ANEXO 5. Validez de un Certificado Digital

CONSIDERACIONES PARA DETERMINAR LA VALIDEZ DE UN CERTIFICADO DIGITAL

(versión 1.0)

Por: Lic. Ana Ampuero Paiss[1] e Ing. María Paula Encinas Zevallos[2]

Contenido

Requisitos para la validación de un certificado

Para aceptar o comprobar la validez de un certificado que va a ser empleado en un proceso de autenticación, firma digital, cifrado de datos, o algún otro en el que dicha validez sea requerida se debe tener en cuenta lo siguiente.

CASO 1. Verificación automática mediante aplicación de software.

El usuario que va aceptar o comprobar la validez de un certificado digital emitido bajo el marco de la Infraestructura Oficial de Firma Electrónica – IOFE, debe emplear una aplicación acreditada por la Autoridad Administrativa Competente (AAC). Dicha aplicación deberá estar apropiadamente configurada de tal forma que estas verificaciones puedan ser realizadas (vale decir, que no estén deshabilitadas o configuradas de manera no apropiada para el tipo de empleo que se va a realizar del certificado en mención).

CASO 2. Verificación manual por parte de un usuario.

---

[1] Coordinador General de Usabilidad y Entrenamiento PKI – Gerencia de Certificación y Registro Digital – RENIEC.

[2] Analista de Servicios PKI – Sub Gerencia de Certificación Digital – RENIEC.

Antes de observar los ejemplos de verificación manual del certificado digital, es recomendable conocer lo siguiente:

1. **Comprobar la integridad del certificado digital:** Al ser el certificado digital un documento electrónico firmado digitalmente, es posible comprobar la integridad de dicho documento, es decir comprobar que no haya sufrido cambios luego de su emisión, mediante la verificación de la firma de dicho certificado digital.
2. **Comprobar la vigencia del certificado.** Los certificados de clave pública se emiten con una duración prevista y con una fecha de vencimiento explícita. Una vez emitido, el certificado se considera válido desde el inicio de su intervalo de vigencia hasta su fecha de caducidad. Se debe comprobar que el certificado va a ser usado (o fue usado) durante su intervalo de vigencia.
3. **Comprobar el estado del certificado.** Existen diversas circunstancias por las cuales un certificado puede dejar de ser válido antes de alcanzar su fecha de expiración. Por ello es necesario verificar adicionalmente el estado del certificado mediante alguno de los mecanismos que la Autoridad Certificadora pone a disposición para tal fin: OCSP y CRL.
   - Si se cuenta con el servicio de consultas de estado del certificado mediante OCSP, éste debería ser elegido por ser el mecanismo más apropiado para establecer, con un menor margen de error, el estado actual del certificado (vale decir, que el certificado no se encuentre revocado).
   - Otra alternativa, siempre disponible, es la descarga de la CRL y constatación de que el certificado no se encuentra en dicha lista. Por el contrario, si dicho certificado se señalara en esta lista implicaría que dicho certificado se encuentra revocado.

     En ambos casos, tanto la respuesta que emite el servidor que atiende las consultas OCSP como la CRL son documentos que presentan firma digital, por lo que se debe validar dicha firma así como al certificado de la autoridad que la realizara con un proceso similar al que se describe acá a partir del punto 1.

4. **Comprobar si el certificado es confiable**. Por defecto un certificado de entidad final por sí mismo no es confiable. Éste hereda la confianza depositada en la autoridad que firmó dicho certificado. Para ello es necesario obtener el certificado digital de la Autoridad Certificadora que firmara el certificado digital materia de verificación de confiabilidad y realizar un proceso similar al descrito acá desde el punto 1. Al realizar esto es muy probable la generación de una cadena de certificados que constituyen la denominada ruta de validación (Path Validation) que debería finalizar en un certificado de confianza probada, generalmente un certificado de Autoridad de Certificación Raíz (Root CA).

Introducción sobre certificados digitales en páginas web:

Las páginas (o sitios) web pueden o no poseer un certificado digital dependiendo del contenido que alberguen y de la finalidad de su sitio web. Así, existen sitios web que no necesitan un certificado digital pues su contenido es puramente informativo y el usuario no interactúa ni ingresa datos (Por ejemplo, un blog, una wiki[3], entre otros).

Pero también existen sitios web que requieren autenticación de usuario, ingreso de datos y password por parte del usuario y estos sitios web si requieren un certificado digital para asegurar al usuario que se trata de un sitio seguro (Por ejemplo, un servidor de correo electrónico, entre otros). Los sitios web que utilizan certificados digitales pueden, además, cifrar su contenido para incrementar la seguridad del usuario y evitar que tercero identifiquen o roben la información que ingresa.

En los diferentes ejemplos presentados se puede observar sitios web que poseen certificados digitales y sitios web que no los poseen.

En el caso particular de **Google Chrome** existen 3 iconos diferentes para indicar el estado del certificado de la página web, o bien la ausencia de certificado como en el caso de Wikipedia o cualquier otro sitio HTTP normal.

Icono	¿Qué significa?
	**El certificado del sitio es válido** y un tercero de confianza ha verificado su identidad.
	**El sitio no ha proporcionado al navegador ningún certificado.** Esto ocurre en los sitios HTTP normales (busca el icono en la barra de direcciones) porque normalmente los certificados solo se proporcionan en los sitios que usan SSL.
	**Google Chrome ha detectado alguna irregularidad en el certificado del sitio.** Debes continuar con cuidado, ya que es posible que el sitio esté suplantando a otro para convencerte de que compartas información personal u otros datos confidenciales.

[3] **Wiki:** es un sitio web cuyas páginas pueden ser editadas por múltiples voluntarios a través del navegador web. Los usuarios pueden crear, modificar o borrar un mismo texto que comparten.

Ejemplo 1: Validar el certificado de un servidor de correos (Gmail) en el navegador Internet Explorer 8

1: En tu página principal de Gmail, hacer click en el ícono del candado que aparece a la derecha de la dirección (en la barra de direcciones).

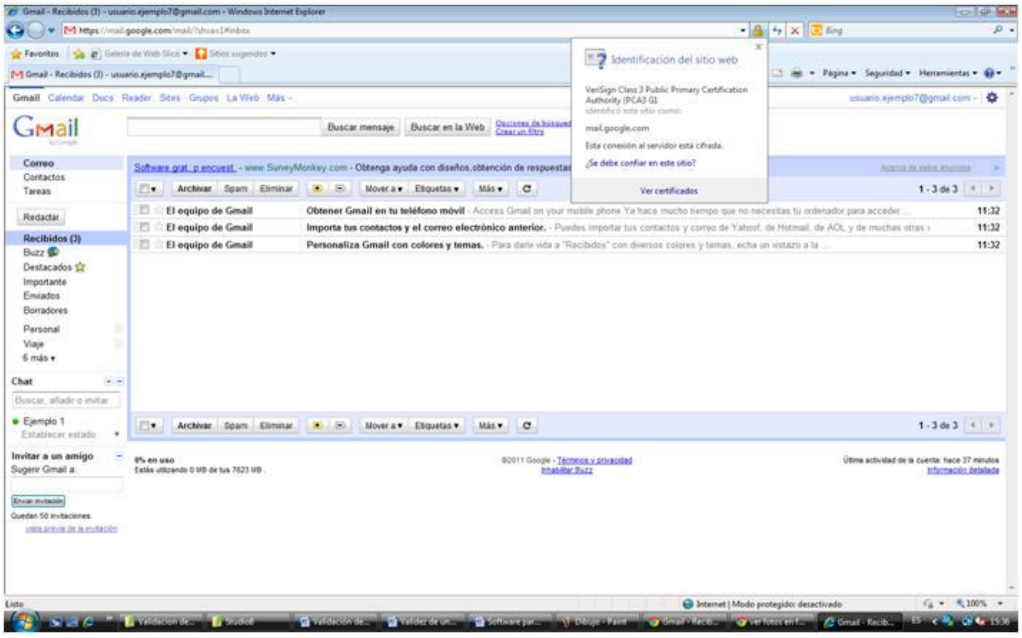


Figura 1. Ventana principal de Gmail

2: Hacer click en “Ver certificados”

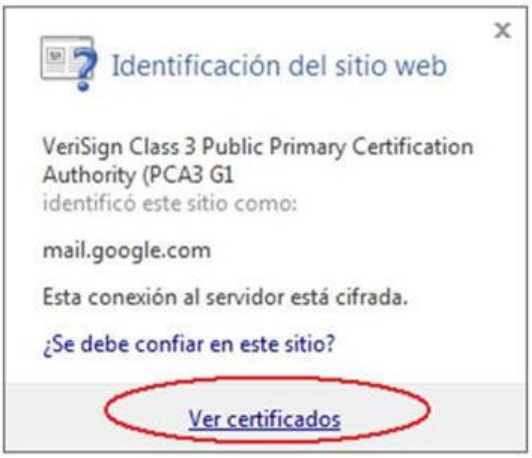


Figura 2. Click en Ver certificados

3: Se abre la ventana que contiene la información del certificado. Aquí se debe verificar la validez mediante los 4 pasos que se detallan a continuación:

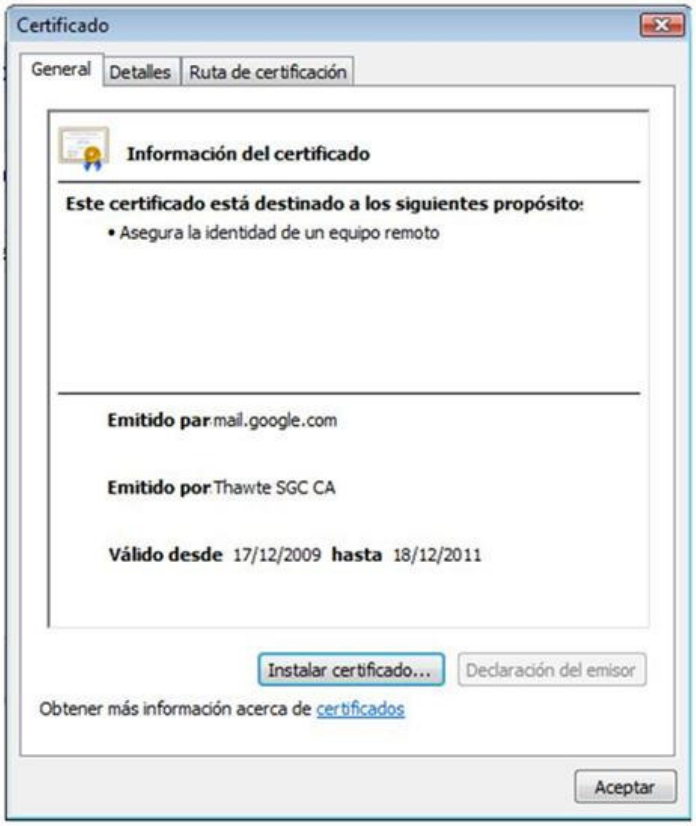


Figura 3. Ventana del certificado

Paso 1 – Integridad: La integridad del certificado digital (que no se haya modificado) es comprobada de manera automática por Internet Explorer. El navegador realiza una comprobación automática utilizando procedimientos tecnológicos, transparentes al usuario, que le permiten conocer si algún tercero ha modificado el sitio web. En caso de algún error o modificación encontrada Internet Explorer indica un error, como se muestra en la figura.

