Вебинар

РУТОКЕН

Применение устройств Рутокен для квалифицированной электронной подписи

Ксения Шаврова
Ведущий менеджер по сопровождению партнеров
Компания «Актив»

Компания «Актив»

На рынке информационной безопасности с 1994 года

Имеем все необходимые лицензии на разработку СКЗИ и СЗИ

Являемся членом АЗИ, РОСЭУ, ТК26, РусКрипто, ISDEF

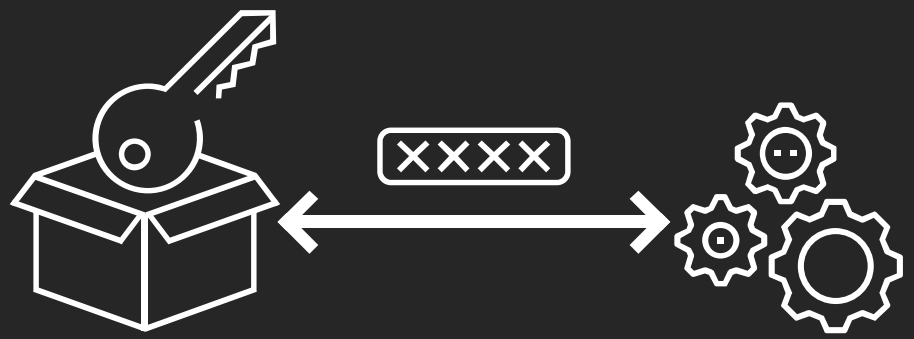
Входим в 20 крупнейших ИБ-компаний в России

Участвуем в международных и российских криптографических конференциях

Разновидности ключей ЭП

Извлекаемые

- Создание ключей и работа с ними с использованием **программного криптопровайдера**
- При работе с подписью **закрытый ключ извлекается в оперативную память компьютера** после ввода PIN-кода
- Ключи ЭП хранятся **в защищённом ключевом контейнере**



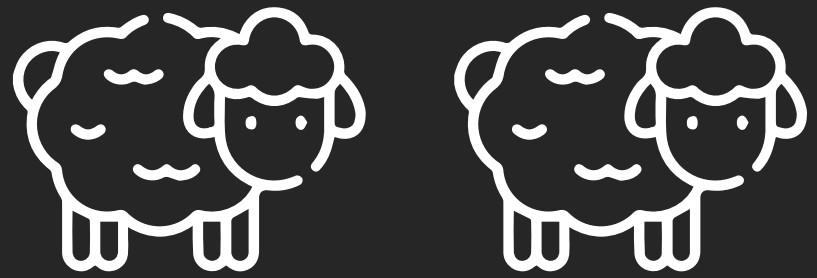
Неизвлекаемые

- Создание ключей и работа с ними с использованием **аппаратных возможностей Рутокена**
- При работе с подписью **закрытый ключ никогда не покидает память Рутокена**
- Ключи ЭП хранятся **в защищённом ключевом контейнере в специальном внутреннем формате**

Виды извлекаемых ключей

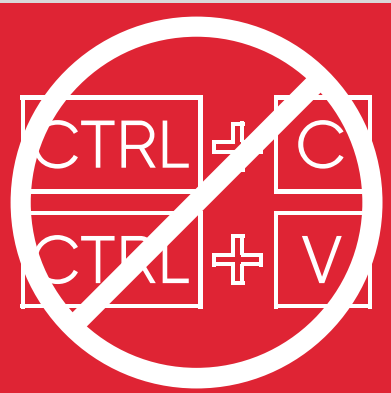
Экспортируемые

Копирование ключей на другие носители
РАЗРЕШЕНО



Неэкспортируемые

Копирование ключей на другие носители
ЗАПРЕЩЕНО



Флаг экспортируемости устанавливается при генерации или импорте ключей на токен. Этот параметр впоследствии нельзя изменить.

Виды неизвлекаемых ключей

PKCS#11

Генерация ключей и работа с ними производится **с помощью аппаратного СКЗИ внутри интеллектуального носителя Рутокен.**

При использовании протокола PKCS#11 программы работают напрямую с аппаратной реализацией электронной подписи и шифрования внутри Рутокена.

