

Установка криптопровайдера КриптоПро CSP

Последние изменения: 2024-03-26

Установка КриптоПро CSP

Пройдите процедуру регистрации и [загрузите](#) дистрибутив КриптоПро CSP с официального сайта разработчика.

Установка дистрибутива СКЗИ КриптоПро CSP должна производиться пользователем, имеющим права администратора.

При установке КриптоПро CSP следуйте инструкциям мастера установки:



Благодарим за выбор КриптоПро CSP.

Продолжая установку, вы принимаете условия Лицензионного соглашения.
Продукт будет установлен с временной лицензией на 3 месяца.

<http://www.cryptopro.ru>

→ **Установить (рекомендуется)**
Продукт будет установлен в конфигурации КС1 и языком операционной системы с настройками по умолчанию.

→ **Дополнительные опции**
Позволяет выбрать конфигурацию КС и язык.

Установить корневые сертификаты

Рекомендуется устанавливать КриптоПро CSP с автоматическими настройками, но вы можете установить язык и конфигурацию уровня безопасности самостоятельно (с помощью кнопки «Дополнительные опции»).

Благодарим за выбор КристоПро CSP.

Язык установки:

- Русский
 English

Уровень безопасности:

- КС1
 КС2
 КС3

→ **Установить**
Установить с выбранными КС-уровнем и языком.

После завершения установки перезагрузите браузер.

КристоПро CSP успешно установлен.
Для корректной работы КристоПро CSP может потребоваться перезапустить браузер.

ОК

Установка контейнера закрытого ключа

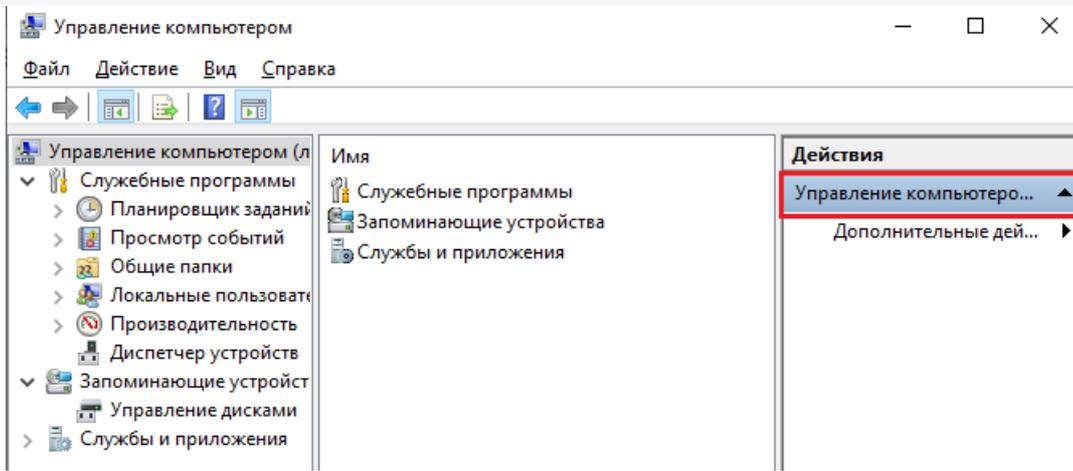
Контейнер закрытого ключа может быть установлен на одном из носителей:

- реестр (для установки в реестр);
- директория;
- съемный диск для хранения ключей (usb-ключ, ffc-карта, виртуальный жесткий диск).

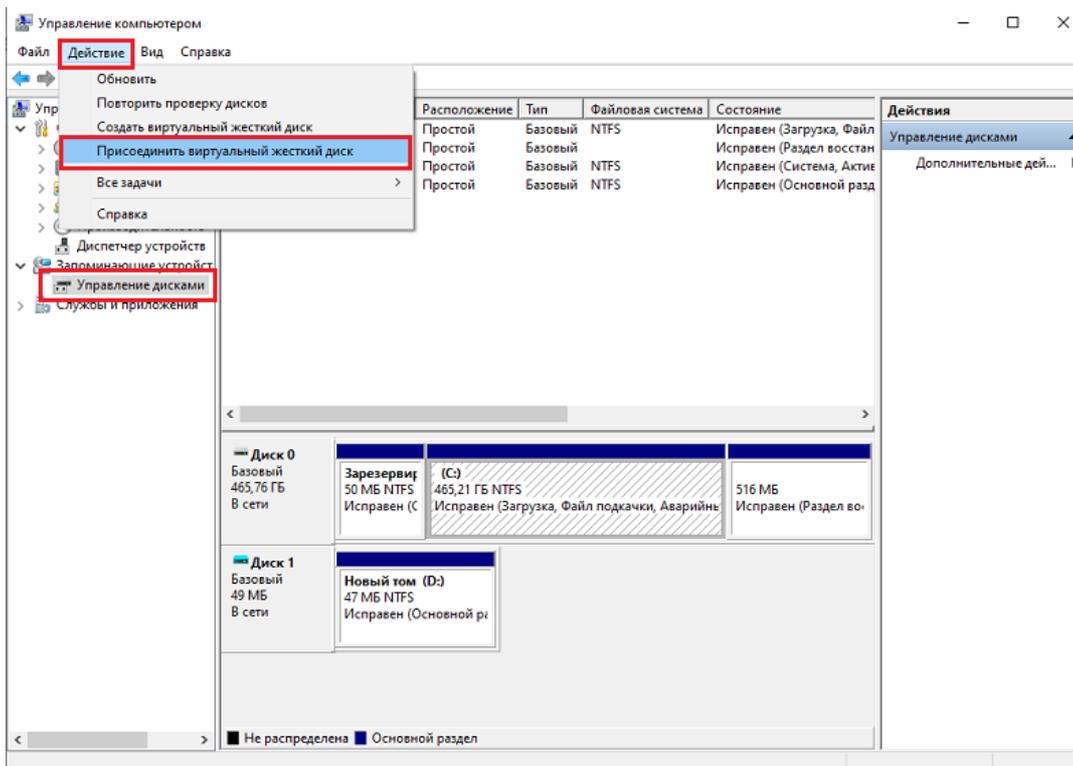
При установке контейнера в реестр или директорию нужно удостовериться, что предоставлены необходимые права на ветку реестра или на папку, в которую устанавливается контейнер.

