

Инструкция по генерации ключа электронной подписи и получению сертификата ключа проверки электронной подписи для совершения торговых операций в информационно-торговой системе «QUIK»

Для того, чтобы в рамках заключенного с Банком договора на брокерское обслуживание совершать сделки в информационно-торговой системе «QUIK» (далее - ИТС «QUIK») с использованием электронной подписи¹ (далее – ЭП), Вам необходимо выполнить следующие действия:

Шаг 1 (Посещение офиса Банка)

- **Подпишите** подготовленные работником Банка следующие документы:
 - 1) Заявление на регистрацию Субъекта информационного обмена².
 - 2) Заявление на изготовление сертификата ключа проверки ЭП (Приложение 1 к настоящей Инструкции).

- **Получите** от работника Банка:
 - 1) Функциональный ключевой носитель (далее – ФКН).
ФКН – это специальный USB флэш-носитель, предназначенный для размещения ключевой информации, используемой для выполнения криптографических процедур шифрования и расшифрования, формирования ЭП.
 - 2) Файл с автономной html-формой для генерации ключей ЭП и соответствующего электронного файла запроса на выдачу сертификата ключа проверки ЭП (направляется на адрес электронной почты клиента, указанный в Заявлении на регистрацию Субъекта информационного обмена).

Шаг 2 (Установка необходимого программного обеспечения для генерации и использования ЭП)

Установите необходимое программное обеспечение на компьютер:

- Выполните установку и настройку СКЗИ «КриптоПро CSP» версии 4.0 и выше в соответствии с Руководством по скачиванию и установке СКЗИ «КриптоПро CSP», доступным по ссылке - [Инструкция](#).

- Вставьте ФКН («eToken PRO (Java)» или «Рутокен ЭЦП 2.0» - тип указан на выданном ФКН) в USB-разъем на компьютере пользователя и произведите установку драйвера ФКН.

Ссылка на драйвер	Ссылка на инструкцию
«eToken PRO (Java)»	Руководство по eToken
«Рутокен ЭЦП 2.0»	Руководство по Рутокен

¹ На основании Уведомления об организации перехода на использование схемы электронной подписи по ГОСТ Р 34.10-2012 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» Федеральной службы безопасности Российской Федерации (письмо от 07.09.2018 № 149/7/6-363 размещено на сайте Минкомсвязи России) после 31.12.2019 запрещается использование схемы электронной подписи, соответствующей стандарту ГОСТ Р 34.10-2001.

² Приложение 8 к Временному регламенту Удостоверяющего центра АО «Россельхозбанк» (приказ АО «Россельхозбанк» от 07.04.2011 № 134-ОД).

Шаг 3 (Генерация ключа ЭП и электронного файла запроса на выдачу сертификата ключа проверки ЭП)

Замечание: Для работы с автономной html-формой необходимо, чтобы на компьютере был установлен Internet Explorer версии не ниже 9.0.

3.1. Сохраните полученный по электронной почте файл с html-формой запроса и снимите с него блокировку. Для этого необходимо нажать правой кнопкой мышки по данному файлу и в раскрывшемся меню нажать на пункт «Свойства». В окне свойств откройте вкладку «Общие» и при наличии сообщения о блокировке файла выберите опцию «Разблокировать», после чего нажмите на кнопку «ОК» внизу окна (Рисунок 1).

