

Настройка клиента Континент TLS с установленным Крипто ПРО

1. Установка Клиента TLS

Требуется установить на ОС Windows ПО Континент TLS Клиент версии 2.0.1482.0. Дистрибутив может быть скачен с официального сайта https://www.securitycode.ru/download_center/?section=downloads&product=Континент%20TLS&version=Клиент%202.0 предоставлен администратором ИБ.

Запустите файл **Континент TLS-клиент.exe** (распаковав архив), поставьте галочку «Я принимаю условия лицензионного соглашения» и нажмите кнопку **Установить**. Сохраните все открытые вкладки и документы и нажмите кнопку **Перезагрузить**.

Регистрация Континет TLS Клиент

Программа необходимо зарегистрировать для ведение журналов учета СКЗИ. Регистрация проводится онлайн с указанием достоверных сведений, после регистрации будет предоставлен регистрационный код и сняты ограничения с программы

2. Выпуск сертификата пользователя

При запуске ПО Клиента TLS отобразится окно, в котором требуется выбрать меню Управления сертификатами (рисунок 1). Требуется нажать на кнопку «Создать запрос».

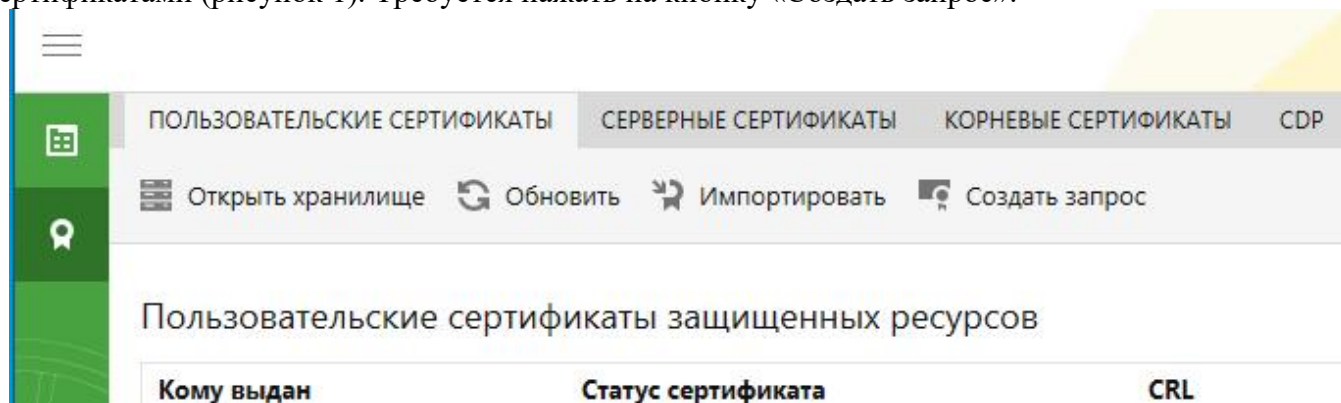


Рисунок 1

Отобразится окно параметров запроса сертификата. Пример настроек указан на рисунке 2.

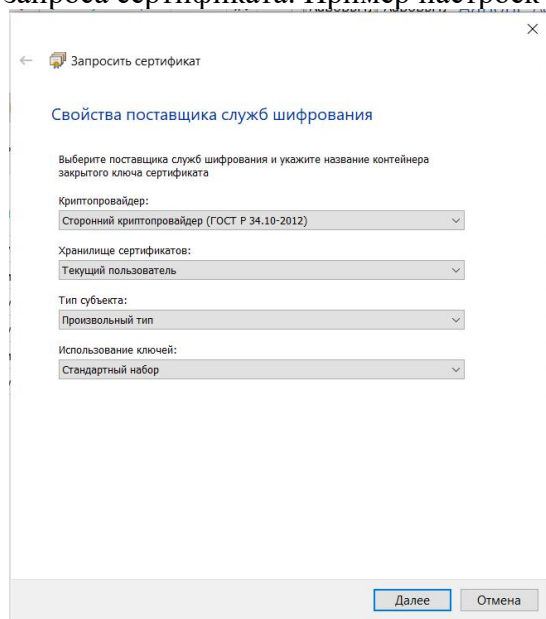


Рисунок 2

На следующем этапе необходимо заполнить запрос (рисунок 3), обязательно необходимо заполнить поля: **общее имя (ФИО полностью), Организация, Подразделение, Должность, Область.**

В запросе не должно быть специальных символов «\», «/», «'» и «'»!

