

Инструкция
по доступу к информационному ресурсу
по протоколу TLS ГОСТ

Оглавление

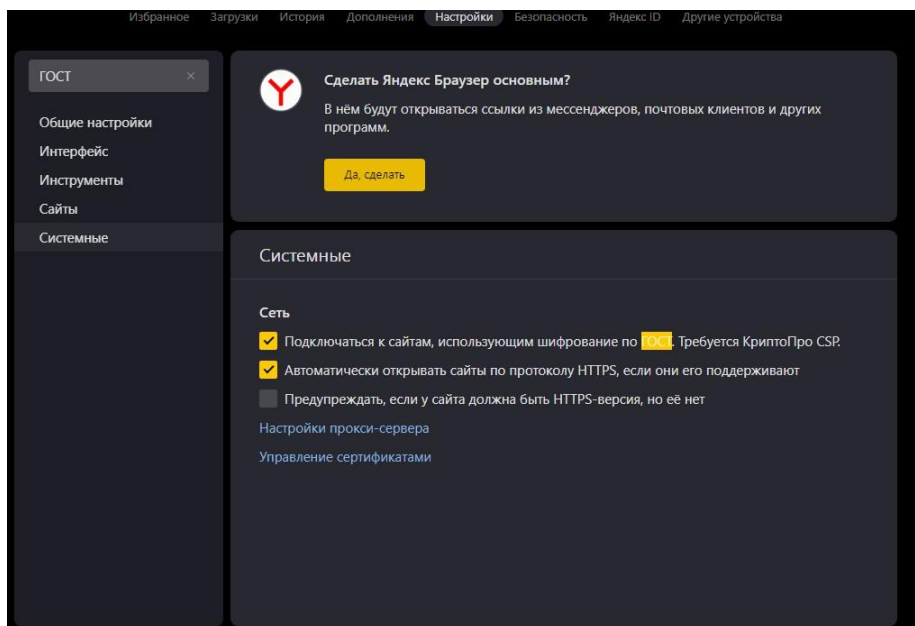
1. Подготовка рабочего места для работы с ресурсами, использующими протокол TLS ГОСТ, с помощью КриптоПро CSP	3
1.1. Выбор браузера	3
1.2. Установка КриптоПРО CSP	4
1.3. Установка сертификатов безопасности	6
1.4. Получение сертификата электронной подписи (ЭП)	6
2. Выгрузка открытого ключа сертификата электронной подписи	7
2.1. Из хранилища «Личные» (для Windows)	7
2.2. С помощью КриптоПро CSP (для Windows)	10
2.3. С помощью программы «Инструменты КриптоПро» (для macOS и Linux)	14
3. Передача открытого ключа и проверка доступа к защищённому ресурсу	15
3.1. Проверка подключения к защищённому ресурсу	15
3.2. Проверка безопасности подключения	17

1. Подготовка рабочего места для работы с ресурсами, использующими протокол TLS ГОСТ, с помощью КриптоПро CSP

1.1. Выбор браузера

Для доступа к веб-ресурсам, использующим отечественные алгоритмы, требуется применение специализированных браузеров. На текущий момент наилучшую поддержку протокола ГОСТ TLS обеспечивают браузеры [Chromium-Gost](#) и [Яндекс Браузер](#), каждый из них совместим с программным обеспечением **КриптоПро CSP** для установления защищённого соединения с использованием российских криптографических алгоритмов шифрования.

В случае использования Яндекс.Браузера убедитесь, что выполнены настройки представленные ниже:



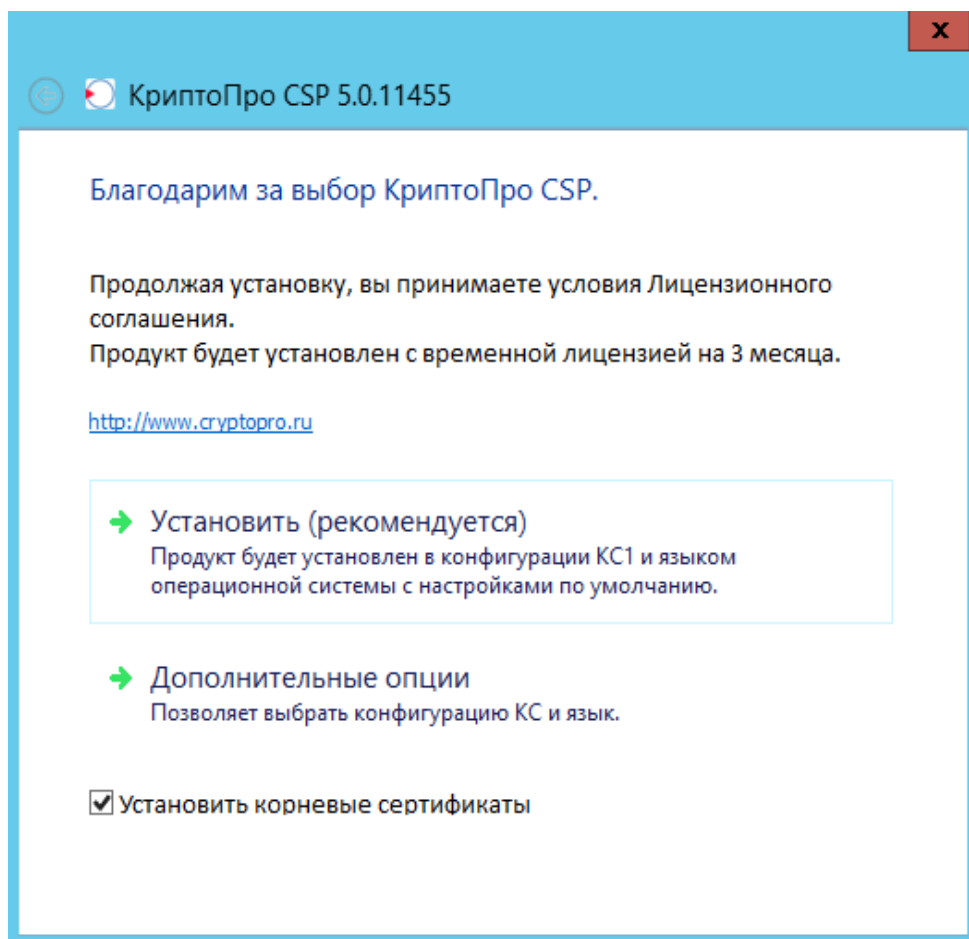
1.2. Установка КриптоПРО CSP

Скачайте с официального сайта компании «КриптоПро» (<https://cryptopro.ru/>) программное обеспечение «**КриптоПро CSP**». Для возможности скачивания программы необходима регистрация пользователя.

Примечание. Действие пробного периода использования указанного продукта – 3 месяца, позже потребуется его приобретение (<https://cryptopro.ru/products/csp?csp=download>).

