(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 311 673**

(51) Int. Cl.:
H04L 12/58 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **03104388 .8**
(96) Fecha de presentación : **26.11.2003**
(97) Número de publicación de la solicitud: **1536601**
(97) Fecha de publicación de la solicitud: **01.06.2005**

(54) Título: **Procedimiento y sistema de encriptación de correos electrónicos.**

(73) Titular/es: **Totemo AG.**
Seestrasse 134a
8700 Küsnacht, CH

(72) Inventor/es: **Mock, Marcel y**
Swedor, Olivier

(74) Agente: **Sugrañes Moliné, Pedro**

(45) Fecha de publicación de la mención BOPI:
16.02.2009

(45) Fecha de la publicación del folleto de la patente:
16.02.2009

DESCRIPCIÓN

Procedimiento y sistema de encriptación de correos electrónicos.

La presente invención se refiere a un procedimiento de cifrado para correos electrónicos enviados desde un emisor a un receptor, y a un sistema de cifrado. La presente invención también se refiere a un procedimiento y sistema de cifrado global (end-to-end). La presente invención también se refiere a la protección de correos electrónicos entre un cliente de correo electrónico y un sistema de cifrado dentro de la misma red privada, por ejemplo, dentro de la misma red de área local o entre un proveedor de servicios de Internet y un cliente.

Ya se conocen soluciones del lado del servidor para proteger la confidencialidad de los correos electrónicos mientras viajan por internet en su camino hacia su correspondiente receptor. Un ejemplo de una solución de este tipo la ofrece, entre otras personas, el solicitante con el nombre comercial TrustMail. Con una solución de este tipo, el cifrado del correo electrónico sólo se produce una vez que el correo electrónico saliente ha alcanzado el sistema 16 de cifrado (normalmente justo antes de salir de la red 13 privada de la empresa del emisor) tal como se muestra en la figura 1.

En esta figura, un servidor de correo electrónico que incluye un sistema 16 de cifrado se instala dentro de la red 13 privada de la empresa del emisor y se conecta directamente a un cortafuegos 17. La red 13 privada de la empresa comprende una pluralidad de clientes 10, 11 de correo electrónico conectados mutuamente con nodos 12 y/o conmutadores 14. La referencia 10 indica el cliente de correo electrónico del emisor 1. Los correos electrónicos cifrados que salen del cortafuegos 17 son enviados por un router 18 a través de Internet 3 y recibidos por un servidor 5 de correo electrónico en la red del receptor 6. La línea discontinua muestra la parte protegida (cifrada) de la ruta del correo electrónico.

Esta situación ofrece una seguridad mucho mejor que la convencional, en la que los correos electrónicos viajan a través de Internet 3 sin ninguna protección. El servidor 16 de cifrado es responsable de generar, recopilar y distribuir certificados de cifrado para asegurar que ningún correo electrónico confidencial sale de la red 13 privada de la empresa sin protección, y ofrece una gran comodidad a los usuarios dentro de la empresa.

Sin embargo, en esta solución de la técnica anterior, los correos electrónicos están básicamente desprotegidos hasta que son procesados por el sistema de cifrado en el servidor 16 de correo electrónico. Este problema es común a todas las soluciones de seguridad de correo electrónico que cifran correos electrónicos de forma central en un servidor.

A diferencia de cuando viaja por Internet, los atacantes externos no pueden, o al menos no deberían poder, acceder al correo electrónico en la parte de red privada de su recorrido. Pero cualquier empleado puede acceder a él con bastante facilidad y también un atacante que pudiera entrar en la red 13 e instalar un *packet sniffer* (programa de capturas de tramas de red). En primer lugar, puede ser interceptado en cualquier ordenador o dispositivo de red que cruce en su camino hacia el servidor 16 de correo electrónico seguro. En segundo lugar, e incluso más sencillo, si están conectados múltiples ordenadores a la red a través de nodos 12, al igual que en el ejemplo de la figura 1, cualquiera puede leer todos los correos electrónicos enviados por todos los clientes conectados al mismo nodo. Esto se debe a que la mayoría de redes privadas se basan en protocolos tales como, por ejemplo, Ethernet y TCP-IP, en los que todo se envía a todo el mundo. Todos los ordenadores escuchan permanentemente todos los paquetes de datos, por ejemplo, tramas de Ethernet, pero se supone que sólo procesan los dirigidos a ellos, desechando los otros. Esto significa que cuando un ordenador en la figura 1 envía un correo electrónico, lo reciben los ordenadores conectados al mismo nodo 12, así como el conmutador. El usuario de uno de estos tres ordenadores simplemente tiene que instalar un pequeño software "sniffer" para acceder a todo el tráfico que se origina desde o se envía a los otros tres ordenadores conectados al mismo nodo que él. Incluso si se utilizan conmutadores en lugar de nodos, aún puede haber formas de que los atacantes husmeen en el tráfico de la red LAN.

Por tanto, ya no se consigue una seguridad exhaustiva sin cifrar los correos electrónicos en los clientes internos de correo electrónico de empleados. Sin embargo, instalar certificados de receptores es una tarea pesada y demasiado complicada o que requiere mucho tiempo para muchos usuarios sin experiencia. Además, este proceso sólo es posible si el receptor es realmente capaz de proporcionar un certificado. Esto significa que el emisor primero tiene que solicitar un certificado para el receptor (si nadie de su empresa ha hecho esto antes y ha almacenado de forma central el certificado), y esperar a que el receptor reaccione. Antes de esto no puede enviarse nada. Además, el receptor debe admitir la misma técnica de cifrado que el emisor. Un emisor que desee enviar correos electrónicos cifrados a muchos receptores puede tener que instalar un montón de plug-ins y software de cifrado diferentes.

Asimismo, si los certificados no están almacenados de forma central, cuando múltiples usuarios dentro de una empresa envían correos electrónicos a un mismo receptor, cada usuario que tenga que solicitar un certificado del receptor tiene que repetir todo el proceso, lo cual requiere bastante tiempo tanto para el emisor como para el receptor. Esto hace que el proceso de cifrar un correo electrónico para un receptor nuevo cuyo certificado aún no esté en la libreta de direcciones utilizada por el emisor sea difícil: se requiere una fase de configuración para obtener el certificado del receptor (suponiendo que tiene uno) y añadirlo a la libreta de direcciones antes de que pueda realizarse cualquier comunicación segura. Almacenar los certificados del receptor en cada cliente de correo electrónico de emisor requiere además precauciones de copia de seguridad suplementarias.

Lo que es aún peor, esta solución hace imposible escanear en un lugar central de la red 13 de área local los correos electrónicos en busca de virus o hacer que se ejecute cualquier comprobación de contenido en ellos dado que están cifrados. Esto significa una importante pérdida de control para la empresa sobre lo que se envía o recibe por sus usuarios, ya sea contenido ofensivo, contenido confidencial, virus, etc.

Además, los procedimientos de cifrado "end-to-end" no permiten definir reglas de delegación en el servidor de correo electrónico de la empresa. La delegación permite hacer que un usuario o grupo de usuarios reciba correos electrónicos destinados originalmente a otra persona. Dado que los correos electrónicos están cifrados con el certificado del receptor original, el usuario o grupo de usuarios al que se delega el correo electrónico no será capaz de descifrarlo.

Se conocen varias soluciones en la técnica anterior para cifrar correos electrónicos dentro de una red de área local. Sin embargo, muchas soluciones existentes sólo son capaces de cifrar correos electrónicos internos, es decir, correos electrónicos enviados a un receptor dentro de la misma red. Otras soluciones posibles requieren la instalación de un plug-in en los clientes 11 de correo electrónico de cada usuario, que cifra los correos electrónicos salientes con un certificado del servidor 16 de correo electrónico de la LAN, en lugar de cifrarlos con certificados correspondientes a la dirección de correo electrónico del receptor final. Sin embargo, desarrollar e instalar plug-ins es costoso, especialmente si se utilizan diferentes tipos de clientes 11 de correo electrónico.

Otra posibilidad es cambiar la forma en que los usuarios envían los correos electrónicos. Una forma de cifrar los correos electrónicos para el servidor 16 seguro sin instalar plug-ins sería que los usuarios enviaran todos los correos electrónicos a una dirección de correo electrónico especial (por ejemplo, la dirección del servidor seguro), y poner la dirección del receptor real en el campo de asunto del correo electrónico. Otra opción imaginable es intentar hacer que la comunicación entre el servidor 16 de correo electrónico seguro y los clientes de correo electrónico suceda por una conexión SSL, pero, dependiendo de la arquitectura de la red y el servidor de correo electrónico utilizado, esta opción puede no ser posible. También requiere muchos recursos construir una conexión SSL cada vez, especialmente dado que los clientes de correo electrónico normales comprueban automáticamente y de forma periódica la llegada de nuevos correos electrónicos.

Por tanto, un objetivo de la presente invención es proporcionar una comunicación de correo electrónico cifrada más segura entre los clientes de correo electrónico de usuario y un sistema 16 de cifrado central en la red, preferiblemente sin instalar plug-ins, sin construir conexiones SSL y sin cambiar mucho la forma en que los usuarios envían correos electrónicos.

El documento US-B1-6.609.196 describe un cortafuegos de correo electrónico que aplica políticas a los mensajes de correo electrónico entre un primer sitio y una pluralidad de segundos sitios de acuerdo con una pluralidad de políticas que puede seleccionar el administrador. El cortafuegos comprende un relé de protocolo de transferencia de correo simple (SMTP, Simple Mail Transfer Protocol) para hacer que los mensajes de correo electrónico se transmitan entre el primer sitio y segundos sitios seleccionados. Una pluralidad de gestores de políticas hacen cumplir las políticas seleccionables por el administrador. Las políticas, por ejemplo, políticas de cifrado y descifrado, comprenden al menos una primera política de fuente/destino, al menos una primera política de contenido y al menos una primera política de virus. Las políticas se caracterizan por una pluralidad de criterios que puede seleccionar el administrador, una pluralidad de excepciones a los criterios que puede seleccionar el administrador y una pluralidad de acciones asociadas con los criterios y las excepciones que puede seleccionar el administrador. Los gestores de políticas comprenden un gestor de acceso para restringir la transmisión de mensajes de correo electrónico entre el primer sitio y los segundos sitios de acuerdo con la política de fuente/destino. Los gestores de políticas comprenden además un gestor de contenido para restringir la transmisión de mensajes de correo electrónico entre el primer sitio y los segundos sitios de acuerdo con la política de contenido, y un gestor de virus para restringir la transmisión de mensajes de correo electrónico entre el primer sitio y los segundos sitios de acuerdo con la política de virus.

Otro objetivo de la invención es proporcionar un sistema de cifrado y un procedimiento para cifrar correos electrónicos entre clientes de correo electrónico de usuario y el servidor de correo electrónico de la empresa del usuario.

Otro objetivo de la invención es hacer posible delegar correos electrónicos a otros usuarios, debiendo garantizar el procedimiento y el sistema de la invención la seguridad de los correos electrónicos entre el servidor de correo electrónico que realiza la tarea de delegación y el nuevo receptor.

Otro objetivo de la invención es proporcionar un procedimiento y sistema de cifrado global para cifrar correos electrónicos en toda el recorrido entre el cliente 11 de correo electrónico del usuario y el servidor 5 ó cliente 6 de correo electrónico del receptor sin poner en peligro la posibilidad de realizar una comprobación de seguridad del contenido o los archivos adjuntos del correo electrónico en una aplicación central en la red 13 de la empresa del usuario.

Otro objetivo de la invención es proporcionar un sistema y un procedimiento de cifrado de correo electrónico mejorados que eviten los problemas antes mencionados de la técnica anterior o soluciones relacionadas.

Según la invención, los problemas se resuelven, entre otros, mediante un procedimiento de cifrado para correos electrónicos enviados desde un emisor a un receptor, que comprende los siguientes pasos:

el emisor envía, desde un sistema de cifrado, un certificado correspondiente a dicho receptor,

el sistema de cifrado devuelve a dicho emisor un primer certificado proforma correspondiente a dicho receptor, generándose o recuperándose el certificado proforma por los sistemas de cifrado del receptor y utilizándose únicamente entre el emisor y el sistema de cifrado,

el emisor envía, con su cliente de correo electrónico, un correo electrónico saliente a dicho receptor cifrado con dicho certificado proforma,

dicho correo electrónico se envía a través del sistema de cifrado,

dicho sistema de cifrado descifra el correo electrónico utilizando una clave privada correspondiente a dicho certificado,

dicho sistema de cifrado hace que el contenido del correo electrónico esté disponible al receptor.

Esto tiene la ventaja, entre otras cosas, de que el correo electrónico se cifra entre el cliente de correo electrónico del emisor y el sistema de cifrado, pero puede ser descifrado por este sistema, que utiliza la clave privada correspondiente al certificado proforma suministrado por el sistema al emisor. Así, el sistema de cifrado puede realizar varias tareas de seguridad en el correo electrónico saliente, por ejemplo, detección de contenidos ofensivos y virus.

Esto también tiene la ventaja de que los correos electrónicos pueden enviarse de una forma normal dado que el emisor no sabe necesariamente que el certificado usado no corresponde al receptor pretendido, sino al sistema de cifrado interno. Por tanto, puede realizarse el cifrado con las aplicaciones de seguridad, por ejemplo, S/MIME, disponibles en la mayoría de clientes de correos electrónicos, sin instalar ningún nuevo plug-in o software en el equipo del usuario.

Esto también tiene la ventaja de que todo el proceso de configuración, incluyendo la generación de pares de claves y su instalación en los clientes de correo electrónico, lo realiza el sistema de cifrado, o al menos interviene en él. Asimismo, puede instalarse fácilmente o hacerse accesible al sistema de cifrado un directorio central de certificados y direcciones de receptor.

Por tanto, la presente invención también se refiere a un nuevo tipo de pasarela de correo electrónico segura que no sólo cifra los correos electrónicos salientes entre ésta y el receptor externo, al igual que en las pasarelas de cifrado de correo electrónico normales, sino también entre el emisor interno y el sistema de cifrado. Esto se consigue preferiblemente sin instalar ningún plug-in en los clientes de correo electrónico internos, sin ningún cambio significativo en los hábitos de los emisores y sin pérdida de control del contenido por parte de la empresa que utiliza el sistema (al igual que en el caso del cifrado "end-to-end"). El objetivo es contar con tantas de las ventajas de los tipos de cifrado del lado de servidor y "end-to-end" como sea posible.

Éstas y otras ventajas se comprenderán mejor con la descripción de varias realizaciones ilustradas por las figuras adjuntas, en las que:

la fig. 1 es una representación esquemática de una red de la técnica anterior con una solución de cifrado en el lado del servidor;

la fig. 2 es una representación esquemática de los procesos que intervienen cuando un usuario interno envía un correo electrónico cifrado de salida mediante el procedimiento y el sistema según una realización de la invención;

la fig. 3 es una representación esquemática de una red que incluye un sistema de cifrado con un servidor de correo electrónico, una pasarela de cifrado y un directorio según una realización de la invención;

la fig. 4 es una representación esquemática de una red que incluye un sistema de cifrado con un servidor de correo electrónico y una pasarela de cifrado según una realización de la invención;

la fig. 5 es una representación esquemática de una red que incluye un servidor de correo electrónico de cifrado y un directorio según una realización de la invención;

la fig. 6 es una representación esquemática de una red que incluye un servidor de correo electrónico de cifrado según una realización de la invención;

la fig. 7 es una representación esquemática de una red que incluye un sistema de cifrado con un servidor de correo electrónico, una pasarela de cifrado y un directorio alojado por el proveedor de servicios de Internet o proveedor de correo electrónico del usuario, según una realización de la invención.

la fig. 8 es una representación esquemática de una red que incluye un sistema de cifrado con un servidor de correo electrónico, una pasarela de cifrado y un directorio según una realización de la invención.

En la siguiente sección de la descripción y en las reivindicaciones, cuando hablamos de una "red privada", puede ser una red de área local (LAN), una pluralidad de redes de área local conectadas entre sí, una red VPN (virtual private network, red privada virtual), o una pluralidad de redes LAN y/o VPN y/o WLAN conectadas entre sí. Así, partes de la red pueden ser públicas; sin embargo, una característica de la red privada es que debe ser posible instalar en la red un sistema de cifrado que será capaz de descifrar correos electrónicos seguros; por tanto, debe existir una relación de confianza entre todos los usuarios de la red privada y el administrador del sistema de cifrado de confianza. En la mayoría de realizaciones, la red privada tiene un administrador que también administra el sistema de cifrado.

Cuando decimos "certificado" o "clave pública", queremos decir lo mismo, salvo si se indica expresamente. Para cifrar datos utilizando cifrado simétrico y/o asimétrico, se necesita la clave pública del receptor de los datos. Un certificado es simplemente una clave pública con cierta información adjunta. Diferentes tecnologías utilizan diferente terminología, con S/MIME normalmente se prefiere la palabra "certificado" y con PGP, el término "clave pública".

Cuando decimos "sistema de cifrado", queremos decir no sólo el módulo de software y/o hardware que realiza realmente el cifrado, sino un sistema completo de servidor para el procesamiento y el cifrado de correos electrónicos. Dependiendo de la realización, el sistema de cifrado puede incluir, por ejemplo, una pasarela de cifrado, un relé de correo electrónico o un servidor de correo electrónico, un directorio de direcciones, un directorio proxy, etc. Los componentes diferentes del sistema de cifrado pueden implementarse mediante uno o varios módulos de software y uno o varios módulos de hardware, por ejemplo, un servidor, una aplicación de seguridad de Internet, o un grupo de servidores conectados entre sí.

Normalmente utilizamos el término "pasarela de cifrado" o "pasarela segura" para designar la parte del sistema de cifrado que realmente genera y suministra certificados, descifra y cifra correos electrónicos entrantes y salientes, etc. La pasarela de correo electrónico segura puede implementarse mediante uno o varios módulos que se ejecutan en uno o varios servidores. El administrador de la pasarela de cifrado es un administrador de confianza de todos los usuarios de la red privada.

"Usuarios internos" son usuarios dentro de la red privada en la que se instala el sistema, por ejemplo, los empleados de la empresa que utilizan el sistema, usuarios conectados a una red de área local común o un grupo de redes de área local, o clientes de un proveedor de servicios de Internet o un proveedor de servicios de valor añadido que utiliza el sistema.

Cuando hablamos de cifrado, éste puede ser cualquier tecnología simétrica y/o preferiblemente asimétrica de cifrado (por ejemplo, S/MIME, PGP, etc.) en la que los correos electrónicos se cifran mediante el certificado del receptor y se descifran mediante la clave pública correspondiente. Los correos electrónicos también pueden firmarse con la clave privada del emisor, permitiendo así a los receptores comprobar la autenticidad del mensaje con el certificado correspondiente.

Cuando decimos "directorio", queremos decir un directorio o base de datos que se ejecuta preferiblemente en un servidor dentro de la red privada y que contiene información de usuario, por ejemplo, certificados y direcciones de correo electrónico de usuario. Puede utilizarse cualquier tipo de lenguaje o protocolo para acceder a él (LDAP, SQL, etc.).

Cuando decimos "correo electrónico", queremos decir correos electrónicos SMTP convencionales, así como equivalentes, tales como mensajes instantáneos u otros mensajes digitales que puedan enviarse y recibirse con clientes de mensajes que se ejecutan en ordenadores de usuario.

La presente descripción se centra en el proceso de enviar correos electrónicos y resolver el problema de proteger los correos electrónicos enviados a nuevos receptores para los que no está disponible ningún certificado. Sin embargo, el sistema de cifrado de la invención también puede utilizarse para procesar correos electrónicos entrantes. El sistema de cifrado de la invención puede, por ejemplo, descifrar correos electrónicos entrantes, comprobar su firma, realizar comprobaciones de contenido y virus, volver a cifrar los mensajes con el certificado de receptor interno y enviar los correos electrónicos.

Para que los clientes de correo electrónico de usuario interno puedan cifrar los correos electrónicos antes de enviarlos a la pasarela segura, este dispositivo se basa en la generación y distribución de certificados proforma y, preferiblemente, en una funcionalidad de directorio proxy. Los certificados proforma son certificados *ad hoc* que sólo se utilizan entre uno o varios clientes de correo electrónico de emisor y la pasarela segura en el sistema de cifrado. El cliente de correo electrónico piensa que está utilizando el certificado del receptor final, pero realmente está utilizando un certificado proforma. La clave privada correspondiente a este certificado proforma la conoce la pasarela de correo electrónico seguro, que de esta forma puede descifrar los correos electrónicos salientes antes de enviarlos a través de Internet, y realizar la detección de contenidos ofensivos o virus. Los certificados proforma pueden tener una validez ilimitada; opcionalmente, se genera un nuevo certificado proforma para cada mensaje, o cada día, etc. En este caso, el certificado proforma sería un tipo de "certificado de sesión". Entonces, la pasarela de correo electrónico seguro cifra el correo electrónico saliente con el certificado del receptor para asegurar el correo electrónico durante su viaje por Internet. De forma alternativa, el receptor también puede acceder a los correos electrónicos en un navegador Web en una conexión protegida, por ejemplo, una conexión SSL, en cuyo caso no se realiza una cifrado basado en certificados.

La funcionalidad de directorio proxy permite la automatización del proceso de envío y configuración de certificados. La tarea de esta funcionalidad es interceptar las peticiones de los certificados del receptor de correo electrónico que normalmente enviarían los usuarios internos al directorio de su empresa, de modo que los certificados no tengan que solicitarse manualmente. La solicitud de certificados puede enviarse al directorio de la empresa, a otro directorio, o puede procesarse utilizando datos almacenados en el propio sistema de cifrado. Si no se encuentra ningún certificado de receptor, o bien el sistema de cifrado genera uno nuevo en el momento, o se solicita uno al receptor. Si se genera un nuevo certificado, preferiblemente es uno proforma, pero también puede ser uno normal que se transmitirá al receptor junto con su clave privada.

El proceso de envío de correo electrónico y configuración de certificados que tiene lugar cuando un usuario interno envía un correo electrónico a un nuevo receptor externo se ilustra en la figura 2.

Durante el primer paso del proceso ilustrado en la figura 2, el usuario 1 interno desea enviar un correo electrónico seguro al receptor 6. El receptor 6 es preferiblemente externo (es decir, está conectado a la red privada del emisor 1 sólo a través de Internet 3). El usuario 1 interno no tiene el certificado del receptor 6 que se necesita para cifrar su correo electrónico saliente y, por tanto, solicita este certificado al sistema 16 de cifrado (flecha A). Esta petición puede enviarse de forma manual o automática con cualquier software convencional como una petición normal a un directorio de empresa, por ejemplo, como solicitud LDAP o SQL, y es interceptada por el sistema de cifrado. En otra realización, se solicita el certificado del receptor por una página web generada por un servidor web en el sistema de cifrado. En otra realización, el cliente de correo electrónico del emisor envía automáticamente una solicitud del certificado del receptor cuando el emisor envía un correo electrónico que debería cifrarse a un nuevo receptor, es decir, un receptor para el que no hay certificado disponible. En una realización preferida, una funcionalidad de directorio proxy permite que la solicitud de usuario se genere automáticamente cuando el usuario está enviando un correo electrónico a un contacto de la agenda de direcciones.

El evento importante de la figura 2 sucede cuando el sistema 16 de cifrado recibe la solicitud de certificado (flecha A) y consulta un directorio (no mostrado) para el certificado correspondiente al receptor deseado. En este caso, no está disponible ningún certificado válido, y el sistema de cifrado crea así un nuevo certificado proforma que se transmite al emisor interno (flecha B). Otra opción es solicitar al receptor final que proporcione un certificado, en lugar de generar un nuevo certificado proforma; dado que no es probable que el receptor envíe su clave privada junto con el certificado, el inconveniente es que no será posible descifrar y volver a cifrar el correo electrónico en el sistema para comprobar su contenido. Otra opción es generar un certificado normal y transmitirlo al receptor final.

Durante el tercer paso de la figura 2, el emisor 1 cifra su correo electrónico con el certificado que acaba de recibir del sistema de cifrado, y lo envía por el sistema de cifrado al receptor (flecha C).

Durante el siguiente paso de la figura 2, el correo electrónico saliente es interceptado por el relé de correo electrónico o el servidor de correo electrónico en el sistema 16 de cifrado, y se envía al sistema de cifrado, que lo descifra utilizando la clave privada correspondiente al certificado proforma. De esta manera pueden realizarse comprobaciones de contenido ofensivo y virus, controles de correo basura y estadísticas en el correo electrónico descifrado.

Tras estas comprobaciones, si también se requiere confidencialidad por Internet, el sistema 16 de cifrado vuelve a cifrar el correo electrónico de salida durante el último paso de la figura 2, utilizando el certificado real del receptor final, que se almacenó en un directorio o que se recuperó previamente durante el paso 2. El correo electrónico cifrado se envía entonces por Internet 3 o por la red 13 de área local al receptor 6, tal como se muestra mediante la flecha D.

En una primera realización ilustrada por la figura 3, el sistema 16 de cifrado comprende una pasarela 160 de cifrado que opera como un relé de correo electrónico que realiza cifrado del lado del servidor y permite cifrado en ambos lados, antes y después del sistema de cifrado. En esta configuración, el sistema de cifrado se utiliza para asegurar el tráfico de correo electrónico de una empresa que ya tiene un servidor 166 de correo electrónico y un directorio 164 que los clientes de 11 de correo electrónico interno consultan para obtener direcciones de correo electrónico. El sistema de cifrado puede comprender un relé SMTP convencional (Simple Email Transfer Protocol) o cualquier otro tipo de relé de correo electrónico adecuado que pueda integrarse con facilidad en una infraestructura existente. El único cambio en los componentes de la infraestructura existente es que el servidor 166 de correo electrónico existente debe enviar correos electrónicos salientes a la pasarela 160 de cifrado, en lugar de enviarlos directamente a Internet 3.

La pasarela 160 de cifrado de la invención puede utilizar diferentes tecnologías, incluyendo, aunque no de forma restrictiva, S/MIME, PGP o, para la parte externa, SSL, para cifrar, firmar y transmitir correos electrónicos de forma segura; la invención no está limitada a un tipo especial de procedimiento de cifrado. Sin embargo, una tecnología preferida para la parte interna del cifrado (entre el usuario interno y la pasarela 16) es S/MIME dado que está admitida por la mayoría de clientes 11 de correo electrónico estándar. Otra posibilidad sería utilizar PGP, pero la mayoría de clientes de correo electrónico requeriría una instalación de plug-ins para ello. Además de ser capaz de realizar el cifrado y descifrado utilizando la tecnología elegida, la pasarela 160 de cifrado también debe ser capaz de generar los pares de claves adecuados, ya sea por sí misma o utilizando una infraestructura de clave pública (PKI) conectada. S/MIME es una buena elección desde ese punto de vista dado que puede utilizar certificados X.509 conocidos como hacen la mayoría de PKI. La pasarela de cifrado puede utilizar una tecnología de cifrado diferente para asegurar la trayectoria de Internet y para la trayectoria a través de la red privada. En una realización preferida, se utiliza S/MIME

para la parte interna y una amplia variedad de tecnologías de cifrado para la parte externa para adaptarse a tantos receptores como sea posible.

En otra realización ilustrada en la figura 5, la pasarela de correo electrónico de cifrado también es un servidor de correo electrónico autónomo. Esto significa que no necesita un servidor de correo electrónico al que transmitir los correos electrónicos entrantes y del que obtener los correos electrónicos salientes. Esta configuración puede utilizarse para asegurar el tráfico de correo electrónico desde una empresa que no tiene ningún servidor de correo electrónico o que desea tener la oportunidad de sustituir su servidor de correo electrónico.

En las dos realizaciones de las figuras 3 y 5, un directorio proxy 162 conectado a o integrado en la pasarela 160 de cifrado espera consultas de direcciones de correo electrónico y/o certificados procedentes de los clientes 11 de correo electrónico de usuarios internos (flecha c1). Si es una petición sencilla de una dirección de correo electrónico, se transmite al directorio 164 de usuarios de la empresa (flecha c2). La respuesta se transmite entonces al cliente 11 de correo electrónico del usuario (flecha c3). Si también se solicita un certificado, surgen dos casos: en el primero, los certificados se almacenan en el directorio de la empresa o en una PKI, de modo que la pasarela busca el certificado adecuado. En el segundo caso, la propia pasarela almacena los certificados, por lo que busca en su almacén de certificados. Si no se encuentra ningún certificado, se genera uno.

Una vez que la pasarela 160 de cifrado tiene todos los elementos requeridos (dirección de correo electrónico, certificado, etc.), los empaqueta en una respuesta cuyo formato depende del protocolo de acceso de directorio que está utilizándose y lo envía nuevamente al cliente de correo electrónico del emisor (flecha c4). El cliente de correo electrónico del usuario no tiene idea de que la respuesta que ha recibido no procede de un servidor de directorio normal, sino que se construyó mediante una funcionalidad de directorio proxy de pasarela segura.

Una tecnología de directorio preferida es LDAP (Lightweight Directory Access Protocol, protocolo ligero de acceso a directorios), dado que muchos clientes de correo electrónico incluyen una funcionalidad para recuperar información de usuario de directorios LDAP. La mayoría de directorios de empresas se basan en este protocolo, de modo que normalmente se utilizaría entre el cliente de correo electrónico y la pasarela, así como entre la pasarela y el directorio de empresa. No es necesario que los dos lados (clientes de correo electrónico y directorio) utilicen el mismo protocolo; en una realización, la pasarela 160, 161, 162 de cifrado es capaz de recibir peticiones en un primer protocolo, convertirlas a un segundo protocolo, procesar la respuesta del segundo protocolo y construir una respuesta adecuada conforme con el primer protocolo.

En entornos existentes en los que la información de usuario no se almacena en un directorio 164, el sistema 16 de cifrado puede ofrecer funcionalidad de directorio en un modo autónomo a través de una interfaz de directorio. Ésta acepta consultas de directorio (por ejemplo, consultas LDAP) y genera una respuesta obteniendo los datos correspondientes de su propio almacén de datos, que normalmente es una base de datos relacional en la pasarela 160 de cifrado.

Así, los clientes 11 de correo electrónico internos normalmente ya no conectan directamente con el directorio 164 de la empresa. En lugar de esto, todas sus consultas van primero a través del directorio proxy 162 del sistema, y es el directorio proxy el que consulta el directorio 164 de la empresa. Dependiendo del resultado de esta consulta, se genera en el momento un certificado proforma.

Los siguientes pasos se realizan en el sistema de la figura 3 cuando un usuario 1 interno envía un correo electrónico con su cliente 11 de correo electrónico a un receptor 6 externo que aún no ha recibido ningún correo electrónico seguro de la red 13 privada a la que está conectado el emisor:

c1. El cliente 11 de correo electrónico realiza una consulta generada de forma manual o automática para solicitar la dirección de correo electrónico y el certificado del receptor 6 deseado, o simplemente su certificado. La dirección y/o el certificado también puede solicitarse a través de una página web.

c2. El directorio proxy 162 en el sistema 16 de cifrado envía la solicitud de directorio al directorio 164.

c3. La respuesta del directorio 164 no contiene un certificado para el receptor dado que es la primera vez que un usuario interno escribe de forma segura al receptor 6.

c4. La pasarela 160 de cifrado genera un certificado proforma para el receptor 6 (o recupera un certificado generado anteriormente), almacena la clave privada correspondiente a este certificado y empaqueta el certificado en la respuesta transmitida al cliente 11 de correo electrónico del emisor. De forma opcional, esta respuesta puede estar firmada electrónicamente con la clave privada de la pasarela 160.

c5. El emisor 1 recibe el certificado proforma, que puede instalarse automáticamente en su cliente 11 de correo electrónico, y envía el correo electrónico a través del servidor 166 de correo electrónico de la empresa. El correo electrónico se cifra con el certificado proforma y se firma opcionalmente con la clave privada del emisor 11.

c6. El servidor 166 de correo electrónico envía el correo electrónico al sistema 160 de cifrado utilizándolo como relé de correo electrónico.

c7. La pasarela 160 de cifrado descifra el correo electrónico utilizando la clave privada almacenada previamente correspondiente al certificado proforma. También puede comprobar la firma del emisor, si está disponible, utilizando el certificado del emisor, que puede recuperarse del directorio 164. Opcionalmente pueden utilizarse dispositivos externos en esta fase para comprobar el contenido del correo electrónico (virus, contenido ofensivo, etc.).

c8. La pasarela 160 de cifrado cifra el correo electrónico con el certificado verdadero del receptor 6 y transmite el correo electrónico de forma segura al receptor. La pasarela 160 de cifrado también puede firmar el correo electrónico con la clave privada del emisor 1 o de la empresa. De forma alternativa, el contenido del correo electrónico se muestra al receptor en una página web segura, a la que puede incluirse un enlace en un correo electrónico enviado al receptor.

La figura 4 describe otra realización del sistema de cifrado de la invención. En esta configuración, el sistema de cifrado se utiliza para asegurar el tráfico de correos electrónicos para una empresa que tiene un servidor de correo electrónico, pero no tiene directorio. En este caso, toda la funcionalidad de directorio necesaria la ofrece el propio sistema.