Запросить сертификат

Параметры сертификата пользователя

Заполните обязательные поля для выпуска запроса сертификата пользователя. В полях должны быть указаны полные официальные названия без сокращений.

Фамилия: Имя Отчество:

Общее имя:

Организация:

Подразделение:

Должность:

Страна: Область:

Населенный пункт:

Адрес:

Электронная почта:

ИНН: СНИЛС:

ОГРН:

Рисунок 3

На следующем этапе требуется выбрать формат «base64», место сохранения запроса (рисунок 4).

Место запроса необходимо запомнить для отправки его на выпуск сертификата!

Запросить сертификат

Имя файла

Имя ключевого контейнера:

Имя файла для запроса сертификата:

Формат файла:
☒ Base64
☐ Двоичные данные

Бланк запроса на сертификат:
☐ Подготовить бланк запроса на сертификат

Рисунок 4

Далее, требуется выбрать место хранения закрытого ключа (рекомендуется использовать Рутокен или реестр Windows). Так же, необходимо сгенерировать случайную последовательность чисел, для этого нужно перемещать курсор в разные стороны (рисунок 6). После завершения операции мастер предложит создать пароль для контейнера закрытого ключа. Требуется ввести пароль длиной 8 символов или более (рисунок 6).

Пароль контейнера необходимо запомнить, он необходим для использования сертификата!

