КриптоПро CSP 5.0 R2

Рутокен используется для безопасного хранения ключей и сертификатов для квалифицированной электронной подписи (КЭП) в контейнерах КриптоПро CSP.

На устройстве объемом 64 Кб можно хранить до 15 ключевых контейнеров.

Для работы КриптоПро CSP с современными устройствами Рутокен не требуется дополнительных настроек. Все необходимые настройки выполняются автоматически при установке криптопровайдера.

Устройства Рутокен работают в семействах операционных систем Windows, Linux (включая отечественные) и macOS. Часть моделей семейства Рутокен ЭЦП работают в мобильных операционных системах Android, iOS и Sailfish OS RUS (переименованная в Аврору).

Совместимость подтверждается сертификатами совместимости.

В КриптоПро CSP 5.0 и новее появился режим, в котором Рутокен выступает как средство формирования электронной подписи – «активный вычислитель». В данном режиме использование КЭП возможно практически во всех продуктах КриптоПро.
Рутокен – рекомендуемый ключевой носитель КЭП при работе с КриптоПро CSP всех версий.

Режимы работы с Рутокенами, доступные в КриптоПро 5.0 R2

1. Работа с внутренним криптоядром Рутокена через библиотеку PKCS#11

Установка на Windows

- Если на компьютере с ОС Windows установлены Драйверы Рутокен, и производится **первичная установка** КриптоПро CSP 5.0 R2, то **необходимая настройка системы будет выполнена автоматически**.
- При **обновлении** программы **с предыдущих версий КриптоПро CSP**, нужно:

  1) Установить актуальную версию «Драйверов Рутокен» (или библиотеку rtpkcs11ecp для Linux и macOS)

  2) Запустить «КриптоПро CSP» с правами Администратора

  3) Выбрать «Оборудование» - «Настроить считыватели» - «Считыватель смарт-карт PKCS#11»

Установка на Linux

Перед инсталляцией КриптоПро необходимо установить библиотеку rtpkcs11ecp.so. Доступна по ссылке https://www.rutoken.ru/support/download/pkcs/

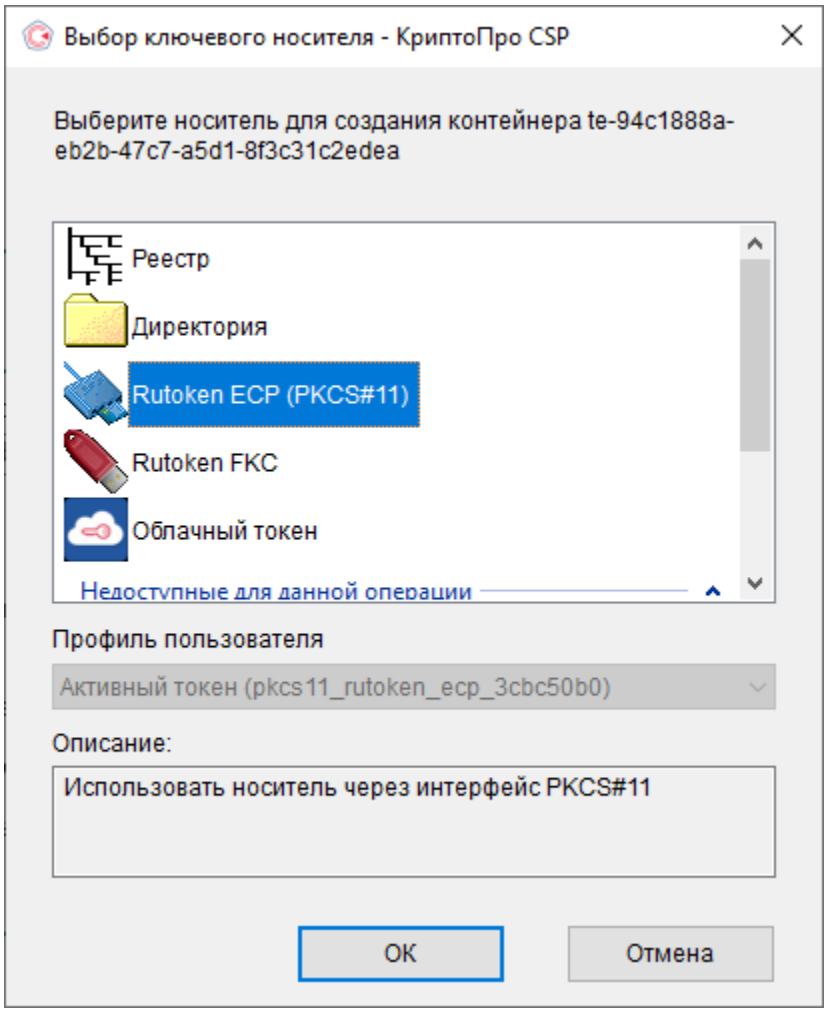
- Если установка КриптоПро происходит скриптом install_gui.sh, то необходимо отметить пункт "Поддержка токенов и смарт-карт".
- Если установка КриптоПро происходит скриптом install.sh, то после установки основных пакетов необходимо установить пакеты cprocsp-rdr-cryptoki и cprocsp-rdr-rutoken.

