Cómo verificar los mensajes recibidos con S/MIME en el ESA

Contenido

[Introducción](#)
[Cómo verificar los mensajes recibidos con S/MIME en el ESA](#)
[Muestra](#)
[Cifre](#)
[Firme/cifre](#)
[Triple](#)
[Verificación del certificado](#)
[Información Relacionada](#)

Introducción

Este documento describe qué verificar en el correo abre una sesión el dispositivo de seguridad del correo electrónico de Cisco (ESA) cuando los mensajes se reciben con un válido configuración aseguran/de los Multipurpose Internet Mail Extension (S/MIME).

Cómo verificar los mensajes recibidos con S/MIME en el ESA

S/MIME es un método de estándares para enviar y recibir los correos electrónicos seguros, verificados. S/MIME utiliza los pares del público/de clave privada para cifrar o para firmar los mensajes.

• Si se cifra el mensaje, sólo el receptor del mensaje puede abrir el mensaje encriptado.
• Si se firma el mensaje, el receptor del mensaje puede validar la identidad del remitente y puede ser confiado que el mensaje no se ha alterado mientras que en el tránsito.

Con un S/MIME válido enviando el perfil configurado en el ESA, los mensajes se pueden enviar con uno de cuatro modos:

• Muestra
• Cifre
• Firme/cifre (la muestra y entonces cifra)
• Triple (la muestra, cifra, y después firma otra vez)

Asimismo, los mensajes se pueden recibir de otros remitentes que han utilizado los Certificados válidos S/MIME para firmar o el cifrado.

Para el beneficiario, necesitarán utilizar una aplicación de correo electrónico para procesar, ver, y validar correctamente la firma digital o el cifrado asociada. Las aplicaciones de correo electrónico comunes que presentarán la firma digital o la opción de encripción son Microsoft Outlook, el correo (OSX), y Mozilla Thunderbird. El mensaje sí mismo contendrá una conexión .p7s (smime.p7s) o de los .p7m (smime.p7m). Estos ficheros de la conexión serán registrados con el

ID del mensaje (MEDIADOS DE) en los registros del correo.

El aspecto de una conexión con el fichero .p7s es indicador que el mensaje lleva una firma digital.
El aspecto de una conexión con el fichero de los .p7m es un indicador que el mensaje lleva una firma cifrada y el cifrado S/MIME. Los contenidos del mensaje y las conexiones se envuelven en un fichero smime.p7m. Una clave privada que corresponde con la clave pública en el mensaje es necesaria abrir el fichero de documento.
Si una aplicación de correo electrónico no maneja las firmas digitales, un .p7s del fichero de los .p7m puede aparecer como conexión al correo electrónico.

Muestra

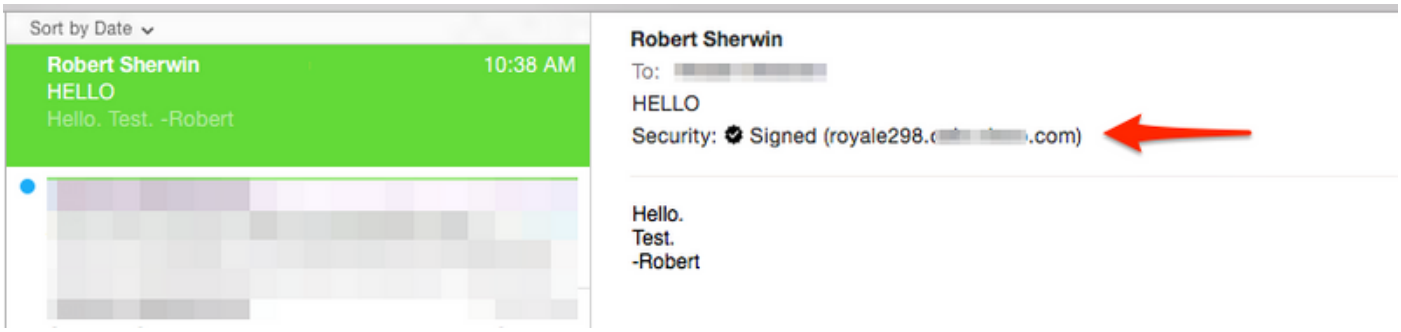
Si el mensaje fuera enviado del remitente con un S/MIME que enviaba el perfil que fue fijado para firmar, en el beneficiario ESA, cuando ver el correo registra para los mensajes entrantes que indicaría un attachement .p7s:

```
Fri Dec  5 10:38:12 2014 Info: MID 471 attachment 'smime.p7s'
```

En la aplicación de correo electrónico receptora éste sería similar visto al siguiente.