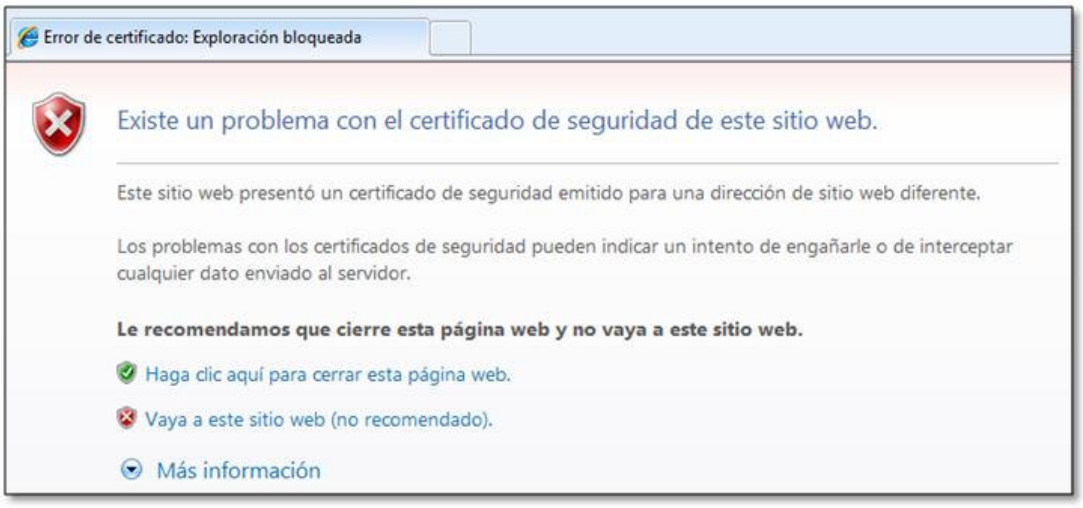


Figura 2 - Error en el certificado digital del sitio web

Paso 2 – Vigencia del certificado: Revisar la fecha de vigencia y contrastarla con la fecha actual. En este ejemplo: la fecha actual es 05/09/2011 y el certificado está vigente entre el 17/12/2009 y el 18/12/2011. Por lo tanto, el certificado se encuentra vigente

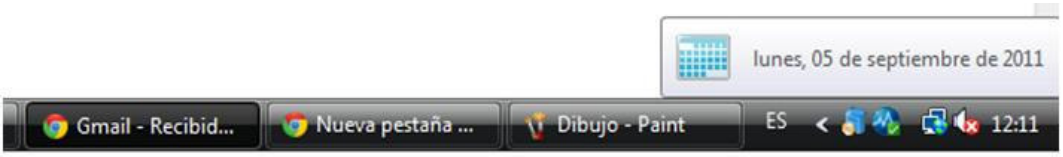


Figura 3. Fecha actual

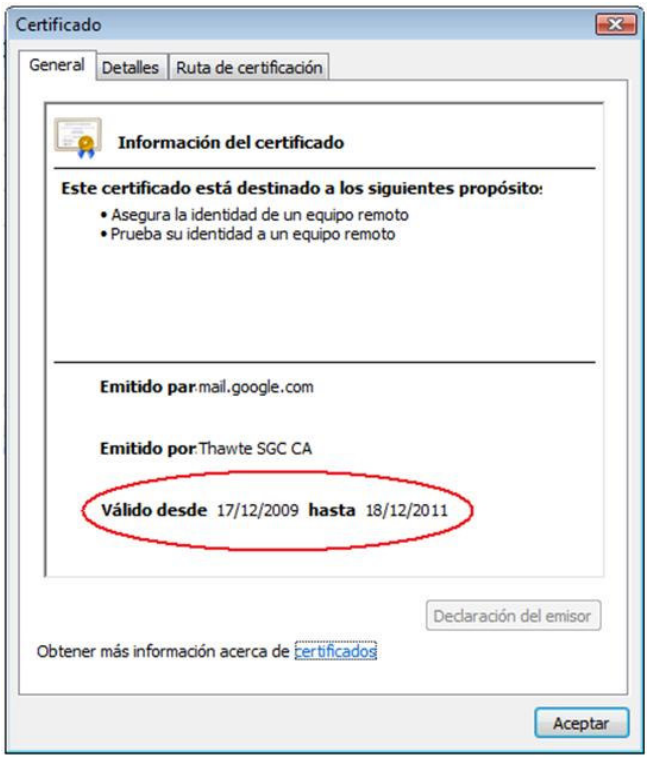
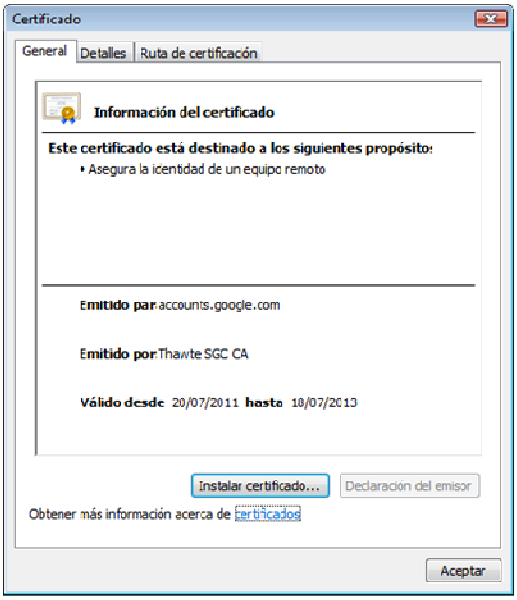


Figura 4. Fecha de validez del certificado

Paso 3 – Comprobar estado:

Mediante CRL: Algunos programas y navegadores permiten comprobar el estado de un certificado mediante CRL de manera automática, que es la más recomendable.

Si usted desea realizarlo manualmente, los pasos se describen a continuación. Seleccionar la pestaña “Detalles”.



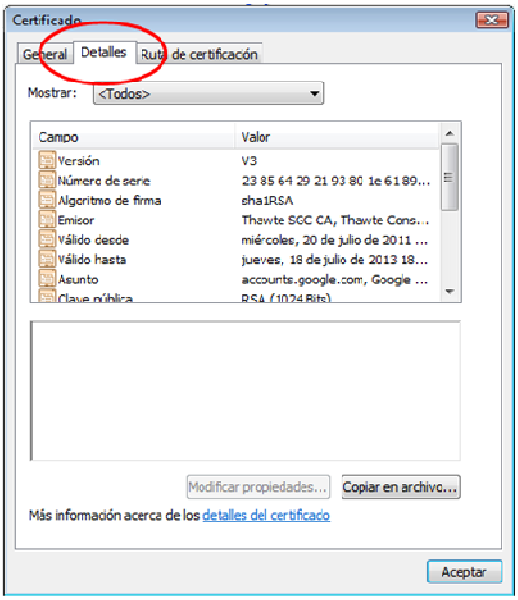


Figura 5. Ventana "Certificado" y pestaña Detalles

Hacer click en el **campo "Número de serie",** el número aparecerá en el cuadro inferior. Se debe seleccionar y copiar (Ctrl+c).

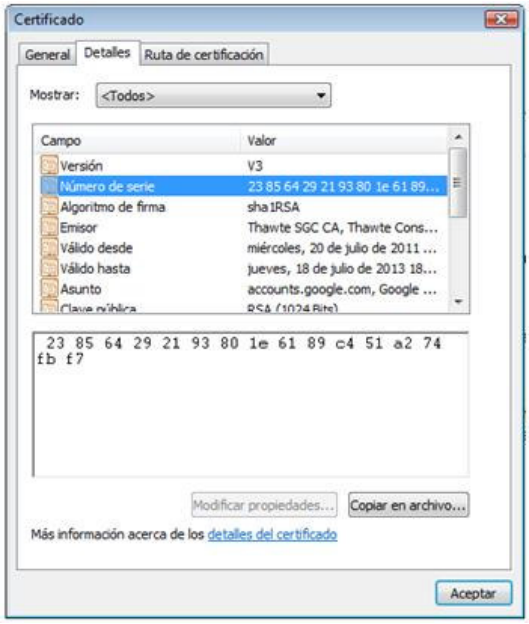


Figura 6. Número de serie del certificado

Abrir un Bloc de notas y pegar (Ctrl+v) el número de serie. Reservar el archivo (bloc de notas) y volver al Internet Explorer.

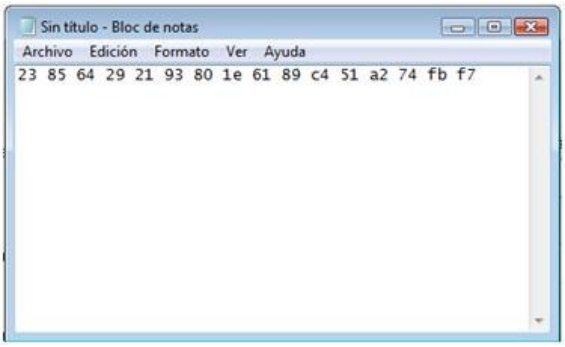


Figura 7. Número de serie del certificado en un bloc de notas

En la ventana "Certificado", pestaña "Detalles", deslizar la barra lateral hacia abajo hasta encontrar el **campo "Puntos de distribución CRL"** y hacer click en él. En el cuadro de abajo aparecerá una ruta URL, copiarla.

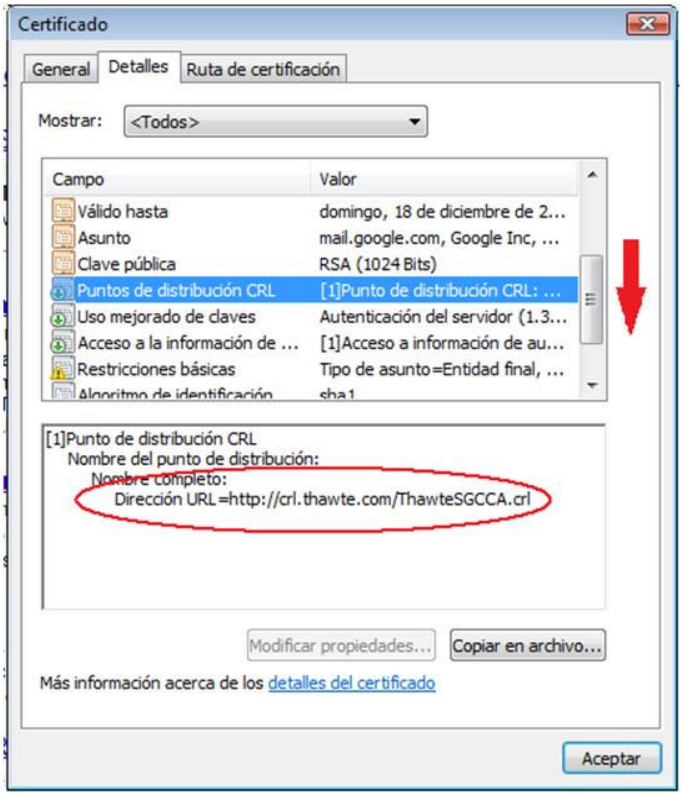


Figura 8. Puntos de distribución CRL

Abrir una nueva ventana de Internet Explorer y pegar la dirección de la CRL y se descargará la CRL actualizada.

Figura 9. Pegar dirección de CRL

En la ventana que aparece, hacer click en Abrir o Guardar, según se requiera.

Figura 10. Descargar CRL

Al abrir el archivo descargado se observa la ventana de “Lista de revocación de certificados”

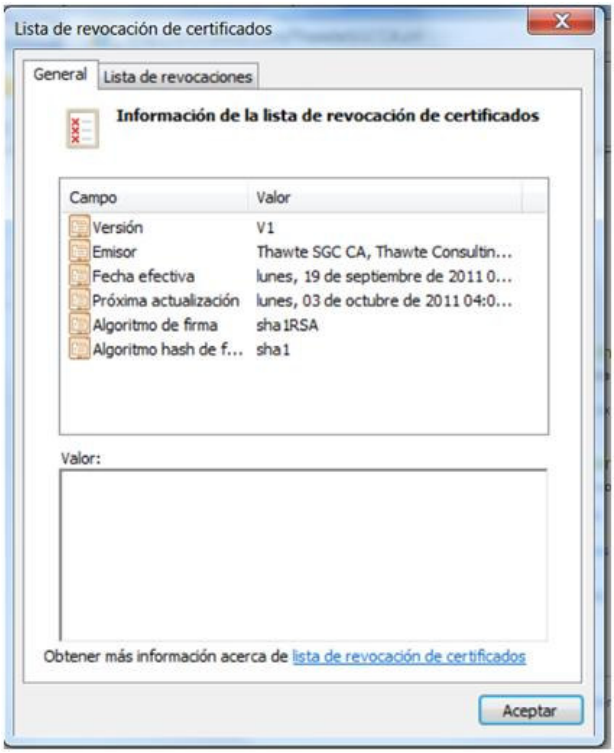


Figura 11. Ventana "Lista de revocación de certificados"

Hacer click en la pestaña “Lista de revocaciones”.

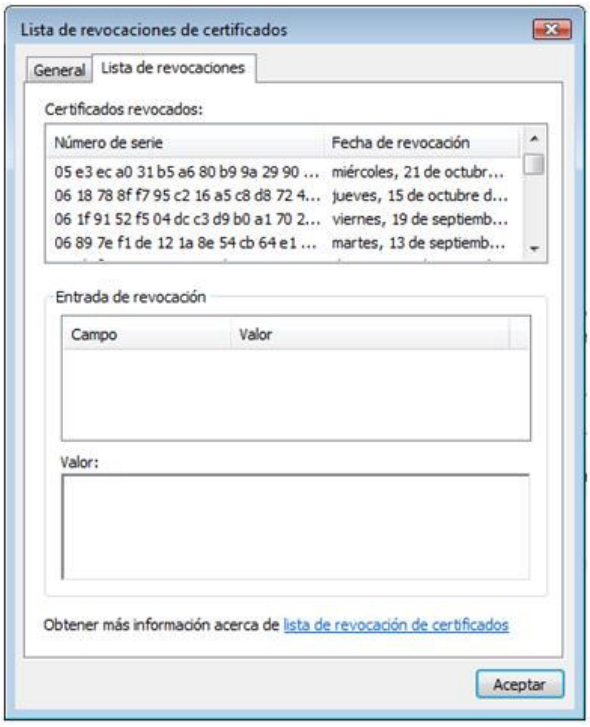


Figura 12 - Pestaña "Lista de revocaciones"

Buscar en esa lista el número de serie del certificado digital (el número que se copio en el bloc de notas). En este caso, se verificó que el número de serie del certificado no se encuentra en la CRL descargada, lo cual significa entonces que el certificado materia de verificación no se encuentra revocado.

NOTA 1:

Es importante recalcar, nuevamente, que este es un proceso engorroso y muy probable de fallar cuando se realiza de manera manual. Es preferible que el navegador o programa lo realice de manera automática.

NOTA 2:

Es importante verificar que la CRL haya sido emitida por una entidad válida. Para verificar el emisor de la CRL se debe hacer click en la pestaña “General” de la ventana “Lista de revocación de certificado” y buscar el **campo “Emisor”.**

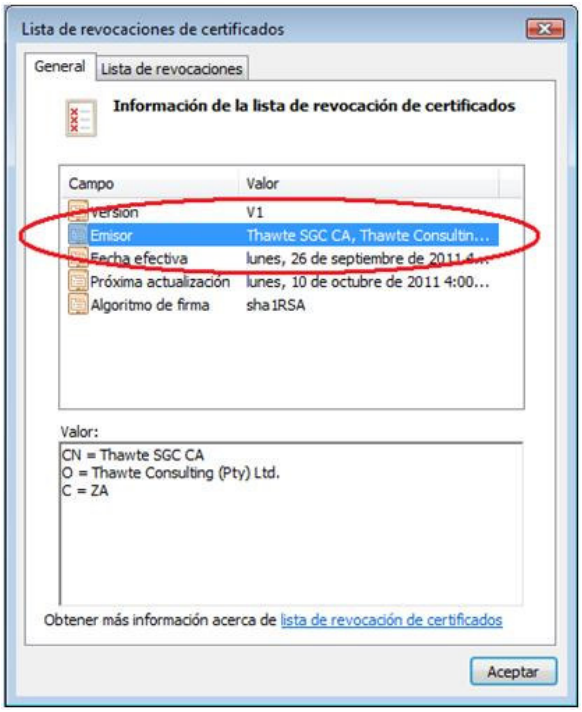


Figura 13. Emisor de la CRL

Paso 4 – Verificar la ruta de certificación: Hacer click en la pestaña "Ruta de Certificación" que se encuentra en la misma ventana **"Certificado"**.

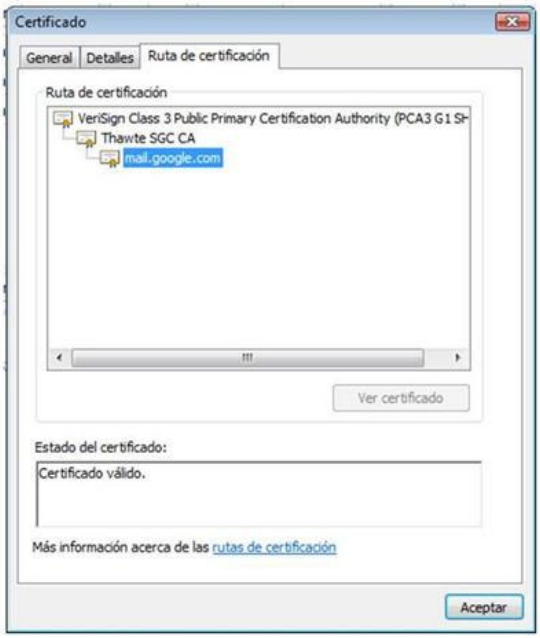


Figura 9. Ruta de Certificación

Para cada uno de los certificados en la ruta se debe verificar su validez, siguiendo el proceso de 4 pasos hasta completar todos los certificados de la ruta de certificación.

Ejemplo 2: Validar el certificado de un servidor de correos (Gmail) en el navegador Mozilla Firefox

1: En su página principal de Gmail, hacer click a la derecha de la dirección (en la barra de direcciones), como se indica en la figura. Hacer click en el botón "Más información…"

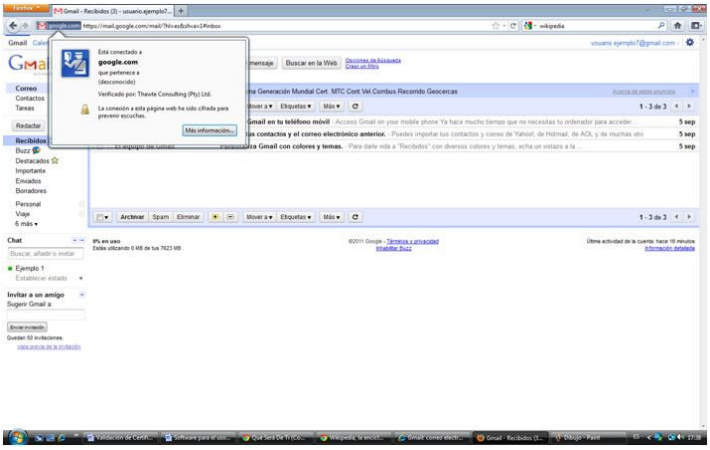


Figura 14. Página principal de Gmail en Mozila Firefox

2: En la ventana que aparece, hacer click en "Ver certificados"

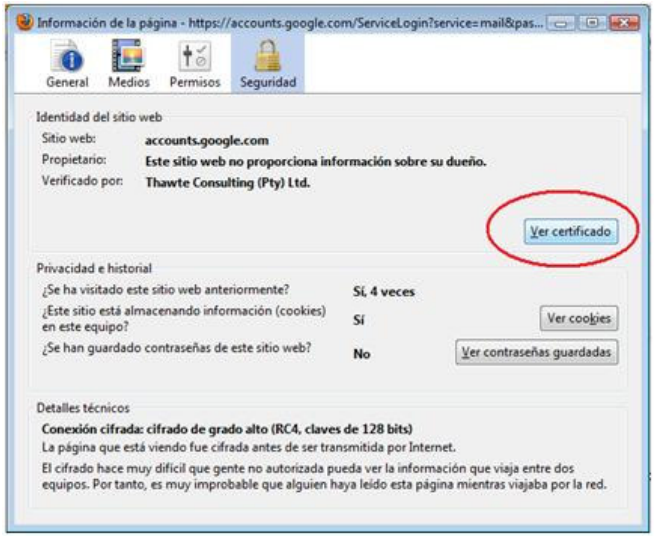


Figura 15. Hacer click en ver certificados

3: Realizar la verificación del certificado siguiendo los 4 pasos indicados anteriormente.

Paso 1 – Integridad:

La integridad del certificado digital (que no se haya modificado) es comprobada de manera automática por Mozilla Firefox. El navegador realiza una comprobación automática utilizando procedimientos tecnológicos, transparentes al usuario, que le

permiten conocer si algún tercero ha modificado el sitio web. En caso de algún error o modificación encontrada Mozilla Firefox indica un error, como se muestra en la figura.

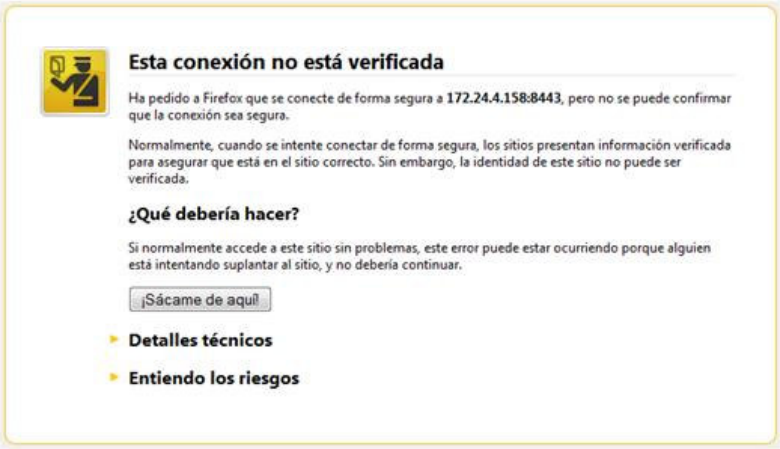


Figura 16. Error encontrado en certificado digital por Mozilla Firefox

Paso 2 – Vigencia del certificado: Revisar la fecha de vigencia y contrastarla con la fecha actual. En este ejemplo: la fecha actual es 07/09/2011 y el certificado está vigente entre el 17/12/2009 y el 18/12/2011. Por lo tanto, el certificado se encuentra vigente. En la ventana "Visor de certificados", verificar la fecha de validez.

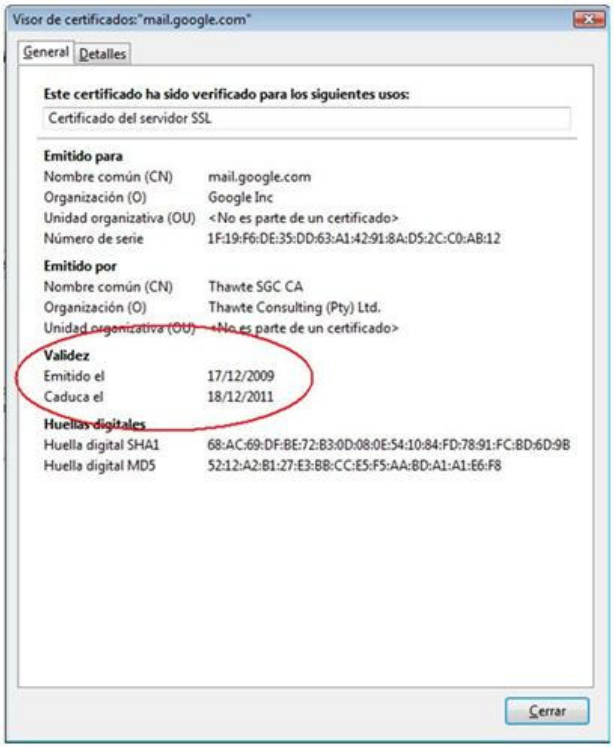


Figura 17. Ventana del certificado

Se comprueba, revisando la fecha del equipo (PC), que el certificado se encuentra dentro del periodo de validez

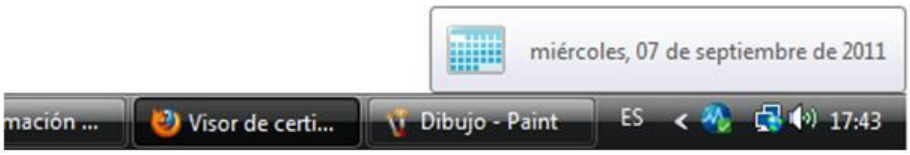


Figura 18. Fecha actual de la PC

Paso 3 – Comprobar estado:

Mediante CRL: Mozilla Firefox permiten comprobar el estado de un certificado mediante CRL de manera automática, que es la más recomendable. A continuación se explican los pasos para configurar la verificación automática del esta de un certificado en la CRL.

Hacer click en la pestaña “Detalles” que se encuentra en la ventana “Visor de certificados”.

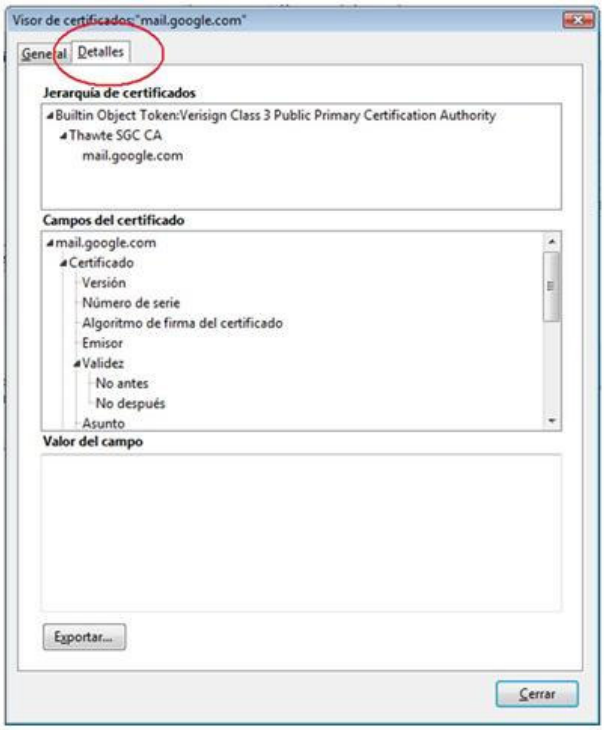


Figura 19. Pestaña Detalles

Desplazar la barra lateral hacia abajo hasta encontrar el campo: "**Punto de distribución de CRL**".

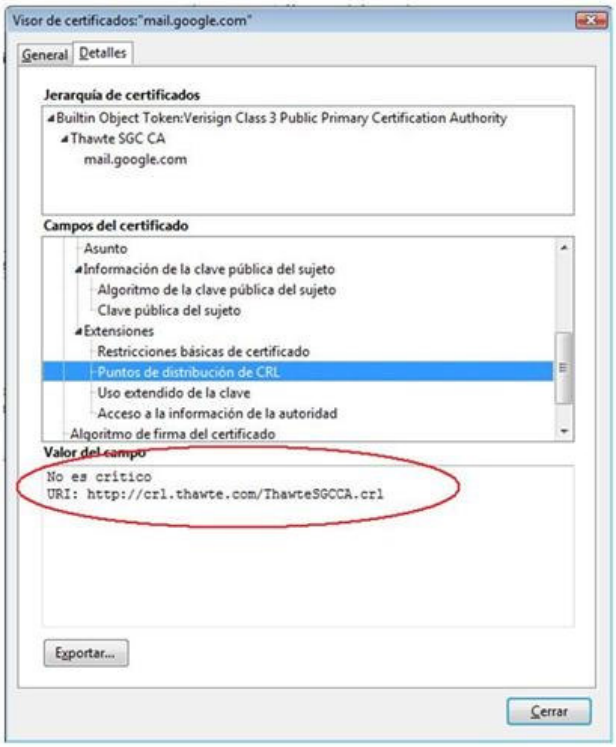


Figura 20. Punto de distribución de CRL

Copiar y pegar la dirección del punto de distribución de CRL en una pestaña nueva. Presionar ENTER.

Figura 21. Abrir CRL

En la ventana que aparece se indica la fecha de la próxima actualización de la CRL. Si desea que su navegador descargue automáticamente las actualizaciones de la CRL presione en botón **"Sí"**. Se observa el nombre del emisor de la CRL, el que debe ser verificado como confiable.

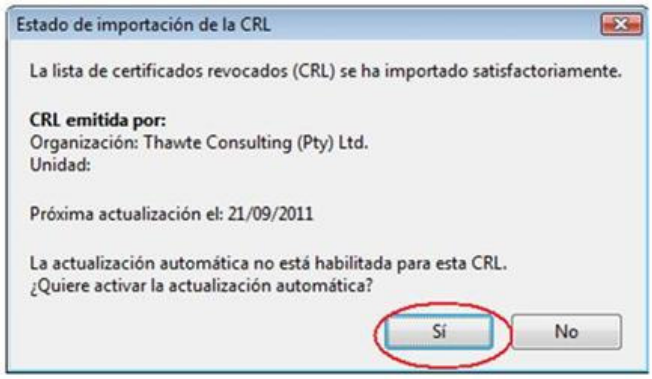


Figura 22. Descarga automática de CRL

Puede configurar sus preferencias en la siguiente ventana que muestra dos opciones de actualización de CRL.

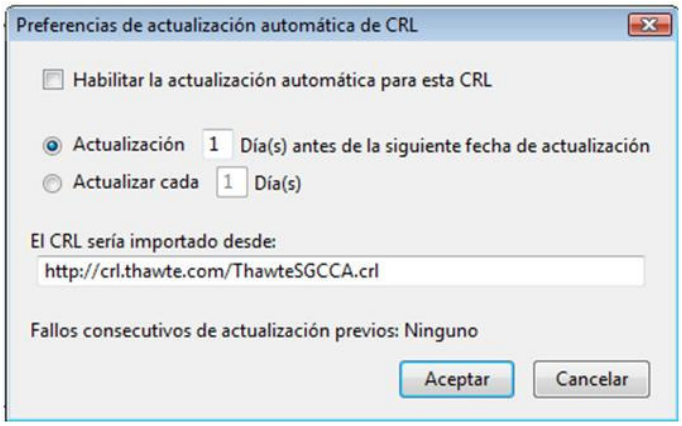


Figura 23. Preferencias de actualización de CRL

Paso 4 – Verificar la ruta de certificación: Regresando a la ventana del certificado denominada **"Visor de certificados"** se puede observar en la pestaña **"Detalles"** una sección llamada **"Jerarquía de certificados"**. En otras palabras, es el nombre que Mozilla Firefox atribuye a la ruta de certificación del certificado consultado.

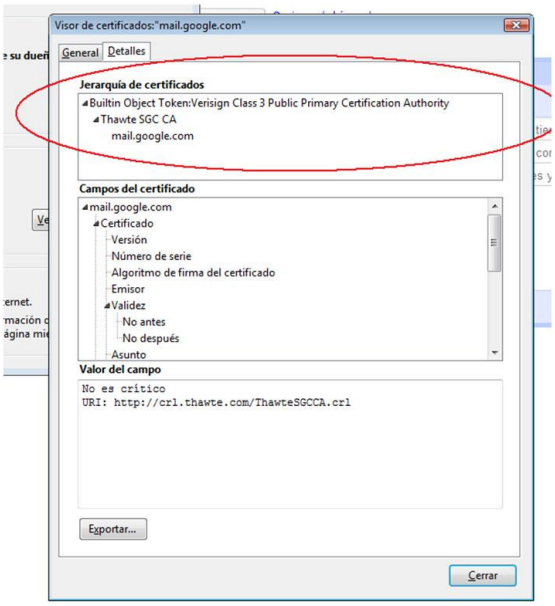


Figura 24. Ruta de certificación

Haciendo click en cualquiera de los certificados de la jerarquía o ruta de certificación, se puede observar sus campos en el cuadro inferior denominado **"Campos del certificado"**.

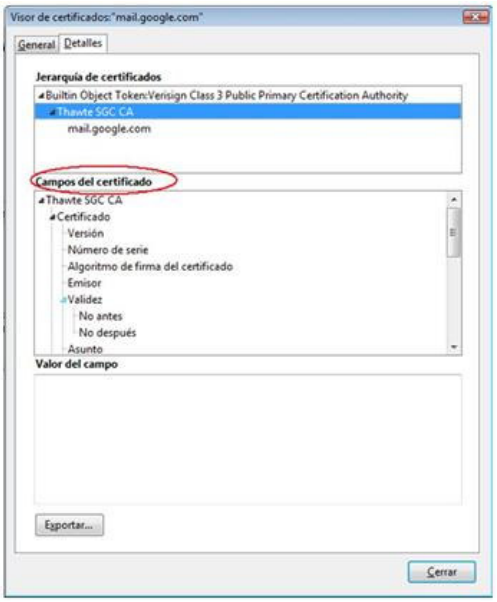


Figura 25. Campos de los certificados de la jerarquía

Ejemplo 3: Validar el certificado de un servidor de correos (Gmail) en el navegador Google Chrome 13

1: En tu página principal de Gmail

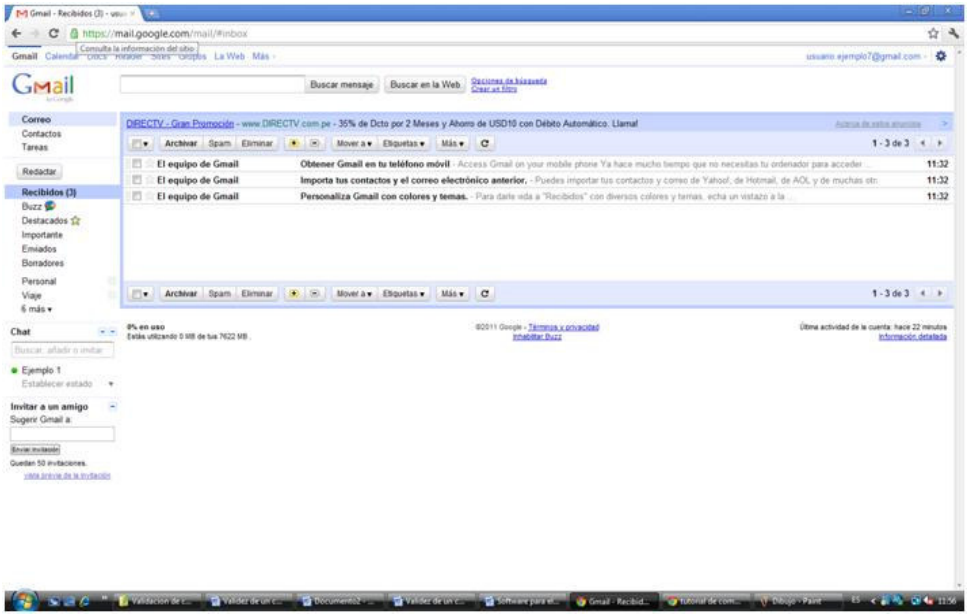


Figura 4. Gmail: Bandeja de entrada

2: Hacer click en el icono del candado que aparece a la izquierda de la dirección (en la barra de direcciones)

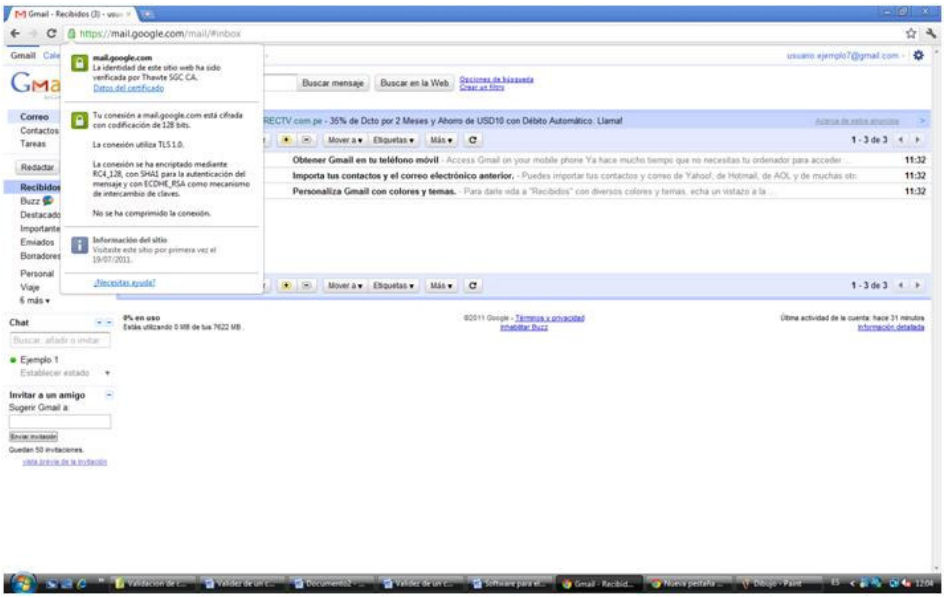


Figura 5. Click en el ícono del candado

3: Hacer click en **“Datos del certificado”**.

Figura 26. Click en “Datos del certificado”

Realizar la verificación del certificado siguiendo los 4 pasos indicados anteriormente.

Paso 1 – Integridad: La integridad del certificado digital (que no se haya modificado) es comprobada de manera automática por Google Chrome. El navegador realiza una comprobación automática utilizando procedimientos tecnológicos, transparentes al usuario, que le permiten conocer si algún tercero ha modificado el sitio web. En caso de algún error o modificación encontrada Google Chrome indica un error, como se muestra en la figura.

Figura 27. Error en el certificado del sitio web mostrado por Google Chrome

Paso 2 – Vigencia del certificado: Revisar la fecha de vigencia y contrastarla con la fecha actual. En este ejemplo: la fecha actual es 05/09/2011 y el certificado está vigente entre el 17/12/2009 y el 18/12/2011. Por lo tanto, el certificado se encuentra vigente.

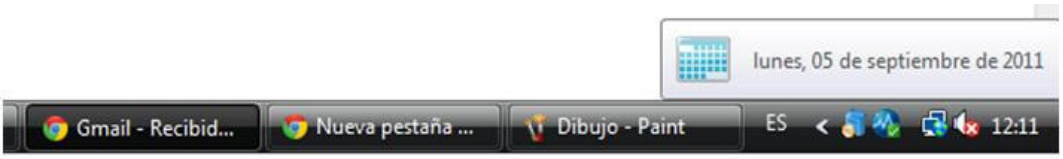


Figura 28. Fecha actual

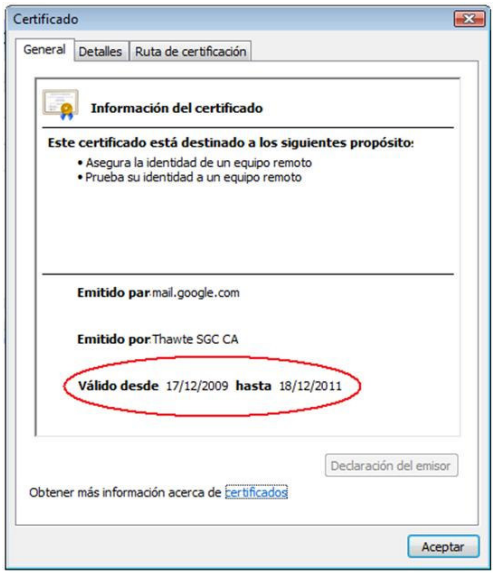


Figura 29. Ventana del certificado

Paso 3 – Comprobar estado:

- Mediante CRL. Algunos programas y navegadores permiten comprobar el estado de un certificado mediante CRL de manera automática, que es la más recomendable.
- Si usted desea realizarlo manualmente, los pasos se describen a continuación.

Hacer click en el **campo "Número de serie",** el número aparecerá en el cuadro inferior. Se debe seleccionar y copiar (Ctrl+c).

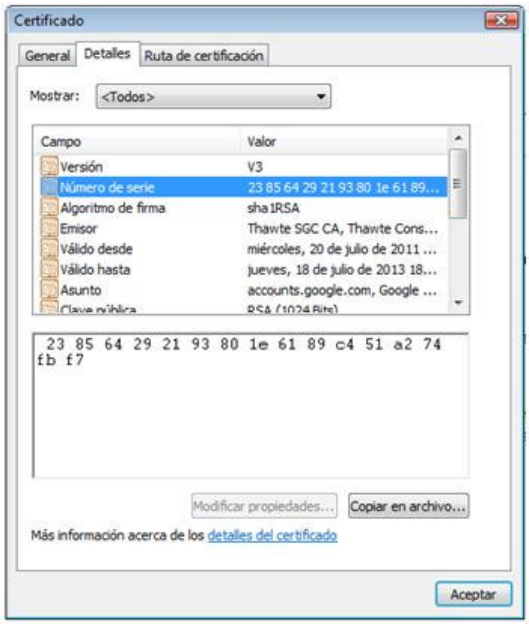


Figura 30. Número de serie del certificado

Abrir un Bloc de notas y pegar (Ctrl+v) el número de serie. Reservar el archivo (bloc de notas) y volver al Internet Explorer.

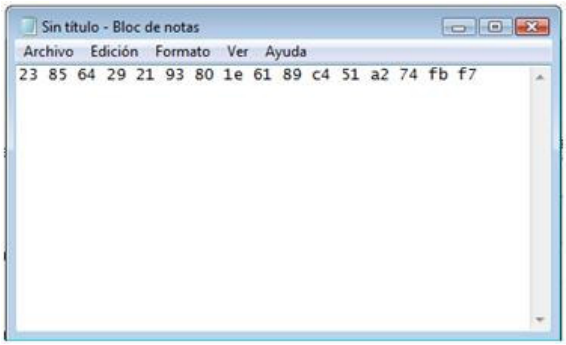


Figura 31. Número de serie del certificado en un bloc de notas

En la ventana "Certificado", pestaña "Detalles", deslizar la barra lateral hacia abajo hasta encontrar el **campo "Puntos de distribución CRL"** y hacer click en él. En el cuadro de abajo aparecerá una ruta URL, copiarla.

Seleccionar la pestaña "Detalles".

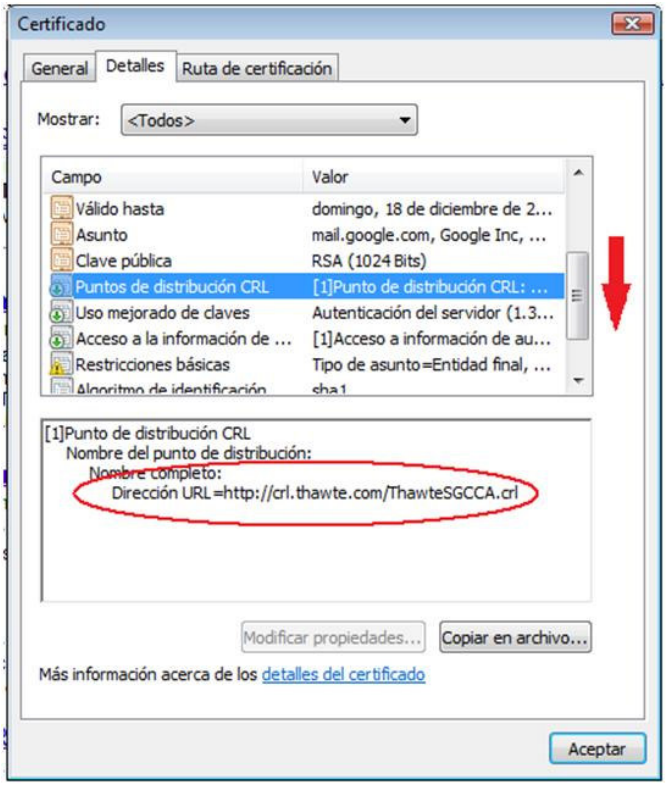


Figura 32. Detalles del Certificado

Deslizar la barra lateral hacia abajo hasta encontrar el campo **"Puntos de distribución CRL"** y hacer click en él. En el cuadro de abajo aparecerá una ruta URL, la cual debe ser copiada.

Abrir una nueva ventana de Google Chrome y pegar la dirección de la CRL.

Figura 33. Pegar dirección de CRL

Se descargará la CRL actualizada.

Figura 34. CRL descargada

Hacer click en el archivo descargado para abrir la ventana “Lista de revocaciones de certificados”.

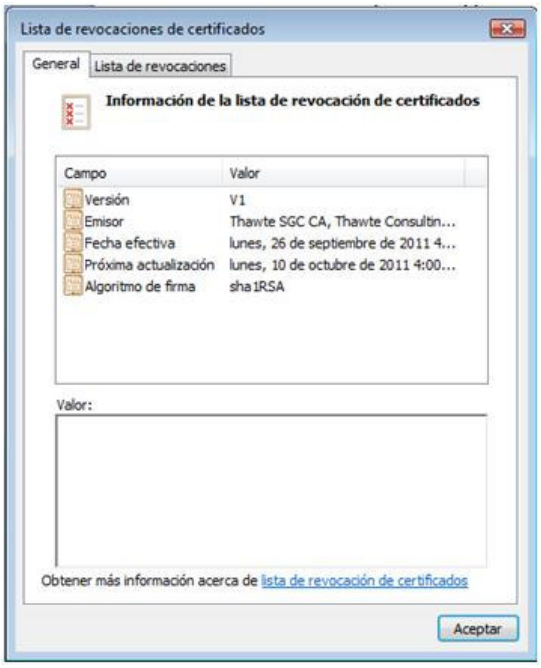


Figura 35. Ventana "Lista de revocaciones de certificados"

Hacer click en la pestaña “Lista de revocaciones”.

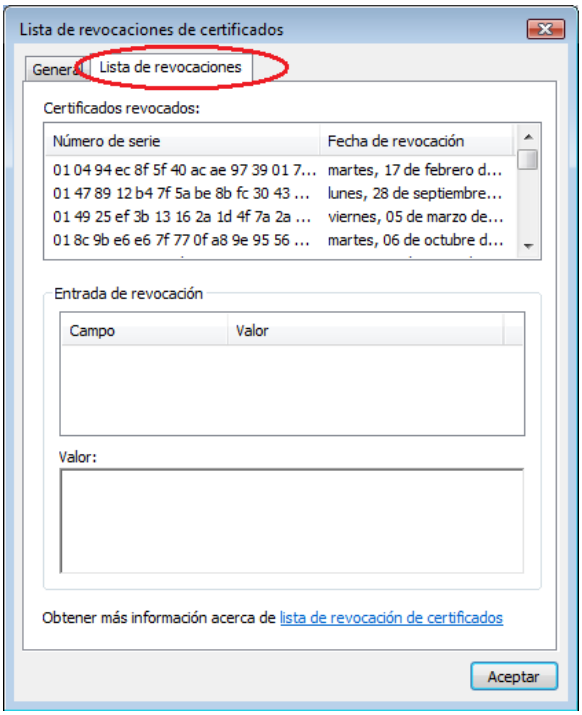


Figura 36. Pestaña "Lista de revocaciones"

Buscar el número de serie del certificado a ser verificado (que ha sido anotado o registrado en un bloc de notas) en la CRL recientemente descargada. En este caso, se verificó que el número de serie del certificado no se encuentra en la CRL descargada.

NOTA 1:
Es importante recalcar, nuevamente, que este es un proceso engorroso y muy probable de fallar cuando se realiza de manera manual. Es preferible que el navegador o programa lo realice de manera automática.

NOTA 2:
Es importante verificar que la CRL haya sido emitida por una entidad válida. Para verificar el emisor de la CRL se debe hacer click en la pestaña "General" de la ventana "Lista de revocación de certificado" y buscar el **campo "Emisor".**

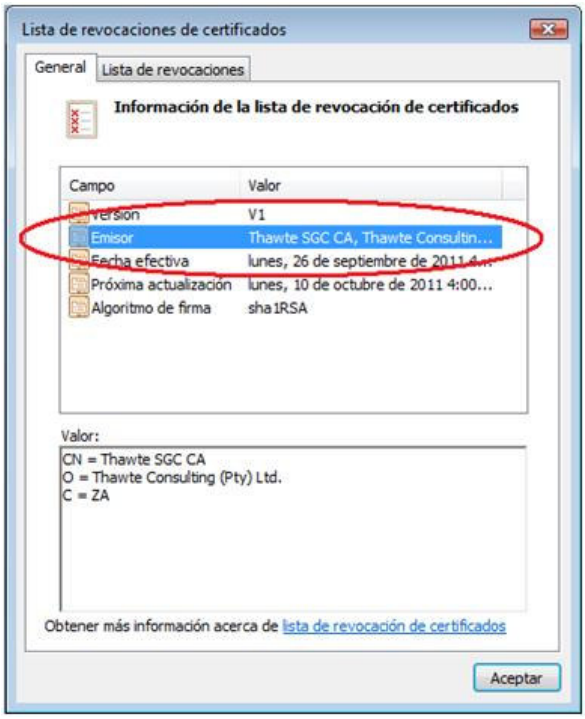


Figura 37. Emisor de la CRL

Paso 4 – Verificar la ruta de certificación: Hacer click en la pestaña "Ruta de Certificación"

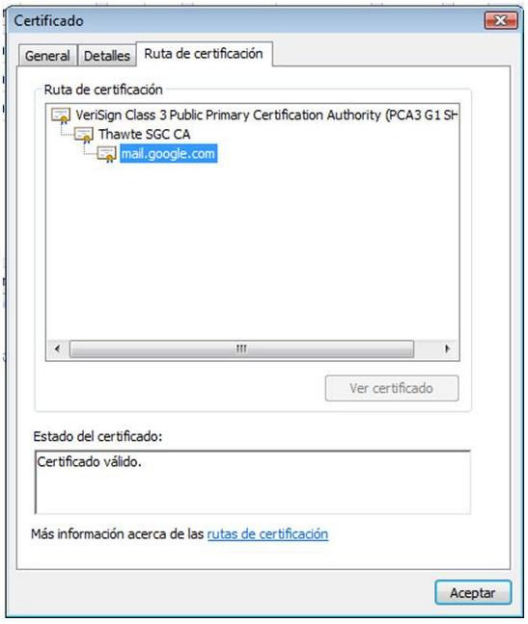


Figura 38. Ruta de Certificación

Para cada uno de los certificados en la ruta se debe verificar su validez, siguiendo el proceso de 4 pasos hasta completar todos los certificados de la ruta de certificación.

Ejemplo 4: Validar el certificado de una página web cualquiera, por ejemplo: http://es.wikipedia.org en el navegador Google Chrome.

1: Ingresar a la página principal de Wikipedia en español

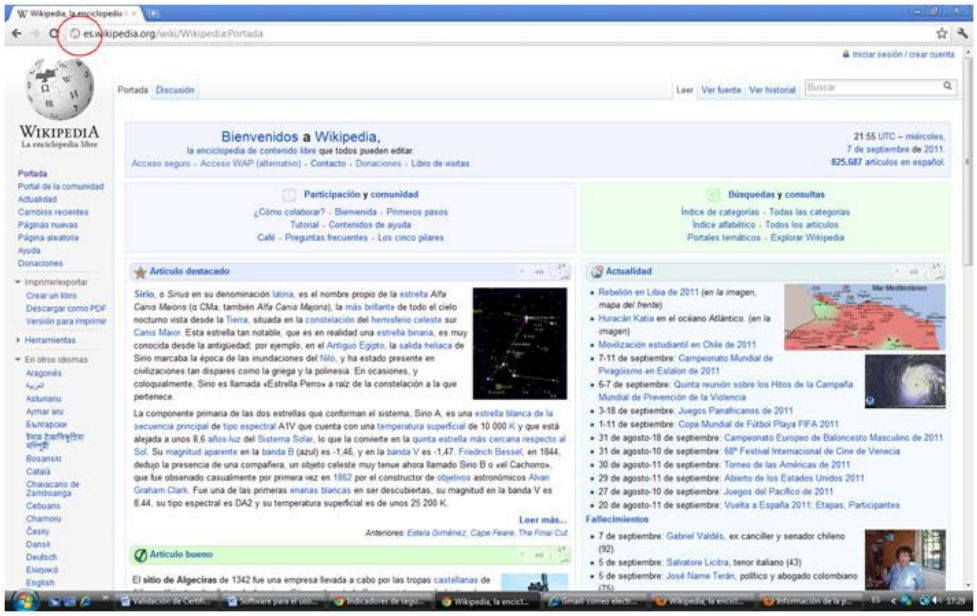


Figura 39. Página principal de Wikipedia en Español

2: Hacer click en el icono que se encuentra a la izquierda de la dirección URL en la barra de direcciones.

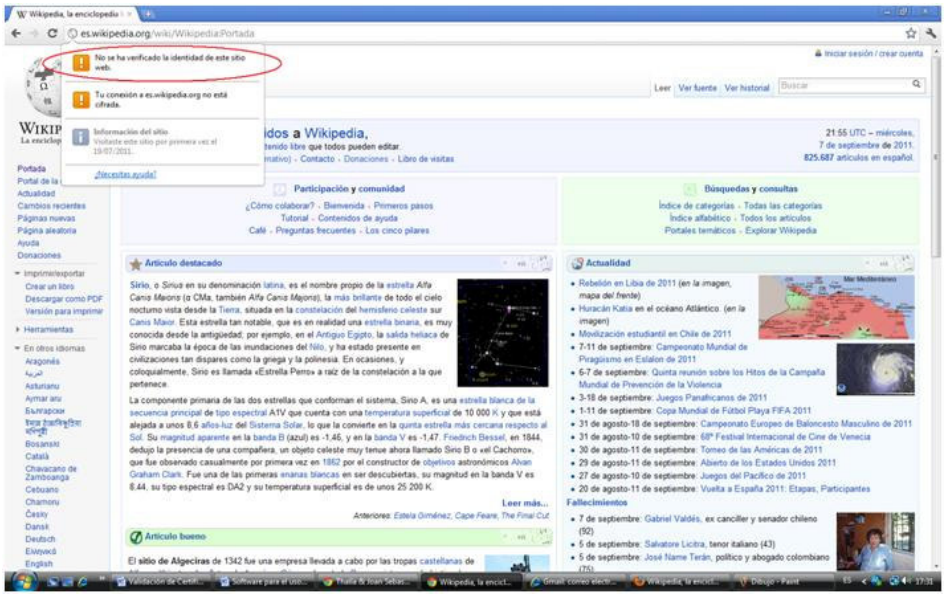


Figura 40. Comprobar certificado

Se puede observar un mensaje que dice: ***"No se ha verificado la identidad de este sitio web"***. Esto quiere decir que dicha página web no posee certificado digital alguno. Algunas páginas web no necesitan conexiones seguras ni certificados digitales pues su contenido es puramente informativo y no es necesario ingresar datos de usuario o contraseñas.

Ejemplo 5: Verificar el certificado de un mensaje de correo electrónico firmado en Microsoft Office Outlook 2007

1: En la Bandeja de entrada de Outlook se observa un correo nuevo con el icono , indicando que el mensaje contiene una firma digital.

2: Hacer doble click para abrir el mensaje.

3: Una vez abierto el mensaje, hacer click en el icono , que se encuentra a la derecha.

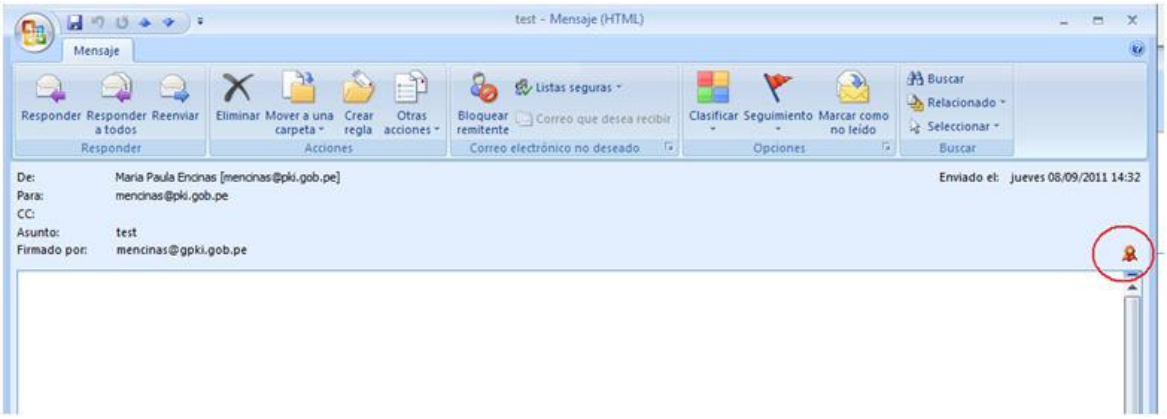


Figura 41. Mensaje firmado

3: Se abrirá la siguiente ventana.

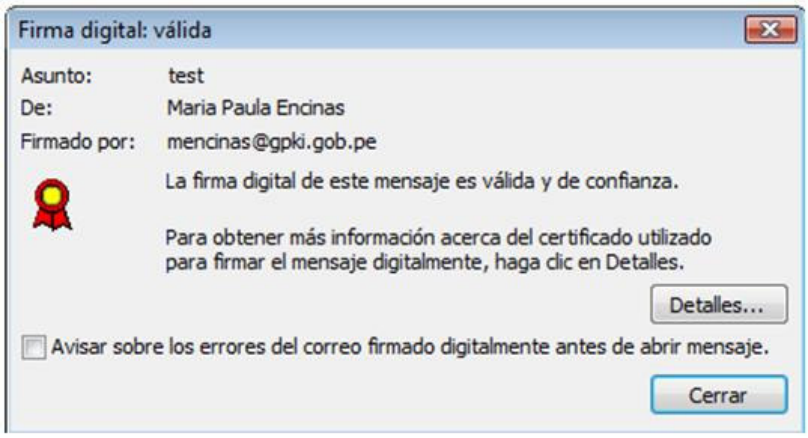


Figura 42. Ventana de firma digital

4: Al presionar el botón “Detalles” de la ventana “Firma Digital” que se muestra en la imagen anterior, se encuentra la siguiente pantalla

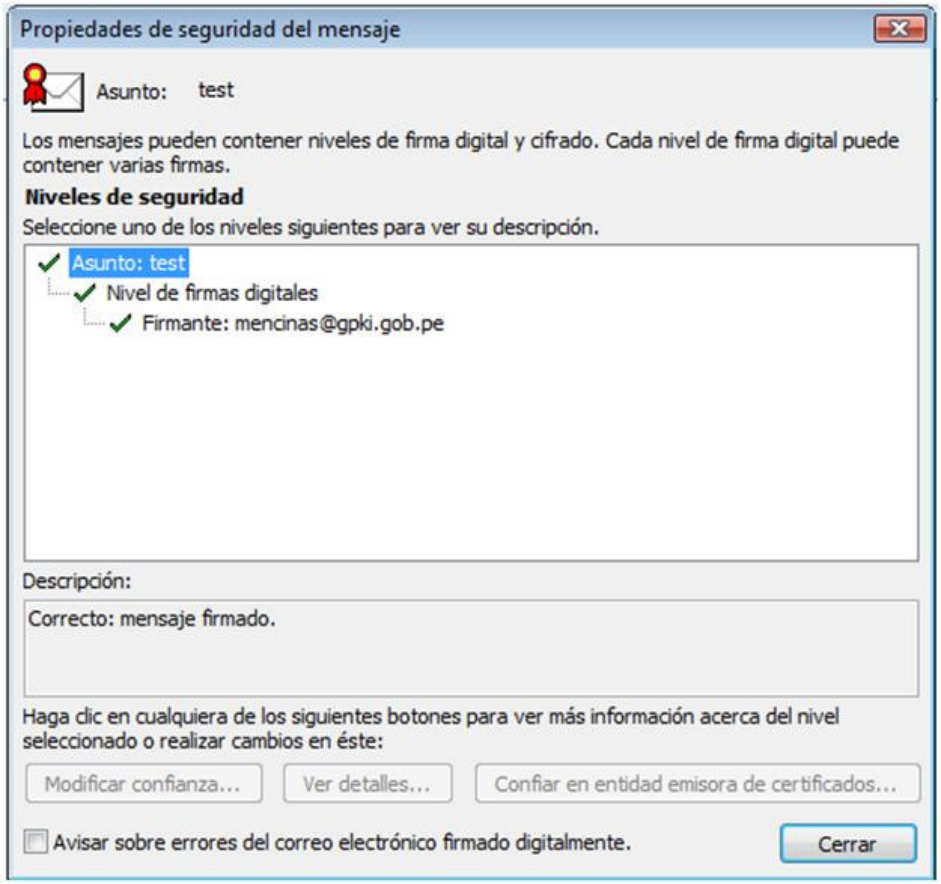


Figura 43. Detalles de la firma

5: Hace click en el nivel “Firmante” y luego en el botón “Ver detalles”

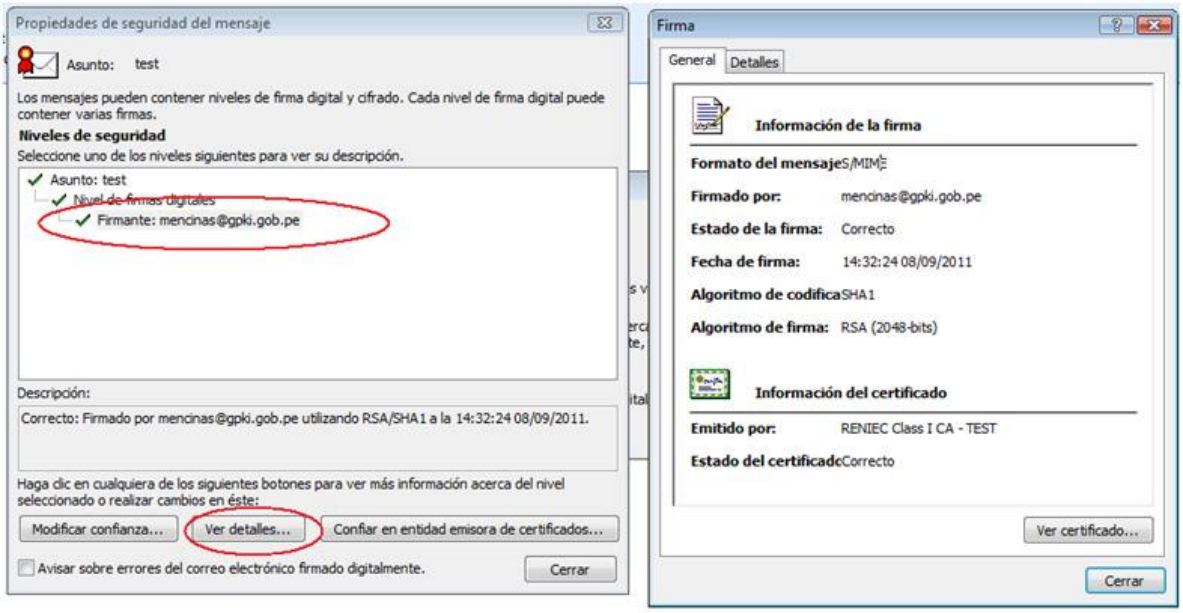


Figura 44. Certificado de la firma

6: La ventana de **"Firma"** contiene información del firmante y del certificado que respalda esta firma. Hacer click en el botón "Ver certificado" para mayor detalle. En la ventana que aparece se encuentra toda la información del certificado.

7: Realizar la verificación del certificado siguiendo los 4 pasos indicados anteriormente.

Paso 1 – Integridad: Comprobado de manera automática por Outlook, de lo contrario se indicaría un error.

Paso 2 – Vigencia del certificado: Revisar la fecha de vigencia y contrastarla con la fecha actual. En este ejemplo: la fecha actual es 26/09/2011 y el certificado está vigente entre el 08/09/2011 y el 07/09/2012. Por lo tanto, el certificado se encuentra vigente.

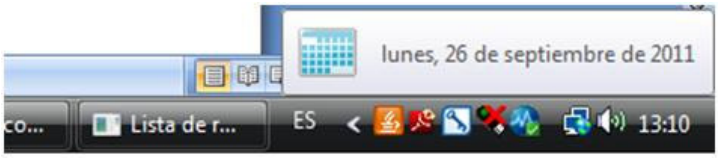


Figura 45. Fecha actual

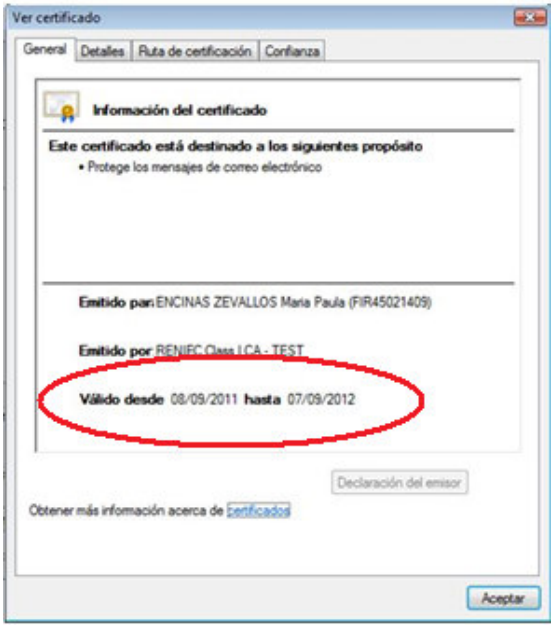


Figura 46. Periodo de validez del certificado

La pestaña “Detalles” contiene la información de todos los campos del certificado así como los puntos de distribución de CRL.

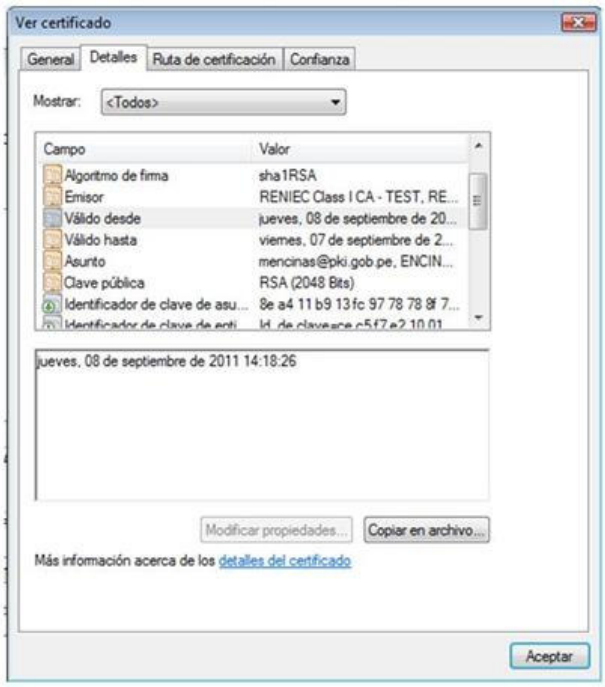


Figura 47. Pestaña Detalles

Paso 3 – Comprobar estado:

Mediante CRL. Algunos programas permiten comprobar el estado de un certificado mediante CRL de manera automática, que es la forma más recomendable.

De forma manual: A continuación se explican los pasos para realizar este tipo de verificación.

En la ventana “Ver Certificado” hacer click en la pestaña “Detalles” y buscar el campo “Número de serie”.

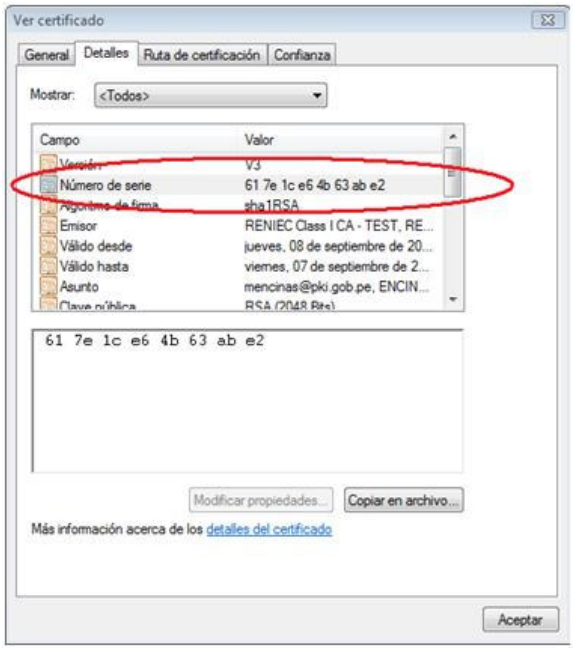


Figura 48. Número de serie del certificado

Se debe seleccionar y copiar (Ctrl+c). Abrir un Bloc de notas y pegar (Ctrl+v) el número de serie. Reservar el archivo (bloc de notas) y volver al Internet Explorer.

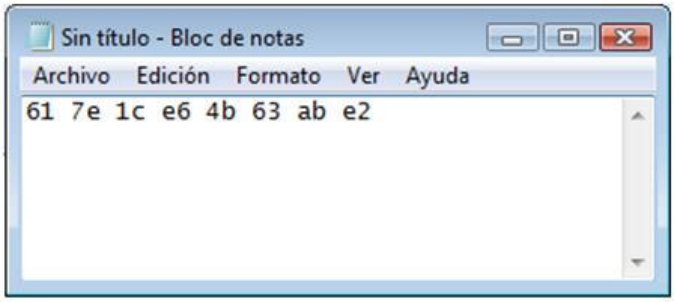


Figura 49. Número de serie del certificado

Hacer click en la pestaña Detalles de la ventana del certificado y buscar el campo "Puntos de distribución de CRL".

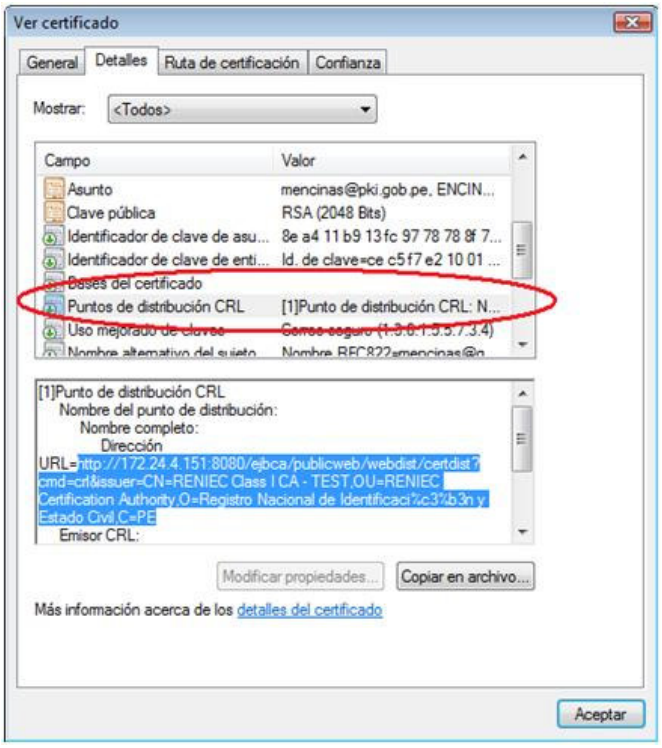


Figura 50. Puntos de distribución CRL

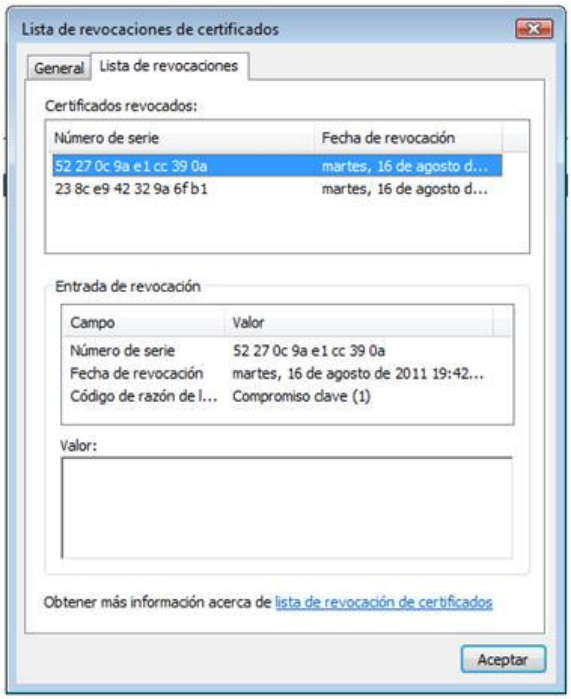
Copiar y pegar la dirección URL en la ventana de un navegador de Internet (en este caso se utilizó Internet Explorer)

Figura 51. URI de CRL

Figura 52. Descargar CRL

Buscar el número de serie (que se encuentra en el bloc de notas) en la CRL recientemente descargada. En este caso, se verificó que el número de serie del certificado no se encuentra en la CRL descargada.

Es importante recalcar, nuevamente, que este es un proceso engorroso y muy probable de fallar cuando se realiza de manera manual. Es preferible que el navegador o programa lo realice de manera automática.



Paso 4 – Verificar la ruta de certificación: La pestaña "Ruta de certificación" contiene todos los certificados de la ruta. Es importante verificar que se confía en todos los certificados de la ruta, para llegar a la conclusión que el certificado que respalda la firma digital contenida en el mensaje de correo electrónico es confiable.

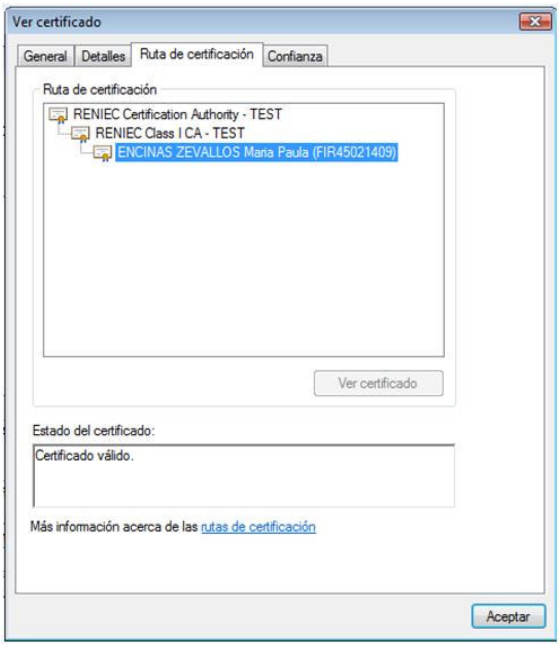


Figura 53. Pestaña Ruta de Certificación

Ejemplo 6: Verificar el certificado de firma digital de un archivo .pdf utilizando Adobe Reader 10

1: Abrir el documento .pdf con Adobe Reader 10. Si el documento presenta una firma digital aparecerá un sello como el que se ve en la Figura 42. Hacer click para ver los detalles de la firma.

