Генерация RSA-ключей

Апрель 2024 г.

Создание запроса на сертификат

Методы генерации RSA-ключей:

- Консольная утилита OPENSSL
- Графическая оболочка XCA

Консольная утилита OPENSSL

Установка OpenSSL
Windows:

1. Скачайте подходящую версию с сайта:
https://slproweb.com/products/Win32OpenSSL.html

2. Запустите скачанный файл для установки утилиты;

Win64 OpenSSL v1.1.1s EXE | MSI	63MB Installer	Installs Win64 OpenSSL v1.1.1s (Recommended for software developers by the creators of OpenSSL). Only installs on 64-bit versions of Windows. Note that this is a default build of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.

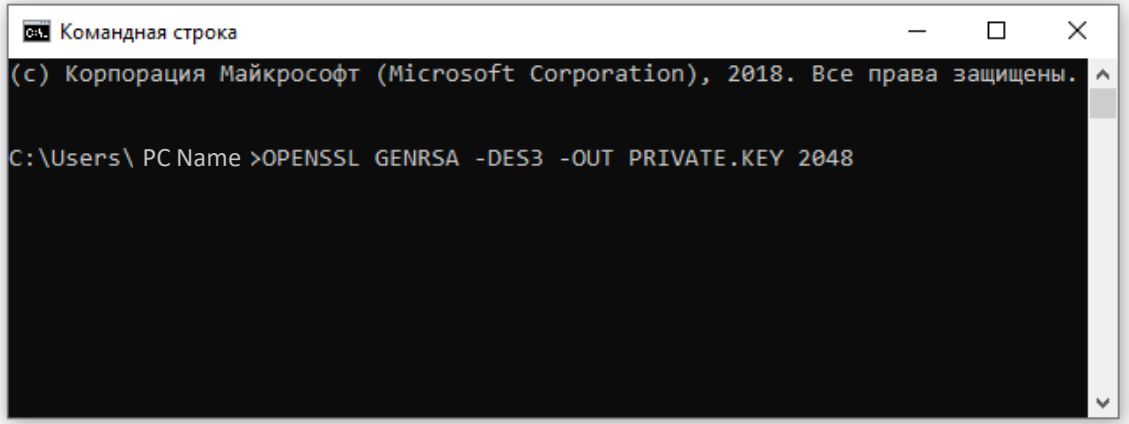
Linux и MacOS:
Не требуется установка дополнительных утилит

Создание ключа и CSR файла с помощью OPENSSL

Шаг 1 В командной строке выполните команду: **OPENSSL GENRSA -DES3 -OUT PRIVATE.KEY 2048**

Шаг 2 В ответ на запрос **ENTER PASS PHRASE FOR PRIVATE.KEY** введите пароль для защиты закрытого ключа

Шаг 3 После запроса **VERIFYING - ENTER PASS PHRASE FOR PRIVATE.KEY** -повторите ввод пароля



- Ваш закрытый ключ будет создан и сохранен в файл **PRIVATE.KEY**
- Посмотреть ключ можно выполнив команду: **LESS PRIVATE.KEY**

Создание ключа и CSR файла с помощью OPENSSL

Шаг 4 В командной строке выполните команду: **OPENSSL REQ-NEW-KEY PRIVATE.KEY-OUT DOMAIN-NAME.CSR**

Шаг 5 Введите пароль закрытого ключа в ответ на запрос: **ENTER PASS PHRASE FOR PRIVATE.KEY**

Шаг 6 После запроса, появятся поля для заполнения

Поля заполняются латинскими символами:

- **Country Name:** двухсимвольный код страны, согласно ISO-3166.«RU»для России;
- **Stateor 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:** контактныйе-mailадрес(необязательное поле);
- **A challenge password и An optional company name:** не заполняется.

Пример заполнения
Country Name: RU
State or Province Name: Moscow
Locality Name: Moscow
Organization Name: OOO Simvol
Organizational Unit Name:
Common Name: Ivanov A.A.
Email Address: simvolivanov@bk.com
A challenge password:
An optional company name:

- Запрос на сертификат будет сохранен в файле **DOMAIN-NAME.CSR** в виде закодированного текста
- Проверить корректность введенных данных можно выполнив команду: **OPENSSL REQ-NOOUT-TEXT-IN DOMAIN-NAME.CSR**

Просмотр значения открытого ключа

Для просмотра открытого ключа, выполните команду:

OPENSSL REQ-IN DOMAIN-NAME.CSR-TEXT

Красным цветом выделено отображение открытого ключа в MODULUS

Полученный CSR файл необходимо передать в Банк для создания Сертификата, который Вы будете использовать в запросах СБП.

При утрате пароля или компрометации закрытого ключа, сертификат необходимо перевыпустить.

Установка XCA

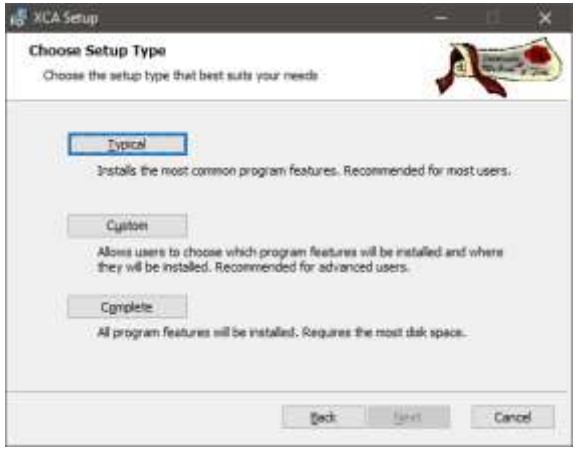
Шаг 1 Скачайте последнюю версию с сайта: **HTTPS://WWW.HOHNSTAEDT.DE/XCA/INDEX.PHP/DOWNLOAD**

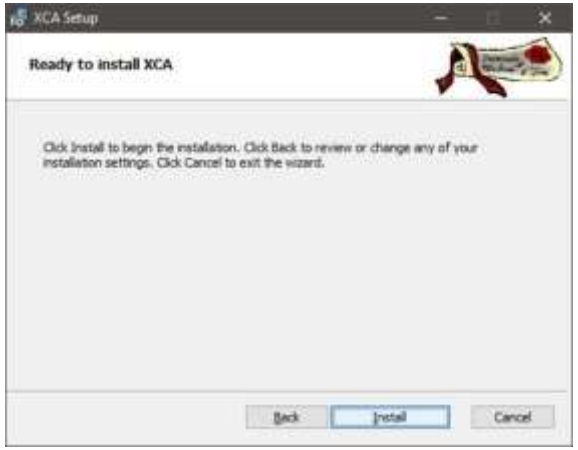
Шаг 2 Запустите скачанный файл для установки. Нажмите **NEXT** для начала установки.

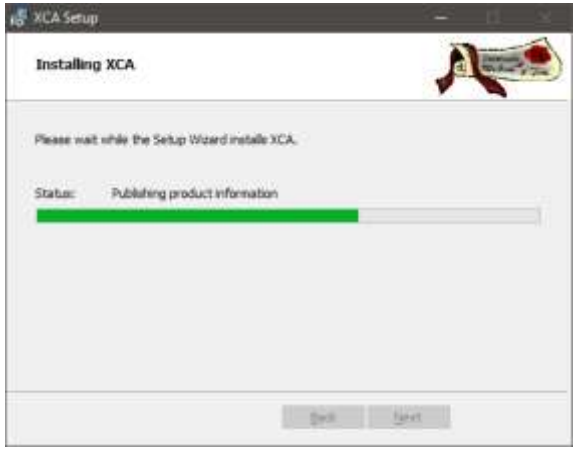
Шаг 3 Прочтите лицензионное соглашение и поставьте «↓», если согласны с его положениями