Для ОС Windows

После загрузки файла, нажмите на него двойным щелчком левой кнопки мыши и проследуйте шагам установщика. После установки ПО потребуется перезагрузить компьютер.

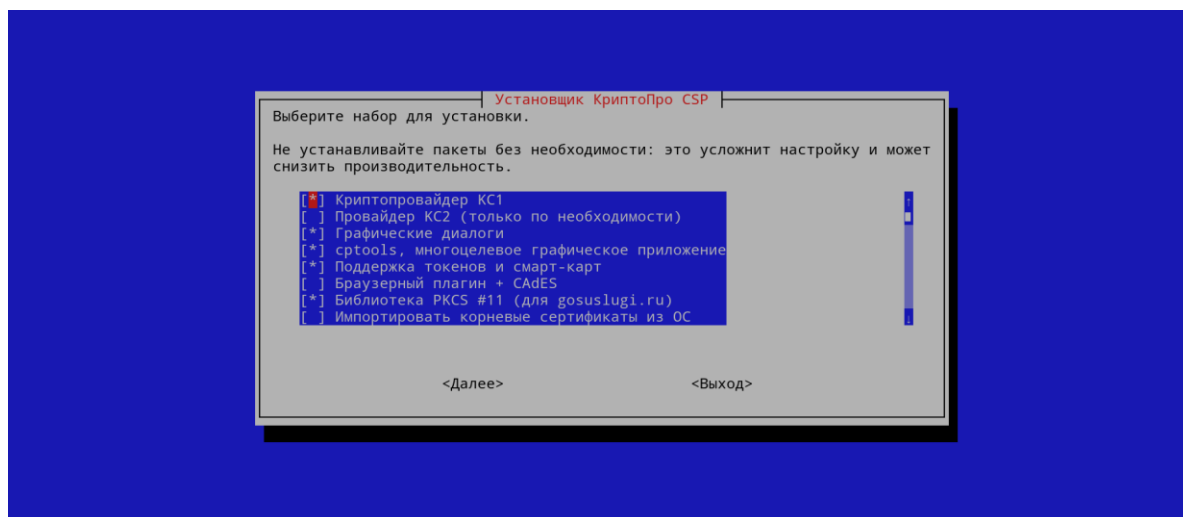


Для ОС Linux

Для загрузки и установки файла воспользуйтесь инструкцией с официального сайта КристоПро по ссылке ниже:

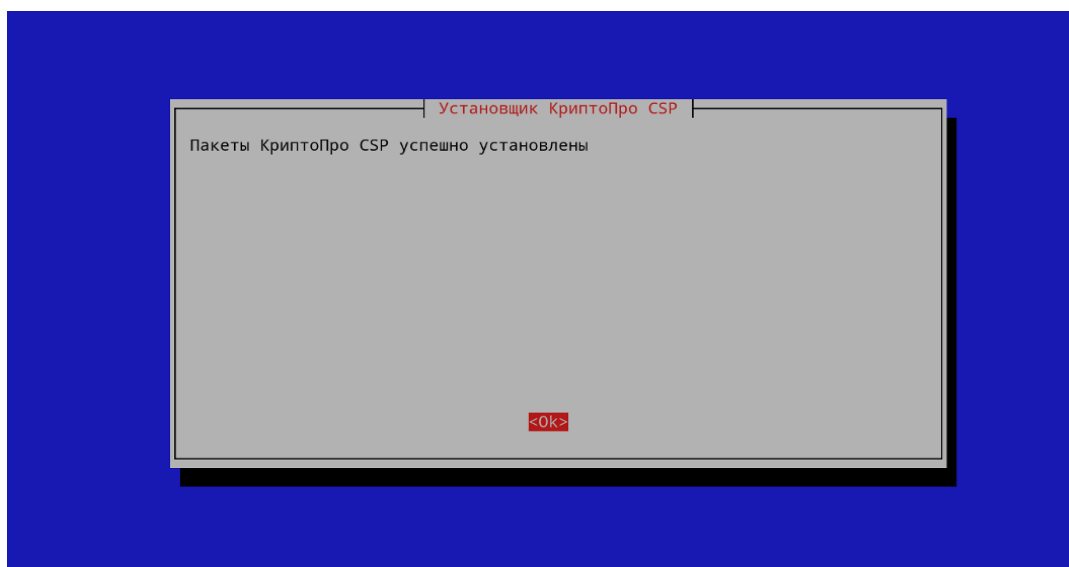
<https://support.cryptopro.ru/index.php?/Knowledgebase/Article/View/390>

В процессе установки выберите компоненты:



Также можно ввести лицензионный ключ на ПО КриптоПро CSP. В противном случае будет активирована пробная лицензия, истекающая через 90 дней. Данный ключ можно будет ввести позже во вкладке «Общее», выбрав там опцию «Ввести лицензию для меня».

По окончании установочного процесса должно появиться окно.



1.3. Установка сертификатов безопасности

Установка сертификатов безопасности. Для установки сертификатов безопасности перейдите на портал Госуслуг по ссылке: <https://www.gosuslugi.ru/crt>.

На сайте предоставлены подробные инструкции по установке корневых и выпускающих сертификатов для доступа к информационному ресурсу с использованием протокола TLS ГОСТ.

1.4. Получение сертификата электронной подписи (ЭП)

Для доступа к информационному ресурсу, функционирующему с использованием протокола TLS ГОСТ, требуется сертификат электронной подписи, записанный на сертифицированный носитель (токен).

Для сотрудников бюджетной сферы (государственные органы, казенные и бюджетные учреждения) получение сертификата ЭП осуществляется в территориальном органе Федерального казначейства (ТОФК). Порядок действий регламентирован официальной инструкцией Казначейства России по ссылке ниже:

<https://old-fk.roskazna.gov.ru/gis/udostoveryayushhiy-centr/onlayn-servispodachi-dokumentov-dlya-polucheniya-sertifikatov-uts/>

Для коммерческих организаций, индивидуальных предпринимателей и физических лиц оформление сертификата ЭП производится на платной основе в любом удостоверяющем центре, аккредитованном Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации.

Актуальный перечень аккредитованных удостоверяющих центров размещен на официальном портале Минцифры России по ссылке ниже: <https://digital.gov.ru/activity/gos-uslugi/akkreditacziya-udostoveryayushhihcentrov>.

