**Инструкция**

**по выпуску тестовых сертификатов TLS**

**Тестового Удостоверяющего Центра**

**ООО ”КРИПТО-ПРО” ГОСТ 2012**

Оглавление

[1 Требования перед началом работы 4](#_Toc140506884)

[2 Регистрация и авторизация 6](#_Toc140506885)

[3 Описание процесса выпуска TLS-сертификата 8](#_Toc140506886)

Настоящая инструкция описывает порядок изготовления и сохранения новых сертификатов пользователя Тестового Удостоверяющего Центра ООО «КРИПТО-ПРО» ГОСТ 2012 и предназначена для пользования неограниченным кругом лиц.

Программный комплекс «КриптоПро УЦ 2.0» представляет собой интегрированный набор служб и средств администрирования для создания и развертывания приложений, применяющих криптографическую защиту информации с сертификатами открытых ключей, а также для управления сертификатами открытых ключей.

Разработчиком КриптоПро УЦ 2.0 является ООО «Крипто-Про», специализирующееся в области разработки и внедрения криптографических средств защиты информации, а также предоставлении услуг удостоверяющего центра.

Обмен информацией с Удостоверяющим Центром осуществляется с использованием защищенного протокола TLS.

По всем вопросам, связанным с КриптоПро УЦ 2.0, следует обращаться на <https://support.cryptopro.ru/>

# Требования перед началом работы

*Важно! Все требования данного пункта должны быть последовательно выполнены до начала работы с сайтом Тестового Удостоверяющего Центра, расположенным по адресу* [*http://testca2012.cryptopro.ru/UI/*](http://testca2012.cryptopro.ru/UI/)*.*

Предварительно, на компьютере требуется установить необходимое программное обеспечение. Краткая инструкция по установке доступна на странице <http://testca2012.cryptopro.ru/UI/Default.aspx>:

1. Установить СКЗИ КриптоПро CSP: версию 5.0 можно [скачать бесплатно](https://www.cryptopro.ru/products/csp) с ознакомительной полнофункциональной 90-дневной лицензией или [купить](https://www.cryptopro.ru/products/csp);
2. Установить КриптоПро ЭЦП Browser [plug-in](https://www.cryptopro.ru/products/cades/plugin);
3. Скачать и установить [корневой сертификат](http://testca2012.cryptopro.ru/cert/rootca.cer) тестового Удостоверяющего центра в хранилище «Доверенные корневые центры сертификации»;
4. Скачать и установить [промежуточный сертификат](http://testca2012.cryptopro.ru/cert/subca.cer) тестового Удостоверяющего центра в хранилище «Промежуточные центры сертификации».
5. Использовать браузер с поддержкой ГОСТ TLS, например: chromium-gost, Internet Explorer, Яндекс.Браузер, Microsoft Edge (в режиме Internet Explorer) и др.
6. Для работы браузеров отличных от IE, установить расширение для Chrome-подобных браузеров или Яндекс.Браузера.

Необходимо [проверить](https://www.cryptopro.ru/sites/default/files/products/cades/demopage/cades_bes_sample.html) работу КриптоПро ЭЦП Browser plug-in в вашем браузере. Диагностика должна быть пройдена успешно, и сертификат от Тестового Удостоверяющего Центра установлен в хранилище (см. Рисунок 1).