Шаг 4 Нажмите на кнопку **TYPICAL**

Шаг 5 Нажмите **INSTALL** для начала установки программы





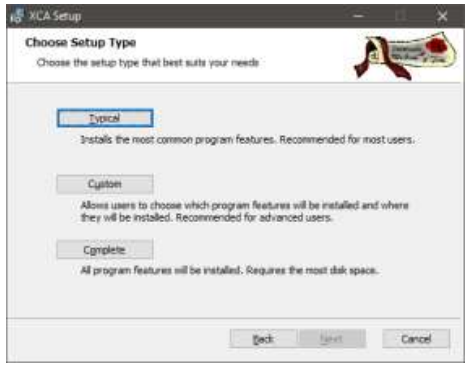


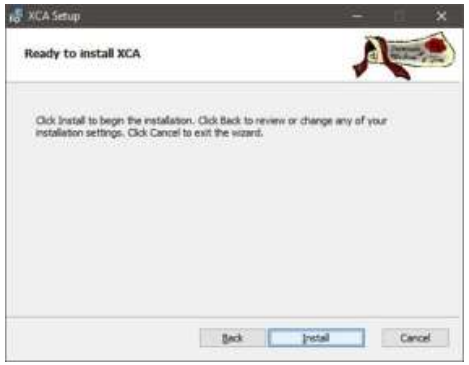
Установка XCA

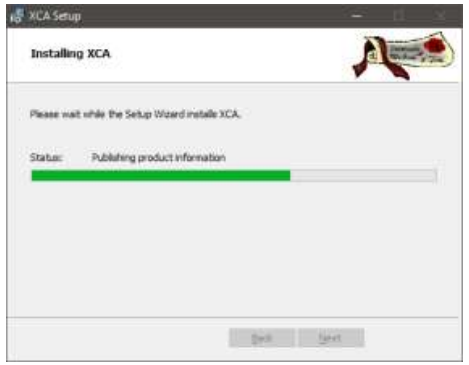
Шаг 3 Прочтите лицензионное соглашение и поставьте «√», если согласны с его положениями

Шаг 4 Нажмите на кнопку **TYPICAL**

Шаг 5 Нажмите **INSTALL** для начала установки программы

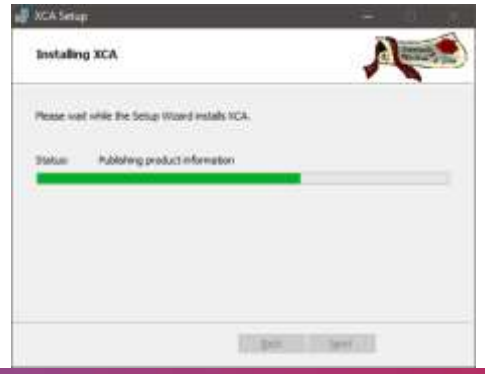






Шаг 6 Дождитесь завершения установки

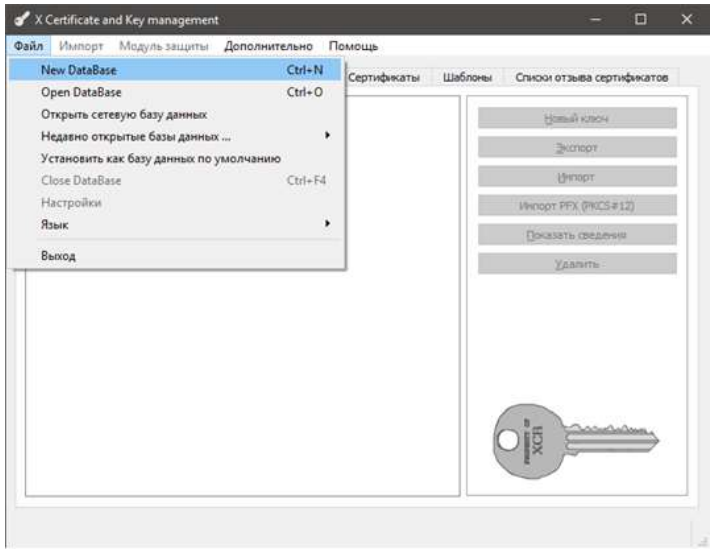
Шаг 7 Нажмите **FINISH** для завершения установки и запуска **XCA**

