

UNIVERSIDAD Servicio de Informática y DE BURGOS

Firmado y cifrado de mensajes de correo electrónico

Autor: Pedro R. Benito da Rocha <pedro@ubu.es>

Última modificación: 01/07/2022

Requisitos previos	2
Cliente Outlook	3
Windows	3
Lectura de un mensaje firmado	3
Envío de un mensaje firmado	5
Lectura de un mensaje encriptado	5
Envío de un mensaje encriptado	6
macOS	7
Lectura de un mensaje firmado	7
Lectura de un mensaje encriptado	7
Envío de un mensaje firmado	7
Envío de un mensaje encriptado	8
Cliente Mozilla Thunderbird	9
Pasos previos	9
Configurar certificados raíz	9
Configuración del certificado de usuario	9
Lectura de mensajes firmados	11
Envío de mensajes firmados	11
Lectura de mensajes encriptados	11
Envío de mensajes encriptados	12
Outlook en la web (OWA)	13
Navegador Edge (solo Windows)	13
Lectura de mensajes firmados	13
Envío de mensajes firmados	14
Lectura de mensaje cifrados	15
Envío de mensaies cifrados	15



UNIVERSIDAD | Ser DE BURGOS | Con

Servicio de Informática y Comunicaciones

Requisitos previos

Para poder enviar un mensaje firmado es necesario:

- Certificado digital asociado a la cuenta de correo. Las pruebas se han hecho con un certificado digital de la FNMT para empleado público. Se puede usar el configurador de la FNMT para instalar los certificados, o se pueden desde cargar desde la página web de la FNMT¹.
- Cliente con capacidad de firmado de correos electrónicos mediante S/MIME usando certificados digitales.

Para poder enviar un mensaje encriptado es necesario:

- Certificado digital asociado a la cuenta de correo. Las pruebas se han hecho con un certificado digital de la FNMT para empleado público.
- Cliente con capacidad de encriptado de correos electrónicos mediante S/MIME usando certificados digitales.
- Certificado del destinatario. Para ello se debe haber intercambiado el certificado (parte pública), por ejemplo enviando un mensaje firmado.

Para poder leer un mensaje firmado:

- Cliente con capacidad de leer mensajes firmados con S/MIME.
- Certificado raíz de la entidad certificadora configurado para su uso en correo electrónico.

Para poder leer un mensaje encriptado:

- Cliente con capacidad de leer mensajes encriptados con S/MIME.
- Certificado raíz de la entidad certificadora configurado para su uso en correo electrónico.
- Certificado (parte pública) del remitente.

¹ https://www.sede.fnmt.gob.es/descargas/certificados-raiz-de-la-fnmt



Cliente Outlook

Windows

Lectura de un mensaje firmado

Los correos firmados se distinguen por una insignia que indica esta circunstancia.



Al abrir el mensaje aparece la insignia a color en la parte superior derecha.

Correo firmado





Este correo está firmado digitalmente.

Haciendo clic en la insignia se muestra la información relativa a la validez de la firma del mensaje.



Para que una firma válida sea reconocida tan solo es necesario que el certificado raíz del remitente esté instalado en el almacén de certificados del sistema. El certificado raíz debe tener activada la función "Correo seguro". Muchas de las firmas digitales ya están reconocidas por el sistema, pero en algunos casos es necesario indicar al sistema que debe usar para correo seguro los certificados que tiene instalados.

Los certificados personales que ofrece la FNMT a los ciudadanos y los certificados de empleado público necesitan la configuración que vamos a describir a continuación.

Para utilizar los certificados de la FNMT se puede usar el configurador que se descarga desde <u>https://www.sede.fnmt.gob.es/descargas/descarga-software/instalacion-software-generacion-de-claves</u>. Este programa hay que ejecutarlo con permisos de administrador.





El configurador instalará los certificados, tras lo cual debemos activar su uso para el correo seguro como se ha descrito anteriormente.

Desde Opciones de Internet > Contenido > Certificados se seleccionará la pestaña en la que se encuentre el certificado raíz, se seleccionará y se pulsará en el botón "Opciones avanzadas".

