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.

Es un documento que recoge ciertos datos de su titular y su clave pública y está firmado electrónicamente por la **Autoridad de Certificación** utilizando su clave privada.

Es un documento que permite al firmante identificarse en Internet. Es necesario para realizar trámites, tanto con las administraciones públicas como con numerosas entidades privadas. Un **certificado revocado** es un certificado que no es válido aunque se emplee dentro de su período de vigencia. Un certificado revocado tiene la condición de suspendido si su vigencia puede restablecerse en determinadas condiciones.

Según la Sede Electrónica del Instituto Nacional de Estadística, un certificado electrónico sirve para:

- Autentificar la identidad del usuario, de forma electrónica, ante terceros.
- Firmar electrónicamente de forma que se garantice la integridad de los datos trasmitidos y su procedencia. Un documento firmado no puede ser manipulado, ya que la firma está asociada matemáticamente tanto al documento como al firmante
- Cifrar datos para que sólo el destinatario del documento pueda acceder a su contenido.

En España, actualmente los certificados electrónicos emitidos por entidades públicas son el **DNIe** o DNI electrónico y el de la Fábrica Nacional de Moneda y Timbre (**FNMT**).

b) Autoridad de certificación

Autoridad de certificación, **certificadora** o **certificante** (**AC** o **CA *Certification Authority***) 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

SKC (*symmetric key cryptography*), también llamada **criptografía de clave secreta** (*secret key cryptography*) o criptografía de una clave(*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. Algunos ejemplos de algoritmos simétricos son DES, 3DES, RC5, AES (**A**dvanced **E**ncryption **S**tandard), Blowfish e IDEA.

d) Criptografía Asimétrica

- La **criptografía asimétrica** (*Asymmetric Key Cryptography*), también llamada **criptografía de clave pública** (*Public Key Cryptography*) o **criptografía de dos claves**[1] (*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. Ejemplos de algoritmos de clave asimétrica son: RSA, DSA y Diffie-Hellman.

e) Comparación entre Criptografía simétrica y asimétrica

Comparación entre criptografía simétrica y asimétrica

Atributo	Clave simétrica	Clave asimétrica
Años en uso	Miles	Menos de 50
Uso principal	Cifrado de grandes volúmenes de datos	Intercambio de claves; firma digital
Estándar actual	DES, Triple DES, AES	RSA, Diffie-Hellman, DSA
Velocidad	Rápida	Lenta
Claves	Compartidas entre emisor y receptor	Privada: sólo conocida por una persona Pública: conocida por todos
Intercambio de claves	Difícil de intercambiar por un canal inseguro	La clave pública se comparte por cualquier canal La privada nunca se comparte
Longitud de claves	56 bits (vulnerable) 256 bits (seguro)	1024 – 2048 (RSA) 172 (curvas elípticas)
Servicios de seguridad	Confidencialidad Integridad Autenticación	Confidencialidad Integridad Autenticación, No repudio

f) SSL

Secure Sockets Layer (***SSL***) «capa de conexión segura» y su sucesor ***Transport Layer Security*** (***TLS***) «seguridad de la capa de transporte» son protocolos criptográficos que proporcionan comunicaciones seguras por una red. SSL proporciona autenticación y privacidad de la información entre extremos sobre Internet mediante el uso de criptografía. Habitualmente, sólo el servidor es autenticado (es decir, se garantiza su identidad) mientras que el cliente se mantiene sin autenticar.

SSL implica una serie de fases básicas:

- Negociar entre las partes el algoritmo que se usará en la comunicación
- Intercambio de claves públicas y autenticación basada en certificados digitales
- Cifrado del tráfico basado en cifrado simétrico

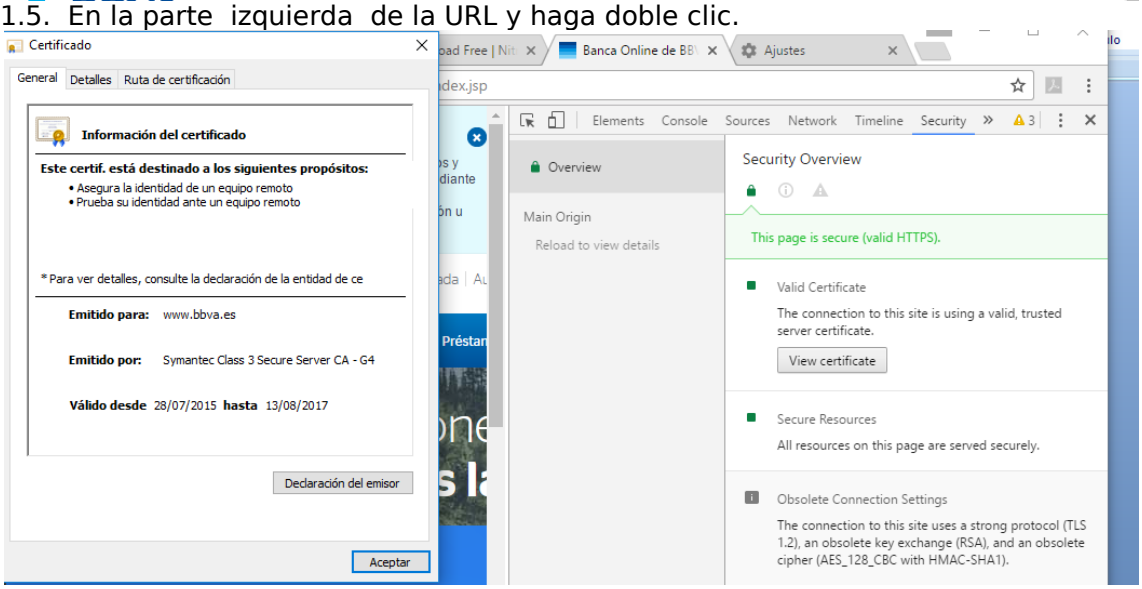
Durante la primera fase, el cliente y el servidor negocian qué algoritmos criptográficos se van a usar. Las implementaciones actuales proporcionan las siguientes opciones:

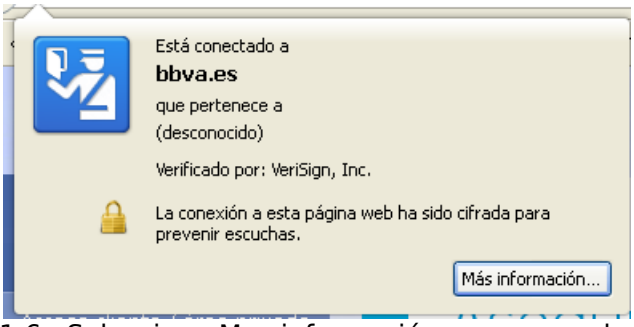
- Para criptografía de clave pública: RSA, Diffie-Hellman, DSA (Digital Signature Algorithm) o Fortezza;
- Para cifrado simétrico: RC2, RC4, IDEA (International Data Encryption Algorithm), DES (Data Encryption Standard), Triple DES y AES (Advanced Encryption Standard);
- Con funciones hash: MD5 o de la familia SHA.

1. Certificado digital verificado

1.1. Inicia sesión en WindowsXP.
1.2. Inicia Firefox.
1.3. Conecte a http://www.bbva.es.
1.4. Observe en la URL que el protocolo usado es https.

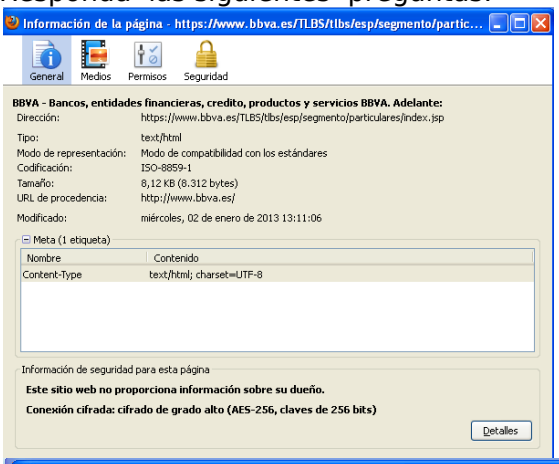
1.5. En la parte izquierda de la URL y haga doble clic.