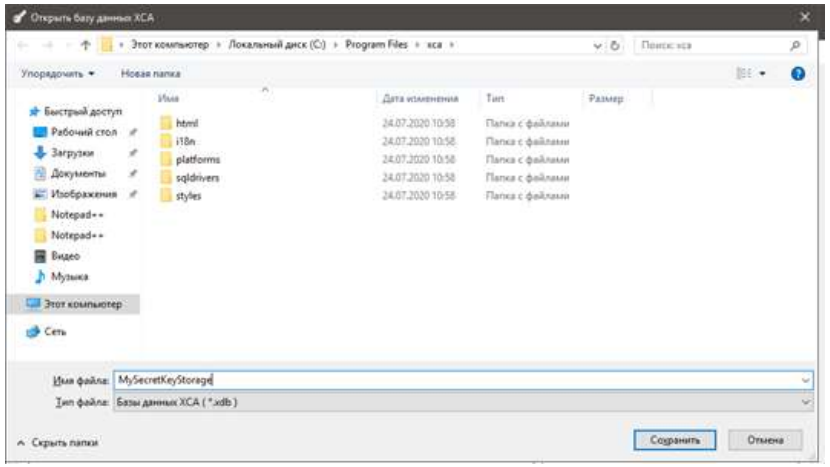


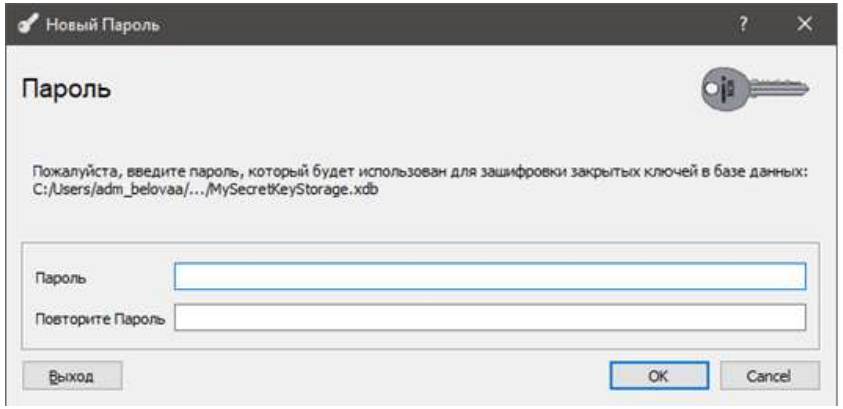
Создание ключа и CSR файла с помощью XCA

1. Запустите программу **XCA**, если она ещё не запущена
2. Выберите в меню вкладку **«Файл»** и пункт **New Database** для создания новой базы, в которой будут храниться секретные ключи
3. Придумайте название файла для базы данных (БД)
4. Придумайте и введите пароль для этой БД. Этот пароль будет использоваться для шифрования всех данных в БД.

