



Удостоверяющий центр «ITCOM»

Генерация КЭП

Руководство по процедуре генерации квалифицированной электронной подписи с помощью приложения УЦ «Айтиком»

Оглавление

1. Перед началом генерации.....	4
2. Установка приложения	5
3. Предоставление доступа.....	6
4. Установка КриптоПРО CSP	7
5. Установка драйвера для токена.....	8
6. Формирование запроса на сертификат.....	10
7. Запись сертификата на ключевой носитель.....	13

ОСНОВНЫЕ ПОНЯТИЯ

КСКПЭП – квалифицированный сертификат ключа проверки электронной подписи.

КЭП – квалифицированная электронная подпись.

Криптопровайдер – средство защиты криптографической защиты информации. Программа с помощью которой генерируется закрытая часть электронной подписи и которая позволяет производить работу с электронной подписью. Данная галочка проставляется автоматически.

Экспортируемый ключ – возможность копирования электронной подписи на другой носитель. При отсутствии галочки копирование электронной подписи будет невозможно.

ЛКМ – левая кнопка мыши.

ПКМ – правая кнопка мыши.

CRM-AGENT – приложение, разработанное специалистами УЦ для упрощения процедуры генерации ключевой пары, создания запроса и записи сертификата.

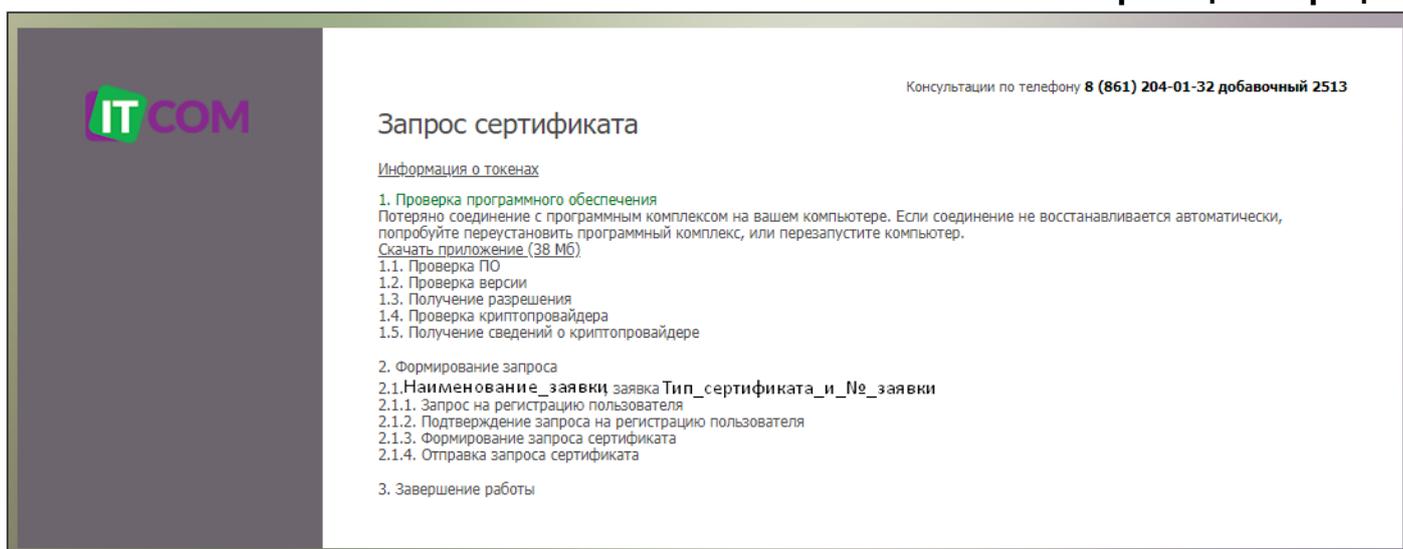
1. Перед началом генерации

После посещения удостоверяющего центра и прохождения процедуры сверки личности, на указанную Вами в заявлении электронную почту, УЦ прислал письмо, содержащее ссылку для генерации. Если Вы не получали письма, обратитесь к Вашему менеджеру или в Техническую поддержку УЦ по контактному номеру из этого руководства.

Откройте ссылку для генерации из письма в одном из рекомендуемых браузеров: [Google Chrome](#), [Mozilla Firefox](#), [Yandex.Браузер](#). Если Вы уже находитесь в одном из вышеперечисленных браузеров, кликните по ссылке **ЛКМ** или **ПКМ** > «Открыть ссылку в новой вкладке». Страница генерации (Рис.1) откроется в новом окне.

