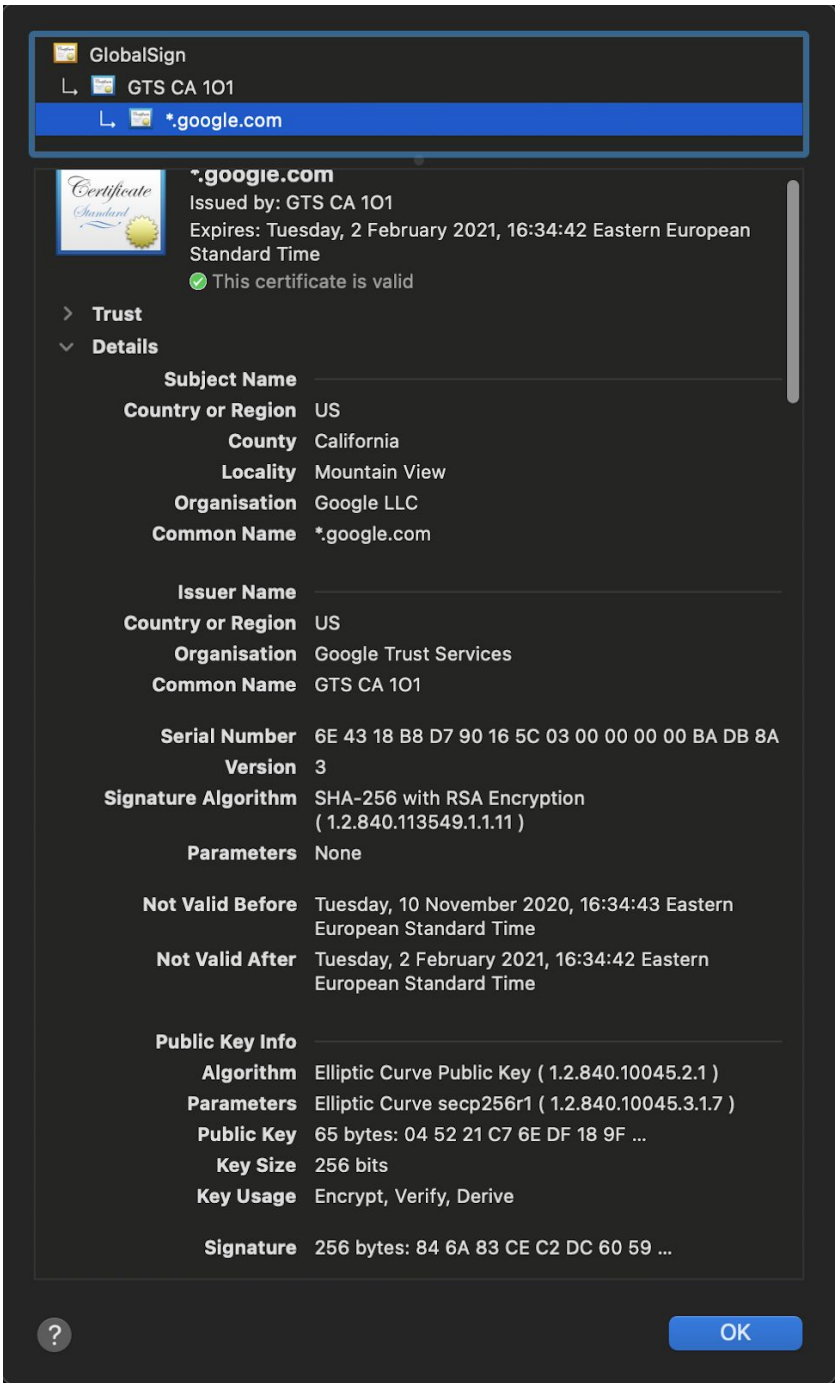
Lab 7 Report

Для вибору алгоритмів генерації ключа було використано сертифікат з сайту youtube.com.



