Comandos de OpenSSL

Algunos ejemplos de comandos de openSSL utilizados en varias actividades de la facturación electrónica.

Convertir certificado en formato PEM

```
openssl x509 -inform DER -outform PEM -in nombreArchivo.cer -pubkey -out
nombreArchivo.pem
```

Convertir certificado PEM a formato DER

```
openssl x509 -outform der -in nombreArchivo.pem -out nombreArchivo.der
```

Crear llave en formato PEM

```
openssl pkcs8 -inform DER -in nombreLlave.key -passin pass:12345678a -out
nombreLlave.pem
```

Encriptar en DES3 la llave del certificado de sello digital

```
openssl rsa -in key.pem -des3 -out key.enc -passout pass:"Finkok Password"
```

Desencriptar la llave del paso anterior

```
openssl rsa -in nombredelArchivoEncriptado -out nombreNuevoArchivo.pem
```

posteriormente se le pedirá que ingrese la contraseña que utilizo para encriptar la llave.

Crear Sello digital CFDI 3.2

```
openssl dgst -sha1 -out sign.bin -sign nombreLlave.pem cadenaoriginal.txt
openssl enc -in sign.bin -a -A -out sello.txt
```

Crear Sello digital CFDI 3.3

```
openssl dgst -sha256 -out sign.bin -sign nombreLlave.pem cadenaoriginal.txt
openssl enc -in sign.bin -a -A -out sello.txt
```

Obtener Numero de serie del certificado

```
openssl x509 -inform DER -in C:\aad990814bp7_1210261233s.cer -noout -serial >
"C:\numero.txt"
```

Aplicamos un ciclo para extraer solo las posiciones pares del resultado obtenido.

Verificar que el certificado y la llave sean correctos

Para esto primero tienes que tener la llave y el certificado en formato PEM

```
openssl x509 -noout -modulus -in cer.pem
openssl rsa -noout -modulus -in key.pem
```

Si ambas cadenas son iguales significa que la llave pertenece a ese certificado.

Verificar el periodo de validez de un certificado

Para ejecutar este comando se debe de tener el certificado en formato PEM

```
openssl x509 -noout -in certificado.pem -dates
```

Al ejecuta ese comando se obtiene una respuesta como esta:

```
notBefore=Oct 26 19:22:43 2012 GMT
notAfter=Oct 26 19:22:43 2016 GMT
```

Mostrar RFC del propietario del certificado

Para ejecutar este comando se debe de tener el certificado en formato PEM

```
openssl x509 -in cert.pem -noout -subject -nameopt RFC2253
```

Al ejecuta ese comando se obtiene una respuesta como esta:

```
subject= OU=Servidor,serialNumber=\ /
HEGT761003MDFRNN09,x500UniqueIdentifier=AAD990814BP7 /
HEGT7610034S2,O=ASOCIACION DE AGRICULTORES DEL DISTRITO DE RIEGO 004 DON
MARTIN\ ,name=ASOCIACION DE AGRICULTORES DEL DISTRITO DE RIEGO 004 DON MARTIN
COAHUILA Y NUEVO LEON AC,CN=ASOCIACION DE AGRICULTORES DEL DISTRITO DE RIEGO
004 DON MARTIN\
```

Saber si el certificado pertenece a una FIEL o a un CSD

Para ejecutar este comando se realiza lo siguiente

```
openssl x509 -inform DER -in certificadoPublico.cer -subject -noout
```

Al ejecuta ese comando se obtiene una respuesta como esta en caso de ser FIEL:

```
subject= /CN=ASOCIACION DE AGRICULTORES DEL DISTRITO DE RIEGO 004 DON MARTIN
/name=ASOCIACION DE AGRICULTORES DEL DISTRITO DE RIEGO 004 DON MARTIN COAHUILA
Y NUEVO LEON AC/O=ASOCIACION DE AGRICULTORES DEL DISTRITO DE RIEGO 004 DON
MARTIN /C=MX/x500UniqueIdentifier=AAD990814BP7 / HEGT7610034S2/serialNumber= /
HEGT761003MDFRNN09
```

Si es un CSD la respuesta sera como la siguiente:

```
subject= /CN=ASOCIACION DE AGRICULTORES DEL DISTRITO DE RIEGO 004 DON MARTIN
/name=ASOCIACION DE AGRICULTORES DEL DISTRITO DE RIEGO 004 DON MARTIN COAHUILA
Y NUEVO LEON AC/O=ASOCIACION DE AGRICULTORES DEL DISTRITO DE RIEGO 004 DON
MARTIN /x500UniqueIdentifier=AAD990814BP7 / HEGT7610034S2/serialNumber= /
HEGT761003MDFRNN09/OU=Servidor
```

Como se puede observar el subject perteneciente a una FIEL no contiene el siguiente atributo **OU=Servidor** al final de la cadena, en cambio el perteneciente a un CSD si lo contiene, esta es la diferencia con la cual podemos saber si es un certificado de tipo FIEL o CSD.