



техно infotecs  
2024 Фест  
ТЕХНИЧЕСКАЯ  
КОНФЕРЕНЦИЯ

# Новые технологии Рутокен и поддержка в продуктах ИнфоТекс

Дмитрий Горелов  
Коммерческий директор  
Компания «Актив»

Владимир Иванов  
Директор по развитию  
Компания «Актив»

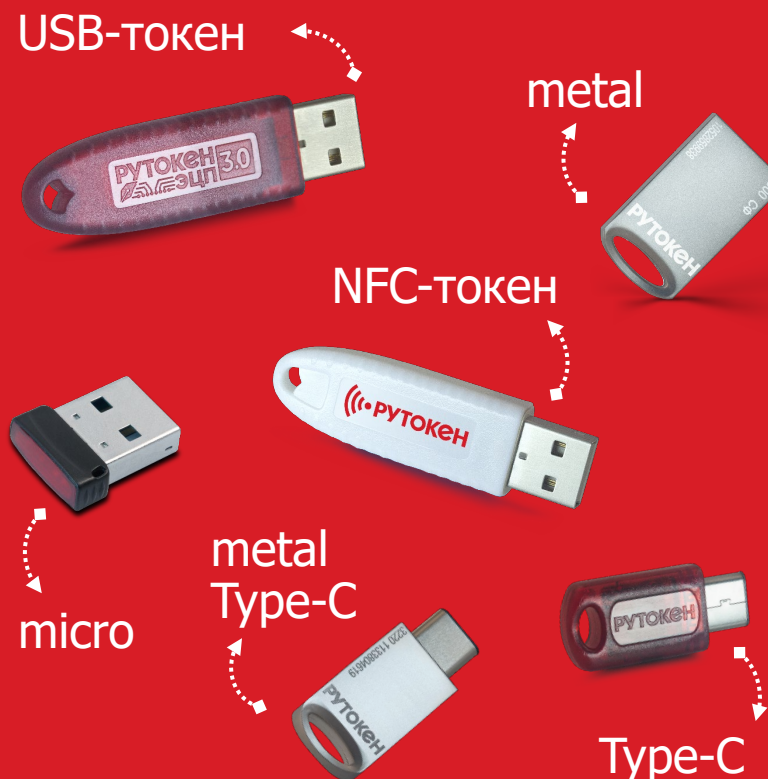
# РУТОКЕН ЭЦП 3.0

## Что сейчас и что в ближайшем будущем?

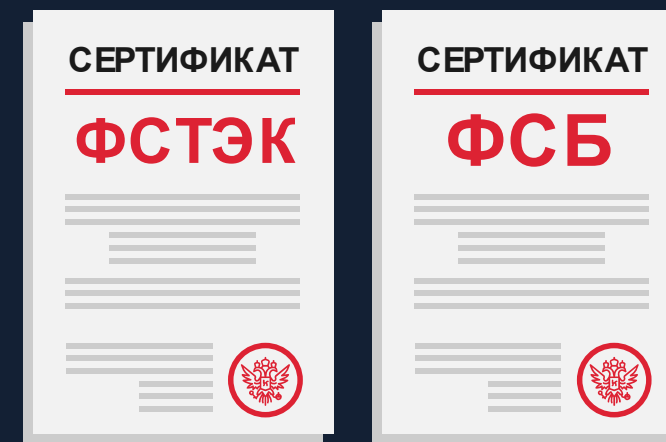
### ■ ■ ■ Модели

- 3220
- 3100 NFC
- 3220 Исп. А (экспортный)
- 3120  
(смарт-карточный чип, повышена надежность, выше скорость, журнал событий безопасности, длинные кривые ECDSA)\*
- 3120 Touch (с кнопкой)\*

