Инструкция
для пользователей

Запрос и установка сертификата с помощью
программы PkiTools Online Client

 **1. Генерация ключей ЭЦП и запроса на сертификат**

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.

Чтобы сгенерировать ключи электронной цифровой подписи (ЭЦП) и запрос на сертификат с помощью программы **PkiTools OnlineClient,** выполните следующие действия:

1. Установите программу **PkiTools OnlineClient.**

Возможны два варианта установки:

- автоматическая установка;

Если вы воспользуетесь установочным диском для автоматической установки системы **Контур-Экстерн**, то программа **PkiTools OnlineClient** будет **автоматически** установлена вместе с системой **Контур-Экстерн.**- установка вручную.

Установка вручную подробно описана в документе **Инструкция по установке и настройке рабочего места для работы с PkiTools OnlineClient,** находящемся на установочном диске системы **Контур-Экстерн** в папке**Документация Инструменты PKI.**Для установки программы **PkiTools OnlineClient** и дальнейшей работы с ней требуется, чтобы:

- на рабочем месте было установлено **СКЗИ КриптоПро CSP** 3.0.3293 (SP3 и выше) или **КриптоПро CSP** 3.6.5141 и выше;
- компьютер должен быть подключен к сети Интернет;
- на компьютере должен быть открыт 443 порт (за помощью обращайтесь к
системному администратору).

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

1. В открывшемся окне (см. рис. 2) выберите ключевой носитель, полученный в сервисном центре. Нажмите на кнопку **Обновить список**, если ключевой носитель был подключен к компьютеру после появления этого окна.


Рис. 2. Окно выбора ключевого носителя

*Для формирования запроса должен использоваться только ключевой носитель, выданный в сервисном центре. В случае выбора другого ключевого носителя генерация запроса и установка сертификата будут невозможны (рис. 3).*


Рис. 3. Выбор ключевого носителя

 *Если в открывшемся окне отображено сообщение****Ключевой носитель не инициализирован****(рис. 3), обратитесь в сервисный центр.*

1. Нажмите на кнопку **Далее,** тем самым вызвав процесс соединения с сетью Интернет и получения данных с сервера (см. рис. 4).


Рис. 4. Окно загрузки данных с сервера

1. После загрузки данных (рис. 5) будет отображено Общее имя сертификата (ваши ФИО).



Рис. 5. Окно загрузки данных с сервера

*Если в качестве ключевого носителя используется Рутокен, на который сохраняются сертификаты одного пользователя для сдачи отчетности за несколько организаций, то после загрузки данных в виде списка будут указаны Общие имена
сертификатов (ФИО владельца) и статусы соответствующих запросов (см. рис. 6).*


Рис. 6. Окно загрузки данных с сервера

1. Проверьте данные, указанные в запросе на сертификат (рис. 7), нажав на ссылку с Общим именем сертификата (ваши ФИО).


Рис. 7. Данные запроса

 *Если данные указаны неверно, обратитесь в сервисный центр.*

1. При необходимости введите кодовую фразу и сохраните её.

 *Кодовую фразу указывать не обязательно, она может потребоваться для отзыва сертификата.*

1. Нажмите на кнопку **Создать запрос** (рис. 8).


Рис. 8. Окно загрузки данных с сервера

1. В открывшемся окне **КриптоПро CSP** (рис. 9) выберите инициализированный ключевой носитель с помощью полосы прокрутки и нажмите на кнопку **OK.**


Рис. 9. Окно выбора ключевого носителя

1. Для формирования закрытого ключа выполните движения курсором мыши в области окна генератора случайных чисел.
2. В открывшемся <окне (см. рис. 10) установки пароля на ключевой контейнер действия выполняются в зависимости от вида ключевого носителя:


Рис. 10. Окно ввода пароля

* + Если в качестве ключевого носителя используется **Рутокен,** предложение ввести пароль носит **обязательный**характер (без ввода пароля формирование запроса будет невозможно – рис. 11). Необходимо ввести пароль (pin-код по умолчанию) 12345678 для того, чтобы активировать данный ключевой носитель.


