



Удостоверяющий
центр

Федеральная
кадастровая
палата

ИНСТРУКЦИЯ

по установке личного сертификата, выпущенного Удостоверяющим центром ФГБУ «ФКП Росреестра»





Оглавление

Термины и определения.....	3
1. Подготовка рабочего места	4
2. Установка личного сертификата из файла	5
3. Установка личного Сертификата из контейнера закрытого ключа на отчуждаемом носителе/реестра ОС	14



Данная инструкция предназначена для руководства при установке личного сертификата, полученного в УЦ ФГБУ «ФКП Росреестра».

Термины и определения

- **Владелец Сертификата** – физическое, юридическое лицо или индивидуальный предприниматель.
- **Криптопровайдер (КриптоПро CSP)** – средство криптографической защиты информации (СКЗИ), программный продукт, для авторизации и обеспечения юридической значимости электронных документов при обмене между пользователями, посредством использования процедур формирования и проверки электронной подписи (ЭП), а также обеспечения конфиденциальности и контроля целостности информации посредством ее шифрования и имитозащиты.
- **Корневой сертификат** – сертификат УЦ, обеспечивающий безопасность в едином пространстве доверия при электронном взаимодействии.
- **Личный кабинет (ЛК)** – сервис на Сайте УЦ, предназначенный для взаимодействия участников, определяемых ролями, для хранения и обработки сведений с целью получения/предоставления услуг УЦ.
- **Список отозванных сертификатов (CRL – Certificate Revocation List)** – это электронный документ, который содержит перечень идентификаторов сертификатов, являющихся отозванными из обращения в УЦ. УЦ осуществляет отзыв сертификатов и публикацию Списков отозванных сертификатов в соответствии с Регламентом, размещенным на официальном сайте УЦ в сети интернет по адресу <https://uc.kadastr.ru>, в разделе «О Центре».
- **Сертификат** – квалифицированный сертификат ключа проверки электронной подписи, соответствующий требованиям, установленным Федеральным законом от 06.04.2011 № 63-ФЗ «Об электронной подписи» и иными принимаемыми в соответствии с ним нормативными правовыми актами, и созданный аккредитованным удостоверяющим центром (КСКП ЭП).
- **УЦ** – удостоверяющий центр ФГБУ «ФКП Росреестра».
- **ФГБУ «ФКП Росреестра»** – федеральное государственное бюджетное учреждение «Федеральная кадастровая палата Федеральной службы государственной регистрации, кадастра и картографии».
- **ЭП** – электронная подпись.

1. Подготовка рабочего места

Для начала работы с Сертификатом, полученным в УЦ ФГБУ «ФКП Росреестра», необходимо:

- установить Криптопровайдер КриптоПро CSP;
- установить Корневые сертификаты;
- установить Сертификат (личный Сертификат);
- установить КриптоПро ЭЦП Browser plug-in

(работоспособность плагина можно проверить, перейдя по ссылке <https://www.cryptopro.ru/sites/default/files/products/cades/demopage/simple.html>, при этом должно отобразиться сообщение о том, что плагин загружен. Сообщение также должно содержать информацию о версии плагина и о составе используемого Сертификата);

- установить программное обеспечение, предназначенное для создания ЭП с использованием полученного в УЦ Сертификата.

Внимание!

С 01.01.2019 применение схемы электронной подписи, соответствующей ГОСТ Р 34.10-2001 для изготовления Сертификатов исключено ввиду действующих ограничений Минкомсвязи России, опубликованных в соответствующем уведомлении на официальном сайте Федерального ситуационного центра электронного правительства по адресу: <https://sc-new.minsvyaz.ru/> в блоке «Справочные материалы» раздела «Документы».

Сертификаты, изготовленные до 31.12.2018 по схеме электронной подписи, соответствующей ГОСТ Р 34.10-2001, являются работоспособными в течение срока действия, указанного в таких Сертификатах, но не превышающего 31.12.2019.


В случае, если Сертификат был получен в УЦ ФГБУ «ФКП Росреестра» в результате услуги **«Сертификат электронной подписи в электронном виде»**, необходимо выполнить установку Сертификата согласно рекомендациям **раздела 2** настоящей Инструкции.

В случае, если Сертификат был получен в УЦ ФГБУ «ФКП Росреестра» в результате услуги **«Сертификат электронной подписи на носителе ключевой информации»**, установка Сертификата

осуществляется из контейнера закрытого ключа. Для этого необходимо выполнить установку Сертификата согласно рекомендациям **раздела 3** настоящей Инструкции.

В случае, если Сертификат был сохранен на отчуждаемый носитель, перед началом установки Сертификата необходимо подключить отчуждаемый носитель, содержащий контейнер закрытого ключа и Сертификат, к рабочему месту, на котором предполагается применение Сертификата.

