Práctica Protocolo HTTPS y Certificados Digitales

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

**a) certificado digital**

Un **certificado digital** o **certificado electrónico** es un fichero informático firmado electrónicamente por un prestador de servicios de certificación, considerado por otras entidades como una autoridad para este tipo de contenido, que vincula unos datos de verificación de firma a un firmante, de forma que únicamente puede firmar este firmante, y confirma su identidad. Tiene una estructura de datos que contiene información sobre la entidad (por ejemplo una clave pública, una identidad o un conjunto de privilegios). La firma de la estructura de datos agrupa la información que contiene de forma que no puede ser modificada sin que esta modificación sea detectada.

Normalmente cuando se habla de certificado digital se está hablando de los certificados de clave pública que son un tipo de certificado digital.

**b)** **Autoridad de certificación**

En criptografía, las expresiones **autoridad de certificación**, o **certificadora**, o **certificante**, o las siglas **AC** o **CA** (por la denominación en idioma inglés *Certification Authority*), señalan a una entidad de confianza, responsable de emitir y revocar los certificados, utilizando en ellos la firma electrónica, para lo cual se emplea la criptografía de clave pública. Jurídicamente, se trata de un caso particular de Prestador de Servicios de Certificación. Una autoridad de certificación expide los certificados digitales, que ya contienen las identificaciones numéricas y las contraseñas que se necesitan, poniendo a disposición el procedimiento de verificación para validar el certificado proporcionado.

Los servicios de una autoridad de certificación, son principalmente utilizados para garantizar la seguridad de las comunicaciones digitales vía el protocolo TLS (Transport Layer Security), utilizados en las comunicaciones web (HTTPS) o las comunicaciones de correos electrónicos (SMTP, POP3, IMAP), así como para resguardar documentos digitales (por ejemplo, utilizando firmas electrónicas avanzadas con el sistema PAdES para documentos PDF, o vía el protocolo S/MIME para los correos electrónicos).

**c) Criptografía simétrica**

La **criptografía de clave simétrica** (en inglés *symmetric key cryptography*), también llamada **criptografía de clave secreta** (en inglés *secret key cryptography*) o criptografía de una clave[1](https://es.wikipedia.org/wiki/Criptograf%C3%ADa_sim%C3%A9trica#cite_note-simmons-1)​ (en inglés *single-key cryptography*), es un método criptográfico en el cual se usa una misma clave para cifrar y descifrar mensajes en el emisor y el receptor. 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 este lo descifra con la misma clave.

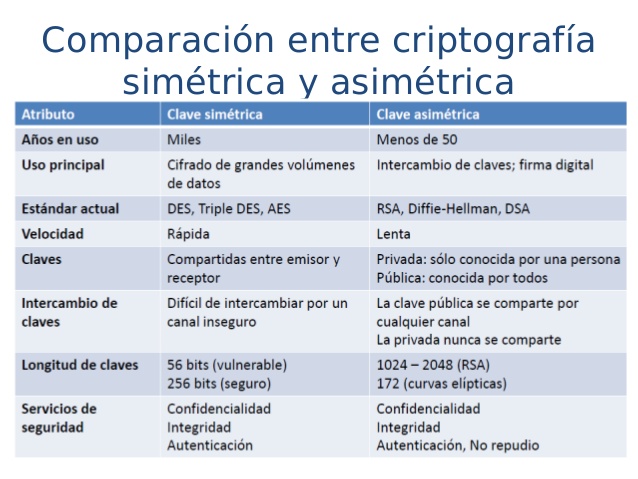
**d) Criptografía Asimétrica**

La **criptografía asimétrica** (en inglés *asymmetric key cryptography*), también llamada **criptografía de clave pública** (en inglés *public key cryptography*) o **criptografía de dos claves**[1](https://es.wikipedia.org/wiki/Criptograf%C3%ADa_asim%C3%A9trica#cite_note-simmons-1)​(en inglés *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 recibirá 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.

