

ИНСТРУКЦИЯ

для пользователей

ЗАПРОС И УСТАНОВКА СЕРТИФИКАТА С ПОМОЩЬЮ ПРОГРАММЫ PkiTools-OnlineClient

Оглавление

1. Формирование запроса на сертификат.....1
2. Установка сертификата на ключевой контейнер6


Программа **Инструменты PKI (PkiTools-OnlineClient)** предназначена для получения сертификатов в Удостоверяющем Центре СКБ Контур для работы в системе **Контур-Экстерн** и других сервисах, предоставляемых компанией СКБ Контур. Программа устанавливается вместе с системой **Контур-Экстерн**.



Если в процессе установки системы Контур-Экстерн программа Инструменты PKI не была установлена, установите ее вручную. Дистрибутив находится на установочном диске в папке Программное обеспечение / Инструменты PKI / pki-tools-online-client.msi.

1. Формирование запроса на сертификат

Для формирования запроса на сертификат выполните следующие действия:

1. Вставьте в компьютер ключевой носитель, полученный в сервисном центре.
2. Запустите программу **Инструменты PKI** с помощью ярлыка , размещенного на рабочем столе, или пункта меню **Пуск / Все программы / СКБ Контур / Инструменты PKI / Получение сертификатов в УЦ СКБ Контур**.
3. В открывшемся окне мастера создания запроса (рис. 1) выберите пункт **Получить сертификат** и нажмите на кнопку **Далее**.

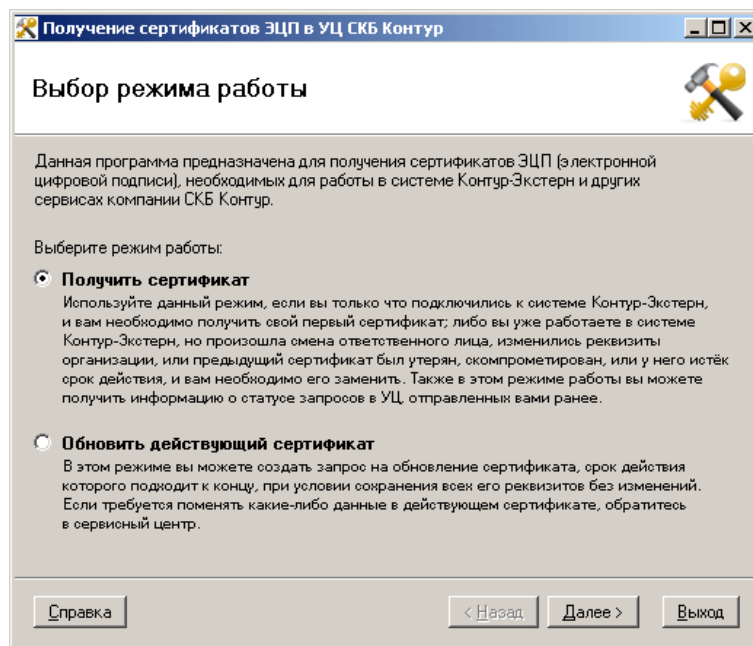


Рис. 1. Окно выбора режима работы

4. В открывшемся окне (рис. 2) выберите ключевой носитель, полученный в сервисном центре.



*Если в окне не отображается нужный ключевой носитель, вставьте его в компьютер и нажмите на кнопку **Обновить список**.*

