

Как скопировать контейнер с сертификатом на другой носитель

◆ Как скопировать сертификат с рутокена на компьютер или из криптопро на флешку? Ответ на kontur-extern.ru.

Jul 08, 2021 12:00 AM · 5 min. read ·
[View original](#)

Подробная инструкция о том, как скопировать сертификат на другой носитель: копирование средствами Windows, копирование на профиле диагностики, массовое копирование, копирование с помощью КриптоПро CSP, экспорт PFX-файла и его установка, а также копирование контейнера из реестра другого пользователя.

Отчитайтесь легко и без ошибок



Удобный сервис для подготовки и сдачи отчетов через интернет.

[14 дней бесплатно](#)

Копирование средствами Windows

Если для работы используется дискета или flash-накопитель, скопировать контейнер с сертификатом можно средствами Windows (этот способ подходит для версий КристоПро CSP не ниже 3.0). Папку с закрытым ключом (и, если есть, файл сертификата — открытый ключ) поместите в корень дискеты / flash-накопителя (если поместить не в корень, то работа с сертификатом будет невозможна). Название папки при копировании рекомендуется не изменять.

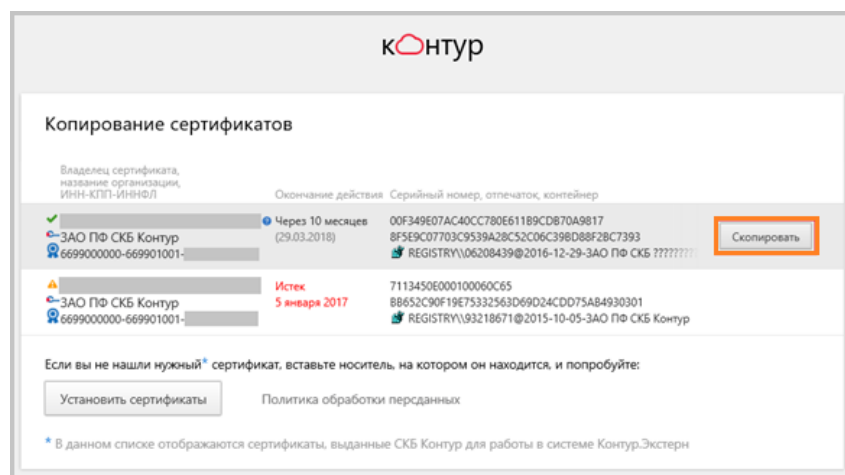
В папке с закрытым ключом должно быть 6 файлов с расширением.key. Как правило, в закрытом ключе присутствует открытый ключ (файл header.key в этом случае будет весить больше 1 Кб). В этом случае копировать открытый ключ необязательно. Пример закрытого ключа — папки с шестью файлами и открытого ключа — файла с расширением.cer.

 <div>65306963.000</div> <ul style="list-style-type: none">header.keymasks.keymasks2.keyname.keyprimary.keyprimary2.key	 <div>65306963@2013-02-08-ЗАО ПФ СКБ Контур.cer</div>
<i>Закрытый ключ</i>	<i>Открытый ключ</i>

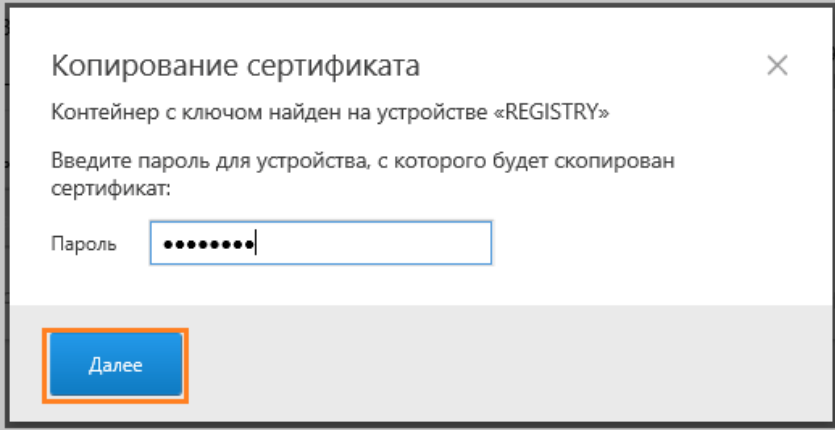
Если у вас MacOS, смотрите инструкцию
«[Как скопировать контейнер
с сертификатом на MacOS](#)».

Копирование на профиле Диагностики

1. Зайдите на профиль Диагностики
«Копирования» [по ссылке](#).
2. Вставьте носитель, на который
необходимо скопировать сертификат.
3. На нужном сертификате нажмите
на кнопку «Скопировать».

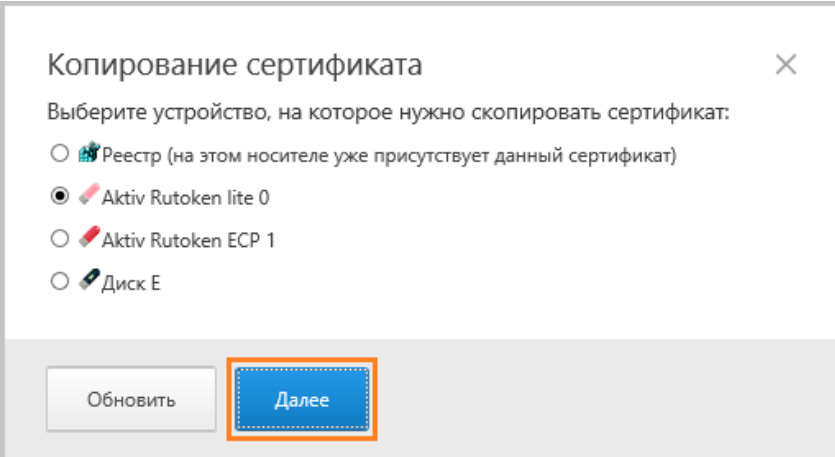


Если на контейнер был задан пароль —
появится сообщение «Введите пароль
для устройства с которого будет
скопирован сертификат».

