(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 393 306**

(51) Int. CI.:

H04L 12/58 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **07120418 .4**

(96) Fecha de presentación: **09.11.2007**

(97) Número de publicación de la solicitud: **1956776**

(97) Fecha de publicación de la solicitud: **13.08.2008**

(54) Título: **Procedimiento y sistema para la transmisión de un mensaje electrónico**

(30) Prioridad:

08.02.2007 NL 1033356

(45) Fecha de publicación de la mención BOPI:

20.12.2012

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

20.12.2012

(73) Titular/es:

DLB FINANCE & CONSULTANCY B.V. (50.0%)
LAAKSEWEG 24
4874 LV ETTEN-LEUR, NL y
HITD INFORMATION TECHNOLOGY B.V. (50.0%)

(72) Inventor/es:

BENSCHOP, DIRK LEONARD y
BENSCHOP, HENDERIK REINOUT

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCION

Procedimiento y sistema para la transmisión de un mensaje electrónico

SECTOR DE LA INVENCIÓN

La invención se refiere a un procedimiento y sistema para la transmisión de un mensaje electrónico en un sistema de comunicación. De manera más específica, la invención se refiere a un procedimiento y sistema para la transmisión del mensaje electrónico desde el dispositivo de un primer usuario al dispositivo de un segundo usuario, comprendiendo el sistema, como mínimo, un primer servidor y un segundo servidor que están conectados en comunicación entre sí y al primer y segundo dispositivos de usuario.

ANTECEDENTES

El spam ("correo basura") de correo electrónico se puede definir en general como mensajes de correo electrónico no solicitados y/o no deseados recibidos por un usuario de correo electrónico ("e-mail").

La magnitud de los mensajes de spam de correo electrónico ha aumentado notablemente en la última década. La razón de ello es el enorme número de direcciones a las que se puede tener acceso con un correo electrónico con un coste poco importante. Esta combinación de factores, junto con la entrega obligatoria de un correo electrónico ha hecho de este último o, dicho de forma más general, del envío de mensajes electrónicos un medio atractivo de comunicación para anunciar una serie de productos y servicios. Se pueden adquirir colecciones de direcciones de correo electrónico de individuos en todo el mundo de numerosos suministradores a precios muy bajos. En la actualidad, los mensajes spam de correo electrónico representan más del 90% de todos los mensajes de correo electrónico transmitidos por Internet. Como consecuencia, los recursos electrónicos se desperdician de manera importante.

El incremento de la cantidad de mensajes spam de correo electrónico ha provocado que otros proporcionen filtros de spam de correo electrónico ("e-mail"). Estos filtros se pueden instalar tanto en el lado del servidor como en el lado de los dispositivos de cliente para detectar y borrar mensajes spam de correo electrónico sin molestar al usuario. De manera típica, estos filtros analizan los mensajes de correo electrónico y comparan los resultados del análisis con respecto a normas de spam de correo electrónico a efectos de reconocer el spam de los correos electrónicos. Estas normas de spam de correos electrónicos están diseñadas en base a características típicas conocidas de mensajes de spam de correo electrónico, tal como el número de direcciones en la cabecera del correo electrónico o la aparición de ciertas palabras en el cuerpo del texto del correo electrónico.

No obstante, las nuevas formas de spam no siempre serán reconocidas e interceptadas por estos filtros, dado que las normas de spam de correo electrónico no son capaces de reconocer estas nuevas formas de spam, dado que estas normas de spam para la forma nueva de mensajes spam de correo electrónico ("e-mail") no se han podido implementar todavía en el filtro de spam. Como consecuencia, existe una carrera continuada entre los que envían mensajes spam por correo electrónico y los proveedores de filtros de spam, encontrándose por definición estos últimos por detrás de los primeros. Por otra parte, mensajes de correo electrónico solicitados y deseados por un receptor determinado son eliminados por filtrado del buzón de correo electrónico porque el mensaje de correo electrónico se califica como spam, de acuerdo con las normas de spam de correo electrónico que impone el filtro de spam.

El documento WO 03/061213 da a conocer un procedimiento de aviso y descarga de correo electrónico. Se introduce un buzón de emisor en un servidor "downemail" fuente y el lugar en el que se almacena el mensaje original hasta que el receptor previsto lo lee se desplaza desde el buzón del receptor a un servidor "downemail" de destino con respecto al buzón del emisor. Para enviar un mensaje desde el sistema de correo electrónico al sistema de correo receptor, se diseña también un servidor de intervención de mensajes. El servidor "downemail" fuente genera un mensaje de señalización para notificar el envío de un mensaje y luego lo transmite al receptor previsto. Después de leer el mensaje de señalización, el receptor puede conseguir el mensaje original del buzón del emisor.

El documento US 2002/0174194 se refiere a un sistema que prevé un único interfaz basado en la web que proporciona al usuario acceso a una serie de cuentas de mensajes en diferentes servidores de mensajes. Además, los tiempos de registro y las exigencias de ancho de banda de la red se reducen almacenando información de mensajes almacenada en un "cookie" en el terminal del usuario.

El documento WO 00/42748 da a conocer un sistema de suministro de documentos electrónicos que posibilita el intercambio de paquetes firmados digitalmente y codificados con una clave pública sin requerir aplicaciones de software de seguridad de clave pública especializadas preinstaladas en el ordenador del receptor. Un URL que identifica este paquete es enviado al receptor por correo electrónico. Después de someter el URL a través de la World Wide Web, se envían al receptor instrucciones de ordenador en forma de una aplicación ("applet"), por ejemplo, para realizar la recuperación y procesado del paquete. Este procesado puede incluir la decodificación de una o varias partes del paquete y la verificación de una firma del paquete.

El documento WO 03/003234 da a conocer un sistema, procedimiento y programa de ordenador formando un producto para proporcionar mensajes unificados utilizando almacenamiento separado de componentes de medios, permitiendo un almacenamiento y recuperación más eficaces de mensajes. Un mensaje es enviado desde un segundo usuario a un primer usuario a través de la red. El mensaje es recibido por un primer servidor. El primer servidor almacena el componente de medios del mensaje en un dispositivo de almacenamiento en masa. El primer servidor almacena también en un servidor de correo electrónico una cabecera, incluyendo información con respecto al mensaje, y una referencia al componente de medios correspondiente del mensaje almacenado en el dispositivo de almacenamiento en masa. Cuando se recupera un mensaje almacenado por el primer usuario, el servidor de correo electrónico es preguntado a través del primer servidor. A continuación, el servidor de correo electrónico proporciona al primer usuario, con intermedio del primer servidor: la cabecera, o componente sin medios del mensaje, y la referencia al componente de medios correspondiente del mensaje almacenado en el dispositivo de almacenamiento en masa. Entonces, la referencia puede ser utilizada por el primer usuario para recuperar del dispositivo de almacenamiento en masa la componente de medios correspondiente del mensaje. A continuación, el primer usuario puede visionar el mensaje completo.

El documento WO 2004/071035 da a conocer un filtrado dinámico basado en el servidor que borra selectivamente o facilita mensajes basados en características del mensaje recibido y las normas de filtrado implementadas en el servidor.

El documento EP-A-1 496 655 da a conocer un sistema para detectar y prevenir un spam. El sistema proporciona varias técnicas para controlar comunicaciones salientes para identificar potenciales emisores de spam, tal como identificación y puntuación. Se pueden tomar otras acciones para verificar si el emisor de spam potencial es un emisor de spam. Estas acciones incluyen la inspección humana de una muestra de los mensajes, envío de pruebas a la cuenta, enviando un aviso legal para advertir a los potenciales emisores de spam y/o cerrar la cuenta.

Además, si se instalan filtros de spam de correo electrónico, todos los filtros analizan cada mensaje individual de correo electrónico a efectos de detectar mensajes de spam de correo electrónico. Como consecuencia, se retrasa la transferencia de mensajes y se desperdician recursos.

Teniendo en cuenta lo anterior, existe la necesidad evidente en esta técnica para conseguir un procedimiento y sistema para transmitir mensajes electrónicos desperdiciando menos recursos.

RESUMEN DE LA INVENCIÓN

Es un objetivo de la invención dar a conocer un procedimiento y sistema mejorados para transmitir mensajes electrónicos en una red de comunicaciones.

Con este objetivo, se da a conocer un sistema tal como se define en la reivindicación 1.

Además, se da a conocer en la reivindicación 12 un procedimiento para la transmisión de un mensaje electrónico.

La invención está dirigida también a un programa de ordenador según la reivindicación 21 y a un soporte que contiene dicho programa de ordenador, de manera que el programa de ordenador contiene partes de código de software capaces de, cuando se han instalado y ejecutado por un dispositivo electrónico, llevar a cabo el procedimiento descrito en el párrafo anterior.

El solicitante ha observado que el procedimiento convencional y sistema para la transmisión de mensajes electrónicos utilizando servidores de correo electrónico tiene como resultado un desperdicio considerable de recursos (electrónicos). Los servidores de correo duplican de manera típica un mensaje electrónico recibido para cada destinatario del mensaje electrónico y llenan los buzones de cada uno de los destinatarios del mensaje electrónico con copias de los mensajes electrónicos. Dado que los mensajes electrónicos spam están dirigidos típicamente a grandes números de destinatarios y estos mensajes de spam representan una parte muy grande del tráfico de mensajes electrónicos, se puede comprender fácilmente el desperdicio de recursos. Los recursos se desperdician de diferentes maneras, por ejemplo, al requerir una capacidad de transmisión más grande de las conexiones de red y un proceso intenso por los servidores para duplicación de correo. Además, se instalan filtros de spam que necesitan ser actualizados regularmente. Los filtros de spam retrasan la transmisión de los mensajes electrónicos como resultado del proceso de filtrado. El “buzón” de los destinatarios del mensaje electrónico está construido dinámicamente a partir del primer servidor o servidores bajo petición del segundo dispositivo de usuario. Los destinatarios pueden informar al sistema sobre posible spam electrónico. La percepción de los seres humanos de un mensaje electrónico es la mejor garantía de reconocimiento de spam. La señal de notificación de spam recibida por el sistema puede iniciar operaciones por el sistema sobre el mensaje electrónico (y posiblemente otros mensajes previos o futuros), el emisor del mensaje electrónico y/o el destinatario o destinatarios de los mensajes electrónicos. La señal de notificación de spam se puede considerar como una orden al sistema del servidor. Se hará referencia a la solicitud de patente internacional pendiente con la actual del propio solicitante (“Procedimiento y sistema para la reducción de la proliferación de mensajes electrónicos”) presentada en la misma fecha de la

presente solicitud.

