



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.



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

dependiente	Extensiones			
Use esta págir a consola,	na para agrega	ır o quitar un complen	nento indepen	diente de
Complementos agregados a:	Raí	z de consola		
Descripción				
- Descripción	Quitar	Arerca de		

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





PRESIDENCIA REPÚBLICA ORIENTAL DEL URUGUAY

Complemento de certificados	
Este complemento administrará siempre certificados de: Mi cuenta de usuario Cuenta de servicio Cuenta de equipo 	
< <u>A</u> trás Siguiente > Cancelar	

Figura 3: Seleccionar la ubicación del almacén

- 4. Seleccionar la opción Cuenta de equipo \rightarrow 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.

1 P 1	
idependiente	Extensiones
Use esta págir la consola,	na para agregar o quitar un complemento independiente d
Complementos agregados a:	; 🔄 Raíz de consola 💌
Certificad	los (equino local)
-	A A A A A A A A A A A A A A A A A A A
Descripción	
Descripción El complemer almacenes de	nto de certificados le permite examinar el contenido de los e certificados, un servicio o un equipo.
Descripción El complemer almacenes de	nto de certificados le permite examinar el contenido de los e certificados, un servicio o un equipo.
Descripción El complemer almacenes de	nto de certificados le permite examinar el contenido de lo: e certificados, un servicio o un equipo.
Descripción El complemer almacenes de Agr <u>eg</u> ar	nto de certificados le permite examinar el contenido de los e certificados, un servicio o un equipo.
Descripción El complemer almacenes de Agregar	nto de certificados le permite examinar el contenido de los e certificados, un servicio o un equipo. Quitar Acerca de Aceptar Car

(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.





PRESIDENCIA república oriental del uruguay

🚡 Consola1 - [Raíz de	consola\Cer	tificados (equipo lo	cal)\Personal\Certificados]	
hrchivo Acción Ve	r Favoritos	Ventana Ayuda		_ 8 ×
📄 Raíz de consola	- Is sell	Enviado a 🕢	Emitido por	
Personal	o local)	No hay	elementos disponibles en esta vista.	
Entidades en	Todas las tarea	as 🕨	Solicitar un nuevo certificado	
🕀 🧰 Confianza er	Ver	•	Importar	
	Nueva ventana	a desde aquí		
🕀 🧰 Certificados	Nueva vista de	l cuadro de tareas		
	Actualizar Exportar lista			
	Ayuda			
<	>	<		>
Agregar <mark>un certificado en el</mark>	almacén			

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

.red.uy.pfx Examinar
oft (.SST)

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.
- 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)

🚡 Consola1 - [Raíz de consola\Ce	rtificados (equipo local)\Pe	sonal\Certificados]		
🚡 Archivo <u>A</u> cción <u>V</u> er Eavoritos	Ve <u>n</u> tana Ay <u>u</u> da		_ 8 ×	
] 🖻 🗟 😫 🗰			
📄 Raíz de consola	Enviado a 🕢	Emitido por		
Certificados (equipo local) Personal Confianza empresarial Confianza Confianza	Agesic Testing	HGTivoliCA		
< >	<	J	>	

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.





PRESIDENCIA república oriental del uruguay

Certificado 🛛 🕐 🔀
General Detalles Ruta de certificación
Información del certificado
No se puede comprobar este certificado hasta una entidad emisora de certificados en que se confía.
Equiado au Aposis Testino
Enviauu a: Agesic resulty
Emitido por HGTivoliCA
Válido desde 26/01/2011 hasta 26/01/2012
🌮 Tiene una clave privada correspondiente a este certificado.
Declaración del emi <u>s</u> or
Aceptar

Figura 8: Certificado no válido

 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





 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."

Asiste	ente para importación de certificados	×
Are	chivo para importar	
	Especifique el archivo que desea importar.	
	Nombre de archivo:	_
	C:\Materiales\certificados PGE\hgca.cer E⊻aminar	
Not	a: se puede almacenar más de un certificado en un mismo archivo en los siguientes formatos: Intercambio de información personal: PKCS #12 (.PFX,.P12) Estándar de sintaxis de cifrado de mensajes: certificados PKCS #7 (.P7B) Almacén de certificados en serie de Microsoft (.SST)	
	< <u>A</u> trás Siguien <u>t</u> e > Cancelar	

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.

🚡 Consola1 - [Raíz de consola\Cer 📸 Archivo Acción Ver Favoritos	<mark>tificados (equipo local)</mark> Ventana Ayuda	VPersonas de confianza\ 💶 🗖 🗙
	F	
Raíz de consola Certificados (equipo local) Certificados Certificados Certificados Certificados Certificados Confianza empresarial Certificados Certific	Enviado a 🗡 No hay elem	Emitido por
SPC Ver Nueva ventana Nueva vista de	as 1	importar
Actualizar Exportar lista	,	
Ayuda		
<u>< </u>	K	<u> </u>
Agregar un certificado en el almacén		

Figura 12: Importar certificado de la PGE

 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.

sistente para importación de certificados	×
Archivo para importar	
Especifique el archivo que desea importar.	
N <u>o</u> mbre de archivo:	
C:\Materiales\certificados PGE\testservicios	s.pge.red.uy.cer Examinar
Nota: se puede almacenar más de un certificado e	en un mismo archivo en los siguientes formatos:
Intercambio de información personal: PKC	S #12 (.PFX,.P12)
Estándar de sintaxis de cifrado de mensa	jes: certificados PKCS #7 (.P7B)
Almacén de certificados en serie de Micro	soft (.SST)

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