Práctica Protocolo HTTPS y Certificados Digitales

**0.1.- Define los siguientes conceptos:**

**a) certificado digital**

Un certificado digital o certificado electrónico es un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad.

**b)** **Autoridad de certificación**

es una entidad de confianza, responsable de emitir y revocar los certificados digitales, utilizados en la firma electrónica, para lo cual se emplea la criptografía de clave pública. Jurídicamente es un caso particular de Prestador de Servicios de Certificación.

**c) Criptografía simétrica**

La criptografía simétrica (SKC symmetric key cryptography), también llamada criptografía de clave secreta (secret key cryptography) o criptografía de una clave (en inglés single-key cryptography), es un método criptográfico en el cual se usa una misma clave para cifrar y descifrar mensajes. Las dos partes que se comunican han de ponerse de acuerdo de antemano sobre la clave a usar. Una vez que ambas partes tienen acceso a esta clave, el remitente cifra un mensaje usando la clave, lo envía al destinatario, y éste lo descifra con la misma clave.

**d) Criptografía Asimétrica**

La criptografía asimétrica (Asymmetric Key Cryptography), también llamada criptografía de clave pública (Public Key Cryptography) o criptografía de dos claves (Two-Key Cryptography), es el método criptográfico que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona que ha enviado el mensaje. Una clave es pública y se puede entregar a cualquier persona, la otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella. Además, los métodos criptográficos garantizan que esa pareja de claves sólo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves.

**e) Comparación entre Criptografía simétrica y asimétrica**

****

**f) SSL → Secure Sockets Layer)**

**Es un protocolo criptográfico que proporciona confidecialidad , autenticidad e integridad en una comunicación cliente/servidor.**

**1. Certificado digital verificado**

1.1. Inicia sesión en Windows7

1.2. Inicia Firefox.

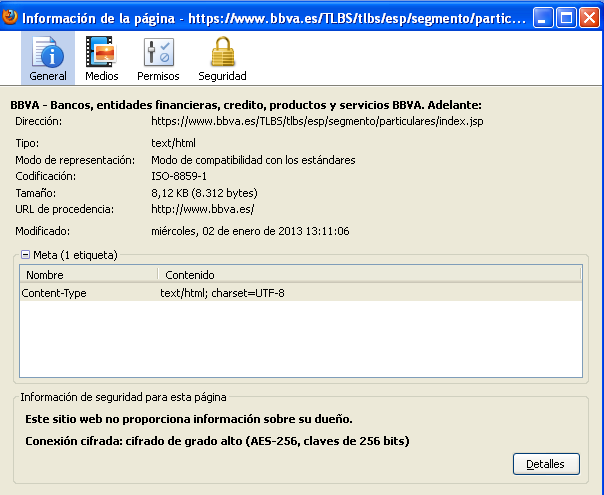
1.3. Conecte a mediante http a la web de cualquier sitio web seguro.

1.4. Observe en la URL que el protocolo usado es https.

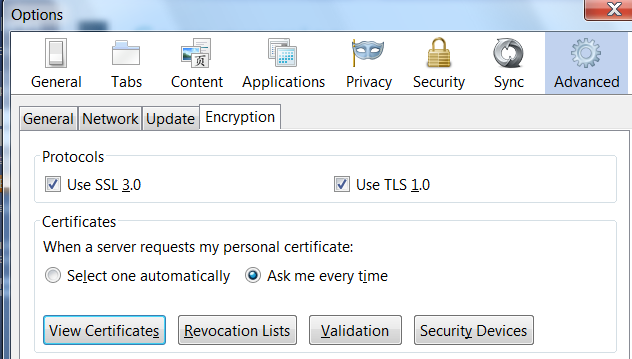
1.5. En la parte izquierda de la URL y haga doble clic.

1.6. Seleccione Mas información para consular el certificado digital que ha enviado el servidor web. También se puede acceder a través de Herramientas => Información de la página.

Responda las siguientes preguntas:



En Windows 2007:



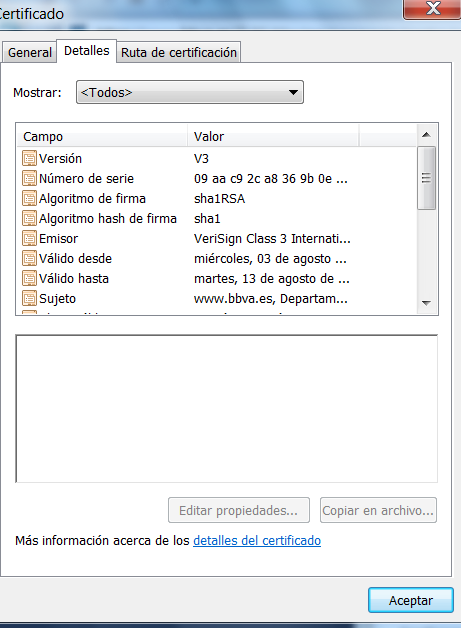


Figura 1: Certificado digital

a ¿Qué algoritmo de clave simétrica se ha utilizado para cifrar la información que viaja por la red?