	1000000						-
Entidades de certifica	ción int	ermedias	Entidades de ce	ertificación raíz	de confianza	Editore	4
Emitido para		Emitido p	or	Fecha de	Nombre desc	riptivo	^
AAA Certificate Ser AAA Ce		AAA Cer	tificate Services	01/01/2029	Sectigo (AAA)		
AC RAIZ FNMT	RCM	AC RAIZ	FNMT-RCM	01/01/2030	AC RAIZ FN	ит	
AddTrust Exter	nal	AddTrust	External CA	30/05/2020	Sectigo (Add	Trust)	
Autoridad de C	ertifi	Autorida	d de Certifica	31/12/2030	CAROOT Firr	map	
Baltimore Cybe	Tru	Baltimore	CyberTrust	13/05/2025	DigiCert Balti	mor	
Class 3 Public P	rima	Class 3 P	ublic Primary	02/08/2028	VeriSign Clas	s 3	
COMODO RSA	Cert	COMODO	RSA Certific	19/01/2038	Sectigo (form	nerl	
Copyright (c) 1	997	Copyrigh	t (c) 1997 Mi	31/12/1999	Microsoft Tim	est	*
Importar Exp	ortar		Quitar		Opciones a	avanzad	as
Propósitos planteado Autenticación del clie	s del ce nte, Fir	rtificado ma de doc	umento, Correo	seguro, Auten	ticación		
del servidor, Impresio	ón de fe	cha				Ver	

Aparecerá un cuadro de diálogo en el que hay que marcar la opción "Correo seguro", y luego aceptar los cambios.

Seleccione uno propósitos ava	o más propósitos que figurarán (anzados.	en la lista de	
Propósitos de	certificado:		
Autentica	ción del servidor		^
Autentica	ción del diente		
✓ Firma de	código		
	guro de fecha		~
<		>	
ormato de exp	portación		
	ormato de exportación predeterm	inado que se usar	a
Seleccione el fo cuando arrastr	e y coloque un certificado en una	carpeta de	
Seleccione el fo cuando arrastr archivos.	e y coloque un certificado en una	carpeta de	
Seleccione el fo cuando arrastr archivos. Formato de	DER binario codificado X 509 ((* cer)	,



Envío de un mensaje firmado

Antes de poder enviar correos firmados y/o encriptados se debe configurar el certificado digital a utilizar. Para ello hay que ir a Archivo > Opciones > Centro de confianza > Configuración del Centro de confianza > Seguridad del correo electrónico.

Centro de confianza				?	×
Editores de confianza	Correo e	lectrónico cifrado			
Opciones de privacidad Inicio de sesión basado en formularios	<u> </u>	 Cifrar contenido y datos adjuntos para mensajes sali Agregar firma digital a los mensajes salientes 	entes		
Seguridad del correo electrónico		 Enviar mensaje firmado de <u>t</u>exto no cifrado al enviar 	mensajes firmados		
Tratamiento de datos adjuntos		Solicitar confirmación S/MIME para todos los mensa	ajes S/MIME firmados		
Descarga automática		Con <u>f</u> iguración predeterminada:	▼ <u>C</u> onfi	iguración	

Hay que elegir la configuración predeterminada con el botón "Configuración", donde podemos elegir el certificado digital a usar, en el caso de tener varios. Para seleccionar los certificados se debe pulsar el botón "Elegir".

Nombre de configuraci	ón de seg	guridad:		
1				```
Formato de cifrado:	S/MIM	IE		
Configuración pred	eterminad	la para todos lo	os mensajes cifrad	los
Etiquetas de segur	idad	Nueva	Eliminar	
Etiquetas de segur Certificados y algoritmo	idad	Nueva	Eliminar	
Etiquetas de segur Certificados y algoritmo Certificado de firma:	idad	Nueva	Eliminar	Elegir
Etiquetas de segur Certificados y algoritmo Certificado de firma: Algoritmo de tipo hash	idad os	Nueva	Eliminar	Elegir
Etiquetas de segur Certificados y algoritmo Certificado de firma: Algoritmo de tipo hash Certificado de cifrado:	idad os	Nueva	Eliminar	Elegir Elegir

Aquí podemos elegir "Agregar firma digital a los mensajes salientes" si queremos que se firmen todos los mensajes salientes. <u>Si queremos firmar de forma manual cada uno de los mensajes que enviemos, no hay que marcar esta casilla</u>.