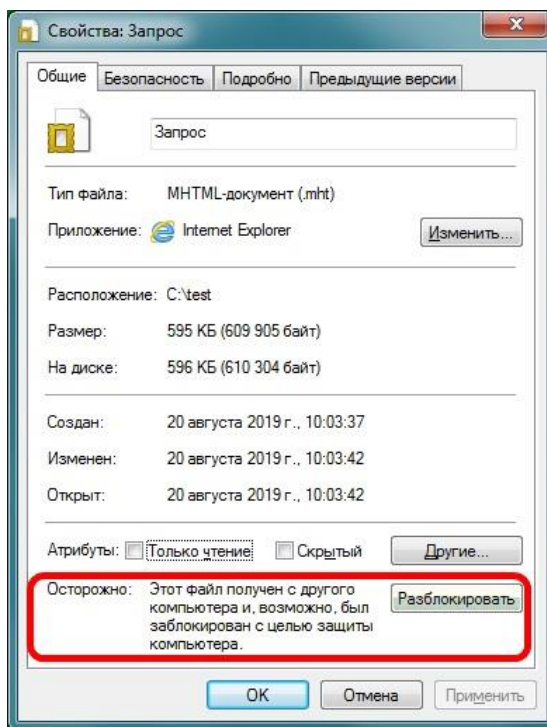


Рисунок 1. Разблокировка файла с html-формой запроса

3.2. Вставьте в USB-порт компьютера ФКН, полученный ранее в офисе Банка, и откройте html-форму, полученную по электронной почте (Рисунок 2).

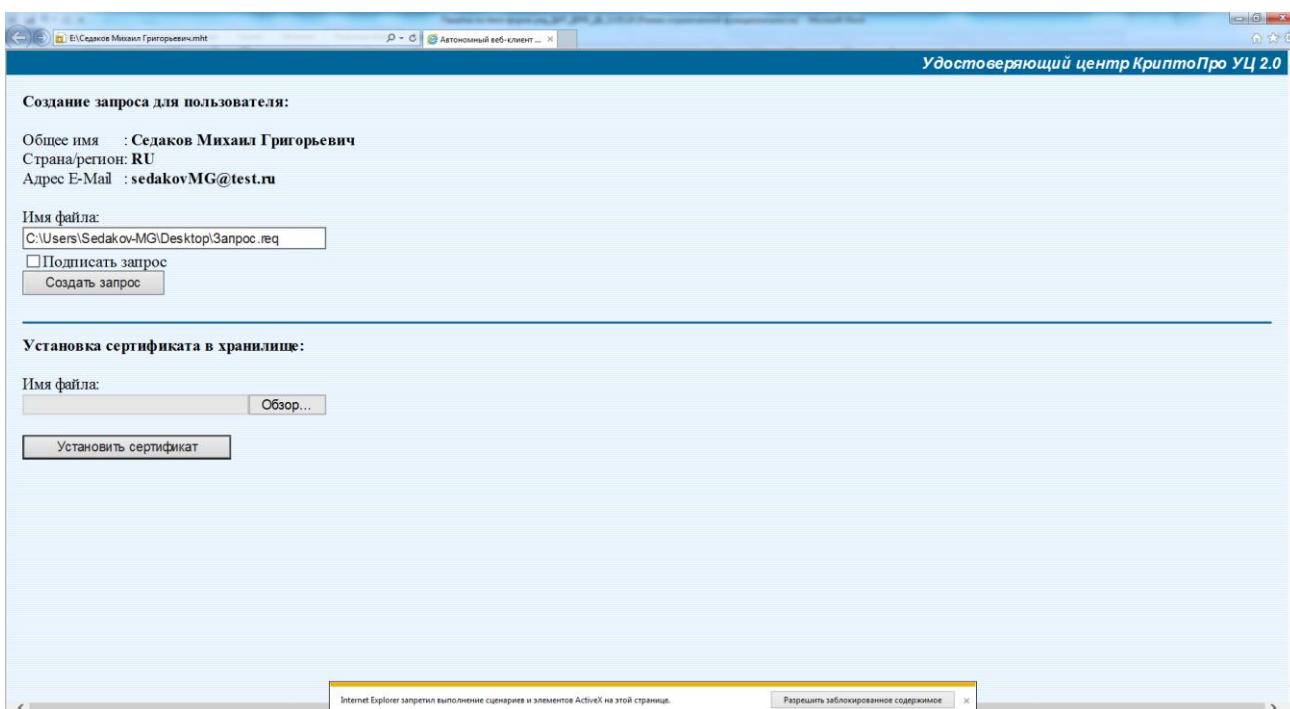


Рисунок 2. html-форма для автономной работы

3.3. В случае появления в Internet Explorer информационных сообщений о блокировке содержимого html-формы, следует разрешить заблокированное содержимое (Рисунок 3).

