uc3m | Universidad Carlos III de Madrid

PRÁCTICA: Firma Digital y PKI. OpenSSL

CURSO CRIPTOGRAFÍA Y SEGURIDAD INFORMÁTICA

Ana I. González-Tablas Ferreres
José María de Fuentes García-Romero de Tejada
Lorena González Manzano
Pablo Martín González
UC3M | GRUPO COMPUTER SECURITY LAB (COSEC)

HERRAMIENTAS

OpenSSL es un paquete criptográfico disponible en Linux, por ejemplo en Ubuntu. Preste atención a los cambios que se van produciendo en el directorio en el que se ejecutan los comandos indicados.

OPENSSL. Disponible en el aula (Linux), información para Windows: https://wiki.openssl.org/index.php/Binaries

- En Windows, para poder ejecutarlo desde cualquier ruta del sistema debe incluir la carpeta bin de OpenSSL dentro de la variable de entorno PATH. Utilice el comando: set PATH=%PATH%;"PATH DONDE INSTALE OPENSSL"/bin

INTRODUCCIÓN

La práctica se estructura en 4 partes: 1) Creación de una PKI, 2) Firma digital, 3) Obtención de un certificado digital a través de una web, 4) Obtención del certificado digital de la Fábrica Nacional de Moneda y Timbre (Opcional)

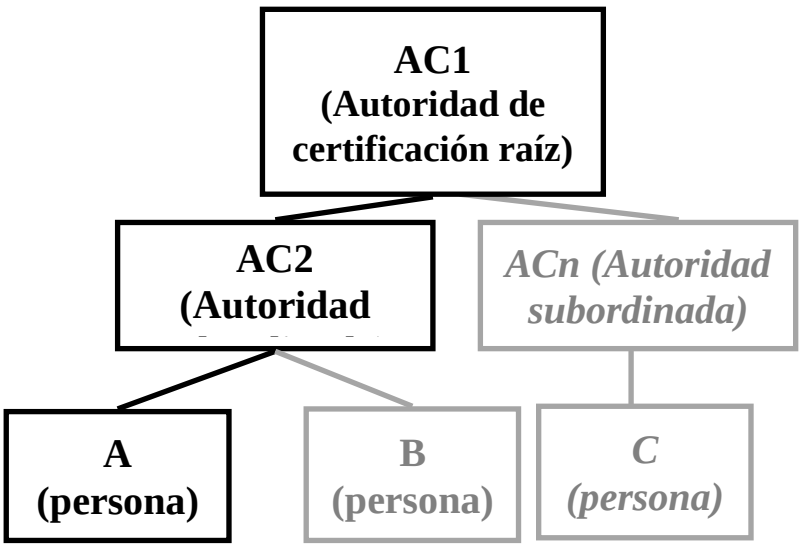
El objetivo de esta práctica es comprender los **fundamentos** sobre los que se basan las **infraestructuras de clave pública**. Particularmente, los objetivos concretos son los siguientes:

1. Comprender los pasos necesarios para que una Autoridad emita un certificado.
2. Entender qué papel juegan los certificados en la firma y verificación de documentos.

Para alcanzar estos objetivos, en esta práctica cada grupo de alumnos se convierte en una AUTORIDAD DE CERTIFICACIÓN RAÍZ (como puede ser en el mundo real, la Fábrica Nacional de Moneda y Timbre). Dicha Autoridad (AC1), por cuestiones organizativas (por ejemplo, para tener una delegación en cada comunidad autónoma) tiene varias AUTORIDADES DE CERTIFICACIÓN

SUBORDINADAS (AC2,…, ACn), las cuales se dedican a emitir certificados de clave pública a las personas (A, B, C).

El conjunto de todas estas Autoridades conforma una INFRAESTRUCTURA DE CLAVE PÚBLICA (en inglés, PKI).



Para limitar la carga de trabajo, en esta práctica sólo se gestionará la autoridad raíz (AC1), una única autoridad subordinada (AC2) y una persona (A).

