Совместимость с продуктами компании КриптоПро

Содержание

КриптоПро CSP

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

На устройстве 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 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.
Полезные знания и руководства:

- 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

КриптоПро CSP версии 4.0

Устройства Рутокен позволяют пользователям криптопровайдера версии 4.0 обезопасить ключевую информацию от несанкционированного использования. Ключи и сертификаты надежно хранятся в защищенной файловой системе Рутокен.

- Рутокен ЭЦП 2.0 2100 (micro)
- Рутокен S (micro)
- Рутокен Lite (micro)
- Рутокен ЭЦП Flash
- Рутокен ЭЦП 2.0 (micro)
- Рутокен ЭЦП 2.0 Touch
- Рутокен ЭЦП PKI
- Рутокен ЭЦП Bluetooth
- Смарт-карта Рутокен ЭЦП SC
- Смарт-карта Рутокен ЭЦП 2.0 2100

КриптоПро CSP версии 5.0

В этой версии криптопровайдера поддерживается три режима работы с Рутокенами:

Работа с внутренним криптоядром Рутокена

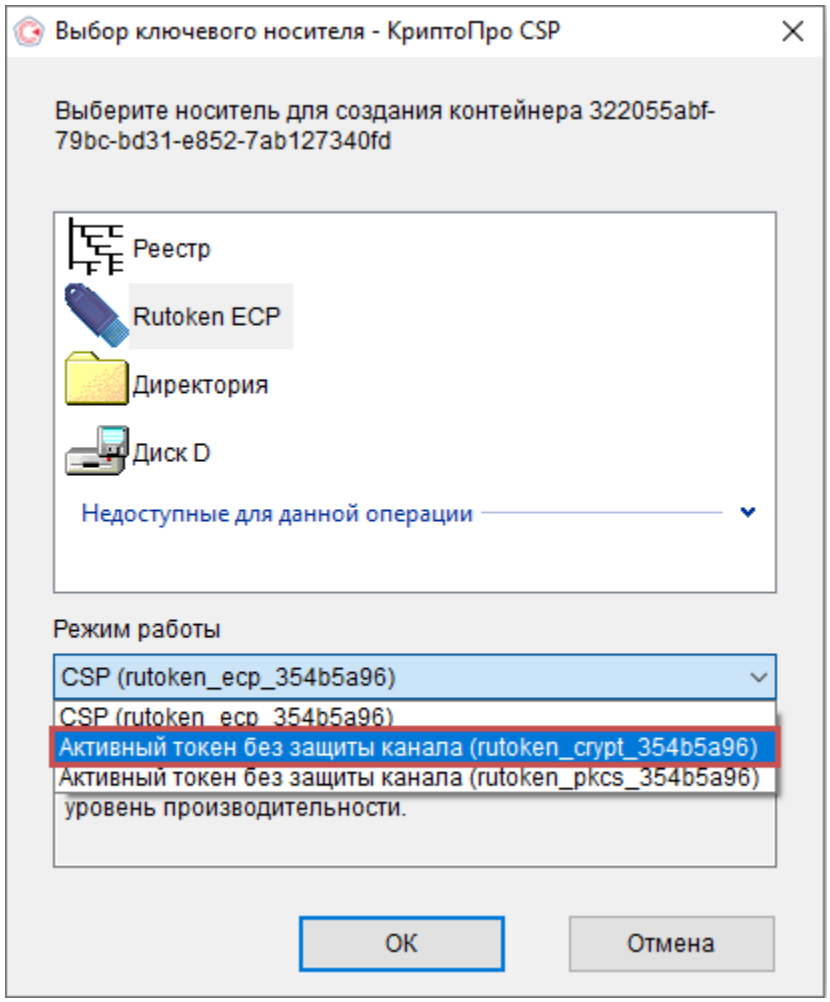
В режиме «ФКН без защиты канала» ключи контейнера КриптоПро создаются сразу в защищенной памяти устройства.

Подписание документов теперь возможно и на неизвлекаемых аппаратных ключах. Этот режим предотвращает извлечение ключа в память компьютера в момент подписания.

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 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.