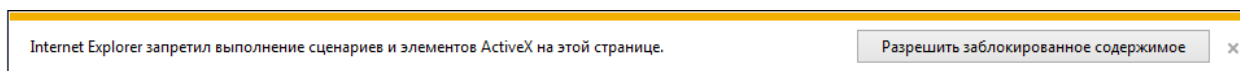


Рисунок 3. Информационное сообщение о блокировке содержимого HTML-формы

3.4. Проверьте личные данные в верхней части окна (Рисунок 2). Если в данных есть ошибка, то необходимо об этом сообщить по адресу invest@rshb.ru или телефону 8 (800) 100-40-40.

3.5. Если данные корректны, то необходимо в поле «Имя файла» задать путь и имя электронного файла запроса на выдачу сертификата ключа проверки ЭП с расширением «*.req» (имя может быть любым, в качестве примера использовано имя «Запрос»).

Замечание: Не сохраняйте файл запроса в корень диска C. Рекомендуется указывать путь в формате C:\Users\Sedakov\Desktop\Запрос.req

3.6. Без установки опции «Подписать запрос» нажмите на кнопку «Создать запрос». В зависимости от настроек Вашего рабочего места возможно появление различных предупреждений, в которых необходимо будет разрешить дальнейшую работу html-формы.

3.7. Далее необходимо выбрать ФКН, на который будет произведена запись ключа ЭП (Рисунок 4).

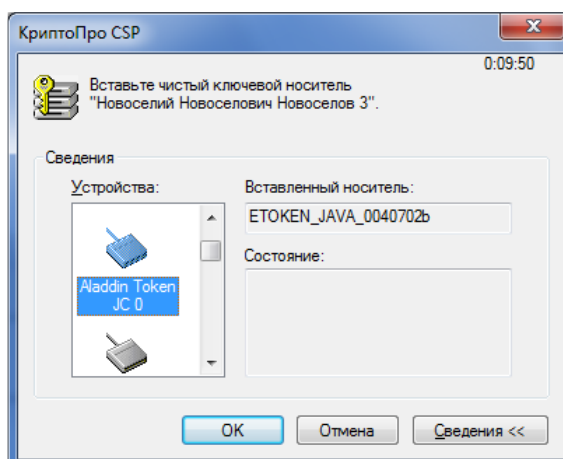


Рисунок 4. Выбор ключевого носителя

3.8. После выбора ФКН откроется биологический датчик случайных чисел (Рисунок 5). Необходимо двигать мышью и/или нажимать случайные клавиши на клавиатуре до завершения процедуры.

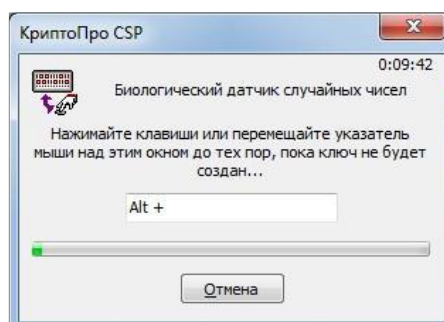


Рисунок 5. Биологический датчик случайных чисел

3.9. После завершения работы биологического датчика случайных чисел необходимо ввести pin-код для ключевого контейнера на ФКН (pin-код по умолчанию³ для eToken: 1234567890, pin-код для Рутокен: 12345678) (Рисунок 6). Pin-код будет необходим для последующего использования, поэтому его необходимо запомнить/записать.

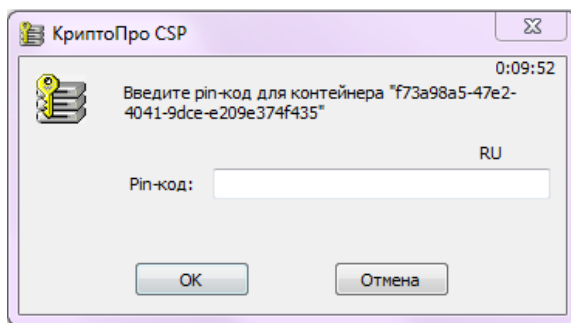


Рисунок 6. Окно ввода pin-кода для ключевого контейнера на ФКН

3.10. Электронный файл запроса на выдачу сертификата ключа проверки ЭП будет сформирован и сохранен по указанному Вами ранее пути в html-форме для автономной работы (в примере – C:\Users\Sedakov\Desktop\Запрос.req). Одновременно будет сгенерирован и записан на ФКН ключ ЭП. Подтверждением будет являться появление следующего информационного сообщения (Рисунок 7).

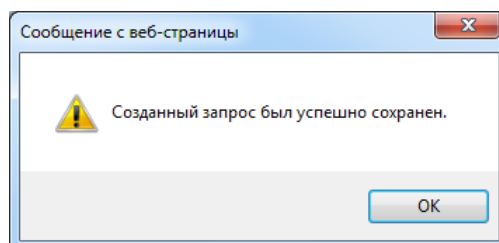


Рисунок 7. Окно успешного создания запроса на выдачу сертификата ключа проверки ЭП

3.11. Созданный электронный файл запроса на выдачу сертификата ключа проверки ЭП (Запрос.req) необходимо направить на адрес электронной почты клиентского менеджера Банка, принявшего Заявление на регистрацию Субъекта информационного обмена, с обязательным указанием темы письма «ФИО клиента, Запрос на выдачу сертификата ключа проверки ЭП».

3.12. В ответ на запрос в течение 3-х рабочих дней по электронной почте клиентским менеджером направляется личный сертификат ключа проверки ЭП клиента, который необходимо сохранить на компьютере пользователя (к примеру, в каталог C:\RSHB_QUIK\). Порядок установки личного сертификата ключа проверки ЭП клиентом описан далее (шаг 5).

³ Pin-код по умолчанию рекомендуется сменить после установки сертификата ключа проверки ЭП (шаг 5).

Шаг 4 (Установка корневого сертификата ключа проверки ЭП УЦ РСХБ)

Установите актуальный корневой сертификат ключа проверки ЭП УЦ РСХБ на компьютере пользователя. Для этого

- **Скачайте** актуальный корневой сертификат ключа проверки ЭП УЦ РСХБ (ГОСТ Р 34.10-2012) с официального сайта АО «Россельхозбанк» по ссылке https://www.rshb.ru/legal/remote_banking/cert. Запустите сохранённый файл.
- В открывшемся окне выберите **«Установить сертификат...»** - откроется окно мастера импорта сертификатов (Рисунок 8).

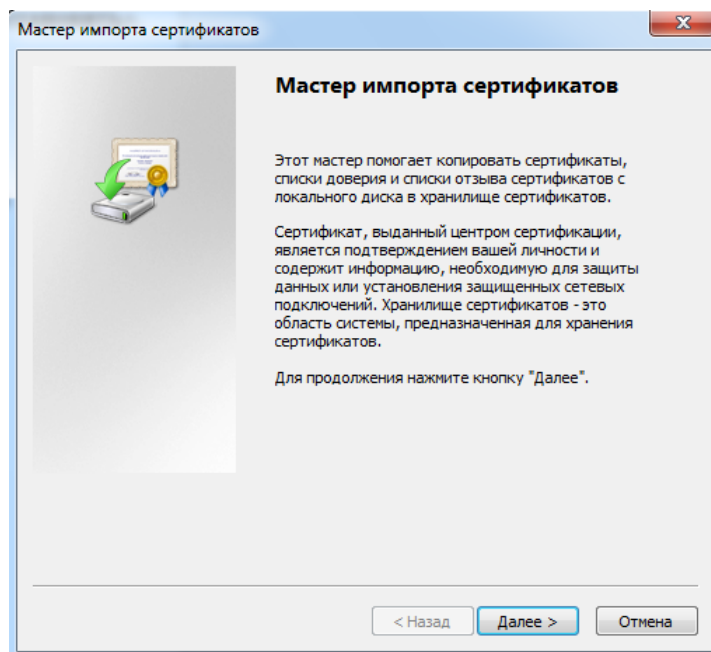


Рисунок 8. Стартовое окно мастера импорта сертификатов

- Нажмите на кнопку «Далее» - откроется окно выбора пути к хранилищу сертификатов (Рис. 9).