Un (primer) lector del mensaje electrónico puede calificar un mensaje electrónico como spam y al enviar una señal de notificación de spam puede restringir el acceso al mensaje electrónico para otros destinatarios. Como consecuencia, se ahorran recursos (electrónicos). El solicitante propone una utilización (única) de una señal de notificación de spam desde los usuarios para detectar mensajes spam electrónicos y, al recibir dicha señal de notificación de spam, restringir el acceso al mensaje electrónico correspondiente para otros (usuarios de) dispositivos de usuario. El sistema servidor permite, por lo tanto, que los destinatarios de un mensaje electrónico determinen por sí mismos qué mensajes electrónicos son mensajes spam y que los destinatarios sean capaces como consecuencia de determinar el acceso (derechos) de otros destinatarios a dicho mensaje. Por ejemplo, los otros (usuarios de) dispositivos de usuario pueden no representar o descargar el mensaje electrónico. Los filtros de spam que utilizan conjuntos de normas de reconocimiento de spam, parámetros de spam y criterios de spam, pueden encontrarse ausentes del sistema del servidor, como mínimo, para los mensajes electrónicos para los que se ha recibido una señal de notificación de spam.

Al proporcionar a los destinatarios solamente con una parte (pequeña) del mensaje electrónico en vez del mensaje electrónico completo, se pueden obtener considerables ahorros de recursos. La parte puede ser, por ejemplo, menor de 200 bytes o incluso menos de 100 bytes. La anchura de banda para la transmisión únicamente de estas pequeñas partes del mensaje electrónico es, por lo tanto, inferior y además no se requiere la duplicación del correo. Asimismo, el filtrado de mensajes electrónicos spam no es necesario para estas partes. Si los destinatarios tienen interés en obtener el mensaje electrónico completo, pueden seleccionar la parte del mensaje electrónico para recuperar el mensaje electrónico completo. La parte contiene una clave de recuperación para el mensaje electrónico completo en el primer servidor.

Las realizaciones de las reivindicaciones 2, 3, 13 y 14 definen que la duplicación del mensaje está limitada o queda incluso excluida, resultando en una mejora de la utilización de los recursos (electrónicos).

El primer y segundo servidores pueden ser integrados físicamente o conceptualmente. Un sistema servidor único conectado a múltiples destinatarios de un mensaje electrónico puede proporcionar a los destinatarios solamente una parte del mensaje electrónico antes de facilitar la opción de recuperar el mensaje electrónico completo.

Las realizaciones de las reivindicaciones 5 y 16 definen que la parte o partes del mensaje electrónico también son borradas, por ejemplo, después de haber recibido la señal de notificación de spam. Estas realizaciones pueden ser aplicadas, por ejemplo, por restricción del acceso para el usuario del segundo dispositivo de usuario para conseguir el correspondiente correo electrónico.

La realización de la reivindicación 6 facilita la ventaja de establecer un sistema único para suscritores para la distribución de mensajes electrónicos. Dado que los suscriptores son conocidos, se pueden identificar y excluir de participación los emisores de spam de correo electrónico y otros que utilizan mal el sistema. Además, esta realización permite la identificación de usuarios del sistema servidor.

La realización de la reivindicación 7 impide la posibilidad de averiguar la identidad de participantes en el sistema y transmitir mensajes de correo electrónico bajo una falsa identidad. La comunicación segura se puede conseguir por una o varias técnicas conocidas, tales como codificando datos o proporcionando conexiones de red seguras.

Las realizaciones de las reivindicaciones 8 y 17 proporcionan la ventaja de autorizar a los usuarios restringir acceso a otros mensajes previos y/o futuros desde la misma fuente en base de la identificación de un emisor de un mensaje electrónico para el que se ha recibido una señal de notificación de spam. Se pueden hacer disposiciones para mitigar la severidad de esta medida para el emisor en base a varios parámetros, tales como el número de agresiones por parte del emisor. En particular, el solicitante propone restringir el acceso a otros mensajes electrónicos para destinatarios del mensaje electrónico para el cual se ha recibido, como mínimo, una señal de notificación de spam dependiendo de un historial de comunicación entre dicho emisor y dichos destinatarios de los que se ha recibido una señal de notificación de spam. Por ejemplo, se puede llevar a cabo restricción de acceso a otros mensajes electrónicos inmediatamente si el emisor no es conocido del receptor (por ejemplo, si el emisor y el receptor no han intercambiado previamente mensajes electrónicos). No obstante, si el emisor y el receptor se conocen, el acceso a otros mensajes electrónicos no está restringido de modo inmediato (pero posiblemente solamente después de que se hayan recibido señales de notificación de spam para diferentes mensajes electrónicos).

Las realizaciones de las reivindicaciones 9 y 18 proporcionan la posibilidad de que el sistema envíe una señal de aviso al emisor del mensaje electrónico para el que se ha recibido una señal de notificación de spam. Esto permite proporcionar al emisor información referente a las consecuencias de futuras agresiones. La consecuencia de restringir acceso al sistema se puede obtener por las realizaciones de las reivindicaciones 10 y 19. La consecuencia de no proporcionar por más tiempo acceso al sistema se puede mitigar. En particular, el solicitante propone restringir acceso al sistema para emisores de mensaje electrónico para los que se ha recibido, como mínimo, una señal de notificación de spam dependiendo de la historia de comunicación entre dichos emisor y uno o varios receptores de

los que se ha recibido señal de notificación de spam. Por ejemplo, la restricción de acceso al sistema se puede llevar a cabo inmediatamente si el emisor es desconocido para el receptor (por ejemplo, si el emisor y el receptor no han intercambiado mensajes electrónicos previamente) y el emisor emite una notificación de spam. No obstante, el acceso al sistema no queda restringido inmediatamente como respuesta a una señal de notificación de spam emitida por el dispositivo usuario de un receptor conocido (pero posiblemente solo después de que se han recibido señales de notificación de spam para diferentes mensajes electrónicos). Se hace referencia a una solicitud de patente internacional pendiente con la actual del propio solicitante ("Procedimiento y sistema para restringir acceso a un sistema de mensajes electrónicos") presentado en la misma fecha que la presente solicitud, los contenidos de la solicitud internacional se incorporan a la presente solicitud como referencia en su totalidad.

Desde luego, el sistema puede utilizar filtros de spam además de la funcionalidad descrita en la presente solicitud para reducir la proliferación de mensajes electrónicos. No obstante, el funcionamiento del sistema servidor, tal como se ha definido anteriormente, opera independientemente del funcionamiento de estos posibles filtros de spam.

Las realizaciones de las reivindicaciones 11 y 20 definen la aplicación de bases de datos programables. Las bases de datos programables permiten la programación de respuestas predeterminadas, dependiendo del tipo de petición recibida. Por ejemplo, para notificación de spam, los usuarios pueden llevar a cabo una operación (peticiones) en una base de datos, de manera que la respuesta de la base de datos es, por ejemplo, la restricción de acceso a otros destinatarios del mensaje electrónico, restricción de acceso a otros mensajes electrónicos de la misma fuente y/o exclusión del emisor con respecto al sistema. Además, una base de datos programable permite el control de relaciones con varios parámetros.

A continuación, se describirán realizaciones de la invención de manera detallada. Se debe observar, no obstante, que estas realizaciones no se deben considerar como limitativas del ámbito de protección de la presente invención.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

En los dibujos:
La figura 1 es una representación esquemática de un sistema de acuerdo con una realización de la invención;
La figura 2 es una representación esquemática de un sistema de acuerdo con una realización de la invención;
Las figura 3A y 3B muestran un ejemplo esquemático de un servidor del sistema, según las figuras 1 y 2;
La figura 4 es un diagrama de temporización que muestra un método según una realización de la invención;
La figura 5 es una representación esquemática de un sistema según una realización de la invención;
La figura 6 muestra un diagrama de flujo representando etapas de un procedimiento para reducir la proliferación de mensajes electrónicos para el sistema de comunicación de la figura 5; y
La figura 7 muestra un modelo a título de ejemplo para una base de datos de un servidor de un sistema servidor de acuerdo con una realización de la invención.

DESCRIPCIÓN DETALLADA DE LOS DIBUJOS

La figura 1 muestra un sistema 1 que comprende un primer servidor 2 y un segundo servidor 3 conectados con intermedio de una red 4. El primer servidor 2 está conectado a una primera estación I de usuario. El segundo servidor 3 está conectado a una segunda estación II de usuario y a una estación III de usuario.

Los componentes del sistema 1 están conectados por conexiones de red 5, 6 que se encuentran presentes también en la red 4. La red 4 y las conexiones de red 5 pueden involucrar múltiples redes, cableadas e inalámbricas. La conexión de los dispositivos de usuario I, II y III no es necesariamente directa a los servidores 2 y 3.

El primer, segundo y tercer dispositivos de usuario I, II y III están dispuestos para recibir mensajes electrónicos, tales como, por ejemplo, mensajes de correo electrónico, y pueden ser ordenadores personales, dispositivos de comunicación móviles, etc.

La figura 2 muestra un sistema alternativo 1, en el que los servidores 2 y 3 han sido integrados en un servidor único 2. En este caso, los procesos que se describen más adelante pueden ser procesos internos.

Las figuras 3A y 3B muestran un ejemplo esquemático de un servidor 2 y/o servidor 3 del sistema 1, de acuerdo con las figura 1 y 2. A continuación se supondrá que, si bien no necesariamente, ambos servidores 2 y 3 están dispuestos tal como se describe más adelante.

