Exercici 1.- Generar les claus (0.5p)

a. Indiqueu les comandes que heu emprat per generar la llavor aleatòria i les claus, indicant el significat de cadascun dels paràmetres que heu fet servir.

openssl rand -base64 -out randFile.txt 512
Explicació d'instruccions llavor:

- openssl: cridem al paquet d'eines OpenSSL.
- rand: genera un numero aleatori utilitzant CSPRNG.
- -base64: codifica la informació seguint la especificació de base64.
- -out randFile: guardem la informació generada al randFile.
- 512: numero de bits o mida que es generen aleatòriament.

openssl genrsa -out ca.key -rand randFile.txt 2048

Explicació d'instruccions clau:

- genrsa: genera una RSA clau Privada.
- -out filename.key: la clau generada s'emmagatzema en filename.key
- -rand randFile.txt: utilitzem la llavor creada anteriorment per a generar els valors aleatoris.
- 2048: numero de bits o mida que es generen aleatòriament.

b. Verifiqueu que la clau generada és correcta emprant l'eina OpenSSL.

Verificació de la clau generada : openssl rsa -in ca.key -check

```
user@gis-2022:~/Desktop/p2/private$ openssl rsa -in ca.key -check
RSA key ok
```

c. Visualitzeu el fitxer de claus que heu generat emprant l'eina OpenSSL i comenteu la informació que es mostra de la clau.

Inicialment tenim aquesta vista del fitxer de claus, que no ens aporta molta informació al estar codificat:

```
user@gis-2022:~/Desktop/P2/private$ cat ca.key
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAuWI/vH7BtwF40Mon1iquTVPxUkLn4WUdgtxynj6leWflNQn9
AYsER4K/kASUKQMkemPOEY4CS0403JlDQ7thQ7h4/F5Q5XhDE+I70fHdZcsKPxg8
+fLtEyEQz1arIQhOLLmRri165YqAqrhvHiw9F7gK65QSu+3ez2JTwaYN1/skpjD9
Oh+S5Cb06zHkuFZ5A7k3wJ2NG+Z4LWb5NnWTTza2nQoiG7XOx+QKQjnY65iQQ6cZ
Pj37yBQiMsb/GuidFPeMJBHL1TwGCMb6j1qG/tGD3wJkCO087B2P7YDFZS+BPVVA
IguSKC5H61acFNSJ/GbYjwVkbuMYE7ygQyACjwIDAQABAoIBAQClznIjLVwlSnM0
l9q5esMa9pFIef7bYYzblkANuQpXY81leuGHl8bkDtU3AmFhrSXbMZkFqnXy1KgD
BjFUI2wDHeNYFSNVmhKknhvS0viqKsenVw5yoAvaqCBY0bONf9gruG3L03GwDAi4
qOz5l6espzddLLr0yvQVmGRBNzv6h2VNNnigMTefKn7I1wv69D9m/Qa1/s+19Ib9
2zc5LbHN2uUGItbZPEpn5WRgba+GwY6M/43mqytJ4cIRIQaArLi7e4bZ2gBUBCP5
dgs3FACwmAXHhKxlQkHmrl3GlL5POgE68e0uN1uBmA4ipWKdDIjSJXWyj2B4/agJ
clv82NiBAoGBAPN57Z9QDoEsiWSTSopOwvVj4xVvHsxsrFQUkljttNWWAefgw5nz
MAbA4zG3+fWZmjvPmoHotOTJ6oJyurqLnNjessT+2h3wQHvUMPnEpDavRnxIziR0
43UFZKcSFaWTa6YXCPbFb9Q6G7fQicD2pnUADxW2UZXBNEvjv04JnKXpAoGBAMLr
XU0dR5NFNw+c0Dy9f9VDZxtsD05ye/Hp7rQcSeZOsN1EA+GD4AN5x5jAHe1dB5DM
u7qhaz4+FFQp+GOUEY0uh0rF5kLiV7WuKnCKSZ5hQRIAKgdsJLkDVh3ognown7Eh
iE/KOlvQ/MwDg+oqhG0buc0nSyanZuNbKfwaU4G3AoGAawv6i4bZObXpGk0gArsq
QFWQa8YVVm+ZPMZmqa6pSRbQ87AAj9k6Dl4UBbILtg24n/9gwSkdD1IvRvdGXeow
JbGUC8S5BVyyHT9n4Qix4lEhvlcMOz8hGjwqysHKvqeYNsf96vFXf4mk0iZfynUn
Ll2+RB+Kszrk0VDqtVbIhrECgYA7REN3ShrUTaxjQ+QRQ/FVkAwOy3mP+cF0GhQp
kZxquayParnfXTDE/cdRy8CNxsahIY9HPQOVxlx6BtTuujvn+KjMdIYB+j5/EHj5
BSNDVADsDz64SQqVcs1BhMv/iT9VJYQD9tJtzoq/IaZ/kfP4FQEWvwbbtvTS1opa
jEqt2wKBgGtdrB5CJEl5W7ElwLxtmP4crEsdWSG1h2qpY6xz45KecByyo4FQDnf+
dVZyQU6rXKoRIGPjwbP7KE/MxPbAkyT7dH9e+3MuFAOP0ReuTEweLO6xKd+4vvhA
yhEVRlXVgyDQtS5nlTq1/YAaqSRwr4xSPlGxbAiMuU+l/tQZn27B
-----END RSA PRIVATE KEY-----
```