При установке контейнера на виртуальный жесткий диск, необходимо подключить его следующим путем:

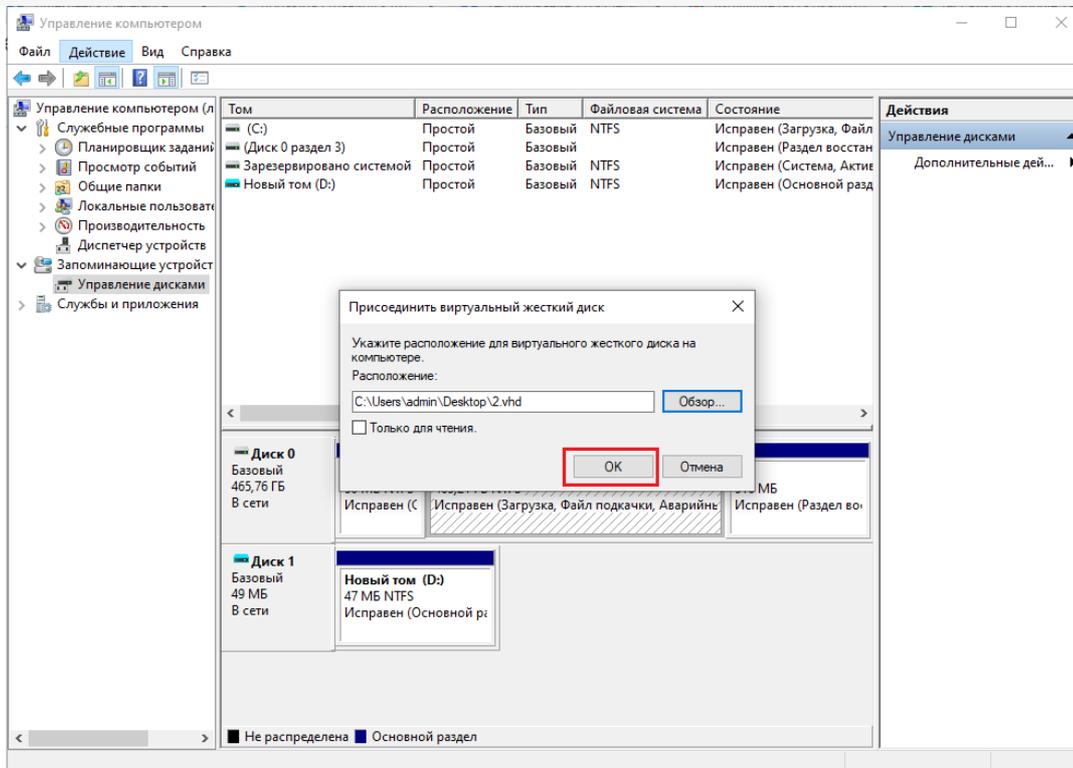
- ПУСК → «Средства администрирования» → «Управление компьютером».



- Открыть вкладку «Управление дисками», нажать «Действие» → «Присоединить виртуальный жесткий диск».



- Выбрать загруженный ранее контейнер, нажать «ОК».



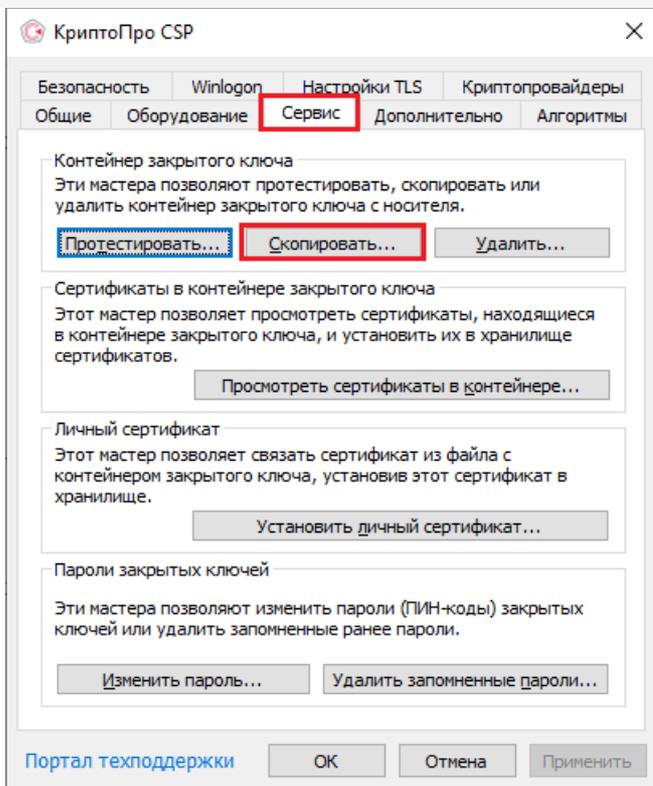
- После этого новый диск будет добавлен.

Том	Расположение	Тип	Файловая система	Состояние	Емкость	Свободно	Свободно %
(C:)	Простой	Базовый	NTFS	Исправен (Загрузка, Аварийный дамп памяти, Основной раздел)	49,40 ГБ	18,63 ГБ	38 %
(Диск 0 раздел 1)	Простой	Базовый	Исправен (Раздел восстановления)	499 МБ	499 МБ	100 %	
(Диск 0 раздел 2)	Простой	Базовый	Исправен (Шифрованный (EFI) системный раздел)	99 МБ	99 МБ	100 %	
Новый том (D:)	Простой	Базовый	NTFS	Исправен (Основной раздел)	47 МБ	32 МБ	68 %

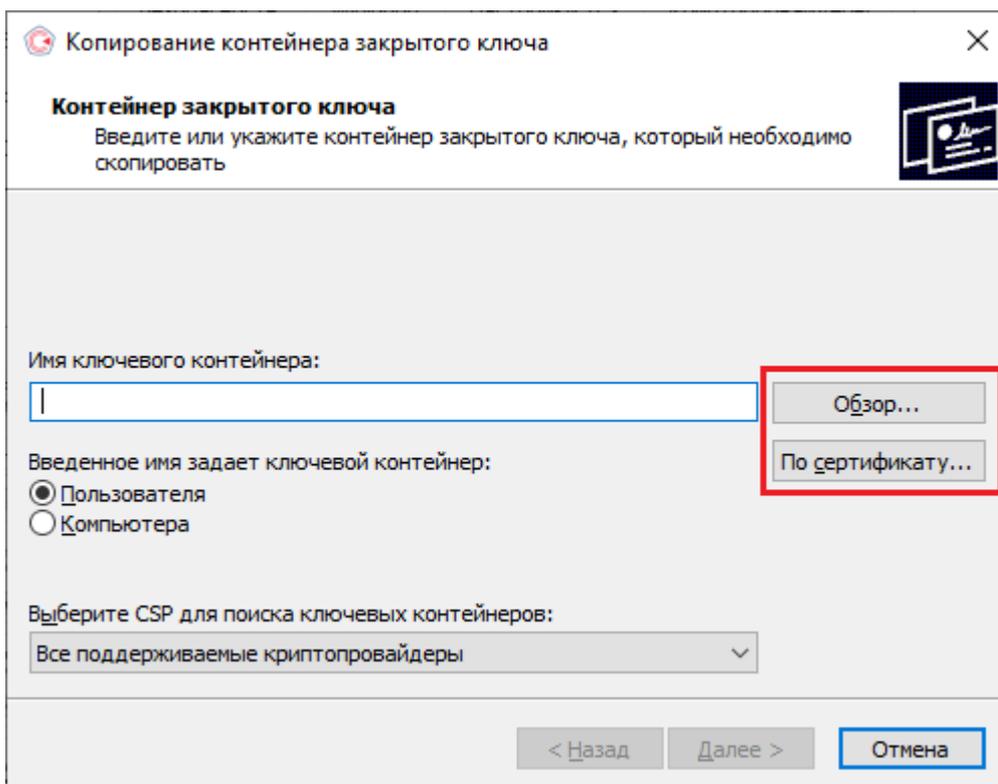
Диск 0	Базовый	49,98 ГБ	В сети	499 МБ	Исправен (Раздел восстановления)	99 МБ	Исправен (Шифрованный (EFI) системный)	(C:)	49,40 ГБ NTFS	Исправен (Загрузка, Аварийный дамп памяти, Основной раздел)
Диск 1	Базовый	49 МБ	В сети	Новый том (D:)	47 МБ NTFS	Исправен (Основной раздел)				
Диск 2	Базовый	49 МБ	Вне сети	47 МБ						