Важно! При потере пароля восстановить его будет невозможно





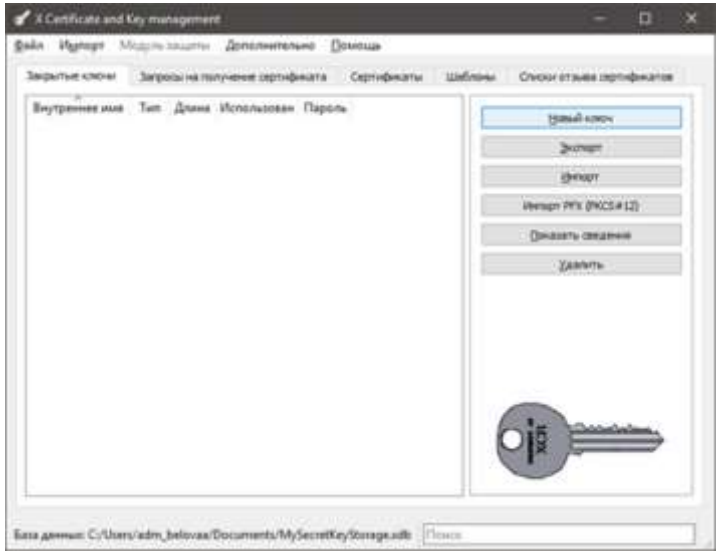


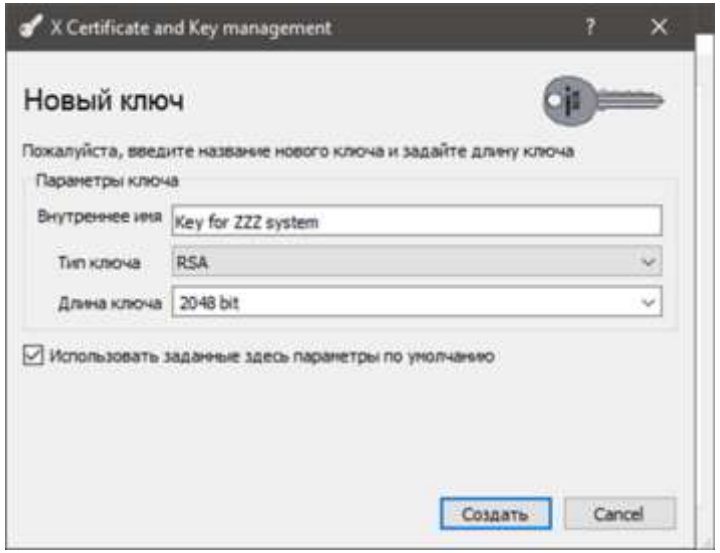
Создание ключа и CSR файла с помощью XCA

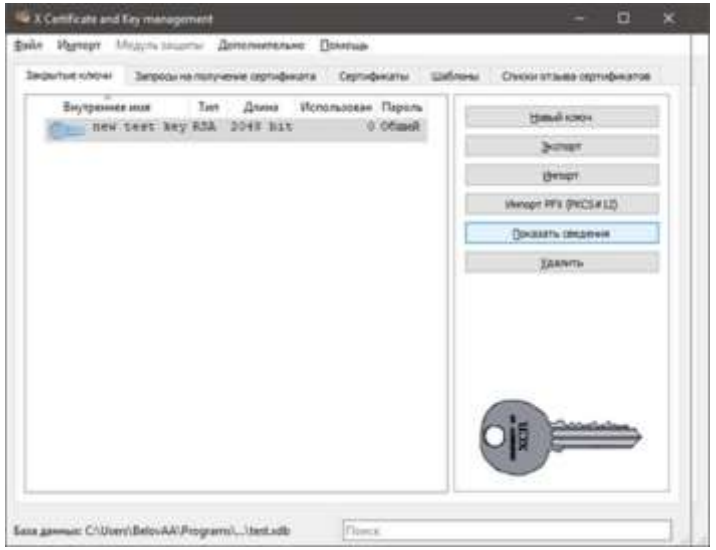
5. На вкладке «Закрытые ключи» нажмите кнопку «Новый ключ»

6. 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»