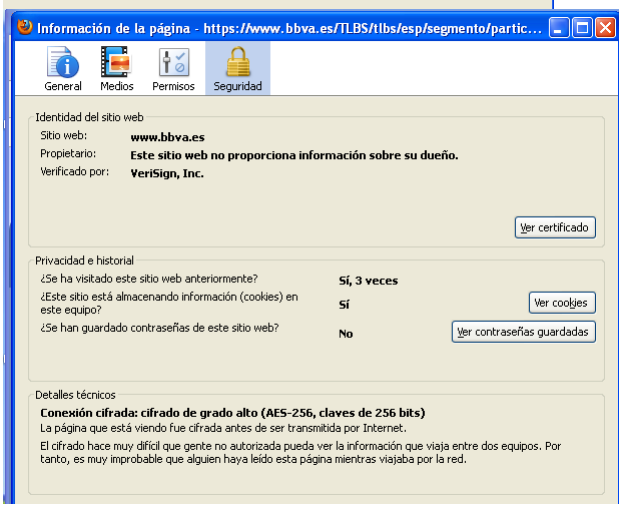


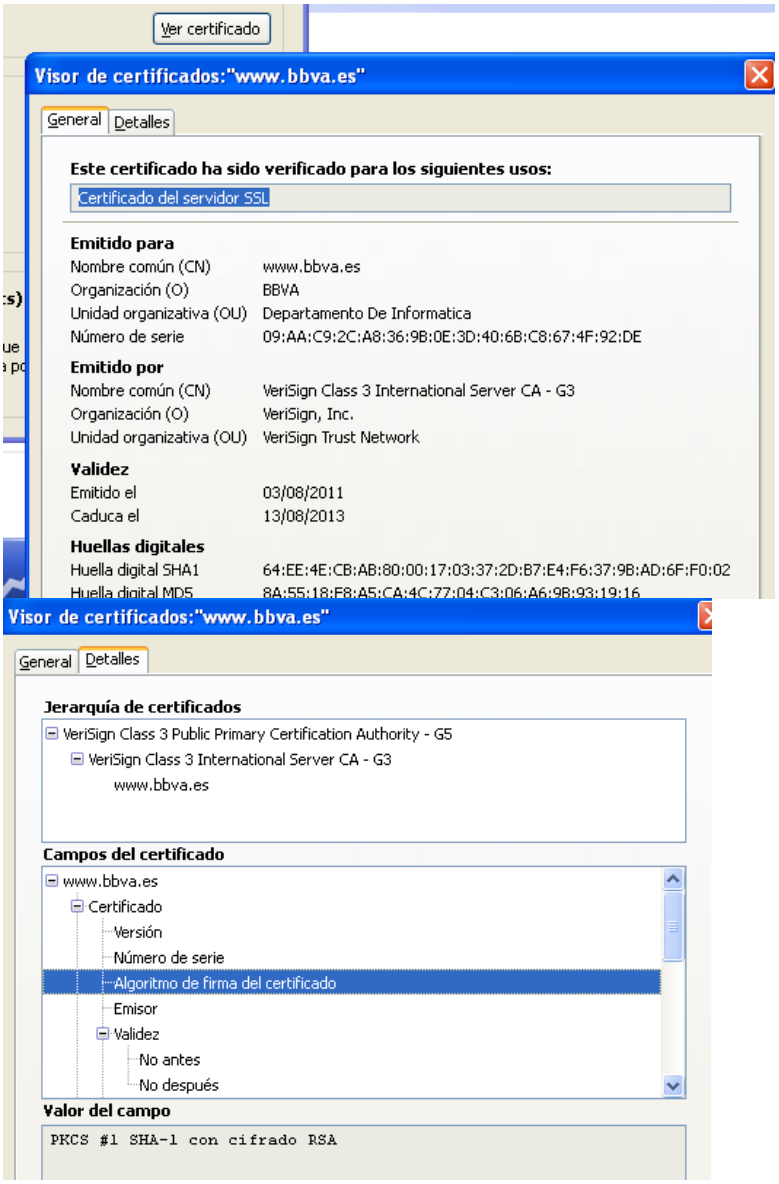


1.6. Seleccione Mas información para consular el certificado digital que ha enviado el servidor web. También se puede acceder a través de Herramientas => Información de la página.

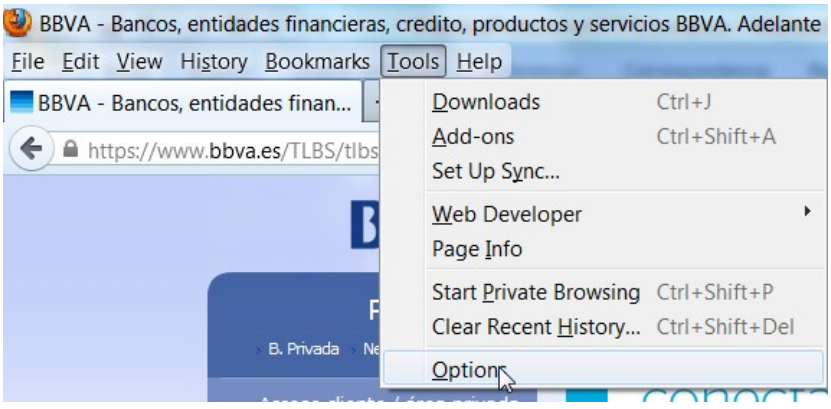
Responda las siguientes preguntas:

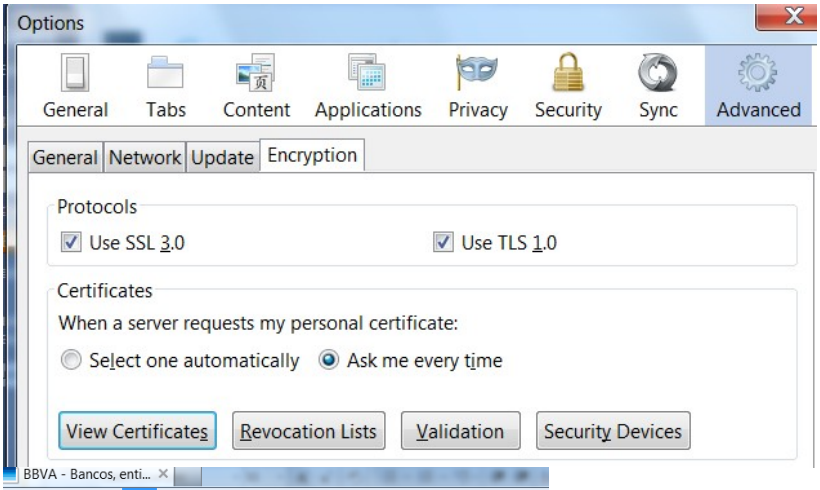


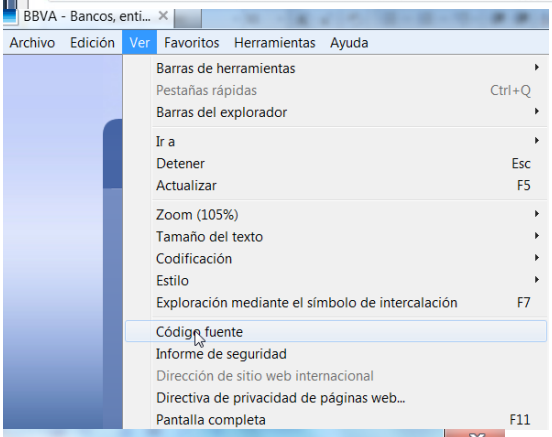




En Windows 2007:




Options
General
Tabs
Content
Applications
Privacy
Security
Sync
Advanced
General
Network
Update
Encryption
Protocols
Use SSL 3.0
Use TLS 1.0
Certificates
When a server requests my personal certificate:
Select one automatically
Ask me every time
View Certificates
Revocation Lists
Validation
Security Devices


BBVA - Bancos, enti...
Archivo
Edición
Ver
Favoritos
Herramientas
Ayuda
Barras de herramientas
Pestañas rápidas
Ctrl+Q
Barras del explorador
Ir a
Detener
Esc
Actualizar
F5
Zoom (105%)
Tamaño del texto
Codificación
Estilo
Exploración mediante el símbolo de intercalación
F7
Código fuente
Informe de seguridad
Dirección de sitio web internacional
Directiva de privacidad de páginas web...
Pantalla completa
F11


