

Подпись файлов в Windows с помощью сертификата на Рутокен

Современные сервисы по выпуску сертификатов могут использовать размер ключа **RSA 4096**.

Импорт и работа с такими ключами и алгоритмом возможны только с использованием семейства **Рутокен ЭЦП 3.0**

Для подписи файлов или кода приложений в Windows необходим сертификат со следующим полем:

Подписание кода (1.3.6.1.5.5.7.3.3)

Подобные сертификаты можно получить, например, в следующих сервисах:

<https://sectigo.com/cps-repository>

<https://shop.globalsign.com/ru-ru/code-signing>

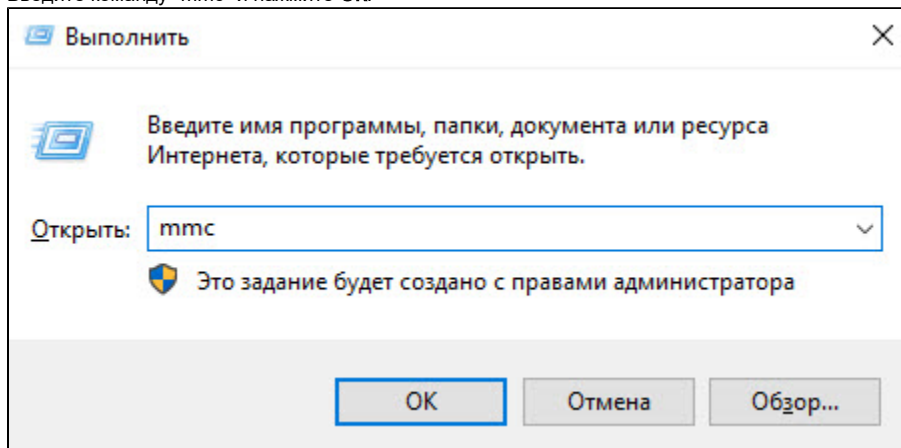
- Экспорт сертификата с закрытым ключом из реестра Windows
- Импорт сертификат на Рутокен
- Подпись файлов с помощью сертификата на Рутокен

Экспорт сертификата с закрытым ключом из реестра Windows

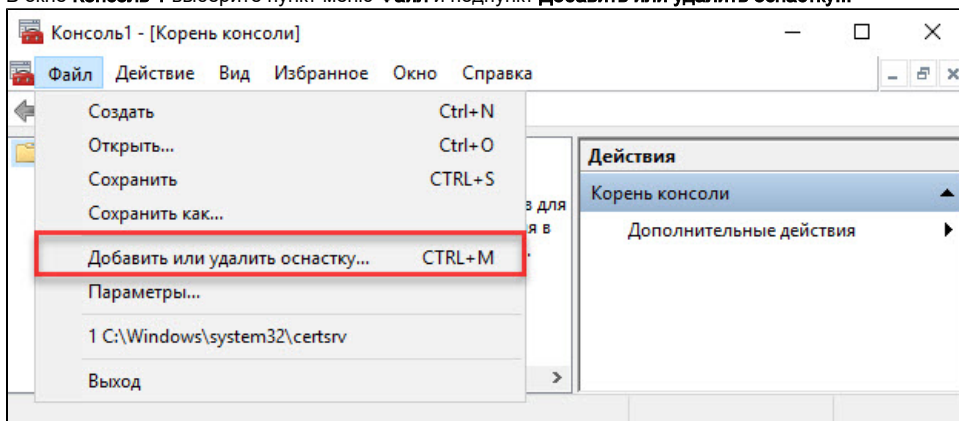
Если сертификат был выписан в реестр Windows, его необходимо экспортировать в файл формата pfx.

Для этого необходимо выполнить следующие действия:

1. Нажмите комбинацию клавиш **Windows + X** и выберите пункт меню **Выполнить**.
2. Введите команду "mmc" и нажмите **OK**.

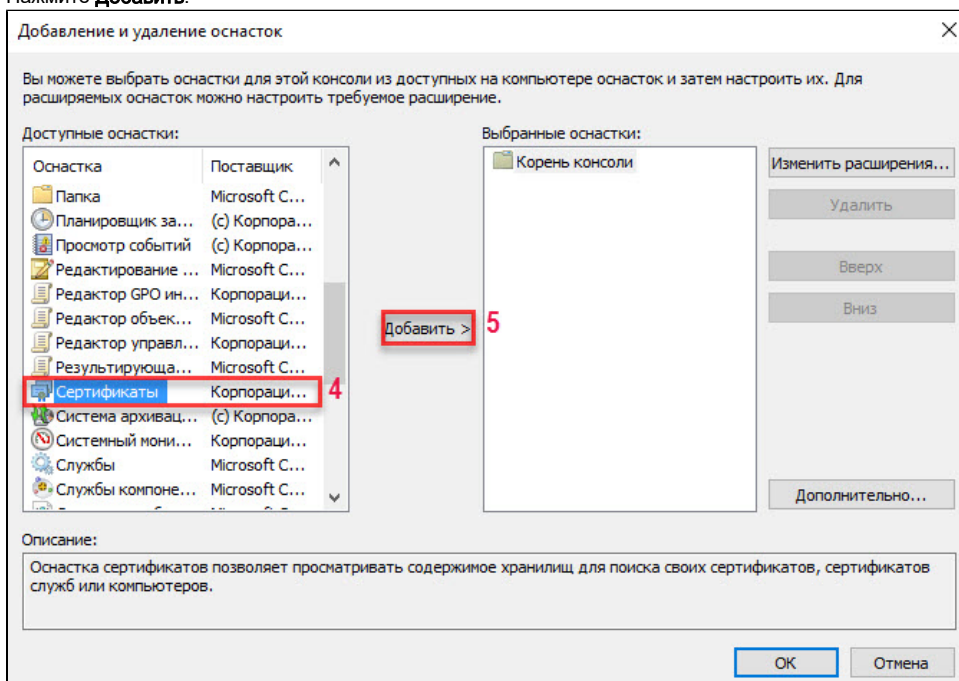


3. В окне **Консоль 1** выберите пункт меню **Файл** и подпункт **Добавить или удалить оснастку...**