2. Установка личного сертификата из файла

2.1. В результате полученной услуги Сертификат становится доступен в Личном кабинете Владельца Сертификата. Находясь в Личном кабинете Владельца Сертификата, необходимо «перейти» в раздел **«Скачайте сертификат»** или **«Мои сертификаты»**, найти запрос, в соответствии с которым был выпущен Сертификат, затем в блоке **«Действия»** активировать ссылку для автоматического скачивания Сертификата  (см. Рисунок 2.1.1):

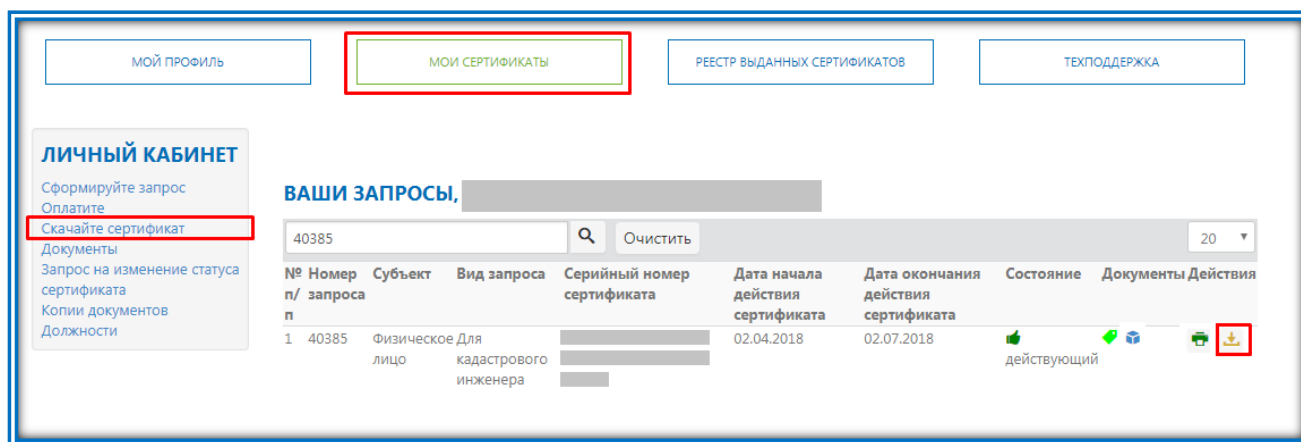


Рисунок 2.1.1

2.2. В результате «перехода» по ссылке откроется модальное окно **«Ознакомление с сертификатом»**, содержащее сведения о составе получаемого Сертификата (данное действие необходимо выполнить только при первоначальном обращении к Сертификату) (см. Рисунок 2.2.1):

