R301 ФОРОС USB-ФКН для СКЗИ «КриптоПро CSP»
Инструкция по установке и эксплуатации

Версия: 2K.1.Ф1.U.07

ООО "СмартПарк",
Москва, 127220, ул. 2-я Квесисская д. 24, корп. 3, офис №10.
Тел./факс: (495) 927-0033
Web: www.smart-park.ru
Техническая поддержка: help@smart-park.ru

Оглавление

Используемые термины, определения и сокращения

Администратор - администратор безопасности, администратор защиты - должностное лицо, устанавливающее политику безопасности и идентифицирующее объекты и участников, к которым применяется эта политика. Это субъект доступа, ответственный за защиту автоматизированной системы от несанкционированного доступа к информации.

Криптопровайдер (Cryptography Service Provider, CSP) - это независимый программный модуль, позволяющий осуществлять криптографические операции в операционных системах Microsoft.

Ключ - секретная информация, используемая криптографическим алгоритмом при зашифровании/расшифровании сообщений, генерации и проверке цифровой подписи, вычислении имитовставки.

Оператор – физическое лицо управляющее работой компьютера.

Пароль - это секретное слово или набор символов, предназначенный для подтверждения личности или полномочий.

ПИН - (англ. Personal Identification Number — персональный идентификационный номер) аналог Пароля.

Ути́лита (англ. *utility*) - специальная компьютерная программа, расширяющая стандартные возможности оборудования, выполняющая узкий круг специфических задач по администрированию оборудования

ФКН - функциональный ключевой носитель - неизвлекаемые ключи с защитой канала связи с носителем.

1 Применение и назначение

Носитель R301 ФОРОС USB-ФКН для СКЗИ «КриптоПро CSP» (далее - Носитель) применяется совместно с криптопровайдерами компании КриптоПро (КриптоПро CSP 5.0 R2 и выше) в любых системах в качестве носителя ключевой и идентификационной информации. При этом обеспечивается неизвлекаемость закрытых ключей электронной подписи и защита канала связи криптопровайдера с Носителем.

Носитель логически и физически объединяет два устройства:

- смарт-карт ридер соответствующий спецификации CCID;
- смарт-карту с программным обеспечением аппаратного модуля СКЗИ Форос 2 в конфигурации «ФКН» с установленным приложением «Ключевой контейнер КриптоПро CSP-ФКН».

Носитель применяется в использующих криптопровайдеры КриптоПро CSP прикладных системах в соответствии с правилами и регламентами этих систем, правилами и регламентами СКЗИ КриптоПро CSP, а также с учетом положений настоящей Инструкции.

Носитель поддерживает протокол CCID и не требует установки дополнительных драйверов.

Основным назначением Носителя является:

- обеспечение защищенного хранения ключей и сертификатов, применяемых в рамках информационной технологии криптопровайдеров КриптоПро CSP;
- обеспечение защиты критических данных в случае утери или хищения Носителя, а также от их перехвата в канале связи с крипто провайдером;
- обеспечение возможности выполнения административных функций связанных с разблокировкой Носителя, заблокированного по причине превышения допустимого числа попыток неудачного предъявления пароля пользователя (ПИН пользователя).

Носитель R301 ФОРОС USB-ФКН, смарт-карта ФОРОС-ФКН для СКЗИ «КриптоПро CSP» (сертификат ФСБ) представляет собой исполнение сертифицированного СКЗИ Форос 2.

Сертификаты соответствия:

- сертификаты ФСБ России СФ/114-3909, СФ/124-3910 от 22.09.2020, выписка из Заключения ЦЗИ и СС ФСБ России (предоставляется по отдельному запросу);
- сертификат ООО «КРИПТО-ПРО» от 24.01.2021г.;

На Носитель распространяется действие сертификата ФСТЭК России №4490 от 14 декабря 2021 г. (ПАК ФОРОС 2 6958 6427.58.29.29.000.003).

Носитель работает в любых ОС с поддержкой спецификации PCSC. В частности:

- Microsoft Windows 7 и новее
- Microsoft Windows Server 2008 и новее
- GNU/Linux, в том числе отечественные
- Apple macOS 10.9 и новее
- Android 5 и новее
- iOS 11 и новее
- Аврора 4+

Поддерживаемые ОС в рамках работы носителя с СКЗИ «КриптоПро CSP» смотрите в формуляре соответствующей версии СКЗИ «КриптоПро CSP».

Поддерживаемые ОС в рамках работы носителя с СКЗИ «VipNet CSP» смотрите в формуляре соответствующей версии СКЗИ «VipNet CSP».

2 Технические характеристики и конфигурация

Носитель содержит защищенный микроконтроллер с объемом энергонезависимой памяти 80 или 160 Кбайт, в которой размещается его файловая структура.

Основные характеристики Носителя приведены в таблице:

Параметр	R301 Форос 80	R301 Форос 160
Технические характеристики		
Физический объем защищенной памяти	80 Кбайт	160 Кбайт
Тип USB-разъема	Стандартный Тип А	
Интерфейс подключения	USB 2.0 Full Speed Device, 12 Мбит/сек	
Скорость обмена данными	до 323 Кбит/сек, 4 МГц; 500кбит/сек, 6МГц	
Поддерживаемые протоколы	ISO 7816 T=0	
Скорость чтения данных	до 13000 байт/с	
Поддержка CCID	Есть	
Габаритные размеры [Д х Ш х В]	48 х 16 х 8 мм	
Масса	6.3 г. +\-10%	
Потребляемая мощность	около 130 мВт в активном состоянии	
Диапазон рабочих температур	от 0 до +50˚С	
Диапазон температур хранения	от -20 до +50˚С	
Допустимая относительная влажность	от 0 до 85% (без конденсата)	
Время хранения данных	30 лет	
Гарантированное количество циклов стирания\записи	500 000	