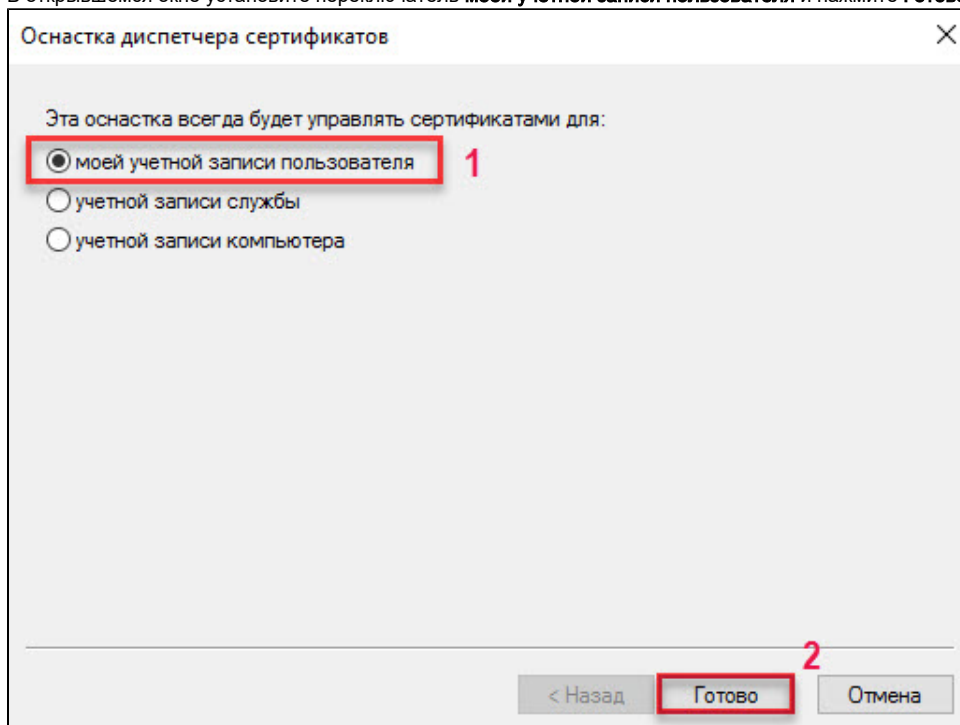


4. В левой части окна **Добавление и удаление оснастки** щелкните по названию **Сертификаты**.

5. Нажмите **Добавить**.

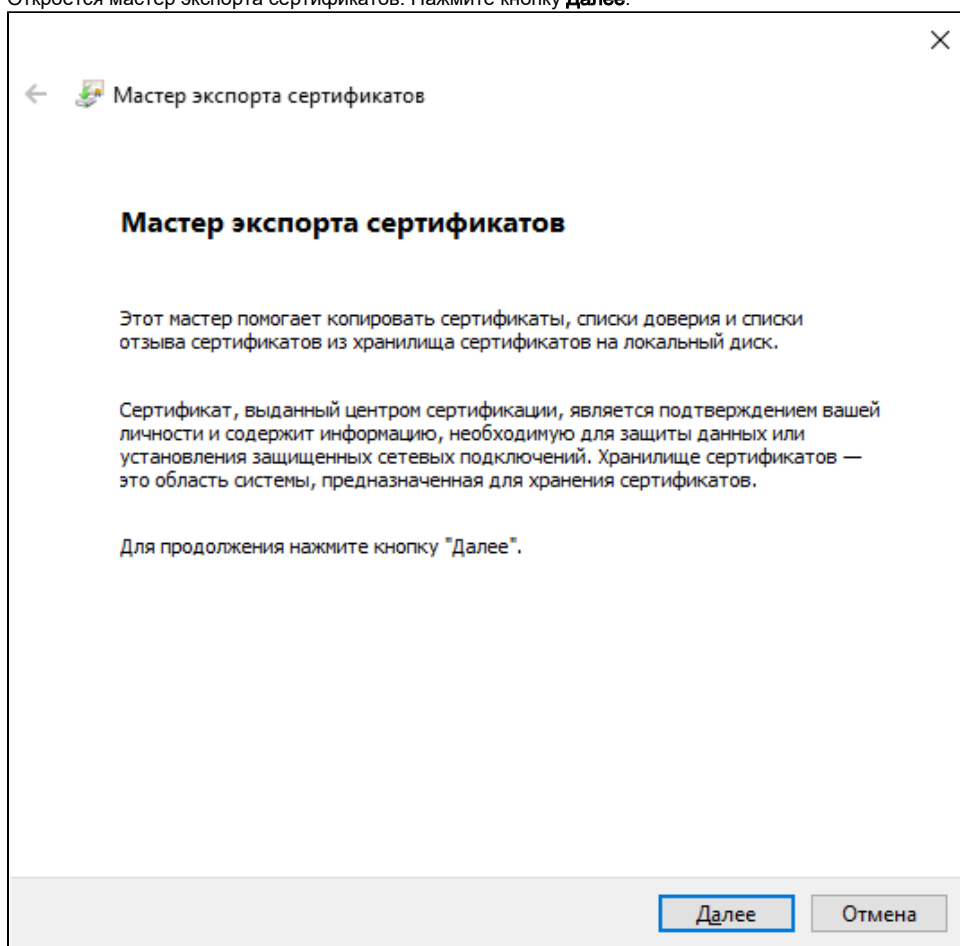


6. В открывшемся окне установите переключатель **моей учетной записи пользователя** и нажмите **Готово**.