La perspectiva 2013 (Windows) del ejemplo como se muestra, nota el símbolo de la insignia o del certificado indicado:

Correo del ejemplo como se muestra (OSX):



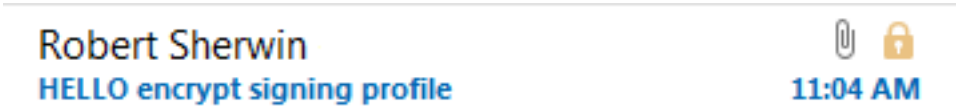
Cifre

Si el mensaje fuera enviado del remitente con un S/MIME que enviaba el perfil que fue fijado para cifrar, en el beneficiario ESA, cuando ver el correo registra para los mensajes entrantes que indicaría un attachement de los .p7m:

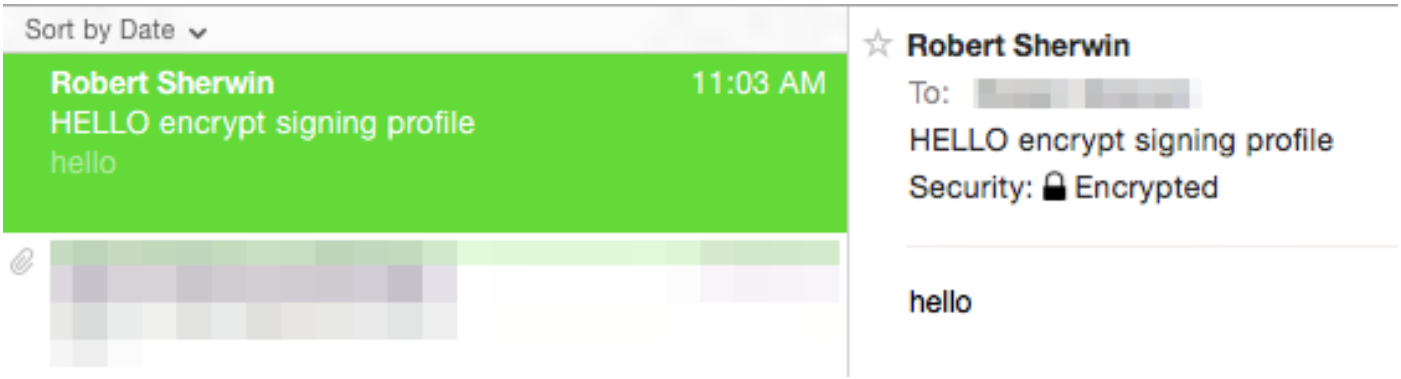
```
Fri Dec 5 11:03:44 2014 Info: MID 474 attachment 'smime.p7m'
```

En la aplicación de correo electrónico receptora que éste sería similar visto al siguiente, note el símbolo del candado indicado por ambos ejemplos.

Perspectiva 2013 (Windows) del ejemplo como se muestra:



Correo del ejemplo como se muestra (OSX):



Firme/cifre

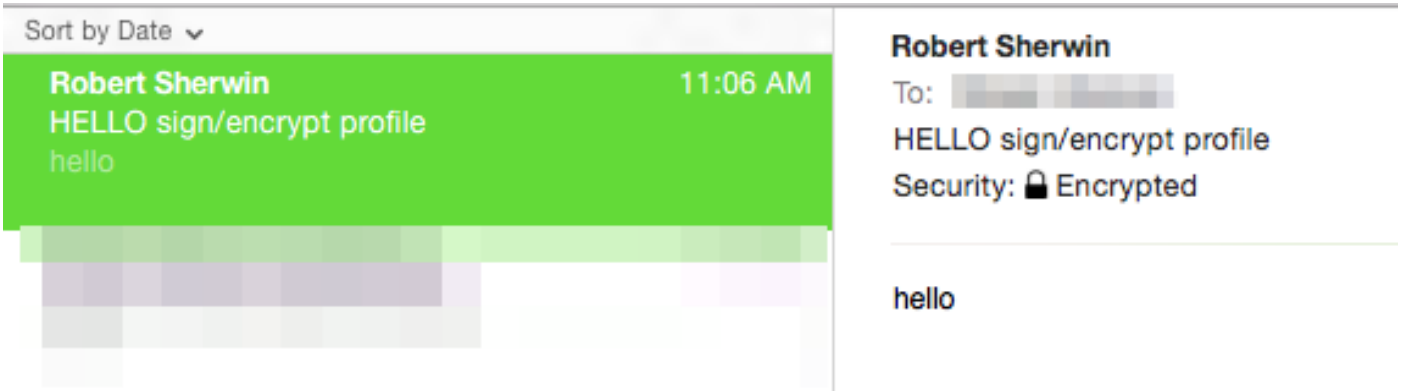
Si el mensaje fuera enviado del remitente con un S/MIME que enviaba el perfil que fue fijado para firmar/cifre, en el beneficiario ESA, cuando ver el correo registra para los mensajes entrantes que indicaría un attachement de los .p7m:

```
Fri Dec  5 11:06:43 2014 Info: MID 475 attachment 'smime.p7m'
```