2. Выгрузка открытого ключа сертификата электронной подписи

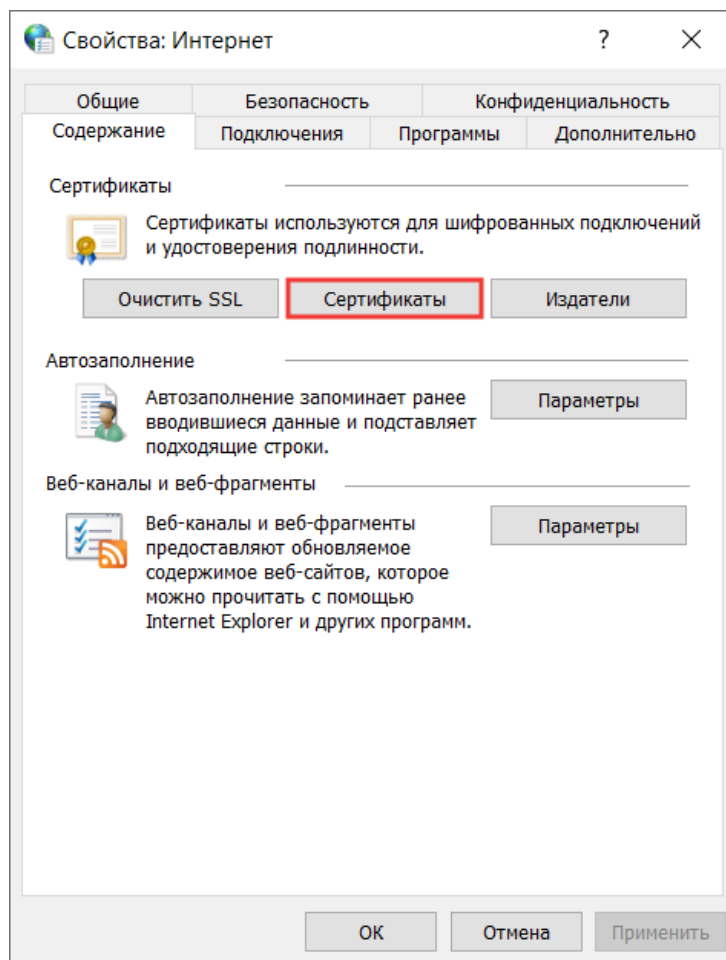
Экспортировать файл открытого ключа можно одним из способов:

- [Из хранилища «Личные» \(для Windows\)](#)
- [С помощью КриптоПро CSP \(для Windows\)](#)
- [С помощью программы «Инструменты КриптоПро \(для macOS и Linux\)](#)

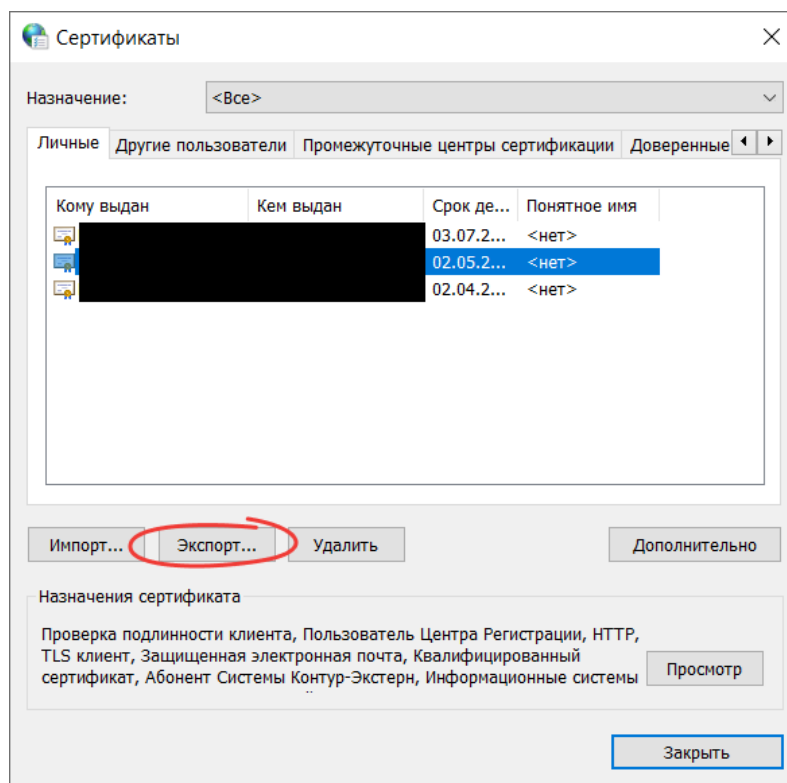
2.1. Из хранилища «Личные» (для Windows)

Чтобы скачать файл открытого ключа из хранилища «Личные» выполните следующее:

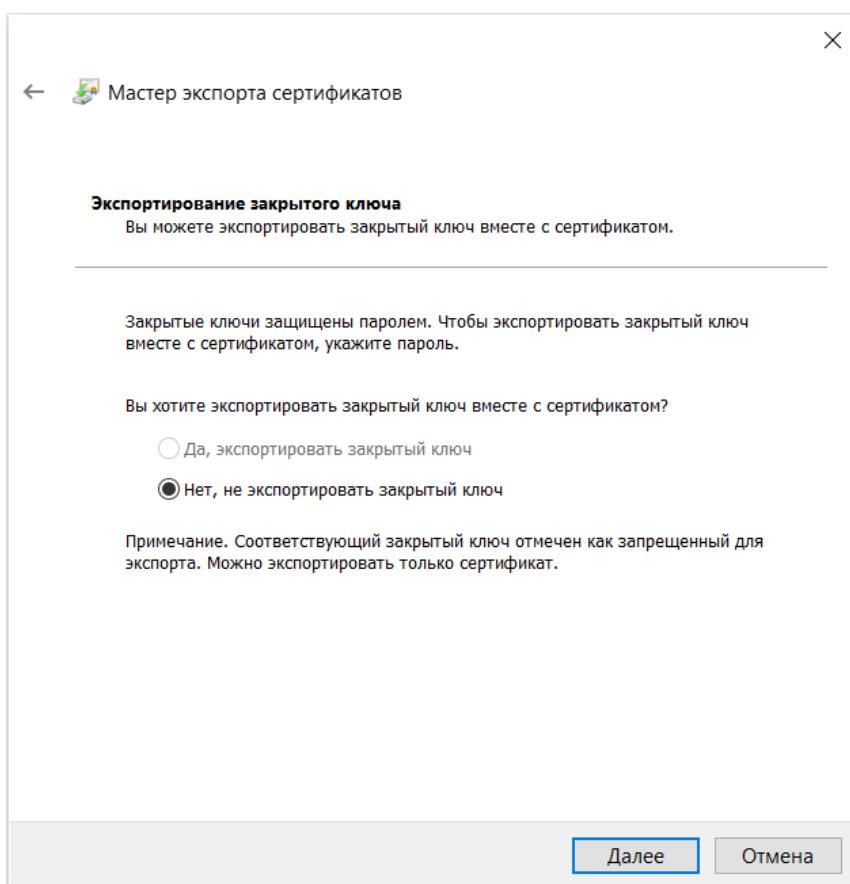
1. В строке поиска в меню «Пуск» напишите «Свойства браузера» и откройте их. Если строки поиска нет, перейдите в меню «Пуск» («Настройки») → «Службные Windows» («Инструменты Windows») → «Панель управления» → «Сеть и интернет» → «Свойства обозревателя» («Свойства браузера»).
2. Выберите вкладку «Содержание» и нажмите на кнопку «Сертификаты».



