Лабораторная работа №2.
Сценарий «PKCS#12 и загрузка в хранилище Windows»

Работа является продолжением работы №1. Для её выполнения преподавателем предоставляется скрипт создания сертификата с использованием криптобиблиотеки openssl в режиме командной строки. Для успешного выполнения нужно изменить некоторые параметры скрипта согласно задания ниже.

Скрипт собирает все 3 сертификата (root, mca, user) и закрытый ключ конечного сертификата собираются в 1 пакетный файл формата .p12 (PKCS#12). Обратите внимание, что транспортный контейнер PKCS#12 позволяет включать и закрытый ключ, и всю цепочку сертификатов. Это делает его популярным для передачи (в 1 файле) всей ключевой информации. Однако, **запомните, что хранить ключи и сертификат в PKCS#12 на постоянной основе нельзя! Для этого есть хранилище системы с необходимыми правами доступа.**

Сертификаты собираются в 1 файл (консольная команда type), после чего экспортируются в p12.

```
type usercert.crt groupmca.crt rootca.crt > certs.crt

openssl.exe pkcs12 -export -passin pass:"HSEPassw0rd" -passout
pass:"UserPass123" -in certs.crt -inkey usercert.key -out final.p12
```

Файл .p12 автоматически импортируется в хранилище Windows с помощью штатной утилиты certutil (можно использовать аналог,например, Certmgr.exe)

```
certutil -f -p UserPass123 -importpfx final.p12
```

Приступайте к работе 2 после того, как внесли в скрипт все изменения согласно требованиям работы 1.

Необходимо воспроизвести действия преподавателя с помощью предоставленного скрипта, изменив несколько простых параметров в базовом скрипте:

- Пароли защиты всех сертификатов
- Увеличить размер ключа в битах (до 8K)
- Экспорт закрытого ключа из .p12 (PKCS#12) должен быть разрешен (NoExport)

Итог работы (ВАЖНО подгрузить все файлы): в LMS загрузите 2 файла (с изменениями согласно заданию):

- итоговые сертификат в формате .p12
- скриншот установленного сертификата, одновременно с запущенным окном экспорта к котором видено, что можно экспортировать закрытый ключ (см. пример ниже)

Вес работы при выполнении всех условий: _____

!!! Обратите внимание, что:

- Предоставленный скрип уже **содержит все необходимые действия** (необходимо только изменить значения некоторых параметров, см. выше).
- Для корректной работы утилиты certutil необходимо запускать .bat файл с правами администратора. В этом случае сертификат будет установлен в хранилища локального администратора. Для доступа в хранилище запустите Консоль управления windows (Win-S →)mmc), выберете оснастку «Сертификаты». Порядок действий в MCC: «Файл» → «Добавить или удалить оснастку…»→ «Сертификаты» → Кнопка «Добавить» → в появившемся окне выбрать пункт «учетной записи компьютера» → ОК. Откроется хранилище администратора.

