

Guía para configurar Thunderbird para envío de correos firmados y cifrados con certificado de la FNMT.

<u>Objeto</u>

El objeto de la guía es facilitar la configuración del cliente de correo Mozilla Thunderbird, para enviar y recibir correos firmados y cifrados con un certificado digital emitido por la FNMT, en particular el certificado de empleado público, aunque puede hacerse extensivo a otro de similares características.

Consideraciones previas

Antes de nada, se debe estar en posesión de un certificado digital emitido por la Fábrica Nacional de Moneda y timbre. En la siguiente dirección se explica cómo poder conseguirlo.

https://www.ucm.es/faq/proceso-de-solicitud-y-descarga/

Este certificado debe tener registrada la cuenta de correo electrónico que se quiere utilizar para firmar y cifrar.

Instrucciones

Por seguridad, se recomienda que el cliente esté actualizado a la última versión (32 y 64 bits indistintamente). En el momento de realizar este manual, la versión utilizada de Mozilla Thunderbird es:

68.6.0 (64-bit)

1.- Instalar certificados.

Para instalar el certificado en Thunderbird primero iremos a la siguiente ruta.

Desde el menú superior:

Herramientas -> Opciones -> (En el menú de la izquierda) Avanzado -> Pestaña Certificados

Una vez que hemos llegado hasta aquí, pulsamos en el botón "Administrar certificados"



Bandeja de entrada -	🖹 Catendario X 🛠 Opciones X
🔆 General	General Elección de datos Red y espacio en disco Actualización Certificados
Visualización	Cuando un servidor solicite mi certificado personal:
🖍 Redacción	Seleccionar uno automáticamente Preguntarme cada vez
🖵 Chat	Preguntar a los servidores respondedores de OCSP para confirmar la validez actual de los certificado
🗪 Privacidad	
🔒 Seguridad	Administrar certificados Dispositivos de seguridad
Adjuntos	
d=b	
Calendario	

Una vez pulsemos en el botón Administrar certificados, se nos abrirá una nueva venta que nos mostrará los certificados personales que tenemos instalados.

× Administrador de certificados nar uno a Sus certificados Personas Servidores Autoridades os servido Tiene certificados de estas organizaciones que le identifican tificados Nombre del certificado Dispositivo de seguridad Número de serie Caduca el 85 - FNMT-RCM Disp. software de seguridad 5:D1:D9... domingo, 30 de... :6C:92:... sábado, 18 de f... Disp. software de seguridad Ver... Hacer copia... Hacer copia de todo... Importar... Eliminar... Aceptar

Una vez aquí debemos pulsar en Importar...

Después buscaremos el certificado que hemos creado y que queremos importar para el Thunderbird.



		^			
	^	Nombre	Fecha de modifica	Tipo	Tamaño
Búsquedas		🨡 Certificado empleado publico.p12	13/03/2020 12:46	Personal Informati	8 KB
Contactos					
Descargas					
Documentos					
Escritorio					
Favoritos					

Introducimos la contraseña (deberían haberla puesto)

Una vez instalado, aparecerá el certificado bajo la pestaña "Sus certificados"

2.- Comprobar certificados de la entidad certificadora de confianza

Una vez estén instalados los certificados personales debemos asegurarnos de que estén los de la entidad certificadora instalados y configurados para poder recibir y enviar.

Primero pulsamos en la pestaña "Autoridades"

Nos vamos a la F y buscamos FNMT

Sus certificados Personas Servidores	Autoridades		
Tiene certificados guardados que identifican estas a	autoridades de certificació	ón	
Nombre del certificado		Dispositivo de seguridad	
Entrust.net Premium 2048 Secure Server CA		Builtin Object Token	
~ FNMT-RCM			
⇒ AC RAIZ FNMT-RCM		Builtin Object Token	
AC Representación	Disp. software de seguridad		
-> AC Administración Pública	Disp. software de seguridad		
AC Sector Público		Disp. software de seguridad	
AC Componentes Informáticos		Disp. software de seguridad	
AC FNMT Usuarios		Disp. software de seguridad	
AC Unidades de Sellado de Tiempo		Disp. software de seguridad	
 ✓ GeoTrust Inc. 			
GeoTrust Global CA		Builtin Object Token	
GeoTrust Primary Certification Authority - G2		Builtin Object Token	
GeoTrust Primary Certification Authority - G3		Builtin Object Token	
GeoTrust Primary Certification Authority		Builtin Object Token	
GeoTrust Universal CA		Builtin Object Token	
GeoTrust Universal CA 2		Builtin Object Token	
Ver Editar confianza Importar	Exportar Elimina	ar o dejar de confiar	



