Упрощенная настройка аутентификации в домене FreeIPA с помощью Рутокен ЭЦП

Astra Linux, РЕД ОС, ROSA Linux

Смена домена

При выходе из домена желательно очистить директорию, содержащую сертификаты старого домена. Для этого достаточно выполнить команду:

```
sudo rm -r  /etc/pki/nssdb/
```

Это необходимо для того, чтобы при входе в новый домен, корневой сертификат старого домена не помешал установке нового.

Для Astra Linux Смоленск и РЕД ОС

Использование домена и клиента с разными ОС

Доменная и клиентская машины не обязательно должны иметь одинаковую операционную систему для корректной аутентификации по смарт-картам. Но тем не менее, если версии SSSD – разные, как у Astra Linux (SSSD 16.1.3) и РЕД ОС (SSSD 2.0.0), то на доменной машине должна быть установлена ОС с более новой версией SSSD.

В обратную же сторону настройка домена возможна.

Настройка сервера. Создание домена FreeIPA и пользователя

Для демонстрации настройки было использовано два стенда. Первый был использован в качестве сервера FreeIPA. Он был настроен с помощью следующей последовательности команд:

Astra Linux. Настройка сервера

```
#       astradomain.ad  server
sudo hostnamectl set-hostname server.astradomain.ad

#

#   fly-admin-freeipa-server
sudo apt-get update
sudo apt-get install fly-admin-freeipa-server

#   freeipa
sudo fly-admin-freeipa-server
```

РЕД ОС. Настройка сервера

```
#       astradomain.ad  server
sudo hostnamectl set-hostname server.astradomain.ad

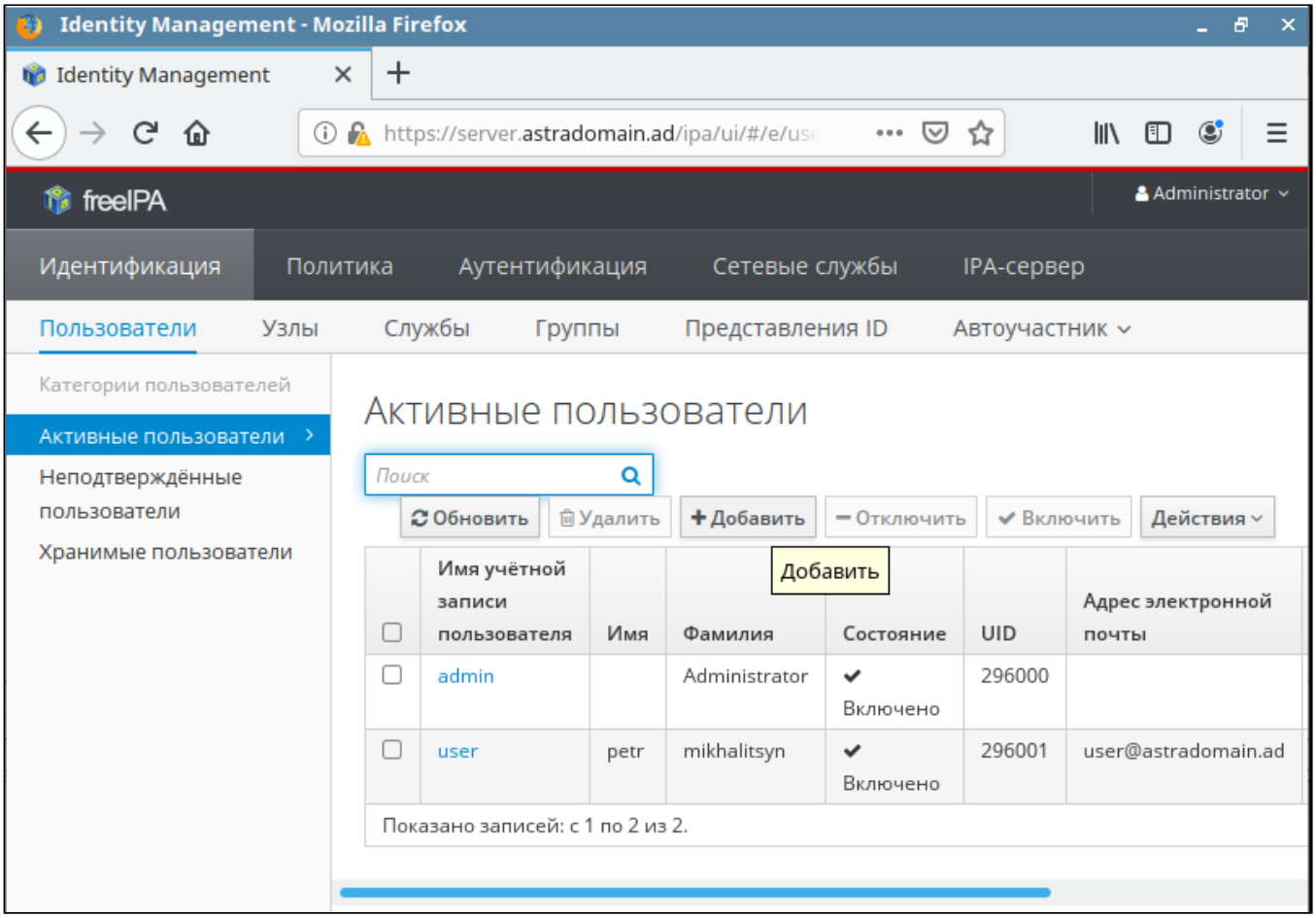
#

#   ipa-server
sudo yum update
sudo yum -y install bind bind-dyndb-ldap ipa-server*

#   freeipa
sudo ipa-server-install --mkhomedir
```

После настройки программы установки сервера FreeIPA отобразится ссылка на веб-интерфейс для управления доменом. Вам потребуется создать нового пользователя, для которого и будет настраиваться доступ по Рутокену.

Для этого перейдите на вкладку "Идентификация" → "Пользователи" → "Активные пользователи" и добавьте нового пользователя. В нашем случае был создан пользователь "user".



Настройка клиента. Подключение к домену

Для пользователей Astra Linux

Если в качестве клиента выступает Astra Linux Smolensk, то на нем должно быть установлено пятое обновление безопасности.

После добавления нового пользователя, переходим к настройке клиента. Настройка была осуществлена с помощью следующих команд:

Настройка клиента

```
#       astradomain.ad  client
sudo hostnamectl set-hostname client.astradomain.ad

#

#    .
CON_NAME="  1"
#  ,
INT_NAME="eth0"
#  dns
DNS_SERVER_IP=10.0.2.37
#
sudo nmcli con down "$CON_NAME"

#     -   $INT_NAME
sudo nmcli con mod "$CON_NAME" connection.interface-name $INT_NAME

#  DNS -  DNS_SERVER_IP  IP-  DNS.       DNS.      DNS     FreeIPA.     IP
sudo nmcli con mod "$CON_NAME" ipv4.dns "$DNS_SERVER_IP 8.8.8.8"
sudo nmcli con mod "$CON_NAME" ipv4.ignore-auto-dns yes

#
sudo nmcli con up "$CON_NAME"


###  Astra Linux
#
sudo apt-get update
sudo apt-get install fly-admin-freeipa-client

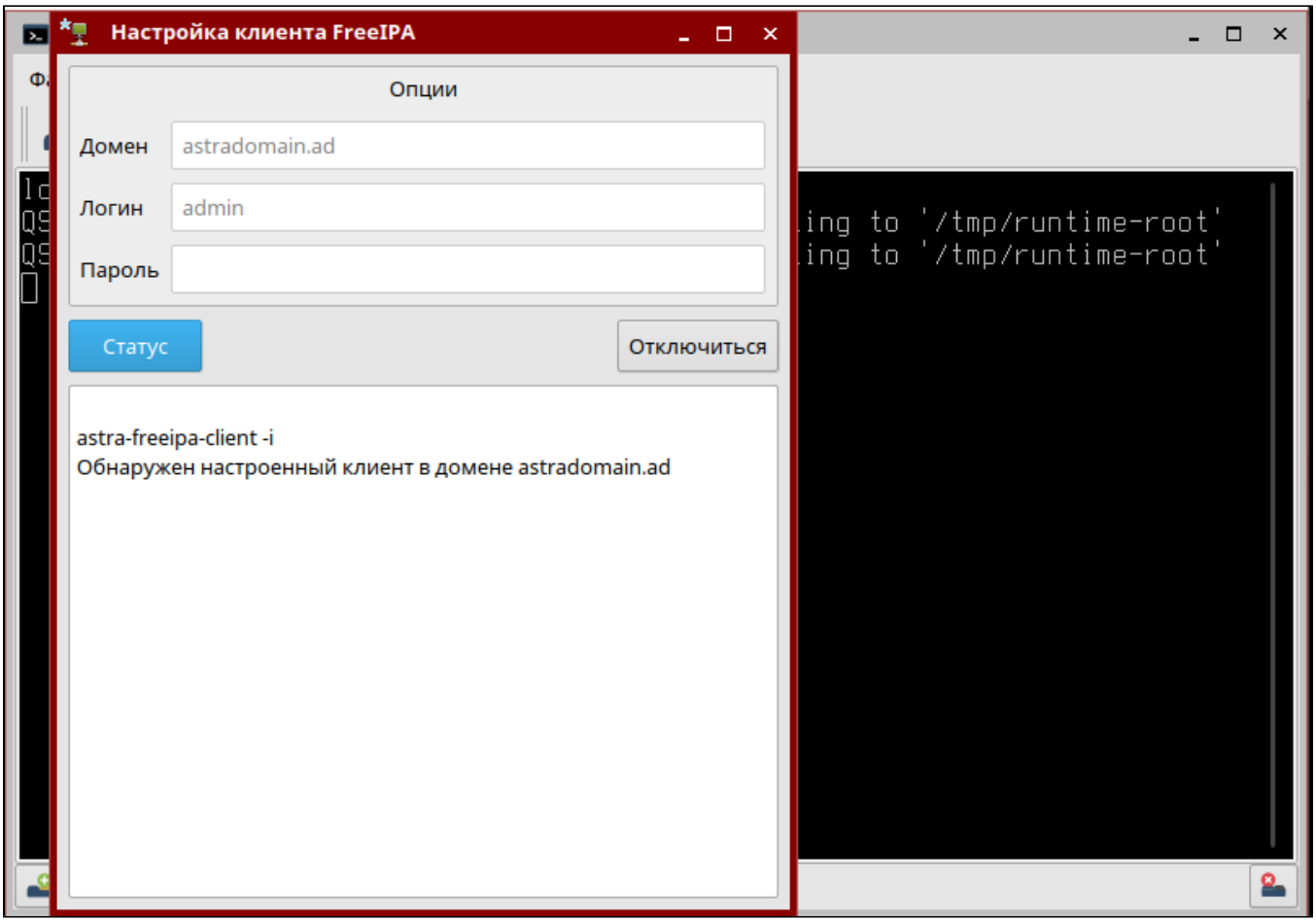
#      admin
sudo fly-admin-freeipa-client


###
#
sudo yum update
sudo yum -y install ipa-client

###  Rosa
#
sudo urpmi --auto-update
sudo urpmi ipa-client libini_config5 compiz ldb-utils

#      admin
sudo ipa-client-install --mkhomedir --enable-dns-updates
```

После подключения настройщик должен написать, что обнаружен настроенный клиент в домене astradomain.ad.



Попробуем подключиться к созданному пользователю user:

Аутентификация в качестве пользователя user
`su user`

Если после ввода пароля вам удалось аутентифицироваться как пользователь user, значит настройка прошла успешно.

Настройка аутентификации по Рутокену для клиента

Создание заявки на сертификат

Для упрощения настройки можно воспользоваться графической утилитой по работе с Рутокенами в линукс. Скачаем ее:

Установка скрипта настройки

```
#  red os
sudo yum update
sudo yum install git

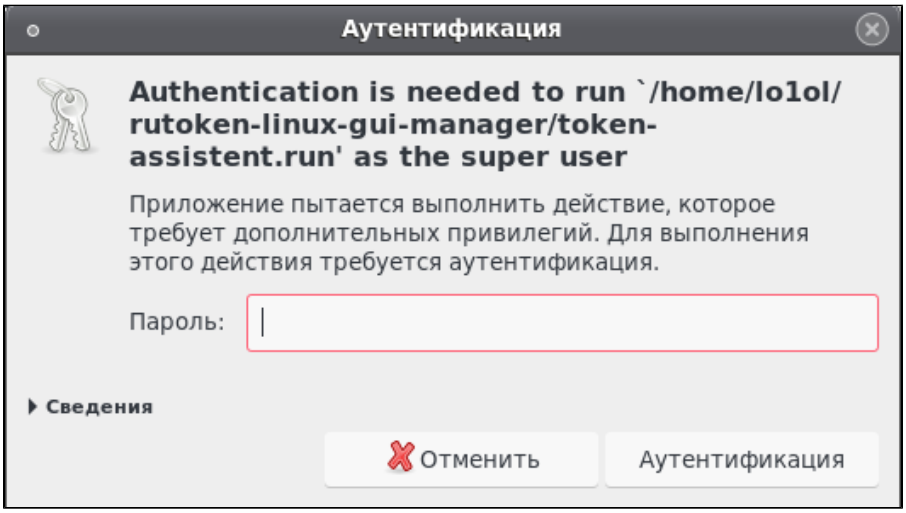
#  astra  alt linux
sudo apt-get update
sudo apt-get install git

#  rosa
sudo urpmi --auto-update
sudo urpmi git

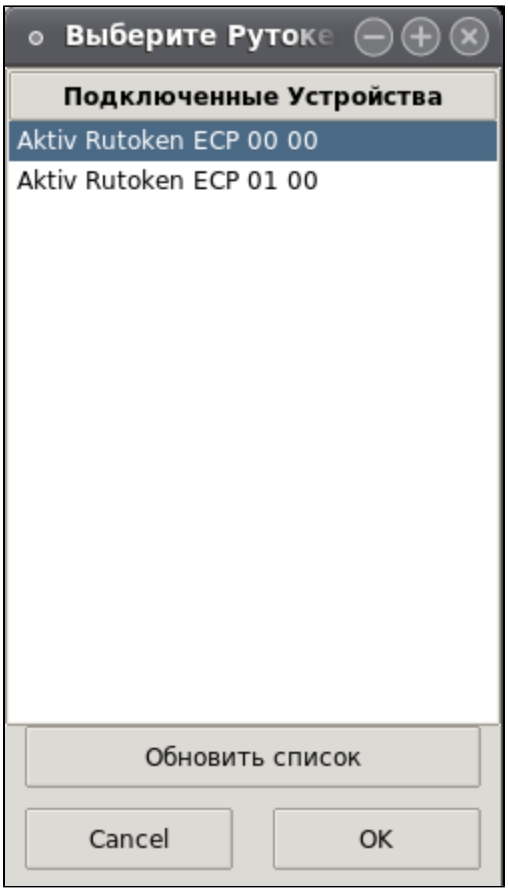
git clone https://github.com/AktivCo/rutoken-linux-gui-manager --recursive
```

После того, как настройщик был загружен, его можно запустить двойным щелчком по названию файла *token-assistent.run.* Если программа открылась вместе с терминалом, то для запуска необходимо создать ярлык, с помощью установщика *token-assistent.installer*. После запуска установщика появится ярлык *token-assistent.desktop*, который нужно использовать для запуска программы.

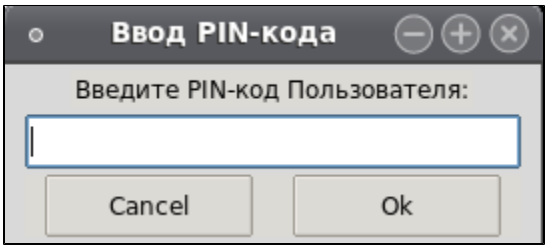
При первом запуске программа может запросить пароль администратора для получения обновлений. Загрузка обновлений может занять несколько минут.



