Телефон в Ижевске: +7 (3412) 72-11-00
Телефон в Москве: +7 (499) 277-1560
Сайт: www.directum.ru
E-mail: support@directum.ru

Инструкция по использованию Rutoken в системе DIRECTUM

Назначение документа

В целях повышения безопасности данных, закрытые ключи, используемые для шифрования и подписания документов системы DIRECTUM ЭП, рекомендуется хранить на съемных носителях. В роли таких носителей могут выступать различные устройства: смарт-карты, i-button, дискеты и прочие.

От устройства, используемого для хранения закрытых ключей, зависит порядок настройки системы DIRECTUM на работу с шифрованием и ЭП.

В настоящей инструкции описан порядок настройки системы DIRECTUM на работу с шифрованием и ЭП в случае, если закрытые ключи планируется хранить на электронных идентификаторах Rutoken.

Электронный идентификатор Rutoken – это персональное устройство доступа к информационным ресурсам, полнофункциональный аналог смарт-карты, выполненный в виде usb-брелока. Более подробную информацию см. на официальном сайте Rutoken по адресу www.rutoken.ru.

В инструкции изложены положения:

Перечень терминов и сокращений

Закрытый ключ

Уникальная последовательность символов, известная владельцу сертификата и предназначенная для создания в электронных документах электронной подписи с использованием средств электронной подписи или шифрования документов с использованием средств шифрования.

Криптопровайдер (Cryptography Service Provider, CSP)

Независимый модуль, содержащий библиотеку криптографических функций со стандартизованным интерфейсом.

Сертификат

Уникальная последовательность символов, соответствующая закрытому ключу, доступная любому пользователю информационной системы.

Центр сертификации

Организация, которая выпускает сертификаты ключей электронной подписи.

Подготовка к использованию Rutoken

Общие сведения о подготовке к использованию

Под подготовкой к использованию Rutoken подразумеваются все действия, которые необходимо выполнить для того, чтобы конкретные пользователи системы DIRECTUM имели возможность шифровать и подписывать документы ЭП с использованием Rutoken.

Подготовка к использованию Rutoken в общем случае состоит из этапов:

1. Установка Центра сертификации.
2. Установка драйверов Rutoken.
3. Генерация закрытых ключей и сертификатов.
4. Перенос закрытых ключей и сертификатов на Rutoken.
5. Регистрация сертификатов в системе DIRECTUM.

Этапы 2, 4 и 5 являются обязательными и выполняются всегда.

Этапы 1 и 3 выполняются по мере необходимости.

Этап 1 – установка центра сертификации - выполняется в том случае, если центр сертификации ранее не был установлен в организации.

Этап 3 – генерация закрытых ключей и сертификатов – выполняется в том случае, если планируется обновить существующие закрытые ключи и сертификаты или выдать закрытые ключи и сертификаты новым пользователям.

Установка центра сертификации

Установка центра сертификации описана в документе «DIRECTUM. Инструкция по установке и настройке центра сертификации», входит в комплект поставки.

Установка драйверов Rutoken

Драйверы Rutoken следует устанавливать на все компьютеры, на которых установлена клиентская часть системы DIRECTUM, и на компьютер с центром сертификации.

Для того чтобы установить драйверы Rutoken:

- войдите на компьютер от имени пользователя, обладающего правами локального администратора;
- запустите файл rtDrivers.exe. Файл находится на установочном диске Rutoken;
- следуйте инструкциям мастера установки драйверов Rutoken.

В результате на компьютер будут установлены все драйверы, необходимые для использования ключевого носителя Rutoken, сервисных утилит, а так же любых решений на основе Rutoken.

Генерация закрытых ключей и сертификатов

Способы генерации закрытых ключей для Rutoken

Генерация закрытых ключей и сертификатов выполняется на рабочем месте пользователя, ответственного за выдачу сертификатов.