Рис. 11. Окно ошибки при вводе pin-кода

* + Если в качестве ключевого контейнера используется **дискета**, то предложение ввести пароль носит**рекомендательный**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.*

1. 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 9.*

1. Если к рабочему месту, на котором формируется запрос на сертификат, подключен принтер, то пользователь распечатывает бланк запроса и подписывает его (см. рис. 12).


Рис. 12. Бланк запроса на сертификат

 *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. 13)


Рис. 13. Окно запроса на получение сертификата

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

1. Сохранить файл запроса, нажав на кнопку **ОК.**
2. Готовность сертификата можно проверить, нажав на кнопку **Обновить.** При этом произойдет соединение с сервером, в результате которого будет получена информация о состоянии запроса.

Кнопка **Выход** позволяет закрыть окно программы **PkiTools OnlineClient.**

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

 *В соответствии с действующим регламентом Удостоверяющего центра сертификаты выдаются в течение 3-х рабочих дней (на практике запрос обрабатывается в течение 10-20 минут).*

После получения сертификата выполните его установку.
 **2. Получение сертификата и его установка в ключевой контейнер**

Спустя 10-20 минут после создания запроса на сертификат можно проверить статус запроса и, если сертификат получен, установить его.

Для этого выполните следующие действия:
*Если окно программы****Инструменты PKI (PkiTools OnlineClient)****не было закрыто, нажмите на кнопку****Обновить****и выполните установку, начиная с пункта 4. Если окно программы было закрыто, выполните установку, начиная с пункта 1.*

1. 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.**
2. В открывшемся окне мастера создания запроса (см. рис. 14) выберите пункт **Получить сертификат** и нажмите на кнопку **Далее.**


Рис. 14. Окно выбора режима работы

1. В открывшемся окне выберите носитель, на который генерировался ключевой контейнер, и нажмите на кнопку**Далее.**
2. В открывшемся окне (рис. 15) будет отображено сообщение о готовности сертификата.

 *Если справа от файла сертификата отображается надпись «Отказано в выдаче», пользователю необходимо обратиться в сервисный центр.*


Рис. 15. Окно запроса на получение сертификата



При нажатии на ссылку **Сертификат** открывается окно со сведениями о сертификате (см. рис. 16). При нажатии на ссылку с Общим именем сертификата (вашими ФИО) откроется окно с данными запроса.


Рис. 16.Сведения о сертификате

1. Если сертификат имеет статус **готов,** нажмите на кнопку**Установить.**

Если в качестве ключевого носителя используется Рутокен, то во время установки сертификата появится окно установки пароля на ключевой контейнер (рис. 17). Введите пароль (pin-код по умолчанию) 12345678 и нажмите на кнопку **ОК.**


Рис. 17. Окно ввода пароля

1. Дождитесь завершения установки и нажмите на кнопку **Выход** (см. рис. 18).


Рис. 18. Окно запроса на получение сертификата

Установка сертификата завершена.

После того как вы сделаете запрос на сертификат и установите сертификат в ключевой контейнер, необходимо:

- во-первых, передать сотруднику сервисного центра подписанный бланк запроса на сертификат;

- во-вторых, подписать и заверить бланк сертификата (сотрудник сервисного центра может предоставить бланк сертификата только после того, как сертификат будет выдан Удостоверяющим центром СКБ Контур. Один из экземпляров бланка сертификата остается у вас, другой экземпляр, подписанный вами и заверенный печатью организации, передается сотруднику сервисного центра для последующей передачи в Удостоверяющий
центр СКБ Контур).

***В случае если бланки документов****(бланк запроса на сертификат, бланк сертификата; доверенность, если получение инициализированного носителя, выполнение действий по созданию запроса на сертификат и установке сертификата выполняет доверенный представитель)****НЕ БУДУТ переданы в сервисный центр, Удостоверяющий центр компании СКБ Контур имеет право отозвать выданные сертификаты.***