Аутентификация в CentOS 7 и Goslinux при помощи ГОСТ ключей на Рутокен ЭЦП

Проверка работы Рутокен ЭЦП 2.0

Подключите Рутокен ЭЦП 2.0 к компьютеру.

Убедитесь в том, что на USB-токене или считывателе для смарт-карт светится индикатор.

Откройте Terminal.

Для проверки корректности работы Рутокен ЭЦП 2.0 введите команду:

```
$ pcsc_scan
```

Если Рутокен ЭЦП 2.0 не работает, то в окне терминала отобразится сообщение об этом.

Если Рутокен ЭЦП 2.0 работает, то в окне терминала отобразится сообщение об этом.

Для остановки сервиса pcscd введите команду:

```
$ sudo service pcscd stop
```

Настройка системы

Перед началом работы, установите следующие пакеты:

```
sudo yum install ccid opensc pam_pkcs11 gdm-plugin-smartcard p11-kit
```

Проверьте, что у вас установлен openssl версии 1.1 и выше

Скачайте pam модуль и положите его по адресу /usr/lib64/security (или /lib64/security для goslinux)

Установите права доступа:

```
sudo chmod 644 /usr/lib/x86_64-linux-gnu/librtpam.so.1.0.0
```

Загрузите модуль librtpkcs11ecp.so и установите:

```
sudo rpm -i librtpkcs11ecp_1.9.15.0-1_x86_64.rpm
```

Проверяем, что все настроили правильно:

```
pkcs11-tool --module /usr/lib64/librtpkcs11ecp.so -T
```

Далее потребуется скачать сертификат с токена, если его нету, то генерируем его согласно следующему пункту

Генерация сертификата и запись его на Рутокен

Собирайте OpenSC новее чем 0.19.0.

https://github.com/OpenSC/OpenSC/

Создаем ключи на токене

```
pkcs11-tool --module /usr/lib64/librtpkcs11ecp.so --keypairgen --key-type GOSTR3410-2012-256:B -l --id 3435
```

Узнайте где находится файл с конфигурацией и папка с энджинами openssl с помощью команды:

```
openssl version -a
```

Скачайте rtengine, который можно найти в комплекте разработчика и поместите его в директорию энджинов

Зайдите в файл конфигурации openssl.cnf и впишите туда следующее:

```
#
openssl_conf = openssl_def
...
#
# OpenSSL default section
[openssl_def]
engines = engine_section
# Engine section
[engine_section]
rtengine = rtengine_section
# Engine rtengine section
[rtengine_section]
engine_id = rtengine
dynamic_path = /path/to/engine/librtengine.so
pkcs11_path = /usr/lib64/librtpkcs11ecp.so
RAND_TOKEN = pkcs11:manufacturer=Aktiv%20Co.;model=Rutoken%20ECP;serial=2adc8d87 #
default_algorithms = CIPHERS, DIGEST, PKEY, RAND
```

Теперь создадим самоподписанный сертификат для наших ключей на токене:

```
openssl req -utf8 -x509 -keyform engine -key "pkcs11:id=45" -engine rtengine -out cert.crt
```

Загружаем его на токен:

```
pkcs11-tool --module /usr/lib64/librtpkcs11ecp.so -l -y cert -w cert.crt --id 3435
```

Регистрация сертификата в системе

Скачиваем сертификат с токена (если вы пользовались вышеописанной инструкцией для получения сертификата, то ID = 45)

```
pkcs11-tool --module /usr/lib64/librtpkcs11ecp.so -r -y cert --id 3435 --output-file cert.crt
```

Конвертируем его в PEM формат

```
openssl x509 -in cert.crt -out cert.pem -inform DER -outform PEM
```

Добавляем сертификат в список доверенных сертификатов для данного пользователя

```
mkdir ~/.eid

chmod 0755 ~/.eid

cat cert.pem >> ~/.eid/authorized_certificates

chmod 0644 ~/.eid/authorized_certificates
```

Настройка аутентификации

Открываем файл /etc/pam.d/system-auth

```
sudo vim /etc/pam.d/system-auth
```

И записываем в самом начале следующую строчку:

```
auth sufficient librtpam.so.1.0.0 /usr/lib64/librtpkcs11ecp.so
```