Если хранить контейнер на виртуальном жестком диске, то после перезагрузки ПК этот жесткий диск потребуется подключать заново. Поэтому рекомендуем скопировать контейнер на любой из доступных носителей с помощью программы КриптоПро CSP. Для этого:

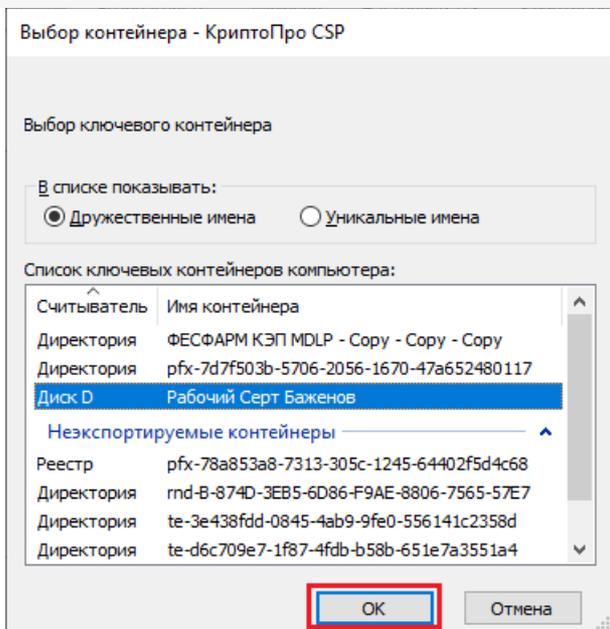
Запустите КриптоПро CSP от имени администратора, откройте вкладку «Сервис» и нажмите на кнопку «Скопировать».



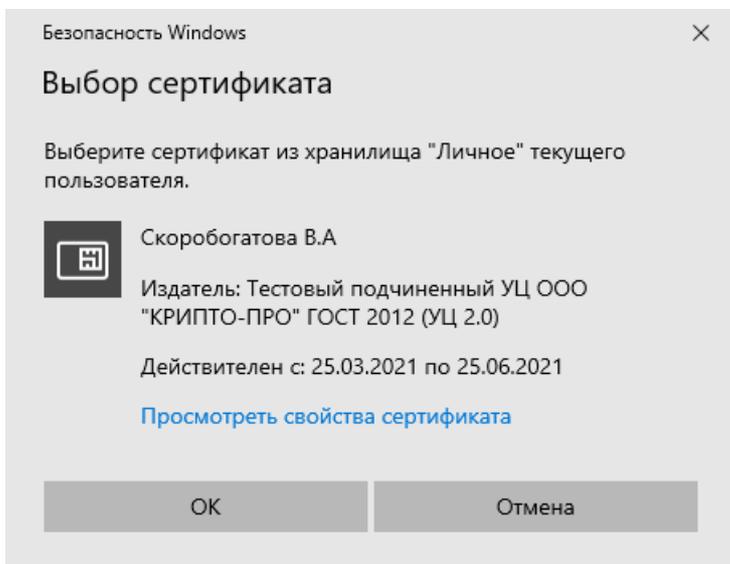
В открывшемся окне необходимо выбрать, где будет располагаться ключевой контейнер (пользователь или компьютер) с помощью кнопки «Обзор» или «По сертификату».



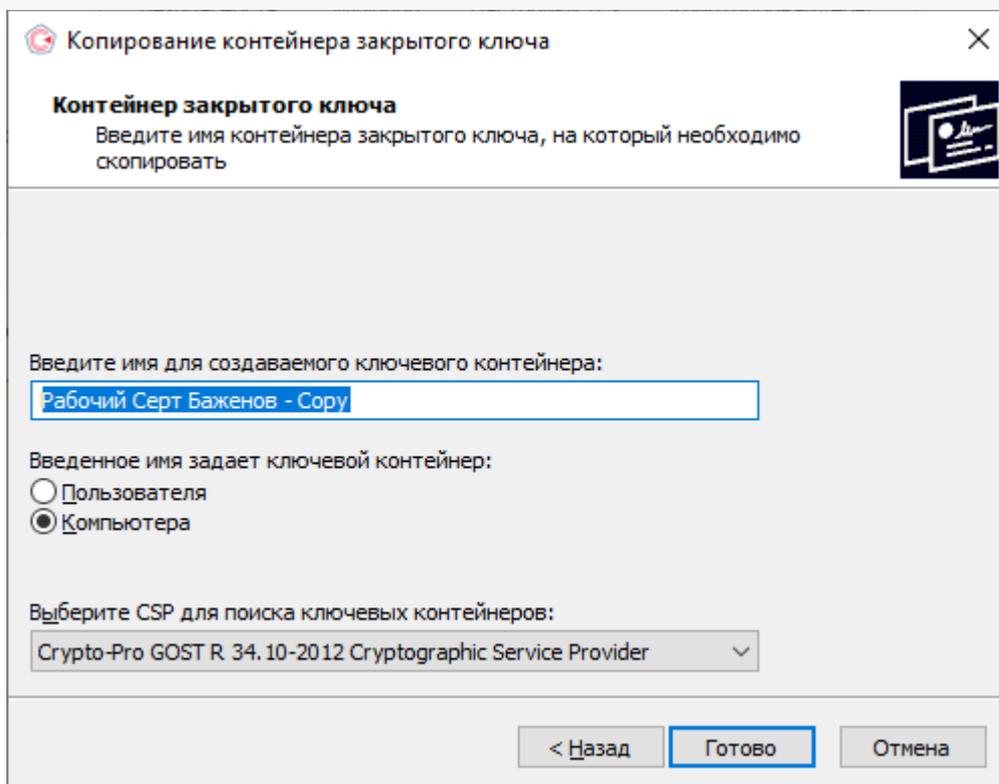
При нажатии на кнопку «Обзор», потребуется выбрать контейнер из списка:



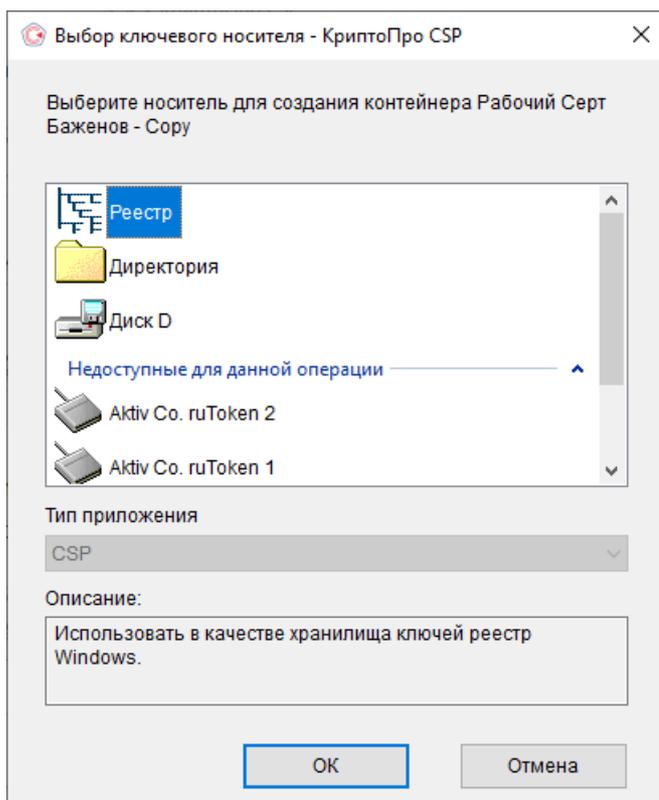
При нажатии на кнопку «По сертификату» потребуется выбрать нужный сертификат.



После того как выбран нужный контейнер, выберите имя и доступ сертификата. Нажмите кнопку «Готово».



После этого откроется окно выбора ключевого носителя, на который будет копироваться контейнер. укажите нужный и нажмите «ОК».



После выбора ключевого носителя создайте пароль на контейнер. Нажмите «ОК».

Аутентификация - КриптоПро CSP

Сурто-Pro GOST R 34.10-2012 Cryptographic Service Provider запрашивает новый пароль на контейнер

Считыватель: REGISTRY
 Носитель: Уникальное имя отсутствует
 Контейнер: TestSertwithoutFATPCRegedit - Copy - Copy - Copy - Copy - t

Новый пароль:

Повторите ввод:

⚠ Выбран язык ввода, отличный от английского

OK Отмена

При успешном завершении операции появится следующее уведомление.

КриптоПро CSP

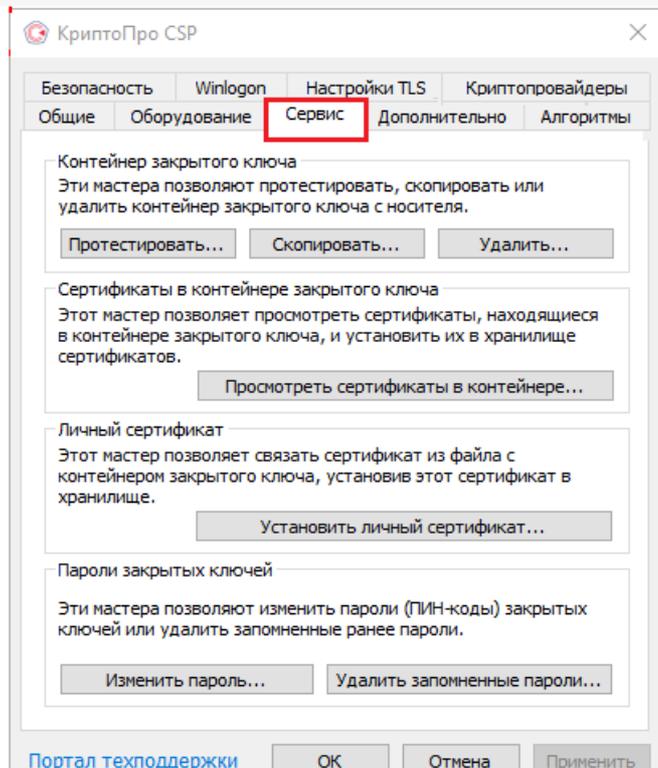
Контейнер 'Рабочий Серт Баженов' успешно скопирован в 'Рабочий Серт Баженов - Copy'.

OK

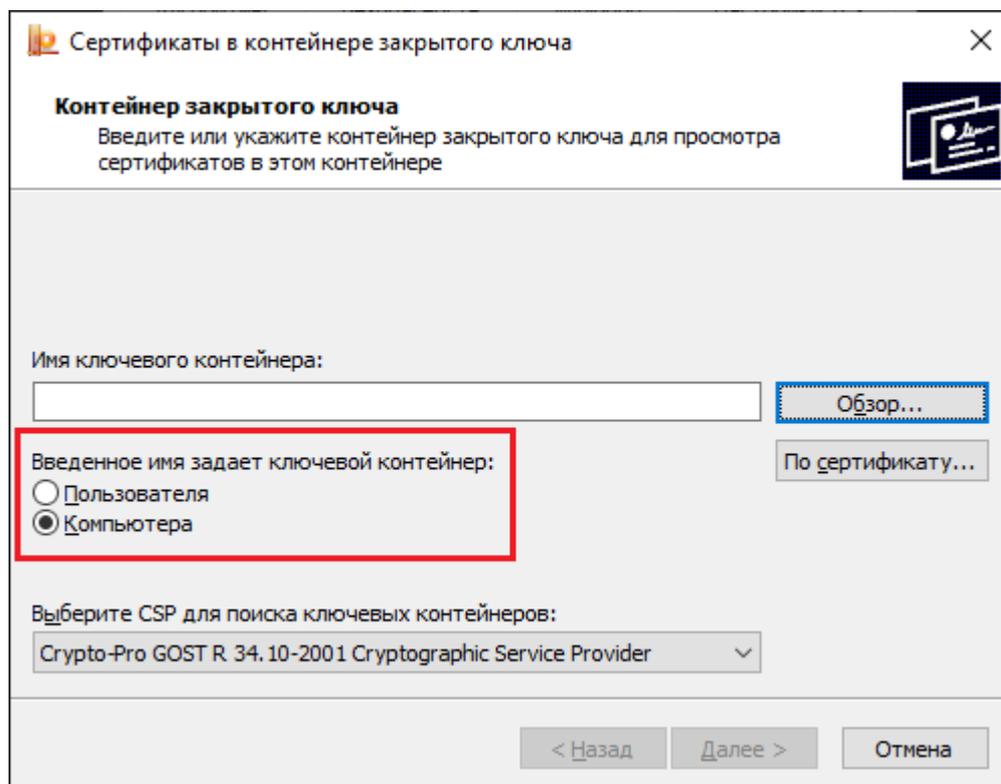
Установка сертификата в Личные

Для корректной работы «Кировки» с ГИС МТ, необходимо установить сертификат КЭП в хранилище компьютера (Local Machine).

- Для того чтобы просмотреть сертификат, хранящийся в контейнере закрытого ключа, запустите КриптоПро CSP от имени администратора. Откроется «Панель управления» СКЗИ КриптоПро CSP, где необходимо перейти на вкладку «Сервис».