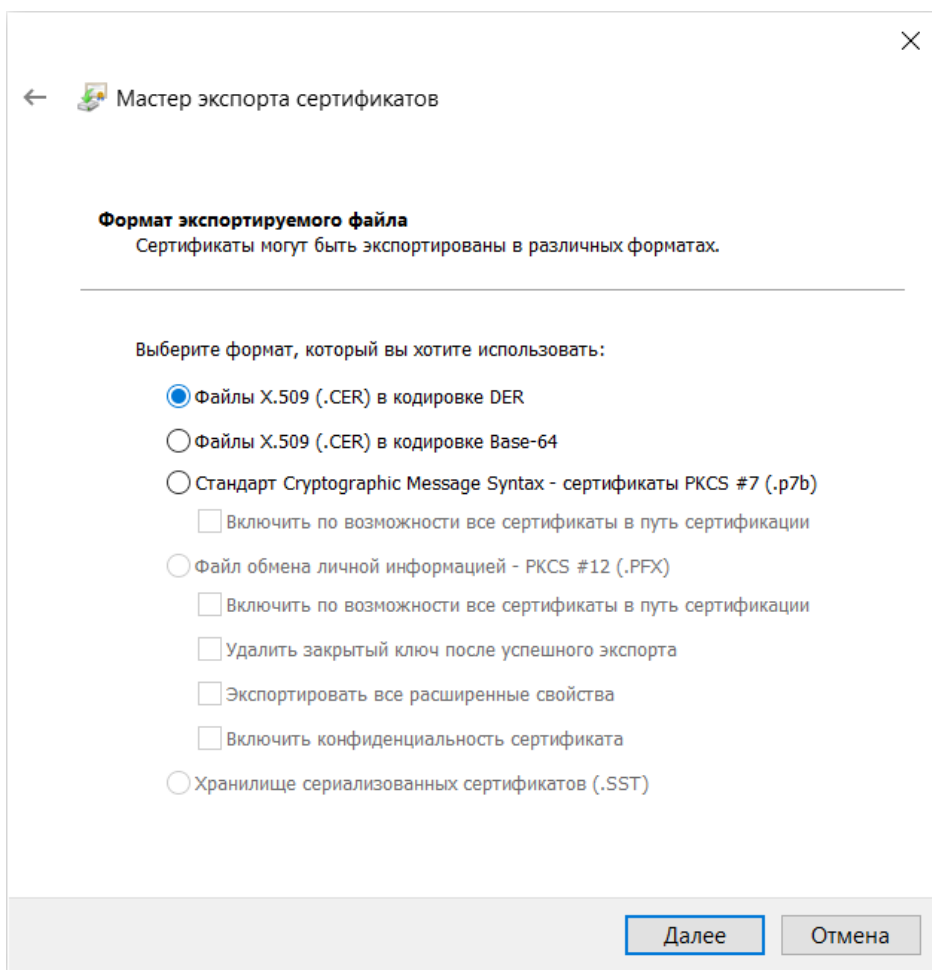
3. Найдите в списке нужный сертификат и нажмите на кнопку «Экспорт».



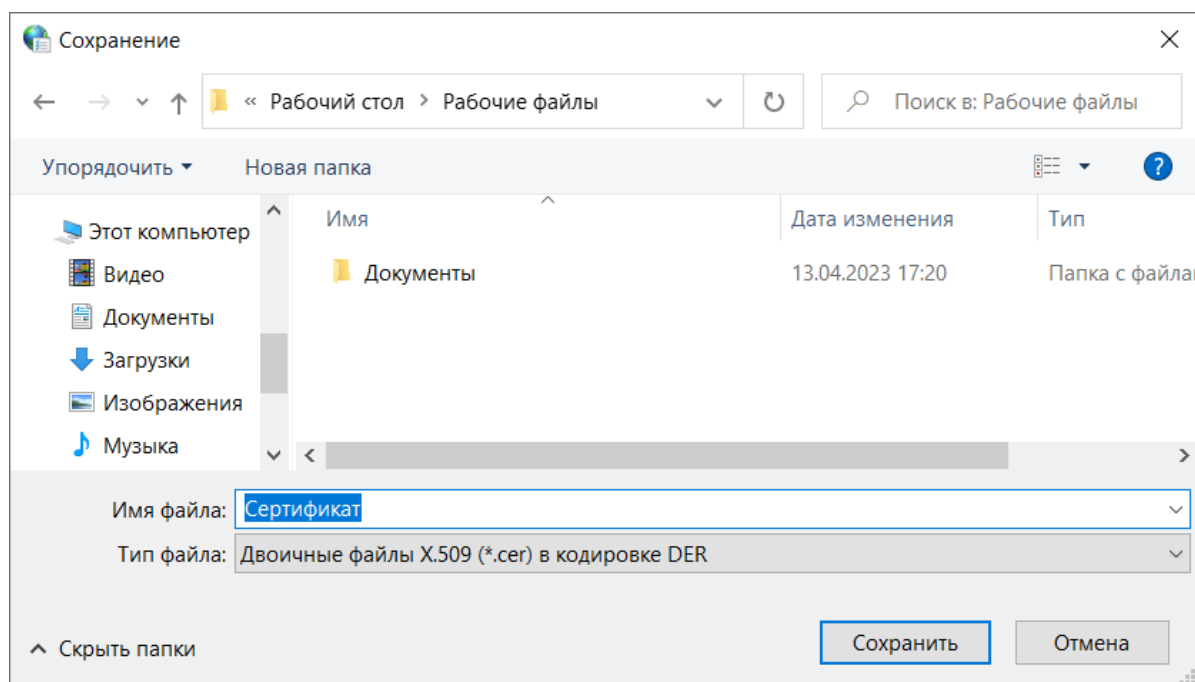
4. Если в списке отсутствует нужный сертификат, перейдите к экспорту [с помощью КриптоПро CSP](#).
5. В окне «Мастер экспорта сертификатов» нажмите «Далее».
6. Выберите «Нет, не экспортировать закрытый ключ» и нажмите «Далее».



7. Выберите «Файлы X.509 (.CER) в кодировке DER» и нажмите «Далее».



8. Нажмите на кнопку «Обзор», выберите папку для сохранения и впишите название файла. Нажмите «Сохранить».



