КриптоПро CSP 5.0

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 5.0

В этой версии криптопровайдера поддерживается три режима работы с Рутокенами:

Работа с внутренним криптоядром Рутокена

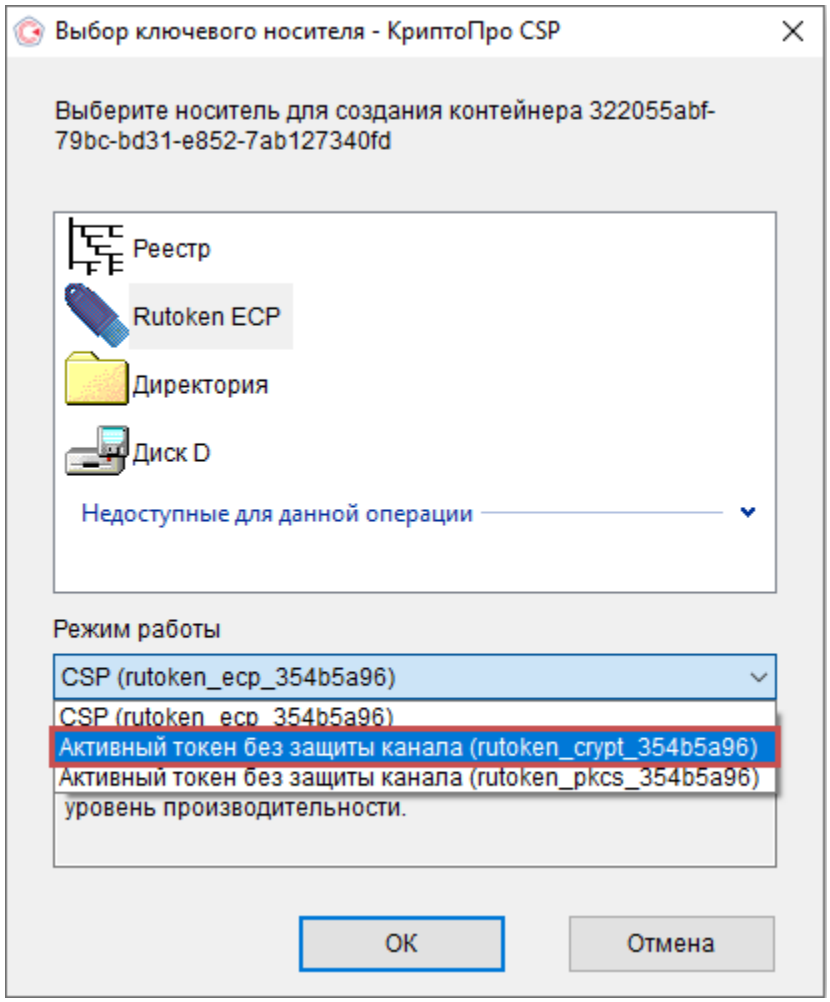
В режиме «ФКН без защиты канала» ключи контейнера КриптоПро создаются сразу в защищенной памяти устройства.

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.

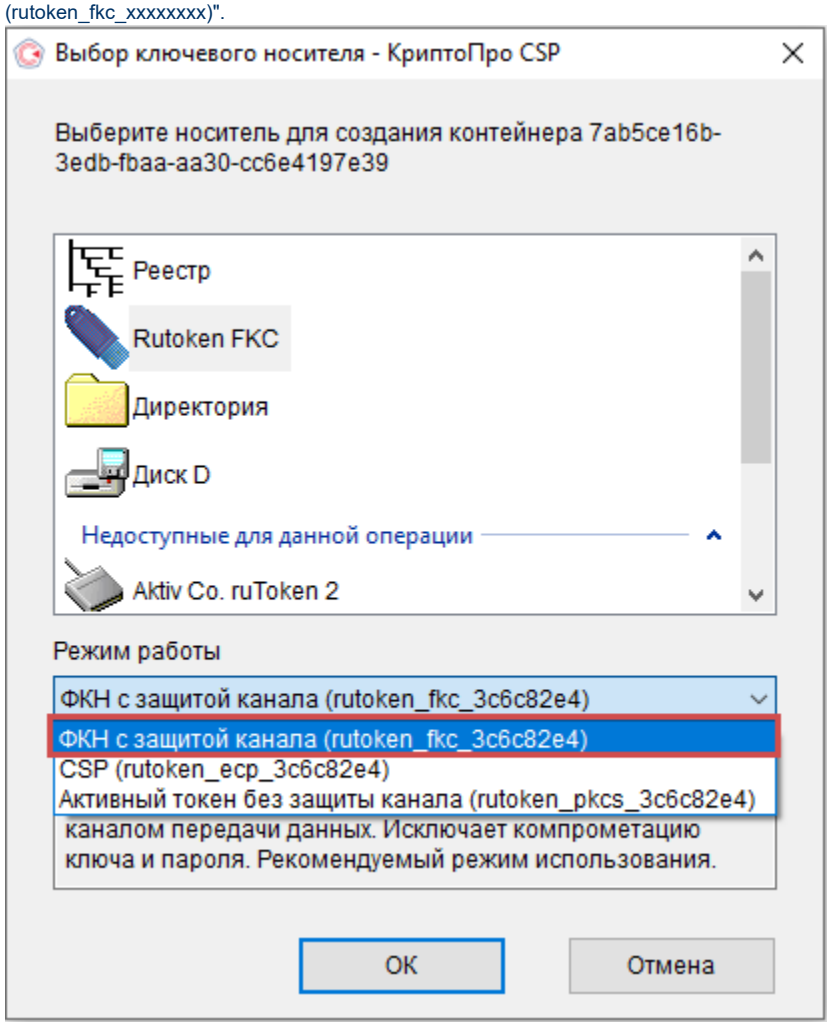
Чтобы на токене был создан ключ в режиме "ФКН без защиты канала", при генерации в окне выбора носителя надо выбирать режим работы: "Активный токен без защиты канала (rutoken_crypt_xxxx)".



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.

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)".



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)".