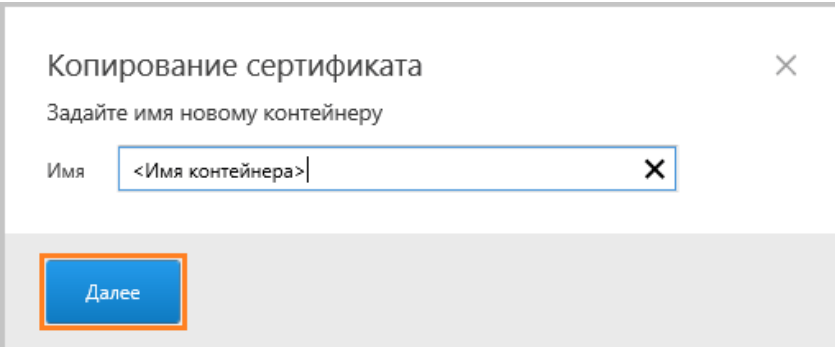


Введите пароль и нажмите на кнопку «Далее».

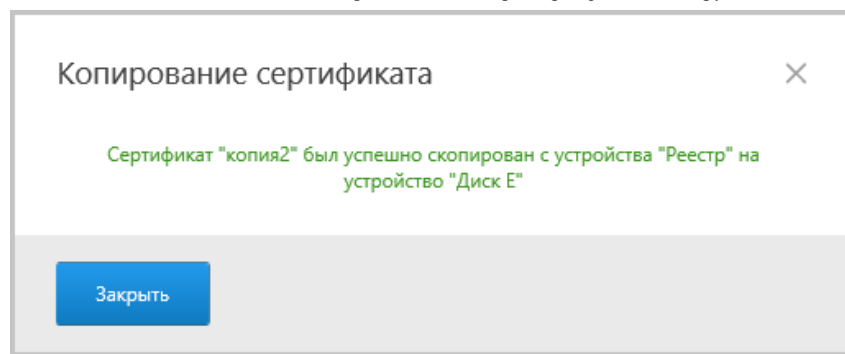
4. Выберите носитель, куда необходимо скопировать сертификат и нажмите «Далее».



5. Задайте имя новому контейнеру и нажмите на кнопку «Далее».

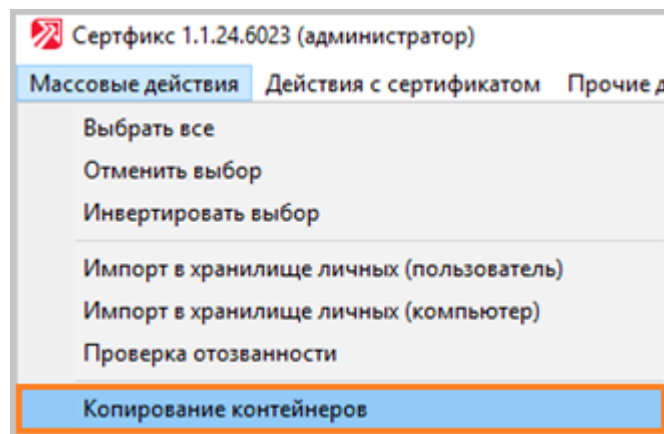


6. Должно появиться сообщение об успешном копировании сертификата.



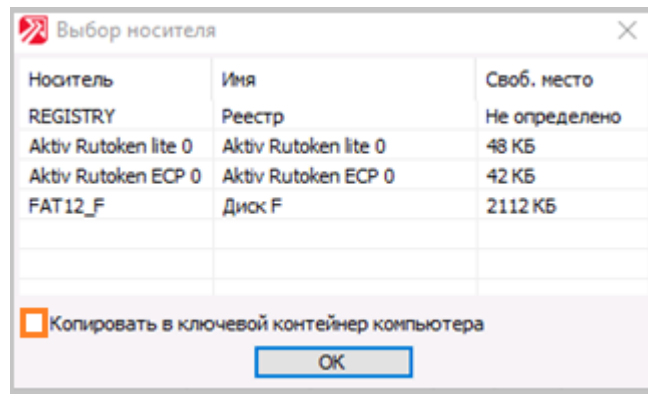
Массовое копирование

1. Скачайте и запустите [утилиту](#).
Дождитесь загрузки всего списка контейнеров/сертификатов и отметьте нужные галочками.
2. Выберите меню «Массовые действия» и нажмите на кнопку «Копирование контейнеров».



3. Выберите носитель для хранения копии контейнера и нажмите «ОК».

При копировании в реестр можно поставить галочку на пункте «Копировать к ключевой контейнер компьютера», тогда после копирования контейнер будет доступен всем пользователям данного компьютера.



4. После копирования нажмите внизу слева кнопку «Обновить».

Если хотите работать со скопированными контейнерами — необходимо [установить сертификаты](#).

