Cifrado y firmado de correo electrónico con dispotivos iOS (iPhone/iPad)

El presente documento se basa en la versión 7.1 del software iOS, siendo esta la versión mínima recomendada para el cifrado/firmado de correo electrónico. Por cuestiones de seguridad, recomendamos que se cuente con la última versión del software iOS en su dispositivo.

También recomendamos proteger su iPhone/iPad con una contraseña de acceso, pues en caso de pérdida o robo del dispositivo dicho aparato cuenta en su interior con su certificado digital personal, de especial valor.

1 Instalación del certificado raíz de la FNMT.
2 Instalación del certificado personal de la FNMT.
3 Configuración de firmado y/o cifrado de correos electrónicos salientes.
4 Verificación de la firma y/o descifrado de correos electrónicos entrantes.

Instalación del certificado raíz de la FNMT.

El primer paso a realizar es la instalación del certificado raíz de la Fábrica Nacional de Moneda y Timbre (en adelante, FNMT). Si se tiene configurada la conexión a la red wifi Eduroam en el dispositivo iPhone/iPad ya se cuenta con el certificado raíz de la FNMT, por lo que no es necesario volverlo a instalar.

En caso de no poseer el certificado raiz de la FNMT, para obtener dicho certificado hay que visitar con el navegador Safari la página web de la Sede Electrónica de la Universidad de Sevilla, o bien directamente acceder a este enlace directo.

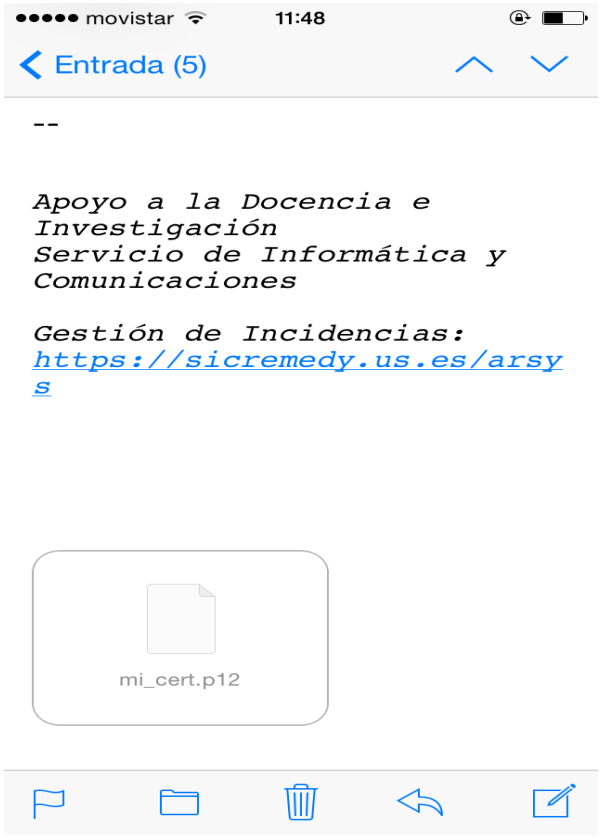
Cuando se abre con el navegador el certificado aparece una pantalla similar a la siguiente:

Hemos de presionar en "Instalar" para que se acepte a la FNMT como autoridad certificadora de confianza.

Instalación del certificado personal de la FNMT.

Una vez tenemos instalado el certificado digital raíz de la FNMT el siguiente paso es instalar nuestro propio certificado digital personal. El certificado personal debe tener como dirección de correo electrónica de contacto su dirección de correo electrónico de la Universidad de Sevilla.

Para importar nuestro certificado digital, nos enviaremos como adjunto por correo electrónico (usando nuestra cuenta de la US) nuestro propio certificado personal en formato **.p12**



Presionamos sobre nuestro certificado y nos aparecerá una imagen similar a la siguiente:

Presionamos instalar, nos solicitará la contraseña de importación del certificado y tras esto ya

tenemos instalado nuestro certificado digital personal en el navegador.