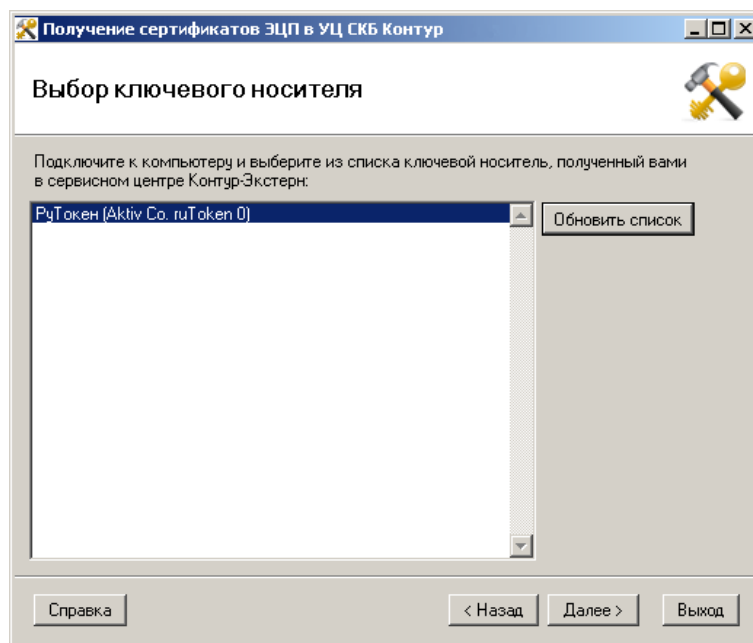


Рис. 2. Окно выбора ключевого носителя



Для формирования запроса должен использоваться только ключевой носитель, выданный в сервисном центре. В случае выбора другого ключевого носителя появится предупреждение «Ключевой носитель»

не инициализирован», и формирование запроса будет невозможно.

5. Нажмите на кнопку **Далее**. В результате этого действия начнется процесс соединения с Интернетом и получения данных с сервера. После загрузки данных в окне (рис. 4) будет отображено название организации (организаций), для которой запрашивается сертификат.

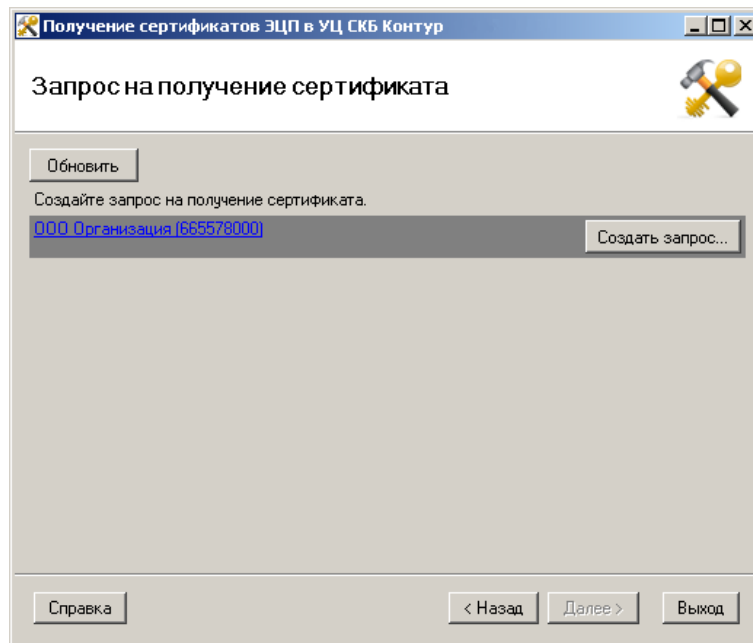


Рис. 4. Окно загрузки данных с сервера

Если в окне не отображается нужная организация, обратитесь в сервисный центр.



Если в качестве ключевого носителя используется Рутокен, на который сохраняются сертификаты одного пользователя для сдачи отчетности за несколько организаций, то после загрузки данных в списке будет указано несколько имен сертификатов и статусы соответствующих запросов.

6. Проверьте данные, указанные в запросе на сертификат, нажав на ссылку с именем сертификата.



Если данные указаны неверно, обратитесь в сервисный центр, иначе отчетность будет передаваться с неверными реквизитами организации.

7. Закройте окно с данными сертификата и нажмите на кнопку **Создать запрос**.

8. В открывшемся окне **КриптоПро CSP** (рис. 5) с помощью полосы прокрутки выберите ключевой носитель, выданный в сервисном центре, и нажмите на кнопку **ОК**.