**Llave** o **clave** es lo mismo. Existiendo por tanto: **llave** o **clave** privada y **llave** o **clave** pública.

Si una persona que emite un mensaje a un destinatario, usa la llave pública de este último para cifrarlo; una vez cifrado, sólo la clave privada del destinatario podrá descifrar el mensaje, ya que es el único que debería conocerla. Por tanto se logra la *confidencialidad* del envío del mensaje, *es extremadamente difícil que lo descifre alguien salvo el destinatario* . Cualquiera, usando la llave pública del destinatario, puede cifrarle mensajes; los que serán descifrados por el destinatario usando su clave privada.

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



**f) SSL**

El SSL (Security Socket Layer) y el TLS (Transport Layer Security) son los protocolos de seguridad de uso común que establecen un canal seguro entre dos ordenadores conectados a través de Internet o de una red interna. En nuestra vida cotidiana, tan dependiente de Internet, solemos comprobar que las conexiones entre un navegador web y un servidor web realizadas a través de una conexión de Internet no segura emplean tecnología SSL.

Técnicamente, el protocolo SSL es un método transparente para establecer una sesión segura que requiere una mínima intervención por parte del usuario final. Por ejemplo, el navegador alerta al usuario de la presencia de un certificado SSL cuando se muestra un candado o cuando la barra de dirección aparece en verde cuando se trata de un certificado [EV SSL](https://www.globalsign.com/es/ssl/ev-ssl/) con validación ampliada. En este hecho reside el éxito del protocolo SSL: es una experiencia sorprendentemente sencilla para los usuarios finales.

**1. Certificado digital verificado**

1.1. Inicia sesión en Windows7

1.2. Inicia Firefox.

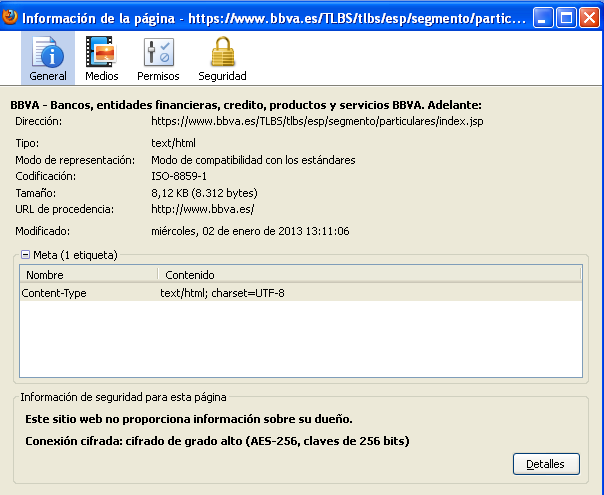
1.3. Conecte a mediante http a la web de cualquier sitio web seguro.

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

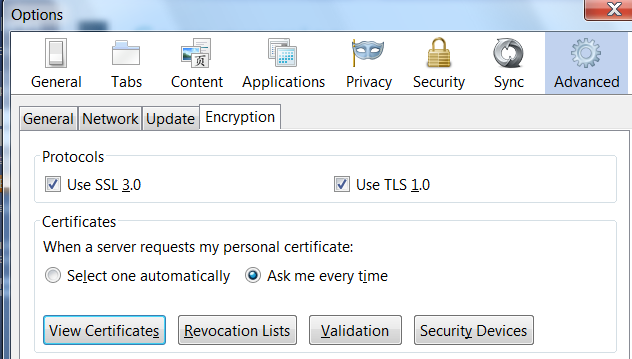
1.5. En la parte izquierda de la URL y haga doble clic.

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:



