**Лабораторная работа 22**

**ПСКП, ПОИТ-3**

1. Для выполнения лабораторной работы, студенты должны работать по парам, поочередно выполняя роли **CA** (Certification authority) и **Resource**.
2. В создаваемых в процессе выполнения лабораторной работы данных будет использоваться обозначения **XYZ, ABC** – инициалы студентов (IPN – Иванов Петр Николаевич).
3. Для генерации сертификатов примените библиотеку **OpenSSL**.

**Задание 01 CA**

1. Создайте сертификат CA с CN = **CA-LAB22-XYZ**.
2. Получите от **Resource** запрос на генерацию сертификата.
3. Сгенерируйте сертификат для **Resource** позаданному им запросу. Разрешите доступ к следующим доменам: **LAB22-ABC** и **ABC**
4. Передайте **Resource** сгенерированный сертификат и свой CA- сертификат.

**Задание 02 Resource**

1. Сгенерируйте запрос на сертификат к CA с CN = **RS-LAB22- ABC** и передайте его CA для генерации сертификата.
2. Получите от СА два сертификата.
3. Импортируйте СА-сертификат в хранилище сертификатов (доверенные центры сертификации).
4. Разработайте приложение **22-01**, которое принимает GET-запросы по https-протоколу. Тестирование выполните с помощью браузера.

**Задание 03 CA/Resource**

1. Поменяйтесь dв паре ролями и выполните лабораторную работу с другой ролью.

**ТЕОРИЯ**

1)команда genrsa – генер приват ключ  
алгоритм rsa

библиотека openssl  
алг шифрования (и хеширования) des3 (ключ слово?)  
вых файл CA.key  
Использ 2018 байт

