Упрощенная настройка локальной аутентификации с помощью Рутокен ЭЦП

Astra Linux, РЕД ОС, ALT Linux, ROSA Linux, Ubuntu

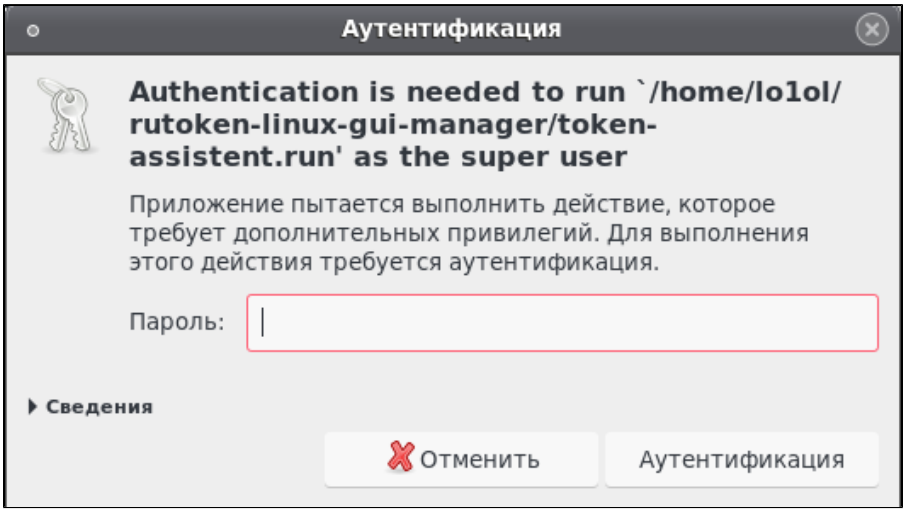
Для упрощения процесса настройки локальной аутентификации по Рутокену можно воспользоваться графической утилитой. Загрузить ее можно с помощью следующей последовательности команд:

Загрузка

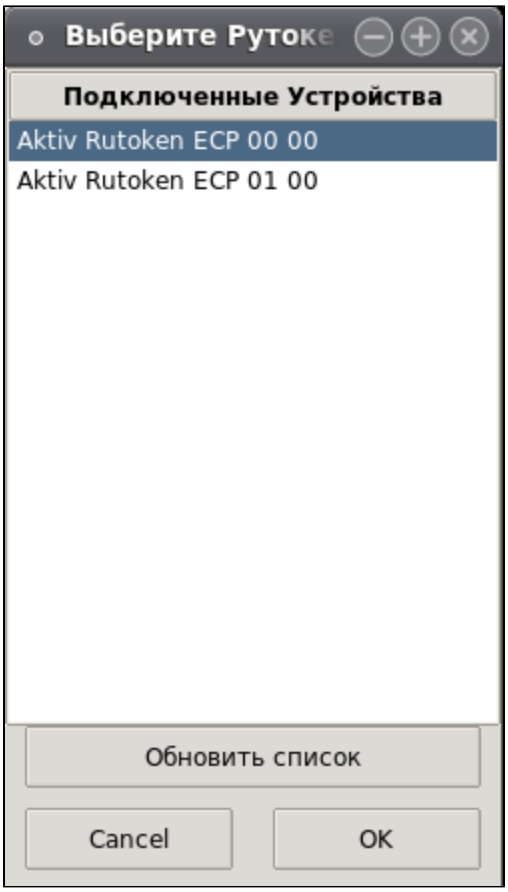
```
#  red os
sudo yum update
sudo yum install git

#  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 *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.

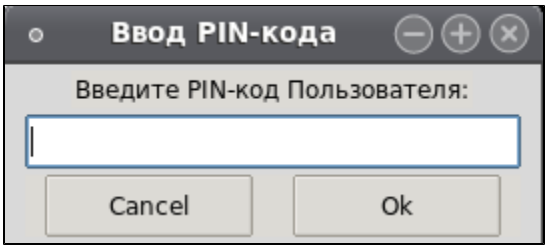
При первом запуске программа может запросить пароль администратора для получения обновлений. Загрузка обновлений может занять несколько минут.