Certificado
General
Detalles
Ruta de certificación
Información del certificado
Este certif. está destinado a los siguientes propósitos:
• Asegura la identidad de un equipo remoto
* Para ver detalles, consulte la declaración de la entidad de
Emitido para: www.bbva.es
Emitido por: VeriSign Class 3 International Server CA - G3
Válido desde 03/ 08/ 2011 hasta 13/ 08/ 2013
Declaración del emisor
Obtener más información acerca de certificados
Aceptar

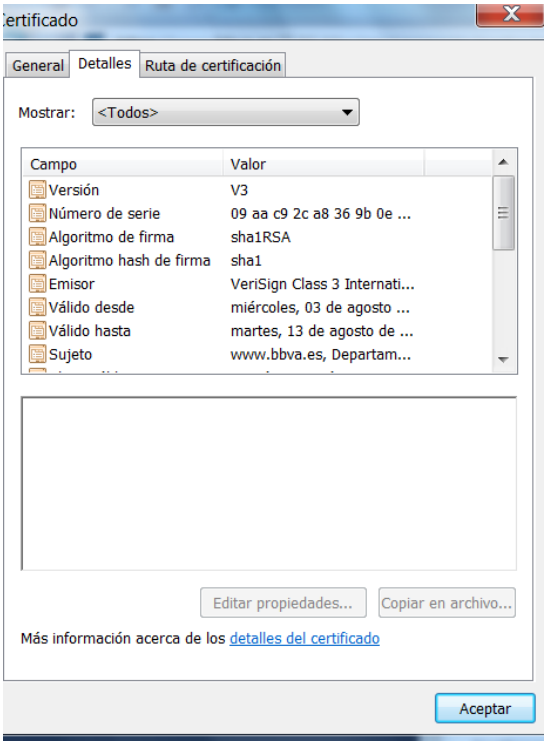


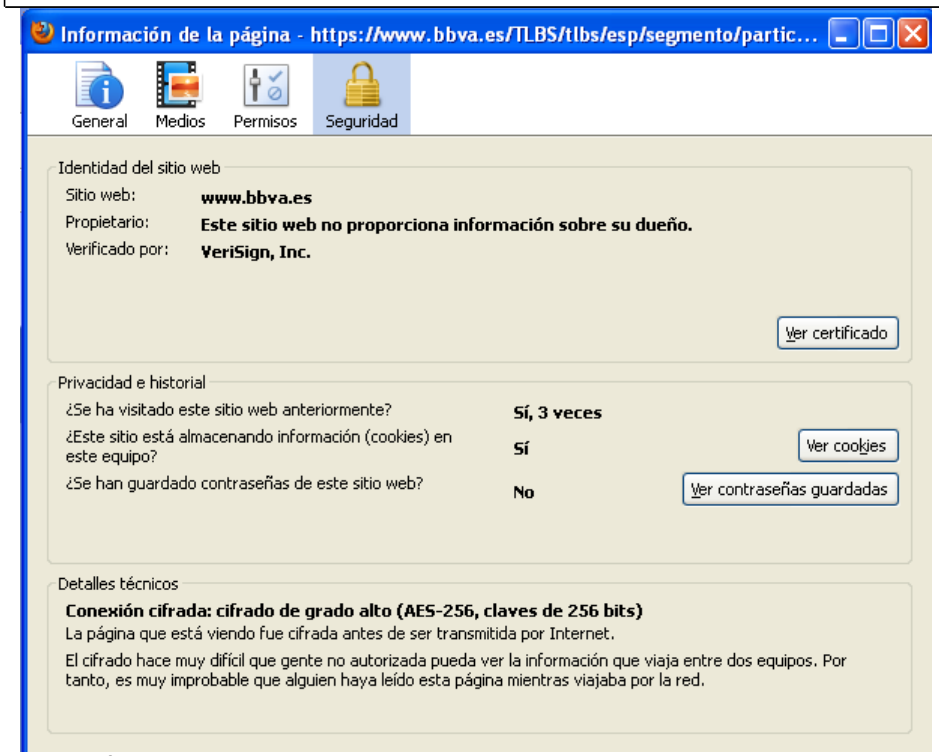
Figura 1: Certificado digital

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

AES

¿Cuál es la longitud de la clave utilizada?

256 bits.



b ¿Cuál es el periodo de validez del certificado?

Del 03/08/2011 al 13/08/2013.