Valdría con tener instalados AC RAIZ FNMT-RCM y AC Administración Pública. Si no se tienen se pueden descargar del siguiente enlace:

https://www.sede.fnmt.gob.es/descargas/certificados-raiz-de-la-fnmt

Pulsando en importar y siguiendo el mismo procedimiento como si fueran personales.

Una vez hecho esto seleccionamos cada uno de los certificados y pulsamos en editar confianza

Nos aseguraremos que están marcados los dos tics.

	Personas Servidores Auto	ridades	
Tiene certificados guarda	dos que identifican estas autoridade	es de certificación	
Nombre del certificado		Dispositivo de seguridad	
Entrust.net Premium	2048 Secure Server CA	Builtin Object Token	
✓ FNMT-RCM			
AC RAIZ FNMT-RCM		Builtin Object Token	
AC Sector Público AC Componentes Inf AC FNMT Usuarios AC Unidades de Sella ~ GeoTrust Inc.	El certificado "" representa a una auto Editar configuraciones de confianza: Este certificado puede identificar s Este certificado puede identificar a ado	ridad certificadora. itios web. a los usuarios de correo. <u>Aceptar</u> Cancelar	
GeoTrust Global CA		Builtin Object Token	
GeoTrust Primary Ce	rtification Authority - G2	Builtin Object Token	
GeoTrust Primary Ce	rtification Authority - G3	Builtin Object Token	
Geo Irust Primary Ce	rtification Authority	Builtin Object Token	
	A	Builtin Object Token	
GeoTrust Universal C	A 2	Builtin Object Token	
GeoTrust Universal C GeoTrust Universal C			

Lo haremos en los dos certificados.

Una vez terminado pulsamos en aceptar y vamos cerrando las ventanas hasta llegar a la pantalla inicial del correo.

3.-Seleccionar certificados

Para seleccionar el certificado que queremos usar para firmar y cifrar correos (en este caso el de empleado público) seleccionaremos del menú superior:

Herramientas -> configuración de cuenta -> y en el menú de la izquierda seguridad (de la cuenta que hayamos dado de alta al solicitar el certificado)



	Seguridad								
Configuración del servidor Copias y carpetas	Para enviar y ree	cibir mensajes firmados o c	ifrados, debe especificar tanto un certificado pa	ara firma digital como uno para cifi	ado.				
Redacción y direcciones Correo no deseado	Firmado digita Usar este certif	il īcado para firmar los mens	ijes que envíe:						
Sincronización y almacena Seguridad de OpenPGP Acuses de recibo	Firmar men	ısajes <u>d</u> igitalmente		Seleccionar	Limpiar				
	Cifrado Usar este certif	icado para cifrar/descifrar r	nensajes enviados a Vd.:	Sele <u>c</u> cionar	Li <u>m</u> piar				
Configuración del servidor Copias y carpetas Redacción y direcciones Correo no deseado	Cifrado elegido <u>N</u> unca (no Si <u>e</u> mpre (no	o para enviar mensajes: usar cifrado) o podrá enviar si algún rece	ptor carece de certificado)						
Sincronización y almacena Seguridad de OpenPGP Acuses de recibo Seguridad	Certificados	Administrar certificados	Dispositivos de seguridad						

Seleccionamos el certificado que queremos para firmar.

and a contract	Seguridad	
Configuración del servidor Copias y carpetas	Para enviar y recibir mensajes firmados o cifrados, debe especificar tanto un certificado para firma digital como uno para	i cifrado.
Redaccion y direcciones Correo no deseado	Firmado digital	
Sincronización y almacena Seguridad de OpenPGP Acuses de recibo	DNI Sec control of an annu of mension of the second s	. <u>L</u> impiar
Seguridad Seguridad Segurances Configuración del servidor Copias y carpetas Redacción y direcciones Correo no deseado	Thunderbird × Debería específicar también un certificado para que lo usen otras personas cuando le envien mensajes cifrados. ¿Quiere utilizar el mismo certificado para cifrar y descrifrar mensajes enviados a Vd.? nar. Si No Sigmpre (no podra enviar si algún receptor carece de certificado)	. Lī <u>m</u> piar
Sincronización y almacena Seguridad de OpenPGP Acuses de recibo Seguridad Carpetas locales	Certificados Administrar certificados Dispositivos de seguridad	

Configuración sin conexión

Nos preguntara que si queremos utilizar el mismo certificado para firmar.