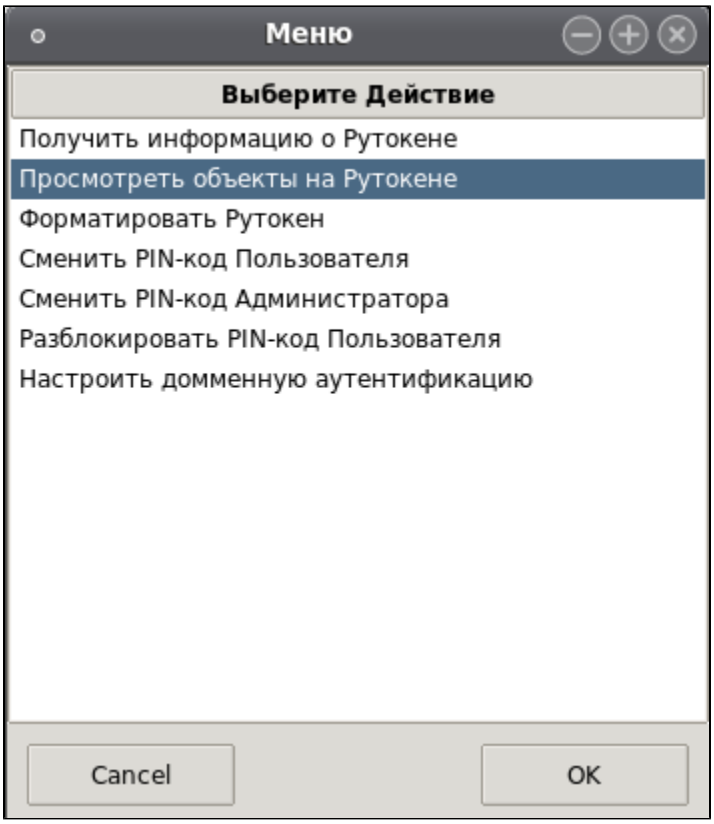
После загрузки обновлений, программа предложит выбрать устройство, которое мы хотим использовать для локальной аутентификации. Если нужный Рутокен не появился в списке, то можно нажать на клавишу для обновления списка Рутокенов:



Далее вводим PIN-код Рутокена:

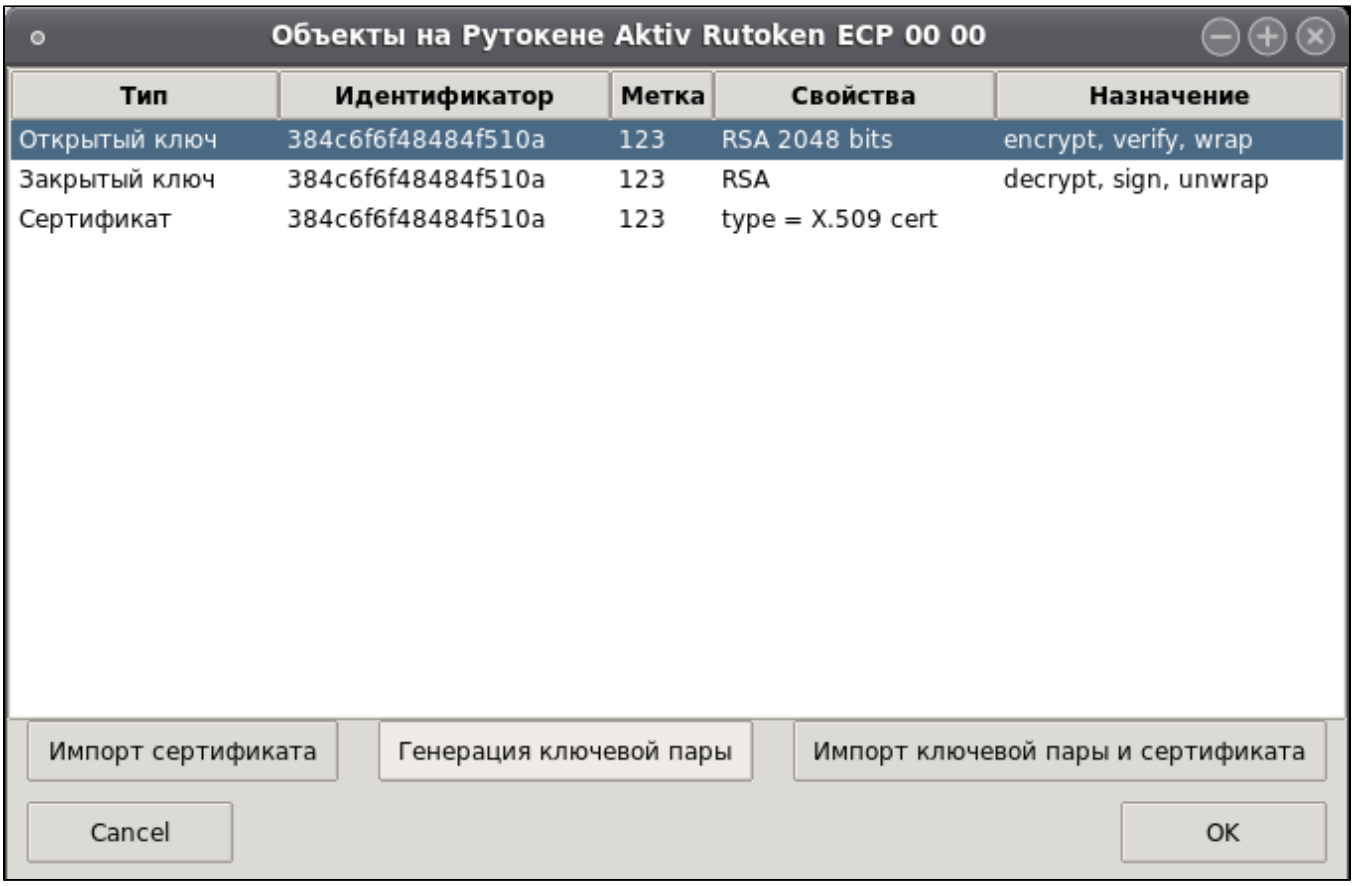


Откроем список объектов на Рутокене:

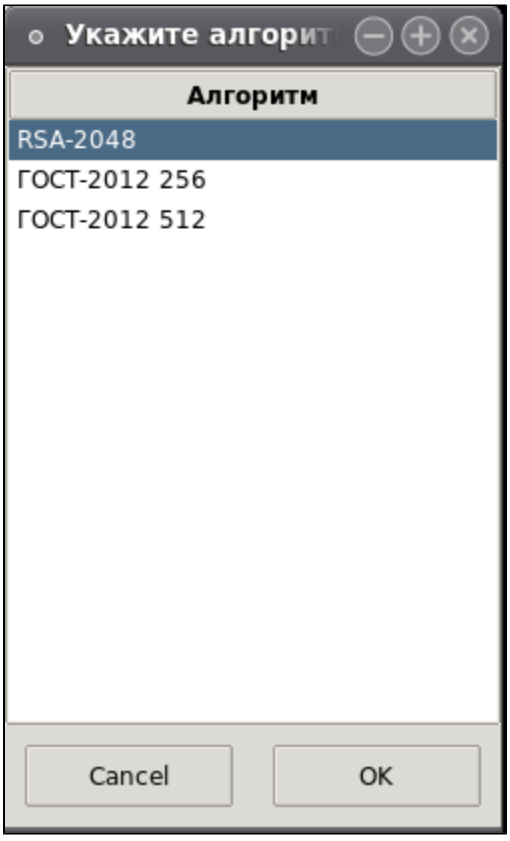


Если сертификат и ключевая пара отсутствуют на Рутокене:

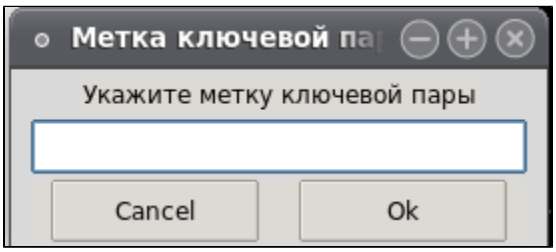
В первую очередь сгенерируем ключ. Для этого в окне просмотра объектов выберем опцию генерации ключевой пары:



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

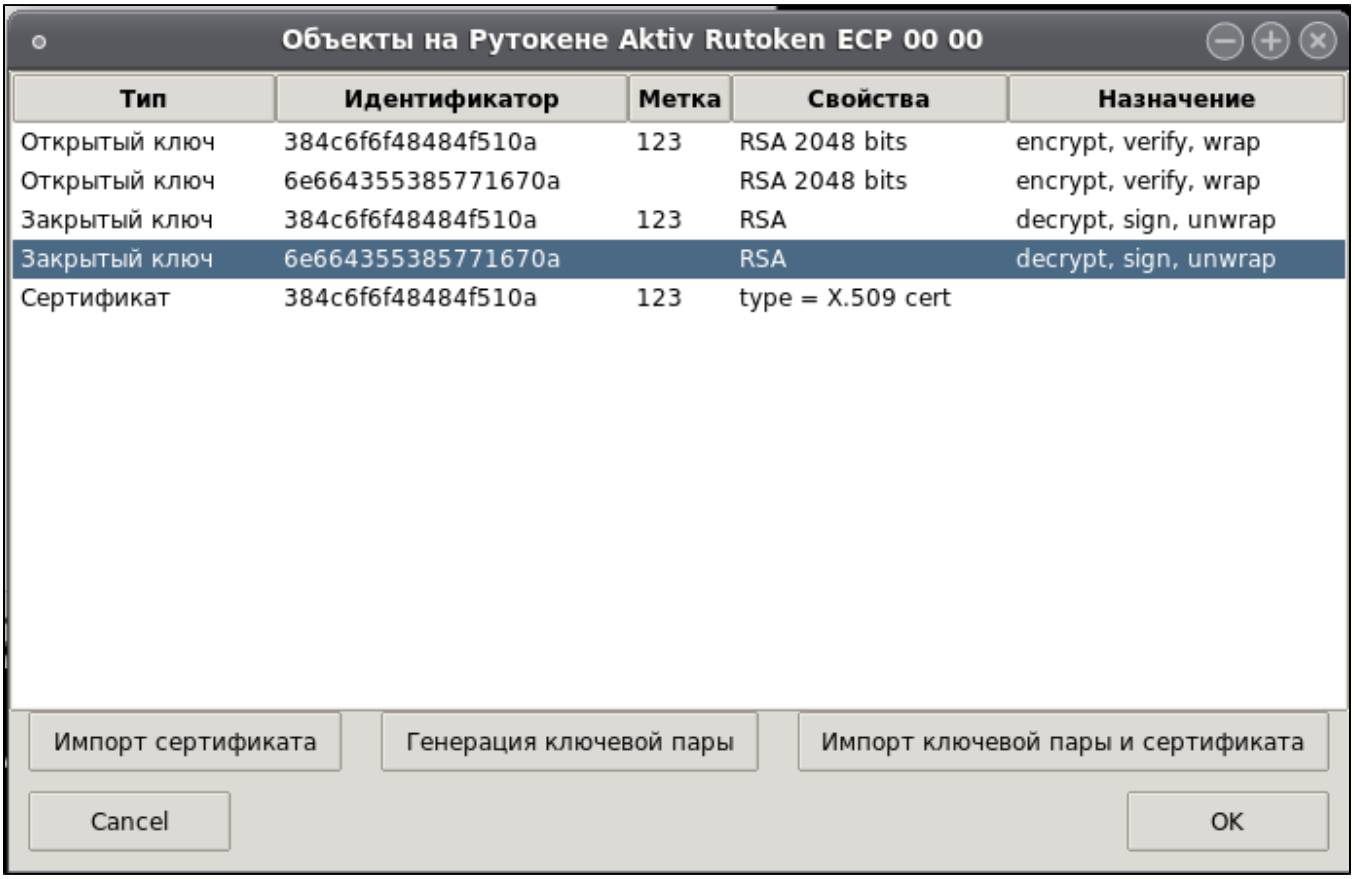


Метку ключа можно оставить пустой:

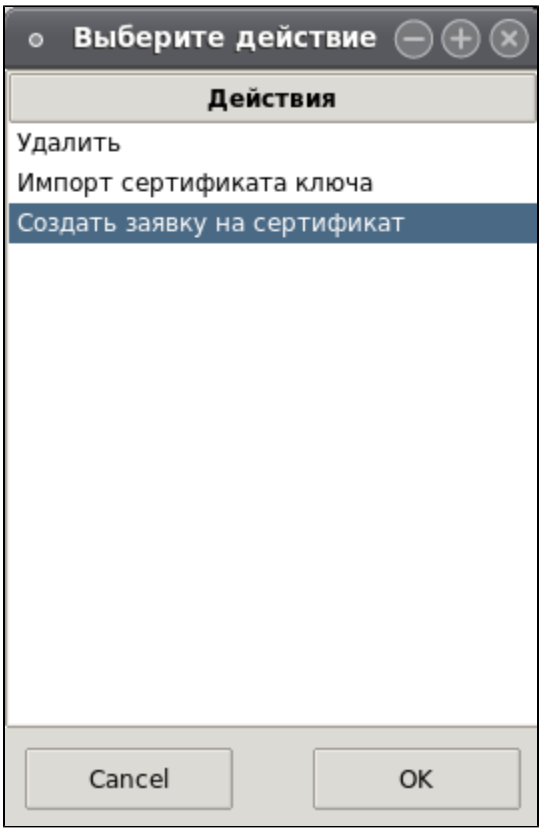


Если ключевая пара присутствует на Рутокене, но сертификата нет:

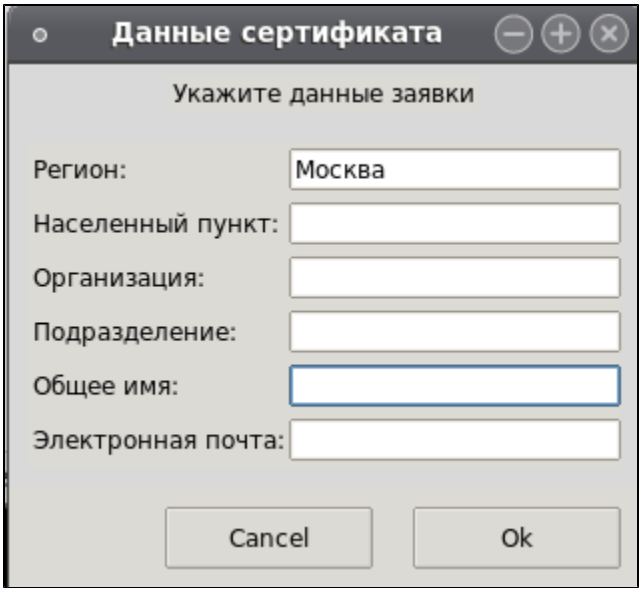
