Práctica 5.18: HTTPS y certificados digitales

1. **Certificado digital verificado**

   1.1. Inicia sesión en **DesarrolloW7XX**.

   1.2. Inicia *Firefox*.

   1.3. Conéctate a `https://www.bbva.es`.

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

   1.5. Pincha en la parte izquierda de la URL.

   1.6. Pincha sobre **Mas información** para consular el certificado digital que ha enviado el servidor web y responde de a las siguientes preguntas, Figura 1.

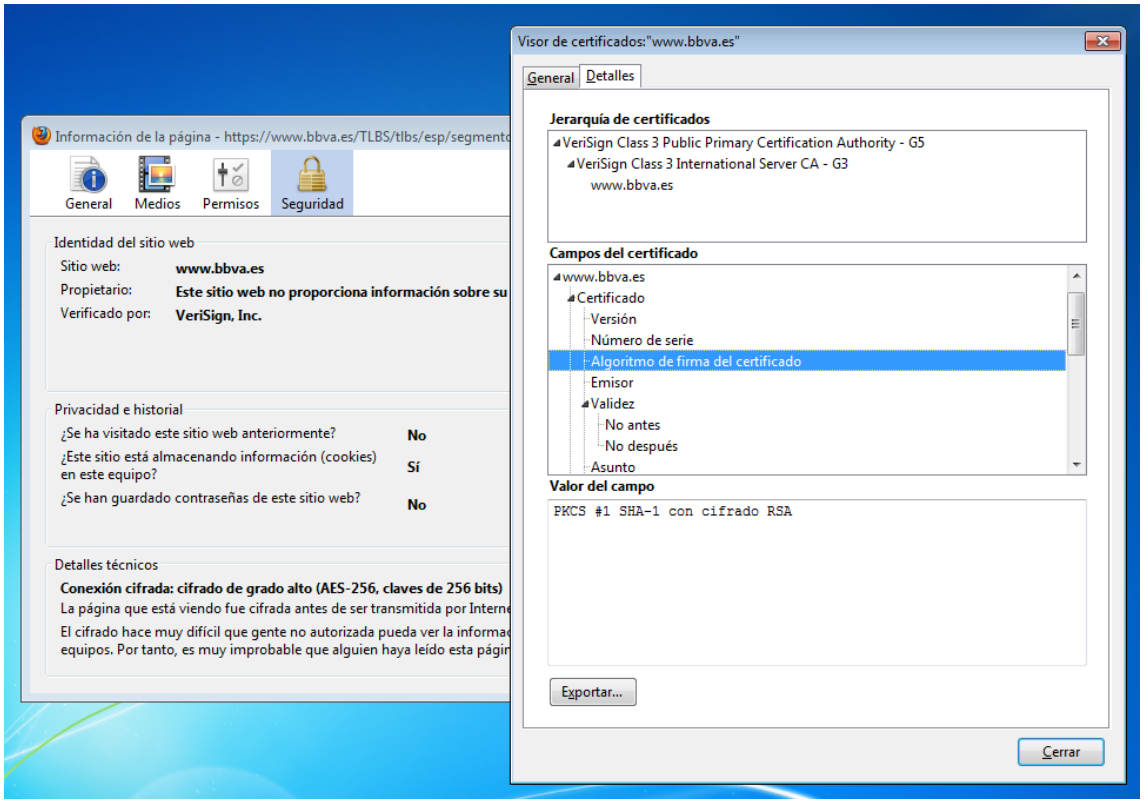

Figura 1: Certificado digital

   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*.

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 International 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.

