(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 362 743**

(51) Int. Cl.:
G06Q 10/00 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **06841209 .7**
(96) Fecha de presentación : **29.12.2006**
(97) Número de publicación de la solicitud: **1969544**
(97) Fecha de publicación de la solicitud: **17.09.2008**

(54) Título: **Sistema de comunicaciones para el envío de mensajes de correo electrónico.**

(30) Prioridad: **29.12.2005 EP 05028663**
29.12.2005 US 754729 P

(45) Fecha de publicación de la mención BOPI:
12.07.2011

(45) Fecha de la publicación del folleto de la patente:
12.07.2011

(73) Titular/es: **REGIFY AG.**
Romerstrasse 39
78183 Hüfingen-Behla, DE

(72) Inventor/es: **Schmid, Volker**

(74) Agente: **Isern Jara, Jorge**

DESCRIPCIÓN

Sistema de comunicaciones para el envío de mensajes de correo electrónico.

La invención se refiere a un sistema de comunicaciones.

La invención se refiere, además, a un método de comunicaciones.

Además, la invención se refiere al elemento de programa.

Además, la invención se refiere a un soporte que puede ser leído por ordenador.

Además, la invención se refiere a una unidad de control.

En la actualidad, la comunicación electrónica se ha hecho cada vez más popular. El documento US 2005/0021963 A1 da a conocer un sistema y método para llevar a cabo la transmisión, recepción y contenido de una contestación a un mensaje electrónico. Un servidor recibe un mensaje procedente de un emisor y transmite el mensaje a un receptor. El servidor recibe del receptor una incorporación como indicación de la apertura del mensaje en el receptor y relativo a la ruta del mensaje entre el servidor y el receptor. El servidor transmite al emisor el mensaje y la incorporación y sus huellas digitales codificadas y cancela la información transmitida. Para autentificar posteriormente el mensaje y la incorporación, el emisor envía al servidor lo que previamente ha enviado el servidor al emisor. El servidor prepara a continuación una huella dactilar digital del mensaje y decodifica la huella dactilar digital codificada del mensaje y compara estas huellas dactilares digitales para autentificar el mensaje. El servidor lleva a cabo la misma rutina con respecto a la incorporación y a la huella dactilar digital codificada de la incorporación para autentificar esta última.

El documento US 6.904.521 B1 da a conocer un sistema para enviar un correo electrónico codificado. El sistema comprende un emisor, un receptor y un árbitro. El emisor codifica un mensaje y lo envía al receptor. Mientras tanto, el emisor ha enviado, también la información de decodificación al servidor árbitro, cuya información es almacenada por dicho servidor árbitro para su posterior utilización. Cuando el receptor intenta abrir el mensaje de correo electrónico codificado, el programa de correo electrónico del cliente receptor envía una petición al servidor árbitro para la decodificación de la información. Como respuesta a esta petición, el servidor árbitro devuelve la información decodificada solicitada al receptor y crea una prueba que no puede ser rechazada por el receptor de que el receptor ha intentado abrir el mensaje de correo electrónico.

El documento US 6158003 da a conocer un método para la transmisión de un mensaje codificado desde un emisor a un receptor con el intermedio de un sistema de certificación. De esta manera, el sistema de certificación proporciona al emisor una clave pública. El emisor codifica el mensaje, genera una suma de comprobación y proporciona la suma de comprobación al sistema de certificación. El emisor transmite el mensaje codificado al receptor.

Es un objetivo de esta invención posibilitar una comunicación eficaz.

A efectos de conseguir el objetivo definido anteriormente, se da a conocer un sistema de comunicaciones, un método de comunicación, un elemento de programa, un soporte legible por ordenador y una unidad de control, de acuerdo con las reivindicaciones independientes.

De acuerdo con una realización a título de ejemplo de la invención, se da a conocer un sistema de comunicaciones que comprende una unidad emisora, una unidad de receptor y una unidad de control, de manera que la unidad emisora está adaptada para generar un mensaje electrónico, para enviar el mensaje electrónico directamente a la unidad del receptor y para enviar un mensaje de información de envío a la unidad de control indicando que la unidad emisora ha enviado el mensaje electrónico a la unidad del receptor, de manera que la unidad del receptor está adaptada para recibir el mensaje electrónico directamente de la unidad emisora y para enviar un mensaje de información de recepción a la unidad de control, indicando el mensaje de información de recepción que el usuario de la unidad del receptor ha recibido el mensaje electrónico.

De acuerdo con otra realización a título de ejemplo de la invención, se da a conocer un método de comunicación, cuyo método comprende la generación del mensaje electrónico por medio de una unidad emisora, enviar el mensaje electrónico desde la unidad emisora directamente a una unidad receptora, enviando un mensaje de envío de la información de la unidad emisora a una unidad de control indicando que, la unidad emisora ha enviado el mensaje electrónico a la unidad receptora, recibiendo, por medio de la unidad receptora, el mensaje electrónico directamente de la unidad emisora y enviar un mensaje de información de recepción de la unidad receptora a la unidad de control, indicando el mensaje de información de recepción que un usuario de la unidad receptora ha recibido el mensaje electrónico.

De acuerdo con otra realización, también a título de ejemplo de la invención, se da a conocer un elemento de programa que cuando es ejecutado por el sistema de comunicaciones reivindicado, está adaptado para controlar o

para llevar a cabo el método de comunicaciones reivindicado que tiene las características anteriormente mencionadas.

De acuerdo con otra realización adicional de la invención, se da a conocer un soporte que puede ser leído por ordenador, en el que se ha almacenado un programa de ordenador que cuando es ejecutado por el sistema de comunicaciones reivindicado, está adaptado para controlar o para llevar a cabo el método de comunicación reivindicado que tiene las características anteriormente mencionadas.

De acuerdo con un ejemplo, se da a conocer una unidad emisora en la que la unidad emisora está adaptada para generar un mensaje electrónico, enviar el mensaje electrónico directamente a una unidad receptora y para enviar un mensaje de información a una unidad de control indicando que la unidad emisora ha enviado el mensaje electrónico a la unidad receptora.

De acuerdo con otro ejemplo, se da a conocer una unidad receptora en la que la unidad receptora está adaptada para recibir un mensaje electrónico directamente desde una unidad emisora y para enviar un mensaje de información recibida a una unidad de control, indicando el mensaje de información recibida que el usuario de la unidad receptora ha recibido el mensaje electrónico.

De acuerdo con otra realización adicional a título de ejemplo de la invención, se da a conocer una unidad de control, de manera que la unidad de control está adaptada para recibir un mensaje de información de envío procedente de una unidad emisora, indicando el mensaje de información de envío que la unidad emisora ha enviado el mensaje electrónico a una unidad receptora y para recibir un mensaje de información de recepción desde la unidad receptora, indicando el mensaje de información de recepción que el usuario de la unidad receptora ha recibido el mensaje electrónico.

La comunicación de acuerdo con realizaciones de la invención, se puede realizar por un programa de ordenador, es decir, mediante software, o utilizando uno o varios circuitos de optimización electrónica especiales, es decir, en forma de hardware o en forma híbrida, es decir, por medio de componentes de software y componentes de hardware.

