S/MIME de oficio

firmado digital transparente para mensajes oficiales

RedIRIS

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Jornadas Técnicas 2014. Cáceres

Miguel Macías Enguídanos

De: Universidad Politécnica de Valencia E-mail [mailto:blanche@3web.net]

Estimado Universidad Politécnica de Valencia los usuarios de correo web,

Este mensaje es de la Universidad Politécnica de Valencia, centro de mensajería para todos Universidad Politécnica de Valencia webmail **users**. **We son** actualmente la mejora de nuestra base de datos y e-mail centro. Estamos suprimiendo todos los no utilizados **upf.edu** correo electrónico, Usted está obligado a verificar y actualizar su mensaje de correo electrónico confirmando su identidad. Esto evitará que su dirección de correo electrónico de concluidos durante este ejercicio. Con el fin de confirmar la identidad de correo electrónico que usted, usted es para proporcionar los siguientes datos;

Confirmar su identidad por debajo de correo electrónico

Nombre :.....
Apellido :.....
Email Nombre de usuario: .....
E-mail Contraseña: .....

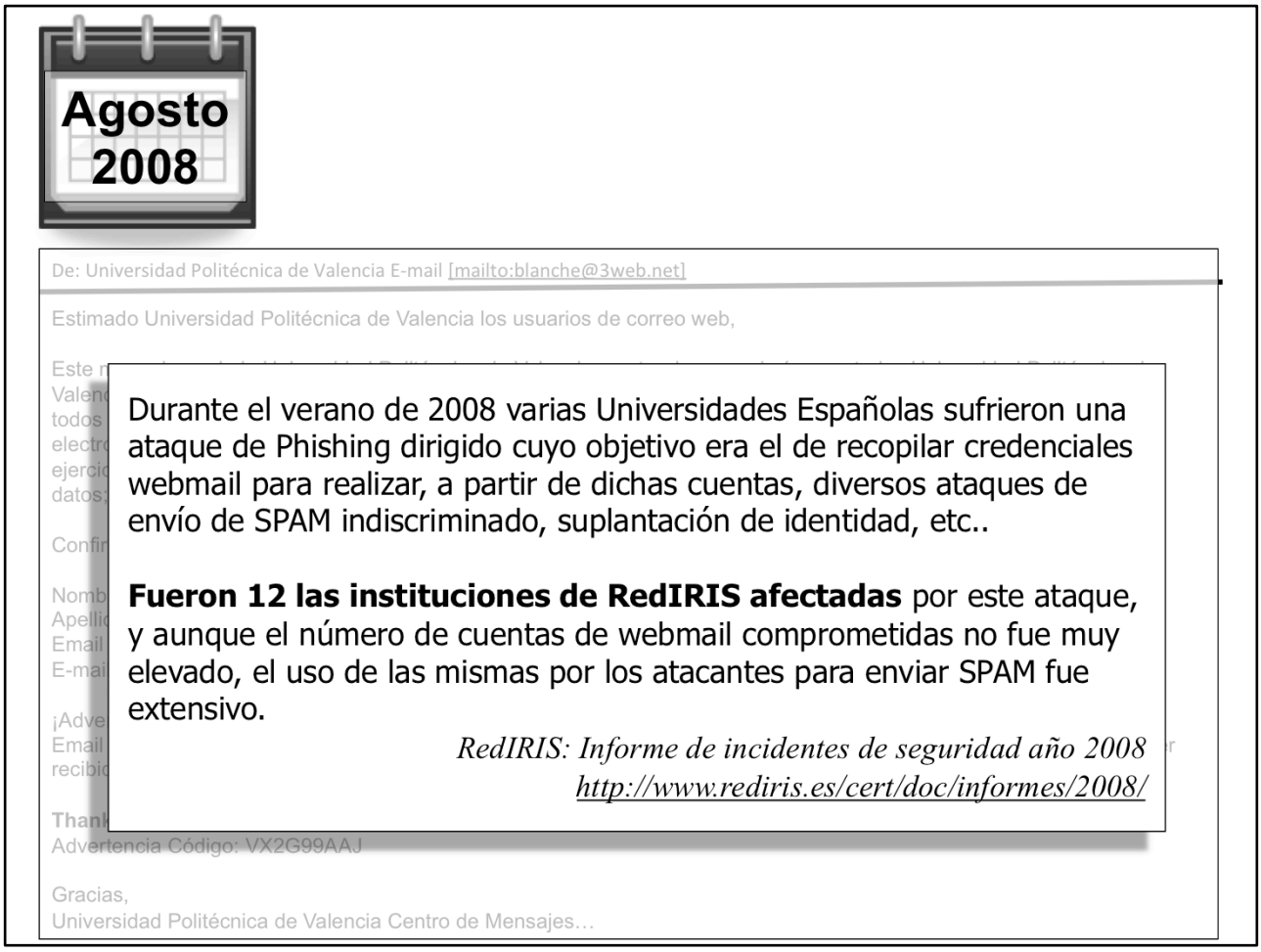
¡Advertencia! Universidad Politécnica de Valencia
Email usuario que se niega a verificar y, posteriormente, actualizar su correo electrónico dentro de los siete días de haber recibido esta advertencia **perderá su correo electrónico permanentemente**.

Thank you for using Universidad Politécnica de correo electrónico!
Advertencia Código: VX2G99AAJ

Gracias,
Universidad Politécnica de Valencia Centro de Mensajes…

Ataque de phishing recibido en la UPV en agosto de 2008.

A pesar de su mala traducción, de la incongruencia de enviar la contraseña por correo electrónico, de utilizar un remitente externo… varios usuarios pican el anzuelo. Hasta el vicerrector interrumpe sus vacaciones para interesarse por el ataque.



Este ataque, como muchos otros, está (relativamente) personalizado pero tiene un objetivo sectorial.

UNIVERSIDAD POLITECNICA DE VALENCIA

Hola,

Debido a la actualización de nuestro SECURTY nuevos y la eliminación de todas las cuentas no utilizadas tendrá que confirmar su dirección de e-mail con la firma en su cuenta. También sería cerrar todas las cuentas no utilizadas.

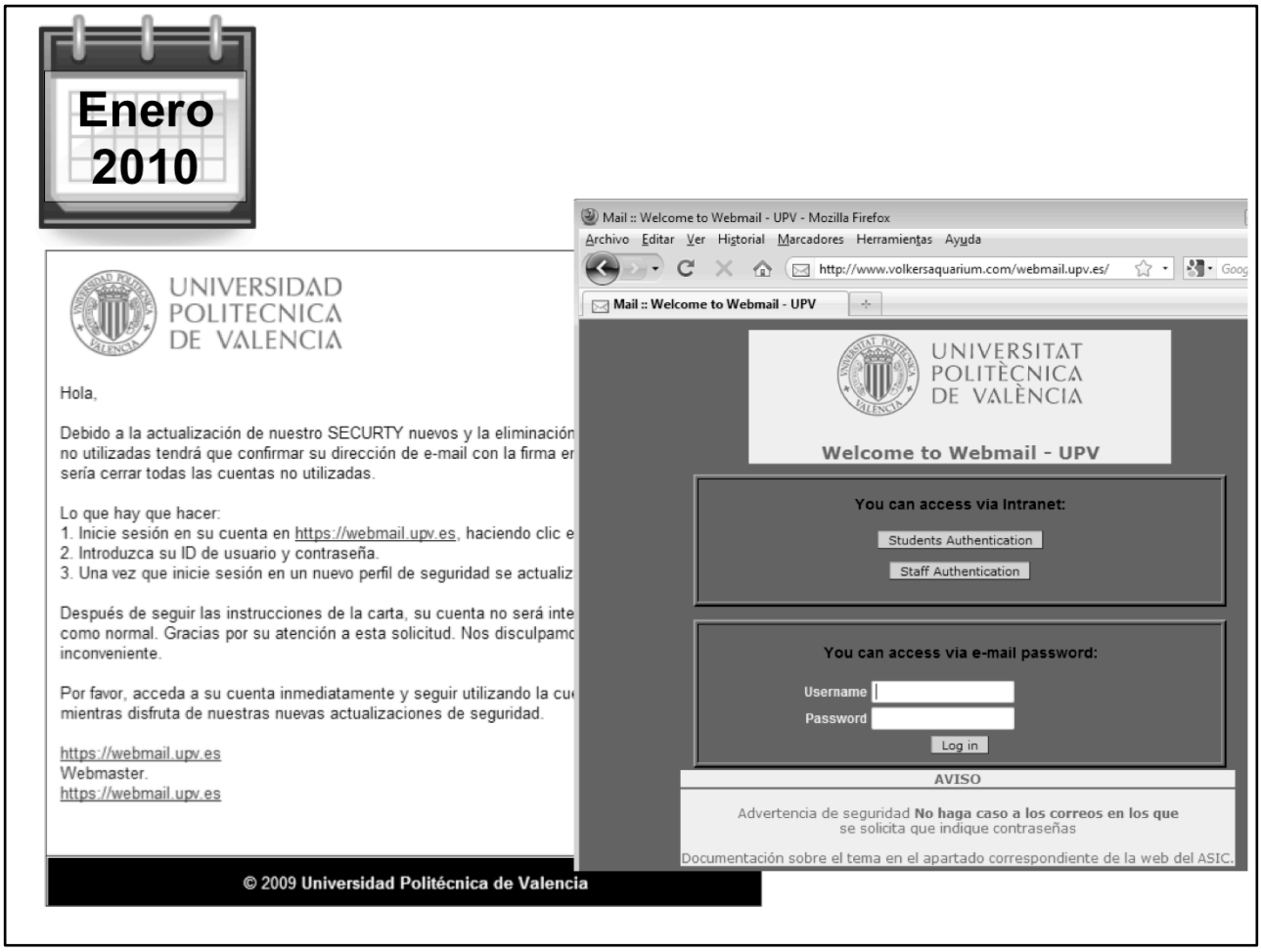
Lo que hay que hacer:
1. Inicie sesión en su cuenta en https://webmail.upv.es, haciendo clic en la URL.
2. Introduzca su ID de usuario y contraseña.
3. Una vez que inicie sesión en un nuevo perfil de seguridad se actualizará para su cuenta.