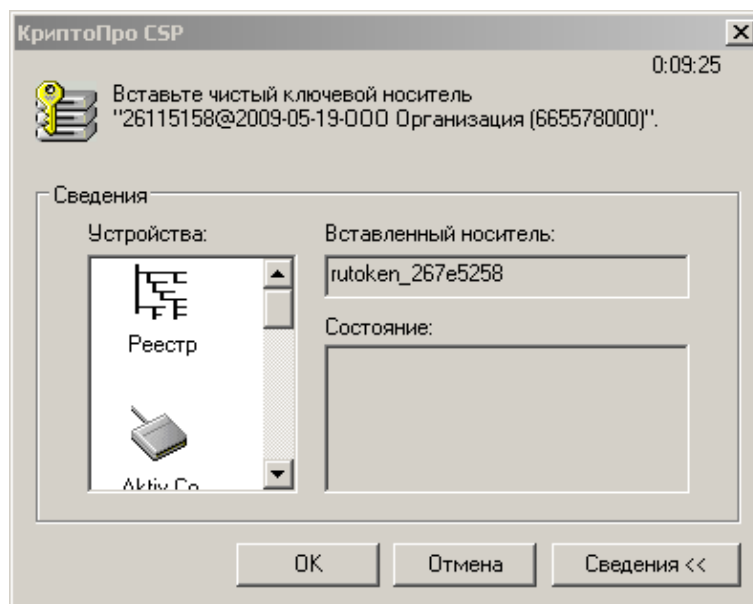


Рис. 5. Окно выбора ключевого носителя

9. Для формирования закрытого ключа выполните движения курсором мыши в области окна генератора случайных чисел (рис. 6).

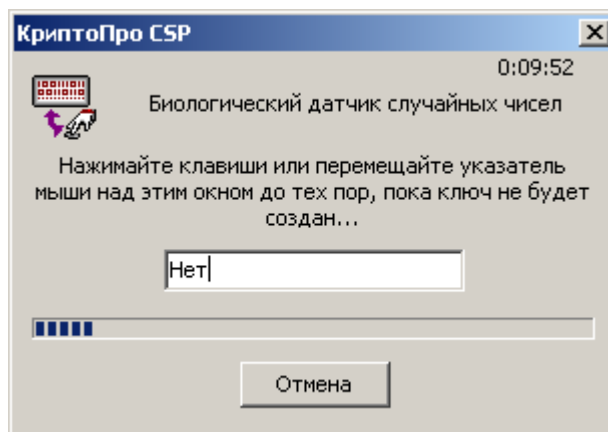


Рис. 6. Окно генератора случайных чисел

10. В открывшемся окне установки пароля на ключевой контейнер (рис. 7) действия выполняются в зависимости от вида ключевого носителя:
 - Если в качестве ключевого носителя используется **Рутокен**, предложение ввести пароль носит **обязательный** характер (без ввода пароля формирование запроса будет невозможно). Необходимо ввести pin-код (по умолчанию 12345678) для того, чтобы активировать данный ключевой носитель.

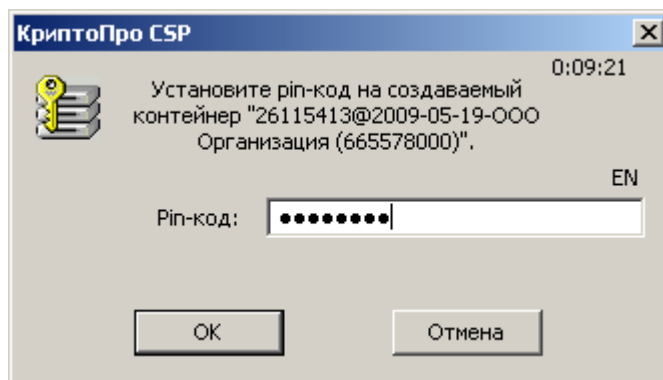


Рис. 7. Окно ввода pin-кода

- Если в качестве ключевого контейнера используется **дискета**, то предложение ввести пароль носит **необязательный** характер.



Установка пароля повышает уровень защиты ключевой информации от использования посторонними лицами. Указанный пароль будет запрашиваться при каждом обращении системы к закрытому ключу. Но следует помнить: при утере пароля дальнейшее использование ключа становится невозможным. При работе с дискетой рекомендуется не вводить пароль, а оставлять поля пустыми.

11. Нажмите на кнопку **ОК**. В результате этого действия создается запрос на сертификат, открывается файл запроса и окно печати.



*При нажатии на кнопку **Отмена** процесс формирования запроса прерывается, после чего следует нажать на кнопку **Назад** и повторить все действия, начиная с пункта 7.*

12. Если к рабочему месту, на котором формируется запрос на сертификат, подключен принтер, то необходимо распечатать бланк запроса и подписать его.