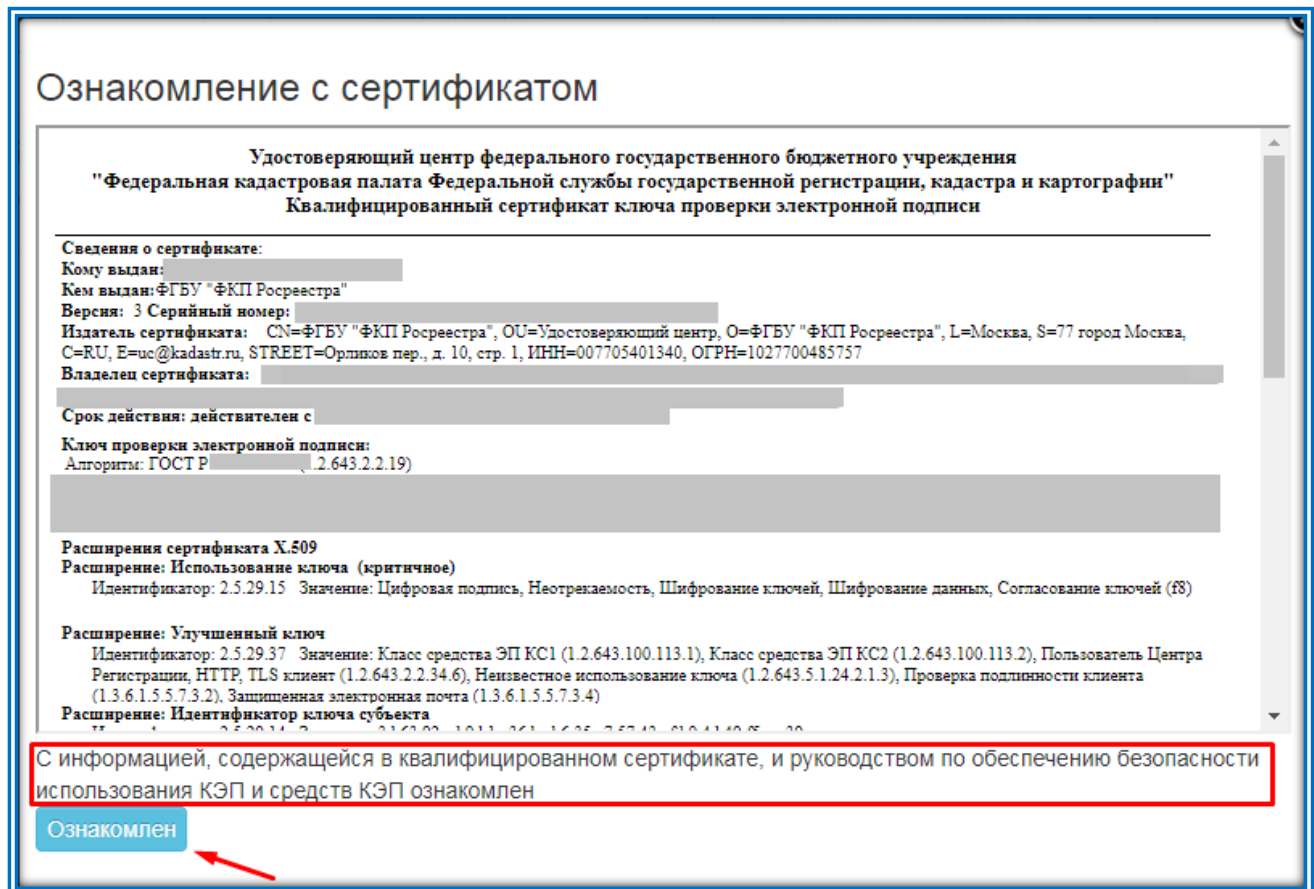





Рисунок 2.2.1

2.3. В соответствии с пунктом 4 статьи 18 Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи», на данном этапе необходимо внимательно ознакомиться со сведениями, включенными в состав изготовленного Сертификата, нажать кнопку **«Ознакомлен»**.

В результате проделанных действий, Владелец Сертификата будет зафиксирован факт ознакомления с составом Сертификата путем подписания документа, содержащего указанные сведения, простой электронной подписью Владельца Сертификата (в соответствии с Соглашением об использовании простой электронной подписи). Далее следует повторно нажать ссылку для автоматического скачивания Сертификата . В результате системой будет инициирована «загрузка» Сертификата.

Примечание: Сертификат доступен для «загрузки» исключительно в случае подтверждения ознакомления и согласия с составом и сведениями, содержащимися в выпущенном Сертификате. В случае несогласия, спорные ситуации решаются в порядке, определенном Договором.

Дополнительно в блоке **«Действия»**, при нажатии на кнопку , предусмотрена возможность вывода на печать документа, содержащего сведения о составе получаемого Сертификата, в формате *.pdf. Также документ, содержащий сведения о составе получаемого Сертификата, подписанный усиленной квалифицированной подписью работника УЦ, вместе с файлом подписи хранится в Личном кабинете Владельца Сертификата и доступен в блоке **«Документы»** при нажатии на кнопку .

2.4. Для установки Сертификата из файла необходимо последовательно выбрать в меню: **Пуск -> Панель управления** (или если на компьютере установлена ОС WindowsXP: **Пуск -> Настройка -> Панель управления**). Затем в появившемся окне выбрать **КриптоПро CSP** и «запустить», дважды кликнув левой кнопкой мыши.

2.5. В появившемся окне **«КриптоПро CSP»** необходимо перейти на вкладку **«Сервис»** и нажать кнопку **«Установить личный сертификат»** (см. Рисунок 2.5.1):

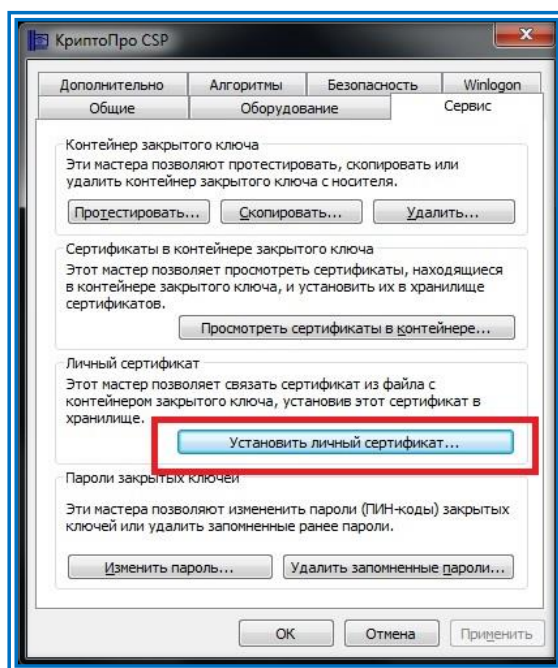


Рисунок 2.5.1

2.6. Далее в окне «**Мастера установки личного сертификата**» необходимо указать место расположения файла Сертификата. Для этого необходимо нажать кнопку «**Обзор**», указать местоположение файла Сертификата и нажать кнопку «**Открыть**» (см. Рисунок 2.6.1):

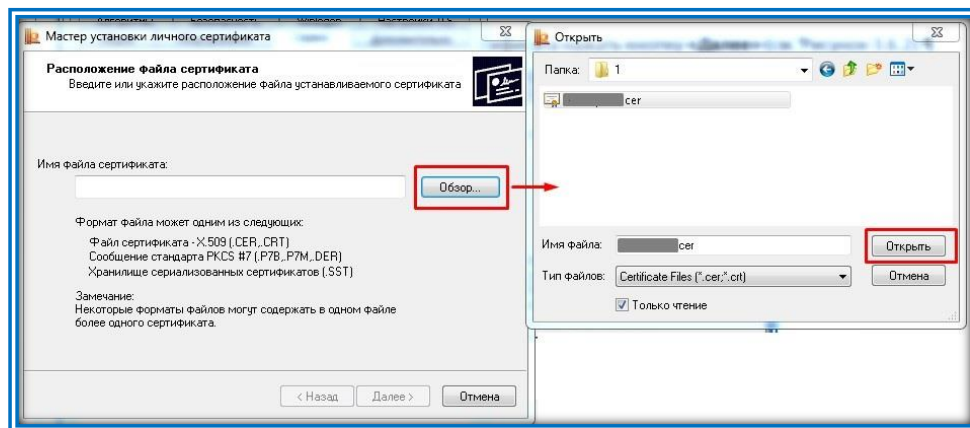


Рисунок 2.6.1

после того, как будет указан путь к файлу Сертификата, нажать кнопку «**Далее**» (см. Рисунок 2.6.2):