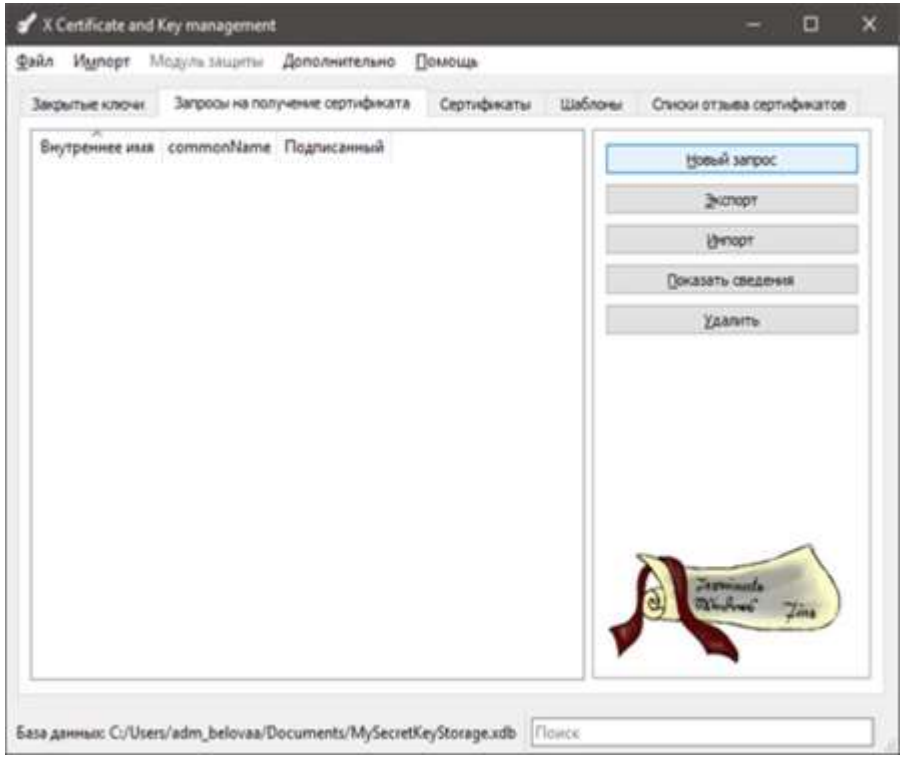


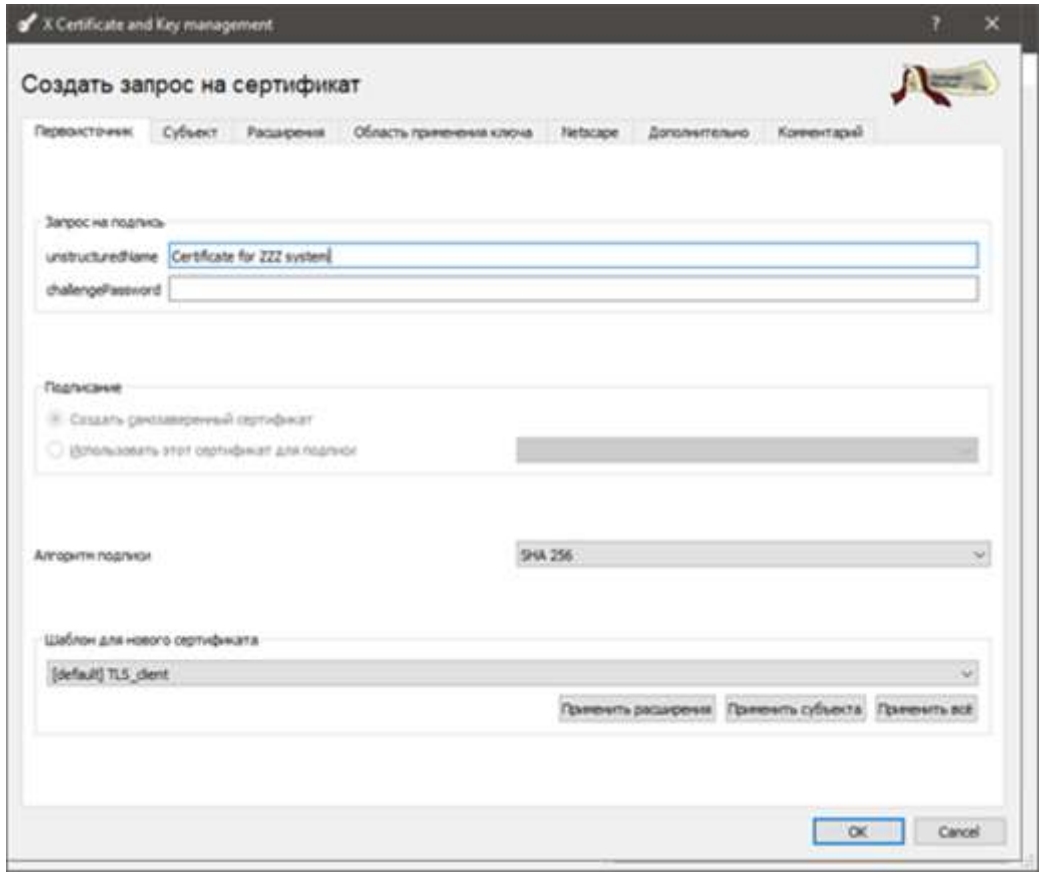


Создание ключа и CSR файла с помощью XCA

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

8. 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





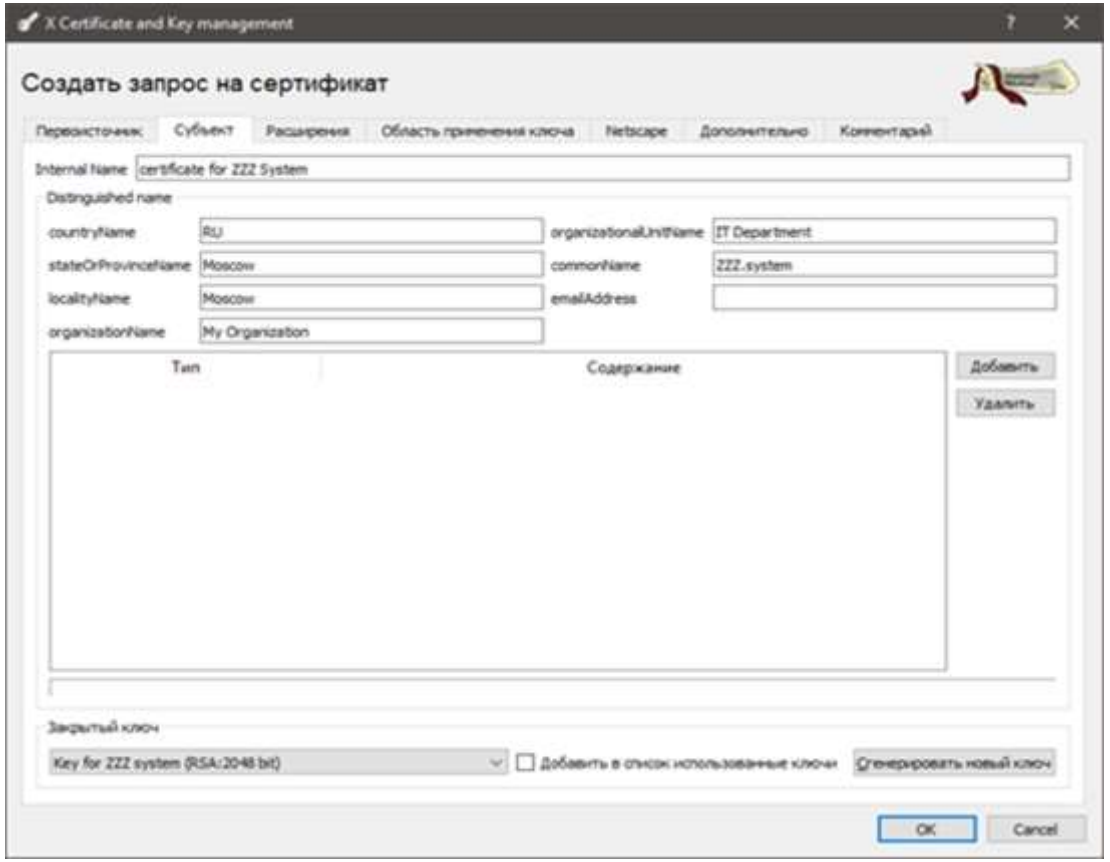
Создание ключа и CSR файла с помощью XCA

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

- **Internal name** – Внутреннее имя для идентификации запроса
- **Country name** – код страны, для России (код должен быть RU)
- **State or province name** – область/регион
- **Locality name** – Город
- **Organization name** – Наименование организации
- **Organization unit name** – Наименование подразделения организации
- **Common name** – ФИО ответственного лица

Убедитесь, правильно ли выбран закрытый ключ, к которому создаётся запрос на сертификат!

