INTRODUCCIÓN

La Organización Médica Colegial y el Colegio desean ofrecer a los colegiados las máximas garantías de seguridad en su trabajo en internet. La firma electrónica nos proporciona los mecanismos ideales para conseguir este objetivo.

Con esta guía de uso ponemos al servicio de los colegiados todo el proceso de instalación y gestión de la tarjeta criptográfica del Colegio.

Además se encuentran los procedimientos de gestión que pueden utilizar los colegiados como usuarios del certificado electrónico.

HERRAMIENTAS NECESARIAS

El colegiado necesita:

- Un ordenador con un sistema operativo MS Windows 2000, XP o Vista

- Conexión a **Internet** (se recomienda ADSL), a la que está conectado el ordenador.

- Un lector de tarjetas criptográficas conectado al ordenador

- El **software SafeSign** proporcionado por el Colegio y que encontrará en el apartado "Software" del CD.

- La **tarjeta** criptográfica, a nombre del colegiado, proporcionada por el Colegio.

- La **carta** que el colegiado ha recibido en su domicilio, en la que se incluyen los números PIN y PUK, necesarios para utilizar la tarjeta.

SOFTWARE SAFESIGN

Esta aplicación permite la gestión de la tarjeta criptográfica de la OMC.

Además, consigue que el certificado electrónico incluido en la tarjeta sea reconocido por los diversos programas de Microsoft Windows.

PASO 1:

- Poner el CD (que viene con el pack de la OMC) en el ordenador donde tenemos el lector de tarjetas.

- El cd debe arrancar automáticamente, si no, iremos al explorador del windows y realizaremos la función manualmente.



PASO 2:

- Se instalará el programa safesign



Podemos elegir el idioma deseado



i SafeSign - InstallShield Wizard				
E	Bienvenido a SafeSign - InstallShield Wizard			
	InstallShield(R) Wizard instalará SafeSign en su equipo. Para continuar, haga dic en Siguiente.			
	ADVERTENCIA: Este programa está protegido por las leyes de derechos de autor y otros tratados internacionales.			
	< Atrás Siguiente > Cancelar			

Debemos aceptar la licencia. [Tenemos que hacer un clic manualmente en "Acepto los términos del contrato de licencia"]

🔂 SafeSi	gn - InstallShield Wizard	×		
Contrato de licencia				
SafeSig	SafeSign Identity Client License Terms and Conditions			
1	Clause 1	-		
⊙ Acepto	Clause 1 Subject to the terms and conditions of this Agreement, A.E.T. Europe B.V. (hereinafter: AET) grants to Licensee a non-exclusive, non-transferable and non- objectionable license to use SafeSign Identity Client. Licensee is not granted any ownership rights. Licenses are granted on the condition that the Licensee fully complies with the terms and conditions of this Agreement. All intellectual and industrial ownership rights are and will remain the exclusive property of AET. Licensee is explicitly forbidden at all times to transfer, lease, sub-license or grant limited rights to (portions of) SafeSign Identity Client, or to transfer SafeSign Identity. Client to any third parties in whatever mapper or for whatever nurpose Acepto los términos del contrato de licencia			
u istalisrilela	< Atrás Siguiente > Cancelar			

Si no hay ningún inconveniente, podemos aceptar la carpeta que nos propone el programa. [Hacer clic en "siguiente"]

🙀 SafeSig	n - InstallShield Wizard	X
Carpeta d Haga clic en una c	de destino : en Siguiente para instalar en esta carpeta o en Cambiar para instalar arpeta diferente.	
	InstalarSafeSign en: C:\Archivos de programa\A.E.T. Europe B.V.\SafeSign\ Cambiar	
InstallShield -	< Atrás Siguiente > Cancelar	

Personalizaremos la instalación

🛱 SafeSign - InstallShield Wizard	
Instalación personalizada Seleccione los componentes del programa que desee instalar.	
Para cambiar la forma de instalación de un componente, haga de la co	lic en un icono de la lista siguiente. Descripción del componente Compatibilidad criptográfica con Firefox, Mozilla, Netscape y otros productos que reconocen la biblioteca PKCS #11 Este componente requiere 2608KB en el disco duro.
InstallShield	Cambiar Siguiente > Cancelar

Tenemos que incluir el apartado GINA como muestra la imagen

🛃 SafeSign - InstallShield Wizard	\mathbf{X}
Instalación personalizada Seleccione los componentes del programa que desee instalar.	~
Para cambiar la forma de instalación de un componente, haga clic en un icono de la lista siguient PKCS #11 Diálogos comunes de SafeSign CSP GINA Dialogos comunes de SafeSign	e. n
📰 Este componente se instalará en el disco duro local.	
Este componente se instalará en el disco duro local. Image: Base componente y todos sus subcomponentes se instalarán en el disco duro local.	al.
 Este componente se instalará en el disco duro local. Este componente y todos sus subcomponentes se instalarán en el disco duro local. Este componente no estará disponible. 	al.
 Este componente se instalará en el disco duro local. Este componente y todos sus subcomponentes se instalarán en el disco duro local. Este componente no estará disponible. 	al.
Este componente se instalará en el disco duro local. Este componente y todos sus subcomponentes se instalarán en el disco duro loc Este componente no estará disponible. Instalar en: Cambiar Cambiar	:al.