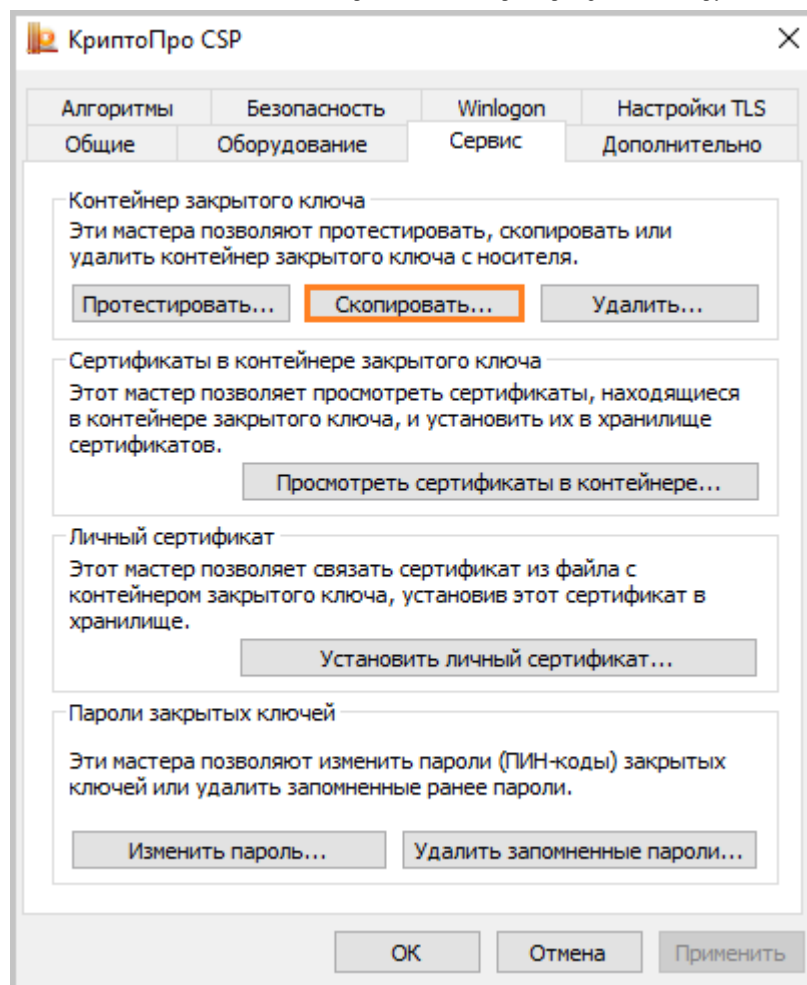
Отчитайтесь легко и без ошибок

Удобный сервис для подготовки и сдачи отчетов через интернет.

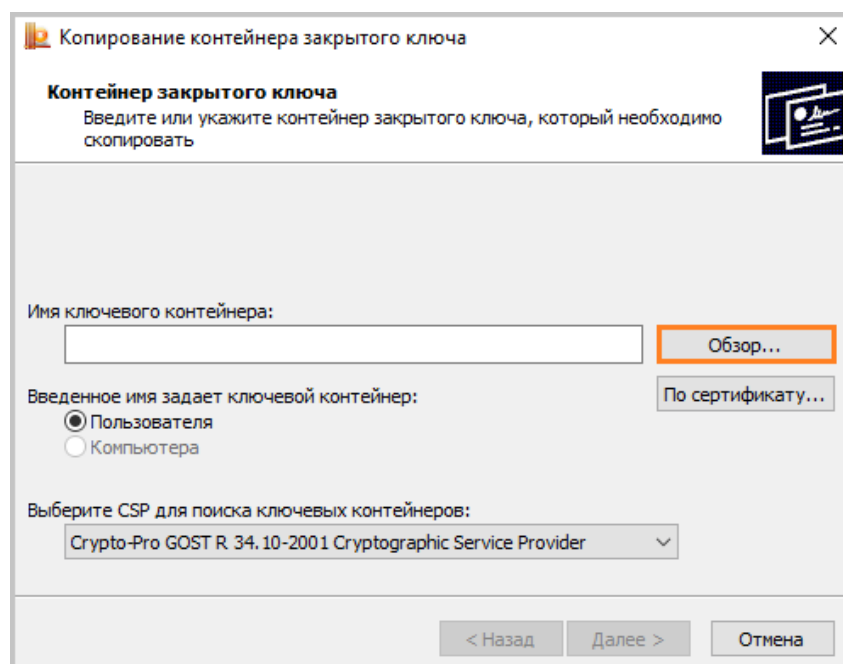
[14 дней бесплатно](#)

Копирование с помощью КriptoПро CSP

Выберите «Пуск» > «Панель управления» > «КriptoПро CSP». Перейдите на вкладку «Сервис» и кликните по кнопке «Скопировать».

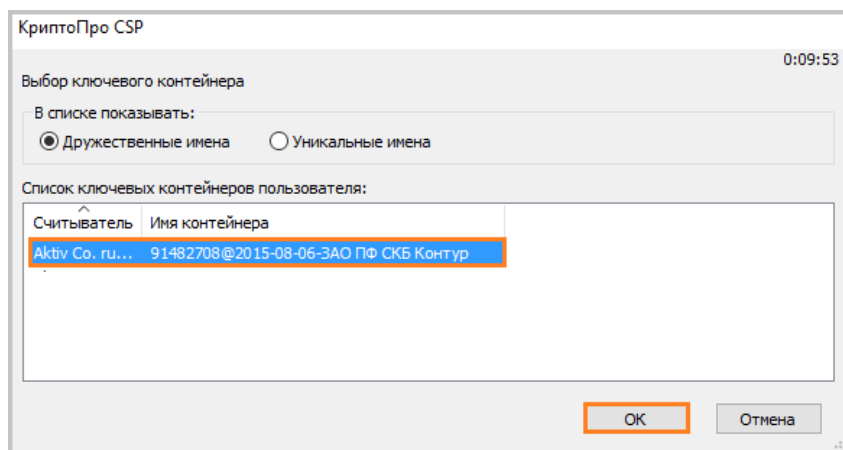


В окне «Копирование контейнера закрытого ключа» нажмите на кнопку «Обзор».

