

Технологии Рутокен в российских продуктах информационной безопасности на примере решений ViPNet

Павел Анфимов
Руководитель отдела
продуктов и интеграций Рутокен
Компания «Актив»

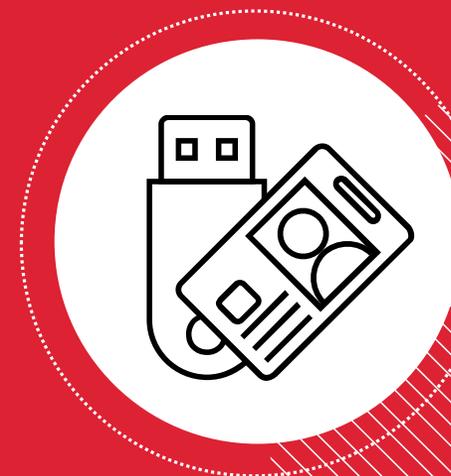


техно infotecs
2023 Фест
ТЕХНИЧЕСКАЯ
КОНФЕРЕНЦИЯ

Технологии Рутокен в российских продуктах информационной безопасности на примере решений ViPNet

Павел Анфимов

Руководитель отдела
продуктов и интеграций Рутокен
Компания «Актив»



Компания «АКТИВ»



РУТОКЕН

AKTIV.
CONSULTING



На рынке
информационной
безопасности
с 1994 года



Имеем все
необходимые лицензии
на разработку
СКЗИ и СЗИ

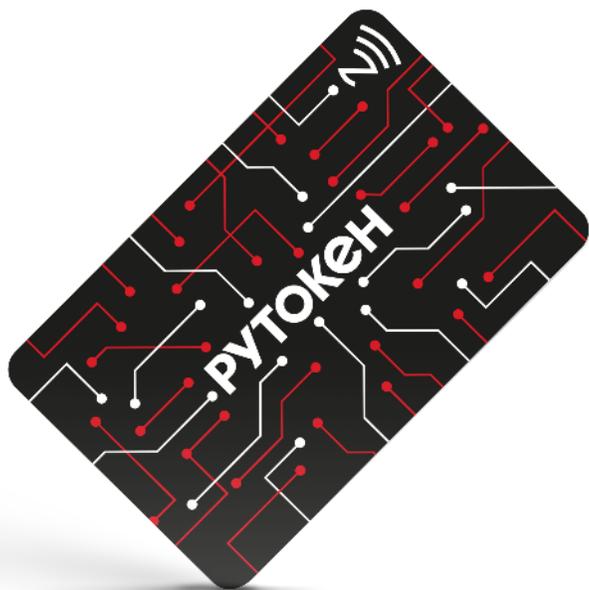


Являемся членом
АЗИ, РОСЭУ, ТК26,
ТК362, РусКрипто,
АПКИТ, АБИСС



Три направления
бизнеса

Форм-факторы и назначение Рутокен



Смарт-карта



USB-токены



Виды токенов по типу выработки ключа

Пассивные —

используются для хранения ключа (не генерации).

Рутокен Lite



Активные —

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

Линейка Рутокен ЭЦП 3.0



Активные токены позволяют использовать ключ подписи — 3 года!

Что внутри Рутокен ЭЦП 3.0

- Скоростное криптоядро на защищенном микроконтроллере
- Совместимость с Рутокен ЭЦП 2.0
- Единая ОС для разных исполнений СКЗИ Рутокен ЭЦП 3.0
- Работа на всех настольных и мобильных ОС



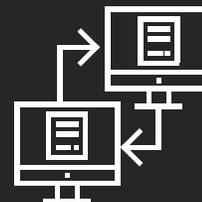
- Современные криптоалгоритмы: Кузнечик, Магма, RSA-4096, ECDSA
- Расширенные политики качества PIN-кодов
- Беспроводной канал NFC



Решения на базе **Рутокен**



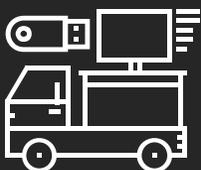
ЕГАИС



Офисные пакеты,
ЭДО



Участие
в электронных
торгах



Работа выездных
бригад



Доступ к ИТ-
ресурсам (VPN,
VDI, ГОСТ-TLS)



Защита от НСД
и эл. замки



ГОСТ-
криптопровайдеры



Сдача
отчетности



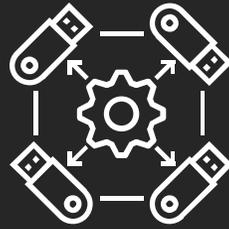
Работа в
среде отечественных
решений



Работа с ДБО



Единая карта
сотрудника



Актуальные и перспективные продукты Рутокен



Рутокен ЭЦП 3.0

Модели

- 3220
- 3100 NFC
- Экспортный
(на базе 3220)
- 3120
(смарт-карточный чип,
повышена надежность,
выше скорость)
- 3120 Touch

