

## 4. Administración de Apache

### 4.18. HTTPS y certificados digitales

#### 1. Certificado digital verificado

- 1.1. Inicia sesión en **DesarrolloW7XX**.
- 1.2. *Inicia Chrome* y conéctate a <https://www.bbva.es>. Observa en la URL que el protocolo usado es https. En la parte izquierda de la URL y haz doble clic.(El candado doble clic)
- 1.3. Pincha sobre **más información** para consular el certificado digital que ha enviado el servidor web y responde a las siguientes preguntas, Figura 4.105. Con el Chrome podemos ver la información directamente pinchando sobre el candado de la URL.

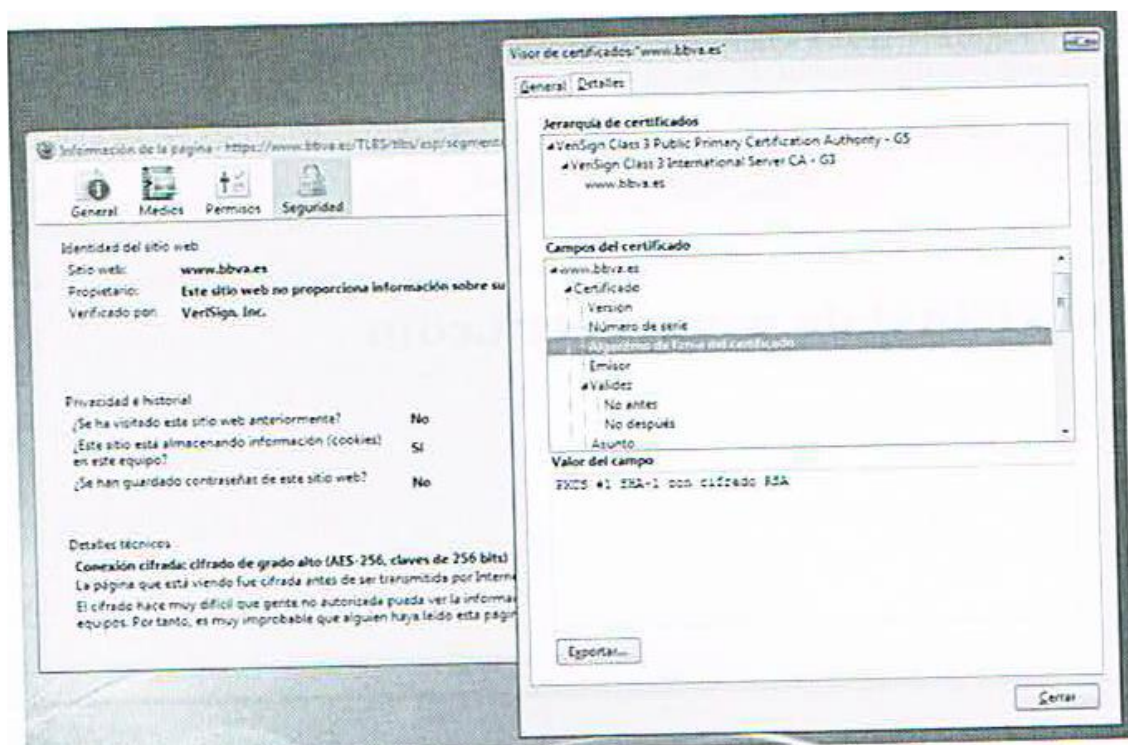


Figura 4.105: Certificado digital

- 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*.

- 1.4. En el menú de *Chrome* accede a **Opciones, Opciones, pestaña Avanzado, Pestaña Cifrado, Ver certificados** y busca el certificado de la autoridad certificadora que ha firmado el certificado, Figura 4.106

