

Подготовка Рутокен ЭЦП для работы с luks

В данной статье описано, как подготовить Рутокен ЭЦП для работы в качестве носителя ключей при шифровании разделов в Linux с помощью Luks.

Использование смарт-карт описано по ссылке <https://github.com/swoopla/smartcard-luks>

Для Рутокен ЭЦП процесс подготовки выглядит следующим образом:

1. Установка пакетов для работы со смарт-картами

```
$ sudo apt-get install pcscd opensc
```

2. Форматируем Рутокен ЭЦП 2.0

```
$ pkcs15-init --erase-card -p rutoken_ecp
```

3. Инициализируем Рутокен ЭЦП 2.0

```
$ pkcs15-init --create-pkcs15 --so-pin "87654321" --so-puk ""
```

```
$ pkcs15-init --store-pin --label "User PIN" --auth-id 02 --pin "12345678" --puk "" --so-pin "87654321" --finalize
```

4. Создаем ключевую пару на Рутокен ЭЦП 2.0

```
$ pkcs15-init -G rsa/2048 --auth-id 02 -u decrypt --id 01
```

5. Создаем случайный файл и привязываем его в качестве ключевого к LUKS

```
$ sudo touch /root/rootkey
```

```
$ sudo chmod 600 /root/rootkey
```

```
$ sudo dd if=/dev/random of=/root/rootkey bs=1 count=245 #change to urandom if you can't wait
```

```
$ sudo cryptsetup luksAddKey /dev/sda2 /root/rootkey
```

6. Экспортируем открытый ключ из Рутокен ЭЦП 2.0

```
$ pkcs15-tool --read-public-key 01 -o public_key_rsa2048.pem
```

7. Шифруем ключевой файл с помощью открытого ключа

```
$ sudo openssl rsautl -encrypt -pubin -inkey public_key_rsa2048.pem -in /root/rootkey -out /root/rootkey.enc
```

8. Проверяем, что файл успешно может расшифроваться на ключе с Рутокен ЭЦП 2.0

```
$ sudo pkcs15-crypt --decipher --input /root/rootkey.enc --pkcs1 --raw -k 01 --output /root/rootkey.dec
```

9. Сравниваем файлы /root/rootkey и /root/rootkey.dec. Если они идентичны, то удаляем их и оставляем только зашифрованный файл

```
$ sudo rm /root/rootkey
```

```
$ sudo rm /root/rootkey.dec
```

Далее продолжить настройку по [инструкции](#):

1) Выполнить 1-8 пункты. Зашифрованный ключ может лежать или в /boot, или в initramfs или в любом другом месте. Его местонахождение нужно описать в crypttab.

2) Затем шаг 13 (без патча decrypt_opensc). Убедиться, что в initramfs попал /root/luks-secret.key (посмотреть содержимое initramfs можно с помощью утилиты lsinitramfs)