En la aplicación de correo electrónico receptora que éste sería similar visto al siguiente, note el símbolo del candado indicado.

Perspectiva 2013 (Windows) del ejemplo como se muestra:

Correo del ejemplo como se muestra (OSX):



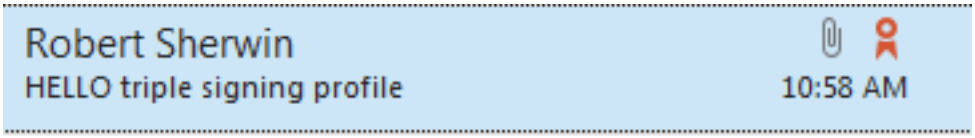
Triple

Finalmente, si el mensaje fuera enviado del remitente con un S/MIME que enviaba el perfil que fue fijado para triplicar, en el beneficiario ESA, cuando ver el correo lo registra para los mensajes entrantes indicaría los .p7m y la conexión .p7s:

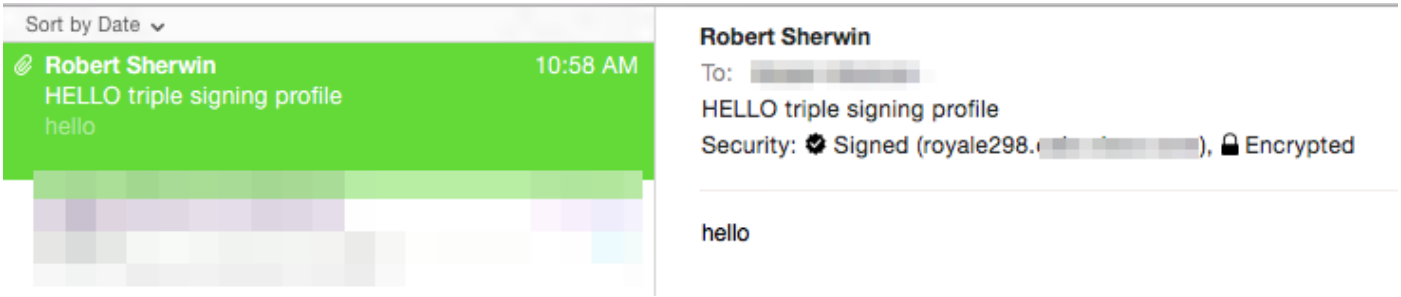
```
Fri Dec 5 10:58:11 2014 Info: MID 473 attachment 'smime.p7m'
Fri Dec 5 10:58:11 2014 Info: MID 473 attachment 'smime.p7s'
```

En la aplicación de correo electrónico receptora esto puede variar, sobre la base de la aplicación de correo electrónico funcionando.

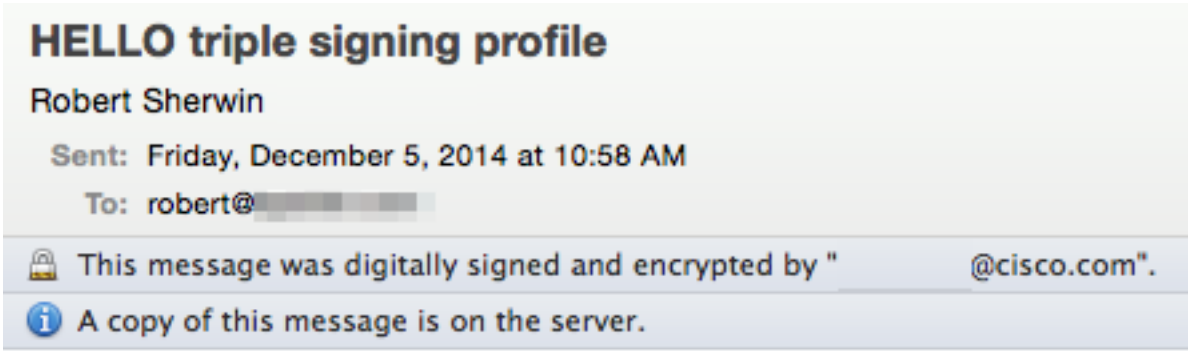
La perspectiva 2013 (Windows) del ejemplo como se muestra, nota el símbolo de la insignia o del certificado indicado:



El correo del ejemplo como se muestra (OSX), nota que la insignia para firmado está presentada y el candado para el cifrado está indicado:



La oficina 2011 (OSX) del ejemplo como se muestra, nota el candado indicado y el mensaje, “este mensaje fue firmado digitalmente y cifró” incluido:

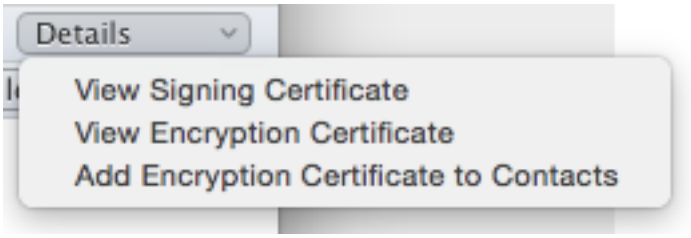



```
hello
```

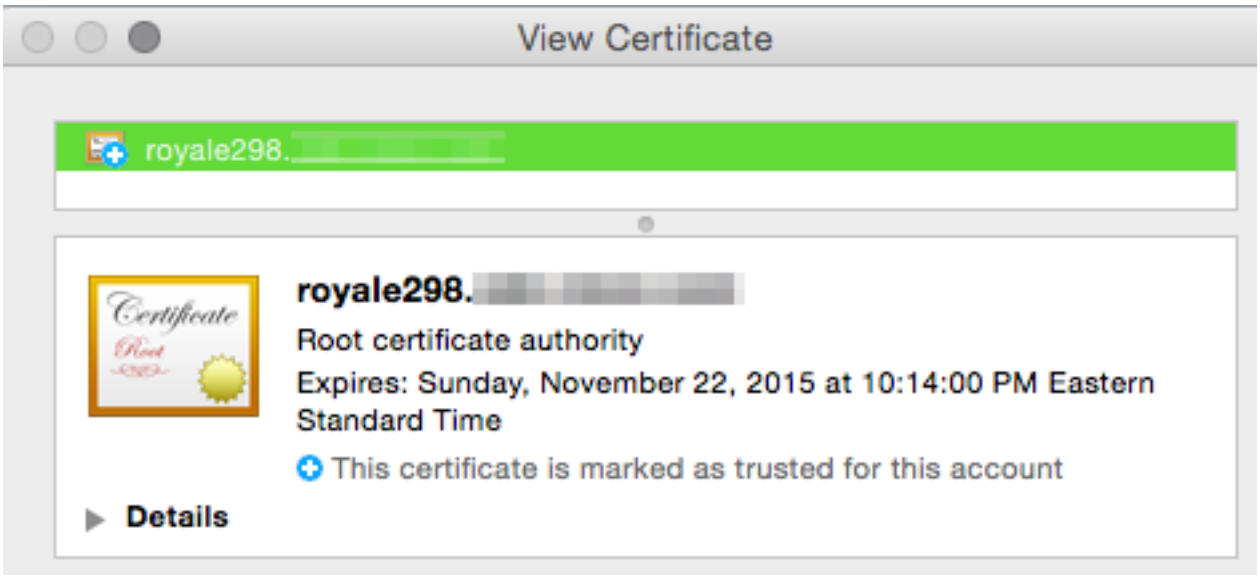
Verificación del certificado

De acuerdo con la aplicación de correo electrónico funcionando, y la preferencia del beneficiario, o las políticas de seguridad de la compañía, ver y validar el certificado variarán.

Para el ejemplo anterior triple, con la oficina 2011 (OSX), en la línea firmada y de mensaje encriptado hay una opción dropdown de los detalles:



La selección del **certificado de firma de la visión** presenta la información de firma real del certificado del ESA que esto fue enviada originalmente de:



Información Relacionada

- Cómo verificar los mensajes enviados con S/MIME que envía el perfil en el ESA
- Soporte Técnico y Documentación - Cisco Systems
- Dispositivo de seguridad del correo electrónico de Cisco - Guías de usuario