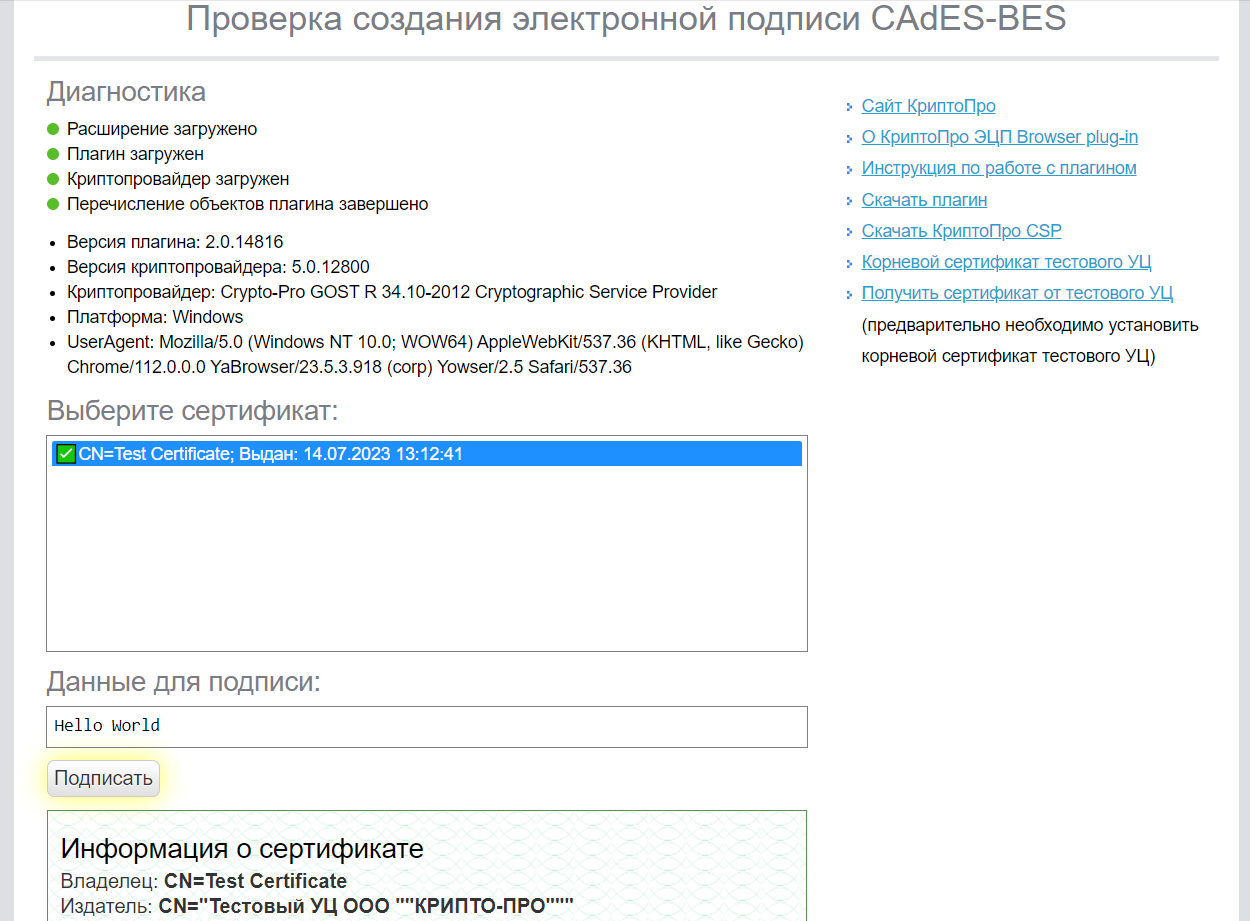


Рисунок 1. Проверка создания электронной подписи

# Регистрация и авторизация

*Важно! К регистрации и авторизации следует переходить только после того, как необходимое программное обеспечение из п. 1 будет установлено на компьютер. Страницы авторизации и регистрации будут недоступны до установки необходимого программного обеспечения.*

Для начала работы необходимо перейти на сайт <https://testca2012.cryptopro.ru/UI/Default.aspx>.

Если вход осуществляется впервые, следует нажать на кнопку «Регистрация» и перейти на страницу <https://testca2012.cryptopro.ru/UI/1/RegRequest.aspx> для создания новой учетной записи. На форме регистрации необходимо указать данные нового пользователя. Для начала работы с Тестовым Удостоверяющим Центром достаточно заполнить отмеченные значком астериск \* обязательные поля. Для выпуска TLS-сертификатов обязательно заполнение пункта «Список полных имён DNS», - можно указывать как полное DNS-имя, так и wildcard, например, \*.ebs.ru. (см. Рисунок 2).

