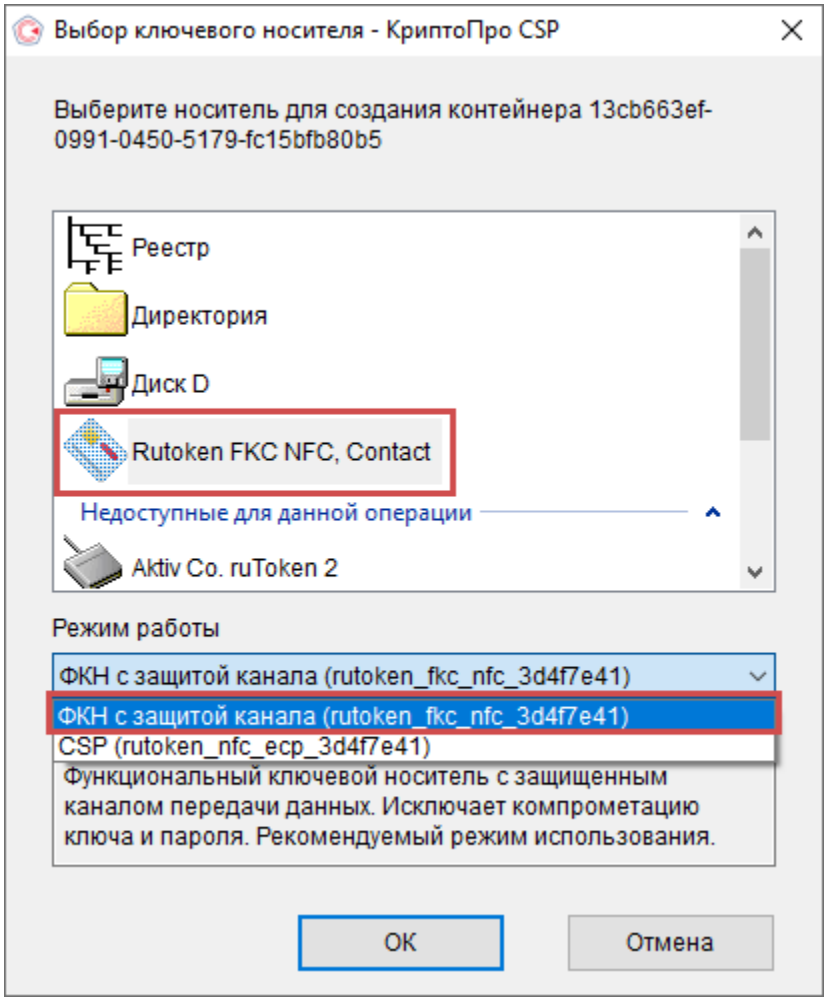
Генерация контейнера ФКН на Рутокен ЭЦП 3.0 NFC с помощью КриптоПро CSP 5.0 R2

Для генерации контейнера функционального ключевого носителя (ФКН) с защитой канала на **Рутокен ЭЦП 3.0 NFC** должно использоваться СКЗИ «КриптоПро CSP» **версии 5.0 R2.**