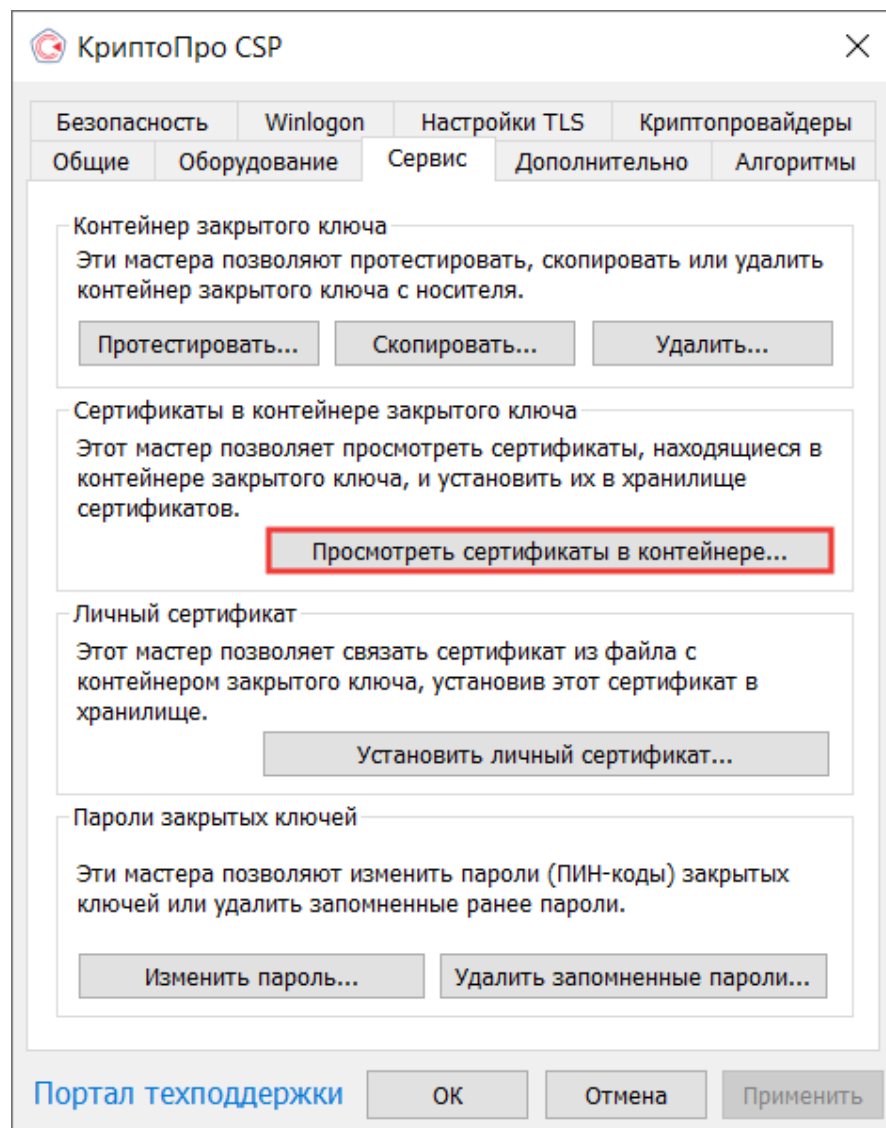
9. Нажмите «Далее».

10. Нажмите «Готово». Дождитесь сообщения об успешном экспорте.

2.2. С помощью КристоПро CSP (для Windows)

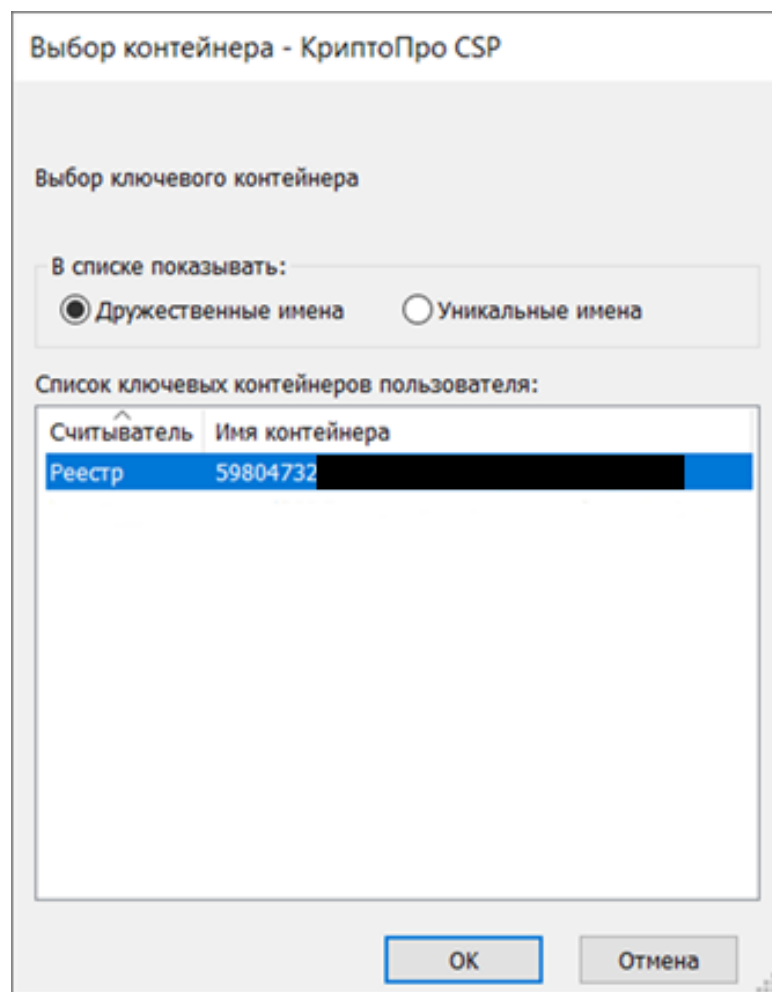
Для экспорта выполните следующее:

1. Выберите меню «Пуск» → «Панель управления» → «КристоПро CSP» или укажите в строке поиска на панели Windows «КристоПро CSP» и нажмите на него.
2. Выберите вкладку «Сервис» и нажмите «Просмотреть сертификаты в контейнере».

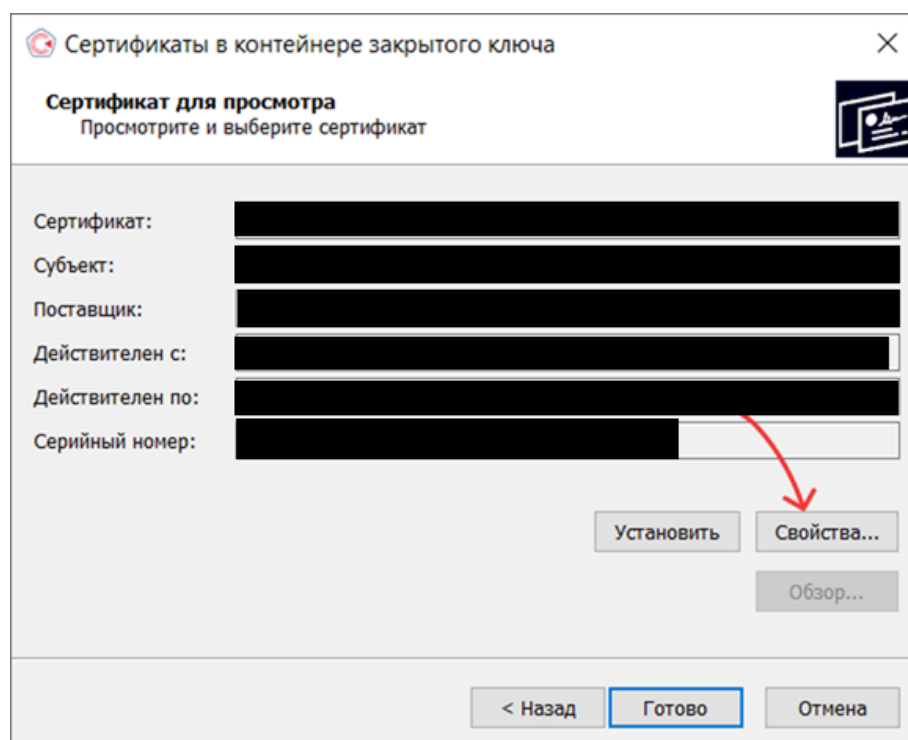


3. В открывшемся окне нажмите «Обзор», чтобы выбрать контейнер для просмотра.