Форм-факторы



Смарт-карты

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

Сертификаты



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

Рутокен ЭЦП 3.0 3220 SD

- Платформа ЭЦП 3.0
- Неуправляемая microSD
- Два устройства в одном
- Сертифицирован ФСТЭК России



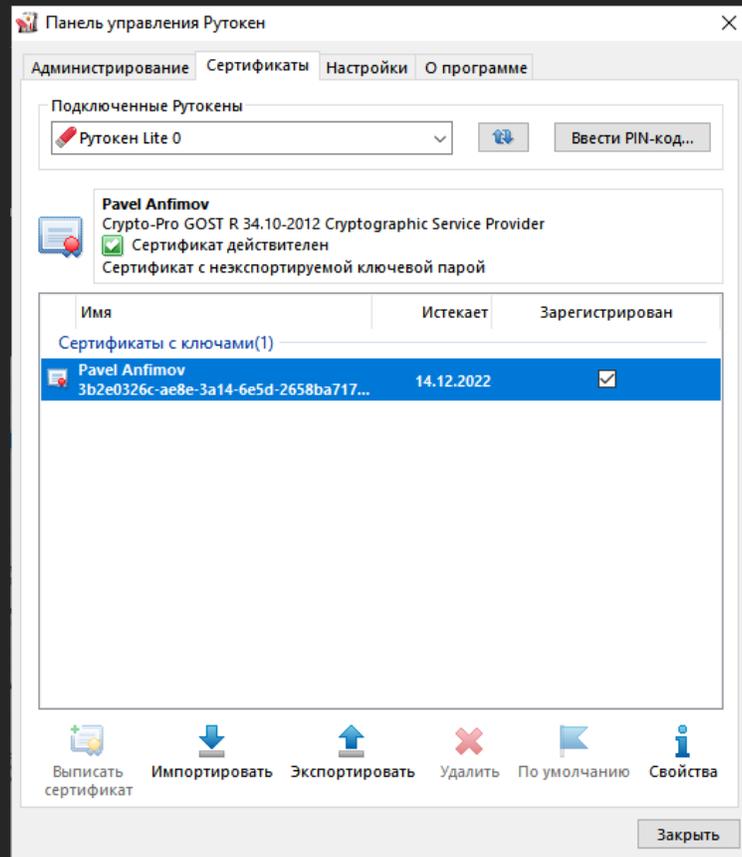
Семейство Рутокен ЭЦП 3.0 **Flash**



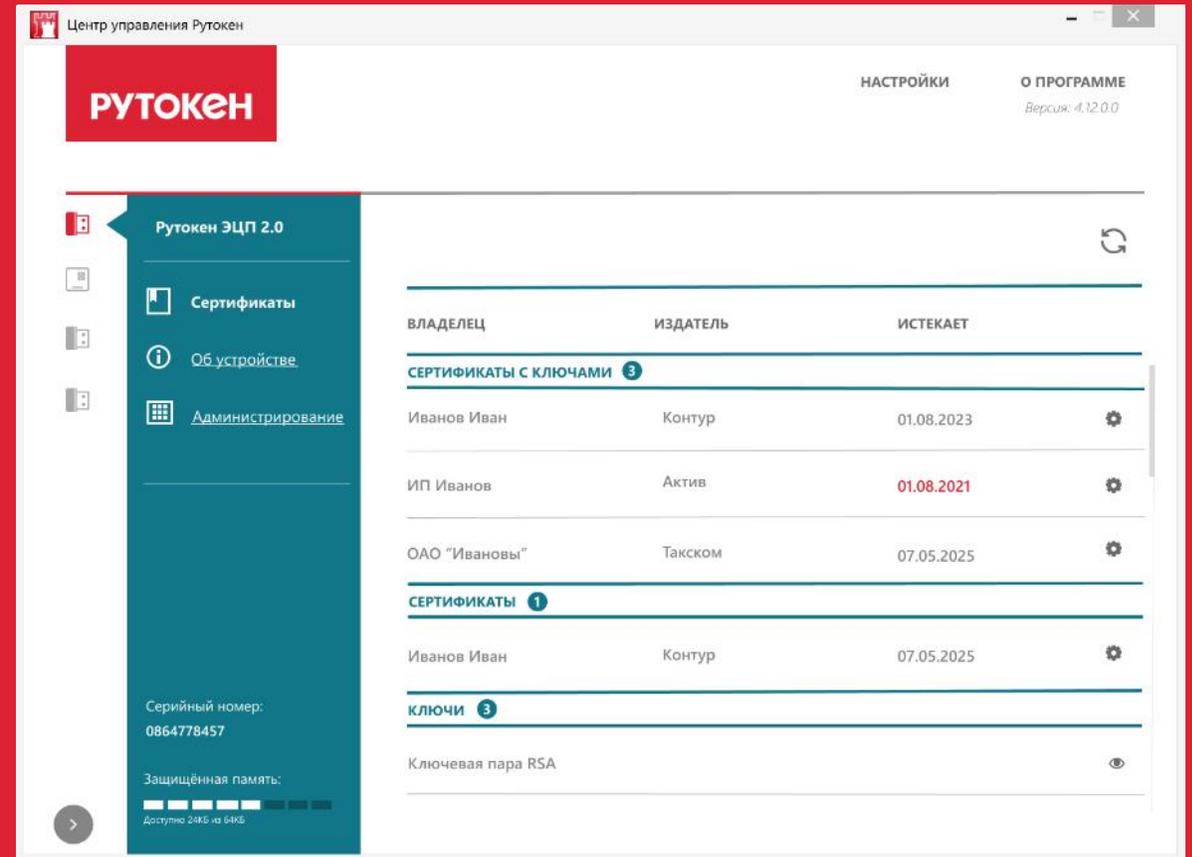
- Возможности Рутокен ЭЦП 2.0 Flash
 - Контроль и установка прав на разделы Flash-памяти
 - Блокирует доступ к разделам Flash-памяти и хранилищу ключей до ввода PIN-кода
- Обновление ОС Рутокен
- Ограничение количества ПК для работы
- Журналирование событий безопасности