ФКН

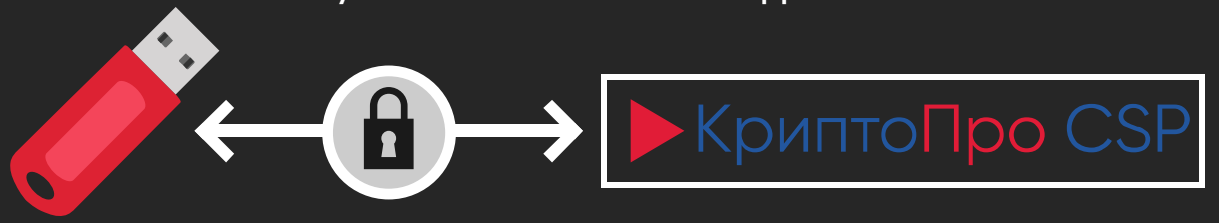
Генерация ключей и работа с ними производится с помощью двух компонентов:

- **аппаратных возможностей устройства Рутокен**
- **программных возможностей СКЗИ «КриптоПро CSP»**

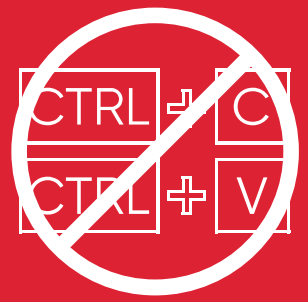
+

Защита канала с помощью протокола SESPAKE*

* PIN-код пользователя не передается в открытом виде для обмена сообщений между криптопровайдером и носителем устанавливается зашифрованный канал.



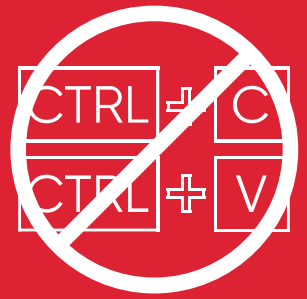
Важно!



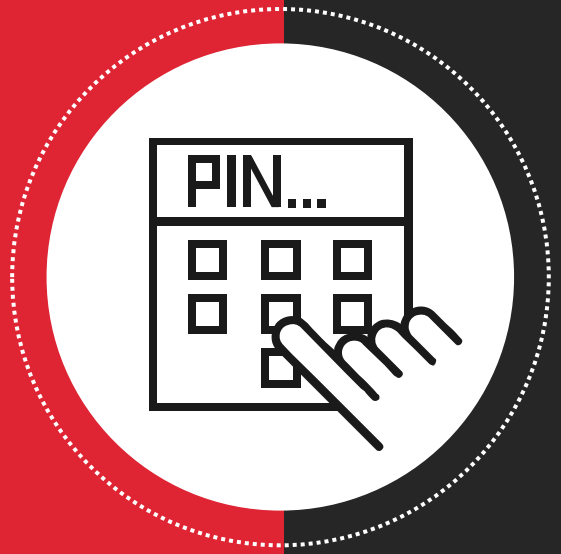
НЕЭКСПОРТИРУЕМОСТЬ ≠ НЕИЗВЛЕКАЕМОСТЬ

НО

НЕИЗВЛЕКАЕМЫЕ КЛЮЧИ ВСЕГДА НЕЭКСПОРТИРУЕМЫЕ!



Защита памяти

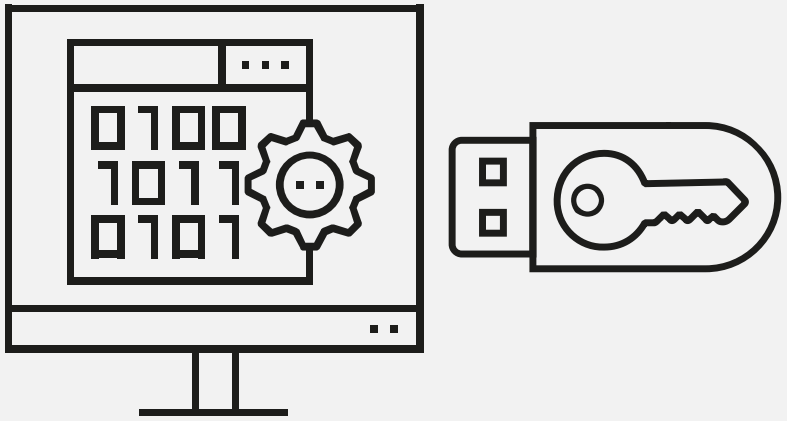


- Для доступа к защищенному содержимому любого Рутокена нужно ввести PIN-код Пользователя
- На всех Рутокенах установлено ограничение попыток ввода неправильного PIN-кода

