Поддержка двухфакторной аутентификации в инфраструктуре Samba AD

Урал Раилевич Ахметов[1]
[1]Российский государственный университет нефти и газа (национальный исследовательский университет) имени И.М Губкина, Москва, Россия, ahmetovural.ru@gmail.com
Васильев Александр Андреевич[2]
[2] Российский государственный университет нефти и газа (национальный исследовательский университет) имени И.М Губкина, Москва, Россия, Sawa141299@yandex.ru

Аннотация:

В данной статье осуществляется настройка двухфакторной аутентификации на основе инфраструктуры Samba AD и рассматриваются другие методы аутентификации. Осуществляется внедрение аппаратных решений в инфраструктуре Samba AD, где за основу взята российская разработка - Рутокен, цель которой заключается в повышении безопасности доменных аутентификационных процессов.

Ключевые слова: Samba AD, двухфакторная аутентификация, безопасность, аутентификация, Рутокен, Active Directory, Alt Linux.

Для цитирования:

Ахметов У. Р., Васильев А. А. Поддержка двухфакторной аутентификации в инфраструктуре Samba AD // Информационная безопасность: теория и практика.

Введение:

В эпоху постоянных информационных угроз рассматривается вопрос повышения безопасности с доступом к корпоративным сетям. Чтобы решить данную проблему, на помощь приходят средства двухфакторной

аутентификации, являющиеся одним из наиболее эффективным методом защиты от несанкционированного доступа. В данной работе рассматривается внедрение двухфакторной аутентификации в инфраструктуру Samba AD с использованием Рутокена.

1. Теоретические аспекты двухфакторной аутентификации

Основы двухфакторной аутентификации

Для подтверждения своей подлинности субъект должен предоставить некоторую секретную информацию, которая должна быть доступна только ему одному. Он может предъявлять системе различные виды информации.

Фактор аутентификации — определенный вид информации, предоставляемой субъектом системе при его аутентификации.

Компоненты двухфакторной аутентификации.

Выделяют три фактора аутентификации[1], используемые в различных комбинациях: на основе знания чего-либо, обладания чем-либо, на основе биометрических характеристик (табл. 1)

[1] Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов / А. А. Афанасьев, Л. Т. Веденьев, А. А. Воронцов и др.; Под ред. А. А. Шелупанова, С. Л. Грузаева, Ю.С. Нахаева — М.: 2009. — 552 с.

Таблица 1

Факторы аутентификации

Фактор аутентификации	**Классификация типов факторов аутентификации NCSC-TG-017** [2]	**Примеры факторов аутентификации**
На основе знания чего-либо (1-й)	Type 1: Authentication by Knowledge	1. Пароль или парольная фраза 2. PIN-код
На основе обладания чего-либо (2-й)	Type 2: Authentication by Ownership	1. Физический ключ 2. Карта с магнитной полоской 3. OTP-токен, генерирующий одноразовый пароль
На основе биометрических-характеристик (3-й)	Type 3: Authentication by Characteristic	1. Отпечаток пальцев 2. Рисунок сетчатки 3. Голос

Обзор инструментов и технологий для двухфакторной аутентификации:

Принцип работы двухфакторной аутентификации состоит из двух взаимосвязанных компонентов:

[2] NCSC-TG-017 — документ «A Guide to Understanding Identification and Authentication in Trusted Systems», опубликованный U.S. National Computer Security Center. Руководство содержит комплект рекомендуемых инструкций по процедурам идентифицкации и аутентификации.

1. Пароль, который требуется при доступе к ресурсу и хранится у пользователя.
2. Сгенерированный тип данных, который может может храниться на физическом устройстве или в зависимости от времени пересоздаваться

Только при наличии этих компонентов у пользователя имеется доступ к данным.

Для реализации данной технологии существуют различные инструменты двухфакторной аутентификации, примеры которых приведены ниже.