De acuerdo con una realización a título de ejemplo de la invención, se da a conocer un esquema de comunicaciones entre una unidad emisora, una unidad receptora y una unidad de control. La unidad emisora y la unidad receptora intercambian mensajes de comunicación bajo el control de la unidad de control. En este contexto, la unidad emisora envía un mensaje electrónico directamente, es decir, sin ningún elemento intermedio, a la unidad receptora para su recepción. Esto puede permitir un procedimiento de comunicación simple y rápida. No obstante, a efectos de control y de seguridad, la unidad emisora indica a la unidad de control la transmisión del mensaje electrónico a la unidad receptora. Además, la unidad receptora puede confirmar el recepción del mensaje electrónico devolviendo un mensaje correspondiente a la unidad de control. La unidad de control puede informar a continuación a la unidad emisora (y bajo que circunstancias, por ejemplo, en qué momento) de que el mensaje electrónico ha sido abierto por el usuario de la unidad receptora. Al tomar estas medidas, toda la información referente a la comunicación (por ejemplo, información de identificación, información de tiempo, información de codificación, etc.) se puede almacenar centralmente, se puede evaluar y gestionar en la unidad de control que tiene información apropiada de las circunstancias de la comunicación.

Esto puede permitir un sistema de comunicaciones seguro, rápido y adecuado para los usuarios. Al enviar el mensaje electrónico directamente desde el emisor al receptor sin direccionado sobre la unidad de control, se pueden mantener reducidas las capacidades necesarias de almacenamiento y de proceso. Además, el sistema de “triángulo” puede funcionar de manera segura, dado que las rutas de transmisión para el mensaje real y para la clave de descodificación se pueden separar.

El término “directo” puede describir, especialmente, una comunicación entre la unidad emisora y la unidad receptora que no necesita ningún elemento intermedio, de manera que el mensaje electrónico puede ser transmitido entre el lugar del emisor y el lugar del receptor sin otros servicios intermedios. Por lo tanto, puede ser posible que el mensaje transmitido directamente sea enrutado por nodos de una red de comunicaciones, pero habitualmente no es procesado (por ejemplo, almacenado y enviado) por un elemento intermedio. Por lo tanto, es posible que ningún elemento intermedio tenga posesión del mensaje.

Este sistema puede permitir especialmente proporcionar un sistema de correo electrónico registrado, adecuado para los usuarios, que puede hacer posible con un simple cliqueo de un ratón de ordenador, generar un correo electrónico registrado con característica de confirmación de recepción. Por lo tanto, el sistema puede combinar de manera simple las ventajas de un correo postal tradicional registrado con las ventajas de tiempo y coste de la comunicación electrónica. Para el emisor de un correo electrónico confidencial, el envío es muy fácil, y lo mismo es cierto para el receptor cuando abra su correo electrónico registrado personal.

Además, es posible que el emisor y/o receptor trabajen con un servicio convencional de correo electrónico, sin necesidad de modificación alguna en base al interfaz del usuario. Por ejemplo, el sistema puede ser compatible con sistemas de gestión convencionales de correo electrónico tales como “Microsoft Outlook™”.

Por lo tanto, es posible para el emisor enviar mensajes de manera simple con un elevado grado de control de recepción. En particular, una transferencia codificada puede mejorar el nivel de seguridad cuando se envía un mensaje confidencial. Se puede obtener, por parte del emisor, una ventaja de tiempo y de costes. Además, el interfaz emisor puede ser independiente de un programa de correo o de un proveedor de red.

Cuando se transmite ese tipo de mensaje por medio de un correo electrónico a un receptor, el receptor puede simplemente abrir el mensaje, por ejemplo, con un lector convencional tal como “Acrobat Reader ™”. La transferencia puede ser codificada y se pueden obtener asimismo ventajas de coste y de tiempo para el receptor. Además, también la operativa en el lado del receptor puede ser independiente de un programa de correo específico o del operador de la red.

Haciendo referencia nuevamente al emisor, el sistema, según las realizaciones de la invención, asegura que el receptor entra en conocimiento del importante mensaje electrónico del emisor. El emisor recibe una confirmación automática y tiene, por lo tanto, la posibilidad de reaccionar de acuerdo con el correspondiente grado de urgencia.

El emisor puede generar el correo electrónico registrado como correo electrónico normal, por ejemplo, utilizando un cliente convencional de correo electrónico o, de manera alternativa, un cliente específicamente ajustado del correo electrónico en el que se puede integrar el sistema de correo electrónico registrado.

El sistema puede empaquetar el correo electrónico incluyendo su incorporación automáticamente en un archivo electrónico que puede ser codificado. Este archivo puede ser enviado como correo electrónico convencional y puede ser recibido por el receptor de forma directa. Tan pronto como el receptor abre el archivo, el emisor puede recibir un mensaje de confirmación incluyendo el momento en el que el receptor ha abierto realmente el mensaje. En el caso de que el correo electrónico no ha sido abierto por el receptor dentro de un periodo de tiempo que puede ser definido por el usuario de la unidad emisora, se puede suministrar al emisor una confirmación automática.

El receptor puede recibir el correo electrónico registrado como correo electrónico y, por lo tanto, está capacitado para trabajar con este correo electrónico. Al abrir el archivo-contenedor incorporado por el receptor, el emisor puede entrar en conocimiento automáticamente de que se ha recibido un mensaje importante por el receptor y que el receptor ha tomado incorporación del mensaje.

El receptor puede recibir el correo electrónico registrado electrónicamente en forma de un correo electrónico común. No obstante, este correo electrónico común puede tener una incorporación que incluye el archivo transmitido desde el emisor. Por ejemplo, el doble cliqueo de un elemento de incorporación puede iniciar automáticamente una aplicación de lectura, por ejemplo, un lector de “shareware” o el “Acrobat Reader™”.

El lector puede abrir automáticamente y puede decodificar la incorporación. El contenido del mensaje electrónico se encuentra en este momento disponible para el receptor. Al abrir el mensaje electrónico, el receptor inicia automáticamente la transmisión de un mensaje de confirmación de recepción de manera que el emisor puede tomar incorporación de la recepción del mensaje electrónico por el receptor.

La transmisión del mensaje electrónico puede ser llevada a cabo empezando desde la unidad emisora y alcanzando la unidad receptora. El transporte del mensaje electrónico puede encontrarse libre de cualquier agente intermedio, particularmente, se puede llevar a cabo con el intermedio de una ruta de transmisión que no incluye la unidad de control. El transporte puede ser puramente electrónico (por ejemplo, por medio de un correo electrónico enviado desde la unidad emisora a la unidad receptora), puede ser puramente no electrónico (por ejemplo, generando una copia del mensaje al imprimirlo por la unidad emisora, transportando la copia físicamente a la unidad receptora y escaneando el mensaje nuevamente en forma electrónica en el lugar de la unidad receptora) o puede ser parcialmente electrónico (por ejemplo, al copiar el mensaje en un lápiz USB, transportar el lápiz USB físicamente a la unidad receptora y copiar el mensaje desde el lápiz USB a una unidad de almacenamiento de la unidad receptora). No obstante, la unidad de control puede ser dispuesta, funcionalmente y/o físicamente, fuera de una ruta de transmisión o transmitiendo el mensaje entre el emisor y el receptor. La unidad de control puede servir entonces, como agente coordinador y/o autentificador, pero no contribuye a la transmisión del mensaje electrónico propiamente dicho. Como consecuencia, un proveedor del sistema de servicio puede resultar independiente de cualquier canal de transmisión y la flexibilidad del sistema puede ser mejorada. El mensaje electrónico puede ser transmitido en cualquier forma, por ejemplo, como MMS o por un lápiz USB o una tarjeta de memoria “flash”.

Se puede desear que el mensaje electrónico sea recibido por un receptor determinado, que puede ser designado también como “destinatario”. No obstante, puede ocurrir que el receptor real, que puede ser designado también como el” receptor” sea distinto del destinatario. En esta situación, el receptor no autorizado puede verse impedido de

acceso al contenido del mensaje electrónico al decodificar el mensaje electrónico o al proporcionar al usuario una clave de decodificación necesaria solamente después de una autentificación apropiada.

