(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 316 008**

(51) Int. Cl.:
G06Q 10/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **06116961 .1**
(96) Fecha de presentación : **11.07.2006**
(97) Número de publicación de la solicitud: **1879135**
(97) Fecha de publicación de la solicitud: **16.01.2008**

(54) Título: **Sistema y método para la modificación dinámica de las propiedades permisibles de mensajes electrónicos.**

(45) Fecha de publicación de la mención BOPI:
01.04.2009

(45) Fecha de la publicación del folleto de la patente:
01.04.2009

(73) Titular/es: **Research In Motion Limited**
295 Phillip Street
Waterloo, Ontario N2L 3W8, CA

(72) Inventor/es: **Brown, Michael K.;**
Brown, Michael S. y
Kirkup, Michael G.

(74) Agente: **Elzaburu Márquez, Alberto**

DESCRIPCIÓN

Sistema y método para la modificación dinámica de las propiedades permisibles de mensajes electrónicos.

Antecedentes

1. **Campo técnico**

La presente exposición se refiere generalmente a la aplicación de diversas propiedades, tales como, por ejemplo, propiedades de seguridad, a mensajes electrónicos. En particular, la exposición está dirigida a un sistema y a un método para modificar dinámicamente propiedades permisibles de mensajes electrónicos basándose en los contenidos del mensaje que se está componiendo.

2. **Técnica relacionada**

Es bien conocida la práctica de intercambiar mensajes y datos electrónicos seguros, tales como mensajes de correo electrónico. La mensajería electrónica segura requiere, típicamente, que el usuario implemente o aplique codificación de seguridad diversa u otras propiedades de seguridad al mensaje, basándose en los criterios o pautas de seguridad en las que se está haciendo funcionar el sistema. Se han desarrollado diversos métodos para garantizar que un usuario implementa adecuadamente el criterio de seguridad del sistema a la hora de componer mensajes electrónicos.

El documento WO 03/001326 A se refiere a un sistema en el que un cortafuegos para correo electrónico aplica ciertos criterios a mensajes de correo electrónico. El documento US 2003/0222923 se refiere a una interfaz de usuario con elementos de menú cuyas ubicaciones o lugares dependen de que su estado sea habilitado o inhabilitado.

La Solicitud de Patente Europea Nº EP 1365340 describe un método para la modificación dinámica de propiedades de mensaje electrónico permisibles, el cual se implementa como un módulo insertable o susceptible de ser acoplado y perteneciente a una aplicación de cliente para correo electrónico. El módulo susceptible de ser acoplado analiza el contenido de un mensaje antes de que el mensaje sea transmitido y, de acuerdo con unos criterios predefinidos, adopta automáticamente una acción con respecto al mensaje electrónico o sugiere al usuario la acción apropiada que llevar a cabo.

Por ejemplo, el usuario puede seleccionar un cierto tipo de servicio de mensaje, la codificación de seguridad y las propiedades de seguridad que se han de aplicar al mensaje. Sin embargo, con la introducción de la recuperación de antecedentes de criterios y claves de seguridad basándose en criterios concomitantes con el sistema, podrían no estar permitidos el tipo de servicio de mensaje, la codificación de seguridad o las propiedades de seguridad seleccionadas por el usuario. Por ejemplo, el criterio de seguridad del sistema puede requerir que todos los mensajes protegidos estén firmados en PGP y cifrados. Sin embargo, cuando un usuario elige componer y enviar un mensaje protegido, puede darse al usuario la opción de seleccionar la firma en S/MIME y el cifrado con el fin de proteger el mensaje, además de la opción de utilizar la firma en PGP y el cifrado. Debido a que se le han dado al usuario múltiples opciones, el usuario puede seleccionar la firma en S/MIME y el cifrado para el mensaje protegido. En este caso proporcionado a modo de ejemplo, debido a que la codificación de seguridad seleccionada por el usuario no está permitida por el criterio de seguridad del sistema, el usuario no tendrá la posibilidad de enviar el mensaje. Típicamente, el usuario no sabrá que ha violado un criterio de seguridad hasta que trate de enviar el mensaje. El usuario debe determinar entonces qué propiedades de seguridad son aceptables a la vista del criterio de IT, y aplicar entonces propiedades apropiadas al mensaje protegido. Este tipo de disposición puede ser muy frustrante y llevar mucho tiempo, y es innecesariamente compleja para los usuarios que simplemente desean enviar un mensaje protegido. Se necesita, así, un sistema y un método para paliar semejantes confusión y frustración del usuario, a fin de mejorar la práctica del usuario y garantizar que un usuario implementa el criterio de seguridad en lugar de enviar simplemente mensajes inocuos o libres de sospecha o eludir de otro modo el criterio de seguridad del sistema.

La presente invención se expone en las reivindicaciones independientes. Algunas características opcionales se exponen en las reivindicaciones dependientes de éstas.

En un aspecto, se dan un sistema y un método mejorados para actualizar dinámica y automáticamente los campos apropiados de la pantalla de aplicación del mensaje, a fin de mostrar cuáles de los tipos de servicios de mensaje, codificaciones de seguridad o propiedades de seguridad apropiados son aceptables o permisibles para el mensaje que se está componiendo. Esta actualización se producirá de forma automática basándose en el contenido de los campos que se modifican durante la composición del mensaje, tales como, por ejemplo, las modificaciones en la clasificación del mensaje, los destinatarios, las palabras clave o similares. Así pues, las propiedades aplicadas a un mensaje dado se ven reflejadas en una lista de opciones dinámicas que se proporciona al usuario basándose en el contenido de los diversos campos del mensaje electrónico y en el criterio de IT que está vigente en el sistema. Si bien este sistema resulta adecuado para cualquier tipo de sistema de mensajería electrónica, tiene una aplicabilidad particular en sistemas que utilizan dispositivos de comunicación inalámbrica móviles con capacidad de mensajería electrónica.

De acuerdo con una realización proporcionada a modo de ejemplo, las opciones de seguridad disponibles para un usuario se actualizan automáticamente basándose en las introducciones realizadas por el usuario en diversos campos del mensaje. Las opciones de seguridad actualizadas pueden ser presentadas visualmente al usuario en una lista de op-

ciones actualizada. Por ejemplo, el mensaje electrónico puede incluir campos relativos a la clasificación del mensaje, a las opciones de codificación disponibles para el mensaje, a los destinatarios del mensaje (incluyendo el(los) destinatario(s) principal(es) y los adjuntados con copia (c. c.) a ellos), al tema del mensaje, al texto del mensaje, o similares. De acuerdo con la selección de clasificación hecha por el usuario, por ejemplo, las opciones de codificación disponibles son actualizadas automáticamente con el fin de reflejar las opciones que se encuentran disponibles para el usuario y son permitidas por el criterio de seguridad del sistema. El usuario puede ser instado entonces a realizar una selección a partir de la lista actualizada si la opción previamente seleccionada ya no es válida o aplicable. De la misma manera, si ciertos destinatarios del mensaje están asociados con diversos requisitos relacionados con la seguridad, los ajustes de codificación de seguridad disponibles para el usuario o requeridos por el sistema se actualizarán automáticamente. El sistema puede también comprobar los contenidos de la línea del asunto y/o el texto objeto del mensaje en sí, en relación con las palabras clave que pudieran requerir la aplicación de ciertas propiedades de seguridad, basándose en los criterios de seguridad del sistema. Si se produce una actualización de las opciones de seguridad disponibles para el mensaje, el usuario puede ser instado a seleccionar las opciones de seguridad de entre la lista de opciones actualizada dinámicamente, antes de enviar el mensaje. La lista actualizada de opciones típicamente incluye los requisitos de codificación mínimos, y puede hacerse referencia a ella como una lista recortada o truncada.

De acuerdo con otro ejemplo, si los contenidos del mensaje dan pie a una actualización de las opciones de seguridad disponibles para enviar el mensaje, pueden implementarse automáticamente por parte del sistema los ajustes de seguridad actualizados, cuando el usuario ejecuta o lleva a cabo la orden. Por ejemplo, si el destinatario de un mensaje es un agente corporativo importante, el criterio de seguridad puede requerir que todos los mensajes enviados a este agente deban ser, como mínimo, firmados electrónicamente. En consecuencia, incluso un mensaje de texto simple y no clasificado puede requerir una firma en virtud de los destinatarios a los que se ha de enviar el mensaje. En este ejemplo, el usuario puede ser instado a cambiar la codificación del mensaje a un nivel adecuado antes de su envío. Por otra parte, el usuario puede ser informado de que la codificación del mensaje ha cambiado automáticamente a un nivel de seguridad más alto que refleja un nivel mínimo de seguridad en correspondencia con el criterio de seguridad asociado con el destinatario. Puede hacerse referencia a este tipo de actualización automática de ajustes de seguridad como "redondeo al alza" de los ajustes de seguridad. El usuario puede, bien aceptar los ajustes de seguridad automáticamente actualizados mediante, por ejemplo, la ejecución de la orden de envío, o bien puede, opcionalmente, escoger de entre la lista actualizada de opciones de seguridad y seleccionar un nivel incluso superior de codificación de seguridad para el mensaje, que esté permitido por el criterio de seguridad según se refleja en las propiedades de seguridad actualizadas o las opciones de codificación puestas a disposición del usuario.

En aún otra realización proporcionada a modo de ejemplo, los ajustes de seguridad pueden ser establecidos basándose en el tipo de servicio de mensaje que se está utilizando. Por ejemplo, en un entorno de servicios de mensaje múltiples en el que se estén utilizando múltiples cuentas de correo electrónico (por ejemplo, cuentas doméstica y de oficina), pueden aplicarse diferentes niveles de clasificación y criterios de seguridad. Así, las opciones de seguridad que se proporcionan al usuario pueden estar basadas en la selección sobre cuál de los múltiples tipos de servicios de mensaje se esté utilizando.

De acuerdo con otra realización proporcionada a modo de ejemplo, las opciones de seguridad pueden estar basadas en reglas asociadas con los servicios proporcionados por terceros diferentes del administrador del sistema. Por ejemplo, puede emplearse el servidor de un tercero para establecer criterios o pautas de seguridad de los correos electrónicos para los usuarios del sistema. Del resto de criterios de seguridad del sistema puede encargarse el administrador del sistema. Las limitaciones que proporciona el servidor del tercero pueden ser reflejadas dinámicamente ante un usuario de un modo según se ha establecido anteriormente, de tal manera que el usuario puede evitar realizar selecciones que sean rechazadas más tarde por razón de que las selecciones violan los criterios basados en el servidor. Los criterios de seguridad que se establecen por terceros pueden también implementar la actualización dinámica de opciones de seguridad proporcionada al usuario de la manera que aquí se expone, con respecto a las realizaciones proporcionadas a modo de ejemplo.