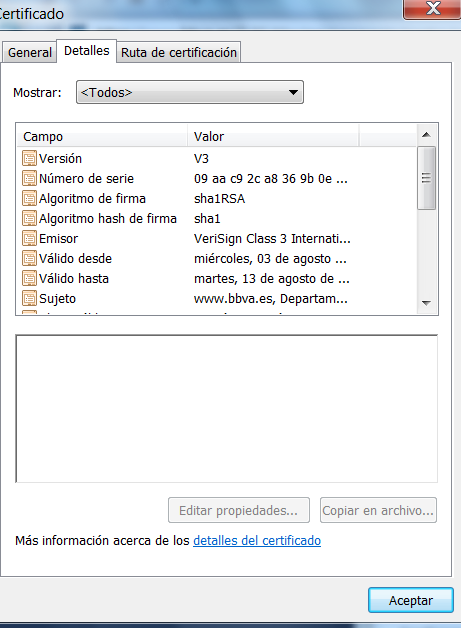
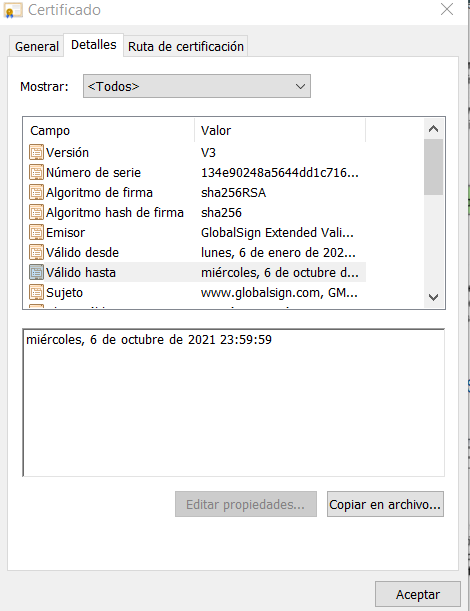
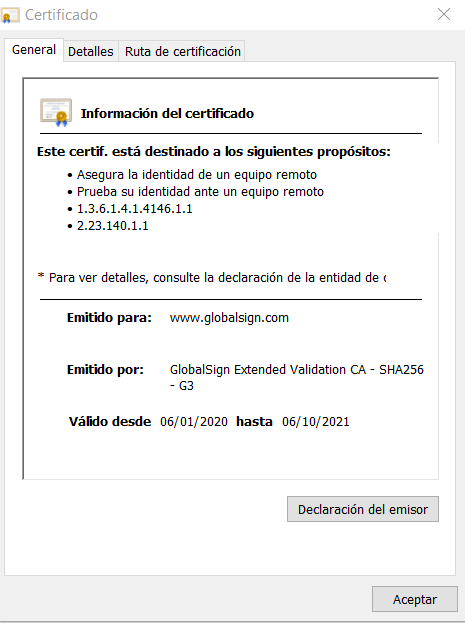


Figura 1: Certificado digital





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

Sha256RSA

¿Cuál es la longitud de la clave utilizada?

256 bits

b ¿Cuál es el periodo de validez del certificado?

