Упрощенная настройка аутентификации в домене AD с помощью Рутокен ЭЦП

Astra Linux, РЕД ОС

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.

Настройка сервера AD

Описание настройки сервера Active Directory можно найти здесь

Настройка клиента для подключения к домену

Для пользователей Astra Linux

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

Настройка подключения к домену

Описание настройки клиента для подключения к домену можно найти здесь. Необходимо выполнить все действия по настройке клиента вплоть до **"проверки аутентификации под пользователем в домене без Рутокена"**. Далее нужно будет перейти обратно к этой инструкции.

Настройка аутентификации по Рутокену для клиента

Установка утилиты для работы с Рутокеном

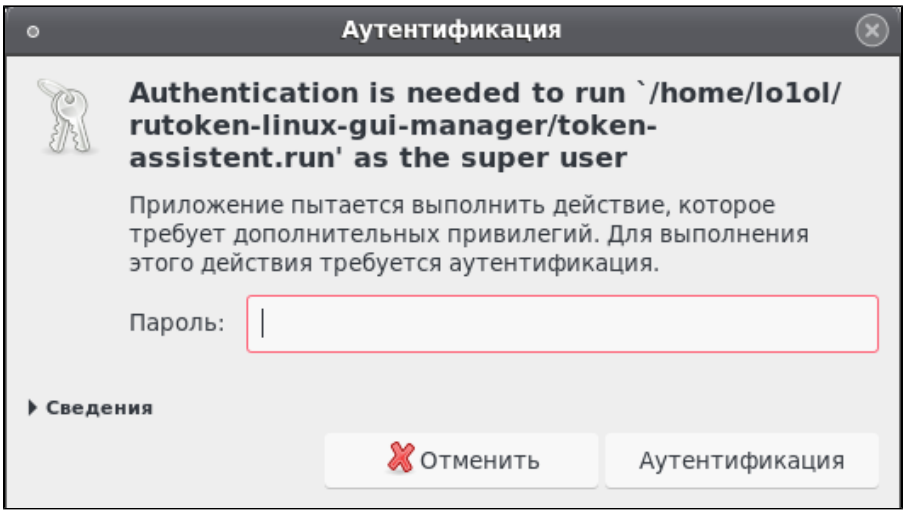
Для упрощения настройки можно воспользоваться графической утилитой для работы с Рутокенами в Linux. Скачаем ее:

Установка скрипта настройки

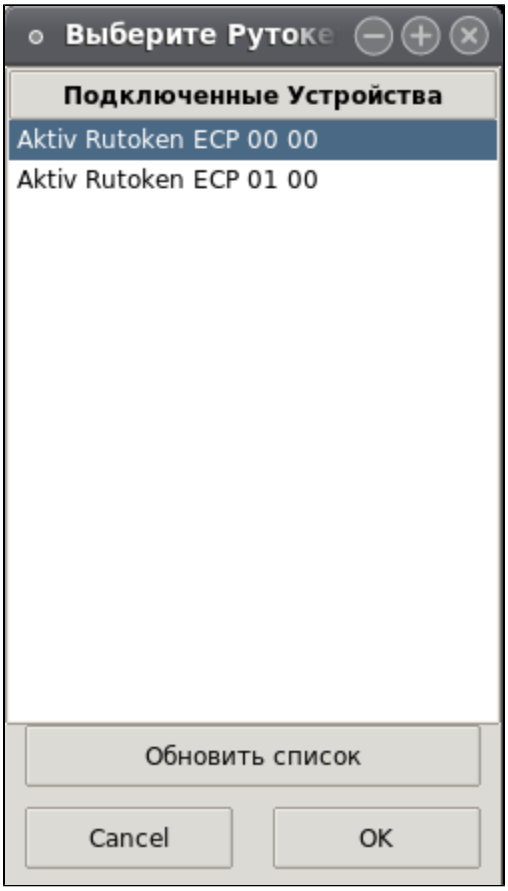
```
#  red os
sudo yum update
sudo yum install git

#  astra, alt linux  ubuntu
sudo apt-get update
sudo apt-get install 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.

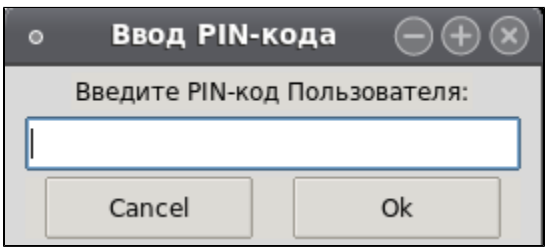
При первом запуске программа может запросить пароль администратора для получения обновлений. Загрузка обновлений может занять несколько минут.