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

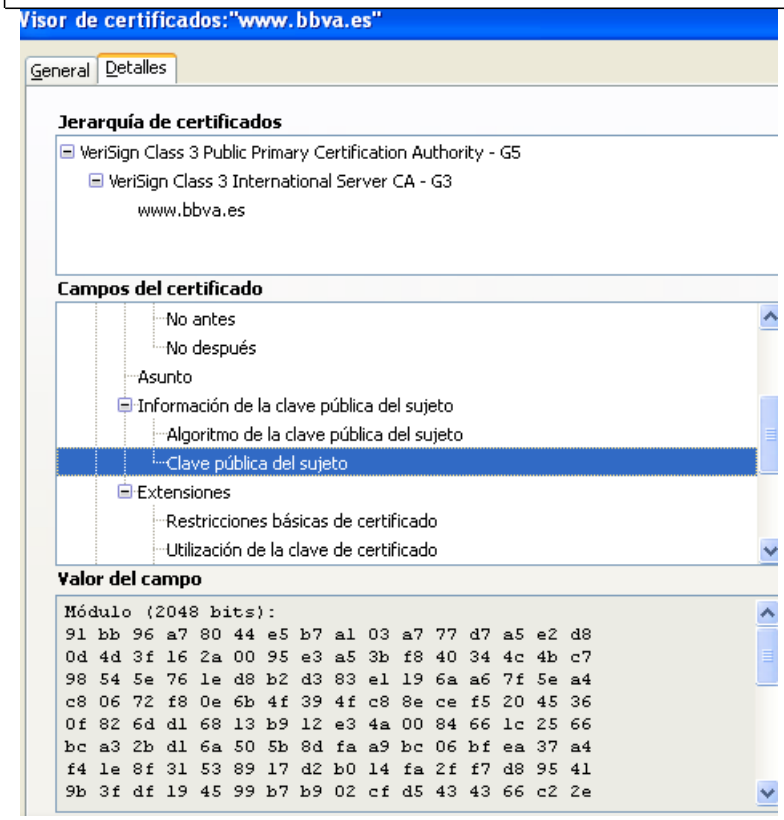
SHA1 con cifrado RSA

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.

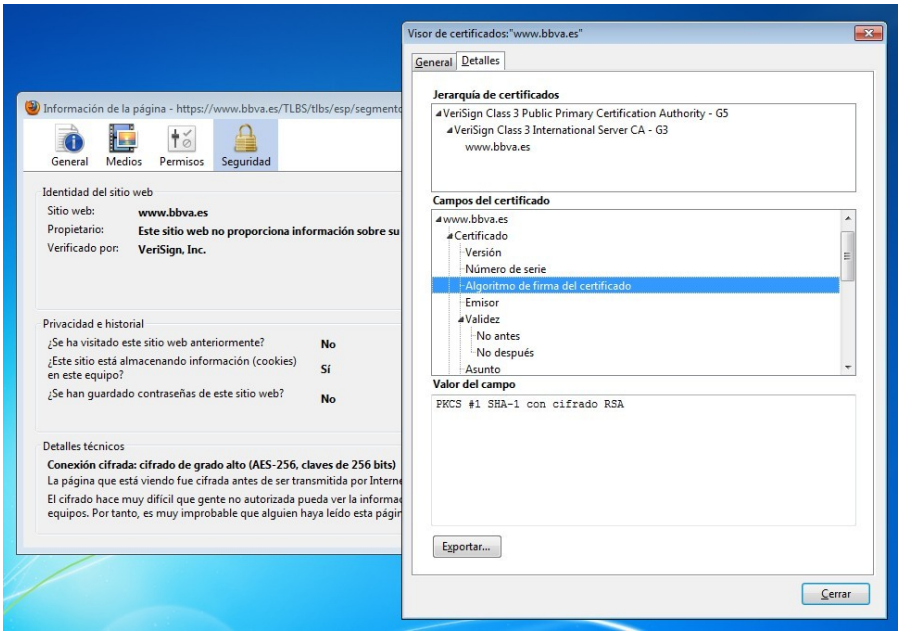


f ¿Qué autoridad de certificación ha firmado el certificado?

VeriSign Class 3 Internatio- nal Server CA - G3

¿De quién depende?

VeriSign Class 3 Public Primary Certification Authority - G5.



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.