- Нажмите кнопку «Просмотреть сертификаты в контейнере». Откроется окно «Сертификаты в контейнере закрытого ключа». На этой форме в пункте «Введенное имя задает ключевой контейнер» необходимо установить флаг в пункте «Компьютера» (возможно только в случае если вы открыли КриптоПро CSP от имени администратора).



- Далее необходимо заполнить поле «Имя ключевого контейнера». Оно может быть введено вручную или найдено в списках контейнеров (кнопка «Обзор») или сертификатов (кнопка «По сертификату»). Если сертификат в выбранном контейнере имеется, откроется окно «Сертификат для просмотра».

Выбор контейнера - КриптоПро CSP

Выбор ключевого контейнера

В списке показывать:

Дружественные имена Уникальные имена

Список ключевых контейнеров компьютера:

Считыватель	Имя контейнера
Директория	prfx-7d7f503b-5706-2056-1670-47a652480117
Директория	rnd-B-874D-3EB5-6D86-F9AE-8806-7565-57E7
Директория	te-3e438fdd-0845-4ab9-9fe0-556141c2358d
Директория	te-d6c709e7-1f87-4fdb-b58b-651e7a3551a4
Директория	ФЕСФАРМ КЭП MDLP - Copy - Copy - Copy
Диск D	Рабочий Серт Баженов
Реестр	prfx-78a853a8-7313-305c-1245-64402f5d4c68

OK Отмена

Сертификаты в контейнере закрытого ключа

Сертификат для просмотра
Просмотрите и выберите сертификат

Сертификат: Баженов Сергей Витальевич

Субъект: [Имя субъекта]

Поставщик: E=info@cryptopro.ru, ОГРН=1037700085444, ИНН=007717107991, С=I

Действителен с: [Дата]

Действителен до: [Дата]

Серийный номер: [Номер]

Установить Свойства... Обзор...

< Назад Готово Отмена

- В окне «Сертификаты в контейнере закрытого ключа» нажмите кнопку «Установить» (для связи сертификата и закрытого ключа). После этого установите сертификат в личное хранилище («Свойства» → «Установить сертификат»).

Сертификат

Общие Состав Путь сертификации

Сведения о сертификате

Этот сертификат предназначен для:

- Защищает сообщения электронной почты
- Подтверждает удаленному компьютеру идентификацию вашего компьютера
- Класс средства ЭП КС2
- Класс средства ЭП КС1
- Пользователь Центра Регистрации, HTTP, TLS клиент

Кому выдан: Баженов Сергей Витальевич

Кем выдан: Тестовый подчиненный УЦ ООО "КРИПТО-ПРО" ГОСТ 2012 (УЦ 2.0)

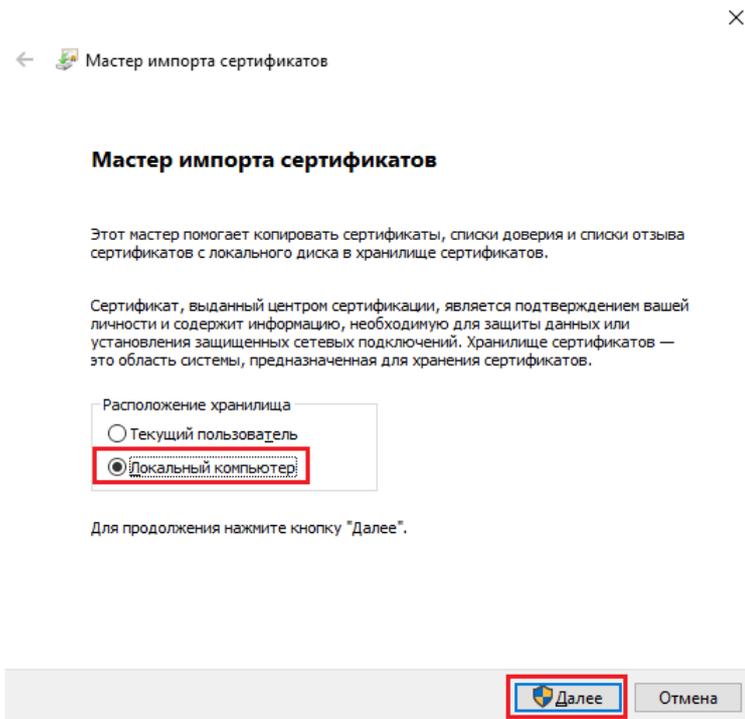
Действителен с 25.03.2021 по 25.06.2021

Есть закрытый ключ для этого сертификата.

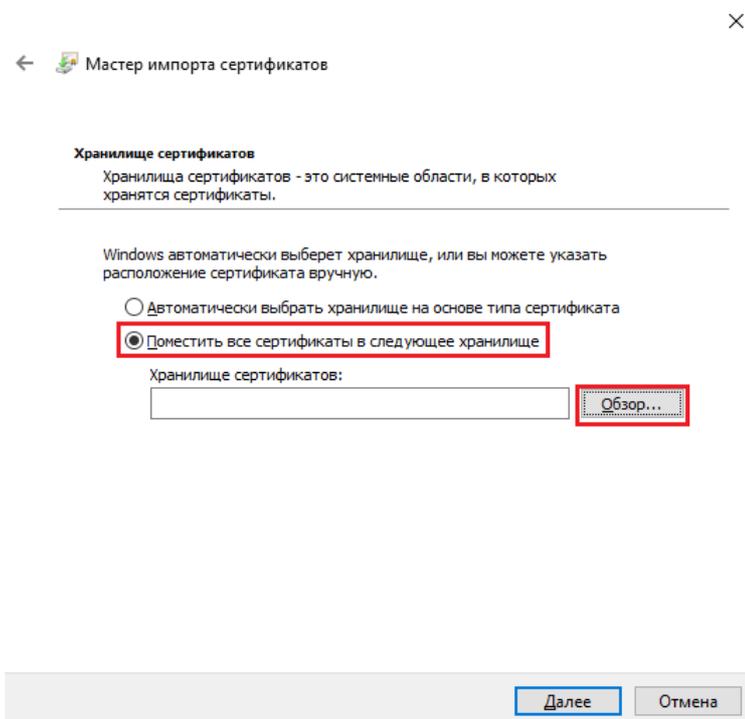
Установить сертификат... Заявление поставщика

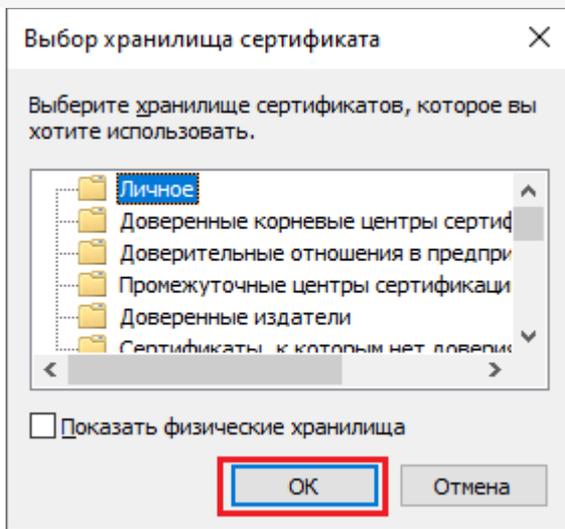
OK

- В качестве расположения хранилища выберите «Локальный компьютер» и нажмите кнопку «Далее».