### ■ ■ ■ Форм-факторы



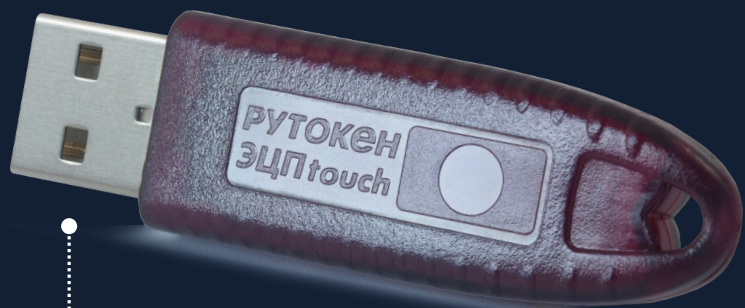
### ■ ■ ■ Сертификаты



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

\* 3120: срок сертификации — Q3 2024

# РУТОКЕН ЭЦП 3.0 3120 TOUCH



Рутокен ЭЦП  
3.0 3120 Touch



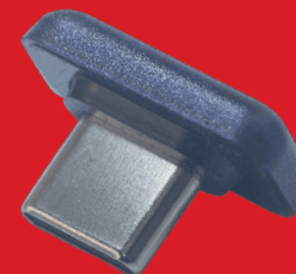
Type-C



Micro



Nano



# РУТОКЕН ЭЦП 3.0 3220 SD



Два устройства в одном



Сертифицирован  
ФСТЭК России



Уже в продаже



# РУТОКЕН ЭЦП 3.0 FLASH 5100/5900

## #1 Возможности

- Контроль прав на разделы Flash-памяти
- Доступ к разделу Flash по PIN-коду

## #2 Обновление

операционной системы  
Рутокен

## #3 Журналирование событий безопасности

## #4 Ограничение

количества ПК для работы

## #5 Шифрование разделов для модели 5900



# ФЛАГМАНЫ

## Рутокен ЭЦП 3.0



## Аппаратная криптография:

- ГОСТ Р 34.10-2012 (256/512 бит)
- ГОСТ Р 34.11-2012
- VKO GOST
- ГОСТ Р 34.12-2015 Магма
- ГОСТ Р 34.12-2015 Кузнечик

## Рутокен ЭЦП 3.0 NFC



- Совместимость с современными ОС
- Защита NFC-канала (SESPAKE)
- Высокая производительность
- SDK для встраивания
- Работа на ПК и мобильных устройствах