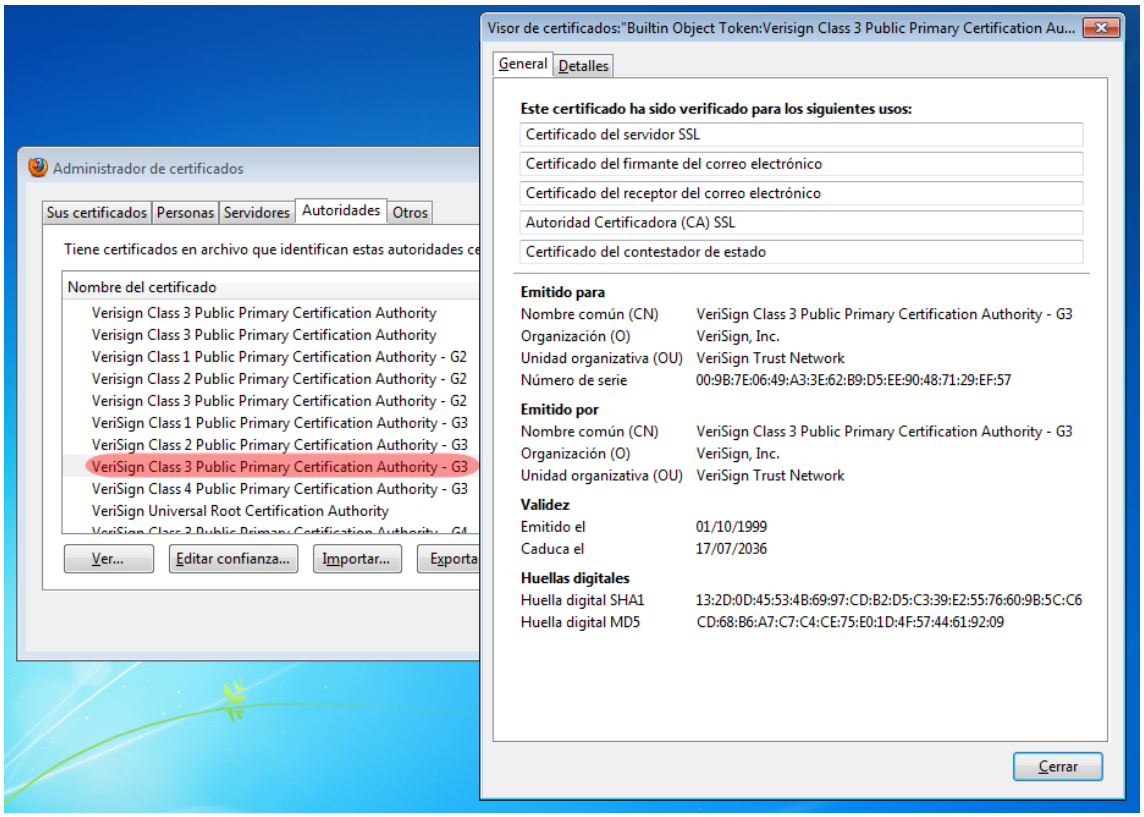

Figura 2: Certificado digital de la autoridad de certificación

2. **Certificado no verificado**

2.1. Inicia Firefox.

2.2. Conéctate a la url que indique el profesor.

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.

2.4. Pincha en **Entiendo los riesgos**.

2.5. Pincha en **Añadir Excepción**, Figura 4. Observa que está marcada la opción **Guardar excepción de forma permanente**.