В списке объектов выберем закрытый ключ из ключевой пары, для которой хотим создать заявку на сертификат:



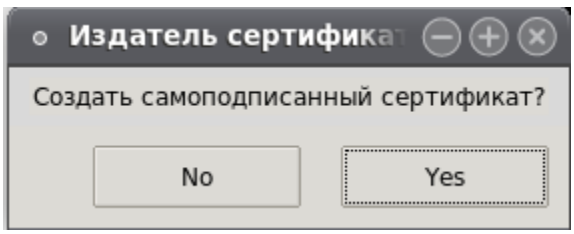
В открывшемся окне выберем опцию создания заявки на сертификат:



Введем данные сертификата:

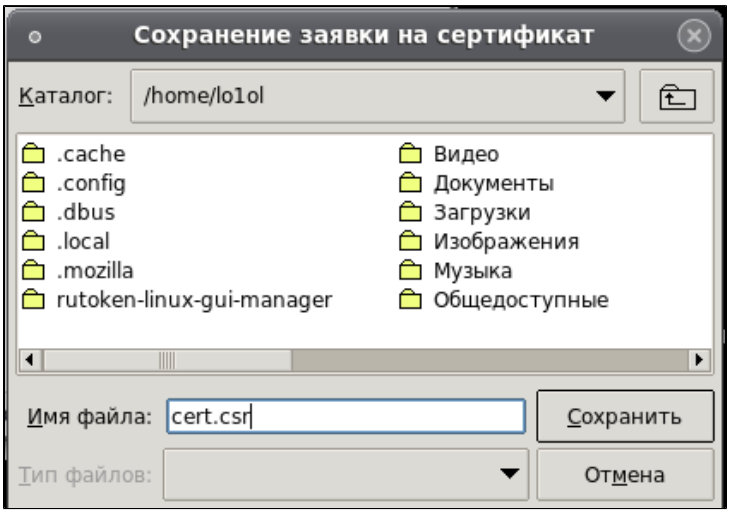


Далее выберем какой сертификат нужно создать (самоподписанный сертификат, заявку на сертификат):



В случае создания самоподписанного сертификата, он будет автоматически импортирован на Рутокен и следующий раздел в инструкции можно пропустить.