Типовые параметры логической конфигурации		
Число контейнеров	2	8
Размер контейнера (допустимый размер сертификата)	7 Кбайт	7 Кбайт
Максимальное число последовательных неуспешных попыток ввода пароля пользователя	10	
Допустимое общее число неудачных попыток предъявления паролей пользователя и администратора	96	
Функция разблокирования/восстановления пароля пользователя по паролю администратора	Есть	
Максимальное число последовательных неуспешных попыток ввода пароля администратора	10	
Допустимые размеры паролей пользователя и администратора	От 6 до 160 символов	
Функция форматирования (очистки)	Нет	
Транспортное значение пароля Пользователя [символы ASCII – текста]	123456	
Транспортное значение пароля Администратора [символы ASCII – текста]	123456	

Возможно изменение параметров конфигурации Носителя и/или встраивание в Носитель дополнительных функциональных приложений, разработанных по запросам корпоративных Заказчиков.

3 Аппаратные криптографические возможности

- ГОСТ Р 34.10-2001 генерация ключевых пар с проверкой качества, формирование и проверка электронной подписи;

- ГОСТ Р 34.10-2012/ГОСТ 34.10-2018 (256 бит и 512 бит[1,2]): генерация ключевых пар с проверкой качества, формирование и проверка электронной подписи;

- ГОСТ Р 34.11-94: вычисление значения хеш-функции данных, в том числе с возможностью последующего формирования электронной подписи;

- ГОСТ Р 34.11-2012/ГОСТ 34.11-2018 (256 бит и 512 бит[1,2]): вычисление значения хеш-функции данных, в том числе с возможностью последующего формирования электронной подписи;

- ГОСТ 28147-89: генерация ключей шифрования, шифрование данных в режимах простой замены, гаммирования и гаммирования с обратной связью, вычисление и проверка криптографической контрольной суммы данных (имитовставки ГОСТ);

- ГОСТ Р 34.12-2015/ГОСТ 34.12-2018, ГОСТ Р 34.13-2015/ГОСТ 34.13-2018 алгоритм шифрования «Кузнечик»: генерация и импорт ключей

шифрования, шифрование данных в режимах простой замены, гаммирования и гаммирования с обратной связью, вычисление и проверка криптографической контрольной суммы данных (имитовставки ГОСТ)[1,2];

- ГОСТ Р 34.12-2015/ГОСТ 34.12-2018, ГОСТ Р 34.13-2015/ГОСТ 34.13-2018 алгоритм шифрования «Магма»: генерация и импорт ключей шифрования, шифрование данных в режимах простой замены, гаммирования и гаммирования с обратной связью, вычисление и проверка криптографической контрольной суммы данных (имитовставки ГОСТ)[2,3];

- выработка сессионных ключей (ключей парной связи):

- по схеме VKO GOST R 34.10-2001 (RFC 4357);
- по схеме VKO GOST R 34.10-2012 (RFC 7836)[2,3];

- Расшифрование по схеме EC El-Gamal[2];

- RSA: поддержка ключей размером 1024, 2048, 4096[4] бит, генерация ключевых пар с настраиваемой проверкой качества[4], импорт ключевых пар, формирование электронной подписи;

- ECDSA с кривыми secp256k1[4] и secp256r1[2]: генерация ключевых пар с настраиваемой проверкой качества, импорт ключевых пар, формирование электронной подписи;

- генерация последовательности случайных чисел требуемой длины

1 – в СКЗИ «ФОРОС 2» применяется совместно с использованием соответствующего криптопровайдера

2 – доступно в СКЗИ «ФОРОС 3»

3 – доступно в СКЗИ «ФОРОС 2»

4 – применяется совместно с использованием соответствующего криптопровайдера

4 Световая индикация режимов работы

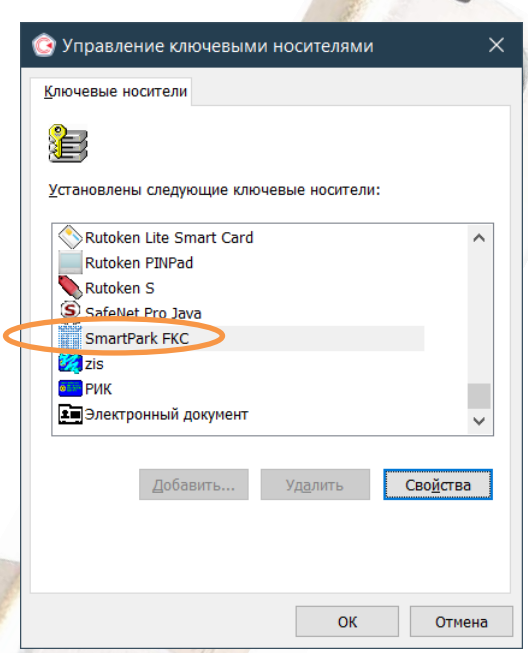
Носитель имеет два встроенных светодиодных индикатора. Красный индикатор отображает состояние процессов информационного обмена смарт-карт ридера с компьютером по USB, синий - отображает состояние процессов информационного обмена смарт-карт ридера с установленной в него смарт-картой.

Детализация состояний индикаторов приведена в нижеследующей таблице:

Назначение индикатора	Цвет	Состояние	Процесс
Индикатор USB	**Красный**	Мигает	Установка соединения по USB
		Непрерывно светит	Соединение по USB установлено
		Мигает нерегулярно	Обмен данными по USB
Индикатор смарт-карты	**Синий**	Выключен	Смарт-карты нет или она неисправна
		Непрерывно светит	Смарт-карта установлена
		Мигает	Обмен данными со смарт-картой

5 Поддержка Носителя в КриптоПро CSP

Программный модуль поддержки Носителя встроен в дистрибутив КриптоПро CSP (начиная с версии 5.0 R2 и далее во всех последующих) Дополнительная инсталляция Носителя в криптопровайдере не требуется.
Носитель распознается встроенным в КриптоПро CSP модулем поддержки как носитель «SmartPark FKC».



