Как происходит handshake?

Какие бывают версии TLS ? (1.0, 1.1, 1.2, 1.3)

Какая в данном случае используется версия TLS (в зависимости от алгоритма)?

CA (ZSS)

1. Сгенерировать приватный ключ: sh generateKey.sh
2. Сгенерировать сертификат СА: sh generateCA.sh

При создании CN = CA-LAB22-ZSS

Появились key – закрытый ключ и crt – самоподписанный сертификат СА

1. Получаем csr от ресурса (запрос на сертификат)
2. Подписываем запрос ресурса sh responseReq.sh

Появился crt ресурса, подписанный мной

1. Передаем 2 сертификата

Resource (KAV)

1. Сгенерировать приватный ключ: sh generateKey.sh
2. Сгенерировать csr: sh generateReq.sh
3. Принимаем 2 сертификата

На сертификат CA 2 раза лкм, устанавливаем в «Доверенные корневые центры сертификации». Он будет корневым.

Нужно, чтобы windows доверяла сертификату ресурса.

Также устанавливаем сертификат ресурса, только в «Личное».

Это нужно, если сервер работает на Windows и будет использовать HTTPS.

Открываем certmgr.msc для проверки.

notepad C:/Windows/System32/drivers/etc/hosts – устанавливаем домен

127.0.0.1 ZSS

127.0.0.1 KAV

127.0.0.1 LAB22-ZSS

127.0.0.1 LAB22-KAV