- Линейка устройств Рутокен ЭЦП 3.0
- Рутокен ЭЦП 2.0 2100
- Рутокен ЭЦП 2.0 (micro)
- Рутокен ЭЦП 2.0 3000 (Type-C/micro)
- Рутокен ЭЦП 2.0 Flash/Touch
- Рутокен ЭЦП Bluetooth
- Рутокен ЭЦП PKI
- Смарт-карты Рутокен ЭЦП 2.0 2100
- Смарт-карты Рутокен ЭЦП SC
- Смарт-карта Рутокен ЭЦП 3.0 NFC по контактному подключению

Работа теперь возможна через библиотеку rtpkcs11ecp. В этом режиме ключи создаются сразу в защищенной памяти устройства.
Этот режим предотвращает извлечение ключа в память компьютера в момент подписания.

Ключи и сертификаты, созданные в этом режиме полностью совместимы с ключами, созданными, например, через Рутокен Плагин.

При создании ключей необходимо выбирать считыватель **PKCS#11**.



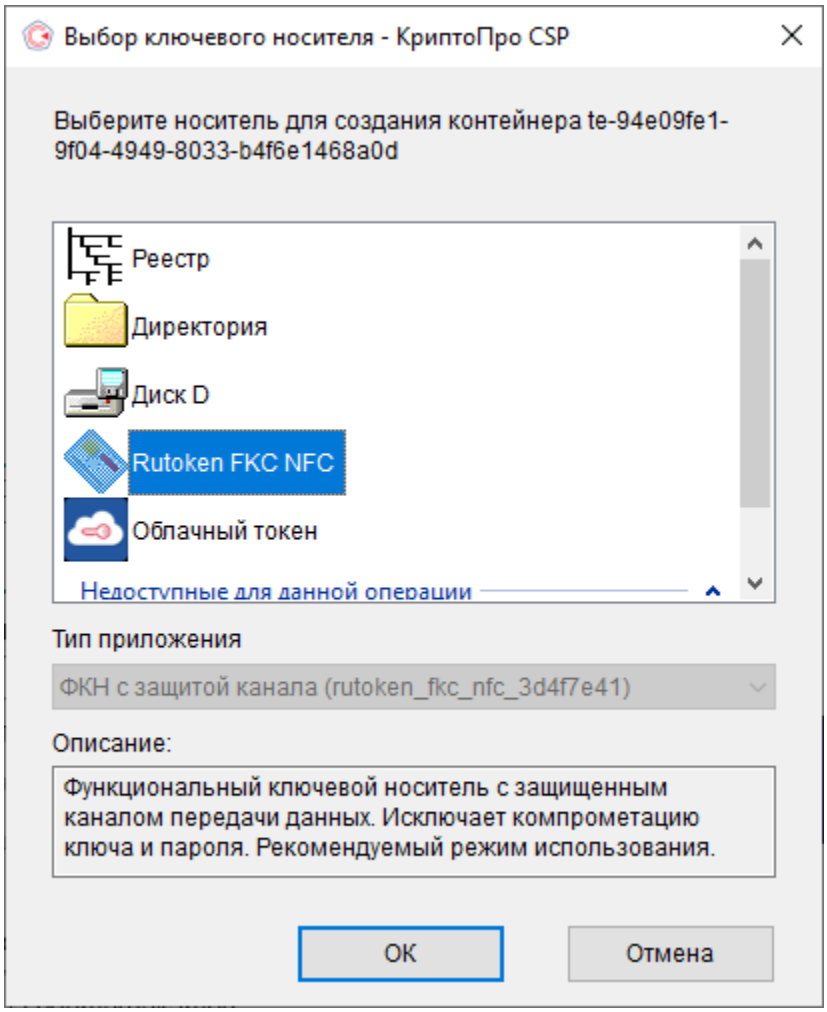
Для работы со смарт-картой Рутокен ЭЦП 3.0 NFC по беспроводному каналу NFC, необходимо выбирать режим "Работа с внутренним криптоядром Рутокена с обеспечением защиты канала".