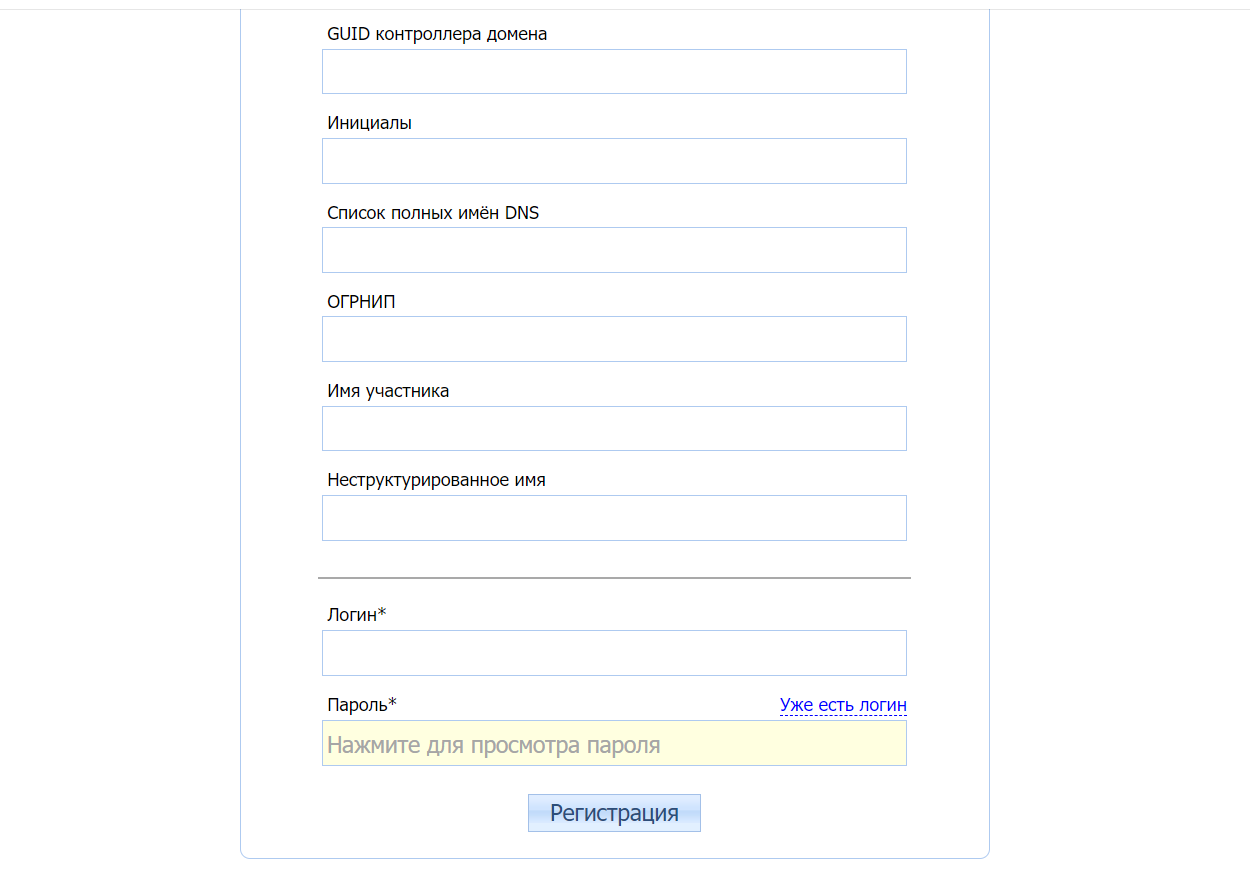


Рисунок 2. Форма регистрации пользователя

Если учетная запись уже существует, следует нажать на кнопку «Вход в личный кабинет» и авторизоваться на странице <https://testca2012.cryptopro.ru/UI/1/Login.aspx>, под имеющимися логином и паролем (см. Рисунок 3).