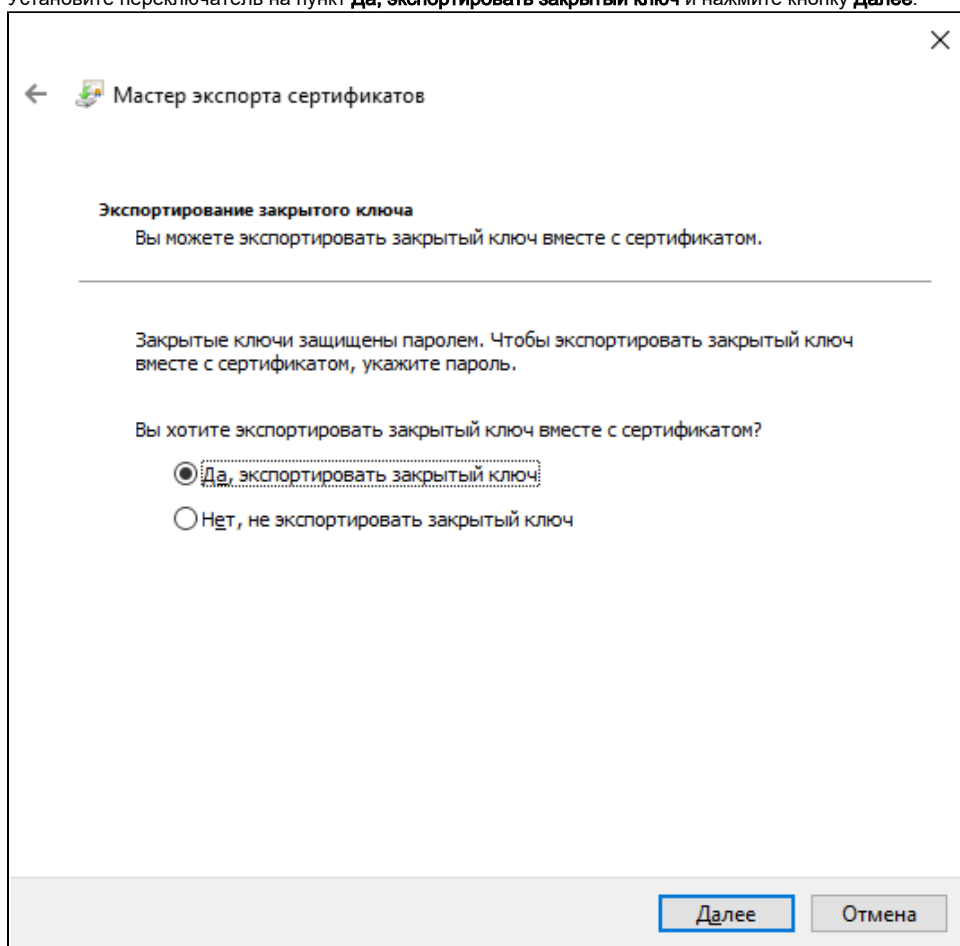


7. В окне **Добавление и удаление оснасток** нажмите **ОК**.
8. В левой части окна **Консоль1** щелкните по названию папки **Личные**.
9. Щелкните по названию папки **Сертификаты**.
10. В правой части окна выберите нужный сертификат и нажмите на его имени правой кнопкой мыши.
11. Выберите пункт меню **Все задачи\Экспорт**.

12. Откроется мастер экспорта сертификатов. Нажмите кнопку **Далее**.



13. Установите переключатель на пункт **Да, экспортировать закрытый ключ** и нажмите кнопку **Далее**.



14. Установите дополнительные пункты экспорта при необходимости и нажмите кнопку **Далее**.

  Мастер экспорта сертификатов ✕

Формат экспортируемого файла
Сертификаты могут быть экспортированы в различных форматах.

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)

Далее

Отмена

15. Установите переключатель **Пароль**, введите пароль и нажмите кнопку **Далее**.

  Мастер экспорта сертификатов ✕

Безопасность
Для обеспечения безопасности вам необходимо защитить закрытый ключ для субъекта безопасности или воспользоваться паролем.