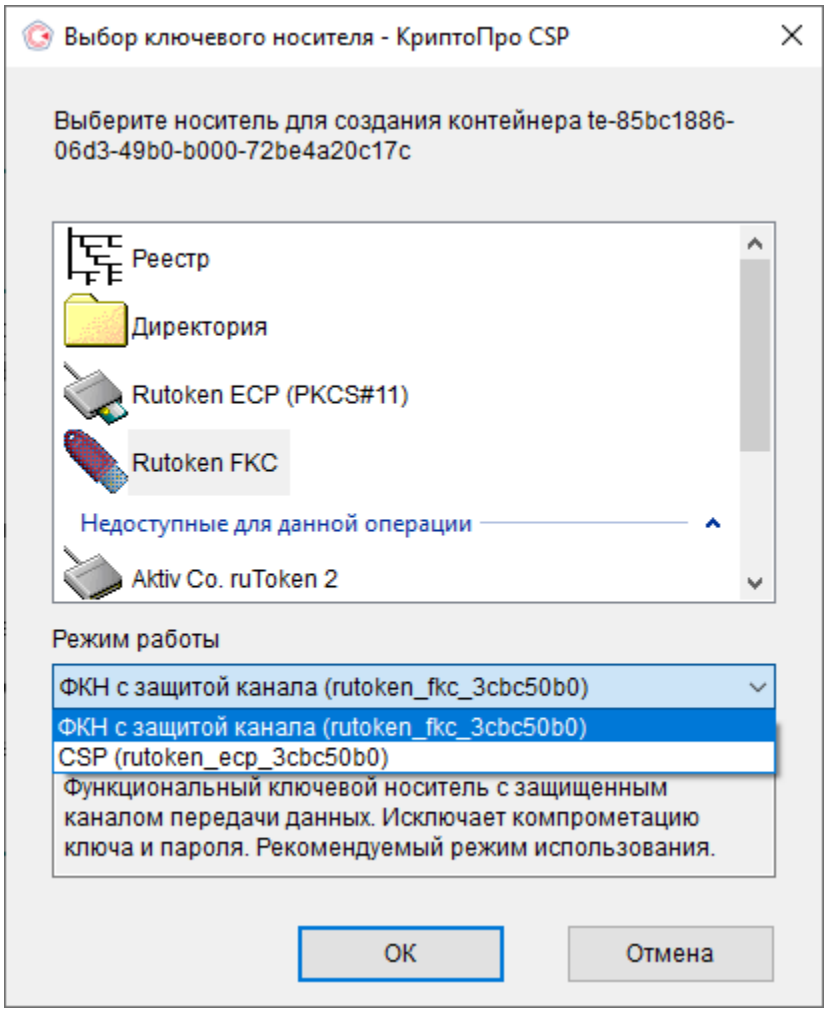
2. Работа с внутренним криптоядром Рутокена с обеспечением защиты канала

В КриптоПро CSP версии 5.0 реализован криптографический протокол SESPAKE, который поддерживается во всех моделях линейки Рутокен ЭЦП 3.0 и в модели Рутокен ЭЦП 2.0 3000.

Данный протокол позволяет провести аутентификацию, не передавая в открытом виде PIN-код Пользователя, и установить зашифрованный канал для обмена сообщениями между криптопровайдером и носителем.
Для работы в режиме функционального ключевого носителя (ФКН) при генерации надо выбирать: "**ФКН с защитой канала** (rutoken_fkc_xxxxxxxx)".

Для работы с Рутокен ЭЦП 3.0 NFC по беспроводному каналу NFC, необходимо выбирать данный режим.