При открытии ссылки, появится первоначальное предупреждение. Ознакомьтесь с ним, если для хранения КЭП вы используете носитель **Jacarta LT**. Подробнее о носителях в [Таблице 1](#) ниже. Если используете иной носитель, то нажмите кнопку «**Закреть**».

Рис.1 – Страница генерации



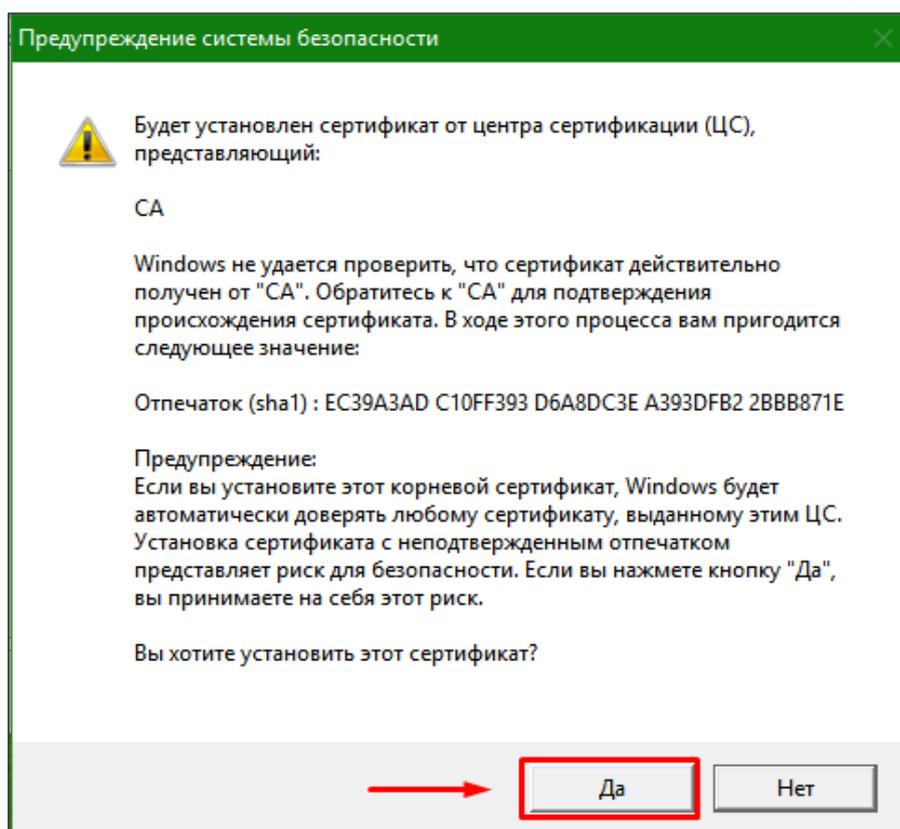
2. Установка приложения

Нажмите на ссылку «**Скачать приложение**» для начала загрузки. Если ничего не произошло после нажатия, кликните по ссылке **ПКМ** > «**Открыть ссылку в новой вкладке**». После скачивания приложения запустите установку.

Рекомендуется отключить антивирусное ПО перед загрузкой программы!

В процессе установки приложения «**crm-agent**» появится сообщение с запросом доступа (Рис.2).