- Сквозное шифрование до 7 Мб/с в отдельном исполнении

Центр Управления Рутокен

Было



Стало



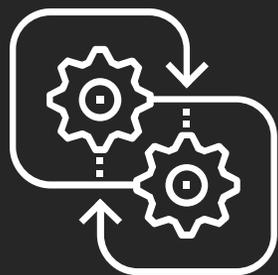
Аутентификаторы в семействе Рутокен



- **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 MFA** — устройство с поддержкой стандартов U2F/FIDO2
- 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



Сценарии:

- Работа в системах ЭДО и сдачи отчетности в Windows и Linux
- Вход в информационные системы:
 - Госуслуги
 - ЛК ФНС
 - Национальная система маркировки «Честный знак»

Преимущества для заказчика:

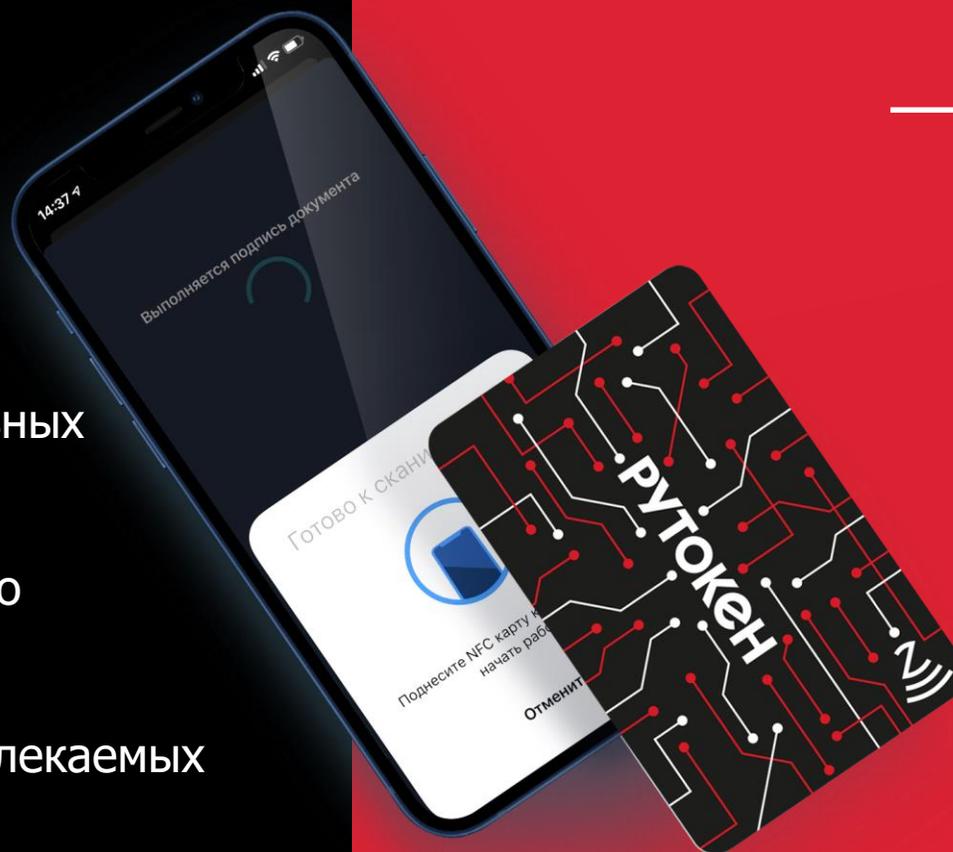
- Срок действия ключа ЭП — 3 года
- Увеличение уровня ИБ за счет хранения ключа отдельно от АРМ-а пользователя