¿Cuál es la longitud de la clave utilizada?

b ¿Cuál es el periodo de validez del certificado?

No antes 7/11/2018 1:00:00

No después 6/11/2020 13:00:00

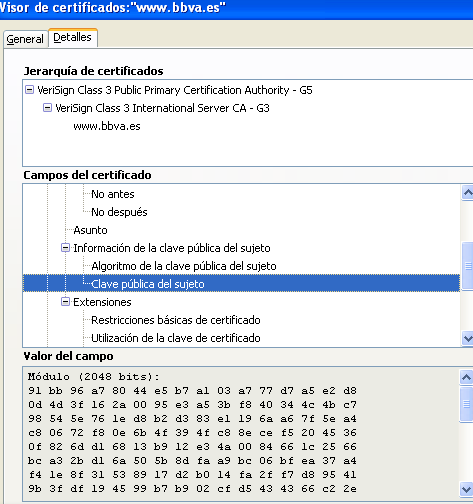
c ¿Qué función resumen (hash) ha utilizado la autoridad de certificación para firmar el certificado?

No

d ¿Qué algoritmo de clave asimétrica ha utilizado la autoridad de certificación para firmar el certificado?

Elliptic Curve

e ¿De qué tamaño es la clave pública del certificado? 256



f ¿Qué autoridad de certificación ha firmado el certificado?

DigiCert Server

¿De quién depende?

1.7. En el menú de Firefox accede a Opciones, Opciones, pestaña Avanzado, Pestaña Cifrado, Ver certificados y busca el certificado de la autoridad certificadora que ha firmado el certificado.

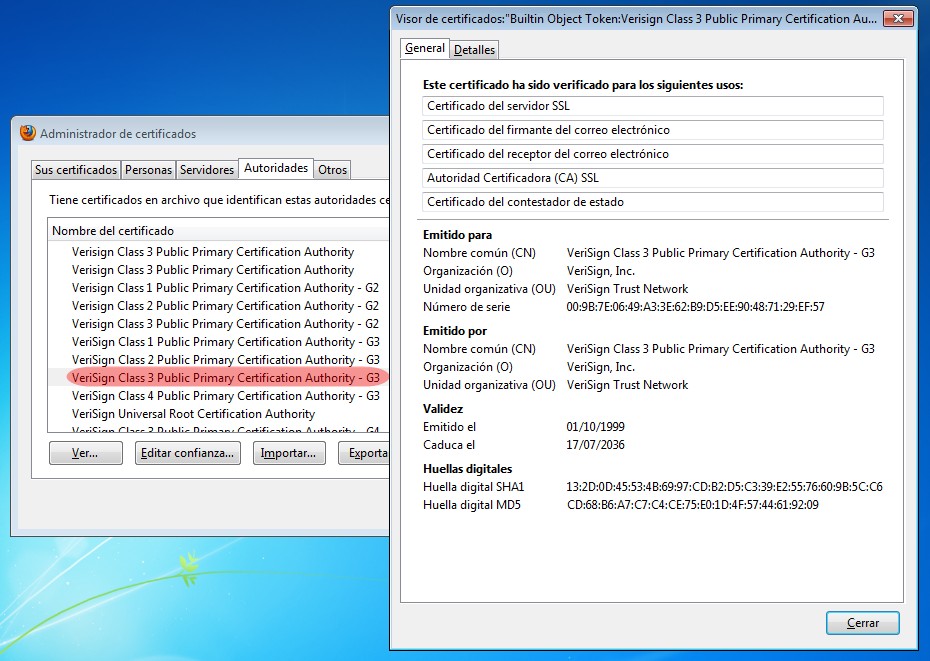
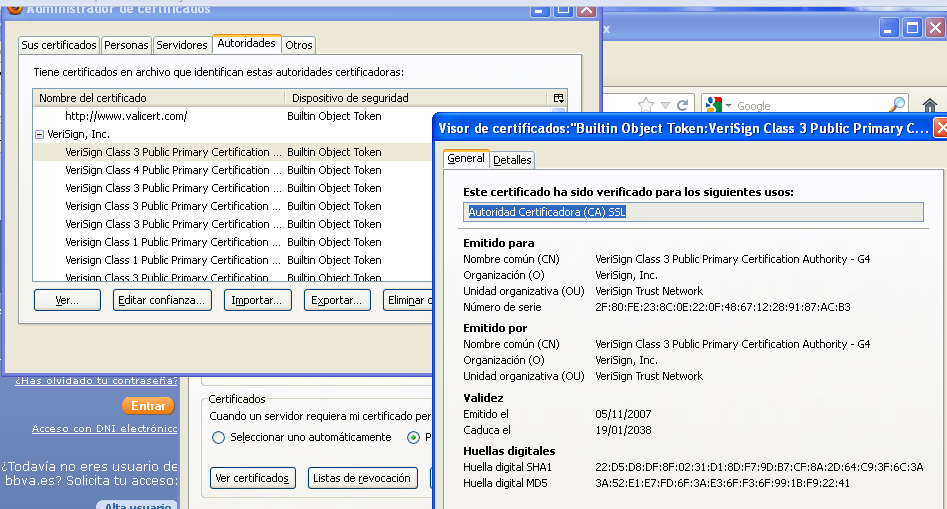