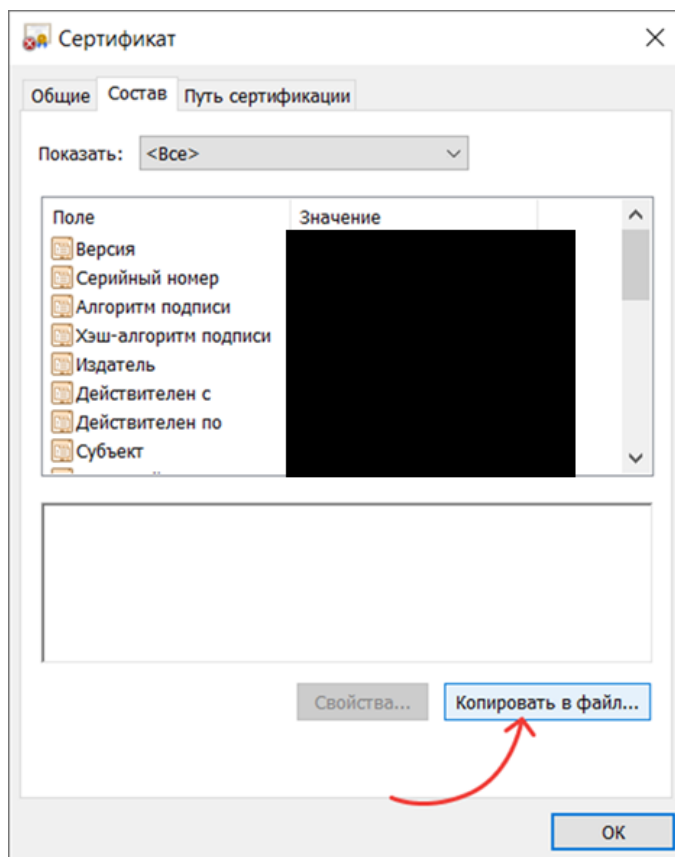
4. После выбора контейнера нажмите «ОК».



5. Нажмите на кнопку «Свойства».

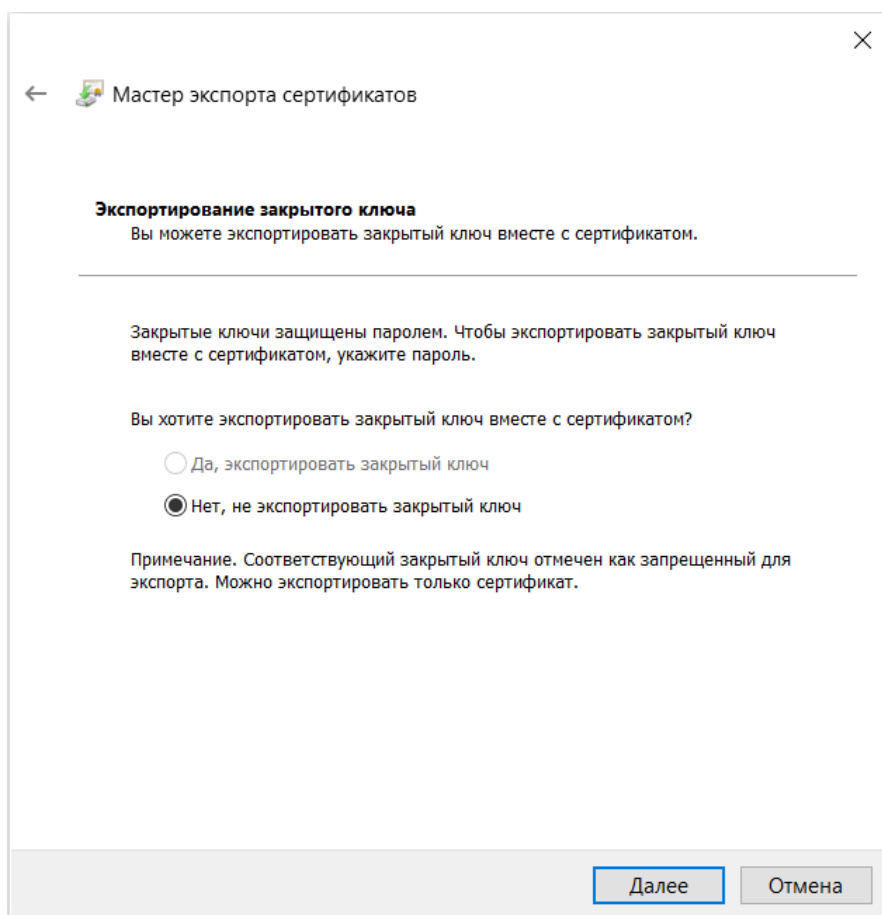


6. Выберите вкладку «Состав» и нажмите «Копировать в файл».