Мобильное подписание документов

Электронная подпись и шифрование файлов на любых платформах

Преимущества использования Рутокен ЭЦП 3.0:

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

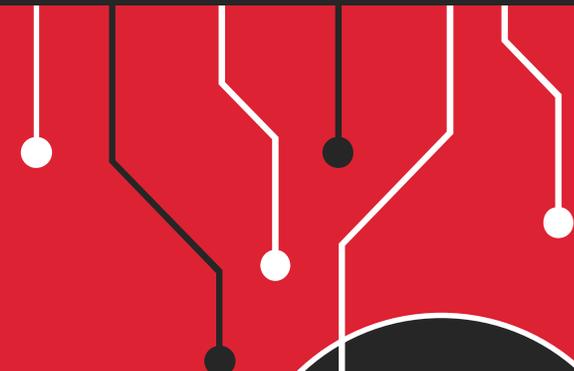
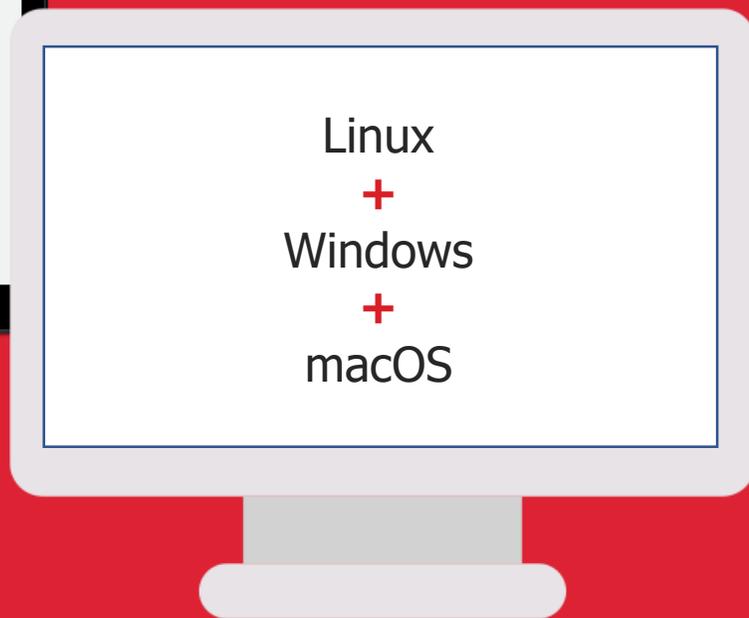


infotecs

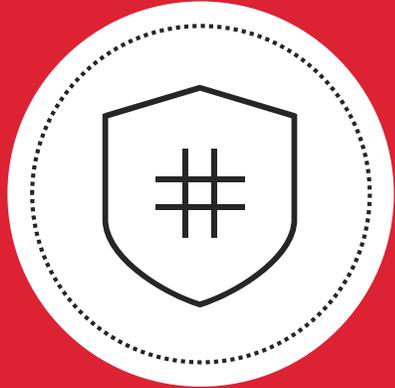
ViPNet PKI Client

РУТОКЕН

SDK для разработчиков



Аутентификация при контроле АРМ-ов



ViPNet SafeBoot 3.0 + Рутокен

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



ViPNet SafePoint + Рутокен

- 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

- Хранение пароля для входа в клиент на Рутокене
- Сертификат пользователя на Рутокене (PKI)
- Администратор может записать ключ во время распределения устройств между клиентами
- Пользователь может сам сгенерировать ключ для установленного клиента



Контактная информация

Павел Анфимов

Руководитель отдела
продуктов и интеграций Рутокен
Компания «Актив»



panfimov@rutoken.ru
info@rutoken.ru



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



+7 495 925-77-90
+7 926 586-90-96



Технологическая рассылка