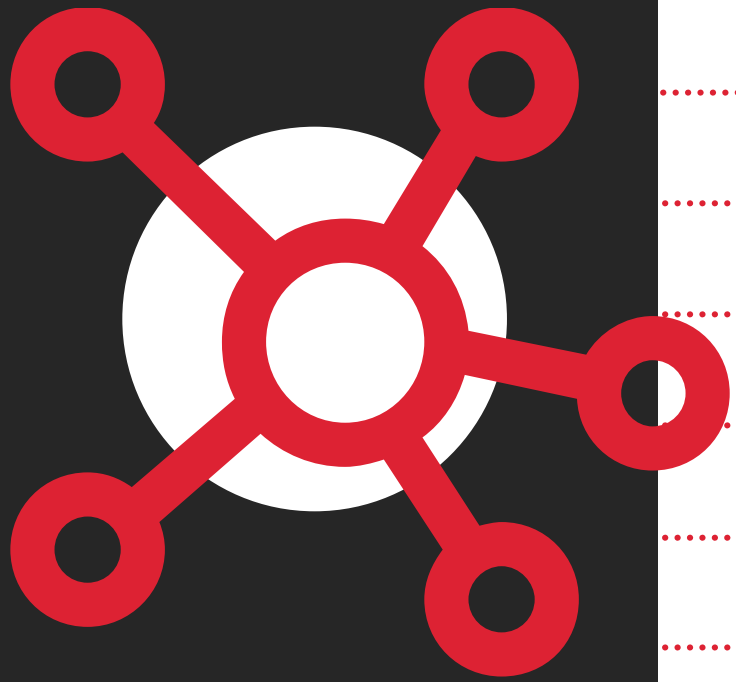
Бесконтактная работа, ГОСТ-криптография с неизвлекаемыми ключами



Настольные компьютеры с Windows, Linux, macOS

Контактная и бесконтактная работа с программными и неизвлекаемыми ключами

Области применения



- Цифровизация городского хозяйства
- Логистика, транспорт, складское хозяйство
- Оптовая торговля, поставки маркированной продукции
- Сельское хозяйство
- Биотехнологии, медицина, чистые помещения
- Сменная работа на одном мобильном устройстве
- Массовое обслуживание клиентов
- Промышленность

Электронное подписание документов

Электронная подпись и шифрование файлов на любых платформах

Преимущества использования Рутокен ЭЦП 3.0 NFC:

- Универсальная работа на мобильный устройствах и настольных ПК
- Ключи доступа хранятся отдельно от приложения
- Криптография на борту на неизвлекаемых ключах

РУТОКЕН

КриптоАРМ ГОСТ

infotecs

ViPNet PKI Client

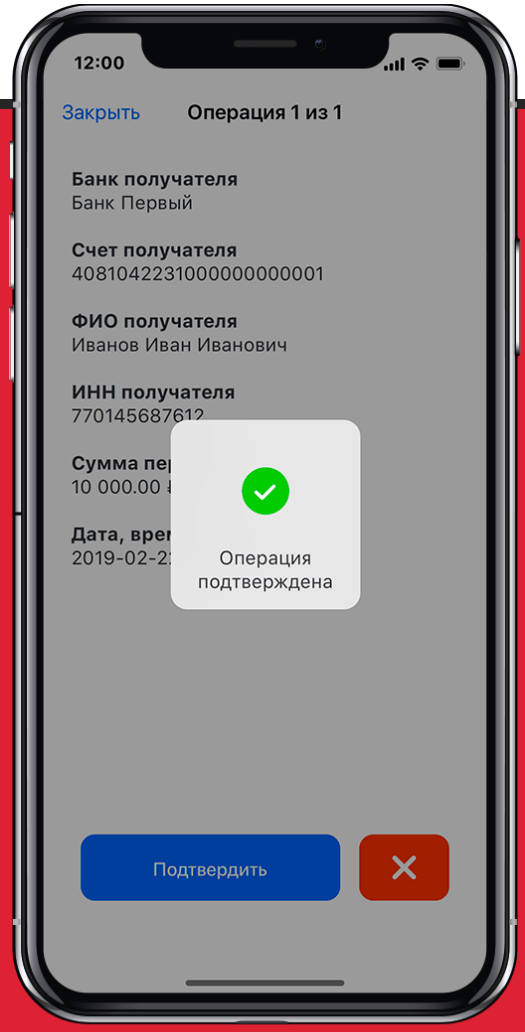
Замена PUSH/SMS

Подтверждения пользователем операций
в банковских системах

PayControl
РУТОКЕН

Преимущества использования Рутокен ЭЦП 3.0 NFC:

- Безопасное и быстрое подтверждение операций без ожиданий и ввода кодов
- Подтверждение содержит информацию о документе и авторстве
- Эл. подпись хранится отдельно от приложения



