

Manual Instalación de certificados digitales en Outlook 2000

Documento SIGNE_GCSWIE. Ver. 1.0 Fecha de aplicación 12/07/2011



Este documento ha sido generado por el Departamento de Sistemas de Información del Grupo Signe, S.A.

El contenido es confidencial y no puede ser difundido a terceros, ni utilizado para otros propósitos que los que han originado su distribución, sin el previo permiso escrito del Departamento de Sistemas de Información del Grupo Signe.

Introducción

A continuación se detallan las instrucciones para la configuración y uso de los certificados en la aplicación de correo Microsoft Outlook.

Puede tener el certificado digital en software o en tarjeta inteligente. Si su certificado se encuentra en una tarjeta, introduzca la misma en el lector de tarjetas. Si tiene el certificado digital en software con un nivel de seguridad alto, se le pedirá la contraseña cada vez que vaya a usarlo. Del mismo modo, si posee su certificado en una tarjeta, se le pedirá la contraseña con la que protegió la tarjeta, cada vez que vaya a utilizar el certificado.

Procedimiento

Para configurar el envío de correos firmados en Microsoft Outlook, independientemente de dónde tenga alojado su certificado (software o tarjeta), deberá seguir los siguientes pasos:

Una vez abierta la aplicación, seleccione "Opciones", en el menú contextual de "Herramientas".



Se mostrará la siguiente ventana, en la que hay que seleccionar la pestaña "Seguridad".

Opciones	<u>? ×</u>						
Preferenci	as Configuración de correo Formato de correo Ortografía Seguridad Otros						
Correo e	ectrónico cifrado						
<u> </u>	Cifrar contenido y datos adjuntos para mensajes salientes						
A	Agregar firma digital a los mensajes salientes						
	Enviar mensaje firmado sin cifrar al enviar mensajes firmados						
	Solicitar confirmación S/MIME para todos los mensajes S/MIME firmados						
	Configuración predeterminada: Configuración						
Zonas de	seguridad						
9	Las zonas de seguridad le permiten personalizar si se pueden ejecutar o no secuencias de comandos y contenido activo en mensajes HTML.						
	Zona: Restricted sites Configuración de zonas						
Descarga	r imágenes						
	Cambiar configuración de descarga automática						
Id. digita	les (Certificados)						
Los Id. digitales o certificados son documentos que le permiten probar su identidad en transacciones electrónicas.							
	Importar o exportar un Id. digital Obtener un Id. digital						
	Aceptar Cancelar Apligar						

Dentro del apartado "Correo electrónico seguro", hay que pulsar el botón "Configuración", que mostrará la siguiente ventana.

Cambiar la configuración de segu	uridad		×			
Preferencias de configuración de seguridad						
Nombre de configuración de segu	ıridad:					
			▼			
Eormato de cifrado: S/MIME			•			
🔽 Configuración prede <u>t</u> erminad	a para este fori	mato de men:	saje cifrado			
Config <u>u</u> ración predetermina	ada para todos	los mensajes	cifrados			
Etiquetas de seguridad	Nueva	Eli <u>m</u> inar	<u>⊂</u> ontraseña			
Certificados y algoritmos						
Certificado de firma:			<u>E</u> legir			
Algoritmo de tipo <u>h</u> ash:		7				
Certificado de cifrado:			Eļegir			
Algoritmo de cifrado:		7				
🔽 Enviar estos certificados con mensajes firmados						
	A	ceptar	Cancelar			

En primer lugar, se le da un nombre a la configuración de seguridad que se va a crear.

Cambiar la configuración (de seguridad	×			
Preferencias de configuración de seguridad					
Nombre de configuración	de seguridad:				
mi configuración		•			
Eormato de cifrado:	S/MIME	•			
🔽 Configuración predet	erminada para este formato de l	mensaje cifrado			
Config <u>u</u> ración pred	eterminada para todos los mens	ajes cifrados			
Etiquetas de <u>s</u> egurio	dad <u>N</u> ueva Eli <u>m</u> inar	⊆ontraseña			
Certificados y algoritmos 🛛 —					
Certificado de firma:		<u>E</u> legir			
Algoritmo de tipo <u>h</u> ash:		2			
Certificado de cifrado:		Elegir			
<u>Algoritmo de cifrado:</u>	ļ	-			
🔽 Enviar estos certificados con mensajes firmados					
	Aceptar	Cancelar			

A continuación se pulsa el botón "Elegir" perteneciente a "Certificado de firma". Se abrirá una pantalla en la que aparecerán los distintos certificados válidos, para su cuenta de correo.