Пример заполнения
Country Name: RU
State or Province Name: Moscow
Locality Name: Moscow
Organization Name: OOO Simvol
Organizational Unit Name:
Common Name: IvanovA.A.
Email Address:
A challenge password:
An optional company name:

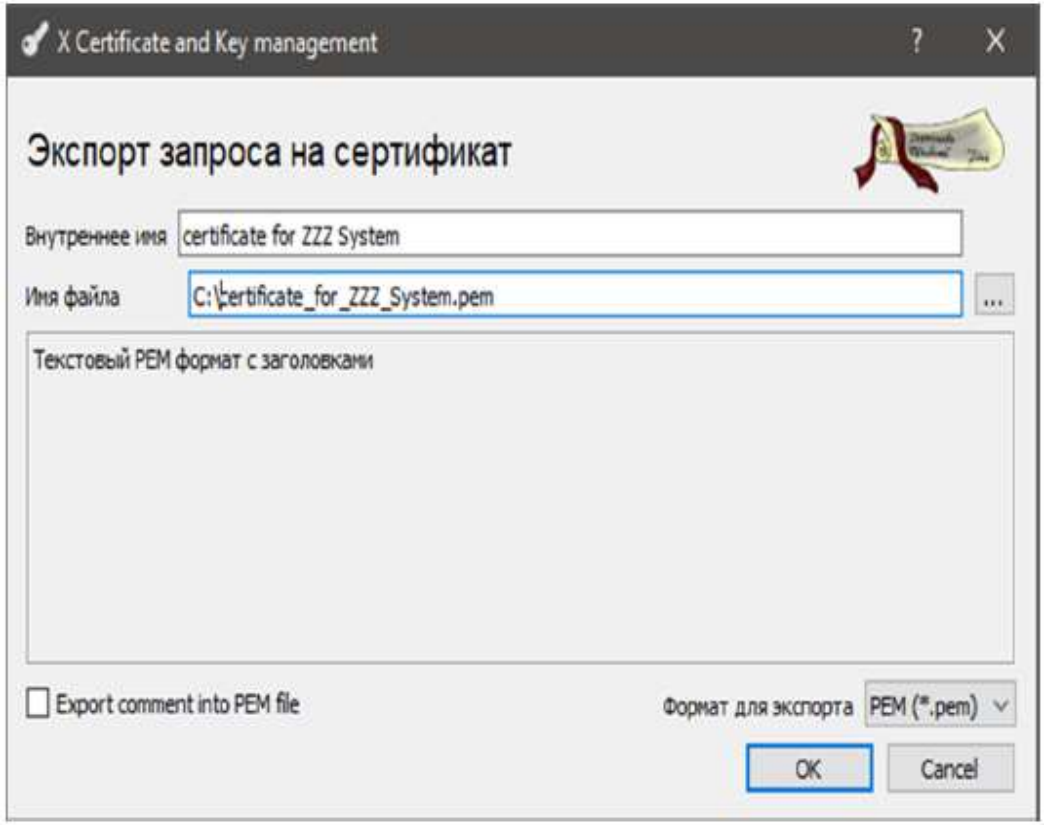


Создание ключа и CSR файла с помощью XCA

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

11. 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

Полученный файл необходимо передать в Банк для создания Сертификата, который Вы будете использовать в запросах СБП



МКБ

Спасибо за внимание!

Техническая поддержка интернет-эквайринга
ecomsupport@mkb.ru

Отдел посопровождению эквайринговых сервисов
acquiring@mkb.ru

8 800 200-34-74 ежедневно с 6:00 до 21:00 (по Мск)