- В следующем окне выберите пункт «Поместить все сертификаты в следующее хранилище», нажмите кнопку «Обзор» и из списка хранилищ выберите «Личное».



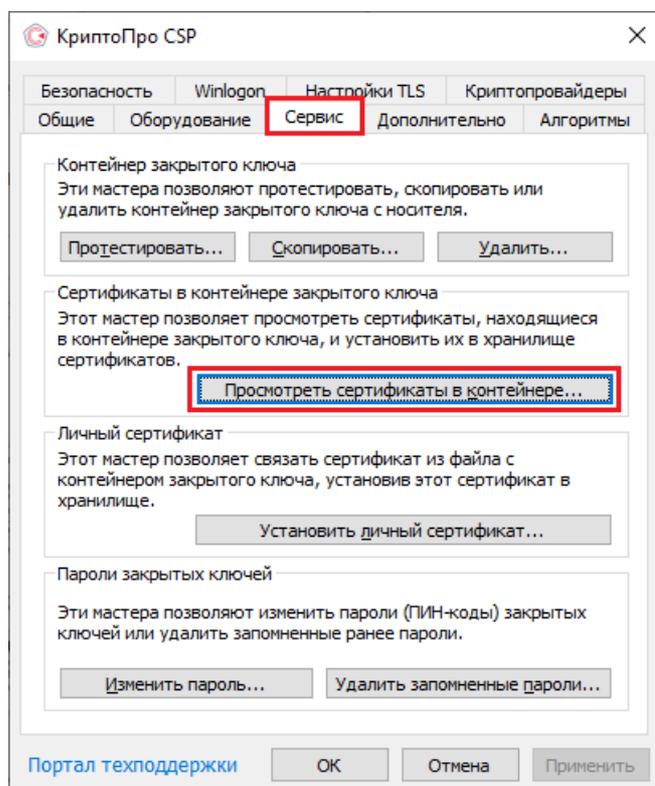


- Нажмите «ОК» → «Далее» → «Готово».

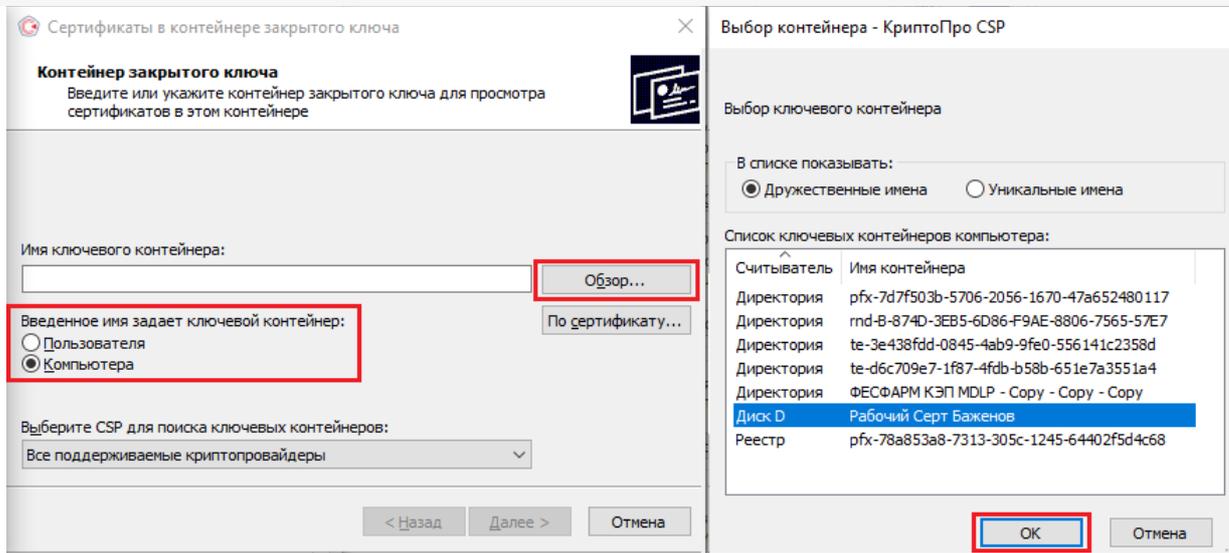
Проверка и сопоставление текущего личного сертификата и сертификата в контейнере

Данное действие можно выполнить двумя способами.

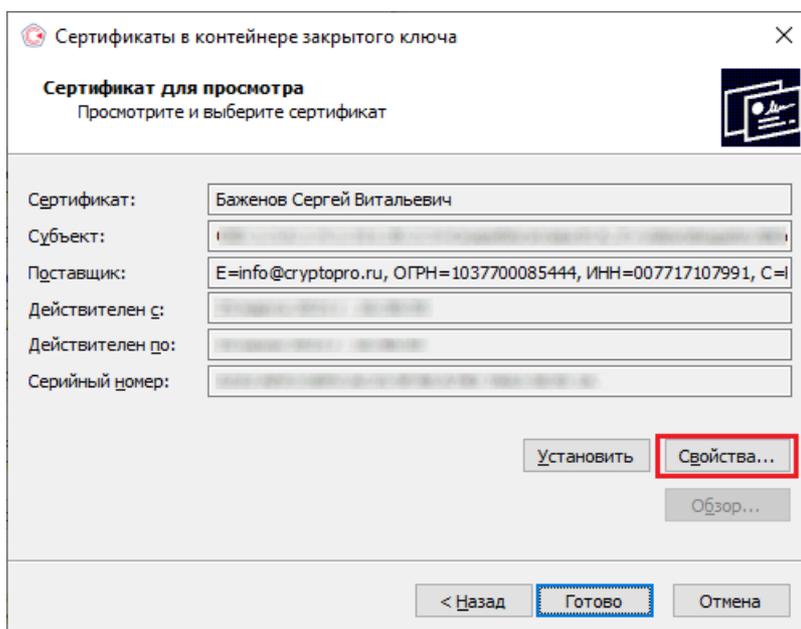
Способ 1. Сравнить отпечатки сертификата в контейнере и сертификата, установленного на ПК. Для проверки сертификата в контейнере нужно запустить КриптоПРО CSP от имени администратора, перейти во вкладку «Сервис» и нажать на кнопку «Просмотреть сертификаты в контейнере».