Рис.2 – Запрос доступа

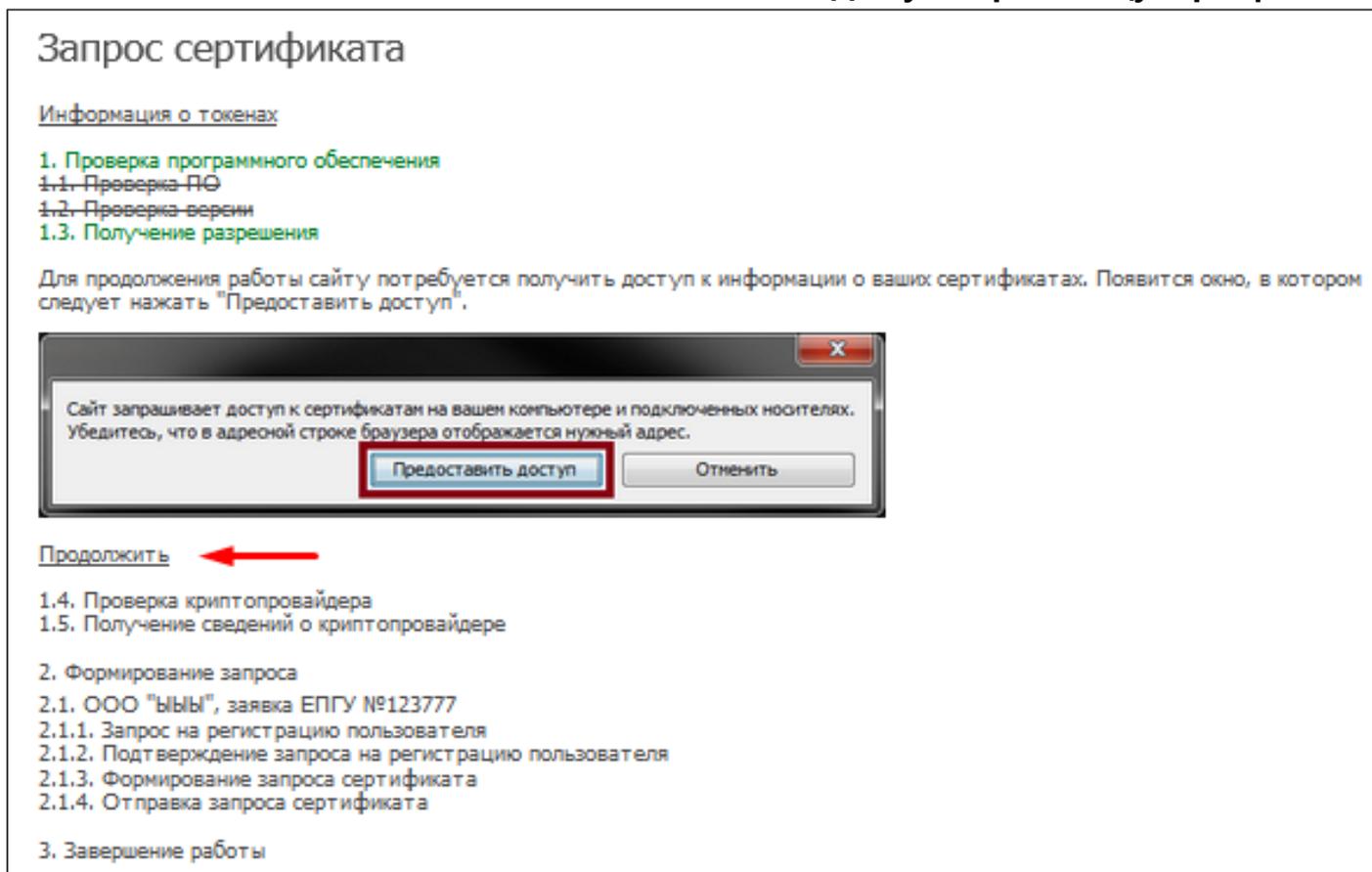


Нажмите кнопку «**Да**».

3. Предоставление доступа

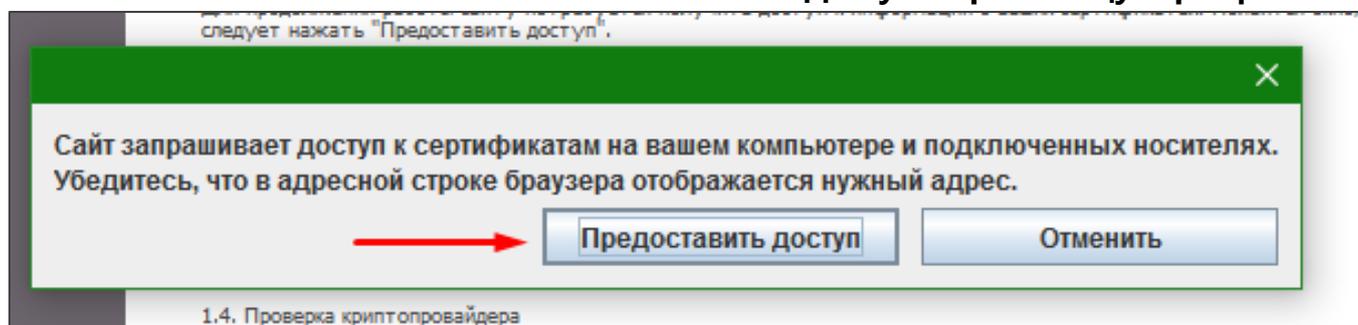
После окончания установки приложения вернитесь на страницу с генерацией. Появится сообщение о «Предоставлении доступа» (Рис.3).