Después de seguir las instrucciones de la carta, su cuenta no será interrumpido y continuará como normal. Gracias por su atención a esta solicitud. Nos disculpamos por cualquier inconveniente.

Por favor, acceda a su cuenta inmediatamente y seguir utilizando la cuenta de forma habitual mientras disfruta de nuestras nuevas actualizaciones de seguridad.

https://webmail.upv.es
Webmaster.
https://webmail.upv.es

Nuevo ataque de phishing, más sofisticado que el anterior: formato HTML, logotipo corporativo, enlace camuflado…



Es el primer phishing que sufre la UPV donde se replica la página web.

En este caso, se redirige al usuario a la página de entrada al WebMail. El atacante sólo ha replicado la versión en inglés.

Se demuestra, una vez más, lo inútiles que son los mensajes de advertencia en la propia página.

La historia de este phishing puede encontrarse en: http://asic.blogs.upv.es/%C2%A1no-te-dejes-enganar/

De: Michael Antonio Romero Guerrero [mailto:maromerogue@unal.edu.co]

--

Advertencia: UPV Universitat Politècnica de València

Su buzón ha superado el límite de almacenamiento de 100 MB es posible que no pueda para recibir o enviar correo electrónico hasta que actualice su buzón. Para **Upgrade** haga clic en el enlace de abajo y **llenar** para completar la actualización a su buzón

http://upv.jigsy.com/

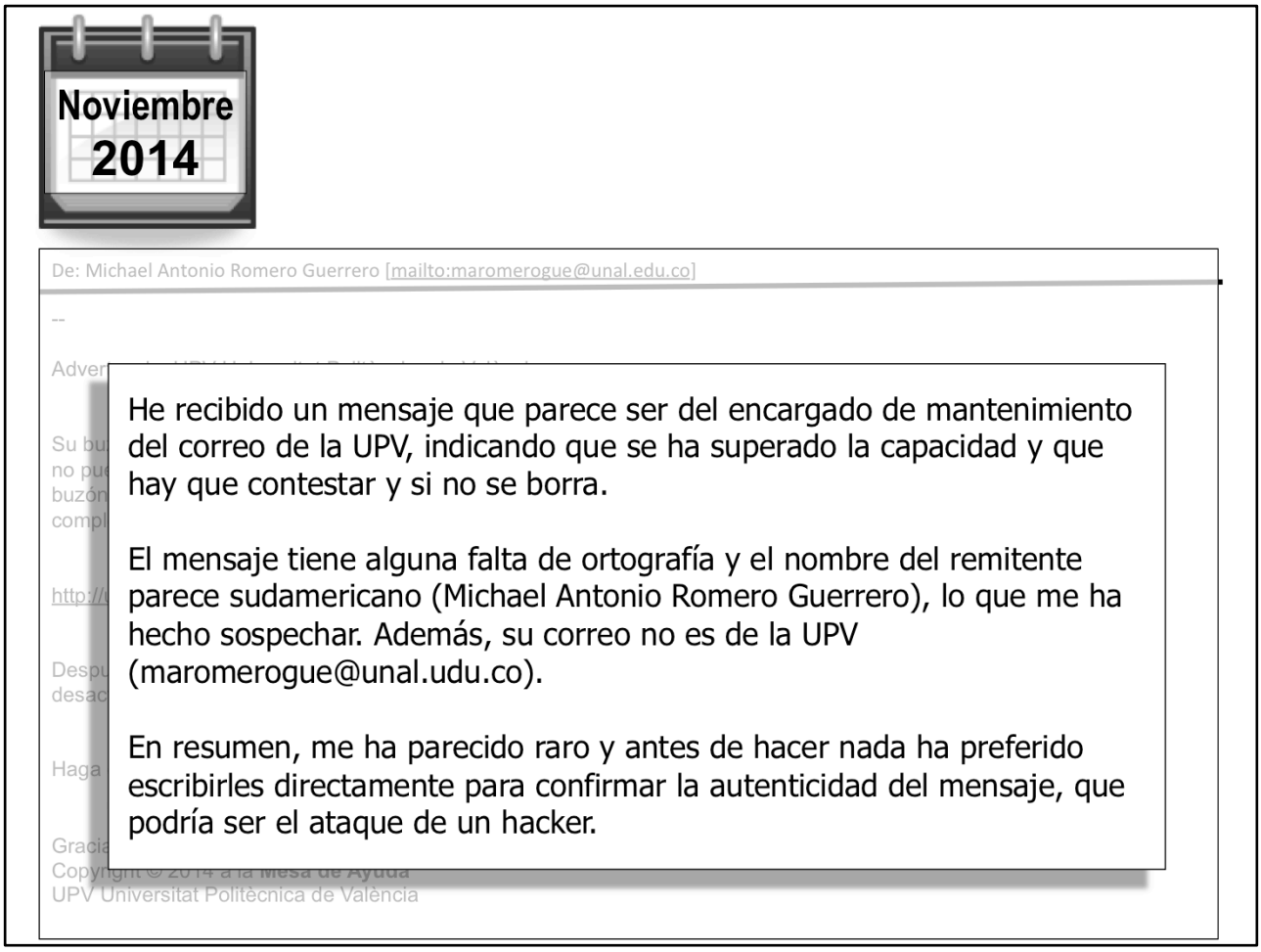
Después de 24 horas sin recibir ninguna respuesta de usted **Nosotros** desactivar su buzón de correo.

Haga clic aquí: http://upv.jigsy.com/

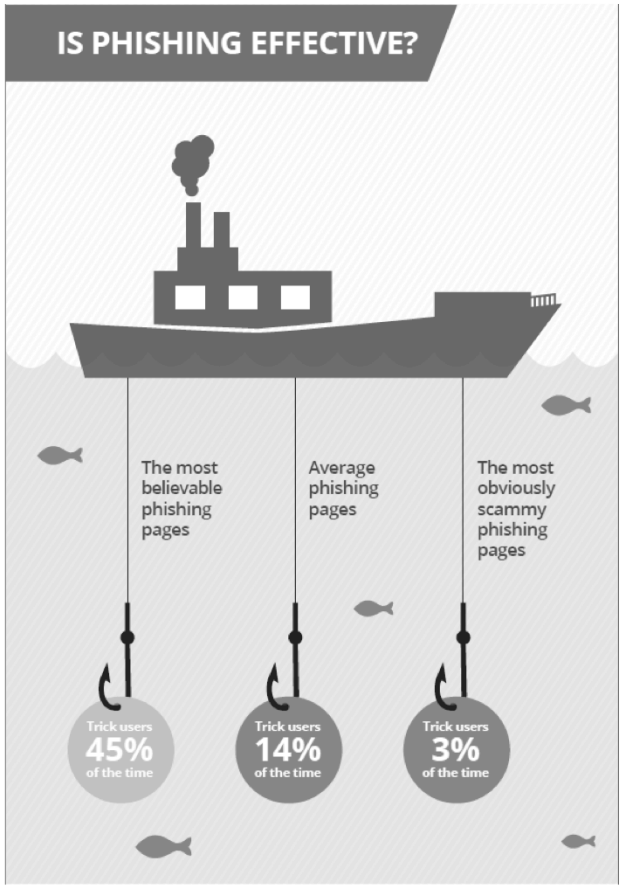
Gracias por usar UPV
Copyright © 2014 a la **Mesa de Ayuda**
UPV Universitat Politècnica de València

Los ataques se siguen recibiendo.

Con los mismos errores, pero con la misma efectividad…



… aunque ya hay muchos usuarios concienciados, que no pican el anzuelo, que advierten a su entorno, que ponen sobre alerta a la institución, etc.



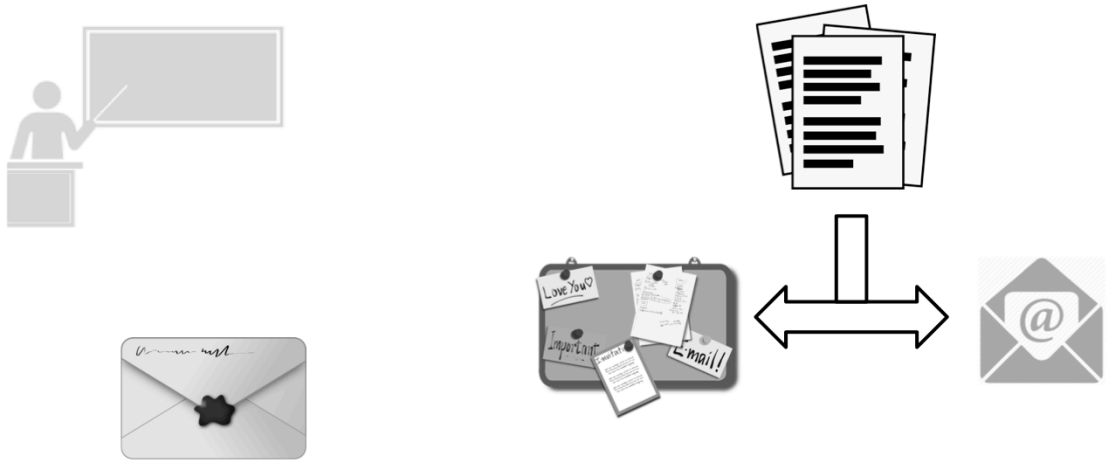
Handcrafted Fraud and Extortion:
Manual Account Hijacking in the Wild
November 2014

Un estudio llevado a cabo por investigadores de Google y de la universidad de California, muestra que el phishing sigue siendo muy efectivo para los atacantes:
http://services.google.com/fh/files/blogs/google_hijacking_study_2014.pdf

¿Cómo podríamos evitar los fraudes por correo electrónico?

Los problemas que estamos intentando resolver tienen que ver con la autenticidad de los mensajes: ¿cómo puede un usuario determinar si un correo es legítimo o no?

¿Cómo podríamos evitar los fraudes por correo electrónico?



Se pueden tomar múltiples medidas para evitar, en lo posible, los fraudes cometidos a través del correo electrónico:

La formación en seguridad informática siempre es importante. Sólo con usuarios concienciados se podrán evitar la mayoría de ataques informáticos.

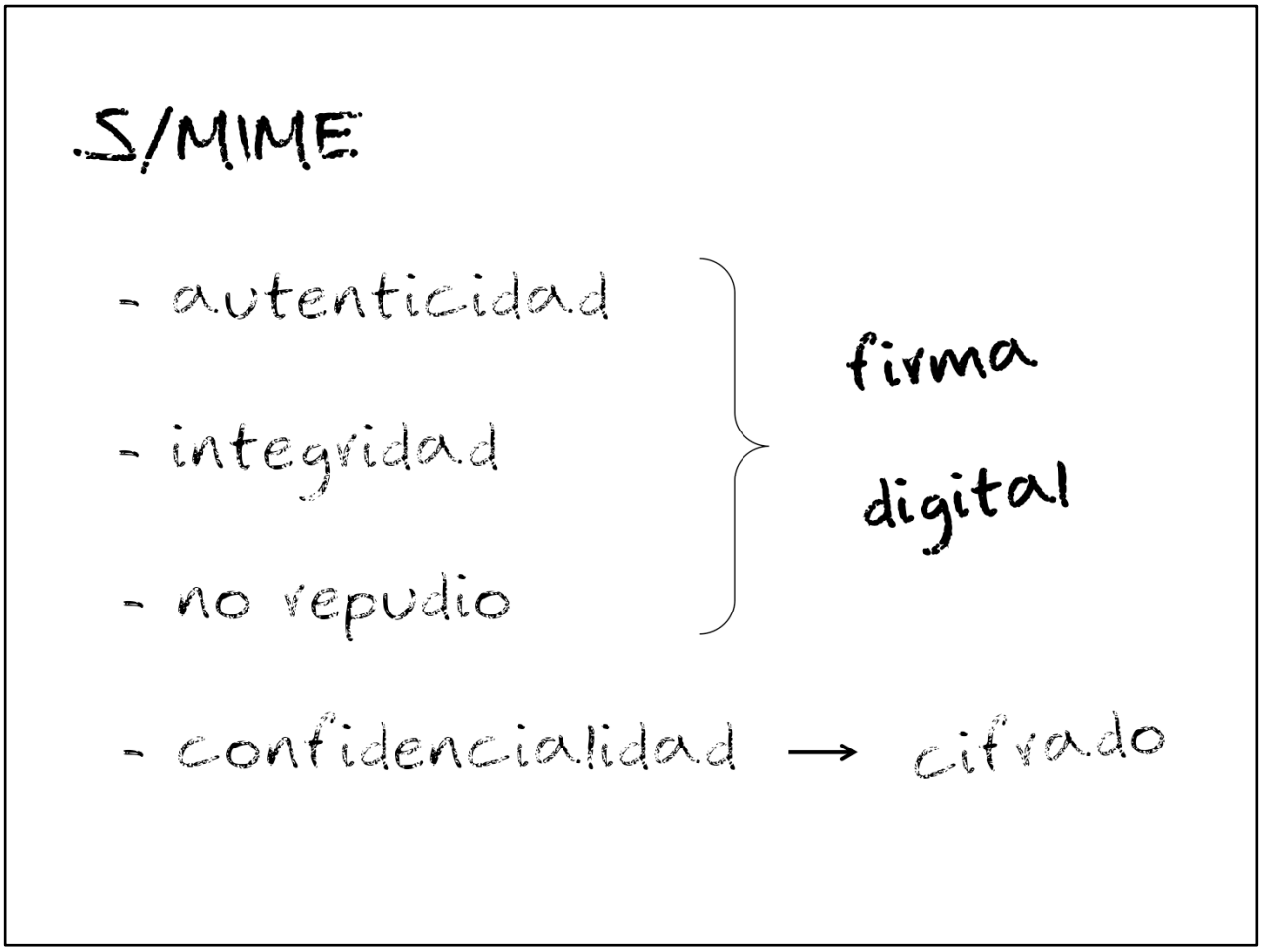
Entregar los mensajes por un doble canal también podría ser una solución: el usuario considerará legítimo un correo sólo si puede leerlo a través de ambos canales de comunicación.

Utilizar un “lacre” para identificar unívocamente al remitente y para garantizar que el mensaje no ha sido modificado también ayudaría a descubrir los mensajes falsos. La firma digital es el equivalente al sobre lacrado.

Los dos sistemas más utilizados para firmar digitalmente mensajes de correo son:

S/MIME (Secure/Multipurpose Internet Mail Extensions)
http://tools.ietf.org/html/rfc5751

PGP (Pretty Good Privacy)
http://www.ietf.org/rfc/rfc4880.txt



La firma digital aporta características útiles para nuestro propósito:

tendremos certeza de que los mensajes no se han alterado y sabremos que lo ha enviado, realmente, la cuenta que aparece como remitente.

Así pues, S/MIME puede ayudar a determinar la autenticidad de un mensaje.

S/MIME

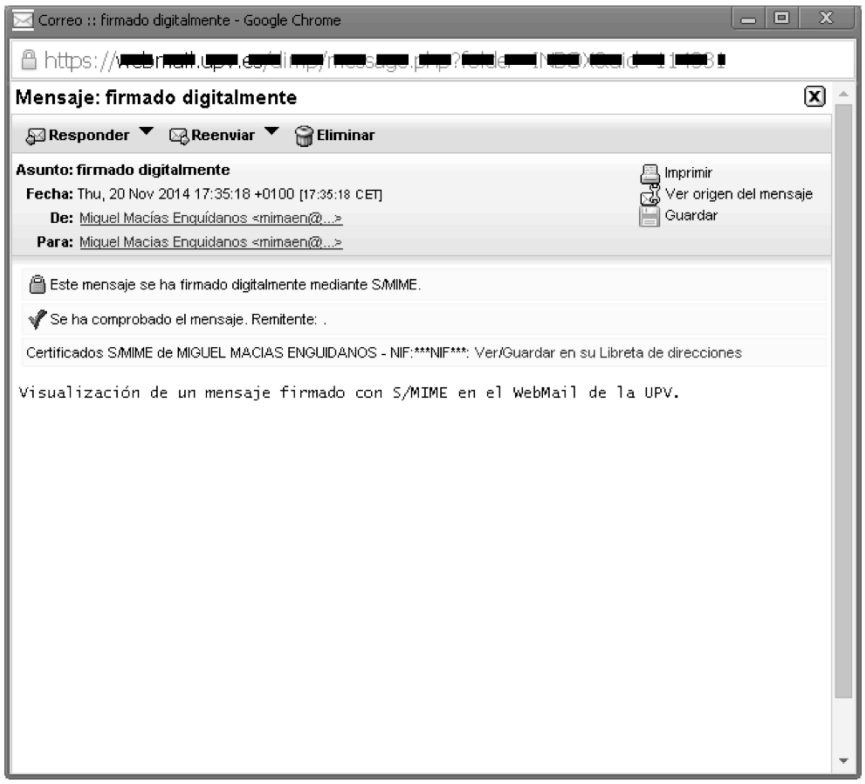
- requiere certificados
- no está soportado por todos los clientes de correo
- los usuarios no lo conocen

S/MIME tiene algunos inconvenientes, aunque ninguno de ellos es grave :-)

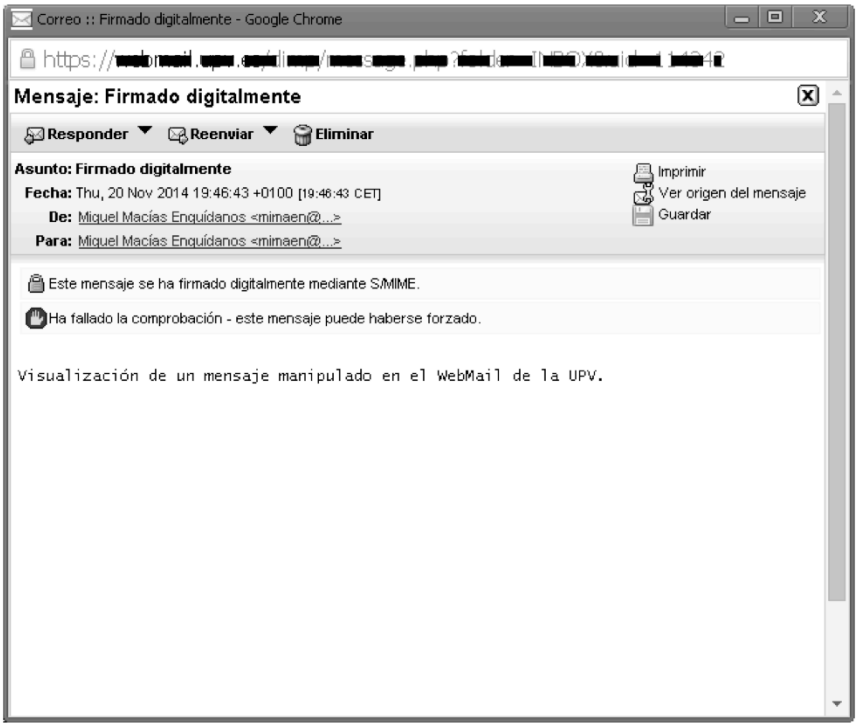
S/MIME

- ayuda a detectar los mensajes fraudulentos
- la firma digital está soportada en muchos clientes
- es sencillo de utilizar