Nota: En caso de que el certificado esté en soporte software, sólo podrá elegir de entre los que hayan sido previamente instalados en Internet Explorer. Los certificados que tenga instalados en Netscape, Mozilla u otros también deberán ser instalados en Internet Explorer para poder usarlos con el Outlook. En caso de que tenga un certificado en tarjeta, podrá seleccionar también de entre los certificados que estén en la tarjeta.

Si el e-mail del certificado y el de su cuenta no coinciden, el certificado no le aparecerá. En el caso de que no tenga instalada la clave pública de la Autoridad de Certificación que ha emitido el certificado, éste tampoco aparecerá. Por último, en el caso de que el certificado esté revocado o haya caducado, tampoco le aparecerá dicho certificado.

S	eleccionar cert	ificado			? ×
	Seleccione el cerl	tificado que quier	e usar.		
	Enviado a	Emitido por	Propósitos	Nombre de	Fecha de c
	Raquel G	AC Camerfi	Autenticaci	Ninguno	20/12/2005
		Ace	eptar Car	celar Ver	certificado

Si selecciona uno y pulsa en "Ver certificado" podrá comprobar que los datos que se visualizan sean los correctos y que al lado del icono que representa el certificado no haya ningún signo de exclamación, tal y como aparece en la imagen.



En la pestaña "Ruta de certificación" debe verse el nombre de la Autoridad Certificadora que firma el certificado y el nombre de nuestro certificado. En el apartado "Estado del certificado" debe leerse Certificado válido.

Certificado						? ×
General Detalles	Ruta de cert	ificación	Confianz	a		
- <u>R</u> uta de certifica Chambersi ≌ AC Ca 	nción gn Chambers merfirma Certif rquel García L	of Comme icados C. .aguna	erce Root amerales			
				⊻er cer	rtificado	
Estado del certific	ado:					
Certificado válido.						
					[Aceptar

Si el certificado es correcto, marcamos "Aceptar" en la ventana "Certificado". Y aparecerá de nuevo la pantalla de selección de un certificado.

5eleccionar cert	ificado			? ×		
Seleccione el certificado que quiere usar.						
Enviado a	Emitido por	Propósitos	Nombre de	Fecha de c		
Raguel G	AC Camerfi	Autenticaci	Ninguno	20/12/2005		
4				► 1		
	0.00	antar Car		r contificado		
	AC			Certificado		

Una vez seleccionado el certificado, pulse "Aceptar". Y podrá comprobar que en la ventana "Cambiar la configuración de seguridad", en la sección "Certificados y algoritmos", aparece el nombre del certificado, tanto en "Certificado de firma" como en "Certificado de cifrado".

Cambiar la configuración de seguridad	×				
Preferencias de configuración de seguridad					
mi configuracion	•				
Eormato de cifrado: S/MIME	•				
🔽 Configuración predeterminada para este formato de mensaje cif	rado				
🔽 Configuración predeterminada para todos los mensajes cifrado	os				
Etiquetas de seguridad Nueva Eliminar Contr	aseña				
Certificados y algoritmos					
Certificado de firma: Raquel García Laguna	egir				
Algoritmo de tipo <u>h</u> ash: SHA1					
Certificado de cifrado: Raquel García Laguna Ele	egir				
Algoritmo de cifrado: 3DES					
🔽 Enviar estos certificados con mensajes firmados					
Aceptar Ca	ncelar				

El certificado de cifrado se incluye en el correo firmado digitalmente, de forma que otras personas puedan enviarle correo cifrado con estas opciones. Es decir, que cuando a un usuario le llegue un mensaje suyo firmado, el certificado que él almacenará para cifrar los correos que quiera enviarle, será este.

Si desea que este certificado sea diferente del certificado de firma, puede cambiarlo, pulsando el botón "Elegir", el proceso es exactamente igual que el seguido para el certificado de firma.

Se recomienda que en ambos apartados, se utilice el mismo certificado, y que los algoritmos sean los que aparecen por defecto, por razones de seguridad.