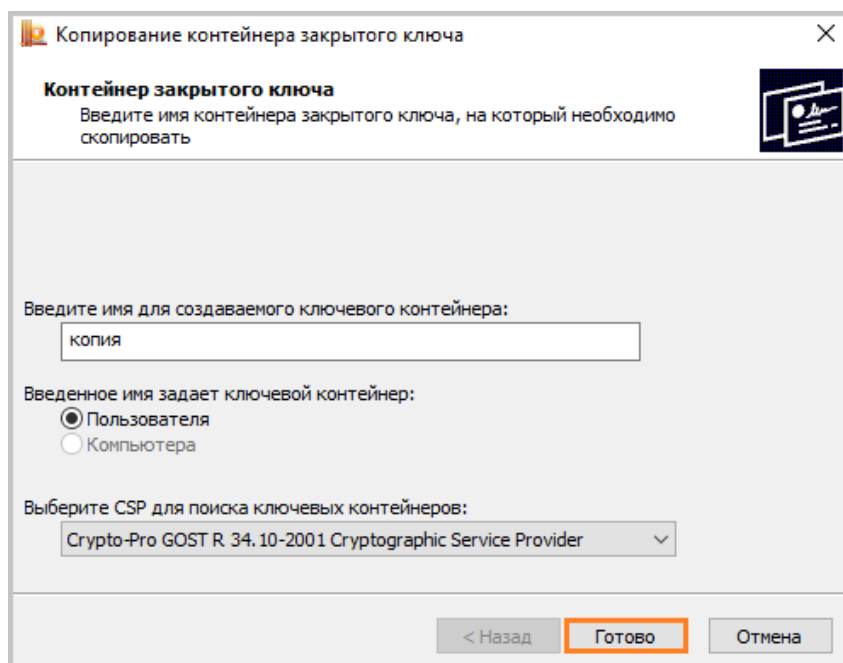


Выберите контейнер, который необходимо скопировать, и кликните по кнопке «Ок»,

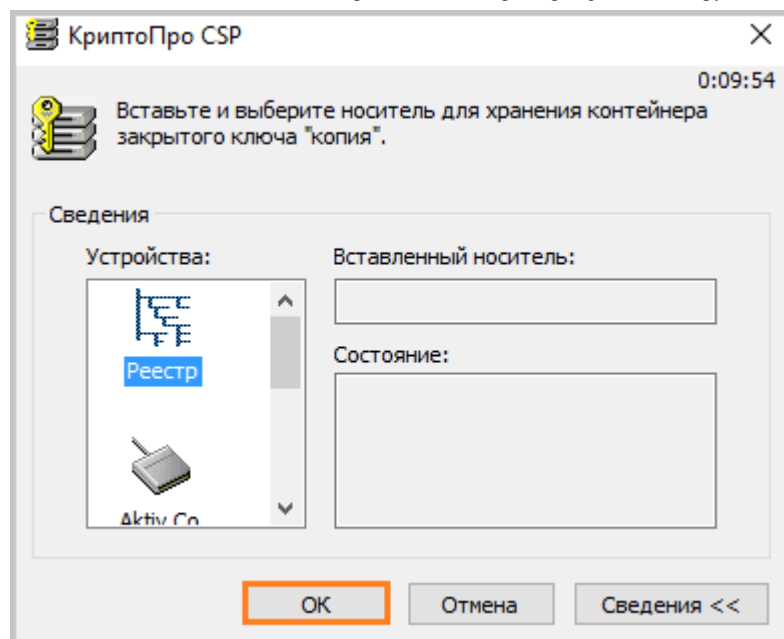
затем «Далее». Если вы копируете с рутокена, то появится окно ввода, в котором следует указать pin-код. Если вы не меняли pin-код на носителе, стандартный pin-код — 12345678.



Придумайте и укажите вручную имя для нового контейнера. В названии контейнера допускается русская раскладка и пробелы. Затем кликните «Готово».

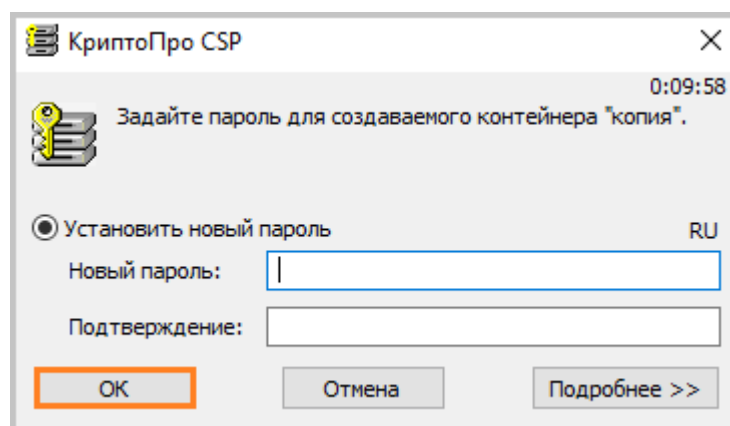


В окне «Вставьте чистый ключевой носитель» выберите носитель, на который будет помещен новый контейнер.

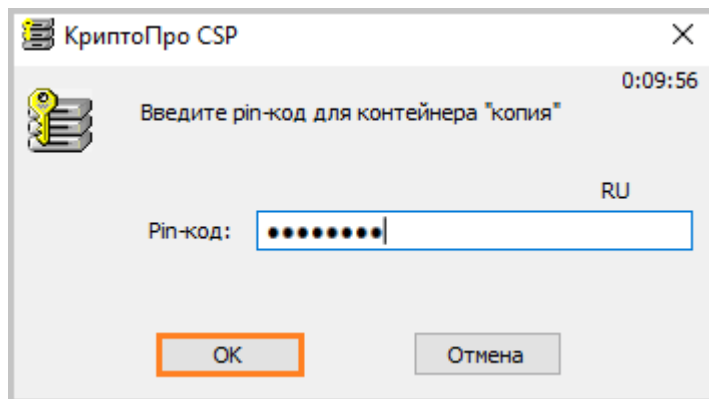


На новый контейнер будет предложено установить пароль. Рекомендуем установить такой пароль, чтобы вам было легко его запомнить, но посторонние не могли его угадать или подобрать. Если вы не хотите устанавливать пароль, можно оставить поле пустым и нажать «ОК».