Breve descripción de los dibujos

Estos y otros propósitos y ventajas de las realizaciones que se proporcionan a modo de ejemplo de la presente invención, se comprenderán y apreciarán mejor en combinación con la siguiente descripción detallada de realizaciones proporcionadas a modo de ejemplo, tomadas conjuntamente con los dibujos que se acompañan, en los cuales:

la Figura 1 es una amplia vista esquemática de sistema global, que ilustra un sistema de comunicación de correo electrónico inalámbrico proporcionado a modo de ejemplo, que incorpora un dispositivo de comunicaciones inalámbricas de acuerdo con una realización ejemplar de la presente invención;

la Figura 2 es un diagrama de bloques de un sistema de comunicación adicional proporcionado a modo de ejemplo, que incluye múltiples redes y múltiples dispositivos de comunicación móviles;

la Figura 3 es un diagrama esquemático y abreviado de componentes físicos o hardware incluido dentro de un dispositivo de comunicaciones inalámbricas móvil;

la Figura 4 es un diagrama funcional y esquemático, abreviado, del hardware/software que se utiliza en un dispositivo de comunicación inalámbrica móvil proporcionado a modo de ejemplo en la realización ejemplar de la Figura 1;

la Figura 5 es un diagrama de flujo abreviado y ejemplar de un sistema para actualizar dinámica y automáticamente las opciones de seguridad disponibles para un mensaje basándose en el contenido del mensaje;

la Figura 6 es un diagrama de flujo abreviado y ejemplar de un sistema para redondear al alza de forma dinámica y automática los ajustes de seguridad basándose en el contenido de un mensaje y, opcionalmente, proporcionar opciones de nivel de seguridad superior a un usuario;

las Figuras 7A-7G son tomas o imágenes ejemplares en pantalla que ilustran la presentación visual a modo de ejemplo de las opciones de seguridad para un usuario de acuerdo con varias realizaciones;

la Figura 8 es una toma o imagen ejemplar en pantalla que ilustra una presentación visual a modo de ejemplo de las opciones de seguridad de acuerdo con el ejemplo que se ilustra en la Figura 6; y

la Figura 9 es un diagrama de flujo abreviado y ejemplar de un sistema para actualizar dinámica y automáticamente las opciones de seguridad disponibles para un mensaje, basándose en cuál de los servicios de mensaje múltiples se está utilizando para enviar un mensaje.

Descripción detallada de realizaciones proporcionadas a modo de ejemplo

La Figura 1 es una vista global de un sistema de comunicación proporcionado a modo de ejemplo, en el cual puede utilizarse un dispositivo de comunicación inalámbrica. Un experto de la técnica apreciará que puede haber muchas topologías diferentes, pero el sistema que se muestra en la Figura 1 ayuda a ilustrar el funcionamiento de los sistemas y métodos de tratamiento de mensajes codificados que se describen en la presente Solicitud. Puede haber también muchos remitentes y destinatarios de mensajes. El sencillo sistema que se muestra en la Figura 1 tiene únicamente propósitos ilustrativos y muestra quizá el entorno más extendido de correo electrónico por Internet, en el que no se utiliza generalmente la seguridad.

La Figura 1 muestra un emisor o remitente 10 de correo electrónico, la Internet 20, un sistema 40 servidor de mensajes, una pasarela inalámbrica 85, una infraestructura inalámbrica 90, una red inalámbrica 105 y un dispositivo de comunicación móvil 100.

Un sistema 10 remitente de correo electrónico puede, por ejemplo, ser conectado a un ISP (Proveedor de Servicios de Internet -“Internet Service Provider”) en el que un usuario del sistema 10 tiene una cuenta, ubicado dentro de una empresa, posiblemente conectado a una red de área local (LAN -“local area network”) y conectado a la Internet 20, ó bien conectado a la Internet 20 a través de un ASP (proveedor de servicios de aplicación -“application service provider”) grande, tal como el America Online (AOL). Los expertos de la técnica apreciarán que los sistemas mostrados en la Figura 1 pueden, en lugar de ello, ser conectados a una red de área extensa (WAN -“wide area network”) distinta de la Internet, si bien las transferencias de correo electrónico se llevan acabo por lo común a través de disposiciones conectadas a la Internet, como se muestra en la Figura 1.

El servidor 40 de mensajes puede ser implementado, por ejemplo, en una computadora de red situada dentro del cortafuegos de una empresa, en una computadora ubicada dentro de un sistema de ISP o de ASP, o similar, y actúa como interfaz principal para el intercambio de correos electrónicos a través de la Internet 20. Aunque otros sistemas de mensajería podrían no requerir un sistema 40 servidor de mensajes, un dispositivo móvil 100 configurado para recibir y, posiblemente, enviar correo electrónico estará normalmente asociado con una cuenta en un servidor de mensajes. Quizá los dos servidores de mensajes más comunes sean el Microsoft Exchange™ y el Lotus Domino™. Estos productos se utilizan a menudo en combinación con *routers* o dispositivos de encaminamiento de correo por Internet que encaminan y entregan el correo. Estos componentes intermedios no se muestran en la Figura 1, ya que no juegan directamente ningún papel en el tratamiento o procesamiento seguro de mensajes anteriormente descrito. Los servidores de mensajes tales como el servidor 40 se extienden típicamente más allá del solo envío y recepción de correos electrónicos; incluyen también máquinas de almacenamiento de base de datos dinámica que tienen formatos de base de datos predefinidos para datos como calendarios, listas de quehaceres, listas de tareas, correo electrónico y documentación.

La pasarela inalámbrica 85 y la infraestructura 90 proporcionan un enlace entre la Internet 20 y la red inalámbrica 105. La infraestructura inalámbrica 90 determina la red más probable para localizar a un usuario dado y realiza un seguimiento del usuario a medida que este se desplaza en movimiento itinerante entre países o redes. Se obtiene entonces un mensaje para el dispositivo móvil 100 mediante transmisión inalámbrica, típicamente, a una frecuencia de radio o radiofrecuencia (RF), desde una estación de base de la red inalámbrica 105 hasta el dispositivo móvil 100. La red concreta 105 puede ser prácticamente cualquier red inalámbrica a través de la cual puedan intercambiarse mensajes con un dispositivo de comunicación móvil.

Como se muestra en la Figura 1, un mensaje de correo electrónico 15 compuesto es enviado por el remitente 10 de correo electrónico, ubicado en alguna parte de la Internet 20. Este mensaje 15 se encuentra normalmente libre de toda sospecha y utiliza cabeceras de Protocolo de Transferencia de Correo Simple (SMTP -"Simple Mail Transfer Protocol") RFC822 y partes de cuerpo de Extensión de Correo por Internet de Propósito Múltiple (MIME -"Multipurpose Internet Mail Extension") para definir el formato del mensaje de correo. Estas técnicas son todas bien conocidas por parte de los expertos en la materia. El mensaje 15 llega al servidor 40 de mensajes y es normalmente almacenado en un dispositivo de almacenamiento de mensajes. La mayor parte de los sistemas de mensajería conocidos proporcionan soporte a un esquema de acceso a mensajes denominado "de extracción", en el cual el dispositivo móvil 100 debe solicitar que los mensajes almacenados sean remitidos por el servidor de mensajes al dispositivo móvil 100. Algunos sistemas proporcionan un encaminamiento automático de tales mensajes, que son encaminados utilizando una dirección de correo electrónico específica asociada con el dispositivo móvil 100. En una realización preferida que se describe con mayor detalle más adelante, los mensajes encaminados a una cuenta de servidor de mensajes asociada con un sistema anfitrión o principal, tal como una computadora doméstica o una computadora de oficina que pertenece al usuario de un dispositivo móvil 100, son redirigidos desde el servidor 40 de mensajes al dispositivo móvil 100 a medida que se reciben.

Con independencia del mecanismo específico que controla la remisión de mensajes al dispositivo móvil 100, el mensaje 15, ó, posiblemente, una versión traducida o reformada del mismo, se envía a la pasarela inalámbrica 85. La infraestructura inalámbrica 90 incluye una serie de conexiones a la red inalámbrica 105. Estas conexiones pueden ser conexiones de Red Digital de Servicios Integrados (ISDN -"Integrated Services Digital Network"), de Retardo de Trama o de T1, que utilizan el protocolo de TCP/IP [Protocolo de Control de Transmisión/Protocolo de Internet -"Transmission Control Protocol/Internet Protocol"] empleado en toda la Internet. Tal y como se utiliza aquí, se pretende que la expresión "red inalámbrica" incluya al menos uno de tres tipos diferentes de redes: (1) las que son redes inalámbricas centradas en datos, (2) las redes inalámbricas centradas en la voz y (3) las redes en modo doble que pueden prestar soporte a comunicaciones tanto de voz como de datos a través de las mismas estaciones físicas de base. Las redes en modo doble combinadas incluyen (1) redes de Acceso Múltiple por División en Código (CDMA -"Code Division Multiple Access"), (2) redes del Grupo Especial Móvil ("Groupe Special Mobile") o Sistema Global para Comunicaciones Móviles (GSM ["Global System for Mobile Communications"]) y las redes del Servicio General de Radio en Paquetes (GPRS -"General Packet Radio Service"), y (3) redes futuras de tercera generación (3G) como las velocidades de transmisión de datos mejoradas para la evolución global (EDGE -"Enhanced Data-rates for Global Evolution"), la Red Mejorada Digital integrada (iDEN -"integrated Digital Enhanced Network"), la Evolución de Datos Optimizada (EvDO -"Evolution Data Optimized"), el Acceso en Paquetes de Enlace Descendente de Alta Velocidad (HSDPA -"High-Speed Downlink Packet Access"), los Sistemas de Telecomunicaciones Móviles Universales (UMTS -"Universal Mobile Telecommunications Systems") o similares, si bien no se limita a éstas. Algunos ejemplos más antiguos de redes centradas en datos incluyen la Red de Radio Mobitex™ y la Red de Radio DataTAC™. Ejemplos de redes de datos centradas en la voz más antiguas incluyen las redes de Sistemas de Comunicación Personal (PCS -"Personal Communication Systems"), como el GSM, y los sistemas de TDMA [Acceso Múltiple por División en el Tiempo -"Time Division Multiple Access"].

La Figura 2 es un diagrama de bloques de un sistema de comunicación adicional a modo de ejemplo, que incluye múltiples redes y múltiples dispositivos de comunicación móvil. El sistema de la Figura 2 es sustancialmente similar al sistema de la Figura 1, pero incluye un sistema anfitrión o principal 300, un programa de re-direccionamiento 45, un acoplador o enganche 65 de dispositivo móvil, un dispositivo de encaminamiento inalámbrico 75 de red privada virtual (VPN -"virtual private network"), una red inalámbrica adicional 110 y múltiples dispositivos de comunicación móviles 100. Como se ha descrito anteriormente en combinación con la Figura 1, la Figura 2 representa una vista global de una topología de red de muestra. Si bien los sistemas y los métodos de tratamiento de mensajes codificados que se han descrito aquí pueden ser aplicados a redes que tienen muchas topologías diferentes, la red de la Figura 2 resulta útil para comprender un sistema de re-direccionamiento automático de correo electrónico que se ha mencionado brevemente en lo anterior.

El sistema anfitrión central 300 consistirá, típicamente, en la oficina de una empresa u otra LAN, si bien, en lugar de ello, puede ser la computadora de una oficina doméstica o algún otro sistema privado en el se estén intercambiando mensajes de correo. Dentro del sistema anfitrión 300 se encuentra el servidor 400 de mensajes, en funcionamiento en alguna computadora ubicada dentro del cortafuegos del sistema anfitrión, que actúa como interfaz principal para el sistema anfitrión con el fin de intercambiar correo electrónico con la Internet 20. En el sistema de la Figura 2, el programa de re-direccionamiento 45 permite el re-direccionamiento de elementos de datos desde el servidor 400 hasta un dispositivo de comunicación móvil 100. Si bien el programa de re-direccionamiento 45 se muestra de manera que reside en la misma máquina que el servidor 400 de mensaje en aras de la facilidad de presentación, no existe ningún requisito que obligue a que resida en el servidor de mensajes. El programa de re-direccionamiento 45 y el servidor 400 de mensajes están diseñados para cooperar e interactuar con el propósito de permitir que se fuerce el paso de la información a los dispositivos móviles 100. En esta instalación, el programa de re-direccionamiento 45 toma información corporativa, confidencial y no confidencial, para un usuario concreto y la redirige al exterior, a través del cortafuegos de la empresa, hacia los dispositivos móviles 100. Puede encontrarse una descripción más detallada del software de re-direccionamiento 45 en la Patente de los Estados Unidos asignada en común con el Nº 6.219.694 ("la Patente Nº 6.219.694"), titulada "Sistema y método para empujar o forzar el paso de información de un sistema anfitrión a un dispositivo móvil de comunicación de datos que tiene una dirección electrónica compartida" ("*System and Method for Pushing Information from a Host System to a Mobile Data Communication Device Having a Shared Electronic Address*"), y expedida al asignatario de la presente Solicitud el 17 de abril de 2001. Esta técnica de empuje

o paso forzado de puede servirse de una técnica de codificación, compresión y cifrado manejable e inalámbrica para suministrar toda la información a un dispositivo móvil, con lo que se extiende de manera efectiva el cortafuegos de seguridad hasta incluir cada dispositivo móvil 100 asociado al sistema anfitrión 300.