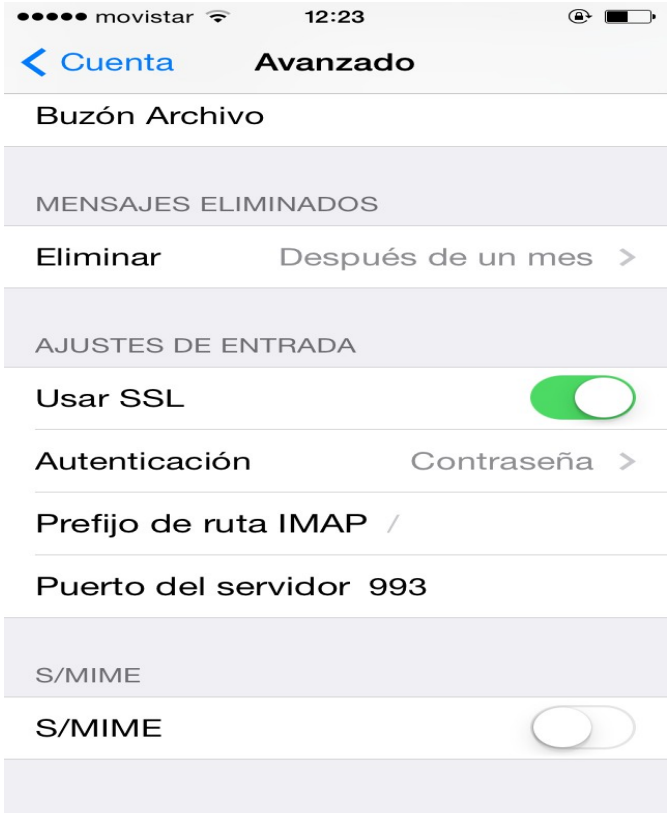
Configuración de firmado y/o cifrado de correos electrónicos salientes.

Una vez instalado el certificado raíz de la FNMT, y su certificado digital de usuario, ya se puede firmar y cifrar el correo electrónico. La configuración a realizar es la siguiente:

Vaya a la pantalla principal de su dispositivo, y presione **Ajustes->Correo, contactos, calendario** , elija su cuenta de correo electrónico de la Universidad de Sevilla.

A continuación, presione sobre el nombre de la cuenta y vaya a la parte inferior, donde indica **Avanzado**

En la parte inferior aparecerá un selector **S/MIME** desactivado:



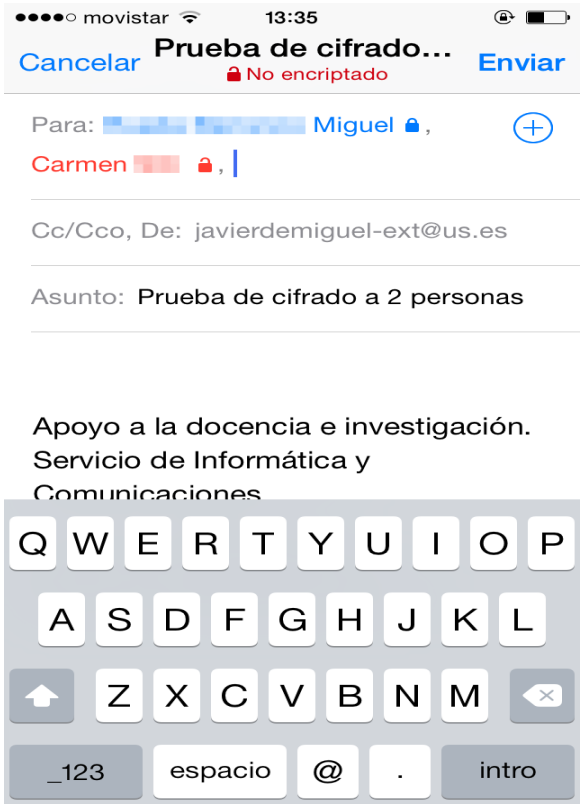
Activamos el selector **S/MIME** y nos aparecerá lo siguiente:

Seleccionamos la opción deseada, según queramos firmar nuestros mensajes salientes, cifrarlos o ambas opciones simultáneamente. Volvemos a la pantalla anterior y no olvide presionar **OK** en la parte superior derecha para los cambios en la configuración queden grabados.

A la hora de redactar un nuevo mensaje de correo electrónico desde su dispositivo, si tiene activada la opción de "Firmar" no tiene que hacer nada especial. Por contra, para mandar mensajes cifrados es necesario haber aceptado como de confianza la clave pública del emisor.

