1. SGSSI-20.Lab07.18.JDOR (S.9.3)

Práctica de SSL y algunas funciones relacionadas con el cifrado, los certificados y la firma digital

1. Tecnologías utilizadas

Linux MX, v.1.1.1

2. Actividad 1

Verificación de las firmas de los compañeros Nº 7, 8 y 9

(El compañero Nº 7 no subio el documento Coplas.txt fimado por lo que no se puede verificar)

```
DarthDorron@tux:~/Desktop/SGSSI/S.9
$ openssl dgst -c -verify SGSSI-20.UBERClavePublica.pem -signature SGSSI-20.UBERCoplas.txt.sig Coplas.txt
Verified OK
DarthDorron@tux:~/Desktop/SGSSI/S.9
$ openssl dgst -c -verify SGSSI-20.AHERClavePublica.pem -signature Coplas.txt.sig Coplas.txt
Verified OK
```

Cifrado de mensajes (el segundo ha sido un error mio)

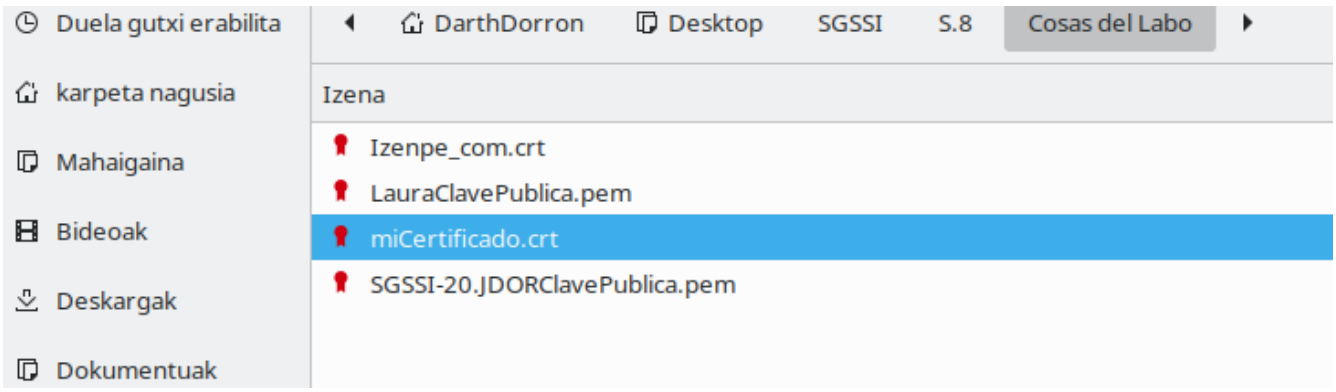
```
DarthDorron@tux:~/Desktop/SGSSI/S.9
$ openssl rsautl -encrypt -in MensajeCifrado.txt -out Mensajecifrado8AHER.enc -inkey SGSSI-20.AHERClavePublica.pe
m -pubin
DarthDorron@tux:~/Desktop/SGSSI/S.9
$ openssl rsautl -encrypt -in MensajeCifrado.txt -out Mensajecifrado9AHER.enc -inkey SGSSI-20.AHERClavePublica.pe
m -pubin
DarthDorron@tux:~/Desktop/SGSSI/S.9
$ openssl rsautl -encrypt -in MensajeCifrado.txt -out Mensajecifrado9UBER.enc -inkey SGSSI-20.UBERClavePublica.pe
m -pubin
DarthDorron@tux:~/Desktop/SGSSI/S.9
$ openssl rsautl -encrypt -in MensajeCifrado.txt -out Mensajecifrado7IARA.enc -inkey SGSSI-20.IARAClavePublica.pe
m -pubin
```