La firma manual de los mensajes se realiza desde Nuevo correo electrónico > Opciones > Firmar.

Archivo Mensaje Inser	rtar Opciones	Formato de	texto Revisar Ayuda 🛛 Ç ¿Qué desea	hac	er?	
Aa Colores *		A A	Solicitar una confirmación de entreg	a	1	A B
Temas Color de	CCO De	Cifrar Firmar	Utilizar botones Solicitar una confirmación de lectura de voto ~	ġ.	Guardar elemento Retra enviado en ∽ entre	sar Dirigir ga respuestas a
Temas	Mostrar campos	Cifrar	Seguimiento	Iي ا	Más opcione	s I

Ahora al enviar el mensaje éste estará firmado.

Lectura de un mensaje encriptado

Es necesario haber intercambiado previamente un mensaje firmado por nosotros para que el remitente pueda cifrarlo. Si hemos recibido un mensaje firmado por la persona que nos envía el correo encriptado, y a su vez hemos enviado un correo firmado por nosotros, ambos podremos intercambiar correos encriptados.



Nota: El correo encriptado solamente se puede leer desde el cliente de correo en el que previamente hemos guardado la clave pública de la otra persona.

Los mensajes encriptados aparecen marcados con un candado en la lista de mensajes.

Todo	No leídos	Por Fecha 🗸	î
Mensaje	encriptado	0 🛆 ma. 11:47	

Esto indica que el emisor ha enviado el mensaje encriptado y solamente lo podemos desencriptar nosotros. Los mensajes encriptados aparecen en el panel de lectura con un candado.

Envío de un mensaje encriptado

Para enviar un mensaje encriptado es necesario haber recibido previamente un mensaje firmado de la persona a la que se va a enviar el mensaje encriptado.

Desde la cinta seleccionamos Opciones > Cifrar. El mensaje se enviará encriptado y solamente el destinatario podrá acceder a su contenido.

<u> 日 </u>	ע ז ט			Mensaje	cifrado - Men	isaje (HTML)			æ			×
Archivo	Mensaje	Insertar	Opciones	Formato de texto	Revisar	Ayuda	♀ ¿Qué de	esea hacer?				
Aa ····································			8		Solicitar	una confirmaciór	n de entrega	Ľ⊻	27	2	3	
Temas V	Color de página ~	CCO De	Cifrar Fin	mar Utilizar boton de voto ~	es 🗌 Solicitar	una confirmaciór	n de lectura	Guardar element enviado en ~	o Retrasa entrega	r Diri a respue	gir stas a	
Temas	s	Mostrar campo	Cifrar		Seguim	iento	آ <u>د</u> ا	Más o	opciones		F3	^
) Enviar	Para			ع								
	Asunto	Mensaje	cifrado									
Cifrado con O	Dutlook.											



macOS

El cliente Microsoft Outlook de macOS está disponible a través de la suscripción A3 de Office 365.

Para poder utilizar las capacidades de firmado y encriptado primero hay que tener instalado el certificado digital en el ordenador. Una vez instalado se ha de ir a Preferencias > Cuentas, elegir la cuenta (si hubiera varias) y seleccionar el botón "Seguridad" del panel de la derecha, abriéndose un cuadro de diálogo en que se ha de elegir el certificado para la firma y para el encriptado de correo:

Certificado:	Distanciana dia histophysionik
	Firmar siempre los mensajes salientes
	Enviar mensajes firmados digitalmente como texto no cifrado
	Incluir mis certificados en los mensajes firmados
	IME
Cifrado S/M	
Cifrado S/M Certificado:	(Alteriodicie dialectric destanticity, Televised and a second second second second second second second second
Cifrado S/M Certificado:	Ciferra siempre los mensajes salientes

En este mismo cuadro de diálogo se puede elegir firmar y/o cifrar todos los mensajes salientes.

Lectura de un mensaje firmado

Tan solo es necesario que el certificado raíz del remitente esté instalado en el llavero del sistema.

Lectura de un mensaje encriptado

Es necesario haber intercambiado previamente un mensaje firmado por nosotros para que el remitente pueda cifrarlo. No es necesaria ninguna acción especial por parte nuestra.

