Вебинар

РУТОКЕН

Всё о квалифицированной электронной подписи

на основе технологий КриптоПро и Рутокен

Ксения Шаврова
Компания «Актив»

Сергей Агафьин
Компания «КриптоПро»

Какие ключи могут храниться на токене?

Программные ключи

- Создание и работа с помощью ГОСТ-криптопровайдера, установленного в ОС
- Подойдет любая модель Рутокен, совместимая с КриптоПро CSP
- Рутокен — защищённое PIN-кодом хранилище
- Все операции с закрытым ключом выполняются в оперативной памяти компьютера
- Закрытый ключ **ненадолго извлекается** в оперативную память

Извлекаемые

Аппаратные ключи

- Создание и работа с использованием встроенных аппаратных криптографических механизмов внутри Рутокена
- Подойдет Рутокен, имеющий криптографическое ядро внутри микроконтроллера устройства
- Рутокен — не только хранит ключи под PIN-кодом, но и создает ключи в специальном формате, с которым умеет работать только криптоядро устройства
- Все операции производятся внутри Рутокена
- Закрытый ключ никогда **не извлекается** из памяти микроконтроллера и не копируется на другие носители

Неизвлекаемые

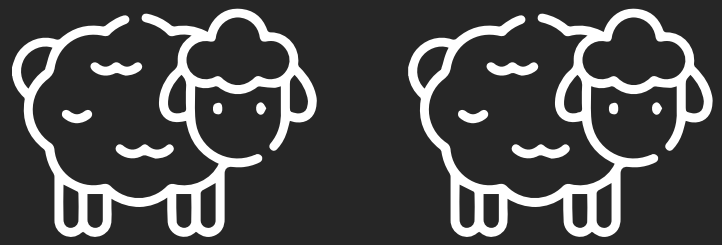
Виды извлекаемых (программных) ключей

Экспортируемые

Пометить ключ как экспортируемый

Копирование ключей на другие носители

РАЗРЕШЕНО

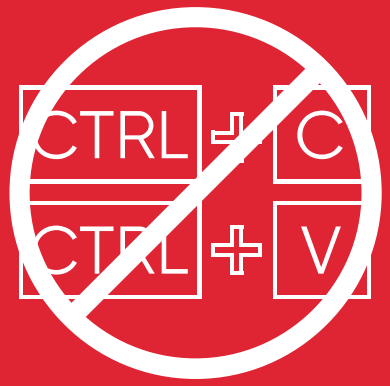


Неэкспортируемые

Пометить ключ как экспортируемый

Копирование ключей на другие носители

ЗАПРЕЩЕНО*



Виды неизвлекаемых (аппаратных) ключей

PKCS#11

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

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

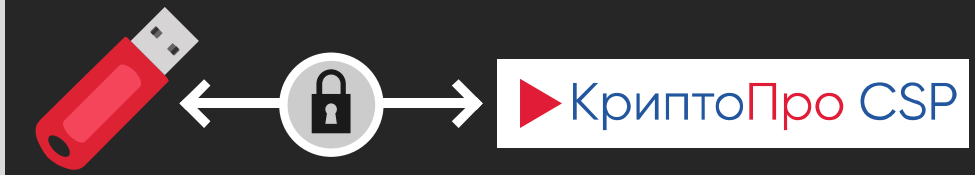
ФКН

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

- **аппаратные возможности устройства Рутокен**
- **программные возможности 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.



Режимы работы «КриптоПро CSP 5.0 R2»

