PKI Forum 2021
15 сентября 2021, Санкт-Петербург

Как аппаратными решениями усилить мобильную подпись. Рутокен ЭЦП 3.0

PKI Форум
Россия 2021

Владимир Иванов
Директор по развитию
Компания «Актив»

КОМПАНИЯ АКТИВ

Хранения ключа подписи в мобильных приложениях

1

- Память мобильного устройства
- Ключ подписи не зашифрован
- Подпись в приложении на мобильном устройстве

2

- Память или Secure Enclave мобильного устройства
- Ключ подписи зашифрован
- Подпись в приложении на мобильном устройстве

3

- Удаленный HSM
- Ключи подписи зашифрован средствами HSM
- Подпись на сервисе дистанционной подписи

4

- Ключевой носитель
- Ключ подписи зашифрован средствами CSP
- Подпись в приложении на мобильном устройстве

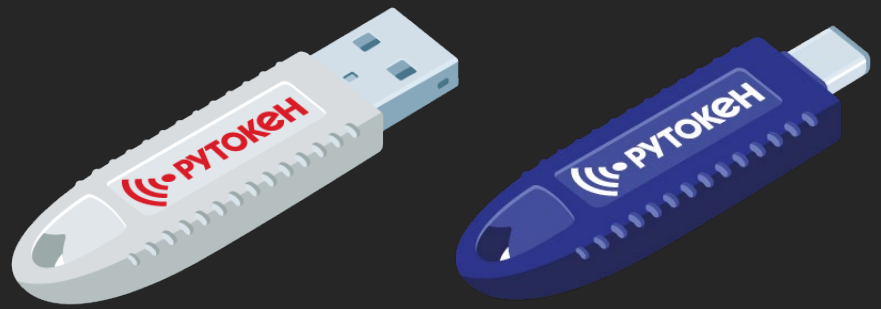
Основы поколения Рутокен 3.0

- Высокоскоростное криптоядро на производительном микроконтроллере
- Криптоалгоритмы ГОСТ 34.10-2012, ГОСТ Р 34.10-2015 «Магма» и «Кузнечик», ECDSA
- Электронная подпись на смартфоне за долю секунды с защитой канала SESPAKE (RFC 8133)
- SDK и middleware высшего качества для всех платформ

Смарт-карта Рутокен ЭЦП 3.0 NFC

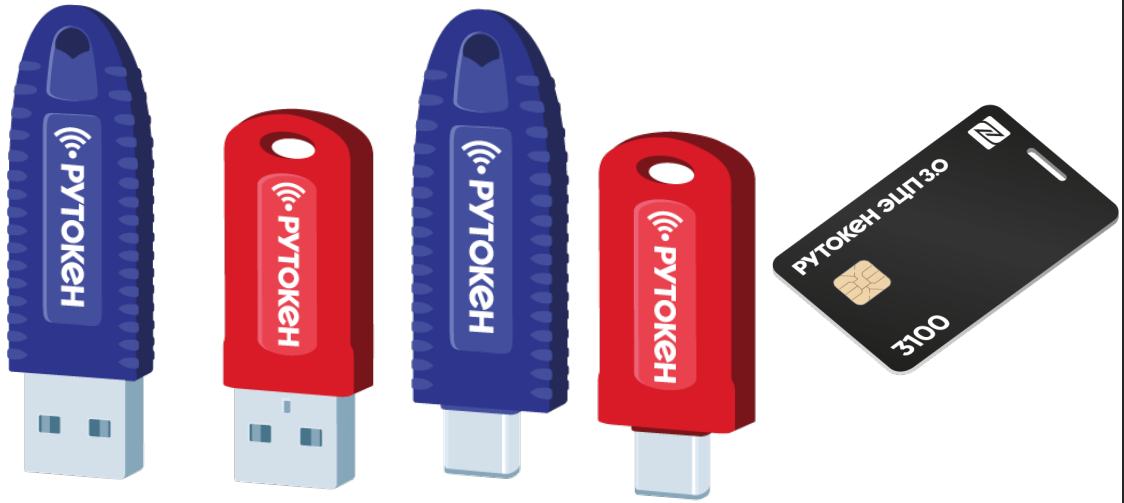
- Дуальные смарт-карты для широкого применения
- Уже работает с десятками партнерских решений на мобильных ОС
- И с сотнями решений на настольных платформах

USB-токен Рутокен ЭЦП 3.0 NFC



- Единое устройство для ЭП на всех настольных и мобильных платформах
- Полная совместимость с интеграциями Рутокен ЭЦП 2.0
- Классическое исполнение или интерфейс Type-C

Бесконтактные технологии Рутокен



Единое устройство – для всех мобильных и настольных ОС

iOS

1. Рутокен ЭЦП 3.0 NFC: мощные технологии в разном исполнении
2. Новая Рутокен ОС и криптоядро: ускорение операций в 2–10 раз
3. Обратная совместимость: работает везде, где поддерживается Рутокен ЭЦП 2.0
4. Проходит сертификацию ФСТЭК и ФСБ:

Как можно усилить имеющиеся решения

1

Хранение ключей подписи и аутентификации на NFC устройстве

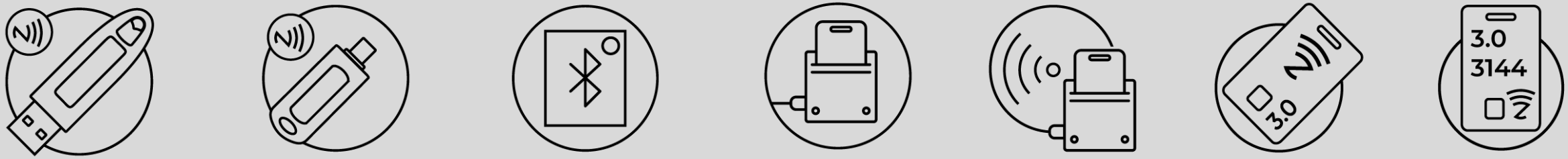
2

Построение защищенного канала (выработка сеансовых ключей, например) до сервиса подписи

3

Вычисление подписи на неизвлекаемых ключах

Криптографическая аутентификация на удаленных сервисах



РКП Форум
Россия 2021

КОМПАНИЯ АКТИВ

Владимир Иванов

info@rutoken.ru

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

+7 495 925-77-90