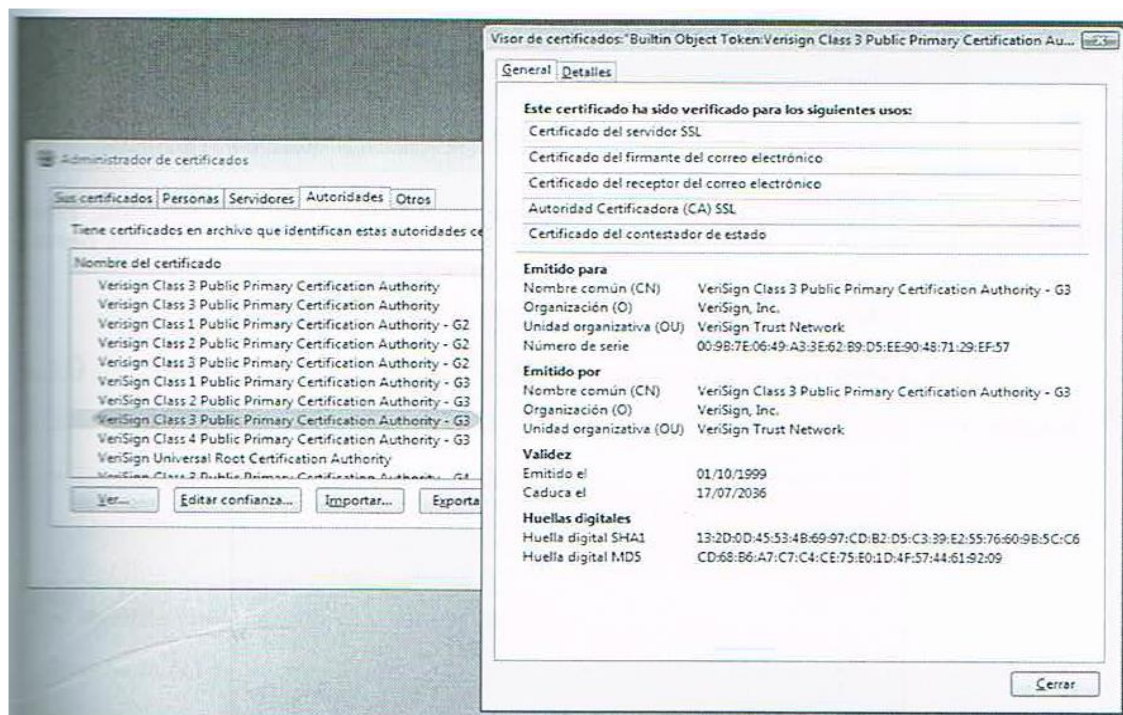


Figura 4.106: Certificado digital de la autoridad de certificación

## 2. Certificado no verificado

2.1. Inicia Firefox y conéctate a <https://sede.muface.gob.es/>.

2.2. El navegador muestra un mensaje de error indicando que no ha podido verificar el certificado que le ha enviado el servidor web, Figura 4.107.

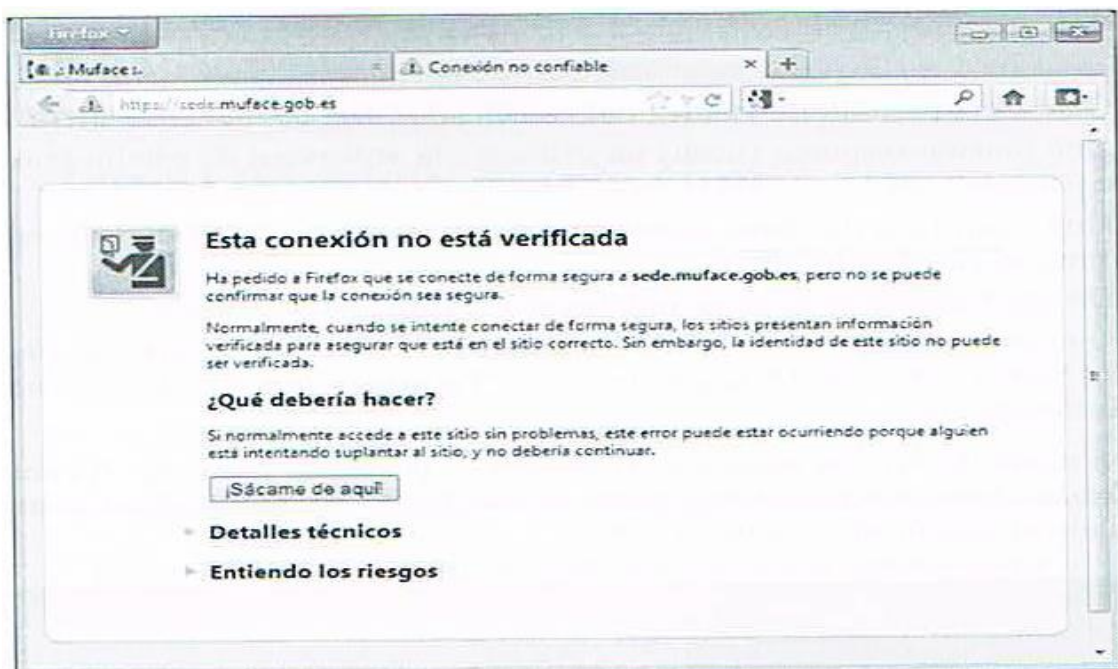


Figura 4.107: Aviso de certificado digital no verificado

2.3. Pincha en **Entiendo los riesgos** y posteriormente en **Añadir Excepción**, Figura 4.108. Observa que está marcada la opción **Guardar excepción de forma permanente**.