Таблица 2

Инструменты двухфакторной аутентификации

Категория	**Название**	**Описание**	**Linux пакеты**
Аутентификационные приложения (Authenticator Apps)	Google Authenticator	Наиболее востребованные приложение среди аналогов, позволяющее генерировать временные, одноразовые пароли	libpam-google-authenticator
	Microsoft Authenticator	Аналог Google Authenticator, с	authenticator

		дополнительными функциями	
	Authy	Аналог с мультиустройственной синхронизацией, так же поддерживает защиту удаленных акаунтов	Perl-WWW-Authy
Аппаратные токены (Hardware Tokens)	Рутокен	Российская разработка для аппаратной аутентификации и ЭЦП (электронной цифровой подписи)	pcsc-lite-ccid, libpcsclite, pcsc-tools, opensc
SMS и Голосовая аутентификация	SMS	Отправка одноразового кода через SMS или звонок на телефон (последнии цифры номера).	Платформа OpenUDS Server с поддержкой OTP: *openuds-server-nginx*
	Голосовые вызовы	Отправка кодов с помощью голосового вызова.	Платформа OpenUDS Server с поддержкой OTP: *openuds-server-nginx*

Биометрическая аутентификация	Распознавание голоса	Встроенное устройство, для сканирования отпечатка пальца (широко распространено)	Платформа VoiceKey.PLATFORM: vk-monitoringcomponent vk-routercomponent vk-securitycomponent vkchroniclercomponent vk-databasecomponent vk-licensingcomponent vk-mediahubcomponent vkvoicegridprocessor
	Распознавание лица	Встроенное устройство для распознавания биометрии лица. Технология, используемая в Apple Face ID и других	howdy
Программные решения для интеграции 2FA	Duo Security	Поддерживает широкий спектр решений для аутентификации.	duo_unix
	Okta Verify	Облачный сервис, который позволяет управлять удостоверениями и доступом	okta (через API)

В нашем случае для примера реализации двухфакторной аутентификации был выбран Рутокен ЭЦП 3.0. Это активный ключевой носитель, являющийся представителем новой линейки USB-токенов и смарт-карт для подписания документов электронной подписью и строгой двухфакторной аутентификации на настольных и мобильных устройствах. Продукты линейки являются полнофункциональными аппаратными СКЗИ.

В смарт-картах и USB-токенах аппаратно реализованы: ГОСТ Р 34.10–2012[3] с длиной ключа 256/512 бит и ГОСТ Р 34.11–2012[4], а также симметричные шифры Магма и Кузнечик и международные алгоритмы электронной подписи RSA и ECDSA. Криптографические операции выполняются без копирования ключа в память компьютера.

Часть моделей линейки, помимо традиционного контактного интерфейса, оснащена бесконтактным интерфейсом (NFC). При этом функции устройств доступны через оба интерфейса. Это позволяет подписывать документы на смартфонах и планшетах так же легко, как расплачиваться бесконтактной банковской картой, при наличии поддержки в используемом мобильном приложении.

Поддержка отечественных и международных стандартов позволяет использовать модели Рутокен ЭЦП 3.0 в информационных системах с высокими требованиями безопасности. ПО Рутокен работает во всех современных настольных и мобильных операционных системах. SDK

---

[3] ГОСТ Р 34.10-2012 "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи" (утв. приказом Федерального агентства по техническому регулированию и метрологии от 7 августа 2012 г. N 215-ст).

[4] ГОСТ Р 34.11-2012 "Информационная технология. Криптографическая защита информации. Функция хэширования" (утв. приказом Федерального агентства по техническому регулированию и метрологии от 7 августа 2012 г. N 216-ст).

позволяет встраивать поддержку устройств в классические, мобильные и веб-приложения.

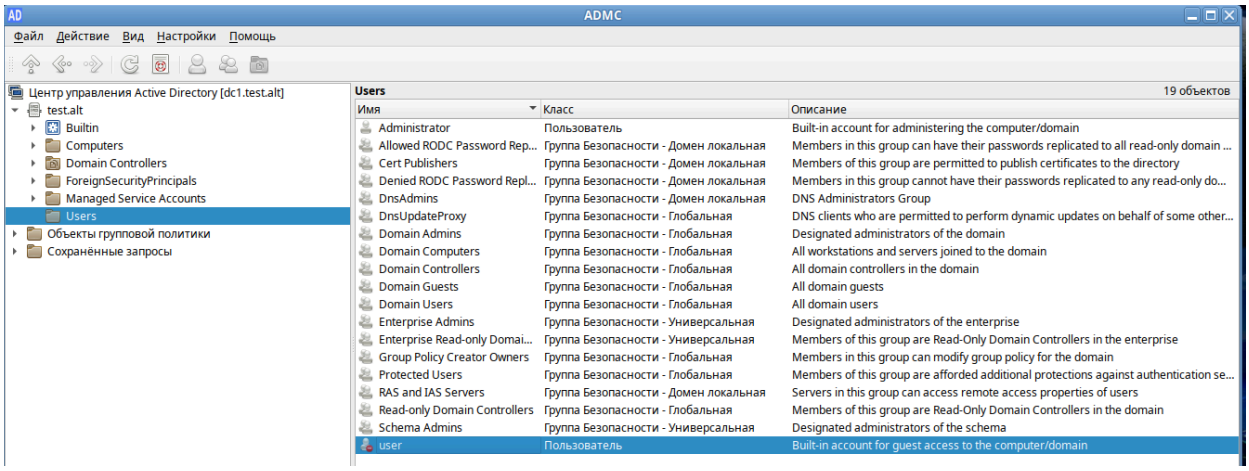
USB-токен Рутокен ЭЦП 3.0, подключенный к USB-порту, работает везде, где поддерживается Рутокен ЭЦП 2.0 (в том числе в ЕГАИС). Дополнительные настройки не требуются. При этом существенно повышена производительность криптографических и файловых операций.