Не храните пароль/pin-код в местах, к которым имеют доступ посторонние. В случае утери пароля/pin-кода использование контейнера станет НЕВОЗМОЖНЫМ.



Если вы копируете контейнер на смарт-карту ruToken, сообщение будет звучать иначе. В окне ввода укажите pin-код. Если вы не меняли pin-код на носителе, стандартный pin-код — 12345678.



После копирования система вернется на вкладку «Сервис» КриптоПро CSP. Копирование завершено. Если вы планируете использовать для работы в Экстерне новый ключевой контейнер, [установите его через Крипто Про](#).

При копировании может возникнуть «Ошибка копирования сертификата», если у вас нет лицензии на КриптоПроCSP или контейнер получил признак «неэкспортируемый». Справиться с этим поможет [инструкция](#).

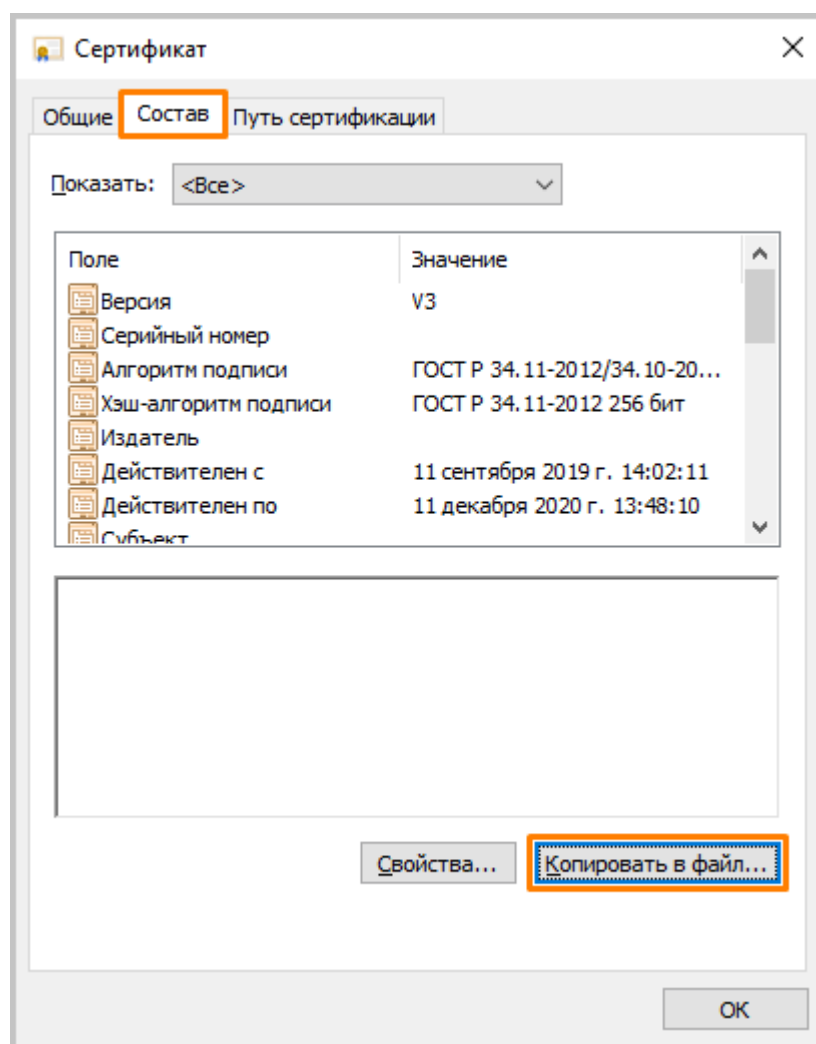
Экспорт PFX-файла и его установка

Экспорт сертификата с закрытым ключом

1. Откройте оснастку работы с сертификатами:

- Пуск → Все программы → КриптоПро → Сертификаты
либо
- Internet Explorer → Сервис → Свойства обозревателя → вкладка Содержание → Сертификаты.

2. Откройте сертификат, который нужно скопировать. На вкладке «Состав» нажмите «Копировать в файл».



3. В «Мастере экспорта сертификатов» нажмите «Далее» и выберите пункт «Да, экспортировать закрытый ключ». Нажмите «Далее».

Вы хотите экспортировать закрытый ключ вместе с сертификатом?

☒ Да, экспортировать закрытый ключ

☐ Нет, не экспортировать закрытый ключ

4. На следующем этапе поставьте галочки у пунктов «Включить по возможности все сертификаты в путь сертификации» и «Экспортировать все расширенные свойства», остальные галочки необходимо убрать. Нажмите «Далее».

Выберите формат, который вы хотите использовать:

☐ Файлы X.509 (.CER) в кодировке DER

☐ Файлы X.509 (.CER) в кодировке Base-64

☐ Стандарт Cryptographic Message Syntax - сертификаты PKCS #7 (.p7b)

☐ Включить по возможности все сертификаты в путь сертификации

☒ Файл обмена личной информацией - PKCS #12 (.PFX)