# NFC-БРЕЛОК РУТОКЕН



Везде, где нужна  
собственноручная подпись



Преимущества

Рутокен TAG

Графическая  
персонализация



Повышенная прочность



Компактный размер



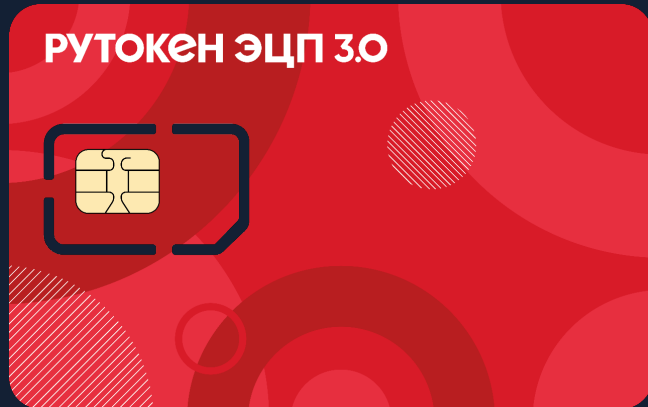
Высокая  
производительность



Удобство использования



# РУТОКЕН ЭЦП 3.0 SAM



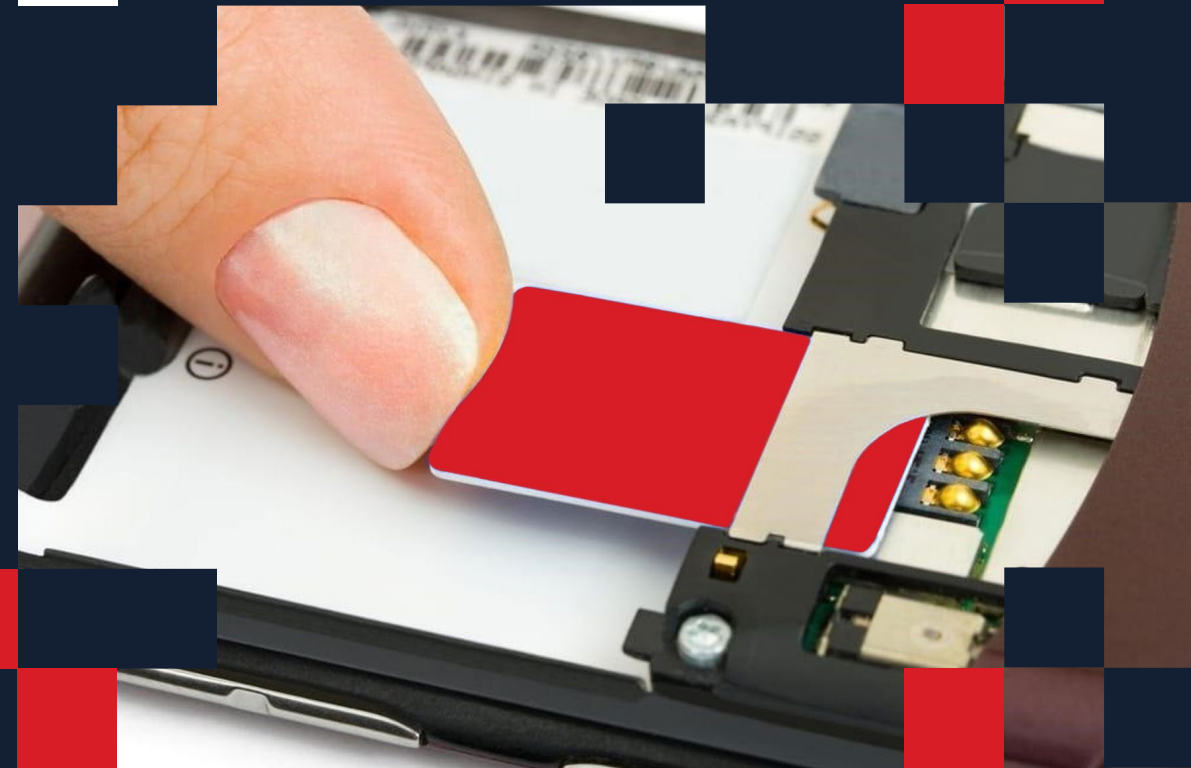
## Модуль безопасного доступа

### Форматы:

- mini SIM
- micro SIM
- nano SIM

### Применение:

- Банкоматы
- POS-терминалы
- M2M
- IoT





# АППАРАТНЫЙ ХОЛОДНЫЙ КОШЕЛЕК РУТОКЕН



## Преимущества криптокошелька:

- ✓ Первый российский аппаратный кошелек
- ✓ Работа со сторонними программными кошельками
- ✓ Подпись транзакций на мобильных устройствах
- ✓ Работа с Ethereum и Bitcoin
- ✓ Резервирование ключей
- ✓ Надежное хранение приватных ключей

РУТОКЕН

СБЕР



METAMASK

# АУТЕНТИФИКАТОРЫ

## РУТОКЕН

### Рутокен ОТР

— доп. аутентификация  
в информационных системах

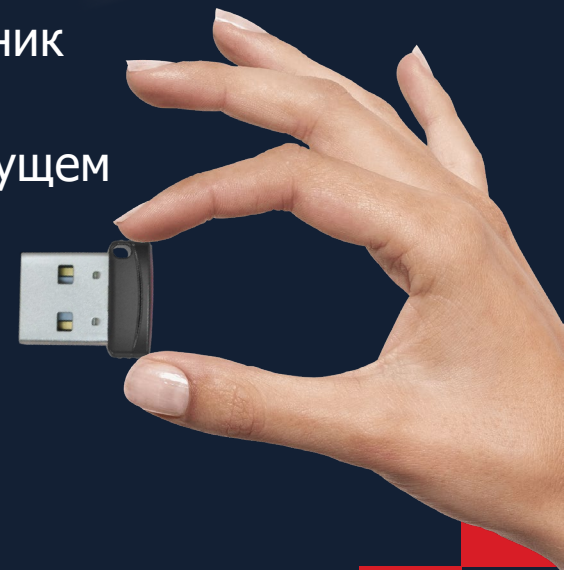
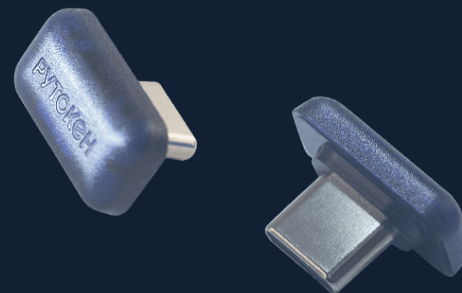
- Алгоритм OATH TOTP (RFC6238)
- Не требует связи с ПК/мобильным устройством для работы
- NFC-интерфейс для настройки
- Аппаратный таймер




