# **Инструкция по генерации RSA-ключей и запроса на сертификат.**

В инструкции рассматриваются два варианта генерации ключей: через консольную утилиту **OpenSSL (п.п. 1-2)** и через графическую оболочку **XCA (п.3)**. Для операционной системы Windows можно воспользоваться любым методом. Для Linux и MacOS лучше воспользоваться утилитой Openssl, которая должна быть уже предустановлена.

## **Установка OpenSSL**

## Для Windows скачайте подходящую версию с сайта <https://slproweb.com/products/Win32OpenSSL.html>. Рекомендуется использовать Win64 OpenSSL v1.1.1g.

## Запустите скачанный файл для установки утилиты.

## Для операционных систем Linux и MacOS установка обычно не требуется и утилита уже установлена в систему.

## **Генерация ключей и запроса в OpenSSL**

## **Создание ключей:**

## В командной строке выполните команду: openssl genrsa -des3 -out private.key 2048;

## В ответ на запрос «Enter pass phrase for private.key» введите пароль для защиты закрытого ключа;

## После запроса «Verifying - Enter pass phrase for private.key» - повторите ввод пароля;

## Ваш закрытый ключ будет создан и сохранен в файле private.key. Просмотреть его можно выполнив команду: less private.key

Внимание: при утрате пароля или компрометации закрытого ключа сертификат необходимо перевыпустить.

## **Создание CSR:**

## В командной строке выполните команду: openssl req -new -key private.key -out domain-name.csr

## Введите пароль закрытого ключа в ответ на запрос «Enter pass phrase for private.key»

## Следующие поля заполняются латинскими символами:

* Country Name - двухсимвольный код страны, согласно ISO-3166. «RU» для России.
* State or Province Name: название области или региона без сокращений;
* Locality Name: название города или населенного пункта;
* Organization Name: название организации в латинском эквиваленте;
* Organizational Unit Name: название подразделения, для которого заказывается сертификат (необязательное поле);
* Common Name: ФИО ответственного лица;
* Email Address: контактный e-mail адрес (необязательное поле);
* A challenge password: не заполняется;
* An optional company name: альтернативное имя компании (не заполняется).

## Запрос на сертификат будет сохранен в файле domain-name.csr в виде закодированного текста.

## Проверьте корректность введенных данных, выполнив следующую команду: openssl req -noout -text -in domain-name.csr

## **Для просмотра значения открытого ключа** нужно выполнить команду: openssl req -in domain-name.csr –text

Где в modulus указан открытый ключ (выделено красным):

##

## Впоследствии данный файл (полученный CSR) необходимо передать в Банк, где будет создан сертификат, который Вы будете использовать в запросах СБП.

## **Установка XCA**

## Скачайте последнюю версию с сайта: <https://www.hohnstaedt.de/xca/index.php/download>

## Запустите скаченный файл для установки:

##

## Нажмите Next для начала продолжения установки.

##

## Прочтите лицензионное соглашение и поставьте галочку, если согласны с его положениями.

##

## Нажмите кнопку Typical.

##

## Нажмите Install для начала установки программы.

##

## Дождитесь завершения установки.

##

## Нажмите Finish для завершения установки и запуска программы XCA.

## **Генерация ключей и запроса в XCA**

## Запустите программу XCA, если она ещё не запущена.

## Выберите в меню вкладку «Файл» и пункт New Database для создания новой базы, в которой будут храниться секретные ключи.

##

## Придумайте название файла для базы данных (БД).

## Придумайте и введите пароль для этой БД. Этот пароль будет использоваться для шифрования всех данных в БД. При потере пароля восстановить его будет невозможно.

## На вкладке «Закрытые ключи» нажмите кнопку «Новый ключ».

##

## Придумайте имя для ключа. Оно будет использоваться только для идентификации ключа в XCA. Остальные параметры оставьте такими, как на скриншоте, и нажмите «Создать».

##

## Для просмотра значения открытого ключа нужно выбрать сам ключ и нажать «Показать сведения»

##

##

## На вкладке «Запросы на получение сертификата» нажмите кнопку «Новый запрос».

## В окне для создания запроса на сертификат выберите шаблон [default] tls\_client в нижней части окна в выпадающем списке шаблона и нажмите кнопку «Применить расширения». Заполните имя сертификата.

## На вкладке «Субъект» заполните по-английски следующие поля:

## Internal Name – внутреннее имя для идентификации запроса

## Сountry Name – код страны, для России код должен быть RU

## State or Province Name – область/регион, в примере Moscow

## Locality Name – город, в примере Moscow

## Organization Name – наименование организации

## Organization Unit Name – наименование подразделения организации

## Common Name – ФИО ответственного лица

## Убедитесь, что внизу окна правильно выбран закрытый ключ, к которому создаётся запрос на сертификат!

## Нажмите ОК для создания запроса на сертификат.

##

## Выделите строку с запросом на сертификат и нажмите «Экспортировать».

## Укажите путь к файлу, в котором будет записан запрос на сертификат. Формат для экспорта рекомендуется оставить в формате PEM. Файл будет содержать base64-закодированный запрос. Его можно копировать как текст и отправлять по почте. Нажмите ОК для экспорта.

## Отправьте экспортированный файл запроса на сертификат для получения готового сертификата.

## Для импорта сертификата на вкладке «Сертификаты» импортируйте полученный сертификат. Привязка к закрытому ключу произойдёт автоматически.

## Закрытый ключ с сертификатом можно экспортировать для установки в систему и дальнейшей работы.