1 año y medio

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

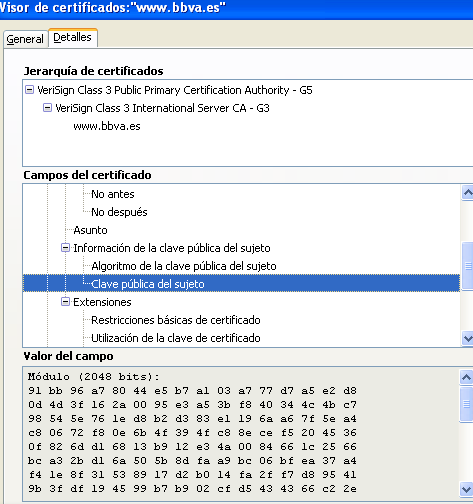
Sha256

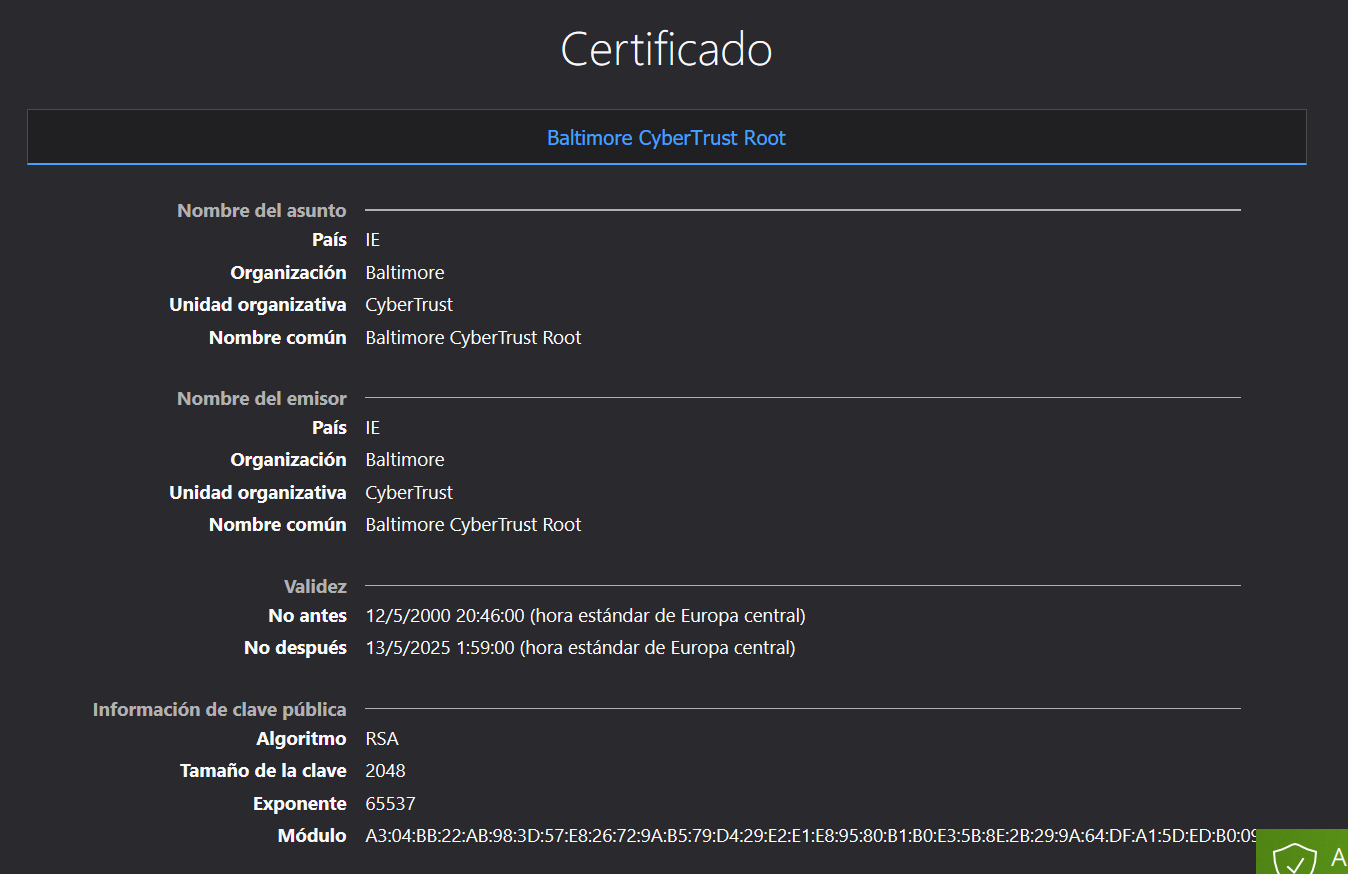
d ¿Qué algoritmo de clave asimétrica ha utilizado la autoridad de certificación para firmar el certificado?