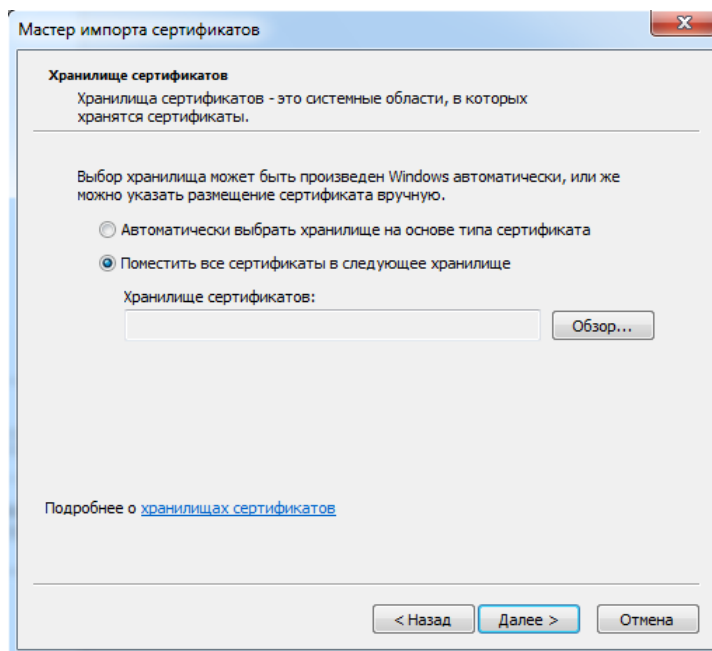


Рисунок 9. Окно выбора пути к хранилищу сертификатов

- **Выберите** опцию «Поместить все сертификаты в следующее хранилище» и нажмите на кнопку «Обзор». Откроется окно выбора хранилища сертификатов (Рисунок 10).

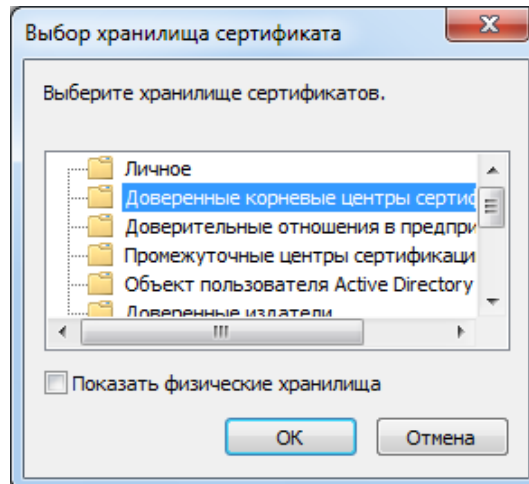


Рисунок 10. Окно выбора хранилища сертификатов

- **Выберите** хранилище «Доверенные корневые центры сертификации» и нажмите кнопку «ОК». Для продолжения импорта сертификата ключа проверки ЭП, в окне хранилища сертификатов нажмите на кнопку «Далее». Откроется окно завершения работы мастера импорта сертификатов (Рисунок 11).

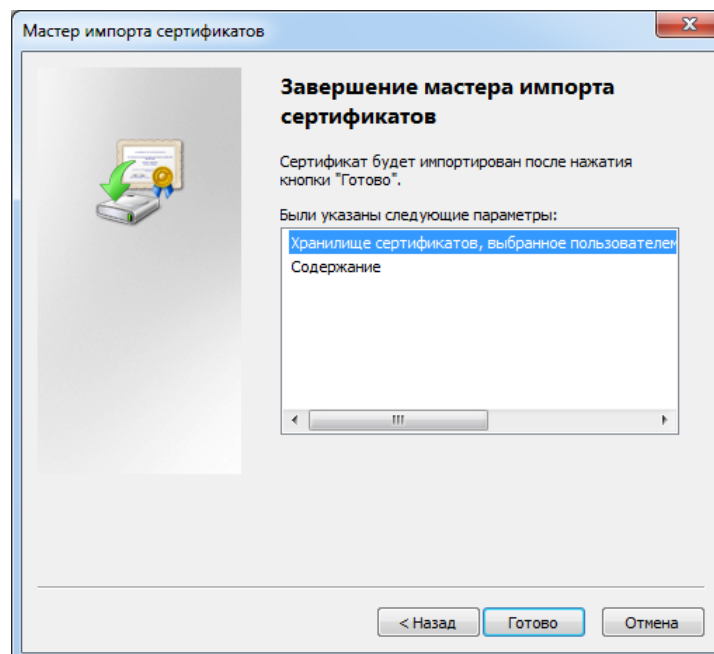


Рисунок 11. Окно завершения работы мастера импорта сертификатов

- Нажмите кнопку «Готово», после чего должно появиться информационное сообщение, что сертификат ключа проверки ЭП успешно импортирован (Рисунок 12).