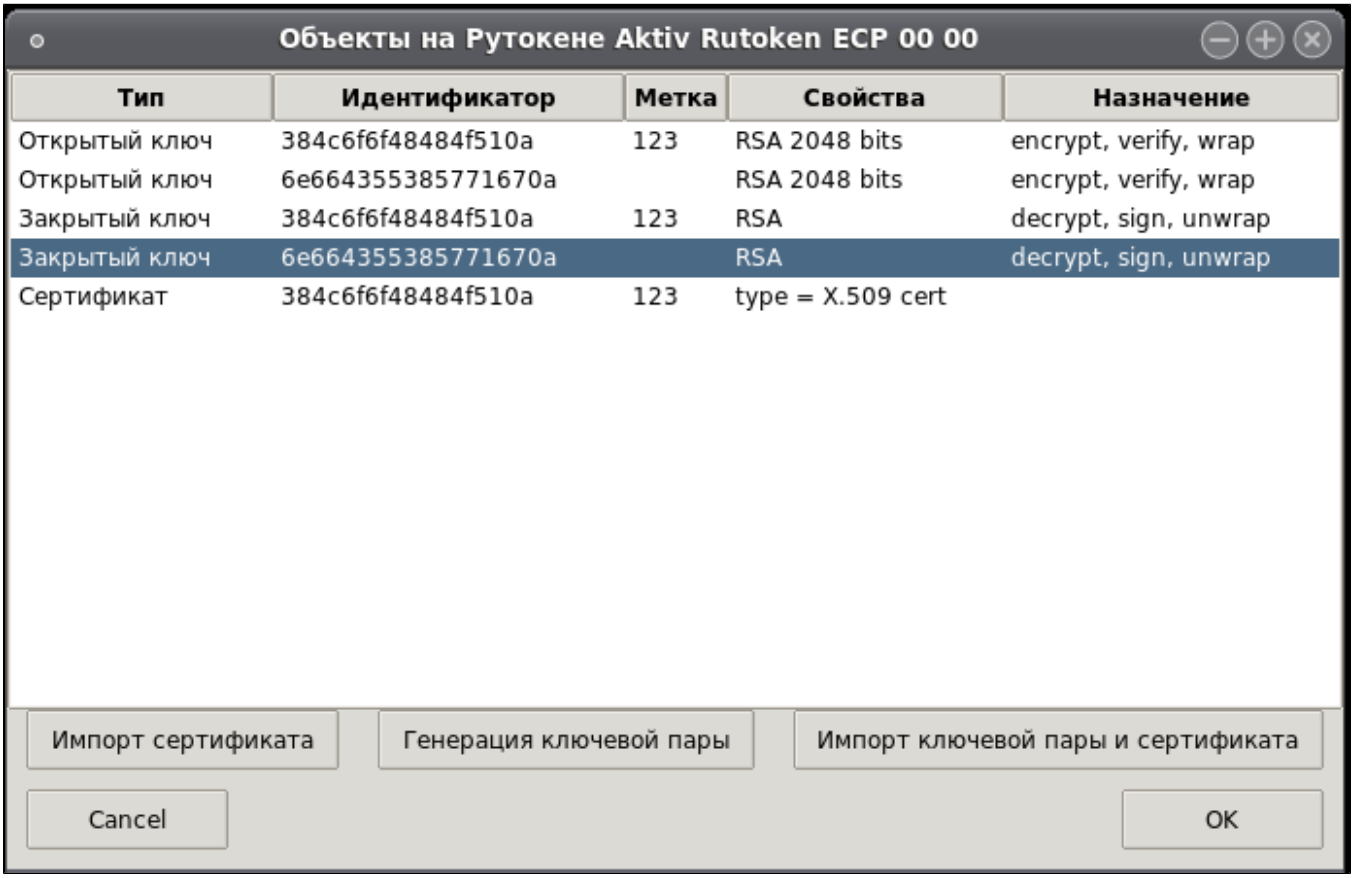
Если же мы выбрали пункт для создания заявки на сертификат, то данную заявку потребуется сохранить в файловой системе:



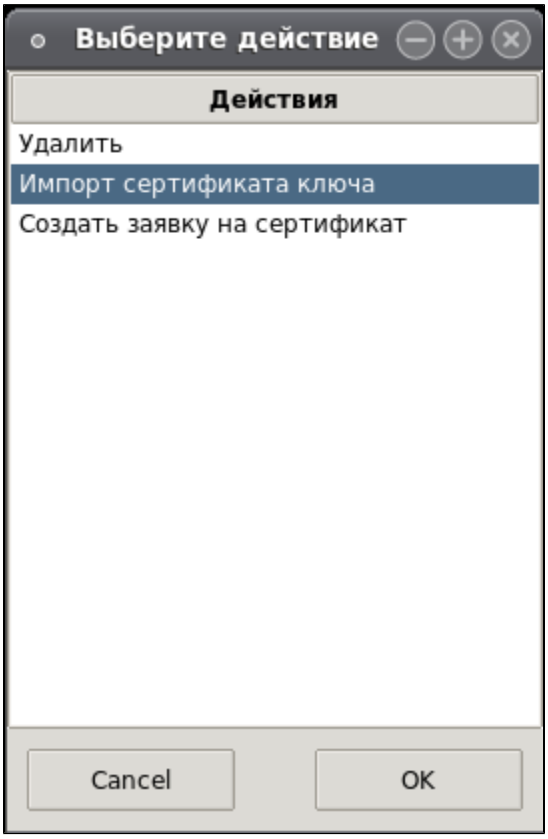
Заявку в дальнейшем следует отправить в ваш УЦ, для получения сертификата.