Сергей Агафьин,
Компания КриптоПро

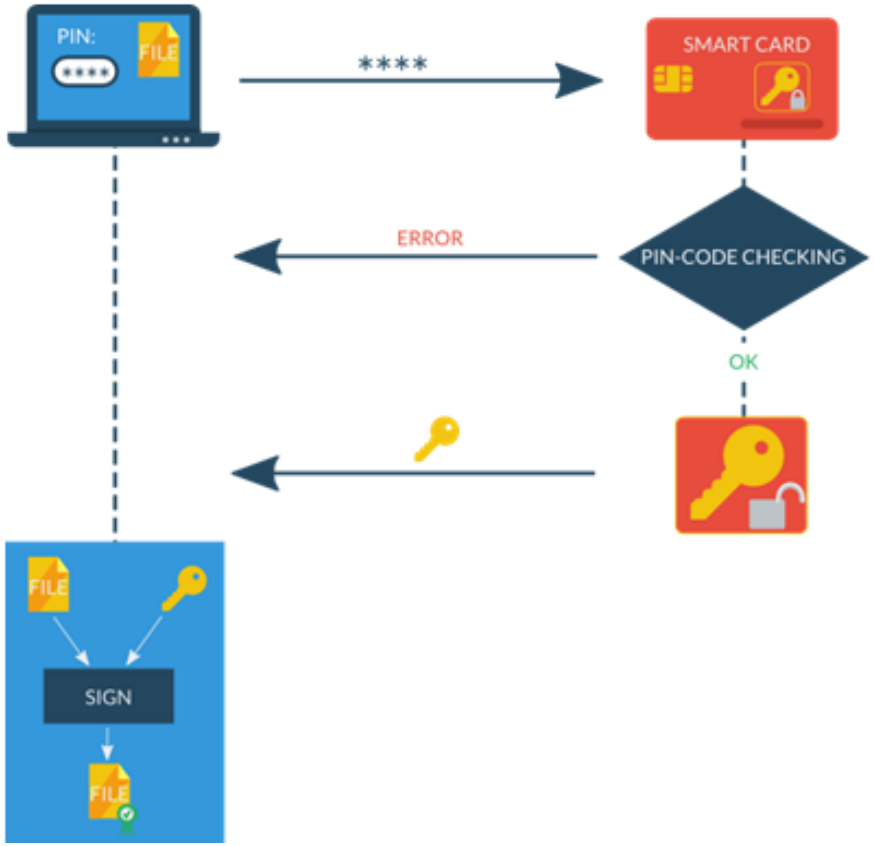
10 ноября 2022

Семейство КриптоПро CSP

1. КриптоПро CSP 3.6–4.0
2. КриптоПро Рутокен CSP3.9
3. КриптоПро CSP 5.0
4. КриптоПро CSP 5.0 R2
5. КриптоПро CSP 5.0 R3

КриптоПро CSP 3.6 – 4.0

Пассивный режим



Актуальный представитель

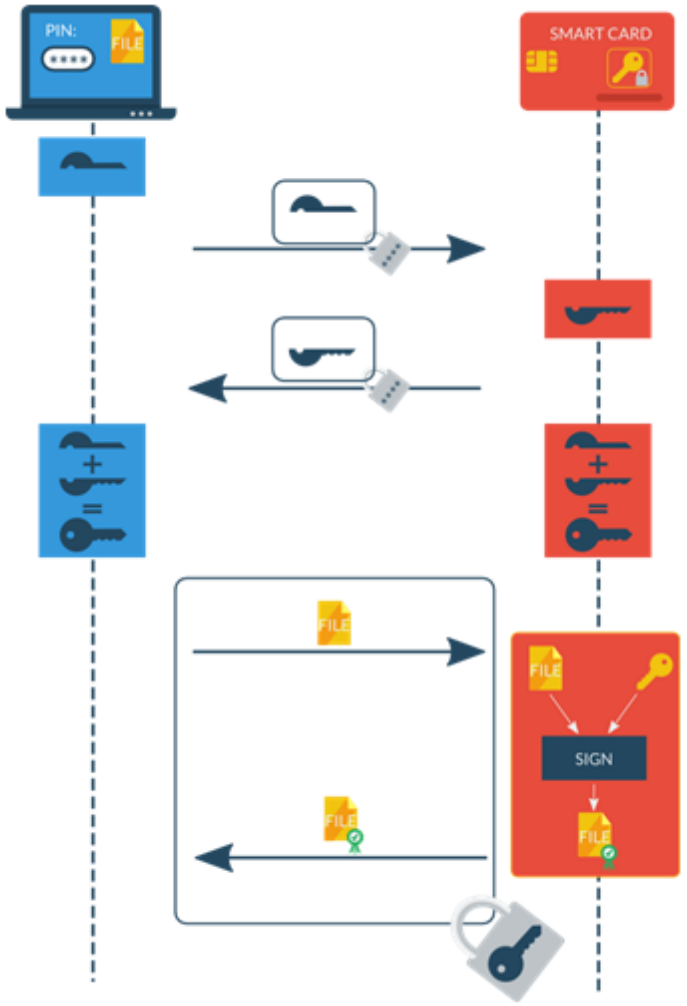
КриптоПро CSP 4.0 R4
(сертификат до 2024 года)