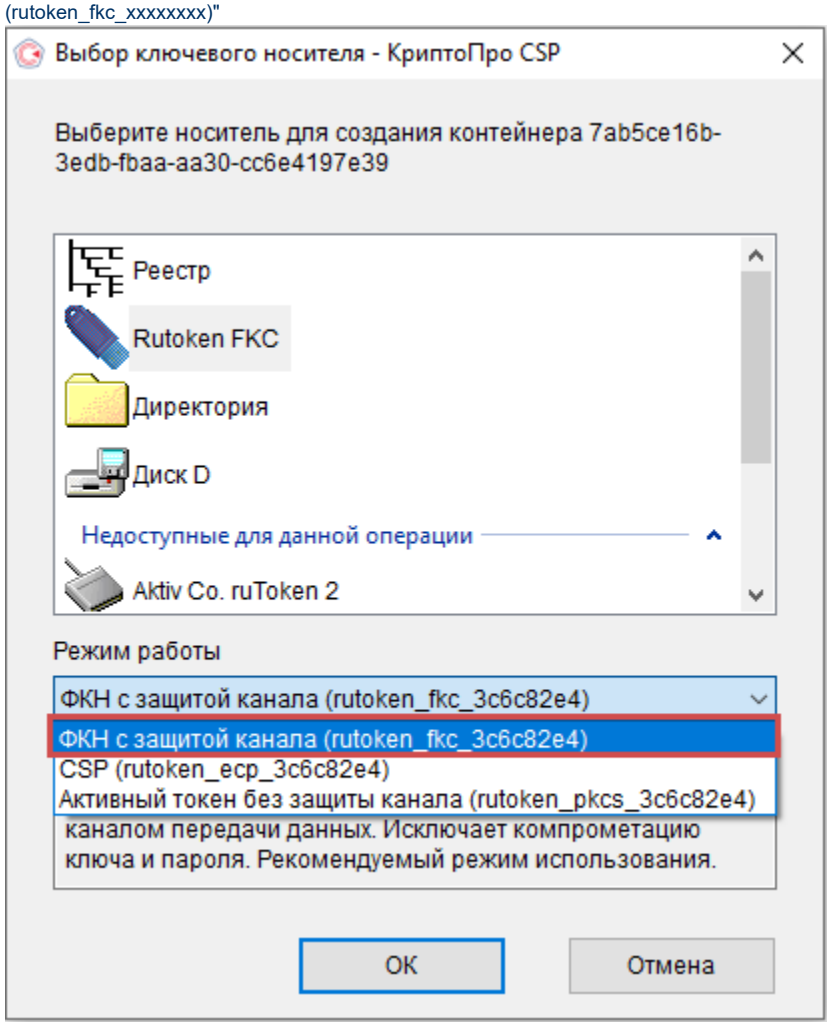
Чтобы на токене был создан ключ в режиме "ФКН без защиты канала", при генерации в окне выбора носителя надо выбирать режим работы: "Активный токен без защиты канала (rutoken_crypt_xxxx)"



Работа с внутренним криптоядром Рутокена с обеспечением защиты канала

В КриптоПро CSP версии 5.0 реализован криптографический протокол SESPAKE, который так же поддерживается в сертифицированной модели Рутокен ЭЦП 2.0 3000 и смарт-карте Рутокен ЭЦП 3.0 NFC в КриптоПро CSP 5.0 R2.