Amb l'ajuda de la instrucció pkey podem, extreure més informació :

```
user@gis-2022:~/Desktop/P2/private$ openssl pkey -in ca.key -text -noout
RSA Private-Key: (2048 bit, 2 primes)
modulus:
    00:b9:62:3f:bc:7e:c1:b7:01:78:38:ca:27:d6:2a:
    ae:4d:53:f1:52:42:e7:e1:65:1d:82:dc:72:9e:3e:
    a5:79:67:e5:35:09:fd:01:8b:04:47:82:bf:90:04:
    94:29:03:24:7a:63:ce:11:8e:02:4b:4e:34:dc:99:
    43:3b:bb:61:43:b8:78:fc:5e:50:e5:78:43:13:e2:
    3b:d1:f1:dd:65:cb:0a:3f:18:3c:f9:f2:ed:13:21:
    10:cf:56:ab:21:08:4e:2c:b9:91:ae:2d:7a:e5:8a:
    80:aa:b8:6f:1e:2c:3d:17:b8:0a:eb:94:12:bb:ed:
    de:cf:62:53:c1:a6:0d:d7:fb:24:a6:30:fd:3a:1f:
    92:e4:26:f4:eb:31:e4:b8:56:79:03:b9:37:c0:9d:
    8d:1b:e6:78:2d:66:f9:36:75:93:4f:36:b6:9d:0a:
    22:1b:b5:ce:c7:e4:0a:42:39:d8:eb:98:90:43:a7:
    19:3e:3d:fb:c8:14:22:32:c6:ff:1a:e8:9d:14:f7:
    8c:24:11:cb:d5:3c:06:08:c6:fa:8f:5a:86:fe:d1:
    83:df:02:64:08:ed:3c:ec:1d:8f:ed:80:c5:65:2f:
    81:3d:55:40:22:0b:92:28:2e:47:eb:56:9c:14:d4:
    89:fc:66:d8:8f:05:64:6e:e3:18:13:bc:a0:43:20:
    02:8f
publicExponent: 65537 (0x10001)
privateExponent:
    00:a5:ce:72:23:2d:5c:25:4a:73:34:97:da:b9:7a:
```

Podem observar que tenim una RSA private key de 2048 bits, amb 2 primers. A mes a més, tenim la clau publica, el mòdul, el exponent privat. A la foto no he inclòs els dos primers, dos exponents i un coeficient, tots aquest se'ns donen codificats.