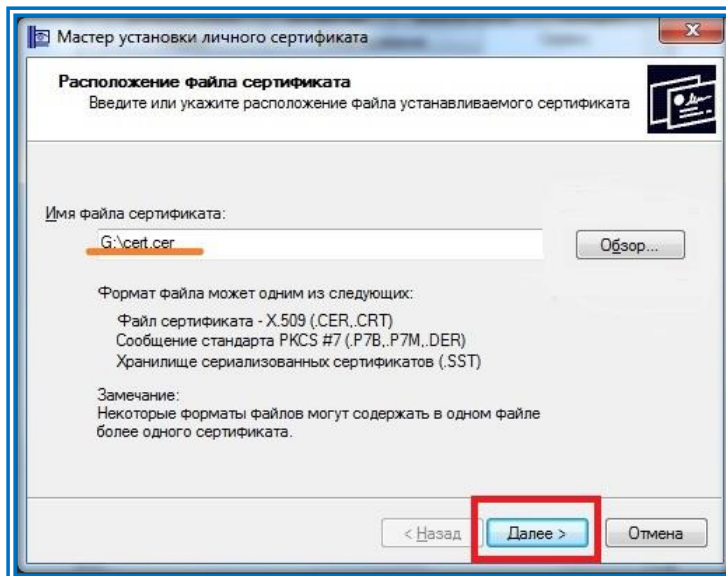


Рисунок 2.6.2

2.7. В окне мастера «**Сертификат для установки**» появится информация о выбранном Сертификате. Необходимо нажать кнопку «**Далее**» (см. Рисунок 2.7.1):



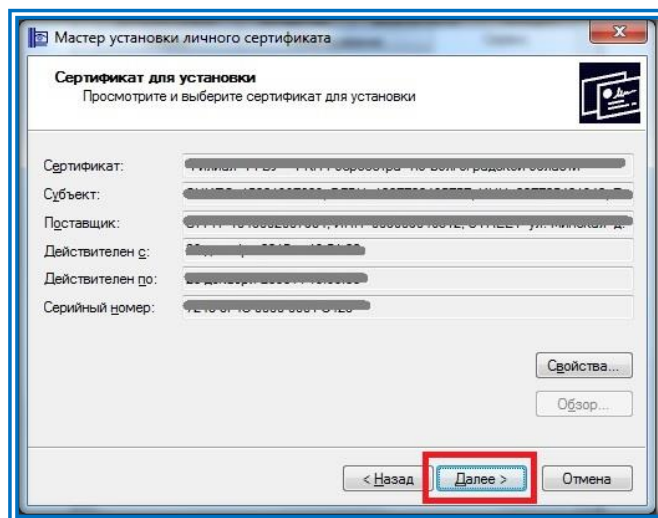


Рисунок 2.7.1

2.8. В появившемся окне для выбора ключевого контейнера в разделе **«Введенное имя задает ключевой контейнер»** «флаг» должен стоять в позиции **Пользователь**. Для выбора контейнера, в который будет установлен Сертификат, необходимо нажать кнопку **«Обзор»**. Далее при необходимости следует выбрать требуемый алгоритм схемы электронной подписи - (**Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider** или **Crypto-Pro GOST R 34.10-2012 Cryptographic Service Provider**) (см. Рисунок 2.8.1):

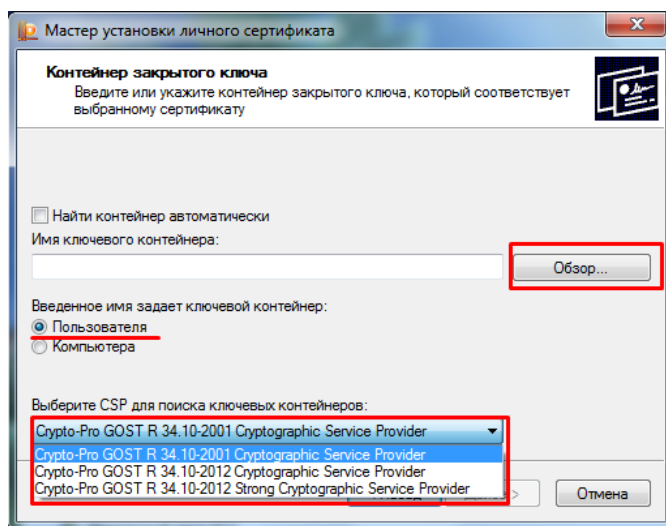


Рисунок 2.8.1

Затем необходимо выбрать контейнер и нажать кнопку «ОК» (см. Рисунок 2.8.2):

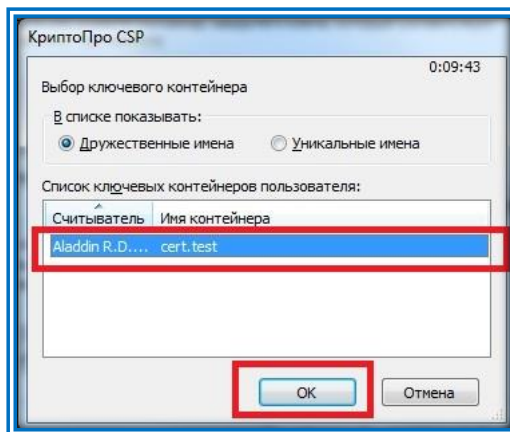


Рисунок 2.8.2

Примечание:

1) Приложение может также запросить ввести пароль доступа к ключевому контейнеру, в случае если пароль был задан в момент формирования запроса на Сертификат. В этом случае, после ввода пароля, необходимо нажать кнопку «ОК».