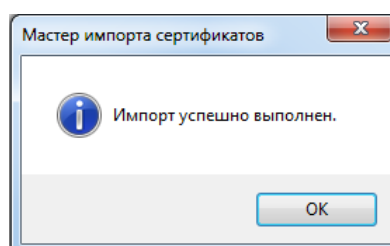


Рисунок 12. Импорт успешно выполнен

Шаг 5 (Установка личного сертификата ключа проверки ЭП клиента)

5.1. Запустите СКЗИ «КриптоПро CSP» путем выполнения команды «Пуск» → «Программы» → «Крипто-Про» → «КриптоПро CSP». При запуске СКЗИ «КриптоПро CSP» откроется основное окно программы (Рисунок 13).

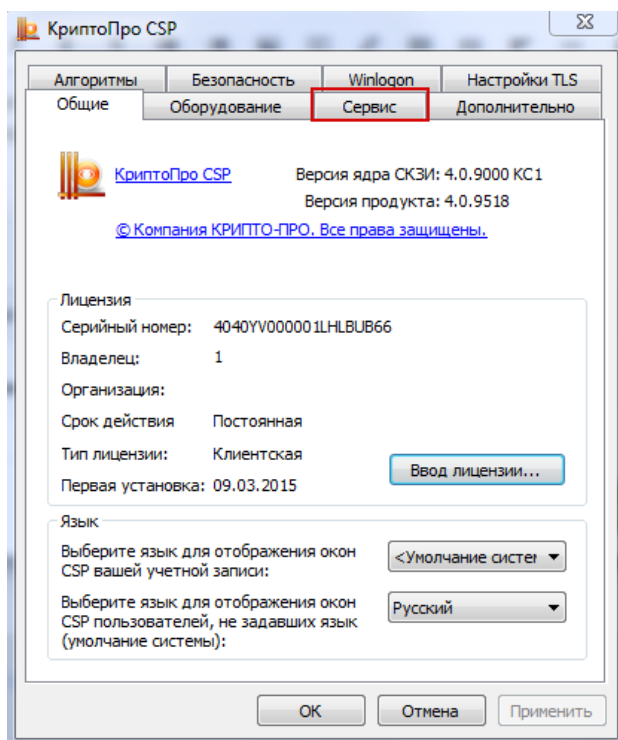


Рисунок 13. Стартовое окно СКЗИ «КриптоПро CSP»

5.2. Перейдите на вкладку «Сервис» и нажмите на кнопку «Установить личный сертификат» (Рисунок 14).

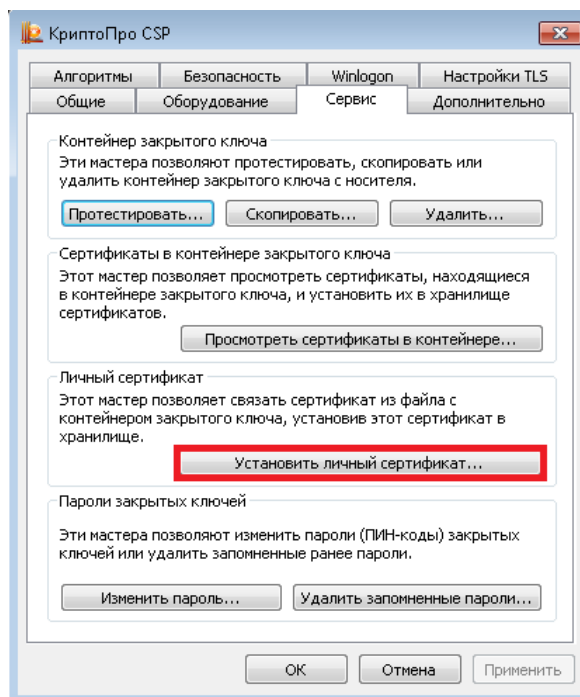


Рисунок 14. Окно вкладки «Сервис»

5.3. С помощью кнопки «Обзор» укажите расположение личного сертификата ключа проверки ЭП (по примеру из Шага 3 каталог C:\RSHB_QUICK) и нажмите на кнопку «Далее». (Рисунок 15).