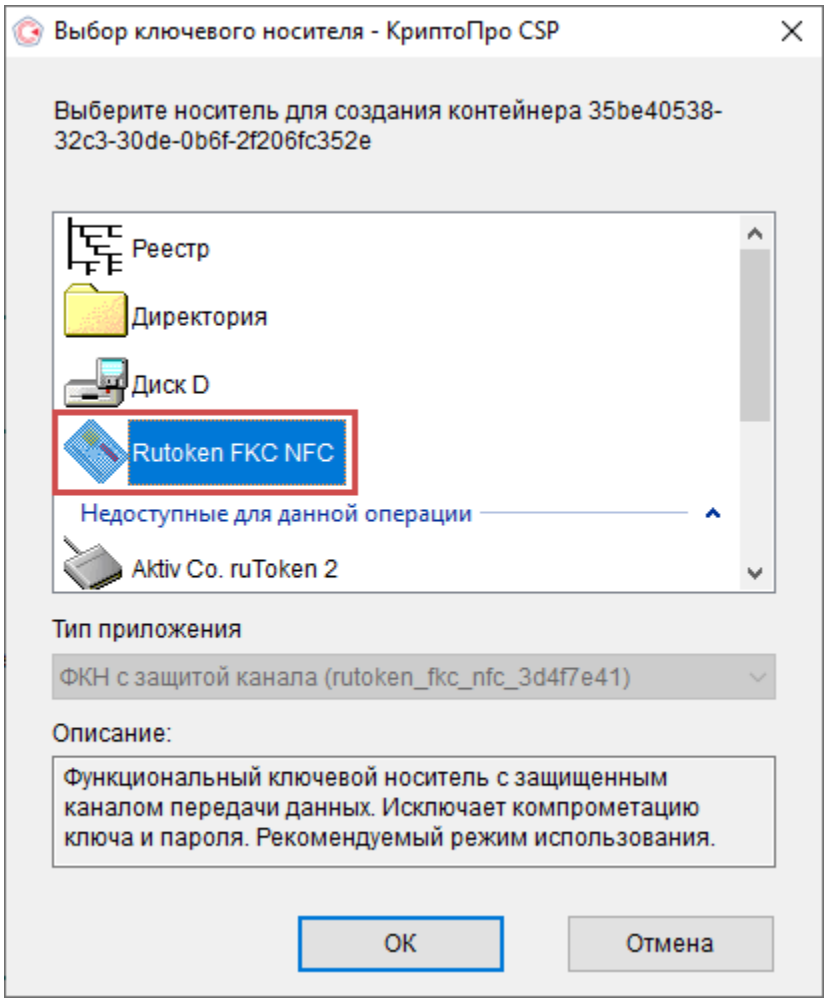
Именно в этой версии КриптоПро CSP была добавлена поддержка этого типа устройств.
Доступность через NFC-канал

При работе с Рутокен ЭЦП 3.0 по каналу NFC на мобильных устройствах или с беспроводными считывателями на настольных ПК в «КриптоПро CSP» **версии 5.0 R2** доступны только контейнеры ФКН

При подключении дуального Рутокен ЭЦП 3.0 NFC контактным способом, выбираем «**Rutoken FKC NFC, Contact**» и режим работы «**ФКН с защитой канала (rutoken_fkc_nfc...)**»



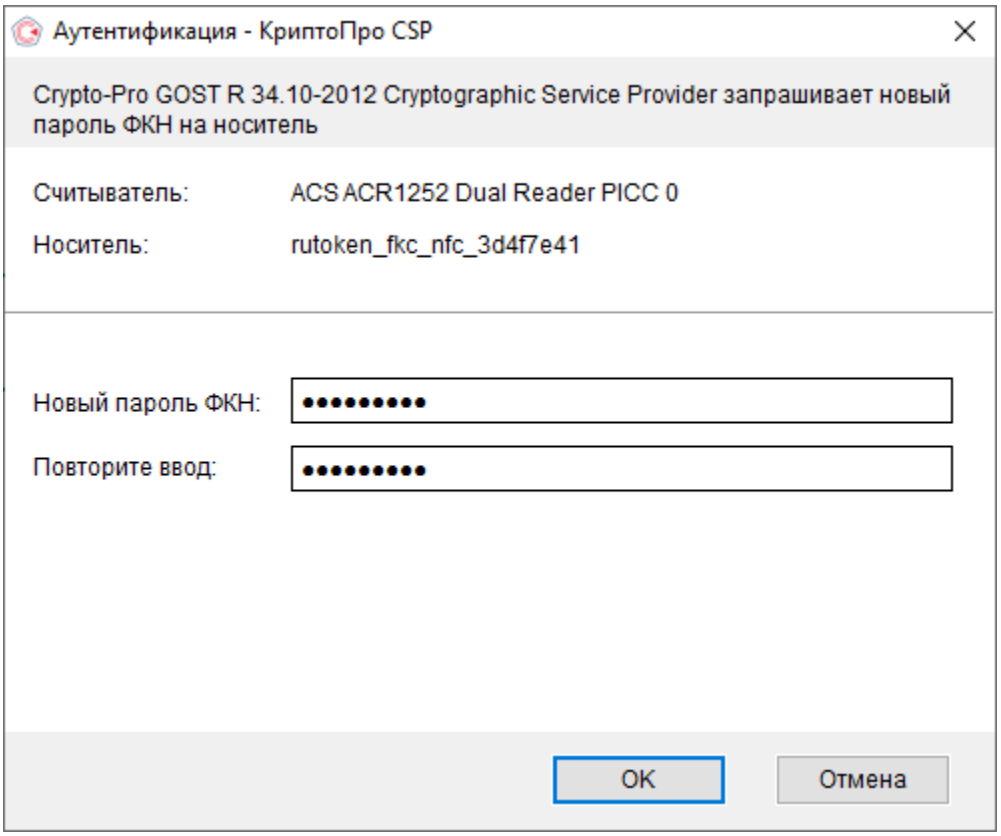
При использовании дуального Рутокен ЭЦП 3.0 NFC по каналу NFC, выбираем «**Rutoken FKC NFC**»