Los siguientes pasos se realizan cuando un usuario interno envía un correo electrónico con su cliente 11 de correo electrónico a un receptor 6 externo que aún no ha recibido ningún correo electrónico seguro de la red 13 privada a la que está conectado el emisor:

d1. El cliente 11 de correo electrónico realiza una consulta para solicitar una dirección de correo electrónico y un certificado del receptor 6 deseado, o simplemente su certificado.

d2. La pasarela 160 de cifrado devuelve un certificado a través de su interfaz 163 de directorio. En este caso, se genera o recupera un certificado proforma para el receptor 6 dado que es la primera vez que alguien le escribe de forma segura en la red 13 privada. La pasarela 160 almacena la clave privada correspondiente a este certificado. De forma opcional, la respuesta puede firmarse electrónicamente con la clave privada de la pasarela 160.

d3. El emisor 1 recibe el certificado proforma, que puede instalarse automáticamente en su cliente 11 de correo electrónico, y envía el correo electrónico a través del servidor 166 de correo electrónico de la empresa. El correo electrónico se cifra con el certificado proforma y se firma opcionalmente con la clave privada del emisor 11. El sistema descifra el correo electrónico.

De forma opcional, pueden utilizarse dispositivos externos en esta etapa para comprobar el contenido del correo electrónico (virus, contenido ofensivo, etc.).

d4. El servidor 166 de correo electrónico envía el correo electrónico al sistema de cifrado utilizándolo como un relé de correo electrónico.

d5. La pasarela 160 de cifrado descifra el correo electrónico utilizando la clave privada almacenada previamente correspondiente al certificado proforma. También puede comprobar la firma del emisor, si está disponible, utilizando el certificado del emisor, que puede recuperarse del directorio 164. De forma opcional, pueden utilizarse dispositivos externos en esta etapa para comprobar el contenido del correo electrónico (virus, contenido ofensivo, etc.).

d6. La pasarela 160 de cifrado cifra el correo electrónico con el certificado verdadero del receptor 6 y transmite el correo electrónico de forma segura al receptor. La pasarela 160 de cifrado también puede firmar el correo electrónico con la clave privada del emisor 1 o de la empresa. De forma alternativa, el contenido del correo electrónico se muestra al receptor en una página web segura, a la que puede incluirse un enlace en un correo electrónico enviado al receptor.

La figura 5 describe otra realización del sistema de cifrado de la invención. En esta configuración, el sistema de cifrado comprende un servidor 161 de correo electrónico y se utiliza para asegurar el tráfico de correos electrónicos desde una empresa que tiene un directorio 164 que los clientes 11 de correo electrónico internos consultan para obtener direcciones de correo electrónico y certificados.

Los clientes 11 de correo electrónico internos ya no conectan directamente con el directorio 164 de la empresa. En lugar de esto, todas sus consultas pasan primero a través del directorio proxy 162 del sistema de cifrado, y es el directorio proxy el que consulta el directorio 164 de la empresa. Dependiendo del resultado de su consulta, se genera en el momento un certificado proforma.

Los siguientes pasos tienen lugar cuando un usuario interno envía un correo electrónico con su cliente 11 de correo electrónico a un receptor 6 externo que aún no ha recibido ningún correo electrónico seguro de la red 13 privada a la que está conectado el emisor:

e1. El cliente 11 de correo electrónico realiza una consulta para solicitar una dirección de correo electrónico y un certificado del receptor 6 deseado, o simplemente su certificado.

e2. El directorio proxy 162 en el sistema 16 de cifrado envía la petición al directorio 164 de la empresa.

e3. La respuesta del directorio 164 no contiene un certificado para el receptor dado que es la primera vez que alguien le escribe de forma segura.

e4. La pasarela 160 de cifrado genera un certificado proforma para el receptor 6 (o recupera un certificado de este tipo), almacena la clave privada correspondiente a este certificado y empaqueta el certificado en la respuesta transmitida al cliente 11 de correo electrónico del emisor.

De forma opcional, esta respuesta puede ir firmada electrónicamente con la clave privada de la pasarela 160.

e5. El emisor 1 recibe el certificado proforma, que puede instalarse de forma automática en su cliente 11 de correo electrónico, y envía el correo electrónico al servidor 161 de correo electrónico. El correo electrónico se cifra con el certificado proforma y se firma opcionalmente con la clave privada del emisor 11.

e6. La pasarela de cifrado en el servidor 161 de correo electrónico descifra el correo electrónico. También puede comprobar la firma del emisor, si está disponible, utilizando el certificado del emisor, que puede recuperarse del directorio 164. De forma opcional, pueden utilizarse dispositivos externos en esta etapa para comprobar el contenido del correo electrónico (virus, contenidos ofensivos, etc.).

e7. El servidor 161 de correo electrónico cifra el correo electrónico con el certificado verdadero del receptor 6, y transmite el correo electrónico de forma segura al receptor. La pasarela 160 de cifrado también puede firmar el correo electrónico con la clave privada del emisor 1 o de la empresa. De forma alternativa, el contenido del correo electrónico se muestra al receptor en una página web segura, a la que puede incluirse un enlace en un correo electrónico al receptor.

La figura 6 describe otra realización del sistema de cifrado de la invención. En esta configuración, el sistema 16 de cifrado se utiliza como servidor de correo electrónico y para asegurar el tráfico de correo electrónico de una empresa que no tiene directorio de usuarios.

Los siguientes pasos pueden tener lugar cuando un usuario interno envía un correo electrónico con su cliente 11 de correo electrónico a un receptor 6 externo que aún no ha recibido ningún correo electrónico seguro de la red 13 privada a la que está conectado el servidor:

f1. El cliente 11 de correo electrónico del emisor realiza una consulta para solicitar una dirección de correo electrónico y un certificado del receptor 6 deseado, o simplemente su certificado.

f2. El sistema 161 de cifrado devuelve un certificado a través de su interfaz 162 de directorio. En este caso, se genera o recupera un certificado proforma para el receptor 6 dado que es la primera vez que alguien le escribe de forma segura. El sistema 161 también almacena la clave privada correspondiente a este certificado. De forma opcional, la respuesta puede firmarse electrónicamente con la clave privada del sistema 161.

f3. El emisor 1 recibe el certificado proforma, que puede instalarse automáticamente en su cliente 11 de correo electrónico, y envía el correo electrónico al servidor 161 de correo electrónico. El correo electrónico se cifra con el certificado proforma y se firma opcionalmente con la clave privada del emisor 11.

f4. El sistema 161 de cifrado descifra el correo electrónico. También puede comprobar la firma del emisor, si está disponible, utilizando el certificado del emisor, que puede recuperarse del directorio 164. De forma opcional, pueden utilizarse dispositivos externos en esta etapa para comprobar el contenido del correo electrónico (virus, contenidos ofensivos, etc.).

f5. El servidor 161 de correo electrónico cifra el correo electrónico con el certificado verdadero del receptor 6, y transmite el correo electrónico de forma segura al receptor. La pasarela 160 de cifrado también puede firmar el correo electrónico con la clave privada del emisor 1 o de la empresa. De forma alternativa, el contenido del correo electrónico se muestra al receptor en una página web segura, a la que puede incluirse un enlace en un correo electrónico enviado al receptor.

La figura 7 describe otra realización del sistema de cifrado de la invención. En esta configuración, el sistema 16 de cifrado se instala en la red local de un proveedor 15 de servicios de Internet y se utiliza para asegurar los correos electrónicos transmitidos desde o hacia sus clientes 1. En otra realización similar, el sistema 16 de cifrado se instala en la red local de un proveedor externo de servicios de correo electrónico, que puede ser diferente del proveedor de servicios de Internet. En otra realización, sólo se externaliza la "pasarela de correo electrónico seguro" y no, toda la gestión de correos electrónicos (en este caso, en la figura 7, el servidor 166 de correo electrónico estaría en la misma red que los clientes 11 de correo electrónico).

En el ejemplo ilustrado en la figura 7, se configuran clientes 11 de correo electrónico para acceder a un directorio 164 en el proveedor 15 de servicios de correo electrónico. Si fuera necesario, se generan en el momento certificados proforma y se devuelven. Otra forma sería que los emisores 11 utilizaran una libreta de direcciones local (una para toda la empresa o una por persona) y solicitaran los nuevos certificados proforma del proveedor 15 a través de una página web o un correo electrónico especial. El certificado proforma se añadiría entonces a la libreta de direcciones local.

Los siguientes pasos se realizan cuando un usuario envía un correo electrónico a un receptor externo:

g1. El cliente 11 de correo electrónico realiza una consulta al directorio para solicitar una dirección de correo electrónico y un certificado del receptor 6 deseado, o simplemente su certificado.

g2. El directorio proxy 162 en el sistema 16 de cifrado transmite la solicitud al directorio 164 de proveedores de servicios de correo electrónico.

g3. En ese caso, la respuesta del directorio 164 no contiene un certificado para el receptor 6 dado que es la primera vez que un cliente del proveedor 15 escribe de forma segura al receptor 6 con el sistema 16.

g4. El sistema 16 de cifrado genera un certificado proforma para el receptor 6 (o recupera un certificado de este tipo), almacena la clave privada correspondiente a este certificado, y empaqueta el certificado en la respuesta transmitida al cliente 11 de correo electrónico del emisor. De forma opcional, esta respuesta puede firmarse electrónicamente con una clave privada del proveedor 15.

g5. El emisor 1 recibe el certificado proforma, que se instala preferiblemente de forma automática en su cliente 11 de correo electrónico, y envía el correo electrónico al servidor 166 de correo electrónico del proveedor de servicios de correo electrónico. El correo electrónico se cifra con el certificado proforma y opcionalmente se firma con la clave privada del emisor 11.

g6. El servidor 166 de correo electrónico transmite el correo electrónico a la pasarela 160 de cifrado, utilizándola como relé de correo electrónico.

g7. La pasarela 160 de cifrado descifra el correo electrónico. De forma opcional, pueden utilizarse dispositivos externos en esta etapa para comprobar el contenido del correo electrónico (virus, contenido ofensivo, etc.). También puede comprobar la firma del emisor, si está disponible, utilizando el certificado del emisor, que puede recuperarse del directorio 164.

g8. El sistema transmite el correo electrónico al receptor 6. El correo electrónico puede cifrarse con el certificado verdadero del receptor 6. La pasarela 160 de cifrado también puede firmar el correo electrónico con la clave privada del emisor 1 o de la empresa. De forma alternativa, el contenido del correo electrónico se muestra al receptor en una página web segura, a la cual puede incluirse un enlace en un correo electrónico enviado al receptor.

La figura 8 describe otra realización del sistema de cifrado de la invención. En esta configuración, el sistema 16 de cifrado se utiliza para asegurar el tráfico de correo electrónico desde una red privada que incluye un servidor 166 de correo electrónico, pero, en lugar de generar un certificado proforma para cada nuevo receptor 6, se utiliza el mismo certificado de sistema para cifrar varios, o incluso todos los correos electrónicos salientes. El sistema también puede tener más de un certificado, por ejemplo, es posible utilizar uno por departamento de la empresa.

