SESION 7 1ER PARICAL

FIRMAS Y CERTIFICADOS DIGITALES

Al finalizar la sesión el alumno realizara firmas y certificados digitales x509 y DSA

Consideraciones teóricas: los certificados digitales apoyan a la administración de la seguridad informática a la cooficialidad. integridad. autenticación de mensajes, no repudio. Imprentado las siguientes acciones: Control de acceso, cifrar, descifrar, seguridad física, mecanismos de anonimato, auditoria y supervisión continua, monitoreo de actividades, demostración de la persona que genero la acción, solo la persona que firma puede reproducir sus acciones.

Una firma digital es el conjunto de procesos y técnicas de algoritmos criptográficos los cuales son emitidos po CA (Entidad certificadora) y llaves públicas y privadas.

Un estándar x509 define un formato de los certificados de clave publica sobre SSL/TLS con firmas digitales y cifrado. Los datos base son:

Para estado de ludan (localidad), organización, giro o ramo de la empresa o persona moral, dirección electrónica

DSA es otro estándar Algoritmo de Firma Digital estándar de gobierno Federal de USA o FIPS, algoritmo asimétrico (Ambas direcciones envía y recibe). Genera claves por medio de números primos, verificando por permutaciones

Desarrollo 1. Genere un Certificado x509 identificando y comentando sus procesos en cada uno de los comandos

Microsoft Windows [Versión 10.0.19045.3930]

(c) Microsoft Corporation. Todos los derechos reservados.

C:\OpenSSL-Win64\bin\certificados\x509>OpenSSL genrsa1024 > privatekey.pem

Invalid command 'genrsa1024'; type "help" for a list.

C:\OpenSSL-Win64\bin\certificados\x509>OpenSSL genrsa 1024 > privatekey.pem

C:\OpenSSL-Win64\bin\certificados\x509>dir

El volumen de la unidad C no tiene etiqueta.

El número de serie del volumen es: 3A17-36D2

Directorio de C:\OpenSSL-Win64\bin\certificados\x509

13/02/2024 10:09 a. m. <DIR> .

13/02/2024 10:09 a. m. <DIR> ..

13/02/2024 10:10 a. m. 932 privatekey.pem

1 archivos 932 bytes

2 dirs 45,935,390,720 bytes libres

C:\OpenSSL-Win64\bin\certificados\x509>OpenSSl req -new -key privatekey.pem -out csr.pem

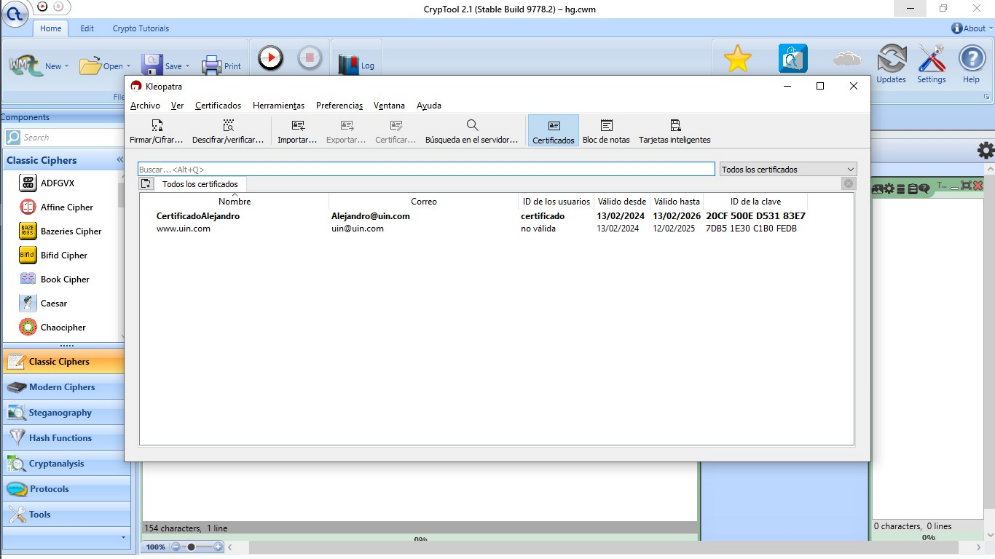
Can't load ./.rnd into RNG

5C360000:error:12000079:random number generator:RAND\_load\_file:Cannot open file:crypto\rand\randfile.c:106:Filename=./.rnd

You are about to be asked to enter information that will be incorporated

into your certificate request.

Desarrollo 2. Descargue e instale GPG y genere un certificado



Conclusión la generación claves de seguridad en 2 formas cleopatra y modo consola, el modo consola es más fácil ya que son 2 líneas de comando y con tener los archivos en la carpeta se puede hacer, en cambio en cleopatra tiene su ventaja de que es más intuitivo y fácil de usar