После загрузки обновлений, программа предложит выбрать токен, который мы хотим использовать для локальной аутентификации. Если нужный Рутокен не появился в списке, то можно нажать на кнопку для обновления списка устройств:



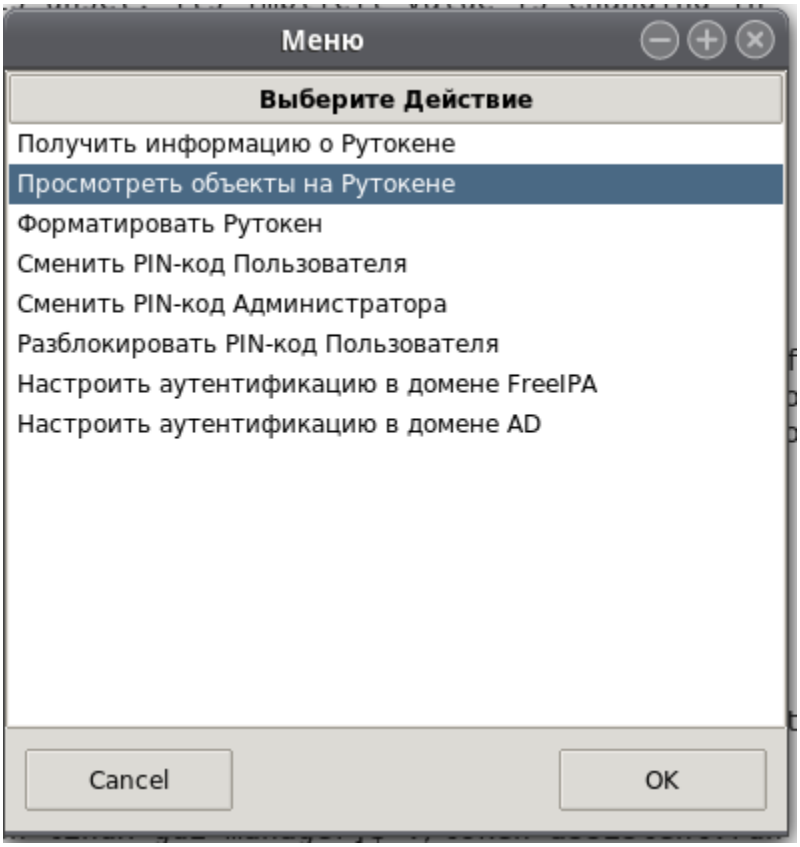
Далее вводим PIN-код Рутокена:



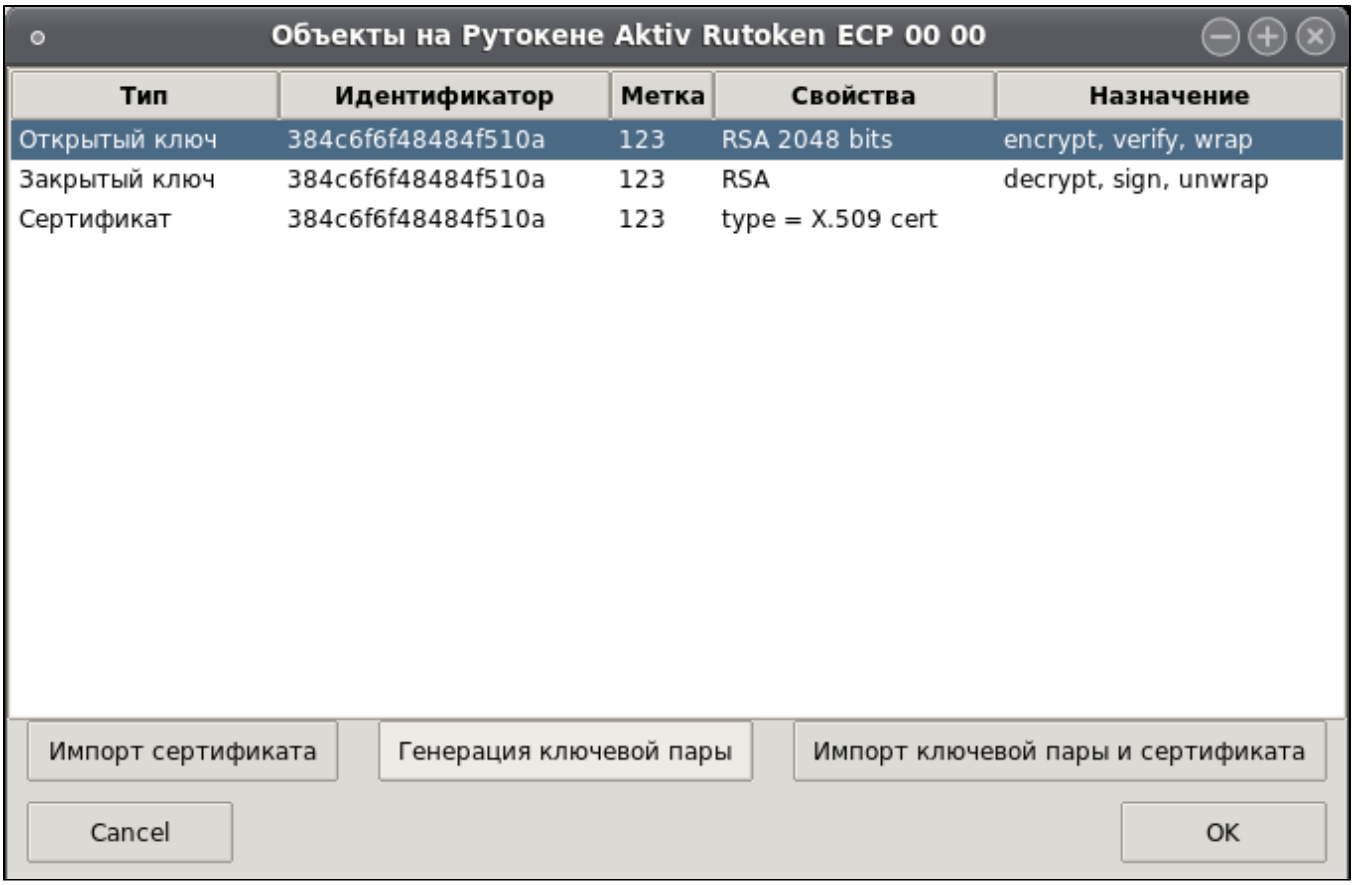
На Рутокене отсутствует ключевая пара и сертификат выданный УЦ для аутентификации:

Генерация ключевой пары

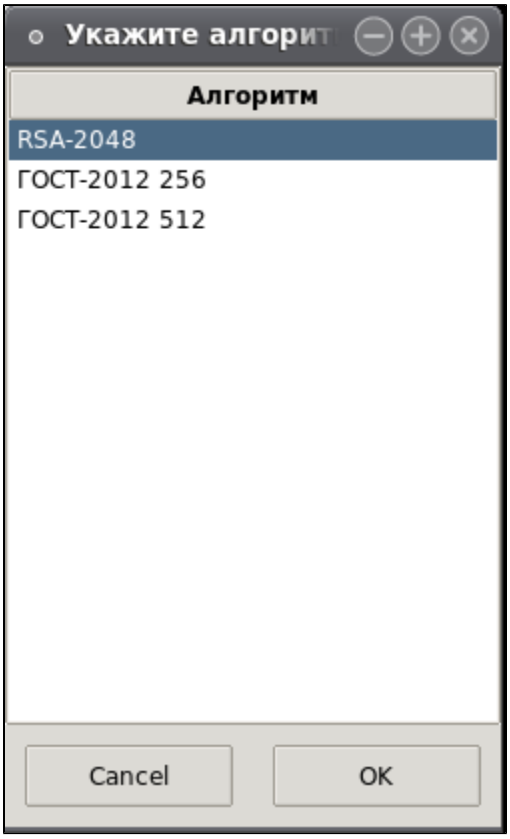
Откроем список объектов на Рутокене:



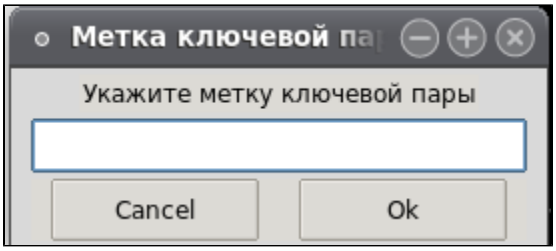
В первую очередь, сгенерируем ключ. Для этого в окне просмотра объектов выберем опцию для генерации ключевой пары:



В окне выбора алгоритма ключа необходимо указать "RSA-2048"

