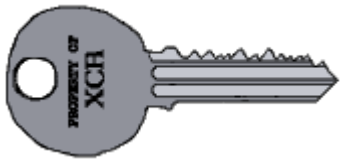
XCA



(**X C**ertificate and Key m**a**nagement) это программа, предоставляющая интерфейс для управления асимметричными ключами RSA/DSA. Программа может использоваться для создания и подписывания сертификатов в рамках небольшого ЦС(CA) и создать собственную инфраструктуру открытых ключей (PKI).

Для шифрования используется библиотека OpenSSL.

Основные возможности:

- Программа позволяет создавать собственные сертификаты, запросы и списки отзыва (CRL)
- Импорт и экспорт ключей в форматах:
  - PEM
  - DER
  - PKCS#7
  - PKCS#12
- Можно управлять Smart-картами через интерфейс PKCS#11
- Экспортировать сертификаты и запросы в файл настроек OpenSSL
- Есть возможность создавать шаблоны для создания сертификатов
- Шаблон можно создать на основе готового сертификата
- Есть поддержка расширений x509v3
- Можно изменять ширину столбцов

Можно использовать для работы с

- IPsec
- **OpenVPN**
- **SSH**
- **libvrt**

Стандарты:

- PKCS#1 unencrypted RSA key storage format.
- PKCS#7 Collection of public certificates.
- PKCS#8 Encrypted private key format for RSA DSA EC keys.
- PKCS#10 Certificate signing request.
- PKCS#11 Security token / Smart card / HSM access.
- PKCS#12 Certificate, Private key and probably a CA chain.

Форматы файлов:

- DER (Distinguished Encoding Rules) — бинарный формат
- PEM Privacy Enhanced Mail — текстовый формат
- SSH2 — Публичные ключи SSH

Удобство использования:

- Templates for common subjects and extensions.
- All subject entries, x509v3 extensions, and other properties can be displayed in separate columns.
- Customizable subject entries
- Drag & Drop support
- Many certificate setting sanity checks
- Easy association and transformation between keys, certificates and requests

http://hohnstaedt.de/xca/

http://hohnstaedt.de/xca/index.php/download

https://github.com/chris2511/xca/

Установка

```
apt install xca
```

Компиляция

Необходимые пакеты:

```
apt install autoconf g++ libltdl-dev qt4-dev-tools libssl-dev pkg-config
```

Пример для версии 2.1.2

Загрузка и компиляция:

xca_download_compile.sh

```
#!/bin/bash
cd /tmp/
wget https://github.com/chris2511/xca/archive/RELEASE.2.1.2.tar.gz
tar -xvf RELEASE.2.1.2.tar.gz

cd /tmp/xca-RELEASE.2.1.2
./bootstrap
./configure; make -j6; make install
```

Типовые действия

- Отзыв сертификата
- Экспорт списка отзыва
- Экспорт сертификата
- Экспорт закрытого ключа
- Генерация параметров Диффи — Хеллмана

Отзыв сертификата

1. Перейти на вкладку Сертификаты
2. Выбрать нужный Сертификат
3. Нажать правую кнопку мыши и в контекстном меню выбрать Отозвать
4. Выполнить Экспорт списка отзыва

Экспорт списка отзыва

1. Перейти на вкладку Сертификаты
2. Выбрать нужный Центр сертификации (ЦС)
3. Нажать правую кнопку мыши и в контекстном меню выбрать ЦС/Сгенерировать CRL
4. Задать нужные значения и нажать кнопку OK
5. Перейти на вкладку Списки отзыва сертификатов
6. Выбрать нужный Список отзыва
7. Нажать на кнопку Экспорт
8. В окне «Экспорт списка отзывов» нужно задать путь и имя файла, формат файла PEM (*.pem)
9. нажать кнопку OK

Экспорт сертификата

1. Перейти на вкладку Сертификаты
2. Выбрать нужный Сертификат
3. Нажать кнопку Экспорт
4. В появившемся окне нужно в поле Формат сертификата выбрать PEM (*.crt), указать путь к файлу
5. Нажать кнопку OK

Экспорт закрытого ключа

1. Перейти на вкладку Закрытые ключи
2. Выбрать нужный Закрытый ключ
3. Нажать кнопку Экспорт
4. В появившемся окне нужно в поле Формат для экспорта выбрать Закрытый ключ PEM (*.pem), указать путь к файлу
5. Нажать кнопку OK

Генерация параметров Диффи — Хеллмана

Алгоритм обмена Диффи-Хеллмана (DH)

1. Меню Дополнительно/Сгенерировать параметры Диффи — Хеллмана
2. В окне появившемся окне нужно выбрать 2048
3. Нажать кнопку OK
4. Начнётся процесс генерации, который может занять несколько минут!
5. После появится диалог с переложением сохранить из в файл dh2048.pem

Поля

Internal Name

Это имя используется только внутри программы XCA и не сохранятся в сертификате.

countryName

[C] Код страны (два символа), например RU

stateOfProvinceName

[ST] Регион (область, республика) внутри страны (128 символов).

localityName

[L] Город или населённый пункт (128 символов).

organizationName

[O] Наименование организации (64 символа).

organizationUnitName

[OU] Наименование подразделения организации.

commonName

`[CN]` Наименование субъекта. (64 символа).

emailAddress

Адрес электронной почты (128 7-битных символов).

Перевод

Для перевода нужно использовать Qt linguist

Исходный файл `xca_ru.ts` нужно скомпилировать в `xca_ru.qm`

```
lrelease xca_ru.ts
```

---

https://hohnstaedt.de/xca/index.php/colaboration/translation

Ссылки

https://www.hohnstaedt.de/xca/templates/g5_hydrogen/custom/images/bigcert.png

https://www.hohnstaedt.de/xca/templates/g5_hydrogen/custom/images/bigkey.png

Защищенный канал передачи данных с помощью самоподписанных SSL-сертификатов и Stunnel

XCA – удостоверяющий центр уровня предприятия или сага о русских и немецких программистах / Хабр

http://sysadminmosaic.ru/xca/xca?rev=1550594401

2019-02-19 19:40