

SUBSECRETARÍA

SUBDIRECCIÓN GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

Requisitos del Componente de Firma.

- El componente de firma es compatible con Internet Explorer y sistemas operativos Windows.
- Microsoft NET Framework 1.1 debe estar instalado previamente.
- Disponer de un certificado de cliente X509 configurado correctamente.

Configuración del Almacén de certificados.

Para el ejemplo se utiliza un certificado de la FNMT. En caso de que se estuviera utilizando otro tipo de certificados los cambios deberían ser sobre el/los certificados raíz de la Entidad emisora y sobre los certificados personales si procede (Ver más adelante apartado **Entidades Emisoras de Confianza**).

El componente de firma necesita que estén configurados correctamente los propósitos del certificado del cliente. Si surge algún problema en la carga del componente seguir los siguientes pasos:

🗿 Servicio De Firma Electronica Del Ministerio De Industria, Turismo Y Comercio - Microsoft Internet Explorer 💦 🗐 💽
Archivo Edición Ver Favoritos Herramientas Ayuda 🥂
Correo y noticias Bioqueador de elementos emergentes Administrar complementos Dirección HINISTERIO MINISTERIO MINISTERIO SERVICIO DE FIRMA ELECTRONICA DEL MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO
Componente de firma XML-Signature, especificación técnica: ETSI TS 101 903 V1.2.2 XML <u>Advanced Electronic Signatures (XAdES)</u> • Enviar uno o varios ficheros para firmar, mediante firma electrónica avanzada XAdES • Volver a firmar un documento electrónico en formato XAdES • Obtener información de un documento electrónico XAdES
Servicio de consulta y validación de certificados
 Servicio Web de consulta, validación del certificado y generación de fichero xml con los datos del certificado cliente Los prestadores de servicios de certificación a los que este servicio accede son: FNMT (Consulta LDAP) Generalitat Valenciana (Servicio descarga CRL) Firma Profesional (Servicio descarga CRL) Consejo General de la Abogacia (Servicio descarga CRL) CamerFirma (Servicio descarga CRL)
Los certificados de los siguientes prestadores de servicios de certificación se encuentran en proceso de adaptación técnica:
o Izenpe S.A.(Servicio descarga CRL) o CATCert - Agència Catalana de Certificació (Servicio descarga CRL)
Ayuda
 Requisitos del componente de firma XML-Signature Configuración del navegador Especificación técnica estándar XAdES Especificación relativa al servicio de firma de MITYC
Permite cambiar la configuración.

1. Acceder al menú de Herramientas/Opciones de Internet de Internet Explorer



SUBDIRECCIÓN GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

2. Acceder a la pestaña de contenido

	Program	Programas Opciones avanzad	
General	Seguridad	Privacidad	Contenido
Asesor de conter Las rest verse er	iido icciones le ayudan a co) este equipo.	ontrolar el contenido o Habilitar	de Internet que pued
Los ceri entidad	ificados le permitirán ide se emisoras de certificad Borrar estado SSL	ntificarse a sí mismo, los y a compañías de Certificados	a e software. Compañías
nformación pers	onal		
Autocor coincide	npletar almacena entrad encias.	as anteriores y sugiel	e Autocompletar.
E 1.4 · · ·	nte para perfiles de Mic ión personal.	rosoft almacena su	Mi perfil
El Asiste informac			

3. Pulsar el botón Certificados y acceder a la pestaña de Entidades Emisoras de Confianza utilizando las flechas de desplazamiento resaltadas en la imagen. Para el ejemplo se utiliza un certificado de la FNMT. En caso de que se estuviera utilizando otro tipo de certificados los cambios deberían ser sobre el/los certificados raíz de la Entidad emisora y sobre los certificados personales si procede (Ver más adelante apartado Entidades Emisoras de Confianza).

Emitido para	Emitido por	Fecha d	Nombre descript
ABA.ECOM Root CA	ABA.ECOM Root CA	09/07/2009	DST (ABA.ECOM
🖴 Autoridad Certifica	Autoridad Certificador	28/06/2009	Autoridad Certifi
🖴 Autoridad Certifica	Autoridad Certificador	29/06/2009	Autoridad Certifi
🔛 Autoridad de Certifi.	. Autoridad de Certifica	24/10/2013	Autoridad de Ce
Baltimore EZ by DST	Baltimore EZ by DST	03/07/2009	DST (Baltimore E
Belgacom E-Trust P	. Belgacom E-Trust Prim	21/01/2010	Belgacom E-Trus
C&W HKT SecureN	C&W HKT SecureNet	16/10/2009	CW HKT Secure
C&W HKT SecureN	C&W HKT SecureNet	16/10/2009	CW HKT Secure
C&W HKT SecureN	C&W HKT SecureNet	16/10/2010	CW HKT Secure
portar	Ouitar		Avanzada
pósitos planteados del	ertificado		