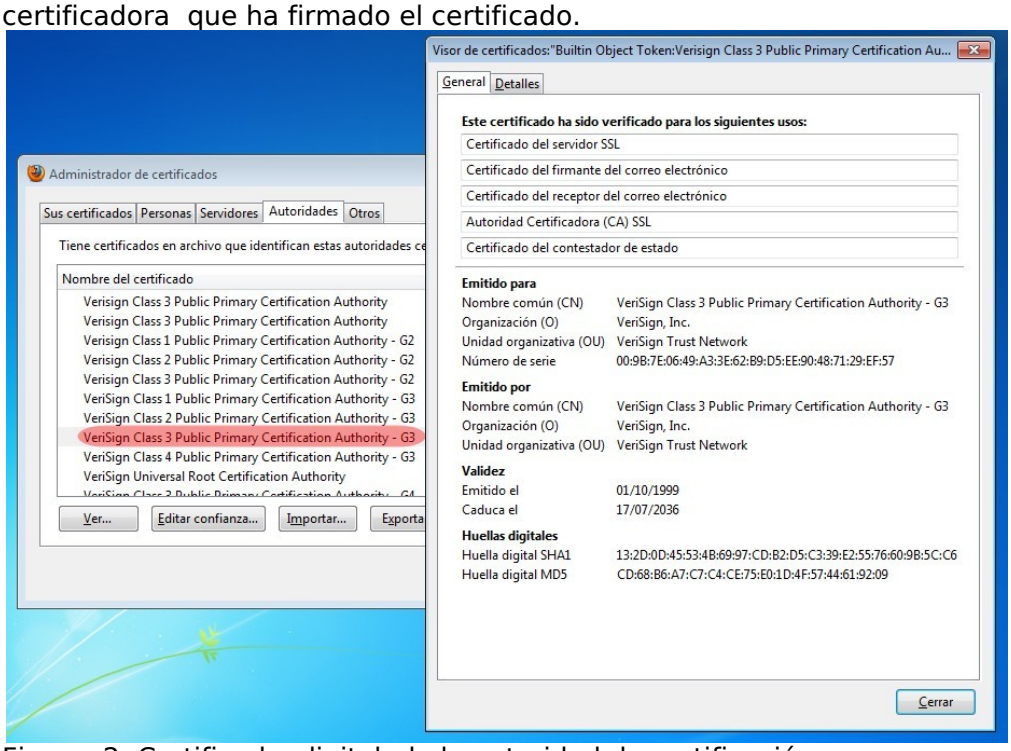
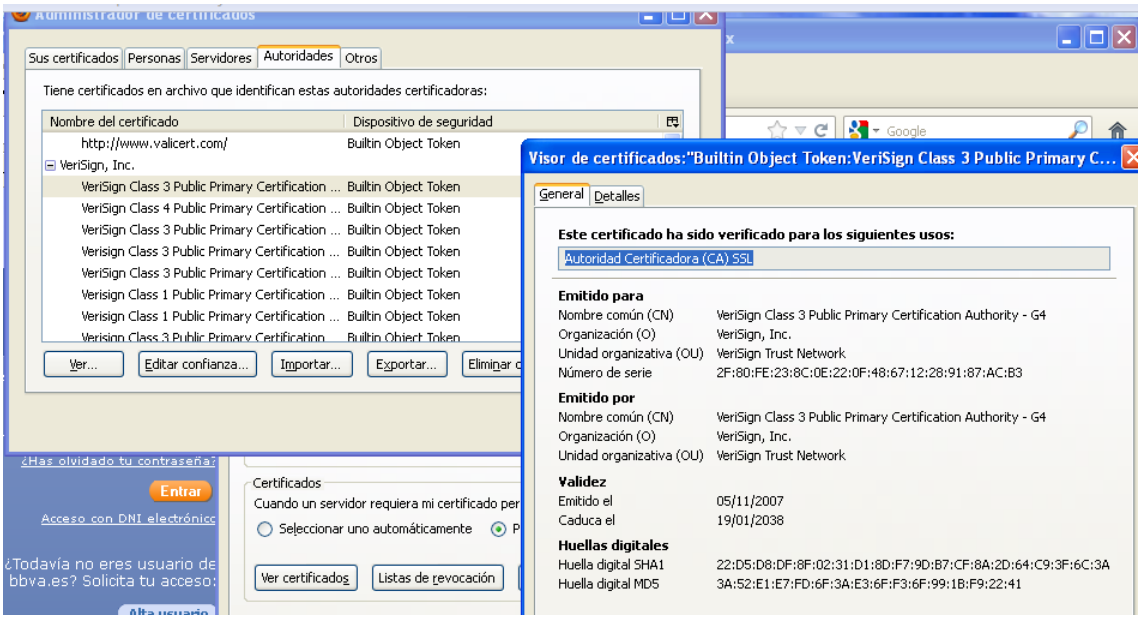
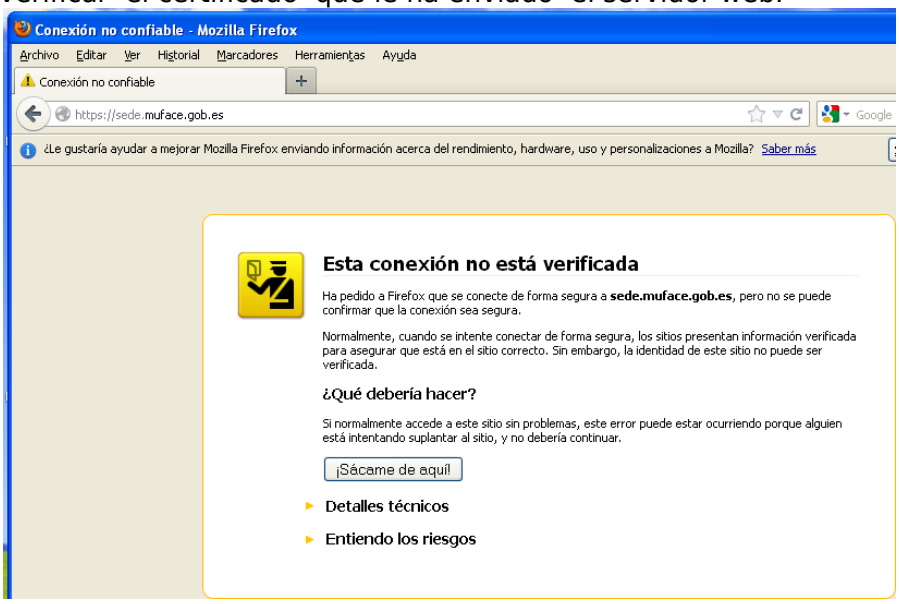


Figura 2: Certificado digital de la autoridad de certificación



2. Certificado no verificado

2.1. Inicia Firefox.
2.2. Conecte a https://sede.muface.gob.es/.
2.3. El navegador muestra un mensaje de error indicando que no ha podido verificar el certificado que le ha enviado el servidor web.