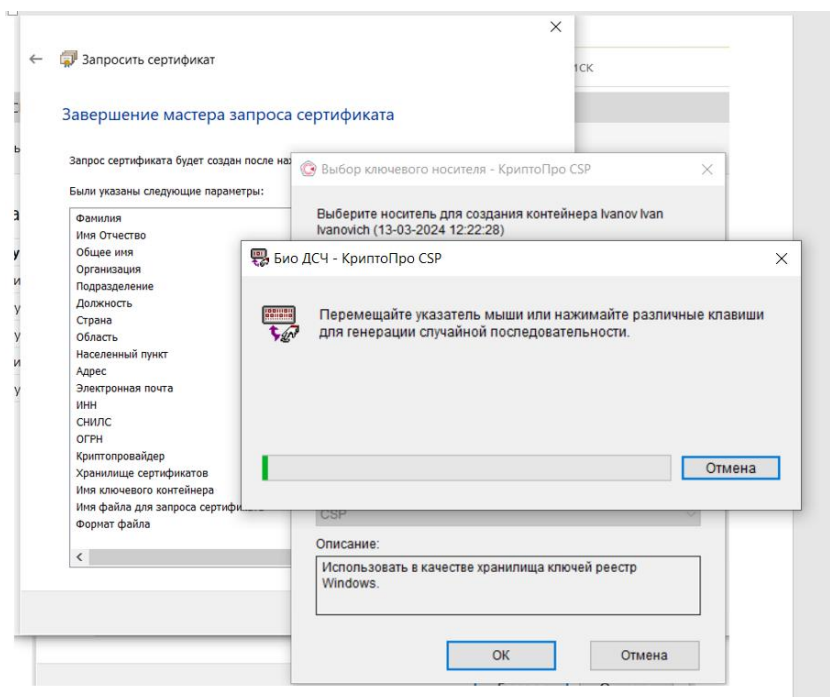


Рисунок 5

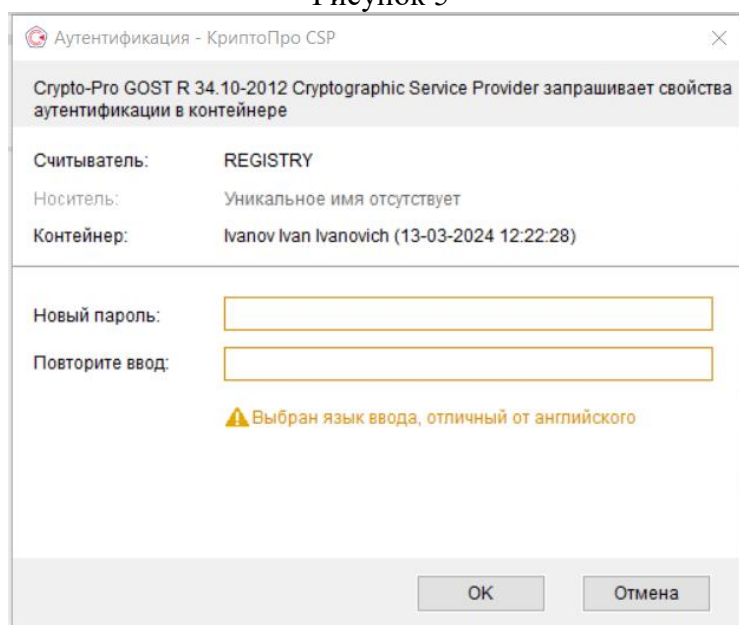


Рисунок 6

После ввода требуемых параметров отобразится окно успешного создания запроса на сертификат. Файл запроса на сертификат требуется передать администратору ИБ. Передача запроса сертификата осуществляется направлением письма на почту rwec@rwec.ru в теме указать «Выпуск сертификатов «наименование организации»», в письме указать ФИО и E-Mail сотрудника(-ов).

3. Установка сертификата пользователя

Администратор ИБ направляет следующие файлы на указанный адрес сотрудника для установки на TLS Клиенте:

- Сертификат пользователя, выпущенный по файлу запроса;
- Корневой сертификат УЦ;
- Сертификат TLS сервера;
- Файл CRL (списка отзыва).

Необходимо зайти в КриптоПро CSP через меню Пуск (рисунок 7).

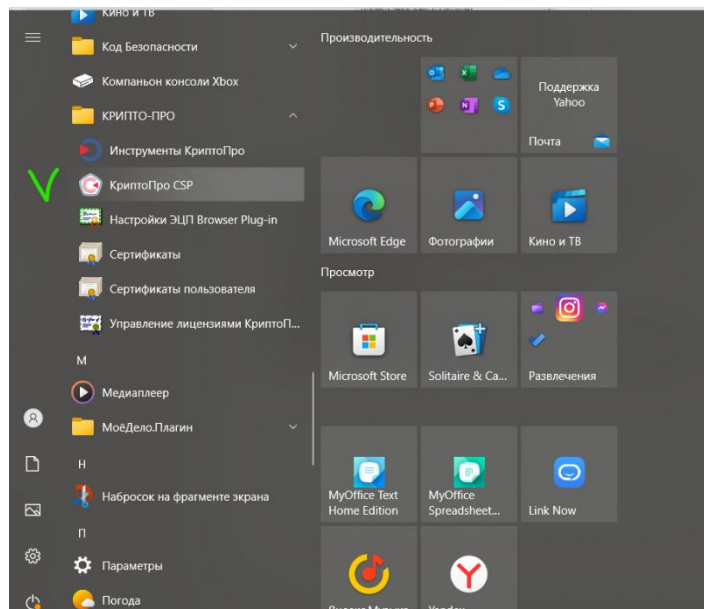


Рисунок 7

Перейти в раздел «Сервис» и «Установить личный сертификат» (рисунок 8).

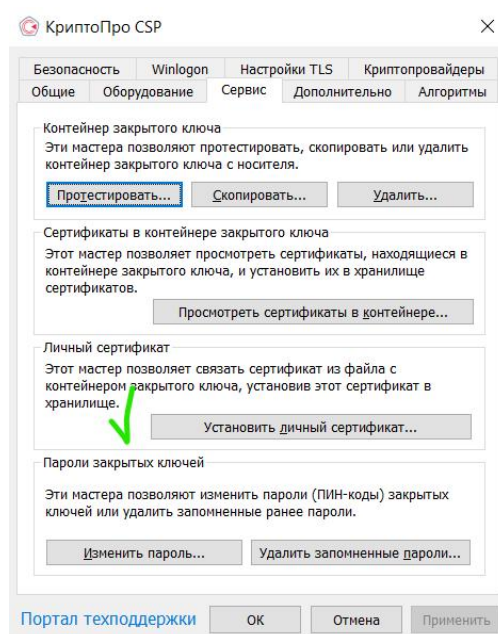


Рисунок 8

Выбрать полученный пользовательский сертификат (Рисунок 9).