Оснастка КриптоПро CSP/Оборудование/Настроить типы носителей.

6 Эксплуатация

6.1 Схема разграничения доступа к данным ФКН-Носителя

Доступ к контейнерам КриптоПро CSP на Носителе защищается Паролем Пользователя (иначе - ПИН Пользователя или Пароль носителя). Сервисы КриптоПро CSP запрашивают ПИН Пользователя при выполнении операций, требующих доступа к закрытой информации, хранящейся на Носителе.

У Пользователя есть 10 (Десять) попыток (параметр устанавливается по умолчанию) для ввода (предъявления) правильного значения ***ПИН*** (Пароля) Пользователя.

Если все разрешенные попытки предъявления ПИН (Пароля) Пользователя будут неудачными, то механизм его ввода будет **заблокирован** внутренними средствами Носителя. Соответственно последующий доступ к закрытой информации Носителя будет невозможен даже в случае ввода верного значения Пароля Пользователя.

Разблокирование механизма ввода Пароля Пользователя и некоторые другие административные функции можно выполнить лишь при условии подтверждения оператором права Администратора путем успешного ввода Пароля Администратора (иначе – PUK-код).

Механизм ввода ***PUK-кода*** допускает строго ограниченное число последовательных попыток неудачного ввода. При достижении этого числа PUK-код безвозвратно блокируется и административные операции на таком носителе становятся невозможными.

При выполнении операции разблокирования Пароля Пользователя по PUK, предусматривается также возможность ввода нового значения Пароля Пользователя

6.2 Транспортные значения пароля Пользователя и PUK-кода

ФКН-Носитель имеет механизм индикации наличия транспортных (первичных) значений паролей.

При поставке ФКН-Носителей, производитель устанавливает Пароль (ПИН) Пользователя и PUK (ПИН Администратора) в транспортные (первичные) значения, которые приведены в разделе 2 (Технические характеристики и конфигурация) данного документа.

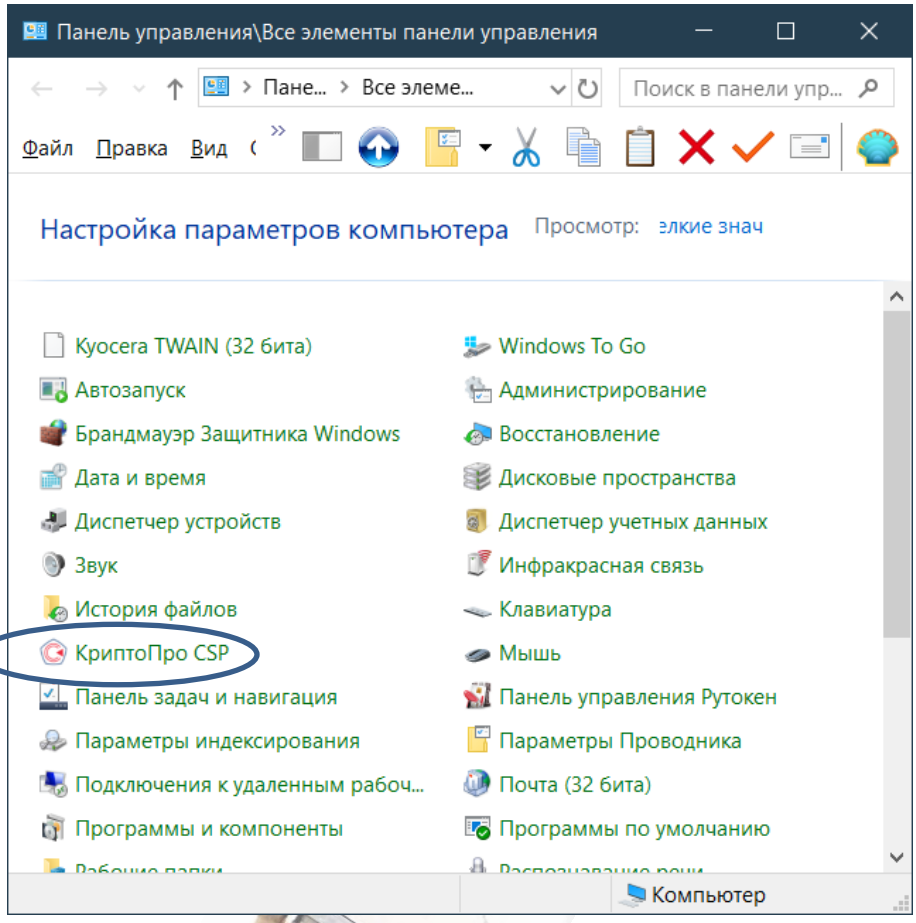
Криптопровайдер, при обнаружении Носителя с первичной установкой паролей, всегда выдает запрос на смену этих значений на рабочие перед выполнением любых операций, требующих предъявления паролей Носителя.