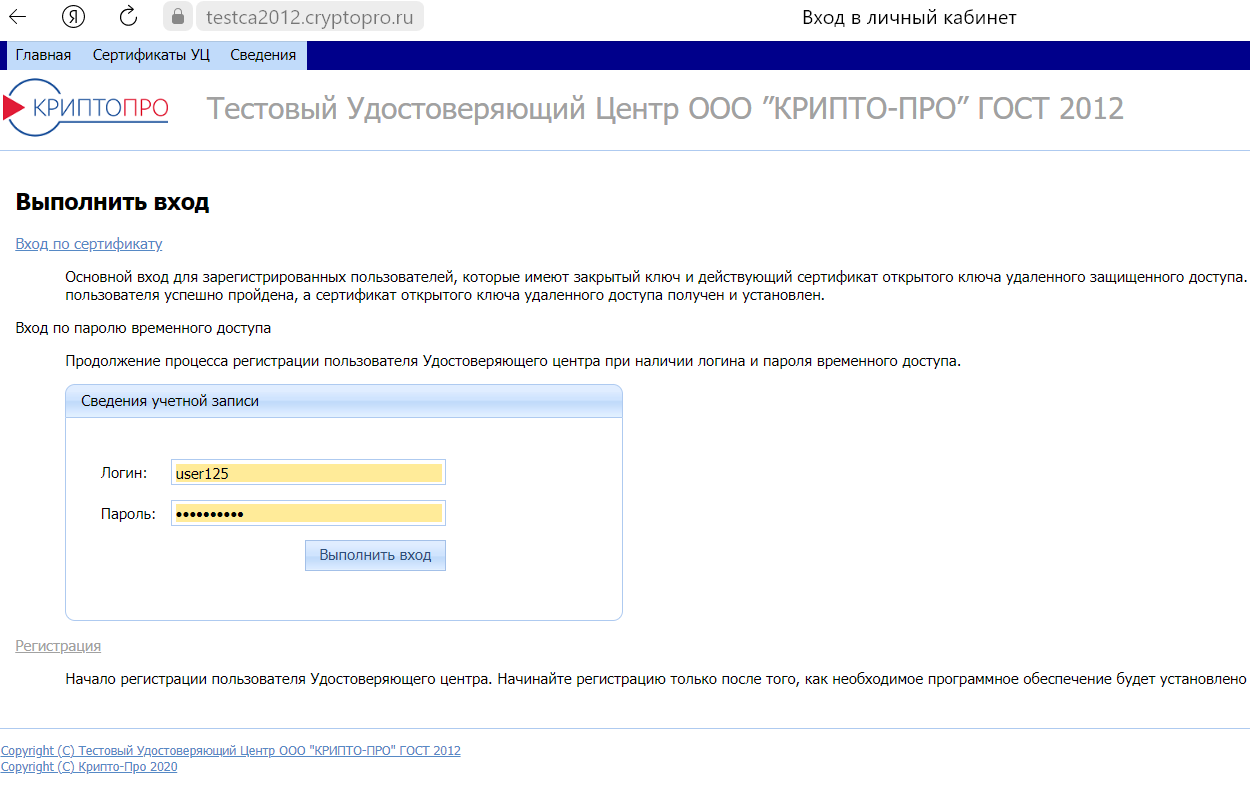


Рисунок 3. Вход для зарегистрированных пользователей

После авторизации откроется интерфейс личного кабинета в Тестовом Удостоверяющем Центре, где в разделе «Журнал» отобразятся все происходившие действия с сертификатами, с возможностью быстрого перехода к событию при нажатии на кнопку «Перейти» (см. Рисунок 4).

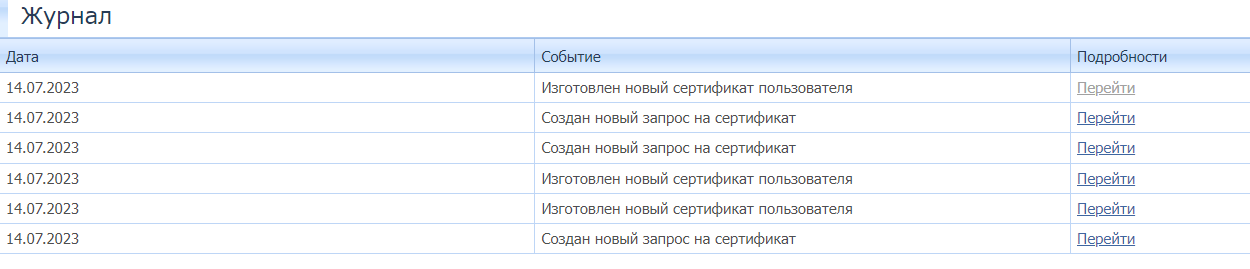


Рисунок 4. Журнал событий

# Описание процесса выпуска TLS-сертификата

Для выпуска нового TLS-сертификата следует после авторизации перейти в интерфейсе личного кабинета в раздел меню «Сертификаты». По клику на вкладку «Создать» будет инициирован запрос на создание нового сертификата (см. Рисунок 5).