Пробуем пройти аутентификацию

```
su <username>
```

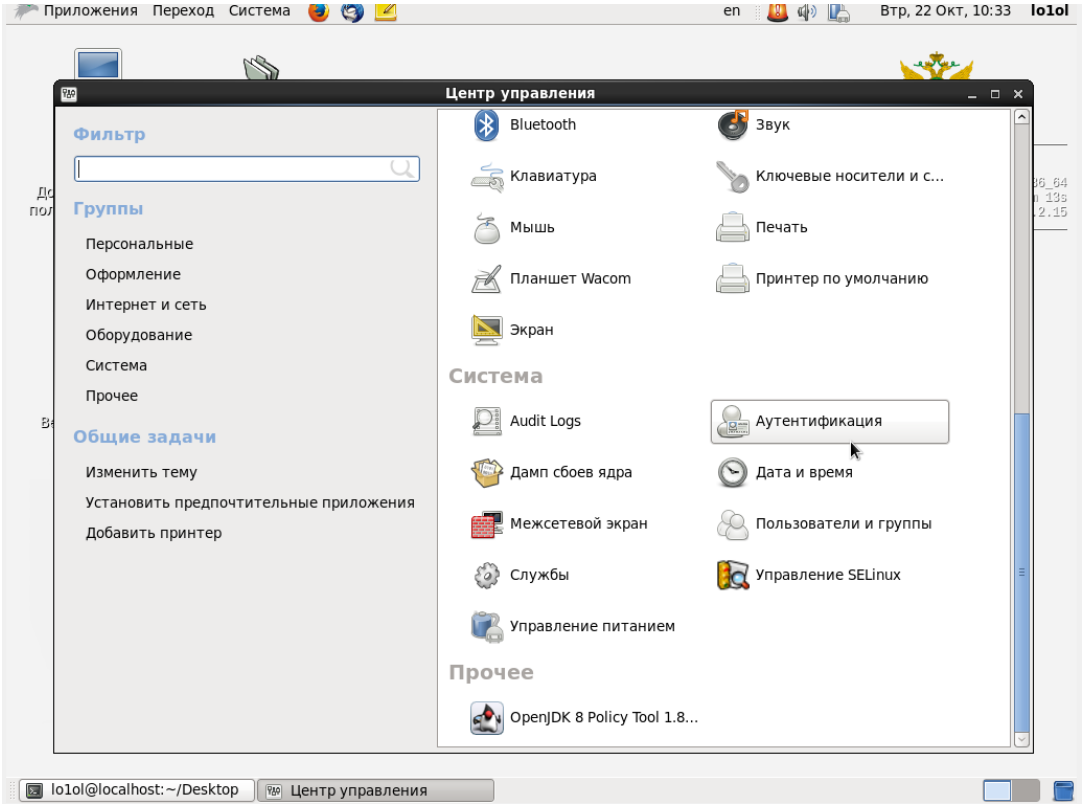
Если все прошло успешно, то появится просьба ввести пароль от токена, иначе что-то пошло не так. Узнать причину того, что пошло не так, можно через логи в /var/log/messages