Рис.3 – Доступ к хранилищу сертификатов



Нажмите «Продолжить» и, в появившемся окне, «Предоставить доступ» (Рис.4).

Рис.4 – Доступ к хранилищу сертификатов 2



Если не появилась кнопка «Продолжить»

Если после установки приложения «**crm-agent**», ссылка на скачивание приложения не исчезла, причиной может быть блокировка подключения вашей системой безопасности.

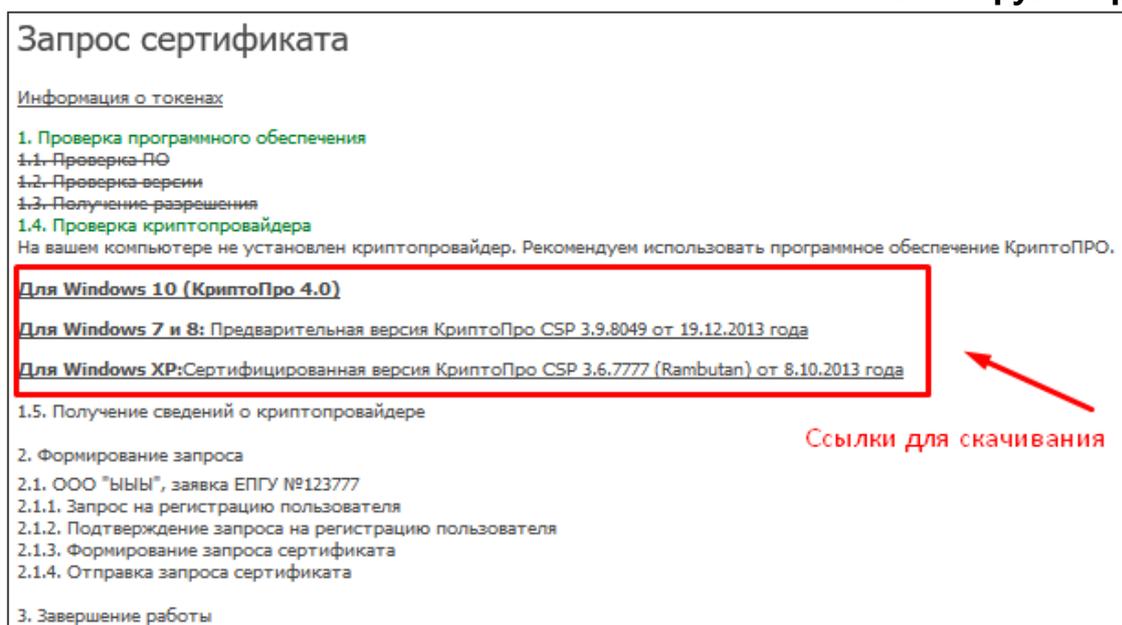
Для устранения ситуации необходимо:

- 1) Отключить антивирус, установленный на вашем компьютере;
- 2) Открыть новую вкладку в браузере;
- 3) Ввести в адресную строку браузера адрес без пробелов - **127.0.0.1:90** – и перейти (нажать **Enter** на клавиатуре);
- 4) При появлении сообщения браузера «**Ваше подключение не защищено**», добавьте страницу в исключения браузера. Например, Chrome: «**Дополнительные**» - «**Все равно перейти на сайт**». Для остальных браузеров воспользуйтесь соответствующей инструкцией разработчика.
- 5) После появления сообщения об ошибке, вернитесь на страницу с генерацией и повторите **Пункт 2** данной инструкции.

4. Установка КриптоПРО CSP

В случае, если у вас отсутствуют предустановленные криптопровайдеры, после этапа предоставления доступа появятся ссылки для скачивания КриптоПРО (Рис.5).