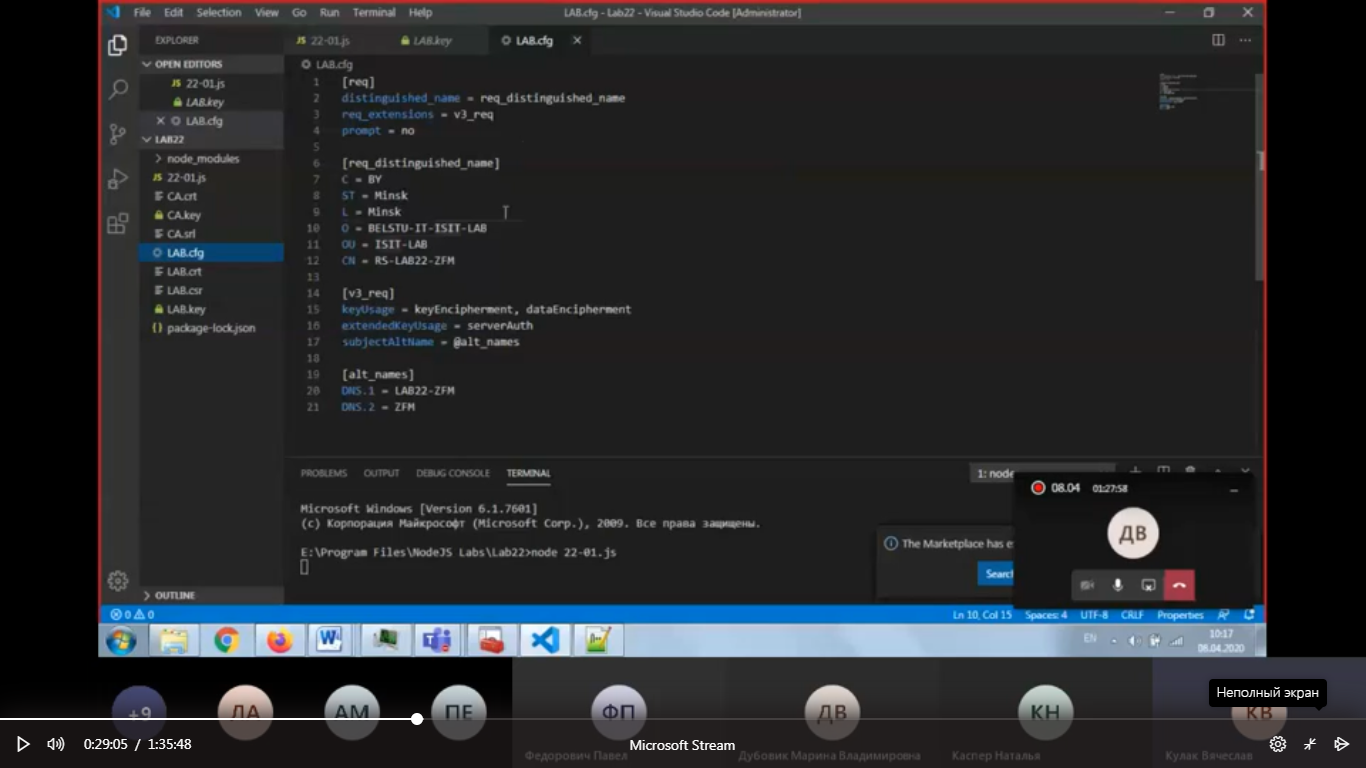
=> ключ

2) генер сертификат  
стандарт –x509  
действит 700 дней  
шифрования –sha256 (затем надо ключ.фразу указ)  
вых. файл CA.crt

далее указ:  
имя страны: BY  
штаты: Minsk  
имя организации: BELSTU-IT…

=> сертификат на кот. мы будем шифровать ресурсы (?)

3) генер приват ключ для ресурса  
openssl genrsa –out LAB.key 2048  
(тут des3 шифрования нет)