Figura 2: Certificado digital de la autoridad de certificación

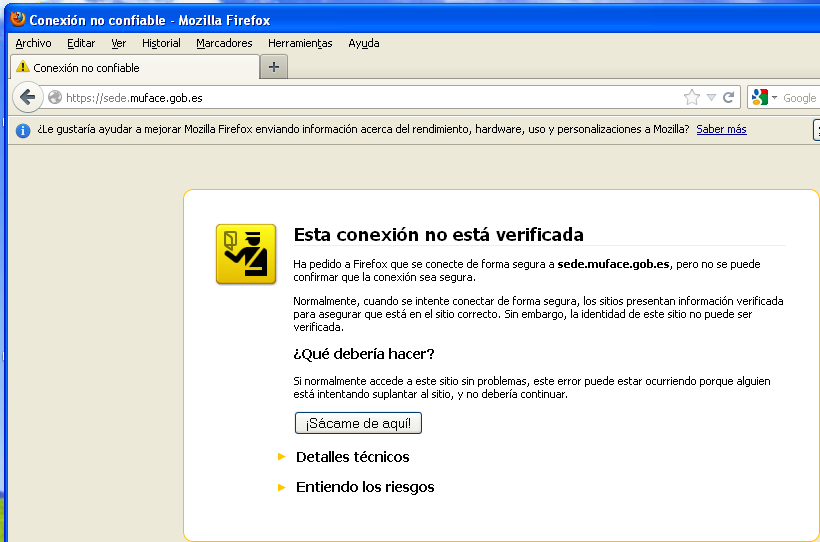


**2. Certificado no verificado**

2.1. Inicia Firefox.

2.2. Conéctate a un sitio web seguro autofirmado.

2.3. El navegador muestra un mensaje de error indicando que no ha podido verificar el certificado que le ha enviado el servidor web.



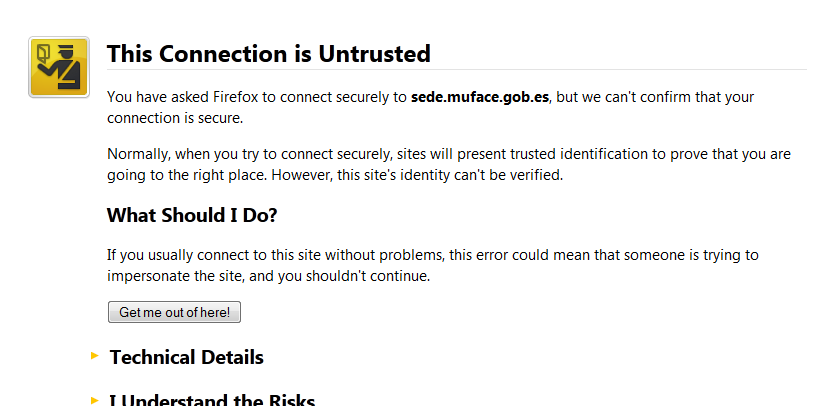
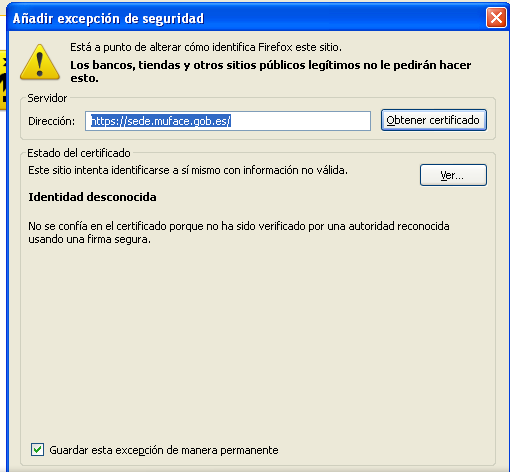