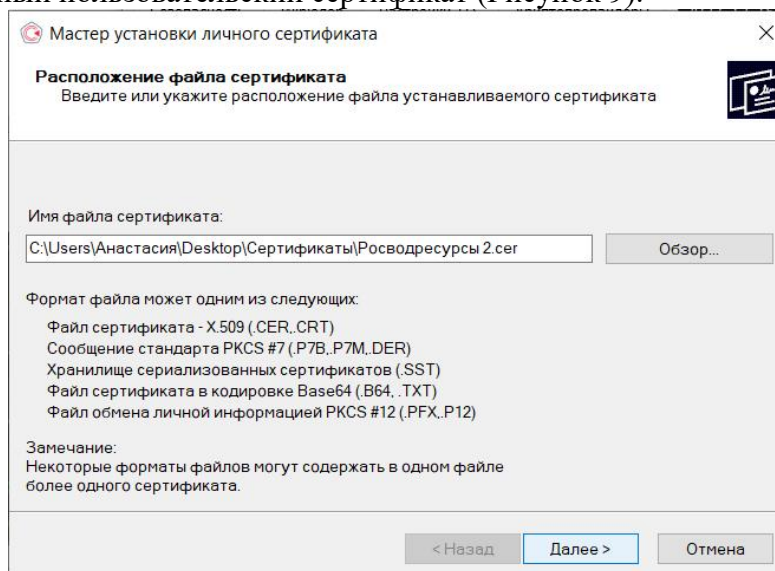


Рисунок 9

На шаге «Сертификат для установки» нажимаем «Далее» (рисунок 10).

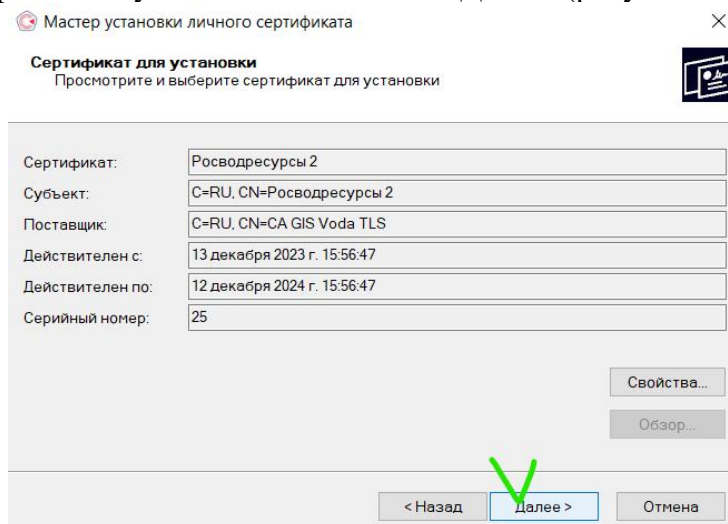


Рисунок 10

Далее нужно выбрать контейнер, который соответствует сертификату (рисунок 11).

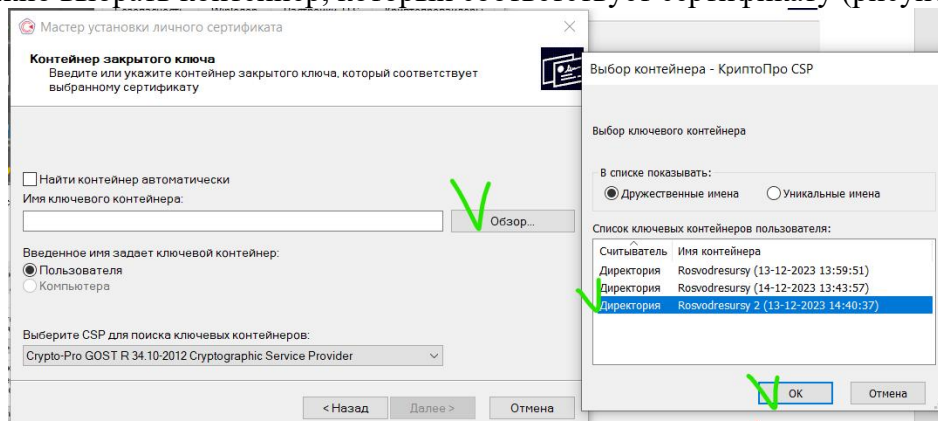


Рисунок 11

Пользовательский сертификат установлен. Нажимаем «Готово» (рисунок 12).