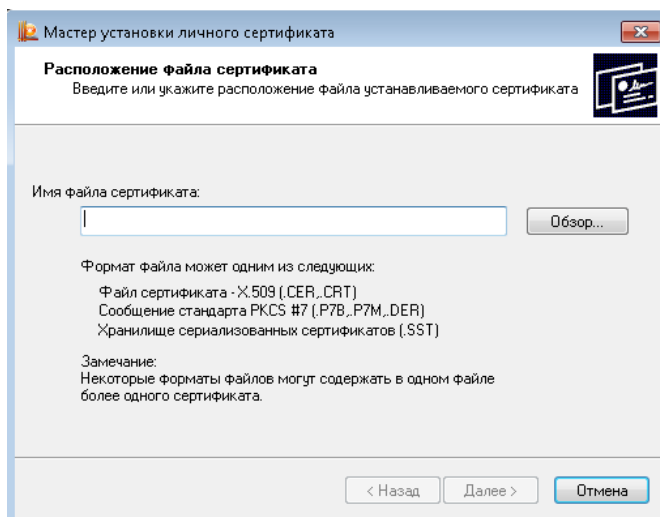


Рисунок 15. Окно импорта сертификатов ключей проверки ЭП

5.4. Откроется окно с информацией о выбранном сертификате ключа проверки ЭП. (Рисунок 16).

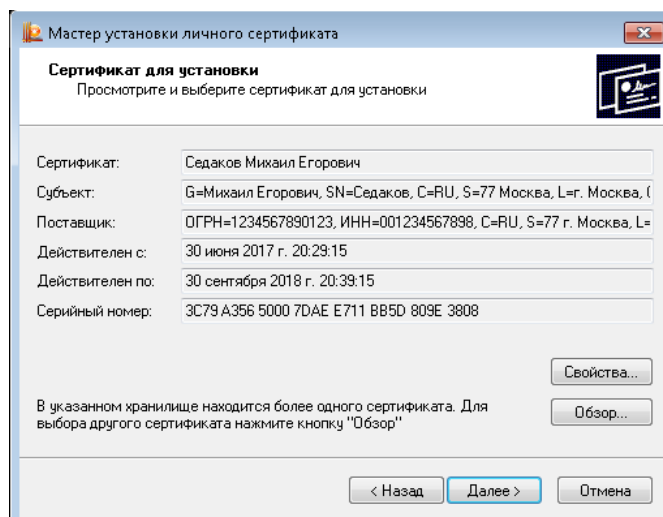


Рисунок 16. Окно с информацией о сертификате ключа проверки ЭП

5.5. Для продолжения установки нажать кнопку «Далее». Откроется окно выбора ключевого контейнера. (Рисунок 17).

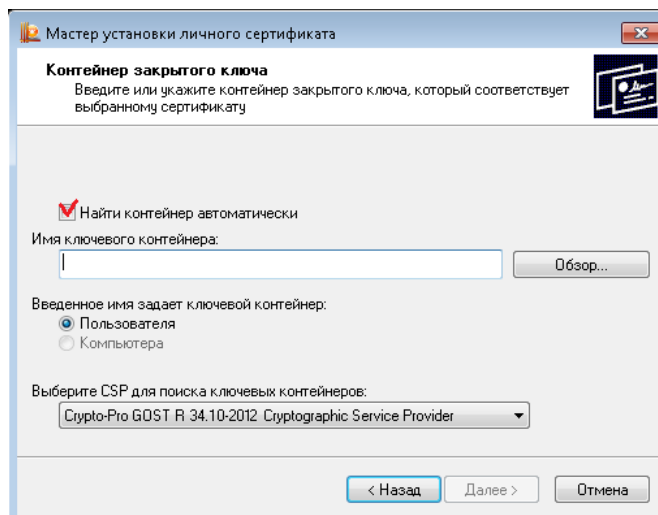


Рисунок 17. Окно выбора контейнера ключа ЭП

5.6. Убедитесь, что подключен ФКН, на котором производилась генерация ключа ЭП и отметьте опцию «Найти контейнер автоматически» либо (если опция «найти контейнер автоматически» не отмечена) найдите ключевой контейнер с помощью кнопки «Обзор». После того, как ключевой контейнер будет найден, необходимо нажать кнопку «Далее». Откроется окно выбора хранилища сертификатов (Рисунок 18).

