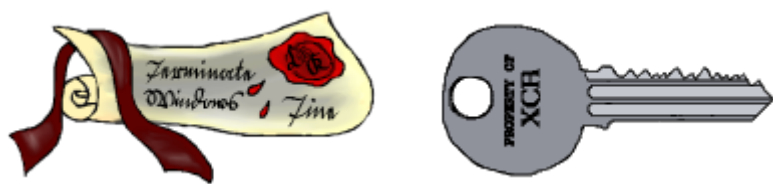


XCA



(**X** Certificate and Key management) 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](#)

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
```

Использование

Использование XCA для работа с [OpenVPN](#) описано [здесь](#)

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](#)

[ХСА – удостоверяющий центр уровня предприятия или сага о русских и немецких программистах / Хабр](#)

<http://sysadminmosaic.ru/xca/xca?rev=1550337461>

2019-02-16 20:17