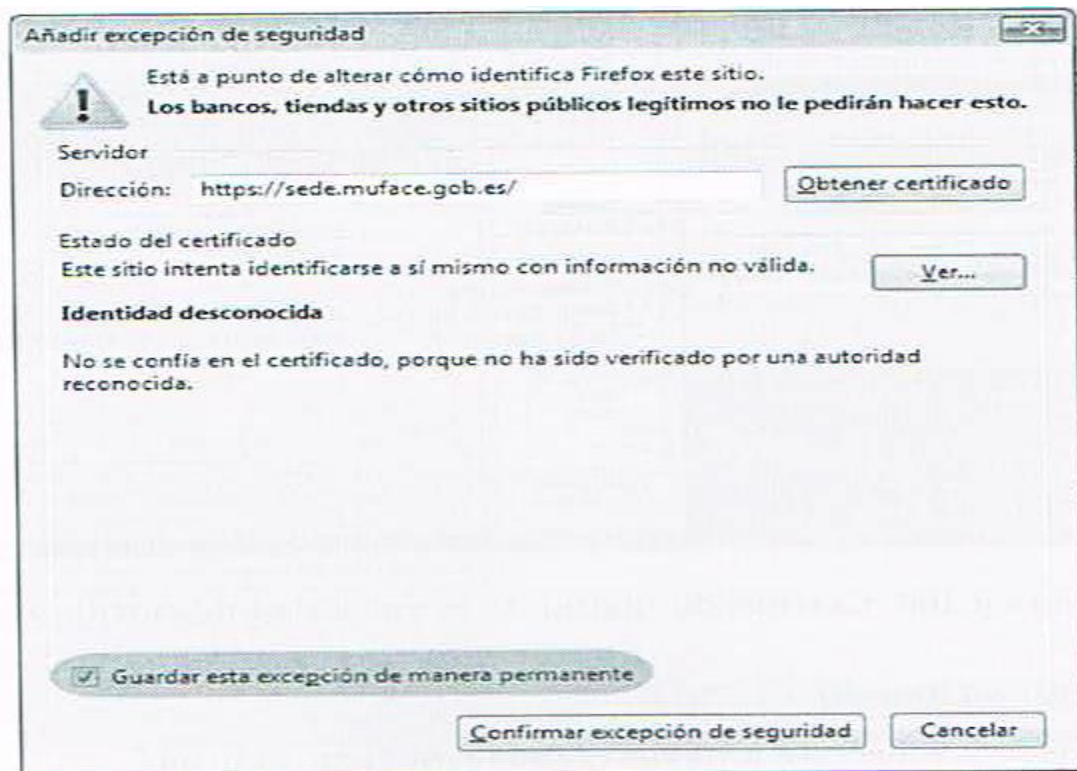


Figura 4.108: Ver el certificado digital no verificado

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

2.5. Pincha en confirmar excepción de seguridad.

2.6. 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 4.109. Recuerda que aparecerá como "sede.muface.gob.es".

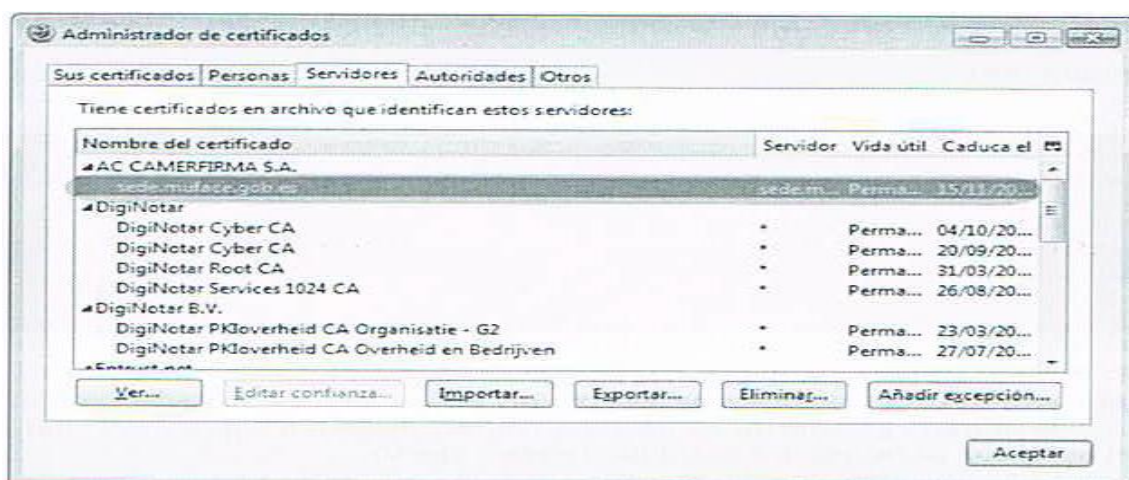


Figura 4.109: Eliminar certificado del servidor