6.3 Механизмы администрирования ФКН- Носителя

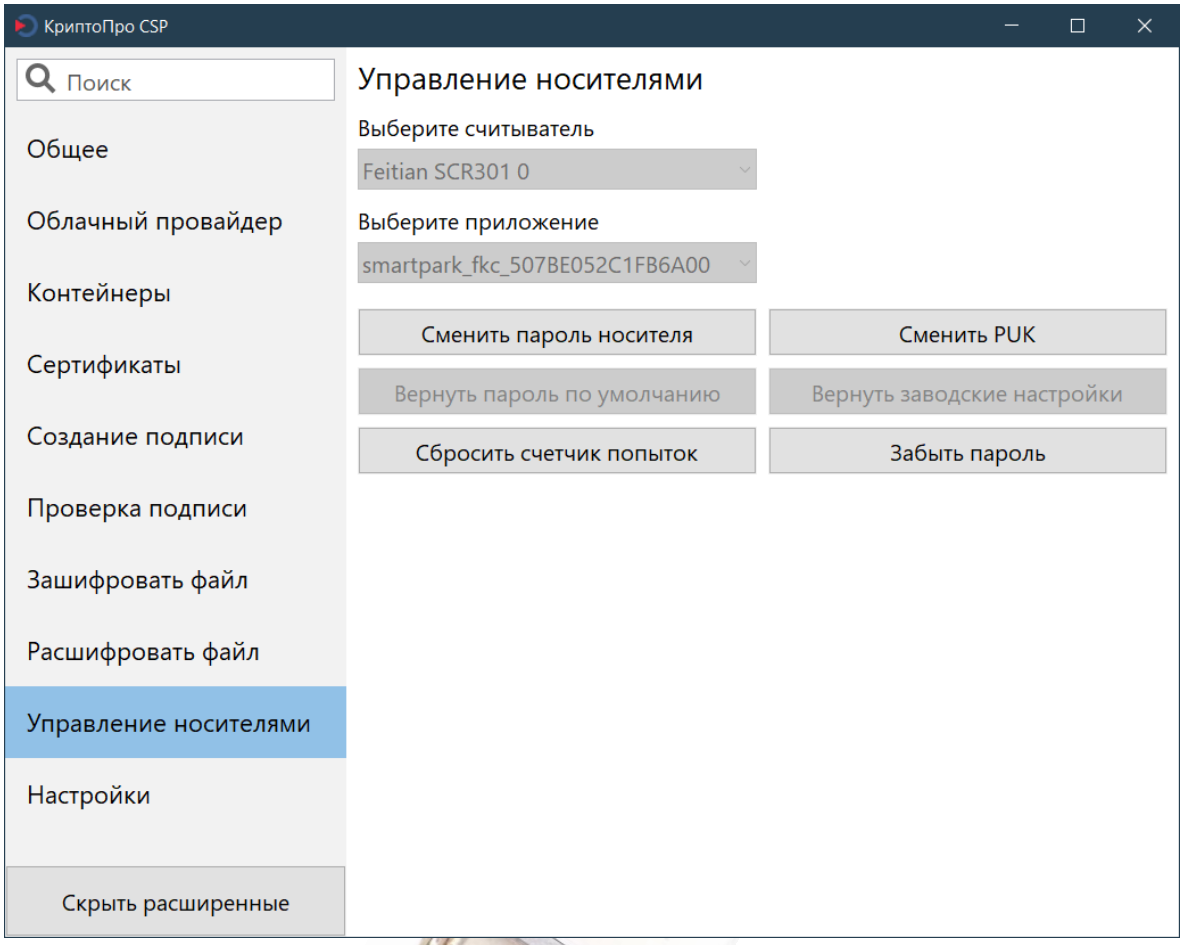
Набор административных функций Носителя включает:

- функция изменения и разблокирования Пароля Пользователя;
- функции изменения значения Пароля Администратора (PUK-кода);
- контрольные функции (проверка СЗИ).

Функции администрирования ФКН-Носителем реализуются через функции панели управления КриптоПро CSP (устанавливается автоматически при установке криптопровайдера)



а также с помощью функций, входящих в состав ПО «Инструменты КриптоПро CSP» (устанавливается автоматически при установке криптопровайдера):



Также функции администрирования ФКН-Носителем реализуются с помощью программного обеспечения Форос-Мастер предназначенного для административного управления приложениями носителей семейства R301 ФОРОС USB/смарт-карты ФОРОС (вкладка «КриптоПро CSP-ФКН»).

Программа Форос-мастер может быть загружена с сайта ООО «СмартПарк» по ссылке:

http://smart-park.ru/wp-content/uploads/utils/FMaster.zip

6.4 Смена ПИН (пароля) Пользователя

Внимание!

