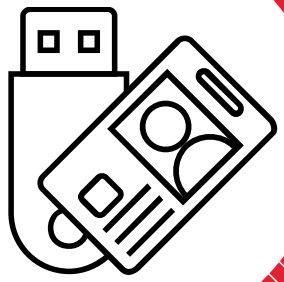
РУТОКЕН

infotecs

Технологии Рутокен в российских продуктах информационной безопасности на примере решений ViPNet



Шпаков Андрей

Руководитель проектов по информационной безопасности
Компания «Актив»

Компания «Актив»

guardant

РУТОКЕН

AKTIV. CONSULTING

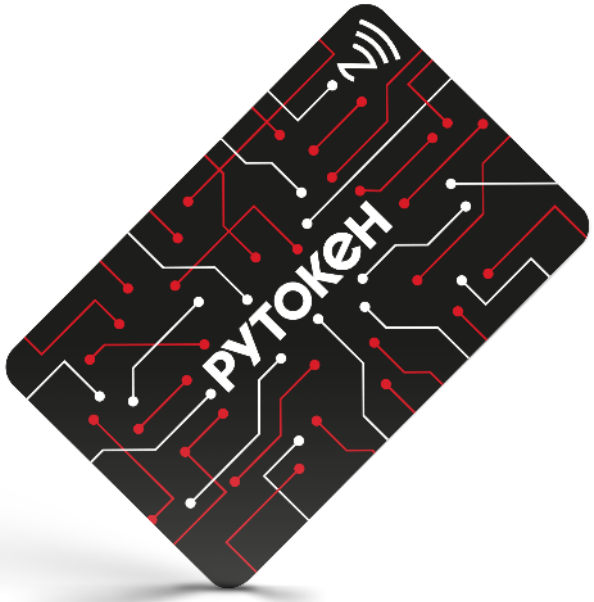
На рынке информационной безопасности с 1994 года

Имеем все необходимые лицензии на разработку СКЗИ и СЗИ

Являемся членом АЗИ, РОСЭУ, ТК26, ТК362, РусКрипто, АПКИТ, АБИСС

Три направления бизнеса

Форм-факторы и назначение Рутокен



Смарт-карта

USB-токены

- Хранение ключевой информации (PKI)
- Расширенная пользовательская аутентификация
- Электронная подпись

Виды токенов по типу выработки ключа

Пассивные —

используются для хранения ключа (а не генерации).

Рутокен Lite

Активные —

генерируют ключ средствами микроконтроллера. Ключи в таких токенах — неизвлекаемые.

Линейка Рутокен ЭЦП

Активные токены позволяют использовать ключ подписи — 3 года!

Что внутри Рутокен ЭЦП 3.0

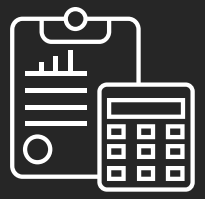
- Скоростное криптоядро на защищенном микроконтроллере
- Разнообразные интерфейсы взаимодействия с устройствами (USB, NFC, BLE, ISO 7816, 14443)
- Единая ОС для разных исполнений СКЗИ Рутокен ЭЦП 3.0
- Работа на всех стационарных (Win, Linux, macOS) и мобильных (Android, iOS, Аврора) ОС с любой архитектурой (x86, ARM, MIPS, включая Эльбрус и Байкал)
- Современные криптоалгоритмы: Кузнечик, Магма, RSA-4096, ECDSA
- Сертификаты ФСБ России и ФСТЭК России
- Расширенные политики качества PIN-кодов

Типичные бизнес-кейсы использования

Работа выездных бригад (в т.ч. с мобильных устройств)

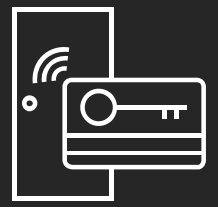
Доступ к ИТ-ресурсам (VPN, VDI)

Целостность и неоткрекаемость данных в IoT



Сдача налоговой отчетности

Участие в электронных торгах

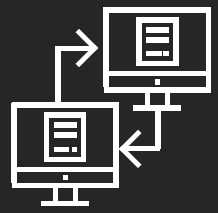


Единый пропуск в помещения

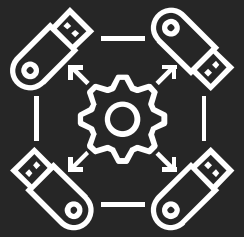
Для большинства задач используется CSP (eg. VipNet CSP)

Работа с ДБО

ЕГАИС



ЭДО



Актуальные и перспективные продукты Рутокен (2023)

