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.

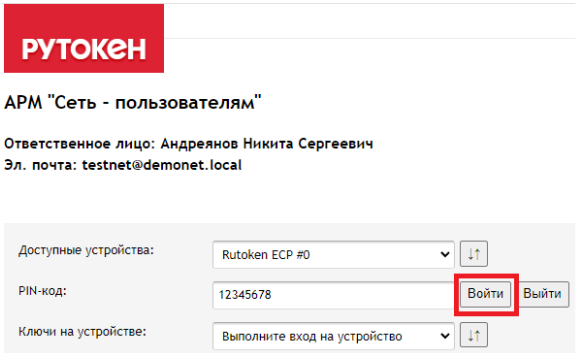
Для этого я разработал веб-приложение «АРМ «Сеть – пользователям», предназначенное для работы с рутокенами и автоматизации генерации ключей. Системный администратор должен установить её на корпоративный веб-сервер, предварительно настроив (приложение 1).

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)

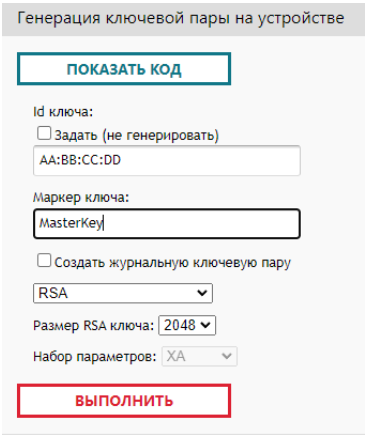
Далее для генерации ключевой пары пользователь должен:

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

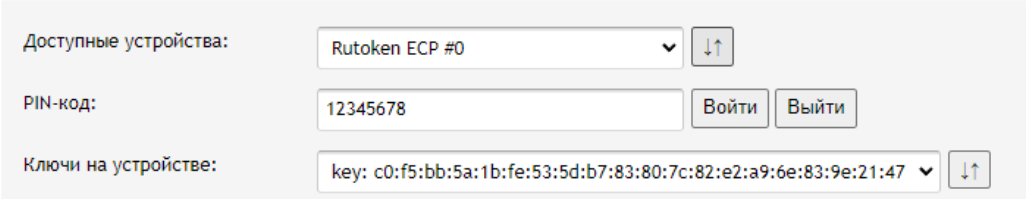


2. Обязательно следует изменить пин-код пользователя рутокена с заводского (12345678) на свой. Пин-код администратора установит системный администратор при выдаче рутокена.

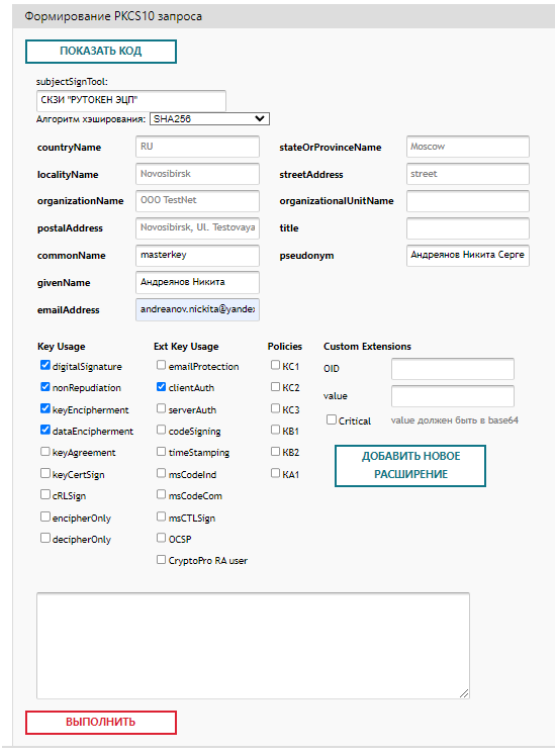
3. Перейти в раздел «Генерация ключевой пары на устройстве», установить параметры по инструкции системного администратора, нажать кнопку «Выполнить».