Устройства Рутокен ЭЦП 3.0 сертифицированы по требованиям ФСБ и ФСТЭК. Подходят для получения квалифицированных сертификатов в УЦ ФНС.

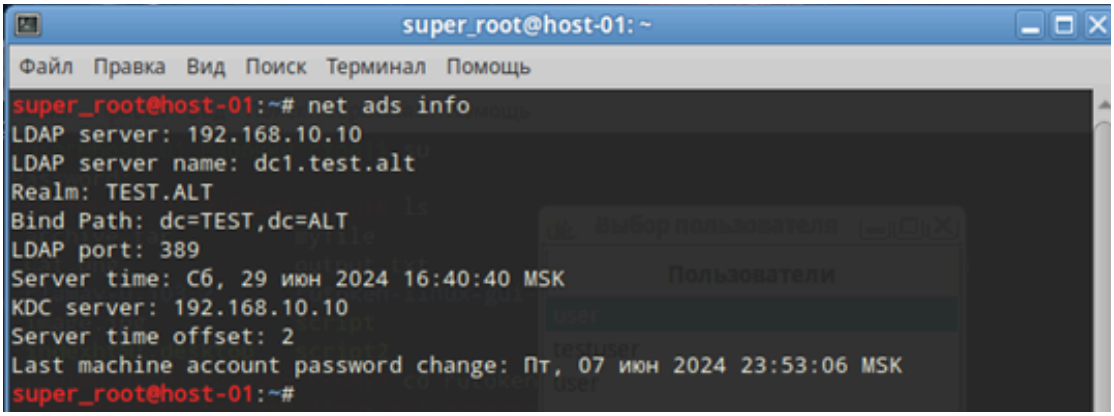
В следующей части мы рассмотрим практическое применение Рутокен ЭЦП 3.0 на базе ОС ALT Linux с заранее установленной и настроенной Samba AD.

3. Практическая часть: настройка Samba AD на базе ОС ALT Linux и интеграция с Рутокеном