Los clientes 11 de correo electrónico interno ya no tienen que conectarse por fuerza directamente al directorio de la empresa. En lugar de esto, todas sus consultas pasan primero a través del directorio proxy 162 del sistema. El proxy 162 devuelve la dirección de correo electrónico del sistema con la dirección y/o el nombre del receptor en la parte de nombre (por ejemplo, reto.schneider@empresa.com<gateway@empresa.com>) y el certificado del sistema de cifrado. Cuando el cliente 11 de correo electrónico del emisor envía entonces el correo electrónico cifrado a esta dirección, la pasarela 160 de cifrado lo descifra y consulta en el directorio 164 de la empresa la dirección de correo electrónico del receptor 6 y transmite el correo electrónico.

Los siguientes pasos pueden tener lugar cuando un usuario 11 interno envía un correo electrónico a un receptor 6 externo.

h1. El cliente 11 de correo electrónico realiza una consulta a la interfaz de directorio del sistema para solicitar un correo electrónico y un certificado para un receptor 6.

h2. El sistema 16 de cifrado devuelve su propio certificado y dirección de correo electrónico. La dirección de correo electrónico contiene la dirección original en el campo de nombre.

h3. El emisor 11 recibe el certificado, que puede instalarse automáticamente en su cliente 11 de correo electrónico, y envía el correo electrónico por el servidor 166 de correo electrónico de la empresa a la dirección del sistema de cifrado, cifrado con el certificado del sistema. El correo electrónico puede firmarse con la clave privada del emisor 11.

h4. El servidor 166 de correo electrónico envía el correo electrónico a la pasarela 160 de cifrado, utilizándola como relé de correo electrónico.

h5. La pasarela 160 de cifrado recibe el correo electrónico. Si en el campo de nombre del correo electrónico sólo aparece el nombre, y no la dirección de correo electrónico, la pasarela 160 solicita la dirección del receptor del directorio 164 de la empresa utilizando el nombre de receptor indicado para la consulta.

h6. El directorio 164 devuelve la dirección de correo electrónico solicitada.

h7. La pasarela 160 de cifrado descifra el correo electrónico con su clave privada. Opcionalmente, pueden utilizarse dispositivos externos en esta fase para comprobar el contenido del correo electrónico (virus, contenido ofensivo, etc.). Puede comprobarse la firma del emisor, si está disponible. La pasarela de cifrado cambia la dirección del receptor de correo electrónico, insertando el nombre y la dirección del receptor final real.

h8. La pasarela 160 de cifrado transmite el correo electrónico de forma segura al receptor. El correo electrónico puede cifrarse con el certificado verdadero del receptor 6.

El sistema de la figura 8 también puede operar sin un directorio de empresa, almacenando las direcciones de correo electrónico de los receptores él mismo. También puede operar sin servidor de correo electrónico externo, actuando él mismo como servidor de correo electrónico.

Dependiendo de las realizaciones, el sistema 16 de cifrado de la invención puede comprender:

- Medios para interconectar al menos dos servidores de correo electrónico (el servidor 166 de correo electrónico de la empresa y el servidor 5 de correo electrónico del servidor fuera de la red 13 de la empresa) para transmitir correos electrónicos entre ellos, o un medio para interconectar un cliente 11 de correo electrónico y un servidor de correo electrónico.

- En una realización, el sistema 16 de cifrado trabaja como un servidor 161 de correo electrónico totalmente equipado, que proporciona a los usuarios 1 internos toda la funcionalidad de servidor de correo electrónico convencional, además de las características de seguridad.

- De forma alternativa, el sistema 16 de cifrado trabaja como un relé 160 de correo electrónico entre dos servidores 166, 5 de correo electrónico o entre un dispositivo de seguridad, por ejemplo, un escáner de virus, y un servidor de correo electrónico.

- En una realización, el sistema 16 de cifrado asegura los correos electrónicos entre un proveedor 15 de servicios de correo electrónico (por ejemplo, un ISP) y sus clientes 11 de correo electrónico de clientes.

- En una realización, el sistema 16 de cifrado proporciona una interfaz 163 de directorio, a través de la cual el software de correo electrónico del emisor consulta el certificado del receptor.

- En una realización, se proporciona una página web al emisor 1 para solicitar manualmente un certificado (proforma o normal) para un receptor 6 particular que va a añadirse a su libreta personal de direcciones.

- En una realización, se proporciona una página web al emisor 1 para solicitar un certificado (proforma o normal) para un receptor particular que va a añadirse al directorio de usuarios de la empresa.

- En una realización, se proporciona una página web al administrador de red para generar certificados proforma para un receptor 6 particular o grupo de receptores y añadirlos al directorio de la empresa o al almacén de datos del sistema.

- En una realización, cuando un usuario 1 interno solicita un certificado, se genera o recupera de un almacén un nuevo certificado proforma que sólo se utilizará entre el cliente 11 de correo electrónico del emisor y el sistema 16 de cifrado.

- En una realización, cuando un usuario 1 interno solicita un certificado, el sistema 16 de cifrado solicita al receptor 6 final un certificado.

- En una realización, cuando un usuario 1 interno solicita un certificado, el sistema 16 de cifrado genera un certificado normal y lo envía al receptor 6 junto con la correspondiente clave privada (posiblemente utilizando el formato PKCS#12).

- En una realización, se proporciona la funcionalidad PKI para:

  - generar certificados para usuarios internos;

  - generar certificados para receptores para el cifrado entre los clientes de correo electrónico de emisores internos y el sistema 16 de cifrado;

  - generar certificados para receptores para el cifrado entre el sistema 16 de cifrado y clientes de correo electrónico de los receptores;

  - almacenar, revocar y renovar los certificados generados.

- En una realización, se generan pares de claves previamente para acelerar el proceso de generación de certificados.

- En una realización, se proporciona conectividad PKI para permitir a las PKI externas generar/renovar/revocar los certificados requeridos.

- En una realización, el sistema 16 de cifrado almacena claves.

- En una realización, las claves se almacenan en un directorio 164 externo.

- En una realización, se almacenan claves mediante una PKI externa.

- Para algunos intercambios de correo electrónico, se utiliza la misma clave para usuarios internos entre el cliente de correo electrónico de los usuarios internos y el sistema 16 de cifrado y entre el sistema 16 de cifrado y el receptor 6 externo.

- En una realización preferida, se utiliza una primera clave para usuarios internos entre el cliente 11 de correo electrónico de los usuarios internos y el sistema 16 de cifrado, y se utiliza una segunda clave entre el sistema 16 de cifrado y el receptor 6 externo.

- Dependiendo de las reglas de seguridad, los correos electrónicos pueden firmarse y cifrarse, sólo cifrarse o sólo firmarse.

- En una realización, el sistema 16 de cifrado comprende una interfaz 162 de directorio a un almacén de datos interno, de modo que no se requiere directorio externo.

- En una realización, el sistema comprende una interfaz 162 de directorio que va a conectarse a un directorio 164 externo y a los clientes de correo electrónico internos.

- El sistema 16 de cifrado comprende medios para descifrar correos electrónicos salientes cifrados por los emisores 11 internos con el certificado proforma de su(s) receptor(es), y transmitirlos de forma segura al (los) receptor(es). Esto puede significar volverlos a cifrar con claves públicas reales del (los) receptor(es) o permitir al (los) receptor(es) acceder al correo electrónico a través de otra forma segura.

- En una realización, el sistema 16 de cifrado envía los correos electrónicos a uno o varios dispositivos de seguridad tras el descifrado (escaneadores de virus, analizadores de seguridad de contenido, etc.). Una vez que se han comprobado, los correos electrónicos se devuelven al mismo dispositivo o a otro. Después, se transmiten de forma segura a su receptor 6.

- El sistema 16 de cifrado comprende preferiblemente medios para descifrar correos electrónicos entrantes que se cifraron utilizando otra tecnología distinta a la admitida por los clientes 11 de correo electrónico del usuario interno y volverlos a cifrar utilizando la tecnología adecuada.

- En una realización, el sistema 16 de cifrado descifra todos los correos electrónicos entrantes y los envía a uno o varios dispositivos de seguridad (escaneadores de virus, analizadores de seguridad de contenido, etc.). Una vez que se han comprobado, los correos electrónicos regresan al mismo dispositivo o a otro. Después, se transmiten de forma segura el usuario 11 interno.

- En una realización, el sistema 16 de cifrado no descifra y vuelve a cifrar todos los correos electrónicos entrantes dado que no tiene acceso a las claves privadas de algunos usuarios internos privilegiados.

- En una realización, un motor de reglas define qué correos electrónicos deben cifrarse en la red 13 privada (puede resultar útil cifrar todos los correos electrónicos por motivos de rendimiento).

- En una realización, el sistema 16 de cifrado no tiene certificados para todos los usuarios internos. En ese caso, los correos electrónicos enviados a usuarios 11 internos que no tienen certificado pueden enviarse en blanco, o puede generarse un nuevo certificado en el momento y proporcionarse al usuario interno, dependiendo de las reglas de seguridad.

- En una realización, las reglas de seguridad definen qué correos electrónicos deben cifrarse en la red 3 externa.

- En una realización, el sistema comprueba periódicamente el directorio de la empresa en busca de nuevos usuarios externos. Si se encuentran nuevos usuarios, se generan certificados proforma para ellos, de modo que, cuando un usuario interno desea enviar un correo electrónico a uno de ellos, el directorio de la empresa puede proporcionarle directamente un certificado, sin necesidad de pasar a través de una funcionalidad de directorio proxy del sistema. De forma opcional, pueden definirse reglas para la creación de certificados, de modo que no todas las nuevas entradas en el directorio reciban un certificado.

- En una realización, pueden definirse reglas para la creación de certificados, de modo que se crean diferentes tipos de certificados, por ejemplo, certificados basados en diferentes técnicas de cifrado o certificados con diferentes longitudes de clave, para diferentes tipos de receptores o diferentes tipos de mensajes.

Otra posibilidad que no se describe en un esquema es utilizar el sistema 16 de cifrado sin funcionalidad de directorio, los usuarios que realizan el envío solicitan los certificados proforma a través de una interfaz web o un correo electrónico especial y después los almacenan opcionalmente en una libreta de direcciones local. Como se ha mencionado anteriormente, se prefiere el uso de certificados proforma, pero no es obligatorio para el sistema de cifrado, que en algunos casos podría solicitar al receptor final un certificado o generar un certificado normal que se enviará al receptor junto con la clave privada.

La invención también se refiere a un producto informático que incluye un programa para implementar el procedimiento de cifrado cuando el producto se carga en el sistema 16 del servidor y el programa se ejecuta por el sistema del servidor.

REIVINDICACIONES

1. Procedimiento de cifrado para correos electrónicos enviados desde un emisor (1) en su red privada a un receptor (6), que comprende los siguientes pasos:

el emisor (1) solicita de dicho sistema (16) de cifrado en la red privada un certificado correspondiente a dicho receptor (6),

el sistema (16) de cifrado devuelve al emisor (1) un primer certificado proforma correspondiente a dicho receptor (6), generándose o recuperándose el certificado proforma por el sistema (16) de cifrado para el receptor (6), y utilizándose únicamente entre el emisor (1) y el sistema (16) de cifrado,

el emisor (1) envía con su cliente (11) de correo electrónico, un correo electrónico saliente a dicho receptor (6), cifrado con dicho certificado proforma,

dicho correo electrónico se envía a través de dicho sistema (16) de cifrado,

dicho sistema (16) de cifrado descifra el correo electrónico utilizando una clave privada correspondiente a dicho certificado,

dicho sistema de cifrado hace que el contenido de dicho correo electrónico esté disponible a dicho receptor (6).