Бланк запроса на сертификат распечатывается в одном экземпляре и передается сотруднику сервисного центра лично или отправляется по почте.

Если с рабочего места, на котором формируется запрос на сертификат, нельзя распечатать бланк запроса, его необходимо сохранить, нажав на кнопку **Сохранить бланк запроса** (рис. 8), и распечатать с другого рабочего места, к которому подключен принтер.



Сохранить бланк запроса на сертификат можно только в текущем сеансе работы. При следующем запуске программы сохранить бланк запроса будет невозможно.

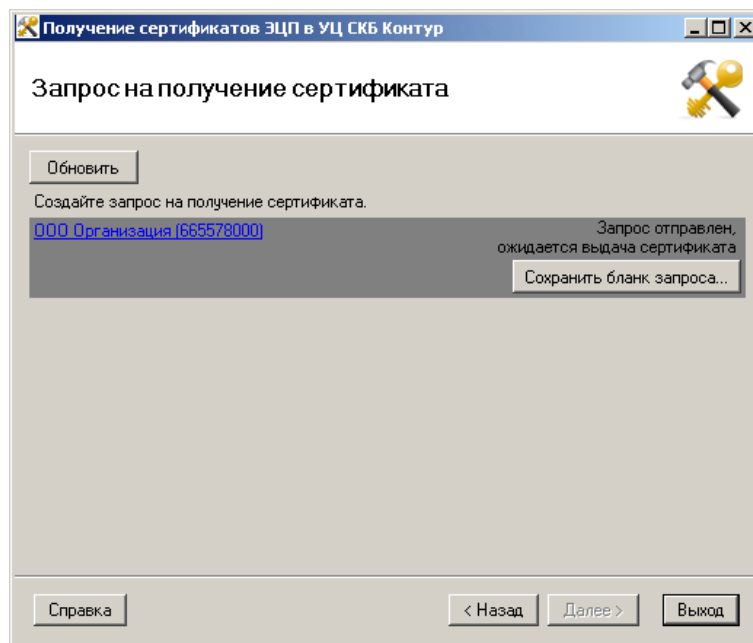


Рис. 8. Окно запроса на получение сертификата

Формирование запроса на сертификат завершено. Запрос отправлен в удостоверяющий центр.

Дождитесь обработки запроса, при этом рекомендуется не закрывать окно программы. Обычно запрос обрабатывается в течение 10-20 минут.



В соответствии с действующим регламентом Удостоверяющего центра сертификаты выдаются в течение 3-х рабочих дней.

Чтобы проверить готовность сертификата нажмите на кнопку **Обновить**. При этом произойдет соединение с сервером, в результате которого будет получена информация о состоянии запроса:

- Если справа от сертификата отображается надпись «Сертификат готов», выполните его установку.
- Если справа от файла сертификата отображается надпись «Отказано в выдаче», обратитесь в сервисный центр.

2. Установка сертификата на ключевой контейнер

Для установки сертификата выполните следующие действия:

*Если окно программы **Инструменты PKI (PkiTools-OnlineClient)** было закрыто, выполните пункты 1-4 раздела «Формирование запроса на сертификат».*

1. В открывшемся окне (рис. 9) нажмите на кнопку **Установить**.