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

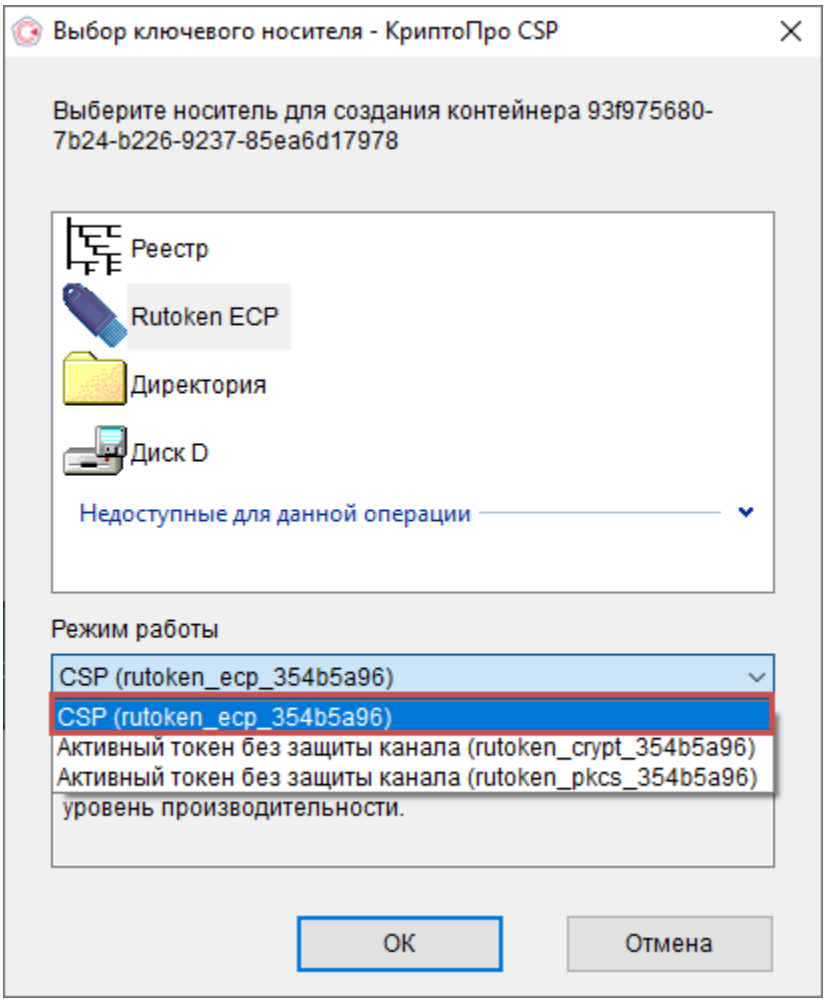


Хранение в защищенной файловой системе Рутокен

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.

- 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

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



КриптоПро ЭЦП Browser plug-in

Рутокен совместно с КриптоПро CSP и компонентом для браузера КриптоПро ЭЦП Browser plug-in комплексно решают задачу применения электронной подписи и двухфакторной аутентификации в веб-сервисах. Есть инструменты для создания запросов и записи сертификатов, вычисления электронной подписи разными алгоритмами, шифрования, управления PIN-кодами, ключами и сертификатами на устройствах.

Для взаимодействия из веб-приложений с контейнерами КриптоПро необходим программный компонент КриптоПро ЭЦП Browser plug-in. Взаимодействие происходит через JavaScript API.

КриптоПро CSP для iOS, Android и Sailfish OS RUS (Аврора)

Модель **Рутокен ЭЦП Bluetooth** надежно и безопасно хранит контейнеры КриптоПро CSP для подписания документов на мобильных устройствах **iOS** и **Android** с помощью специальных мобильных версий криптопровайдера.

Рутокен подключается к мобильному гаджету по Bluetooth как HID-устройство, драйвер для которого встроен в мобильные ОС. В целях обеспечения безопасности передаваемой информации, канал Bluetooth шифруется ГОСТ-алгоритмами. Для работы с Android устройство можно подключить также через разъем microUSB. Устройство предусматривает работу в двух режимах:

1) как USB-токен Рутокен ЭЦП 2.0, заряжающий встроенный аккумулятор при подключении по USB;

2) в Bluetooth-режиме для полноценной работы с смартфонами и планшетами на iOS и Android.

На телефонах и планшетах с **Android** также удобно использовать **Рутокен ЭЦП 2.0 с Type-C разъемами**.

Сертифицированная версия **Sailfish OS RUS** (впоследствии переименованная в ОС «**Аврора**») поддерживает двухфакторную аутентификацию по устройствам семейства Рутокен ЭЦП 2.0, а также хранит ключи и сертификаты в контейнерах КриптоПро в защищенной памяти Рутокен.

КриптоПро JCP

Начиная с версии JCP 2.0.39738, модуль работы с Рутокеном "Rutoken.jar" – часть СКЗИ. Установка дополнительного модуля поддержки при этом не требуется.

Это гарантирует корректную совместную работу КриптоПро JCP и устройств Рутокен. Ключи и сертификаты хранятся в защищенной файловой системе Рутокена.

Контейнеры с КриптоПро JCP защищенно хранят Рутокен S, Рутокен Lite и устройства семейства Рутокен ЭЦП 2.0.

КриптоПро NGate

Технологии удаленного доступа КриптоПро NGate создают безопасное зашифрованное соединение. Но использование логина и пароля в этих технологиях для аутентификации в VPN небезопасно.

Длинные, надежные и уникальные пароли сложны для запоминания и редко используются, а значит, в отсутствии ограничения на перебор – его возможно подобрать. Любой человек, узнавший чужой пароль, может им воспользоваться без ведома владельца. Отследить такую ситуацию довольно сложно, особенно, если злоумышленник технически подкован.

Устройства Рутокен помогут быстро защитить и упростить вход в частную корпоративную сеть, заменяя однофакторную парольную аутентификацию двухфакторной.

Пользователям достаточно установить КриптоПро CSP, NGate-клиент, подключить Рутокен с контейнером и сертификатом внутри. Аутентификационные данные лежат в специальной защищенной PIN-кодом памяти устройства Рутокен.

Таким образом, продукты Рутокен помогают защитить корпоративную сеть от несанкционированного доступа.