

Documento:	Correo Electrónico Seguro
Versión:	0.10b
Unidad:	Servicios Informáticos

Correo Electrónico Seguro

Contenido

Introducción	2
Cifra y Firma	2
Gestión de Certificados	2
Cuenta de correo asociada.....	3
Configuración Gestor de Correo	4
Microsoft Outlook.....	4
Mozilla Thunderbird.....	6
Problemas y mensajes de error.....	8
Fallo en el CIFRADO. El certificado del destinatario no es válido	8

Documento:	Correo Electrónico Seguro
Versión:	0.10b
Unidad:	Servicios Informáticos

Introducción

Cifra y Firma

El Correo Electrónico seguro se basa en la Cifra (Encriptación) y Firma Digital mediante el uso de Criptografía de clave pública/privada:

- **Cifra (Encriptación):** Modificación de un mensaje de modo que sea ilegible excepto para su destinatario. La encriptación o cifrado del mensaje se realiza con la clave pública del destinatario, siendo éste el único que puede descifrar el mensaje mediante su clave privada.
- **Firma Digital:** Generación de una huella digital en un mensaje, de manera que cualquier receptor del mensaje puede comprobar que no fue modificado desde su creación y puede certificar la autoría del mensaje.

Este manual se basa en los Certificados Digitales expedidos por la FNMT Clase 2CA.

Gestión de Certificados

Para poder configurar la Firma Digital debemos tener acceso al Certificado Digital en ficheros PKCS#12 (.p12 ó .pfx) que incluyen certificado y clave privada.

Para poder cifrar mensajes debemos tener acceso al certificado del remitente (.crt .cer ó .p7b)

* Para más información sobre obtención y copia de seguridad de certificados ver documento

Gestión de certificado digital

Documento:	Correo Electrónico Seguro
Versión:	0.10b
Unidad:	Servicios Informáticos

Cuenta de correo asociada

Para poder usar el Correo Electrónico Seguro con el Certificado Digital, éste debe tener asociada la misma cuenta de correo que está configurada en el programa cliente de correo, según lo establecido en el protocolo S/MIME descrito en RFC 1521.

Podemos comprobar la cuenta de correo asociada a nuestro certificado digital de la FNMT en la web <http://www.cert.fnmt.es/> pulsando en Ciudadanos / Verificar estado / COMPROBAR ESTADO DE CERTIFICADO / (seleccionar certificado):



BIENVENIDO | BENVINGUT | BENVÍDO | ONGI ETORRI | WELCOME

Mapa | Contacto | Enlaces | Legislación | Noticias

CERES

Obtenga el CERTIFICADO DE USUARIO CON SU D.N.I. | Obtenga el CERTIFICADO DE USUARIO

Qué es CERES
 Ciudadanos
 Empresas
 Adm. Pública

Certificado de usuario
 Otorgar el certificado
 Renovación de certificado
 Anulación de certificado

Modificar datos
 Verificar estado
 Soporte Técnico
 Otros servicios

Contacto
 Preguntas Frecuentes

Real Casa de la Moneda
 Fábrica Nacional de Moneda y Timbre
CIUDADANOS

COMPRUEBE SU PETICIÓN DE CERTIFICADO
 COMPROBAR ESTADO CERTIFICADO

VERIFICAR ESTADO

COMPROBAR ESTADO CERTIFICADO

COMPROBACION DE SU CERTIFICADO

Estimado Sr/Sra. YBORRA.

Su certificado acaba de ser verificado. Esta usted en disposición de un Certificado Digital Valido y no Revocado.

Con este Certificado usted deberá de poder acreditarse correctamente ante los Servicios ofrecidos por entidades relacionadas con la Fábrica Nacional de Moneda y Timbre.

1.- Verifique no obstante que el NIF, Nombre y Apellidos están correctamente escritos en esta pantalla, y coincidan exactamente con su D.N.I. En caso de ser correctos y tener alguna dificultad al acceder a los Servicios ofrecidos por otras Entidades, serán ellas directamente las que podrán aconsejarle en la resolución de dichas dificultades, ya que su certificado está funcionando correctamente, según acaba de comprobar.