2. El procedimiento según la reivindicación 1, en el que dicho primer certificado proforma se genera en dicho sistema (16) de cifrado.

3. El procedimiento según la reivindicación 1, en el que dicho primer certificado proforma se genera mediante un dispositivo, por ejemplo, una PKI, al que puede acceder dicho sistema (16) de cifrado.

4. El procedimiento según una de las reivindicaciones 1 a 3, en el que dicho sistema (16) de cifrado cifra dicho correo electrónico con dicho certificado de dicho receptor (6) antes de transmitirlo a dicho receptor (6).

5. El procedimiento según una de las reivindicaciones 1 a 4, en el que dicho emisor (1) solicita dicho certificado correspondiente a dicho receptor (6) realizando una petición de directorio.

6. El procedimiento según una de las reivindicaciones 1 a 5, en el que dicho emisor (1) solicita dicho certificado correspondiente a dicho receptor (6) mediante una página web.

7. El procedimiento según una de las reivindicaciones 1 a 6, en el que dicho emisor (1) solicita el certificado correspondiente a dicho receptor (6) utilizando una interfaz de directorio.

8. El procedimiento según una de las reivindicaciones 1 a 7, en el que dicho certificado proforma se devuelve por dicho sistema de cifrado y se almacena en la libreta de direcciones personal del emisor.

9. El procedimiento según una de las reivindicaciones 1 a 7, en el que dicho certificado proforma se devuelve a dicho sistema de cifrado y se almacena en un directorio (164) compartido por varios usuarios que pertenecen a la misma comunidad.

10. El procedimiento según una de las reivindicaciones 1 a 9, en el que dicho certificado proforma correspondiente a dicho receptor (6) únicamente se utiliza para asegurar correos electrónicos entre dicho cliente (11) de correo electrónico del emisor y dicho sistema (16) de cifrado.

11. El procedimiento según una de las reivindicaciones 1 a 10, en el que un certificado proforma común correspondiente a dicho receptor (6) se utiliza entre una pluralidad de clientes (11) de correo electrónico y dicho sistema (16) de cifrado.

12. El procedimiento según una de las reivindicaciones 2 a 11, en el que dicho sistema (16) de cifrado solicita un certificado de dicho receptor (6) cuando dicho certificado de dicho receptor (6) no está disponible, utilizándose dicho certificado de dicho receptor para asegurar correos electrónicos entre dicho sistema (16) de cifrado y dicho receptor (6).

13. El procedimiento según la reivindicación 12, en el que dicho sistema (16) de cifrado envía un primer correo electrónico para solicitar un certificado de dicho receptor (6) cuando dicho certificado de dicho receptor (6) no está disponible.

14. El procedimiento según una de las reivindicaciones 12 a 13, en el que dicho sistema (16) de cifrado genera un certificado para dicho receptor (6) cuando dicho receptor (6) desea un certificado de este tipo para comunicarse con dicho emisor (1).

15. El procedimiento según una de las reivindicaciones 1 a 14, en el que dicho sistema (16) de cifrado hace que el contenido de dicho correo electrónico esté disponible al receptor transmitiendo dicho correo electrónico a dicho receptor (6).

16. El procedimiento según una de las reivindicaciones 1 a 14, en el que dicho sistema (16) de cifrado hace que el contenido de dicho correo electrónico esté disponible para dicho dicho receptor (6) a través de una página web segura.

17. El procedimiento según una de las reivindicaciones 1 a 16, en el que se generan pares de claves de antemano y se almacenan en un almacenamiento disponible para dicho sistema (16) de cifrado.

18. El procedimiento según una de las reivindicaciones 1 a 17, en el que los correos electrónicos se firman con la clave privada de dicho emisor (1).

19. El procedimiento según una de las reivindicaciones 1 a 18, en el que dicho sistema (16) de cifrado descifra los correos electrónicos salientes y los transmite a uno de los siguientes dispositivos antes de hacer que su contenido esté disponible a dicho receptor (6):

escáner de virus,

analizador de seguridad de contenido,

filtro de correo basura,

filtro de contenido.

20. El procedimiento según una de las reivindicaciones 1 a 19, que comprende adicionalmente un paso de recibir un correo electrónico entrante en dicho sistema (16) de cifrado, descifrarlo en dicho sistema (16) de cifrado y cifrarlo con otro certificado antes de transmitirlo a un usuario interno.

21. El procedimiento según una de las reivindicaciones 1 a 20, que comprende adicionalmente un paso, durante el cual dicho sistema (16) de cifrado comprueba un conjunto predefinido de reglas para verificar qué correos electrónicos deben descifrarse, cifrarse nuevamente y/o firmarse.

22. El procedimiento según una de las reivindicaciones 1 a 21, en el que dicho sistema (16) de cifrado comprende un relé (160) de correo electrónico.

23. El procedimiento según la reivindicación 22, en el que el relé de correo electrónico es un relé SMTP.

24. El procedimiento según una de las reivindicaciones 1 a 21, en el que dicho sistema (16) de cifrado es ejecutado por un servidor (161) de correo electrónico al que se envían directamente dichos correos electrónicos salientes.

25. El procedimiento según una de las reivindicaciones 1 a 24, en el que dicho sistema (16) de cifrado puede operarse por el administrador de red de una red (13) de área local y devuelve certificados a una pluralidad de emisores (1) en dicha red de área local o en una pluralidad de redes de área local conectadas entre sí y/o redes privadas virtuales.

26. El procedimiento según la reivindicación 25, en el que dicho sistema (16) de cifrado comprende una pasarela (160, 161) de cifrado en la red (13) de área local.

27. El procedimiento según una de las reivindicaciones 25 a 26, en el que dicho sistema (16) de cifrado comprende un servidor (166) de correo electrónico y/o un relé (160) de correo electrónico en dicha red de área local.

28. El procedimiento según una de las reivindicaciones 25 a 27, en el que dicho sistema (16) de cifrado comprende un directorio (164) en la red (13) de área local.

29. El procedimiento según una de las reivindicaciones 1 a 28, en el que dicho sistema (16) de cifrado es operado por un proveedor (15) de servicios de Internet o un proveedor de servicios de correo electrónico y devuelve certificados para una pluralidad de usuarios o clientes de dicho proveedor (15) de servicios.

30. Sistema (16) de cifrado para cifrar correos electrónicos salientes enviados por un emisor (1) a un receptor (6) externo, que comprende:

medios para proporcionar a dicho emisor (1) un primer certificado proforma correspondiente a dicho receptor (6), generándose o recuperándose dicho certificado proforma por dicho sistema (16) de cifrado para el receptor (6) y utilizándose únicamente entre dicho emisor (1) y dicho sistema (16) de cifrado;

medios para descifrar correos electrónicos cifrados enviados desde dicho emisor (1) a dicho receptor (6) con una clave privada correspondiente al certificado,

medios para cifrar los correos electrónicos con un certificado de dicho receptor (6),

medios para hacer que el contenido de dicho correo electrónico esté disponible a dicho receptor (6).

31. El sistema de cifrado según la reivindicación 30, que incluye un relé de correo electrónico.

32. El sistema de cifrado según la reivindicación 30, que incluye un servidor de correo electrónico.

33. El sistema de cifrado según una de las reivindicaciones 30 a 32, que incluye un directorio (164) de direcciones de receptor (6).

34. El sistema de cifrado según la reivindicación 33, en el que el directorio (164) es un directorio LDAP.

35. El sistema de cifrado según una de las reivindicaciones 33 a 34, incluyendo el directorio (164) los certificados de al menos una pluralidad de receptores (6), incluyendo dicho sistema de cifrado medios de cifrado para cifrar dichos correos electrónicos con certificados, y medios de transmisión para transmitir los correos electrónicos cifrados a dicho receptor (6).

36. El sistema de cifrado según una de las reivindicaciones 30 a 35, dispuesto para realizar los pasos de una de las reivindicaciones 1 a 29.

37. Producto informático que incluye un programa para realizar el procedimiento según una de las reivindicaciones 1 a 29 cuando dicho producto se carga en un sistema (16) de servidor y dicho programa es ejecutado por dicho sistema (16) de servidor.