😸 SafeSign - InstallShield Wizard	
Instalación personalizada Seleccione los componentes del programa que desee instalar	
Para cambiar la forma de instalación de un componente, haga PKCS #11 Diálogos comunes de SafeSign CSP GINA Documentación Compatibilidad con idioma local Administración de tokens Utilidad de comprobación de vencimiento	clic en un icono de la lista siguiente. Descripción del componente Compatibilidad con inicio de sesión mediante dispositivos con ruta de autenticación protegida Este componente requiere 97KB en el disco duro.
	Cambiar
Ayuda Espacio < Atrás	Siguiente > Cancelar

Hacemos clic en instalar

😸 SafeSign - InstallShield Wizard
Preparado para instalar el programa El Asistente está preparado para comenzar la instalación.
Haga clic en Instalar para comenzar la instalación. Si desea revisar la configuración de la instalación o realizar algún cambio, haga clic en Atrás. Haga clic en Cancelar para salir del Asistente.
InstallShield

🔂 SafeSig	n - InstallShield Wizard
Instaland Los comp	lo SafeSign ponentes del programa seleccionados se están instalando.
i de la constante de la consta	Por favor, espere mientras InstallShield Wizard instala SafeSign. Este proceso puede durar varios minutos. Estado:
InstallShield –	< Atrás Siguiente > Cancelar

Se ha terminado la instalación general de la aplicación

😸 SafeSign - InstallShield Wizard				
	Finalizado SafeSign - InstallShield Wizard			
	InstallShield Wizard ha instalado SafeSign correctamente. Haga clic en Finalizar para salir del asistente.			
	< Atrás Finalizar Cancelar			

PASO 3 (opcional) Entrust



Puede ser necesaria la instalación de la opción "entrust".

Hacemos un clic en "instalar".



PASO 4 (opcional) Firefox

Puede ser necesaria la instalación de la opción para los programas de Mozilla (Firefox - Thunderbird)



Seleccionamos el programa y hacemos clic en "instalar".



La instalación abrirá nuestro navegador Firefox. Debemos aceptar cuando se nos pregunte.



SafeS	ign -	Mozilla Fi	irefox
<u>E</u> ditar	<u>V</u> er	Hi <u>s</u> torial	Marcadores Herramien <u>t</u> as Ay <u>u</u> da
-	C	😣 🏠	file:///C:/DOCUME~1/ANTONI~1/CONFIG~1/Temp/8F.tmp
			Alerta 🛛
			Se ha instalado un nuevo módulo de seguridad
			Aceptar

Para terminar haremos un clic en "cerrar"



PASO 5. VER MI CERTIFICADO

Para visualizar nuestro certificado vamos al "inicio" del windows y buscamos la carpeta "SafeSign Standard". Escogemos la opción "Administración de tokens".

Ahora debe introducir la tarjeta en el lector



Observamos como ya nos aparece la tarjeta OMC en la aplicación.

🐳 Utilidad para administración de tokens	
ID digitales Token Integración Tareas Ayuda	
Nombre de lector o token	Estado de token
🖗омс 🚽	operativo
AKS ifdh 0	ausente
AKS ifdh 1	ausente
	.:

Elegiremos la opción "Mostrar ID digitales registrados"



Observaremos qué certificados tenemos en nuestro ordenador.

ID digitales					
ID digitales personales:					
Emitido para	Emitido por	Fecha de vencimiento	Etiqueta	Etiqueta de t	oken 📃 📥
Isacio Siguero Zurdo	OMC	2011-05-05 02:00:00	Isacio Siguero Z	OMC	
and the cardinal	10 00 at	2010/01/02/02	arrise care		
Bel et l	8.40	ELL/288	E-42 Apr		~
Detalles de ID digital	:				
Campo	Valor				
Ruta de certificado:					
Emitido para	Emitido por	r	Fecha de vencimiento	4	Almacén de cer
	Transferir ID a tok	Importar cadena	de confianza Elim	iinar ID digital	Ver certificado
			Actualizar Comp	robar vencimier	nto Cerrar

Si hacemos un clic en la opción "Comprobar vencimiento" la aplicación os indicará qué certificados están a punto de caducar.