El servidor 2, 3 comprende un procesador 10, una memoria 11, un adaptador de red 12 para comunicación con el primer, segundo y tercer dispositivos de usuario I, II y III y una base de datos 13. Se debe observar que el servidor 2, 3 es capaz normalmente de conectarse a más de tres dispositivos de usuario I, II y III mostrados en la figura 1.

Las funciones específicas del servidor 2, 3 se han mostrado esquemáticamente en la figura 3B y se describirán a continuación en mayor detalle. Se debe observar que las funciones se pueden implementar ampliamente como partes de código de software como uno o varios programas de ordenador que funcionan en el procesador 10.

El servidor 2, 3 está dispuesto para recibir mensajes electrónicos del primer dispositivo de usuario I.

El servidor 2, 3 comprende un receptor 15 de mensajes electrónicos dispuesto para recibir un mensaje electrónico o una parte del mismo y transmisor 16 de mensajes electrónicos dispuesto para transmitir un mensaje electrónico o una parte del mismo a otro servidor y/o el segundo dispositivo de usuario II y/o el tercer dispositivo de usuario III.

El servidor 2, 3 comprende además una instrucción receptor de señales de instrucciones 17 dispuesta para recibir una señal de instrucción de los segundo y tercer dispositivos II, III para presentar los mensajes electrónicos recibidos en estos dispositivos.

El servidor 2, 3 comprende también un emisor de consultas 18 para enviar una consulta sobre partes de mensajes electrónicos dirigidas al destinatario de las que se ha recibido señal de instrucciones. La consulta del emisor de consultas es recibida por un receptor de consultas 19 dispuesto para proporcionar una parte del mensaje electrónico en base a datos de la base de datos 13 tal como se describirá más adelante de forma detallada. Se debe observar, no obstante, que la parte o partes del mensaje electrónico pueden ser también impulsadas en vez de ser recuperadas mediante una consulta. En este caso, el receptor de consultas 19 puede ser constituido por un impulsor 19 de partes y el emisor de consultas 18 puede ser constituido por un receptor 18 de empuje de partes. La opción de consulta es típicamente más atractiva desde la perspectiva de ahorro de recursos electrónicos.

El servidor 2, 3 puede contener también un receptor 20 de notificación de spam dispuesto para recibir una notificación de spam desde el segundo/tercer dispositivo de usuario II, III relativo al mensaje electrónico o a la parte del mismo. Asimismo, el servidor 2, 3 tiene un restrictor de acceso 21 dispuesto para restringir el acceso al mensaje electrónico para el (usuario del) tercer dispositivo de usuario III en respuesta a recibir dicha señal de notificación de spam desde el segundo dispositivo de usuario II.

El servidor 2, 3 tiene un registro 22 que almacena un único código de registro que comprende un nombre de usuario y una contraseña específica de usuario requerida para acceder al sistema 1 para cada usuario de los dispositivos de usuario I, II y III.

La comunicación mediante las conexiones de red 5, 6 está asegurada. Con este objetivo, el servidor 2, 3 contiene un codificador 23 para codificar una parte o la totalidad de las comunicaciones entre el sistema 1 y el primer, segundo y tercer dispositivos de usuario I, II y III. Se observará que de manera alternativa o adicional, las conexiones de red 5, 6 pueden ser aseguradas. La comunicación segura impide o reduce la posibilidad de averiguar identidades de los (usuarios del) primer, segundo y tercer dispositivos de usuario I, II y III.

El servidor 2, 3 tiene un borrador de correo electrónico 24 para borrar el correo electrónico y las copias y/o partes de las mismas, si existen, como respuesta a la señal de notificación de spam procedente del segundo/tercer dispositivo de usuario II, III.

Además, el servidor 2, 3 tiene un almacenamiento 25 de identificación de emisor dispuesto para almacenar la identificación de emisor de un emisor del mensaje electrónico para el que se ha recibido en el receptor 15 de señal de notificación de spam una señal de notificación de spam, es decir, la identificación del usuario del primer dispositivo de usuario I en el caso actual. Si se han recibido otros mensajes electrónicos (pasados o futuros) o se han recibido de este usuario, el restrictor de acceso 21 puede utilizar la identificación de emisor para restringir el acceso a estos mensajes electrónicos adicionales para el tercer dispositivo de usuario III de manera automática, es decir, sin requerir una notificación de spam adicional para estos mensajes electrónicos adicionales.

El restrictor de acceso 21 puede estar dispuesto de manera tal que, por ejemplo, se restringe acceso para el (usuario del) tercer dispositivo de usuario III durante un periodo de tiempo determinado o para una parte de los otros mensajes electrónicos. No obstante el restrictor de acceso 21 puede también impedir la descarga del mensaje electrónico a dicho tercer dispositivo de usuario III o puede impedir la visualización del mensaje electrónico en el tercer dispositivo de usuario III. Desde luego, las restricciones de acceso para los otros mensajes electrónicos pueden ser aplicables también directamente para el (usuario del) segundo dispositivo II.

En particular, un historial de comunicación entre un emisor y el receptor del que se ha recibido notificación de spam pueden ser tomadas en cuenta. Por ejemplo, si los usuarios del primer dispositivo de usuario I y el segundo dispositivo de usuario II no se han involucrado en intercambio de mensajes electrónicos anteriormente (es decir, los usuarios no se “conocen” entre sí), la recepción de la señal de notificación de spam puede resultar inmediatamente en la prevención de que otros destinatarios descarguen o visualicen otros mensajes electrónicos pasados y futuros. No obstante, si el usuario del primer dispositivo de usuario I y el segundo dispositivo de usuario II han estado involucrados en intercambios de mensajes electrónicos en el pasado (es decir, los usuarios se “conocen” entre sí), las consecuencias de la señal de notificación de spam pueden ser menos graves. Otro ejemplo de usuarios que se “conocen” entre sí puede ser que cada uno de los usuarios ha indicado anteriormente al intercambio de mensajes electrónicos que aceptará mensajes electrónicos del otro.

El servidor 2, 3 puede contener un contador 26 adaptado para contar el número de señales de notificación de spam recibidas para mensajes electrónicos de un emisor particular y/o para el conteo del número de veces que se ha restringido acceso para mensajes electrónicos de dicho emisor.

El servidor 2, 3 comprende un mensaje de aviso por el transmisor 27 adaptado para enviar un mensaje de aviso a un emisor del mensaje electrónico para el que dicha señal de notificación de spam ha sido recibida del segundo dispositivo de usuario II.

El servidor 2, 3 comprende también un restrictor de acceso 28 adaptado para restringir acceso al sistema 1 para un emisor del mensaje electrónico para el que se ha recibido dicha notificación de spam, es decir, el emisor que utiliza el primer dispositivo electrónico I. La restricción del acceso puede comportar la exención del usuario del primer dispositivo I de envío adicional de mensajes electrónicos por el sistema 1. No obstante, el servidor 2, 3 puede comprender un módulo asesor 24 dispuesto para restringir acceso al sistema dependiendo, por ejemplo, del número de señales de notificación de spam recibidas para mensajes electrónicos del emisor y/o el número de veces que el acceso ha sido restringido para mensajes electrónicos del emisor.

En particular, se puede tener en cuenta el historial de comunicación entre un emisor y el receptor para el que se ha recibido señal de notificación de spam. Por ejemplo, si los usuarios del primer dispositivo 1 y el usuario del dispositivo 2 no han estado involucrados en intercambio de mensajes electrónicos anteriormente (es decir, los usuarios no se “conocen” entre sí), la recepción de la señal de notificación de spam puede resultar de inmediato en prevenir del acceso al sistema servidor 1 del emisor. No obstante, si el usuario del primer dispositivo de usuario I ha estado involucrado en intercambio de mensajes electrónicos en el pasado (es decir, si los usuarios se “conocen” entre sí) las consecuencias de la señal de notificación de spam pueden ser menos severas para el usuario del primer dispositivo de usuario I. Otros ejemplos de usuarios que se “conocen” entre sí puede ser que cada uno de los usuarios ha indicado antes de intercambiar mensajes electrónicos que aceptarán mensajes electrónicos uno de otro.

Se debe observar que el servidor 2, 3 puede contener un filtro de spam (no mostrado) que utiliza un juego de normas de spam, parámetros de spam y/o criterios de spam para detectar y posiblemente restringir acceso a mensajes electrónicos spam. No obstante, el servidor 2, 3 es capaz de restringir el acceso al mensaje electrónico para el usuario del segundo/tercer dispositivo II, III y/o al sistema para el emisor del mensaje de spam electrónico independientemente del funcionamiento del filtro de spam, es decir, únicamente en base a una o varias señales de notificación de spam.

Finalmente, el sistema servidor 1 contiene un módulo de aprobación 29 adaptado para permitir el intercambio de mensajes electrónicos entre un emisor, por ejemplo, el usuario del primer dispositivo de usuario I, y un destinatario, por ejemplo, el usuario del segundo/tercer dispositivo de usuario II, III, solamente si tanto el emisor como el destinatario han marcado aprobación para dicho intercambio al módulo de acceso 29 de forma adelantada. El programa de ordenador que funciona en los dispositivos de usuario I, II y III para enviar y recibir mensajes electrónicos puede comprender, por ejemplo, un libro de direcciones obligatorio bajo el control del módulo de acceso 29. Solamente utilizando este libro de direcciones, un usuario puede dirigirse a destinatarios del mensaje electrónico. Las entradas en el libro de direcciones pueden ser realizadas solamente como respuesta a aprobación mutua de usuarios para intercambiar mensajes electrónicos.

La figura 4 es un diagrama de tiempos que muestra un procedimiento llevado a cabo en el sistema 1 de la figura 1 utilizando servidores 2, 3 tal como se ha descrito haciendo referencia a las figuras 3A y 3B. Se debe observar que el método es aplicable también al sistema 1 mostrado en la figura 2. La parte A del diagrama de tiempos muestra las etapas de transmisión del mensaje electrónico desde un primer dispositivo de usuario I a un segundo dispositivo de usuario II. La parte B del diagrama de tiempos muestra las etapas de un método cuando el usuario del segundo usuario II identifica el mensaje electrónico recibido como mensaje spam.