Рутокен ЭЦП 3.0

Модели

- **3220**
- **3100 NFC**
- **Экспортный (на базе 3220)**
- **3250 (больше памяти, выше скорость)**

>160 КВ

Форм-факторы

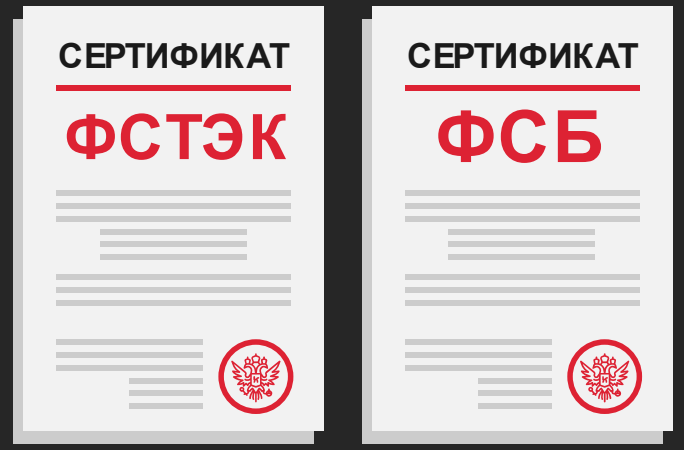
Полноразмерный USB-A. USB-Type C

Полноразмерный USB с NFC

Дуальные смарт-карты

- 3100 **NFC**
- **3100 NFC MF**
- **3100 SAM**

Сертификаты



- ФСБ России: КС1, КС2
- ФСТЭК России: УД-4

Рутокен ЭЦП 3.0 3220 SD

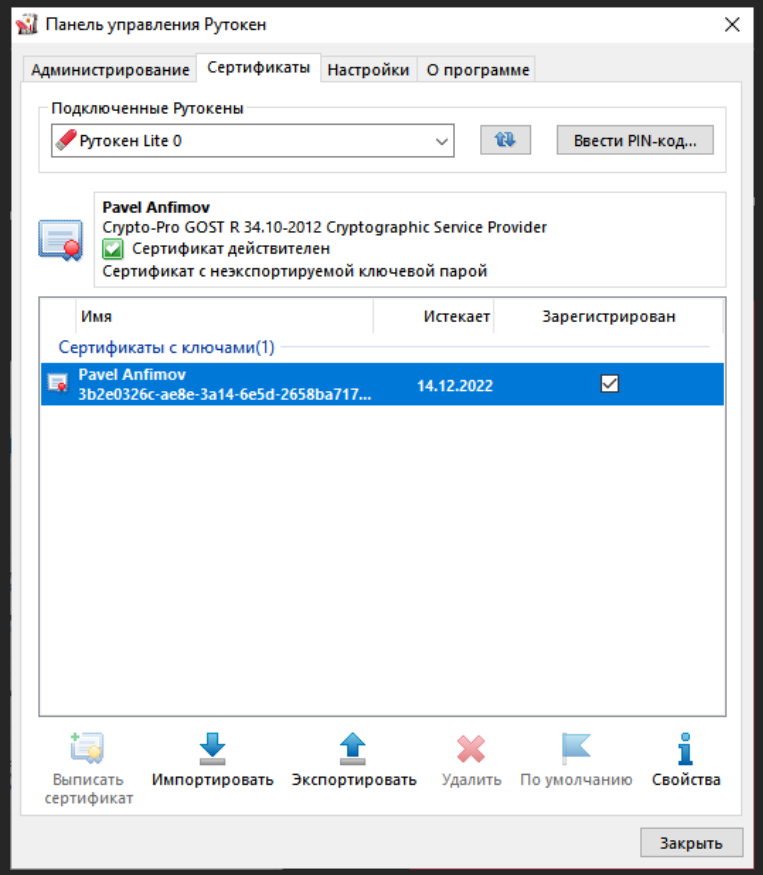
- Два устройства в одном
- Сертифицирован ФСТЭК России
- Уже в продаже