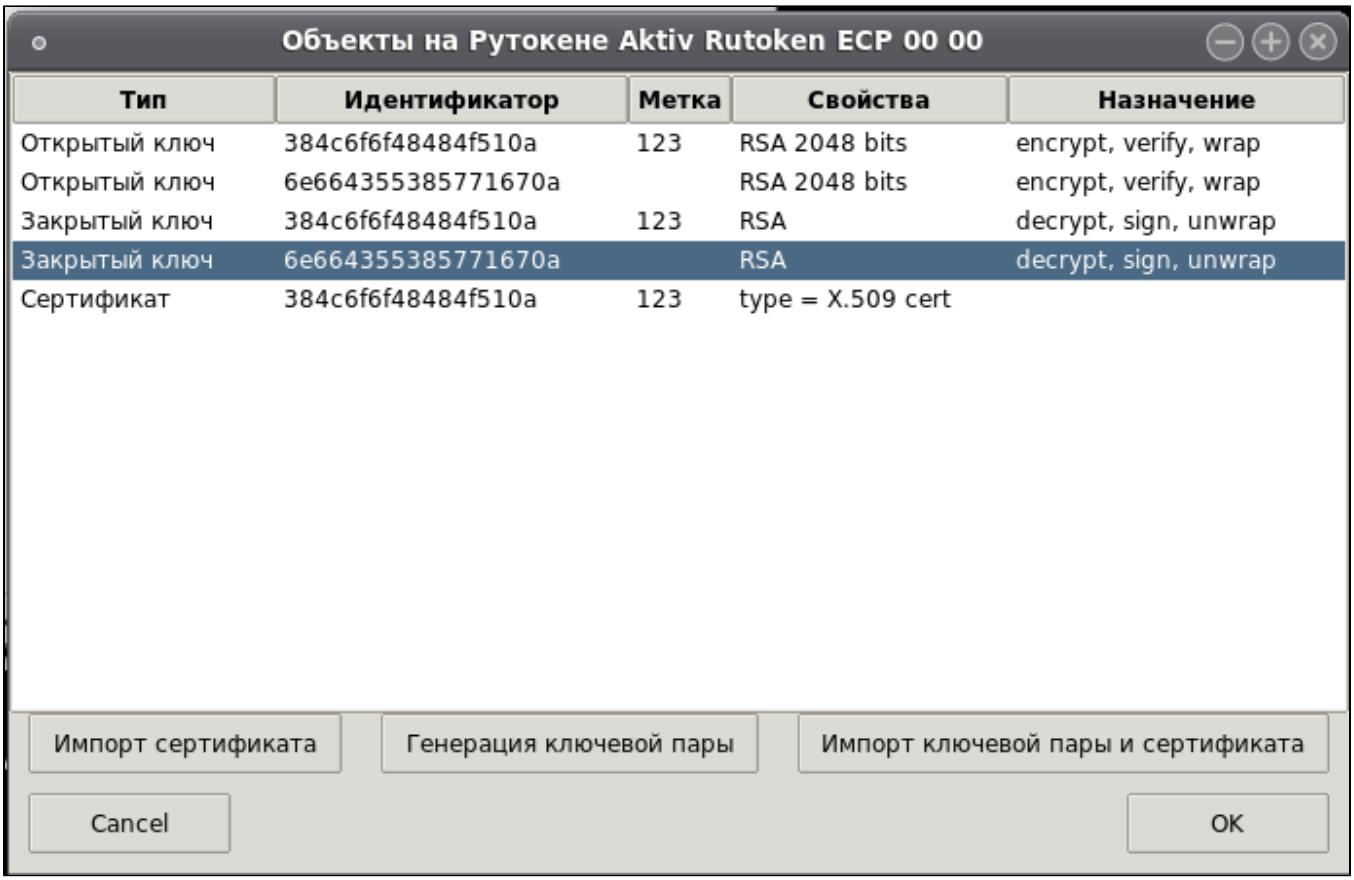


Метку ключа можно оставить пустой:

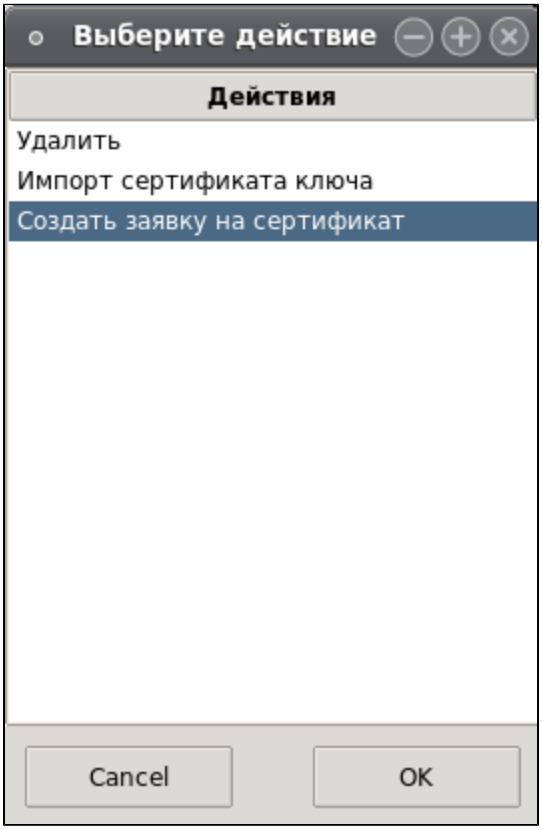


Создание заявки на сертификат

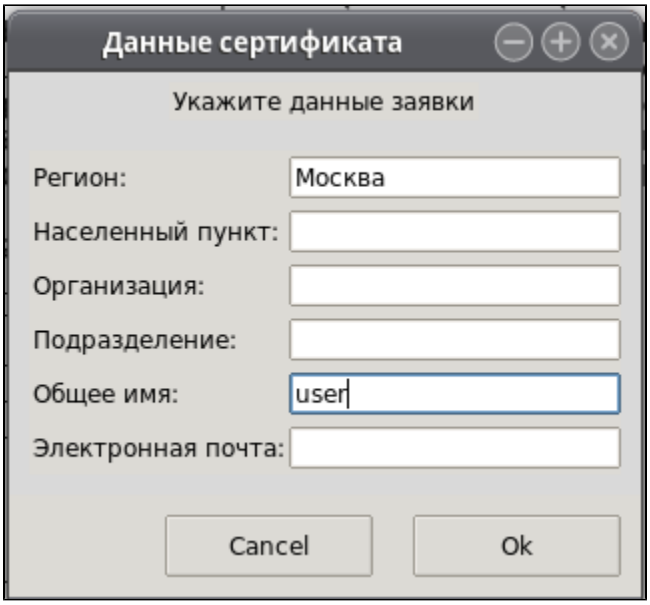
После генерации ключевой пары, необходимо создать для неё заявку на сертификат. В списке объектов выберем закрытый ключ из ключевой пары, для которой хотим создать заявку на сертификат:



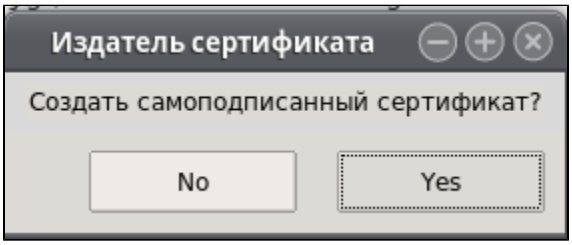
В открывшемся окне выберем опцию для создания заявки на сертификат:



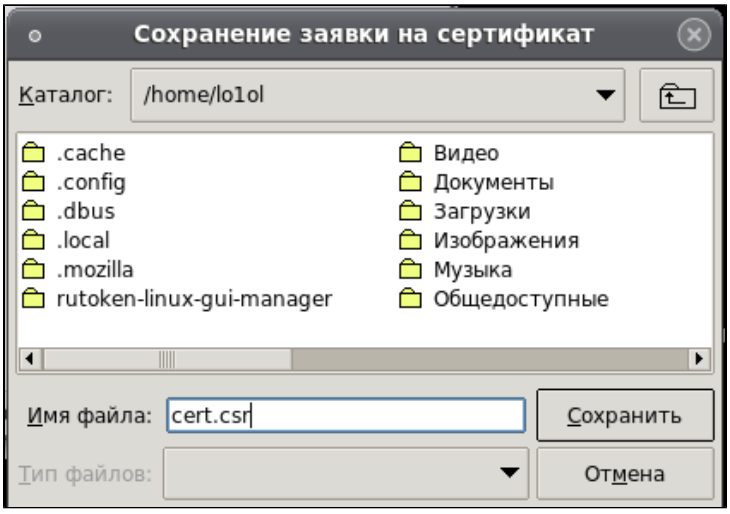
Введём данные сертификата. В графе **Общее имя** необходимо указать имя пользователя, для которого мы создаем сертификат для аутентфиикации:



Далее нас попросят выбрать, создать ли самоподписанный сертификат или создать заявку на сертификат Выбираем **"Нет"**:



Укажем путь, куда сохраним заявку на сертификат:



Данную заявку в дальнейшем следует отправить в ваш УЦ, для выдачи сертификата.