☐ Группы или пользователи (рекомендуется)

Добавить

Удалить

☒ Пароль:

••••••••

Подтверждение:

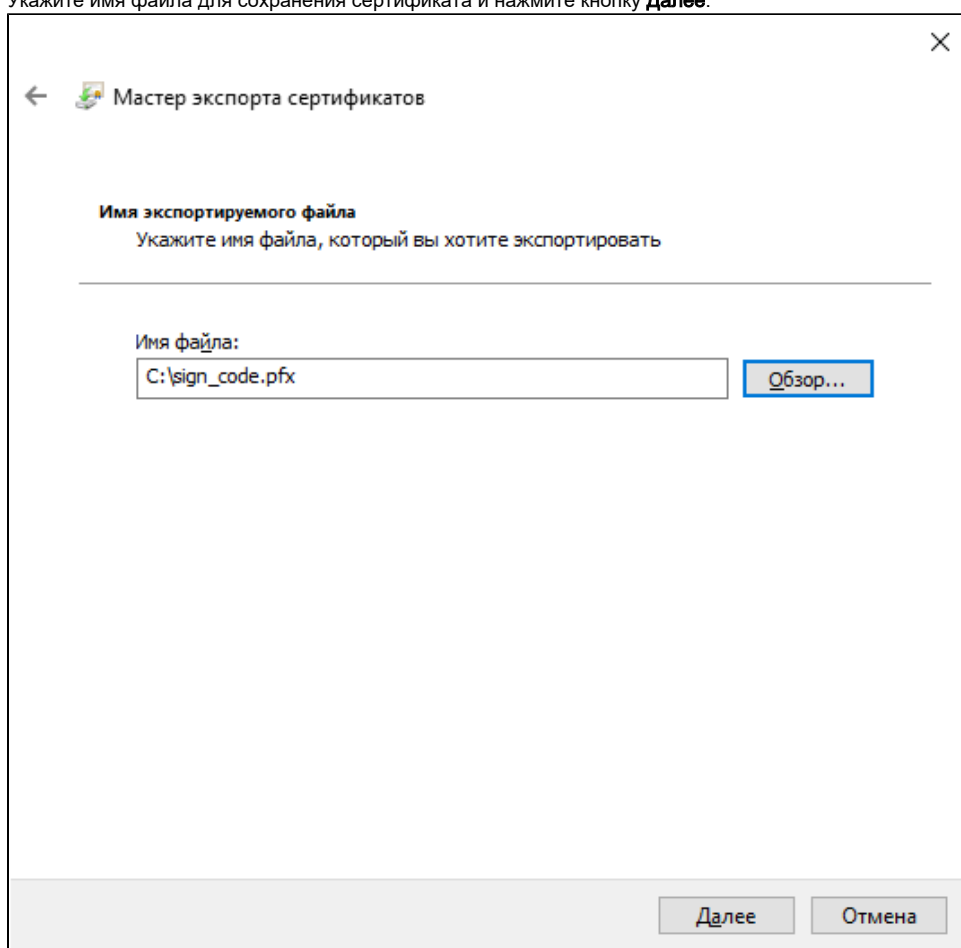
••••••••

Шифрование: TripleDES-SHA1 ▾

Далее

Отмена

16. Укажите имя файла для сохранения сертификата и нажмите кнопку **Далее**.



The image shows a Windows dialog box titled "Мастер экспорта сертификатов" (Certificate Export Wizard). It has a back arrow icon on the left and a close 'X' icon on the right. The main text reads "Имя экспортируемого файла" (Name of the file to be exported) followed by "Укажите имя файла, который вы хотите экспортировать" (Specify the name of the file you want to export). Below this is a text input field containing "C:\sign_code.pfx" and a button labeled "Обзор..." (Browse...). At the bottom right, there are two buttons: "Далее" (Next) and "Отмена" (Cancel).

Мастер экспорта сертификатов

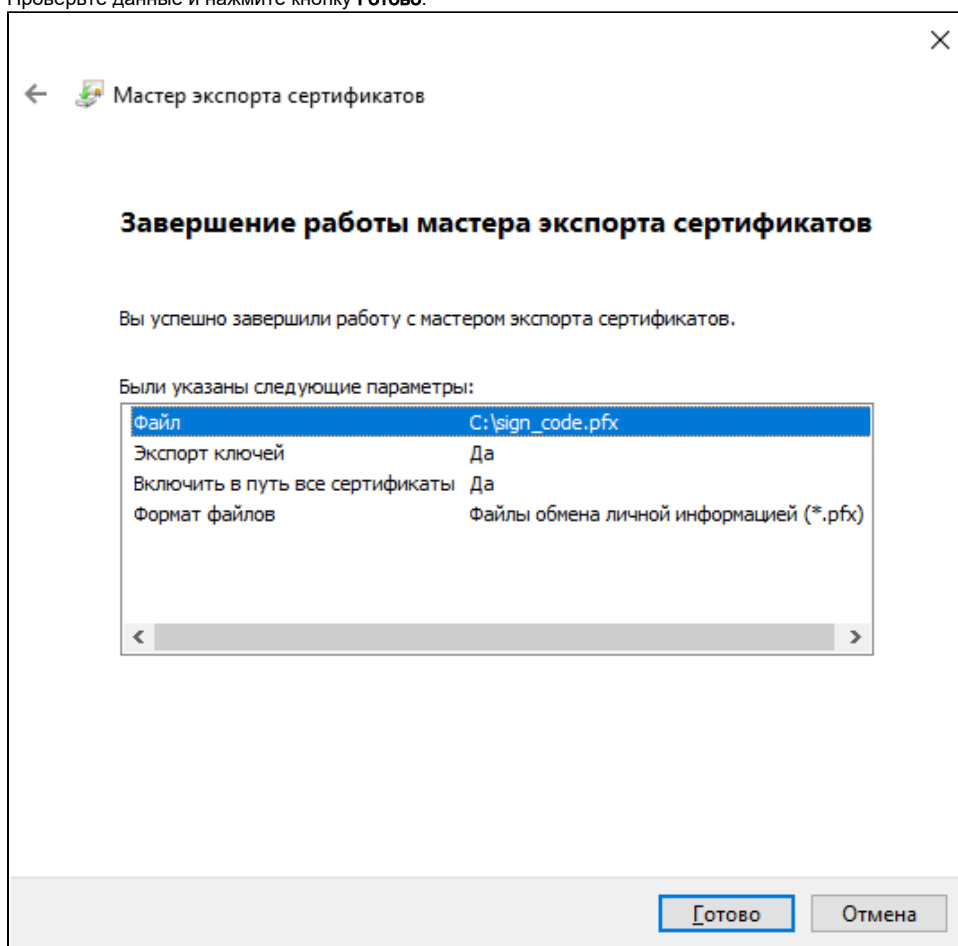
Имя экспортируемого файла
Укажите имя файла, который вы хотите экспортировать