En la etapa 40, el receptor 15 del mensaje electrónico del servidor 2 recibe un mensaje electrónico procedente del primer dispositivo de usuario I a través de la conexión segura de red 5. El mensaje electrónico es dirigido a los usuarios de los dispositivos de usuario II y III. De manera anticipada al envío del mensaje electrónico, el usuario del primer dispositivo de usuario puede haber registrado en el sistema 1 y se ha autentificado utilizando el registro 22. El mensaje electrónico es almacenado en el servidor 2, más particularmente en la base de datos 13, de acuerdo con el modelo de datos mostrado en la figura 7. De modo general, esto significa que el mensaje electrónico recibido es analizado y que diferentes partes del mensaje electrónico son identificadas y almacenadas como campos separados en la base de datos 13. En vez de un mensaje electrónico completo, el mensaje electrónico puede llevar al servidor 2 en campos separados.

En la etapa 41, un usuario del segundo dispositivo de usuario II, que posiblemente se ha registrado también en el sistema 1 utilizando el registro 22, abre su buzón. Al proceder de este modo, el segundo dispositivo de usuario II transmite una señal de instrucción que es recibida por el receptor 17 de señal de instrucción del segundo servidor 3.

Como respuesta a la recepción de la señal de instrucción, un emisor de consultas 18 del segundo servidor 3 emite una consulta al primer servidor 2 referentes a partes de mensajes electrónicos para los que el usuario del segundo

dispositivo de usuario II es el destinatario. Esta etapa se ha mostrado en la etapa 42 en la figura 4.

La consulta es recibida por un receptor de consultan 19 del primer servidor 2. En el primer servidor 2 la consulta es llevada a cabo en la base de datos 13 para proporcionar una parte del mensaje electrónico recibida desde el primer dispositivo de usuario I. La parte puede comprender uno o varios campos almacenados en la base de datos 13 referentes al mensaje electrónico recibido desde el primer dispositivo de usuario. La parte incluye una clave de recuperación que identifica la localización en la que se puede recuperar el mensaje electrónico completo.

En la etapa 43, el transmisor 16 del mensaje electrónico del primer servidor 2 transmite la parte facilitada de este modo del mensaje electrónico del segundo servidor 3 que muestra dicha parte al (usuario del) segundo dispositivo de usuario II. De esta manera, el buzón de usuario del segundo dispositivo de usuario II es constituido dinámicamente, es decir, sustancialmente cada vez que el usuario del segundo dispositivo de usuario II abre su buzón, el sistema 1 es consultado en cuanto a partes de mensajes electrónico (que pueden encontrarse en diferentes servidores) dirigidos a este usuario y las partes recuperadas del buzón.

Tal como se ha observado en lo anterior, la opción de consulta puede ser sustituida por una opción de avance. En esta situación, después de recibir el mensaje electrónico, una parte del mensaje electrónico es transmitida automáticamente al servidor 2. Después de abrir el correo por el usuario del segundo dispositivo II, la parte del mensaje electrónico se encuentra ya presente en el servidor 3.

Si el usuario del segundo dispositivo de usuario II decide que el mensaje electrónico le interesa, puede seleccionar la parte del mensaje electrónico. Después de seleccionar dicha parte, el segundo dispositivo de usuario II inicia un mensaje de selección en la etapa 44 que es recibido por un receptor de mensajes de selección del primer servidor 2 utilizando la clave de recuperación de la parte del mensaje electrónico.

En la etapa 45, el mensaje electrónico completo es recuperado de la base de datos 13 por el segundo dispositivo de usuario II.

Si el primer lector, por ejemplo, el usuario del segundo dispositivo de usuario II, acepta el mensaje electrónico como mensaje deseado, no se recibirá señal de notificación spam por el receptor 20 de notificación de spam del sistema 1. Como consecuencia, el usuario del tercer dispositivo de usuario III puede acceder también al mensaje electrónico.

Si el usuario del segundo dispositivo de usuario II califica el contenido del mensaje electrónico como spam puede transmitir una señal de notificación de spam relativa al mensaje electrónico spam al primer servidor 2. El usuario del segundo dispositivo de usuario II puede, por ejemplo, enviar una notificación de spam al activar un botón específico en un interfaz de usuario del segundo dispositivo de usuario II. La señal de notificación de spam es detectada por el receptor 20 de señal de notificación de spam en el primer servidor 2 en la etapa 50.

El sistema 1 puede llevar a cabo una serie de operaciones como respuesta a la recepción de la señal de notificación de spam desde el segundo dispositivo de usuario II.

El dispositivo 24 de borrado de correo electrónico puede borrar el mensaje electrónico del primer servidor 2, es decir, puede borrar uno o varios campos en la base de datos 13 relativos al mensaje electrónico spam y borrar también la parte del mensaje electrónico en el segundo servidor 3, indicado por la etapa 51.

De manera alternativa o adicional a la etapa 51, el restrictor de acceso 28 puede restringir el acceso al sistema 1 para el (usuario del) primer dispositivo de usuario I, para el que se ha recibido la señal de notificación de spam, tal como se ha indicado en la etapa 52. La restricción del acceso puede comportar la exención del usuario del primer dispositivo I de enviar adicionalmente mensajes electrónicos a través del sistema 1. Dado que dicha medida puede ser desagradable para el usuario del primer dispositivo de usuario I, el acceso al sistema 1 puede ser restringido dependiendo, por ejemplo, del número de señales de notificación de spam recibidas para mensajes electrónicos del emisor y/o del número de veces que se ha restringido el acceso para mensajes electrónicos del emisor, utilizando el contador 26. En particular, si el emisor y el receptor han intercambiado mensajes electrónicos anteriormente, solamente se puede llevar a cabo la restricción de acceso al sistema después de un cierto número de señales de notificación de spam desde un receptor utilizando el contador 26.

Una señal de aviso puede ser transmitida al usuario del primer dispositivo de usuario I por el transmisor 27 de la señal de aviso. La señal de aviso puede indicar a este usuario las consecuencias de continuar proporcionando mensajes electrónicos spam.

Como respuesta a la recepción de la señal de notificación de spam, el restrictor de acceso 21 del primer servidor 2 restringe el acceso para (un usuario de) el tercer dispositivo de usuario III al mensaje electrónico. Un ejemplo de la forma en la que esta realización funcionaría se ha indicado en las etapas 53-55 de la figura 4. En la etapa 53 el usuario del tercer dispositivo de usuario III abre su buzón y se recibe una señal de instrucción por el receptor 17 de señal de instrucción del segundo servidor. Nuevamente se emite una consulta al primer servidor I indicada por la etapa 54. No obstante, dado que el acceso al mensaje electrónico ha sido restringido como respuesta a la recepción

del mensaje de notificación de spam del segundo dispositivo de usuario II, una parte del mensaje electrónico no se puede recuperar de la base de datos 13. Por lo tanto, indicado por la cruz de la etapa 55 de la figura 4, la parte mencionada no será utilizada para construir el buzón del usuario del tercer dispositivo de usuario III. Por lo tanto, el usuario del tercer dispositivo de usuario III no podrá recuperar el mensaje electrónico. En realidad, en la presente realización, el usuario del tercer dispositivo de usuario III no sabrá siquiera que se ha producido el mensaje de spam electrónico.

Otro ejemplo del funcionamiento del sistema 1 como respuesta a la recepción de la señal de notificación de spam incluye lo siguiente. El usuario del primer dispositivo de usuario I que distribuye el mensaje de spam electrónico es conocido para el sistema 1, por ejemplo, al tener almacenado en el registro 22 un único código de registro que comprende un nombre de usuario y una clave específica de usuario requerida para el sistema 1. Utilizando estos datos, el almacenamiento 25 de identificación de emisor puede haber almacenado la identidad del emisor del mensaje electrónico de spam. Si otro mensaje electrónico es enviado o ha sido enviado (no necesariamente un mensaje electrónico de spam) se determina que para este emisor se ha recibido una señal de notificación de spam. El acceso de estos otros mensajes (previos o futuros) del emisor se puede, por lo tanto, rechazar automáticamente. Como consecuencia, ni el segundo dispositivo de usuario II ni el tercer dispositivo de usuario III tendrán acceso a estos otros mensajes electrónicos. Dado que esta medida puede ser más bien desagradable del emisor del mensaje electrónico previo de spam, las consecuencias pueden ser mitigadas permitiendo que el restrictor de acceso 21 restrinja acceso para el (usuario del) segundo dispositivo de usuario II y/o el tercer dispositivo de usuario III durante un determinado periodo de tiempo y/o solamente para una parte de los mensajes electrónicos adicionales. En particular, si el emisor y el receptor han intercambiado anteriormente mensajes electrónicos, el restringir el acceso a otros mensajes electrónicos puede ser llevado a cabo solamente después de un cierto número de señales de notificación de spam desde un receptor, utilizando el contador 21.

La figura 5 muestra un sistema 1 que comprende varios servidores 2A, 2B y 2C en conexión de comunicación entre sí. Los servidores 2A, 2B y 2C forman conjuntamente el sistema 1. Las conexiones 50 que conectan los servidores 1A, 1B y 1C constituyen un anillo interno. El primer, segundo y tercer dispositivos de usuario I, II, y III pueden conectar a diferentes servidores 2A, 2B y 2C de este anillo interno, tal como se ha mostrado en la figura 5, de manera directa o a través de otros servidores (no mostrado). Cada uno de dichos primer, segundo y tercer dispositivos de usuario I, II y III pueden tener acceso también a los servidores 2B y 2C; 2A y 2C y 2A y 2B, respectivamente, sin utilizar el anillo interno formado por las conexiones 50. En la figura 5, este anillo externo formado por las conexiones 51 es válido solamente para el segundo dispositivo de usuario II.

La comunicación se puede asegurar tanto en el anillo interno como en el anillo externo. Esto se puede conseguir al codificar la comunicación a través del anillo interno y el anillo externo y/o utilizando conexiones de seguridad.

