# Лабораторная работа №4

# Сценарий «Пользовательское расширение и ЭП»

Работа является продолжением работы №3 и состоит из 2-х частей:

- Часть 1 — задание на собственное расширение в сертификате X.509 (3 балла).
- Часть 2 — задание на использование цифровых сертификатов для решения прикладных задач, такой как электронная подпись (3 балла).

Все работы выполняются с сертификатом пользователя (usercert.crt).

**Часть 1. Собственное расширение сертификата X.509.**
**Вес части при выполнении всех условий: 3 балла**

Гибкость стандарта X.509 объясняется в т.ч. возможностью добавления собственных полей, т.н. пользовательских расширений. Добавьте в конечный сертификат usercert.crt пользовательское разрешение (англ. custom extension) «Profession» с информацией о профессии пользователя на английском или русском языке. Укажите свою профессию. Для реализации задания добавьте в конфигурационный файл OpenSSL (openssl.cnf) следующую строку в секцию расширений пользовательского сертификата [ usr_cert ].

**1.2.3.412=ASN1:UTF8String:IT Specialist**

Если всё выполнено корректно, то после запуска bat-файла со скриптами для генерации сертификата (do_it.bat) в пользовательском сертификате появится дополнительное поле как на рисунке ниже**. Для выполнения задания на полный балл обозначьте расширение как критическое**.

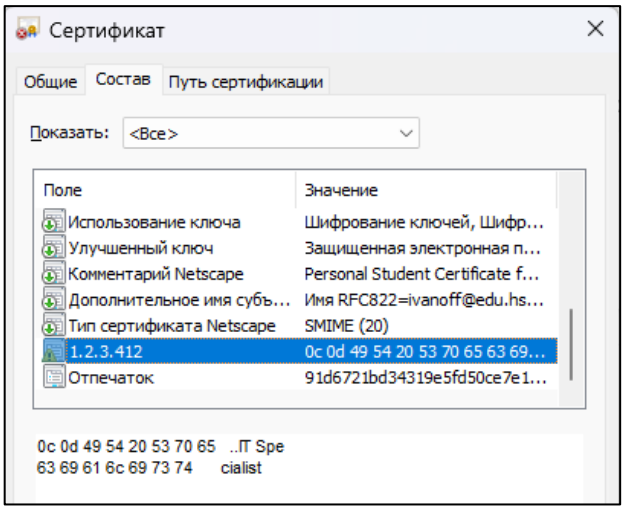


Рисунок 1. Дополнительное расширение сертификата

**По итогу части 2 Л/Р загрузите в LMS скриншот сертификата (1 файл) с указанием Вашей профессии.** Текст на скриншоте должен ясно читаться.

**Часть 2. Подпись и проверка подписи файла с использованием сертификата X.509**
**Вес части при выполнении всех условий: 3 балла**

Цель лабораторной работы — использовать цифровой сертификат для электронной подписи (ЭП) файла, включая: манипуляции с ключами, подписание файла, проверка подписи. Обратите внимание, что ЭП в работе формируется как отдельный файл (detached signature).

Для выполнения работы выполните следующие действия:

1. До всех действий **переименуйте файл readme.txt в папке OpenSSL в свою фамилию (например, ivanov.txt)** для идентификации вас при сдаче работы**.**

2. Подпишите файл (в примере ниже readme.txt, у вас — уже переименованный) закрытым ключом**, получите файл подписи:**

```
openssl dgst -sign usercert.key -sha256 -out readme.txt.sig -binary readme.txt
```

Обратите внимание, что в папке появился файл подписи **с расширением .sig.**

3. Конвертируйте сертификат из формата DER (.crt) в формат PEM (.pem), с которым работает OpenSSL. А затем, экспортируйте открытый ключ из сертификата в файл (pubkey.usercert.pem):

```
openssl x509 -inform PEM -in usercert.crt > usercert.pem
openssl x509 -in usercert.pem -noout -pubkey > pubkey.usercert.pem
```

4. Проверьте подпись, используя публичный ключ (pubkey.usercert.pem). Получите сообщение о том, что проверка прошла (Verified OK).

```
openssl dgst -verify pubkey.usercert.pem -sha256 -signature readme.txt.sig -binary readme.txt
Verified OK
```

5. Измените подписываемый текстовый файл (добавьте 1 символ, например) и проверьте подпись повторно (командой п. 4), используя usercert.pem. Получите сообщение о том, что подпись и файл не соответствуют друг другу (Verification Failure)

**По итогу части 2 Л/Р загрузите в LMS скриншот окна со всеми командами,** перечисленными выше (1 файл). Файл readme.txt должен быть переименован, как сказано в п. 1.