El sistema de comunicación, de acuerdo con una realización a título de ejemplo de la invención, se puede implementar también, mediante una red de telecomunicación (por ejemplo, por cable o sin cable). En este caso, la unidad emisora y/o la unidad receptora puede ser un teléfono, por ejemplo, un teléfono móvil.

También es posible integrar una o varias etiquetas RFID en el sistema de comunicación.

De acuerdo con una realización a título de ejemplo, el archivo-contenedor puede incluir, además del mensaje, otra incorporación de software. Cuando se accede al archivo-contenedor en el lado del receptor, por ejemplo, por doble cliqueo, el mensaje puede ser abierto y simultáneamente se puede llevar a cabo la incorporación de software. Esto puede poner en marcha una instalación de un componente correspondiente de software en la unidad receptora. Por ejemplo, se puede instalar un lector necesario para presentar el mensaje. Adicionalmente o alternativamente, se puede abrir una ventana de registro que permite al receptor registrarse así mismo en el sistema de comunicación, por ejemplo, mediante comunicación con la unidad de control.

En lo que respecta al registro de emisor y/o receptor antes de utilizar el sistema de comunicación, la utilización del sistema puede requerir que ambos participantes de la comunicación se hayan registrado previamente. De manera alternativa, puede ser posible que el registro de un participante de comunicación único sea suficiente para posibilitar el intercambio de un mensaje de comunicación entre estas dos entidades de comunicación.

En una situación en la que se requiere pago para utilizar el sistema, es posible que uno de los participantes en la comunicación soporte todos los costes. O bien, la entidad emisora puede soportar los costes de envío de un mensaje, mientras que la recepción del mensaje es gratuita. O bien, la entidad receptora puede soportar los costes para recibir el mensaje, mientras que el envío del mensaje es gratuito.

A continuación, se explicarán realizaciones adicionales a título de ejemplo del sistema de comunicación. No obstante, estas realizaciones son válidas también para el método de comunicación, para el medio que puede ser leído por ordenador, para el elemento de programa, para la unidad emisora, para la unidad receptora y para la unidad de control, de acuerdo con las reivindicaciones independientes. La unidad emisora puede ser adaptada para enviar el mensaje electrónico a una serie de unidades receptoras. De este modo, un mensaje puede ser enviado a más de un receptor y, por lo tanto, el mensaje puede ser transmitido una serie de veces. En particular, los diferentes procesos de transmisión pueden ser llevados a cabo individualmente e independientemente o separadamente entre sí. Al adoptar esta medida, se podrán ajustar características de los mensajes individuales de diferente manera, por ejemplo, un grado de urgencia que puede ser distinto para diferentes receptores.

La unidad emisora puede estar adaptada para generar el mensaje electrónico basándose en datos electrónicos proporcionados por un usuario de la unidad emisora. Por ejemplo, estos datos electrónicos pueden ser un texto o un contenido de audio o de video que es introducido por el usuario de la unidad emisora, por ejemplo mediante teclado, ratón de ordenador, bola seguidora (“track ball”), micrófono, cartucho de memoria o interfaz gráfico de usuario (GUI) de la unidad emisora o puede ser acoplado a la unidad emisora.

Además, la unidad emisora puede estar adaptada para generar el mensaje electrónico como mensaje electrónico codificado al codificar los datos electrónicos. La codificación del mensaje electrónico, por ejemplo, por medio de un mecanismo de codificación convencional, puede mejorar el nivel de seguridad de la transmisión del mensaje confidencial.

La unidad emisora además puede estar adaptada para generar el mensaje electrónico como correo electrónico, incluyendo una incorporación basada en los datos electrónicos. Por lo tanto, la unidad emisora puede tener software instalado en la misma que es capaz de procesar los datos electrónicos de manera que se pueda enviar un correo electrónico desde la unidad emisora a la unidad receptora teniendo como archivo incorporado los datos electrónicos procesados. Esta incorporación puede tener una extensión específica (por ejemplo “.rgf”) de manera que el software instalado en la unidad receptora puede ser capaz automáticamente de determinar el tipo de mensaje y opcionalmente, abrir automáticamente el mensaje basándose en la información derivada de la extensión.

La unidad emisora puede estar adaptada además, para generar un código de segmentación (hashcode) basado en el mensaje electrónico y/o basado en los datos electrónicos. Un código de segmentación puede ser indicado como código que incluye información tal como, información de usuario y/o información de temporización y/o información de transmisión a efectos de proporcionar un sistema protegido contra falsificaciones. Un código de segmentación de este tipo puede permitir una identificación sin ambigüedades de un documento, y por lo tanto, puede permitir una identificación única, puesto que puede consistir en algún tipo de “huella dactilar” del mensaje.

La unidad emisora puede estar adaptada para enviar el código de segmentación a la unidad de control, como mínimo, como una parte del mensaje de información enviado. Por lo tanto, la unidad de control recibe la información

necesaria para controlar o supervisar la totalidad del sistema, de manera que cualquier abuso puede ser detectado de manera segura y se puede impedir por la unidad de control.

La unidad emisora puede estar adaptada además, para enviar una clave de decodificación a la unidad de control como una parte, como mínimo, del mensaje de información de envío, estando adaptada la clave de decodificación para decodificar el mensaje electrónico codificado. Por lo tanto, al no enviar directamente la clave de decodificación a la unidad receptora, el nivel de seguridad se mejora adicionalmente. No obstante, dado que la clave de decodificación es enviada a la unidad de control y la unidad de control puede ser llevada a comunicar con la unidad receptora, es posible que la unidad de control proporcione a la unidad receptora la clave de decodificación, de manera que se obtiene un sistema triangular con un elevado grado de seguridad.

La unidad emisora puede estar adaptada además, para enviar a la unidad de control, como mínimo, una parte del mensaje de información de envío, por lo menos, uno de los elementos de información del grupo que consiste en información de usuario de la unidad emisora, información de datos electrónicos e información de comunicación. Por lo tanto, el mensaje de envío de información puede incluir datos tales como un código de segmentación, identidad de emisor, identidad de receptor, objeto del mensaje electrónico, clave de decodificación y cualquier otra información necesaria.

La unidad emisora puede estar adaptada además, para sincronizar el envío del mensaje electrónico directamente a la unidad receptora y el envío del mensaje de información a la unidad de control. Por ejemplo, el mensaje electrónico y el mensaje de envío de información pueden ser enviados desde la unidad emisora a los respectivos destinos, esencialmente, de forma simultánea en el tiempo, de manera que se puede asegurar una rápida transmisión del mensaje o mensajes.

La unidad emisora puede estar adaptada para generar el mensaje electrónico en forma de mensaje electrónico comprimido al comprimir los datos electrónicos. Al utilizar un algoritmo de compresión, tal como cualquier algoritmo de compresión convencional, se puede reducir la cantidad de datos a transmitir entre las tres entidades de manera que la velocidad de transmisión se puede incrementar y la carga de computación de todo el sistema se puede reducir significativamente.

La unidad emisora puede estar adaptada para iniciar una comunicación con unidad de control al enviar un mensaje de autentificación a la unidad de control antes de enviar el mensaje de envío de información. Mediante esta autentificación a llevar a cabo entre la unidad emisora y la unidad de control, se puede impedir de manera segura el abuso del sistema dado que, solamente, el código de autentificación o similar puede permitir a la unidad emisora el iniciar una comunicación con la unidad de control y solamente en este caso se puede poner en marcha la transmisión de un código de decodificación desde la unidad de control a la unidad receptora.

La unidad emisora puede comprender además un elemento de software que comprende una aplicación de cliente de correo electrónico. Por lo tanto, el software a instalar en la unidad emisora puede ser completamente autárquico con respecto a cualquier sistema existente, y las condiciones de esta aplicación de cliente de correo electrónico se pueden definir selectivamente a efectos de optimizar el sistema de correo electrónico registrado.