Следует разрешить в появившемся всплывающем окне выполнение операции с ключами или сертификатами от имени пользователя. Далее в выпадающих списках появятся опции выбора шаблона сертификата и опции выбора криптопровайдера. Также можно выбрать для чего будет использоваться ключ: подписи, шифрования или подписи и шифрования (по умолчанию отмечено «подписи и шифрования»). Опционально можно ввести какой-либо комментарий.

Выберите в выпадающем списке шаблона опцию «Тестовый сертификат Веб-сервера», оставьте остальные поля по умолчанию и нажмите на кнопку «Создать».

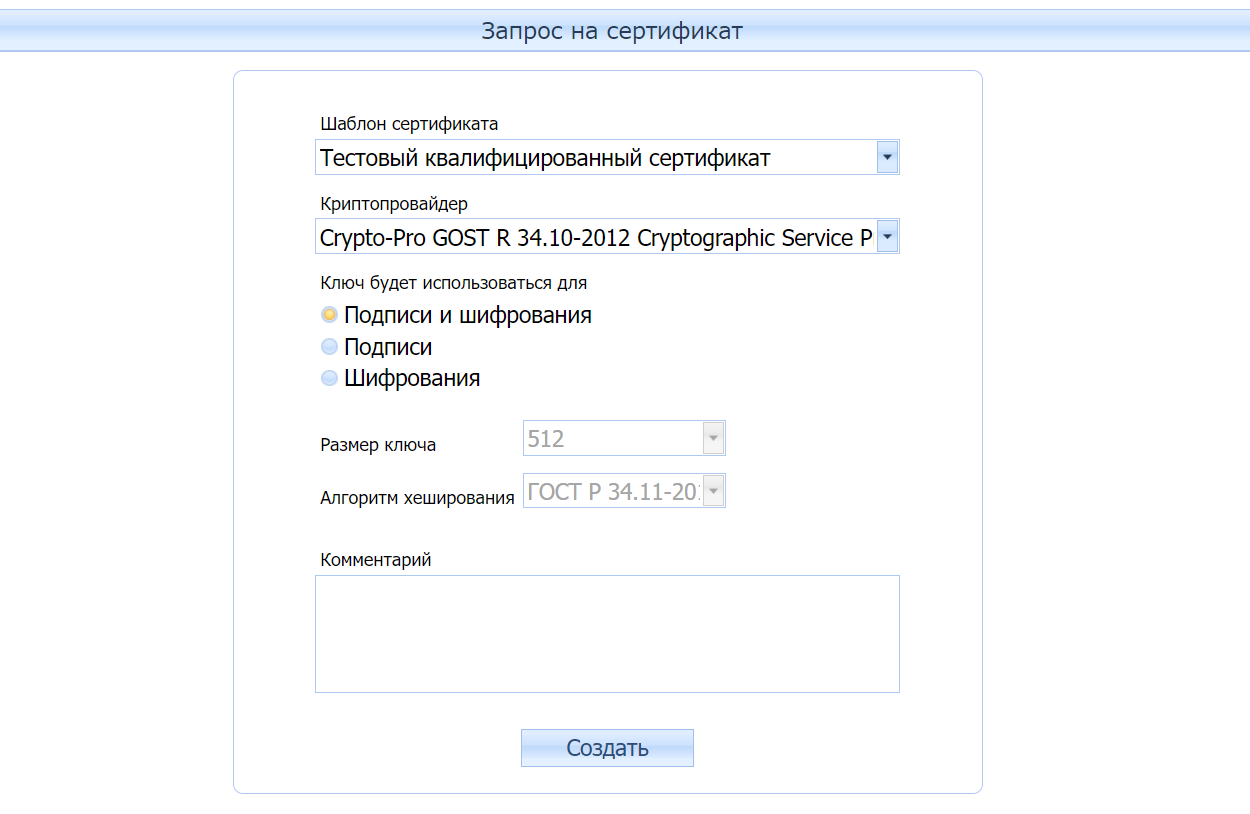


Рисунок 5. Форма запроса на сертификат

Выберите носитель для создания контейнера для ключа. По умолчанию контейнеры создаются в реестре Windows. Можно выбрать «Директория» – в этом случае ключ сохранится в файловой системе компьютере на жестком диске, либо съемный носитель, предварительно вставив USB-накопитель, – и контейнер ключа будет сохранен на него.

