

Муниципальное бюджетное общеобразовательное учреждение
города Новосибирска «Лицей № 136 имени Героя Российской Федерации
Сидорова Романа Викторовича»

**Приложение к исследовательской работе «Обеспечение безопасного
доступа к корпоративной сети»**

**Руководство по эксплуатации
АРМ «Сеть – пользователям»**

Автор: Андреянов Никита Сергеевич,
10 «С» класс

Руководитель: Валюхова Светлана Викторовна,
Учитель информатики высшей категории

г. Новосибирск, 2024 г.

Работа с АРМ «Сеть – пользователям»

Для того, чтобы пользователь мог авторизоваться в сети, ему необходимо получить свою уникальную ключевую пару и сертификат. В целях безопасности пользователю предлагается сгенерировать ключевую пару самостоятельно.

Для этого я разработал веб-приложение «АРМ «Сеть – пользователям», предназначенное для работы с рутокенами и автоматизации генерации ключей. Системный администратор должен установить её на корпоративный веб-сервер, предварительно настроив (приложение 1).

Пользователю необходимо перейти на адрес корпоративного веб сервера с установленным АРМ «Сеть – пользователям», предварительно установив следующий пакет ПО:

- OpenVPN client (community download) по ссылке: <https://openvpn.net/community-downloads/>
- РуТокен плагин (Ссылка появится при переходе на адрес АРМ)
- РуТокен драйверы по ссылке: <https://www.rutoken.ru/support/download/get/rtDrivers-exe.html>
- BAT файл для просмотра контейнеров OpenVPN (Ссылка появится при переходе на адрес АРМ)

Далее для генерации ключевой пары пользователь должен:

1. Перейти на адрес веб-сервера АРМ.
2. Вставить рутокен, выданный организацией, в свой ПК.
3. Ввести пин-код рутокена, нажав на кнопку «войти».

РУТОКЕН

АРМ "Сеть - пользователям"

Ответственное лицо: Андреянов Никита Сергеевич
Эл. почта: testnet@demonet.local

Доступные устройства: Rutoken ECP #0

PIN-код: 12345678 **Войти** Выйти

Ключи на устройстве: Выполните вход на устройство

2. Обязательно следует изменить пин-код пользователя рутокена с заводского (12345678) на свой. Пин-код администратора установит системный администратор при выдаче рутокена.

3. Перейти в раздел «Генерация ключевой пары на устройстве», установить параметры по инструкции системного администратора, нажать кнопку «Выполнить».

Генерация ключевой пары на устройстве

ПОКАЗАТЬ КОД

Id ключа:
☐ Задать (не генерировать)
 AA:BB:CC:DD

Маркер ключа:
 MasterKey

☐ Создать журнальную ключевую пару

RSA

Размер RSA ключа: 2048

Набор параметров: XA

ВЫПОЛНИТЬ

4. После успешного выполнения генерации, выбрать ключевую пару в окне входа.

Доступные устройства: Rutoken ECP #0

PIN-код: 12345678 **Войти** **Выйти**

Ключи на устройстве: key: c0:f5:bb:5a:1b:fe:53:5d:b7:83:80:7c:82:e2:a9:6e:83:9e:21:47

5. Заполнить поля в соответствии с указаниями системного администратора. При настройке АРМ, большинство полей уже будет заполнено и заблокировано системным администратором самостоятельно.

Формирование PKCS10 запроса

ПОКАЗАТЬ КОД

subjectSignTool:
 СКЗИ "РУТOKEN ЭЦП"

Алгоритм хэширования: SHA256

countryName: RU stateOrProvinceName: Moscow

localityName: Novosibirsk streetAddress: street

organizationName: OOO TestNet organizationalUnitName:

postalAddress: Novosibirsk, Ul. Testovaya title:

commonName: masterkey pseudonym: Андреев Никита Серг

givenName: Андреев Никита

emailAddress: andreev.nikita@yandex

Key Usage: ☒ digitalSignature ☒ nonRepudiation ☒ keyEncipherment ☒ dataEncipherment

Ext Key Usage: ☐ emailProtection ☒ clientAuth ☐ serverAuth ☐ codeSigning ☐ timeStamping ☐ msCodeInd ☐ msCodeCom ☐ msCTLSign ☐ OCSP ☐ CryptoPro RA user

Policies: ☐ KC1 ☐ KC2 ☐ KC3 ☐ KB1 ☐ KB2 ☐ KA1

Custom Extensions: ☐ Critical value: value должен быть в base64

ДОБАВИТЬ НОВОЕ РАСШИРЕНИЕ

ВЫПОЛНИТЬ

6. Передать системному администратору значение в белом поле после нажатия кнопки «выполнить».