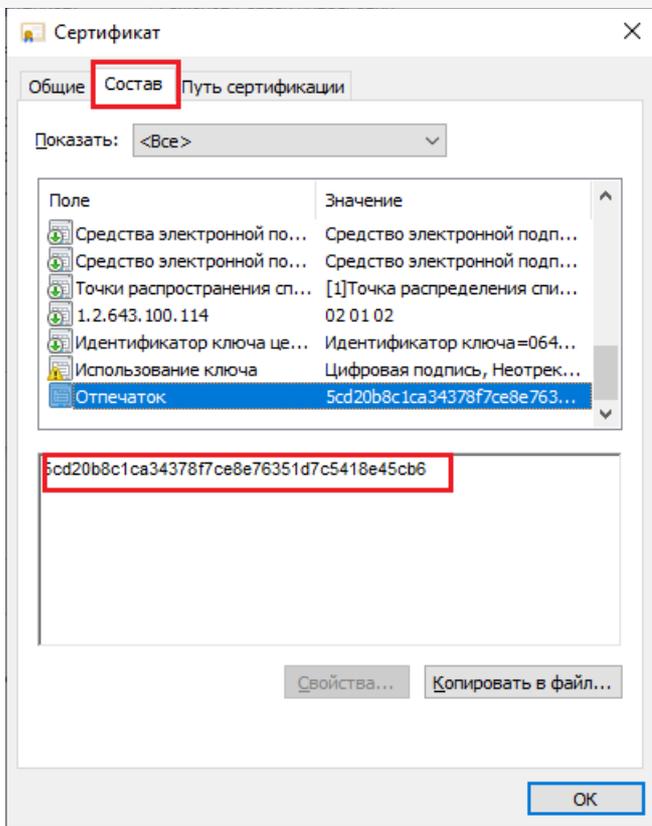
В открывшемся окне нужно выбрать «Введенное имя задает ключевой контейнер» — «Компьютер», далее нажать на кнопку «Обзор», выбрать контейнер из списка и нажать «ОК».



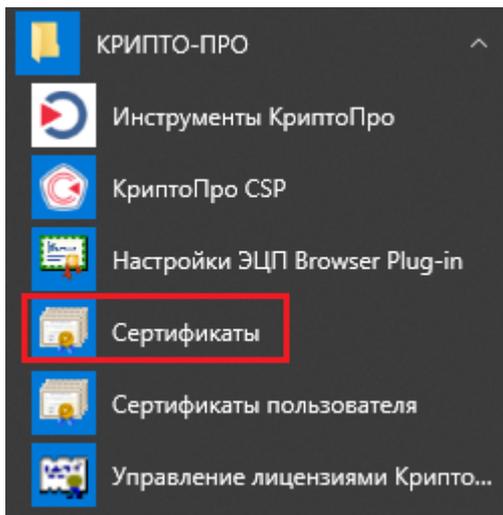
Откроется окно с информацией о сертификате, в котором необходимо нажать на кнопку «Свойства».



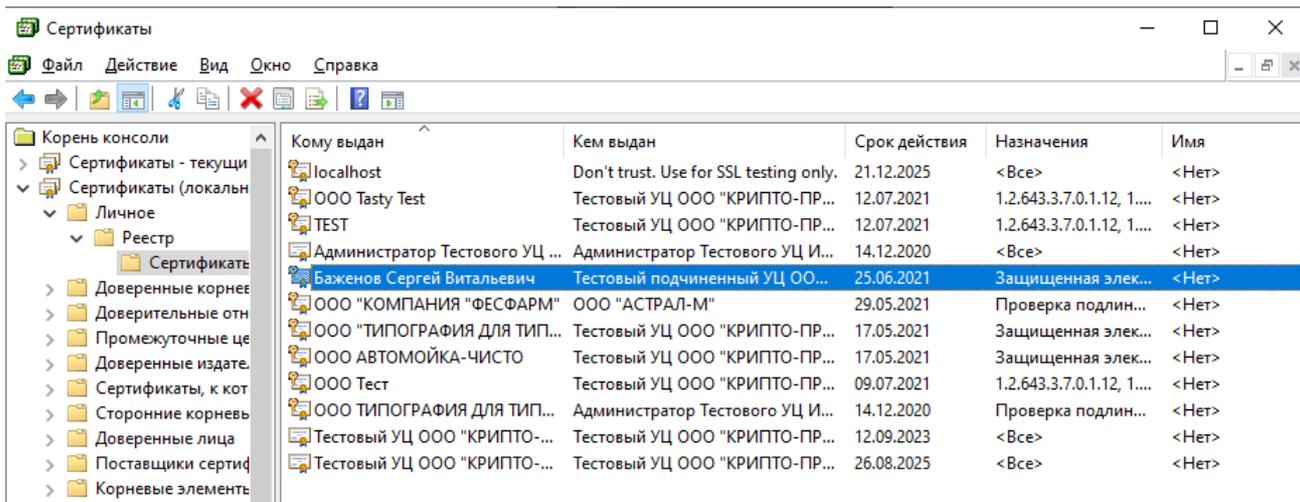
В открывшемся окне перейдите на вкладку «Состав». Вам нужна строка-отпечаток, которую вы можете сравнить наглядно со строкой-отпечатком, установленным на ПК.



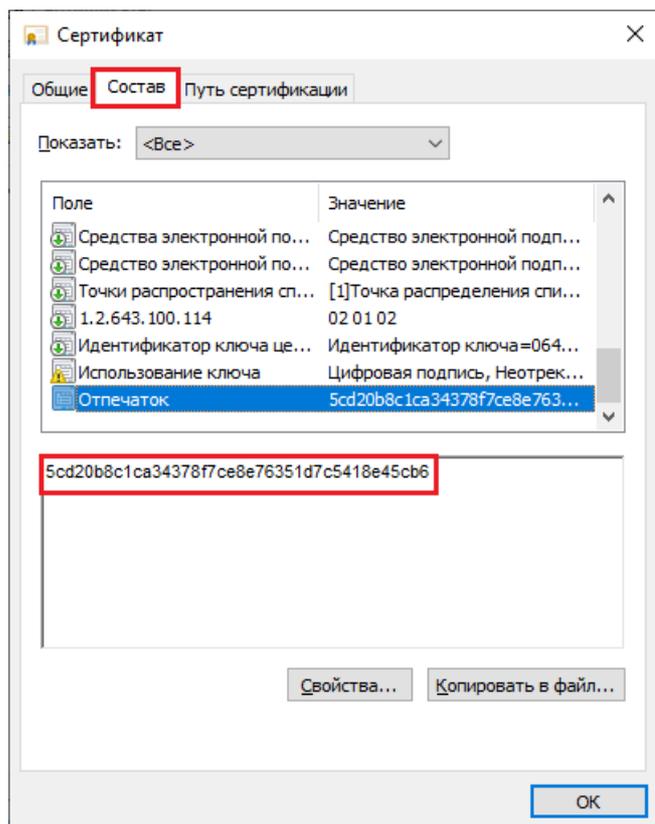
Для того чтобы сверить данный отпечаток с сертификатом, установленным на ПК, необходимо открыть ПУСК → КРИПТО-ПРО → Сертификаты.



В открывшемся окне сертификатов выберите «Сертификаты (локальный компьютер)» → «Личное» → «Реестр» → «Сертификаты», и выберите нужный вам сертификат.