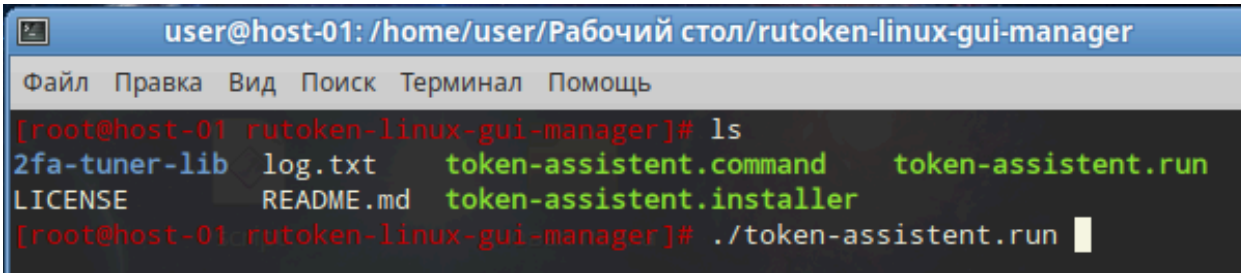
- Установленная и настроенная Samba AD



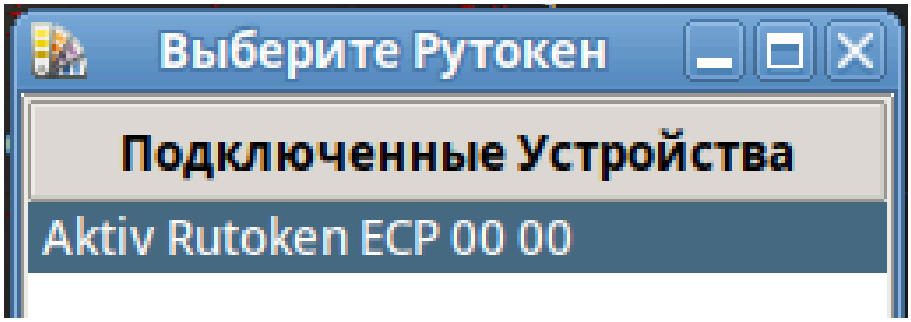
- Введённый ПК пользователя в домен Samba AD



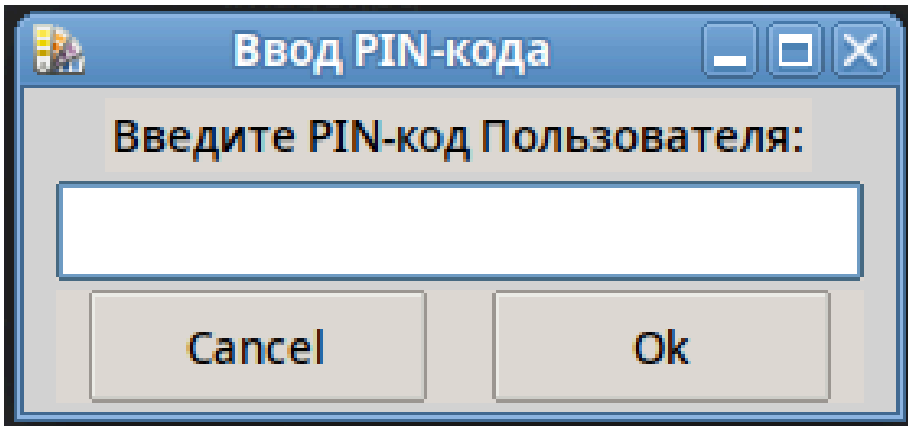
- Последовательность настройки двухфакторной аутентификации:
    1. Подключение Рутокена к USB - Скрипт:
    - # apt-get update
    - # apt-get install git
    - # git clone https://github.com/AktivCo/rutoken-linux-gui-manager --recursive
    - # cd rutoken-linux-gui-manager
    - # ./token-assistent.run”



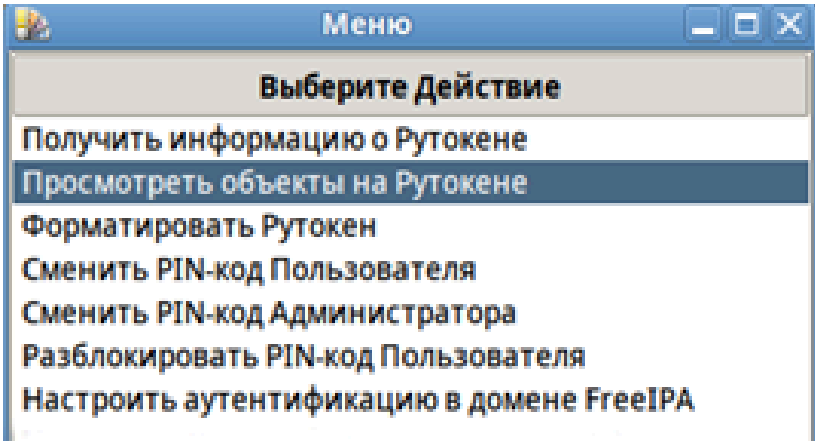
- Установка необходимого программного обеспечения