Exercici 2.- Crear un certificat auto-signat (0.5p)

a. Indiqueu les comandes que heu fet servir per generar el certificat, indicant el significat de cadascun dels paràmetres que heu fet servir.

```
user@gis-2022:~/Desktop/P2/private$ openssl req -key ca.key -new -x509 -days 60 -out ca.crt
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:CATALONIA
Locality Name (eg, city) []:BELLATERRA
Organization Name (eg, company) [Internet Widgits Pty Ltd]:UAB
Organizational Unit Name (eg, section) []:.
Common Name (e.g. server FQDN or YOUR name) []:UAB
Email Address []:GIS@UAB.CAT
```

Explicació d'instruccions generació de certificat:

- openssl: cridem al paquet d'eines OpenSSL.
- req: creació del procés per a un certificat.
- -key ca.key: utilitzem la clau creada anteriorment.
- -new: codifica la informació seguint la especificació de base64.
- -x509 randFile: informa a la instrucció req que volem crear un certificat auto-signat.
- -days 60: numero de dies de validesa del certificat.
- -out ca.crt: el certificat generat s'emmagatzema en ca.crt

b. Visualitzeu el certificat que heu generat i comenteu la informació que us mostra l'eina OpenSSL.

Podem veure diferents paràmetres d'informació del certificat: la versió del certificat, el numero de seqüencia que l'identifica, la signatura que té, les dades de validesa que conformen sent aquest 60 dies des de la data de creació. També tenim dades de qui ha creat aquest certificat, les que jo he emplenat en aquest cas. I per últim dades relacionades a la clau publica, quin tipus de encriptació porta aquesta clau pública, quants bits, mòdul ...

```
user@gis-2022:~/Desktop/P2/certs$ openssl x509 -in ca.crt -text -noout
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            77:dc:56:3a:d9:90:b7:24:11:c5:03:e2:85:0a:97:a6:2f:9e:fb:7a
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: C = ES, ST = CATALONIA, L = BELLATERRA, O = UAB, CN = UAB, emailAddress = GIS@UAB.CAT
        Validity
            Not Before: Apr 26 16:02:39 2022 GMT
            Not After : Jun 25 16:02:39 2022 GMT
        Subject: C = ES, ST = CATALONIA, L = BELLATERRA, O = UAB, CN = UAB, emailAddress = GIS@UAB.CAT
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                RSA Public-Key: (2048 bit)
                Modulus:
                    00:b9:62:3f:bc:7e:c1:b7:01:78:38:ca:27:d6:2a:
```

```
                    89:fc:66:d8:8f:05:64:6e:e3:18:13:bc:a0:43:20:
                    02:8f
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                7F:9F:03:5F:48:4C:FF:67:71:64:CB:95:4E:47:16:8C:F6:48:BC:43
            X509v3 Authority Key Identifier:
                keyid:7F:9F:03:5F:48:4C:FF:67:71:64:CB:95:4E:47:16:8C:F6:48:BC:43

            X509v3 Basic Constraints: critical
                CA:TRUE
    Signature Algorithm: sha256WithRSAEncryption
         7e:d8:86:d2:8d:a5:40:c3:d1:c6:72:96:f4:1b:b9:93:27:7b:
```

Exercici 3

a)

-Comandes per generar claus:

*openssl genrsa -out private/client1.key 1024*

*openssl genrsa -out private/client2.key 1024*

-Comandes per crear les peticions de certificat:

*openssl req -new -key private/client1.key -out csr/client1.csr -config openssl.cnf*

*openssl req -new -key private/client2.key -out csr/client2.csr -config openssl.cnf*

El paràmetre –out ens permet especificar on es guardarà el que s'estigui creant, el paràmetre –new ens permet especificar que s'està creant una nova sol·licitud

de certificat, el paràmetre –key ens permet especificar una contrasenya a partir de la qual es generarà la sol·licitud de certificat, els paràmetres private/client1.key o private/client2.key i certs/client1.csr o certs/client3.csr seran les ubicacions on es generaran les claus (en el primer cas) o les sol·licituds de certificat (en el segon cas),el paràmetre 1024 indica que les claus generades tindran un tamany de 1024 bits, el paràmetre –config ens permet especificar la configuració que utilitzarem i el paràmetre openssl.cnf és el fitxer on tenim tots els detalls de la configuració. Si volem canviar algun detall (per exemple a la hora d'executar la comanda ca) podríem canviar certes línees o valors d'aquest fitxer.