Поддерживаемые носители

1. Рутокен S
2. Рутокен Lite
3. Рутокен ЭЦП 2.0 (2100, 2151)

КриптоПро Рутокен CSP 3.9 (ФКН)

ФКН с КриптоПро EKE



Актуальный представитель

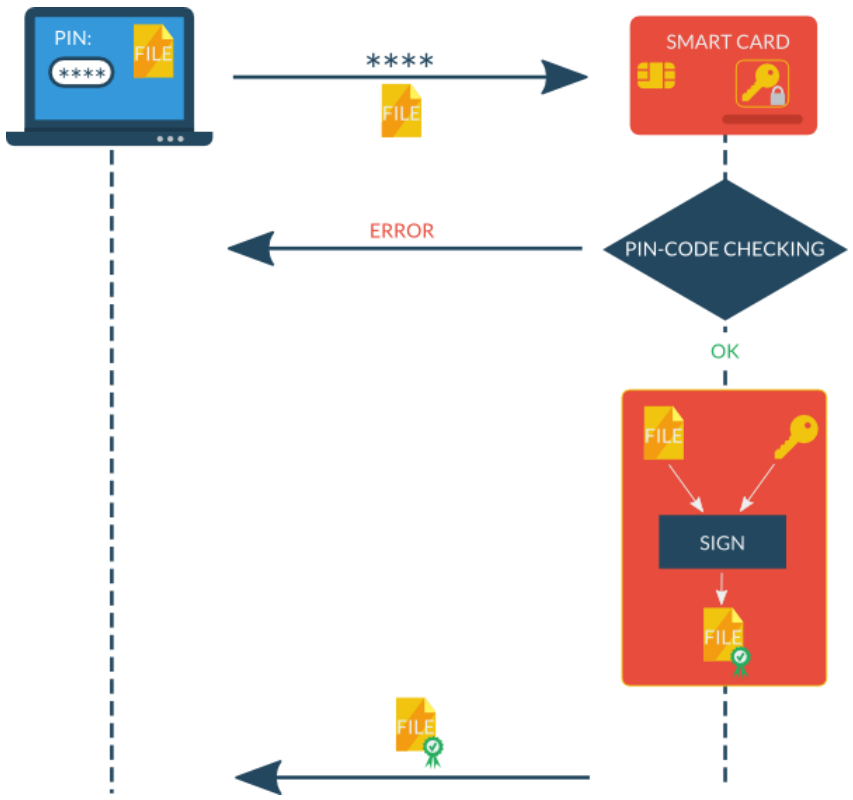
Отсутствует. Сертификат истек в 2018 году.