Закрытые ключи и сертификаты, которые планируется хранить на Rutoken, можно генерировать двумя способами:

- в полном соответствии с общим порядком генерации закрытых ключей и сертификатов. В этом случае закрытый ключ и сертификат после генерации будут находиться в личном хранилище сертификатов пользователя, ответственного за выдачу сертификатов;
- со специализированным типом криптопровайдера «Aktiv ruToken CSP v1.0». В этом случае сертификат после генерации будет находиться в личном хранилище сертификатов пользователя, ответственного за выдачу сертификатов. Закрытый ключ будет находиться на Rutoken.

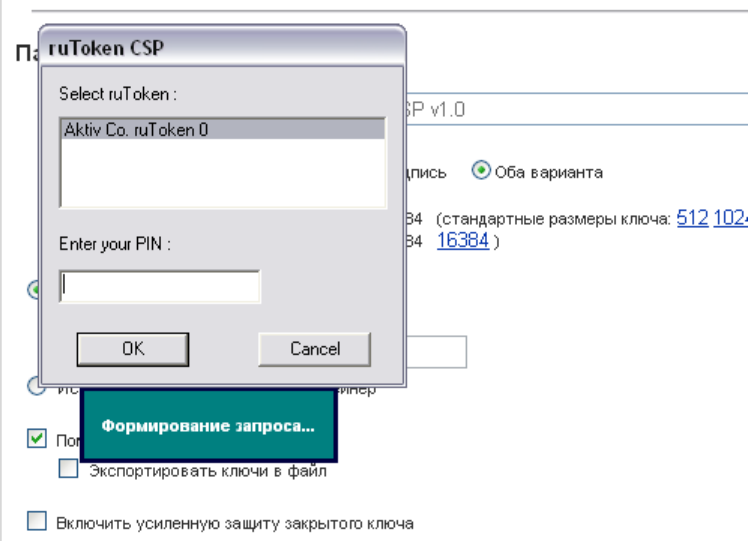
Общий порядок генерации закрытых ключей

Общий порядок генерации закрытых ключей и сертификатов описан в руководстве администратора, в главе «Инструкции администратора», в разделе «Инструкция по работе с сертификатами пользователей в системе DIRECTUM», подраздел «Генерация для пользователя закрытого ключа и сертификата».

Порядок генерации со специализированным типом криптопровайдера

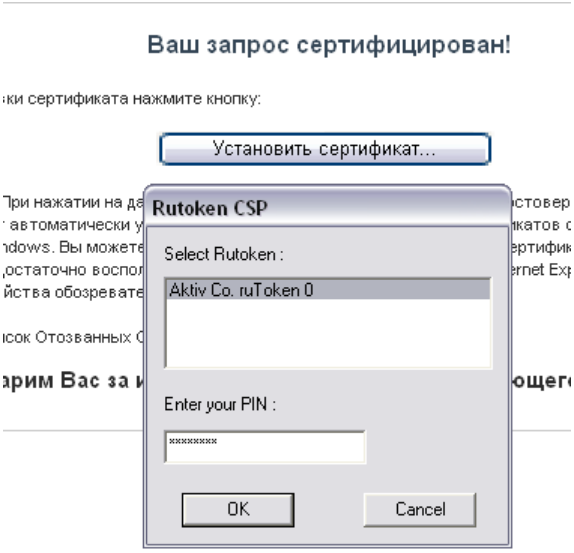
Чтобы сгенерировать закрытый ключ и сертификат со специализированным типом криптопровайдера «Aktiv ruToken CSP v1.0»:

1. Вставьте Rutoken того пользователя, для которого генерируются закрытый ключ и сертификат, в USB-порт.
2. Выполните шаги 1-7 общего порядка генерации закрытых ключей и сертификатов.
3. Выполните шаг 8 общего порядка генерации закрытых ключей и сертификатов. В выпадающем списке **CSP** вместо **Microsoft Base Cryptographic Provider v1.0** выберите значение **Aktiv ruToken CSP v1.0**. После нажатия на кнопку **Выдать запрос** на экране появится окно «ruToken CSP»:



4. Если вставлено несколько ключевых носителей Rutoken, в поле **Select ruToken** выберите тот, на который планируется занести закрытый ключ.