Имя файла:
C:\sign_code.pfx

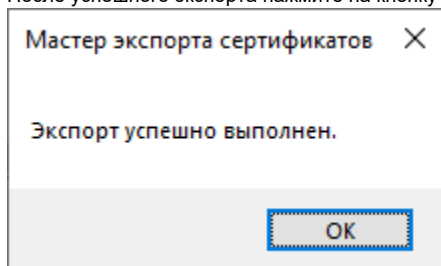
Обзор...

Далее Отмена

17. Проверьте данные и нажмите кнопку **Готово**.



18. После успешного экспорта нажмите на кнопку **ОК**.

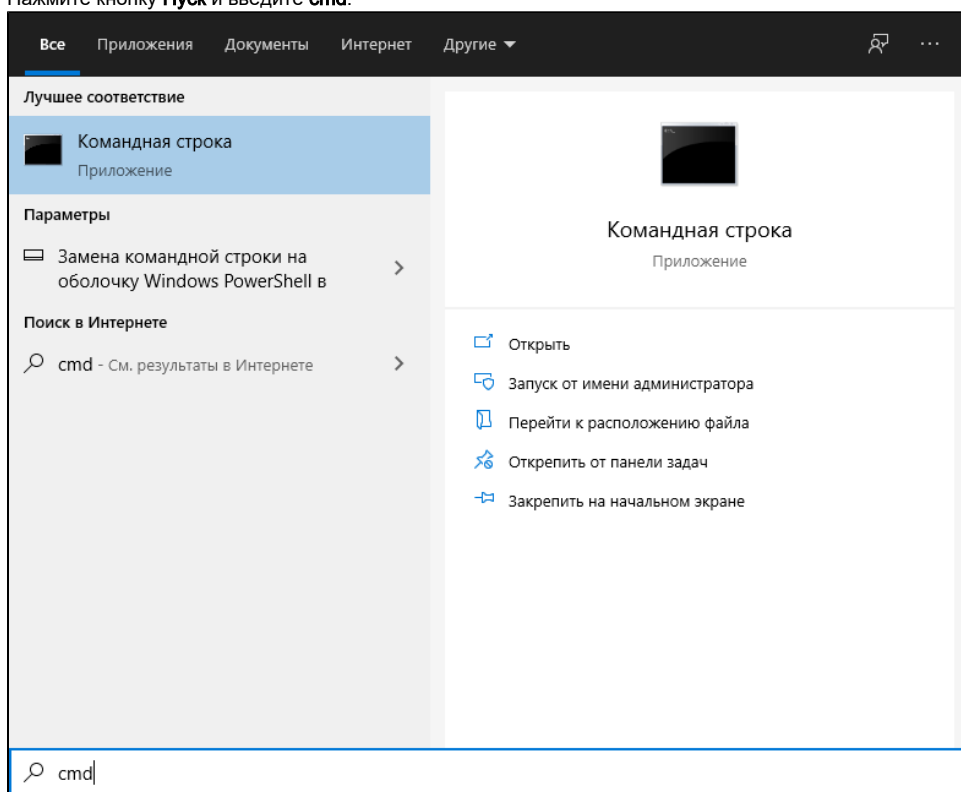


Далее необходимо импортировать сертификат на Рутокен.