В течение нескольких секунд будет проходить процесс генерации запроса, который можно ускорить если следовать рекомендации в диалоговом окне перемещать указатель мыши или нажимать различные клавиши для генерации случайной последовательности (см. Рисунок 6).

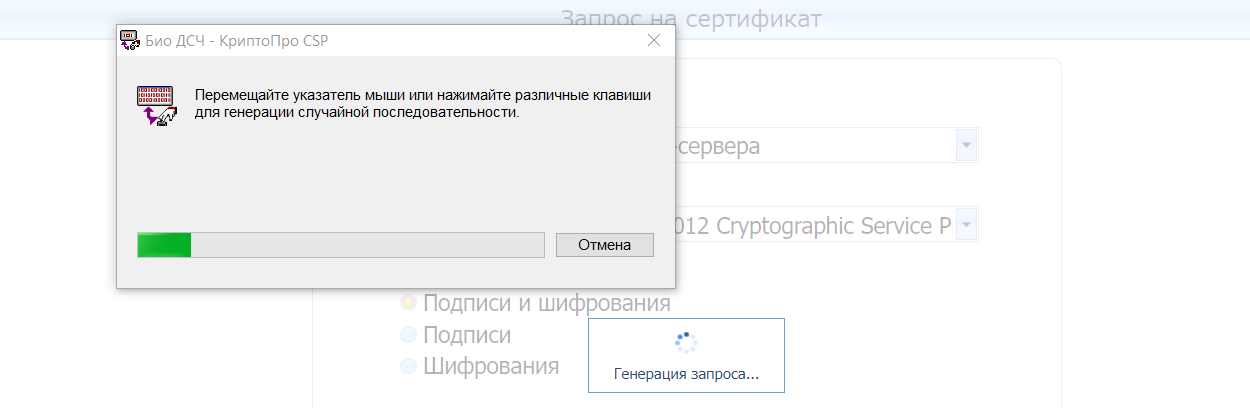


Рисунок 6. Генерация запроса

По завершении процесса появится окно установки пароля на контейнер (см. Рисунок 7). Придумайте и введите его и нажмите на кнопку «ОК».