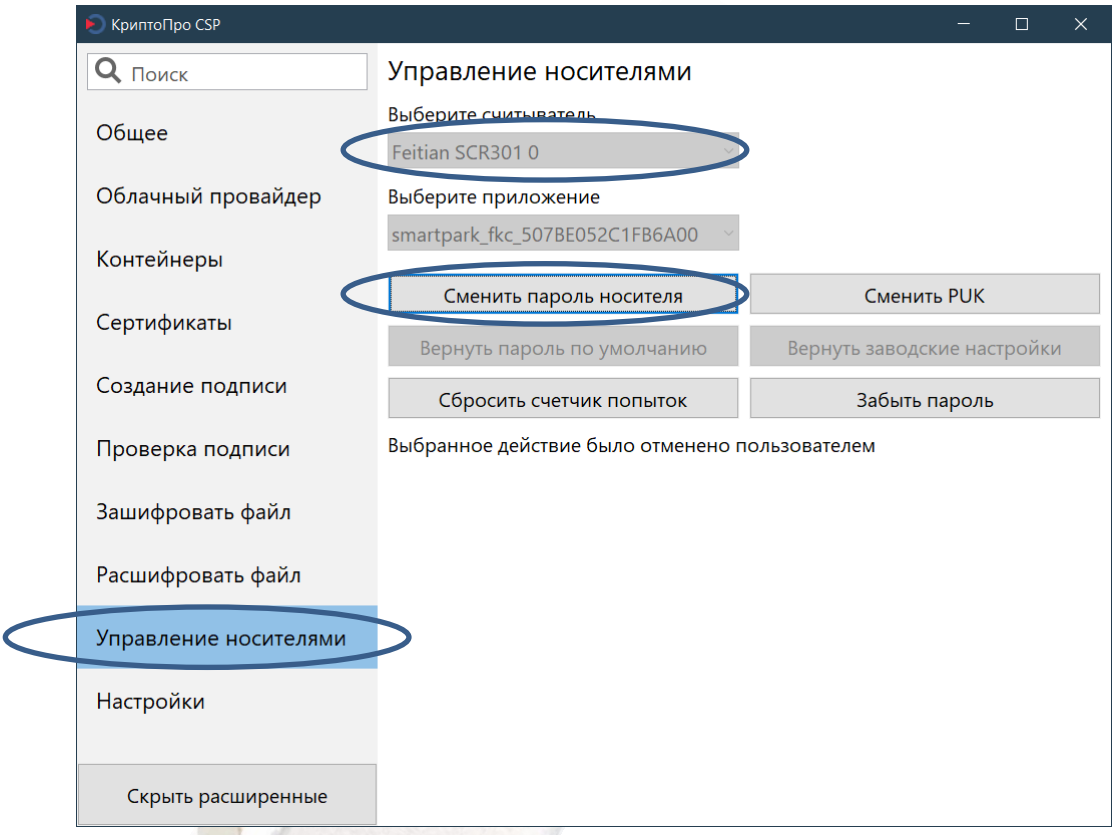
При вводе Носителя в эксплуатацию, Пользователь должен сменить установленное производителем транспортное значение Пароля Пользователя, на собственное.

Сохранение в тайне рабочего значения Пароля Пользователя и его своевременная смена, являются необходимыми условиями безопасной эксплуатации Носителя в рамках сервисов криптопровайдера.

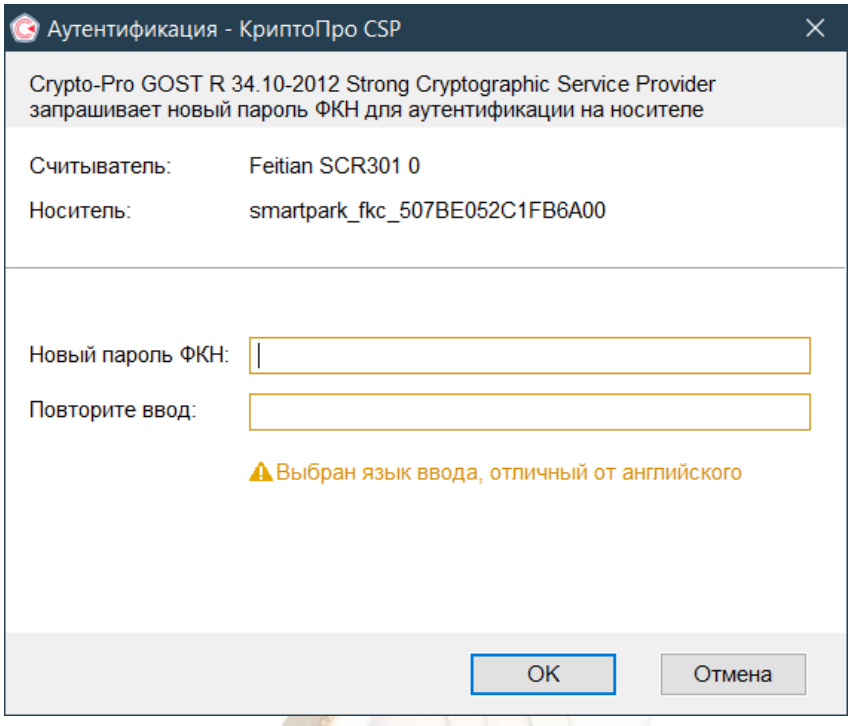
Производитель настоятельно рекомендует не использовать простых комбинаций символов для Пароля Пользователя.

6.4.1 Установка рабочих значений паролей

Запустите программу, далее выберите вкладку /«Управление носителями». После этого выберите Носитель (вкладка «Выберите считыватель» Feitian SCR301, если используете Носитель R301 ФОРОС USB-ФКН) и затем активируйте функцию «Сменить пароль носителя».



В открывшемся окне «Аутентификация-КриптоПро CSP» введите рабочее значение Пароля Пользователя в строку «Новый пароль ФКН»



Аналогичные действия следует выполнить для PUK-кода. Для этого активируйте функцию «Сменить PUK».

Смена транспортных паролей также можно произвести во время записи ключа/сертификата на носитель. Если на данном носителе установлены транспортные пароли, то в таком случае интерфейс КриптоПро CSP сам предложит сменить пароли.

Смена транспортных значений паролей также может быть выполнена с помощью ПО «Форос-Мастер» (вкладка «КриптоПро CSP-ФКН», действие «Разблокировать и сменить») включая поточную смену на нескольких носителей с использованием пакетного режима.