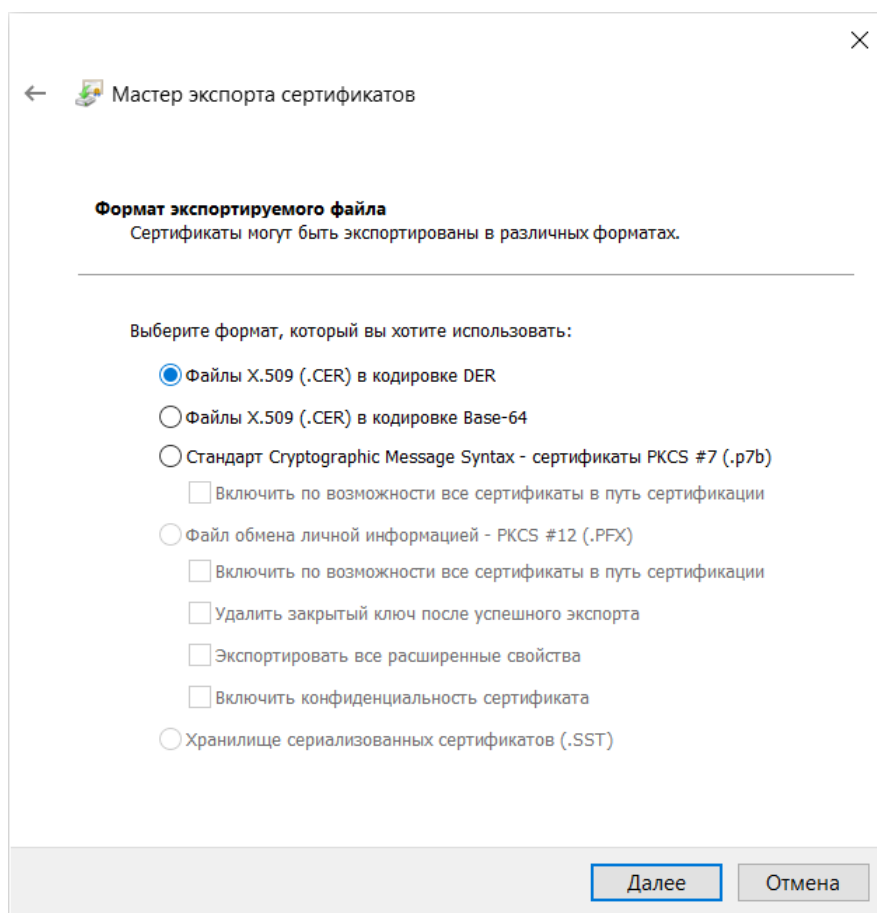


7. В окне «Мастер экспорта сертификатов» нажмите «Далее».

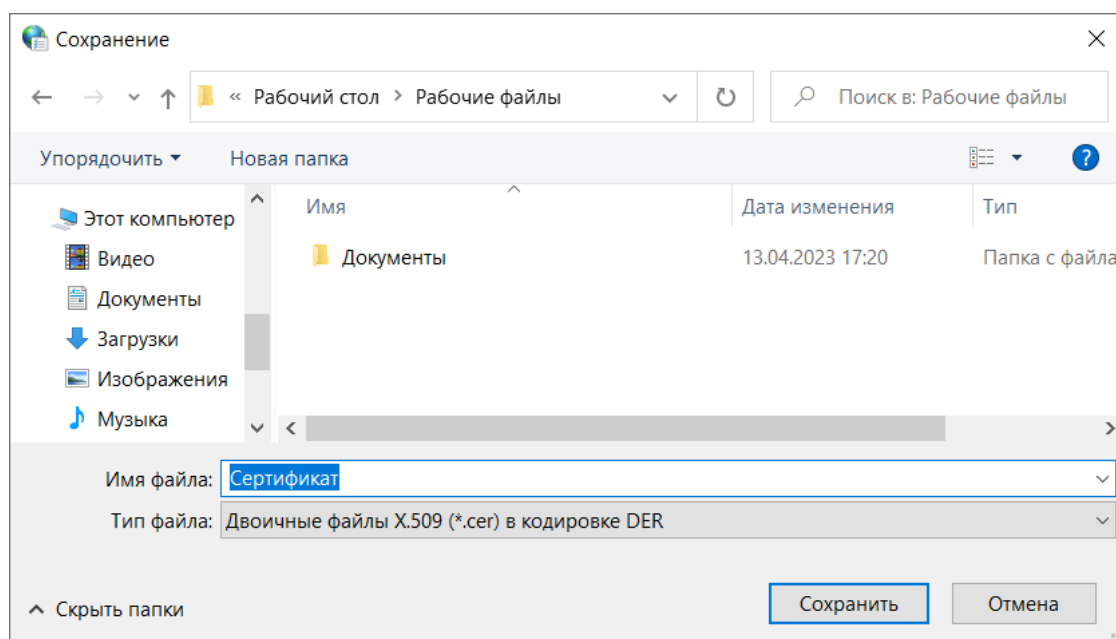
Выберите «Нет, не экспортировать закрытый ключ» и нажмите «Далее».



8. В окне «Формат экспортируемого файла» выберите «Файлы X.509 (.CER) в кодировке DER» и нажмите «Далее».



9. Нажмите на кнопку «Обзор». Выберите папку, в которую сохранится файл, а также придумайте и укажите имя файла. Нажмите «Сохранить».