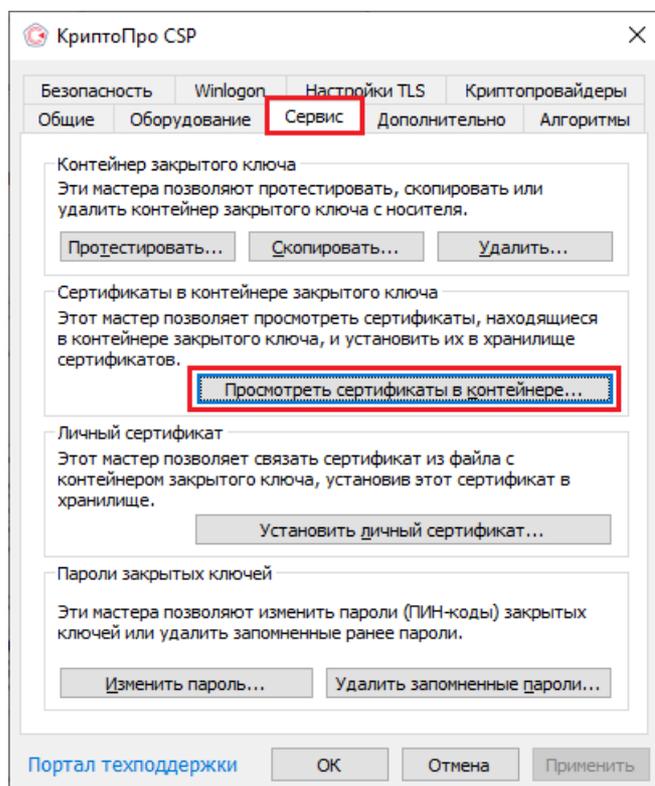


В окне сертификата перейдите на вкладку «Состав», где будет указана строка-отпечаток.

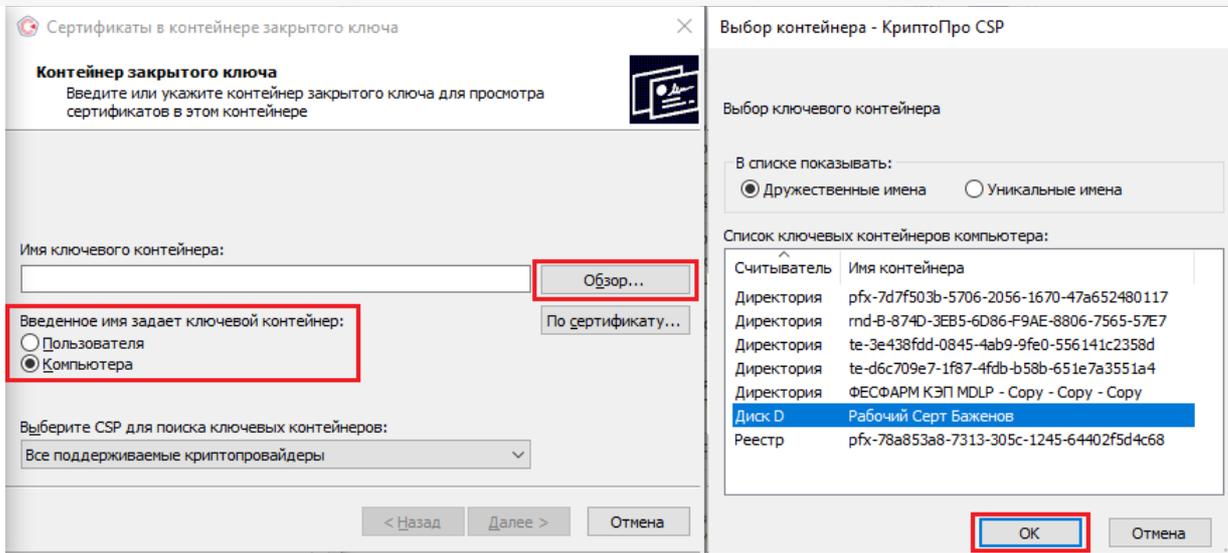


После этого вы можете сравнить два отпечатка.

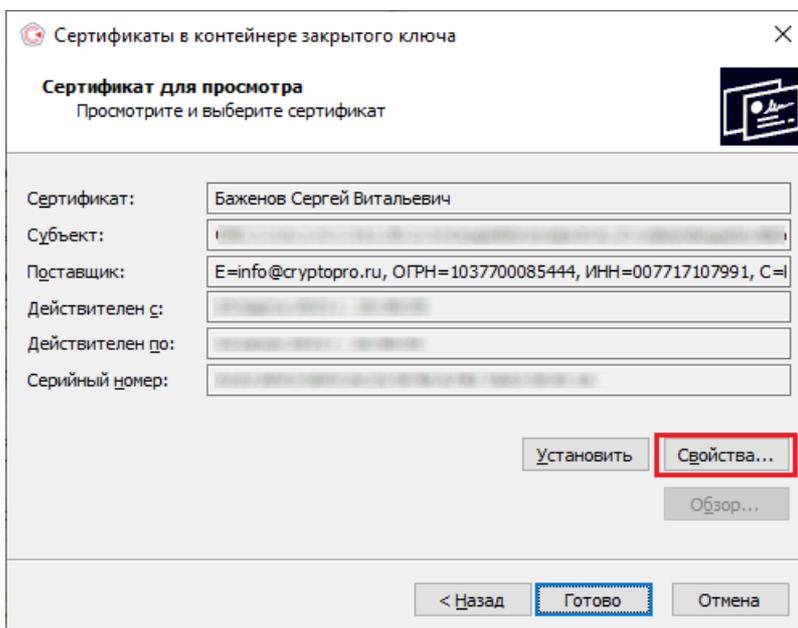
Способ 2. Переустановить сертификат на ПК из контейнера. Для этого запустите КриптоПРО CSP от имени администратора, перейдите во вкладку «Сервис» и нажмите на кнопку «Просмотреть сертификаты в контейнере».



В открывшемся окне нужно выбрать «Введенное имя задает ключевой контейнер» — «Компьютер», далее нажать на кнопку «Обзор», выбрать контейнер из списка и нажать «ОК».



Откроется окно с информацией о сертификате, в котором необходимо нажать на «Свойства» → «Установить сертификат».



В качестве хранилища сертификата необходимо выбрать «Локальный компьютер».

←  Мастер импорта сертификатов

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".

 Далее

Отмена

В следующем окне необходимо выбрать «Поместить все сертификаты в следующее хранилище» → «Обзор» → «Личное».

←  Мастер импорта сертификатов

Хранилище сертификатов

Хранилища сертификатов - это системные области, в которых хранятся сертификаты.

Windows автоматически выберет хранилище, или вы можете указать расположение сертификата вручную.

Автоматически выбрать хранилище на основе типа сертификата

Поместить все сертификаты в следующее хранилище

Хранилище сертификатов:

Обзор...

Далее

Отмена

Нажмите «Далее» → «Готово». После этого импорт сертификата будет успешно выполнен.

Не нашли что искали?



Задать вопрос в техническую поддержку