



Генерация RSA-ключей

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:

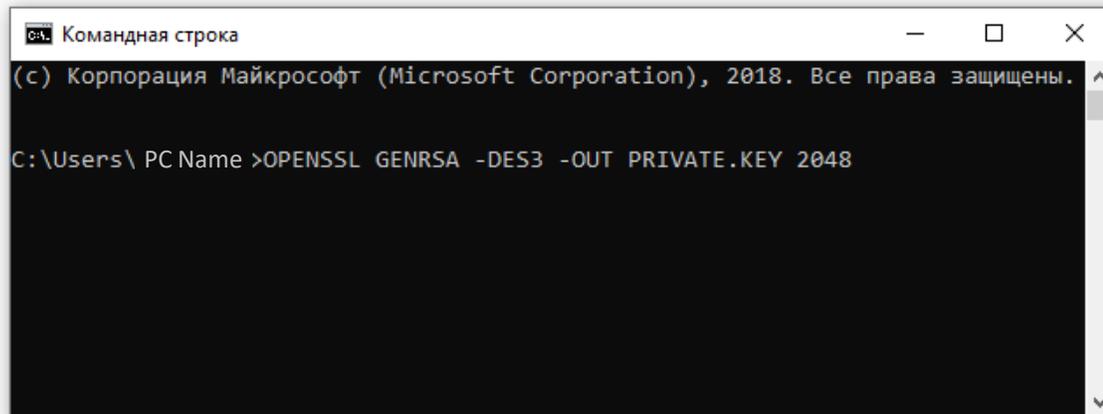
Не требуется установка дополнительных утилит

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



```
Командная строка
(c) Корпорация Майкрософт (Microsoft Corporation), 2018. Все права защищены.
C:\Users\PCName >OPENSSL GENRSA -DES3 -OUT PRIVATE.KEY 2048
```

- 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;
- 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 и An optional company name:** не заполняется.

Пример заполнения

Country Name: RU
State or Province Name: Moscow
Locality Name: Moscow
Organization Name: ООО 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:

```
OPENSSSL REQ-IN DOMAIN-NAME.CSR-TEXT
```

Красным цветом выделено отображение открытого ключа в MODULUS

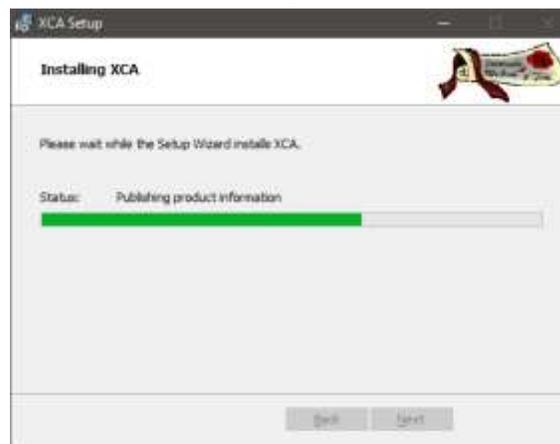
Полученный CSR файл необходимо передать в Банк для создания Сертификата, который Вы будете использовать в запросах СБП.