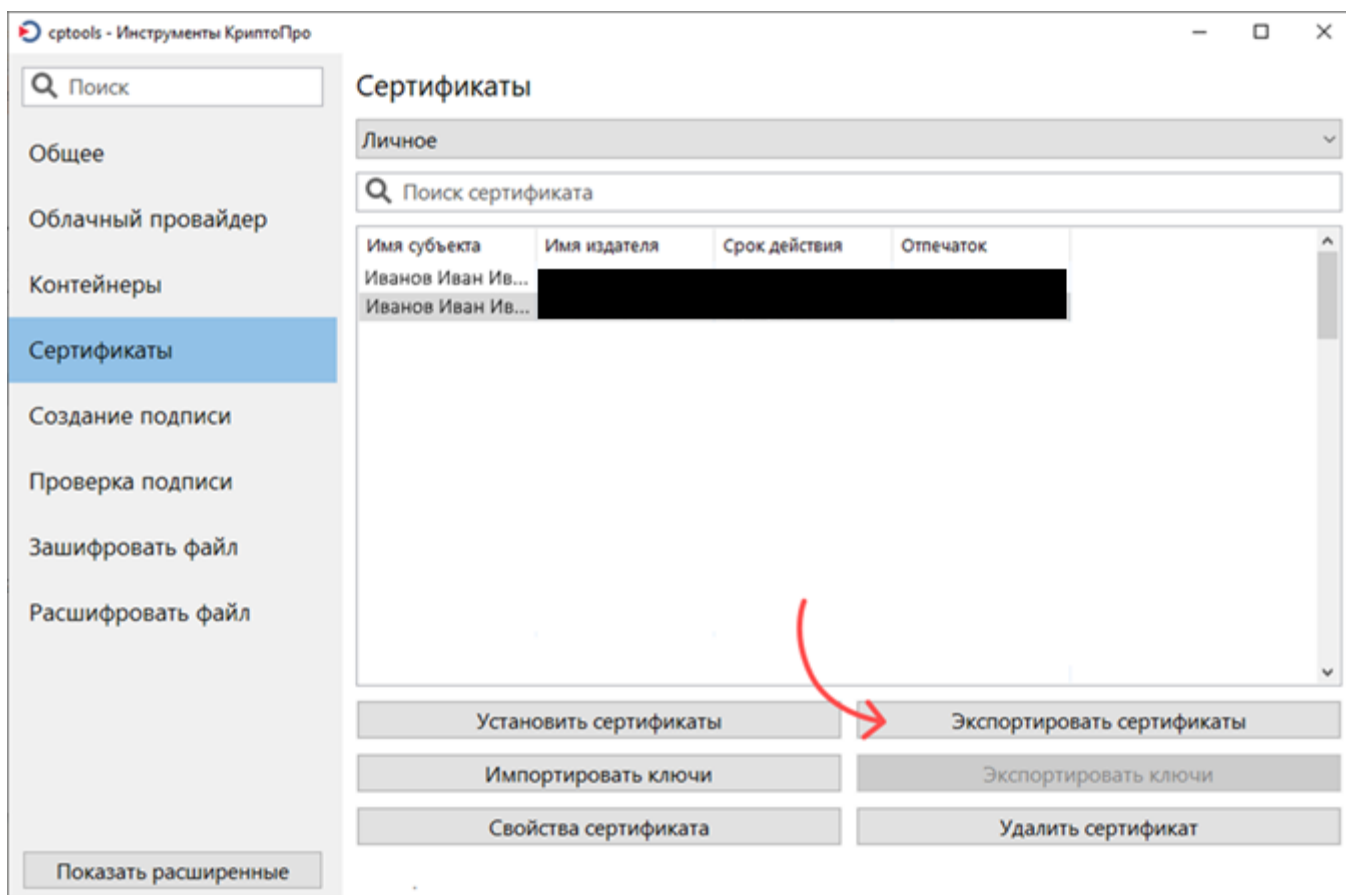


10. Нажмите «Далее».
11. Нажмите «Готово». Дождитесь сообщения об успешном экспорте.

2.3. С помощью программы «Инструменты КриптоПро» (для macOS и Linux)

Данный способ возможен при установленном КриптоПро CSP 5.0

1. Откройте на компьютере программу «Инструменты КриптоПро».
2. Перейдите в раздел «Сертификаты».
3. Выберите нужный сертификат и нажмите «Экспортировать сертификаты».



4. Укажите имя сохраняемого файла. Выберите папку для сохранения и формат файла *.cer в кодировке DER.

3. Передача открытого ключа и проверка доступа к защищённому ресурсу

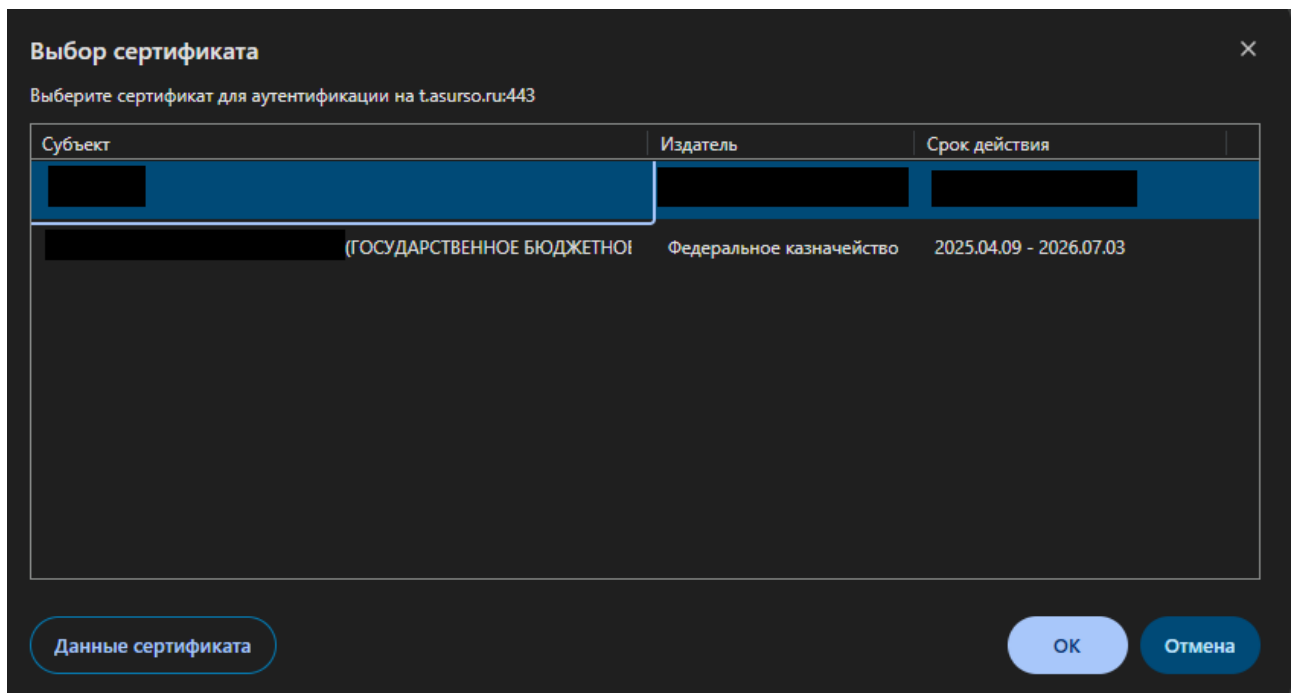
После того как вы выгрузили файл открытого ключа (.cer), его необходимо передать администратору информационного ресурса или в уполномоченную организацию для внесения в список доверенных пользователей.

Порядок передачи определяется внутренним регламентом ресурса.

После передачи ключа и его активации на стороне ресурса выполните проверку доступа.

3.1. Проверка подключения к защищённому ресурсу

1. Убедитесь, что носитель с сертификатом электронной подписи (токен) подключён к компьютеру.
2. Откройте браузер, настроенный для работы с ГОСТ TLS (см. раздел 1.1).
3. Перейдите на единый портал доступа к информационным ресурсам по протоколу TLS ГОСТ: <https://tls.samregion.ru>
4. В открывшемся окне выберите ваш сертификат электронной подписи из списка. Нажмите «ОК».



Важно: Если не выбрать сертификат и закрыть окно или нажать «Отмена», доступ к ресурсу будет запрещён.

400 Bad Request

No required SSL certificate was sent

nginx

5. После выбора сертификата появится окно для ввода пароля к контейнеру закрытого ключа (пароль от токена/носителя). Введите пароль и нажмите «ОК».

Аутентификация - КриптоПро CSP

Crypto-Pro GOST R 34.10-2012 Cryptographic Service Provider запрашивает пин-код на носитель

Считыватель:

Носитель:

Введите пин-код:

☐ Сохранить пароль в приложении

☐ Сохранить пароль в системе

⚠ Выбран язык ввода, отличный от английского

ОК Отмена

6. При успешном подключении откроется главная страница ресурса.

Государственное бюджетное учреждение Самарской области
«ЦИФРОВОЙ РЕГИОН»

Доступные ресурсы

ИС
Веб-ресурс

Краткое описание назначения и функциональных возможностей ресурса

Если вы не видите в списке нужный вам ресурс, вы можете запросить к нему доступ

[Создать или изменить запрос](#)

3.2. Проверка безопасности подключения

Для проверки безопасности подключения на ОС Windows необходимо в браузере активировать индикатор идентификатора сайта (значок замка) в адресной строке. Далее следует перейти в раздел «Безопасное подключение». В браузере на ОС Linux проверка осуществляется аналогично.