Импорт выданного сертификата для ключевой пары на Рутокен:

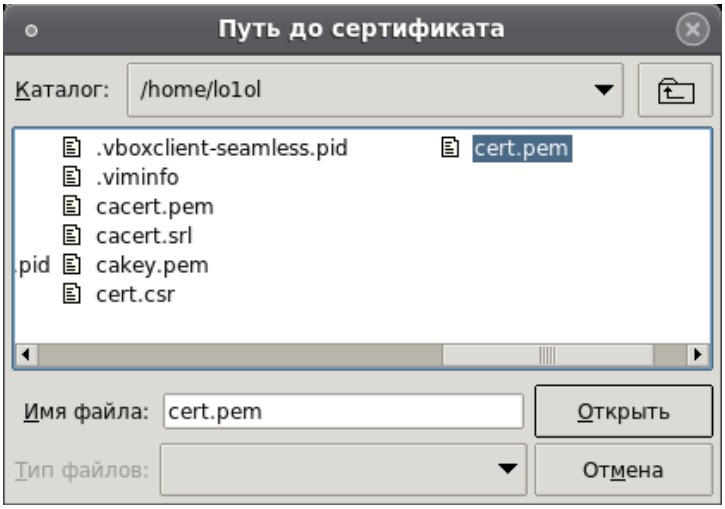
В окне для просмотра объектов выберем закрытый ключ, для которого выдан сертификат:



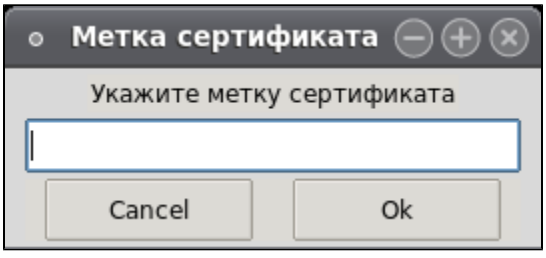
В открывшемся окне выберем опцию импорта сертификата ключа.



Укажем путь до сертификата:

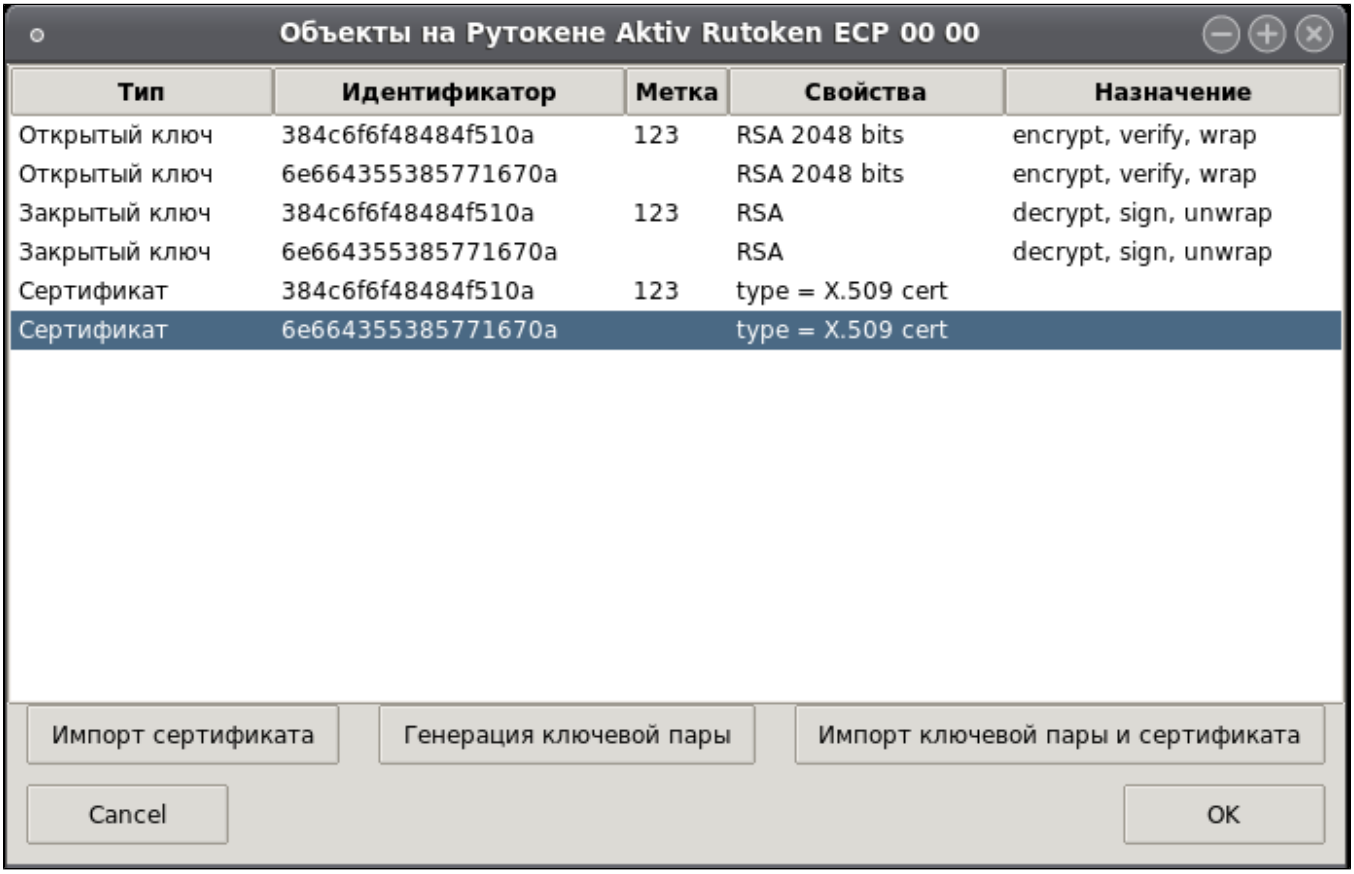


При желании можно задать метку сертификата:

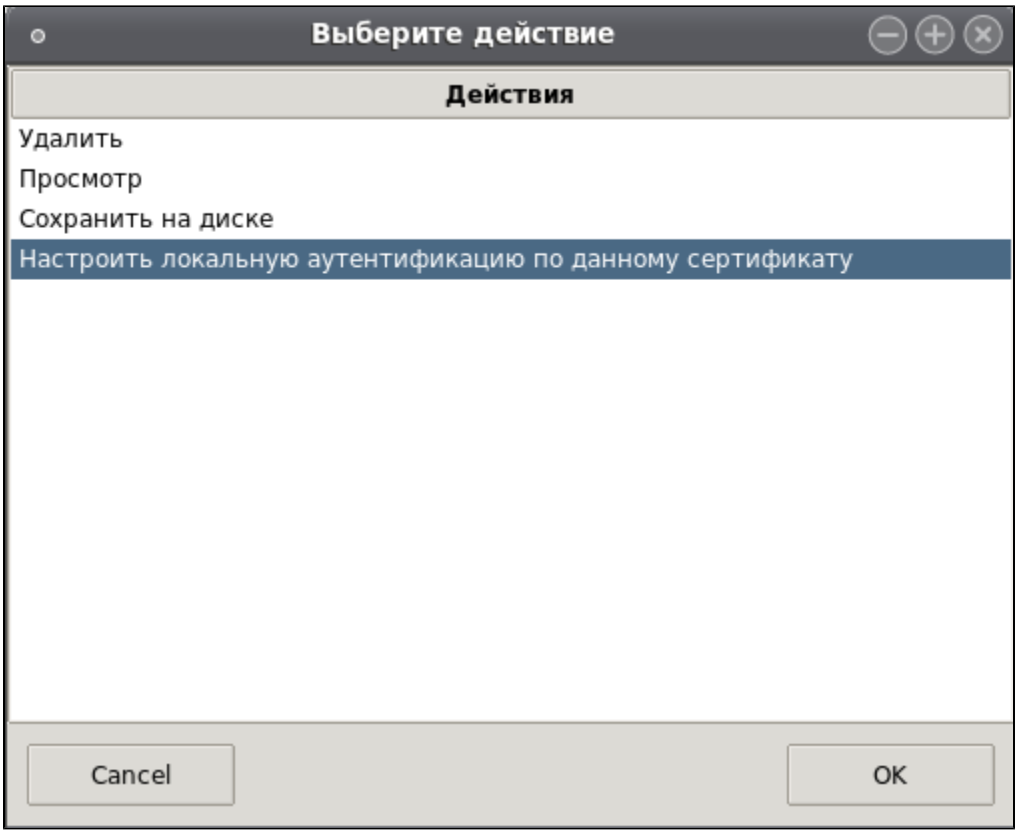