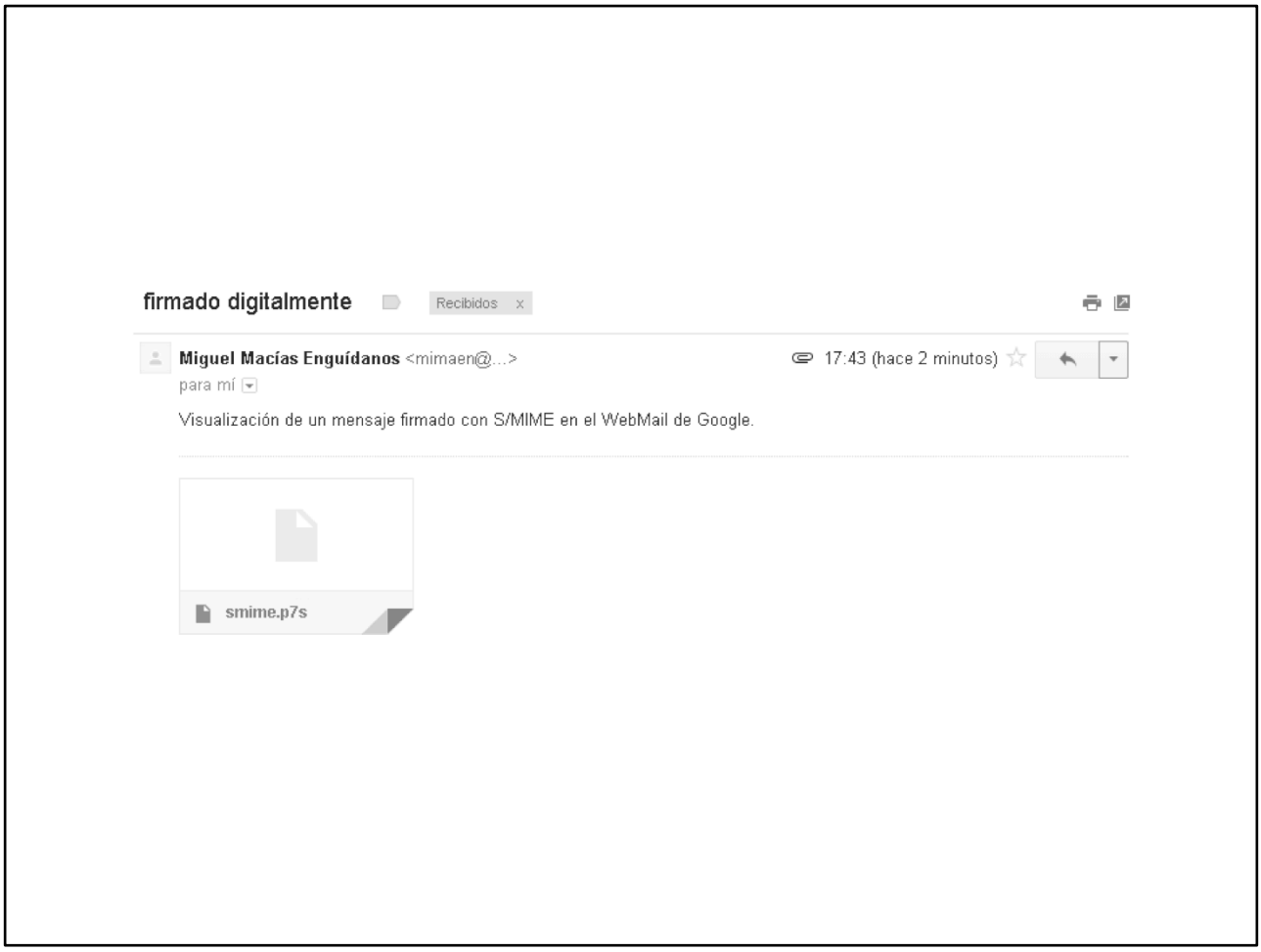
S/MIME aporta ventajas que vale la pena explotar. Además, a medida que se vaya utilizando, se extenderá la cultura entre los usuarios



El WebMail de la UPV es un Horde bastante antiguo. No obstante, activar el soporte S/MIME para la firma digital es sencillo y proporciona información válida y útil para los usuarios.



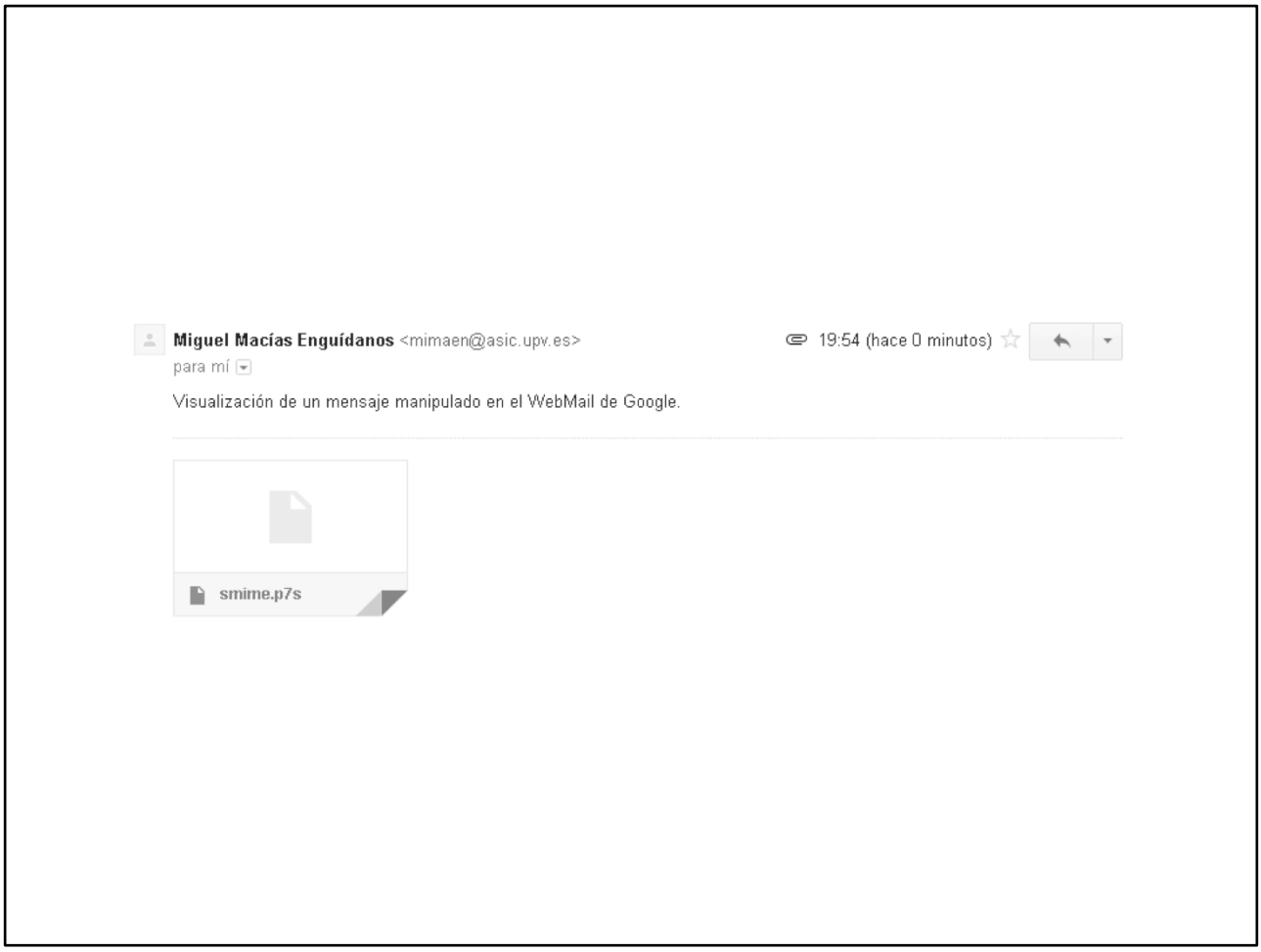
El hecho de incorporar firmas digitales nos aporta ventajas añadidas: se detecta la manipulación de los correos.



En otros WebMail (en este ejemplo vemos GMail), no hay soporte para S/MIME:

- el firmado digital no aporta ninguna ventaja al usuario (por las limitaciones de su cliente)

- se indica, equivocadamente, que hay un adjunto al mensaje. Se trata de la firma digital



Si el cliente no tiene soporte de S/MIME, la manipulación de los correos (evidente cuando hay firma digital) no es detectada ni comunicada al usuario.

UNIVERSITAT POLITÈCNICA DE VALÈNCIA

procedimiento CFD

Se firman digitalmente todos los correos oficiales

También se permite consultarlos en la Intranet

El procedimiento CFD (Correos Firmados Digitalmente) es un servicio horizontal que permite el envío de mensajes a través de plantillas.

Todos los mensajes de CFD se firman digitalmente y, además, permiten que el usuario los consulte en su Intranet. De esta forma, tiene dos mecanismos disponibles para garantizar la autenticidad de los mensajes.

CFD se presentó en las Jornadas Técnicas de RedIRIS 2011 (Valladolid):
http://www.rediris.es/jt/jt2011/programa/jt/

¿Qué es un correo oficial?