Cada uno de los servidores 2A, 2B y 2C del sistema 1 puede contener los mismos módulos funcionales 15-29, tal como se ha descrito con referencia a las figuras 3A, 3B. No obstante, los módulos funcionales pueden ser también distribuidos por los diferentes servidores 2A, 2B y 2C.

A continuación se describirá con referencia a la figura 6 una realización del funcionamiento del sistema 1 de acuerdo con la figura 6.

El usuario del primer dispositivo de usuario I envía un mensaje electrónico de spam al sistema 1 con los usuarios de los dispositivos de usuario II y III como destinatarios.

El receptor 15 del mensaje electrónico del servidor 2A recibe el mensaje electrónico de spam y almacena el mensaje en la base de datos 13 en la etapa 60, tal como se ha descrito anteriormente. De forma breve, en vez de almacenar el mensaje electrónico tal como se realiza en un servidor de correo electrónico convencional se almacenan separadamente partes individuales del mensaje electrónico como campos en un modelo de base de datos (ver la figura 7).

Si el usuario del segundo dispositivo de usuario II abre su buzón, se emite una consulta tanto al primer servidor 1A como al tercer servidor 3 (posiblemente en combinación con una consulta interna en el segundo servidor 2B) para partes de los mensajes electrónicos para los que este usuario es el destinatario. El sistema 1 de servidores 2A, 2B y 2C en combinación con el anillo interno de conexiones 50 se puede considerar técnicamente como una base de datos conceptualmente única a este respecto. Para el mensaje electrónico del dispositivo de usuario I, en la etapa 61, el transmisor de mensajes electrónicos 16 transmite un mensaje electrónico con una parte del primer servidor 2A al segundo servidor 2B. Una parte del mensaje electrónico puede comprender, por ejemplo, un campo de emisor, un campo de sujeto y una calve de recuperación para recuperar el mensaje electrónico completo. El tamaño de datos de la parte del mensaje electrónico puede ser menor de 200 bytes. El mensaje electrónico completo es almacenado solamente en el servidor 1A. Desde luego, la parte de avance para distribuir la parte del mensaje electrónico a los servidores 2B y 2C puede ser utilizada asimismo.

En la etapa 62, la parte es representada al usuario del segundo dispositivo de usuario II. El mensaje electrónico en sí mismo puede ser recuperado en la etapa 63 por el segundo dispositivo de usuario II desde el primer servidor 2A a

través de las conexiones 51 que forman el anillo externo al seleccionar la parte del mensaje electrónico proporcionada desde el segundo servidor 2B.

Si el usuario del segundo dispositivo de usuario II no califica el mensaje electrónico como spam, el usuario del tercer dispositivo III puede acceder al mensaje electrónico igualmente. En este caso, cuando el usuario del tercer dispositivo III abre su buzón, el tercer servidor 2C, consulta los servidores 2A y 2B con respecto a las conexiones 50 para partes de los mensajes electrónicos dirigidos a su cuenta. El primer servidor 2A proporciona al tercer servidor 2C dicha parte y, después de la selección de esta parte, se pueden descargar el mensaje electrónico completo al tercer dispositivo de usuario III (etapa 64). De manera alternativa, la parte puede encontrarse ya a disposición en el tercer servidor 2C si se ha utilizado la acción de empuje o avance.

Si el usuario del segundo dispositivo de usuario II califica el contenido del mensaje electrónico como spam, puede transmitir una señal de notificación de spam con respecto al mensaje electrónico de spam al servidor 2A. El usuario del segundo dispositivo de usuario II puede enviar, por ejemplo, una señal de notificación de spam activando un pulsador específico en un interfaz de usuario del segundo dispositivo de usuario II. La señal de notificación de spam es detectada por el receptor de señal de notificación de spam 20 del primer servidor 1A. Como respuesta a la recepción de la señal de notificación de spam, el restrictor de acceso 21 del servidor 1A restringe el acceso para (un usuario de) el tercer dispositivo de usuario III al mensaje electrónico, indicado por la etapa 55. El borrador 24 del mensaje electrónico del servidor 1A puede borrar, por ejemplo, el mensaje electrónico de spam, de manera que el usuario del tercer dispositivo III no tiene acceso al mensaje electrónico de spam en el primer servidor 1C (o ni siquiera se visualizará una parte del mismo) y dicha parte en el servidor 2B (etapa 66 y 67). El borrador de (partes de) mensaje electrónico es informado mediante el anillo interno de la figura 4.

Tal como se ha mencionado anteriormente, el servidor 2A almacena solamente una única copia del mensaje electrónico independiente del número de destinatarios. Se notifica a los destinatarios del mensaje electrónico por medio de partes que caracterizan el mensaje electrónico de pequeñas dimensiones. Esto ahorra una gran cantidad de recursos, por ejemplo, una gran capacidad de transmisión. No obstante, el sistema 1 puede proporcionar múltiples copias del mensaje electrónico si dicho enfoque se demuestra más efectivo. El número de copias del mensaje electrónico es menor que el número de direcciones de dicho mensaje electrónico.

En cuanto a la realización de las figuras 1 y 2, el usuario del primer dispositivo de usuario I que distribuye el mensaje electrónico de spam puede ser conocido por el sistema servidor 1, por ejemplo, al tener almacenado en el registro 22 del sistema 1 un código único de registro que comprende una dirección de usuario y una clave específica de usuario requerida para el acceso al sistema 1. Utilizando estos datos, el almacenamiento 20 de identificación de emisor ha almacenado la identidad del emisor del mensaje electrónico de spam. Si se envía otro mensaje electrónico (no necesariamente un mensaje electrónico spam), se determina que para este emisor ya se ha recibido anteriormente una señal de notificación de spam. El acceso a estos otros mensajes del emisor puede ser, por lo tanto, denegado para los usuarios de ambos dispositivos II y III. Como consecuencia, ni el (usuario del) segundo dispositivo de usuario II ni el tercer dispositivo de usuario III tendrá acceso a estos otros mensajes electrónicos. Dado que esta medida puede ser más bien desagradable para el emisor del primer mensaje electrónico spam, las consecuencias se pueden mitigar al permitir al restrictor de acceso 21 del primer servidor 2A que restrinja el acceso para el (usuario del) segundo dispositivo de usuario II durante un periodo de tiempo determinado y/o solamente para una parte de los otros mensajes electrónicos.

Se debe apreciar que el registro 22 puede ser compartido por múltiples servidores 1A, 1B y 1C, así como el almacenamiento 20 de identificación de emisor para emisores de mensajes electrónicos spam anteriores.

Asimismo, tal como se ha descrito anteriormente para las realizaciones de las figuras 1 y 2. El sistema 1 puede ser puesto en marcha utilizando la señal de notificación de spam para bloquear el acceso para el usuario del primer dispositivo de usuario I al sistema 1 (incluyendo variantes más ligeras) o el envío de un mensaje de aviso.

Se debe observar que, si bien en el ejemplo anterior una única señal de notificación de spam era suficiente para excluir a otros destinatarios que recibieran (otros) mensajes electrónicos y para excluir un emisor de participación en el sistema, se puede disponer otra serie de señales de notificación spam antes de que sean aplicables dichas consecuencias.

También se debe observar que la historia de comunicación entre un emisor y un receptor puede ser un factor para restringir el acceso a otros mensajes electrónicos y/o al sistema 1.

Los servidores 2A, 2B y 2C del sistema 1 son preferentemente servidores de mensajes electrónicos no convencionales. Estos servidores de correo electrónico almacenan mensajes de correo electrónico, duplican los mensajes de correo electrónico para el número de destinatarios y proporcionan los mensajes de correo electrónico bajo petición para un mensaje específico de aquellos mensajes. La funcionalidad de estos servidores de correo es más bien limitada.

El solicitante propone la utilización de una o varias bases de datos, tales como la base de datos Oracle®, para la

que la respuesta puede ser programada, dependiendo de la petición realizada a la base de datos. Los mensajes electrónicos entrantes son analizados y predeterminadas partes son almacenadas en campos de la base o bases de datos.

La utilización de las bases de datos para los servidores 1A, 1B y 1C permite el controlar las relaciones entre los diferentes campos, tal como se ha mostrado en la figura 7.

La funcionalidad descrita anteriormente se puede obtener utilizando el modelo de base de datos de la figura 7.

Por ejemplo, si un usuario permite una señal de notificación de spam, el estado del receptor y la fecha del estado del receptor son actualizados. Si una única señal de notificación de spam es suficiente para restringir acceso al mensaje electrónico para otros receptores y para restringir el acceso al sistema servidor 1 para un emisor, este estado se propagará al estado de mensaje y al estado de miembro, respectivamente. Al añadir una fecha de estado del mensaje y fecha de estado del miembro, al modelo de datos, se obtiene flexibilidad.

Los campos de la casilla “mensajes” pueden formar parte de la parte del mensaje electrónico que ha sido introducido o consultado en el sistema servidor. Se incluyen entre los ejemplos el propietario/emisor del mensaje, el sujeto del mensaje y la fecha de envío del mensaje. La ID o identificación del mensaje se refiere a la clave de recuperación para recuperar el mensaje electrónico completo.

Se debe observar que cuando no se utiliza una agenda obligatoria para dirigirse a los destinatarios del mensaje electrónico, la casilla “contactos” se puede eliminar en el modelo de la base de datos y se puede establecer un enlace directamente desde la casilla “miembros” a la casilla “receptores”.

El sistema servidor 1 puede contener un módulo de aprobación 25. En este caso, el sistema servidor 1 puede estar configurado de forma tal para todos los participantes que cualquiera y todas las informaciones dirigidas a ellos como participantes no puedan alcanzarlos y antes de la primera comunicación dentro del sistema entre dos participantes A y B, los dos participantes A y B tendrán que pasar primero por un protocolo de disposición/aprobación.