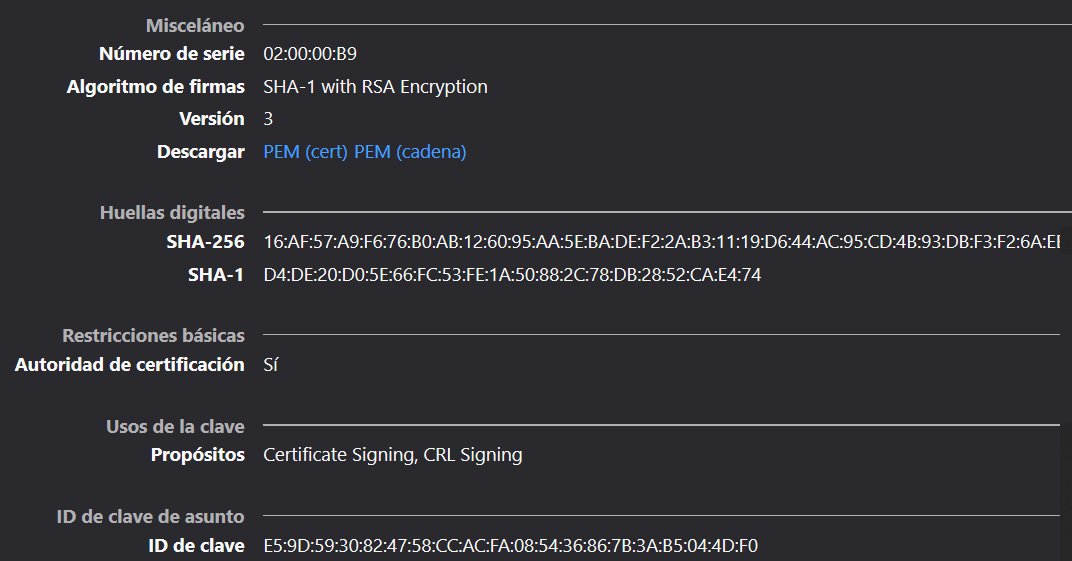
RSA

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

2048 bits







f ¿Qué autoridad de certificación ha firmado el certificado?

Baltimore CyberTrust Root

¿De quién depende?

Baltimore Co

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.

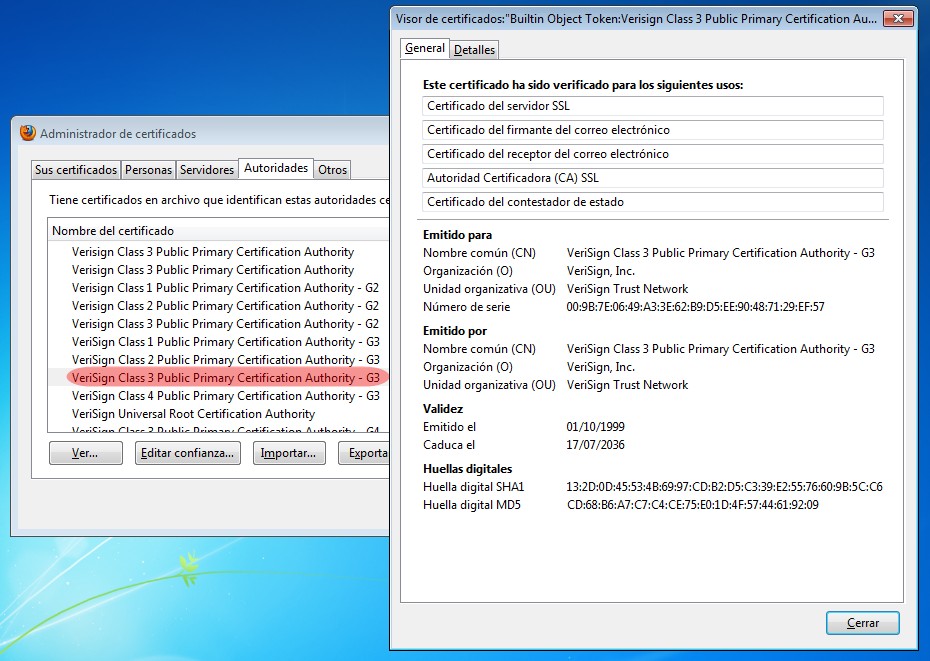
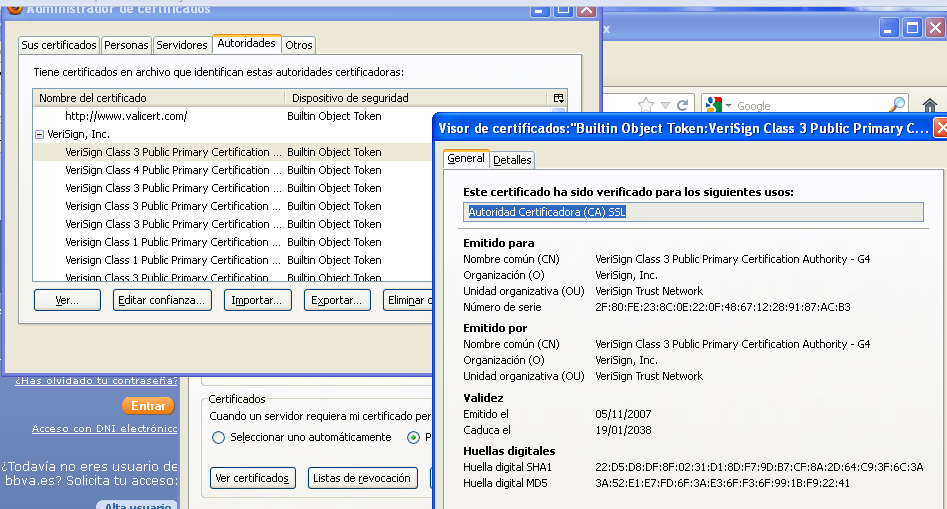