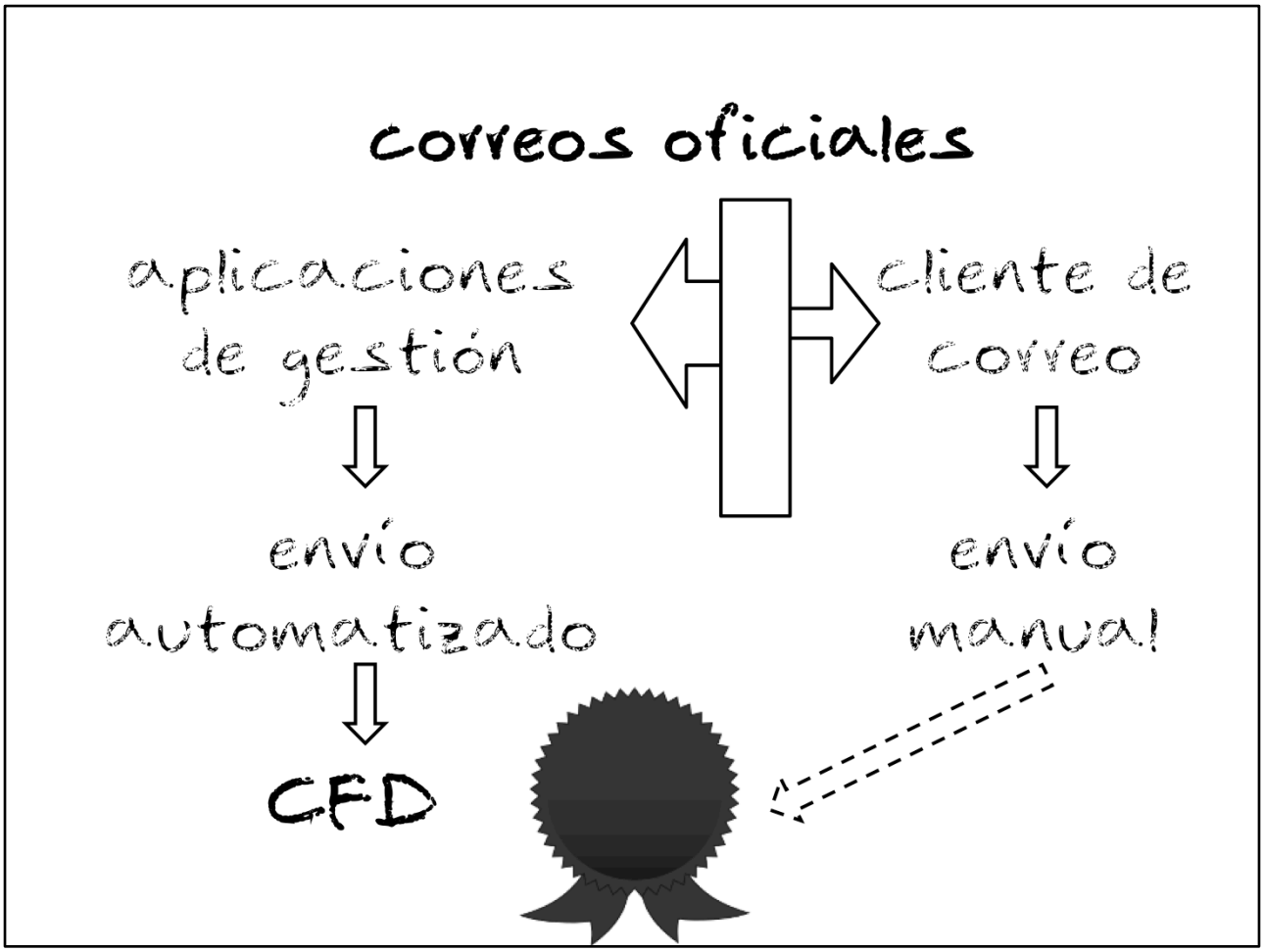
Un mensaje que se envía desde una cuenta corporativa

ejemplos:

rrhh@...

deportes@...

Las cuentas no personales, pertenecientes a servicios, centros, departamentos… de la universidad son las que generan correos oficiales.

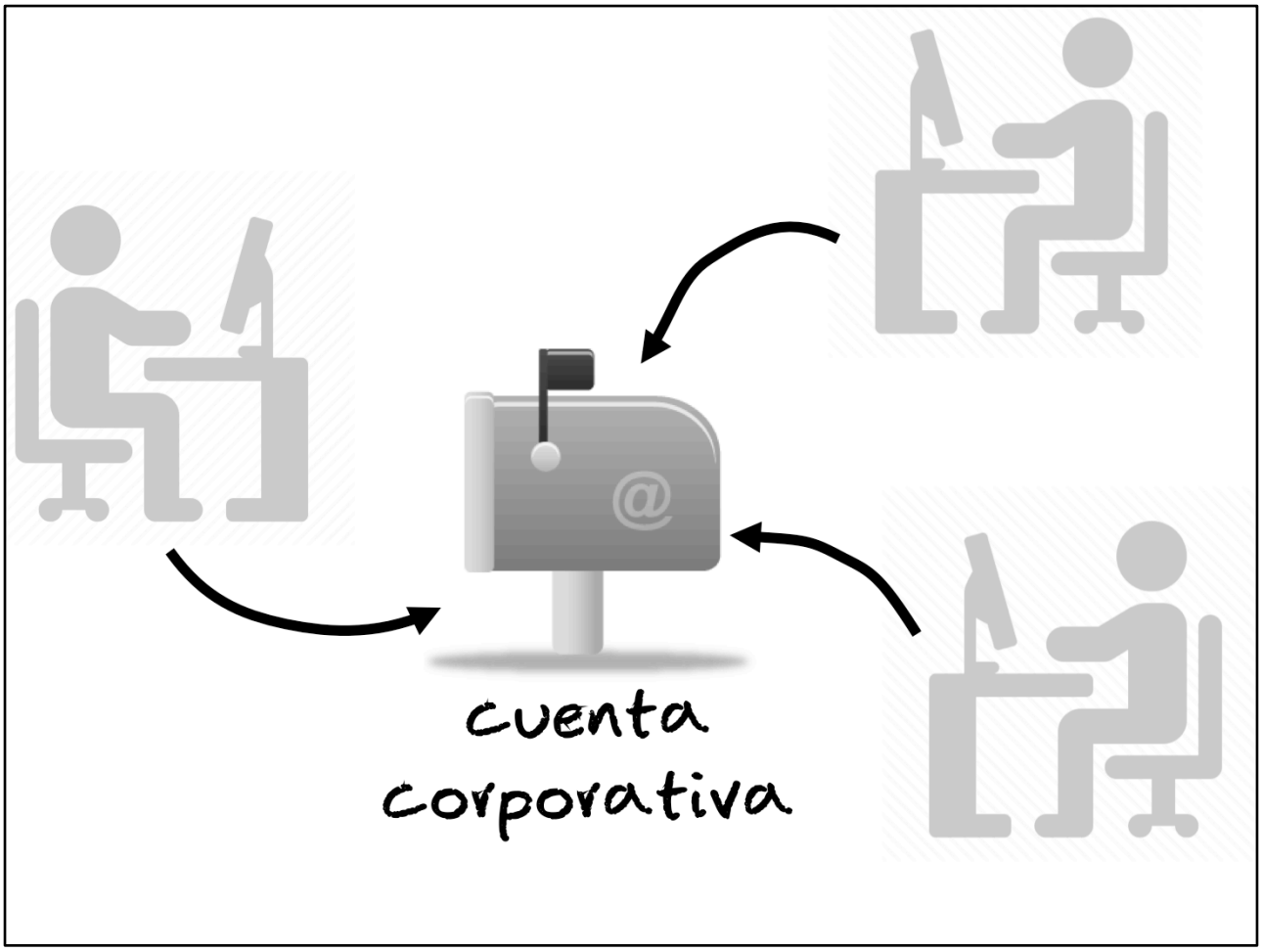


¿Cómo se envían los correos oficiales?

En su gran mayoría, a través de aplicaciones de gestión, es decir, a través de un programa. Todos estos programas están conectados a CFD y se obtiene, de forma transparente, el firmado digital de los mensajes salientes.

Pero siempre hay un número de mensajes que se envían “a mano”, a través del cliente de correo que tienen instalado los gestores de la cuenta corporativa.

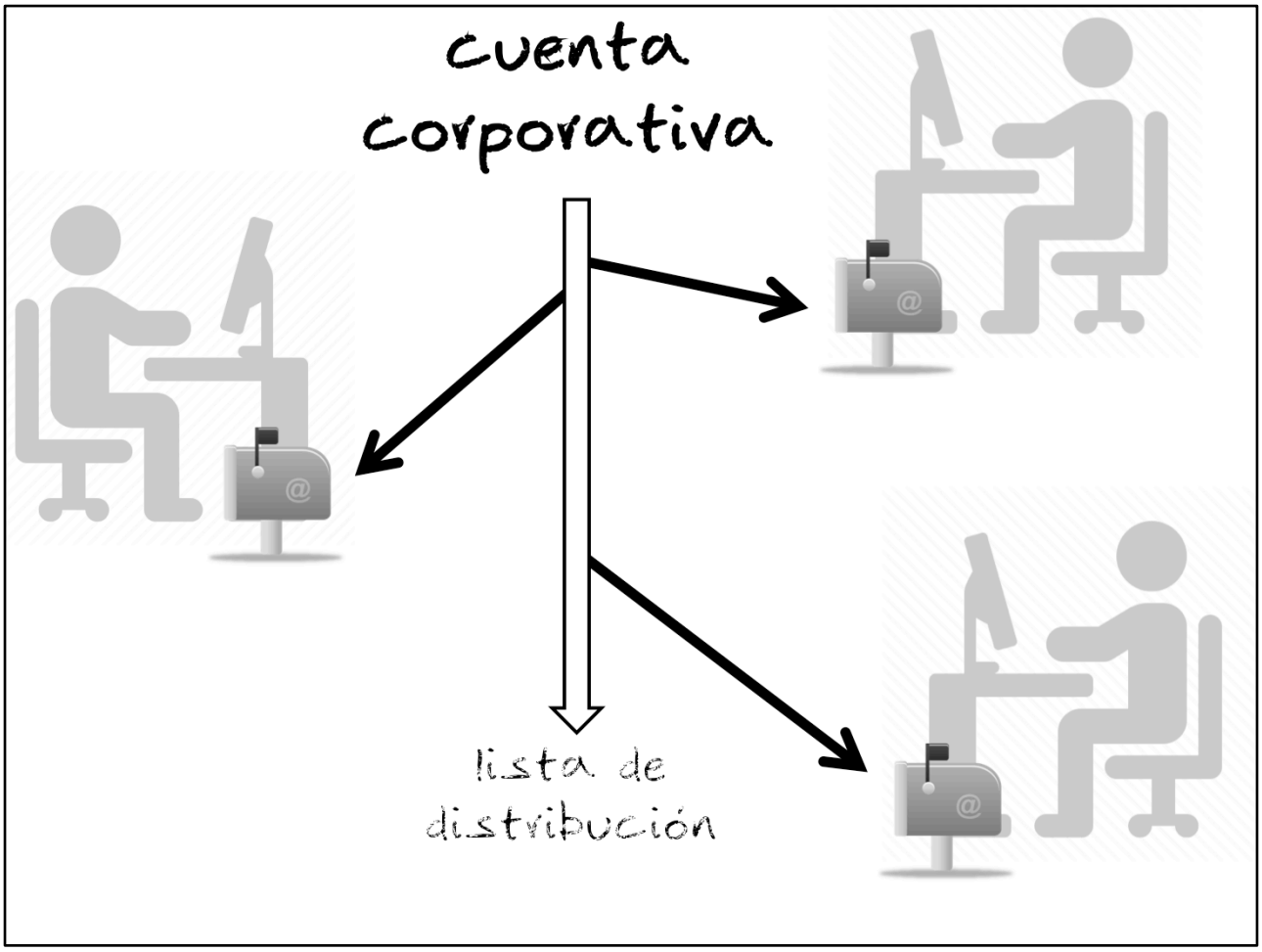
Conseguir que estos mensajes salgan firmados digitalmente no es trivial…