☒ Включить по возможности все сертификаты в путь сертификации

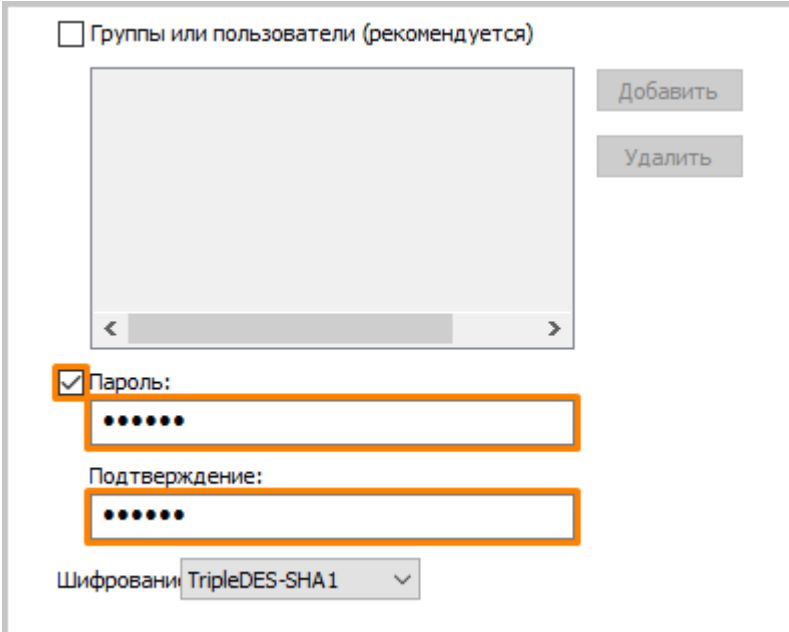
☐ Удалить закрытый ключ после успешного экспорта

☒ Экспортировать все расширенные свойства

☐ Включить конфиденциальность сертификата

☐ Хранилище сериализованных сертификатов (.SST)

5. Обязательно задайте пароль для экспортируемого файла. Данный пароль не рекомендуется сообщать по электронной почте. Нажмите «Далее».



6. Укажите имя файла, выберите путь сохранения и нажмите «Далее», затем нажмите «Готово».



7. Экспортируйте открытый ключ сертификата (см. [Экспорт открытого ключа](#)).

8. Заархивируйте полученные файлы форматов.pfx и.cer.

Установка сертификата с закрытым ключом

1. Откройте.pfx файл. Сразу запустится «Мастер импорта сертификатов».

2. Укажите хранилище «Текущий пользователь» и нажмите «Далее», затем снова «Далее».

Мастер импорта сертификатов

Этот мастер помогает копировать сертификаты, списки доверия и списки отзыва сертификатов с локального диска в хранилище сертификатов.

Сертификат, выданный центром сертификации, является подтверждением вашей личности и содержит информацию, необходимую для защиты данных или установления защищенных сетевых подключений. Хранилище сертификатов — это область системы, предназначенная для хранения сертификатов.

Расположение хранилища

☒ Текущий пользователь

☐ Локальный компьютер

Для продолжения нажмите кнопку "Далее".

3. Введите пароль, который указывали при экспорте и поставьте галочку на пункте «Пометить этот ключ как экспортируемый...», иначе нече контейнер нельзя будет скопировать в дальнейшем. Нажмите «Далее».

Пароль:

.....

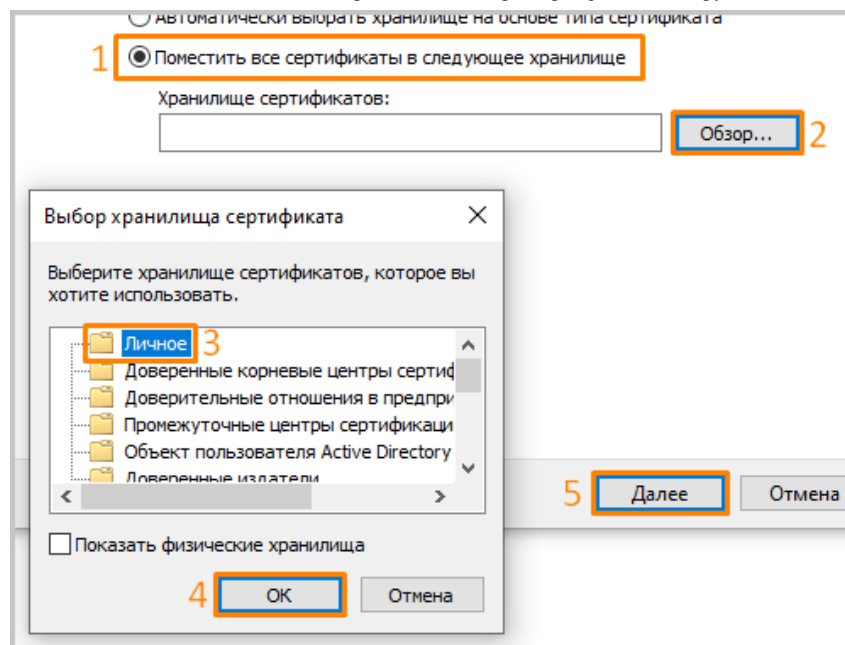
☐ Показывать пароль

Параметры импорта:

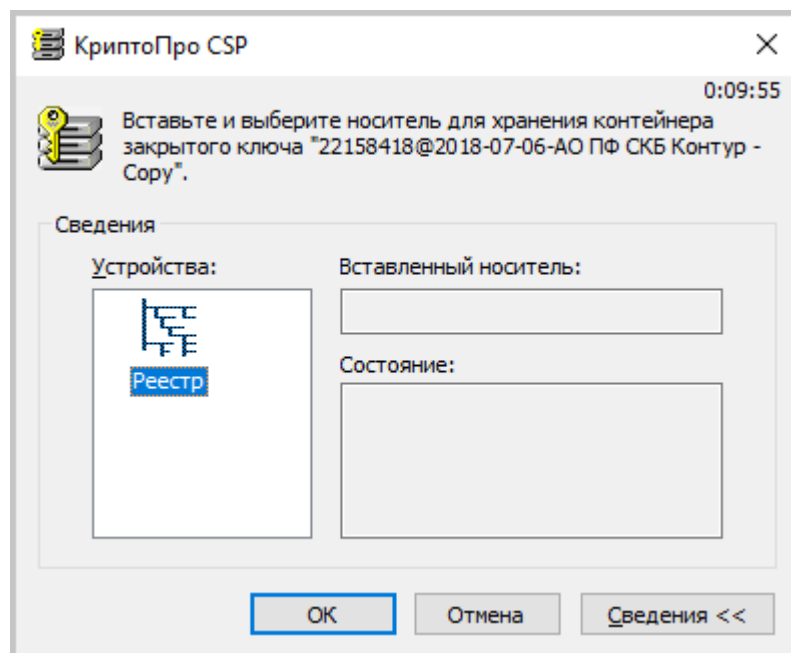
☐ Включить усиленную защиту закрытого ключа. В этом случае при каждом использовании закрытого ключа приложением будет запрашиваться разрешение.