Figura 2: Certificado digital de la autoridad de certificación

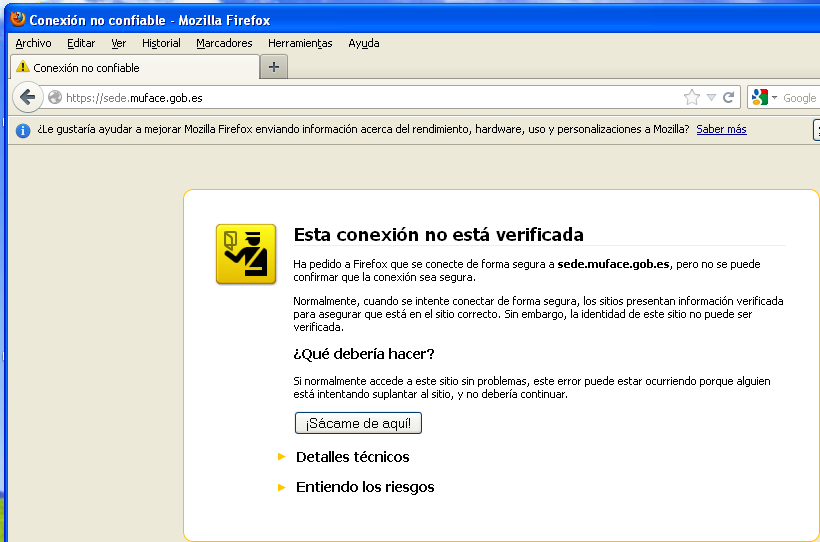


**2. Certificado no verificado**

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.