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:

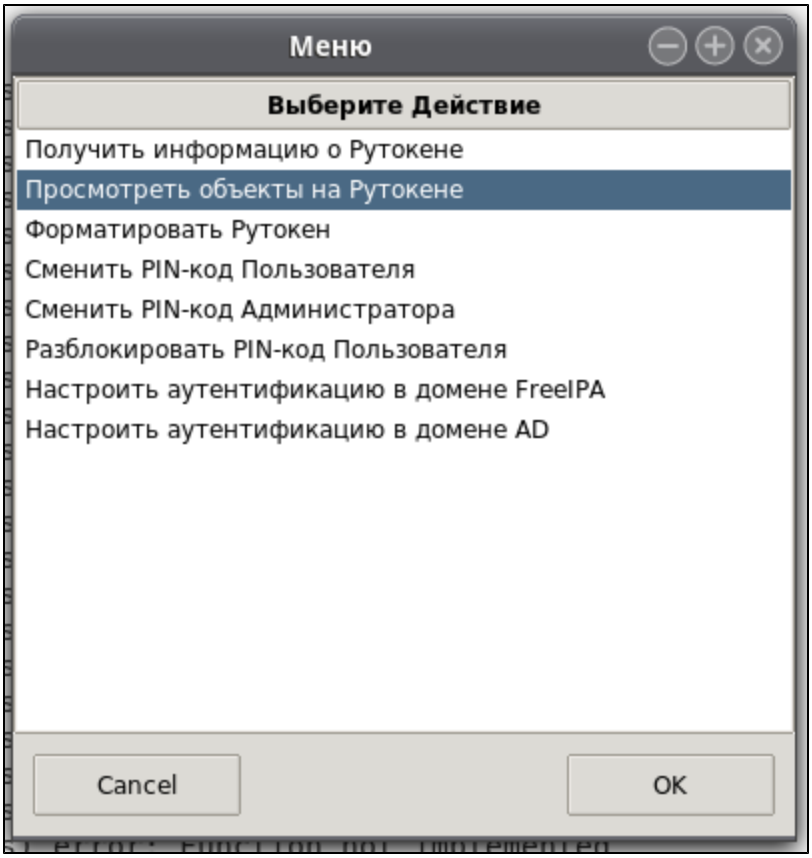


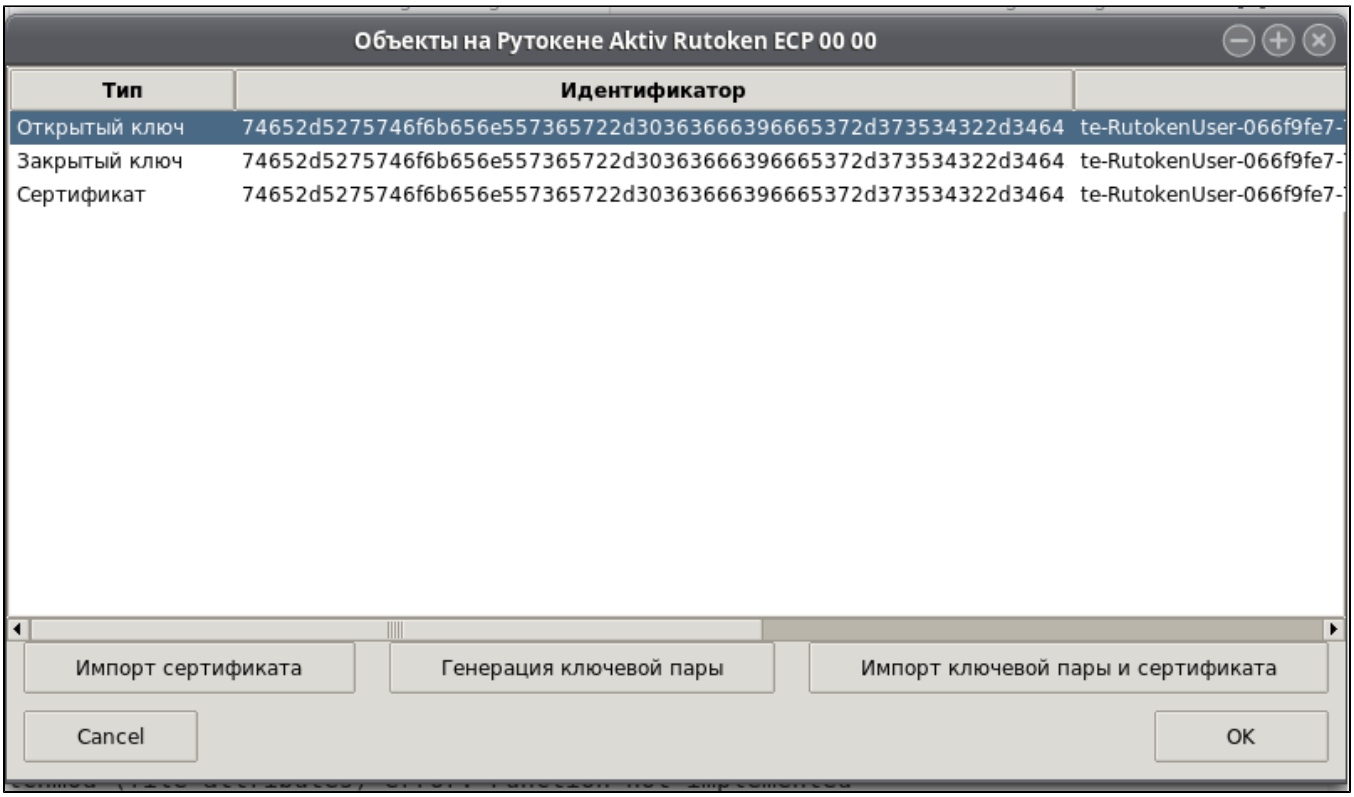
Далее вводим PIN-код Рутокена:



Проверка наличия сертификата и ключевой пары клиента для аутентификации

Откроем список объектов на Рутокене:

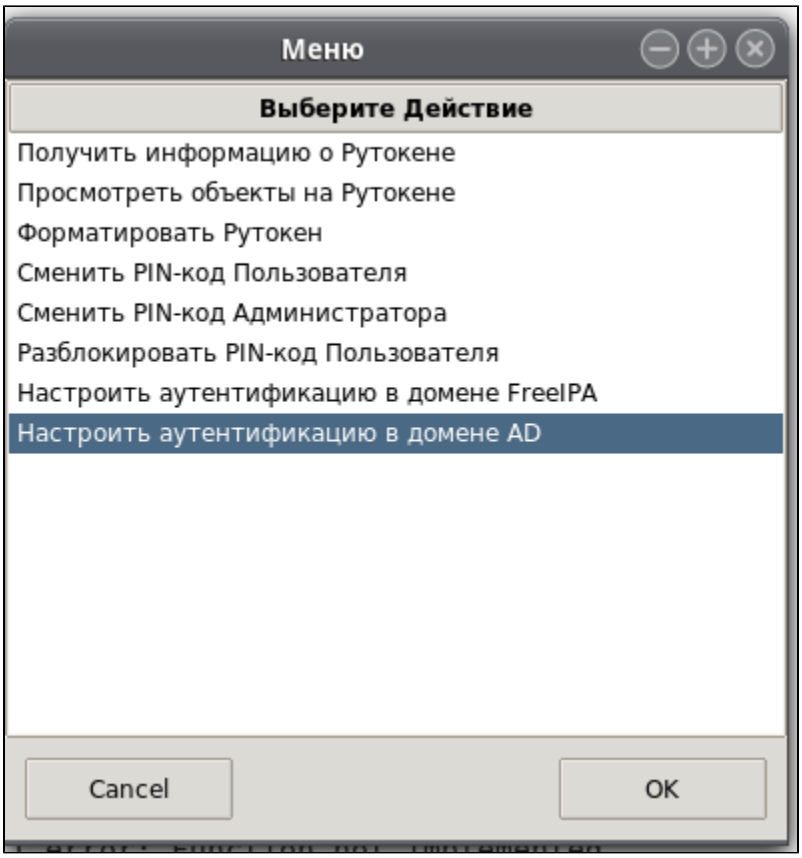




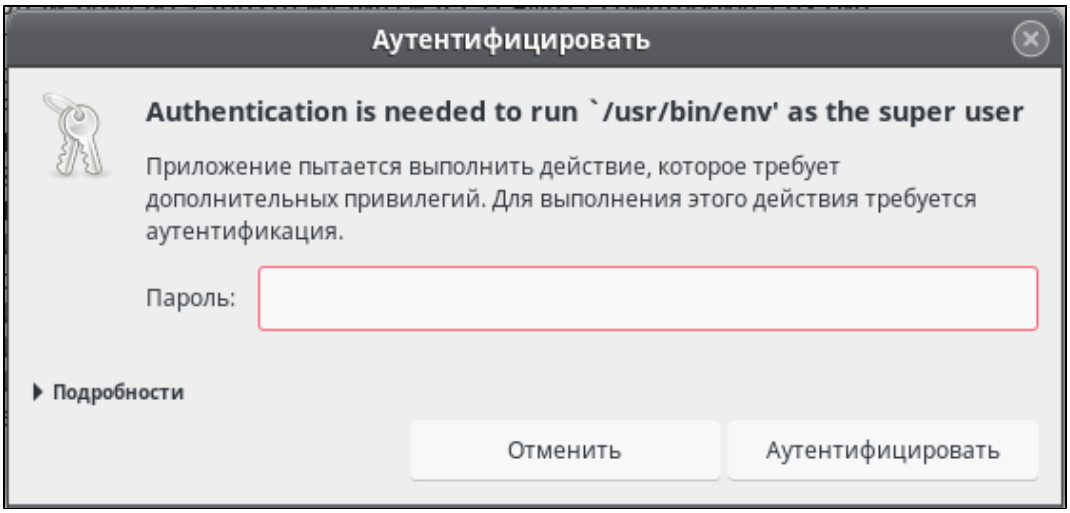