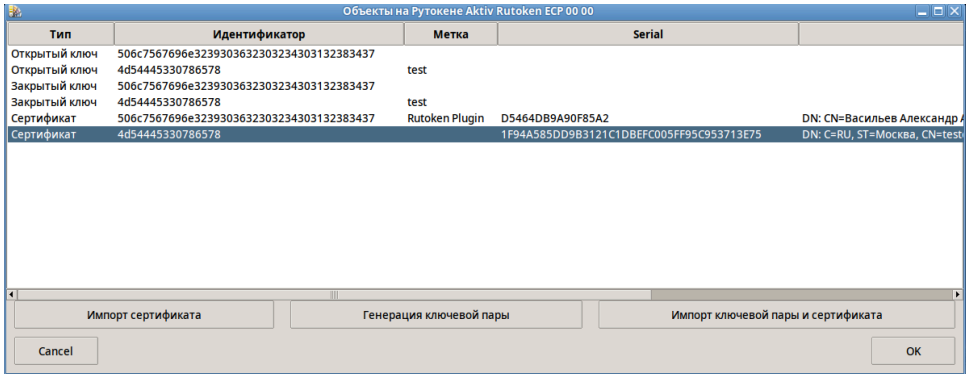
- Вводим PIN-код (Заводской PIN-код при покупке рутокена: «12345678»)



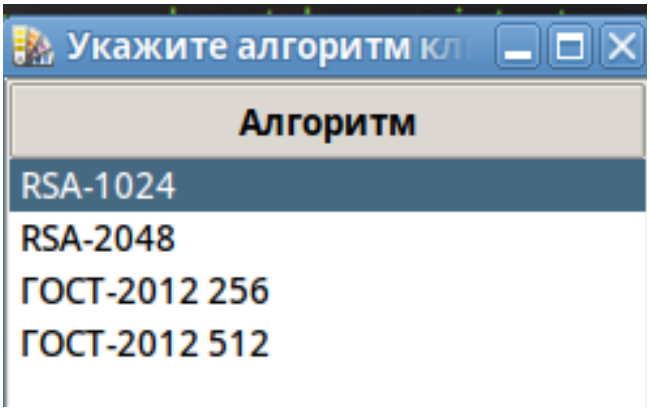
- Генерация ключевой пары и создание сертификата. Нажимаем «Просмотреть объекты на Рутокене»



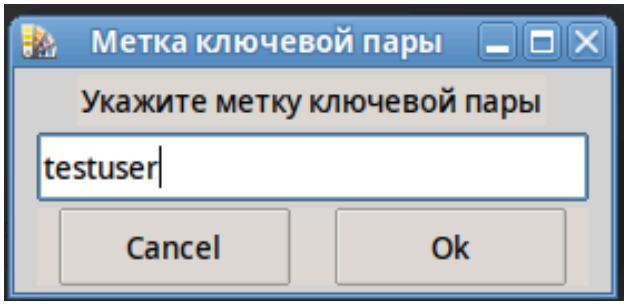
- Нажимаем «Генерация ключевой пары»



- Выбираем «RSA-1024»



- Указываем метку. В нашем случае пусть будет «testuser»

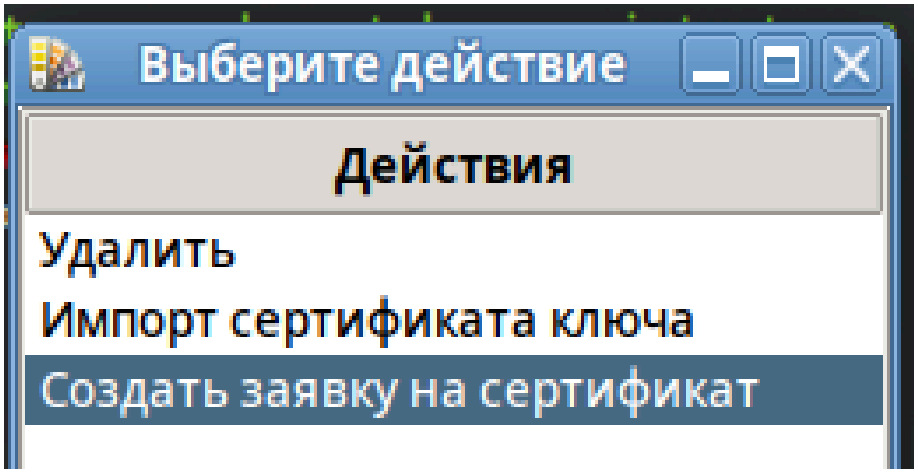


- Настройка локальной аутентификации и тестирование. После генерации переходим обратно в «Просмотреть объекты на Рутокене». Затем нажимаем на наш созданный закрытый ключ.