REIVINDICACIONES

1. Sistema para la transmisión de un mensaje electrónico desde un primer dispositivo de usuario a un segundo dispositivo de usuario y a un tercer dispositivo de usuario, cuyo sistema comprende, como mínimo, un primer servidor y un segundo servidor conectables en comunicación entre sí, de manera que el primer dispositivo de usuario es conectable al primer servidor y el segundo dispositivo de usuario y el tercer dispositivo de usuario son conectables al segundo servidor:
estando dispuesto el primer servidor para:
- recibir y almacenar el mensaje electrónico procedente del primer dispositivo de usuario dirigido al segundo dispositivo de usuario y al tercer dispositivo de usuario;
- recibir una consulta para una parte del mensaje electrónico desde el segundo servidor;
- transmitir una parte del mensaje electrónico al segundo servidor; y
- transmitir el mensaje electrónico al segundo dispositivo de usuario después de la selección de dicha parte de dicho mensaje electrónico en dicho segundo dispositivo de usuario, y en el que
el segundo servidor está dispuesto para:
- emitir una consulta para la parte del mensaje electrónico como respuesta a la recepción de una señal de instrucción desde el segundo dispositivo de usuario;
- recibir dicha parte de dicho mensaje electrónico desde dicho primer servidor como respuesta a la consulta, y
- presentar dicha parte de dicho mensaje electrónico de manera seleccionable a dicho segundo dispositivo de usuario
en el que el primer servidor está dispuesto además para:
- recibir una señal de notificación de spam relativa al mensaje electrónico almacenado procedente del segundo dispositivo de usuario; y
- en respuesta a la recepción de la señal de notificación de spam, evitar el envío de una parte del mensaje electrónico completo al segundo servidor como respuesta a una consulta para la parte del mensaje desde el segundo servidor como respuesta a una señal de instrucción desde el tercer dispositivo de usuario.

2. Sistema, según la reivindicación 1, siendo dirigido dicho mensaje electrónico a una serie de destinatarios, utilizando una serie de dispositivos de usuario, en el que dicho sistema está dispuesto para duplicar dicho mensaje electrónico, de manera que el número resultante de mensajes electrónicos almacenados en el primer servidor es menor que el número de destinatarios de dicho mensaje electrónico.

3. Sistema, según la reivindicación 1, siendo dirigido dicho mensaje electrónico a una serie de destinatarios, utilizando una serie de dispositivos de usuario, en el que dicho sistema está dispuesto de manera tal que solamente dicho primer servidor almacena dicho mensaje electrónico.

4. Sistema, según la reivindicación 1, en el que dicho primer servidor está dispuesto para borrar dicho mensaje electrónico.

5. Sistema, según una o varias de las reivindicaciones anteriores, en el que dicho primer servidor está dispuesto para transmitir una señal de borrado a dicho segundo servidor para borrar dicha parte del mensaje electrónico para dicho segundo dispositivo de usuario.

6. Sistema, según una o varias de las reivindicaciones anteriores, en el que dicho sistema comprende un registro con información de registro de usuario del primer, segundo y tercer dispositivos de usuario.

7. Sistema, según una o varias de las reivindicaciones anteriores, en el que dicho sistema es un sistema seguro.

8. Sistema, según una o varias de las reivindicaciones anteriores, en el que dicho primer servidor está dispuesto para:
- almacenar datos de identificación del usuario de dicho primer dispositivo como respuesta a la recepción de una señal de notificación de spam desde dicho segundo dispositivo con respecto a dicho mensaje electrónico;
- restringir acceso, como mínimo, a otro mensaje electrónico de dicho usuario del primer dispositivo de usuario utilizando dichos datos de identificación.

9. Sistema, según una o varias de las reivindicaciones anteriores, en el que dicho sistema está dispuesto además para enviar un mensaje de aviso a dicho primer dispositivo de usuario como respuesta a recibir una señal de notificación de spam desde dicho segundo dispositivo de usuario.

10. Sistema, según una o varias de las reivindicaciones anteriores, en el que dicho sistema está dispuesto además para restringir acceso a dicho sistema para un usuario de dicho primer dispositivo de usuario como respuesta a la recepción de la señal de notificación de spam desde dicho segundo dispositivo de usuario.

11. Sistema, según una o varias de las reivindicaciones anteriores, en el que dichos primer y segundo servidores comprenden bases de datos programables.

12. Procedimiento para la transmisión de un mensaje electrónico desde un primer dispositivo de usuario a un segundo dispositivo de usuario y un tercer dispositivo de usuario, que comprende las siguientes etapas:
- recibir y almacenar un mensaje electrónico procedente del primer dispositivo de usuario, dirigido al segundo dispositivo de usuario y al tercer dispositivo de usuario, por un primer servidor;
- recibir una señal de instrucción de dicho segundo dispositivo de usuario por un segundo servidor;
- emitir una consulta para una parte del mensaje electrónico desde el segundo servidor al primer servidor como respuesta a la recepción de una señal de instrucción;
- transmitir una parte de dicho mensaje electrónico desde el primer servidor al segundo servidor;
- presentar dicha parte de dicho mensaje electrónico de manera seleccionable desde el segundo servidor al segundo dispositivo de usuario;
- transmitir dicho mensaje electrónico desde dicho primer servidor a dicho segundo dispositivo de usuario como respuesta a la selección de dicha parte de dicho mensaje electrónico y dicho segundo dispositivo de usuario;
- recibir en el primer servidor una señal de notificación de spam relativa al mensaje electrónico almacenado desde el segundo dispositivo electrónico
- recibir una señal de instrucción desde dicho tercer dispositivo de usuario por el segundo servidor para emitir una consulta para la parte del mensaje electrónico cuando se ha recibido en dicho primer servidor la mencionada señal de notificación desde spam,
- como respuesta a la señal de notificación, evitar el envío de la parte del mensaje electrónico al segundo servidor como respuesta a la consulta siguiendo la señal de instrucción desde el tercer dispositivo de usuario.

13. Procedimiento, según la reivindicación 12, que comprende además la etapa de duplicar dicho mensaje electrónico en dicho primer servidor, de manera que el número resultante de mensajes electrónicos es menor que el número de destinatarios de dicho mensaje electrónico.

14. Procedimiento, según la reivindicación 12, que comprende además la etapa de almacenar dicho mensaje electrónico solamente una vez en dicho primer servidor.

15. Procedimiento, según una o varias de las reivindicaciones anteriores 13 ó 14, que comprende además la etapa de borrar dicho mensaje electrónico en dicho primer servidor después de recibir la notificación de spam.

16. Procedimiento, según las reivindicaciones 12 a 15, que comprende además la etapa de transmitir una señal de borrado a dicho segundo servidor para borrar una parte de dicho mensaje electrónico para dicho segundo dispositivo de usuario.

17. Procedimiento, según una o varias de las reivindicaciones 12 a 16, que comprende además las etapas de:
- almacenar datos de identificación de un usuario del primer dispositivo de usuario como respuesta a la recepción de una o varias señales de notificación de spam desde dicho segundo dispositivo de usuario relativo a dicho mensaje electrónico.
- restringir el acceso, como mínimo, a otro mensaje electrónico adicional de dicho usuario del primer dispositivo de usuario utilizando dichos datos de identificación de usuario.

18. Procedimiento, según una o varias de las reivindicaciones 12 a 17, que comprende además la etapa de enviar un mensaje de aviso a dicho primer usuario como respuesta a recibir una señal de notificación de spam desde dicho segundo dispositivo de usuario.

19. Procedimiento, según una o varias de las reivindicaciones 12 a 18, que comprende además la etapa de restringir el acceso a dicho sistema para un usuario de dicho primer dispositivo de usuario como respuesta a la recepción de una señal de notificación de spam desde dicho segundo dispositivo.

20. Procedimiento, según una o varias de las reivindicaciones 12 a 19, que comprende además la etapa de llevar a cabo el funcionamiento, como mínimo, de dicho primer servidor como base de datos programable.

21. Programa de ordenador que comprende partes de código de software adaptadas, una vez instaladas y en funcionamiento en un sistema electrónico, para llevar a cabo el método según una o varias de las reivindicaciones 12-20.