Поддерживаемые носители

КриптоПро Рутокен

Новые ФКН

ФКН без защиты канала



SESPAKE

Public Information: $I, P, Q_1, \ldots, Q_l, m, q$			
$A\ [A_{ID}, PW]$		$B\ [B_{ID}, Q_{PW}, ind, salt]$	
	$\xrightarrow{A_{ID}}$		Key generation
	$\xleftarrow{B_{ID}, ind, salt}$		
$z_A = 0$			
$Q_{PW}^A = F(PW, salt, 2000) \cdot Q_{ind}$			
$\alpha \in_R \{1, \ldots, q-1\}$			
$u_1 = \alpha \cdot P - Q_{PW}^A$	$\xrightarrow{u_1}$		
		if $u_1 \notin E \Rightarrow$ FINISH	
		$z_B = 0$	
		$Q_B = u_1 + Q_{PW}$	
		$\beta \in_R \{1, \ldots, q-1\}$	
		if $\frac{m}{q} Q_B = 0_E \Rightarrow Q_B = P,\ z_B = 1$	
		$K_B = H_{256}((\frac{m}{q} \cdot \beta \mod q) Q_B)$	
	$\xleftarrow{u_2}$	$u_2 = \beta \cdot P + Q_{PW}$	
if $u_2 \notin E \Rightarrow$ FINISH			
$Q_A = u_2 - Q_{PW}^A$			
if $\frac{m}{q} Q_A = 0_E \Rightarrow Q_A = P,\ z_A = 1$			
$K_A = H_{256}((\frac{m}{q} \cdot \alpha \mod q) Q_A)$			
$tag_A = T_A \vert\vert A_{ID} \vert\vert ind \vert\vert salt \vert\vert u_1 \vert\vert u_2$ $M_A = \text{HMAC}_{K_A}(tag_A)$	$\xrightarrow{M_A}$		Authentication
		$tag = T_A \vert\vert A_{ID} \vert\vert ind \vert\vert salt \vert\vert u_1 \vert\vert u_2$ $M = \text{HMAC}_{K_B}(tag)$	
		If $M \neq M_A$ or $z_B \neq 0 \Rightarrow$ FINISH	
	$\xleftarrow{M_B}$	$tag_B = T_B \vert\vert B_{ID} \vert\vert ind \vert\vert salt \vert\vert u_1 \vert\vert u_2$ $M_B = \text{HMAC}_{K_B}(tag_B)$	
$tag = T_B \vert\vert B_{ID} \vert\vert ind \vert\vert salt \vert\vert u_1 \vert\vert u_2$ $M = \text{HMAC}_{K_A}(tag)$			
If $M \neq M_B$ or $z_A \neq 0 \Rightarrow$ FINISH			

КриптоПро CSP 5.0

1. Действующий сертификат до 2024 года
2. Поддерживает пассивные носители
3. Поддерживает активные носители (ФКН без защиты канала)
4. Поддерживает ФКН с SESPAKE (Р 50.1.115–2016 «Информационная технология. Криптографическая защита информации. Протокол выработки общего ключа с аутентификацией на основе пароля»)

Поддерживаемые токены

1. Рутокен ЭЦП 2.0 3000 (SESPAKE + пассивный режим)
2. Рутокен S, Рутокен Lite (пассивные)
3. Рутокен ЭЦП 2.0 (ФКН без защиты канала + пассивный)
4. КриптоПро Рутокен (в пассивном режиме)

КриптоПро CSP 5.0 R2

1. Актуальная сертифицированная версия
2. Дополнительно поддерживает смарт-карты Рутокен ЭЦП 3.0 и токены Рутокен TLS