2) Если в поле «Найти контейнер автоматически» установить «флаг», система автоматически выберет необходимый контейнер.

3) В случае отсутствия подключенного к рабочему месту отчуждаемого носителя, или если система не обнаружила подходящий носитель (считыватель), а так же в случае неверно указанного Сертификата на экране появится окно уведомления, содержащее **сообщение о несоответствии закрытого ключа выбранному Сертификату**.

2.9. После того, как в окне «Мастер установки личного сертификата» будет указан контейнер, а также выбран требуемый алгоритм схемы электронной подписи - (**Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider** или **Crypto-Pro GOST R 34.10-2012 Cryptographic Service Provider**), необходимо нажать кнопку «Далее» (см. Рисунок 2.9.1):

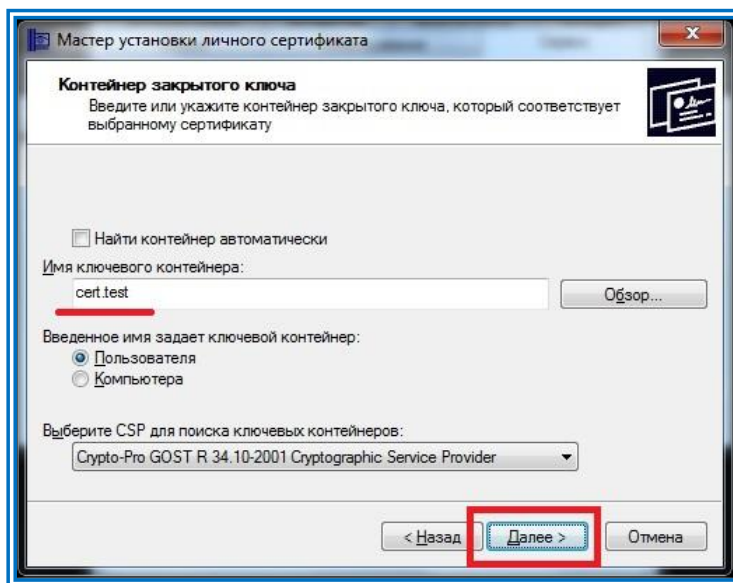


Рисунок 2.9.1

2.10. На следующем шаге «Мастер установки личного сертификата» откроет окно «Хранилище сертификатов» (Окно выбора хранилища сертификатов). Необходимо установить «флаг» в пункте «Установить сертификат в контейнер». Для выбора хранилища «Личные» необходимо нажать кнопку «Обзор» в текущем окне мастера (см. Рисунок 2.10.1):

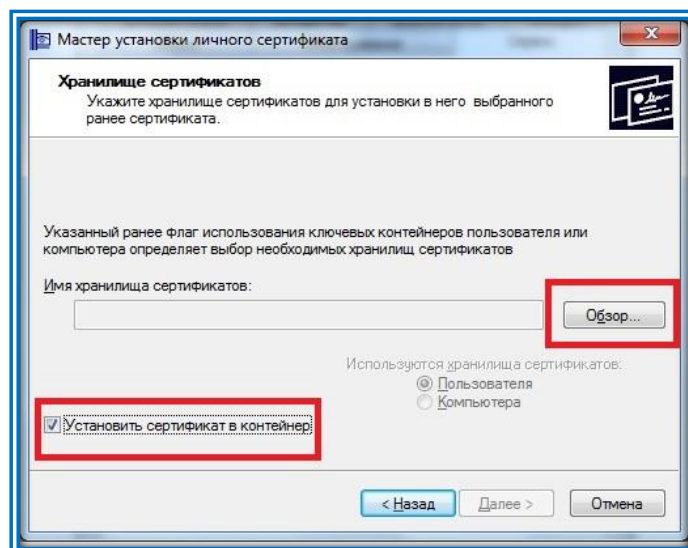


Рисунок 2.10.1

В открывшемся окне необходимо выбрать хранилище сертификатов **«Личное»** и нажать кнопку **«ОК»** (см. Рисунок 2.10.2):