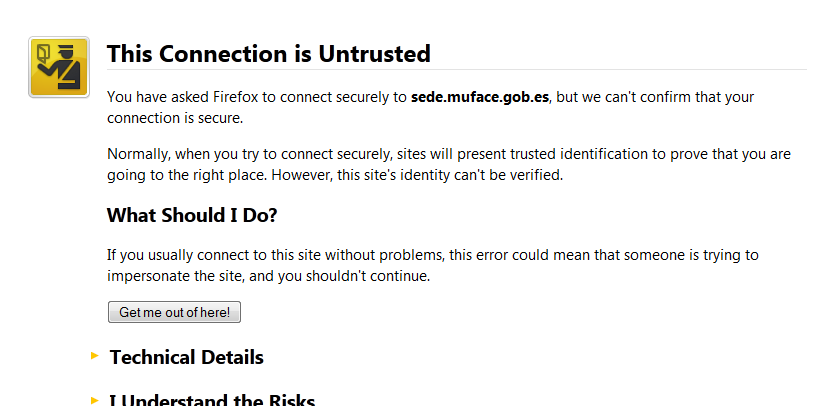
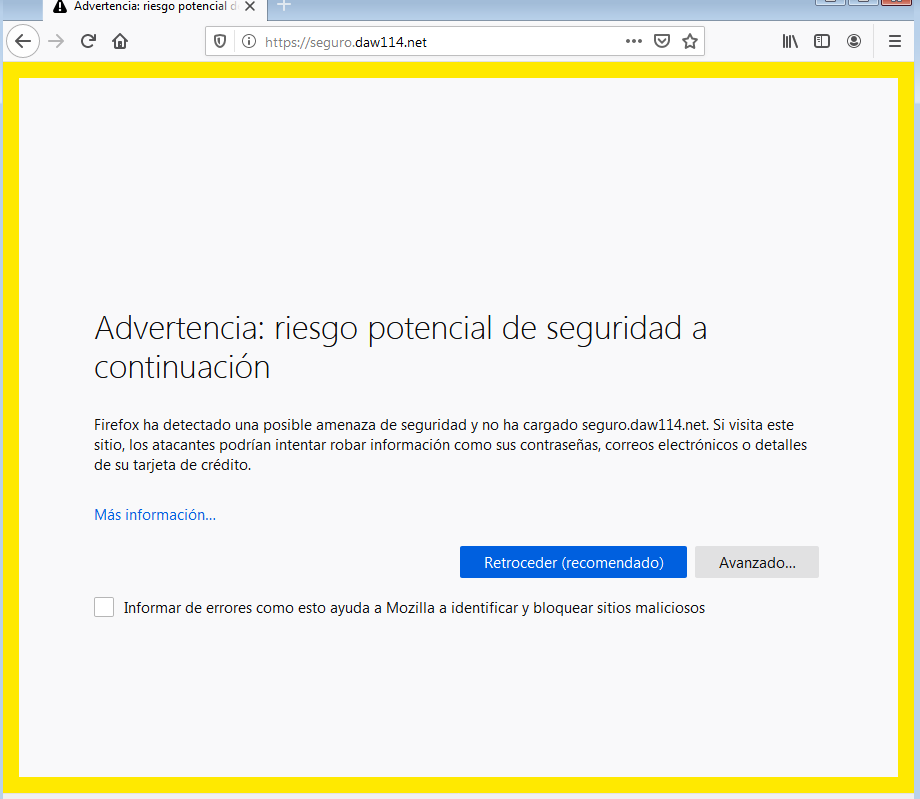
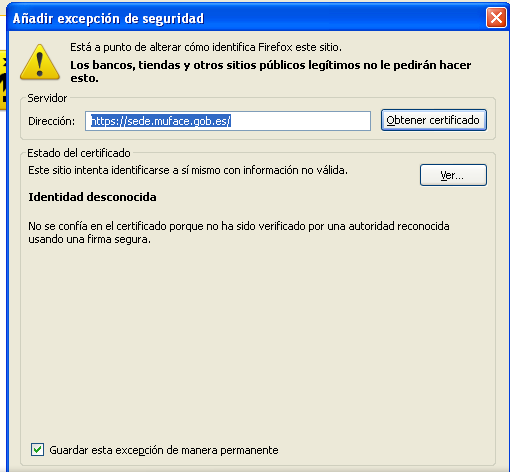