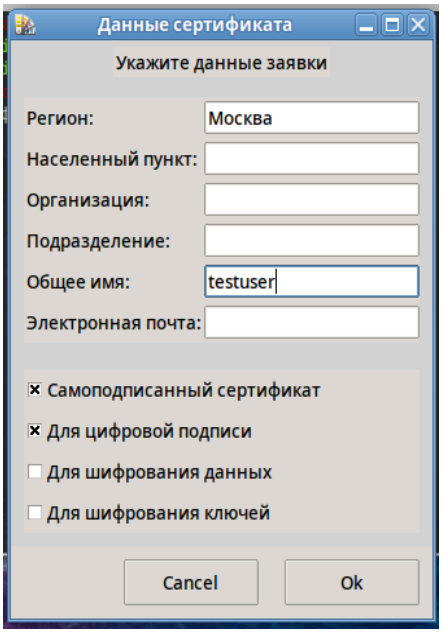
Объекты на Рутокене Aktiv Rutoken ECP 00 00

Тип	Идентификатор	Метка	Serial
Открытый ключ	506c7567696e3239303632303234303132383437		
Открытый ключ	4d54445330786578	test	
Открытый ключ	6f37753767556b6b	testuser	
Закрытый ключ	506c7567696e3239303632303234303132383437		
Закрытый ключ	4d54445330786578	test	
Закрытый ключ	6f37753767556b6b	testuser	
Сертификат	506c7567696e3239303632303234303132383437	Rutoken Plugin	D5464DB9A90F85A2
Сертификат	4d54445330786578		1F94A585DD9B3121C1DBEFC005FF95C953713E75

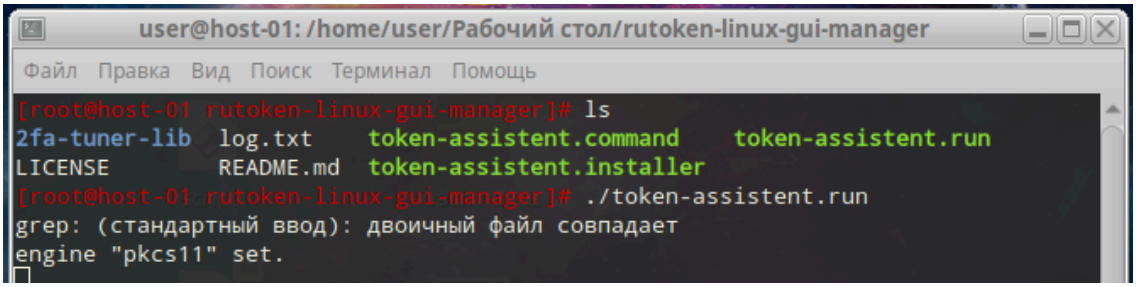
- В следующем меню нам надо создать заявку на сертификат.



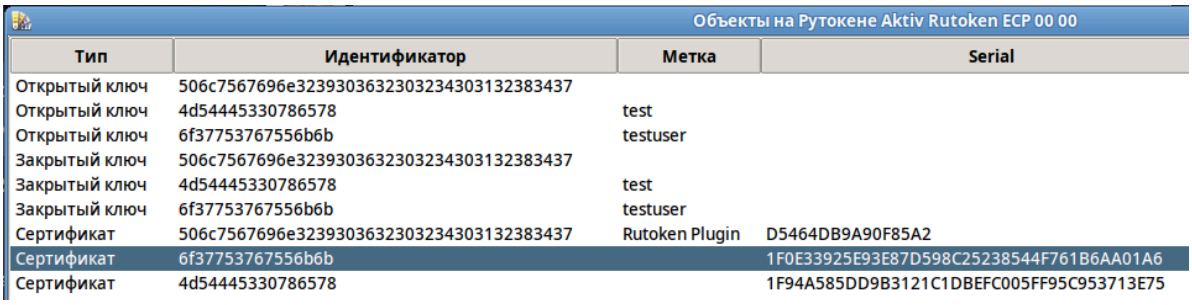
- В нашем случае мы обойдемся самоподписанным сертификатом, поэтому пишем «testuser» в поле «Общее имя».