En la siguiente captura de pantalla se está enviando un mensaje cifrado a una persona que se llama Miguel. Como previamente se tenía como válido el certificado de esta persona, sale en color azul (correcto) y aparece el texto **Encriptado** en la parte superior:

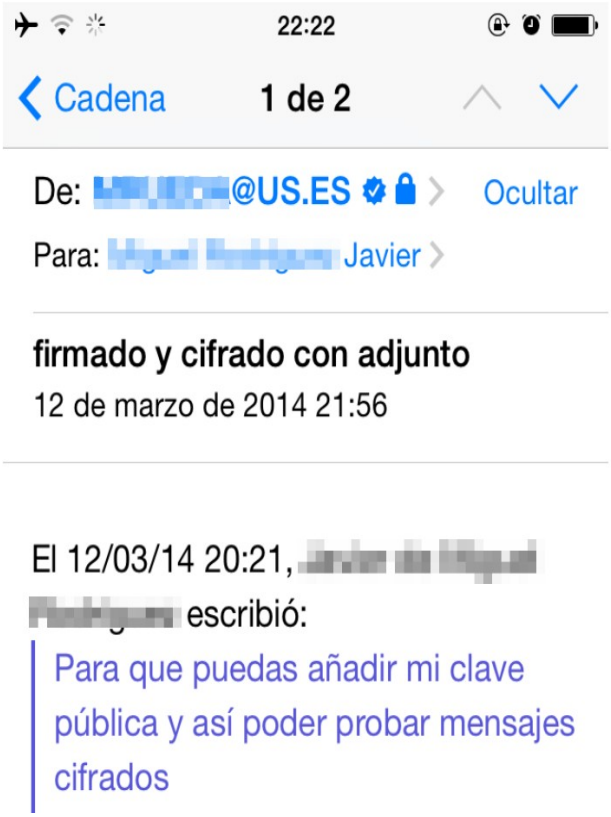
En el caso de múltiples destinatarios, se marcarán en color azul aquellos que se les pueda enviar mensajes cifrados y en color rojo aquellos otros que no sea posible usar el cifrado. Con que uno de los destinatarios no pueda recibir mensajes cifrados, la barra superior de la pantalla de redacción aparecerá el texto **No Encriptado**. No se preocupe, todos aquellos destinatarios marcados en color azul si recibirán el mensaje cifrado.



Por último, tenga en cuenta que a la hora de cifrar mensajes el destinatario debe tener correctamente operativo su dispositivo / cliente de correo electrónico, de lo contrario no podrá leer su mensaje. En el caso de mensajes firmados, si el destinatario no cuenta con estos medios sencillamente no podrá comprobar la validez, pero si podrá acceder al contenido del correo.

Verificación de la firma y/o descifrado de correos electrónicos entrantes.

Cuando recibamos un mensaje de correo electrónico firmado y/o cifrado el aspecto que tendrá será similar a este:



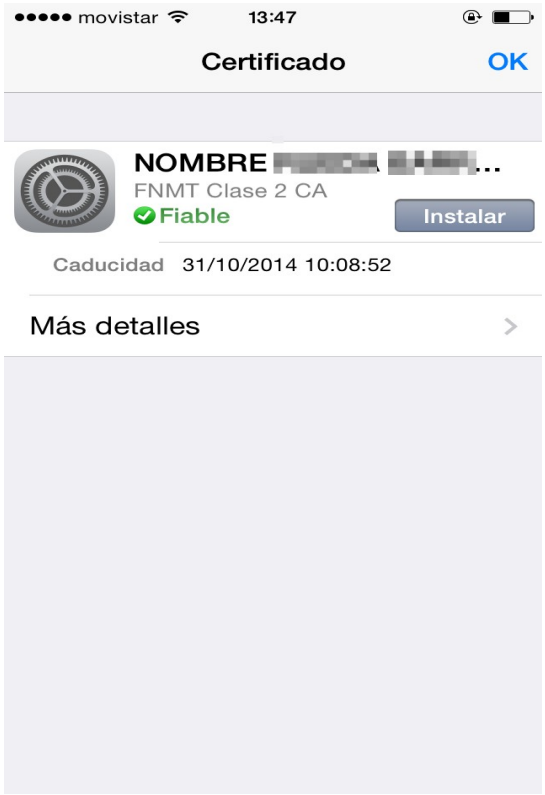
A la derecha del emisor nos pueden aparecer dos símbolos (o uno o ninguno):

 Este icono indica que el mensaje está cifrado digitalmente, y que el cifrado es correcto (color azul) o incorrecto (color rojo).

 Este símbolo indica que el mensaje está firmado digitalmente, y que la firma se ha verificado correctamente (color azul) o incorrectamente (color rojo)

La siguiente captura muestra los detalles de un emisor que ha enviado un correo electrónico firmado electrónicamente de forma correcta:

Es importante destacar que para poder descifrar un mensaje cifrado es necesario haber importado previamente la clave pública del emisor, y que sea una clave pública válida. Para importar la clave pública de un emisor, solicite que le mande un mensaje firmado y cuando lo reciba, presione sobre el emisor que le aparecerá lo siguiente:



Presione **Instalar** y desde ese momento ya podrá enviar mensajes cifrados a dicho destinatario.