Como se muestra en la Figura 2, puede haber muchos caminos alternativos para hacer llegar información al dispositivo móvil 100. Uno de los métodos para cargar información en el dispositivo móvil 100 es a través de un acceso o puerta designada con la referencia 50, utilizando un enganche 65 de dispositivo. Este método tiende a ser útil para las actualizaciones de información a gran escala que se llevan a cabo con frecuencia a la hora de inicializar un dispositivo móvil 100 con el sistema anfitrión o principal 300 ó una computadora 35 dentro del sistema 300. El otro método principal para el intercambio de datos es por el aire, utilizando redes inalámbricas para suministrar la información. Como se muestra en la Figura 2, esto puede lograrse a través de un dispositivo de encaminamiento inalámbrico 75 de VPN o a través de una conexión tradicional 95 por Internet a una pasarela inalámbrica 85 y a una infraestructura inalámbrica 90, como se ha descrito anteriormente. El concepto de un dispositivo de encaminamiento inalámbrico 75 de VPN es nuevo en la industria inalámbrica e implica que es posible establecer una conexión de VPN directamente a través de una red inalámbrica específica 110, con un dispositivo móvil 100. La posibilidad de utilizar un dispositivo de encaminamiento inalámbrico 75 de VPN tan sólo ha llegado a estar disponible recientemente, y puede utilizarse cuando la nueva Versión 6 del Protocolo de Internet (IP -"Internet Protocol") (IPV6) llegue a las redes inalámbricas basadas en IP. Este nuevo protocolo proporcionará suficientes direcciones de IP como para dedicar una dirección de IP a cada dispositivo móvil 100 y, así, hacer posible forzar el paso de información a un dispositivo móvil 100 en cualquier momento. Una ventaja principal de utilizar este dispositivo de encaminamiento inalámbrico 75 de VPN es que podría tratarse de un componente de VPN listo para llevar, por lo que no requeriría el uso de una pasarela inalámbrica independiente 85 ni de una infraestructura inalámbrica 90. Una conexión de VPN será, preferiblemente, una conexión de Protocolo de Control de Transmisión (TCP)/IP o de Protocolo de Datagrama de Usuario (UDP -"User Datagram Protocol")/IP para suministrar mensajes directamente al dispositivo móvil. Si no se dispone de una VPN inalámbrica 75, entonces el mecanismo de conexión más común disponible es un enlace 95 con la Internet 20, que ya se ha descrito anteriormente.

En el sistema de re-direccionamiento automático de la Figura 2, un mensaje de correo electrónico 15 compuesto que sale del remitente 10 de correo electrónico, llega al servidor 400 de mensajes y es redirigido por el programa de re-direccionamiento 45 hacia el dispositivo móvil 100. A medida que este re-direccionamiento tiene lugar, el mensaje 15 es re-encapsulado, según se indica por la referencia numérica 80, y puede aplicarse entonces al mensaje original 15 un algoritmo de compresión y cifrado, posiblemente registrado en propiedad. De esta forma, los mensajes que se leen en el dispositivo móvil 100 no son menos seguros que si fuesen leídos en una estación de trabajo de sobremesa tal como la indicada por la referencia numérica 35, situada dentro del cortafuegos. Todos los mensajes intercambiados entre el programa de re-direccionamiento 45 y el dispositivo móvil 100 utilizan, preferiblemente, esta técnica de re-encapsulado de los mensajes. Otro objetivo de este encapsulado exterior es mantener la información de dirección del mensaje original, a excepción de las direcciones del remitente y del receptor. Esto permite que los mensajes de respuesta lleguen al destino apropiado, y también posibilita que el campo "de" refleje la dirección del equipo de sobremesa del usuario móvil. El uso de la dirección de correo electrónico del usuario obtenida del dispositivo móvil 100 permite que el mensaje recibido tenga aparezca como si se hubiese originado desde el sistema de sobremesa 35 del usuario en lugar de desde el dispositivo móvil 100.

Haciendo referencia de nuevo a la capacidad de conexión o conectividad de la puerta 50 y del dispositivo de enganche 65 al dispositivo móvil 100, este camino de conexión ofrece muchas ventajas por lo que respecta a permitir el intercambio de datos de una sola vez de elementos de gran tamaño. Para los expertos en la técnica de los asistentes digitales personales (PDAs -"personal digital assistants") y la sincronización, los datos más comunes intercambiados a través de este enlace son los datos 55 de Gestión de Información Personal (PIM -"Personal Information Management"). Cuando se intercambian por primera vez, estos datos tienden a darse en gran cantidad y ser de naturaleza voluminosa, por lo que requieren una gran anchura de banda para ser cargados en el dispositivo móvil 100, en el que pueden utilizarse sobre la marcha. Este enlace en serie puede ser utilizado también para otros propósitos, incluyendo el establecimiento de una clave privada de seguridad 111, tal como una clave privada específica de S/MIME o de PGP, el Certificado (Cert) del usuario y sus Listas de Revocación de Certificado (CRLs -"Certificate Revocation Lists") 60. La clave privada se intercambia, preferiblemente, a fin de que el equipo de sobremesa 35 y el dispositivo móvil 100 compartan una única identidad y un solo método para el acceso a todo el correo. El Cert y las CRLs se intercambian normalmente a través de dicho enlace debido a que representan una gran cantidad de los datos que se requieren por el dispositivo para la S/MIME, PGP y otros métodos de seguridad de clave pública. Sin embargo, existen situaciones en las que un usuario no tiene la facultad de establecer dicho enlace con su equipo de sobremesa 35 con el fin de actualizar el dispositivo de almacenamiento de claves del dispositivo móvil 100 con las claves privadas apropiadas. En estas situaciones, el sistema y el método aquí descritos permiten la transferencia segura de información criptográfica a través de un enlace inalámbrico.

Como se ilustra en la Figura 3, el dispositivo de comunicaciones móvil 100 incluye una antena de RF adecuada 102 para la comunicación inalámbrica hacia/desde la red inalámbrica 20. Se proporcionan circuitos 104 de desmodulación/modulación y descodificación/codificación de RF convencionales. Como apreciarán los expertos de la técnica, tales circuitos pueden comprender la posibilidad de muchos procesadores de señal digitales (DSPs -"digital signal processors"), microprocesadores, filtros, circuitos analógicos y digitales, y similares. Sin embargo, puesto que tales circuitos son bien conocidos en la técnica, no se describen adicionalmente aquí.

El dispositivo de comunicaciones móvil 100 también incluirá, típicamente, una CPU [Unidad Central de Procesamiento -"Central Processing Unit"] de control principal que funcione bajo el control de un programa almacenado en una memoria 108 de programa y que tenga acceso a una memoria 110 de datos. La CPU 106 está también en comunicación con un teclado convencional 112 y con un dispositivo de presentación visual 114 (por ejemplo, un dispositivo de presentación visual de cristal líquido o LCD ["Liquid Crystal Display"]) y un transductor de audio o altavoz 116. Una porción de la memoria 310 está disponible para almacenar los datos requeridos para descifrar mensajes cifrados, tales como, por ejemplo, claves privadas, certificados digitales y similares. Un código ejecutable por un programa informático adecuado se encuentra almacenado en ciertas porciones de la memoria 108 de programa a fin de constituir una lógica de programa almacenada para recibir y utilizar claves privadas nuevas o añadidas y/o certificados digitales o similares, según se describe más adelante (por ejemplo, a través de la puerta en serie de E/S (entrada/salida -"I/O" ("Input/Output")) de instalación cableada, o de la antena inalámbrica de RF 102).

Como se ha representado en la Figura 1, se proporciona típicamente una conexión de sincronización 26, de instalación cableada y segura (por ejemplo, entre las puertas de E/S en serie de la unidad de base 24 del usuario y del dispositivo inalámbrico 100), para propósitos de sincronización de datos normales (por ejemplo, para sincronizar bases de datos en los dos dispositivos con respecto a cosas tales como calendarios, listas de quehaceres, listas de tareas, libros de direcciones, etc.). Parte de los procedimientos de sincronización de datos anteriores tienen incluida una lógica de programa tal como la Cert Sync con el fin de mantener la sincronización entre los certificados de mensaje criptográfico. Si se dispone de una conexión de sincronización aérea (OTA -"over the air") segura 28, ésta puede ser utilizada también por la Cert Sync para mantener la sincronización de los certificados de mensaje criptográfico.

Como se ha descrito anteriormente, existe un enlace de comunicaciones (representado, por ejemplo, por líneas discontinuas con la referencia 20 en la Figura 1), que se encuentra típicamente entre la unidad de base 24 del usuario del dispositivo y un servidor 14 de mensajes del sistema. De acuerdo con ello, hay un camino de comunicación ya existente que puede ser utilizado para hacer pasar los datos de sincronización desde la unidad de base 24 del usuario, a través del canal 30, del servidor 14, de la Internet 12, de una pasarela inalámbrica 16 y de una infraestructura inalámbrica 18, a través de la conexión de sincronización OTA 28.

Como se ha ilustrado en la Figura 4, la unidad de base 24 del usuario puede ser utilizada para actualizar el dispositivo de comunicaciones inalámbricas móvil 100 con información que incluye, por ejemplo, información de clave privada e información de certificado digital. La estación de base 24 del usuario es, típicamente, una computadora personal (PC) de sobremesa, y puede ser de componentes físicos o hardware y sistema operativo convencionales. Ésta incluirá, típicamente, lógica 304 de programa gestor de equipo de sobremesa (en forma, por ejemplo, de lógica de programa informático ejecutable) para gestionar, entre otras cosas, una conexión de sincronización de datos normales con el dispositivo 100. Como se ha mencionado anteriormente, en el entorno de los sistemas de comunicaciones inalámbricos móviles, dicho gestor de equipo de sobremesa puede incluir, típicamente, lógica para la sincronización de certificados de mensaje criptográfico. Dicha lógica se denota por Cert Sync.

Los mensajes de correo electrónico generados utilizando las técnicas de S/MIME y de PGP pueden incluir información cifrada, una firma digital sobre el contenido del mensaje, o ambas. En las operaciones de S/MIME firmadas, el remitente toma un compendio de un mensaje y firma el compendio utilizando la clave privada del remitente. Un compendio es, esencialmente, una suma de comprobación, un CRC u otra operación preferiblemente no reversible, tal como una fragmentación y mezcla del mensaje, que se firma a continuación. El compendio firmado se anexa al mensaje saliente, posiblemente junto con el certificado del remitente y, posiblemente, cualesquiera certificados o CRLs requeridas. El receptor de este mensaje firmado debe también tomar un compendio del mensaje, comparar este compendio con el compendio anexado al mensaje, recuperar la clave pública del remitente y verificar la firma en el compendio anexado. Si el contenido del mensaje se ha cambiado, los compendios serán diferentes, o bien la firma en el compendio no se verificará satisfactoriamente. Si el mensaje no está cifrado, esta firma no impide que cualquiera vea el contenido del mensaje, pero sí garantiza que el mensaje no ha sido manipulado o alterado indebidamente y procede realmente de la persona que se indica en el campo "de" del mensaje.