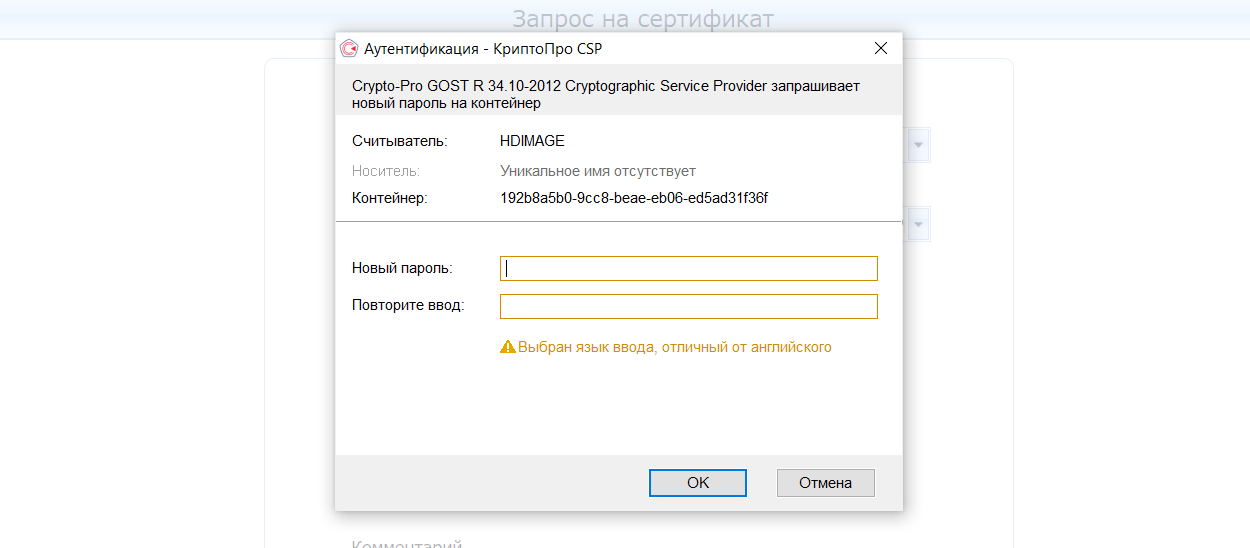


Рисунок 7. Установка пароля на контейнер

В списке запросов в разделе меню «Запросы» отобразятся выполненные запросы на сертификат (см. Рисунок 8).

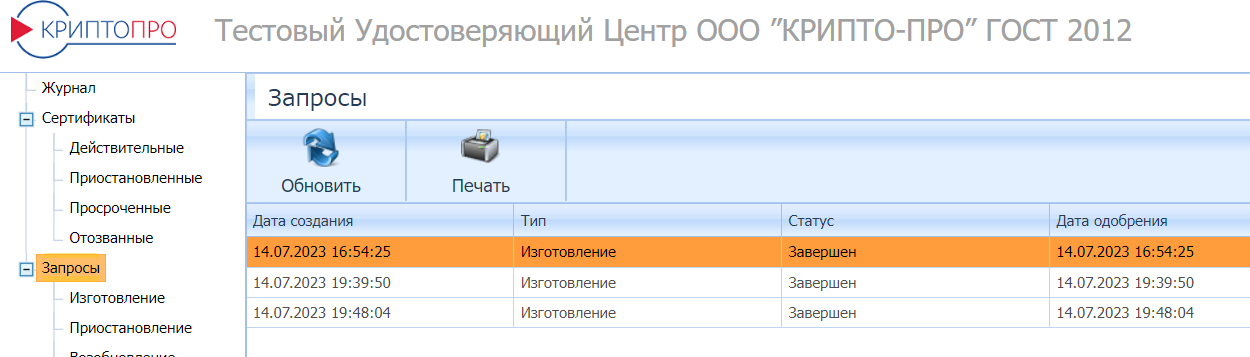


Рисунок 8. Список запросов

В списке запросов в разделе меню «Сертификаты» отобразятся открытые ключи сертификатов, с возможностью скачивания на локальный компьютер в директорию «Загрузки» по ссылке «Скачать» в правой колонке «Файл». (см. Рисунок 9).

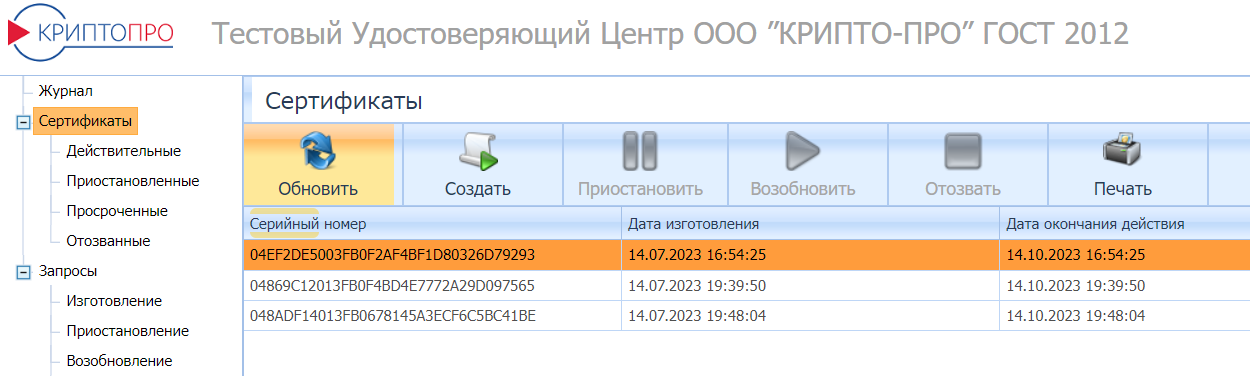


Рисунок 9. Список сертификатов