6.4.2 Смена рабочих значений паролей

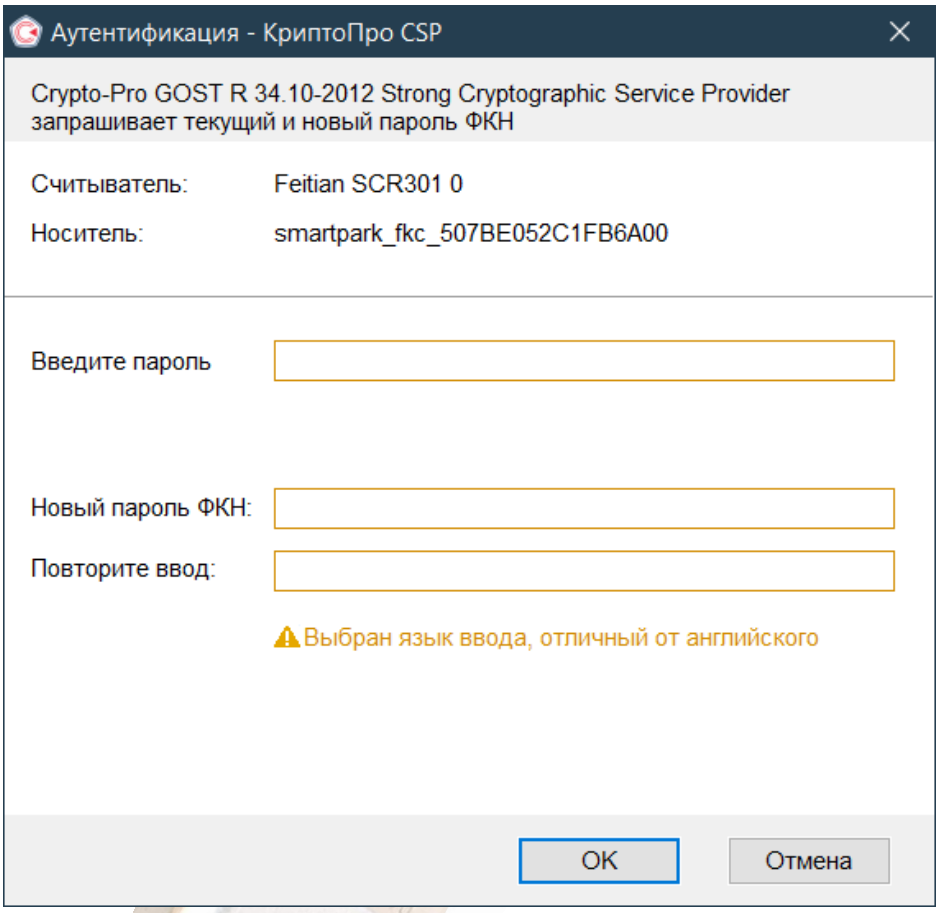
Смену рабочих паролей можно выполнить средствами ПО «Инструменты КриптоПро CSP», а также через Панель управления КриптоПро CSP и ПО «Форос-Мастер» (вкладка «КриптоПро CSP-ФКН», действие «Разблокировать и сменить», «Сменить»).

6.4.2.1 Смена рабочих значений паролей средствами ПО «Инструменты КриптоПро CSP»

Запустите программу, далее выберите вкладку /«Управление носителями». После этого выберите Носитель (вкладка «Выберите считыватель» Feitian SCR301, если используете Носитель R301 ФОРОС USB-ФКН) и затем активируйте функцию «Сменить пароль носителя».

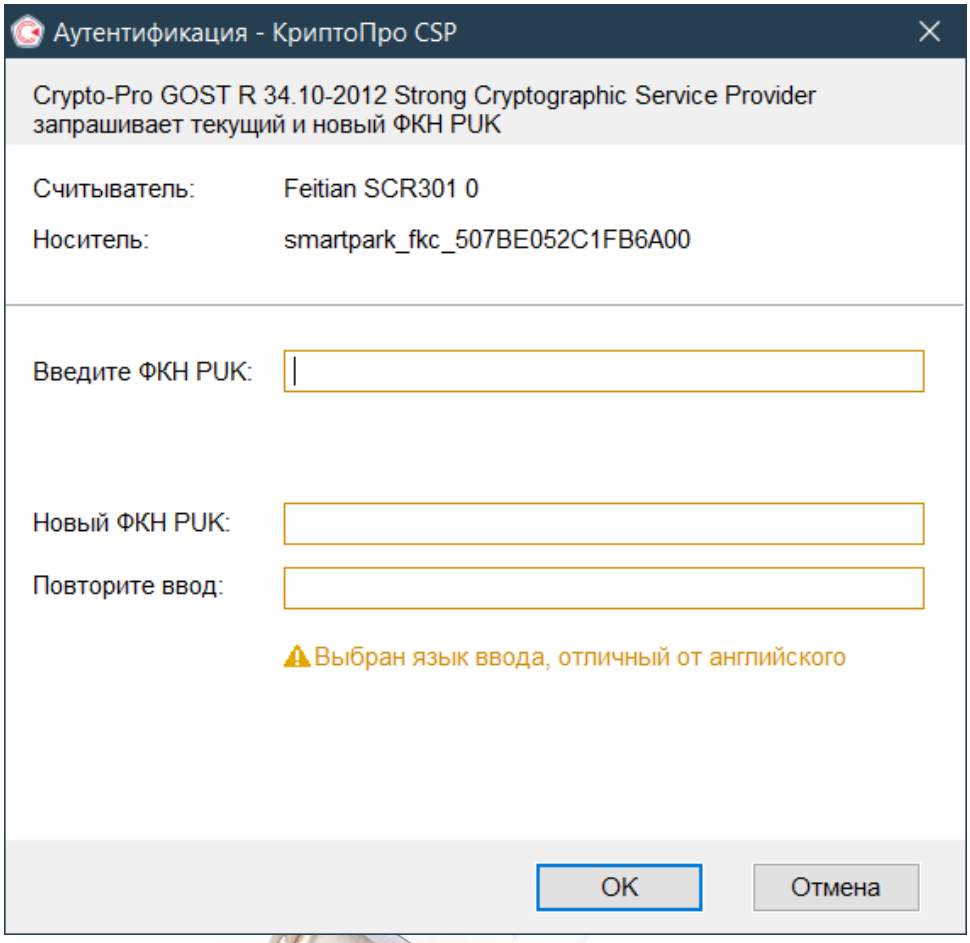
В открывшемся окне «Аутентификация-КриптоПро CSP» введите

рабочее значение Пароля Пользователя в строку «Введите пароль», а затем введите устанавливаемое значение в поле «Новый пароль ФКН»



Если исходное рабочее значение Пароля Пользователя было указано верно, а также совпадают новое значение пароля и его дубль, то в носителе будет установлено новое рабочее значение Пароля Пользователя.