El receptor puede también verificar el certificado y la CRL si se han anexado al mensaje. Una cadena de certificados es un certificado conjuntamente con un cierto número de otros certificados requeridos para verificar que el certificado original es auténtico. Mientras verifica la firma de un mensaje firmado, el receptor del mensaje también obtendrá, típicamente, una cadena de certificados para el certificado de la firma y verificará que cada uno de los certificados de la cadena fue formado por el siguiente certificado de la cadena, hasta que se encuentre que un certificado fue firmado por un certificado raíz desde una fuente de confianza, tal como, por ejemplo, un Servidor de Clave Pública (PKS -"Public Key Server") de gran tamaño, asociado con una Autoridad de Certificado (CA -"Certificate Authority") tal como, por ejemplo, Verisign o Entrust, ambas compañías destacadas en el campo de la criptografía de clave pública. Una vez que se ha encontrado dicho certificado raíz, una firma puede ser verificada o confiarse en ella, puesto que tanto el remitente como el receptor confían en la fuente del certificado raíz.

En las operaciones de mensajes de S/MIME cifrados, se genera una clave para una única sesión, que se utiliza para cifrar el cuerpo del mensaje, típicamente con un cifrador simétrico, tal como, por ejemplo, el DES Triple. La clave de la sesión se cifra entonces utilizando la clave pública del receptor, típicamente con un algoritmo de cifrado de clave pública como el RSA. Si el mensaje está dirigido a más de un receptor, se cifra la misma clave de sesión utilizando la clave pública de cada receptor. El cuerpo de mensaje cifrado, así como todas las claves de sesión cifradas, se envía a todos los receptores. Cada receptor debe entonces localizar su propia clave de sesión basándose, posiblemente, en

un sumario de Información de Destinatario ("Recipient Info") de los receptores, que puede estar anexo al mensaje, y descifra la clave de la sesión utilizando su clave privada. Una vez que se ha descifrado la clave de la sesión, ésta se utiliza entonces para descifrar el cuerpo del mensaje. El anexo de Información de Destinatario de S/MIME puede también especificar el esquema de cifrado particular que se ha de utilizar para descifrar el mensaje. Esta información se sitúa normalmente en la cabecera del mensaje de S/MIME. Los expertos de la técnica apreciarán que estas operaciones se refieren a un ejemplo ilustrativo de mensajería de S/MIME y de sus operaciones de codificación asociadas, sobre todo, el cifrado. Se comprenderá también que la presente descripción no está de ningún modo limitada a ello.

La Figura 5 es un diagrama de flujo proporcionado a modo de ejemplo y abreviado de un sistema para actualizar dinámica automáticamente opciones de seguridad disponibles para un mensaje basándose en el contenido del mensaje. De acuerdo con esta ilustración proporcionada a modo de ejemplo, un usuario introduce, en primer lugar, la aplicación de mensajería electrónica 501 residente en el dispositivo que está siendo utilizado por el usuario o accesible para éste. Tales dispositivos pueden incluir, por ejemplo, un dispositivo de comunicación inalámbrica móvil que sea capaz de prestar soporte a funciones de correo electrónico. Como el usuario está realizando introducciones en los diversos campos de la aplicación de mensajería electrónica, la lógica del programa supervisa las introducciones en los diversos campos, 503, para determinar qué efecto pueden tener, en caso de tener alguno, las introducciones en las opciones de seguridad disponibles para el usuario. Si la(s) introducción (introducciones) efectuadas por el usuario requieren que se cambie la lista de opciones de seguridad disponibles, tal como, por ejemplo, reduciéndola (o recortándola) o expandiéndola, 507, 508, se presenta visualmente al usuario, 511, 512, una lista de opciones de seguridad dinámicamente actualizada y, en el presente ejemplo, recortada o truncada. Ya se haya de actualizar, por ejemplo, recortar, o no, la lista de opciones se determina basándose en el criterio de seguridad que está vigente para el sistema de correo electrónico. El criterio de seguridad puede ser implementado en forma de criterio de IT por el administrador del sistema, o bien puede ser proporcionado por un tercero a través de un servidor de mensajería electrónica o similar. Se comprenderá que el criterio de seguridad puede implementarse por cualesquiera medios adecuados, y que la exposición está dirigida a un sistema y a un método para implementar criterios o pautas de seguridad con independencia de la fuente del criterio. Si el sistema determina que no existe necesidad de modificar o limitar las opciones de seguridad, éste puede presentar visualmente al usuario la matriz o juego completo de opciones de codificación de seguridad, 509. Una vez que se han presentado visualmente al usuario las opciones de seguridad, ya sea recortadas o no, 509, 513, el usuario puede escoger entonces de entre las opciones de seguridad que se están presentando visualmente, 515. La opción de seguridad seleccionada por el usuario es entonces aplicada al mensaje cuando se envía el mensaje.

Ejemplos del aspecto que puede tener para un usuario la realización proporcionada a modo de ejemplo y anteriormente descrita, se ilustran en las Figuras 7A-7G, las cuales proporcionan unas tomas o imágenes en pantalla ejemplares, ilustrativas y no limitativas. Por ejemplo, con referencia a la Figura 7A, al introducir un campo de "clasificación", el número de opciones disponibles para el usuario puede cambiar o no. Por ejemplo, tal como se ilustra en la Figura 7A, si el usuario introduce "no clasificado" como el nivel de clasificación para el mensaje, las opciones de seguridad visualmente presentadas pueden incluir todas las opciones, desde la más alta (por ejemplo, firmado y cifrado en PGP o en S/MIME) hasta la más baja (por ejemplo, texto simple). En este ejemplo, el usuario ha seleccionado "texto simple", como se muestra en la Figura 7B. Sin embargo, si el usuario selecciona, por ejemplo, "protegido" como clasificación para el mensaje, tal como se ilustra en la Figura 7C, la modificación dinámica de las opciones de seguridad permisibles proporciona una lista de opciones de seguridad disponibles para el usuario que puede ser recortada dinámicamente reduciéndola hasta un número de inferior de opciones, basándose en la naturaleza protegida de la clasificación. En este ejemplo, las opciones de codificación de seguridad disponibles pueden ser recortadas de manera que se listen sólo las opciones que incluyen un requisito de firma electrónica. Así, el "texto simple" puede ya no aparecer como una opción en la situación en la que se introduce "protegido" en el campo de clasificación del mensaje, tal y como se ilustra en la Figura 7C. La Figura 7D ilustra la presentación visual una vez que se ha seleccionado una de las opciones permitidas de entre la lista dinámicamente actualizada de la Figura 7C. En las Figuras 7A-7G se muestran varios ejemplos de dicho recorte o truncamiento. Por ejemplo, la Figura 7E ilustra una lista de opciones de codificación de seguridad aún más recortada, basada en una clasificación de "alto secreto".

Pueden supervisarse también otros campos para determinar si puede modificarse, por ejemplo, recortarse o expandirse, y en qué medida, la lista de opciones de seguridad disponibles para un usuario. Por ejemplo, con referencia a las Figuras 7F y 7G, el usuario ha seleccionado un mensaje texto simple y no clasificado que se ha de enviar. Sin embargo, la introducción del destinatario como "John Doe" provoca que la actualización dinámica de la lista de opciones de seguridad refleje el criterio o pauta de seguridad del sistema, de hecho, con respecto a los mensajes que se envían a John Doe. En este contexto proporcionado a modo de ejemplo, John Doe es un agente importante que únicamente puede recibir mensajes electrónicos de los empleados si el mensaje es un mensaje cifrado. Así, cuando se introduce "John Doe" como destinatario por el usuario, el sistema actúa recortando la lista de opciones de seguridad de manera que incluya únicamente las opciones que incluyen una firma, tal como se ilustra en la Figura 7. Se comprenderá que cualquier campo puede ser supervisado en relación con cualquier palabra clave. Por ejemplo, los nombres o referencias de proyectos internos que pueden estar incluidas en el texto del mensaje pueden requerir una seguridad mejorada, incluso aunque el resto del mensaje puede estar clasificado como texto simple. Si se detecta tal palabra clave, por ejemplo, en la línea del asunto o en el propio texto del mensaje, la lista de opciones de seguridad puede ser actualizada dinámicamente, por ejemplo, recortada o truncada, de acuerdo con realizaciones proporcionadas a modo de ejemplo y que se describen aquí. En cualquier caso, los diversos campos son comprobados y, si es apropiada la actualización dinámica de la lista de opciones de seguridad, se le presenta al usuario una lista actualizada de opciones de seguridad para su aplicación al mensaje.

La Figura 6 es un diagrama de flujo proporcionado a modo de ejemplo y abreviado de un sistema para redondear al alza de forma dinámica y automática los ajustes de seguridad basándose en el contenido de un mensaje, y, opcionalmente, proporcionar a un usuario opciones de seguridad de un nivel más alto. De acuerdo con este ejemplo, el usuario introduce la aplicación de mensajería electrónica, 601, e introduce información en los diversos campos. Las introducciones en los diversos campos son supervisadas y comprobadas, 603, de una manera similar a la que se ha descrito anteriormente en relación con referencia a la Figura 5. Si no se requiere ninguna modificación de los ajustes de seguridad, el mensaje puede enviarse con las opciones de seguridad originales seleccionadas por el usuario, 607. Sin embargo, si el sistema detecta una introducción o palabra clave que requiere la modificación de las opciones de seguridad disponibles para el usuario, 605, el sistema y el método de este ejemplo pueden cambiar automáticamente las opciones de seguridad aplicadas, de manera que pasen a un nivel de seguridad más alto que refleje un nivel mínimo de seguridad en correspondencia con el criterio de seguridad asociado con el destinatario 609. Puede hacerse referencia a este tipo de actualización automática de los ajustes de seguridad como "redondeo al alza" de los ajustes de seguridad. El usuario, bien puede aceptar, 611, los ajustes de seguridad automáticamente actualizados, por ejemplo, al ejecutar o llevar a cabo la orden de envío, 613, o bien puede el usuario, opcionalmente, escoger de entre una lista actualizada, por ejemplo, recortada, de opciones de seguridad, 615, y seleccionar un nivel aún más alto de codificación de seguridad, 617, para el mensaje de lo que se permite por el criterio de seguridad según se refleja en las propiedades de seguridad u opciones de codificación actualizadas que se han puesto a disposición del usuario. Tras realizar la selección, 617, el usuario puede enviar entonces el mensaje, habiéndose aplicado al mismo, 619, las opciones de seguridad seleccionadas.

La Figura 8 ilustra el aspecto que puede tener para un usuario el ejemplo representado en la Figura 6. De acuerdo con este ejemplo, la introducción de una clasificación "secreto" y de un destinatario "John Doe" ha provocado que el sistema de modificación dinámica seleccione una opción de seguridad de "PGP [Firmar y Cifrar]" para el mensaje. El usuario es entonces instado a, y se le proporciona la opción de, aceptar el ajuste de seguridad redondeado al alza que el sistema proporciona, mediante la pulsación de la tecla de enviar, o bien a ver, alternativamente, otras opciones de seguridad que podrían estar presentes en una lista de opciones de seguridad actualizada, por ejemplo, recortada (que no se muestra).