No obstante, es también posible, alternativamente, que la unidad emisora comprenda un elemento de software introducido en una aplicación convencional de cliente de correo electrónico o que se tiene que introducir en la misma. Por lo tanto, es posible instalar solamente un componente adicional o una aplicación existente de cliente de correo electrónico, tal como Netscape Navigator™, Outlook™ o similares, de manera que solamente son necesarias ligeras modificaciones para posibilitar a un usuario utilizar simultáneamente una aplicación conocida de software de cliente y tener adicionalmente la oportunidad de enviar un correo registrado por medio de un mensaje electrónico.

A parte de esto, la unidad emisora puede estar adaptada para notificar un evento en el que el usuario de la unidad receptora ha tenido acceso al mensaje electrónico. Por lo tanto, el emisor puede ser informado directamente, tan pronto como sea posible, cuando la unidad receptora ha leído el mensaje electrónico, y por lo tanto, consigue un recepción similar al del caso de un correo postal registrado convencional, no obstante, en forma electrónica y por lo tanto con una velocidad significativamente incrementada.

La unidad emisora puede estar adaptada además, para notificar un evento en el que el usuario de la unidad receptora no ha tenido acceso al mensaje electrónico durante un intervalo de tiempo que supera un intervalo de tiempo umbral predeterminado, por ejemplo, de un día, una semana o un mes. También es posible que el usuario pueda definir este intervalo de tiempo o que este intervalo de tiempo pueda ser prealmacenado en el sistema. Después del transcurso de este intervalo de tiempo de umbral, el emisor puede ser activamente informado de que el receptor no ha abierto todavía el mensaje, de manera que el emisor puede utilizar esta información o puede contactar al receptor para informarle de que debe leer un mensaje importante o urgente.

La unidad receptora puede estar adaptada, después de recibir una instrucción de acceso de un usuario de la unidad receptora, para proporcionar acceso al mensaje electrónico al usuario de la unidad receptora. Esta instrucción de

acceso puede ser un doble cliqueo en un ratón de ordenador o cualquier otra instrucción que se pueda proporcionar por el usuario de la unidad receptora a la unidad receptora con intermedio de un interfaz de usuario.

No obstante, la unidad receptora puede estar adaptada además, después de recibir la instrucción de acceso, para enviar un mensaje de autentificación a la unidad de control antes de proporcionar acceso al mensaje electrónico. Por lo tanto, para mejorar la seguridad del sistema y proporcionar un sistema protegido contra falsificaciones, se puede impedir cualquier tipo de abuso cuando la unidad receptora se autentifica a sí misma a petición de la unidad de control antes de que tenga permiso de abrir el mensaje electrónico.

Esto se puede conseguir enviando una clave de decodificación desde la unidad de control a la unidad receptora solamente después de recibir el mensaje (correcto) de autentificación de la unidad receptora. Por lo tanto, se puede asegurar que la unidad receptora puede abrir solamente el mensaje electrónico codificado, basándose en la clave de decodificación, que es proporcionada solamente a la unidad receptora por la unidad de control después de una autentificación satisfactoria.

Además, la unidad receptora puede estar adaptada para proporcionar acceso al mensaje electrónico al decodificar el mensaje electrónico por medio de la clave de decodificación.

La unidad de control puede estar adaptada además para enviar, después de recibir el mensaje de información de recepción, un mensaje de confirmación a la unidad emisora, indicando el mensaje de confirmación que el usuario de la unidad receptora ha tenido acceso y ha tomado incorporación del mensaje electrónico. Este mensaje de confirmación puede informar al emisor que el mensaje ha llegado al lado receptor y que ha sido abierto/leído por el receptor.

La unidad emisora y la unidad receptora pueden estar adaptadas para comunicación directa entre sí sin ninguna entidad intermedia entre ambas. Por lo tanto, se puede conseguir un sistema rápido, fácil y no propenso a errores, que es muy adecuado para el usuario puesto que no se tiene que instalar ningún recurso de ordenador de envergadura entre la unidad emisora y la unidad receptora.

Como mínimo, una de dichas unidad emisora, unidad receptora y unidad de control puede comprender, como mínimo, un elemento del grupo que comprende: un ordenador servidor, un ordenador de cliente, un ordenador de sobremesa, un ordenador portátil, un asistente digital personal y un teléfono móvil. Por lo tanto, los diferentes elementos están adaptados para comunicar con intermedio de cualquier dispositivo electrónico y no están restringidos a los ordenadores convencionales.

El sistema de comunicación puede estar, además, adaptado para comunicación de la unidad emisora y/o de la unidad receptora y/o unidad de control con intermedio de una red de comunicación, particularmente, por medio de, como mínimo, una red de comunicación del grupo que consiste en Internet, intranet (por ejemplo, en una empresa), WLAN (red de área local sin cables) y una red de comunicaciones móviles. Por lo tanto, el sistema de correo electrónico registrado, de acuerdo con realizaciones de la invención, no está restringido a ninguna red de comunicaciones específicas, sino que se puede instalar en el contexto de cualquier sistema de comunicación con o sin cables.

La utilización del sistema de comunicación puede ser autorizada a un usuario de la unidad emisora y/o de la unidad receptora previo pago.

La unidad de control puede comprender una primera entidad de control (que puede ser una primera unidad proveedora) acoplada con capacidad de comunicación a la unidad emisora (que puede ser un cliente de la primera unidad proveedora) de manera que la transmisión de un mensaje de emisor, desde la unidad emisora a la primera entidad de control, es indicativa de la identidad de la unidad emisora. La unidad de control puede comprender una segunda entidad de control (que puede ser una unidad de comprobación (“clearing”)) acoplada con capacidad de comunicación a la primera entidad de control. La primera entidad de control puede estar adaptada para enviar el mensaje del emisor (es decir, el mensaje electrónico no codificado) a transmitir desde la unidad emisora a la unidad receptora, sin embargo, un mensaje auxiliar que incluye contenido, tal como información de clave de decodificación (código de segmentación, etc.) a la segunda entidad de control, de manera que la segunda entidad de control no está enterada (es decir, no conoce) la identidad de la unidad emisora. Por lo tanto, un proveedor puede comunicar con la unidad emisora de manera que el proveedor conoce la identidad de un usuario de la unidad emisora. No obstante, en contraste con ello, la comunicación entre la primera entidad de control y la segunda entidad de control, con respecto a la unidad emisora, puede ser anónima de manera que la identidad de la unidad emisora no sea conocida por la segunda entidad de control. No obstante, un historial de transacciones que indica cualquier comunicación (incluyendo sellos de tiempo, etc.) entre la primera entidad de control y la segunda entidad de control se puede almacenar en ambas entidades de manera que cualquier comunicación individual puede ser seguida o identificada más adelante.
Por lo tanto, cuando se tomen en consideración ambos historiales de transacción, será posible reconstruir de manera no ambigua cualquier comunicación incluyendo la identidad de la unidad emisora almacenada en la primera entidad de control, si ello es necesario. Este concepto puede permitir un historial de comunicación transparente y

puede hacer que la primera entidad de control pueda prescindir de proporcionar a la segunda entidad de control (y/o a la tercera entidad de control) información confidencial respecto a la unidad emisora, es decir, respecto a su cliente o clientes.

El mensaje del emisor puede ser un mensaje de envío de información, particularmente puede ser el mensaje de envío de información que comprende una clave de decodificación adaptada para decodificar el mensaje electrónico codificado. De este modo, la segunda unidad de control/comprobación puede manejar una transacción de una clave requerida por la unidad receptora para decodificar el mensaje electrónico de manera anónima.