Envío de un mensaje firmado

Para enviar un mensaje firmado se ha de disponer de un certificado como se ha indicado previamente. Se utiliza el botón "Nuevo mensaje" como si fuéramos a redactar un correo normal y corriente. Si no se ha seleccionado "Cifrar siempre los mensajes salientes" en el cuadro de diálogo de la configuración de los certificados será necesario, desde la composición del mensaje, ir al menú Borrador > S/MIME:

Borrador	Formato	Herramientas	Ventana	Ayuda
Enviar		¥⇔		
Enviar más t	arde			
Expandir list	a de distri	bución 🐴 E		
Datos adjun	tos	>		
Insertar vínc	ulo	>		
Firmas		>		
Cifrar		>		
S/MIME		>	Cifrar co	on S/MIME
Clasificar			Agregar	firma digital
Cidsifical			mensaje)	
Solicitar con	firmación	>		
Descartar		H D	ot	
		ton viola provia a	ad mensaje)	



Desde la opción "Agregar firma digital" se indica que se desea firmar el mensaje.

Esta operación hay que realizarla <u>ANTES</u> de escribir los destinatarios del mensaje, o no aparecerá en el menú.

Una vez redactado el mensaje y añadidos los destinatarios es posible que se nos solicite varias veces las credenciales de inicio de sesión para acceder al llavero. Esto es necesario ya que macOS protege el llavero donde se almacenan los certificados para evitar accesos no autorizados a las claves.

Envío de un mensaje encriptado

Para enviar un mensaje encriptado primero hay que disponer del certificado (parte pública) del destinatario. Este certificado se obtiene de un mensaje firmado que nos haya enviado previamente.



Este correo está firmado digitalmente.

Desde el mensaje firmado, se selecciona Detalles > Agregar certificado de encriptado a los contactos. Ahora ya se puede enviar correo encriptado con éste usuario.



Si ya tenemos añadido el certificado, utilizamos el botón "Nuevo mensaje" como si fuéramos a redactar un correo normal y corriente. Si no se ha seleccionado "Cifrar siempre los mensajes salientes" en el cuadro de diálogo de la configuración de los certificados será necesario, desde la composición del mensaje, ir al menú Borrador > S/MIME y seleccionar "Cifrar con S/MIME":

Borrador Formato	Herramientas	Ventana	Ayuda
Enviar Enviar más tarde	G ¥		
Expandir lista de distrib	oución ^% E		
Datos adjuntos	>		
Insertar vínculo	>		
Firmas	>		
Cifrar	>		
S/MIME	>	Cifrar co	on S/MIME
Clasificar	>	Agregar mensaje)	firma digital
Solicitar confirmación	>	,	
Descartar	¥ 9	ot	

El mensaje se enviará encriptado y solamente podrá abrirlo el destinatario.





Cliente Mozilla Thunderbird

Pasos previos

Configurar certificados raíz

Mozilla Thunderbird soporte S/MIME, tanto para enviar correo como para recibir.

Como paso previo, para que se pueda reconocer la firma de los mensajes es necesario que el certificado raíz del emisor esté instalado y además su uso para correo electrónico esté activado. Desde las preferencias de Thunderbird accedemos a "Privacidad y Seguridad" > Seguridad > Certificados, y elegimos el botón "Administrar certificados".

Certificados

Cuando un servidor solicite mi certificado personal:

🔘 Seleccionar uno automáticamente 🔘 Preguntarme cada vez



actual de los certificados

Administrar certificados... Dispositivos de seguridad..

Buscamos el certificado raíz en "Autoridades" y pulsamos el botón "Editar confianza":

		Administr	ador de certif	icados			>
Sus certifi	cados Deci	siones de autentio	cación	Personas	Servidores	Autoridades	
iene certificad	dos guardados que	identifican estas a	autoridades de	certificación			
Nombre del c	El certificado ""	representa a una auto	oridad certificado	ra.			C.
V FNMT-RCM	Editar configurad	ciones de confianza:					
AC RAIZ	Este certifica	do puede identificar	sitios web.				
AC RAIZ	F Ste certifica	do puede identificar	a los usuarios de	correo.			
AC Secto	n			Cance	lar Aceptar		
AC Admi	n						
AC FNM	T Usuarios		Disp. so	ftware de seg	uridad		
Vor	Editor configera	Importor	Exportar	Eliminar o	laiar de confiar		
vei	Eultar connanza	importai	Exportai	Emminal O C	lejar de connar		
						Acepta	r

Por último, seleccionamos "Esta certificado puede identificar a los usuarios de correo." y Pulsamos "Aceptar". Ahora Thunderbird ya puede utilizar correctamente el certificado.