La Figura 9 es un diagrama de flujo proporcionado a modo de ejemplo y abreviado de un sistema para actualizar de forma dinámica y automática las opciones de seguridad disponibles para un mensaje basándose en cuál de los servicios múltiples de mensaje se está utilizando para enviar un mensaje. De acuerdo con esta realización a modo de ejemplo, los ajustes de seguridad pueden establecerse basándose en el tipo de servicio de mensaje que se está empleando. Por ejemplo, en un entorno de servicios de mensaje múltiples en el que se están utilizando múltiples cuentas de correo electrónico (por ejemplo, cuentas domésticas y de oficina), pueden aplicarse diferentes niveles de clasificación y criterios de seguridad. Así, las opciones de seguridad proporcionadas al usuario pueden estar basadas en la selección de cuáles de los múltiples tipos de servicios de mensaje se están utilizando. Una vez que se ha seleccionado el servicio de mensajería, por ejemplo, doméstico o de oficina, por parte del usuario, 901, el sistema y el método determinan si la lista de opciones de seguridad ha de ser actualizada dinámicamente, por ejemplo, recortada o expandida, 903, basándose en los criterios de seguridad que están vigentes para el sistema. Si la lista se ha de actualizar, la lista actualizada, por ejemplo, abreviada, de opciones de seguridad es presentada visualmente al usuario, 905. Por otra parte, si el servicio de mensajería seleccionado no requiere ninguna modificación adicional de la lista de opciones de seguridad, entonces se presenta visualmente al usuario la lista completa de opciones, 907. Cualquiera que sea la lista que se presente visualmente, es la base para proporcionar las opciones que van más allá de la referencia 909, por ejemplo, de acuerdo con las realizaciones ilustrativas descritas en relación con las Figuras 5 y 6.

Si bien se han expuesto las realizaciones ilustrativas con respecto a opciones de seguridad, se consideran dentro del ámbito de esta exposición cualesquiera otras opciones de usuario que resulten adecuadas para ser recortadas o truncadas basándose en el contenido de un mensaje, en el servicio de mensajería que se esté utilizando, o similar. Por otra parte, tal y como se ha expuesto anteriormente, las opciones de seguridad pueden estar basadas en reglas asociadas con servicios proporcionados por terceros diferentes del administrador del sistema. Por ejemplo, puede utilizarse el servidor de un tercero para instaurar criterios de seguridad de correo electrónico para los usuarios del sistema. Del resto de criterios de seguridad del sistema puede encargarse el administrador del sistema. Las limitaciones que proporciona el servidor del tercero pueden ser reflejadas dinámicamente ante un usuario de un modo conforme se ha establecido anteriormente, de tal manera que el usuario puede evitar realizar selecciones que sean rechazadas más tarde por razón de que las selecciones violan los criterios basados en el servidor. Los criterios de seguridad que se establecen por terceros pueden también implementar la actualización dinámica de opciones de seguridad proporcionada al usuario de la manera que aquí se ha expuesto, con respecto a las realizaciones proporcionadas a modo de ejemplo.

Si bien lo anterior se ha descrito en combinación con realizaciones ejemplares concretas, es obvio que resultarán evidentes para los expertos de la técnica muchas alternativas, modificaciones y variaciones. En consecuencia, se pretende que las realizaciones proporcionadas a modo de ejemplo que se han expuesto aquí sean ilustrativas, y no limitativas. Pueden realizarse cambios diversos sin apartarse del ámbito de la invención, tal y como se define en las reivindicaciones que se acompañan.

REIVINDICACIONES

1. Un método para modificación dinámica de propiedades de mensaje electrónico permisibles en una aplicación de mensajería electrónica residente en un dispositivo de comunicación de usuario o accesible a éste, que comprende las etapas de:

generar un mensaje electrónico al recibir introducciones efectuadas por un usuario en diversos campos del mensaje por medio de una interfaz de usuario, y propiedades de mensajería seleccionadas por el usuario de entre una lista de opciones de propiedades disponibles para aplicar a dicho mensaje;

supervisar dichas introducciones mientras los datos están siendo introducidos en los diversos campos a la través de la interfaz de usuario, a fin de determinar si determinar si las introducciones afectan a dicha lista de opciones de propiedades disponibles, y, si es así, actualizar automáticamente dicha lista de opciones de propiedades disponibles para ser aplicadas a dicho mensaje basándose en el contenido de dichas introducciones y en un criterio o pauta del sistema, aplicable a dicho contenido, mientras se está componiendo dicho mensaje;

presentar visualmente una lista actualizada de opciones de propiedades disponibles para ser aplicadas al mensaje basándose en los resultados de la etapa de supervisión y actualización automática, mientras se está componiendo el mensaje;

recibir una propiedad seleccionada por el usuario para ser aplicada al mensaje, de entre la lista actualizada de opciones de propiedades, antes de enviar el mensaje; y

enviar el mensaje, habiéndosele aplicado las opciones de propiedades seleccionadas.

2. El método de acuerdo con la reivindicación 1, en el cual:

dicha lista actualizada de opciones de propiedades comprende un número inferior de opciones de propiedades que el número de opciones de propiedades disponibles antes de la actualización automática, de tal modo que dicho número inferior de opciones de propiedades incluye un requisito de codificación mínimo.

3. El método de acuerdo con la reivindicación 1, en el cual las opciones de propiedades disponibles incluyen propiedades de codificación de seguridad.

4. El método de acuerdo con la reivindicación 1, en el cual la actualización automática de la lista de opciones de propiedades disponibles está basada en un destinatario del mensaje, en una palabra clave presente en el asunto o en el texto del mensaje, o en una clasificación de seguridad seleccionada del mensaje.

5. El método de acuerdo con la reivindicación 1, en el cual la actualización automática de la lista de opciones de propiedades disponibles está basada en cuál de los múltiples tipos de servicios de mensajería se está utilizando.

6. El método de acuerdo con la reivindicación 1, en el cual el criterio o pauta del sistema se proporciona como un criterio de IT gestionado por un administrador del sistema o un criterio de un tercero aplicado a un sistema de mensajería electrónica.

7. El método de acuerdo con la reivindicación 1, en el cual el mensaje electrónico se compone en un dispositivo de comunicación de usuario, inalámbrico y móvil.

8. El método de acuerdo con la reivindicación 6, en el cual el criterio de un tercero se proporciona por medio de un servidor de mensajes electrónicos.

9. Un sistema para la modificación dinámica de propiedades de mensaje electrónico permisibles, que comprende:

un dispositivo de comunicación de usuario, capaz de enviar y recibir mensajes electrónicos y que incluye un dispositivo de presentación visual;

lógica de programación, residente en dicho dispositivo de comunicación de usuario con el fin de supervisar las introducciones por parte del usuario en diversos campos de un mensaje electrónico, mientras un usuario está realizando introducciones en los diversos campos, al objeto de determinar si las entradas afectan a una lista de opciones de propiedades disponibles para ser aplicadas al mensaje electrónico, y, si es así, actualizar automáticamente la lista de opciones de propiedades disponibles para ser aplicadas al mensaje electrónico, basándose en el contenido de dichas introducciones y en un criterio o pauta del sistema referente a dichas propiedades, mientras se está componiendo dicho mensaje;

de manera que dicho dispositivo de presentación visual está dispuesto para presentar visualmente una lista actualizada de opciones de propiedades disponibles para ser aplicadas al mensaje electrónico, basándose en los resultados de la supervisión y de la actualización automática; y

dicho dispositivo de comunicación de usuario está dispuesto para enviar dicho mensaje que tiene, aplicada al mismo, una opción de propiedad seleccionada por el usuario de entre la lista actualizada de opciones de propiedades, seleccionada antes del envío del mensaje.

10. El sistema de acuerdo con la reivindicación 9, en el cual:

dicha lista actualizada de opciones de propiedades comprende un número inferior de opciones de propiedades que el número de opciones de propiedades disponibles antes de la actualización automática, de tal modo que dicho número inferior de opciones de propiedades incluye un requisito de codificación mínimo.

11. El sistema de acuerdo con la reivindicación 9, en el cual las opciones de propiedades disponibles incluyen propiedades de codificación de seguridad.

12. El sistema de acuerdo con la reivindicación 9, en el cual la actualización automática de la lista de opciones de propiedades disponibles está basada en un destinatario del mensaje, en una palabra clave presente en el asunto o en el texto del mensaje, o en una clasificación de seguridad para el mensaje.

13. El sistema de acuerdo con la reivindicación 9, en el cual la actualización automática de la lista de opciones de propiedades disponibles está basada en cuál de los múltiples tipos de servicios de mensajería está siendo utilizado por el dispositivo de comunicación de usuario.

14. El sistema de acuerdo con la reivindicación 9, en el cual el criterio o pauta del sistema se proporciona como un criterio de IT gestionado por un administrador del sistema o un criterio de un tercero aplicado a un sistema de mensajería electrónica.

15. El sistema de acuerdo con la reivindicación 9, en el cual el dispositivo de comunicación de usuario comprende un dispositivo de comunicación de usuario, inalámbrico y móvil.

16. El sistema de acuerdo con la reivindicación 14, en el cual el criterio de un tercero se proporciona por medio de un servidor de mensajes electrónicos.

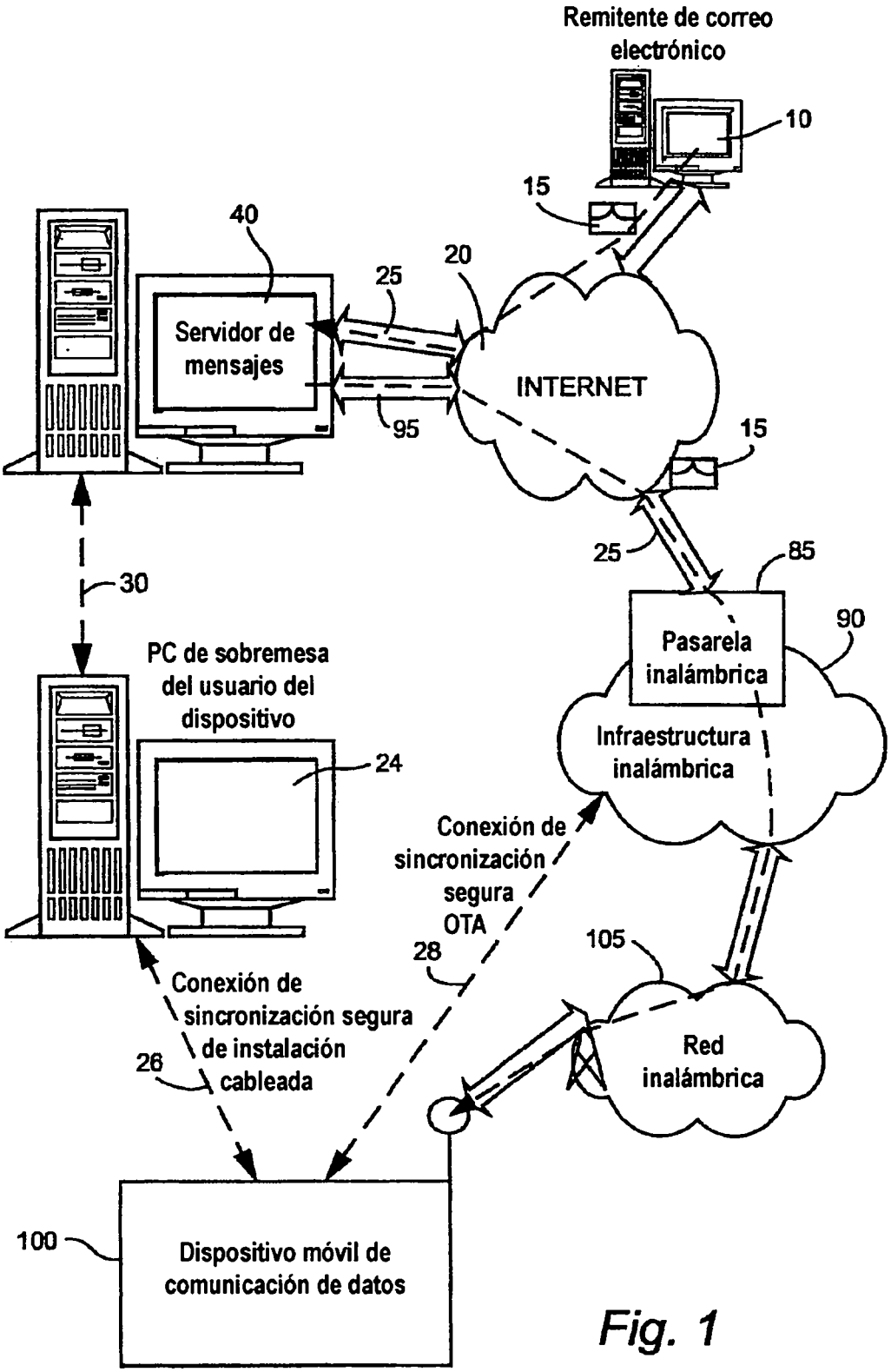
Remitente de correo electrónico
10
15
40
20
25
Servidor de mensajes
INTERNET
95
15
25
85
30
90
Pasarela inalámbrica
PC de sobremesa del usuario del dispositivo
24
Infraestructura inalámbrica
Conexión de sincronización segura OTA
28
105
Conexión de sincronización segura de instalación cableada
26
Red inalámbrica
100
Dispositivo móvil de comunicación de datos