Сертификат для аутентификации уже присутствует на Рутокене

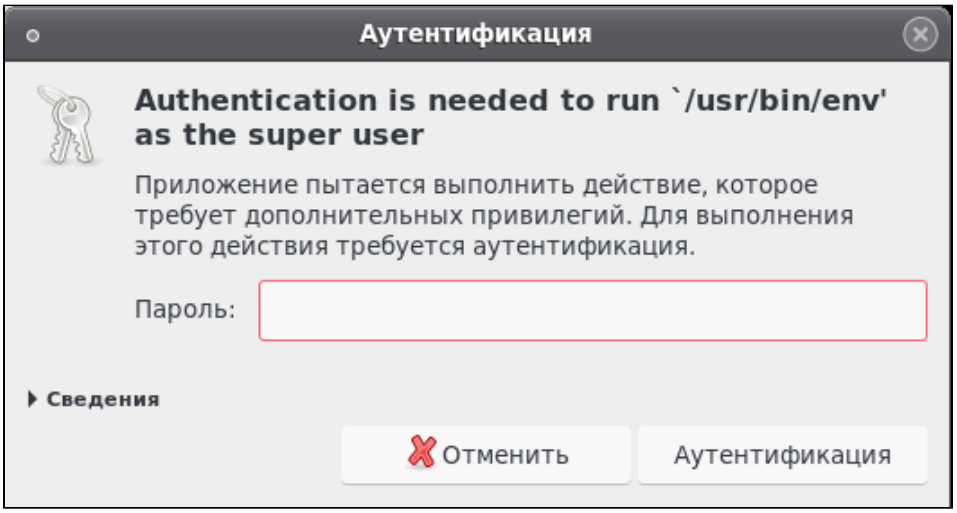
Если нужный сертификат уже присутствует на Рутокене, то щелкаем два раза мышью по нему:



И выбираем пункт для настройки локальной аутентификации:

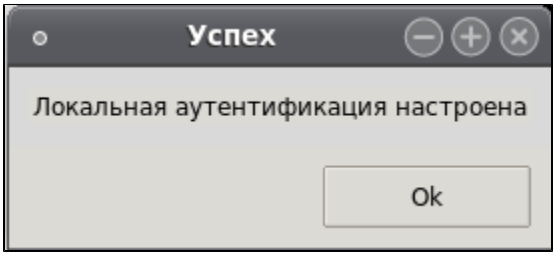


Для данной опции система может ещё раз проверить наличие прав суперпользователя:



Выберем пользователя, для которого хотим произвести настройку.