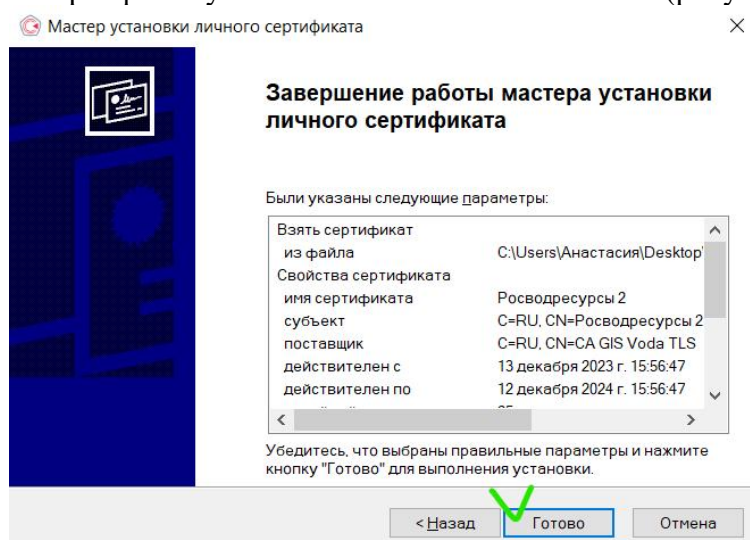


Рисунок 12

4. Установка серверного и корневого сертификата

В разделе «Серверные сертификаты» импортируется файл «_favr.ru.cer», в разделе «Корневые сертификаты» импортируется «CA GIS Voda TLS.cer». На вкладке CDP, выбрать импорт CRL (список отзыва сертификатов) (рисунок 13).