b)

Els fitxer client1.csr i client2.csr s'haurien de guardar en la carpeta csr ja que són sol·licitud de certificats i els fitxers client1.key i client2.key s'haurien de guardar en la carpeta private ja que són fitxers de contrasenyes.

c)

Si no se l'hi especifica cap, la funció hash utilitzada que utilitzarà serà la funció SHA-256 (amb encriptació RSA).

d)

Les comandes utilitzades per verificar les sol·licituds de certificat són la següent:

*openssl req -text -in csr/client1.csr -noout -verify*

*openssl req -text -in csr/client2.csr -noout -verify*

Amb aquestes comandes, a part d'obtenir informació de les sol·licitud de certificat, també obtenim un missatge de "verify OK" que ens indica que les verificacions s'han realitzat correctament.

Exercici 4

a)

Comandes utilitzades per signar les sol·licituds de certificat:

*openssl ca -days 365 -in csr/client1.csr -out newcerts/client1.crt -config openssl.cnf*

*openssl ca -days 30 -in csr/client2.csr -out newcerts/client2.crt -config openssl.cnf*

El paràmetre –days ens permet especificar el número de dies que tindrà validesa el certificat creat, el paràmetre –in ens permet especificar quina sol·licitud de certificat serà signada,el paràmetre –out ens indica on es guardarà el certificat creat, el paràmetre –config ens permet especificar la configuració que utilitzarem, el paràmetre openssl.cnf és el fitxer on tenim tots els detalls de la configuració, els paràmetres csr/client1.csr o csr/client2.csr i newcerts/client1.crt o newcerts/client2.crt seran les ubicacions de les sol·licituds de certificat (primers cas) o les ubicacions on es guardaran els certificats creats i el paràmetre 365 o 30 ens especifica el número de dies que tindrà validesa els certificat creat.

PD: Per a realitzar el certificat em canviat certs valors dels paràmetres de l'arxiu openssl.cnf per a que es creí correctament el certificat. Tots el paràmetres countryName, stateOrProvinceName, organitzationName, organitzationalUnitName, commonName i emailAddress, els hi em posat el valor optional i em actualitzar el paràmetre dir amb el directori on estem treballant i on trobem l'arbre de tots el arxius.

b)

En el directori newcerts s'han creat els fitxers client1.crt, 01.pem, client2.crt i 02.pem, en el fitxer index.txt s'han generat dos noves files amb informació dels certificats, en el fitxer serial.txt el número ha augmentat a 03 i per últim s'han creat tres nous fitxers en el directori principal amb els noms index.txt.attr, index.txt.attr.old, index.txt.old i serial.txt.old.

Exercici 5.- Verificar els certificats (1p)

a. Comproveu la validesa dels certificats testX.crt adjunts a aquest enunciat. En cas de no ser vàlids expliqueu que passa.

```
user@gis-2022:~/Documents/Practiques-GIS/P2$ openssl verify -CAfile certs/ca_gis.crt certs/test1.crt
certs/test1.crt: OK
user@gis-2022:~/Documents/Practiques-GIS/P2$ openssl verify -CAfile certs/ca_gis.crt certs/test2.crt
C = ES, ST = BCN, L = Barcelona, O = UAB, OU = DEIC, CN = GIS, emailAddress = test2@uab.cat
error 10 at 0 depth lookup: certificate has expired
error certs/test2.crt: verification failed
user@gis-2022:~/Documents/Practiques-GIS/P2$ openssl verify -CAfile certs/ca_gis.crt certs/test3.crt
C = ES, ST = BCN, L = Barcelona, O = UAB, OU = DEIC, CN = GIS, emailAddress = test3@uab.cat
error 20 at 0 depth lookup: unable to get local issuer certificate
error certs/test3.crt: verification failed
user@gis-2022:~/Documents/Practiques-GIS/P2$ openssl verify -CAfile certs/ca_gis.crt certs/test4.crt
C = ES, ST = BCN, L = Barcelona, O = UAB, OU = DEIC, CN = GIS, emailAddress = test4@uab.cat
error 7 at 0 depth lookup: certificate signature failure
error certs/test4.crt: verification failed
140519960491328:error:04091068:rsa routines:int_rsa_verify:bad signature:../crypto/rsa/rsa_sign.c:220:
140519960491328:error:0D0C5006:asn1 encoding routines:ASN1_item_verify:EVP lib:../crypto/asn1/a_verify.
c:170:
```

Hem procedit a comprovar la validesa amb la instrucció:

openssl verify -CAfile ca_gis.crt testX.crt

Aquesta instrucció verifica el certificat testX.crt comparant amb el certificat ca_gis.crt (aquest ens és donat a els arxius de la pràctica).