Если настройка прошла успешно, то утилита уведомит вас об этом:



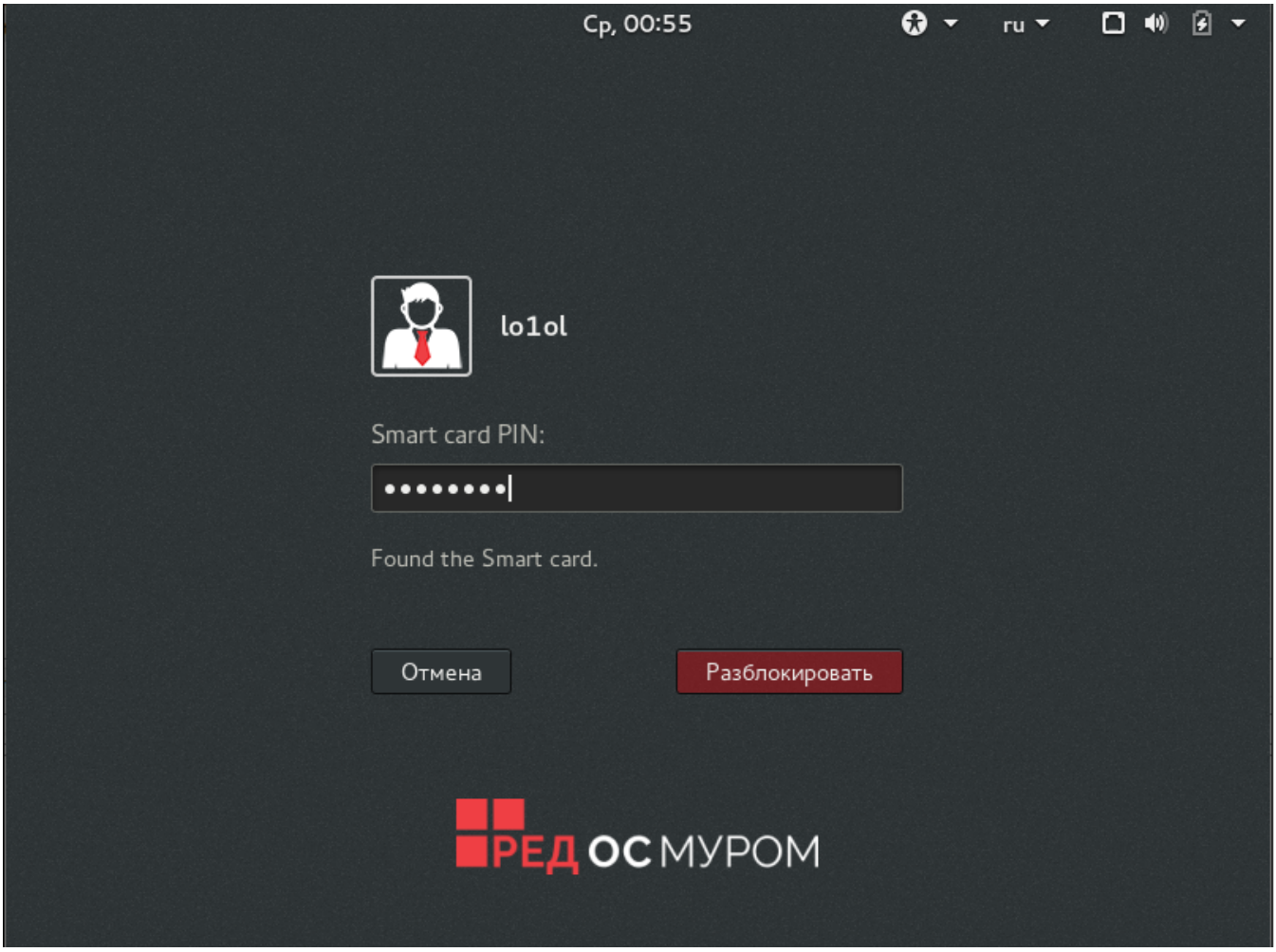
Чтобы проверить результат проверки, выполните команду:

Проверка
`su $USER`

Лампочка на токене начнет мигать и отобразится предложение с вводом PIN-кода:

```
[lo1ol@server ~]$ su lo1ol
Please insert your Smart card or enter your username.
Found the Smart card.
Добро пожаловать Rutoken!
Smart card PIN:
[lo1ol@server ~]$
```

После этого, проверку можно произвести через Greeter:



Помимо настройки входа с помощью Рутокена, автоматически была настроена автоблокировка при извлечении устройства. Ее можно проверить с помощью извлечения Рутокена.