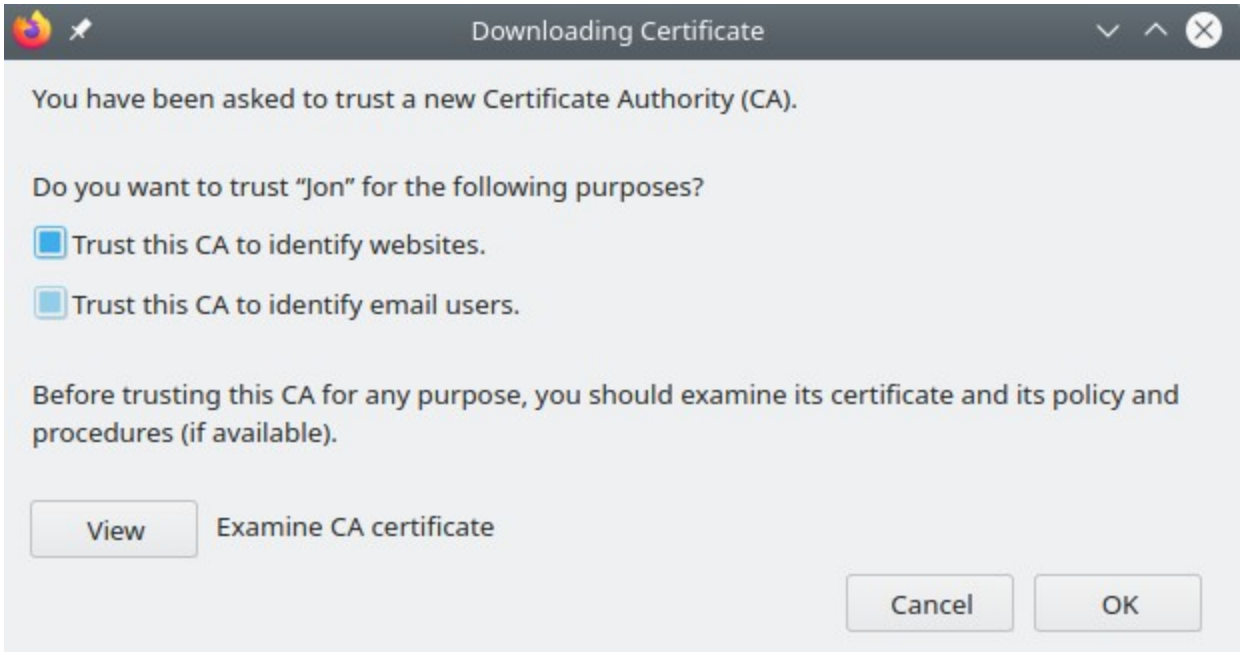
3. Actividad 2

Actividad 2.1

Exportat el certificado de IZENPE

Importar certificado autogenerado





Comparación de los dos certificados:

Para empezar resalta que el cifrado usado por IZENPE sea de 4096, el doble del nuestro. Tambien le añade más seriedad que el de Izenpe ofrezca una dirección fisica e incluso un CIF. Ademas el de Izenpe tiene estos tres (las de la imajen) campos más:

El lo demás son bastante parecidos los dos certificados.

Actividad 2.2

```
DarthDorron@tux:~/Desktop/SGSSI/S.8/Cosas del Labo
$ openssl x509 -req -days 365 -in server.csr -signkey miClavePrivadaCifrada.key -out miCertificado2.crt
Signature ok
subject=C = EH, ST = Gipuzkoa, L = Donostia, O = EHU, OU = Unibertsitatea, CN = Jon, emailAddress = jdorronsoro005@ikasle.ehu.eus
Getting Private key
Enter pass phrase for miClavePrivadaCifrada.key:
DarthDorron@tux:~/Desktop/SGSSI/S.8/Cosas del Labo
$ openssl x509 -req -days 365 -in server.csr -signkey miClavePrivadaCifrada.key -out miCertificado3.crt
Signature ok
subject=C = EH, ST = Gipuzkoa, L = Donostia, O = EHU, OU = Unibertsitatea, CN = Jon, emailAddress = jdorronsoro005@ikasle.ehu.eus
Getting Private key
Enter pass phrase for miClavePrivadaCifrada.key:
DarthDorron@tux:~/Desktop/SGSSI/S.8/Cosas del Labo
$ openssl x509 -req -days 365 -in server.csr -signkey miClavePrivadaCifrada.key -out miCertificado4.crt
Signature ok
subject=C = EH, ST = Gipuzkoa, L = Donostia, O = EHU, OU = Unibertsitatea, CN = Jon, emailAddress = jdorronsoro005@ikasle.ehu.eus
Getting Private key
Enter pass phrase for miClavePrivadaCifrada.key:
```