Рис.5 – Загрузка КриптоПРО



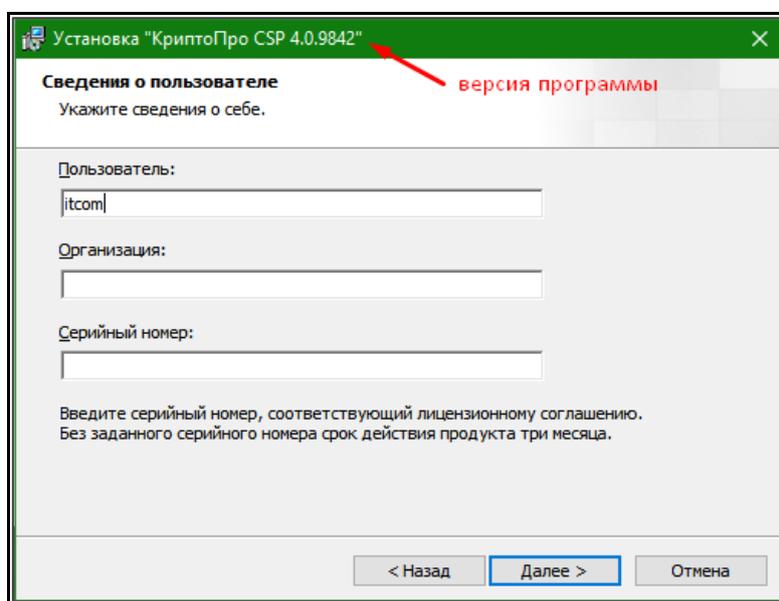
Это важно: приложение «**crm-agent**» обнаруживает любые криптопровайдеры на компьютере, и, если у Вас установлена отличная от **КриптоПРО CSP** программа (например, **VipNET CSP**), свяжитесь со специалистами технической поддержки УЦ для консультации.

Нажмите на ссылку «**КриптоПРО 4.0**» на странице генерации или на аналогичную ссылку ниже для загрузки файла установки КриптоПРО на компьютер.

- [КриптоПро CSP 4.0 – версия для ОС Win 7 / 8 / 10](#)

После окончания загрузки откройте zip-архив с помощью соответствующей программы-архиватора (например, **Win-RAR**). Внутри будет сам файл установки КриптоПРО. Запустите его и установите с параметрами по умолчанию. В процессе установки у Вас может появиться следующее окно:

Рис.5 – Установка КриптоПРО



Пропустите окно, нажав «**Далее**». Установка КриптоПРО завершена.

5. Установка драйвера для токена

Подписи можно хранить в реестре компьютера, на обычных флеш-накопителях и на специальных usb-токенах. Список токенов, пин-коды и ссылки на ПО представлены в таблице ниже (Таблица 1).

Таблица 1 – Драйверы для защищенных носителей

Тип USB-носителя	Внешний вид USB-носителя	Ссылка на загрузку драйверов	PIN-код
ruToken		Драйверы Рутокен для Windows	12345678
eToken		Драйверы eToken для Windows	1234567890
JaCarta LT		Единый клиент JC	1234567890
MSKey		MSKey Driver	11111111
Esmart		ESMART PKI Client	12345678
JaCarta LT Nano JaCarta ГОСТ JaCarta S/E		Единый клиент JC	ГОСТ 0987654321 PKI 11111111

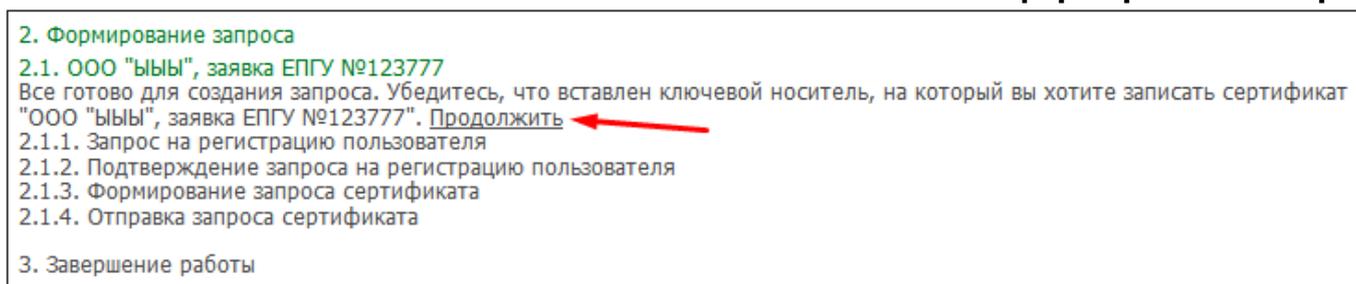
Визуально определите ваш носитель.

Для работы с одним из этих носителей необходимо установить драйвер. Перейдите по соответствующей ссылке, скачайте драйвер и установите его на компьютер. Установку драйвера проводите с параметрами по умолчанию.

6. Формирование запроса на сертификат

Теперь Вы можете приступать к формированию запроса на сертификат. На экране у вас появится сообщение об этом (Рис.6). Нажмите кнопку **«Продолжить»** для начала формирования запроса.