2.- En caso de ser incorrecto algunos de los valores contenidos en el NIF, Nombre y Apellidos deberá revocar el certificado actual y solicitar uno nuevo. Estos dos pasos los podrá realizar en una sola visita a cualquiera de las **Oficinas de Registro**

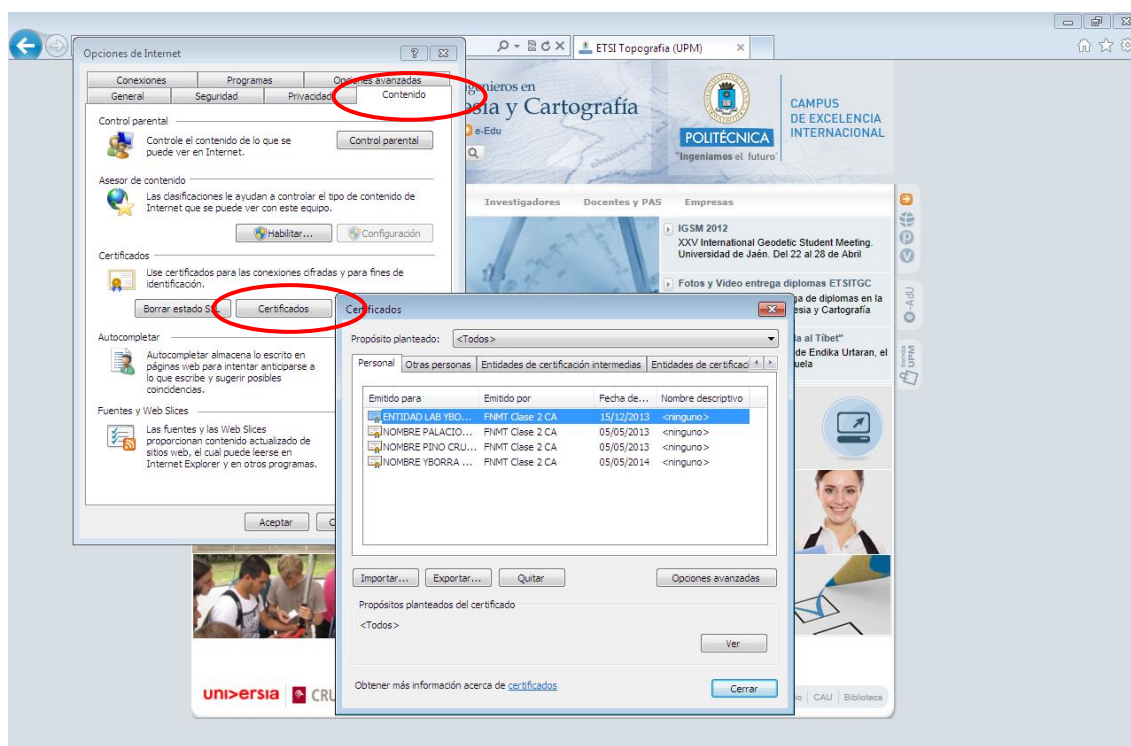
Identificador	Valor
INFORMACION SOBRE LA IDENTIDAD	(Valores Personales)
Nombre	DANIEL JUAN
Primer Apellido	YBORRA
Segundo Apellido	FLORES
NIF	C-460591K
Dirección de Correo Electrónico	DJ.YBORRA@UPM.ES
INFORMACION SOBRE LAS CLAVES	(Valores Técnicos)
Numero de Serie del Certificado	1020130710
Autoridad Emisora	OU=FNMT CLASE 2 CA, O=FNMT, C=ES
Propietario	OU=HOMBRE YBORRA FLORES DANIEL JUAN - NIF 51948054R, OU=500730027, OU=FNMT CLASE 2 CA, O=FNMT, C=ES
Comienzo de la Validez del Certificado	5 de mayo de 2011
Fin de Validez del Certificado	5 de mayo de 2014

Documento:	Correo Electrónico Seguro
Versión:	0.10b
Unidad:	Servicios Informáticos

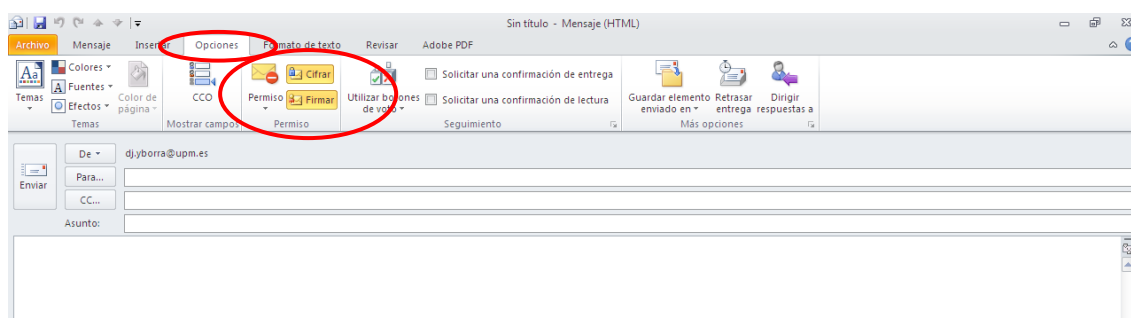
Configuración Gestor de Correo

Microsoft Outlook

Microsoft Outlook maneja los certificados del Sistema gestionados desde Opciones de Internet Explorer / Contenido / Certificados



