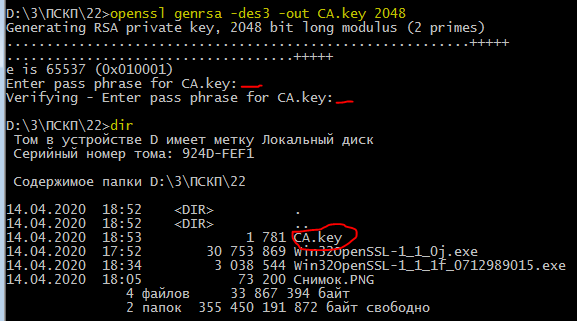
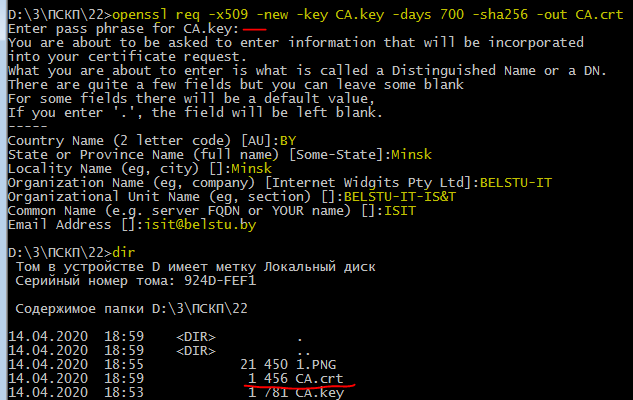
**HTTPS** позв. аутентифицировать С  
(К если надо созд. безопасный зашифр. канал связи)  
в основе протокол *TSL* (обесп аутен+шифр), он расп ниже протокола HTTP

Чтобы браузер мог делать HTTPS-запросы к др. серверам, у него дб сертификаты этих удост центров с откр ключами

1) команда genrsa – генер **приват ключ Са** (он шифрует цифр.подпись, кот. мб прочитана с пом. откр ключа)  
**(CA.key)**

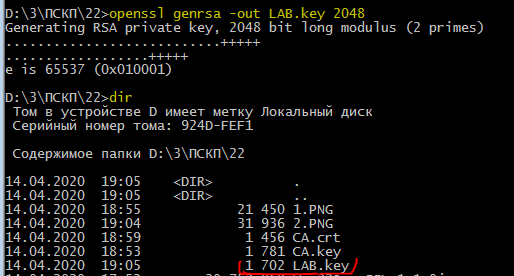


2) генер **сертификат** (в основе TSL-протокола. Предполаг, что К и С доверяют общему центру серт.  
=> сертификат на кот. мы будем шифровать ресурсы  
**(CA.crt)**



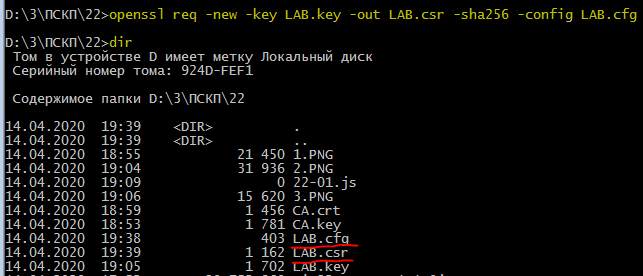
3) генер **публич ключ** для ресурса (Тут des3 нет)   
генер из прив.ключа (в обр сторону нельзя)

чтобы К мог проверить правильность сертификата со стороны С надо наличие на стороне К сертификата с публ. ключом  
тогда он м прочитать цифр. подпись к-ю сделал удост.центр на сертификате сервера  
т.о. он м проверить правильность сертификата  
**(LAB.key)**

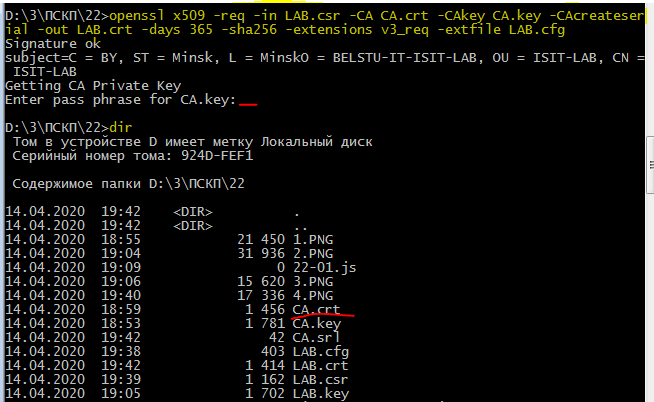


4) **конфиг. файл** для ресурса LAB.cfg  
тут сами все пишем: версия, имя  
*[alt\_names]* – какие адреса поддерживает наш ресурс.  
Если вместо этих адресов (LAB22-CJA, CJA) пропишем например localhost, нам выдаст предупреждение «такие имена в сертификате не упомянуты»  
**(LAB.cfg)**

5) генер **запрос на получение** сертификата: (исп. конф.файл, кот отвеч на вопросы)  
(сод. инфу: кто выдал, кому, ск.действи, для каких целей исп)  
(сод. в себе публ ключ, кот. генер на основе прив.ключа)  
**(LAB.csr)**



6) генер **сертификат** на основе запроса (исп. публ ключ) передаем наш запрос certification-authority, а тот д.подписать след. командой:  
(созд. серийный №)  
**(LAB.crt)**



7) заносим наш сертификат в наше **хранилище сертификатов (mmc.exe – открыть Косно)**  
Сертификаты – Импорт…  
\* POIT (Издатель – наши д-е: кто,email,город…)  
\* RS-LAB22-CJA (для нашего ресурса. Издатель + папка Субъект: то же самое но для ресурса)

цифр.подпись берется в хэш, кот. потом шифруется -> м показать сертификат кому угодно  
  
8) заносим домены в **hosts** (C:\Windows\System32\drivers\etc\hosts)

9) **тестирование** в браузере (FIREFOX)  
https://localhost:3000/ – «на ваш страх и риск»  
https://cja:3000/ – ок  
https://lab22-cja:3000/ - ок

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

К посыл запрос на С, С подпис и обратно,К провер сертиф и отсылает какие шифры м использ для переадчи д-х  
С получ откр ключ и с пом него шифруется инфа и предается др между другом с пом tls

**x509** – стандарт формата файлов, кот используют сертификат (есть еще 500, групповые, многодоменные, разный формат)

**кто выдает этот сетификат?**  
есть утвержденный серт.центры, кот. уже в доверии  
или м. самому выдавать, но надо зарегать свой серт. центр