5. В поле **Enter your PIN** введите PIN-код доступа к выбранному Rutoken и нажмите на кнопку **OK**.
6. При установке сертификата в личное хранилище появится окно:



7. В поле **Enter your PIN** введите PIN-код доступа к выбранному Rutoken и нажмите на кнопку **OK**.

В результате будут сгенерированы закрытый ключ и сертификат. Сертификат после генерации будет находиться в личном хранилище сертификатов пользователя, ответственного за выдачу сертификатов, и на Rutoken. Закрытый ключ будет находиться на Rutoken.

Перенос закрытых ключей и сертификатов на Rutoken

Этапы переноса закрытых ключей

Перенос закрытых ключей и сертификатов на Rutoken состоит из двух этапов:

1. Экспорт закрытого ключа и/или сертификата из личного хранилища сертификатов в файлы;
2. Импорт закрытого ключа и сертификата из файла на Rutoken.

Экспорт закрытого ключа и сертификата выполняется на том компьютере, на котором находятся закрытый ключ и сертификат:

- если закрытый ключ и сертификат были только что сгенерированы, то они находятся на компьютере пользователя, ответственного за выдачу сертификатов;
- если закрытый ключ и сертификат уже использовались для шифрования и подписания документов ЭП, то они находятся на компьютере того пользователя, которому были выданы.

Импорт закрытого ключа и сертификата удобно выполнять на том же компьютере, на котором выполняется экспорт закрытого ключа. До начала переноса закрытых ключей и сертификатов на этот компьютер необходимо установить браузер сертификатов Rutoken, rtCert.exe. Файл rtCert.exe можно скачать с официального сайта Rutoken.

Варианты переноса закрытых ключей

Порядок переноса закрытых ключей и сертификатов зависит от того, где находится закрытый ключ:

- если закрытый ключ и сертификат были только что сгенерированы, и при генерации был использован специализированный тип криптопровайдера «Aktiv ruToken CSP v1.0», то закрытый ключ находится на Rutoken;
- в противном случае закрытый ключ находится в личном хранилище сертификатов.

Порядок переноса закрытого ключа

Если закрытый ключ находится в личном хранилище сертификатов, то переносить из личного хранилища на Rutoken надо закрытый ключ и сертификат. Для того чтобы перенести закрытый ключ и сертификат:

1. Войдите на компьютер, на котором находятся закрытый ключ и сертификат.
2. Экспортируйте закрытый ключ в файл *.pfx. Порядок экспорта описан в руководстве администратора, в главе «Инструкции администратора», в разделе «Инструкция по работе с сертификатами пользователей в системе DIRECTUM», подраздел «Экспорт сертификата и закрытого ключа».
3. Вставьте Rutoken того пользователя, которому были выданы закрытый ключ и сертификат, в USB-порт.
4. Откройте браузер сертификатов Rutoken из файла rtCert.exe.
5. В меню **Действия** выберите пункт **Login**. Введите пароль пользователя Rutoken.
6. В меню **Действия** выберите пункт **Импорт сертификата из файла**. Откроется окно «Импорт сертификата из файла…».
7. В поле **Имя файла** укажите имя файла *.pfx, в который был экспортирован закрытый ключ, и нажмите на кнопку **Выбрать**. Откроется окно «Импорт из файла PFX».
8. В поле **Пароль** укажите пароль для закрытого ключа, заданный при экспорте, и нажмите на кнопку **Далее.** Откроется окно «Импорт из файла PFX».
9. В поле **Имя контейнера** ведите имя контейнера, в который будут импортированы закрытый ключ. При необходимости в дальнейшем переносить ключ, пометьте его как экспортируемый, поставив галочку.
10. Нажмите на кнопку **Далее**, нажмите на кнопку **Готово**. Импорт успешно произведен.