Созданную заявку копируем и отправляем на сервер. Распечатать ее можно с помощью команды:

Вывод заявки

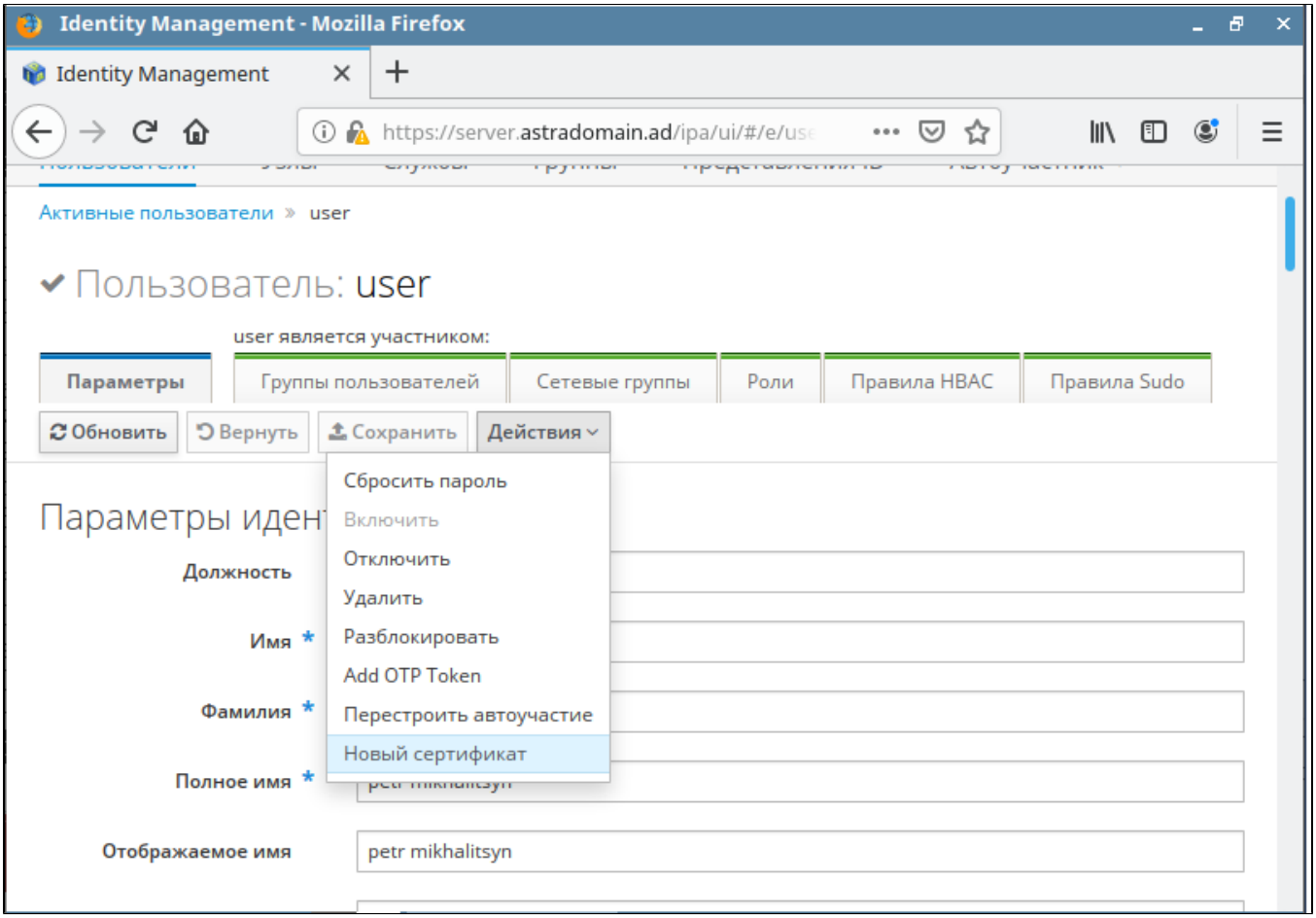
```
cat cert.csr
```

Создание сертификата

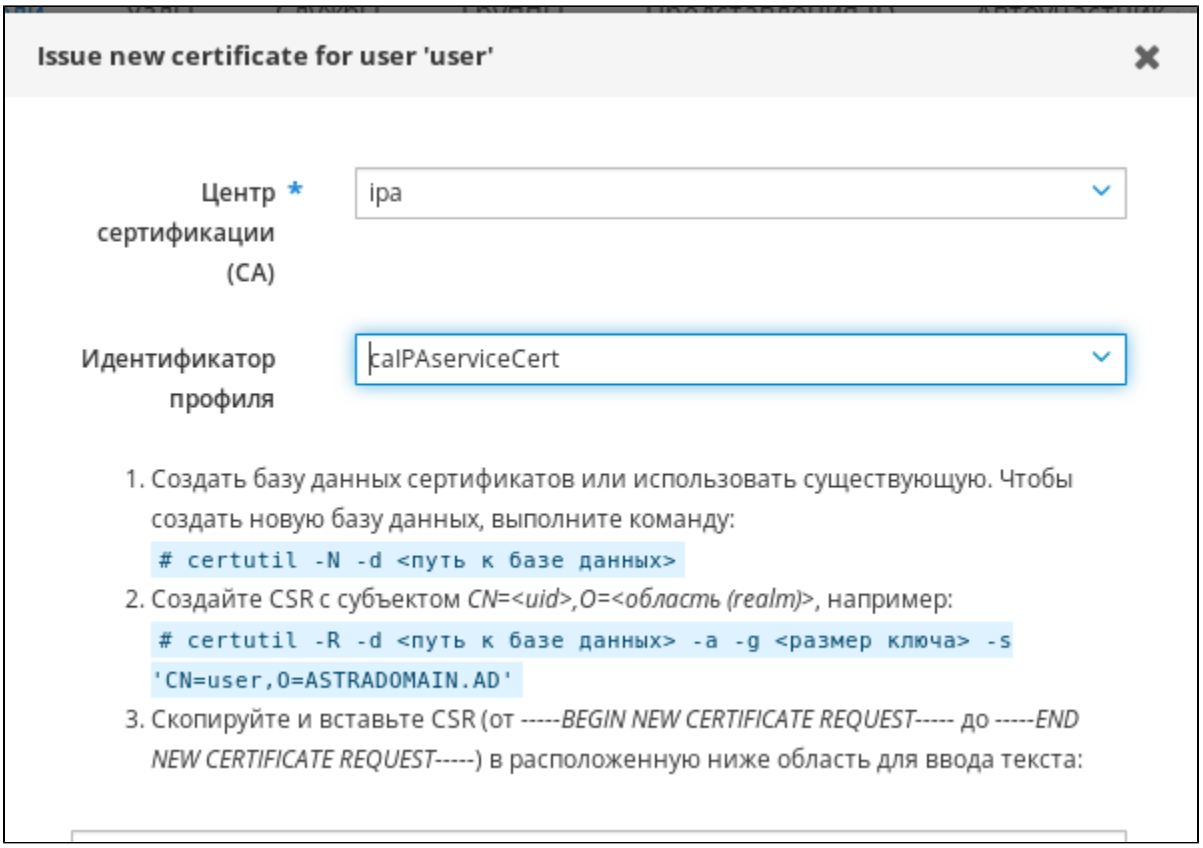
Переходим к серверу, который получил нашу заявку.

Чтобы создать сертификат по данной заявке для данного пользователя, перейдем на вкладку "Идентификация" → "Пользователи" → "Активные пользователи" и выберем нашего пользователя.

На новой вкладке выбираем "Действия"→"Новый сертификат". В открывшееся окно вставляем нашу заявку.