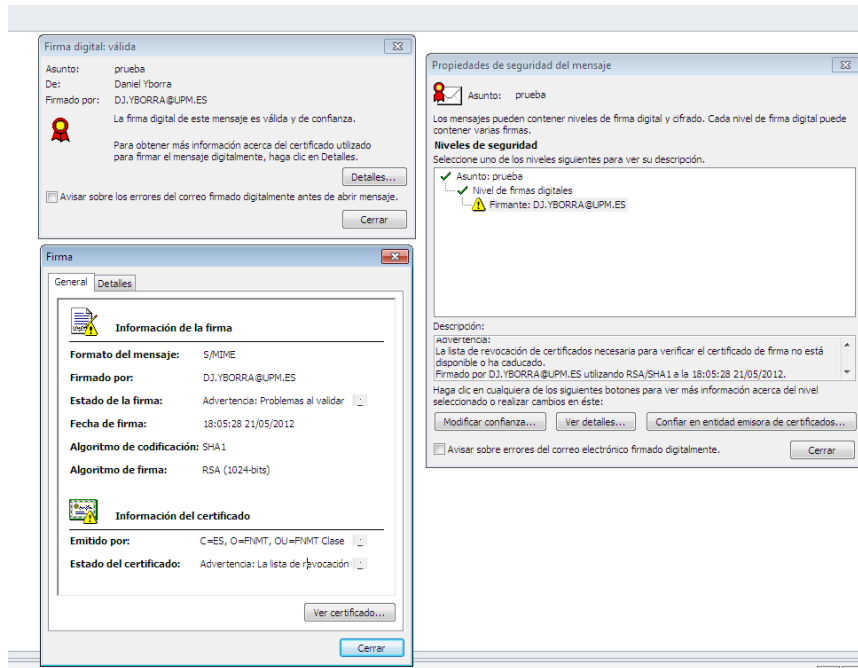
Al enviar un mensaje a través de Microsoft Outlook es posible Cifrar y/o Firmar seleccionando Opciones / Cifrar/Firmar:



Documento:	Correo Electrónico Seguro
Versión:	0.10b
Unidad:	Servicios Informáticos

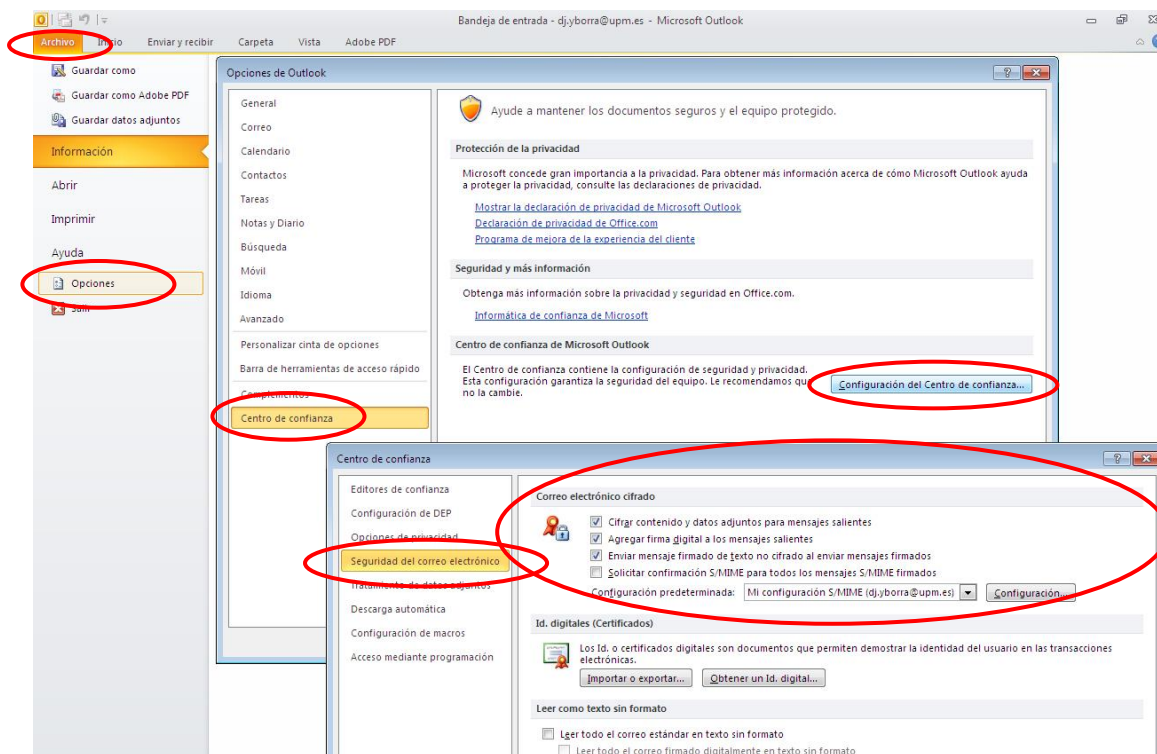
El programa revisará de entre los certificados instalados el que tenga la cuenta de correo del remitente asociada y enviará el mensaje FIRMADO. Si tenemos instalado el certificado del receptor podremos enviarlo CIFRADO.