La unidad de control puede comprender una tercera entidad de control (que puede ser una segunda unidad proveedora) acoplada con capacidad de comunicación a la unidad receptora (que puede ser un cliente de la segunda unidad proveedora) de manera que una transmisión de un mensaje de receptor, entre la unidad receptora y la tercera entidad de control, es indicativa de la identidad de la unidad receptora. La tercera entidad de control puede estar acoplada con capacidad de comunicación a la segunda entidad de control. La tercera entidad de control puede estar adaptada para intercambiar datos con la segunda entidad de control, de manera que la segunda entidad de control no está enterada (es decir, no conoce) la identidad de la unidad receptora. Por lo tanto, un proveedor puede comunicar con la unidad receptora, de manera que el proveedor conoce la identidad de un usuario de la unidad receptora. No obstante, en contraste con ello, una comunicación entre la tercera entidad de control y la segunda entidad de control, con respecto a la unidad receptora, puede ser anónima de manera que la identidad de la unidad receptora no sea conocida para la segunda unidad de control. No obstante, un historial de transacción indicativo de cualquier comunicación entre la tercera entidad de control y la segunda entidad de control se puede establecer en ambas entidades, de manera que se pueda efectuar el seguimiento de cualquier comunicación más adelante. Por lo tanto, considerando ambos historiales de transacciones en combinación, será posible reconstruir cualquier comunicación, incluyendo la identidad de la unidad receptora almacenada en la tercera entidad de control, en caso necesario. Este concepto puede permitir transparencia del historial de comunicación y puede hacer prescindible que la tercera entidad de control proporcione a la segunda entidad de control (y/o la primera entidad de control) información confidencial respecto a la unidad receptora, es decir, con respecto a su cliente o clientes.

El mensaje del receptor puede ser, como mínimo, uno de un grupo que consiste en un mensaje de información al receptor y una clave de decodificación adaptada para decodificar el mensaje electrónico codificado.

Por lo tanto, un usuario emisor que desee enviar un mensaje electrónico lo más anónimo posible a un usuario receptor puede dar a conocer su identidad solamente a este servidor proveedor, a saber la primera identidad de control. Entonces, la primera entidad de control puede almacenar la identidad del usuario emisor y puede enviar un mensaje anónimo libre de la identidad del usuario emisor a la segunda entidad de control. Esto puede permitir al usuario emisor permanecer anónimo para el sistema, a excepción de la primera entidad de control. Este sistema puede ser ideal para un sistema de comprobación.

Una comunicación segura entre el usuario emisor y el usuario receptor a través de sus respectivos servidores proveedores, a saber la primera unidad de control y la tercera unidad de control, es posible. Solamente la primera entidad de control y la tercera entidad de control están enteradas de la identidad de su respectivo cliente (usuario emisor/usuario receptor), mientras que ni los mensajes intercambiados entre las entidades de control son indicativos de la identidad de los respectivos usuarios, ni la segunda entidad de control está enterada de la identidad del usuario correspondiente.

Este sistema de comunicación puede estar configurado como sistema de gestión de transacciones anónimo, particularmente, como sistema de comprobación anónimo. Este sistema de comprobación anónimo puede permitir gestionar transacciones de forma anónima y posibilita un negocio de proveedor múltiple con transacciones de correo electrónico a través de proveedores.

De manera adicional o alternativa, por lo menos uno de los grupos que consiste en la unidad emisora, la unidad receptora y la unidad de control pueden estar adaptadas para impedir accesibilidad a la información incluida en el mensaje electrónico en el caso de que falte una incorporación predeterminada al mensaje electrónico. Por ejemplo, en caso de que dicha incorporación esperada es una exigencia de transacción y decodificación satisfactorias del mensaje electrónico, puede ser una incorporación de un documento de puesta en vigor. Esto puede permitir al sistema de comunicación poner en vigor incorporaciones tales como firmas digitales, asegurando de esta manera una comunicación vinculante legalmente. Por ejemplo, la unidad emisora puede permitir el inicio de la transmisión del mensaje electrónico solamente cuando una incorporación especial está incorporada en el mensaje electrónico o puede incorporar automáticamente dicha incorporación al mensaje electrónico sin darle al usuario la opción de impedir dicha incorporación. De manera adicional o alternativa, la unidad receptora puede rechazar el mensaje electrónico cuando falta la incorporación especial en dicho mensaje electrónico. De manera adicional o alternativa, la unidad de control puede rechazar el suministro de una clave necesaria para que la unidad receptora decodifique el mensaje electrónico cuando falta la incorporación especial en el mensaje electrónico.

Específicamente, la unidad emisora puede estar adaptada para incorporar de manera obligatoria una incorporación predeterminada al mensaje electrónico. En otras palabras, sin un usuario de la unidad emisora que tenga

oportunidad de decidir si el mensaje será enviado con o sin la incorporación, dicha incorporación puede ser incorporada automáticamente al mensaje por la unidad emisora. De este modo, la unidad emisora puede obligar a que la incorporación sea realmente incorporada en el mensaje. Cuando un receptor tiene acceso al mensaje, puede ver inmediatamente la incorporación del usuario tal como un certificado electrónico. Esto puede asegurar que no se puede enviar mensaje alguno sin autorización del emisor.

La incorporación predeterminada puede comprender, como mínimo, una de un grupo que consiste en una identificación de un usuario de la unidad emisora, una autentificación de un usuario de la unidad emisora, una obligación de un usuario de la unidad emisora y un logotipo caracterizador de un usuario de la unidad emisora. Estas incorporaciones o certificados pueden incluir derechos y/o restricciones mantenidas por las organizaciones de las que el usuario es miembro, por ejemplo para órdenes o restricciones de competencia del usuario, tales como "el usuario está autorizado a comprar mercancías hasta un valor de…"

A continuación, se describirá un procedimiento para asegurar una autorización de acuerdo con una realización a título de ejemplo de la invención. Esta realización puede ser implementada en una situación en la que es de particular importancia que el usuario de la unidad emisora sea una persona específica con alta fiabilidad.

En esta realización, el usuario de la unidad emisora puede estar invitado a proporcionar un documento de identificación adicional con información tal como número de teléfono, copia del pasaporte, etc. Entonces, el sistema puede verificar que el documento adicional de la información de identificación es correcto, por ejemplo, puede llamar al usuario de la unidad emisora que utiliza el número de teléfono que se ha proporcionado. Este proceso de contacto puede ser llevado a cabo por una actividad humana o de manera completamente automatizada. Si el proceso de identificación es satisfactorio, es decir, cuando el documento adicional facilitado de información de identificación se manifiesta verdadero o la identidad es verificada, el sistema puede proporcionar al usuario identificado datos de acceso a un archivo de identidad tal como una clave utilizable para comunicación, con intermedio de un sistema de comunicación de acuerdo con una realización de la invención. Por ejemplo, el usuario puede recibir una contraseña que puede introducir en la página de Internet. Después de introducir dicha contraseña, la unidad emisora puede recibir, procedente de la página de Internet, un archivo de identidad que comprende información de identificación del usuario. Este archivo de identidad puede ser utilizado para comunicación subsiguiente con un receptor y puede formar la base de una notificación a un receptor de un mensaje enviado desde el usuario identificado a la unidad receptora de que el usuario de la unidad emisora ha sido identificado de manera apropiada.

El término "archivo-contenedor" ("container-file") puede indicar, particularmente, cualquier archivo que incluya contenidos de un correo electrónico, por ejemplo de manera codificada. El archivo-contenedor puede contener un cuerpo de mensaje y puede comprender diferentes informaciones de gestión. El archivo-contenedor puede tener una extensión específica (por ejemplo ".rgf"), de manera que una aplicación de lectura puede reconocer automáticamente qué tipo de mensaje se ha presentado y si tiene que ser mostrado o presentado.