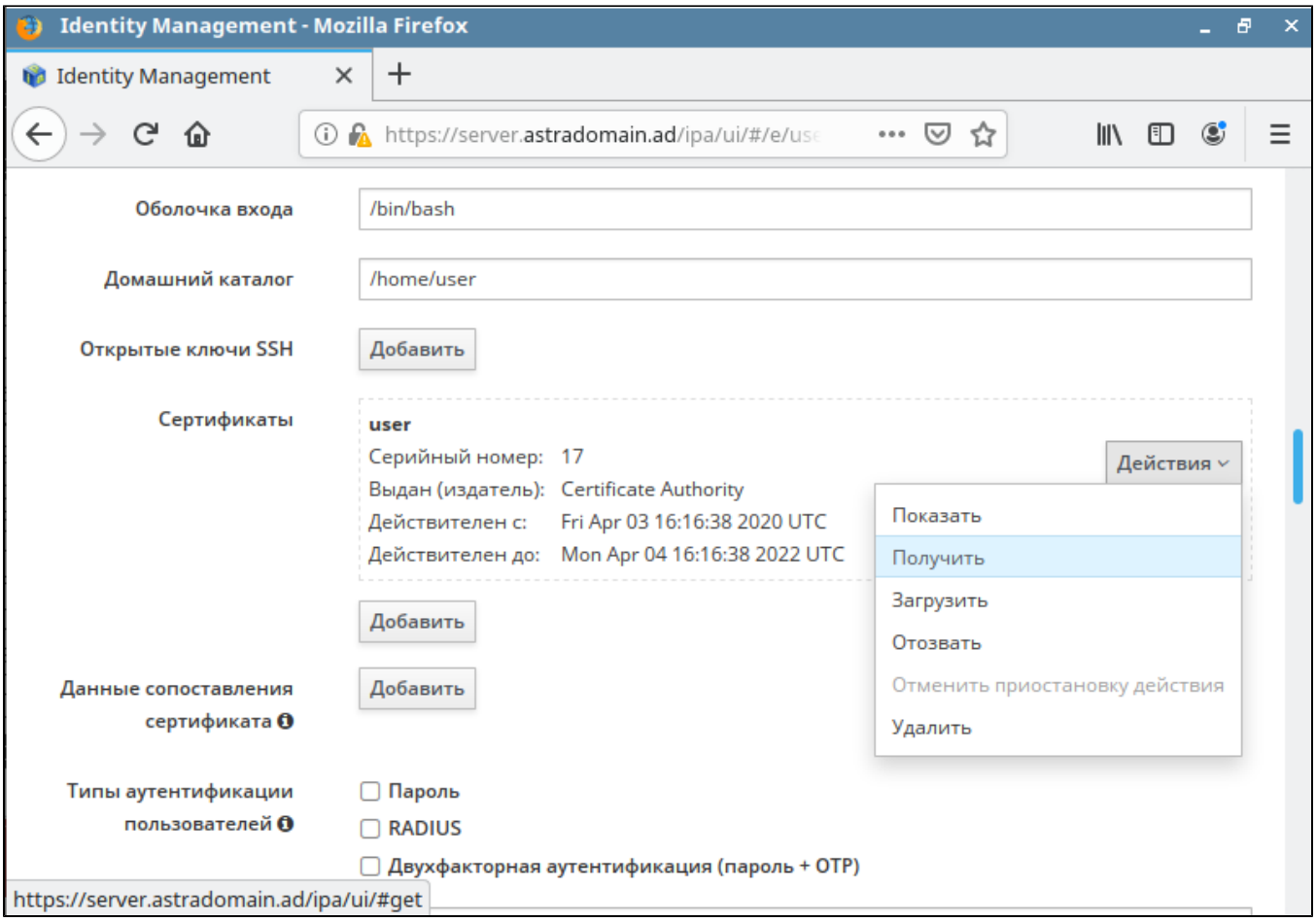


В поле **Идентификатор пользователя** необходимо указать **caIPAserviceCert**



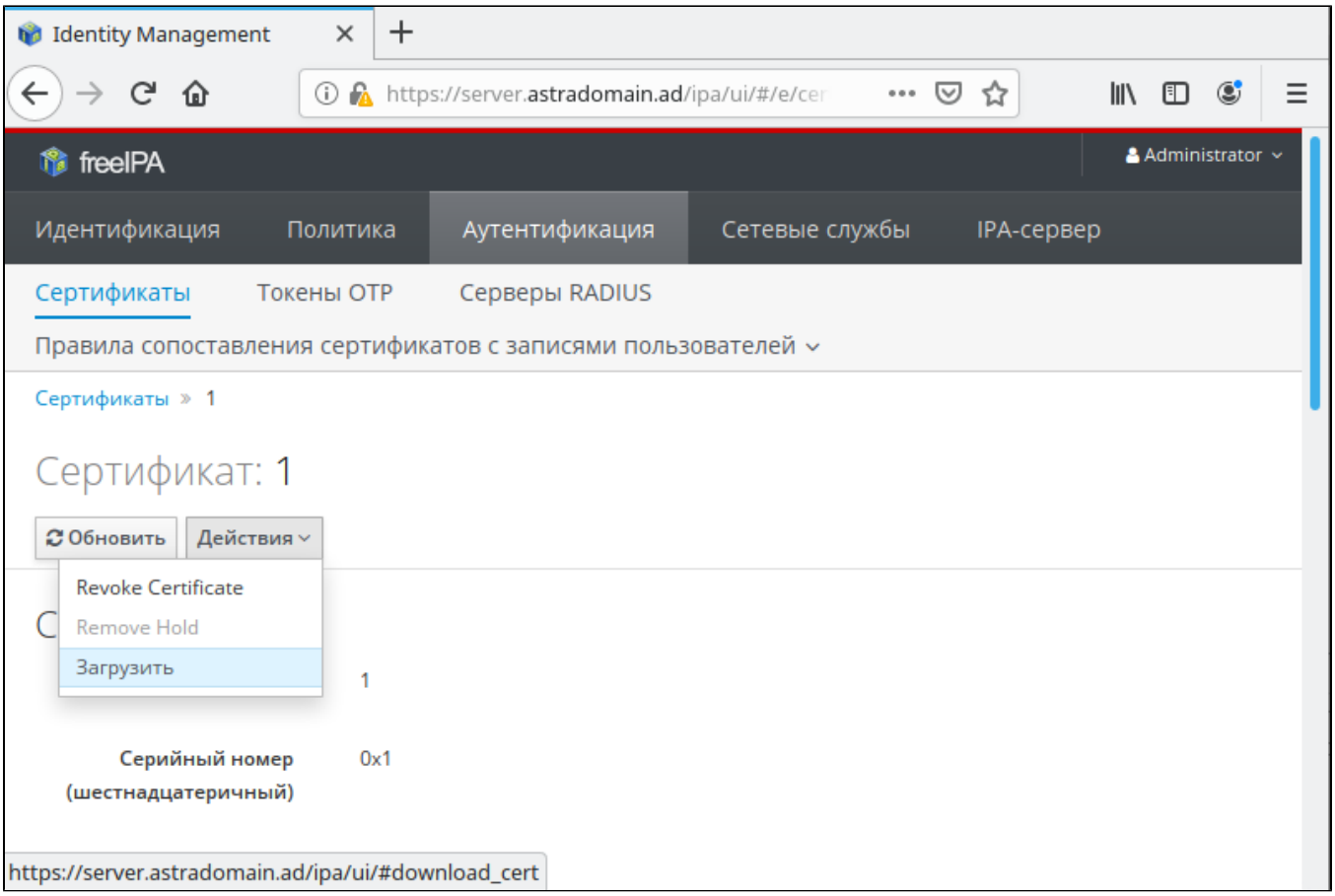
Выданный сертификат можно получить на этой же вкладке, переместившись чуть ниже до пункта с сертификатами.

Нажмем "Загрузить" и отправим сертификат пользователю.



Также пользователю потребуется корневой сертификат УЦ, его можно получить на вкладке "Аутентификация"→"Сертификаты".