El mensaje enviado estará autenticado y pulsando sobre el icono del sello podremos ver los detalles del certificado y la autoridad emisora:



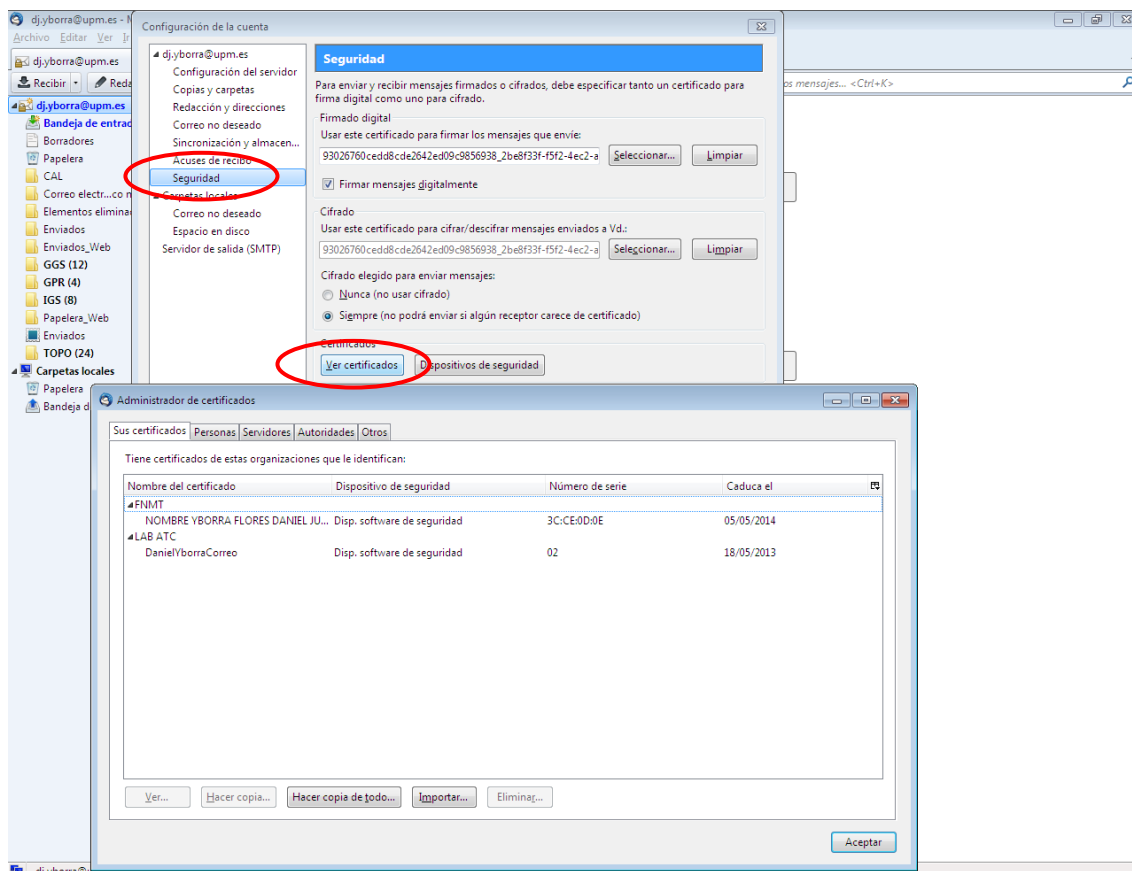
Para habilitar el Correo Seguro en Microsoft Outlook es necesario pulsar sobre Archivo / Opciones / pestaña Centro de Confianza / Configuración del Centro de confianza / pestaña Seguridad del correo electrónico y marcar las opciones correspondientes:

Documento:	Correo Electrónico Seguro
Versión:	0.10b
Unidad:	Servicios Informáticos

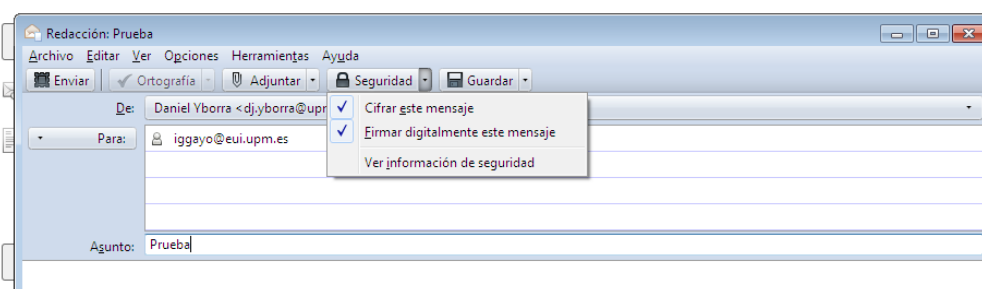


Mozilla Thunderbird

Mozilla Thunderbird maneja los certificados desde la propia aplicación en Configuración de la Cuenta / Seguridad / Ver certificados



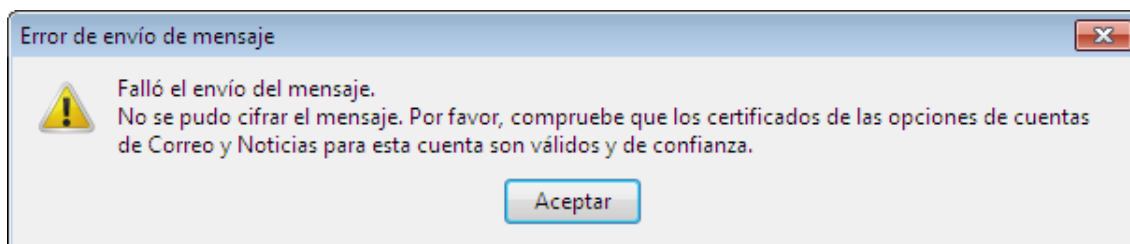
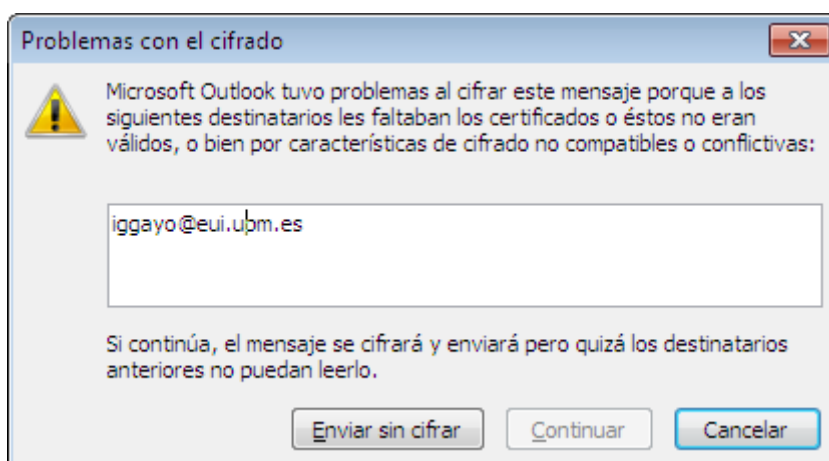
Al enviar un mensaje podemos seleccionar Firmar/Cifrar en la pestaña Opciones:



Documento:	Correo Electrónico Seguro
Versión:	0.10b
Unidad:	Servicios Informáticos

Problemas y mensajes de error

Fallo en el CIFRADO. El certificado del destinatario no es válido



El certificado del remitente está expedido por una Autoridad certificadora que debemos tener instalado en el repositorio correspondiente.