Порядок переноса открытого ключа

Если закрытый ключ находится на Rutoken, то переносить на Rutoken надо только сертификат. Чтобы перенести сертификат:

1. Экспортируйте сертификат в файл *.cer. Порядок экспорта описан в руководстве администратора, в главе «Инструкции администратора», в разделе «Инструкция по работе с сертификатами пользователей в системе DIRECTUM», подраздел «Экспорт сертификата и закрытого ключа».
2. Вставьте Rutoken того пользователя, которому были выданы закрытый ключ и сертификат, в USB-порт.
3. Откройте браузер сертификатов Rutoken из файла rtCert.exe.
4. Выберите контейнер и в нем закрытый ключ, в который необходимо импортировать сертификат.

5. В меню **Действия** выберите пункт **Импорт сертификата из файла**.
6. В поле **Имя файла** укажите имя файла *.cer, в который был экспортирован соответствующий закрытому ключу сертификат из личного хранилища, и нажмите на кнопку **Выбрать...**.

После успешного импорта сертификата на Rutoken, удалить сертификат из личного хранилища, для этого:

1. В окне Internet Explorer в меню **Сервис** выбрать **Свойства обозревателя**, перейти на закладку «Содержание», нажать кнопку **Сертификаты...**.
2. В окне «Сертификаты»: перейти на закладку «Личные», выбрать из списка сертификат, который нужно экспортировать, нажать кнопку **Удалить**.

Регистрация сертификатов в системе DIRECTUM

Регистрация сертификатов в системе DIRECTUM выполняется на рабочем месте администратора системы DIRECTUM.

До начала регистрации сертификатов на это рабочее место необходимо установить браузер сертификатов Rutoken, rtCert.exe. Файл rtCert.exe можно скачать с официального сайта Rutoken www.rutoken.ru.

Чтобы зарегистрировать сертификат в системе DIRECTUM:

1. Войдите на компьютер с правами локального администратора.
2. Откройте браузер сертификатов Rutoken из файла rtCert.
3. Вставьте Rutoken пользователя, для которого будет регистрироваться сертификат, в USB-порт.
4. В меню **Действия** выберите пункт **Login**. Введите пароль пользователя Rutoken.
5. Выберите ключевой контейнер и закрытый ключ, из которого будет экспортироваться сертификат.
6. В меню **Действия** выберите пункт **Добавить сертификат в хранилище сертификатов**. Откроется сообщение об успешной регистрации сертификата.
7. Нажмите на кнопку **ОК.**
8. Экспортируйте сертификат в файл *.cer. Порядок экспорта описан в руководстве администратора, в инструкции по работе с сертификатами пользователей в системе DIRECTUM, в разделе «Экспорт сертификата и закрытого ключа».
9. Зарегистрируйте сертификат в компоненте **Пользователи**. Порядок регистрации описан в руководстве администратора, в инструкции по работе с сертификатами пользователей системы DIRECTUM, в разделе «Регистрация сертификатов в системе DIRECTUM».

Использование Rutoken

Общий порядок шифрования и подписания документов ЭП

Общий порядок шифрования и подписания документов ЭП описан в руководстве пользователя.

Шифрования и подписания документов ЭП с использованием Rutoken

Порядок шифрования и подписания документов ЭП с использованием Rutoken в целом совпадает с общим порядком шифрования и подписания документов ЭП. Отличия:

1. Перед тем как зашифровать или подписать документ ЭП, надо вставить Rutoken в USB-порт.
2. После выбора действия шифрования или подписания документа ЭП у пользователя запрашивается PIN-код доступа к Rutoken. После ввода PIN-кода выбранное действие выполняется обычным образом.
3. Если попытаться выполнить действие до того как в USB-порт будет вставлен Rutoken, то на экране появится запрос PIN-кода с недоступным полем ввода. В этом случае надо вставить Rutoken в USB-порт или отказаться от выполнения действия.