Семейство Рутокен ЭЦП 3.0 Flash

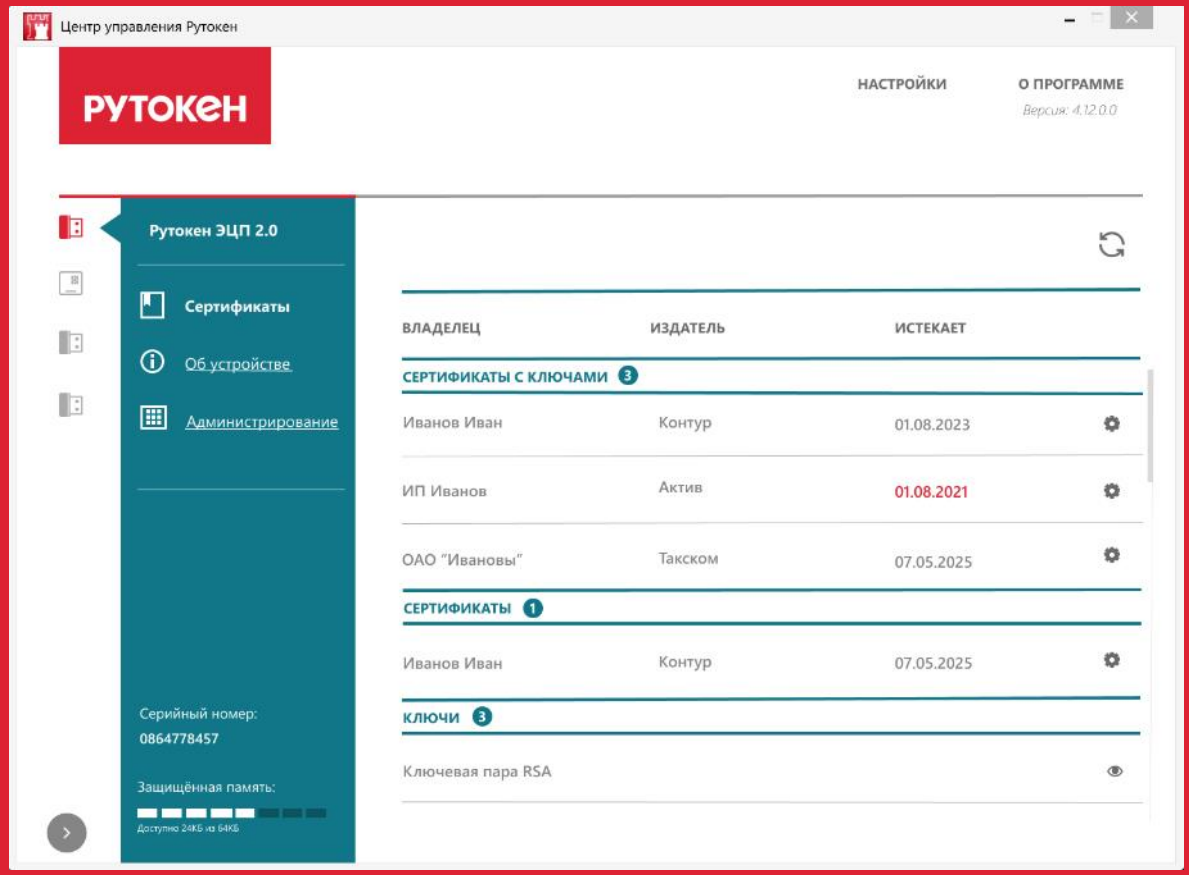
- Возможности Рутокен ЭЦП 2.0 Flash
- Обновление ОС Рутокен
- Аутентификация ПК перед устройством
- Журналирование событий безопасности
- Сквозное шифрование до 7мбит/с
  в отдельном исполнении

Центр Управления Рутокен

Было



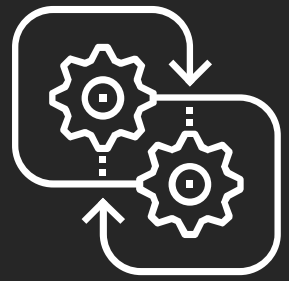
Стало



Аутентификаторы в семействе Рутокен

- Рутокен OTP – доп. Аутентификация в информационных системах
- Алгоритм OATH TOTP (RFC6238)
- Не требует связи с ПК/мобильным устройством для работы
- NFC-интерфейс для настройки
- Аппаратный таймер для подсчета времени

- Рутокен FIDO — устройство с поддержкой стандартов U2F/FIDO2 и HOTP
- Беспарольная аутентификация в веб-приложениях
- Замена ушедшим конкурентам и преемник текущей линейки
- Поддержка NFC в будущем



Совместные решения на основе продуктов Рутокен и ViPNet

Работа ViPNet CSP и Рутокен ЭЦП\Lite

Сценарии:

- Работа в системах ЭДО и сдачи отчетности (1С, TrustDoc, TrustTax)
- Вход в информационные системы:
  - Госуслуги
  - ЛК ФНС
  - Национальная система маркировки «Честный знак»

Преимущества для заказчика:

- Срок действия ключа ЭП — 3 года
  (в случае применения Рутокен ЭЦП)
- Увеличение уровня ИБ за счет хранения ключа отдельно от АРМ-а пользователя

