**СОЗДАНИЕ ЗАПРОСА НА ПОЛУЧЕНИЕ СЕРТИФИКАТА ОТКРЫТОГО КЛЮЧА АУТЕНТИФИКАЦИИ**

Запрос на получение сертификата создается пользователем средствами абонентского пункта.

Запрос в виде файла сохраняется в указанную пользователем папку, ключевой контейнер с закрытым ключом сохраняется на ключевом носителе, указанном в настройках.

**Для создания запроса на получение сертификата:**

1. Зайдите на официальный сайт УФК по Омской области в раздел ГИС\Удостоверяющий центр\Инструкции и разъяснения\Установка СКЗИ «Континент-АП».

2. Скачайте Шаблон печати «Континента-АП» (файл request.xsl).

3. Замените файл request.xsl, расположенный в директории:

C:\Program Files\Security Code\Terminal Station\vpn,

скачанным ранее (см. п. 2) файлом (копирование с заменой)

4. Вызовите контекстное меню пиктограммы абонентского пункта, расположенной на панели задач Windows.

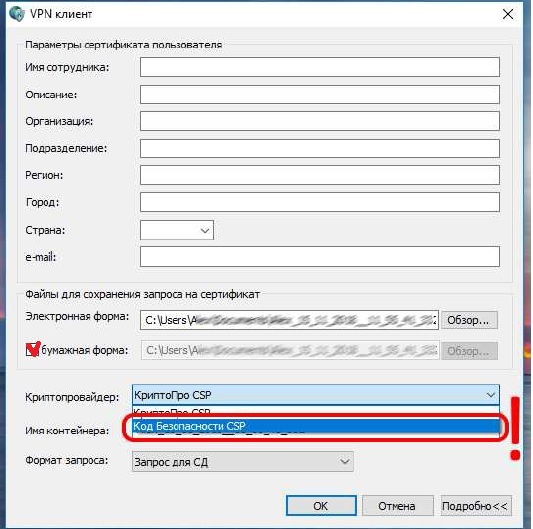
5. В меню "Сертификаты" активируйте команду «Создать запрос на пользовательский

сертификат».

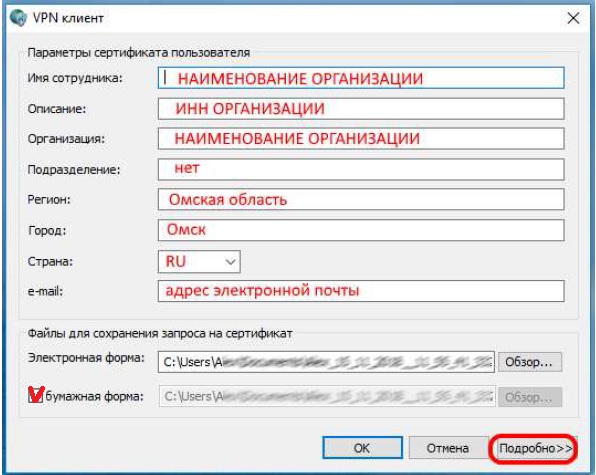
5.1. .,На экране появится диалоговое окно для создания запроса. Необходимо нажать на кнопку

**Подробно>>**

Укажите в качестве крипторпровайдера Код безопасности CSP.



5.2. Необходимо заполнить форму (выделено красным)



После заполнения всех необходимых полей (как на приведенном выше примере) нажмите

кнопку **OK**.

Криптопровайдер приступит к созданию закрытого ключа. Необходимо выполнить следующие операции:

• сформировать закрытый ключ с помощью датчика случайных чисел;

• выбрать тип ключевого носителя для записи закрытого ключа;

• ввести пароль для ограничения доступа к ключевому контейнеру.

Следуйте указаниям, появляющимся на экране.

Нажмите кнопку **OK** в окне сообщения для завершения процедуры создания запроса.