La verificació de la validesa del test1.crt, ha sigut tot un èxit.

La verificació de la validesa del test2.crt, no ha tingut èxit, com podem veure el certificat ja no es vàlid, la seva dada de validesa esta caducada.

La verificació de la validesa del test3.crt, no ha tingut èxit. El problema el tenim al test3.crt, quant intentem verificar la cadena de certificat d'aquets la cadena no esta completa.

La verificació de la validesa del test4.crt, no ha tingut èxit. OpenSSL ens informa que tenim un error amb la signatura. Tenim més informació dels errors específics al error d'aquesta signatura. Primerament, un error al rsa, aquest esta marcat com una mala signatura, després veiem un error al codificar amb asn1 es possible que la signatura estigues codificada amb base64 com he fet al 1r exercici.

Exercici 6

a)

La comanda utilitzada per revocar el certificat ha estat la següent:

*openssl ca -revoke newcerts/client2.crt -config openssl.cnf*

El paràmetre –revoke ens permet especificar que es vol eliminar un certificat, el paràmetre newcerts/client2.crt ens indica el certificat que volem eliminar, el paràmetre –config ens permet especificar la configuració que utilitzarem i el paràmetre openssl.cnf és el fitxer on tenim tots els detalls de la configuració.

b)

Els fitxers que es modifiquen són els fitxers index.txt i serial.txt, ja que aquests contenen informació dels certificats signats i firmats, i al eliminar un d'aquests certificats que ja s'havia signat, el número del fitxer serial.txt disminueix i s'elimina un número de sèrie del fitxer index.txt. A més a més, en el directori newcerts també s'elimina el certificat client2.crt.

7. Llista de certificats revocats (1p)

a)

8. Exportar i importació de certificats i claus associades (1p)

a. Indiqueu les comandes que heu fet servir per exportar certificat i la corresponent clau privada, indicant el significat de cadascun dels paràmetres que heu emprat.

   openssl pkcs12 -export -out client.p12 -inkey private/ca.key -in certs/ca.crt

   Explicació d'instruccions per a exportar certificats i la clau privada:
   - pkcs12: una instrucció que bàsicament empaqueta una clau privada i el seu certificat en format .p12
   - -export: el arxiu empaquetat es crea, en comptes de analitzar-lo.
   - -out client.p12: guarda el fitxer creat en client.p12
   - -inkey private/ca.key: aquesta es la clau privada que s'empaqueta.
   - -in certs/ca.crt: aquest es el certificat que s'empaqueta.

b. Comproveu el contingut del fitxer PKCS12 i mostreu els resultats, tot comentant la informació que ens proporciona OpenSSL.

   openssl pkcs12 -info -in client.p12 -nodes

   La informació més important que se'ns proporciona es la visualització de el certificat i de la clau privada tot i que codificat. També tenim paràmetres d'interès, per una banda paràmetres del fitxer i de la seva forma de

codificació en aquest cas PKCS7. Del certificat podem veure dades de interès, com: la empresa que el signa, des de on es signa, el seu contacte de email...

