

## Настройка модуля

### Получение ключей в формате CryptoPro (ГОСТ)

В соответствии с протоколом обмена с ЕСИА запрос должен быть подписан электронной подписью в формате ГОСТ, для этого понадобится контейнер, содержащий закрытый ключ в формате CryptoPro и сертификат. Для промышленной среды ЕСИА эту пару вы должны получить в аккредитованном УЦ.

### Генерация ключей для тестовой среды

Для тестовой среды эту пару можно сгенерировать в тестовом УЦ компании «КриптоПро»: <https://testca2012.cryptopro.ru/ui/Default.aspx> (для доступа требуется браузер, поддерживающий ГОСТ TLS, например Яндекс.Браузер или Chromium-ГОСТ). На машине, с которой вы отправляете запрос, должно быть установлено ПО CryptoPro CSP версии 5 (<https://www.cryptopro.ru/products/csp>).

**Важно! При регистрации заполните форму до поля «Должность» включительно, а также СНИЛС, ОГРН, ИНН ЮЛ и КПП. иначе выпущенный с этими данными сертификат может быть отклонён при его регистрации в тестовом контуре ЕСИА.**

Общее имя*	<input type="text"/>
Фамилия	<input type="text"/>
Имя и отчество	<input type="text"/>
Страна/регион	Российская Федерация <input type="button" value="v"/>
Область	<input type="text"/>
Город	<input type="text"/>
Адрес	<input type="text"/>
Организация	<input type="text"/>
Подразделение	<input type="text"/>
Должность или звание	<input type="text"/>
ОГРН	<input type="text"/>

---

После бесплатной регистрации зайдите в личный кабинет и запросите выпуск сертификата, следуйте инструкциям УЦ. **При выборе типа запрашиваемого сертификата – выбирайте КЭП.**

Скриншот веб-интерфейса «КРИПТОПРО Тестовый Удостоверяющий Центр ООО "КРИПТО-ПРО" ГОСТ 2012». Вкладка «Запрос на сертификат».

Шаблон сертификата: Тестовый квалифицированный сертификат

Криптопровайдер: Crypto-Pro GOST R 34.10-2012 Cryptographic Service Provider

Ключ будет использоваться для:

- Подписи и шифрования
- Подписи
- Шифрования

Размер ключа: 512

Алгоритм хеширования: ГОСТ Р 34.11-2012 256

Комментарий: [пустое поле]

Кнопка: Создать

При сохранении закрытого ключа – сохраните его на диск. В результате у вас на диске должна появиться директория, содержащая закрытый ключ в формате CryptoPro (набор файлов с расширением key).

Скриншот веб-интерфейса «КРИПТОПРО Тестовый Удостоверяющий Центр ООО "КРИПТО-ПРО" ГОСТ 2012». Вкладка «Запрос на сертификат».

Диалог «Выбор ключевого носителя - КриптоПро CSP»:

Выберите носитель для создания контейнера cbf31f262-0ef7-a66a-ca97-8258137e8c8

- Реестр
- Директория
- Диск Z
- Диск G
- Диск E

Недоступные для данной операции: [пустое поле]

Тип приложения: CSP (14800980\_79037909334)

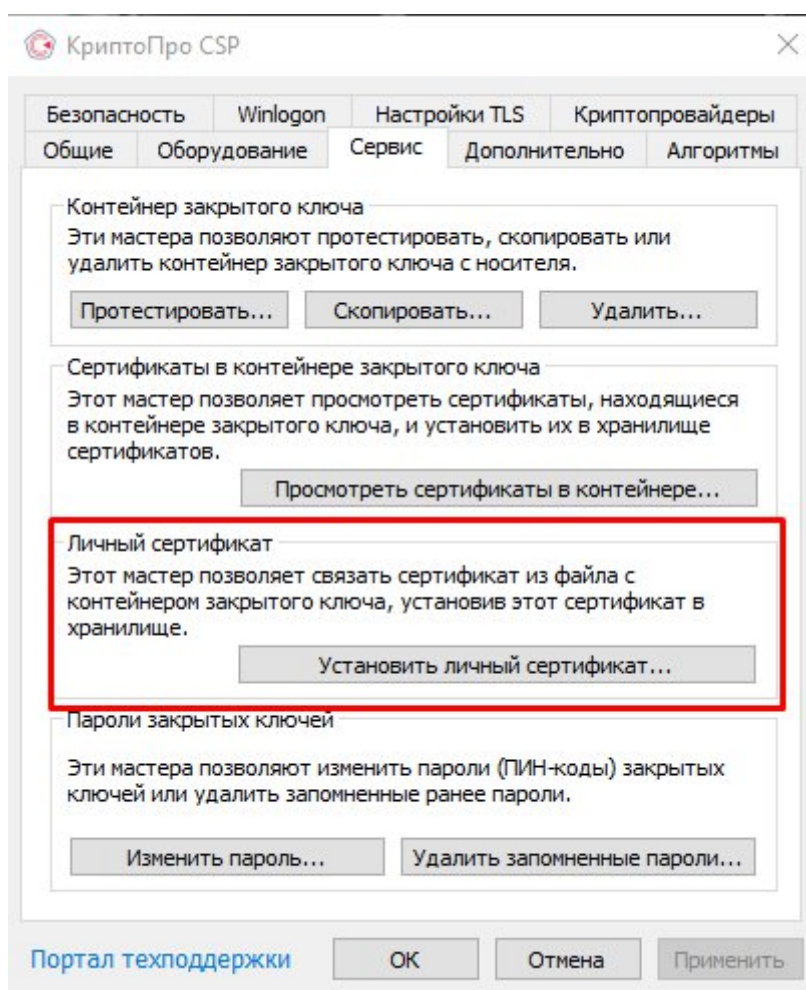
Описание: Использовать для хранения ключей съемный диск.

Кнопки: ОК, Отмена

Фон: Видно часть формы «Запрос на сертификат» с теми же полями, что и в первом скриншоте.

Имя	Дата изменения	Тип	Размер
header.key	04.03.2024 16:01	Файл "KEY"	1 КБ
masks.key	04.03.2024 16:01	Файл "KEY"	1 КБ
masks2.key	04.03.2024 16:01	Файл "KEY"	1 КБ
name.key	04.03.2024 16:01	Файл "KEY"	1 КБ
primary.key	04.03.2024 16:01	Файл "KEY"	1 КБ
primary2.key	04.03.2024 16:01	Файл "KEY"	1 КБ

Скачайте сформированный по вашему запросу сертификат и с помощью CryptoPro CSP запишите его в этот контейнер.



Также с помощью CryptoPro CSP найдите и скопируйте идентификатор закрытого ключа – это понадобится при настройке модуля через административный интерфейс Keycloak.



## Проверка настроек в личном кабинете ЕСИА

В соответствии с руководством по работе с ЕСИА войдите в личный кабинет ЕСИА, найдите в списке свою организацию и в ней информационную систему, для которой вы настраиваете доступ, введите в список разрешённых URL адрес сервера, на котором вы установили ваш экземпляр Keycloak.

После этого добавьте полученный от УЦ сертификат в список сертификатов информационной системы.