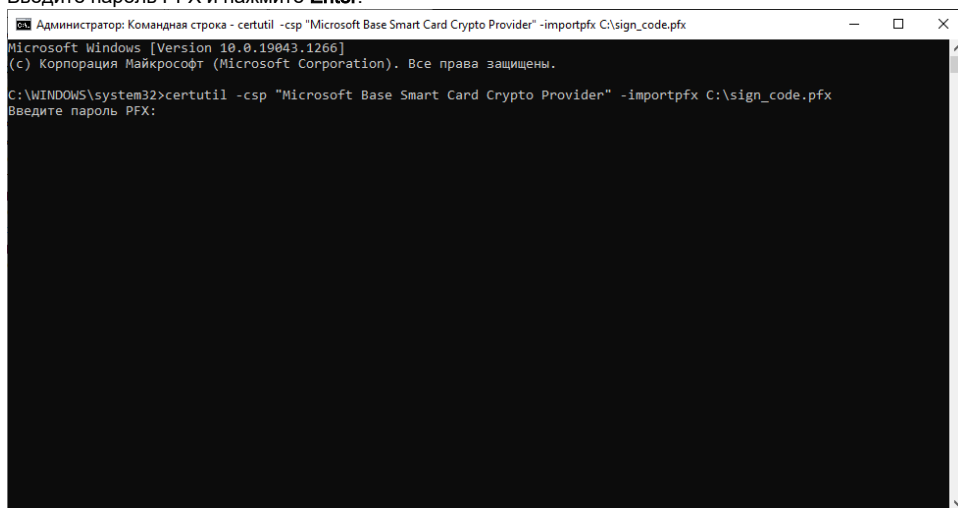
Импорт сертификат на Рутокен

Для импорта сертификата на Рутокен необходимо выполнить следующие действия

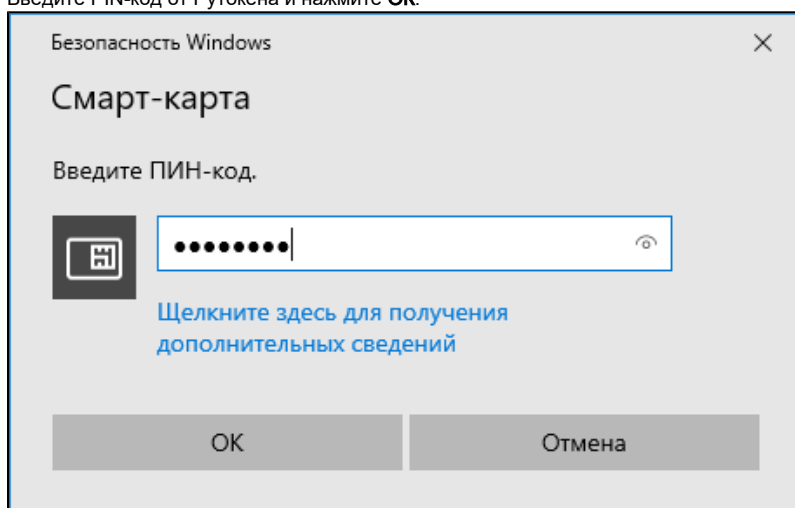
1. Нажмите кнопку **Пуск** и введите **cmd**.



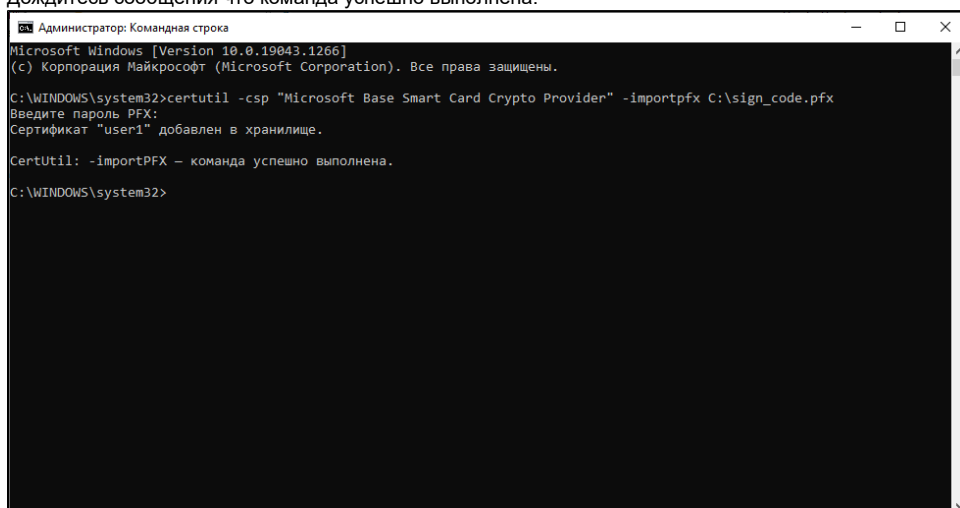
2. Выберите пункт **Запуск от имени администратора**.
3. Если необходимо введите имя и пароль администратора компьютера.
4. Подключите Рутокен к компьютеру.
5. В командной строке наберите следующую команду: **certutil -csp "Microsoft Base Smart Card Crypto Provider" -importpfx C:\sign_code.pfx** и нажмите **Enter**.
6. Введите пароль PFX и нажмите **Enter**.



7. Введите PIN-код от Рутокена и нажмите **ОК**.