Pulse el botón "Aceptar". Aparecerá de nuevo la ventana de "Opciones", en esta pantalla debe marcar la casilla "Enviar mensaje firmado sin cifrar al enviar mensajes firmados"

Opciones	?×					
Preferencia	s Configuración de correo Formato de correo Ortografía Seguridad Otros					
Correo ele	ectrónico cifrado					
2	Cifrar contenido y datos adjuntos para mensajes salientes Agregar firma digital a los mensajes salientes					
 Enviar mensaje firmado sin cifrar al enviar mensajes firmados 						
	Solicitar confirmación S/MIME para todos los mensajes S/MIME firmados					
	Configuración predeterminada: Imi configuración					
Zonas de	seguridad					
3	Las zonas de seguridad le permiten personalizar si se pueden ejecutar o no secuencias de comandos y contenido activo en mensajes HTML.					
	Zona: Restricted sites Configuración de zonas					
Descarga	r imágenes					
	Cambiar configuración de descarga automática					
Id. digital	es (Certificados)					
	Los Id. digitales o certificados son documentos que le permiten probar su identidad en transacciones electrónicas.					
Importar o exportar un Id. digital Obtener un Id. digital						
	Aceptar Cancelar Apli <u>c</u> ar					

Si se quiere que todos los mensajes se envíen por defecto firmados, marque la casilla "Agregar firma digital a los mensajes salientes"; si por el contrario desea hacerlo manualmente, déjela sin marcar.

Pulse "Aceptar", y de este modo ya está configurado el envío de mensajes firmados. Una vez configurado el certificado en Microsoft Outlook, el certificado está listo para ser utilizado para firmar correos electrónicos.

IMPORTANTE: No podrá firmar mensajes enviados desde una dirección de correo que no sea la que aparece en el certificado digital. Es decir, en el certificado digital, aparece una dirección de correo electrónico facilitada por usted. Sólo podrá firmar mensajes enviados desde la dirección que aparece en su certificado.

El primer paso es el de confeccionar su mensaje (escribir el texto, adjuntar los archivos, escribir el/los destinatario/s, etc.).



Una vez rellenados todos los datos, puede proceder a firmar el mensaje. Para ello, puede hacerlo de varias formas:

a) Pulse en "Opciones". A continuación pulse en el botón "Configuración de seguridad".

Opciones <mark>de mens</mark> aje					
Configuración de mensaje S	jeguridad				
Importancia: Normal	Cambiar la configuración de seguridad p				
C <u>a</u> rácter: Normal 🔽	Configuración de seguridad				
Opciones de votación y seguimiento					
 Usar botones de voto: Solicitar confirmación de entrega para este mensaje Solicitar confirmación de lectura para este mensaje 					
Opciones de entrega					
📺 🗖 Enviar las respuestas a:					
Guardar el mensaje enviado en:	Elementos enviados				
No entregar antes <u>d</u> el:	No disponible 🔽 0:00				

Aparece la siguiente ventana, en la cual debe marcar la casilla "Agregar firma digital a este mensaje". Y en la sección "Configuración de seguridad", seleccione la configuración que creó cuando instaló el certificado en Microsoft Outlook.

Propiedades de seguridad						
Cifrar el contenido del mensaje y los datos adjuntos						
🔽 Agregar firma digital a este mensaje						
🔽 Enviar este mensaje firmado con texto simple						
🔲 Solici <u>t</u> ar confirmación S/MIME para este mensaje						
Configuración de seguridad						
Configuración de seguridad:						
mi configuracion						
Etiqueta de seguridad						
Módulo de directiv <u>a</u> s: <ninguno> Configurar</ninguno>						
Clasificación:						
Marca de privacidad:						
Aceptar Cancelar						

Pulse el botón "Aceptar", y el botón "Cerrar" de la ventana "Opciones del mensaje".

 b) Otra opción (más rapida) para firmar el mensaje es seleccionar el icono marcado en rojo que aparece en la ventana donde se redacta un mensaje de correo electrónico.



Puede observar que el resultado que se obtiene siguiendo cualquiera de los opciones explicadas anteriormente es el mismo.

Si al configurar Microsoft Outlook, hubiera marcado la casilla "Agregar firma digital a los mensajes salientes" ...



... al pulsar en "Nuevo mensaje", aparecería marcado de forma automática el icono de firma.



Una vez escrito el correo electrónico y marcada la opción de firma, pulse el botón "Enviar".

Cuando pulse sobre el botón de envío del mensaje, la aplicación le pedirá que introduzca el PIN de la tarjeta si el certificado esta contenido en la misma.



O el del certificado en software si el nivel de seguridad del mismo es alto; en este caso aparecerá la pantalla para la confirmación de uso de su clave privada. Deberá escribir el password (PIN) que le puso a su certificado durante la instalación. NO seleccione Recordar contraseña, si lo hace, cualquiera podría usar su clave privada. Pulse "Aceptar".