Figura 3: Aviso de certificado digital no verificado

2.4. Selecciona en Entiendo los riesgos.



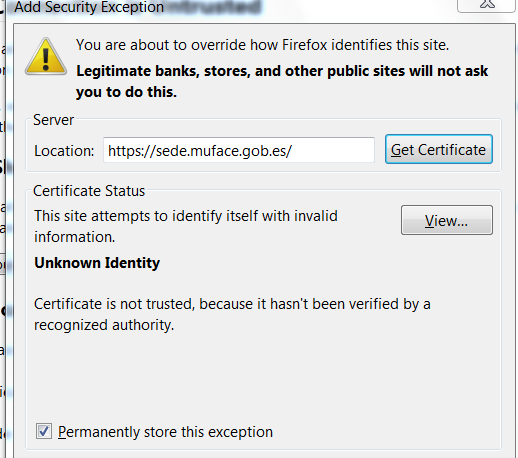
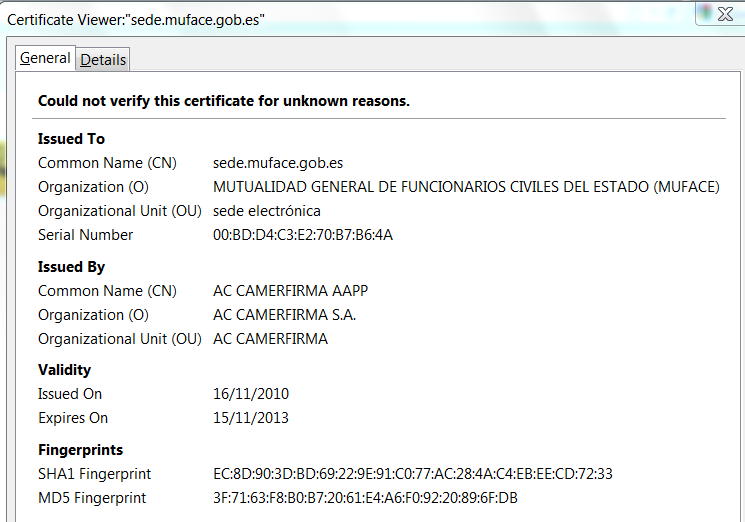


Figura 3b: Añadir excepción

2.5. Añade Excepción, Figura 3b. Observa que está marcada la opción Guardar excepción de forma permanente.



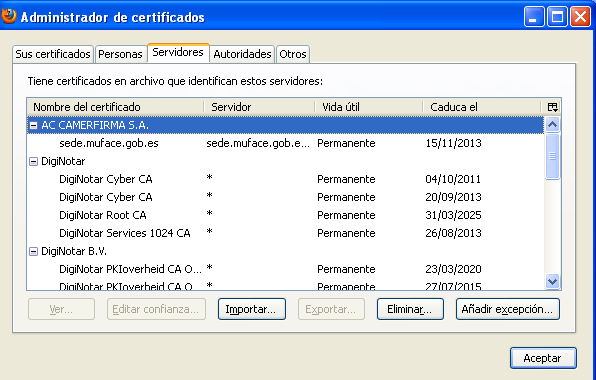


Figura 4: Ver el certificado digital no verificado

2.6. Selecciona Obtener certificado y Ver para mostrar los datos del certificado digital que ha enviado el navegador



2.7. Confirma excepción de seguridad.

2.8. En el menú de Firefox accede a Opciones, Opciones, pestaña Avanzado, Pes taña Cifrado, Ver certificados busca el certificado del servidor que has aceptado y elimínalo.

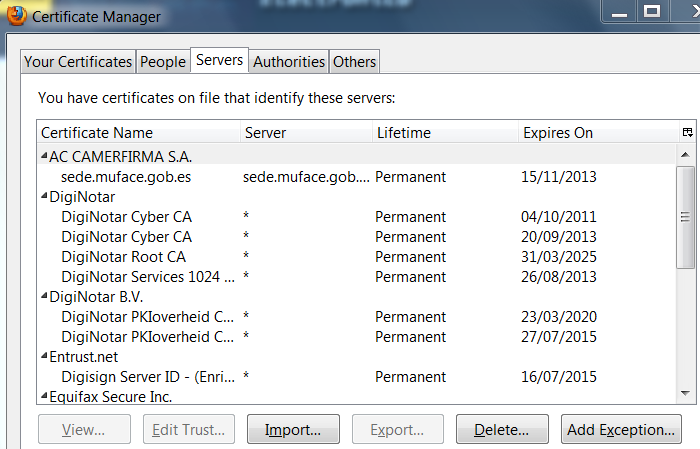


Figura 5: Eliminar certificado del servidor