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

```
[service@acq-mpi-test SamoylovaD]$ openssl req -in domain-name.csr -text
logger: invalid option -- 'n'
usage: logger [-is] [-f file] [-p pri] [-t tag] [-u socket] [ message ...
Certificate Request:
  Data:
    Version: 0 (0x0)
    Subject: C=RU, ST=Moscow, L=Moscow, O=MKB, OU=IT, CN=QQ
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      Public-Key: (2048 bit)
      Modulus:
        00:c6:2d:10:b6:81:bl:46:28:04:55:4a:16:65:ec:
        55:bl:86:ab:aa:c9:17:c1:71:98:64:19:1c:5d:10:
        ae:52:56:18:a9:76:90:3a:b3:46:82:e7:63:9d:2f:
        3f:05:c0:eb:43:7e:78:8f:31:3a:6b:09:42:13:d0:
        9e:0f:01:6f:5b:40:1c:67:60:e8:5b:85:ff:08:50:
        a3:93:03:c8:dc:15:4f:d7:d9:65:bl:c4:a5:f5:81:
        8c:ad:cf:44:21:ed:3d:0e:4c:e1:fl:b7:f7:78:4a:
        43:2d:6c:92:bc:03:d4:33:5b:39:2b:9c:el:ec:1f:
        d4:29:59:0b:ld:5e:45:b8:13:58:e3:b2:b0:38:34:
        30:a1:bc:5b:16:f3:e9:0f:17:f0:47:3e:15:29:a5:
        88:14:3b:ee:14:60:5d:75:47:4b:28:1c:e5:d5:ba:
        ce:00:47:18:70:61:24:49:58:95:a8:12:62:53:ba:
        c8:6d:b2:63:e9:58:ed:f6:c5:a7:16:b0:40:e6:88:
        18:31:3a:02:15:93:25:5c:1b:65:c2:5c:ac:55:5b:
        16:02:a5:cc:ca:b4:8f:8b:4b:0b:4f:ec:fa:ad:ac:
        f4:05:58:83:2e:04:9f:12:e2:0c:7a:5e:1a:7c:f5:
        68:3c:55:ee:1a:53:b4:f5:de:d8:29:d0:36:9f:2e:
        b2:71
      Exponent: 65537 (0x10001)
    Attributes:
      a0:00
  Signature Algorithm: sha1WithRSAEncryption
    63:52:ea:f4:c4:05:60:62:04:e2:b8:a7:86:5d:c6:fc:a4:f0:
    26:25:8a:56:b9:6c:46:15:43:cb:a3:da:cb:e9:96:79:7b:18:
    21:29:1e:4a:ac:ba:d0:ed:49:f6:2d:9e:f8:f6:1b:a9:e6:67:
    c2:88:ca:7f:1a:0e:38:f9:a2:7c:9c:80:d5:64:35:c7:20:53:
    7f:58:bc:9e:f7:e8:bc:cd:4f:5c:ed:91:5d:13:b4:22:4d:f6:
```

Установка XCA

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

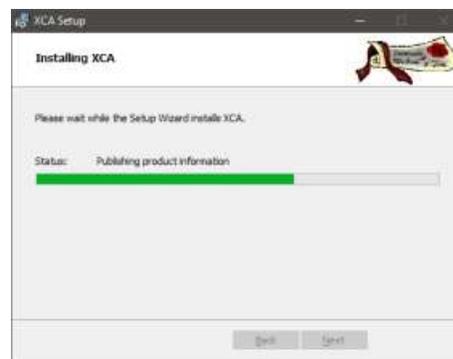
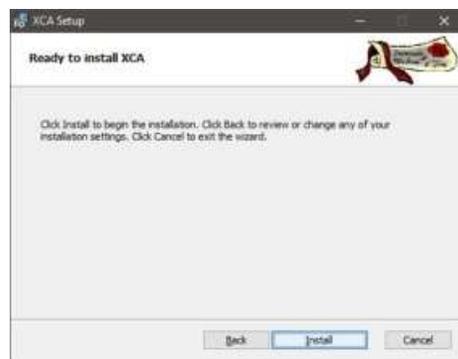
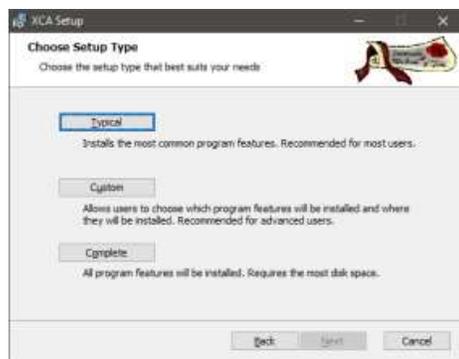