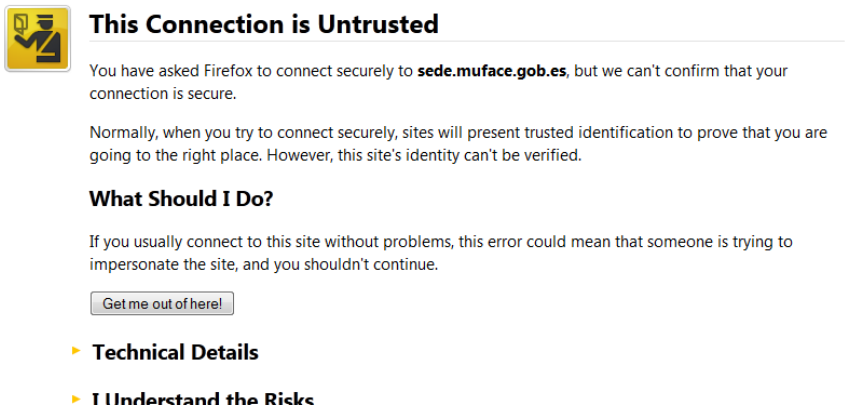
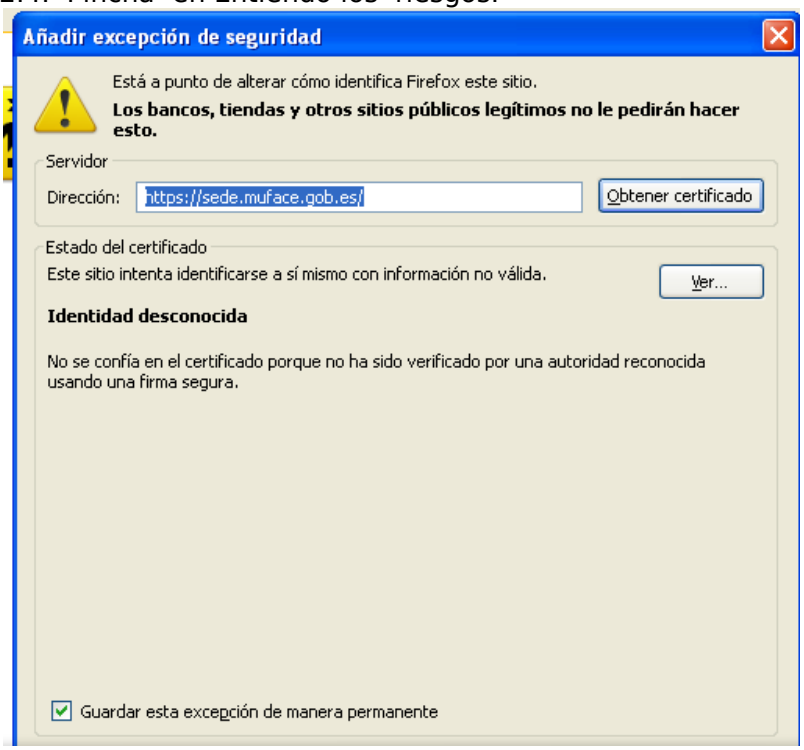


Figura 3: Aviso de certificado digital no verificado

2.4. Pincha en Entiendo los riesgos.



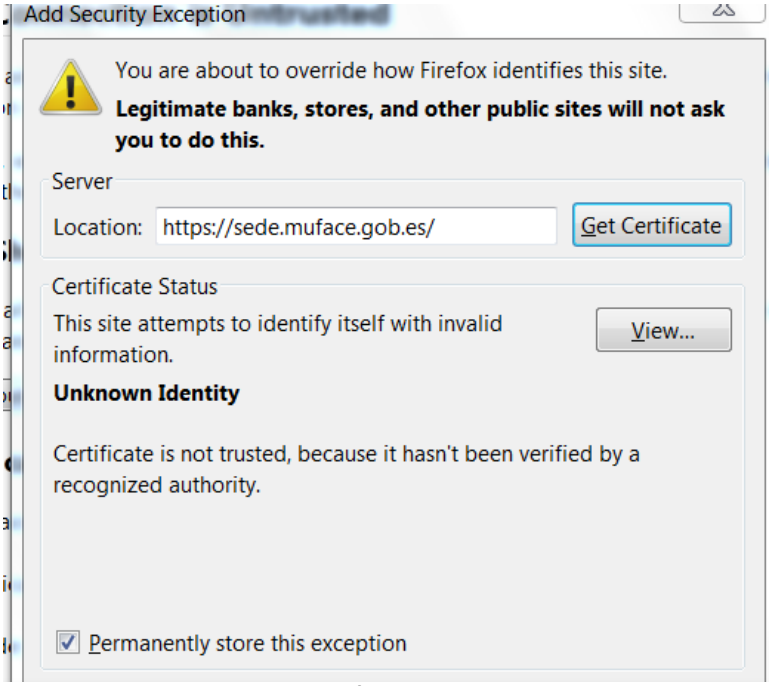
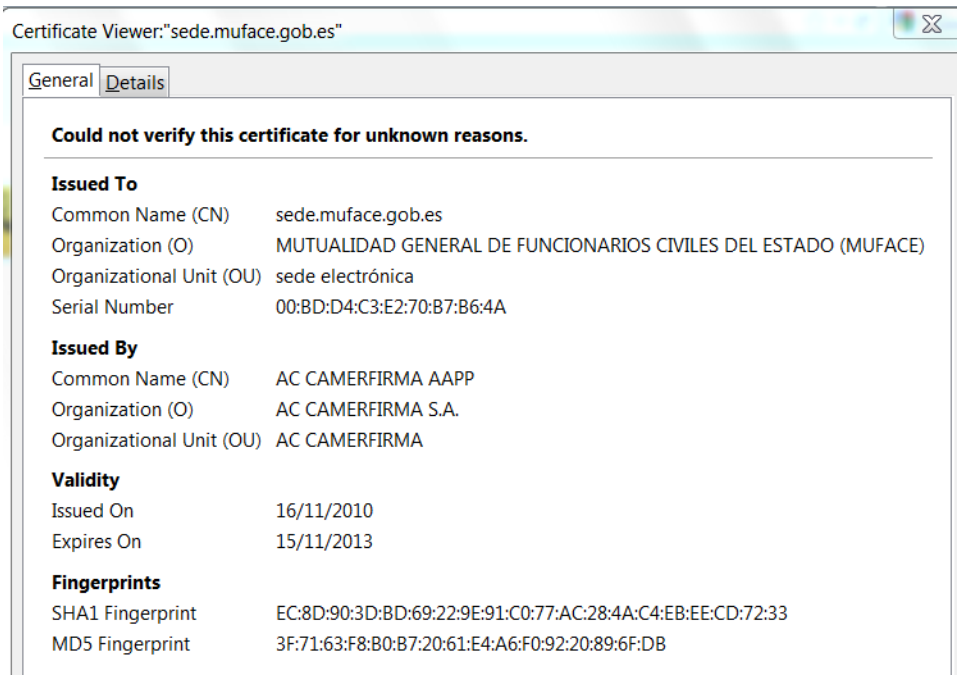