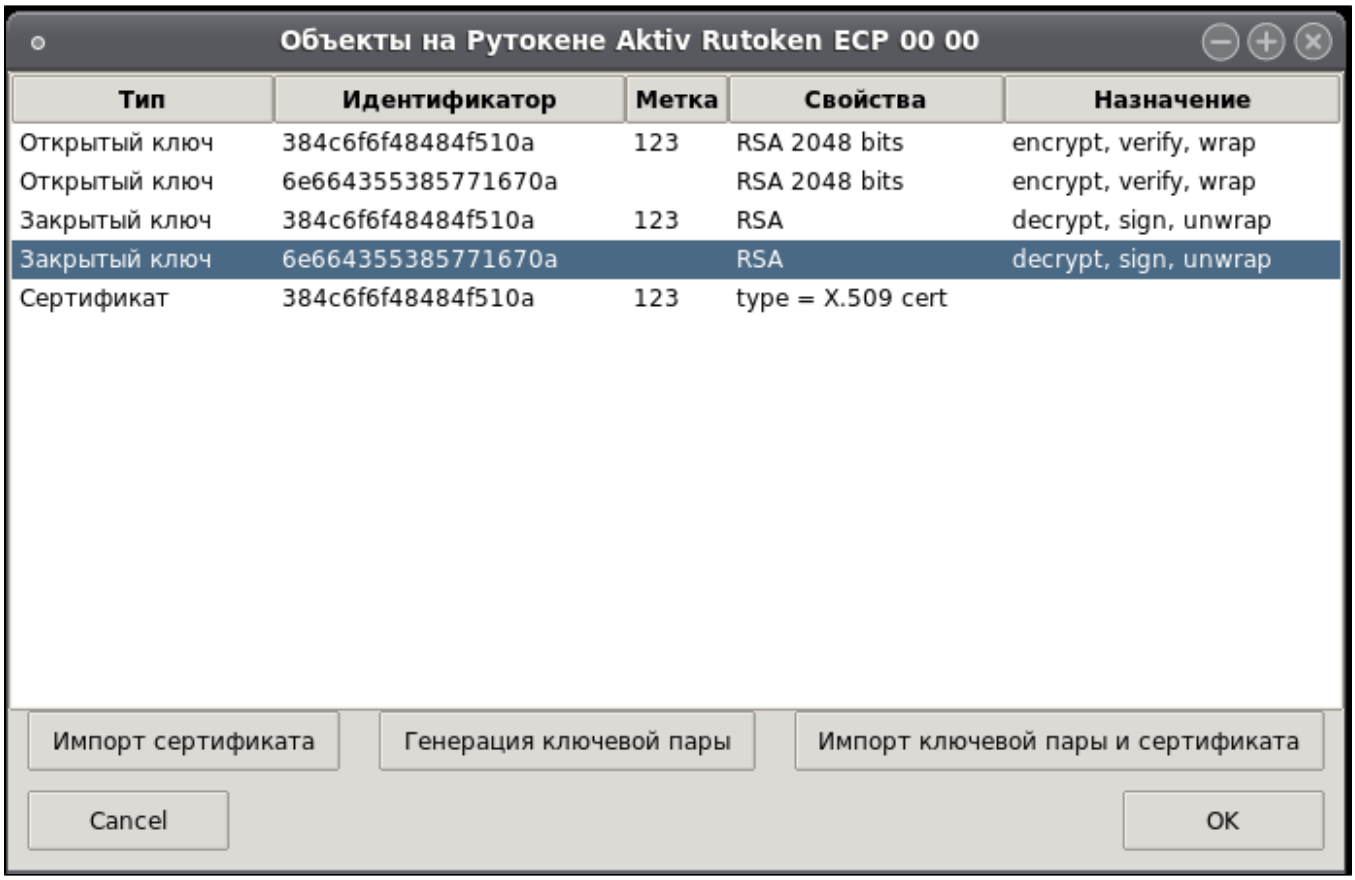
Выбираем самый первый сертификат и переходим на вкладку "Действия"→ "Загрузить".



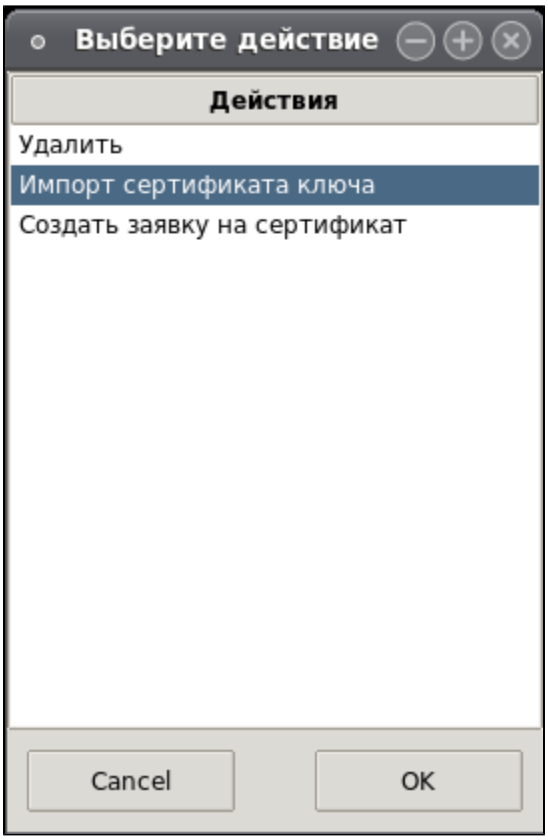
После этого полученный сертификат пользователя и УЦ отправляем клиенту.

Импорт сертификата на Рутокен

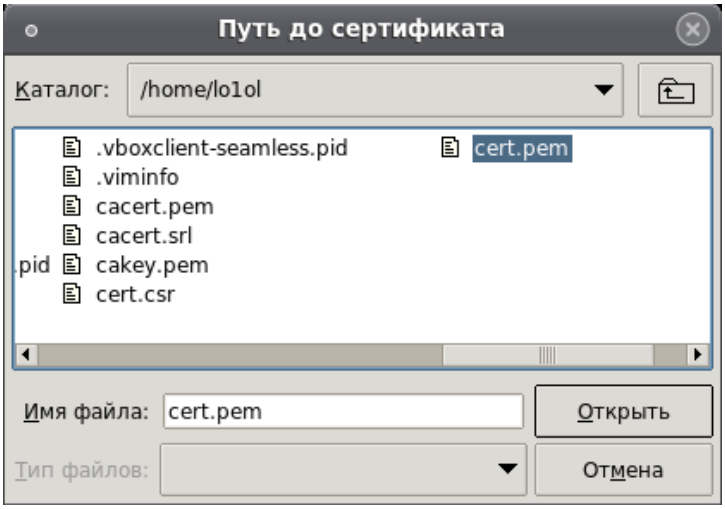
Повторно запускаем программу по работе с Рутокенами. Выбираем необходимый токен, вводим PIN-код. Открываем просмотр объектов. В окне просмотра объектов выберем закрытый ключ, для которого выдан сертификат:



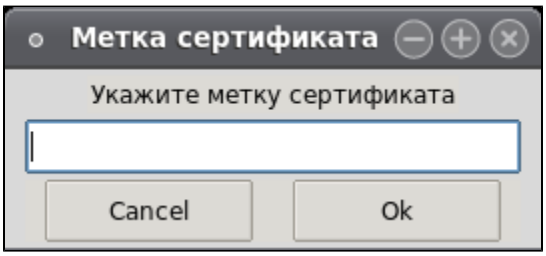
В открывшемся окне выберем опцию импорта сертификата ключа



Укажем путь до сертификата:

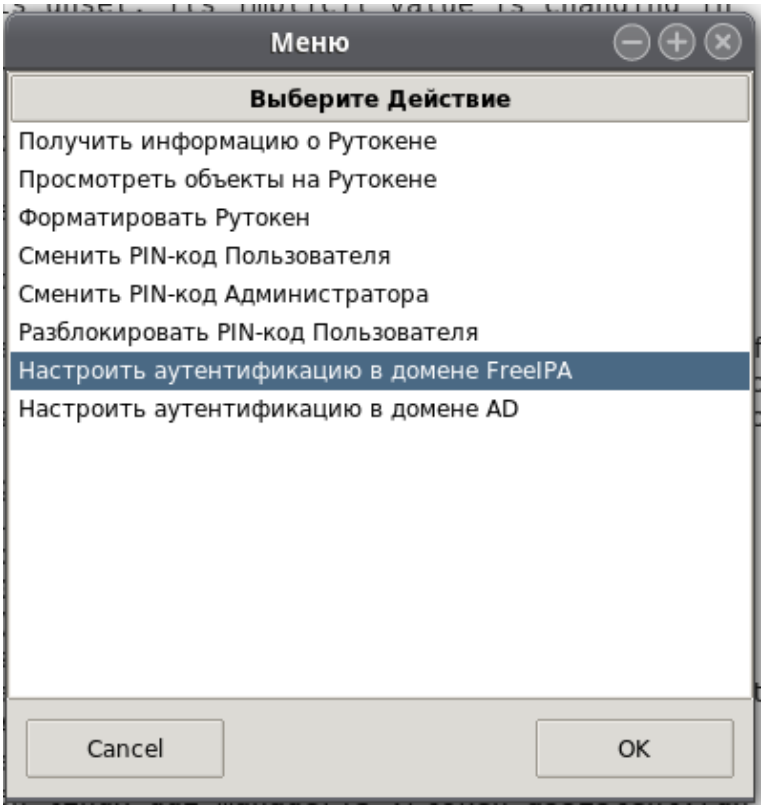


При желании можно задать метку сертификата:

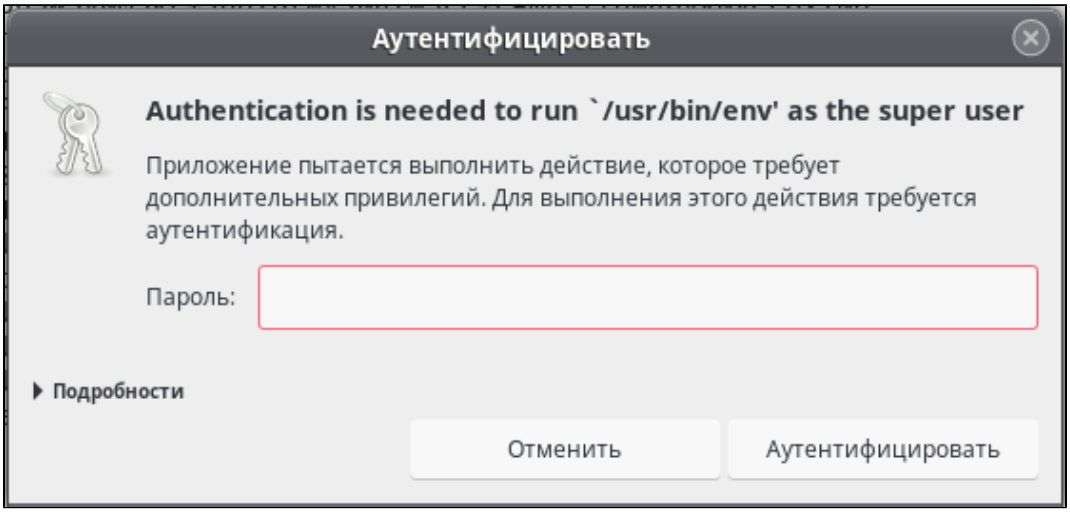


Финальная настройка на стороне клиента

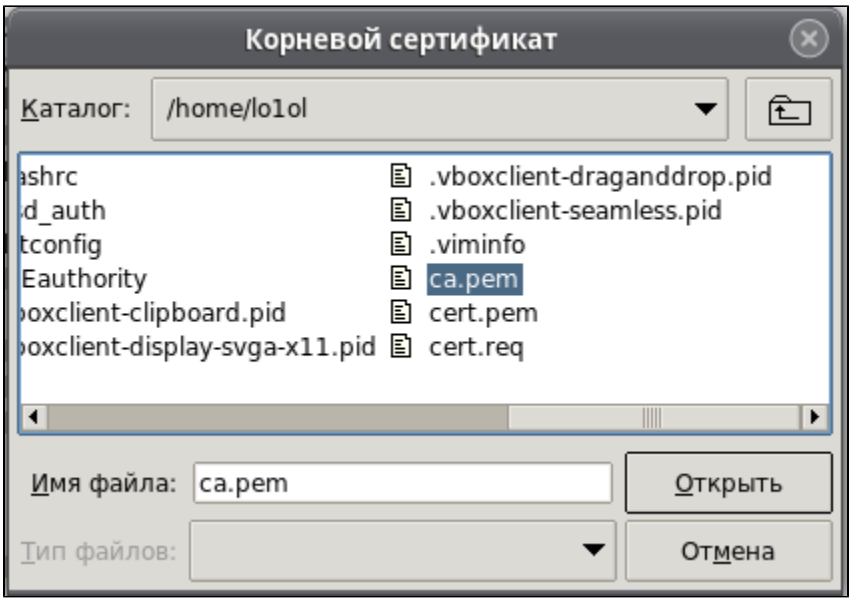
Теперь, когда на Рутокене присутствует ключевая пара и сертификат клиента? можно приступить к финальной настройке. Для этого откроем в меню команд Рутокена выберем пункт **Настройки аутентификации в домене FreeIPA**.



Нам необходимо получить права суперпользователя, для проведения настройки. Поэтому вводит пароль суперпользователя:



В открывшемся окне укажем путь до корневого сертификата УЦ:

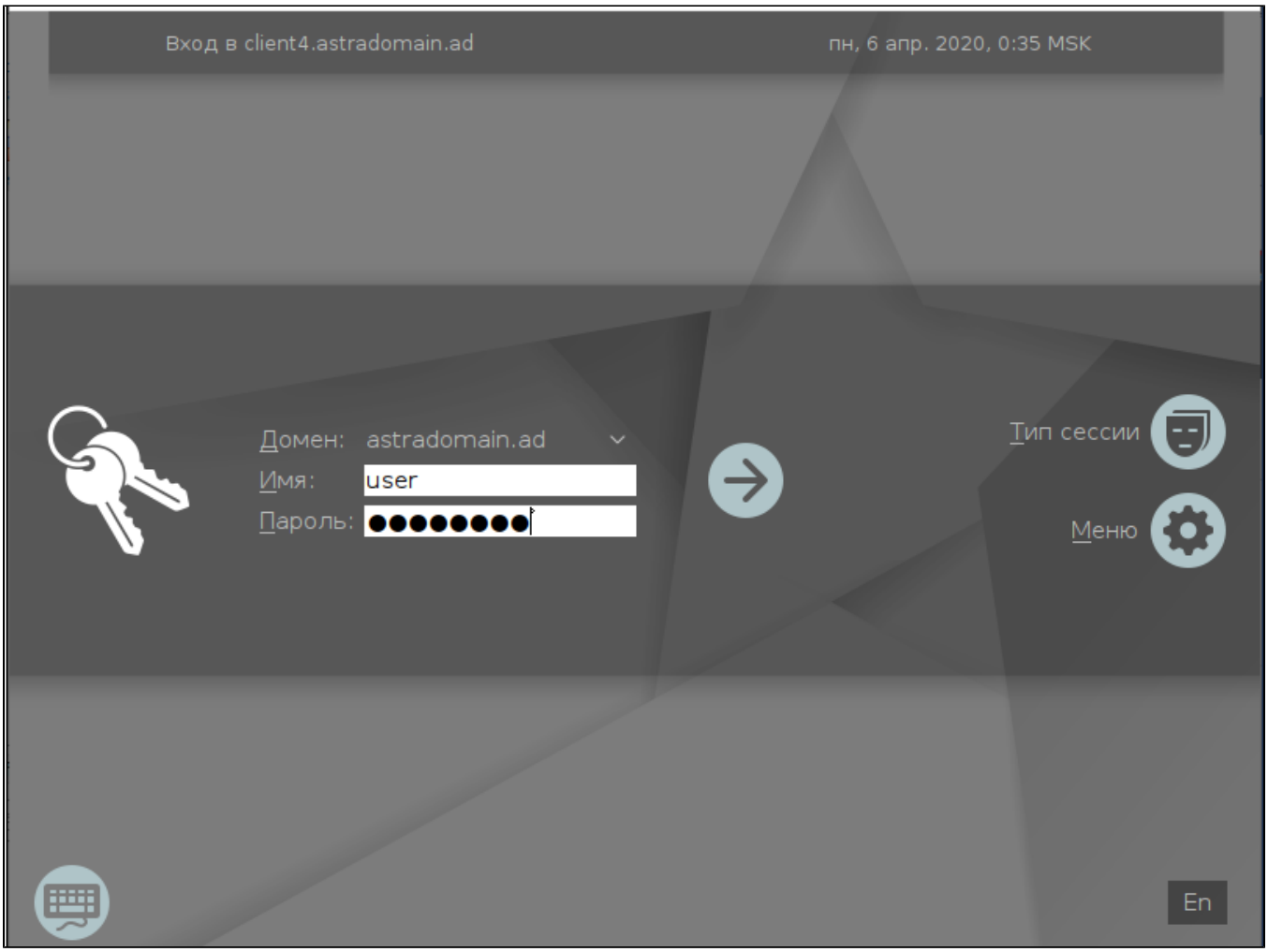


Настройка завершена. Проверим, что все установлено правильно. Для этого попробуем зайти под пользователем user.

```
[lo1ol@redosclie rutoken-linux-gui-manager]$ su user
PIN for Rutoken
sh-4.2$
```

Лампочка на Рутокене замигает и отобразится окно для ввода PIN-кода.

Если все прошло успешно, то можно попробовать осуществить аналогичную аутентификацию через greeter.


Вход в client4.astradomain.ad
пн, 6 апр. 2020, 0:35 MSK
Домен: astradomain.ad
Имя: user
Пароль:
Тип сессии
Меню
En