Выбор ключевого носителя - КриптоПро CSP
Выберите носитель для создания контейнера te-94e09fe1-9f04-4949-8033-b4f6e1468a0d
Реестр
Директория
Диск D
Rutoken FKC NFC
Облачный токен
Недоступные для данной операции
Тип приложения
ФКН с защитой канала (rutoken_fkc_nfc_3d4f7e41)
Описание:
Функциональный ключевой носитель с защищенным каналом передачи данных. Исключает компрометацию ключа и пароля. Рекомендуемый режим использования.
OK
Отмена

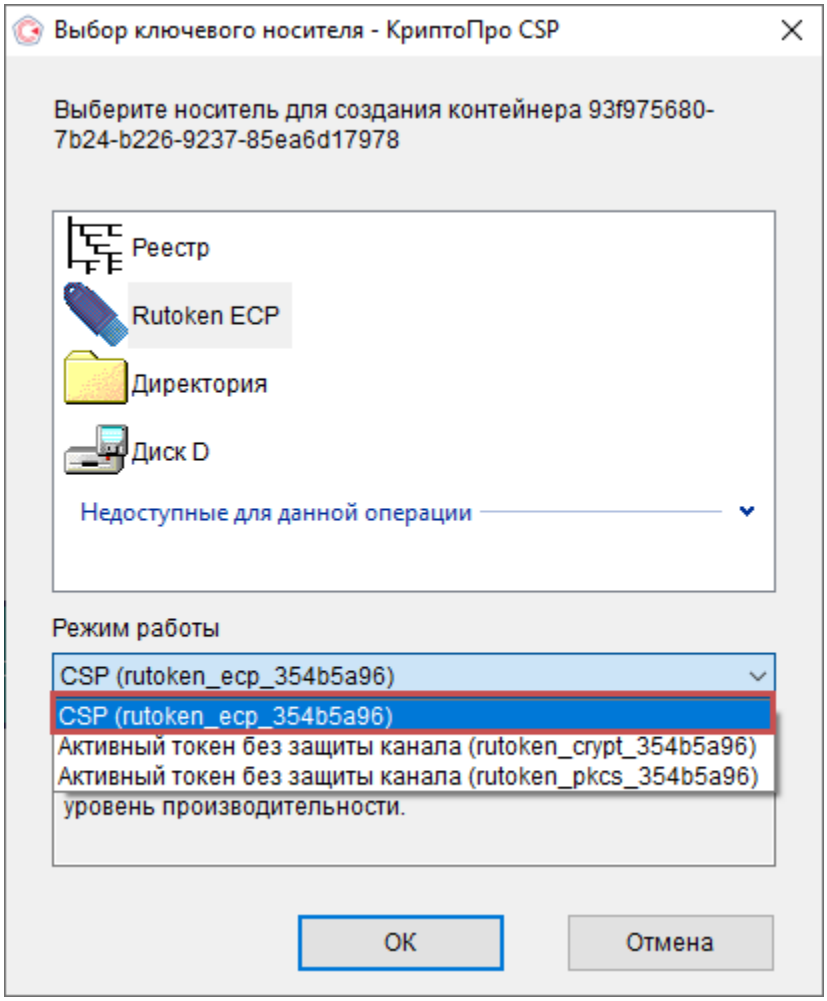

Выбор ключевого носителя - КриптоПро CSP
Выберите носитель для создания контейнера te-85bc1886-06d3-49b0-b000-72be4a20c17c
Реестр
Директория
Rutoken ECP (PKCS#11)
Rutoken FKC
Недоступные для данной операции
Aktiv Co. ruToken 2
Режим работы
ФКН с защитой канала (rutoken_fkc_3cbc50b0)
ФКН с защитой канала (rutoken_fkc_3cbc50b0)
CSP (rutoken_ecp_3cbc50b0)
Функциональный ключевой носитель с защищенным каналом передачи данных. Исключает компрометацию ключа и пароля. Рекомендуемый режим использования.
OK
Отмена

3. Хранение в защищенной файловой системе Рутокен

Как и в КриптоПро CSP версии 4.0, использование Рутокена в этом режиме позволяет обезопасить ключевую информацию от несанкционированного использования. Ключи и сертификаты надежно хранятся в защищенной файловой системе Рутокена.

- Линейка устройств Рутокен ЭЦП 3.0
- Рутокен ЭЦП 2.0 2100 (Type-C/micro)
- Рутокен S (micro)
- Рутокен Lite (micro)
- Рутокен ЭЦП Flash
- Рутокен ЭЦП 2.0 (micro)
- Рутокен ЭЦП 2.0 Touch
- Рутокен ЭЦП 2.0 3000 (Type-C/micro)
- Рутокен ЭЦП PKI
- Рутокен ЭЦП Bluetooth
- Смарт-карта Рутокен ЭЦП SC
- Смарт-карта Рутокен ЭЦП 2.0
- Смарт-карта Рутокен ЭЦП 3.0 NFC по контактному подключению

Для генерации такого типа ключей надо выбирать режим работы: "**CSP** (rutoken_xxxx_xxxxxxxx)".