Установка XCA

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

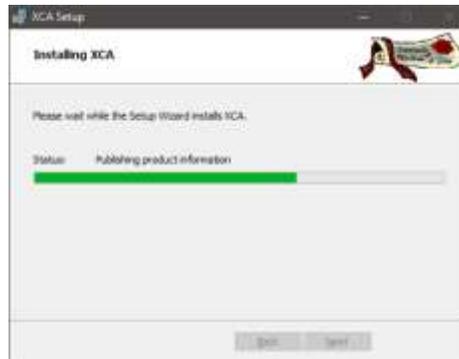
Шаг 4 Нажмите на кнопку **TYPICAL**

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



Шаг 6 Дождитесь завершения установки

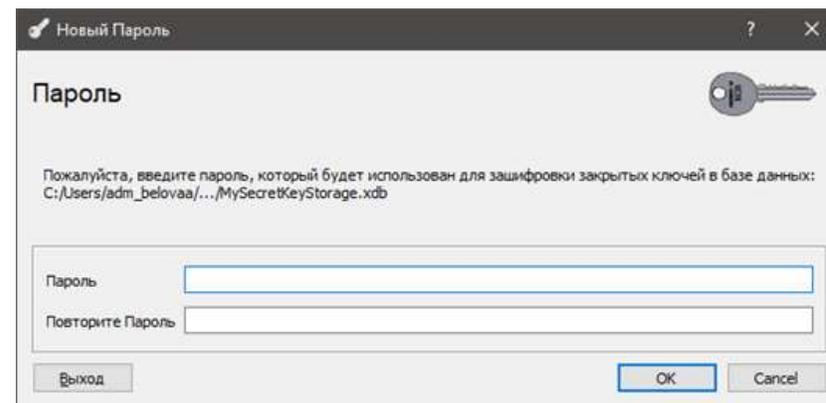
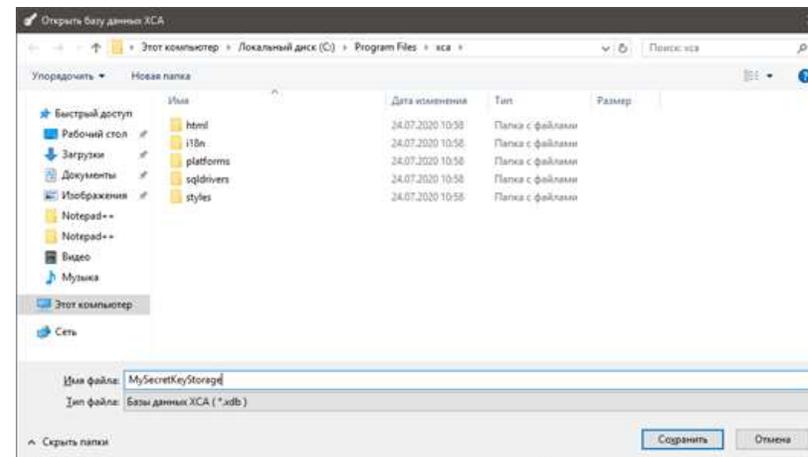
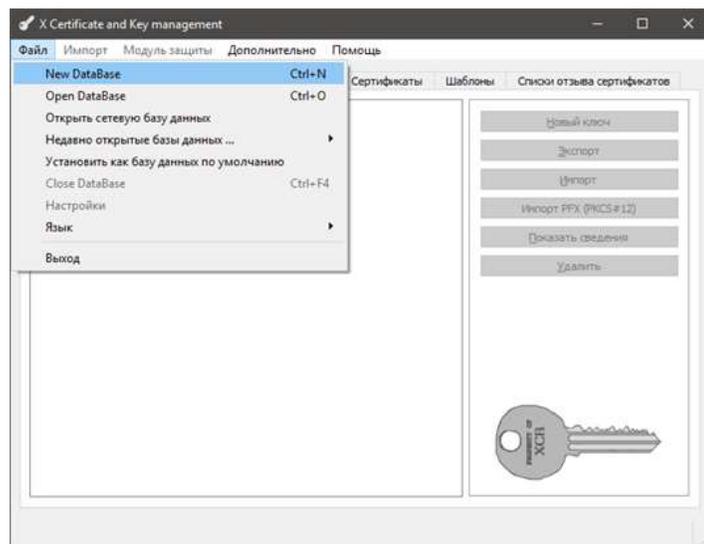
Шаг 7 Нажмите **FINISH** для завершения установки и запуска **XCA**



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.