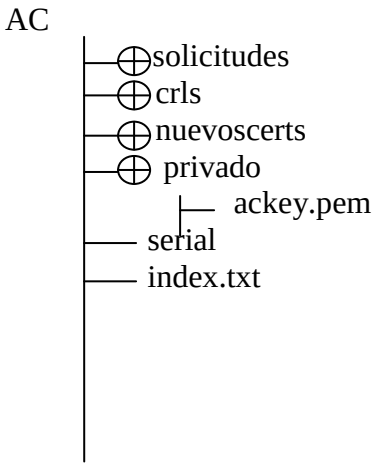
Para organizar el desarrollo de la práctica, cree tres carpetas, una cada para entidad: AC1, AC2 y A.

```
# practica> mkdir AC1 AC2 A
```

Para emitir los certificados, las Autoridades utilizan una POLÍTICA de certificación. Copie los ficheros que contienen estas políticas openssl_AC1.cnf y openssl_AC2.cnf (disponibles en Aula Global) en el directorio AC1 y AC2 respectivamente. Analice los ficheros openssl_ACx.cnf dados, comparándolos entre sí y con el fichero de configuración por defecto, el cual se encuentra en /etc/ssl/*openssl*.cnf.

Antes de comenzar la práctica, modifique los ficheros de políticas de tal forma que el nombre de sus AC sea AC1-XXXXX y AC2-XXXXX, donde XXXXX son los cinco últimos dígitos de su identificador de alumno en la Universidad.

La estructura de los directorios y archivos quedará en un principio como sigue:



Configuración de AC1 (Autoridad de Certificación raíz)

Los comandos de OpenSSL necesarios para la realización de la práctica son:

- ca: permite crear y gestionar una Autoridad de Certificación basada en el modelo de confianza jerárquico.
- req: permite crear y gestionar peticiones de emisión de certificados X.509.
- x509: permite gestionar certificados X.509.
- verify: permite verificar certificados X.509.

1. Genere la estructura de directorios necesaria para AC1 e inicialice los ficheros serial e index.txt.

   # AC1> mkdir solicitudes crls nuevoscerts privado

   # AC1> echo '01' > serial

   # AC1> touch index.txt

2. Genere un par de claves RSA junto con el certificado autofirmado por AC1. Estudie los cambios producidos en el directorio AC1.

   # AC1> openssl req -x509 -newkey rsa:2048 -days 360 -out ac1cert.pem -outform PEM -config openssl_AC1.cnf

   Se pide un passphrase para crear la clave privada de AC1, que habrá que recordar cuando queramos utilizarla.

   # AC1> openssl x509 -in ac1cert.pem -text -noout

Configuración de AC2 (Autoridad de Certificación subordinada)

3. Genere la estructura de directorios necesaria para AC2 e inicialice los ficheros serial e index.txt.

   # AC2> mkdir solicitudes crls nuevoscerts privado

   # AC2> echo '01' > serial

   # AC2> touch index.txt

4. Genere un par de claves de RSA junto con una solicitud de emisión de certificado y "envíesela" a AC1. Estudie los cambios producidos en el directorio AC2.

AC2> openssl req -newkey rsa:2048 -days 360 -out ac2req.pem -outform PEM -config openssl_AC2.cnf

Al igual que antes en AC1, se pide un passphrase que habrá que recordar cuando se utilice la clave privada de AC2

AC2> openssl req -in ac2req.pem -text -noout

AC2> cp ac2req.pem ../AC1/solicitudes

Generación del certificado de AC2 por AC1

5. Verifique la solicitud de emisión de certificado "enviada" por AC2.

AC1> openssl req -in ./solicitudes/ac2req.pem -text -noout

6. Genere el certificado de AC2 y "envíeselo" (en el proceso, cambie el nombre del nuevo certificado - actualmente 01.pem - a ac2cert.pem, ya que AC2 tiene configurado en su fichero de configuración este último nombre). Estudie los cambios producidos en el directorio AC1.

   # AC1> openssl ca -in ./solicitudes/ac2req.pem -notext -extensions v3_subca -config openssl_AC1.cnf

   AC1 utiliza su clave privada para crear el certificado de AC2, por lo que se pide el passphrase de AC1.

   # AC1> cp ./nuevoscerts/01.pem ../AC2/ac2cert.pem

Generación de las claves de A y su solicitud de emisión de certificado para AC2

7. Para la entidad A, genere un par de claves de RSA junto con una solicitud de emisión de certificado y "envíeselas" a AC2 (en el proceso de generación de solicitudes de emisión de certificado, rellene todos los campos que se le soliciten e indique que el país es "ES", que la provincia es "MADRID", que la organización es "UC3M", que el nombre común es XXXXX (según lo indicado anteriormente), y que su email es su dirección de correo de estudiante). Estudie los cambios producidos en el directorio A.