Se están firmar	ndo datos con su clave privada de intercambio	×
	Una aplicación está solicitando acceso a un elemento protegido.	
	Llave privada de CryptoA ji <u>R</u> ecordar contraseña <u>Aceptar</u> <u>Cancelar</u> <u>D</u> etalles	

Una vez introducido el código PIN correctamente, se hace efectivo el envío.

Para validar un correo firmado, es necesario tener instalados los certificados de la Autoridad de Certificación del certificado que ha firmado el correo recibido. Microsoft Outlook comprueba si estos certificados se encuentran en los almacenes de "Entidades emisoras de certificados intermedias" y en "Entidades emisoras raíz de confianza". Si no estuvieran, los instala automáticamente; de esta manera la firma del correo sería válida.

Cuando reciba un correo electrónico firmado digitalmente por otro usuario, dicho mensaje tendrá asociado un icono que contendrá un sello lacrado, el cual indicará que el mensaje está firmado:



Si pulsa sobre el icono marcado en rojo, podrá ver quién ha firmado el mensaje, si la firma digital es válida y de confianza.



Para ver más información, pulse en el botón "Detalles".

En la siguiente imagen se puede observar que el mensaje fue firmado correctamente.

Propiedades de seguridad del mensaje	×
Asunto: Prueba	
Los mensajes pueden contener niveles de firma digital y cifrado. Cada nivel de firma digital puede contener varias firmas. Niveles de seguridad	
Seleccione uno de los niveles siguientes para ver su descripción.	
✓ <mark>Asunto: Prueba</mark> ✓ Nivel de firmas digitales ✓ Firmante: rgarcia@netsignia.es	
Descripción:	
Correcto: mensaje firmado.	
, Haga clic en cualquiera de los siguientes botones para ver más información acerca del nivel seleccionado o realizar cambios en éste:	
Modificar confianza Ver detalles Confiar en entidad emisora de certificados	
☐ <u>A</u> visar sobre errores del correo electrónico firmado digitalmente. <u>C</u> errar]

Si pulsamos en "Firmante", se puede ver quien ha firmado el correo.



Pulse en "Ver detalles".

Firm Ge	eneral Detalles	? ×		
	Información de la firma			
	Formato del mensaje:	5/MIME		
	Firmado por:	rgarcia@netsignia.es		
	Estado de la firma:	Correcto		
	Fecha de firma:	15:44:19 14/03/2005		
	Algoritmo de codificación:	SHA1		
	Algoritmo de firma:	RSA (1024-bits)		
	Información del certif	ìcado		
	Emitido por:	AC Camerfirma Certificados 🛛 🗮		
	Estado del certificado:	Correcto		
		<u>V</u> er certificado		
		<u>C</u> errar		

A continuación pulse en "Ver certificado". De esta forma podemos visualizar todos los detalles del certificado que firmó el correo.



En la pestaña "Detalles", obtenemos información sobre el emisor del certificado, el titular, la fecha de validez del certificado, la huella digital, etc.

'er certificado	? ×				
General Detalles Ruta de certifica	ación Confianza				
Mostrar: <todos></todos>					
Campo	Valor 🔺				
💳 Versión	V3				
🔚 Número de serie	Oe 2f				
🗖 Algoritmo de firma	sha1RSA				
Emisor	AC Camerfirma Certificados Ca				
🖃 Válido desde	lunes, 20 de diciembre de 2004				
🔚 Válido hasta	martes, 20 de diciembre de 200				
Asunto	Chambers of Commerce Qualifie				
🔚 🔚 Clave pública	RSA (1024 Bits)				
CN = AC Camerfirma Certificados Camerales O = AC Camerfirma SA Número de serie = A82743287 L = Madrid (see current address at www.camerfirma.com/address) E = ac_camerfirma_cc@camerfirma.com C = ES					
M <u>o</u> dificar prop	iedades <u>C</u> opiar en archivo				
	Aceptar				

En la pestaña "Ruta de certificación", aparece la jerarquía de confianza a la que pertenece el certificado.

Además en la sección "Estado del certificado", se presentan los problemas encontrados en la verificación de certificado, si los hubiera.

General Detalles Ru Buta de certificación Chambersign C Comparing AC Camerfi	ta de certificación Confia hambers of Commerce Roo rma Certificados Camerales García Laguna	inza ot s	<u>? ×</u>
Estado del certificado:		<u>⊻</u> er certificado]
Certificado válido.			Aceptar





www.signe.es

Avda. de la Industria, 18 28760 Tres Cantos (Madrid) España Tel.: + 34 918 06 00 99 comercial@signe.es