Se puede facilitar al sistema un "creador" que puede permitir al usuario generar un correo electrónico que puede ser enviado de acuerdo con realizaciones de la invención. Este creador puede operar independientemente de un programa de correo electrónico específico. Es posible utilizar el creador, además de la generación de correos electrónicos, cuando no se necesita un programa separado de correo electrónico. Las exigencias para utilizar este creador es solamente un acceso a una red tal como Internet y una cuenta de correo electrónico. Este creador puede utilizar una puerta especial del protocolo Internet TCP/IP o la norma común conocida SSL para conexiones seguras. Por ejemplo, este creador puede utilizar el puerto 8080 del protocolo Internet TCP/IP.

Además, se puede facilitar un "lector" para leer y mostrar herramientas para archivos-contenedor. Se puede utilizar como herramienta estándar de visualización para archivos con la extensión ".rgf". A efectos de utilizar este lector cualquier lector de acceso a la red de comunicación puede ser ventajoso, por ejemplo, un acceso a Internet y una cuenta de usuario correspondiente o cuenta de miembro. Este lector puede utilizar una puerta especial del protocolo de Internet TCP/IP o la norma común conocida SSL para conseguir conexiones seguras. Por ejemplo, este lector puede utilizar también el puerto 8080 del protocolo Internet TCP/IP.

Los "AES245" o "Blowfish" pueden ser indicados específicamente como métodos de codificación que pueden ser utilizados para codificar los datos y el mensaje electrónico en el archivo-contenedor. La comunicación a través de Internet puede ser codificada mediante "AES245" o "Blowfish".

Se pueden indicar específicamente los códigos de segmentación ("Hashcodes") como huellas dactilares de un archivo o un texto. La asignación de un archivo a un código de segmentación calculado puede ser no ambigua. Por medio de un código de segmentación calculado es posible determinar si se ha modificado algo en un archivo entre la generación con un creador y la lectura con un lector. Cuando los códigos de segmentación son idénticos, el archivo es idéntico.

Una "incorporación" puede ser un archivo incorporado a un correo electrónico. Cuando se envía un correo electrónico la incorporación puede comprender el archivo-contenedor.

El término “clave” puede indicar una contraseña utilizada para codificar o decodificar datos o texto. De este modo, esta contraseña puede ser utilizada para codificar y para decodificar. La longitud de la clave puede ser seleccionada de manera tal que se puede conseguir el grado deseado de seguridad.

A parte de los datos del archivo-contenedor, también se puede codificar la comunicación con el servidor o con la unidad de control. En este contexto, es posible calcular una nueva clave para cada conexión (por ejemplo, un intercambio con clave Diffie-Hellmann) con la que se puede codificar la comunicación.

Cada correo enviado o recibido puede comprender un plazo recordatorio asignado. Cuando el correo electrónico no ha sido recibido o confirmado dentro de este plazo, el emisor puede recibir un mensaje referente a la falta de acceso del correo electrónico al receptor.

Es posible distinguir, particularmente, entre dos tipos de pertenencia como miembro al sistema, a saber, cuenta de usuario y cuenta de miembro. La cuenta de usuario puede permitir la recepción de correos electrónicos. Puede encontrarse libre de pago. La cuenta de miembro puede permitir, además, el envío de correos y puede ser facilitada solamente mediante pago.

A continuación se describirá de manera más detallada un sistema para un método de control del envío, recepción e integridad del mensaje de correo electrónico de acuerdo con una realización a título de ejemplo de la invención.

A continuación se llevará a cabo una explicación general del sistema.

El sistema está diseñado para proporcionar un servicio para suministro registrado (o certificado) de información mediante correo electrónico. Este servicio, utilizando el método del sistema que se describe más adelante, facilitará el suministro de un correo electrónico registrado tanto para el emisor como para el receptor y reducirá las complejidades en comparación con servicios conocidos. Este sistema elimina la necesidad de tomar posesión de un correo electrónico para transporte desde el emisor al destinatario. Esto se consigue puesto que potencia servicios de correo electrónico existentes que pueden tener ya en uso tanto el emisor como el receptor. Esto elimina automáticamente todas las disposiciones que se tendrían que tomar de otro modo para asegurar una manipulación apropiada de un correo electrónico que se encuentra en posesión.

El sistema y método se pueden resumir de la manera siguiente:

Un emisor puede desear enviar un correo electrónico a un destinatario y puede compilar este correo electrónico y enviarlo utilizando un servicio ordinario de correo electrónico. El proceso ordinario de envío y recepción se puede sincronizar con un nuevo proceso. Después del envío, el proceso puede codificar el correo electrónico dando como resultado un correo electrónico con una incorporación específica y puede enviar información de codificación (por ejemplo, código de segmentación) y la dirección de correo electrónico del destinatario a un servidor. Después de recibir el correo electrónico a través del servicio regular de correo electrónico del receptor, el proceso puede reconocer el correo específico (por ejemplo, incorporación “.rgf”), puede calcular un código de segmentación con respecto al correo electrónico específico y puede transmitir el código de segmentación e información del receptor al servidor.

El servidor puede comparar los códigos de segmentación “enviado” y “recibido” e información de receptor/destinatario y si se cumple su correspondencia positiva, puede enviar una clave al receptor. Una clave de receptor y un programa especial de lector pueden decodificar el correo electrónico y pueden proporcionar acceso al contenido del correo electrónico.

A continuación se explicará de manera más detallada el proceso de envío.

El emisor puede crear un correo electrónico. Después de empezar el proceso de envío se puede invocar un programa especial (creador). El programa creador puede fusionar el contenido del correo electrónico en un archivo (archivo-contenedor). El contenido puede incluir archivos incorporados, mensajes de texto y otras informaciones. El contenido en este archivo-contenedor puede ser codificado utilizando un algoritmo de codificación común. Opcionalmente, el archivo-contenedor puede ser comprimido utilizando un algoritmo de compresión común. La clave de codificación puede ser generada por un algoritmo al azar. A continuación, se puede calcular un código de segmentación para el archivo-contenedor completo. El creador puede utilizar un algoritmo de código de segmentación común, tal como SHA-256. Después de ello, el creador puede establecer contacto con el servidor para autentificar el emisor (por ejemplo, nombre del usuario/contraseña) utilizando un protocolo de transmisión seguro y codificado. Después de la autentificación, el creador puede transmitir el código de segmentación del archivo-contenedor, la clave de codificación y otras informaciones al servidor. El archivo contendor puede ser una incorporación ordinaria a un correo electrónico genérico.

El programa creador puede ser diseñado para soportar una serie de alternativas de composición y envío de un correo electrónico:

1. Utilizando el creador como cliente de correo electrónico, no requiere otro cliente de correo electrónico (tal como Outlook). El creador puede permitir que el emisor componga un correo electrónico completo.

2. Utilizando el creador con parámetros de línea de mando. De este modo, es posible incorporar el creador en otros programas (por ejemplo, Microsoft™-Outlook™, Novell™ Groupwise™ ó Mozilla Thunderbird™ y muchos otros).

El control de la recepción del correo electrónico puede incluir la notificación automática al emisor en el caso de que el receptor (o los receptores no hayan) no haya abierto el correo electrónico dentro del tiempo especificado por el emisor.

A continuación, se describirá de manera más detallada el proceso de recepción.