Начинаем встраивать PKCS#11

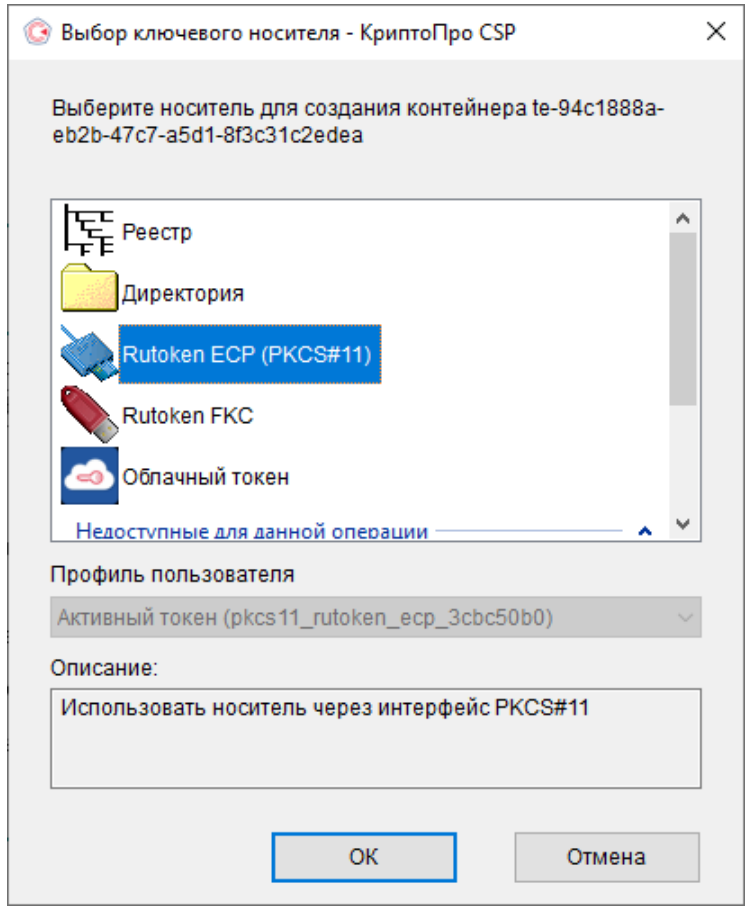
1. Актив пишет библиотеку rtPKCS11ECP.dll, которая реализует интерфейс встраивания PKCS#11 (Cryptoki)
2. Мы подгружаем библиотеку в провайдер и через неё генерируем ключи и подписываем документы

Особенности работы

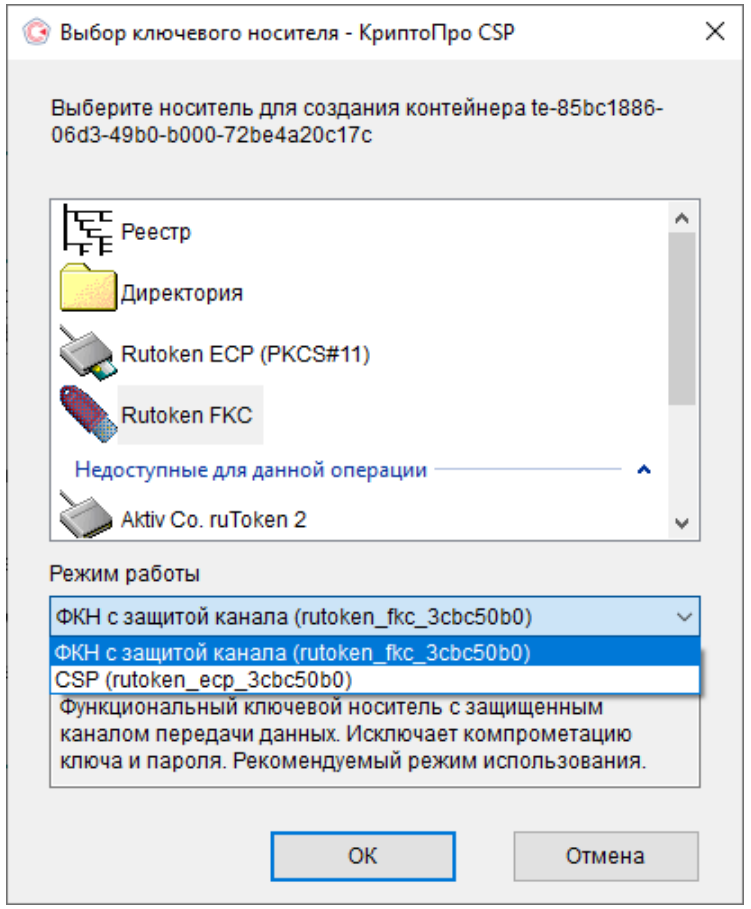
1. Обязательно устанавливать «Драйверы Рутокен» или спец.сборку CSP 5.0 R2 с библиотеками PKCS#11
2. PKCS#11 реализован как отдельный считыватель