   # A> openssl req -newkey rsa:1024 -days 360 -sha1 -keyout Akey.pem -out Areq.pem

Al igual que antes, se pide un passphrase que habrá que recordar cuando se quiera utilizar la clave privada de A.

```
# A> openssl req -in Areq.pem -text -noout
# A> cp Areq.pem ../AC2/solicitudes
```

Generación del certificado de A por AC2

8. Compruebe la solicitud de emisión de certificados "enviada" por A.

   ```
   # AC2> openssl req -in ./solicitudes/Areq.pem -text -noout
   ```

9. Genere el certificado de A y "envíeselo" de vuelta (en el proceso, cambie el nombre del nuevo certificado - actualmente 01.pem - a Acert.pem).

   ```
   # AC2> openssl ca -in ./solicitudes/Areq.pem -notext -config ./openssl_AC2.cnf
   ```

   AC2 utiliza su clave privada para crear el certificado de A, por lo que se pide el passphrase de AC2.

   ```
   # AC2> cp ./nuevoscerts/01.pem ../A/Acert.pem
   ```

10. Estudie los cambios producidos en el directorio AC2 y compruebe el certificado resultante:

    ```
    # A> openssl x509 -in Acert.pem -text -noout
    ```

Verificación del certificado de A

11. Obtenga una copia auténtica de los certificados de clave pública de AC1 y AC2 y verifique el certificado de A (para ello necesitara concatenar los certificados de AC1 y AC2 en un único fichero).

    ```
    # A> cp ../AC1/ac1cert.pem ./
    # A> cp ../AC2/ac2cert.pem ./
    # A> cat ac1cert.pem ac2cert.pem > certs.pem
    # A> openssl verify -CAfile certs.pem Acert.pem
    ```

    Si todo es correcto, marcará un OK al ejecutar el último comando

Uniendo el certificado y la clave privada para firmar en aplicaciones habituales (Word / correo electrónico)

12. Exporte el certificado de A, su clave privada y la concatenación de los certificados de AC1 y AC2 al formato PKCS12.

    # A> openssl pkcs12 -export -in Acert.pem -inkey Akey.pem -certfile certs.pem -out Acert.p12

Se solicita el passphrase de A para exportar su clave privada, y un nuevo passphrase para el certificado .p12

EJERCICIOS

Ejercicio 1 :

a) ¿Para qué se usa el fichero "serial"?

Solución:

Número de serie de los certificados

b) ¿Para qué se usa el fichero "index.txt"?

Solución:

Es la "base de datos" de los certificados

c) ¿Podría AC2 crear su certificado utilizando el paso 2 de este guión?

Solución:

No, porque AC2 no puede autofirmarse porque no es la entidad de certificación raíz

d) Si su grupo de prácticas se convirtiera en una Autoridad de Certificación de verdad, explique razonadamente (i.e. ventajas, inconvenientes, otras alternativas razonables, etc.) qué valor le pondría a cada uno de los siguientes parámetros de su política de certificación: default_days, default_crl_days, countryName

Solución:

default_days = Un valor muy largo es peligroso (compromiso de la clave) pero uno muy corto es impráctico (caduca muy rápido)

default_crl_days = Lo más corto posible

countryName = si ponemos un match, evitamos que nos hagan solicitudes válidas de otros países (lógico para la FNMT, por ejemplo)

Utilización de la clave privada de A para firmar un documento

13. Elabore un documento en Microsoft Word que esté firmado electrónicamente utilizando la clave privada de A. Para ello, será necesario importar previamente el fichero Acert.p12 en el navegador (en Internet Explorer: Herramientas > Opciones de Internet > Contenido > Certificados > Importar… Se pedirá el passphrase del certficado .p12) y posteriormente, utilizando Microsoft Word, utilizar la opción Botón de Office > Preparar > Agregar una firma digital…

Ejercicio 2:

e) Respecto al documento Word creado y firmado, cuando lo abra, verá un "Error de comprobación". ¿Cuál es la causa? ¿Se podría solucionar?

Solución:

No es posible verificar el certificado, ya que las autoridades emisoras no están instaladas en el equipo. Si se instalaran, la validación sería correcta.

La Autoridad Pública de Certificación CERES de la FNMT-RCM

14. Acceda a su página web http://www.cert.fnmt.es/home.
15. Consulte el manual de solicitud de certificado de persona física, accesible en esta direcciónweb: http://www.cert.fnmt.es/documents/10445900/10528353/solicitud_certificado_persona_fisica.pdf
16. Consulte el documento de "Declaración General de Prácticas de Certificación" (https://www.sede.fnmt.gob.es/documents/10445900/10536309/dgpc.pdf).