El archivo-contenedor puede ser recibido como incorporación ordinaria a un correo electrónico. Al abrir el archivo-contenedor (por ejemplo, doble cliqueo) u otros métodos (tales como parámetros de línea de mando), el receptor puede poner en marcha el lector (que puede encontrarse a disposición como descarga libre). Este puede ser un proceso automático, dado que el lector puede ser asociado con el final del nombre del archivo-contenedor. El lector puede establecer contacto con el servidor para autentificar el receptor (nombre de usuario/contraseña) utilizando un protocolo de transmisión seguro y codificado. Después de la autentificación, el lector puede calcular el código de segmentación del archivo de contendor recibido y puede transmitir este código de segmentación acompañado de otras informaciones, al servidor. El servidor puede comprobar este código de segmentación con respecto al código de segmentación que ha sido calculado por el creador como parte del proceso de envío. Si ambos códigos de segmentación, así como la dirección del destino del correo electrónico (receptor = destinatario) se corresponden, el servidor puede transmitir la clave de codificación al lector. Esta clave puede ser necesaria para decodificar el contenido del archivo-contenedor. Después de la transmisión de la clave, el servidor puede enviar un correo electrónico al emisor del archivo contendor para indicar que el destinatario ha recibido el mensaje y que lo ha abierto satisfactoriamente. Cuando hay correspondencia positiva, el lector puede descodificar el contenido, proporcionando de esta manera acceso a los archivos y otras informaciones dentro del archivo-contenedor.

Este proceso de recepción puede ser ventajoso dado que la autentificación del receptor puede asegurar que solamente el destinatario, tal como se ha estipulado por el emisor, tendrá acceso al correo electrónico.

Las siguientes condiciones previas deben cumplirse para que el receptor pueda tener acceso al contenido del correo electrónico:

- el receptor debe encontrarse en posesión del archivo-contenedor no manipulado.
- el receptor debe tener una cuenta de usuario o cuenta de miembro en la base de datos del servidor del servicio.
- la dirección de correo electrónico del receptor debe ser única y el servicio debe asegurarse de que una dirección de correo electrónico puede ser registrada solamente una vez.

Los códigos de segmentación (“hashcode”) pueden proporcionar las siguientes ventajas:

- es posible que un archivo-contenedor sea aceptado solamente por el servidor si el archivo contendor no está manipulado.
- la integridad de archivo-contenedor: códigos de segmentación idénticos para archivo-contenedor enviado y recibido, significan que los archivos contenedor recibidos y el contenido son idénticos a los archivos contenedor enviados y su contenido.

La transferencia codificada puede proporcionar seguridad, dado que el algoritmo de codificación y de segmentación puede ser un algoritmo utilizado de manera común, también utilizado para firmas digitales por el estamento militar y el gobierno.

A continuación, se explicará el registro de usuario.

Antes de que un usuario pueda enviar un correo electrónico utilizando el servicio, es posible que el usuario tenga que ser conocido por el servidor. Es posible que tenga que existir una entrada en un tipo de base de datos de usuario. Esta entrada puede ser creada manualmente por una persona administrativa o, de modo preferente, utilizando un lugar de web que permita al usuario firmar como miembro del servicio. Este lugar web puede ofrecer servicios adicionales para los miembros, tales como administrar la cuenta de usuario y descrubrir y seguir todas las transacciones.

Este proceso puede tener las siguientes ventajas:

El emisor puede controlar el recepción del correo electrónico enviado (correo certificado). La transferencia codificada del contenido completo (incorporaciones y otras informaciones) puede ser posible. La integridad del contenido (solamente un archivo-contenedor con el código de segmentación correcto que pondrá en marcha la clave correcta)

puede ser asegurado. El correo electrónico puede ser enviado de forma habitual (a través del proveedor del emisor y cuenta de correo electrónico del emisor). Se puede obtener la compatibilidad con otros servicios de correo tales como firma digital. El proveedor del servicio puede tener solamente una transferencia limitada (aproximadamente 1kB por transacción completa para código de clave y códigos de segmentación y otras informaciones, pero no el correo electrónico y las incorporaciones). Se puede conseguir la compatibilidad con otros métodos tales como firmas digitales o procesos de codificación. El proceso puede trabajar a escala mundial sin fronteras. Es posible una fácil integración en procesos comunes de correo electrónico. El servicio no tiene que preocuparse de exigencias legales que emanan de la posesión del correo electrónico. Como consecuencia, se pueden evitar todas las disposiciones técnicas para cumplir estas exigencias. El sistema puede proporcionar pruebas legales.

A continuación, se describirán detalles referentes al archivo-contenedor, de acuerdo con una realización a título de ejemplo de la invención.

Un archivo-contenedor (o contenedor) puede ser un archivo único, conteniendo el contenido completo de un correo electrónico, los archivos incorporados, mensajes y otras informaciones necesarias para la transferencia segura y certificada del correo electrónico. Un correo electrónico puede comprender uno o varios receptores del mensaje, el emisor, el objeto, el cuerpo del mensaje (el texto escrito como mensaje al receptor) y las incorporaciones (otros archivos incorporados al mensaje para su transferencia).

Con el proceso, el cuerpo del mensaje y la incorporación o incorporaciones pueden ser puestos en un archivo-contenedor. Este archivo-contenedor puede ser incorporado a continuación al correo electrónico.

Un archivo-contenedor puede comprender dos partes, a saber, la cabecera del contenedor y datos codificados binarios.

La cabecera del contendor puede contener todas las informaciones necesarias para transferir y decodificar los datos binarios de la segunda parte del archivo. Además, la cabecera del contenedor puede proporcionar datos para asegurar la autentificación con respecto al servidor y mostrar información legible para el receptor.

En realidad, la cabecera completa no puede ser codificada (excepto el cuerpo del mensaje). Cada archivo puede ser codificado o comprimido de forma separada de manera que es más rápida la extracción de un archivo único. Todo campo dentro de la cabecera del contenedor puede ser dividido por un Carácter de Alimentación de Línea (&H0A). El divisor entre las cabeceras de entrada puede ser un carácter PIPE (&H7C).

La siguiente tabla muestra una cabecera de contenedor a título de ejemplo:

Campo	Descripción	Ejemplo de contenido
Identificador	Las primeras dos letras de un archivo contenedor son EM. Esto significa “contenido de correo electrónico codificado”	“EM”
Destinatario	La dirección de correo electrónico del destinatario.	“alice@inter.net”
Emisor	Nombre completo o nombre de la empresa del emisor.	“ V.Schmid Inspirant Germany”
Fechadecreación	Fecha y hora de la creación del archivo contenedor. Este sello de tiempo es la fecha/hora en la que funciona el ordenador de creación y no una fecha certificada	“16/11/2005 10:32:54”
Usuariodelacreación	El nombre de usuario de PC de la persona creadora. Éste es un nombre de entrada (“logon”) del ordenador, preparado por el creador durante la creación.	“Usuariodelacreación”
Mensaje *)	Cuerpo del mensaje codificado. Es simple texto ASCII codificado con la clave de archivo contenedor. El texto es almacenado codificado HEX para evitar tareas molestas.	“7ECAC0DA2C5D6B94C69CE884F395C70...”
Conteoarchivo	Número de archivos contenidos	“8”
Entrada 1	Entrada única para cada archivo	ver Cabecera-Entrada
Entrada n	Entrada única para cada archivo (n=Número de archivos	ver Cabecera-Entrada
Finaldecódigo	Una única tarea ASCII-255	&HFF
Archivos *)	Binario, datos codificados y comprimidos definidos en las cabeceras de entrada	-

*) Datos codificados. Los archivos pueden estar comprimidos.

La siguiente tabla muestra una cabecera de entrada a título de ejemplo (para cada elemento de entrada de la cabecera de contenedor)
Valores divididos por PIPE (&H7C)

Campo	Descripción	Ejemplo
Nombredearchivo	Nombre de archivo del archivo almacenado	“Rechnung.pdf”
CP	Indica, si el archivo se ha almacenado de forma comprimida. Si el valor es “0”, no se utiliza compresión. “1” indica compresión ZIP estándar. Otros métodos de compresión pueden seguir.	“0”
Desplazamiento	Desplazamiento en bytes para el inicio de los datos del archivo. El desplazamiento es adicional a la posición del primer byte de datos binarios (un byte por detrás de la última tarea ASCII-255 de la cabecera).	“1234”
Longitud	Longitud de los datos de archivo en bytes	“16384”

A continuación se explicará de manera más detallada una realización a título de ejemplo de un Protocolo de Transferencia.