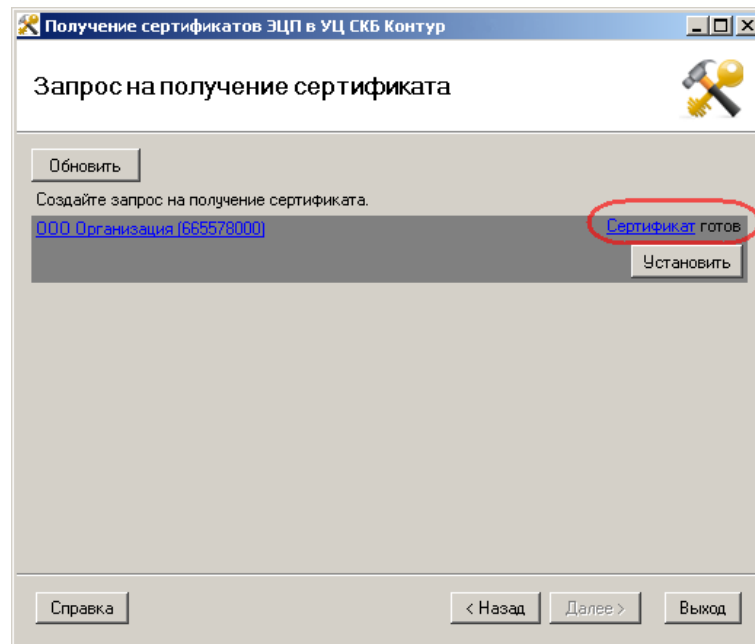


Рис. 9. Окно запроса на получение сертификата



При нажатии на ссылку **Сертификат** открывается окно со сведениями о сертификате.



Если в качестве ключевого носителя используется Рутокен, то во время установки сертификата появится окно установки пароля на ключевой контейнер (рис. 10). Введите pin-код (по умолчанию 12345678) и нажмите на кнопку **ОК**.

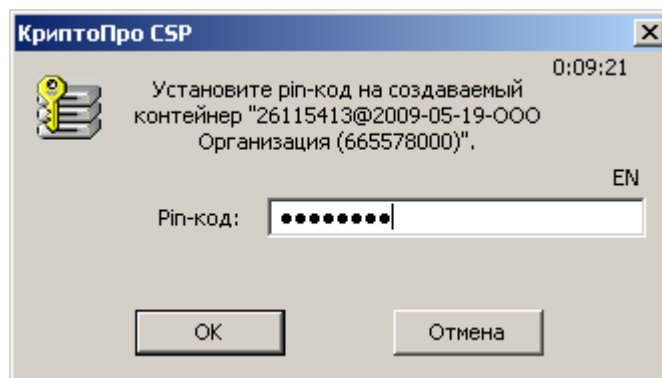


Рис. 10. Окно ввода пароля

2. Дождитесь завершения установки. В результате успешной установки справа от сертификата будет отображена надпись «Сертификат установлен». Нажмите на кнопку **Выход** (рис. 11).

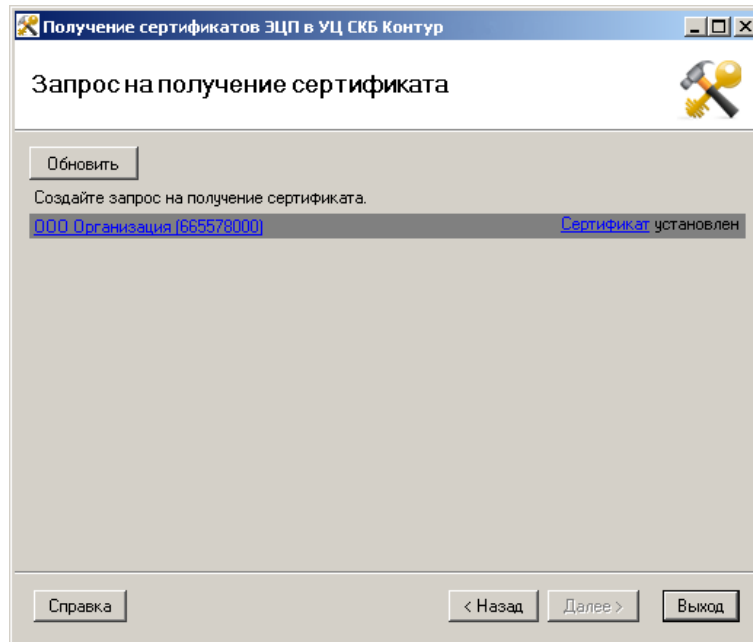


Рис. 11. Окно запроса на получение сертификата

Установка сертификата завершена.

После того как вы сделаете запрос на сертификат и установите сертификат в ключевой контейнер, необходимо передать подписанный бланк запроса на сертификат сотруднику сервисного центра.



Удостоверяющий центр компании СКБ Контур имеет право отозвать выданные сертификаты в том случае, если абонент не предоставит в сервисный центр следующие документы:

- бланк запроса на сертификат;
- доверенность (если получение инициализированного носителя выполняет доверенный представитель).