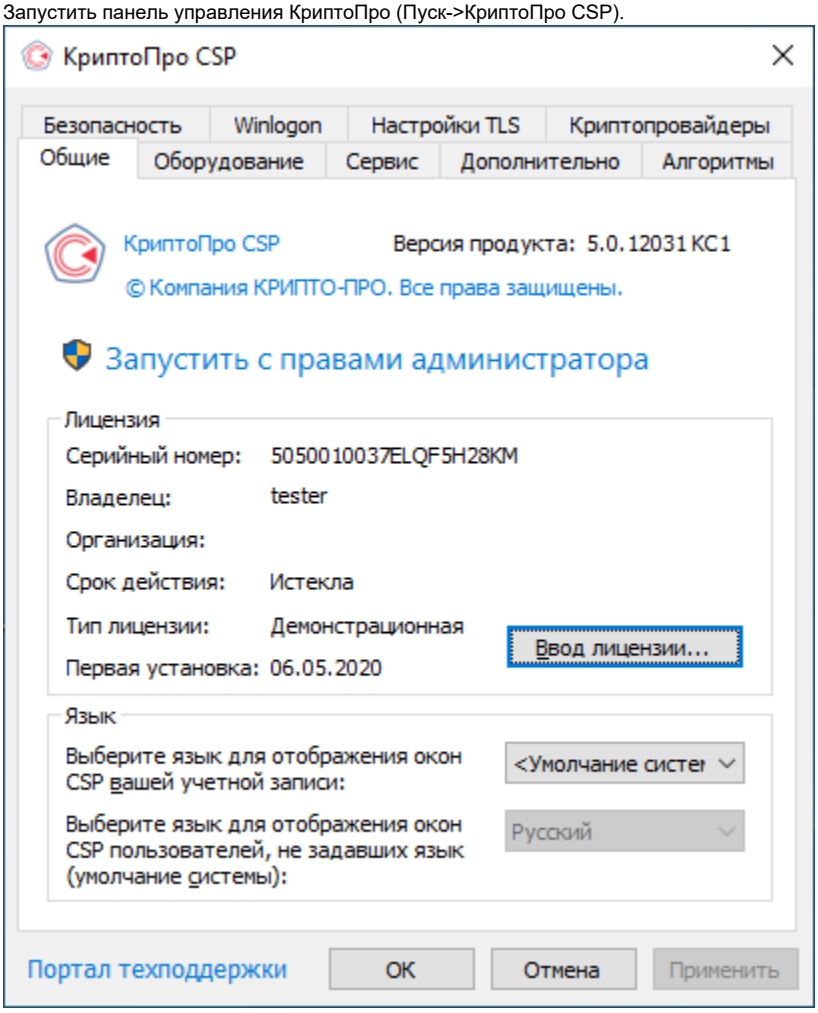
Данный режим по умолчанию отключен в этой версии криптопровайдера и оставлен для совместимости.

Этот режим не совместим с Рутокен ЭЦП 2.0 3000 и смарт-картой Рутокен ЭЦП 3.0 NFC.

Для включения этого режима необходимо выполнить следующие действия:

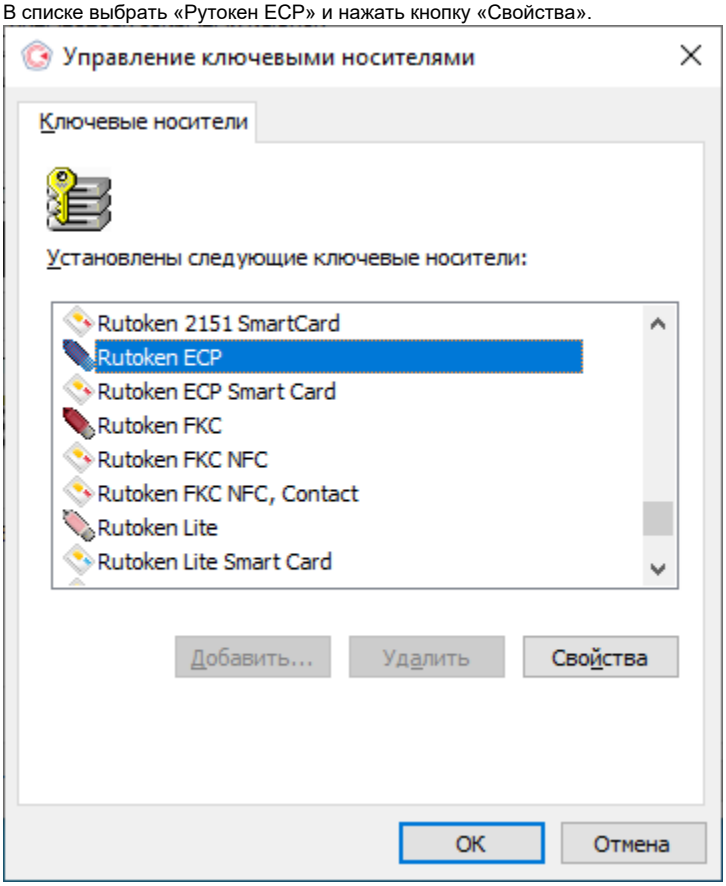
В операционной системе Windows

1. Запустить панель управления КриптоПро (Пуск->КриптоПро CSP).

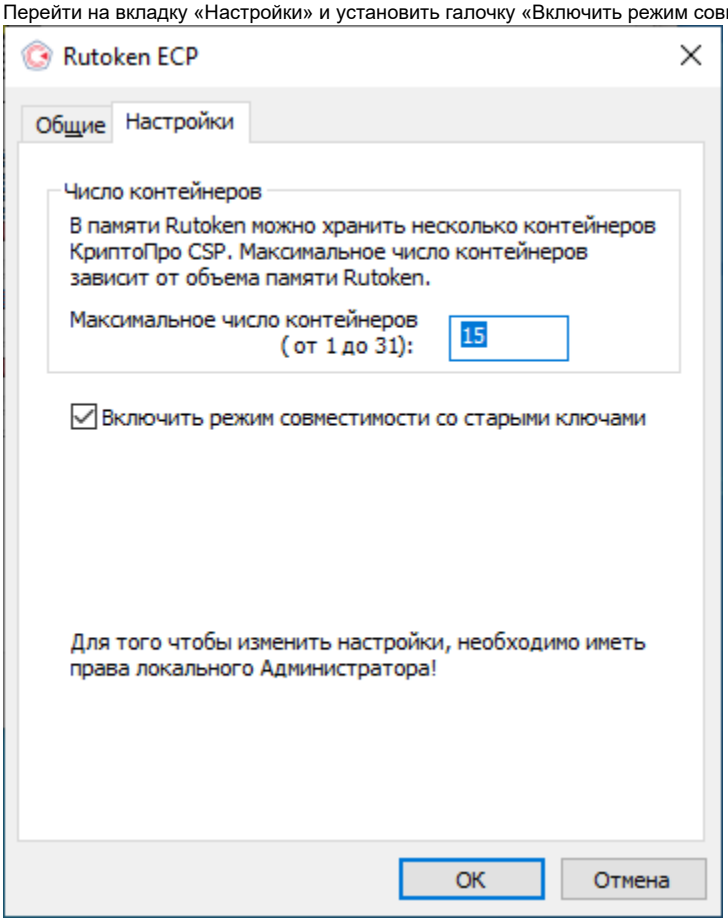


2. Нажать «Запустить с правами администратора».
3. Перейти на вкладку «Оборудование» и нажать кнопку «Настроить типы носителей…».

4. В списке выбрать «Рутокен ECP» и нажать кнопку «Свойства».



5. Перейти на вкладку «Настройки» и установить галочку «Включить режим совместимости со старыми ключами».



В операционной системе Linux

Запустить терминал и выполнить следующую команду:

> *sudo /opt/cprocsp/sbin/amd64/cpconfig -ini "\config\Parameters" -add long EnableNativeTokenCryptMode 1*

В операционной системе macOS

Запустить терминал и выполнить следующую команду:

> *sudo /opt/cprocsp/sbin/cpconfig -ini '\config\Parameters' -add long EnableNativeTokenCryptMode 1*

В режиме «ФКН без защиты канала» ключи контейнера КриптоПро создаются сразу в защищенной памяти устройства.