Аналогичные действия следует выполнить для смены рабочего значения PUK-кода на новое. Для этого активируйте функцию «Сменить PUK» и заполните соответствующую экранную форму.

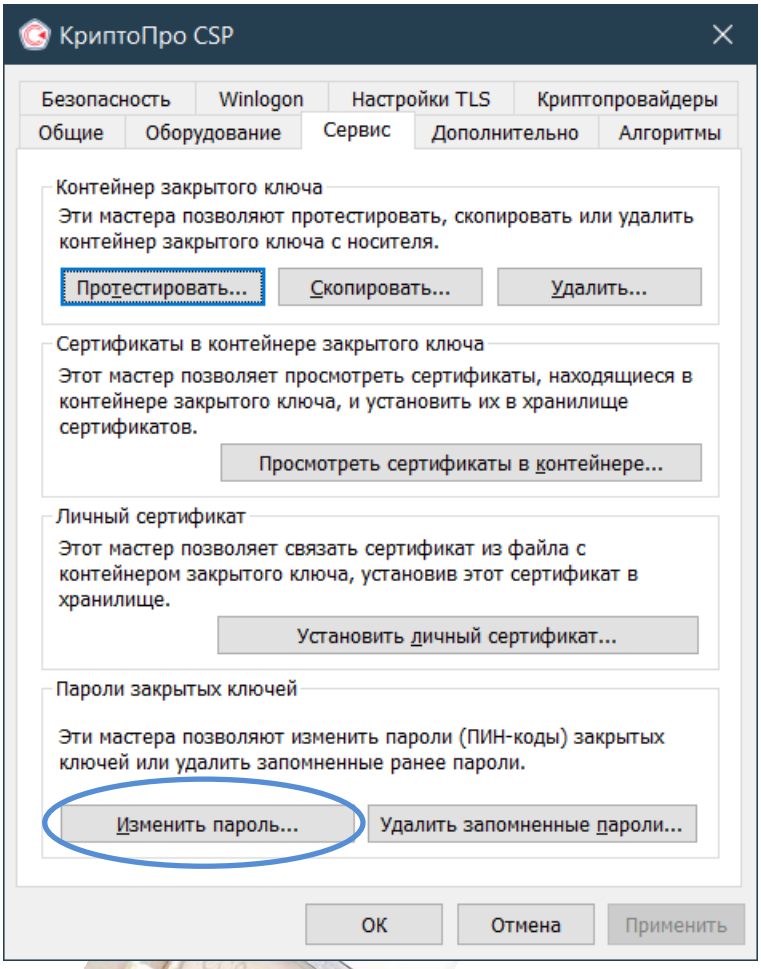


6.4.2.2 Смена Пароля Пользователя через Панель управления КриптоПро CSP

Смена Пароля Пользователя ФКН-Носителя возможна также через «Панель управления» криптопровайдера КриптоПро CSP.

Откройте оснастку управления КриптоПро CSP в «Панели управления» (Пуск/Настройка/Панель управления/КриптоПро CSP)

Далее выберите вкладку «Сервис» и нажмите кнопку «Изменить пароль»:



Далее следуйте указаниям мастера изменения пароля.

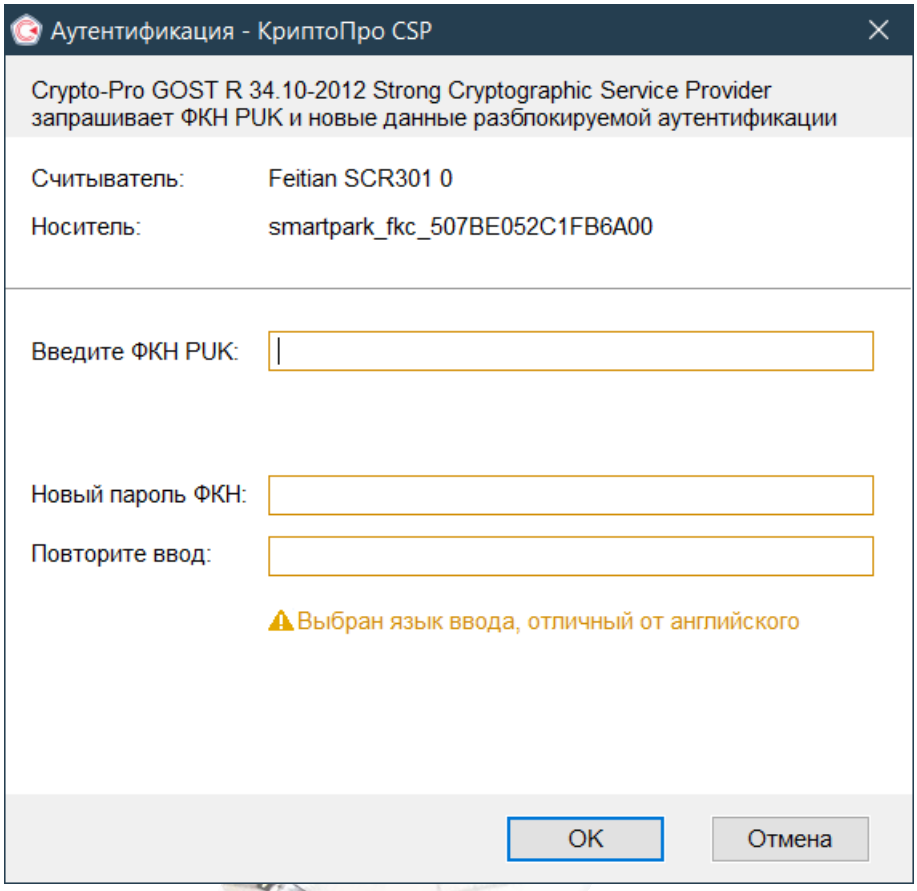
Эта процедура происходит в соответствии с регламентом КриптоПро CSP и описана в документации на криптопровайдер.