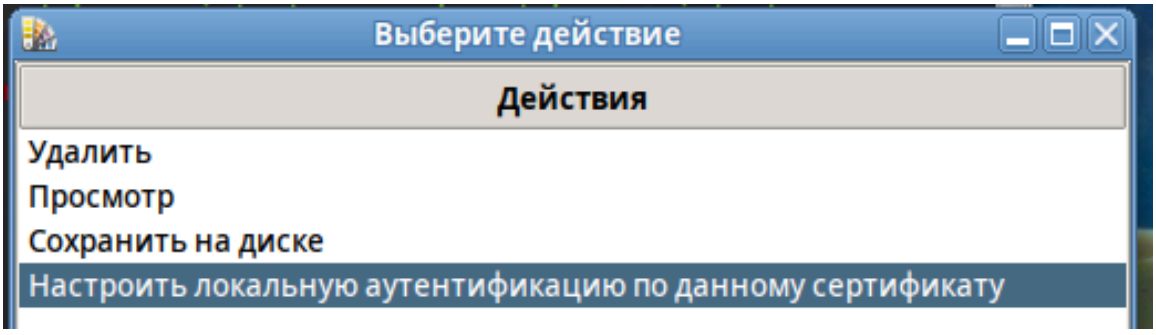
- Ждем создания сертификата



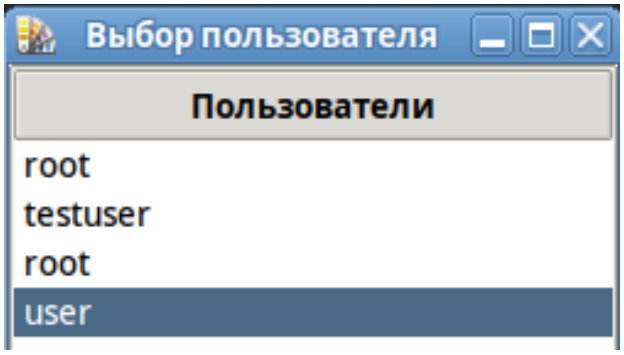
- После генерации переходим обратно в «Просмотреть объекты на Рутокене». Затем нажимаем на наш созданный сертификат.

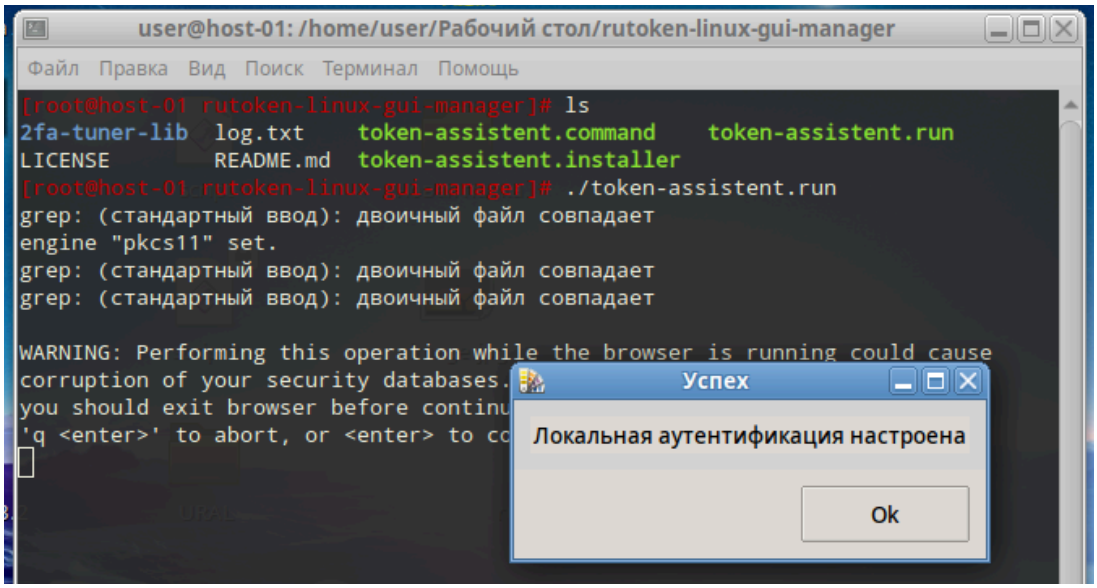


- Затем нажимаем на «Настроить локальную аутентификацию по данному сертификату»