Configuración del certificado de usuario

Thunderbird utiliza su propio almacén de certificados, por lo que instalar un certificado en el sistema operativo (por ejemplo, en Windows, usando las opciones de Internet) no sirve para utilizar correo seguro en Thunderbird.

Desde las preferencias de Thunderbird vamos a "Configuración de la cuenta". Seleccionaremos la cuenta que deseamos configurar e iremos a la sección "Cifrado extremo a extremo". En la sección S/MIME debemos importar y seleccionar el certificado de usuario que queremos utilizar.



UNIVERSIDAD | DE BURGOS |

Servicio de Informática y Comunicaciones

Para importar el certificado hacemos clic en el botón "Administrar certificados S/MIME", buscamos el fichero con el certificado y lo importamos.

 Dedro@ubu.es Configuración del servidor Copias y carpetas Redacción y direcciones Correo no deseado Sincronización y almacenami Cifrado extremo a extremo Acuses de recibo Carpetas locales Correo no deseado Espacio en disco Servidor de salida (SMTP) 	S/MIME Certificado persona Certificado persona Administrar certif Configuración pro Sin cifrado de extre correo y a la vigilan O No activar cifra	l para la firma digi l para cifrado: ficados S/MIME edeterminada pa mo a extremo los o cia masiva. frado por defecto	Dispositivos de seguridar Dispositivos de seguridar ra el envío de mensajes ontenidos del mensaje que	Seleccion Seleccion d S/MIME edan expuestos fácilmente	nar Limpiar nar Limpiar		
Configuración del servidor Copias y carpetas Redacción y direcciones Correo no deseado Sincronización y almacenami Cifrado extremo a extremo Acuses de recibo Correo no deseado Espacio en disco Servidor de salida (SMTP)	Certificado persona Certificado persona Administrar certi Configuración pro Sin cifrado de extre correo y a la vigilan O No activar cifra	I para ia Tirma digi I para cifrado: ficados S/MIME edeterminada pa mo a extremo los o cia masiva. frado por defecto	Dispositivos de seguridar ra el envío de mensajes ontenidos del mensaje que	Seleccion Seleccion d S/MIME edan expuestos fácilmente	nar Limpiar nar Limpiar		
Copias y carpetas Redacción y direcciones Correo no deseado Sincronización y almacenami Cifrado extremo a extremo Acuses de recibo Correo no deseado Espacio en disco Servidor de salida (SMTP)	Certificado persona Administrar certin Configuración pro Sin cifrado de extre correo y a la vigilan O No activar cir O Requerir cifra	l para cifrado: ficados S/MIME edeterminada pa mo a extremo los o cia masiva. frado por defecto	Dispositivos de seguridar ra el envío de mensajes ontenidos del mensaje que	Seleccion Seleccion d S/MIME edan expuestos fácilmente	nar Limpiar nar Limpiar		
Redacción y direcciones Correo no deseado Sincronización y almacenami Cifrado extremo a extremo Acuses de recibo Correo no deseado Espacio en disco Servidor de salida (SMTP)	Certificado persona Administrar certif Configuración pro Sin cifrado de extre correo y a la vigilan O No activar cifra	I para cifrado: ficados S/MIME edeterminada pa mo a extremo los o cia masiva. frado por defecto	Dispositivos de seguridar ra el envío de mensajes ontenidos del mensaje que	Selegcion d S/MIME edan expuestos fácilmente	e a su proveedor de		