Выбор режима в CSP 5.0 R2

PKCS#11



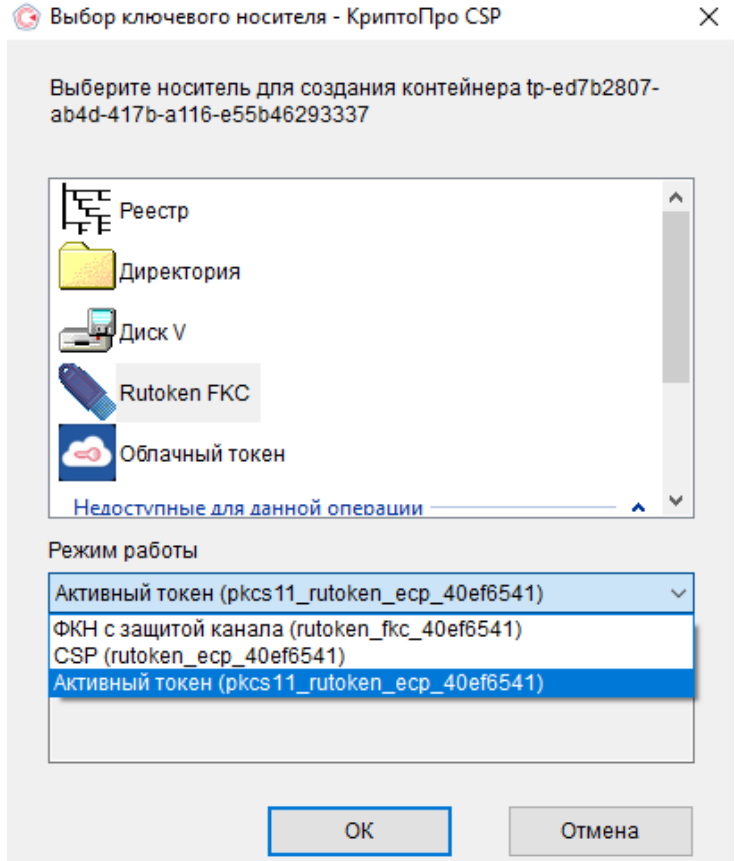
ФКН с SESPAKE



КриптоПро CSP 5.0 R3

1. Сертификация в 2023 году
2. Поддержка всех носителей Рутокен, включая Рутокен ЭЦП 2.0
3. Появилась полная поддержка Рутокен ЭЦП 3.0 (3100 и 3220)
4. PKCS#11 можно использовать в Winlogon/RDP

Доработано встраивание через PKCS#11

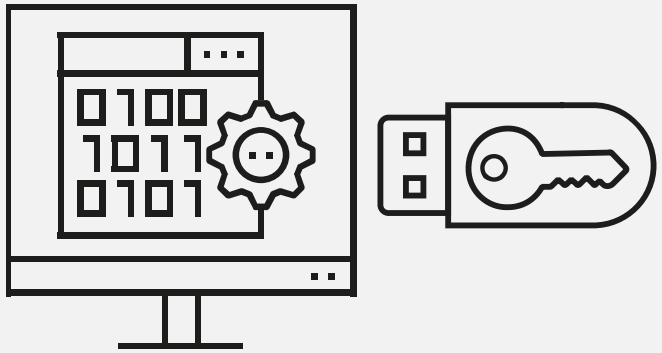


Функциональные возможности устройств Рутокен

Рутокен Lite

Пассивный токен

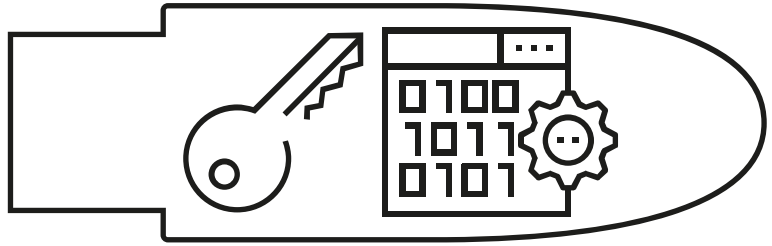
Защищённое хранилище для
извлекаемых ключей
(экпортируемых и неэкспортируемых)



Рутокен ЭЦП 3.0

Активный токен

Является СКЗИ,
генерирует **неизвлекаемые ключи,**
формирует электронную подпись
с использованием аппаратной криптографии



+

Может выступать в роли
пассивного токена

Важно!