¿Cómo se gestionan las cuentas corporativas?

Puede tratarse de una cuenta con buzón propio, donde los distintos gestores acceden a la misma (vía IMAP), compartiendo las credenciales de acceso.

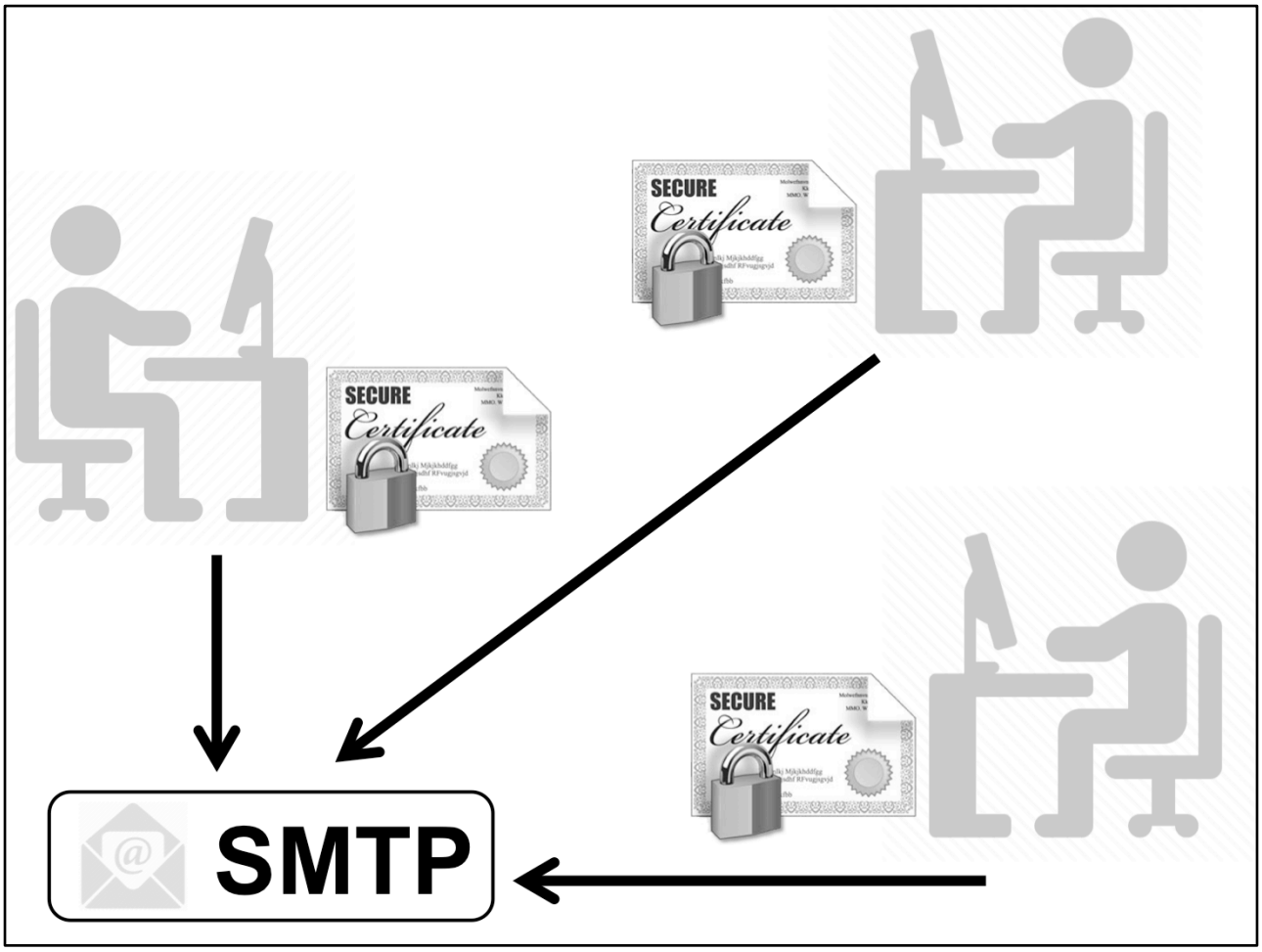
Todos los usuarios ven las mismas carpetas y mensajes, incluidos los enviados desde dicha cuenta.



¿Cómo se gestionan las cuentas corporativas?

Puede tratarse de una lista de distribución, sin buzón propio.

En este caso, los usuarios reciben los mensajes y los clasifican en sus propias carpetas. Los mensajes enviados desde dicha cuenta sólo serán vistos por el resto de gestores si se envía una copia a la propia dirección.

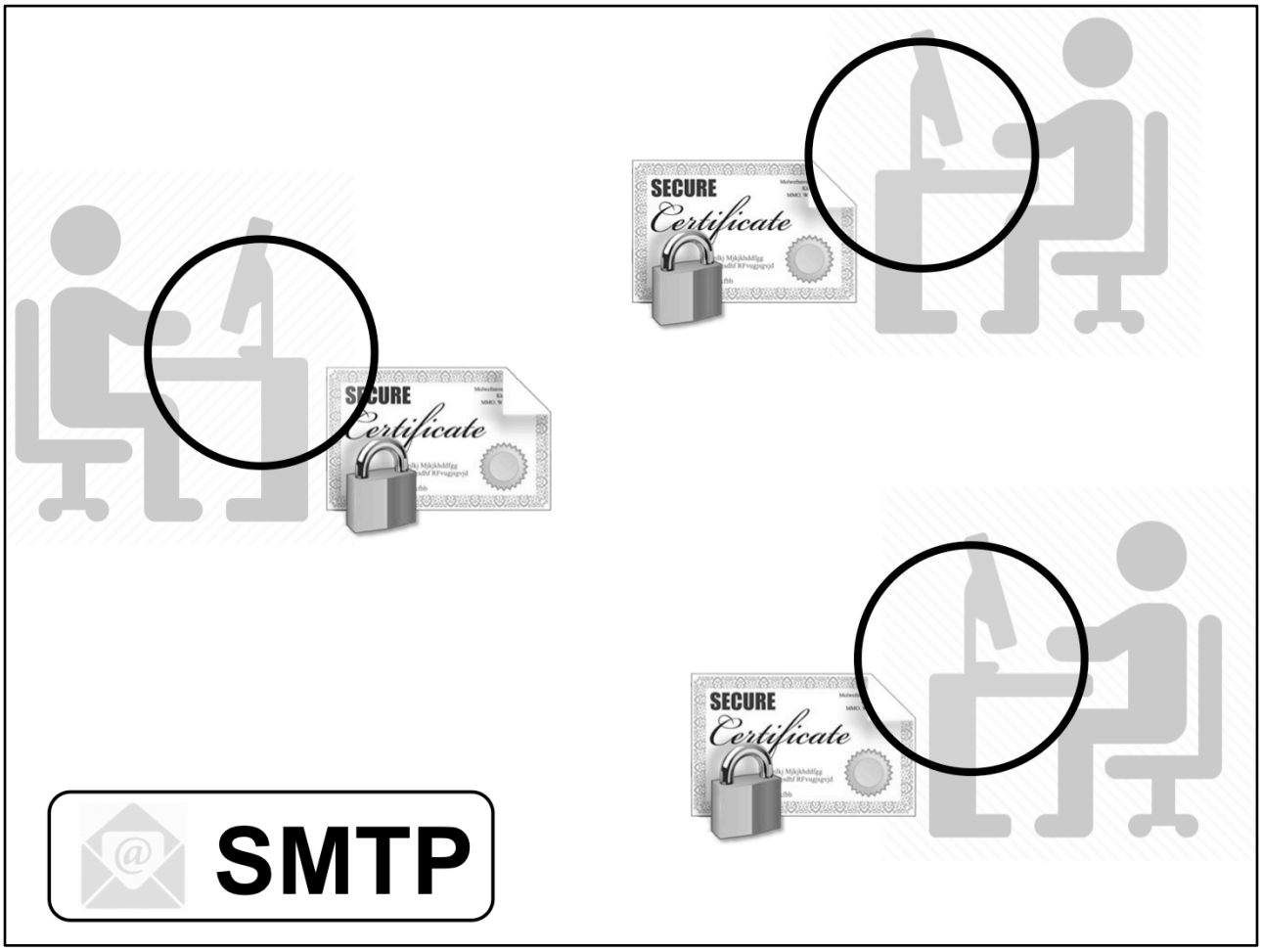


En cualquier caso, ya se trate de una lista de distribución o de una cuenta propia, es necesario distribuir el certificado digital a cada usuario que vaya a realizar envíos con dicha cuenta.