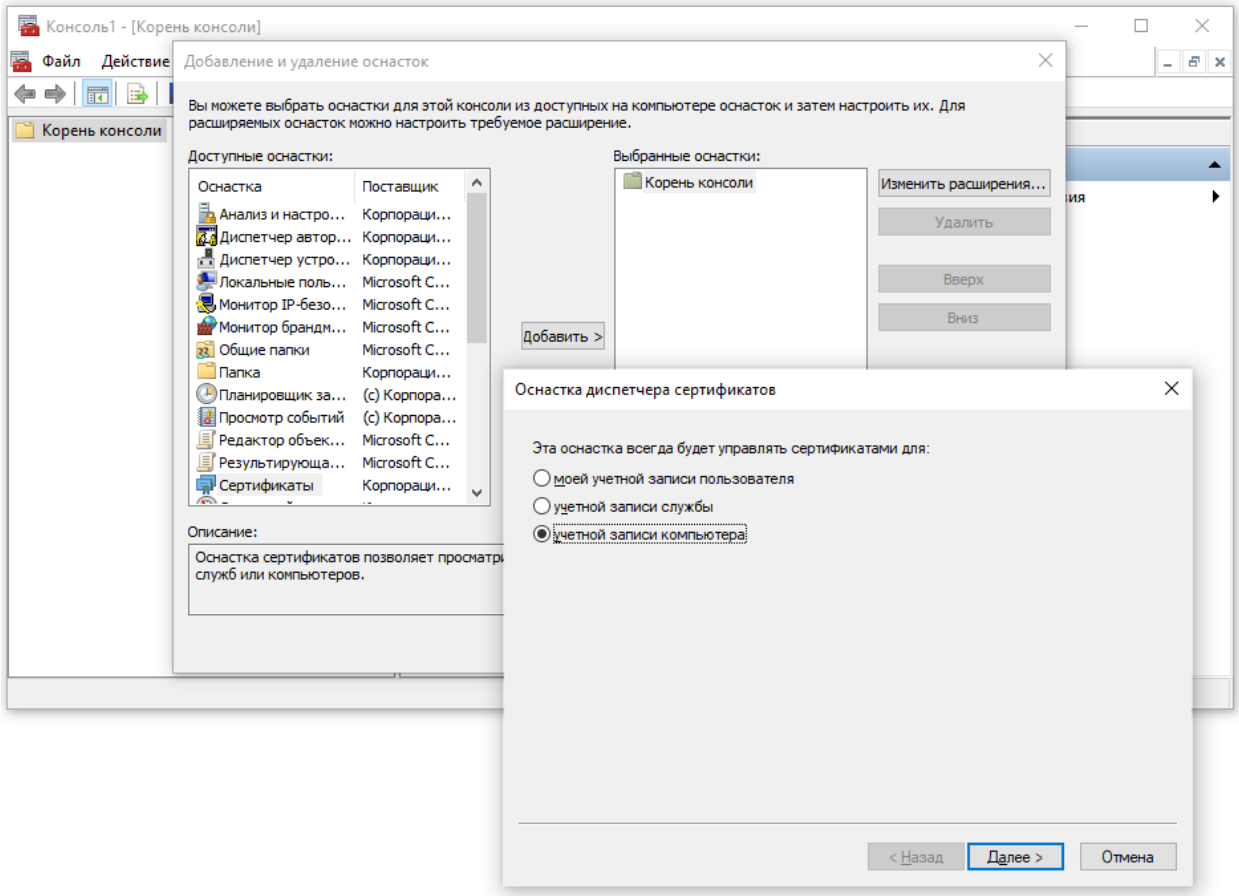

Рисунок 1. MMC – Оснастка «Сертификаты»

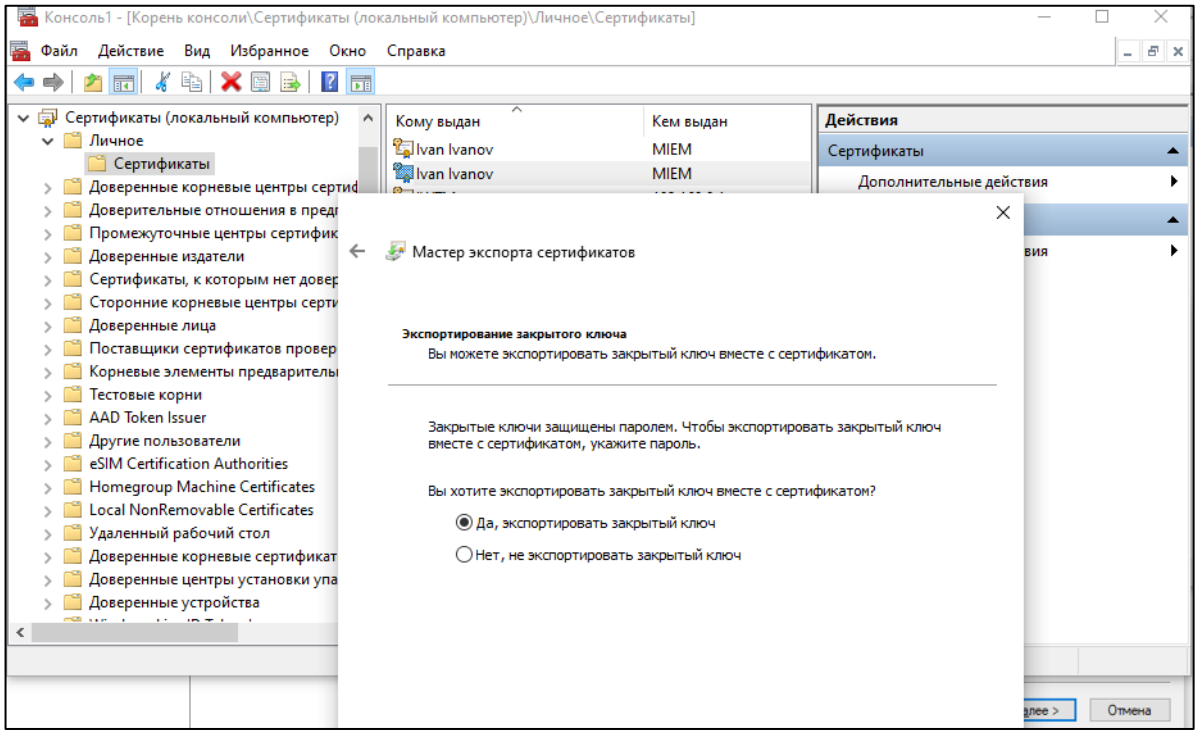

Рисунок 2. Пример скриншота с разрешением на экспорт закрытого ключа. Для отчета по л/р необходимо предоставить такой скриншот с параметрами, указанными в л/р 1 и 2.