Аппаратная криптография на токене

встроенный «КриптоПро CSP»

Особенности применения

Только PKCS#11 если...

ЕГАИС

Алкогольрегулирование

Рутокен SDK

Средства генерации ключей и модели Рутокен

Извлекаемые

КриптоПро CSP 4.0 и выше

Рутокен ЭЦП 3.0

Рутокен Lite

Неизвлекаемые

PKCS#11

- КриптоПро CSP 5.0 R2 и выше
- Генератор запросов Рутокен

Рутокен ЭЦП 3.0

ФКН

КриптоПро CSP 5.0 R2 и выше

Рутокен ЭЦП 3.0

Какая сертификация нужна токену?

СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.030BB0

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 3753

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В.Лютиков

ФСТЭК

Когда токен выступает в роли защищённого хранилища программных ключей (извлекаемые ключи)

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Система сертификации РОСС RU.0001.030001

СЕРТИФИКАТ СООТВЕТСТВИЯ

Регистрационный номер СФ/124-4129 от "25" августа 2021 г.

Действителен до "01" июня 2023 г.

Выдан акционерному обществу «Актив-софт»

обществу с ограниченной ответственностью Фирма «АНКАД»

Настоящий сертификат удостоверяет, что средство криптографической защиты информации (СКЗИ) «Сокет-карта Рутокен ЭЦП 2.0 2100» (исполнения TS, T13 и комплектация согласно формуляру АЛЕК.468244.003 ФО)

соответствует Требованиям к средствам криптографической защиты информации, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну, классов КС1, КС2. Требованиям к средствам электронной подписи, утвержденным приказом ФСБ России от 27 декабря 2011 г. № 796, устанавливающим для классов КС1, КС2, и может использоваться для криптографической защиты (шифрование и управление ключевой информацией, информации данных, содержащихся в областях оперативной памяти СКЗИ, вычисление значения электронной подписи для данных, содержащихся в областях оперативной памяти СКЗИ, вычисление значения электронной подписи для данных, содержащихся в областях оперативной памяти СКЗИ, создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи, создание ключа проверки электронной подписи) информации, не содержащей сведений, составляющих государственную тайну.

Сертификат выдан на основании результатов проведенных Обществом с ограниченной ответственностью «Центр сертификационных исследований» сертификационных испытаний образца продукции № 3681-04101

Безопасность информации обеспечивается при использовании СКЗИ в соответствии с требованиями эксплуатационной документации согласно формуляру АЛЕК.468244.003 ФО

Заместитель руководителя Научно-технической службы – начальник Центра защиты информации и специальной связи ФСБ России

О.В. Скрабин

ФСБ

Когда используется внутренняя криптография токена (неизвлекаемые ключи PKCS#11 и ФКН)

Для квалифицированной ЭП

Подведем итоги... Выбираем...

ФКН

- Если нужна защита канала обмена между токеном и криптопровайдером
- Если НЕ требуется работа в системе ЕГАИС Алкогольрегулирование

PKCS#11

- Если нужно универсальное средство для работы со всеми сервисами с поддержкой КриптоПро Browser Plug-In и других браузерных плагинов с библиотекой rtpkcs11ecp, например Рутокен Плагин или плагин Госуслуг
- Если нужна работа с ЕГАИС Алкогольрегулирование