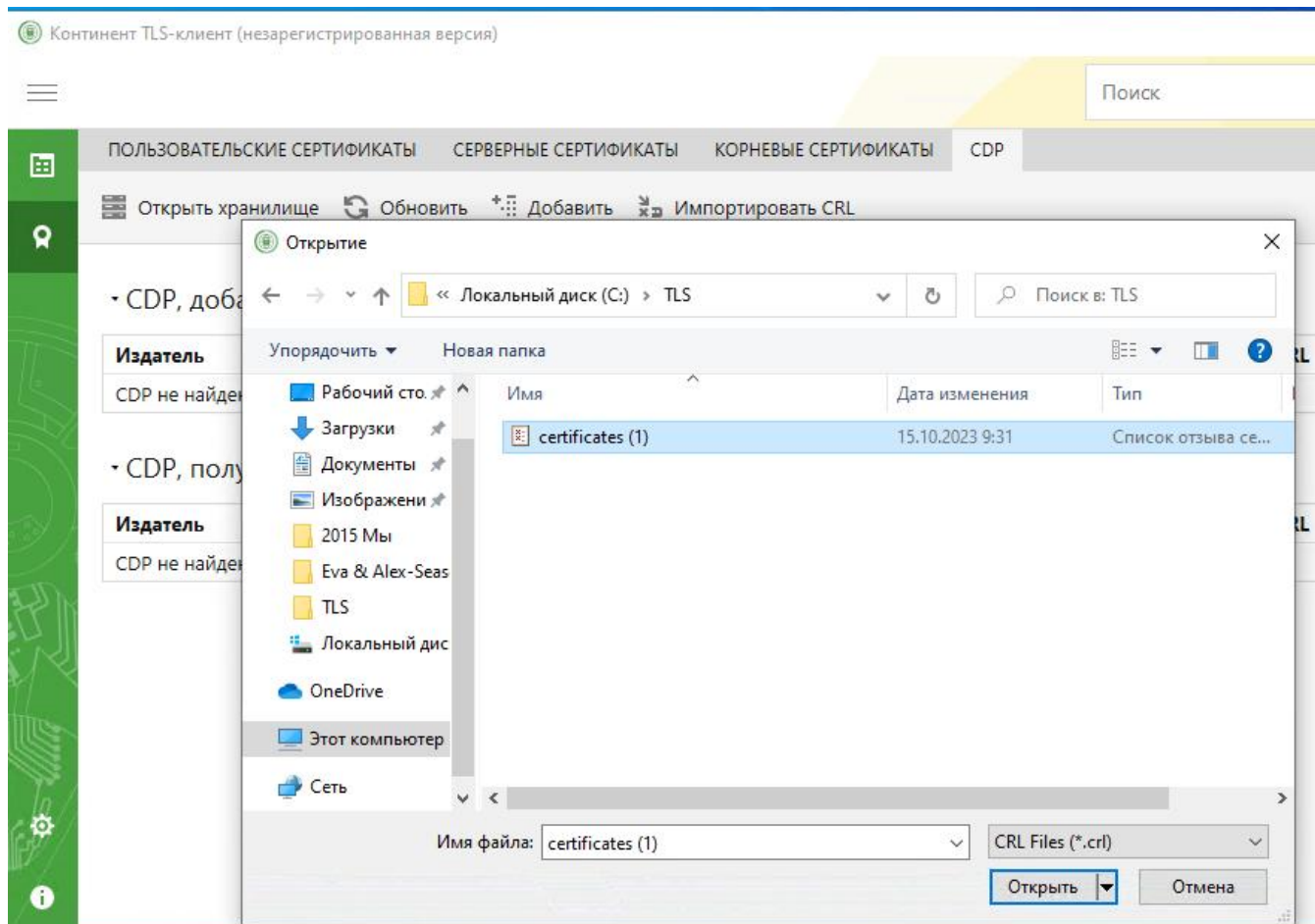


Рисунок 13

Выбрать файл «certificates.crl», полученный от администратора ИБ и загрузить его в Клиент TLS. Отобразится окно успешной загрузки (рисунок 14).

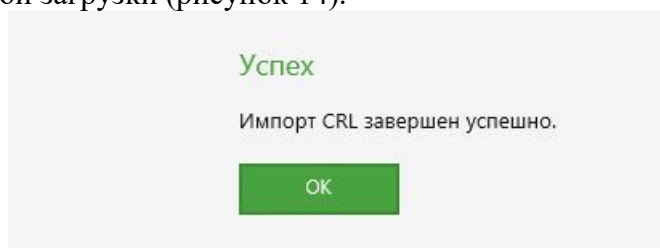


Рисунок 14

Для автоматического обновления CRL, можно добавить CDP и указать адрес «tls.favr.ru/certificates.crl»

5. Проверка сертификатов

В Клиенте TLS требуется перейти во вкладки «Пользовательские сертификаты», «Серверные сертификаты», «Корневые сертификаты». Все загруженные сертификаты должны иметь статус Действителен (рисунок 15).

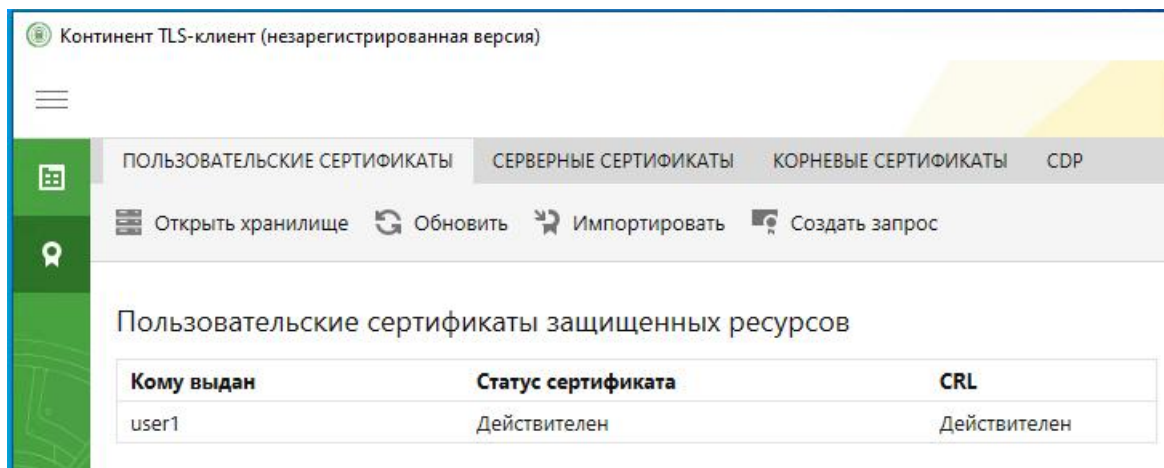


Рисунок 15

6. Настройка подключения к Серверу TLS

В меню «Главная» требуется нажать «Добавить / Ресурс». В открывшемся окне требуется указать имя сервера «*sslgis.favr.ru*». Параметры настройки указаны на рисунке 16 и сохранить. После сохранения в браузере будет доступен закрытый контур ГИС ЦП Вода <https://sslgis.favr.ru/>.

Редактирование ресурса

Адрес:

sslgis.favr.ru

Имя ресурса:

sslgis.favr.ru

Порт ресурса:

443

Тип:

Прокси

Стандартный порт:

☒

Локальный порт:

443

Описание:

Стартовая страница:

☐

Сохранить

Отменить

Рисунок 16