6. Откройте сформированную форму для печати текстовым редактором (например, Microsoft Word) и заполните ее следующим образом:



7.Передайте созданный файл запроса (с расширением .req), распечатанный и подписанный запрос в УФК по Омской области.

**Регистрация сертификата**

1. После обработки файла запроса УФК по Омской области предоставляет два файла:

- сертификат для связи с сервером доступа (имя файла совпадает с наименованием организации);

- корневой сертификат на котором выпущен сертификат для связи с сервером доступа (имя файла - CA-ROOT52\_КВ.cer)

2. Для регистрации сертификатов:

1. Вызовите контекстное меню пиктограммы абонентского пункта, расположенной на панели задач Windows.

2. В меню **Сертификаты** активируйте команду **Установить сертификат пользователя**.

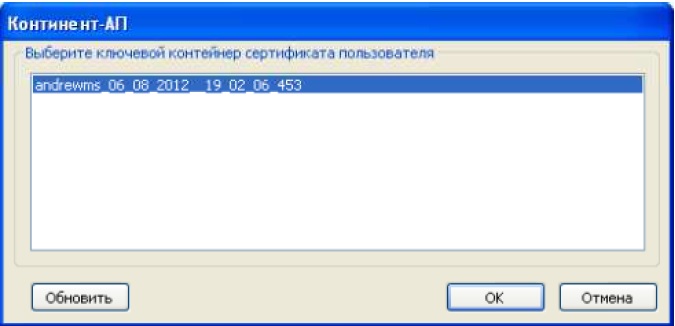
На экране появится стандартное диалоговое окно Windows для работы с файлами.

3. Выберите файл сертификата *\*\*наименование организации\*\**.cer и нажмите кнопку **Открыть**.

На экране появится диалог выбора ключевого контейнера для чтения закрытого ключа сертификата пользователя.

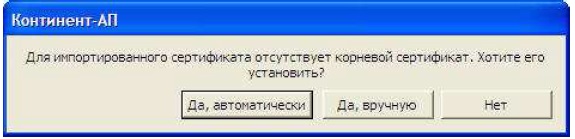
4. Вставьте в устройство ключевой носитель и нажмите кнопку **Обновить**.

В диалоге появится список ключевых контейнеров.



5. Выберите нужный ключевой контейнер и нажмите кнопку **ОК**. На экране появится запрос пароля доступа к выбранному ключевому контейнеру. Заполните поля диалога и нажмите кнопку **ОК**.

6. На экране появится запрос на установку корневого сертификата.

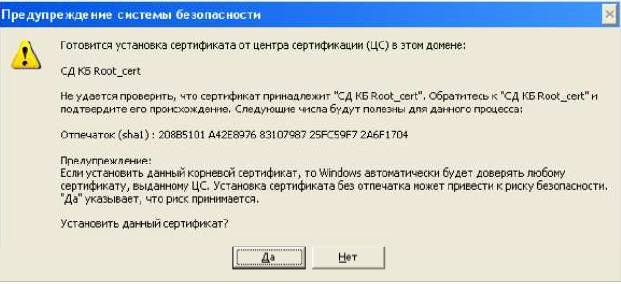


7. Для регистрации корневого сертификата нажмите кнопку:

• **Да, автоматически** — в случае если корневой сертификат хранится в одной папке с сертификатом пользователя. Будет выполнен автоматический поиск сертификата. Если корневой сертификат не будет найден, пользователю будет предложено самостоятельно указать расположение корневого сертификата.

• **Да, вручную** — в случае если корневой сертификат и сертификат пользователя хранятся в разных папках. Пользователю будет предложено самостоятельно указать расположение корневого сертификата.

На экране появится сообщение системы безопасности Windows о том, что сейчас будет выполнена регистрация корневого сертификата.



8. Нажмите кнопку **Да**.

На экране появится сообщение об успешном завершении импорта пользовательского сертификата.

9. Нажмите кнопку **ОК**.