Correo no deseado Sincronización y almacenami Cifrado extremo a extremo Acuses de recibo Carpetas locales Correo no deseado Espacio en disco Servidor de salida (SMTP)	Administrar certii Configuración pro Sin cifrado de extre correo y a la vigilan O No activar cir O Requerir cifra	ficados S/MIM <u>E</u> edeterminada pa mo a extremo los o cia masiva. irado por defecto	Dispositivos de seguridar ra el envío de mensajes ontenidos del mensaje que	d S/MIME edan expuestos fácilmente	e a su proveedor de		
Sincronización y almacenami Cifrado extremo a extremo Acuses de recibo Carpetas locales Correo no deseado Espacio en disco Servidor de salida (SMTP)	Administrar certif Configuración pre Sin cifrado de extre correo y a la vigilan No activar cir Requerir cifra	ficados S/MIM <u>E</u> edeterminada pa mo a extremo los o cia masiva. irado por defecto	<u>D</u> ispositivos de seguridar ra el envío de mensajes ontenidos del mensaje que	d S/MIME edan expuestos fácilmente	e a su proveedor de		
Cifrado extremo a extremo Acuses de recibo ~ Carpetas locales Correo no deseado Espacio en disco Servidor de salida (SMTP)	Administrar certif	edeterminada pa mo a extremo los o cia masiva. irado por defecto	Dispositivos de segundar ra el envío de mensajes ontenidos del mensaje que	d S/MIME edan expuestos fácilmente	e a su proveedor de		
Acuses de recibo Carpetas locales Correo no deseado Espacio en disco Servidor de salida (SMTP)	Configuración pro Sin cifrado de extre correo y a la vigilan No activar cir Requerir cifra	edeterminada pa mo a extremo los o cia masiva. irado por defecto	ra el envío de mensajes ontenidos del mensaje que	edan expuestos fácilmente	e a su proveedor de		
✓ ■ Carpetas locales Correo no deseado Espacio en disco ※ Servidor de salida (SMTP)	Configuración pro Sin cifrado de extre correo y a la vigilan O No activar cif Requerir cifra	edeterminada pa mo a extremo los o cia masiva. frado por defecto	ra el envío de mensajes ontenidos del mensaje qui	edan expuestos fácilmente	e a su proveedor de		
Correo no deseado Espacio en disco ⊗Servidor de salida (SMTP)	Sin cifrado de extre correo y a la vigilan No activar cir Requerir cifra	mo a extremo los c cia masiva. írado por defecto	ontenidos del mensaje qu	edan expuestos fácilmente	e a su proveedor de		
Espacio en disco Servidor de salida (SMTP)	correo y a la vigilan No activar cit <u>R</u>equerir cifra 	cia masiva. írado por defecto					
®Servidor de salida (SMTP)	 No activar cit <u>R</u>equerir cifra 	irado por defecto					
	<u>R</u> equerir cifra						
		ido por defecto					
	Si necesita ci	frado, para enviar un	mensaje debe tener la clave	pública o certificado de cada	a destinatario.		
	Una firma digital pe	ermite a los destina	tarios verificar que el men	saje fue enviado por usted	l y que el contenido		
	no ha sido modifica	ido.					
	🦳 Aña <u>d</u> ir mi firma	digital de forma pr	edeterminada				
Adm	inistrador de certificados		×				
Adm Sus certificados Decisiones de au	no na sido modifica Añadir mi firma inistrador de certificados tenticación Persona	ido. digital de forma pr s Servidores	edeterminada × Autoridades				
ne certificados de estas organizaciones o Iombre del certificado Dispositivo	que le identifican o de seguridad 🛛 🗍 No	imero de serie	Caduca el 🛛				