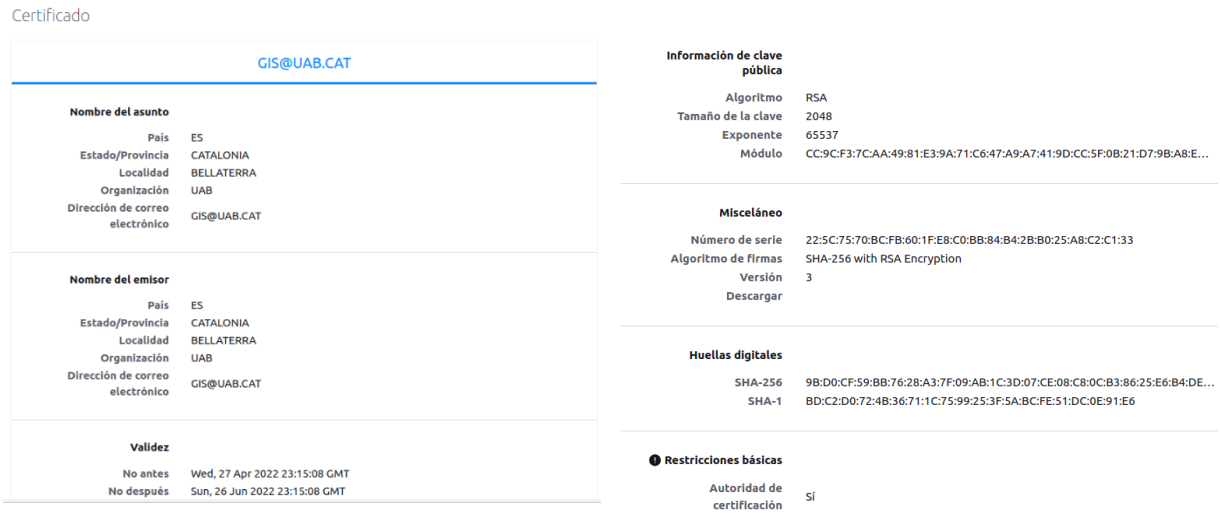
```
user@gis-2022:~/Documents/Practiques-GIS/P2$ openssl pkcs12 -info -in client.p12
Enter Import Password:
MAC: sha1, Iteration 2048
MAC length: 20, salt length: 8
PKCS7 Encrypted data: pbeWithSHA1And40BitRC2-CBC, Iteration 2048
Certificate bag
Bag Attributes
    localKeyID: BD C2 D0 72 4B 36 71 1C 75 99 25 3F 5A BC FE 51 DC 0E 91 E6
subject=C = ES, ST = CATALONIA, L = BELLATERRA, O = UAB, emailAddress = GIS@UAB.CAT

issuer=C = ES, ST = CATALONIA, L = BELLATERRA, O = UAB, emailAddress = GIS@UAB.CAT

-----BEGIN CERTIFICATE-----
MIIDoTCCAomgAwIBAgIUIlx1cLz7YB/owLuEtCuwJajCwTMwDQYJKoZIhvcNAQEL
BQAwYDELMAkGA1UEBhMCRVMxEjAQBgNVBAgMCUNBVEFMT05JQTETMBEGA1UEBwwK
QkVMTEFURVJSQTEMMAoGA1UECgwDVUFCMRowGAYJKoZIhvcNAQkBFgtHSVNAVUFC
LkNBVDAeFw0yMjA0MjcyMzE1MDhaFw0yMjA2MjYyMzE1MDhaMGAxCzAJBgNVBAYT
AkVTMRIwEAYDVQQIDAlDQVRBTE90SUExEzARBgNVBAcMCkJFTExBVEVSUkExDDAK
BgNVBAoMA1VBQjEaMBgGCSqGSIb3DQEJARYLR0lTQFVBQi5DQVQwggEiMA0GCSqG
SIb3DQEBAQUAA4IBDwAwggEKAoIBAQDMnPN8qkmB45pxxkepp0GdzF8LIdebqOtc
TS33APus0hNpOA7vqc5a/Z3xvRH58ZM35gQAA6gn5oOxdZz0Wuh5FCzpqDefv6Ug
oYuweeizQeHqbvV5yHNZlSvBvA6VyHJuQiZqI2HEVYy338v3S5xiwGldXnA4ZGdt
MLjjbTGNcbGcA5w9gHl/4ts/4E6vITDvqcmow+SSTA2oL+N0Fh5pNWkA7mtNr3DB
w00y3XjRORiMcztCe26od43bNR1s6W6ITtMYRAUAEDDmo1l0gcD8xKR1+oJt2w8A
2S+WUI9g3vmKexz8RYsgDIJWK7q5Zo8F9Cf+55kM4OsU597hK7SVAgMBAAGjUzBR
MB0GA1UdDgQWBBSv54vqCqw7bWlXMU19CqrEIPHnLzAfBgNVHSMEGDAWgBSv54vq
Cqw7bWlXMU19CqrEIPHnLzAPBgNVHRMBAf8EBTADAQH/MA0GCSqGSIb3DQEBCwUA
A4IBAQCJ95FOY3uDZ4ZohIHTkjn4jeMMng/uVd0jbdIx7fXeDugxMf7Xqj79ytt3
MYJF3GUUcJ+lxs4KYH65lSR88Rfc/pb0xVzWn+MWAYAWpMif1yn/S4KJfat/js1X
lnTUkPY0yfeqEaAv4LASUDbNOmoGUNmKw097E2tXa9mNf2qe+jyA4cpYVRz4I/Cv
5WvG/JOsm0fykuXr3VFNn0CqYRgLjuer32P/3WYJTa3VMTkghBictjaUvdlBIEpa
FZcSH62C+xhq9jZQLr5YTxSZyN/tmVY/IazMZahSs4tz3oaPNAX79tUENLS3exon
ZMz3ahIWjy2kCuQ71WslolCmNq84
-----END CERTIFICATE-----
PKCS7 Data
Shrouded Keybag: pbeWithSHA1And3-KeyTripleDES-CBC, Iteration 2048
Bag Attributes
    localKeyID: BD C2 D0 72 4B 36 71 1C 75 99 25 3F 5A BC FE 51 DC 0E 91 E6
Key Attributes: <No Attributes>
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFHDBOBgkqhkiG9w0BBQ0wQTApBgkqhkiG9w0BBQwwHAQIXHE5I5UpsAgCAggA