-----BEGIN CERTIFICATE REQUEST-----
MIID6TCCAIECAQAwggFCMQswCQYDVQQGEwJ5VTEPMA0GA1UEC4wGTW9zY293MRQw
EgYDVQQHDA0b3Zvc2liaXJzazEPMA0GA1UECQwGc3RyZWV0MRQwEgYDVQQKDA0P
T08gVGVzdE5ldDEwMC4GA1UEEAwnTm92b3NpYmlyc2sslFVsLiBUZXN0b3ZheWEs
IGQuIDESIGt2LyAxMRIwEAYDVQQDDA0tYXN0ZXJrZXIwOzA5BghNVBEEMMtCQ0L3Q
tNGA0LXRj9C90L7QsiDQndC40LrQuNGC0LA0KHQtdGA0LPQtdC10LLQuNGHMTsw
OQYDVQQqDD0LQkNC90LTrgNC10Y/QvdC+0LIg0J3QuNC60LjRgtCwINCh0LXRgNCz
0LYQtdCw0LiRbzEIMCMGCSqGSIb3DQEFJARYWw3LzYWRB+ZW5A7GVtb25ldC5eb2Nh

ВЫПОЛНИТЬ

Внимание! Запрещается вносить изменения в данное поле после генерации запроса!

9. Системный администратор выполнит генерацию сертификата, после чего пришлёт его. Далее необходимо его загрузить на рутокен. Для этого нужно перейти в меню «Работа с сертификатами», «Импорт сертификата на устройство». Поместить туда данные сертификата, который предоставил администратор.

Импорт сертификата на устройство

ПОКАЗАТЬ КОД

Сертификат в формате PEM

-----BEGIN CERTIFICATE-----
MIIFBTCCA+2gAwIBAgIRALwdWpluAQavbQ/vJNAxH3UwDQYJKoZIhvcNAQELBQAw
ga8xCzAJBgNVBAYTALJVMRQwEgYDVQQJDA0b3Zvc2liaXJzazEZMBcGA1UEBwwwQ
Tm92b3NpYmlyc2sgQ2l0eTEQMA4GA1UECgwHVEVTVCBBDQTEfMB0GA1UECwwWTXkg
T3JnYW5pemF0aW9uYWwgVW5pdDEQMA4GA1UEAwwHVEVTVCBBDQTEqMCgGCsGSIb3
DQEFJARYbYW5kcmVhbm92Lm5pY2tpdGFAeWfuZGV4LnJ1MB4XDTI0MDcwNzE3NTIw
NV0XDTM0MDcwNTE3NTIwNVowgYUxCzAJBgNVBAYTALJVMQ8wDQYDVQQJDAZNb3Nj
b3cyFDASRbNVR4cMC05vdm9zaWJncnNrMRQwEgYDVQOQKDA+PT08eVGVzdE5ldDES

Категория сертификата:
☒ Пользовательский
☐ Корневой
☐ Другой

ВЫПОЛНИТЬ

10. Выполнить bat файл для чтения контейнеров OpenVPN на рутокене.

```

E:\Desktop>"C:\Program Files\OpenVPN\bin\openvpn.exe" --show-pkcs11-ids "C:\Windows\System32\rtPKCS11ECP.dll"
2024-07-08 01:48:10 PKCS#11: Adding PKCS#11 provider 'C:\Windows\System32\rtPKCS11ECP.dll'

The following objects are available for use.
Each object shown below may be used as parameter to
--pkcs11-id option please remember to use single quote mark.

Certificate
  DN: C=RU, ST=Moscow, L=Novosibirsk, O=000 TestNet, CN=masterkey, emailAddress=sysadmin@demone
  Serial: BC1D5A922E0106AF6D0FEF24D0311F75
  Serialized id: pkcs11:model=Rutoken%20ECP;token=Rutoken%20ECP%20%3cno%20label%3e;manufacturer=Aktiv%20Co
=4352782a;id=%c0%f5%bbZ%1b%feS%5d%b7%83%80%7c%82%e2%a9n%83%9e%21G

E:\Desktop>pause
Press any key to continue . . .

```

11. Скопировать строку после «serialized id:» в поле pkcs11-id файла конфигурации клиента.

Если выбран метод подключения при помощи файла конфигурации (образец файла представлен в Приложении 2), системный администратор его самостоятельно сгенерирует и предоставит.