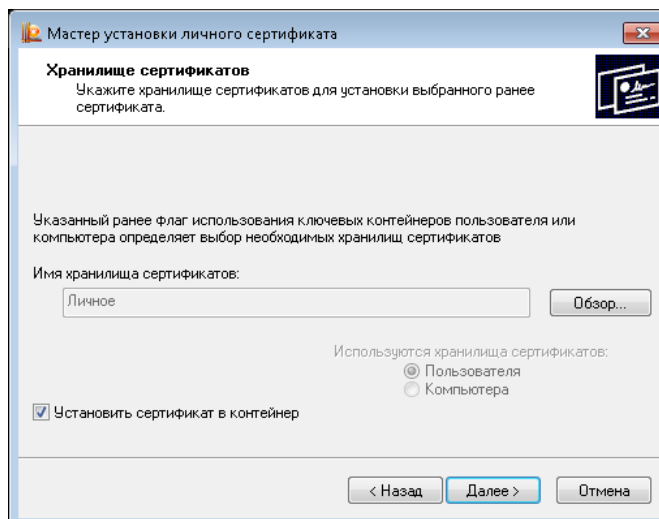


Рисунок 18. Окно выбора хранилища сертификатов

5.7. В поле «Имя хранилища сертификатов» выберите хранилище «Личное» и установите опцию «Установить сертификат в контейнер». Для продолжения установки нажмите на кнопку «Далее». Откроется окно завершения работы мастера установки личного сертификата (Рисунок 19).

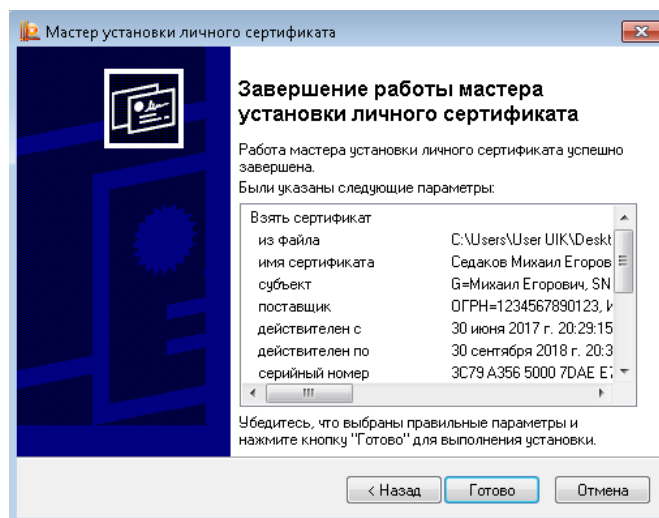


Рисунок 19. Окно завершения работы мастера установки личного сертификата

5.8. Для завершения установки личного сертификата ключа проверки ЭП нажать кнопку «Готово».

Приложение 1

к Инструкции по генерации ключа электронной подписи и получению сертификата ключа проверки электронной подписи для совершения торговых операций в информационно-торговой системе «QUIK»

Заявление на изготовление сертификата ключа проверки электронной подписи

Настоящим,

(Фамилия, Имя, Отчество (полностью) Клиента/Уполномоченного представителя,
паспорт № _____, выдан _____
паспортные данные,
_____ «___» _____ 20__ г.

должность, наименование Клиента Юридического лица)

просит изготовить на своё имя сертификат ключа проверки электронной подписи.

К настоящему заявлению прилагаются:

1. электронный файл запроса на выдачу сертификата ключа проверки электронной подписи;
2. сканированная копия Заявления на регистрацию Субъекта информационного обмена.

заявитель _____
(подпись) (расшифровка подписи)
руководитель _____
(подпись) (расшифровка подписи)
«___» _____ 20__ г.

М.П.

Принято

Отказано¹ _____
(указать причину отказа в принятии заявления)

Ответственный работник
АО «Россельхозбанк»

(должность)

(подпись) (расшифровка подписи)
«___» _____ 20__ г.
М.П.

¹ Заполняется в случае отказа в принятии заявления.