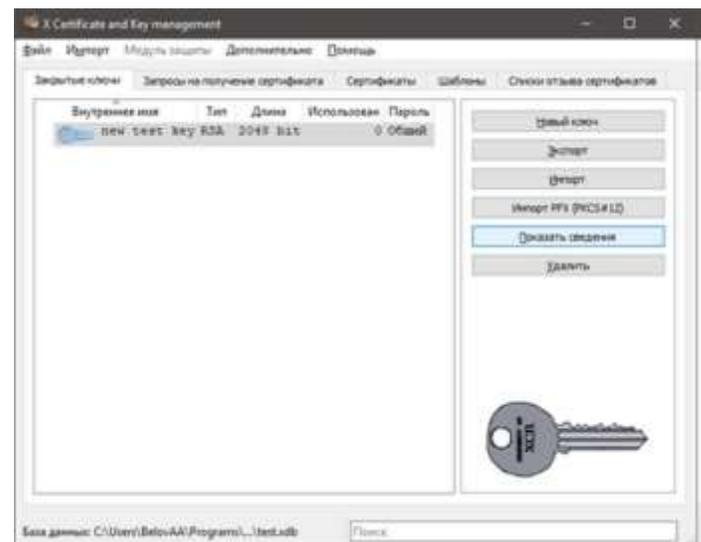
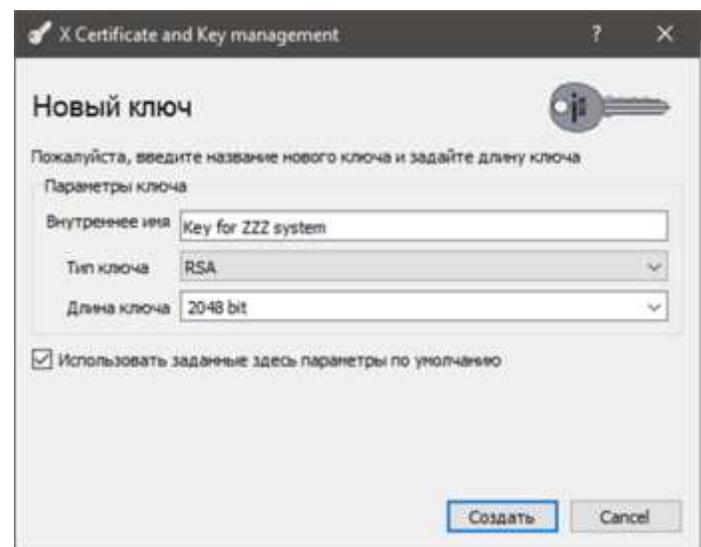
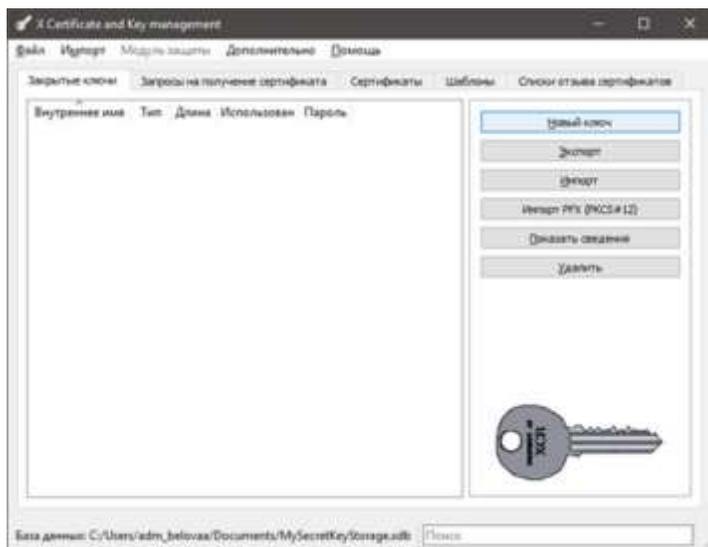
Важно! При потере пароля восстановить его будет невозможно



Создание ключа и CSR файла с помощью XCA

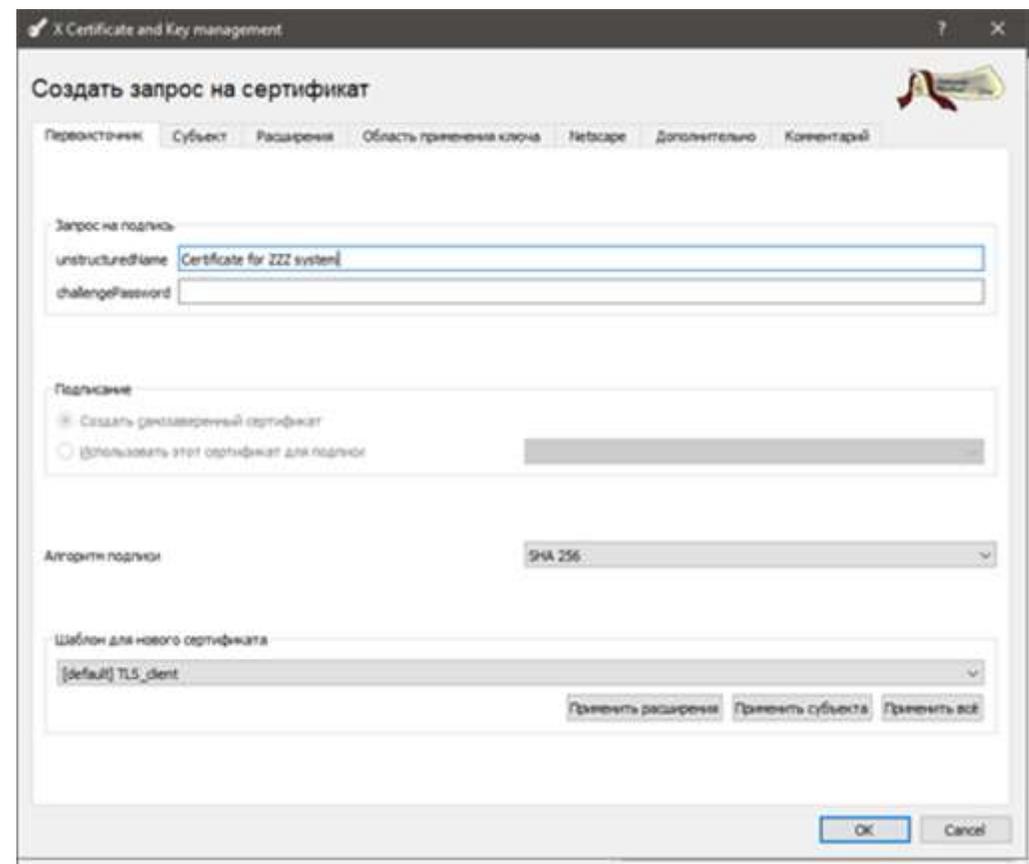
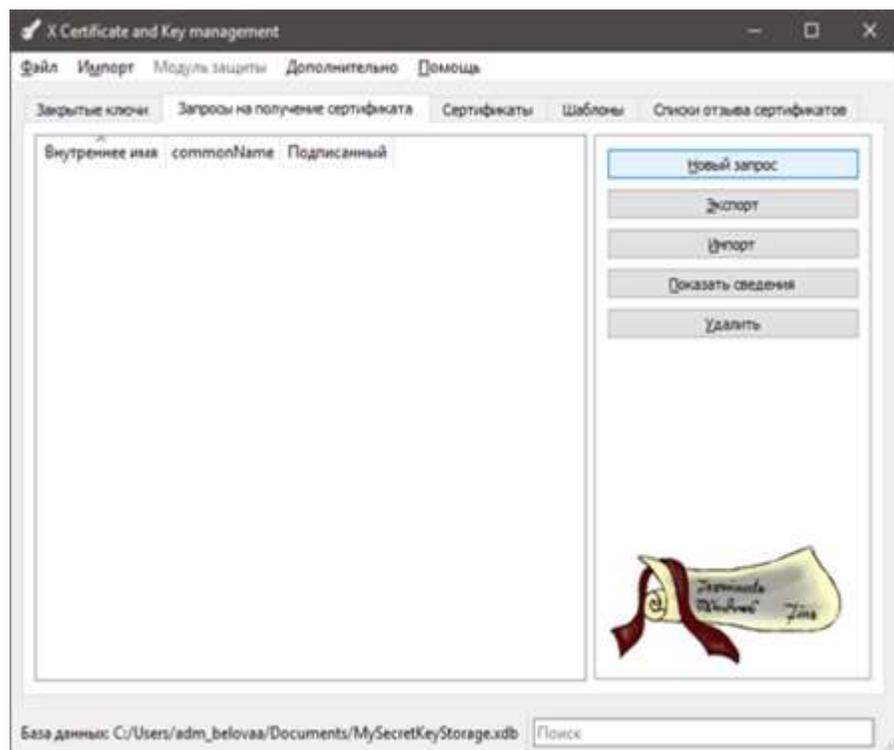
5. На вкладке «Закрытые ключи» нажмите кнопку «Новый ключ»
6. Придумайте имя для ключа Оно будет использоваться только для идентификации ключа в XCA Остальные параметры оставьте такими, как на скриншоте, и нажмите «создать»