Figura 3b: Añadir excepción

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



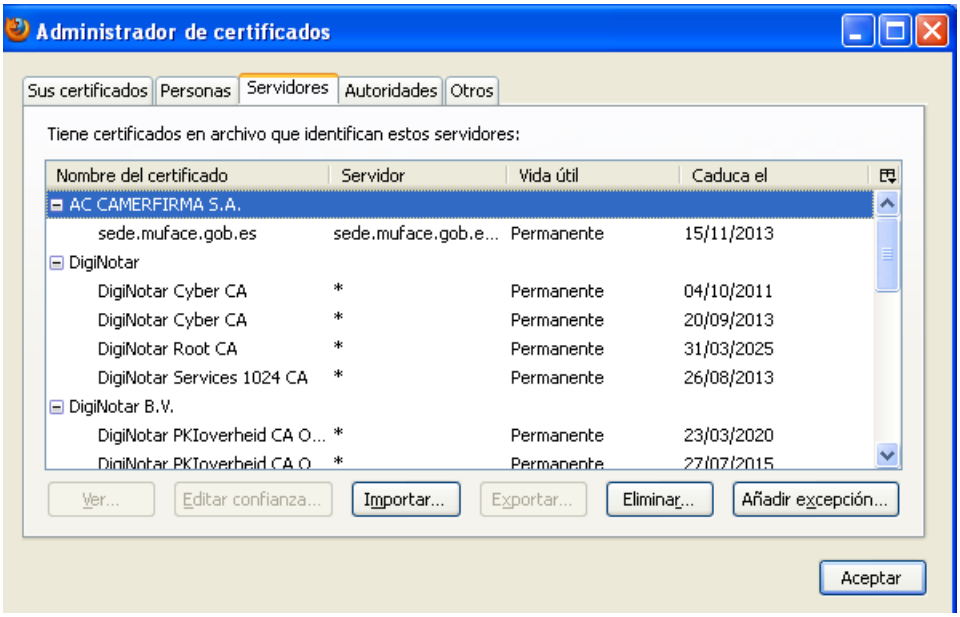


Figura 4: Ver el certificado digital no verificado

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

2.7. Pincha en confirmar 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.

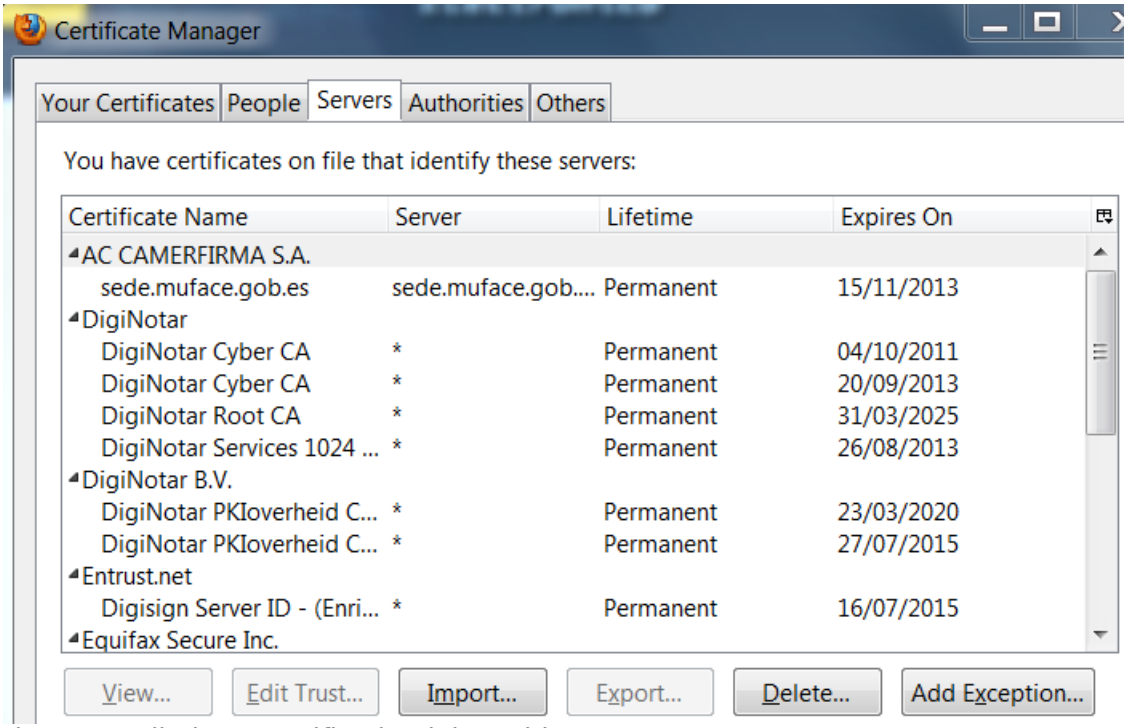


Figura 5: Eliminar certificado del servidor