

Продление сертификата текущего пользователя

Для продления сертификата ключа пользователя АП (если пользователь не менялся) необходимо выполнить следующие действия:

1. В панели задач Windows нажать ПКМ по иконке Континет-АП, выбрать пункт «Сертификаты», подпункт «Создать запрос на пользовательский сертификат» (Рисунок 1).

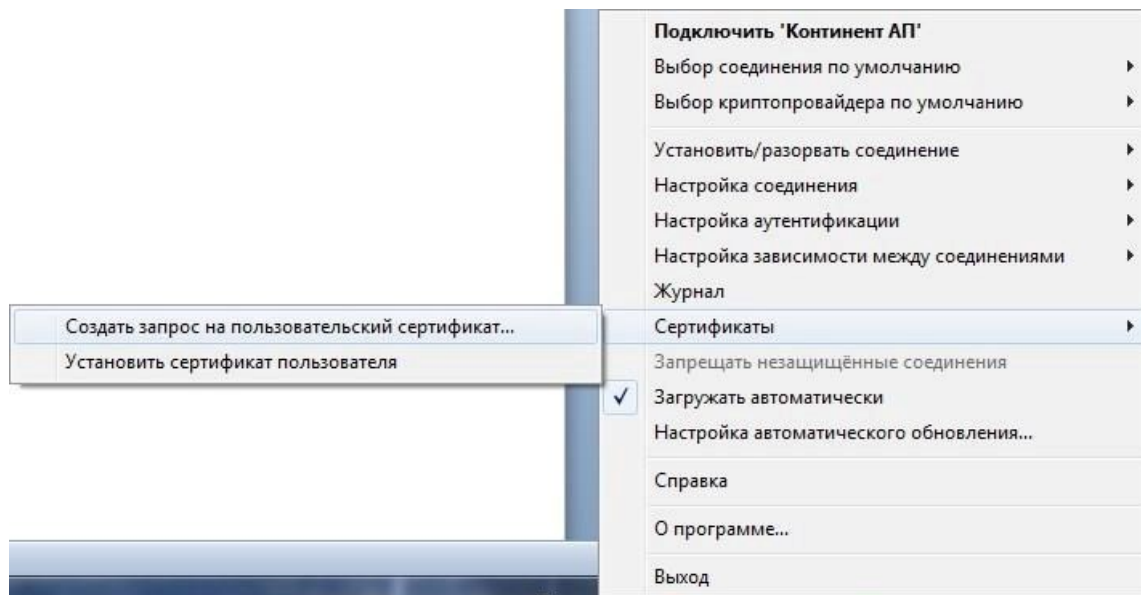


Рисунок 1 – Вызов панели создания запроса на пользовательский сертификат

2. В открывшемся окне необходимо заполнить все графы и выбрать пункт «Бумажная форма»*.

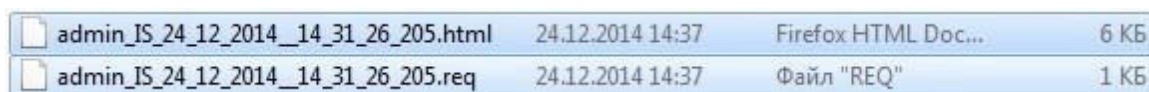
The image shows the 'Континет-АП' dialog box titled 'Параметры сертификата пользователя'. It contains several input fields: 'Имя сотрудника' (Ivanov Ivan Ivanovich), 'Описание' (Ведущий специалист), 'Организация' (ОАО Стройпром), 'Подразделение' (Планово-экономический отдел), 'Регион' (Московская область), 'Город' (Москва), 'Страна' (RU), and 'e-mail' (ivanov@stroiprom.ru). Below these are fields for 'Электронная форма' and 'бумажная форма', both pointing to a file path in the C:\Users\admin_IS\Documents folder. There are also dropdown menus for 'Криптопровайдер' (КриптоПро CSP), 'Имя контейнера' (IvanovII_02_03_2015_13_46_26_156), and 'Формат запроса' (Запрос для СД). At the bottom are 'OK', 'Отмена', and 'Подробнее <<' buttons.

Рисунок 2 - Создание запроса на пользовательский сертификат

*В случае возникновения ошибки в процессе формирования файлов запроса необходимо снять выбор пункта «бумажная форма». В этом случае, вместо отсканированной копии бумажной формы необходимо заполнить и отсканировать «Заявление на изготовление сертификата ключа пользователя АП» из стартового пакета документов (можно скачать с сайта instel.ru, раздел ИАС). В разделе «Заявление на изготовление сертификата ключа пользователя АП» в пункте «Даю согласие на изготовление ...» необходимо написать «Согласен» если ключ (RuToken) отправляется в ГК «Ростех».

3. Далее необходимо подключить ключевой носитель и выбрать соответствующий пункт в новом окне (по умолчанию: ActiveCo roToken 0). Затем задать пароль на ключевой контейнер: «12345678» (без кавычек).

4. После завершения записи по пути, указанному в пункте 2 (Рисунок 2) будут сформированы файл .req, и файл .html (либо только файл .req, если галочка «бумажная форма» была снята).



admin_IS_24_12_2014_14_31_26_205.html	24.12.2014 14:37	Firefox HTML Дос...	6 КБ
admin_IS_24_12_2014_14_31_26_205.req	24.12.2014 14:37	Файл "REQ"	1 КБ

5. Внести запись в журнал учета ключевых носителей (см. Приказ ФАПСИ от 13.06.2001 №152).

6. HTML-файл (либо вручную заполненное заявление на изготовление сертификата ключа) необходимо распечатать, подписать, поставить печать организации, отсканировать и отправить на почту helpdesk@rtinform.ru вместе с файлом.req

Через некоторое время на ваш почтовый ящик придет письмо от helpdesk@rtinform.ru с файлами сертификатов, которые нужно самостоятельно установить на АРМ пользователя с помощью Инструкции для подключения удаленных АРМ. Пункт «Установка сертификатов» (шаг 14 дорожной карты).

7. Если в организации меняется пользователь, необходимо выполнить шаг № 1 данной инструкции. Затем при создании запроса на пользовательский сертификат (шаг №2) в обязательном порядке в окне КонтинентАП убрать галочку «Бумажная форма».

Далее по инструкции следуем шагу № 3, 4, 5. После, необходимо заполнить заявку на подключение к КИС (которая находится на instel.ru), с указанием лишения прав доступа на сотрудника, который перестал работать. На нового сотрудника также заполняется заявка на подключения к КИС с указанием обоснования.

Отсканированные копии двух заявок на подключение к КИС и сформированный файл .req необходимо отправить на адрес helpdesk@rtinform.ru.

8. **Не нужно** отправлять существующий ключ Rutoken, если организация меняет одного сотрудника на другого.

9. Оригиналы заполненных заявок на подключение к КИС необходимо отправить почтой по адресу: 119048, г. Москва, ул. Усачева, д. 24, на имя директора по безопасности Митюка Михаила Юрьевича.