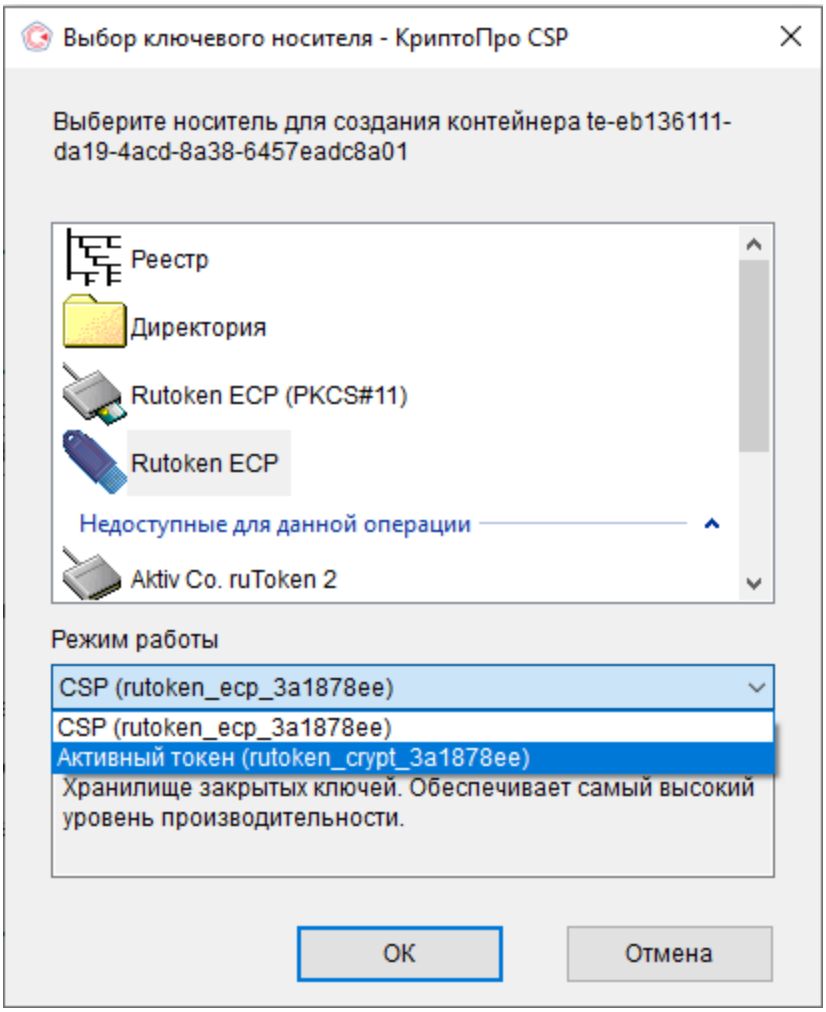
Этот режим предотвращает извлечение ключа в память компьютера в момент подписания.

Ключи, созданные в этом режиме, частично совместимы с режимом считывателя PKCS#11.

С ключами и сертификатами в контейнерах, созданными в режиме "ФКН без защиты канала", возможна работа практически во всех продуктах КриптоПро.

- Рутокен ЭЦП 2.0 2100
- Рутокен ЭЦП 2.0 (micro)
- Рутокен ЭЦП 2.0 Flash/Touch
- Рутокен ЭЦП Bluetooth
- Рутокен ЭЦП PKI
- Смарт-карты Рутокен ЭЦП 2.0 2100
- Смарт-карты Рутокен ЭЦП SC

Чтобы на токене был создан ключ в режиме "ФКН без защиты канала", при генерации в окне выбора носителя надо выбирать режим работы: "Активный токен без защиты канала (rutoken_crypt_xxxx)".



Полезные знания и руководства:

- Генерация контейнера ФКН на смарт-карте Рутокен ЭЦП 3.0 NFC с помощью КриптоПро CSP 5.0 R2
- Как проверить, что ключи на смарт-карте Рутокен ЭЦП 3.0 NFC сгенерированы в формате ФКН?
- Установка КриптоПро CSP и Cades Plugin для работы с Рутокен на Linux
- Тестирование целостности контейнера через КриптоПро CSP
- Установка личного сертификата
- Срок действия этой версии КриптоПро CSP истек / Как ввести серийный номер КриптоПро CSP?
- Изменение максимального количества контейнеров в КриптоПро CSP