22. Soporte que contiene el programa de ordenador según la reivindicación 21.

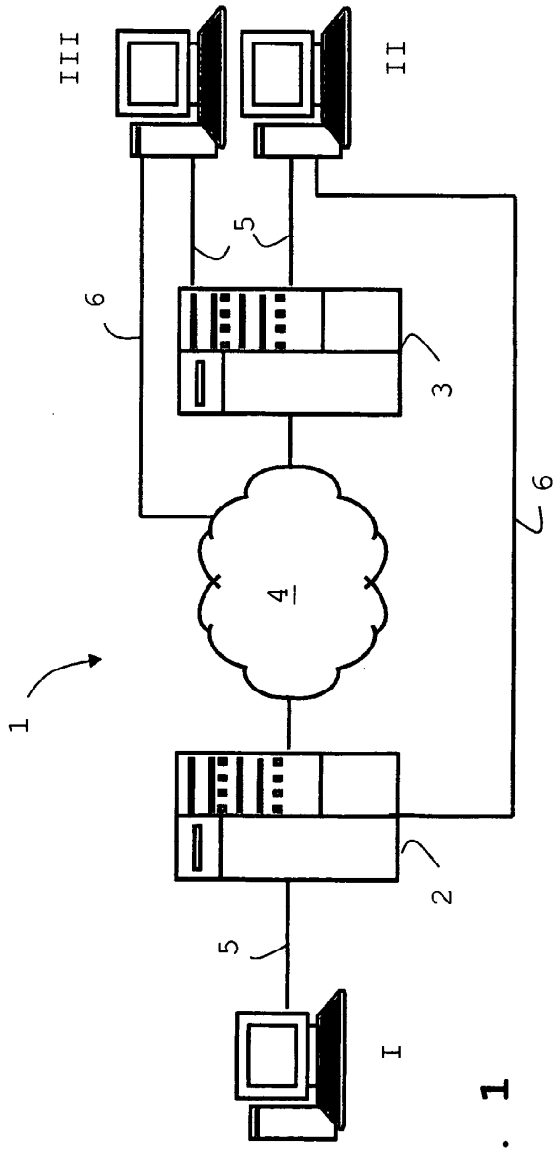

FIG. 1

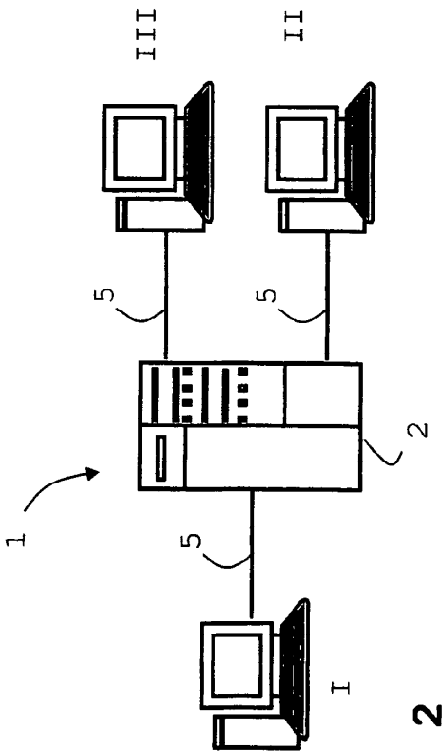

FIG. 2

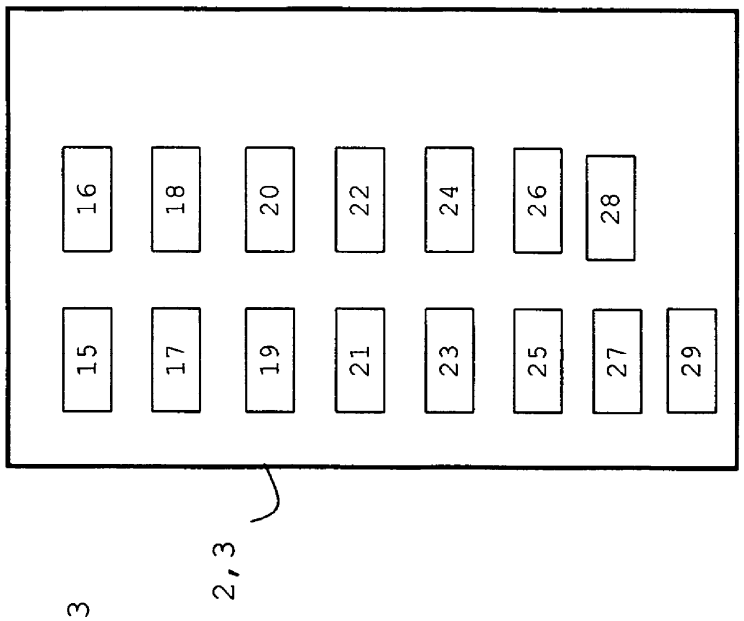

FIG. 3B

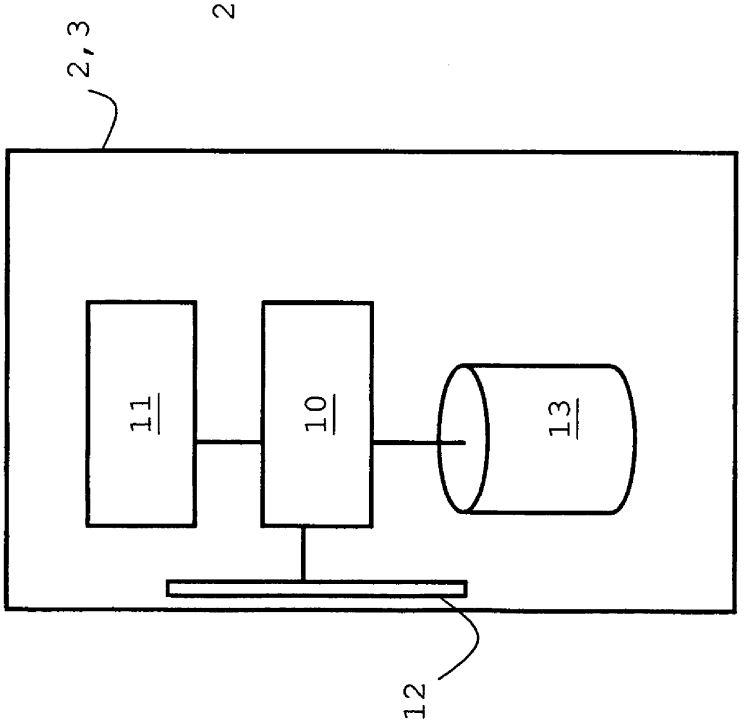

FIG. 3A

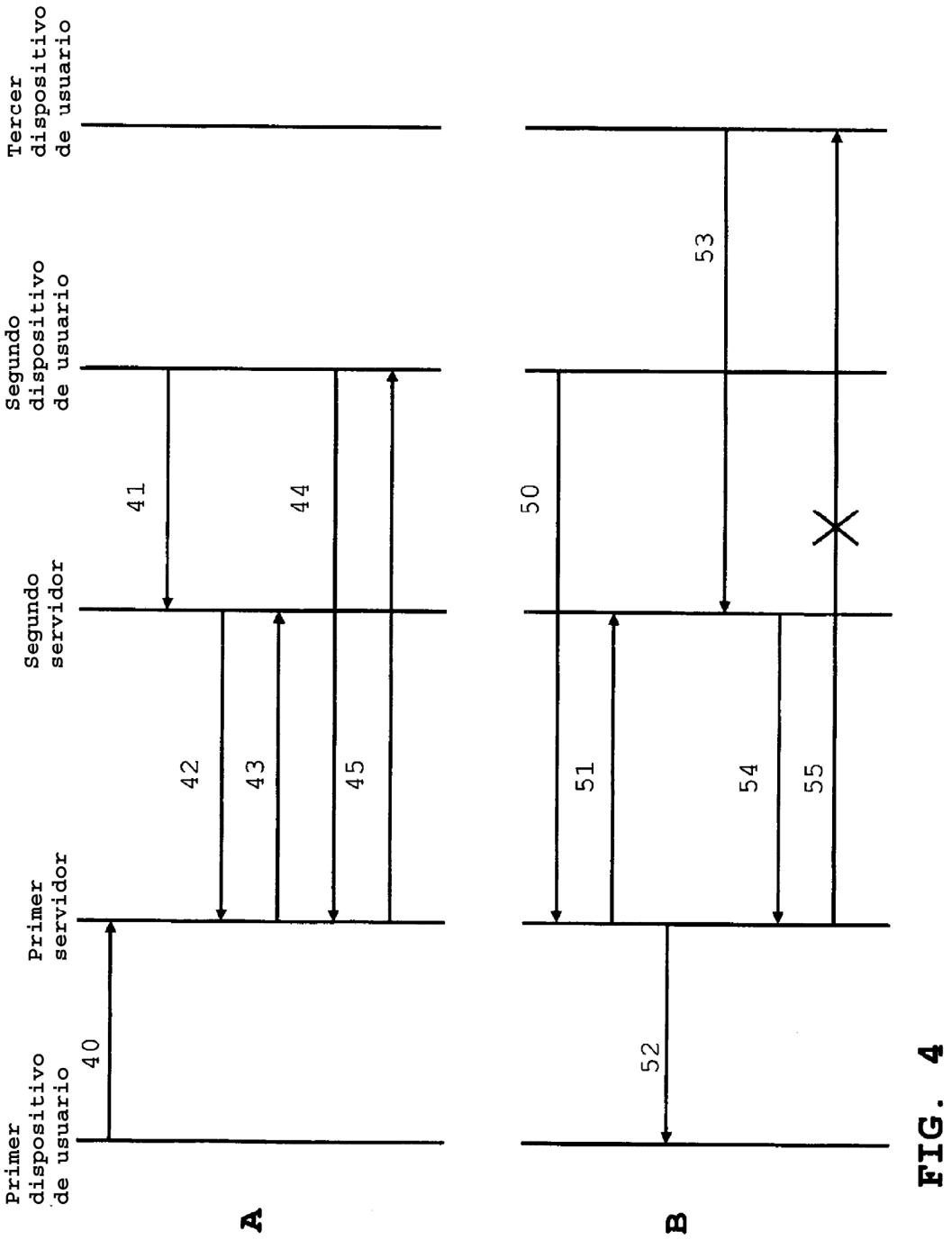
Primer dispositivo de usuario
Primer servidor
Segundo servidor
Segundo dispositivo de usuario
Tercer dispositivo de usuario
40
41
42
43
44
45
A
50
51
52
53
54
55
B