A continuación, debemos usar el botón "Seleccionar" para elegir el certificado que deseamos utilizar.

🖸 Bandeja de entrada 🛛 🔅 Preferenc	ias 🗙 🔟 Configuración de la cuenta 🗙	Ē	E.	-	٥	×
✓ ☑ <u>pedro@ubu.es</u> Configuración del servidor Copias y carpetas	S/MIME Certificado personal para la firma digital: Certificado personal para cifrado:	iar				~
Redacción y direcciones Correo no deseado Sincronización y almacenami	Seleccionar Limpi Administrar certificados S/MIME Dispositivos de seguridad S/MIME	iar				
Cifrado extremo a extremo Acuses de recibo Correo no deseado Espacio en disco Servidor de salida (SMTP)	 Configuración predeterminada para el envío de mensajes Sin cifrado de extremo a extremo los contenidos del mensaje quedan expuestos fácilmente a su proveedor correo y a la vigilancia masiva. No activar cifrado por defecto Requerir cifrado por defecto Si necesita cifrado, para enviar un mensaje debe tener la dave pública o certificado de cada destinatario. Una firma digital permite a los destinatarios verificar que el mensaje fue enviado por usted y que el content no ha sido modificado. 	de ido				



Seleccione certificado		×
Certificado:	u da recha petro da recha da la construcción da recha da la construcción da la construcción da la construcción	×
Detalles del certificad	lo seleccionado:	
Emitido a: CN=E	H,giv	renName=Performance, Statute DA
COMUNICACIONES, O	U=CERTIFICADO ELECTRONICO DE EMPLEADO	PUBLICO,O=UNIVERSIDAD DE
BURGOS, C=ES	Out of the Date of the P	
Válido de martes 15	de marzo de 2022 10:45:02 a sábado 15 de marz	o de 2025 10:45:02
Correo electrónico:	pedro@ubu.es	
Emitido por: CN=AC	Sector Público, OID.2.5.4.97=VATES-Q2826004J, O	U=Ceres,O=FNMT-RCM,C=ES
Guardado en: Disp. so	ftware de seguridad	~

Thunderbird nos sugiere usar el mismo certificado para los mensajes encriptados. Si vamos a usar esta característica contestamos "Sí".

Thunde	bird		×
?	Debería especificar también un certificado para que lo usen otras perso	onas cuando le	envíen
	mensajes cifrados. ¿Quiere utilizar el mismo certificado para cifrar y de	scrifrar mensaje	25 enviados a
	Vd.?	<u>S</u> í	<u>N</u> o

Lectura de mensajes firmados

Si se han seguido los pasos previos, Mozilla Thunderbird reconocerá los mensajes firmados, y en el caso de que la firma sea correcta se mostrará un icono en la parte derecha del encabezado indicando esta situación.

S/MIME 🞗

Haciendo clic en el icono se puede obtener más información sobre la firma del mensaje.

Envío de mensajes firmados

Para enviar un mensaje firmado basta con usar la opción Seguridad > Firmar digitalmente este mensaje al redactar el mensaje.



El mensaje será firmado cuando pulsemos el botón "Enviar".

Lectura de mensajes encriptados

Los mensajes encriptados que pueden ser leídos correctamente tiene éste icono en la parte derecha del encabezado:

S/MIME 🔒

Un correo puede estar cifrado y firmado, con lo que aparecen los dos iconos:



S/MIME 🛃 🤱

Para que un mensaje encriptado pueda ser leído es necesario haber intercambiado con el remitente al menos un correo firmado. De esta forma ambos intervinientes tienen la información necesaria para poder cifrar y descifrar el mensaje.

Envío de mensajes encriptados

Como paso previo deberemos haber recibido correctamente un mensaje firmado por el remitente.

Desde la redacción del mensaje seleccionamos la opción Seguridad > Requerir cifrado.



Este mensaje está cifrado con Thunderbird.

Si todo está correcto, se enviará el mensaje cifrado.





Outlook en la web (OWA)

Navegador Edge (solo Windows)

Para poder acceder a la firma y cifrado de mensajes es necesario tener la última versión del navegador Edge.

Lectura de mensajes firmados

Los correos firmados se distinguen por una insignia que indica esta circunstancia.



Por defecto, el navegador no soporta la comprobación de mensajes firmados. Para poder procesar la firma de los mensajes hay que instalar una extensión en el navegador. Esta circunstancia se indica con el siguiente mensaje:

No se puede verificar la firma digital de este mensaje. Este mensaje tiene una firma digital, pero no se ha comprobado porque la extensión S/MIME no está instalada. Para instalar la extensión, haga clic aquí.

Al hacer clic en el enlace se accede a la página de descarga del complemento de Edge para S/MIME². Las funcionalidades de S/MIME requieren la instalación de una extensión y de un control.

=	Microsoft	8,
Complemento	is de Edge BETA \checkmark	
Inicio / Product	ividad / Microsoft S/MIME	
0	Microsoft S/MIME <u>Microsoft Corporation</u> ★★☆☆☆ (500) 400,000+ usuarios Productividad	Obtener Compatible con tu explorador

Una vez estemos en la página de descargas se debe pulsar el botón "Obtener".



Cuando se solicite debemos pulsar el botón "Agregar extensión".

