Импорт ключей и RSA сертификата на Рутокен из PFX-файла

В данной инструкции описывается, как записать на Рутокен ЭЦП готовые RSA сертификат и закрытый ключ в формате PFX.

Проверка модели устройства

1. Подключите USB-токен к компьютеру.
2. Для определения названия модели USB-токена откройте **Терминал** и введите команду:

```
$ lsusb
```

В результате в окне Терминала отобразится название модели USB-токена:

```
[dmitrieva@localhost ~]$ lsusb
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
Bus 002 Device 004: ID 0a89:0030 Aktiv Rutoken ECP
Bus 002 Device 003: ID 0e0f:0002 VMware, Inc. Virtual USB Hub
Bus 002 Device 002: ID 0e0f:0003 VMware, Inc. Virtual Mouse
Bus 002 Device 001: ID 1d6b:0001 Linux Foundation 1.1 root hub
```

Убедитесь, что используете: **Aktiv Rutoken ECP**

Порядок действий

1. С помощью OpenSSL экспортируем закрытый ключ из PFX-файла:

```
openssl
OpenSSL> pkcs12 -in newcert.pfx -nocerts -out encrypted.key
```

2. Проводим те же действия с сертификатом:

```
OpenSSL> pkcs12 -in newcert.pfx -nokeys -out cert.pem
```

3. Конвертируем полученные сертификат и закрытый ключ в формат DER:

```
OpenSSL> x509 -in cert.pem -out cert.crt -outform DER
OpenSSL> rsa -in encrypted.key -out key.der -outform DER
```

4. Получаем открытый ключ в формате DER:

```
OpenSSL> rsa -in encrypted.key -out pub.der -outform DER -pubout
```

5. Записываем сконвертированный закрытый ключ на Рутокен:

```
pkcs11-tool --module /usr/lib/librtpkcs11ecp.so -l -y privkey -w key.der --id 10 --label Rutoken1
```

6. Записываем сертификат *.CRT на токен:

```
pkcs11-tool --module /usr/lib/librtpkcs11ecp.so -l -y cert -w cert.crt --id 10 --label Rutoken1
```

7. Записываем открытый ключ на токен:

```
pkcs11-tool --module /usr/lib/librtpkcs11ecp.so -l -y pubkey -w pub.der --id 10 --label Rutoken1
```