*Лабораторная работа №5*

**Инфраструктура открытых ключей**

Цель работы: ознакомиться с принципами работы инфраструктуры открытых ключей, методами ее работы, хранения ключей и форматом сертификатов X.509. Разработать консольное приложение, работающее со встроенным в операционную систему хранилищем сертификатов.

Задание:

1. Сгенерировать самоподписанный сертификат CA. В качестве CN указываем 127.0.0.1, остальные данные можно указать вымышленные
   - вариант с openssl описан в статье на habr
   - вариант с CA Smallstep описан в статье на habr
2. Установить сертификат CA
   - перевести сертификат в формат PEM
     `openssl x509 -in root_ca.crt -out root_ca.pem -outform PEM`
   - установить сертификат CA
     - на ubuntu
     - на windows
3. Сгенерировать сертификат для сервера
   - вариант с openssl описан в статье на habr
   - вариант с CA Smallstep описан в статье на habr
4. Запустить сервер
   - Вариант с Node.js описан в статье на habr
   - Вариант с Nginx описан в gist на github
5. Обратиться к серверу
   `curl https://127.0.0.1:9443`
6. Опционально можно выпустить сертификат для localhost и зайти на сервер через браузер, но всегда надо помнить о MitM

*В отчёт обязательно надо включить описание хода работы и вывод `openssl X509 --text` для выпущенных сертификатов.*

Об инфраструктуре открытых ключей:

- Лекция
- http://www.intuit.ru/studies/courses/110/110/info - курс на интуите (в частности 3 и 6 лекции)
- https://habrahabr.ru/post/194664/ - разбираем X.509 сертификат
- https://ru.wikibooks.org/wiki/Введение_в_PKI - введение в PKI
- https://habr.com/ru/articles/671730/ - Практика на примере OpenSSL и CA Smallstep

Контрольные вопросы

1. Принципы работы PKI;
2. Механизмы PKI;

3. Структура PKI;
4. Сертификаты в PKI;
5. Жизненный цикл сертификатов;
6. Форматы хранения сертификатов;
7. Цепочки сертификатов;
8. Структура сертификата X.509;
9. Нотация ASN.1.
10. Методы кодирования сертификатов. BEM, DER, PER.