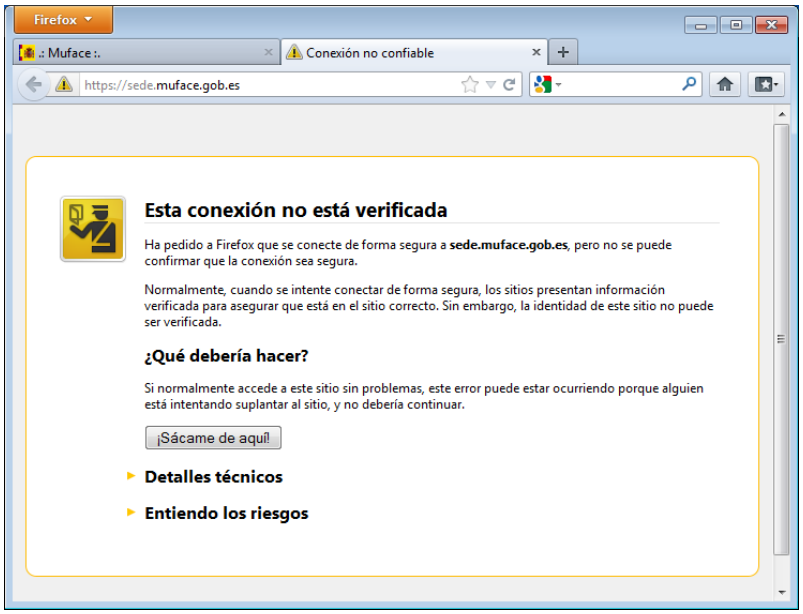

Figura 3: Aviso de certificado digital no verificado

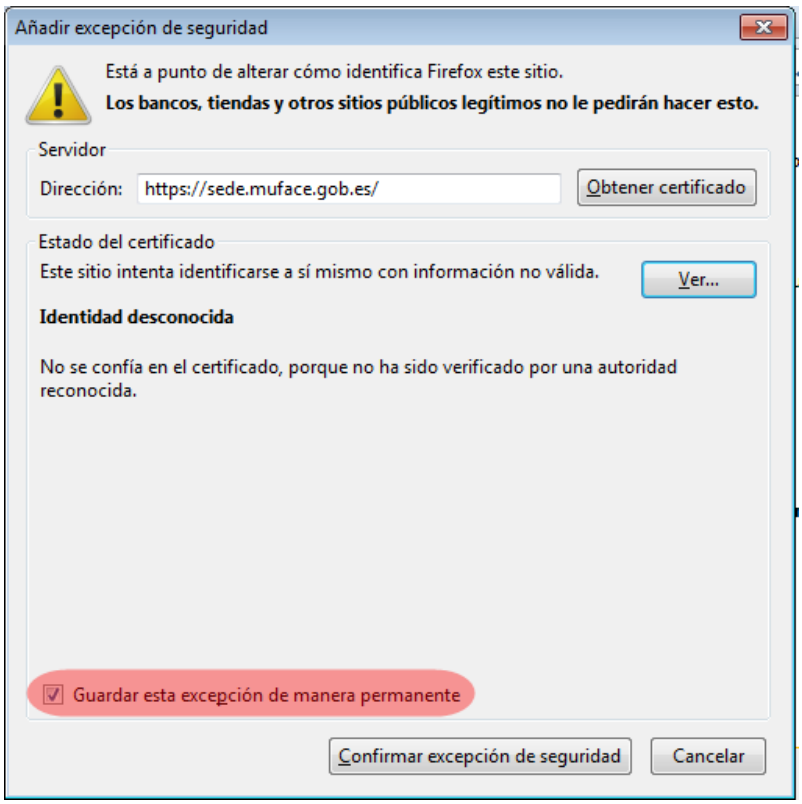

Figura 4: Ver el certificado digital no verificado

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, Pestaña Cifrado, Ver certificados** busca el certificado del servidor que has aceptado y elimínalo, Figura 5.

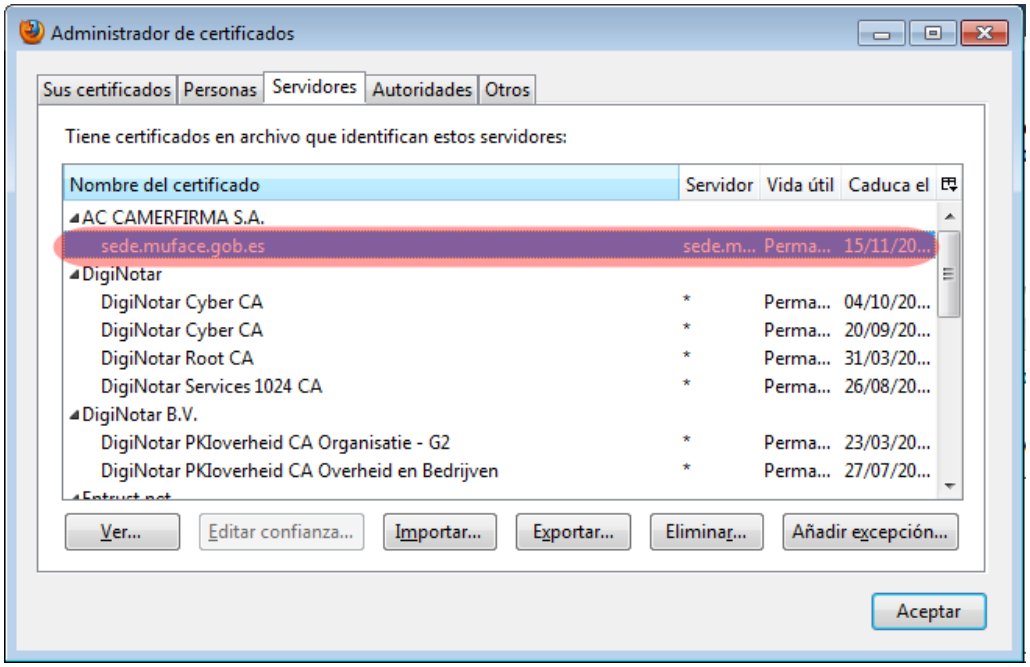

Figura 5: Eliminar certificado del servidor

◇