Виды ключевых носителей Рутокен

Пассивные

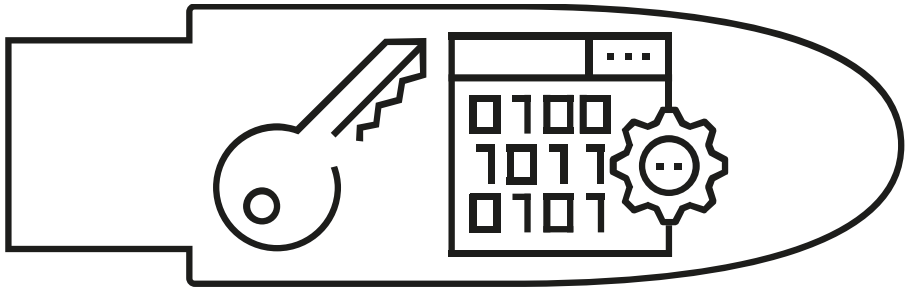
Защищённое хранилище для
извлекаемых ключей
(экпортируемых и неэкспортируемых)



- Рутокен Lite
- Рутокен S

Активные

Являются СКЗИ,
генерируют **неизвлекаемые ключи,**
формируют электронную подпись
с использованием аппаратной криптографии



- Семейство Рутокен ЭЦП 2.0
- Семейство Рутокен ЭЦП 3.0

Важно!

Аппаратная криптография на токене

встроенный «КриптоПро CSP»

Средства генерации ключей

Извлекаемые

КриптоПро CSP 4.0 и выше (режим «CSP»)
- Рутокен Lite
- Рутокен S
- Линейка Рутокен ЭЦП 2.0
- Линейка Рутокен ЭЦП 3.0

VipNet CSP
с пассивными ключевыми носителями:
- Рутокен Lite
- Рутокен S

Signal-COM CSP
с пассивными ключевыми носителями:
- Рутокен Lite
- Рутокен S

Неизвлекаемые

Ключи PKCS#11

- **Рутокен SDK** (кроссплатформенная библиотека rtpkcs11ecp)
- **КриптоПро CSP 5.0 R2 и выше** (режим «Активный токен pkcs#11»)
- **Vip Net CSP**
- **Signal-COM CSP**

с активными ключевыми носителями:
- Линейка Рутокен ЭЦП 2.0
- Линейка Рутокен ЭЦП 3.0

Ключи ФКН

КриптоПро CSP 5.0 и выше (режим «ФКН с защитой канала»)

с активными ключевыми носителями:
- Рутокен ЭЦП 2.0 3000
- Линейка Рутокен ЭЦП 3.0

Токены и сертификация

ФСТЭК

ФСБ

для квалифицированой электронной подписи

О соответствии требованиям по безопасности информации, устанавливающим уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий.

ПАК «Рутокен» сертифицирован по УД4:
Токены и смарт-карты:

- Рутокен ЭЦП 2.0 2100
- Рутокен ЭЦП 2.0 Flash
- Рутокен ЭЦП PKI
- Рутокен Lite
- Рутокен S

**Программное СКЗИ должно быть сертифицировано в ФСБ*

О соответствии требованиям, предъявляемым к СКЗИ по классу КС1, КС2)

Токены и смарт-карты:

- Рутокен ЭЦП 2.0 2100
- Рутокен ЭЦП 2.0 3000
- Рутокен ЭЦП 2.0 Flash

Контактная информация

Ксения Шаврова

shavrova@rutoken.ru

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

+7 495 925-77-90, доб.234
+7 906 747-00-94