Примечание. Если носитель еще не содержит ключей и сертификатов, то тогда смену паролей можно выполнить средствами ПО «Инструменты КриптоПро CSP» или ПО «Форос-Мастер».

6.5 Разблокировка ПИН (пароля) Пользователя

Разблокирование Пароля Пользователя может быть выполнено как через Панель управления, так через ПО «Инструменты КриптоПро CSP» и ПО «Форос-Мастер» (вкладка «КриптоПро CSP-ФКН», действие «Разблокировать и сменить»).

Экранная форма функции разблокирования предлагается оператору автоматически, если вы пытаетесь использовать носитель с заблокированным паролем Пользователя:



6.6 Справочные функции

6.6.1 Получение количества оставшихся попыток предъявления Пароля Администратора/Пользователя

Число оставшихся попыток предъявления Пароля Пользователя и PUK выводятся на экран в составе информации, выводимой при их неуспешном предъявлении .

Также справочная информация доступна с помощью и ПО «Форос-Мастер» (вкладка «Общее»).

7 Контроль носителя

Контроль подлинности/целостности Носителя в соответствии с требованиями ФСБ, производится по ключевой контрольной сумме. Операции контроля выполняются в соответствии с п. 5 Формуляра 6958 6427.58.29.29.000.002.30.01.1. Формуляр и/или программное средство контроля предоставляется Заказчику отдельному запросу.

Контроль подлинности/целостности изделия по требованиям ФСТЭК производится по ключевой контрольной сумме, контроль целостности - по контрольной сумме CRC32. Операции контроля выполняются в соответствии

с п. 6.1 Формуляра 6958 6427.58.29.29.000.003.30.01.1. Операция контроля по CRC32 выполняется средствами административной утилиты. Программное средство контроля может быть получено с сайта компании ООО «СмартПарк» со страницы:

http://www.smart-park.ru/index.php/support/driver.html
или непосредственно по ссылке:
http://smart-park.ru/util/checkSZI.zip

Также операции контроля доступны с помощью и ПО «Форос-Мастер» (вкладка «Общее», действия «Проверка целостности», «Проверка целостности и подлинности»).

8 Требования к условиям применения

8.1 Условия применения

1. Носители предназначаются для использования в закрытых помещениях, в условиях влажности воздуха без конденсации влаги, при температуре окружающей среды от 0º С до плюс 50º С.
2. Носители не должны подвергаться механическим воздействиям, приводящим к деформации, нарушению целостности корпуса, USB-разъема, внутренней платы.
3. Носители можно подключать только к USB-разъемам исправного компьютера. Параметры USB-порта должны соответствовать спецификации для USB.
4. Для подключения Носителей не рекомендуется использовать USB-удлинители, а также USB-хабы без дополнительного питания.
5. Запрещается извлекать Носитель из порта компьютера, если на Носителе происходит работа с данными и мигает светодиодный индикатор.
6. Не рекомендуется оставлять Носитель подключенным к компьютеру во время перезагрузки, ухода в режим sleep.
7. Не рекомендуется оставлять Носитель подключенным к компьютеру, когда он не используется.
8. На время работы с Носителем рекомендуется отключать не используемые в настоящий момент USB-устройства и носители других типов.
9. Носители нельзя подвергать воздействию влаги, воздействию паров кислот, щелочей и других агрессивных примесей. Для очистки корпуса и разъема USB-носителя используйте сухую ткань. Использование органических растворителей недопустимо.
10. Запрещается разбирать Носители.

8.2 Условия хранения

При складском хранении должны обеспечиваться следующие условия:

- хранение в складских помещениях, защищающих Носители от воздействия атмосферных осадков, в упаковке при отсутствии в воздухе паров кислот, щелочей и других агрессивных примесей;
- при длительном хранении Носителей, в складских помещениях должна обеспечиваться температура от плюс 5 до плюс 30°С и относительная влажность воздуха не более 85%;
- предельная температура хранения составляет от минус 20°С до плюс 50°С.

При хранении не допускаются резкие изменения температуры окружающего воздуха (более 20°С в час);

Распаковку Носителей в зимнее время после воздействия отрицательных температур следует производить в отапливаемом помещении, предварительно выдержав его в этом помещении не распакованным не менее двух часов.

8.3 Условия транспортировки

Транспортирование Носителей может производиться авиационным, автомобильным, железнодорожным или иным транспортом в условиях, исключающих механические повреждения, прямое попадание на транспортную упаковку влаги, пыли и грязи, превышение предельных значений температуры окружающей среды.

При транспортировке должны соблюдаться следующие условия:

- температура окружающего воздуха от –20°С до +50°С;
- относительная влажность воздуха до 95% (без конденсации);
- исключение прямого воздействия солнечных лучей, атмосферных осадков и агрессивных примесей (паров кислот, щелочей);
- отсутствие повреждений упаковки.

После транспортировки Носителей при пониженной температуре, при последующем повышении температуры до нормальной, возможна конденсация влаги, в этом случае Носители необходимо выдержать при комнатной температуре до полного испарения конденсата.