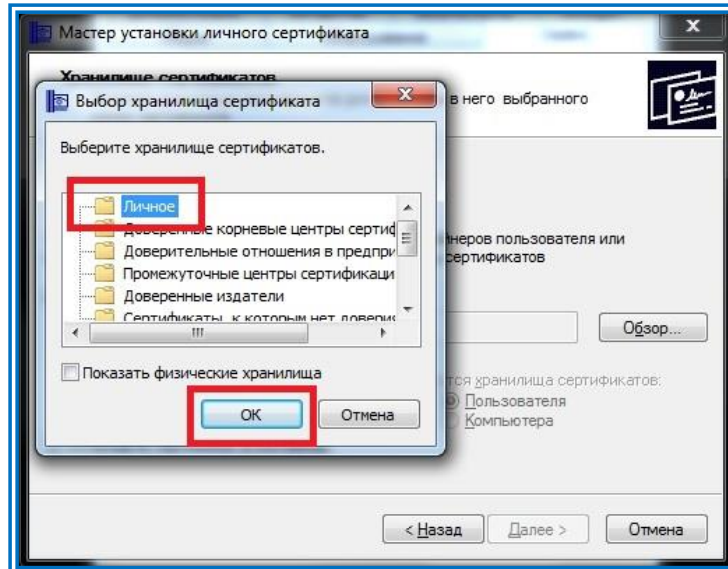


Рисунок 2.10.2

2.11. После выбора хранилища сертификатов необходимо нажать кнопку **«Далее»** (см. Рисунок 2.11.1):

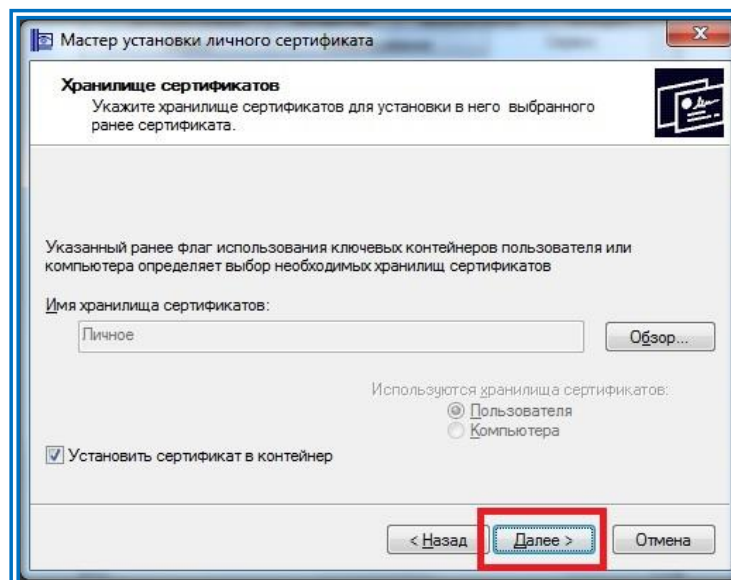


Рисунок 2.11.1

2.12. В результате «**Мастер установки личного сертификата**» перейдет к завершающей стадии установки личного Сертификата. В окне мастера отобразится итоговая информация. Для завершения работы мастера необходимо нажать кнопку «**Готово**» (см. Рисунок 2.12.1):

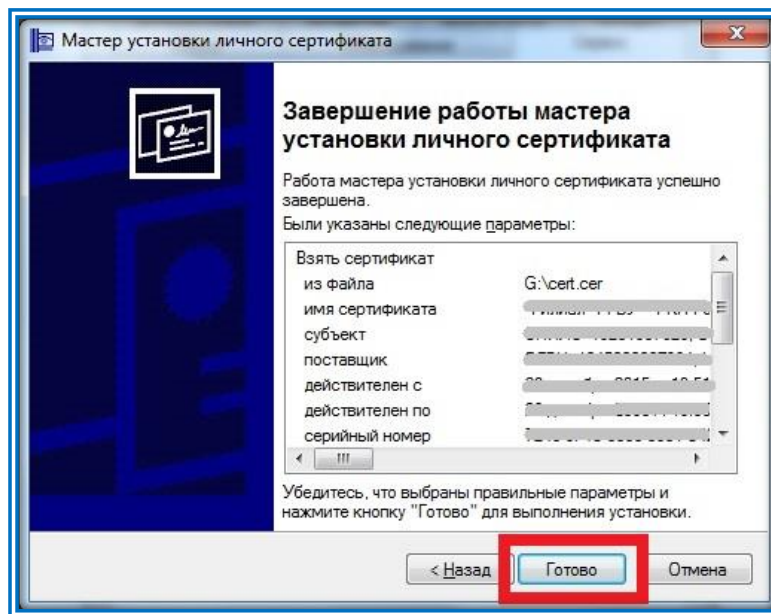


Рисунок 2.12.1

3. Установка личного Сертификата из контейнера закрытого ключа на отчуждаемом носителе/реестра ОС

При получении услуги «Сертификат электронной подписи на носителе ключевой информации» Владелец Сертификата в офисе приема УЦ на руки получает отчуждаемый съемный носитель, предоставленный УЦ в рамках оказания услуги, содержащий Сертификат, установленный в контейнер закрытого ключа.

3.1. Для установки Сертификата из контейнера закрытого ключа на отчуждаемом носителе/реестра ОС последовательно выберите меню **Пуск -> Панель управления** (если на компьютере установлена ОС WindowsXP: **Пуск -> Настройка -> Панель управления**). В появившемся окне выберите **КриптоПро CSP** и запустите, дважды кликнув левой кнопкой мыши.