☒ Пометить этот ключ как экспортируемый, что позволит сохранять резервную копию ключа и перемещать его.

4. Выберите пункт «Поместить все сертификаты в следующее хранилище», нажмите на кнопку «Обзор», выберите «Личное» и нажмите на кнопку «ОК». Нажмите «Далее», а затем «Готово».



5. В окне КристоПро выберите носитель, на который хотите сохранить контейнер. При необходимости задайте пароль.



6. Для корректной работы сертификата со встроенной лицензией переустановите сертификат в контейнер (см. [Как установить личный сертификат в КристоПро](#)).

Отчитайтесь легко и без ошибок

Удобный сервис для подготовки и сдачи отчетов через интернет.

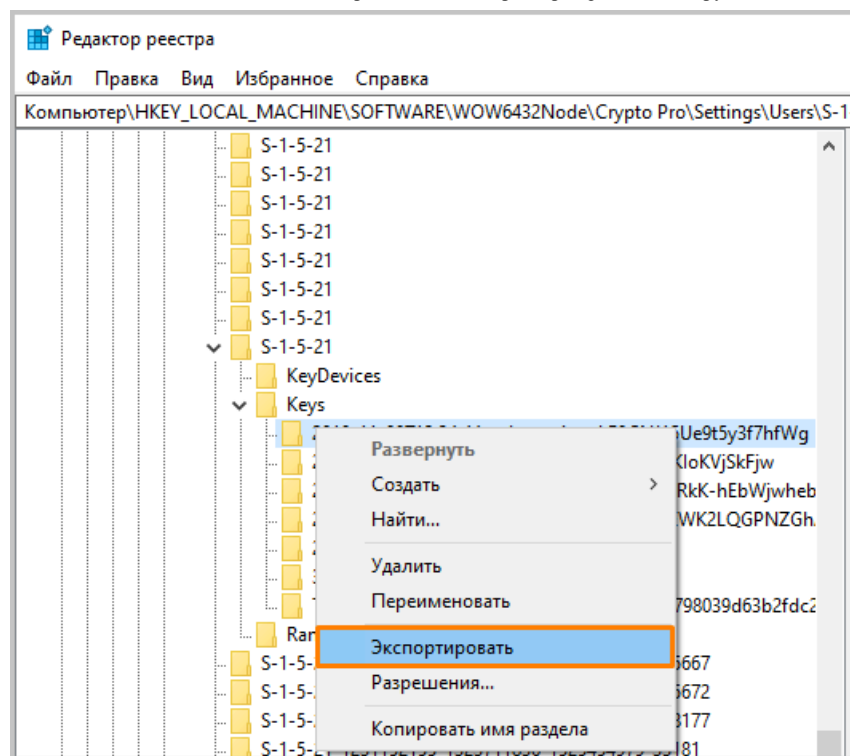
[14 дней бесплатно](#)

Копирование контейнера из реестра другого пользователя

1. Необходимо найти ветку реестра с нужным контейнером. Ветки реестра, в которых может быть контейнер закрытого ключа:

- для 32-битной ОС:
HKEY_LOCAL_MACHINE\SOFTWARE\Crypto Pro\Settings\Users*идентификатор пользователя*\Keys*Название контейнера*;
- для 64-битной ОС:
HKEY_LOCAL_MACHINE\SOFTWARE\Wow64 32Node\Crypto Pro\Settings\USERS*идентификатор пользователя*\Keys*Название контейнера*.

2. После того, как нашли нужную ветку, нажмите правой кнопкой мыши на ветку с контейнером и выберите «Экспортировать».

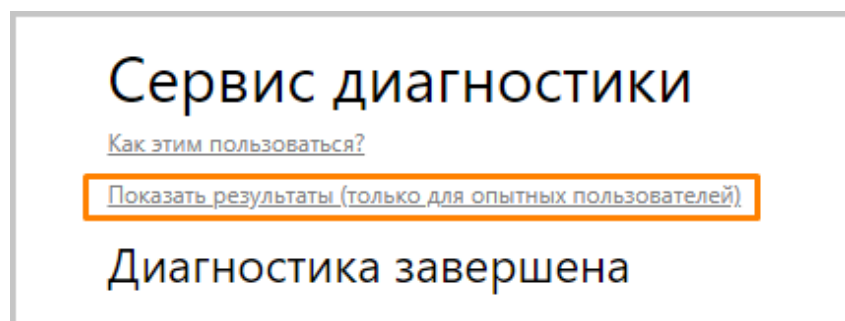


3. Введите имя файла и нажмите на кнопку «Сохранить».