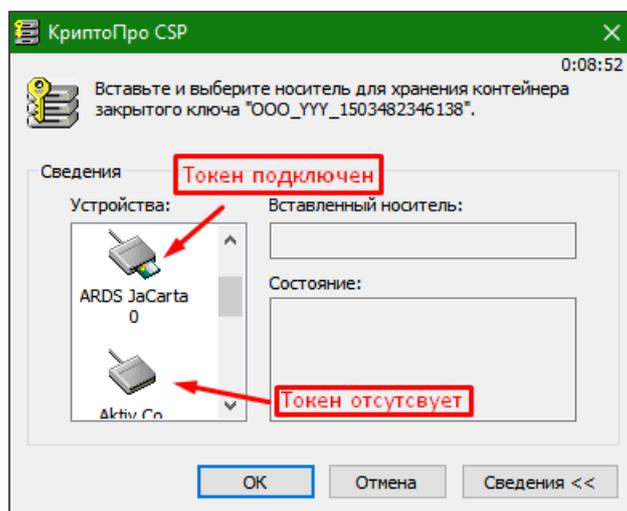
Рис.6 – Начало формирования запроса



Откроется дополнительное окно с предложением выбрать, куда записать КЭП (Рис.7). Есть возможность выбрать в качестве носителя:

- 1) **Реестр** – хранилище «внутри» компьютера;
- 2) **Диск {X}** – обычный флэш-накопитель;
- 3) **ARDS JaCarta 0, Activ Co Rutoken 0** и т.п. – защищенный токен.

Рис.7 – Выбор носителя

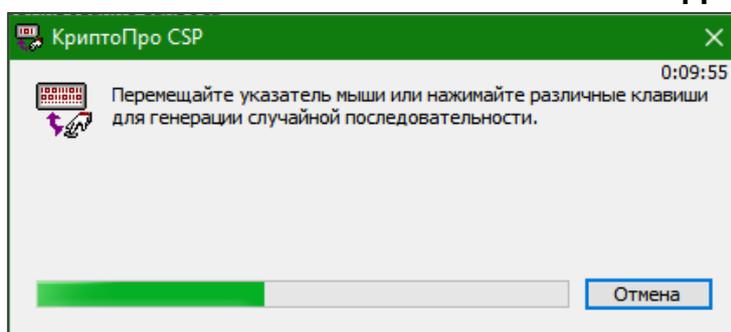


Передвигая ползунок, выберите носитель для хранения КЭП и нажмите **«ОК»**. Если был выбран **«Реестр»**, то система в дальнейшем предупредит о возможном риске. Продолжите, если Вы осознанно выбрали реестр в качестве носителя для КЭП. Если случайно, то повторите формирование запроса повторно.

Это важно: в качестве хранилища КЭП для электронных торговых площадок можно использовать **только** защищенный носитель — токен. Если нет токена или драйвер установлен, но сам токен не работает, то свяжитесь со специалистами технической поддержки УЦ для консультации.

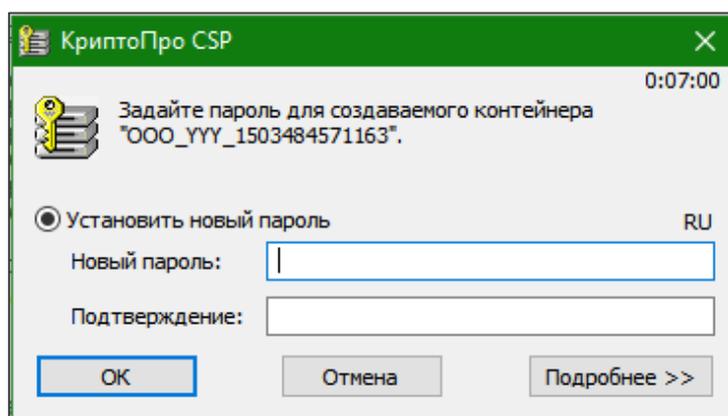
После выбора носителя откроется окно генерации «**Датчик случайных чисел**» (Рис.8). Для заполнения шкалы необходимо быстро и часто нажимать на цифровые клавиши на клавиатуре или передвигать мышь в пределах окна. Может потребоваться повторить процедуру несколько раз.

Рис.8 – Датчик случайных чисел



По окончании процесса откроется окно с предложением задать пароль (Рис.8) для контейнера, если был выбран обычный флеш-накопитель или реестр. Рекомендуется не задавать пароль и пропускать данный пункт нажатием кнопки «**ОК**» без ввода и подтверждения пароля.