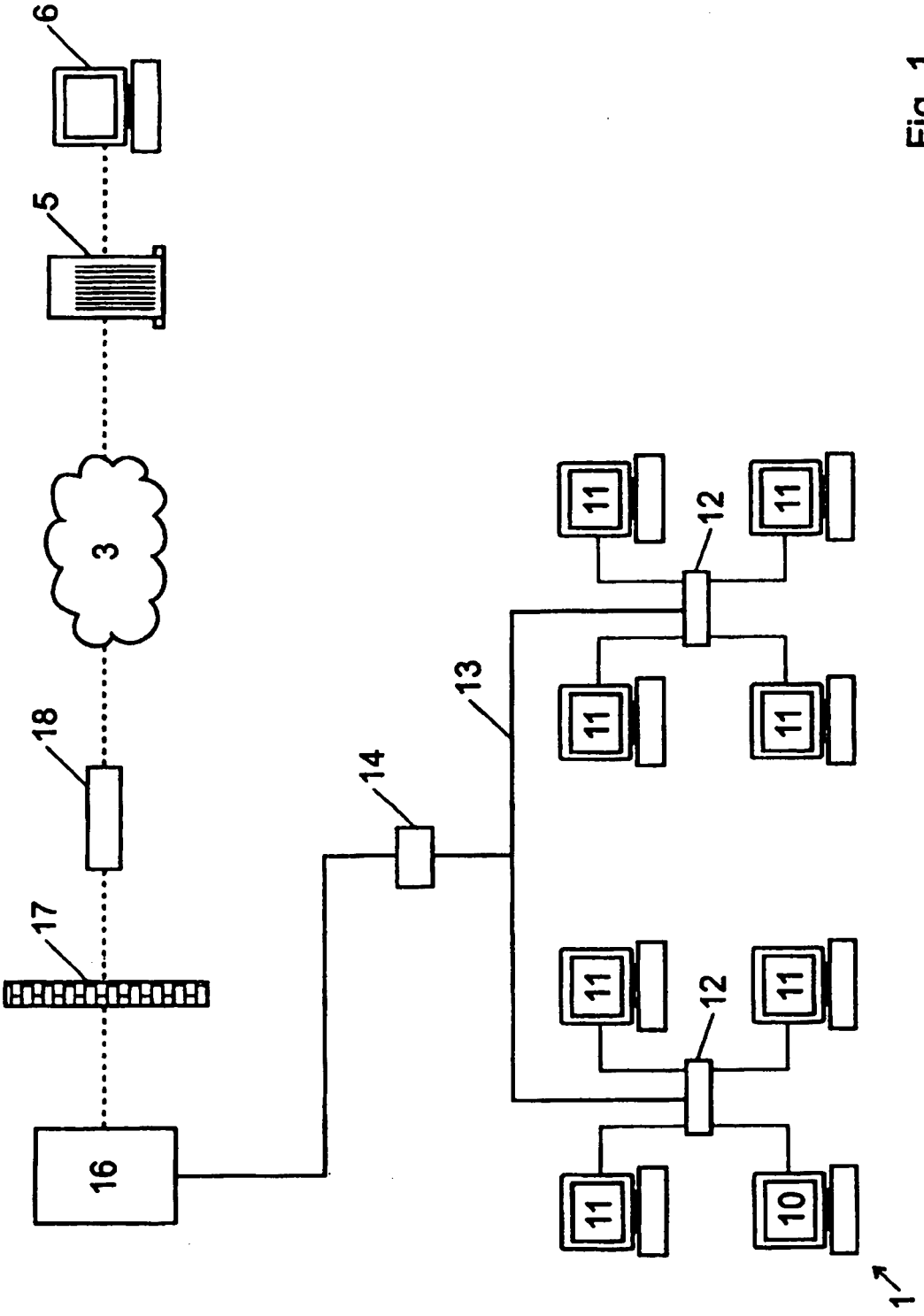

Fig. 1

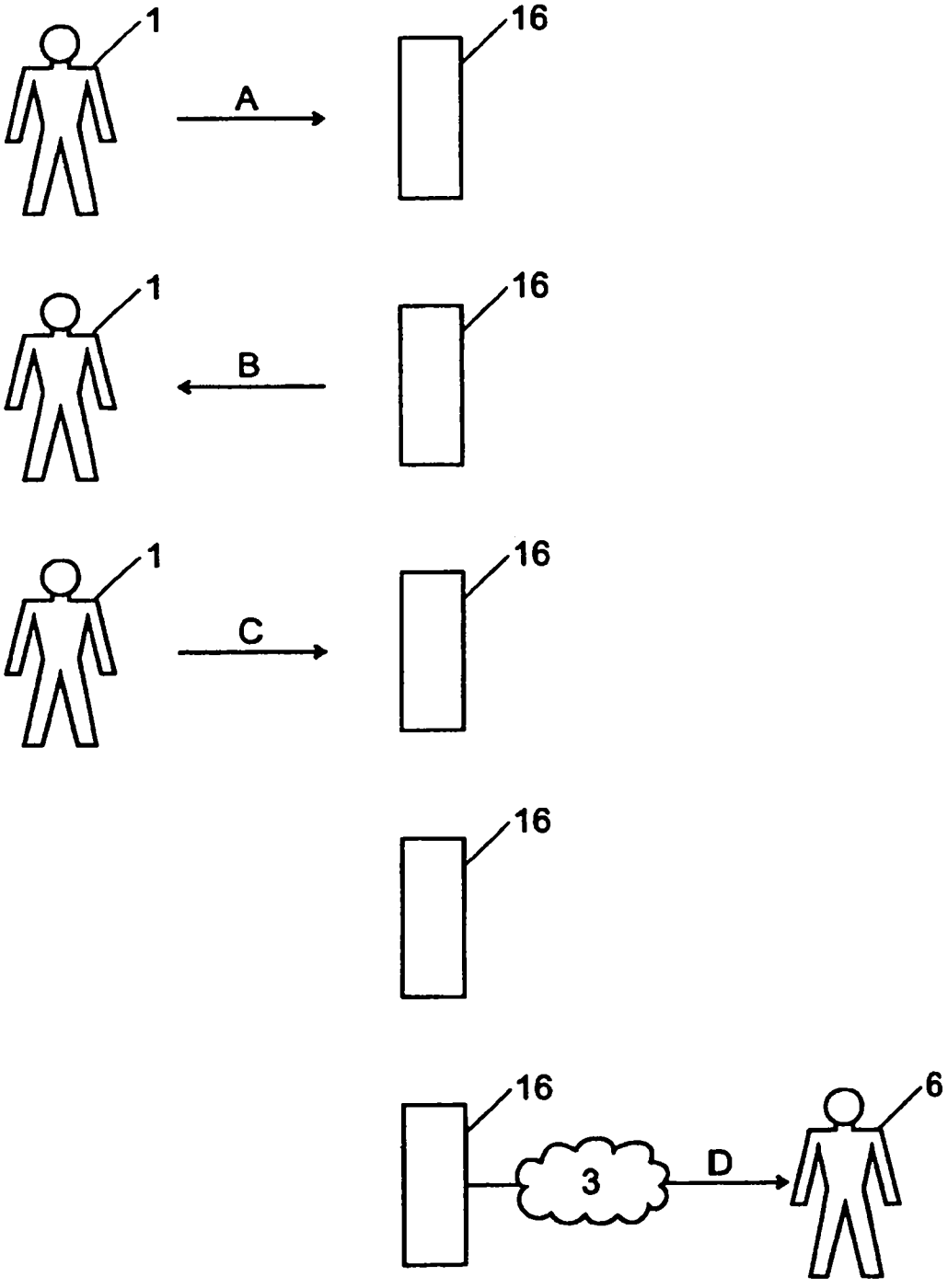

Fig. 2

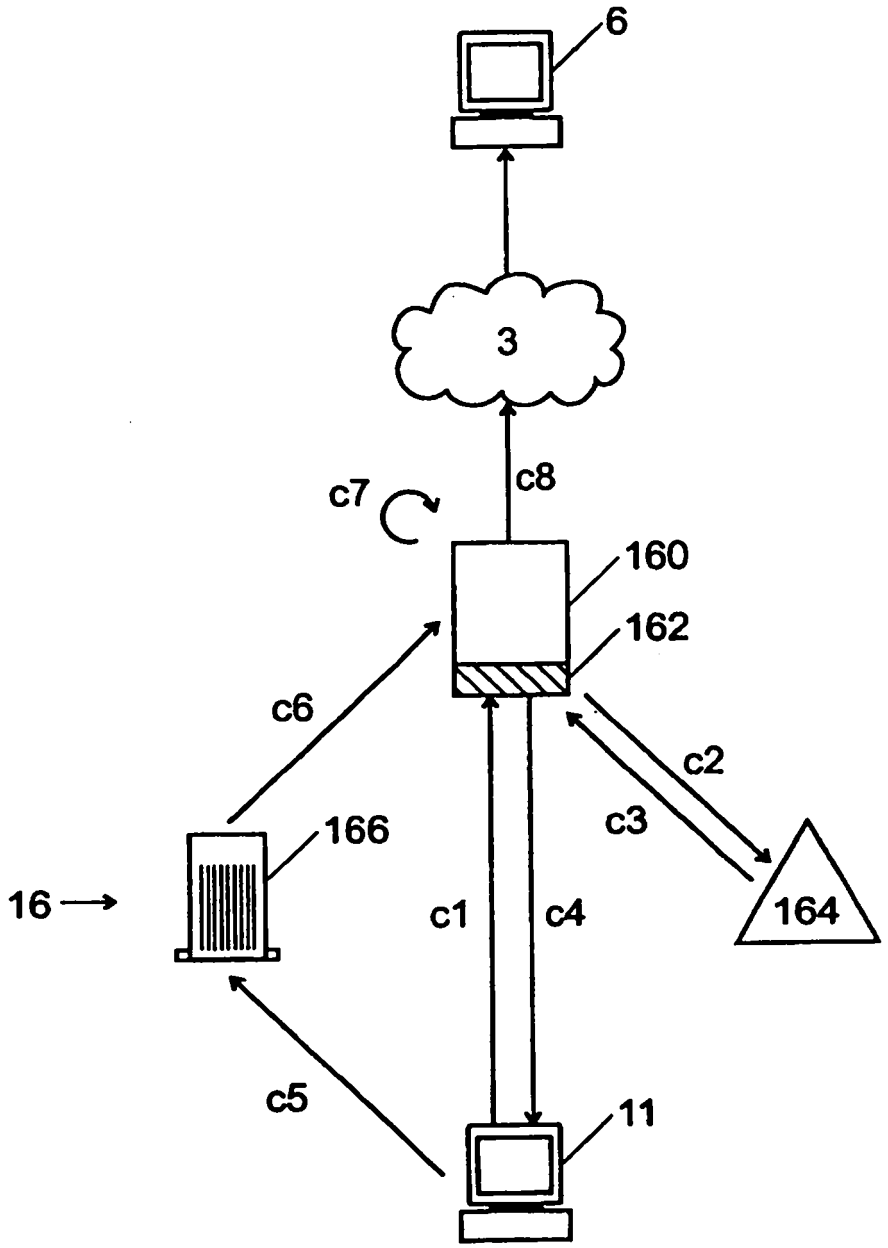

Fig. 3

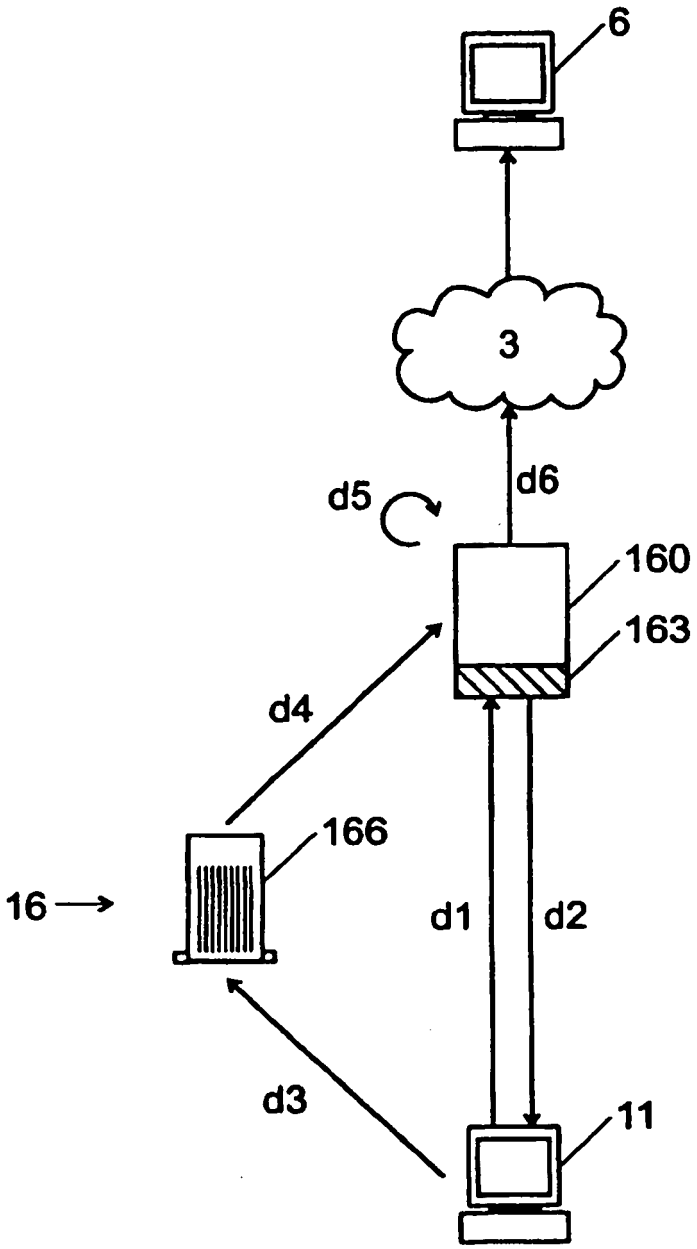

Fig. 4