+

КриптоПро CSP 5.0 R2 и выше

+

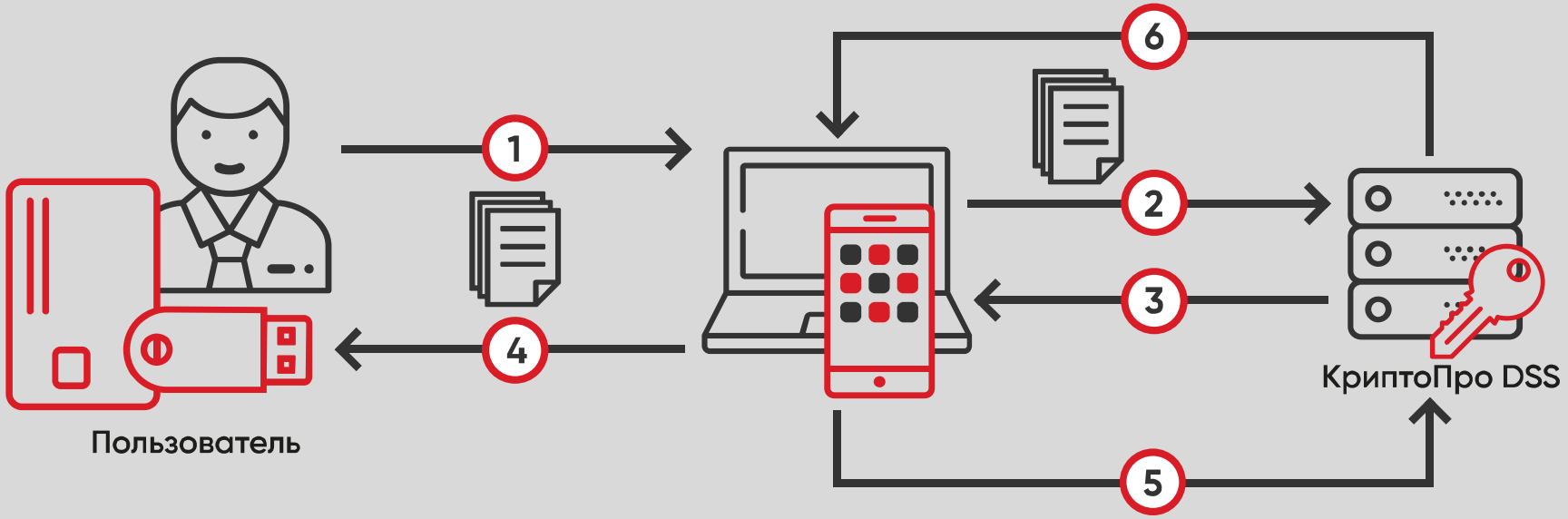
Рутокен ЭЦП 3.0

=

Универсальное и безопасное решение для любой области применения

Средство электронной подписи
на мобильных устройствах

Сервер КриптоПро DSS и myDSS 2.0 + Рутокен ЭЦП 3.0 NFC



1. Пользователь выбирает документ для подписи на своем ПК или смартфоне
2. Приложение отправляет документ в DSS
3. DSS передает документ и краткое содержание в МП для подписания
4. Пользователь проверяет, подтверждает и подписывает
5. Документ подписывается в МП и передается в DSS
6. DSS обрабатывает подпись и передает её по той же цепочке в вашу бизнес-систему

Линейка Рутокен ЭЦП 3.0

Соответствует требованиям 63-ФЗ и Приказа ФСБ России № 796

Сертифицирован в ФСБ и во ФСТЭК

Больше памяти – 128 кб

Подходит для получения ЭП в УЦ ФНС России

Поддержка ключей RSA-4096

Политики PIN-кодов внутри токена

Токены и смарт-карты с NFC

Выше производительность

ECDSA с кривыми secp256k1 и secp256r1

Магма и Кузнечик ГОСТ Р 34.12-2015/34.12-2018

Рекомендован для дистанционного получения ЭП

Подходит для ЕГАИС Алкогольрегулирование

Полностью совместим с КриптоПро CSP 5.0 R3 сборка 12500

Контактная информация

Ксения Шаврова

shavrova@rutoken.ru

www.rutoken.ru

Сергей Агафьин

ssa@cryptopro.ru

www.cryptopro.ru

РУТОКЕН