Рис.8 – Ввод пароля



Если вы выбрали в качестве носителя токен, тогда необходимо ввести pin-код. Стандартные pin-коды носителей указаны в Таблице 1 выше. Выбрать токен для хранения и пройти датчик случайных чисел может потребоваться дважды, так как на данный момент выпускается две аналогичные КЭП: по старому ГОСТ 2001 и по новому ГОСТ 2012.

Это важно: количество попыток ввода pin ограничено и, если pin введен неверно несколько раз, то носитель может быть заблокирован. В таком случае, свяжитесь со специалистами технической поддержки УЦ для консультации.

При успешном завершении генерации появится следующее (Рис.9) сообщение:

Рис.9 – Завершение генерации

3. Завершение работы

Запрос сертификата отправлен! Теперь запрос будет одобрен в нашем Удостоверяющем Центре, после чего вы сможете получить свой сертификат. Отслеживать статус заявки можно, просто [обновив страницу](#).

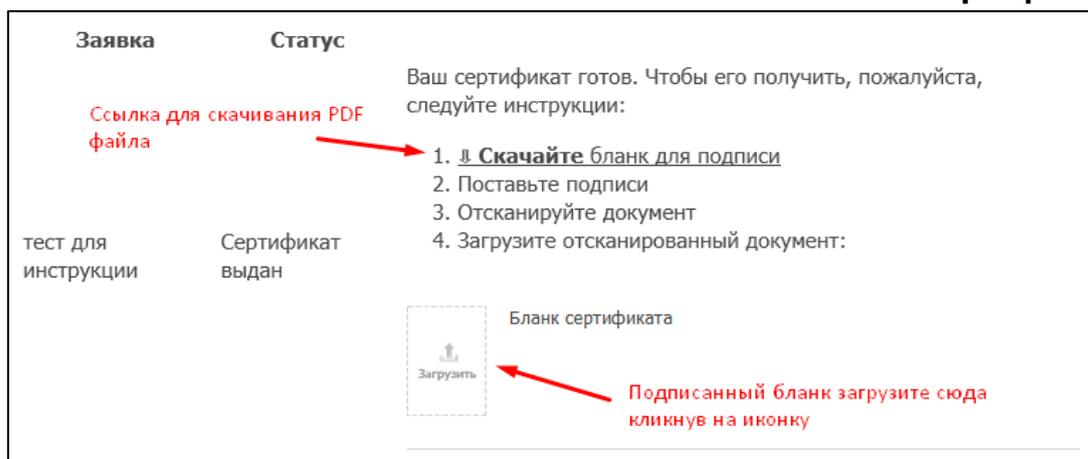
Завершена процедура по созданию закрытой части ключа электронной подписи и отправка запроса на сертификат. Если в качестве носителя у Вас флеш-накопитель (флешка), то доступ к файлам электронной подписи открыт пользователям и антивирусному ПО. В таком случае есть риск утери закрытой части, после чего потребуется перевыпуск. Чтобы обезопасить себя от нежелательных последствий хранения КЭП на флеш-накопителе, сохраните копию папки с флеш-накопителя на своём компьютере и заархивируйте скопированный образец.

Это важно: категорически не рекомендуется осуществлять действия с этими файлами: перенос, изменение наименования, редактирование. При утере электронной подписи, **требуется платный перевыпуск** КЭП. Создавать копию созданной в процессе генерации папки – безопасно.

7. Запись сертификата на ключевой носитель

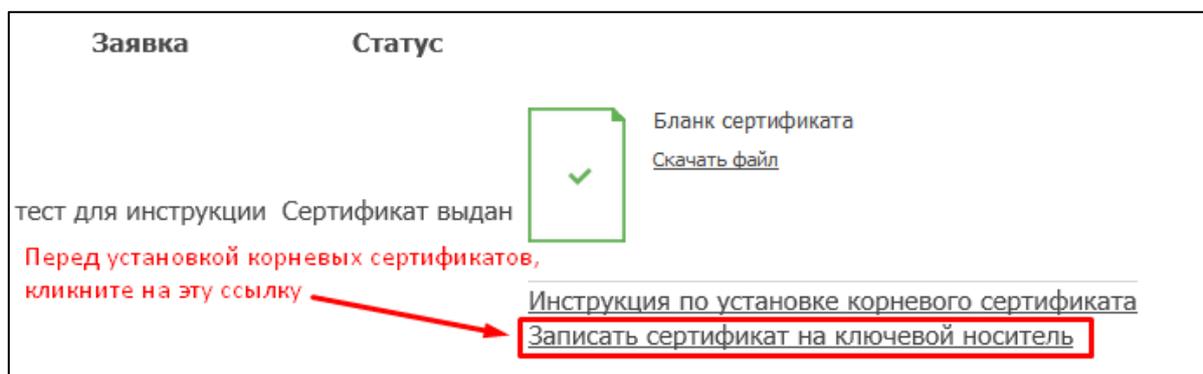
Спустя 5 минут после завершения этапа генерации, обновите страницу генерации, нажав клавишу **F5** или соответствующую кнопку в браузере. Если запрос на выпуск сертификата уже одобрили, появится страница для записи сертификата в контейнер ключа (Рис.10). По ссылке из пункта 1 «**Скачайте бланк для подписи**» на этой странице скачайте **бланк сертификата**, распечатайте его. Владелец сертификата, на чье имя была выпущена КЭП, должен подписать бланк.