Добавление возможности использования смарт-карт и токенов для входа в систему

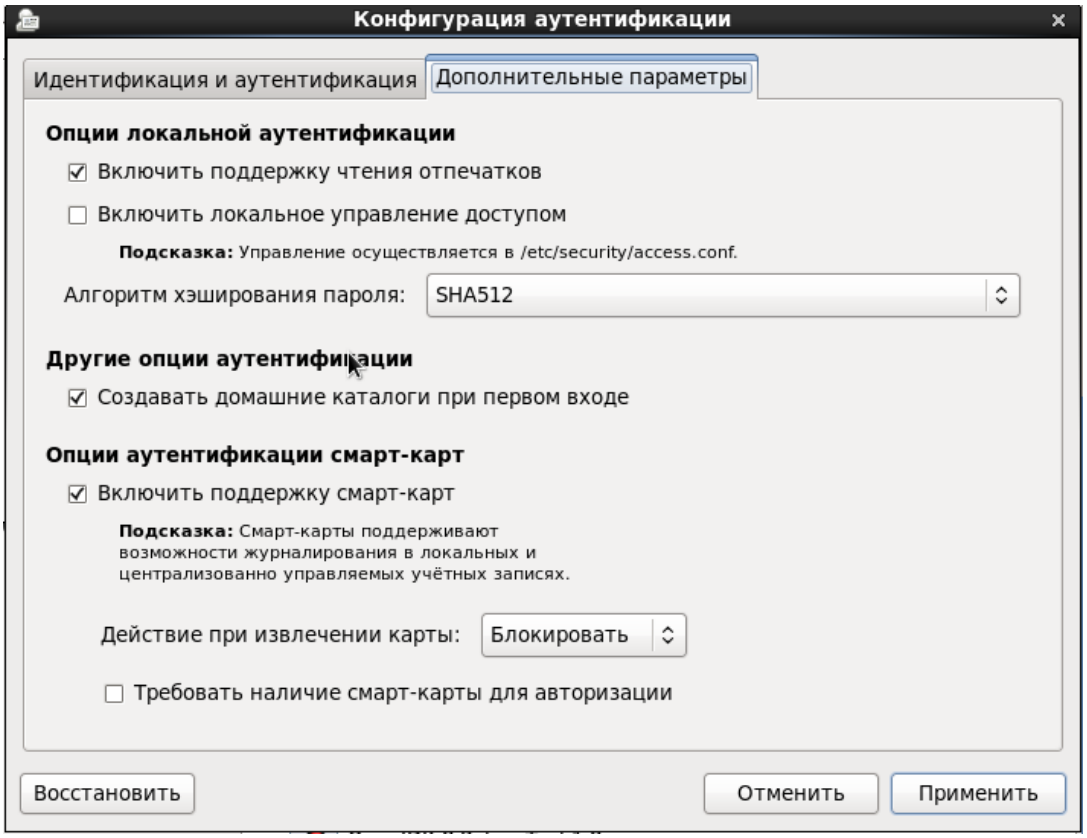
В Goslinux

Для того, чтобы добавить возможность входа в систему с помощью смарт-карт, нужно

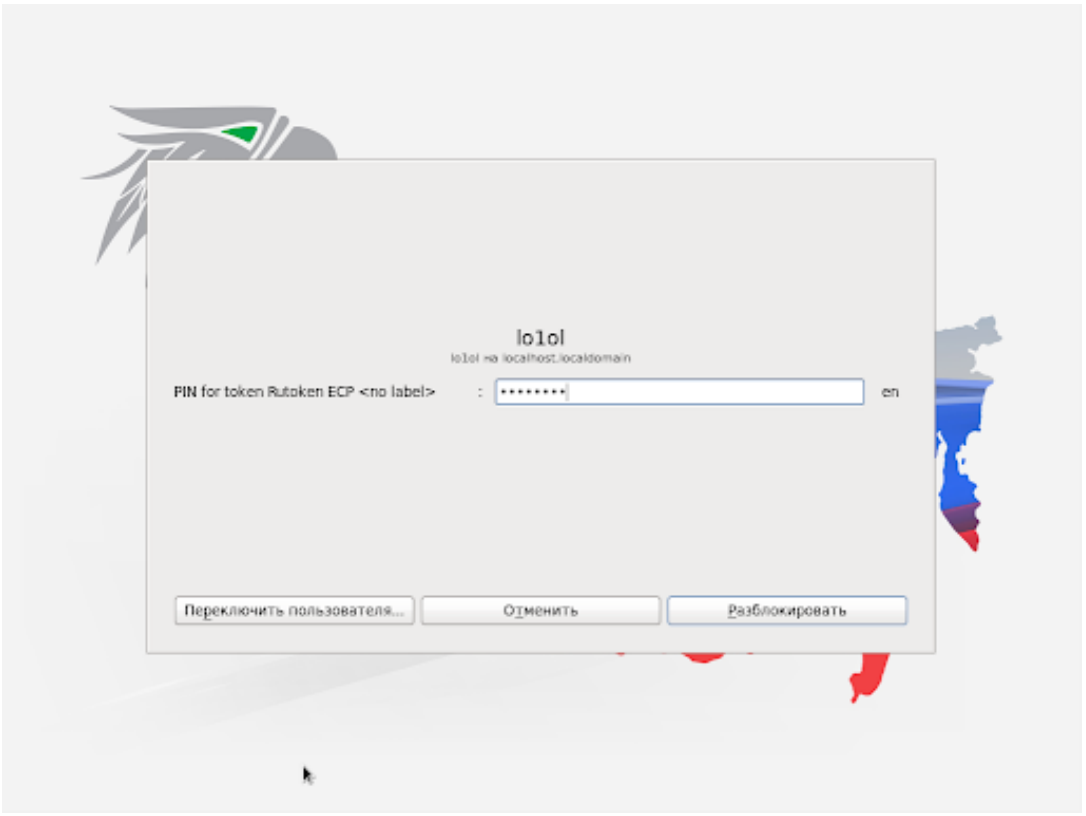
1. Зайти в панель настройки аутентификации



2. Включить поддержку смарт-карт



3. Попробовать войти



В CentOS 7

Пока удалось настроить только для оболочки KDE. Чтобы активировать введите в терминале

```
autoconfig --enablesmartcard
```

Теперь при входе в систему вы можете ввести пароль от токена если он вставлен и аутентификация пройдет успешно