Instituto Politécnico Nacional

Unidad Profesional Interdisciplinaria en Ingeniería y Tecnologías Avanzadas

Seguridad de Redes

Profesor. Polanco Montelongo Francisco Antonio

Alumno: Hernández Guzmán Bryan Alexis

Grupo: 3TV4

Práctica: Certificado Digital, firmar documento y validarlo

Introducción:

El Certificado Digital es el único medio que permite garantizar técnica y legalmente la identidad de una persona en Internet. Se trata de un requisito indispensable para que las instituciones puedan ofrecer servicios seguros a través de Internet. Además:

El certificado digital permite la firma electrónica de documentos El receptor de un documento firmado puede tener la seguridad de que éste es el original y no ha sido manipulado y el autor de la firma electrónica no podrá negar la autoría de esta firma.

El certificado digital permite cifrar las comunicaciones. Solamente el destinatario de la información podrá acceder al contenido de esta.

En definitiva, la principal ventaja es que disponer de un certificado le ahorrará tiempo y dinero al realizar trámites administrativos en Internet, a cualquier hora y desde cualquier lugar.

Un Certificado Digital consta de una pareja de claves criptográficas, una pública y una privada, creadas con un algoritmo matemático, de forma que aquello que se cifra con una de las claves sólo se puede descifrar con su clave pareja.

El titular del certificado debe mantener bajo su poder la clave privada, ya que si ésta es sustraída, el sustractor podría suplantar la identidad del titular en la red. En este caso el titular debe revocar el certificado lo antes posible, igual que se anula una tarjeta de crédito sustraída.

La clave pública forma parte de lo que se denomina Certificado Digital en sí, que es un documento digital que contiene la clave pública junto con los datos del titular, todo ello firmado electrónicamente por una Autoridad de Certificación, que es una tercera entidad de confianza que asegura que la clave pública se corresponde con los datos del titular.

Descripción:

OpenSSL es una herramienta de código abierto que contiene un conjunto de funciones muy útiles para la criptografía aplicada. OpenSSL implementa los protocolos más conocidos y utilizados en computación, por lo que ofrece un amplio rango de alternativas útiles para programar. Se podría definir como un toolkit indispensable para programadores, ya que reúne los algoritmos clave para forjar sistemas criptográficos de seguridad y certificados digitales SSL/TLS.

Procedimiento:

Primeramente creamos una clave privada a extensión será .pem para después generar la solicitud de certificado a la entidad de certificación, nos pedirá datos para tener un certificado y una identidad más específica.

```
bryan@bryan-VirtualBox:~$ openssl req -new -key privatekey.pem -out csr.pem
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]:MX
State or Province Name (full name) [Some-State]:Mexico
Locality Name (eg, city) []:Izcalli
Organization Name (eg, company) [Internet Widgits Pty Ltd]:IPN
Organizational Unit Name (eg, section) []:UPIITA
Common Name (e.g. server FQDN or YOUR name) []:Bryan
Email Address []:bryanhdrz98@gmail.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:hola123
An optional company name []:IPN
```

Procederemos a firmar nuestro certificado:

```
bryan@bryan-VirtualBox:~$ openssl x509 -req -days 365 -in csr.pem -signkey privatekey.pem -out public.crt
Certificate request self-signature ok
subject=C = MX, ST = Mexico, L = Izcalli, O = IPN, OU = UPIITA, CN = Bryan, emailAddress = bryanhdrz98@gmail.com
```

Para después firmar nuestro documento utilizando la clave privada que creamos al principio:

```
bryan@bryan-VirtualBox:~$ openssl dgst -sha256 -sign privatekey.pem -out nuevo.txt.signature nuevo.txt
```

Procedemos a extraer nuestra clave publica de la privada:

```
bryan@bryan-VirtualBox:~$ openssl rsa -in privatekey.pem -outform PEM -pubout -out publickey.pem
writing RSA key
```

Por último, verificamos la firma:

```
bryan@bryan-VirtualBox:~$ openssl dgst -sha256 -verify publickey.pem -signature nuevo.txt.signature nuevo.txt
Verified OK
```

Conclusión:

Este concepto de las claves publicas y privada es nuevo para mí, yo en un principio llegué a pensar que eran cosas que se utilizaban cada una para diferentes tipos de cifrado, sin embargo ahora se puede entender que trabajan a la par, realmente se puede apreciar la importancias de estas cuando puedes conocer que se utilizan en todos lados y para todo, el ejemplo antes realizado nos pudo mostrar de mejor manera como es que trabajan, realmente cuál es su funcionamiento y para qué son.

Referencias:

https://learn.bybit.com/es/blockchain/what-is-public-keys-and-private-keys-in-cryptography-and-how-it-works/

https://www.upv.es/contenidos/CD/info/711545normalc.html