Cada usuario necesita el certificado (con su clave privada asociada) para firmar digitalmente los mensajes antes de enviarlos.

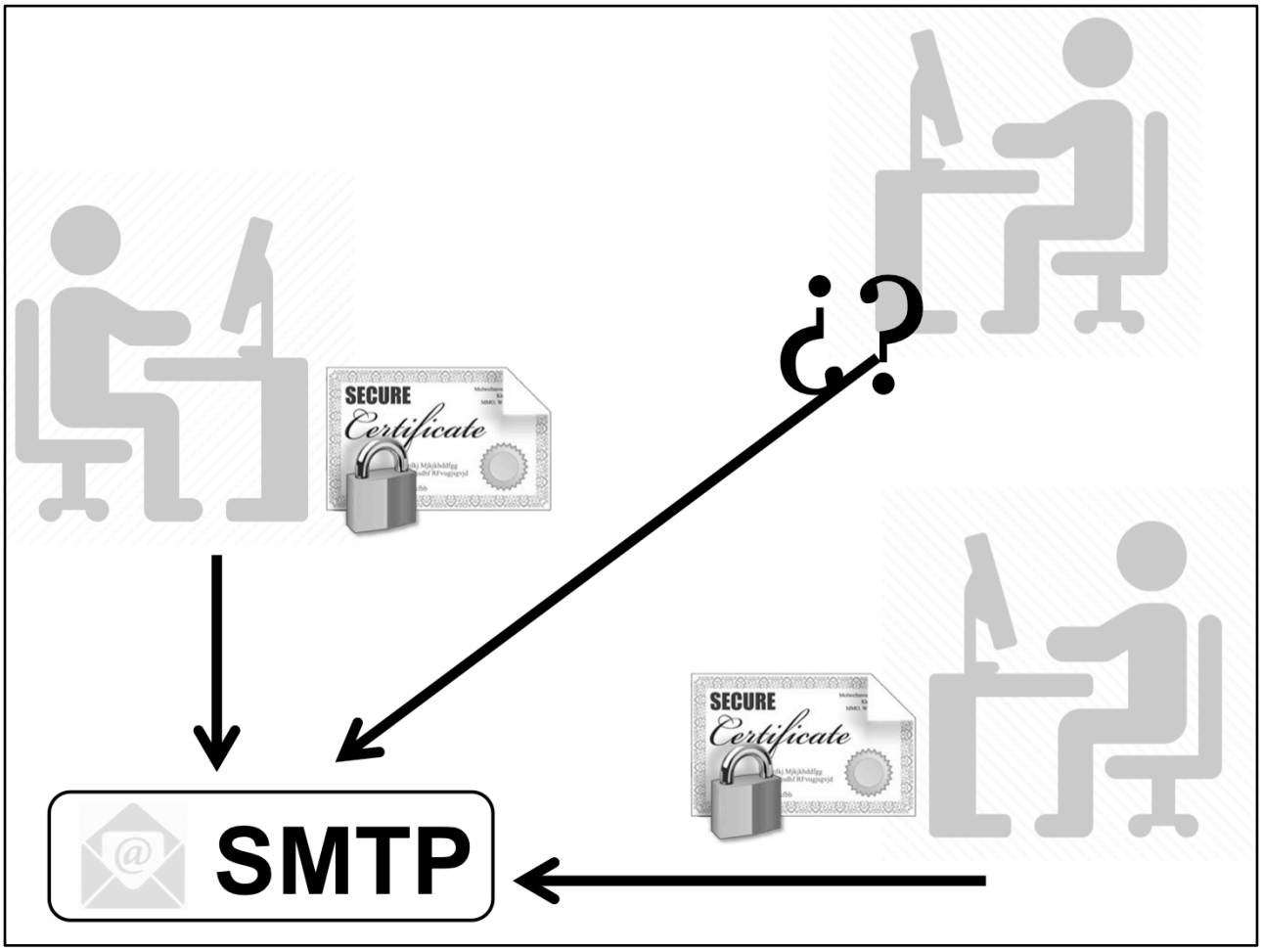
Distribuir el certificado no es inmediato ni automatizable: hay que instalarlo, correctamente, en el perfil del usuario. En la mayoría de los casos, además, el usuario requiere unas indicaciones básicas de cómo utilizarlo.

En muchos casos surgen problemas. Por ejemplo: un usuario tiene configurado un alias de la dirección (por tanto, no es válido para el certificado solicitado) y hay que configurar correctamente la cuenta.



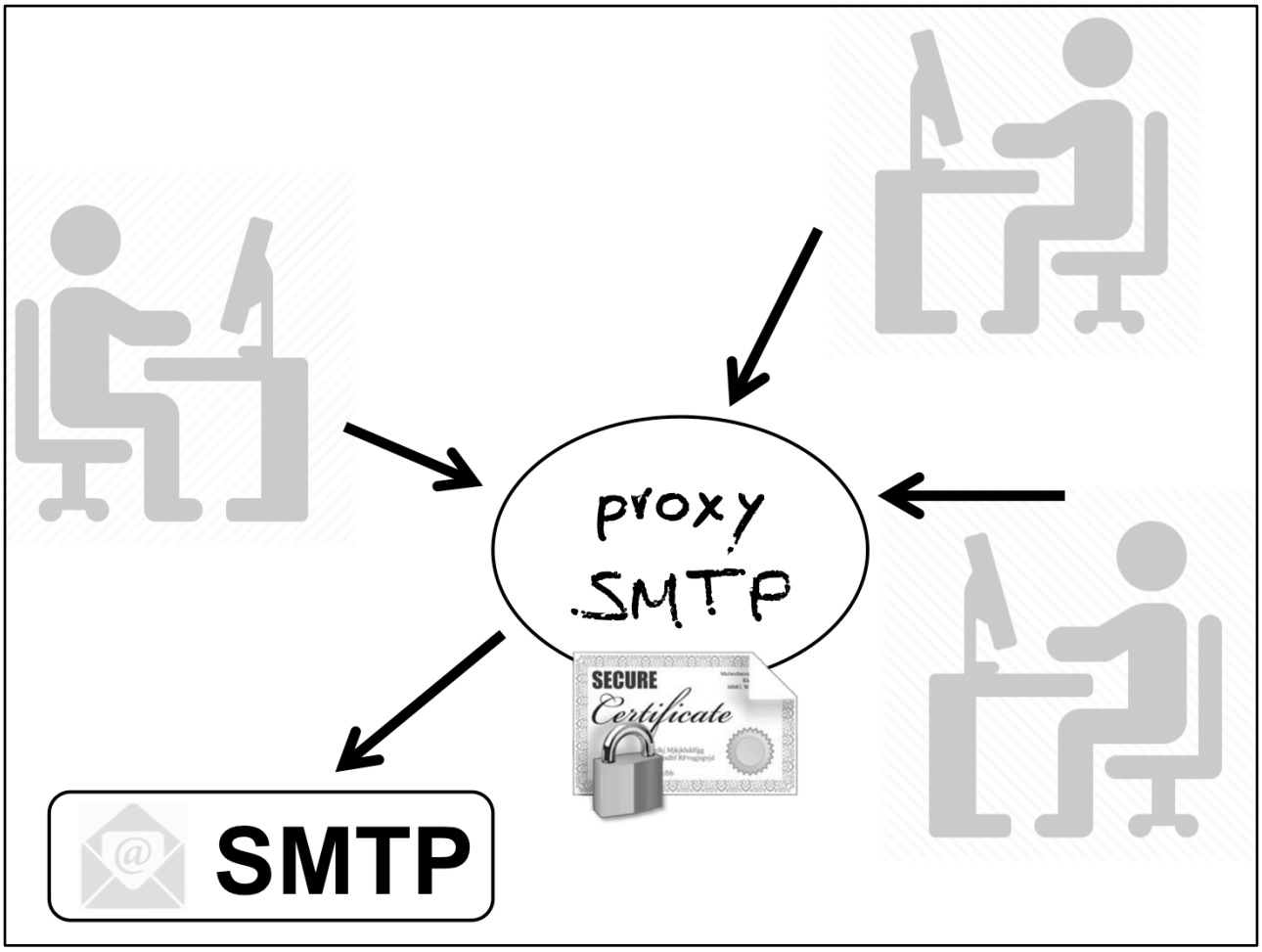
Con esta solución se requiere configurar cada uno de los equipos desde los que se gestiona la cuenta corporativa.

Con cada renovación del certificado será necesario volver a configurar todos y cada uno de los equipos.



¿Qué pasa si un usuario envía un mensaje sin firmarlo? ¿O si no recuerda la contraseña de acceso a la clave privada? ¿O si le han cambiado el equipo y no tiene instalado el certificado?...

Esta solución no garantiza que TODOS los mensajes salgan firmados digitalmente SIEMPRE.