### 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**

# РУТОКЕН ЭЦП

## VIPNET CSP



### Сценарии:

- Работа в системах ЭДО и сдачи отчетности в Windows и Linux
- Аутентификация в ИС:
  - 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 С ViPNet PKI Client

Преимущества использования  
Рутокен ЭЦП

- Смарт-карта — средство ЭП
- Избавляет офис от бумаг
- Не требует физического подключения
- Секреты хранятся отдельно от приложения



### Применение:



Энергетика



Транспорт



Системы  
здравоохранения



Государственные  
органы

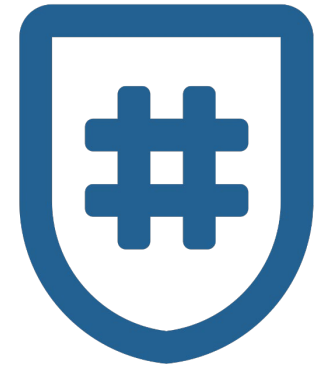


Промышленность

# АУТЕНТИФИКАЦИЯ НА АРМ

## ViPNet SafeBoot 3.0

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



## ViPNet SafePoint

- 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

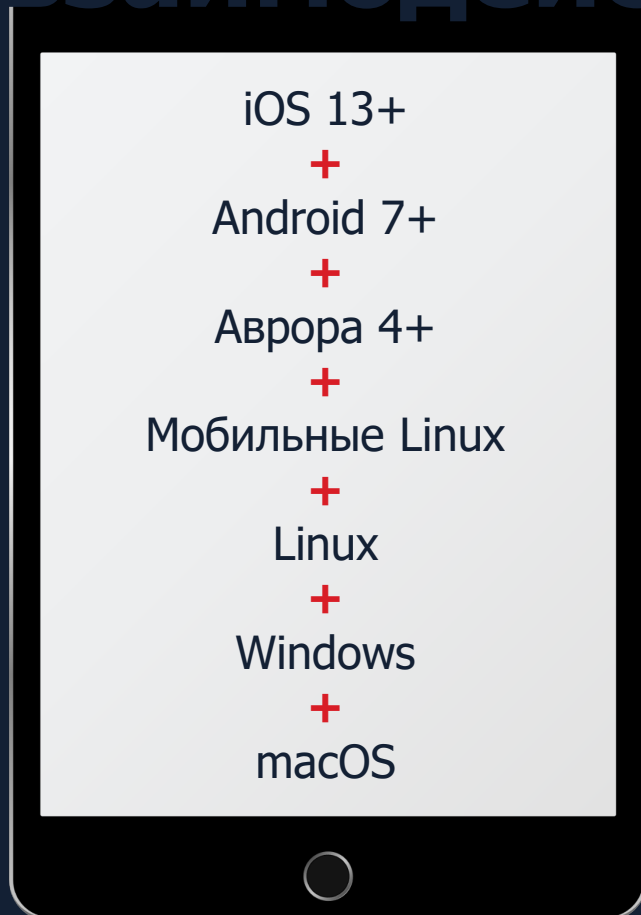
- Хранение пароля для входа в клиент на Рутокене
- Сертификат пользователя на Рутокене (PKI)
- Администратор может записать ключ во время распределения устройств между клиентами
- Пользователь может сам сгенерировать ключ для установленного клиента



# VIPNET OSSSL

ВЗАИМОДЕЙСТВИЕ

OOSSSL



- SDK Рутокен

- PKCS#11

- ViPNet OSSSL





# Спасибо за внимание!



Владимир  
Иванов

info@rutoken.ru  
www.rutoken.ru



Дмитрий  
Горелов