Fig. 1

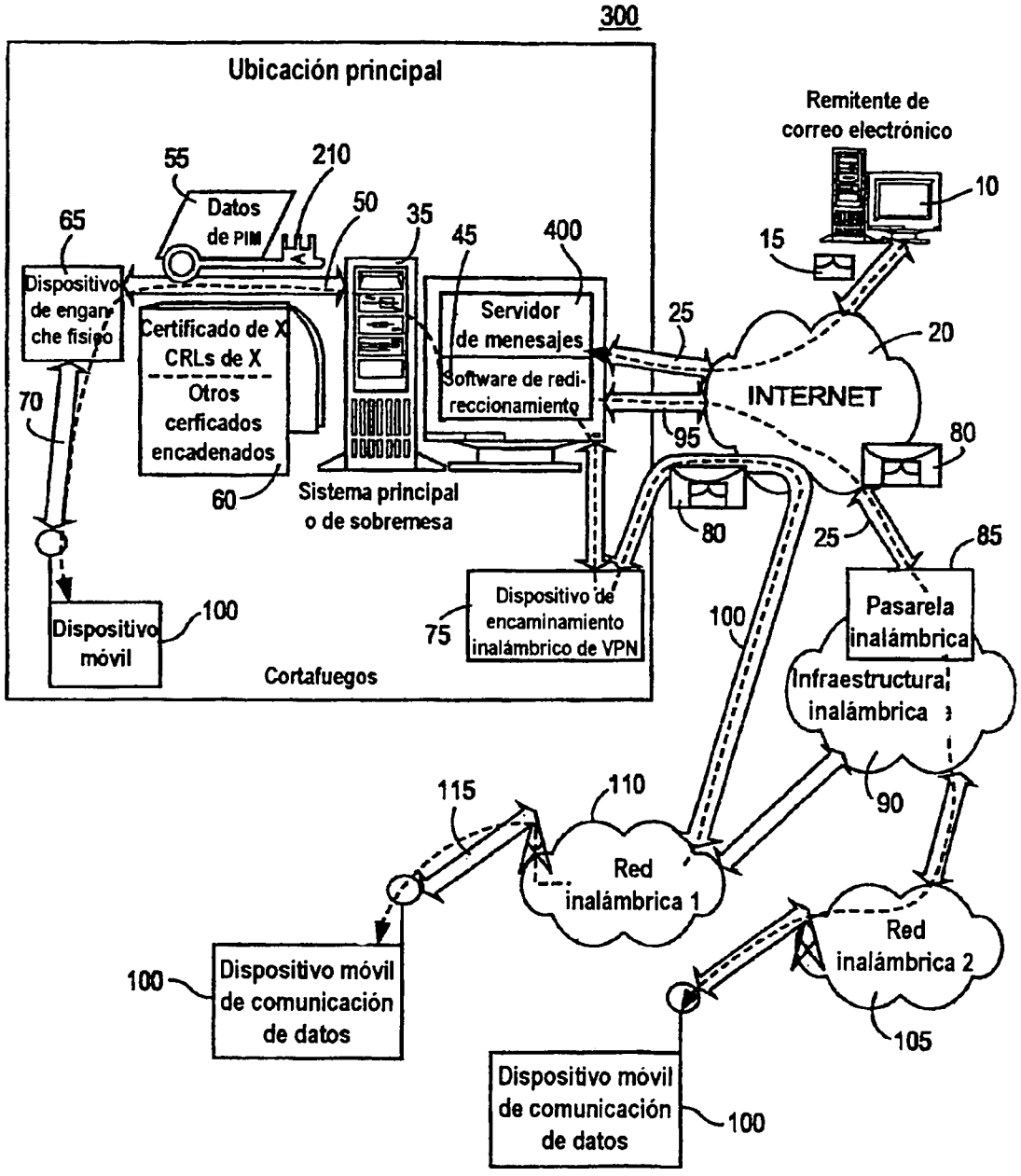
300
Ubicación principal
Remitente de correo electrónico
10
15
55
210
Datos de PIM
50
35
45
400
65
Dispositivo de engan- che físico
Certificado de X
CRLs de X
Otros cerficados encadenados
Servidor de menesajes
Software de redi- reccionamiento
25
20
INTERNET
70
95
80
60
Sistema principal o de sobremesa
80
25
85
Dispositivo de encaminamiento inalámbrico de VPN
75
100
Dispositivo móvil
100
Cortafuegos
Pasarela inalámbrica
Infraestructura inalámbrica
90
115
110
Red inalámbrica 1
Red inalámbrica 2
105
100
Dispositivo móvil de comunicación de datos
100
Dispositivo móvil de comunicación de datos
100

Fig. 2

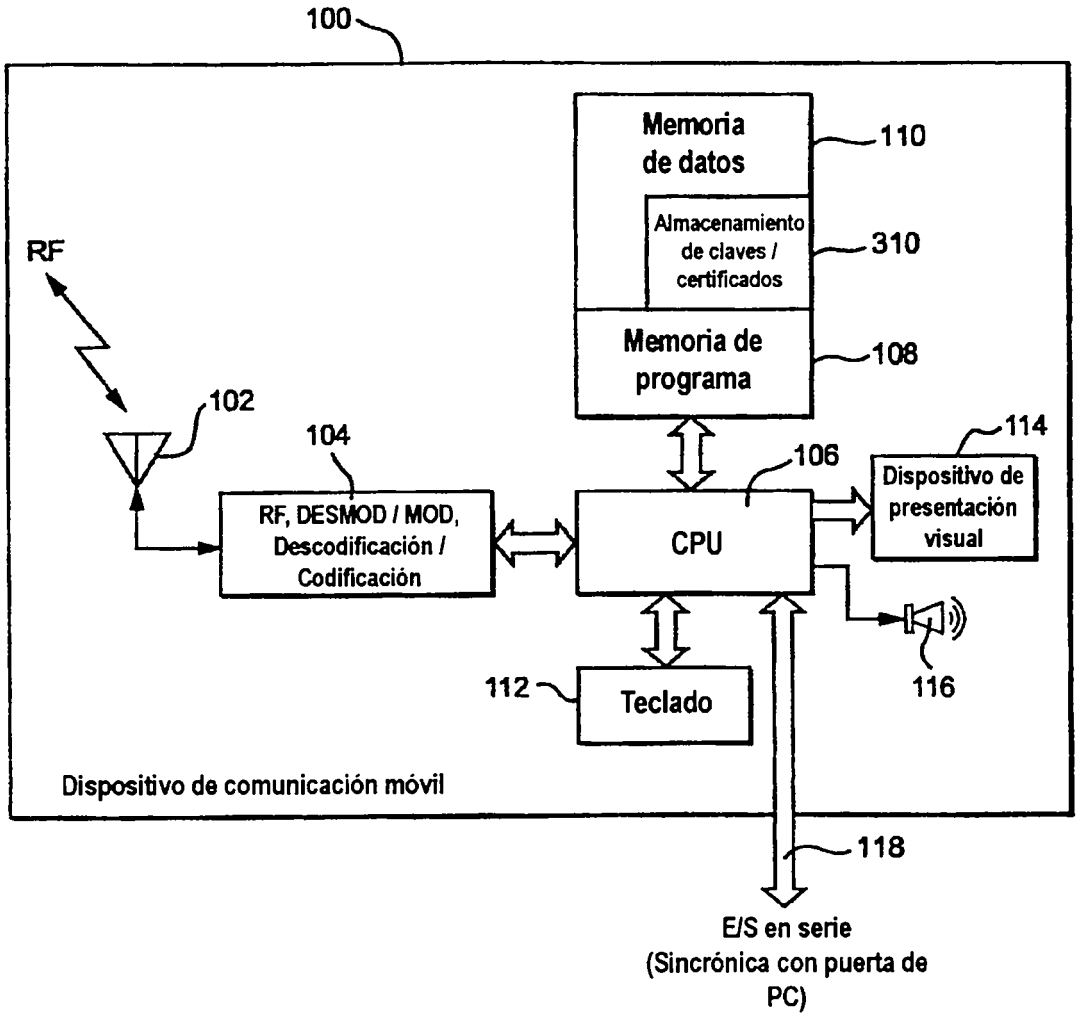
100
Memoria de datos
110
Almacenamiento de claves / certificados
310
Memoria de programa
108
RF
102
104
RF, DESMOD / MOD, Descodificación / Codificación
106
CPU
114
Dispositivo de presentación visual
116
112
Teclado
Dispositivo de comunicación móvil
118
E/S en serie
(Sincrónica con puerta de PC)