Seleccionamos la opción deseada. (Recomendado SI)

En esta pantalla Seleccionamos las opciones que se ajusten a nuestras necesidades.

Podemos seleccionar **"Firmar mensajes digitalmente**" para que lo haga por defecto. En cualquier caso, siempre podremos seleccionarlo desde el menú general. hacerlo desde el menú general.

4.- Para Firmar Mensajes



Pulsamos en redactar mensaje, rellenamos los campos de asunto, para, etc,

Pulsamos en Opciones en el menú superior (del mensaje) y elegimos "firmar digitalmente este mensaje"

rchivo <u>E</u> c	litar <u>v</u> er <u>i</u>	nsertar Formato	Opciones Enigmail Herramientas Ayuda	3		
🕼 Enviar	A Ortog	rafía 🗸 🔒	Revisar <u>o</u> rtografía Ctrl+Mayús.+P Revi <u>s</u> ar mientras escribe			
	<u>D</u> e:		Citar <u>m</u> ensaje	@ucm.es		
××	Para:		Acuse <u>d</u> e recibo <u>N</u> otificación de estado de entrega			
	A <u>s</u> unto:		<u>C</u> odif. de caracteres > <u>F</u> ormato de entrega >			
Párrafo	~	Anchura variable	Prioridad > Enviar una copia a >			
			Personalizar dirección De			
	N I V D B		Cifrar <u>e</u> ste mensaje <u>F</u> irmar digitalmente este mensaje 是			

Enviamos el mensaje y listo.

5.- Para Cifrar mensajes

Para poder cifrar mensajes, **necesitamos tener instaladas las claves públicas de los certificados de empleado público o de la FNMT de las personas a las que queremos enviar los mensajes cifrados**. Hay varias formas de conseguir estas claves. Bien nos las pueden enviar directamente o también las podemos extraer de su firma de mensajes que envíen firmados.

• Si nos la envían.

Tenemos que estar seguros que el medio por el que nos la han enviado es seguro y que la persona que nos la envía es quien dice ser.

Una vez tengamos la clave publica la debemos instalar, para ello, accedemos a la misma ventana del punto 1.

Herramientas->opciones->avanzado->certificados->administrar certificados

Esta vez seleccionamos pestaña "Personas"



Sus certificados	Personas	Servidores	Autoridades	
liene certificados gua	ardados que ide	entifican estas pe	onas	
Nombre del certifica	ido		Dirección de correo electr.	Caduca el
Actalis S.p.A./03358	3520967			
boletines@incibe	e.es		boletines@incibe.es	sábado, 7 de noviem
COMODO CA Limit	ed			
E=boletines@ind	tibe.es		boletines@incibe.es	domingo, 10 de novi
 Entrust, Inc. 				
<u> Karimatina (</u>			@crowdstrike.com	lunes, 21 de diciemb
✓ FNMT-RCM				
			@uclm.es	lunes, 27 de marzo d
			@ucm.es	domingo, 30 de ener
~ TERENA			Lange -	
Canonio canoria			@uv.es	domingo, 9 de mayo
			@cttc.es	lunes, 29 de noviem
			@rediris.es	lunes, 11 de julio de
	in the second second		@rediris.es	viernes, 23 de julio d
			@upvnet.upv.es	miércoles, 12 de may
Ver. Imp	ortar Exc	oortar Flim	ar	

Le damos a importar y realizamos el procedimiento igual que los anteriores.

Los certificados se irán colocando bajo el epígrafe de su entidad certificadora. En nuestro caso, si son los de Empleado público, se colocarán bajo el epígrafe FNMT-RCM.

Aquellas personas de las que no tengamos su clave publica para cifrar no podrán ser destinatarios de nuestros correos cifrados.

• Si la extraemos de un certificado

Otra opción para conseguir la clave pública es desde un mensaje firmado por alguien con certificado valido.

