

1. SGSSI-20.PlantillaLaboratorio08.18.JDOR

1. Tecnologías y plataformas utilizadas


Linux MX, OpenSSL 1.1.1, gnoMint

3. Actividad 2




Extraer del .pfx la clave privada y el certificado:

```
DarthDorron@tux:~/Desktop/SGSSI/S.10
$ openssl pkcs12 -in SGSSI-20.CertificadoEjemplo.pfx -nocerts -out pribatuZifratua.key
Enter Import Password:
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
DarthDorron@tux:~/Desktop/SGSSI/S.10
$ openssl pkcs12 -in SGSSI-20.CertificadoEjemplo.pfx -clcerts -nokeys -out certificate.crt
Enter Import Password:
DarthDorron@tux:~/Desktop/SGSSI/S.10
$ openssl rsa -in pribatuZifratua.key -out pribatua.key
Enter pass phrase for pribatuZifratua.key:
writing RSA key
```

Despues de crear al emisor de las firmas digitales:

Subject		Serial	Activation	Expiration
Certificates				
JDM		01	11/13/2020 08:48 GMT	01/13/2026 08:48 GM

Despues de crear las firmas digitales:

Certificates				
JDM				
		01	11/13/2020 08:48 GMT	01/13/2026 08:48 GM
Ikasle1		02	11/13/2020 08:50 GMT	01/13/2026 08:50 GM
Ikasle2		03	11/13/2020 08:51 GMT	01/13/2026 08:51 GM

Aqui el enlace al documento pfx generado (contraseña **SGSSI-20**):

<https://cryptpad.fr/file/#/2/file/zWbOfU-cXy+V0yNy+PV9xzUq/>

Ejemplo del emisor:

This certificate has been verified for the following uses:	
Certification Authority	
Certificate signing	
CRL signing	
Certificate subject	
Common Name (CN)	JDM
Organization (O)	EHU
Organizational Unit (OU)	EHU
Serial number	01
Emmited by	
Common Name (CN)	JDM
Organization (O)	EHU
Organizational Unit (OU)	EHU

Ejemplo de una de las firmas:

General	Details
This certificate has been verified for the following uses:	
Digital signature	
Key encipherment	
Data encipherment	
Key agreement	
Certificate subject	
Common Name (CN)	Ikasle1
Organization (O)	EHU
Organizational Unit (OU)	EHU
Serial number	02
Emmited by	
Common Name (CN)	JDM
Organization (O)	EHU
Organizational Unit (OU)	EHU

4. Actividad 3

[sólo si da tiempo a abordar la actividad 3 por haber realizado la 2 previamente]