Рис.10 – Сертификат одобрен



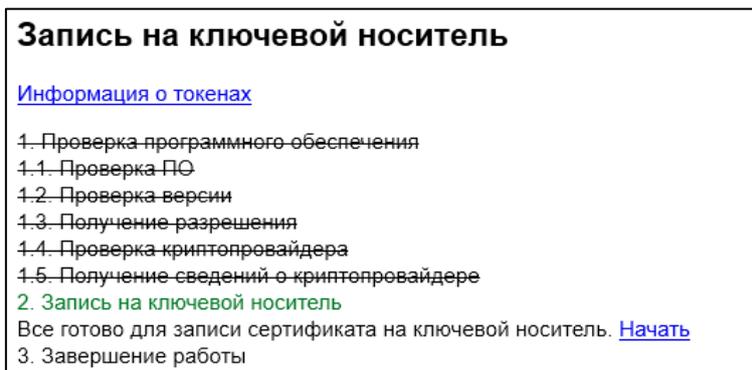
Подписанный документ необходимо отсканировать и загрузить скан на сервер нашего удостоверяющего центра с помощью кнопки на этой же странице. После этого станут доступны две ссылки (Рис.11).

Рис.11 – Бланк загружен



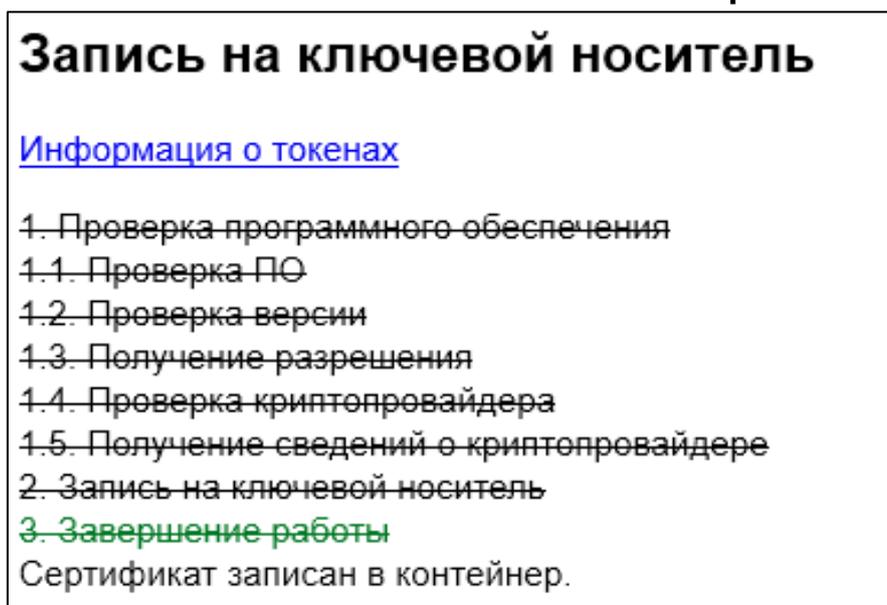
Кликните на ссылку «**Записать сертификат на ключевой носитель**», откроется дополнительное окно (Рис.12).

Рис.12 – Запись сертификата



Нажмите кнопку «**Продолжить**» - в появившемся окошке «**Предоставить доступ**». Для завершения записи кликните кнопку «**Начать**». Появится сообщение об успехе операции (Рис. 13).

Рис.12 – Завершение записи сертификата



Все готово, электронная подпись успешно создана. Для проверки работоспособности КЭП, откройте письмо, которое придёт после создания КЭП. В письме будет содержаться ссылка на сервис по подписанию закрывающих документов с помощью электронной подписи. Пройдите процедуру подписания и скачайте подписанные документы.