Работа ViPNet PKI Client и Рутокен ЭЦП/Lite

Сценарии:

- Электронная подпись данных
- Шифрование файлов
- Построение TLS-соединений по ГОСТ-у (согласно спецификации ТК26)

Преимущества для заказчика:

- Срок действия ключа ЭП — 3 года (в случае применения Рутокен ЭЦП)
- Увеличение уровня ИБ за счет хранения ключа отдельно от АРМ-а пользователя
- Снижение затрат корпоративных клиентов на администрирование ключевой информации (за счет урежения частоты выпуска сертификатов)

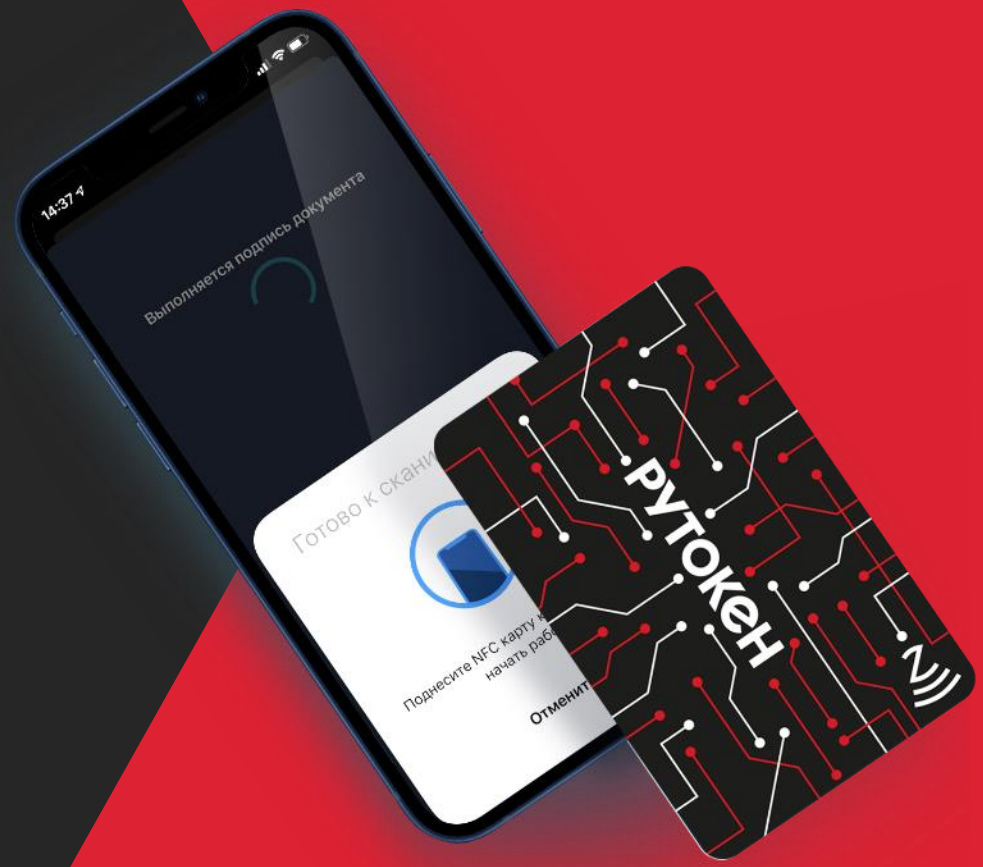
Мобильная электронная подпись

VipNet PKI Client (Android) + Рутокен ЭЦП 3.0

- Работа через USB-интерфейс
- Ключи доступа хранятся отдельно от приложения
- Панель управления Рутокен для Android

VipNet PKI Client (Android, iOS) + Рутокен ЭЦП 3.0 NFC

- Работа через NFC-интерфейс
- Ключи доступа хранятся отдельно от приложения
- Не требуются драйвера для iOS
- Панель управления Рутокен для Android



Интеграция ГОСТ-ов для разработчиков

Библиотека ViPNet OSSL

- Шифрование/Электронная подпись/Построение TLS-канала с акуальными криптоалгоритмами ГОСТ (Магма, Кузнечик)
- Актуальные криптоалгоритмы (Магма, Кузнечик)
- Любая ОС (Windows/Linux/macOS/Android/iOS)

Добавление Рутокен ЭЦП\Lite обеспечит:

- Работа через USB-интерфейс и **NFC-интерфейс**
- Двухфакторную аутентификацию пользователя на клиентской стороне.
- Срок действия ключа ЭП — 3 года (в случае применения Рутокен ЭЦП)