Fig. 3

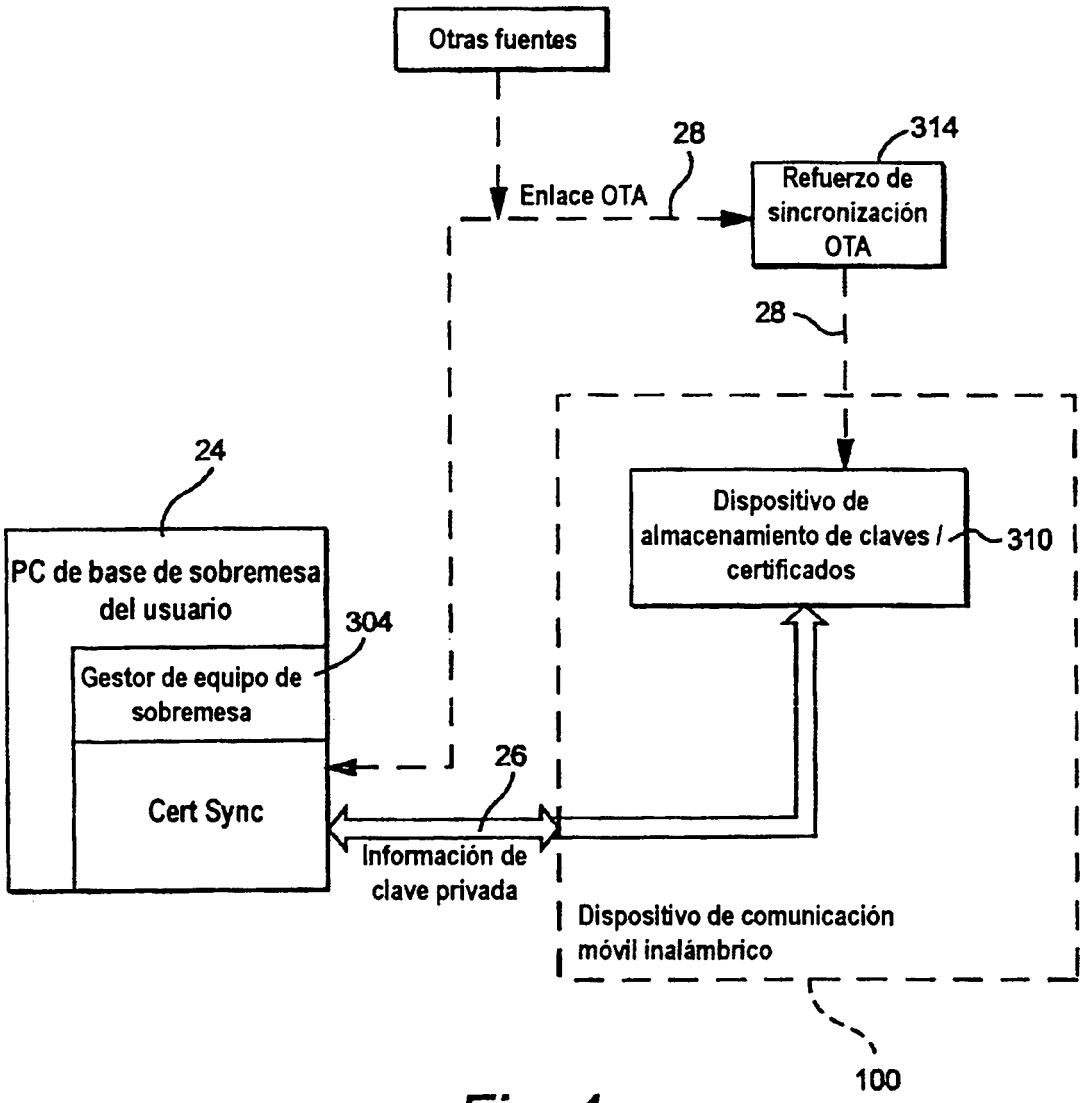
Otras fuentes
28
314
Enlace OTA
Refuerzo de sincronización OTA
28
24
Dispositivo de almacenamiento de claves / certificados
310
PC de base de sobremesa del usuario
304
Gestor de equipo de sobremesa
26
Cert Sync
Información de clave privada
Dispositivo de comunicación móvil inalámbrico
100

Fig. 4

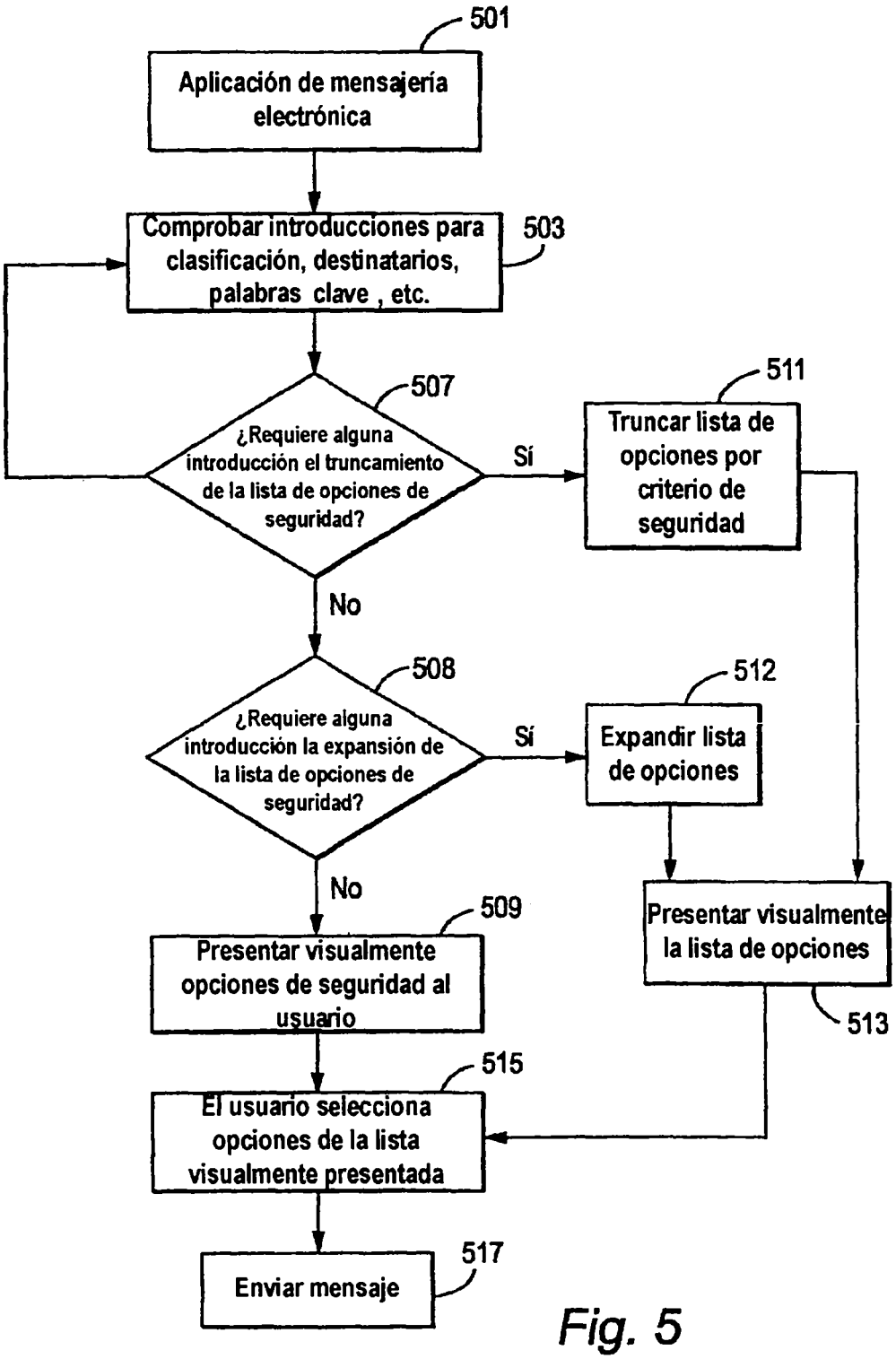
501
Aplicación de mensajería electrónica
Comprobar introducciones para clasificación, destinatarios, palabras clave , etc.
503
507
¿Requiere alguna introducción el truncamiento de la lista de opciones de seguridad?
Sí
511
Truncar lista de opciones por criterio de seguridad
No
508
¿Requiere alguna introducción la expansión de la lista de opciones de seguridad?
Sí
512
Expandir lista de opciones
No
509
Presentar visualmente opciones de seguridad al usuario
Presentar visualmente la lista de opciones
513
515
El usuario selecciona opciones de la lista visualmente presentada
Enviar mensaje
517

Fig. 5

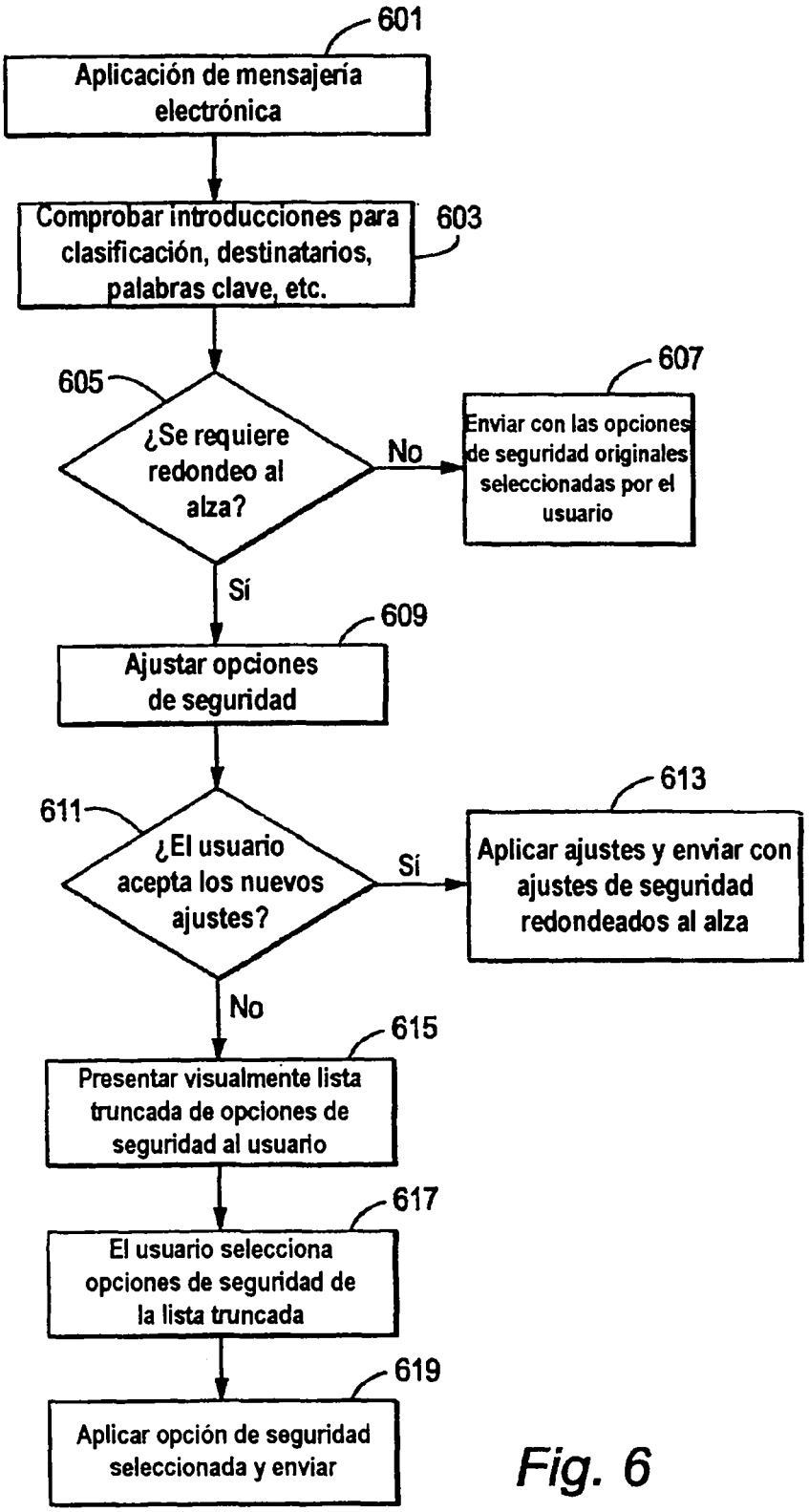
601
Aplicación de mensajería electrónica
Comprobar introducciones para clasificación, destinatarios, palabras clave, etc.
603
605
¿Se requiere redondeo al alza?
No
607
Enviar con las opciones de seguridad originales seleccionadas por el usuario
Sí
609
Ajustar opciones de seguridad
611
¿El usuario acepta los nuevos ajustes?
Sí
613
Aplicar ajustes y enviar con ajustes de seguridad redondeados al alza
No
615
Presentar visualmente lista truncada de opciones de seguridad al usuario
617
El usuario selecciona opciones de seguridad de la lista truncada
619
Aplicar opción de seguridad seleccionada y enviar

