Локальная аутентификация в ОС Атлант по Рутокену семейства ЭЦП

Предварительная настройка

Если вы планируете использовать устройства Рутокен семейства ЭЦП, то в хост-машине необходимо в настройках роли добавить слой 18.layer.smartcards.sfs

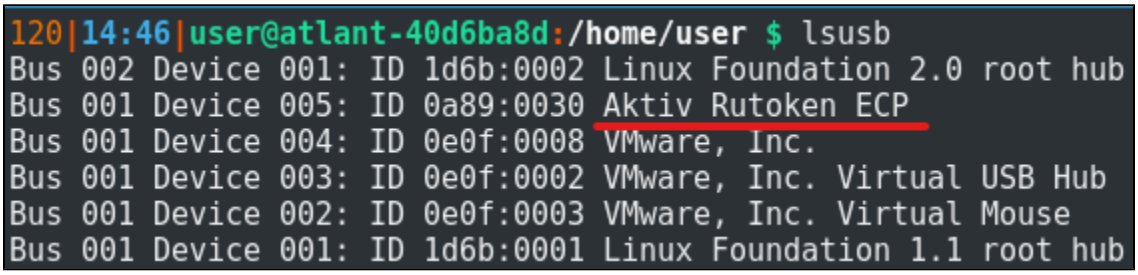
Проверка модели устройства

Подключите Рутокен к компьютеру.

Для определения названия модели откройте **Терминал** и введите команду:

```
lsusb
```

В результате в окне Терминала отобразится название модели Рутокена:



Убедитесь в том, что используете: **Aktiv Rutoken ECP**.

Создание ключей на Рутокене

Загрузите библиотеку rtpkcs11ecp по ссылке https://www.rutoken.ru/support/download/pkcs/ и установите ее в ОС командой:

```
sudo dpkg -i librtpkcs11ecp-X.X.X.X-X.x86_64.deb
```

Создайте ключевую пару RSA длиной 2048 бит с id "45" (его стоит запомнить, он понадобится при создании сертификата):

```
pkcs11-tool --module /usr/lib/librtpkcs11ecp.so --keypairgen --key-type rsa:2048 -l --id 45
```

Проверьте сгенерированный ключ:

```
pkcs11-tool --module /usr/lib/librtpkcs11ecp.so -O
```

Создание сертификата и импорт его на Рутокен через OpenSSL 1.1.x

Запустите `openssl`:

```
openssl
```

Сформируйте самоподписанный сертификат или заявку на сертификат:

```
engine dynamic -pre SO_PATH:/usr/lib/x86_64-linux-gnu/engines-1.1/pkcs11.so -pre ID:pkcs11 -pre LIST_ADD:1 -pre
LOAD -pre MODULE_PATH:librtpkcs11ecp.so

req -engine pkcs11 -x509 -new -key 0:45 -keyform engine -out client.pem -subj "/C=RU/ST=Moscow/L=Moscow/O=Aktiv
/OU=dev/CN=testuser/emailAddress=testuser@mail.com"
```

Сохраните сертификат на Рутокене:

```
pkcs11-tool --module /usr/lib/librtpkcs11ecp.so -l -y cert -w ./client.pem --id 45
```

Занесение сертификата в список доверенных

Занесите сертификат в список доверенных сертификатов:

```
mkdir ~/.eid
chmod 0755 ~/.eid
cat client.pem >> ~/.eid/authorized_certificates
chmod 0644 ~/.eid/authorized_certificates
```

Настройка pam_pkcs11

Создайте (например, на Рабочем столе) текстовый файл pam_pkcs11.conf со следующим содержимым:

```
pam_pkcs11 {
  nullok = false;
  debug = false;
  use_first_pass = false;
  use_authtok = false;
  card_only = false;
  wait_for_card = false;
  use_pkcs11_module = rutokenecp;

  # Aktiv Rutoken ECP
  pkcs11_module rutokenecp {
    module = /usr/lib/librtpkcs11ecp.so;
    slot_num = 0;
    support_thread = true;
    ca_dir = /etc/pam_pkcs11/cacerts;
    crl_dir = /etc/pam_pkcs11/crls;
    cert_policy = signature;
  }

  use_mappers = digest;

  mapper_search_path = /usr/lib/pam_pkcs11;

  mapper digest {
   debug = false;
   module = internal;
   algorithm = "sha1";
   mapfile = file:///etc/pam_pkcs11/digest_mapping;
  }

}
```

Поместите файл в каталог /etc/pam_pkcs11/:

```
cd /etc/pam_pkcs11/

sudo mv pam_pkcs11.conf pam_pkcs11.conf.default #

sudo mkdir cacerts crls

sudo cp /path/to/your/pam_pkcs11.conf /etc/pam_pkcs11/
```

Настройка Digest Mapping

Определите поля вашего сертификата с помощью следующей команды:

```
sudo pkcs11_inspect
```

В результате отобразится сообщение:

```
sudo pkcs11_inspect
PIN for token:
Printing data for mapper digest:
CB:13:CA:34:AC:04:CD:BF:A6:17:29:2F:C8:00:6A:D5:54:B8:0B:BB
```

Скопируйте строчку с описанием сертификата в файл /etc/pam_pkcs11/digest_mapping в формате:

```
<  pkcs11_inspect> -> <_>
```

Пример заполнения файла:

```
sudo cat /etc/pam_pkcs11/digest_mapping
CB:13:CA:34:AC:04:CD:BF:A6:17:29:2F:C8:00:6A:D5:54:B8:0B:BB -> user
```

Попробуйте аутентифицироваться:

```
su <username>
```

Терминал должен запросить PIN-код Рутокена:

```
120|15:05|user@atlant-40d6ba8d:/home/user $ su user
Smartcard authentication starts
Smart card found.
Добро пожаловать Rutoken ECP <no label>!
Smart card PIN:
verifying certificate
Checking signature
```

На экране отобразится приветствие: