Apéndice: Preparación del ambiente .NET

Autor: Guzmán Llambías
Primera versión: 31 de enero, 2011

Objetivo

El objetivo de este tutorial es proveer una guía paso a paso para la preparación del ambiente para el desarrollo del tutorial .NET.

Prerrequisitos

Se debe contar con el material proporcionado en el taller el cuál puede ser ubicado en el servidor ftp de agesic. Los datos del servidor son:

- url: ftp://soporte.agesic.gub.uy/publico/Tutoriales/.NET
- usuario: agesic
- contraseña: publico

Requerimientos del software

La tabla 1 presenta las herramientas y productos de *software* requeridos para preparar el ambiente.

Producto	Versión
Windows	XP
Materiales Tutorial	N/A

Tabla 1 – Requerimientos de Software

Peparación del ambiente

En esta sección se describen los pasos necesarios para preparar el ambiente para desarrollar el tutorial .NET.

La preparación del ambiente incluye las siguientes etapas:

- Implantación de certificados para SSL.
- Implantación de certificados de organismo.

En las siguientes sub-secciones se describen en detalle cada una de ellas.

Implantación de certificados para SSL

La plataforma Microsoft provee la herramienta *Certificate Manager* para llevar a cabo todas las tareas relativas a la administración de certificados. En esta sección se utilizará esta herramienta para implantar los certificados necesarios para la conexión SSL. En particular, se instalarán tres certificados:

- el certificado del cliente
- el certificado del servidor (PGE)
- el certificado de la Autoridad Certificadora de la PGE

Instalar certificado del cliente

El certificado del cliente es un certificado con propósito *Autenticación de Clientes* y necesario para llevar a cabo la autenticación mútua entre el cliente y PGE al utilizar SSL. A continuación se describen los pasos para instalarlo.

1. En windows, seleccionar Inicio → *Ejecutar* y luego introducir el comando *mmc* como se muestra en la figura 1.

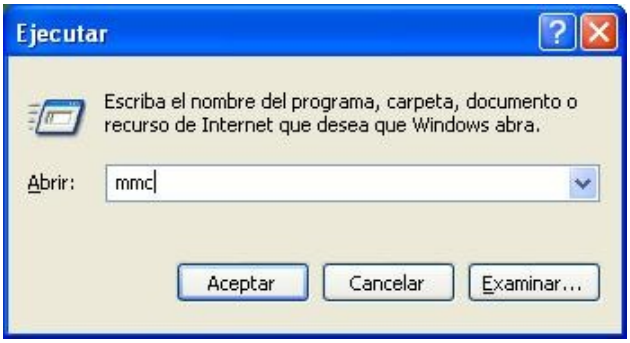

Figura 1: Levantar la aplicación Certificate Manager

2. En la aplicación *Certificate Manager* seleccionar *Archivo → Agregar o quitar complemento.* Se debe obtener un resultado similar al de la figura 2.

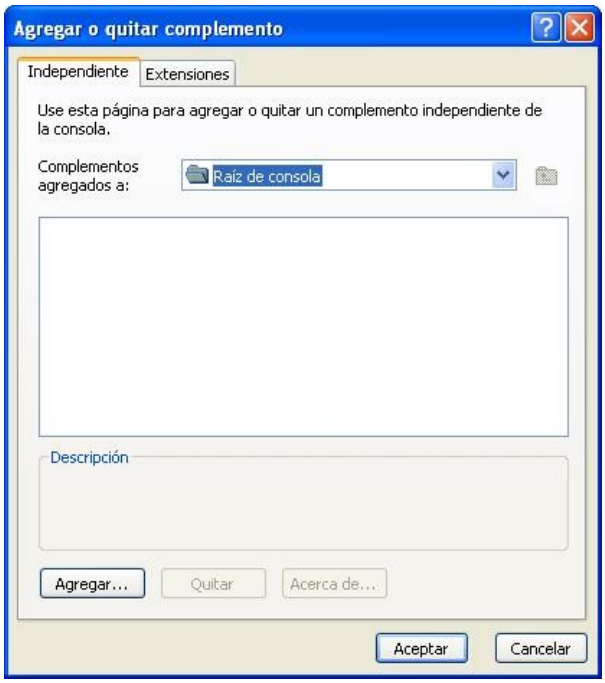

Figura 2: Agregar o quitar complemento

3. Hacer clic en el botón *Agregar → Certificados → Agregar.* Se debe obtener un resultado similar al de la figura 3.

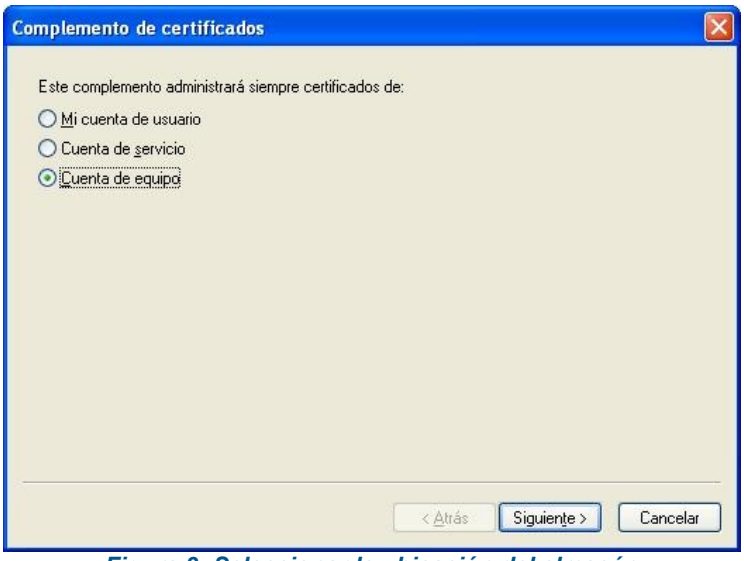

Figura 3: Seleccionar la ubicación del almacén

4. Seleccionar la opción *Cuenta de equipo* → *Siguiente* y luego *Finalizar*.

5. Seleccionar el botón *Cerrar* y obtener un resultado similar al de la figura 4. Luego, seleccionar el botón *Aceptar* para cerrar la ventana.

Figura 4: Complemento de certificados (equipo local) agregado correctamente

6. Seleccionar *Certificados (equipo local)* → *Personal* → *Certificados.* Luego, hacer clic derecho y seleccionar *Todas las tareas* → *Importar...* como se muestra en la figura 5.

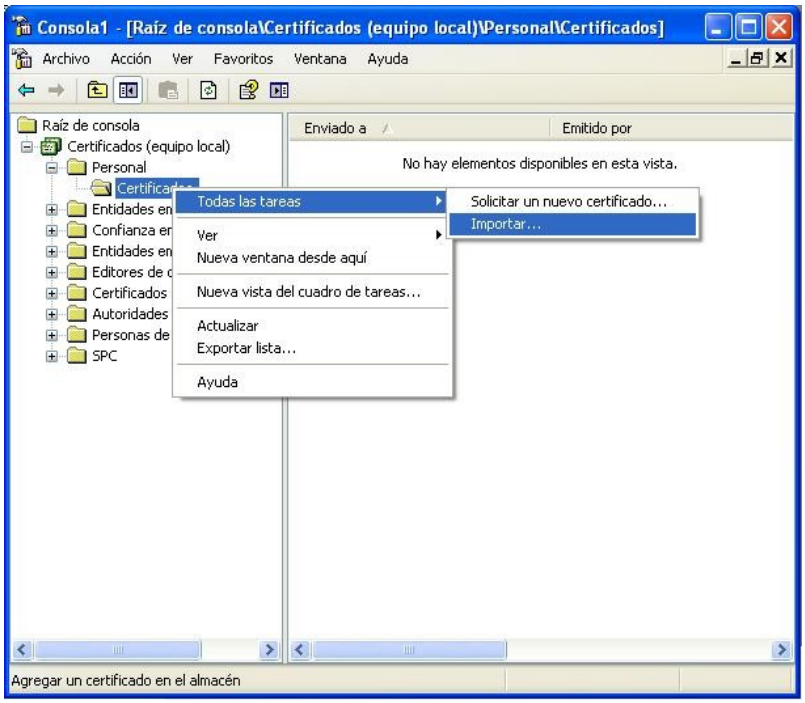

Figura 5: Importar certificado

7. En el asistente de importación de certificados, apretar el botón *Siguiente* y luego indicar la ubicación del certificado c:\Materiales\certificados\test-agesic-04022010.pfx similar a como se presenta en el figura 7.

Importante: el certificado utilizado en este tutorial vence el 4 de febrero del 2011 por lo que deberá utilizarse otro certificado una vez pasada esta fecha

Figura 6: Importar certificado

8. Seleccionar siguiente y luego introducir la constraseña de la clave privada. La contraseña de la clave privada se encuentra en c:\Materiales\certificados\readme.txt.
9. Una vez introducida la clave, apretar el botón *Siguiente* y luego *Siguiente → Finalizar.* Como resultado se debe presentar el siguiente mensaje: “La importación se completó correctamente.” y modificaciones en el almacén de certificados similares a las de la figura 8. En dicha figura se muestran dos certificados, el test_agesic (certificado del cliente) y HGTivoliCA (certificado de la CA de la PGE)

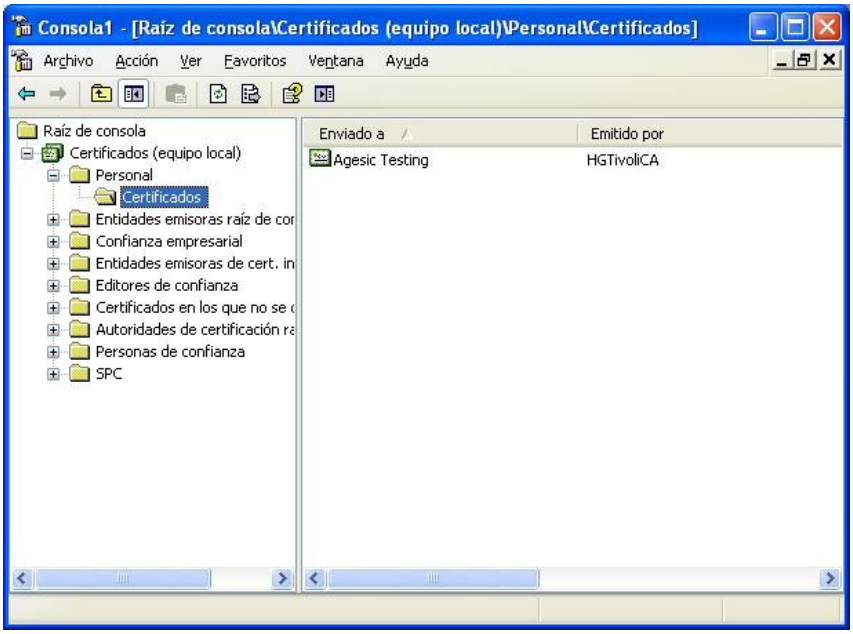

Figura 7: Importación realizada con éxito

Instalar certificado de la CA

Para completar la instalación del certificado se debe instalar el certificado de la CA que firmó test_agesic (HGTivoliCA) en el almacén de *Entidades emisoras raíz de confianza*. De lo contrario, al hacer goble clic en el certificado test_agesic, se obtendrá un resultado similar al de la figura 11.

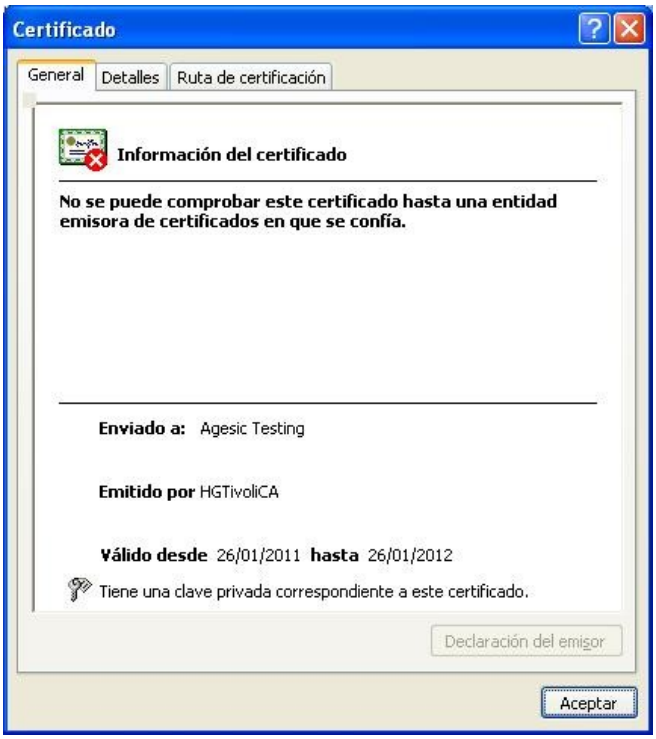

Figura 8: Certificado no válido

1. Seleccionar *Certificados (equipo local) → Entidades emisoras de raíz de confianza → Certificados* y luego clic derecho y seleccionar Todas las tareas → *Importar..., como se muestra en la figura 9.*

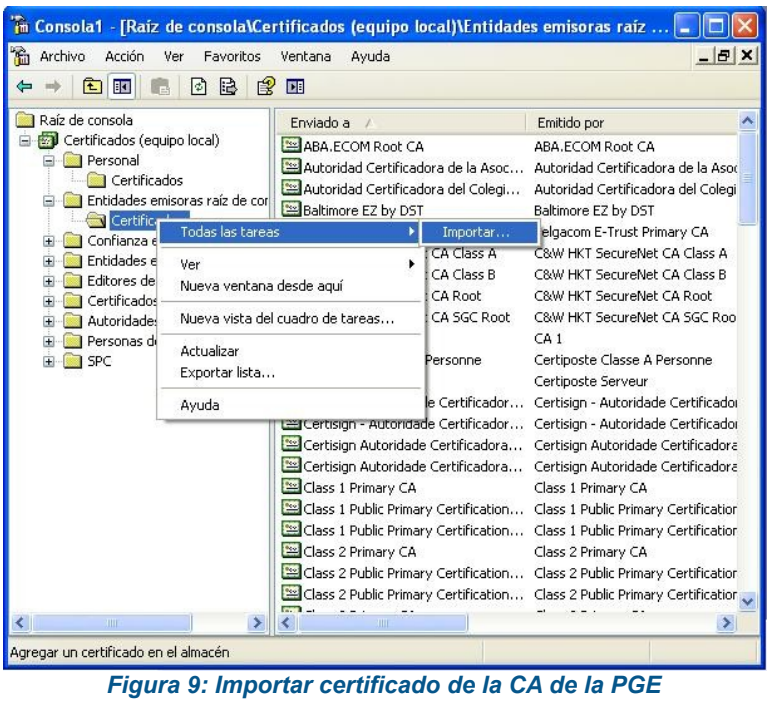

Figura 9: Importar certificado de la CA de la PGE

2. En el *asistente de importación* seleccionar el botón siguiente y luego indicar la ubicación del archivo como c:\Materiales\certificados PGE\hgca.cer similar a como se presenta en la figura 10. Luego, presionar el botón Siguiente → Siguiente → Finalizar. Se debe presentar el siguiente mensaje: "El certificado se importó correctamente."

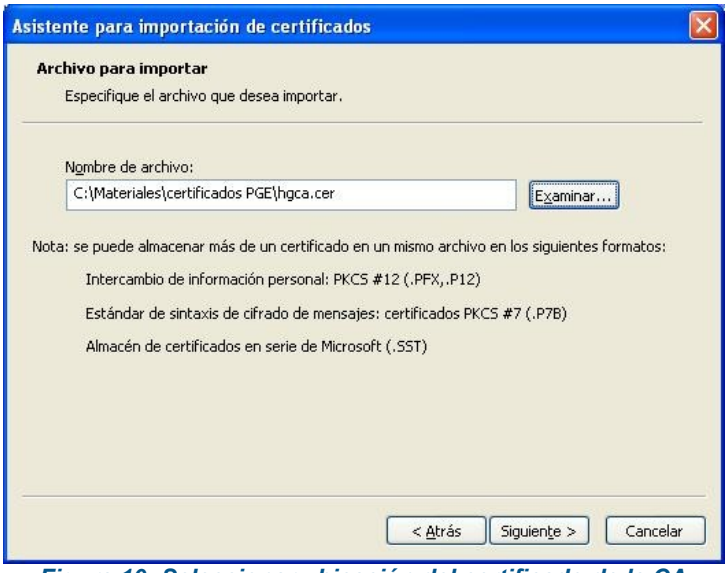

Figura 10: Seleccionar ubicación del certificado de la CA

Ahora al abrir nuevamente el certificado test_agesic, este es válido como se muestra en la figura Error: No se encuentra la fuente de referencia.