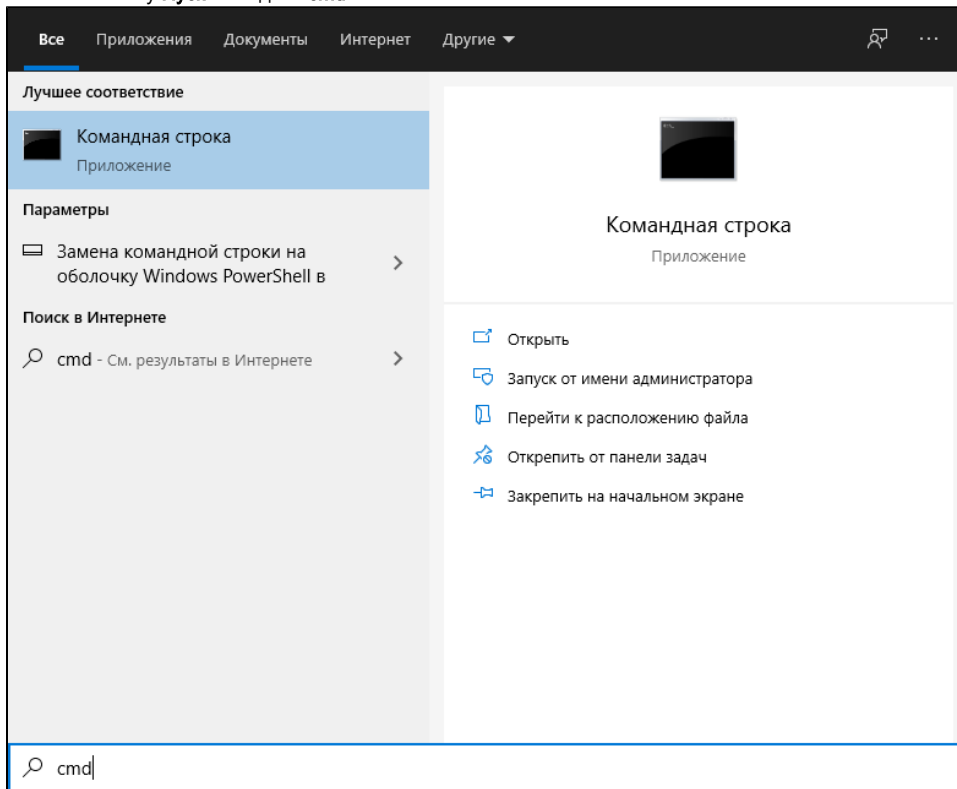


8. Дождитесь сообщения что команда успешно выполнена.

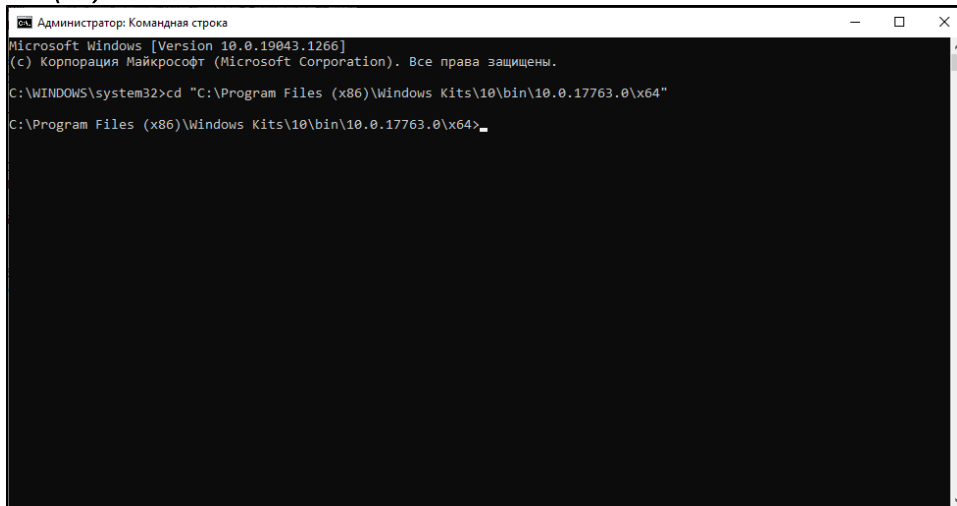


Подпись файлов с помощью сертификата на Рутокен

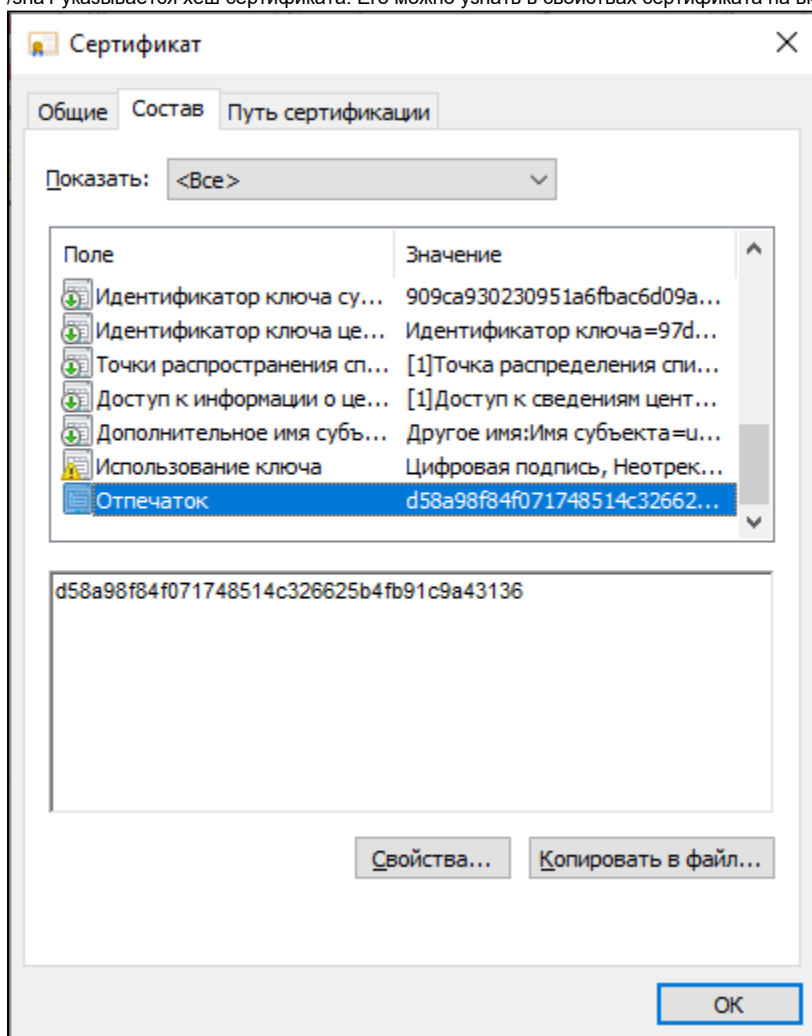
1. Нажмите кнопку **Пуск** и введите **cmd**.