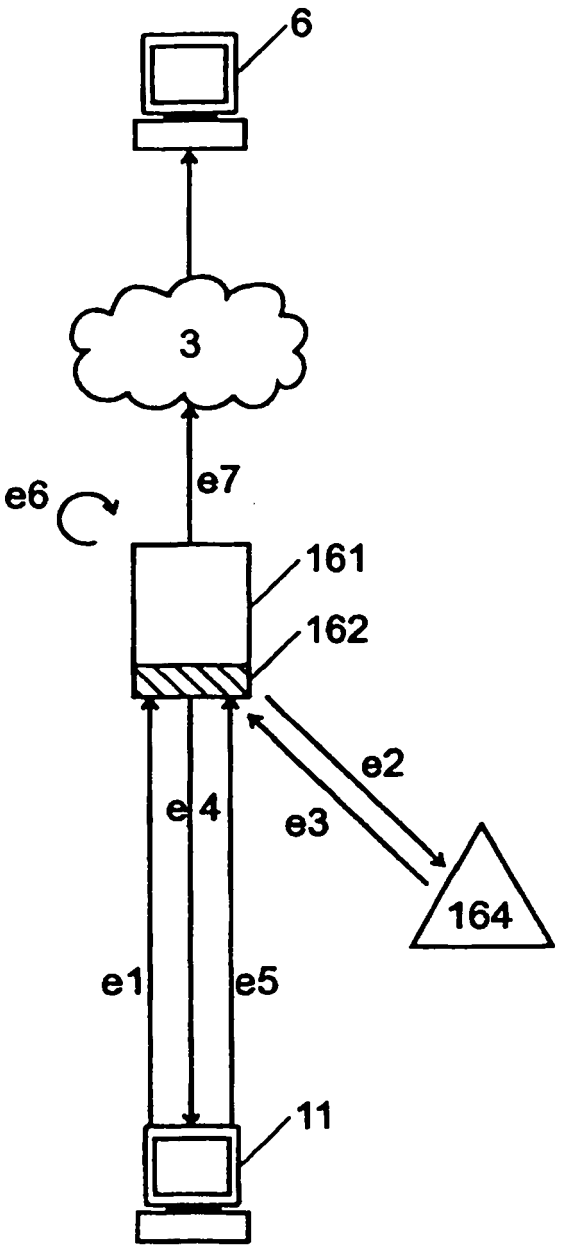

Fig. 5

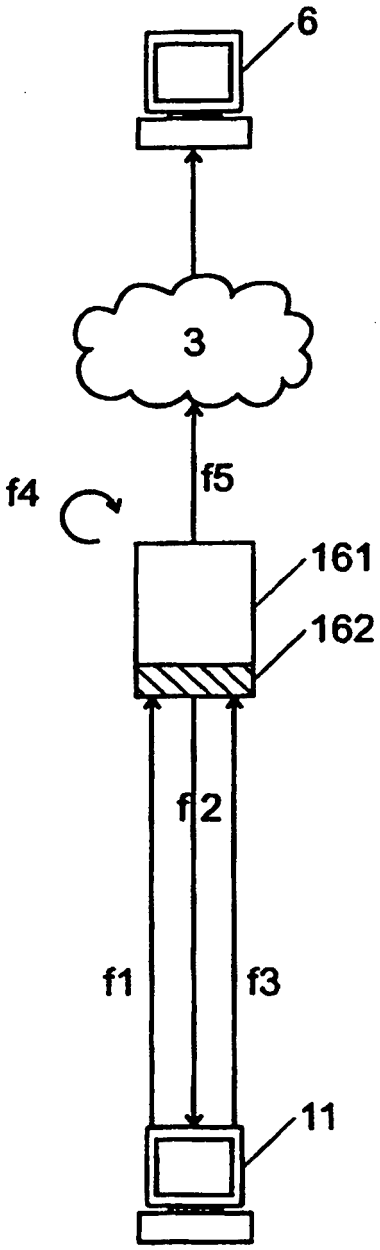

Fig. 6

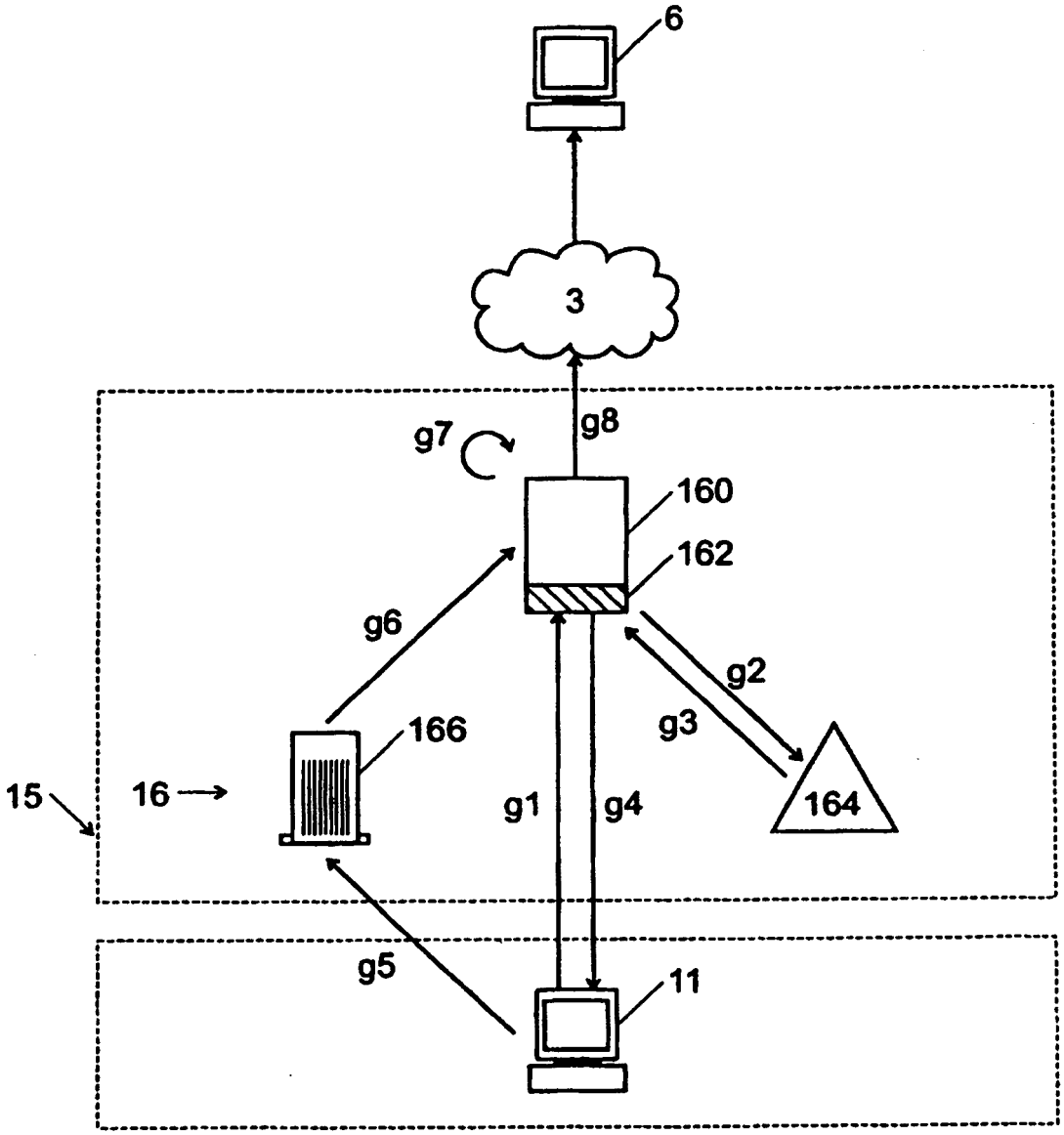

Fig. 7

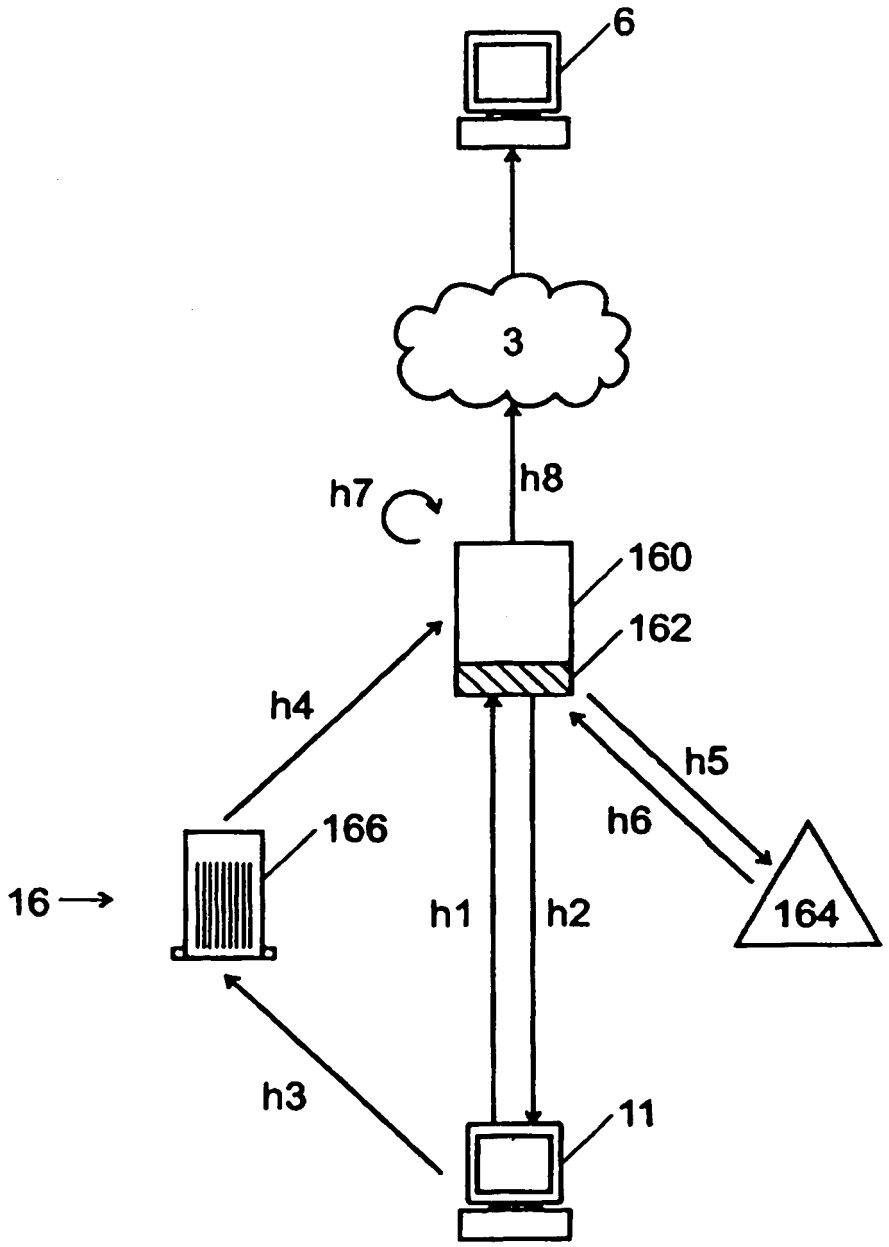

Fig. 8