```

```
ZMz3ahIWjy2kCuQ71WslolCmNq84
-----END CERTIFICATE-----
PKCS7 Data
Shrouded Keybag: pbeWithSHA1And3-KeyTripleDES-CBC, Iteration 2048
Bag Attributes
    localKeyID: BD C2 D0 72 4B 36 71 1C 75 99 25 3F 5A BC FE 51 DC 0E 91 E6
Key Attributes: <No Attributes>
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIFHDBOBgkqhkiG9w0BBQ0wQTApBgkqhkiG9w0BBQwwHAQIXHE5I5UpsAgCAggA
MAwGCCqGSIb3DQIJBQAwFAYIKoZIhvcNAwcECDrWe9puasMxBIIEyKMVuPlUJd+x
9DjDBexRVHXL8BE8aNRG+YLuXkImugddv2RyZOvwCS3DRZ3m+mVYs5PO9XuluNFP
jXvfMkSXUlcd8d9vbzR81IQi/v26ElqhmJWt3R4lg9kZx4cF9mBm08tewpwd8qSR
lc5KLPOFnKxTeq5fnKlQXyokSQymZ9fVjObHRnFh13a38uHRklkYeGSBTHvlxM0R
7tKyMhhBjDLGaA5+Em1dTzGR8NwUDU5xnaq7XUCOmiZJMYLqo4UgleRgRtKG7GrU
4RtKZhvFDP6BJR7LSueg6FoF3BCOsIfq9MrtBiRIrMeLl977i+5Z9ENxiF8+6twb
QbTyOmLdW1LtNut1l7YOX5fJPcOECpnvHGH9E9j636qZ+rGlJpEs3Pl+x9booz28
do46kWbWyvLupdL/scVMqARpgVJ5JM/nH2oJflOtBhmDr6938Hd+a07EEvirn2oy
0tVswsPifp526EOxuzG0AWUrloJkHwvZq3qtIoq5EQbJTMrvav0nsPHp65EdgrUh
DgrGIsoMy9vsNSsHC5jkKkOWFUdbXpIAWn2rGg3fOG2eFnHbvK04dvrI7NNNtQL0
OByp6n00Son4bx+NS0oH+gF7nhi5+2D7cSTRcVAd4spHIlZDMulWJ8eHgaQSqh4r
QQbt6q9vtTeWwwSuOTg3THKe5tOFLtaJ7jY+vPNTBojGt7Qw4YiVPKe5Z0o0Xmbk
0ZYSw3xgF0SbMzSvb0lW4pV+CgM2ry7XLtdHSanpmnXg6j7Ikyat1GySTpShRXy/
hmS3Z1N9jObo30jH0vlsuWYUqiEc+LwA68KGMZi75BdO1ZCl8NuoY9uA/cu32GFI
O8QyDPYa9IS9HEybq2Dxz3y2K7TYSqrSh6AU9BCKn5cme1zR+yHe0HyjUwCmi3gG
n48LrlS6ulybaWwLAM2PgmXC8RcPUXoiUBNq9ZOzwc3TjW+PHqyC3O87YBkvOKa
GKhkxxi13tPmTYVsh8bc0F9Xc9mNURGjWP22gNcdTBvy7JYjBv9iuauTAzA302jG
/N3BgNDuYuPSvc7R2j78CoYEZEr2RX8iCnjsyatxLhEGh3psnY+lb21j4tqMlTaf
IJvJqFLCI78oIqgQT6KPDaoHYGtrGeePA8g5xpXlvZyf4j948h3wj+QFWDGtyTJl
AJJg226bfAKBFP6kwIrxR3ckQ3NUHF+jQb87LBiVK5kvmI8zavxwv9q8gDKZdOed
N6WRAwpMkQ8CKMG5zfLtCZIwMXpz6Xf31WSSELDj020AHusrtoyItM+PUrhYGAsY
T0TQx+S7Re37dZZEYH+lf05hjdYKg4tScTzWiTjyGOe+nO2ZrSeMVUx0MPRDeoKC
aVQjan78pB6Mt2PiHxmZ2fARz3eakySa9rBsrwT1iq0prwEpKa5iMHSO6UcyAlhM
2UxjEBG4N3wTC8AUCouyIHhl6HwBxYa1u+T5ky2npC2qlzfVApIjS/Ft5Nyn7gKc
cKiLtiEBnI3L6VFLL/BVysggoiahPzZKunjnFS9oBFvcOTqneJPrlPzPWyvtZG7j
JwtEN48I3zvodqlph3gK83U15htcnijdrCpKhdVVmDx8MbQZV+OYnXEiXENVrbPi
f58dacrUkm2Dvw4HL0S7Qw==
-----END ENCRYPTED PRIVATE KEY-----
```