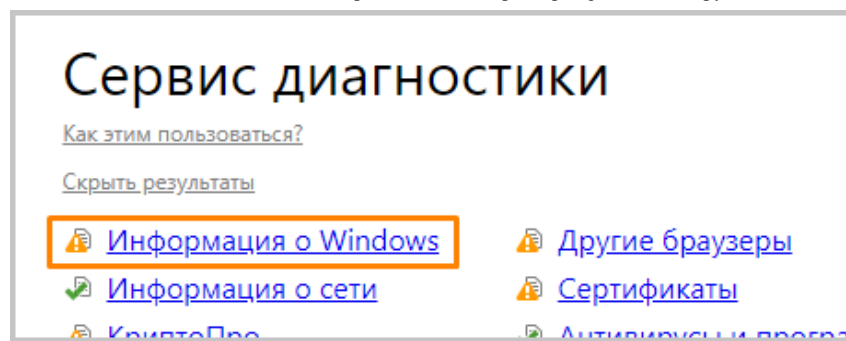
4. Скопируйте файл на тот компьютер, где будете работать с электронной подписью обычными средствами Windows.

5. Пройдите диагностику на сайте <https://help.kontur.ru>.

6. Как диагностика закончится, нажмите на ссылку «Показать результаты».

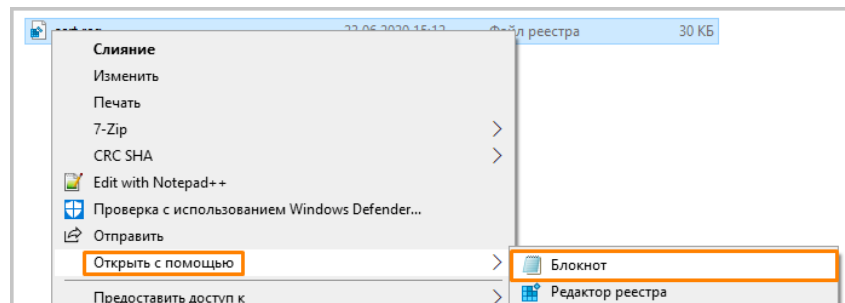


7. В списке результатов выберите «Информация о Windows». Скопируйте оттуда SID текущего пользователя.

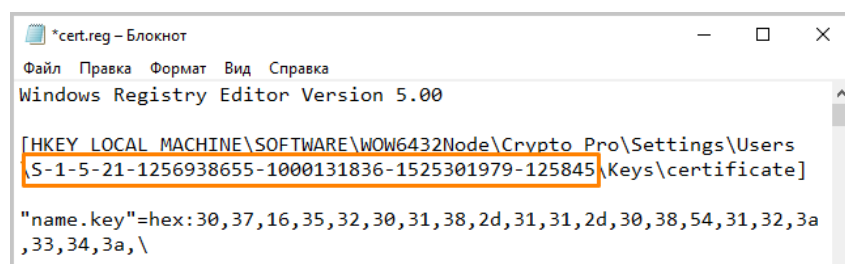


✓ Кодировка	Кириллица (Windows-1251)
✓ Локаль	Русская
✓ Компьютер в домене	Нет
✓ SID текущего пользователя	S-1-5-21-1323711155-1323711836-1525454979-125666 (highlighted with an orange box)
✓ Параметр AppData	C:\Users\AppData\Roaming
✓ Параметр LocalAppData	C:\Users\AppData\Local

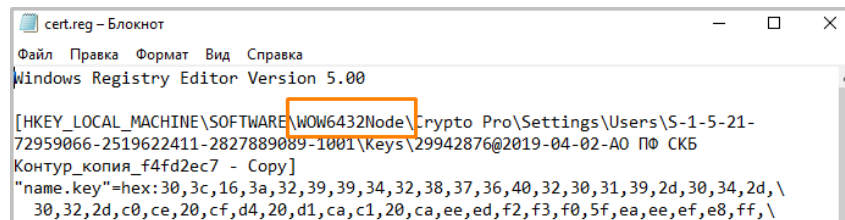
8. Откройте экспортированный файл реестра с помощью «Блокнота».



9. Замените SID пользователя на скопированный ранее.



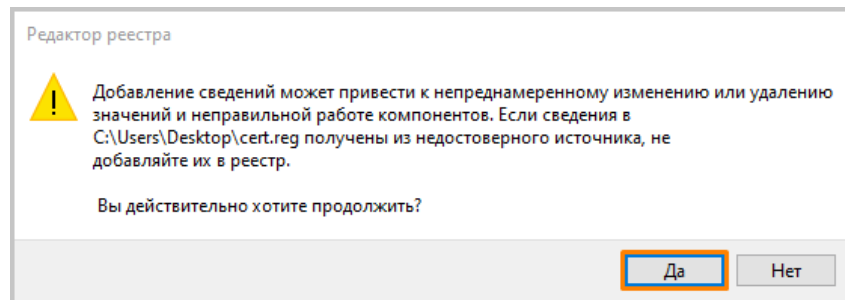
Если ветка реестра экспортируется из 32-битной ОС в 64-битную ОС, добавьте в путь ветки реестра параметр Wow6432Node как на скриншоте:



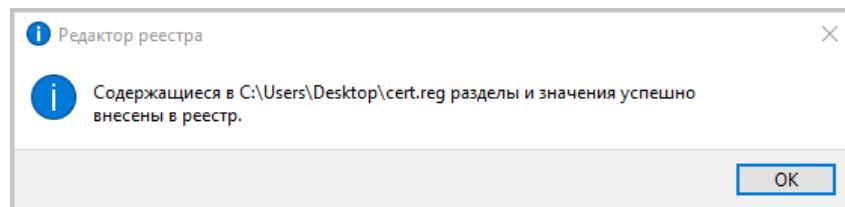
10. Сохраните изменения и закройте файл.

11. Снова нажмите на файл правой кнопкой мыши и выберите «Слияние».

В появившемся окне нажмите «Да».



Должно появиться сообщение о том, что данные успешно внесены в реестр. Нажмите «ОК».



Если появляется сообщение «Ошибка при доступе к реестру», необходимо еще раз проверить все пути в файле на корректность. Также проверьте, чтобы в пути не было лишних пробелов, знаков.

12. После того, как данные будут внесены в реестр, необходимо вручную установить

сертификат (см. [Как установить личный сертификат](#)).