SUBDIRECCIÓN GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

4. Seleccionar la Entidad FNMT Clase 2 CA

rtificados				?
opósito planteado: <pre></pre>	os>			
intidades emisoras de certifi	cados intermedias Entida	des emisoras r	aíz de confianza	Edit 🔨
Emitido para	Emitido por	Fecha d	Nombre descript	🔺
Equifax Secure Glo EUnet International FESTE, Public Notar FESTE, Verified Certs	Equifax Secure Global EUnet International R FESTE, Public Notary FESTE, Verified Certs	21/06/2020 02/10/2018 01/01/2020 01/01/2020	Equifax Secure EUnet Internatio. FESTE, Public No. FESTE, Verified	
FIRST Data Digital C	FIRST Data Digital Certi	18/03/2019	Eabrica Nacional	ii l
GlobalSign Root CA	GlobalSign Root CA GTE CyberTrust Globa GTE CyberTrust Root	28/01/2014 14/08/2018 04/04/2004	GlobalSign Root (GTE CyberTrust , GTE CyberTrust ,	:A 🗸
(mportar) Exportar Propósitos planteados del ce	Quitar		Avar	nzadası
<lodos></lodos>			<u> </u>	er
				<u>errar</u>

5. Hacer **doble click** con el botón izquierdo del ratón para sacar las propiedades de este certificado:

ertifica	ado	?
Seneral	Detalles Ruta de certificación	
	Información del certificado	
Este	e certificado está destinado a los siguientes propósitos: •Todas las directivas de emisión •Todas las directivas de la aplicación	
_	Enviado a: FNMT Clase 2 CA	<u></u> £3
	Emitido por FNMT Clase 2 CA.	
	Válido desde 18/03/1999 hasta 18/03/2019	
1	Declaración del	emisor
		Acepta

6. Acceder a la pestaña Detalles



SUBDIRECCIÓN GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

strar: <pre></pre>	×	
Campo	Valor	^
Versión Número de serie Algoritmo de firma Emisor Válido desde Válido hasta Asunto	V3 36 f1 1b 19 sha1RSA FNMT Clase 2 CA, FNMT, ES jueves, 18 de marzo de 1999 lunes, 18 de marzo de 2019 1 FNMT Clase 2 CA. FNMT, FS	
Clave pública	R5A (1024 Bits)	×

7. Pulsar el botón **Modificar Propiedades** y asegurarse que la opción **Habilitar todos los propósitos para este certificado** esta seleccionado:

General	Certificados cruzados
Nombre	e descriptivo: Fabrica Nacional de Moneda y Timbre
Descrip	ción:
Propo	ísitos de certificado
⊙ H.	abilitar todos los propósitos para este certificado
OD	eshabilitar todos los propósitos para este certificado
Oн	abilitar sólo los siguientes propósitos
1	Vota: sólo debe modificar los propósitos de los certificados que la ruta de acceso permite.
	🖉 Autenticación del servidor
	🔽 Autenticación del cliente
	🔽 Firma de código
	Correo seguro
	M Impresión de techa
	Firma de listas de contianza de Microsoft
	Impresion de recha de Microsoft
	Agregar propósito

Pulsar el botón **Aceptar** en todas las ventanas y Cerrar la ventana de Propiedades. Cerrar todas las ventanas abiertas de Internet Explorer y volver a Entrar en la aplicación.



Configuración de Seguridad del Internet Explorer.

1. Acceder al menú de Herramientas/Opciones de Internet de Internet Explorer



 Acceder a la pestaña de seguridad y pulsar seleccionar la zona que desee configurar (por general será Internet). Pulsar el botón de Nivel Personalizado.

Conevion	29	Programas		Oncione	es avanzadas
General	Seguri	dad	Privacid	ad	Contenido
ieleccione una le la misma.	a zona de conteni	ido Web para	especificar I	a configura	ción de segurida
Internet	National Intranet local	Sitios de confianza	Sitio: restringi	s dos	
Web qu zonas Nivel de segu	ue no ha situado e uridad de la zona-	en otras	lecer el nive	al da seguri	da d da 1a anna
Media Media - Characteria establecer el nivel de seguridad de la zona. Media - Characteria esta pero funcional - Pregunta antes de descargar contenido que pueda no ser seguro - No se descargan contreles Actively sin timar - Apropiado par la mayoría de los sitios de Internet Nivel personalizado Nivel predeterminado					
	edia Exploración segu Pregunta antes d. no ser seguro No se descargan Apropiado para ta	ra pero funcion e descargar cr contreles Acti mayoría de lo Nivel pers	nal ontenido que vest sin firma s sitios de li onalizado	e pueda ar Thomet	predeterminado



SUBDIRECCIÓN GENERAL DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

3. Asegurarse que la opción **Ejecutar componentes firmados con Authenticode** está activada.

Configuración de seguridad
Configuración:
Activar
Desactivar
Re Componentes que dependen de .NET Framework
Ejecutar componentes firmados con Authenticode
Activar
Pedir datos
Be Ejecuter componentes no firmados con Authenticode
Activar
Pedir datos
Controles y complementos de ActiveX
Restablecer configuración personal
Restablecer a: Media Restablecer
Aceptar Cancelar

4. Asegurarse que la opción Activar la secuencia de comandos de los controles de ActiveX marcados como seguros está activada:

Configuración de seguridad	
Configuración:	
Ejecutar componentes no firmados con Authenticode Activar	
Desactivar Pedir datos	
Activar la secuencia de comandos de los controles de ActiveX marcad	dos como seguros
Activar Desactivar	
Comportamientos de binarios y secuencias de comandos	
Activar	
O Aprobado por el administrador	
O Desactivar	
Restablecer configuración personal	
Restablecer a: Media Restablecer	
Aceptar Cancelar	