c. <u>Indiqueu els passos que heu fet per importat el fitxer p12.</u>
He importat el fitxer .p12 al navegador web firefox.
<u>Instruccions per importar:</u>

1. Obrir Firefox
2. Anar als 3 puntets verticals, dreta a dalt.
3. Entrar a ajustes.
4. Seleccionem Privacitat i Seguretat.
5. A l'apartat Seguretat, clicar en el apartat ver certificats.
6. En l'apartat seus certificats, clicar importat.
7. Seleccionar el fitxer .p12, i ja estaria.

d. <u>Mostreu una captura de pantalla amb la informació que us mostra del certificat, explicant els principals camps i la informació que contenen.</u>



Al certificat podem veure diferents camps importants: nom del emissor on tenim informació referent als creadors del certificat, validesa on tenim la durada del certificat, informació clau pública on tenim quin tipus de codificació s'utilitza a aquesta, empremtes digitals on es pot veure un valor que assegura que el fitxer no ha sigut modificat ...

9. Crear i instal·lar el certificat digital (2p)

   a. Indiqueu els passos que heu dut a terme per crear el certificat de la CA i el certificat del servidor web.
   b. Indiqueu els passos que heu seguit per a configurar el certificat en el servidor web Apache.
   c. Mostreu una captura de pantalla que mostri que el servidor web Apache està responen en el port 443 (HTTPS).
   d. Mostreu una captura de pantalla del navegador web on es vegi el detall del certificat. Mostra algun avís o error el navegador web? En cas afirmatiu, indiqueu l'error, la causa i una possible solució al problema.