На токене присутствуют ключевая пара и сертифиикат. Закрываем меню просмотра объектов.

Настройка аутентификации в домене AD

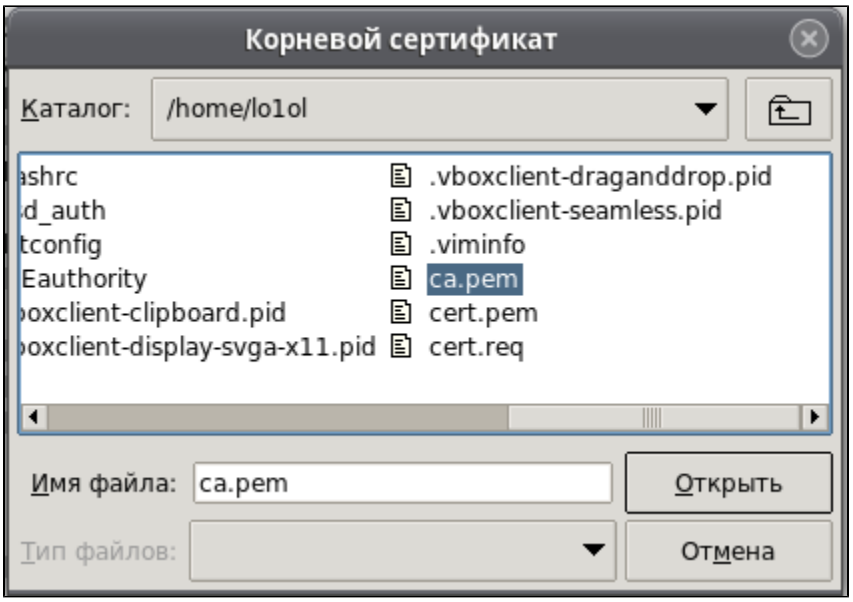
Теперь, когда на Рутокене присутствует ключевая пара и сертификат клиента? можно приступить к финальной настройке. Для этого откроем в меню команд Рутокена выберем пункт **Настроить аутентификацию в домене AD**