FIG. 4

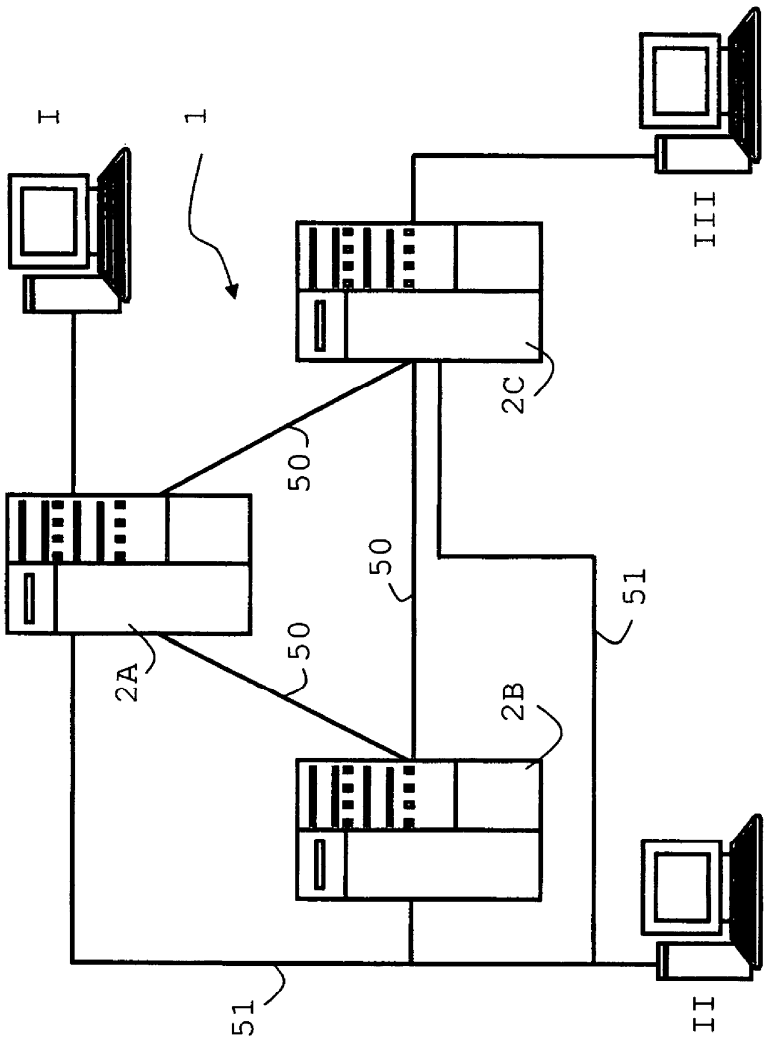

Fig. 5

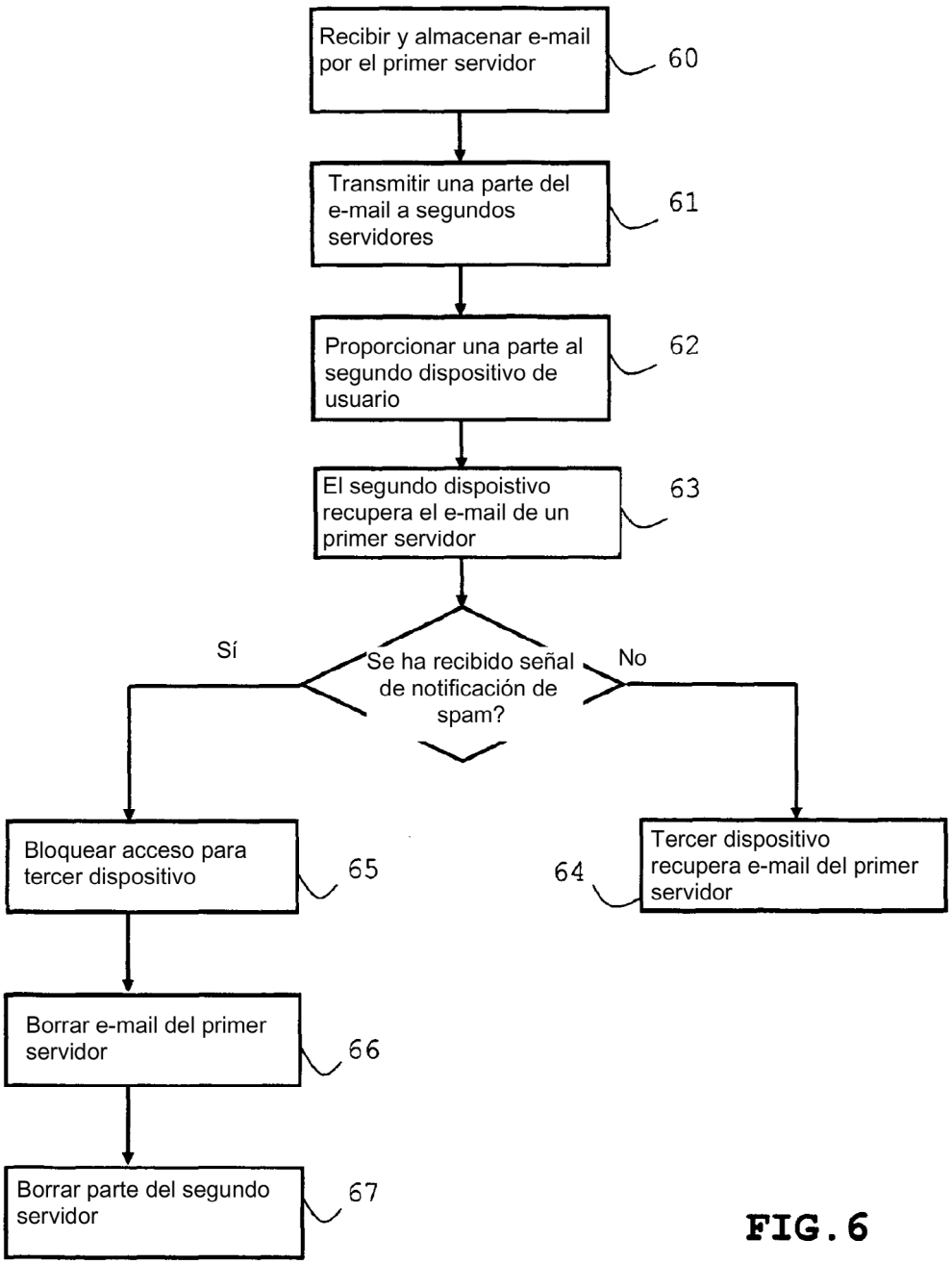
Recibir y almacenar e-mail por el primer servidor
60
Transmitir una parte del e-mail a segundos servidores
61
Proporcionar una parte al segundo dispositivo de usuario
62
El segundo dispoistivo recupera el e-mail de un primer servidor
63
Se ha recibido señal de notificación de spam?
Sí
No
Bloquear acceso para tercer dispositivo
65
Borrar e-mail del primer servidor
66
Borrar parte del segundo servidor
67
64
Tercer dispositivo recupera e-mail del primer servidor

FIG.6

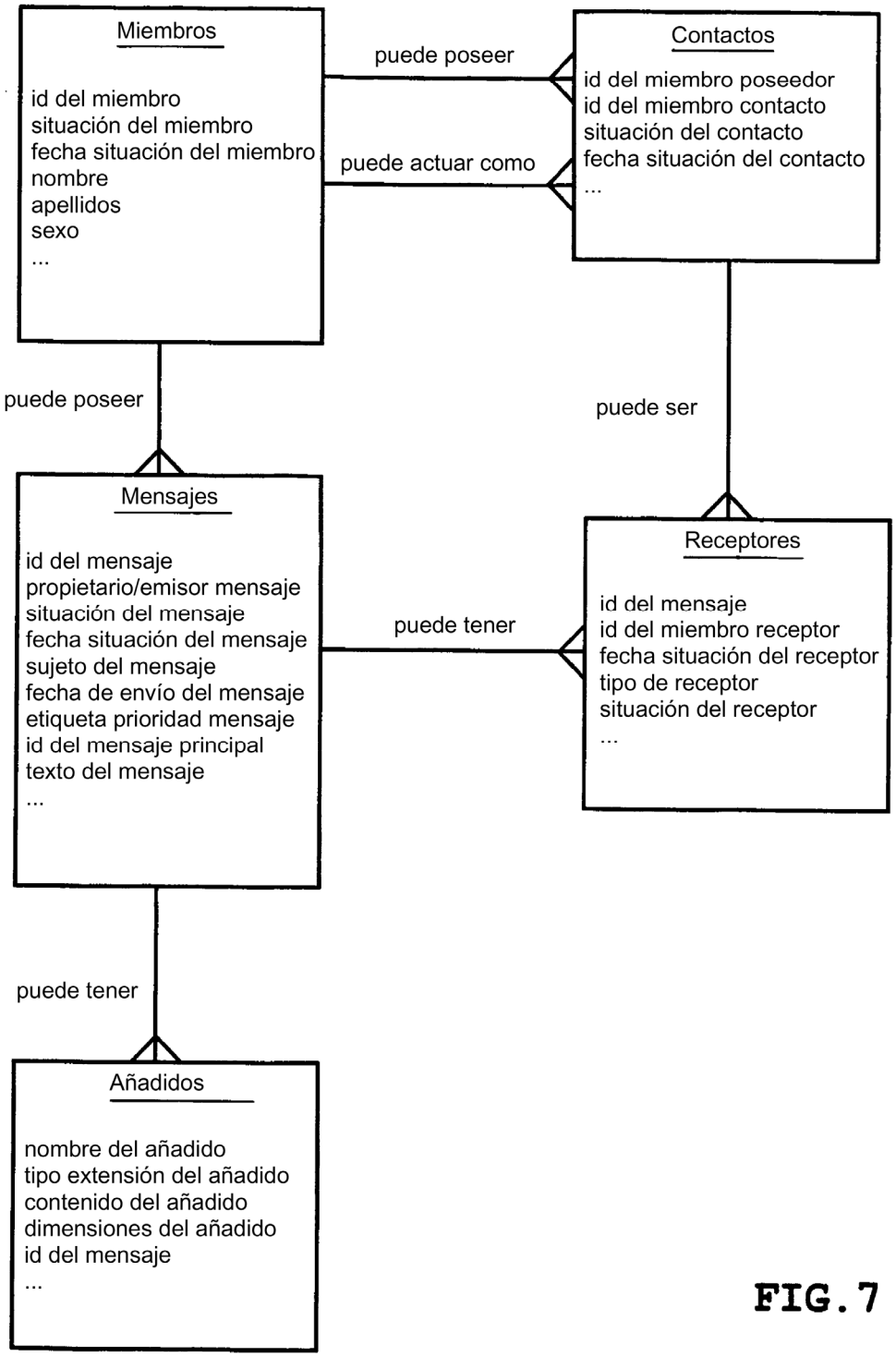
Miembros
id del miembro
situación del miembro
fecha situación del miembro
nombre
apellidos
sexo
...
puede poseer
puede actuar como
Contactos
id del miembro poseedor
id del miembro contacto
situación del contacto
fecha situación del contacto
...
puede poseer
puede ser
Mensajes
id del mensaje
propietario/emisor mensaje
situación del mensaje
fecha situación del mensaje
sujeto del mensaje
fecha de envío del mensaje
etiqueta prioridad mensaje
id del mensaje principal
texto del mensaje
...
puede tener
Receptores
id del mensaje
id del miembro receptor
fecha situación del receptor
tipo de receptor
situación del receptor
...
puede tener
Añadidos
nombre del añadido
tipo extensión del añadido
contenido del añadido
dimensiones del añadido
id del mensaje
...

FIG.7