3.2. В появившемся окне «КриптоПро CSP» необходимо перейти на вкладку «Сервис» и нажать кнопку «Просмотреть сертификаты в контейнере...» (см. Рисунок 3.2.1):

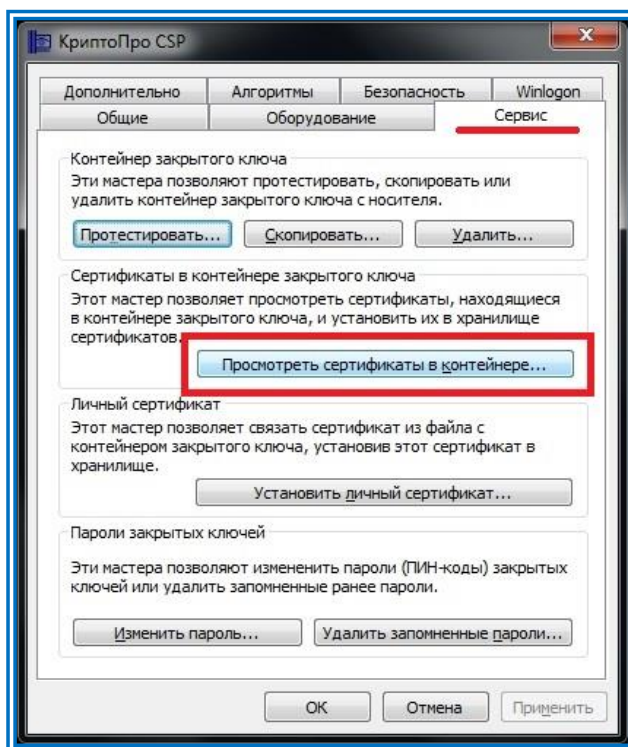


Рисунок 3.2.1

3.3. В окне «Сертификаты в контейнере закрытого ключа» необходимо нажать кнопку «Обзор» (см. Рисунок 3.3.1):

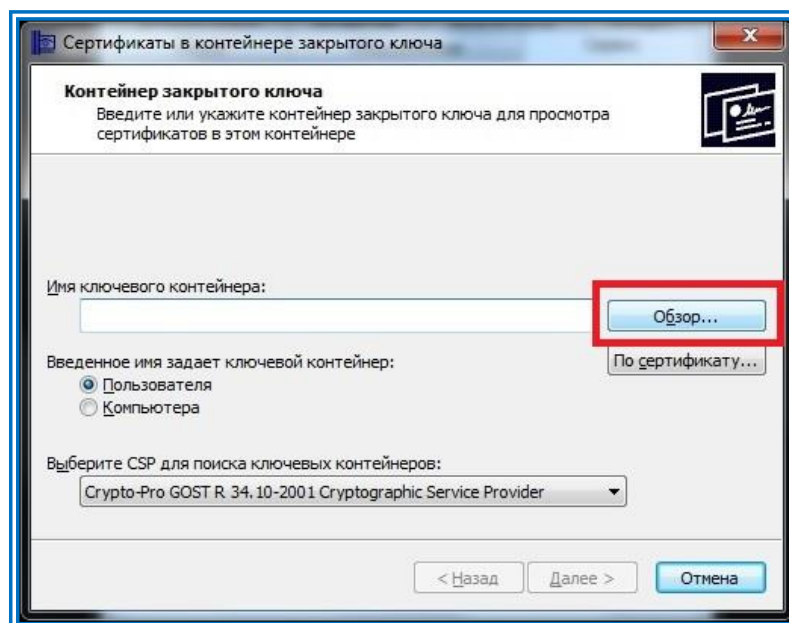


Рисунок 3.3.1

3.4. Далее в окне «КриптоПро CSP» необходимо выбрать требуемый контейнер и нажать кнопку «ОК» (см. Рисунок 3.4.1):

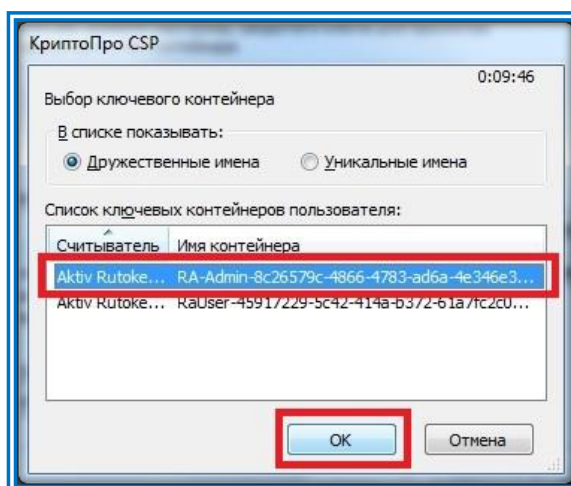


Рисунок 3.4.1

3.5. Программа вернется в окно **«Сертификаты в контейнере закрытого ключа»**. Для продолжения необходимо выбрать требуемый алгоритм схемы электронной подписи - (**Crypto-Pro GOST R 34.10-2001 Cryptographic Service Provider** или **Crypto-Pro GOST R 34.10-2012 Cryptographic Service Provider**), затем нажать кнопку **«Далее»** (см. Рисунок 3.5.1):