Ejercicio 3:

f) ¿Qué es CERES, qué tipo de certificados ofrece y cuáles son los servicios que oferta?

g) ¿Cuando se inicia el procedimiento para solicitar un certificado de clave pública de persona física, dónde se generan las claves pública y privada?

Solución:

En el ordenador del usuario, en caso de disponer de HW criptográfico adecuado, en éste, si no es el caso, en el navegador.

h) ¿Puede el usuario elegir el tamaño de las claves que se acreditarán en dicho certificado?

Solución: Sí

i) ¿Para qué sirve la dirección de correo solicitada durante el proceso de generación de la solicitud de dicho certificado?

Solución:

Para recibir el código identificativo de la solicitud de certificado.

j) ¿Qué es necesario presentar en la oficina de registro y con qué propósito una vez se ha solicitado el certificado de clave pública de persona física a través de Internet?

Solución:

"Tras haber obtenido el código de solicitud, deberá personarse en una oficina de registro para acreditar su identidad. Ha de ser el propio solicitante, futuro suscriptor y titular del certificado quien deberá acudir personalmente a una oficina de registro a acreditar su identidad. En el caso de que no pudiera hacerlo por cualquier circunstancia, podrá ir una tercera persona en su nombre pero previa legitimación de la firma ante notario.

Documentación necesaria para una persona física, deberá presentar:

- DNI o tarjeta de residencia (NIE) para los ciudadanos extracomunitarios.
- Los ciudadanos comunitarios que no tengan la tarjeta de residencia, presentaran el "Certificado de Registro de Ciudadanos de la Unión y su Pasaporte"."

k) ¿Qué condiciones se le exigen al usuario para poder descargar correctamente el certificado de clave pública de persona física?

Solución:

"Para descargar el certificado debe usar el mismo ordenador, el mismo navegador y el mismo usuario con el que realizó la Solicitud. Si usted ha extraviado su código de solicitud, deberá solicitar un nuevo código y hacer el proceso de acreditación de nuevo."

l) ¿Se realiza una copia de seguridad de las claves privadas ("Datos de creación de firma") de la Autoridad de Certificación de la FNMT-RCM?

Solución: Sección 9.3.1.2 (página 36 de DGPC.pdf):

"116. Cuando los Datos de creación de Firma se encuentran fuera del dispositivo criptográfico, se encuentran asimismo protegidos por los mecanismos criptográficos necesarios para procurar su Confidencialidad ante ataques basados en criptoanálisis.

117. Las operaciones de copia, salvaguarda o recuperación de los Datos de creación de Firma se realizan bajo control exclusivo del personal autorizado, usando, al menos, control dual y en un entorno seguro.

118. Se mantiene una copia de los ficheros y componentes necesarios para la restauración del entorno de seguridad del dispositivo criptográfico, para el caso de que haya que hacer uso de ellos, en sobres de seguridad debidamente custodiados dentro de un armario ignífugo, que solo pueden ser obtenidos por personal autorizado."

m) ¿Cuáles son los usos previstos de las claves de firma de la Autoridad de Certificación de la FNMT-RCM y qué algoritmos de firma prevé utilizar?

Solución:

"122. Los Datos de creación y de verificación de Firma de la FNMT-RCM en su actividad como Prestador de Servicios de Certificación serán utilizadas única y exclusivamente para los propósitos de:

- Firma de Certificados.
- Firma de las Listas de Revocación.
- Firma de estructuras de datos relativas a la validez de los Certificados
- Firma de Sellos de Tiempo

- Firma de documentos electrónicos distintos de los Certificados previstos en los fines y actividades de la FNMT-RCM, en los supuestos previstos en esta DGPC y en la normativa correspondiente.

123. Los conjuntos de algoritmos y parámetros empleados para la Firma de la FNMT-RCM en su actividad como Prestador de Servicios de Certificación se corresponden, en parte, con las "suites" de firma "sha1-with-rsa" y "sha2-with-rsa" aprobadas en ETSI TS 102 176 "Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures"."

n) ¿Cuántas personas son necesarias para activar las claves de firma de la Autoridad de Certificación de la FNMT-RCM y con qué mecanismo se verifica que dichas personas están autorizadas para activar las claves?

Solución: "9.3.3. Datos de activación de las claves

138. Las claves privadas de las Autoridades de Certificación son generadas y custodiadas por un dispositivo criptográfico que cumple los requisitos de seguridad FIPS PUB 140-2 Level 3.