Una vez instalada la extensión refrescamos la página (pulsando F5 o usando el botón de recargar del navegador). Al acceder al mensaje aparece un nuevo aviso, indicando que es necesario instalar S/MIME. Esto es normal, ya que Edge usa la extensión del navegador para comunicarse con el control, que es quien procesa la firma del mensaje. Por lo tanto, la extensión por sí sola no es suficiente y debemos instalar también el control a través del enlace que aparece en el aviso:

² S/MIME es un estándar para la firma y cifrado de mensajes de correo electrónico.



Este mensaje tiene una firma digital, pero no se comprobó porque el control S/MIME no está instalado. Para instalar S/MIME, haga clic aquí.

Al hacer clic se descargará el control para ser instalado.

1	\odot	₿	A»	۲ò	¢	1 2	`≡	œ	$\overline{\uparrow}$
D	escar	gas				Đ	Q		\Rightarrow
1	Smir Abrir	meOutl archivo	ookWe	bChron	ne.msi		D	ť	Ù

Seleccionamos "Abrir archivo" desde el botón de descargas y esperamos pacientemente a que se instale. Una vez instalado (no avisa cuando acaba) refrescamos la página y ya podemos comprobar la firma del mensaje.

Los mensajes con firma digital se muestran con un mensaje informativo:

0	La firma digital para <.	en es	te
Ħ	mensaje es válida y de confianza. Para obtener más información, haga	clic ac	quí.

En el caso de aparecer este otro mensaje:

⊗ La firma digital de este mensaje no es válida ni de confianza. Para obtener más información, haga clic aquí.

significará que la firma no puede ser comprobada, y por lo tanto se considera no válida por OWA.

(**Nota:** Esto no significa necesariamente que la firma no sea válida, puede ser que el certificado para comprobar la firma no se haya subido al tenant de Office 365, lo cual debe hacer un administrador.)

Envío de mensajes firmados

Para enviar un mensaje firmado, redactamos el mensaje como cualquier otro, y al final del proceso debemos acceder al menú de opciones del mensaje (icono con tres puntos) y luego seleccionar "Mostrar opciones del mensaje":



En el cuadro de diálogo que aparece debemos marcar "Firmar digitalmente este mensaje /S/MIME)" y pulsar en el botón "Aceptar".

Opciones de mensaje

Normal	\sim
Solicitar confirmación o	de lectura
Solicitar una confirmac	ión de entrega
Cifrar este mensaje (S/	MIME)
 Firmar digitalmente esi (S/MIME) 	te mensaje
Acentar	Cancelar



UNIVERSIDAD DE BURGOS

Servicio de Informática y Comunicaciones

En la parte derecha de la línea del asunto debe aparecer el icono con la insignia que indica que el mensaje se firmará digitalmente.

Lectura de mensaje cifrados

Los mensajes cifrados se muestran en la lista de mensajes con el icono de un candado para indicar que están cifrados y solamente pueden ser abiertos por el destinatario.



Para poder leer los mensajes cifrados es necesario tener instalado el certificado digital personal correspondiente. Si se tiene el certificado instalado el mensaje se mostrará con un icono adicional de un candado:

Mensaje encriptado



Envío de mensajes cifrados

IMPORTANTE: solamente se pueden enviar mensajes cifrados a personas de la propia organización de las que tengamos almacenado su certificado digital (clave pública) en la libreta de direcciones.

Para enviar un mensaje cifrado, redactamos el mensaje como cualquier otro, y al final del proceso debemos acceder al menú de opciones del mensaje (icono con tres puntos) y luego seleccionar "Mostrar opciones del mensaje":



En el cuadro de diálogo que aparece debemos marcar "Cifrar este mensaje (S/MIME).

Opciones de mensaje

Normal		\sim
Solicitar con	firmación de l	ectura
Solicitar una	confirmación	de entrega
🗸 Cifrar este m	iensaje (S/MIN	ЛЕ)
Firmar digita (S/MIME)	ilmente este n	nensaje
	Aceptar	Cancelar

Opcionalmente también podemos marcar "Firmar digitalmente este mensaje /S/MIME)" para agregar una firma digital al mensaje cifrado.

Una vez elegidas las opciones pulsamos el botón "Aceptar".

En la parte derecha de la línea del asunto debe aparecer el icono con un candado que indica que el mensaje se cifrará.