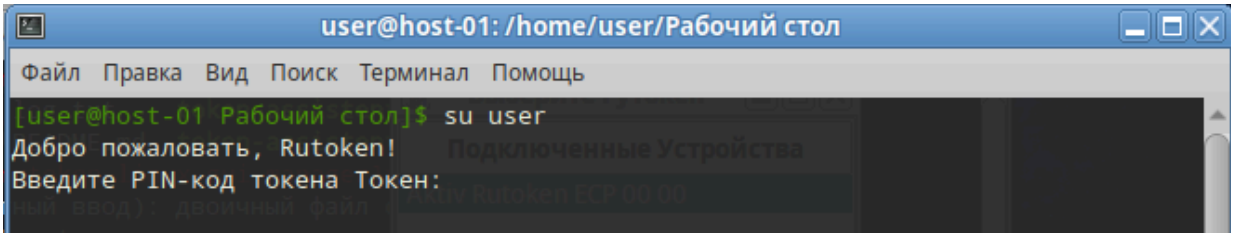


- Выбираем пользователя, который подключен к домену. В нашем случае это пользователь «user»

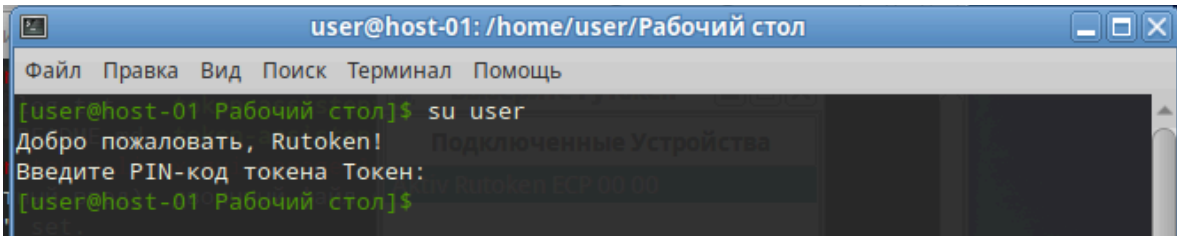




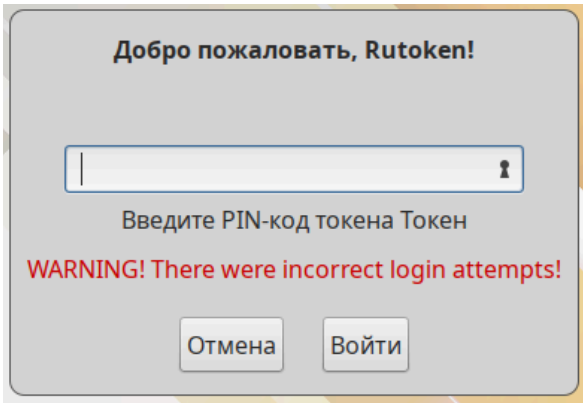
- Проверим. Вводим «su user» и наш PIN-код.



- Проверка пройдена успешно!



- Перезагрузим и зайдем. Вход также будет успешно выполнен при вводе PIN-кода.



Заключение

Использование двухфакторной аутентификации на базе Samba AD, дает возможность повысить уровень безопасности сети, в рамках которой происходит обмен данными. Применение данной технологии на практике продемонстрировало надёжность и эффективность.

Список источников

1. ГОСТ Р 34.10-2012 "Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи" (утв. приказом Федерального агентства по техническому регулированию и метрологии от 7 августа 2012 г. N 215-ст).
2. ГОСТ Р 34.11-2012 "Информационная технология. Криптографическая защита информации. Функция хэширования" (утв. приказом Федерального агентства по техническому регулированию и метрологии от 7 августа 2012 г. N 216-ст).
3. Уймин, А. Г. Разработка методики тестирования системы безопасности автоматизированных систем управления технологическими процессами на основе корпоративного стандарта / А. Г. Уймин // Автоматизация и информатизация ТЭК. – 2024. – № 5(610). – С. 59-65.
4. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам. Учебное пособие для вузов / А. А. Афанасьев, Л. Т. Веденьев, А. А. Воронцов и др.; Под ред. А. А. Шелупанова, С. Л. Грузаева, Ю.С. Нахаева — М.: 2009. — 552 с.
5. Баркалов, К. А. (2018). Информационная безопасность компьютерных систем. Москва: БИНОМ. Лаборатория знаний.
6. Администрирование Samba // BaseALT URL: https://docs.altlinux.org/ru-RU/domain/10.2/html/samba/ch06.html
7. Григорьев, С. В. (2019). Администрирование Linux. Учебное пособие. Санкт-Петербург: Питер.

8. Зырянов, В. И. (2014). Методы и средства обеспечения информационной безопасности. Москва: Горячая линия-Телеком.
9. Константинов, А. Ю. (2017). Информационная безопасность. Практика защиты и анализа. Санкт-Петербург: БХВ-Петербург.