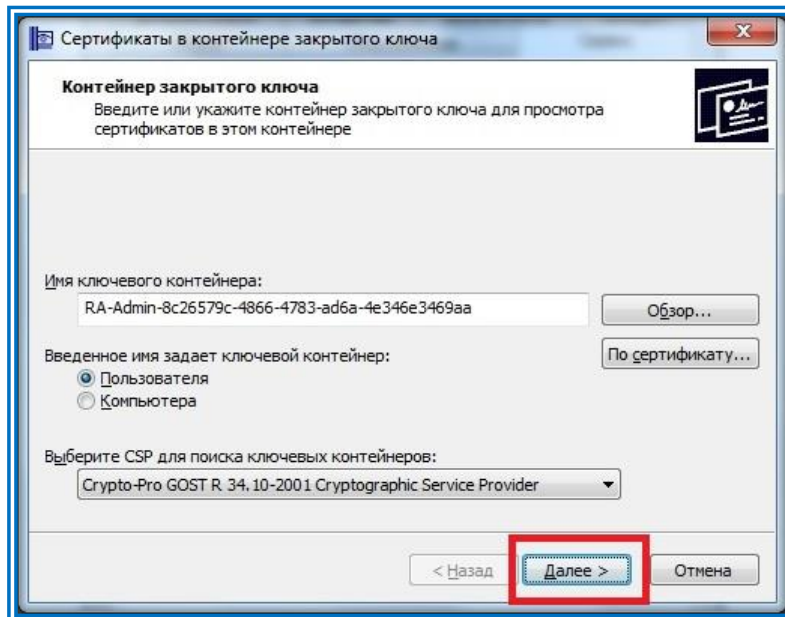


Рисунок 3.5.1

3.6. Отобразится информация об устанавливаемом Сертификате. Для установки Сертификата пользователя необходимо нажать кнопку **«Установить»** (см. Рисунок 3.6.1):

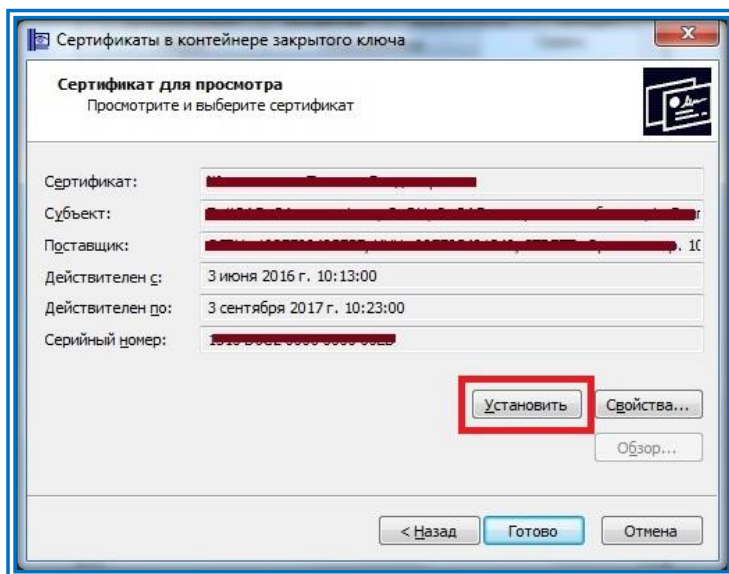


Рисунок 3.6.1

Появится сообщение об успешной установке Сертификата в хранилище. Необходимо нажать кнопку «ОК» и далее кнопку «Готово» (см. Рисунок 3.6.2):

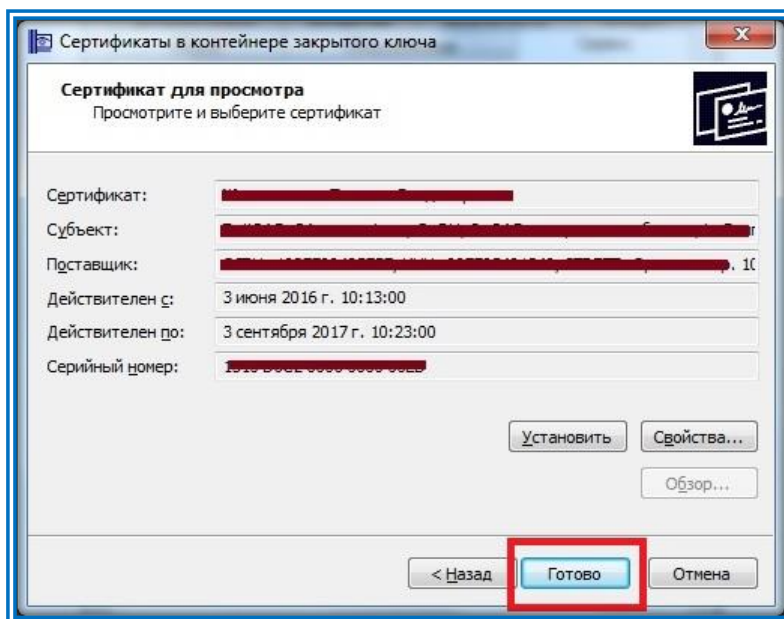


Рисунок 3.6.2

На этом установка Сертификата завершена.



Примечание: В случае если вместо информации о Сертификате пользователя появится сообщение криптопровайдера о том, что в контейнере закрытого ключа отсутствует Сертификат, Сертификат необходимо устанавливать из файла согласно разделу 2 настоящей Инструкции.

Сертификат будет доступен для скачивания в Личном кабинете Владельца Сертификата после осуществления ознакомления с Сертификатом, как описано в разделе 2 настоящей инструкции.