Figura 11: Certificado válido

Instalar certificado del servidor (PGE)

En una comunicación SSL el certificado de servidor permite entre otras cosas, autenticar al servidor con el cual se está comunicando.

1. Seleccionar *Certificados (equipo local) → Personas de confianza → Certificados y luego clic derecho y seleccionar Todas las tareas → Importar..., como se muestra en la figura 12.*

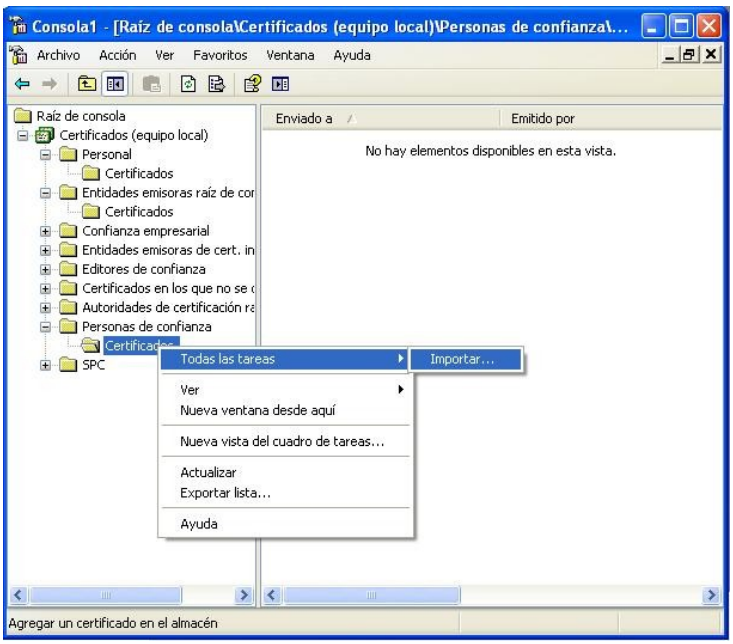

Figura 12: Importar certificado de la PGE

2. Presionar el botón siguiente y luego indicar la ubicación del certificado <como c:\Materiales\certificados PGE\testservicios.pge.red.uy.cer como se muestra en la figura 13. Luego, seleccionar *Siguiente → Siguiente → Finalizar.*

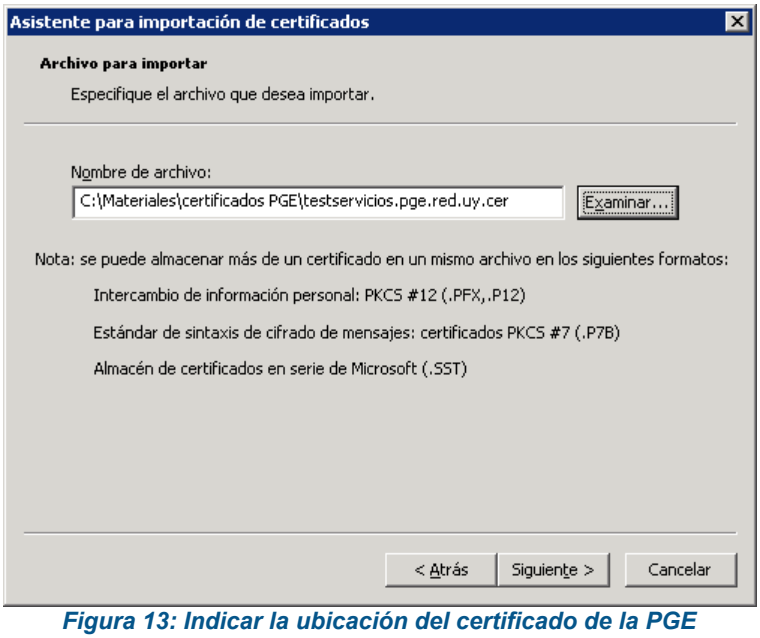

Figura 13: Indicar la ubicación del certificado de la PGE

3. Como resultado se debe presentar un mensaje indicando que el certificado se importó de forma correcta.

Instalar certificado del cliente

En este tutorial, se utiliza el mismo certificado para firmar el token SAML que para llevar a cabo la comunicación SSL. Por lo tanto, no es necesario realizar ningún paso extra para completar esta sección.

> **Importante:** En un ambiente de producción se deberá instalar obligatoriamente un certificado de este tipo