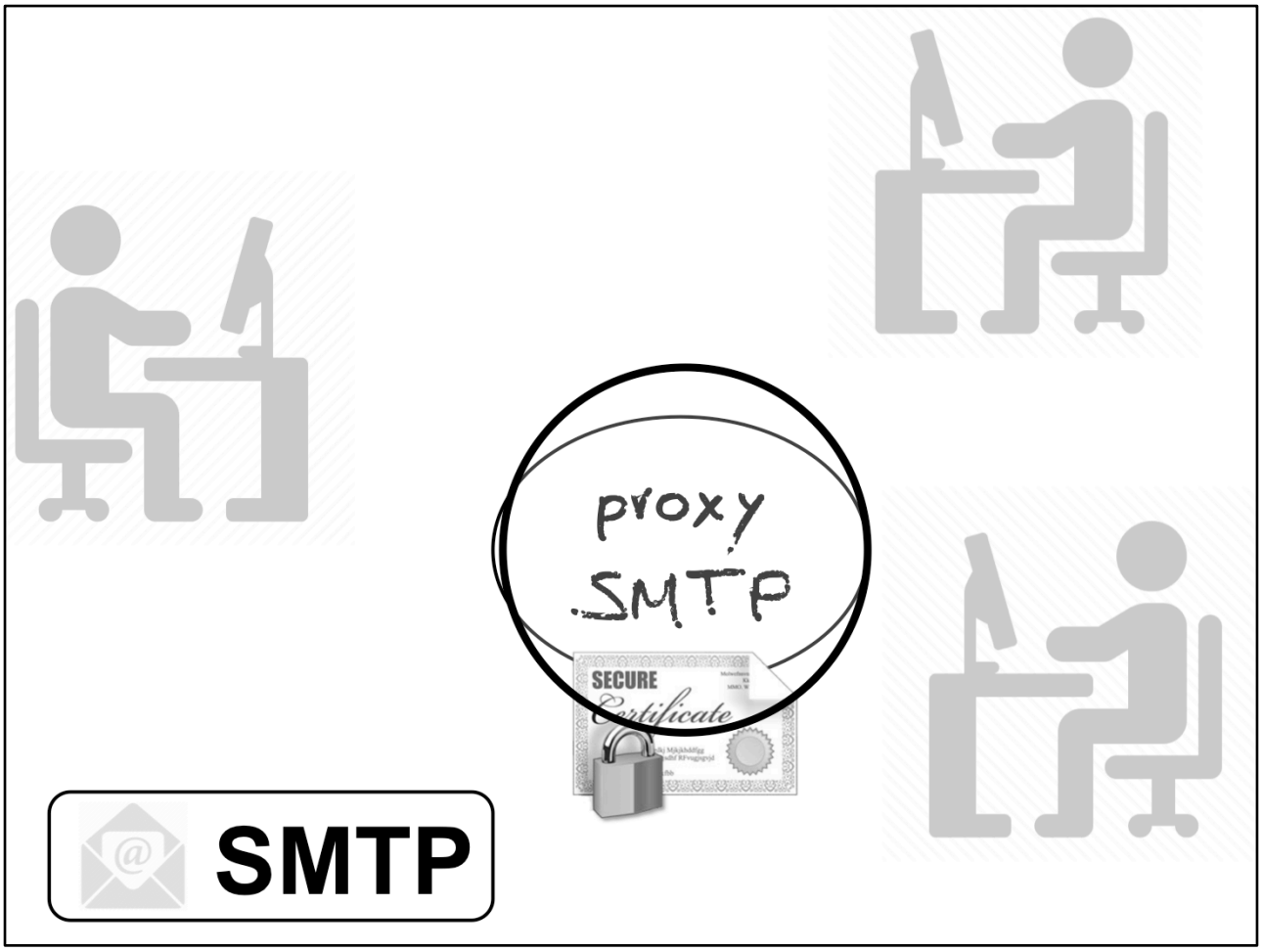


¿Podríamos evitar todos estos problemas y seguir firmando digitalmente todos los mensajes?

Sí, intercalando un proxy SMTP que tenga las características que deseamos.

Para los clientes se comporta como el servidor SMTP asociado a la cuenta corporativa. Es el único punto a configurar en los equipos de usuario.

De forma transparente, enviaremos los mensajes firmados digitalmente. Además, obtendremos otras ventajas con esta infraestructura.



En este caso sólo se requiere configurar correctamente el proxy SMTP.

Los clientes se configuran una única vez para que apunten al proxy SMTP en lugar del SMTP final.

Los mensajes siempre saldrán firmados, independientemente de lo que haga el usuario.

Queremos un **proxy SMTP** que:

- sepa firmar digitalmente
- tenga la seguridad necesaria para evitar fraudes internos
- unifique el nombre y dirección del remitente
- pueda generar autocopias

http://opaquemail.org/

+ proyecto Open Source
+ implementa un proxy SMTP
+ soporte S/MIME completo
+ multiplataforma (.NET)
- pensado para uso individual

-> buen punto de partida

Tomamos como punto de partida OpaqueMail.

Tiene muchas de las características que buscamos, pero necesita ampliarse para generar el proxy SMTP necesario.

Seguridad

- sólo usuarios autenticados
- sólo IP permitidas

- control de acceso por usuario y/o IP para firmar con un certificado concreto

Utilizando la autenticación del servidor SMTP final podemos autenticar a los usuarios en el proxy.

Hay que tener en cuenta que no todo usuario con acceso al proxy tiene derecho a firmar con cualquier certificado.

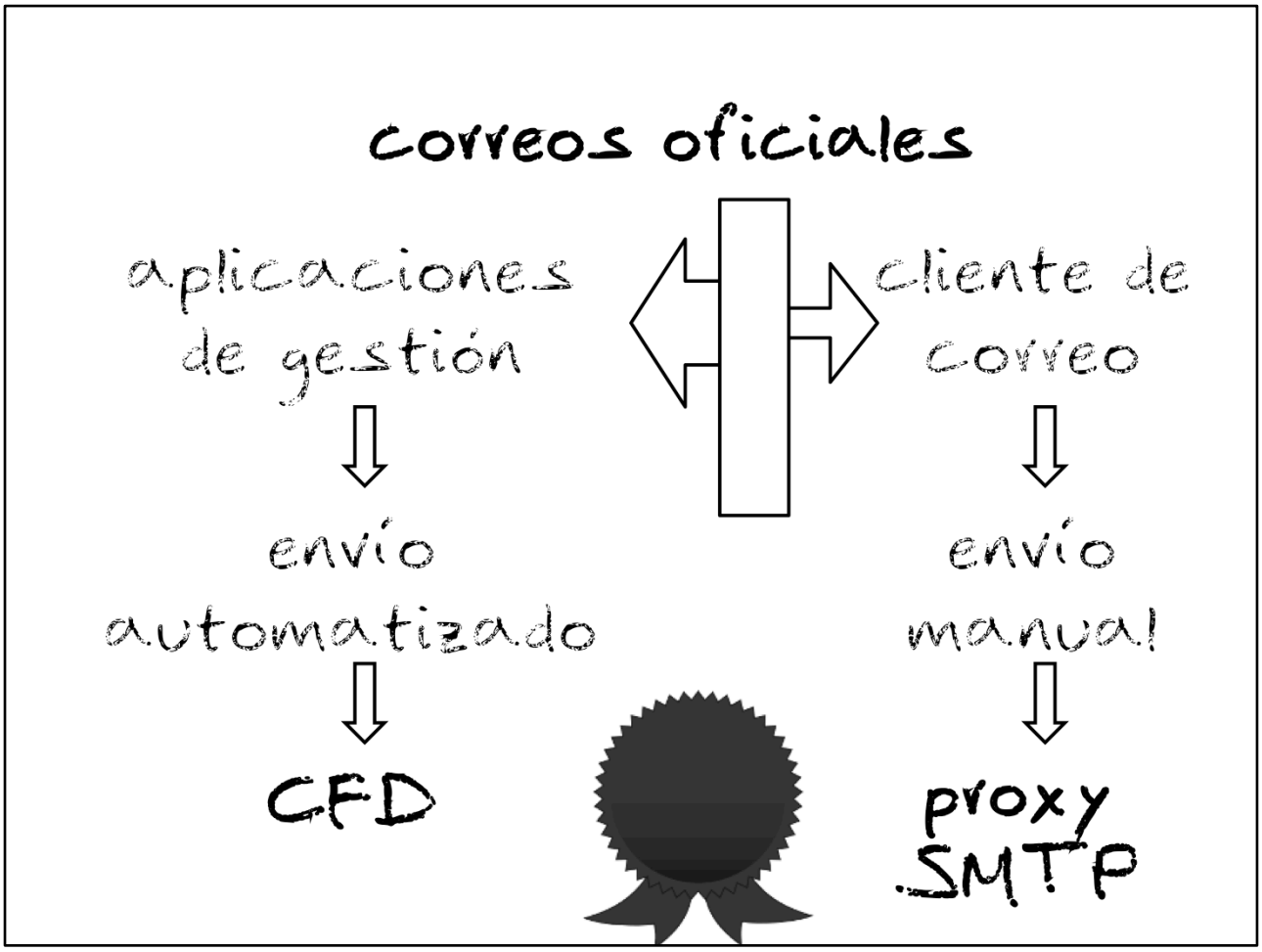
Configuración

```
…
<AcceptedIPs>
…
<AcceptedUsers>
…
<From>
…
<CC>… <BCC>
…
<SMIMESign>
…
<ExportDirectory>
…
<LogFile>
…
```

A través de un XML se puede configurar cada cuenta, estableciendo las características deseadas.

Por ejemplo:

<From> nos permitirá establecer el remitente correcto, independientemente de lo que indique el cliente
<CC> y <BCC> nos permiten añadir destinatarios a los mensajes (para la autocopia, por ejemplo)



Finalmente, conseguimos que todos los correos oficiales salgan firmados digitalmente de forma transparente:

- toda la gestión de certificados está centralizada
- no es necesario modificar la configuración de los clientes
- no hay posibilidad de enviar mensajes que no estén firmados digitalmente
- se pueden obtener copias de los mensajes, automáticamente, en la cuenta remitente
- se garantiza que sólo los usuarios autorizados pueden enviar mensajes firmados con estos certificados
- el formato de los mensajes firmados es coherente y válido para todas las plataformas

S/MIME de oficio

https://github.com/mimaen/opaquemail