Для генерації пари ключів в ньому використовується алгоритм на основі elliptic curves з використанням кривої secp256r1. Щоб згенерувати ключ з таким алгоритмом використовуємо бібліотеку openssl і команду:

openssl ecparam -genkey -name prime256v1 -out key.pem

Як бачимо, назва кривої тут відрізняється, проте згідно специфікації openssl - “***prime256v1***” це аліас до “secp256r1”. Після генерації ключа генеруємо запит на підпис сертифікату за допомогою команди:

openssl req -new -sha256 -key key.pem -out csr.pem -config csr.config

Файл з конфігураціями виглядає наступним чином:

```
[req]
default_bits=2048
prompt=no
default_md=sha256
distinguished_name=distinguished_name

[distinguished_name]
countryName             = UA
stateOrProvinceName     = Kyiv
organizationName        = KPI
organizationalUnitName  = FICT
commonName              = localhost
emailAddress            = ip72@gmail.com
```

Після створення запиту на підписання сертифікату підписуємо його за допомогою раніше створеного ключа, таким чином отримуємо self-signed certificate:

openssl x509 -req -in csr.pem -signkey key.pem -out crt.pem -days 365 -sha256

Добавляємо наш ключ та сертифікат до серверу написаного на node.js.

```
const https = require('https');
const fs = require('fs');
const path = require('path');

const options = {
    cert: fs.readFileSync(path.join(__dirname, 'certs/crt.pem')),
    key: fs.readFileSync(path.join(__dirname, 'certs/key.pem'))
};

https.createServer(options, requestListener: function (req : IncomingMessage , res : ServerResponse ) {
    res.writeHead( statusCode: 200);
    res.end( chunk: "hello world\n");
}).listen( port: 8000);
```

Після цього запускаємо сервер і відкриваємо сторінку в браузері. Можемо переглянути деталі нашого сертифікату:

Issuer Name	
Country or Region	UA
County	Kyiv
Organisation	KPI
Organisational Unit	FICT
Common Name	localhost
Email Address	ip72@gmail.com
Serial Number	00 8A 59 E8 F7 0E BE D1 DD
Version	1
Signature Algorithm	ECDSA Signature with SHA-256 (1.2.840.10045.4.3.2)
Parameters	None
Subject Name	
Country or Region	UA
County	Kyiv
Organisation	KPI
Organisational Unit	FICT
Common Name	localhost
Email Address	ip72@gmail.com
Not Valid Before	Saturday, 12 December 2020, 01:54:55 Eastern European Standard Time
Not Valid After	Sunday, 12 December 2021, 01:54:55 Eastern European Standard Time
Public Key Info	
Algorithm	Elliptic Curve Public Key (1.2.840.10045.2.1)
Parameters	Elliptic Curve secp256r1 (1.2.840.10045.3.1.7)
Public Key	65 bytes: 04 44 4F B7 21 04 DA 30 ...
Key Size	256 bits
Key Usage	Any
Signature	70 bytes: 30 44 02 20 1E 58 62 E5 ...
Fingerprints	
SHA-256	65 92 6C FE 1F 0A 72 68 BE 00 3E 37 65 66 27 AD CE 16 6F 61 7D 29 C7 70 9B 7B BE 5E 6B 5C 54 0E
SHA-1	9A 1C 5A 52 BB 93 5B 9F C2 15 D2 13 59 97 4A F4 3D 94 B7 FA

Для генерації ключа було використано алгоритм на базі еліптичної кривої, так як він вважається більш надійним для шифрування, ніж базовий алгоритм RSA.

Згенерований сертифікат може знаходитись поруч з кодом серверу, так як це не є секретною інформацією. Для збереження приватного ключа бажано використовувати місця з підвищеним захистом та обмеженим доступом, наприклад спеціальні програми по типу “Keychain” для того, щоб безпечно зберігати приватні ключі та надавати до них доступ тільки авторизованим користувачам чи програмам.