При генерации первого контейнера ФКН на защищенный носитель нужно указать новый пароль ФКН.

Этот пароль будет впоследствии использоваться для всех ключей ФКН на этом устройстве.

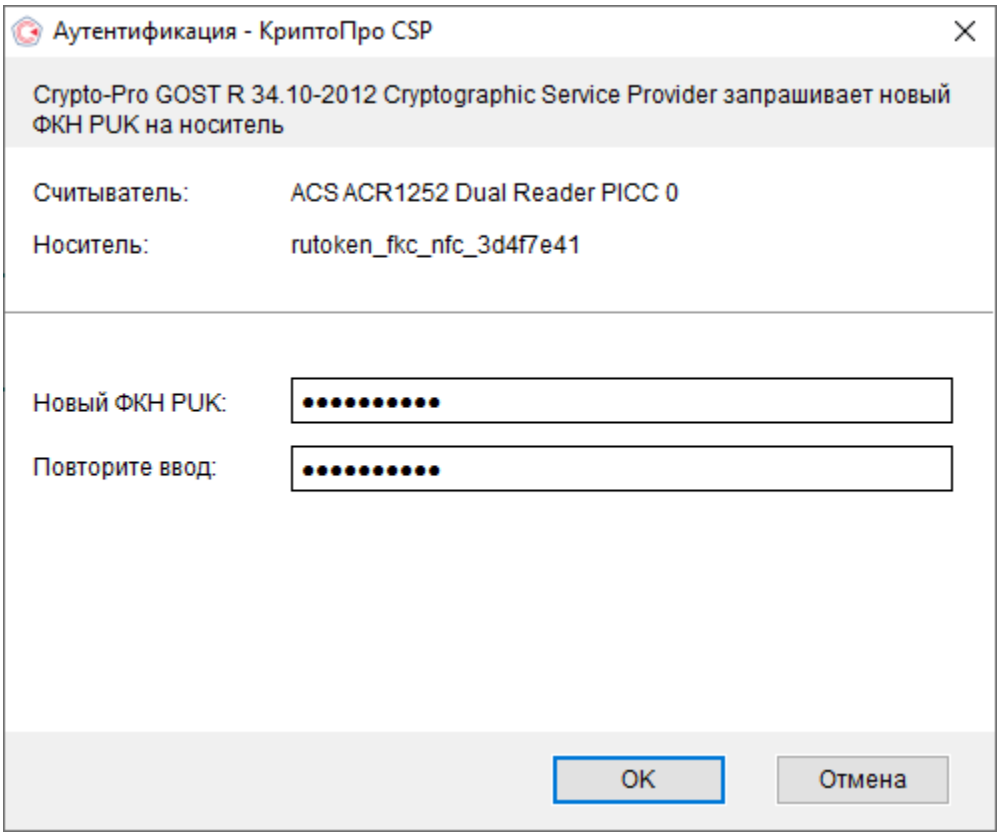
Для работы с ключами других форматов, записанными на устройстве, будет использоваться PIN-код Пользователя, установленный на Рутокен.
Значение может быть отличным от PIN-кода Пользователя на устройство Рутокен.