Figura 3: Aviso de certificado digital no verificado

2.4. Selecciona en Entiendo los riesgos.





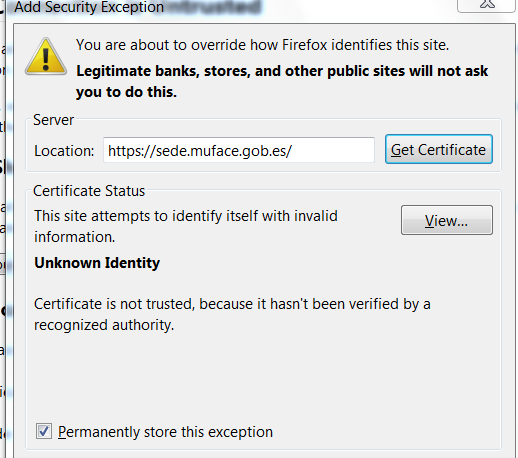
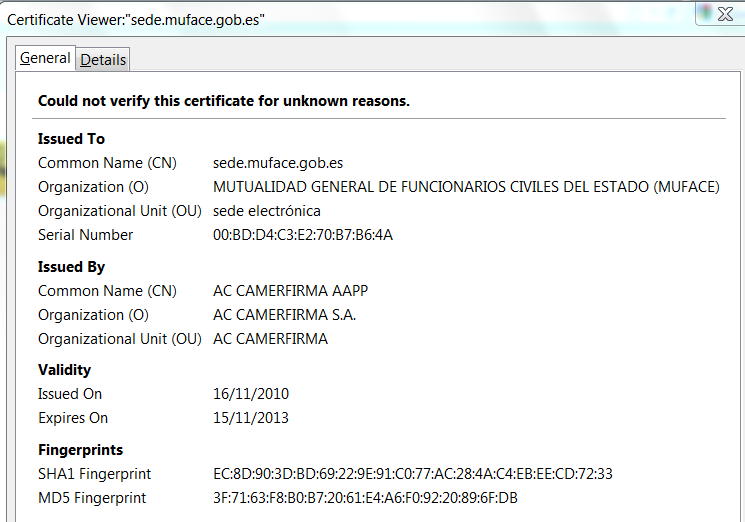
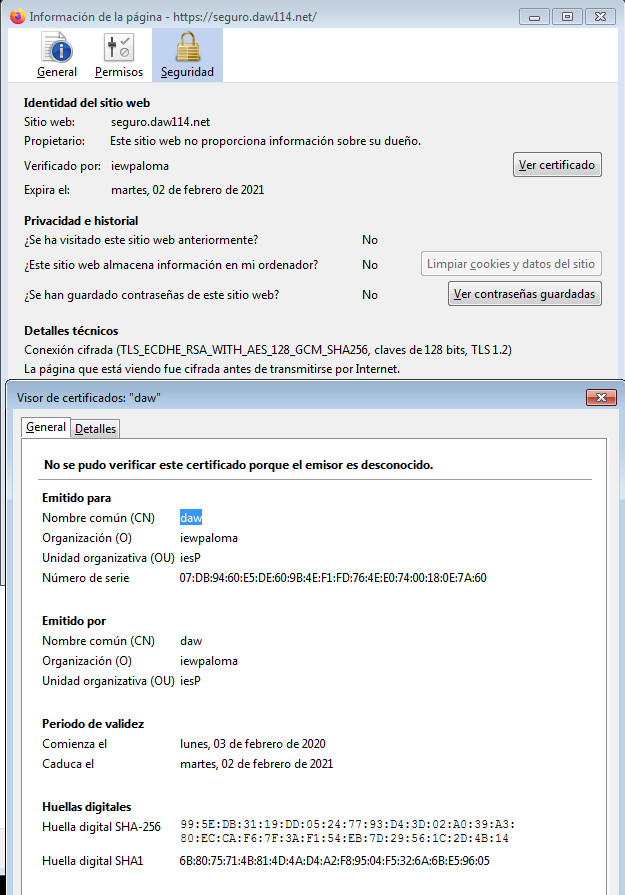


Figura 3b: Añadir excepción

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





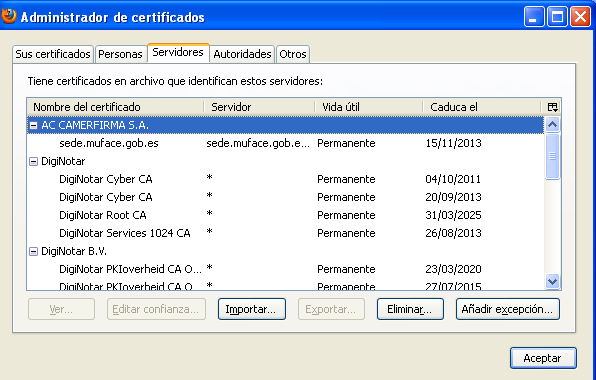


Figura 4: Ver el certificado digital no verificado

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.

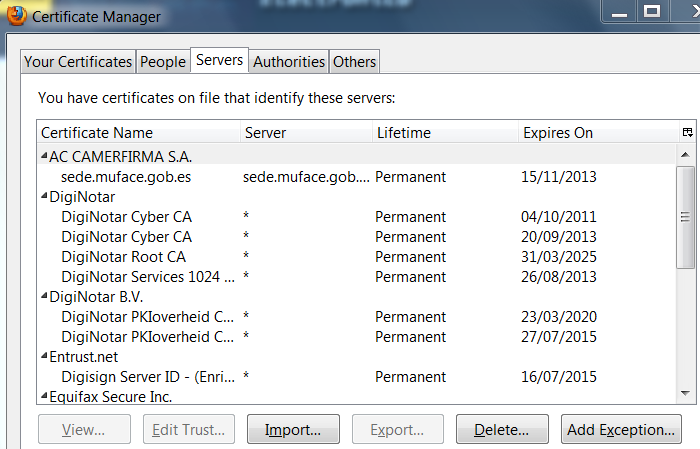


Figura 5: Eliminar certificado del servidor