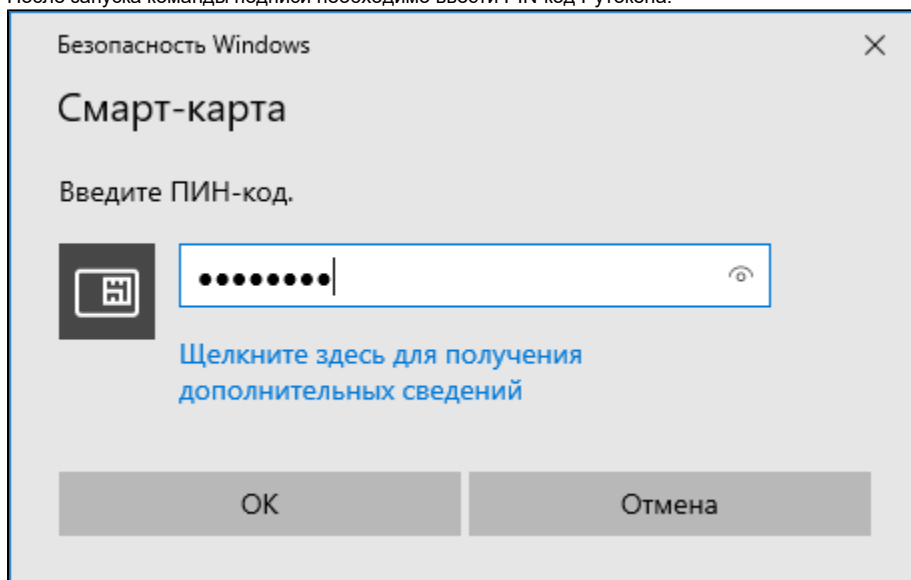
2. Выберите пункт **Запуск от имени администратора**.
3. Если необходимо введите имя и пароль администратора компьютера.
4. Подключите Рутокен к компьютеру.
5. Перейдите в папку с утилитой signtool, например, `C:\Program Files (x86)\Windows Kits\10\bin\10.0.17763.0\x64` командой **`cd "C:\Program Files (x86)\Windows Kits\10\bin\10.0.17763.0\x64"`**



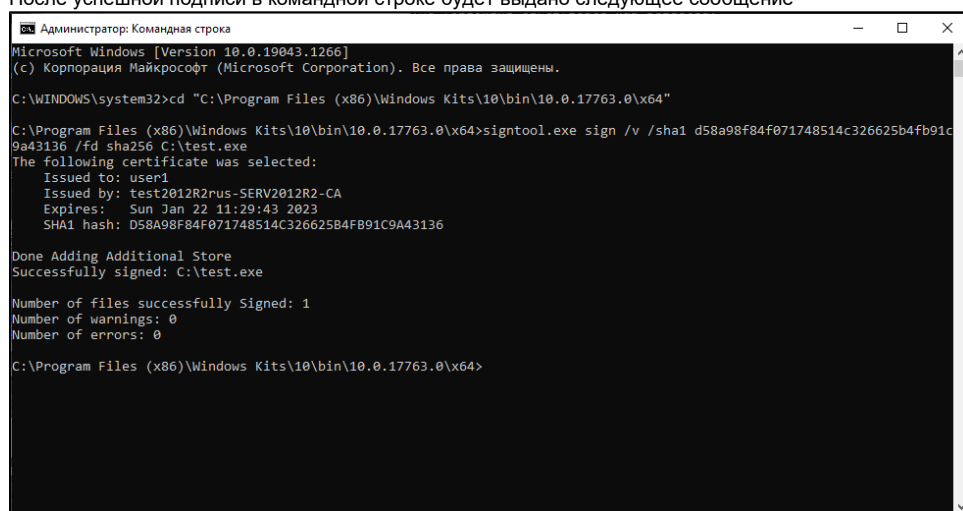
6. Введите команду подписи **signtool.exe sign /v /sha1 d58a98f84f071748514c326625b4fb91c9a43136 /fd sha256 C:\test.exe** где ключем /sha1 указывается хеш сертификата. Его можно узнать в свойствах сертификата на вкладке **Состав** в поле **Отпечаток**.



7. После запуска команды подписи необходимо ввести PIN-код Рутокена.



8. После успешной подписи в командной строке будет выдано следующее сообщение



```
Администратор: Командная строка
Microsoft Windows [Version 10.0.19043.1266]
(c) Корпорация Майкрософт (Microsoft Corporation). Все права защищены.

C:\WINDOWS\system32>cd "C:\Program Files (x86)\Windows Kits\10\bin\10.0.17763.0\x64"

C:\Program Files (x86)\Windows Kits\10\bin\10.0.17763.0\x64>signtool.exe sign /v /sha1 d58a98f84f071748514c326625b4fb91c9a43136 /fd sha256 C:\test.exe
The following certificate was selected:
    Issued to: user1
    Issued by: test2012R2rus-SERV2012R2-CA
    Expires:   Sun Jan 22 11:29:43 2023
    SHA1 hash: D58A98F84F071748514C326625B4FB91C9A43136

Done Adding Additional Store
Successfully signed: C:\test.exe

Number of files successfully Signed: 1
Number of warnings: 0
Number of errors: 0

C:\Program Files (x86)\Windows Kits\10\bin\10.0.17763.0\x64>
```