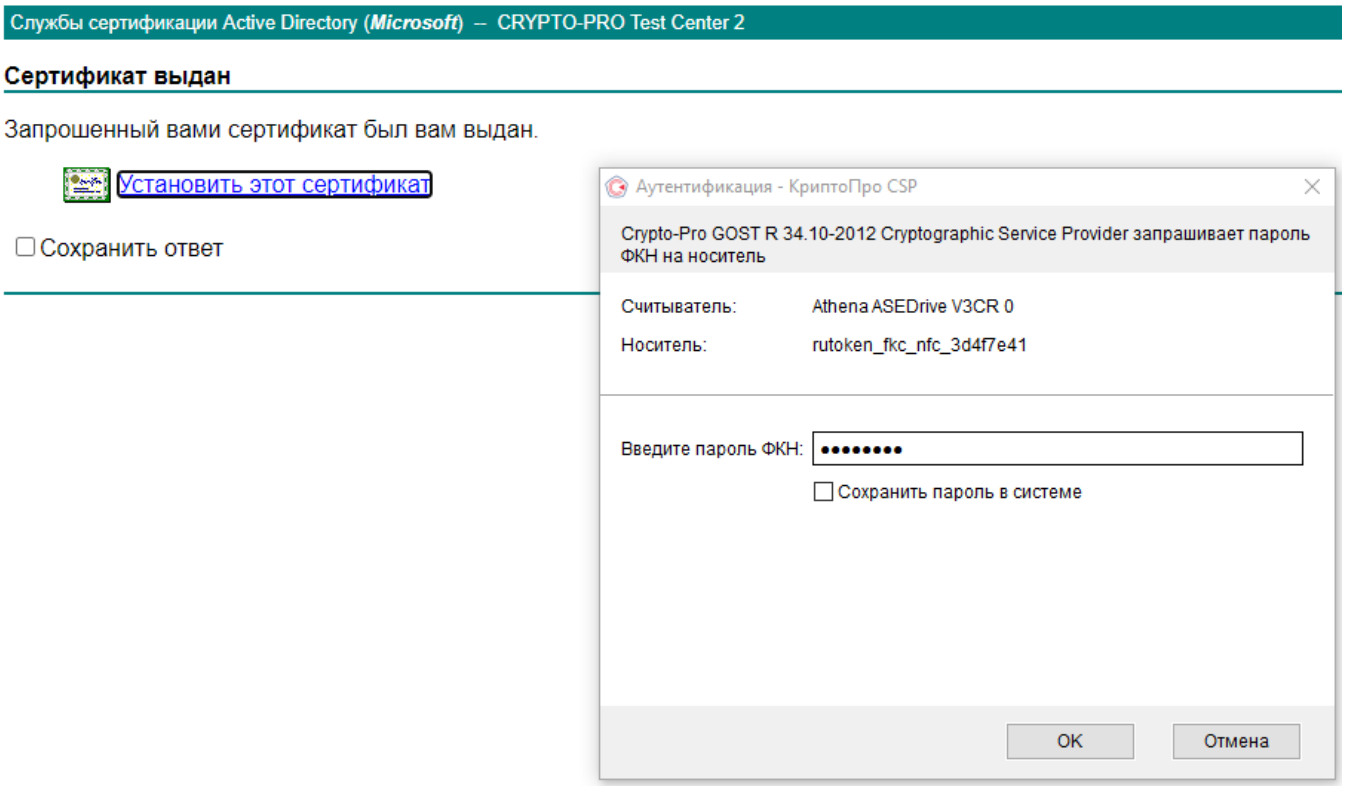
Далее указывается новый ФКН PUK.

Этот PUK-код будет впоследствии использоваться для всех ключей ФКН на этом устройстве.

Для работы с ключами других форматов, записанными на устройстве будет использоваться PIN-код Администратора, установленный на Рутокен.
Значение может быть отличным от PIN-кода Администратора на устройство Рутокен.



Файл сертификата устанавливаем в контейнер ФКН, указав созданный пароль на контейнер.



Генерация контейнера ФКН с защитой канала на **Рутокен ЭЦП 3.0 NFC** завершена.