Una vez recibido el mensaje firmado.

•	¥ ♥ ☆ ☆	Asunto [Avisos] Boletin de INCIBE-CERT del 16-03-2020 A Message to our Customers and Partners	90 0 0	Fecha 16/03/2020 16/03/2020 16/03/2020 1	→ Partic 11:16 BOLE 11:13 ¶	ipantes TINES INCIBE-C	6 0 0	Tama 20,7 38,3 16,3	ño E KB KB
	De J Asunto A Cc			→ Reenviar	Archivar	No deseado	10 EI	iminar 16/03/2	Más 🔪



Pulsamos sobre el sobre que nos sale arriba a la derecha que nos indica que el mensaje está firmado (con el botón izquierdo)

Seguridad del mensaje	\times
El mensaje está firmado	
este mensaje incluye una firma digital valida. El mensaje no ha sido manipulado desde que se envió.	
Firmado por:	
Direcciones de correo electrónico:	
Certificado emitido por: AC Administración Pública	
Ver certificado de la firma	
El mensaje no está cifrado	
Este mensaje no fue cifrado antes de ser enviado. La información que se manda a Internet sin cifrar puede ser vista por otras personas mientras llega a su destino.	
Aceptar	2

Nos saldrá este mensaje y pulsamos en "Ver certificado de la firma"

Elegimos la pestaña detalles y seleccionamos en los campos del certificado "clave

pública del sujeto.

			1003							
✓ AC A	Admini	straciór	Públio	а						
			-							
Campos	s del ce	ertificad	lo							
	Asun	to								-
	r Infor	mación	de la c	lave pú	blica d	el suje	0			
	A	goritmo	o de la	clave p	iblica (del suje	to			
	CI	ave púk	olica de	l sujeto		4		-		
	- Exter	isiones								
	N	ombre a	alternat	ivo del	asunto	del ce	rtifica	obe		
	Re	estriccio	nes bá	sicas de	certifi	cado				
Valor de	el cam					<u>.</u>				
lódulo	(204	8 bits):							
	50 25	00.54	-2 2	3 66 1	h 2f	89 00	b6	98	bd	
57 b8	03 5b	54		7 00 1	0 21		- 20			
		31	20 8	53 c	b 4c	94 e	2 7b	c8	69	
91 cc	ba 4c	a1 8b	3c 0	5 2c ł	3 85	69 f	F 6b	db	c8	
		04 74	Ac c	a de a	a 7e	e1 7	2 f2	e2	16	

Pulsamos en "exportar".



Guardamos la clave en formato crt donde queramos y la instalamos siguiendo las instrucciones anteriores.

6.- Para comprobar si un mensaje firmado o cifrado es corecto

Para comprobar si un mensaje está firmado con un certificado valido, pulsamos sobre el sobre que nos sale arriba a la derecha que nos indica que el mensaje está firmado (con el botón izquierdo)



Nos saldrá el siguiente mensaje en el que nos indicará si la firma digital es válida y que no ha sido manipulado desde que se envió.

e	guridad del mensaje
EI E:	m ensaje está firmado ste mensaje incluye una firma digital válida. El mensaje no ha sido manipulado esde que se envió.
F	Firmado por:
[Direcciones de correo electrónico:
(Certificado emitido por: AC Administración Pública
[Ver certificado de la firma
EI	mensaje no está cifrado
E: In	ste mensaje no fue cifrado antes de ser enviado. La información que se manda a iternet sin cifrar puede ser vista por otras personas mientras llega a su destino.
	Aceptar

En el caso de que esté cifrado nos mostrará un candado al lado derecho del sobre que indica que está firmado.



Si pulsamos en el sobre o el candado que nos sale arriba a la derecha que nos saldrá la siguiente ventana que indica que el mensaje está firmado con un certificado valido y además está cifrado



Fl mensaje está firmado	7
Este mensaje incluye una firma digital válida. El mensaje no ha sido manipulado desde que se envió.	
Firmado por:	
Direcciones de correo electrónico:	
Certificado emitido por: AC Administración Pública	
Ver certificado de la firma	
El mensaje está cifrado	
Este mensaje fue cifrado antes de ser enviado. El cifrado hace muy dificil que otr personas puedan ver información mientras ésta viaja por la red.	35
	ar