Аутентификация при контроле АРМ-ов

ViPNet SafeBoot 3.0 + Рутокен Lite/ЭЦП

- Двухфакторная аутентификация пользователя на этапе BIOS
- Локальная аутентификация администратора при конфигурировании МДЗ

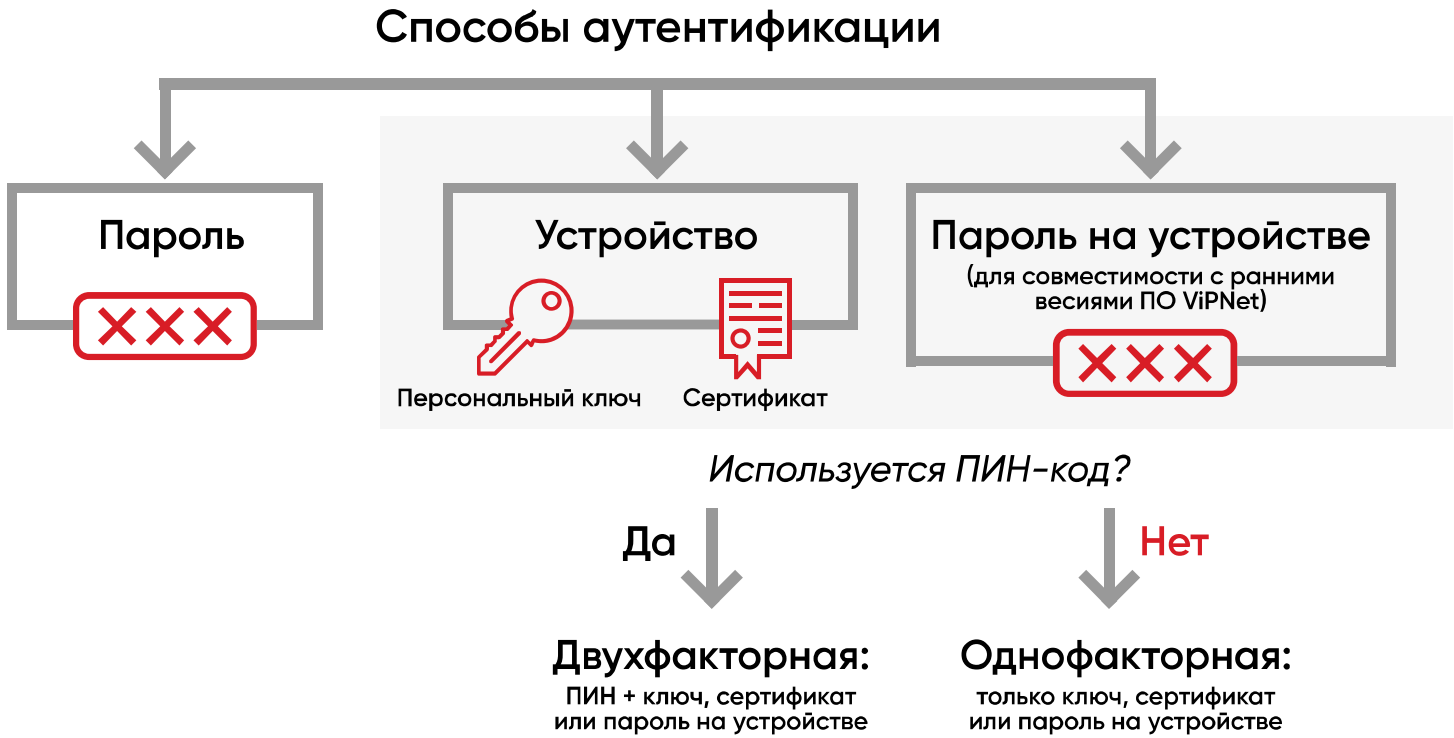
ViPNet SafePoint + Рутокен Lite/ЭЦП

- Двухфакторная аутентификация пользователя при входе в ОС
- Аутентификация администратора при конфигурировании средства защиты от НСД

Аутентификация пользователя в VPN-клиенте

ViPNet Client/Client 4U + Рутокен ЭЦП/Lite

- Хранение пароля для входа в клиент на токене
- Сертификат пользователя на токене (PKI)
- Администратор может записать ключ во время распределения клиентов
- Пользователь может сам записать ключ для установленного клиента



Контактная информация

Шпаков Андрей

Руководитель проектов по информационной безопасности Компания «Актив»

shpakov@rutoken.ru
info@rutoken.ru

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

+7 495 925-77-90
+7 916 518-70-26

Технологическая рассылка

РУТОКЕН