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



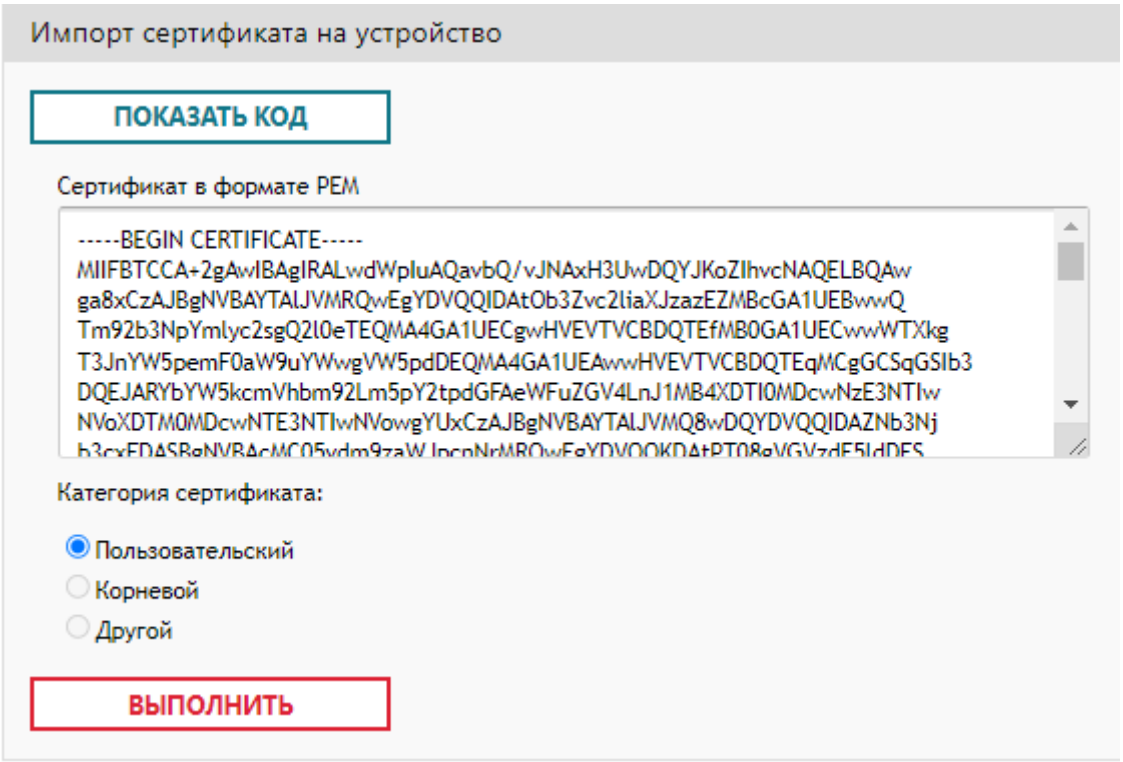
5. Заполнить поля в соответствии с указаниями системного администратора. При настройке АРМ, большинство полей уже будет заполнено и заблокировано системным администратором самостоятельно.



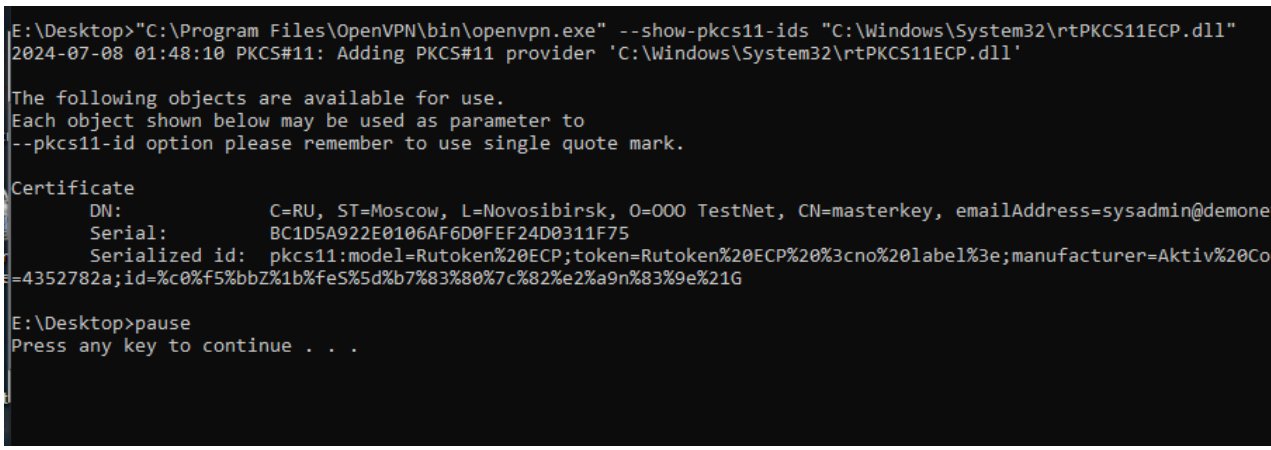
6. Передать системному администратору значение в белом поле после нажатия кнопки «выполнить».

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.



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



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.