ID digitales						
ID digitales personales:						
Emitido para	Emitido por	Fecha de vencimiento	Etiqueta	Etiqueta de token		
Isacio Siguero Zurdo	OMC	2011-05-05 02:00:00	Isacio Siguero Z	OMC		
	01-001ae 01-001	80° 0 8 0040 89 0 1 0 40	411/2012 (1895)			
₽						
-Detalles de ID digital						
Contenido de certificado	n Información					
Campo				-		
	(i) No o	No caducará ningún ID digital en los próximos 30 días				
	_	Aceptar				
Ruta de certificado:						
Emitido para	Emitido po	r F	echa de vencimiento	Alma		

Si hacemos un clic en la opción "ver certificado" la aplicación nos enseñará el contenido del certificado que hayamos señalado.

Certificado		X			
Información de o	certificado				
Emitido para:					
Tratamiento	Presidente				
Nombre de pila	Isacio				
Apellidos (SN)	Siguero Zurdo				
Nombre común (CN)	Isacio Siguero Zurdo				
Unidad organizativa (OU)	Condiciones de uso en https://www.cgcom.es/CertOrg (c) 06	~			
Información de emisor:					
Nombre común (CN)	OMC	~			
Unidad organizativa (OU)	VeriSign Trust Network	H			
Unidad organizativa (OU)	Entidad de Certificacion				
Unidad organizativa (OU)	Class 2 Managed PKI Individual Subscriber CA				
Organización (O)	Organizacion Medica Colegial	~			
Validez:					
Válido desde	2008-05-05 02:00:00				
Válido hasta	2011-05-05 02:00:00				
Este certificado es para	:				
Crear firmas digitales	Proteger correo electrónico				
Cifrar claves secretas					
Cifrar datos					
Probar identidad propia a s	ervidor remoto				
Huellas dactilares:					
Huella dactilar SHA1 20:53:BC:74:29:F5:51:3C:C8:DA:4D:C0:2F:32:83:D9:48:4D:66:F3					
Huella dactilar MD5 56:0	CE:6B:53:FA:73:93:7F:EA:0F:FA:C6:BD:E0:67:AC				
	Guardar en archivo Cerrar	-			

La aplicación nos permite el cambio del número PIN

🧼 Utilidad	d para administración de tokens				
ID digitales	Token Integración Tareas Ayuda				
Nombre de	Realizar barrido de token	Estado de token			
🖗 омс	Desbloquear PIN	operativo			
AKS ifdh	Cambiar PIN	ausente			
AKS ifdh	Registrar datos biométricos	ausente			
	Cambiar PUK				
	Mostrar información de token				
	Mostrar objetos de token				
	Volcar contenido de token				
	Realizar una consulta sobre token desconocido				
	Analizar calidad de certificado				
		1			
Cambia el PIN del usuario					

Sólo debemos incluir nuestro actual PIN y el que nosotros deseamos.

Cambiar PIN		×			
Cambiando el PIN por "OMC":					
Introduzca PIN antiguo:					
Introduzca PIN nuevo:					
Confirme PIN nuevo:					
 Longitud mínima de PIN 6 bytes Longitud máxima de PIN 8 bytes Nuevo PIN igual a nuevo PIN confirmado 					
	Aceptar Cancelar				

REVOCACIÓN DEL CERTIFICADO

El procedimiento de revocación está definido en la Política de Certificación y en la Declaración de Prácticas de Certificación.

Un colegiado puede revocar su certificado cuando se produzca:

a) Finalización de la relación jurídica de prestación de servicios entre la Entidad de Certificación de la OMC y el subscriptor.

b) Modificación o extinción de la relación jurídica subyacente o causa que provocó la emisión del certificado.

c) Infracción por el solicitante del certificado de los requisitos preestablecidos para la solicitud del mismo.

d) Infracción del colegiado de sus obligaciones, responsabilidad y garantías, establecidas en el documento jurídico correspondiente.

e) La incapacidad sobrevenida o el fallecimiento del poseedor de claves.

 f) La extinción de la persona jurídica suscriptora del certificado, así como el fin de la autorización del suscriptor al poseedor de claves o la finalización de la relación entre suscriptor y poseedor de claves.

g) Solicitud del suscriptor de revocación del certificado.

LISTAS DE REVOCACIÓN

Para depositar nuestra confianza en un certificado debemos consultar las listas de certificados que la Entidad de Certificación de la OMC ha revocado. Estas listas se pueden encontrar en las siguientes direcciones:

http://crl1.cgcom.es/crl/ec-cgcom.crl

http://crl2.cgcom.es/crl/ec-cgcom.crl

PÉRDIDA DE LA TARJETA CRIPTOGRÁFICA

En caso de pérdida o sustracción, se debe comunicar urgentemente al Colegio.

CONSULTAS

Para todas aquellas consultas que se deseen realizar sobre este servicio deben dirigirse al teléfono 902 365 121.