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

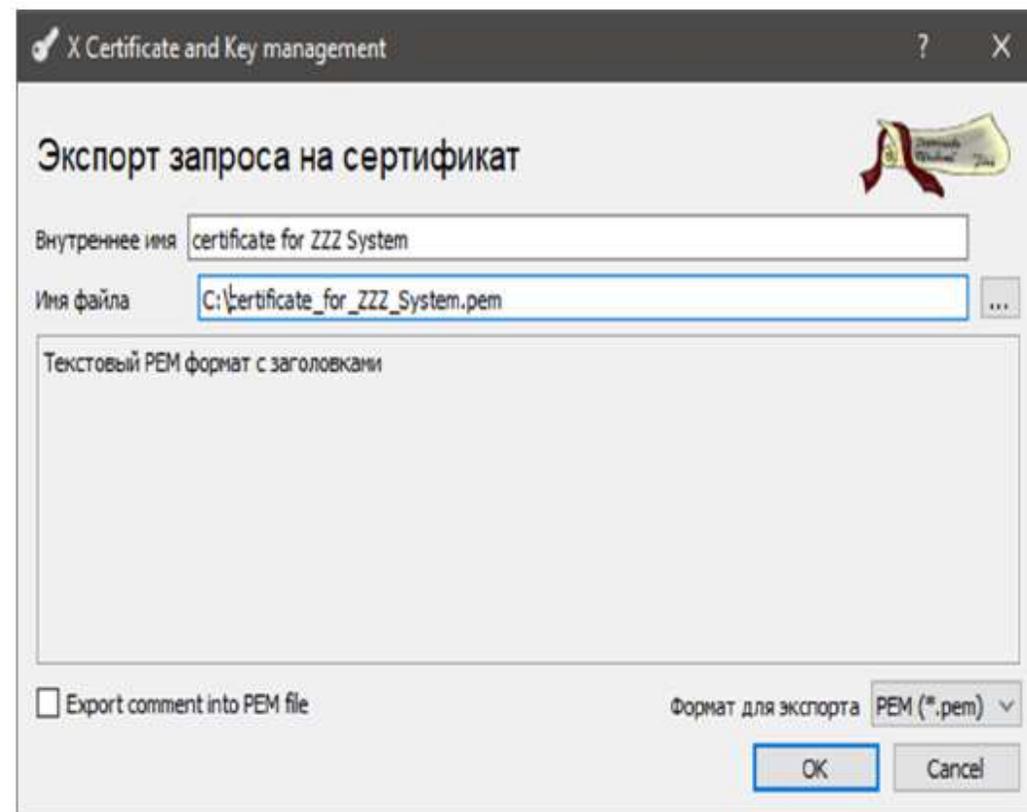
Country Name: RU
State or Province Name: Moscow
Locality Name: Moscow
Organization Name: OOO Simvol
Organizational Unit Name:
Common Name: IvanovA.A.
Email Address:
A challenge password:
An optional company name:

The screenshot shows the 'Create Certificate Request' dialog box in XCA. The 'Subject' tab is selected. The 'Internal Name' field contains 'certificate for ZZZ System'. The 'Distinguished Name' section includes: 'countryName' (RU), 'stateOrProvinceName' (Moscow), 'localityName' (Moscow), 'organizationName' (My Organization), 'organizationalUnitName' (IT Department), and 'commonName' (ZZZ.system). The 'emailAddress' field is empty. At the bottom, the 'Private Key' section shows a dropdown menu with 'Key for ZZZ system (RSA/2048 bit)' selected, a checkbox for 'Add to list of used keys', and a 'Generate new key' button. The 'OK' and 'Cancel' buttons are at the bottom right.

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





**Спасибо
за внимание!**

Техническая поддержка интернет-эквайринга
ecomsupport@mkb.ru

Отдел сопровождению эквайринговых сервисов
acquiring@mkb.ru

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