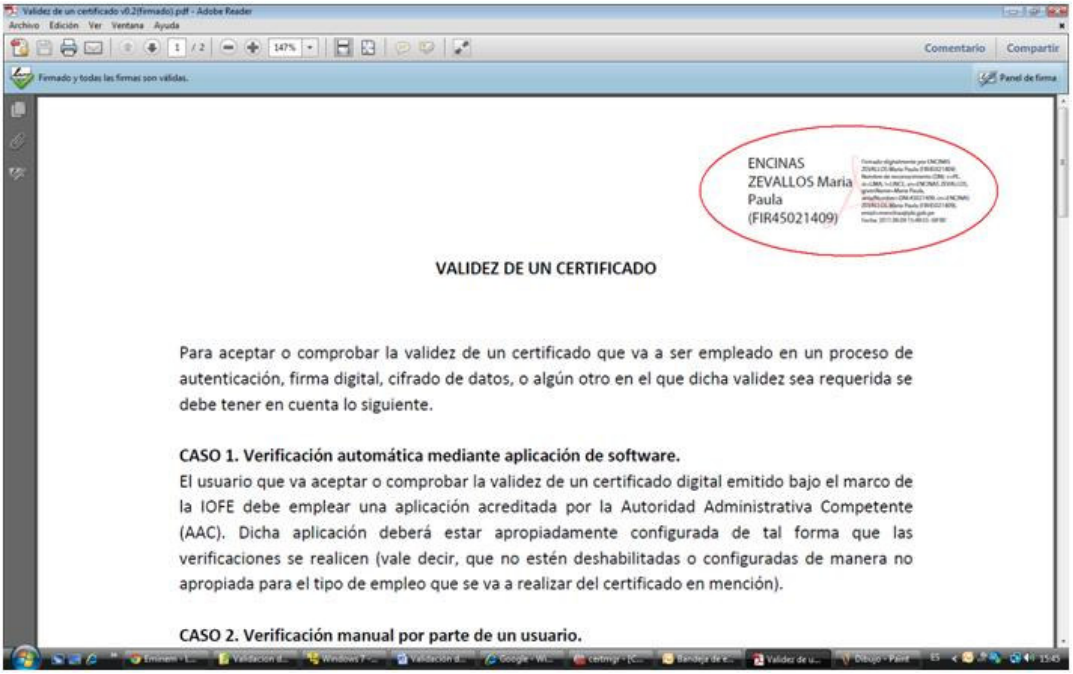


Figura 54. Documento .pdf firmado digitalmente

2: Realizar la verificación del certificado siguiendo los 4 pasos indicados anteriormente.

Paso 1 – Integridad: Comprobado de manera automática por Adobe Reader. Aparecerá una ventana indicando que Adobe Acrobat reconoce como válida o no válida a la firma incluida en el documento. En este caso, se verifica la integridad pues la ventana indica que no ha habido modificaciones en el documento desde que se firmó.

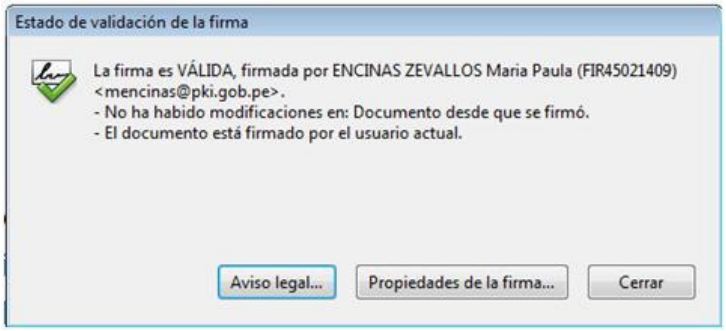


Figura 55. Estado de la firma

Adobe Acrobat resume una serie de condiciones por las cuales considera a esa firma digital como válida. Sin embargo, como se indicó anteriormente, es preferible asegurarse que los certificados asociados a la firma son realmente confiables y no han sido erróneamente declarados como confiables por un tercero. Hacer click en "Mostrar certificado…"

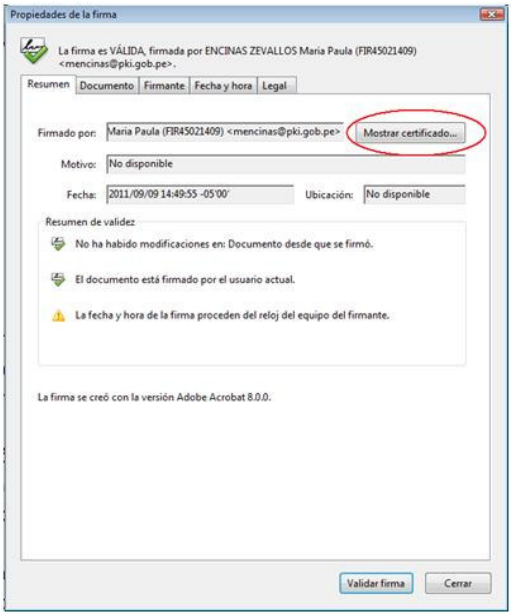


Figura 56. Certificado de la firma

Paso 2 – **Vigencia del certificado:** Revisar la fecha de vigencia y contrastarla con la fecha actual.

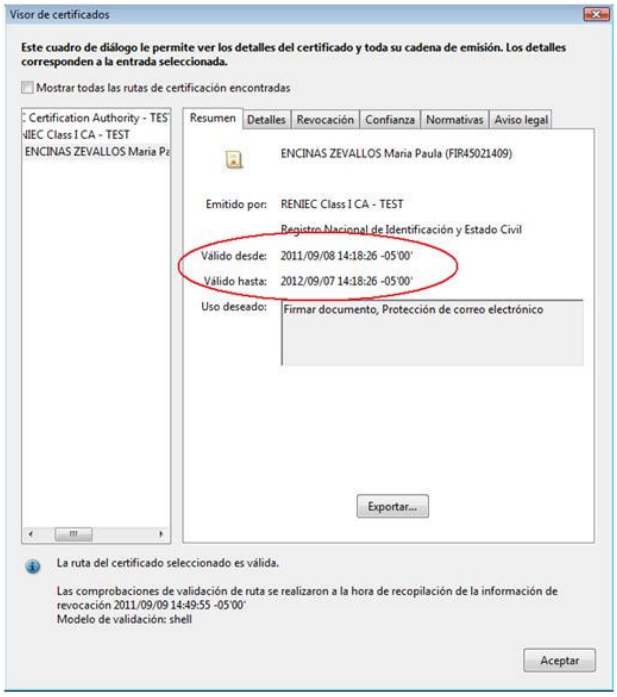


Figura 57. Periodo de validez del certificado

En este ejemplo: la fecha actual es 09/09/2011 y el certificado está vigente entre el 08/09/2011 y el 07/09/2012. Por lo tanto, el certificado se encuentra vigente.

Paso 3 – Comprobar estado: mediante CRL. Algunos programas permiten comprobar el estado de un certificado mediante CRL de manera automática, que es la forma más recomendable. A continuación se explican los pasos para realizar la verificación manual del estado de un certificado en la CRL.

En la pestaña “Detalles” se encuentra toda la información sobre los campos del certificado, como número de serie, emisor, datos del firmante, etc.

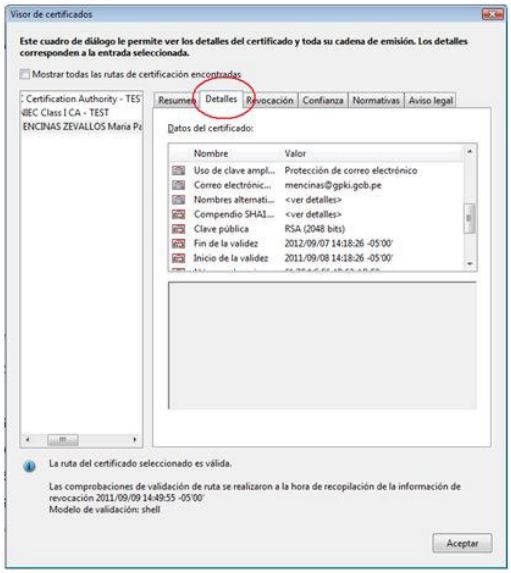


Figura 58. Detalles del certificado

Buscar el campo “Puntos de distribución de CRL”

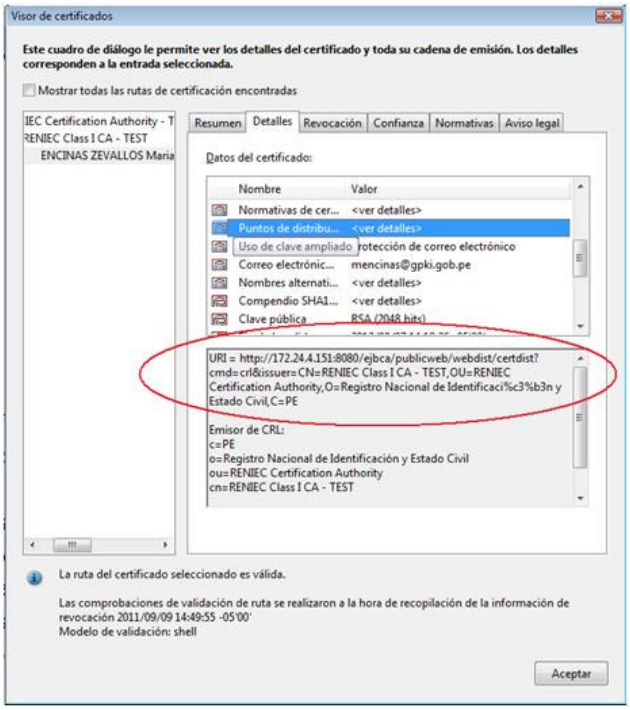


Figura 59. URI de CRL

Copiar y pegar toda la URI en algún explorador de Internet (Google Chrome, Internet Explorer, Mozilla Firefox, etc.) para descargar la CRL, este ejemplo se utilizó Google Chrome.

Figura 60. URI de la CRL en el explorador

Y comprobar que el número de serie del certificado asociado a la firma digital del documento no se encuentre en dicha CRL.

Figura 61. CRL descarga

Paso 4 – Verificar la ruta de certificación: En la ventana del certificado, a la izquierda se encuentra la ruta de certificación. En esta ruta se encuentran todos los certificados asociados a la entidad emisora del certificado que se utilizó para firmar el documento hasta llegar al certificado raíz. Haciendo click en los diferentes certificados de la ruta se puede obtener el detalle de cada uno.

Es importante verificar que se confía en todos los certificados de la ruta, para llegar a la conclusión que el certificado que respalda la firma digital contenida en el mensaje de correo electrónico es confiable.

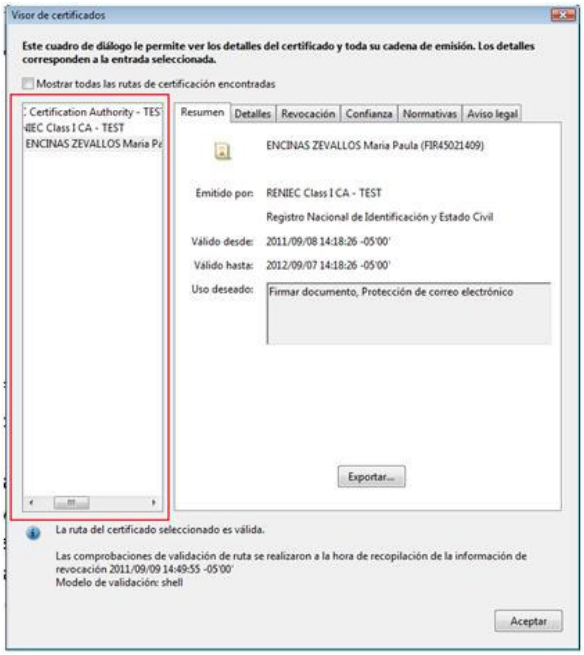


Figura 62. Ruta de certificación

Cabe señalar que se debe realizar el proceso de verificación de fecha de validez y no revocación para cada uno de los certificados de la ruta de certificación.