139. Los mecanismos de activación y uso de las claves privadas de la Autoridad de Certificación se basan en la segmentación de roles de gestión y operación que la FNMT-RCM tiene implementados con mecanismos de acceso multipersona basados en tarjetas criptográficas y sus correspondientes pines en un esquema de uso simultaneo M de N (2 de 5).

140. Los mecanismo de activación y uso de las claves privadas de los certificados de entidad final se basan en pines de acceso a los métodos de generación de claves privadas utilizados por el suscriptor, que en todo caso se mantienen bajo su estricto control y cuya custodia recae bajo su responsabilidad."

o) Los pasos que tiene que seguir un ciudadano para obtener un certificado de clave pública emitido por la Fábrica Nacional de Moneda y Timbre vienen resumidos en la siguiente tabla. Rellene la tabla, que sirve para relacionar cada uno de esos pasos con los realizados en esta práctica: para cada paso de ese proceso, indique en qué punto de esta práctica se ha realizado.

Solución:

Paso	Descripción	Punto de este guión en que se ha realizado
1	Crear un par de claves (pública y privada) y envío de la solicitud de certificado	7
2	Personarse en una oficina de registro	Ninguno
3	Generación del certificado de clave pública de acuerdo a las políticas	8, 9 (primer comando)
4	Descargarse el certificado	9 (segundo comando)

Certificados de servidor Web – visión del cliente

17. Abra una pestaña del navegador y acceda al servicio de Aula Global o Campus Global de la UC3M.

18. Abra otra pestaña del navegador y acceda a la página web principal del buscador Google.

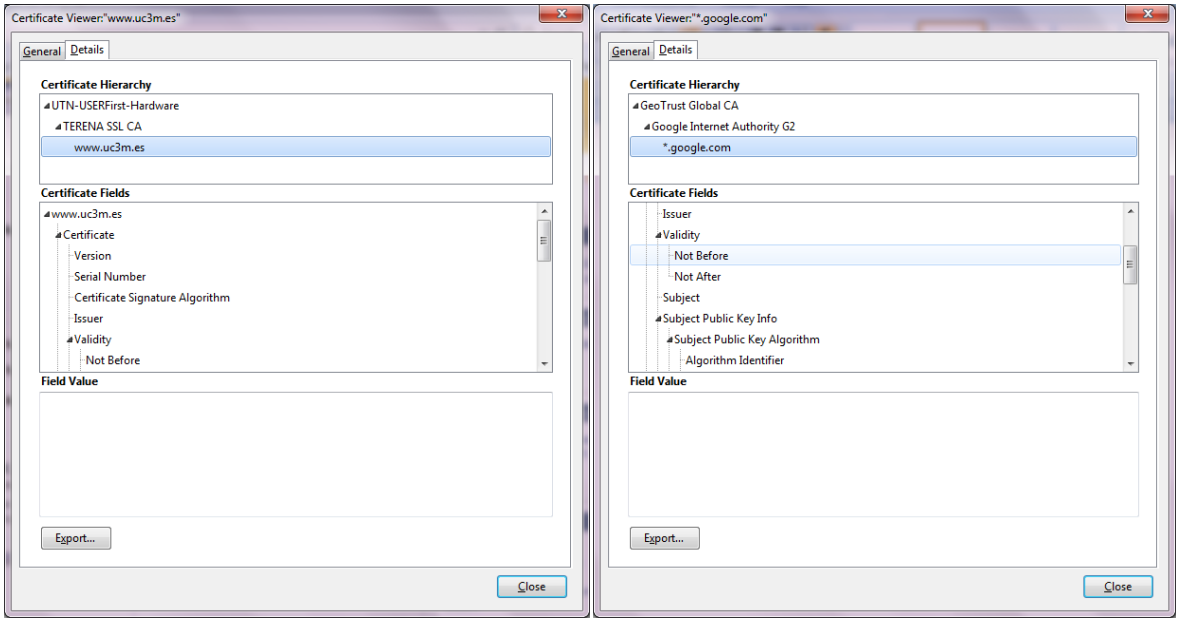
Ejercicio 4:

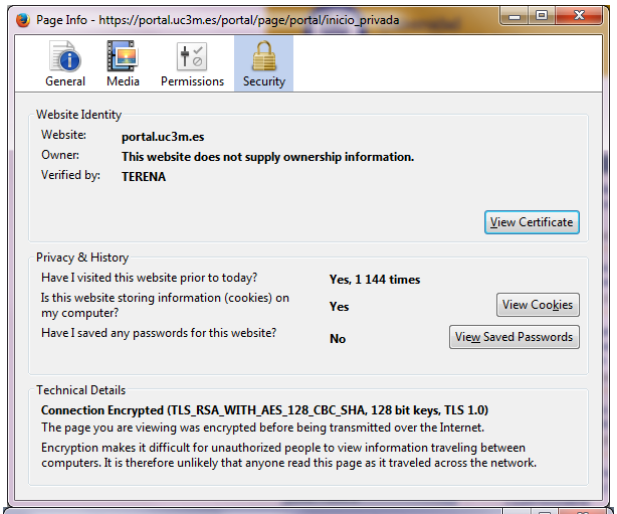
p) Averigüe cuál es el certificado ofrecido para asegurar la conexión con el protocolo TLS por parte de la UC3M. ¿Cuál es la cadena de certificación? ¿Qué algoritmo se está utilizando para negociar la clave, y cifrar y autenticar los datos?

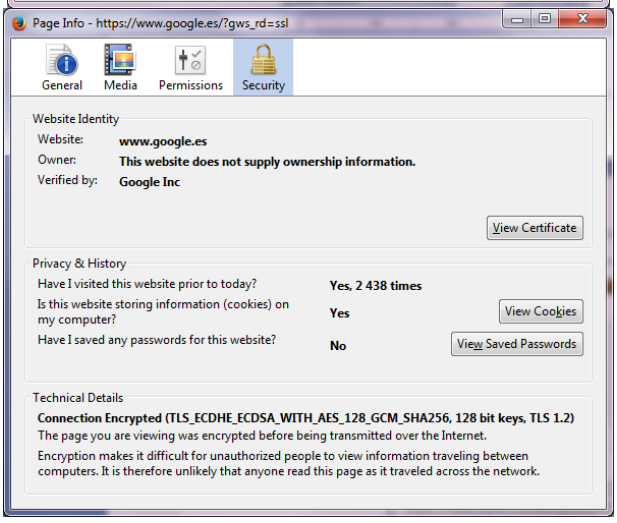
q) Averigüe cuál es el certificado ofrecido para asegurar la conexión con el protocolo TLS por parte de Google. ¿Cuál es la cadena de certificación? ¿Qué algoritmo se está utilizando para negociar la clave, y cifrar y autenticar los datos?

Solución

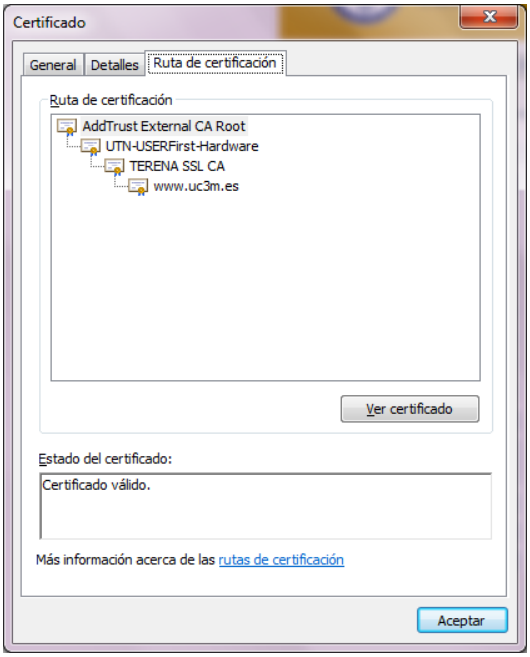
Con Mozilla:

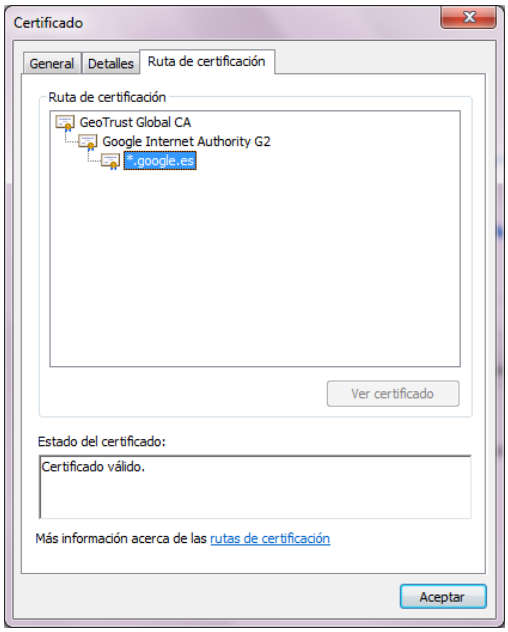


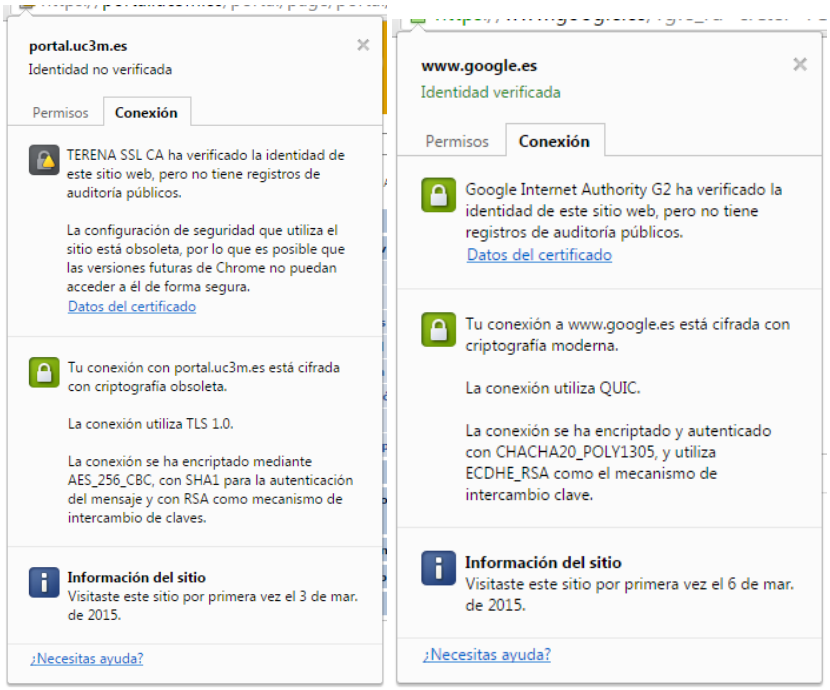

Page Info - https://portal.uc3m.es/portal/page/portal/inicio_privada
General
Media
Permissions
Security
Website Identity
Website: portal.uc3m.es
Owner: This website does not supply ownership information.
Verified by: TERENA
View Certificate
Privacy & History
Have I visited this website prior to today? Yes, 1 144 times
Is this website storing information (cookies) on my computer? Yes
View Cookies
Have I saved any passwords for this website? No
View Saved Passwords
Technical Details
Connection Encrypted (TLS_RSA_WITH_AES_128_CBC_SHA, 128 bit keys, TLS 1.0)
The page you are viewing was encrypted before being transmitted over the Internet.
Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.


Page Info - https://www.google.es/?gws_rd=ssl
General
Media
Permissions
Security
Website Identity
Website: www.google.es
Owner: This website does not supply ownership information.
Verified by: Google Inc
View Certificate
Privacy & History
Have I visited this website prior to today? Yes, 2 438 times
Is this website storing information (cookies) on my computer? Yes
View Cookies
Have I saved any passwords for this website? No
View Saved Passwords
Technical Details
Connection Encrypted (TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, 128 bit keys, TLS 1.2)
The page you are viewing was encrypted before being transmitted over the Internet.
Encryption makes it difficult for unauthorized people to view information traveling between computers. It is therefore unlikely that anyone read this page as it traveled across the network.

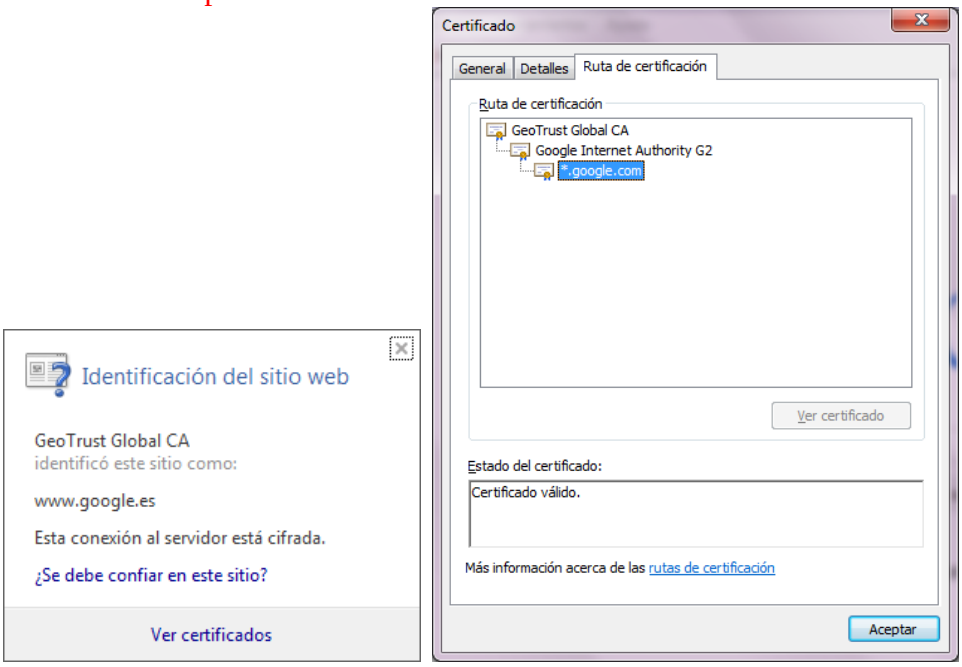
Con Chrome:


Certificado
General
Detalles
Ruta de certificación
Ruta de certificación
AddTrust External CA Root
UTN-USERFirst-Hardware
TERENA SSL CA
www.uc3m.es
Ver certificado
Estado del certificado:
Certificado válido.
Más información acerca de las rutas de certificación
Aceptar


Certificado
General
Detalles
Ruta de certificación
Ruta de certificación
GeoTrust Global CA
Google Internet Authority G2
*.google.es
Ver certificado
Estado del certificado:
Certificado válido.
Más información acerca de las rutas de certificación
Aceptar



Con Internet Explorer:



Certificados de servidor Web – visión del servidor

19. Lea uno de estos dos tutoriales acerca de cómo crear un certificado auto-firmado para servidor web y su instalación en Apache Web Server para ofrecer conexiones cifradas con el protocolo TLS/SSL:
    a) http://www.nanotutoriales.com/como-crear-un-certificado-ssl-de-firma-propia-con-openssl-y-apache-http-server

b) http://linuxconfig.org/apache-web-server-ssl-authentication

20. Abra en otra pestaña del navegador la página web https://letsencrypt.org/ y averigüe qué anuncia. Estudie qué ofrece y cómo funcionaría.

Ejercicio 5:

r) ¿Cuáles serán las ventajas principales de los certificados de servidor emitidos por "Let's Encrypt"?

Solución:

Gratuito, reconocimiento automático por los navegadores, facilidad/transparencia de instalación.

OPCIONAL:

Obtención del certificado de clave pública de la FNMT

La FNMT (Fabrica Nacional de Moneda y Timbre) actúa como Autoridad de Certificación de la Administración Pública del Estado, expidiendo certificados digitales a los ciudadanos que así lo soliciten. Estos certificados pueden ser utilizados por los ciudadanos para identificarse electrónicamente de forma inequívoca ante la Administración Pública, para realizar trámites administrativos como por ejemplo descarga de datos fiscales y presentación de la declaración de la renta, petición de la vida laboral, solicitar la prestación del paro, y un largo etcétera.

Como ejercicio de esta práctica se pide que al menos uno de los alumnos de cada grupo obtenga su certificado digital a través de la FNMT, certificado que luego podrá usar en su vida diaria. Para ello los pasos a realizar son:

1. Introduzca la siguiente URL :

https://www.sede.fnmt.gob.es/certificados/persona-fisica/obtener-certificado-software

2. Siguiendo los pasos que se le indican en la web realice la petición de su certificado. Para ello deberá proporcionar su DNI.
3. Al finalizar el proceso se le proporcionará un código

4. Con dicho código debe personarse en un organismo público acreditado (tesorerías generales de la seguridad social, delegaciones de hacienda, etc), donde identificándose con su DNI y el código del anterior apartado, se le activará su certificado.
5. Por último con el código y su número de DNI, ya estará en disposición de descargarse su certificado.

Ejercicio 5:

s) ¿Qué periodo de validez tiene vuestro certificado?

Solución:

4 años

t) ¿Qué algoritmo de firma utiliza?

Solución:

RSA

u) ¿Qué tamaño tiene la clave?

Solución:

2048 bits

v) ¿Cuál es el identificador de clave de la entidad emisora?

Solución:

b1 d4 4f c4 23 79 fa 44 05 09 c6 eb 39 cf e8 35 b0 b8 20 64

w) Por último ¿Qué periodo de validez tiene el certificado raíz de la FNMT?

Solución:

Hasta el 01/01/2030