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



В открывшемся окне укажем путь до корневого сертификата УЦ:

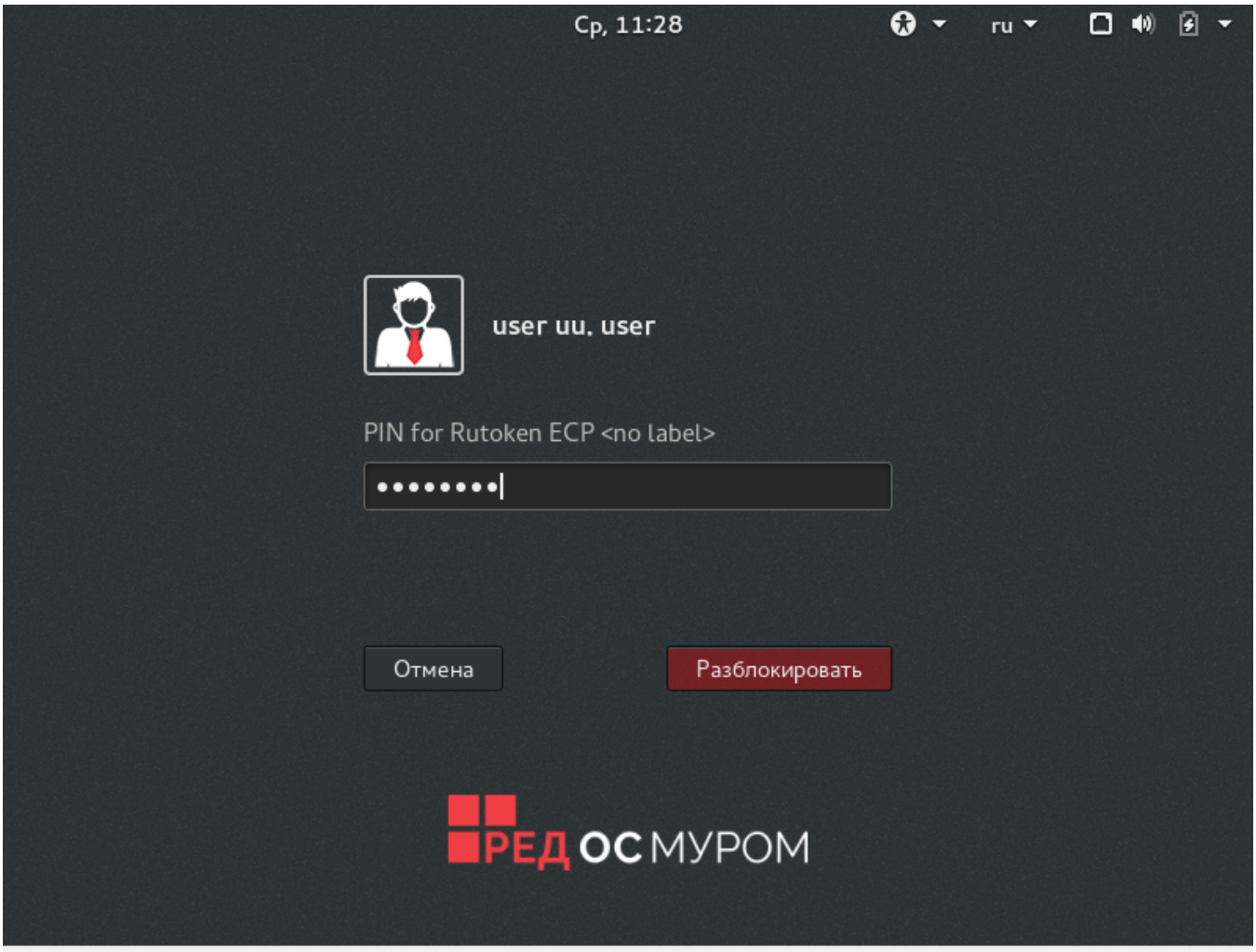


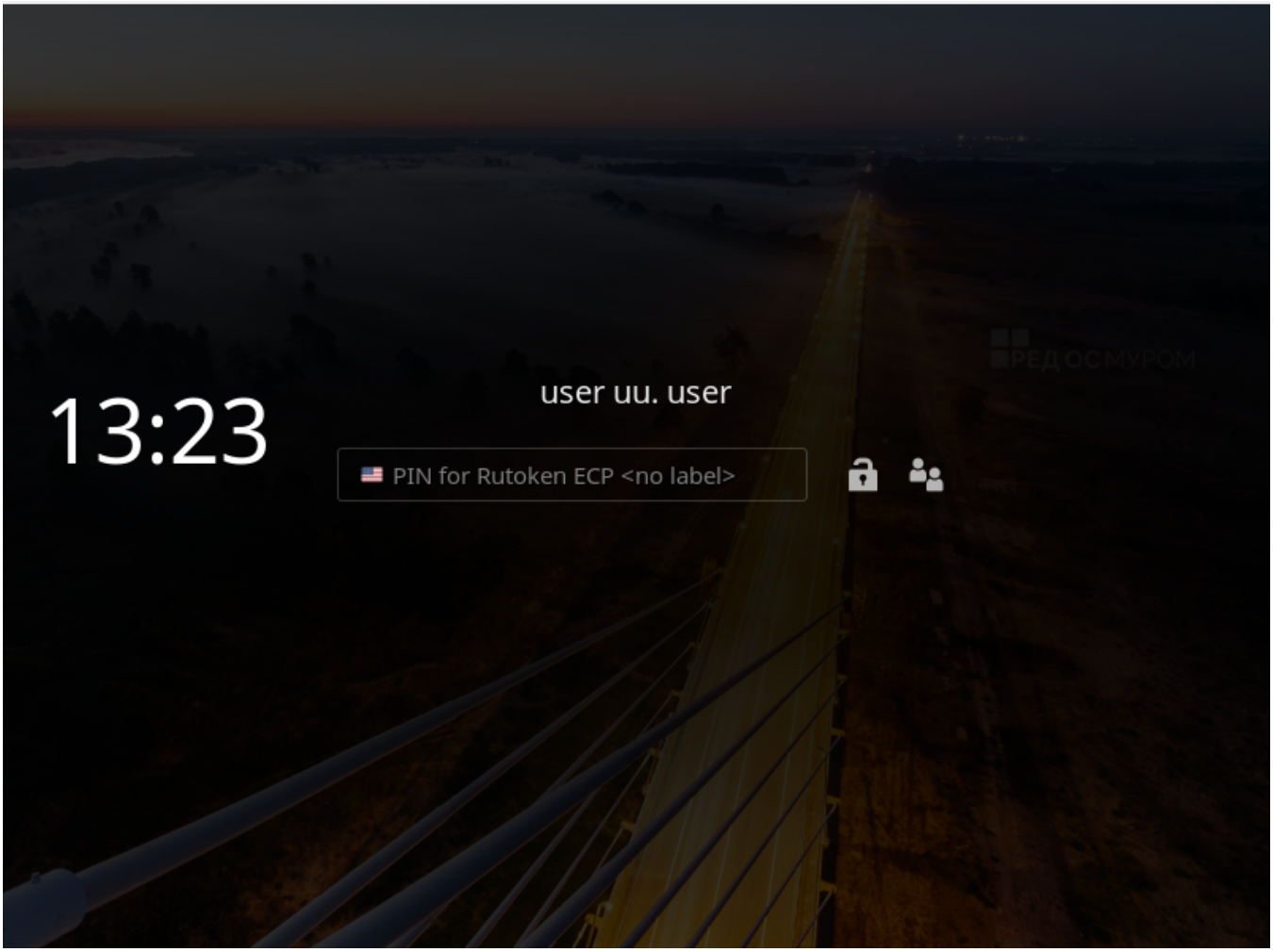
Настройка завершена. Проверим, что все установлено правильно. Для этого попробуем зайти под пользователем user.

```
[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 и лок скрин.


Ср, 11:28
ru
user uu. user
PIN for Rutoken ECP <no label>
Отмена
Разблокировать
РЕД ОС МУРОМ



Для пользователей Astra Linux предложение ввода ПИН-кода не отображается. В поле ввода пароля просто введите ПИН-код от Рутокена:


Вход в smolensk.astradomain.ad
вт, 14 июл. 2020, 16:58 MSK
Имя:
user
Пароль:
Тип сессии
Меню
En


Компьютер smolensk.astradomain.ad
16 : 57
14
Вт.
Введите пароль
Сессии...
****
EN
CapsLock Выкл.