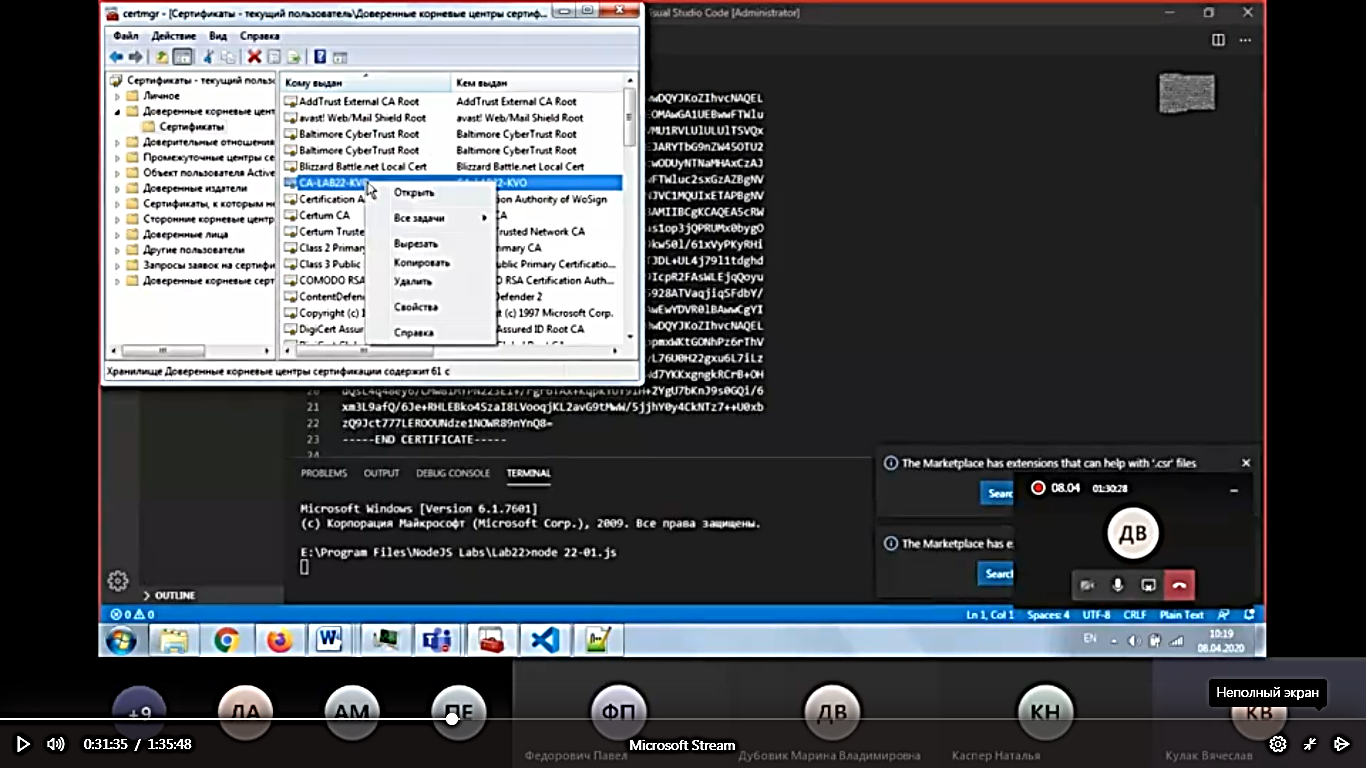
4) конфиг. файл для ресурса LAB.cfg  


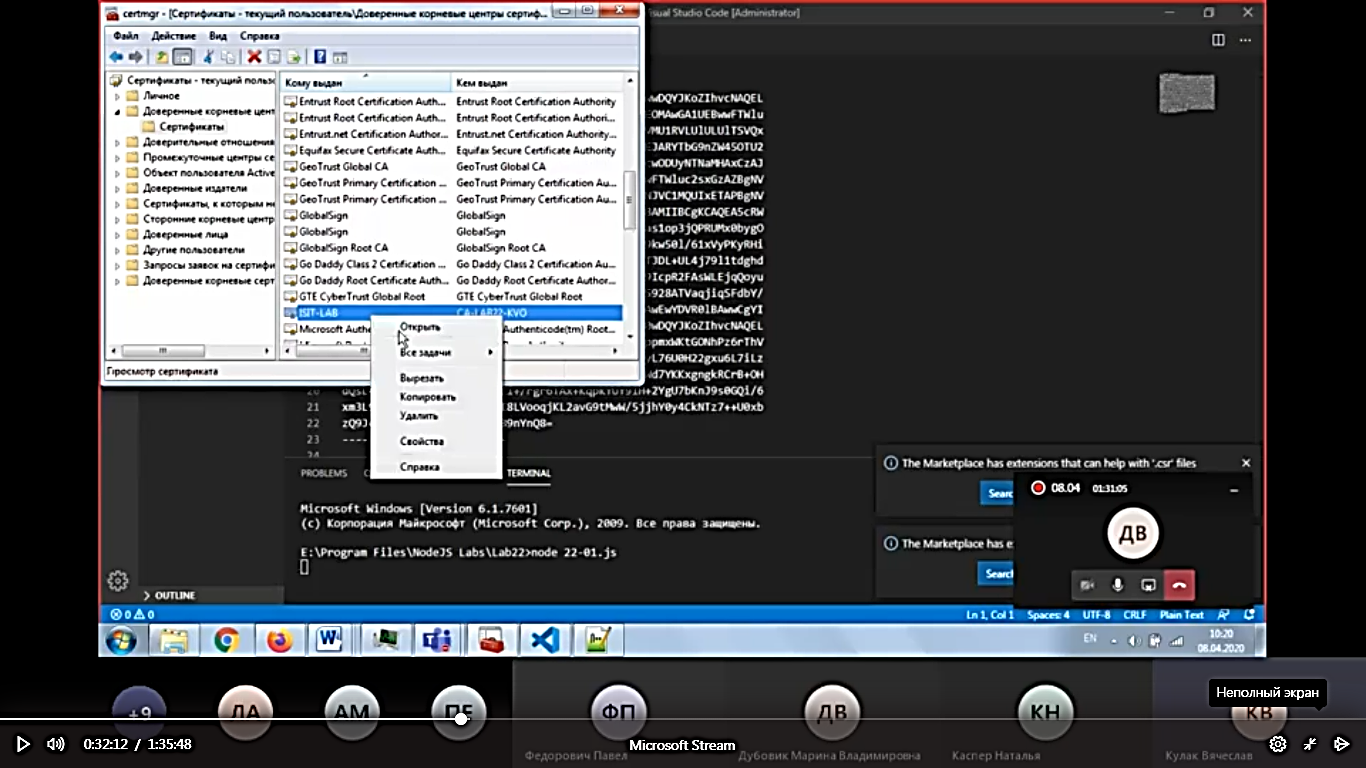
тут пишем: версия, имя  
[alt\_names] – какие адреса поддерживает наш ресурс  
если вместо этих адресов (LAB-22M, 2FM) пропишем например localhost, нам выдаст предупреждение «такие имена в сертификате не упомянуты»

5) генер запрос на сертификат:  
openssl req –new –key LAB.key…  
исп ключ, конф.файл, хеширование –sha256  
вых файл – LAB.csr

6) мы передаем это нашему CA authntification-authority, и он должен подписать это след. командой:  
вх файл – наш запрос   
сертификат, ключ …  
создаем серийный номер  
и вых файл будет действ 365 дней

=> получается наш сертификат LAB.crt

7) заносим наш сертификат в наше хранилище сертификатов  
  
алг хеширования sha256  
подпись, серийный номер, версия v3  
(папка Издатель)наши д-е: кто, емэйл, организация, город…

для нашего ресурса:  
  
Папка Издатель + папка Субъект (то же самое но для ресурса)

если в браузере localhost:8080 – предупреждение (сертиф дейст только для след доменов  
если 2fm:8080 – все ок

hosts? (C:\Windows\System32\drivers\etc\hosts)  
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