Автоматизация аптек и медицинских кабинетов

клеверенс
РУТОКЕН

Для контроля движения товаров нужны подписанные передаточные документы

Преимущества использования Рутокен ЭЦП 3.0 NFC:

- Ускорение и оптимизация бизнес-процессов
- Удобство
- Смарт-карта как средство эл. подписи
- У каждого сотрудника свой ключ подписи

Корпоративная мобильность

ЭНЕРГИЯ ЭФФЕКТИВНЫХ РЕШЕНИЙ

Mobile Inform Group

РУТОКЕН

Мобильная электронная подпись заменяет бумажный документооборот каждый день

Преимущества использования Рутокен ЭЦП 3.0 NFC:

- Смарт-карта - средство эл. подписи «в полях» и рабочий пропуск
- Избавляет офис от бумаг
- Не требует физического подключения
- Надежность и производительность
- Секреты хранятся отдельно от приложения

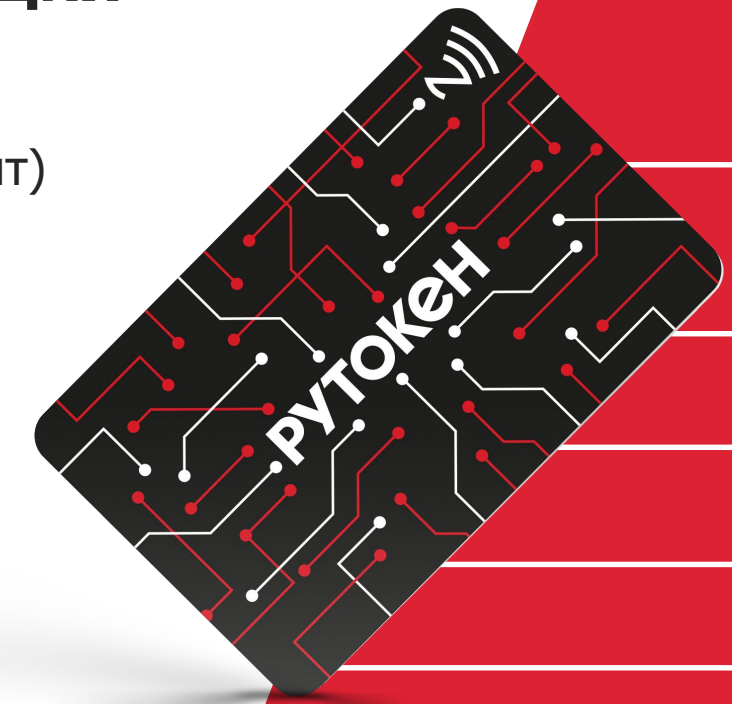
Применение:

- Энергетика
- Транспорт
- Системы здравоохранения
- Государственные органы
- Промышленность

Характеристики
Рутокен ЭЦП 3.0 NFC

Аппаратная реализация криптографии:

- ГОСТ 34.10-2012 (256/512 бит)
- ГОСТ 34.11-2012
- VKO GOST
- ГОСТ Р 34.12-2015 Магма
- ГОСТ Р 34.12-2015 Кузнечик
- RSA 1028, 2048, 4096 бит
- ECDSA с кривыми secp256k1 и secp256r1



- Совместимость с современными ОС, включая отечественные и мобильные
- Совместимость с криптопровайдерами
- Защита NFC-канала (SESPAKE)
- Высокая производительность
- SDK для встраивания

Дайджест

Средства разработки:

- Рутокен SDK
- КриптоПро CSP 5.0 R2

Готовые решения:

- Клеверенс — автоматизация инвентаризации
- VipNet PKI Client — подписание/шифрование/ ГОСТ-TLS
- PayControl — замена PUSH/SMS
- КриптоАРМ ГОСТ — подписание/шифрование

Комплекс решений:

- Mobile Info Group и СИГМА — корпоративная мобильность

Как работать с NFC картой

Перспективные устройства Рутокен для мобильных платформ

Рутокен ЭЦП 3.0 USB+NFC

- Все возможности Рутокен ЭЦП 3.0
- Традиционное подключение через USB
- Не нужен считыватель контактных смарт-карт

Рутокен ЭЦП 3.0 BLE

- Все возможности Рутокен ЭЦП 3.0
- Работает с iPad (у него нет NFC)
- BLE 5.X – высокая скорость и низкое энергопотребление
- Интерфейс USB Type-C
- Меньше габариты
- Высокое удобство — нет кнопок, держит соединение и т.д.
- Защищенный канал передачи

Контактная информация

Владимир Иванов

vov@rutoken.ru
info@rutoken.ru

www.rutoken.ru
www.aktiv-company.ru

+7 495 925-77-90

РУТОКЕН