Fig. 6

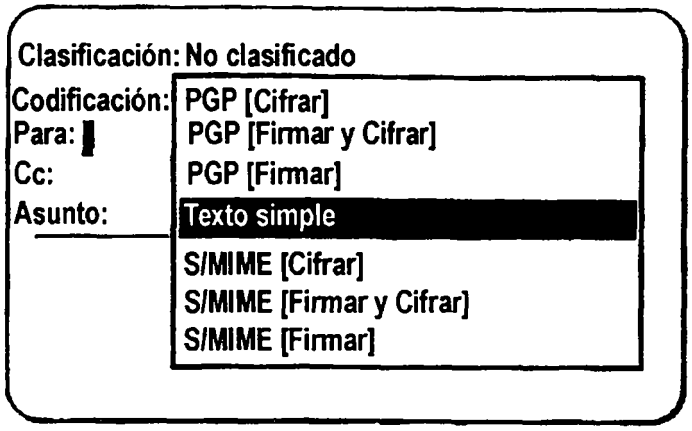

Fig. 7A

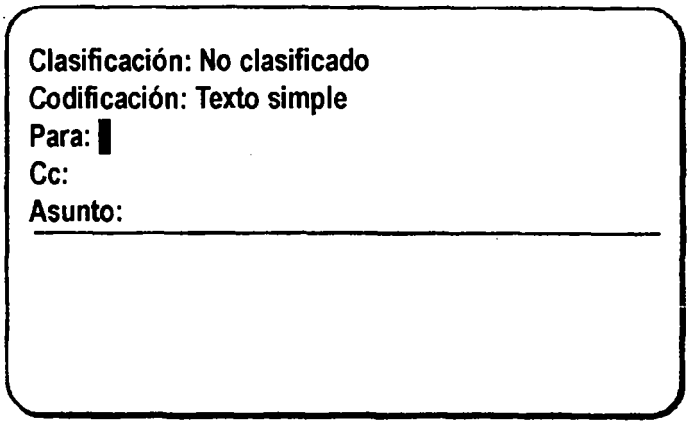

Fig. 7B

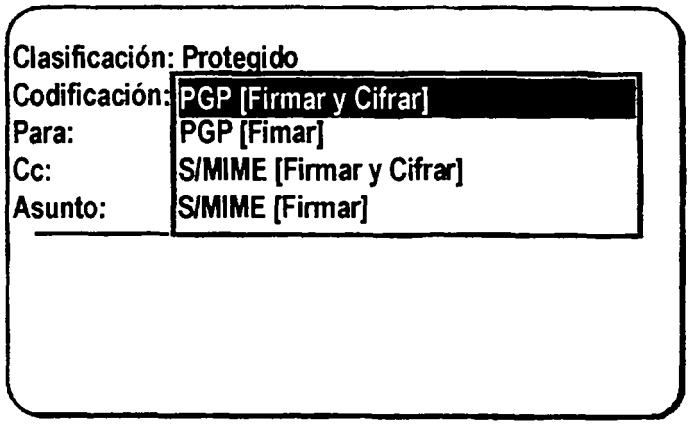

Fig. 7C

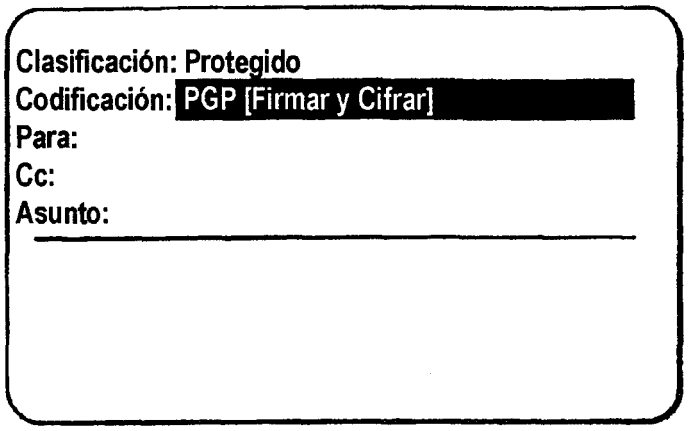

Fig. 7D

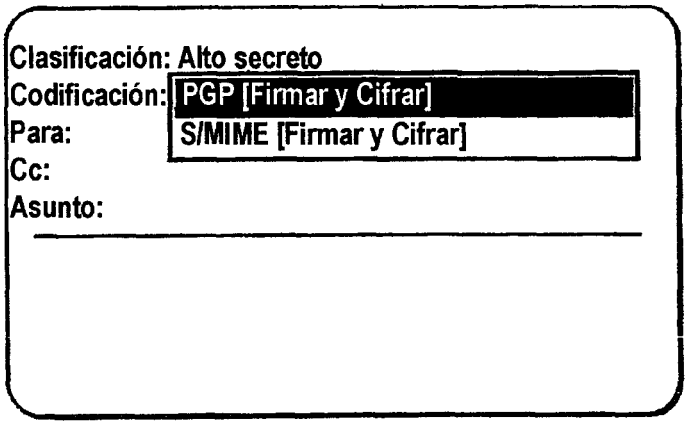

Fig. 7E

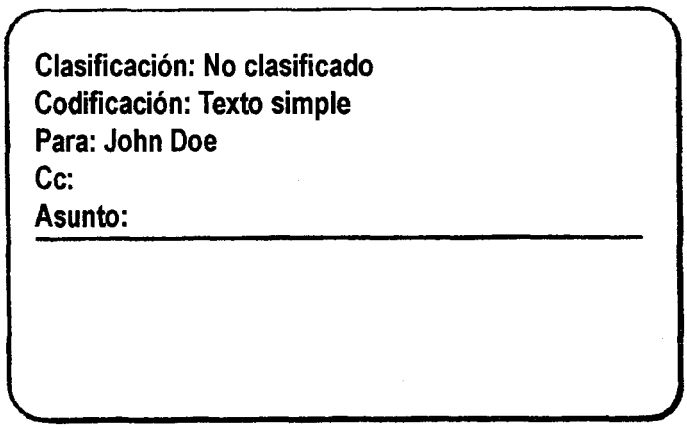

Fig. 7F

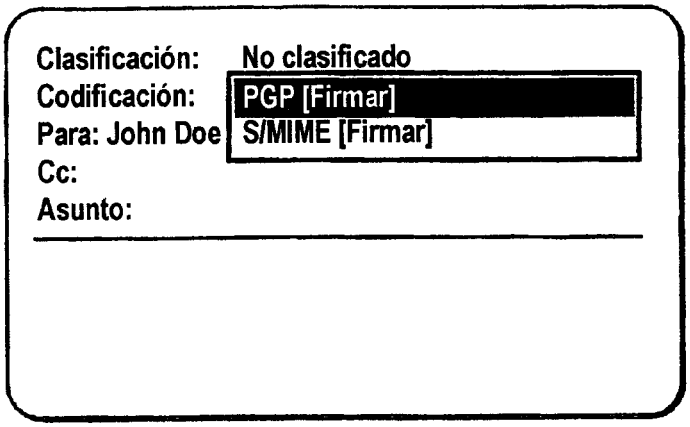
Clasificación: No clasificado
Codificación:
Para: John Doe
Cc:
Asunto:
PGP [Firmar]
S/MIME [Firmar]

Fig. 7G

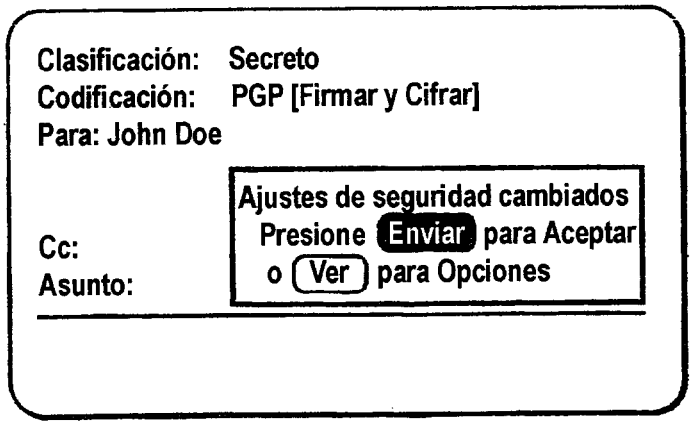
Clasificación: Secreto
Codificación: PGP [Firmar y Cifrar]
Para: John Doe
Cc:
Asunto:
Ajustes de seguridad cambiados
Presione Enviar para Aceptar
o Ver para Opciones

Fig. 8

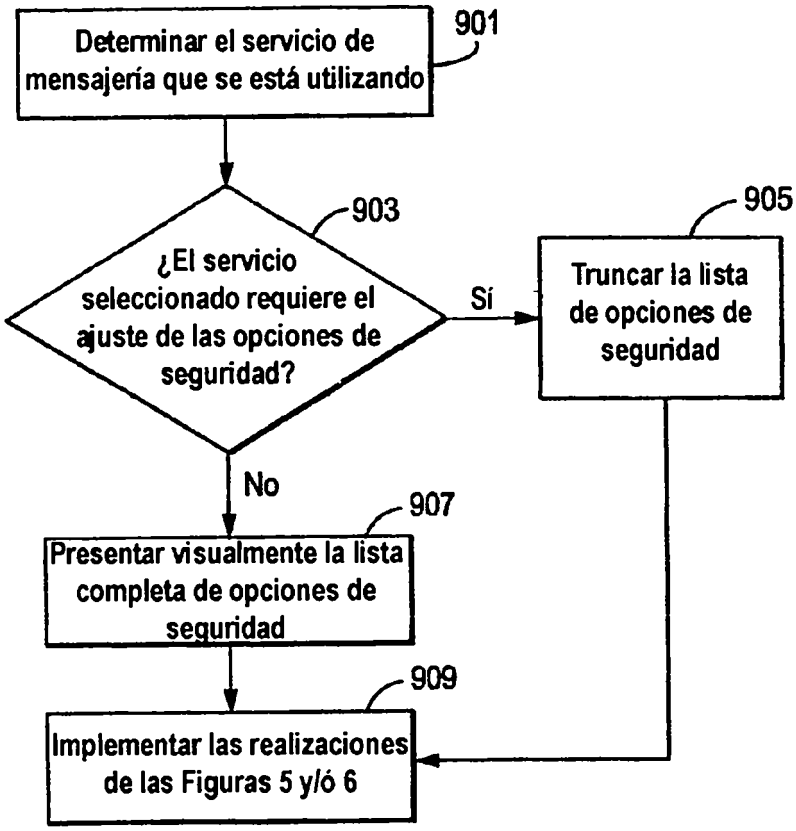
Determinar el servicio de mensajería que se está utilizando
901
¿El servicio seleccionado requiere el ajuste de las opciones de seguridad?
903
Sí
Truncar la lista de opciones de seguridad
905
No
Presentar visualmente la lista completa de opciones de seguridad
907
Implementar las realizaciones de las Figuras 5 y/ó 6
909

Fig. 9