Este documento puede describir la transferencia de datos entre el programa creador, el programa lector y el servidor (que proporciona el servicio), cuyo servidor puede ser designado también como unidad de control.

Un objetivo es que este protocolo pueda describir la transferencia completa entre los programas involucrados en el servicio para el correo electrónico registrado.

Haciendo referencia a los programas involucrados, hay particularmente tres programas que utilizan este protocolo, pero son posibles otras aplicaciones:

- creador (programa para crear archivos contenedor y opcionalmente enviarlos en forma de correo electrónico utilizando SMTP).
- lector (programa para abrir y decodificar archivos de contenedor)
- servidor (el servidor, situado en un lugar de Internet especializado que proporciona las funciones para registrar un correo electrónico con un archivo-contenedor incorporado o para recibir la clave para decodificar un archivo-contenedor. Este servidor puede comprender una base de datos y funciones lógicas para asegurar y registrar transacciones).

El control implementado puede comprender cuatro partes:

1. Inicialización (inicializa una colección segura entre el creador y el servidor o entre el lector y el servidor).
2. Autentificación (autentifica el usuario del creador o el lector con respecto a la base de datos del servidor).
3. Crear una nueva transacción de mensaje (registrar un nuevo archivo de contenedor en la base de datos del servidor. Utilizado por el programa creador).
4. Pedir clave (pide una clave para decodificar un archivo-contenedor. Utilizado por el programa lector).

A continuación se facilitará una descripción detallada del protocolo.

Un protocolo de inicialización puede inicializar una conexión segura entre el creador y el servidor o entre el lector y el servidor. Puede ser necesaria para cada conexión entre el servidor y el creador o lector.

En primer lugar, se puede establecer una conexión TCP/IP entre el programa creador y el servidor o entre el programa lector y el servidor. Ésta puede ser una conexión estándar TCP/IP a una dirección IP especificada y un puerto obligado. Estos parámetros pueden ser configurados en el correspondiente programa (programa creador o lector).

El cliente (creador/lector) puede enviar una cadena de inicialización al servidor. Esta cadena puede contener:

"regify <TAB> G <TAB> P <TAB> Alpha"
<TAB> puede significar código ASCII-9, sin blancos.
regify -> puede ser algo tal como una bienvenida (“handshake”) para asegurar que la otra parte es un programa conocido
G -> puede ser un número al azar para el protocolo de intercambio de la clave Diffie-Hellman.
P -> puede ser un número primo común para el protocolo de intercambio de la clave Diffie-Hellman.
Alpha -> puede ser el Alpha calculado para el protocolo de intercambio de la clave de Diffie-Hellman.

El intercambio por la clave de Diffie-Hellman es un algoritmo ampliamente utilizado y bien conocido.

El servidor puede efectuar el cálculo de sus propios números y devuelve su beta calculada nuevamente al cliente.

El cliente y el servidor pueden calcular una clave compartida, solamente conocida por ellos.

La comunicación siguiente con respecto a esta conexión puede ser codificada utilizando esta clave calculada, compartida.

En caso de errores (fallo de mensaje de bienvenida, parámetros faltantes, etcétera), se puede devolver un mensaje de error al emisor. El mensaje de error puede ser simple, para reducir la vulnerabilidad a intentos de acceso ilícito ("hacking").

A continuación, se explicarán de manera más detallada temas relacionados con la autentificación.

Este procedimiento puede autentificar al usuario del creador o lector con respecto a la base de datos del servidor externo. Esto puede ser necesario para cada conexión entre el servidor y el creador o lector.

Después de la inicialización, los clientes pueden enviar una petición de registro (logon) de la siguiente manera:

Registro <TAB> Nombre de usuario <TAB> Contraseña <TAB> NTUsuario <TAB>NTOrdenador
Se recuerda que esta transferencia puede ser codificada
Registro -> puede definir la acción deseada
Nombre de usuario -> puede ser el nombre del usuario, es decir, elemento registrado del servicio
Contraseña-> puede ser la contraseña del usuario
NTUsuario-> puede ser el nombre del usuario del ordenador que utiliza habitualmente el emisor
NTOrdenador-> puede ser el nombre del ordenador NT al que el emisor está habitualmente registrado

El servidor puede calcular la segmentación de la contraseña transferida y puede autentificar al usuario con el nombre del usuario y la contraseña con respecto a la base de datos del miembro. Si el usuario no es autentificado, se devuelve un mensaje de error tal como "nombre de usuario desconocido" o bien "contraseña errónea". El código de retorno "OK" puede poner en marcha la fase siguiente.

En esta etapa, el protocolo puede ofrecer varias opciones. Las siguientes opciones son posibles:

- NuevoCorreo para crear una nueva transacción de mensaje
- ConseguirClave para recuperar una clave para un archivo-contenedor/receptor existente
- ConseguirEstado para recuperar información sobre el elemento corriente (estadísticas, transvers activos…). Este protocolo puede ser ampliado para proporcionar otras funciones.

A continuación se describirá la forma en la que se puede crear una nueva transferencia de mensaje.

Este método puede ser disponible después de la inicialización y autentificación satisfactorias. Puede permitir crear una nueva transacción para una transferencia de mensaje deseada. Esta opción del protocolo puede ser utilizada (solamente) por aplicaciones que crean una nueva transacción de una transferencia de mensaje deseada.
El cliente puede enviar el siguiente mensaje al servidor:

NuevoCorreo <TAB> Receptor <TAB> Tema <TAB> Segmentación <TAB> Clave <TAB>Días
Esta transferencia puede ser codificada.
NuevoCorreo-> define la acción deseada
Receptor-> puede ser la dirección de correo receptora del receptor deseado (destinatario)
Tema-> puede ser el tema del mensaje. Esto está destinado a identificación fácil en transacciones-registros.
Segmentación-> puede ser el código de segmentación calculado del archivo-contenedor completo.
Clave-> puede ser la clave necesaria para decodificar el contenido del archivo-contenedor.
Días-> puede indicar cuántos días se tendrá a disposición esta transacción para el receptor. Este valor es importante también para la creación de correos de estado por el servidor (Después de expiración se puede enviar un mensaje de aviso "correo no recogido" al origen de transferencia del mensaje, es decir, al emisor).

El servidor puede crear una nueva entrada de base de datos para crear esta transacción. La siguiente información puede ser almacenada en la base de datos en una tabla de transacción:

Transacción-ID (puede ser un número de serie para cada nueva transacción)
Usuario destinatario-ID (puede encontrarse disponible solamente si el receptor es ya conocido)
Dirección de correo electrónico del destinatario
Usuario emisor-ID
Tema
Código segmentación

Clave
Fecha-Inicio (puede ser la fecha/hora corriente del servidor)
Fecha-Terminación (puede ser la fecha del servidor corriente incrementada por el número de días para recogida)
Contador-Recogida (puede aumentar para cada recogida satisfactoria del mensaje)
Emisor-IP (puede ser una dirección IP del ordenador del cliente-emisor)
Emisor-Nombre-NT (puede ser el nombre de registro del usuario en el lado correspondiente al cliente)
Emisor- Nombre del ordenador- NT (puede ser un nombre del ordenador del usuario corriente en el lado que corresponde al cliente).

El servidor puede devolver “OK” al cliente. En caso de errores, el servidor puede informar de errores en texto normal al cliente.
La petición (“Request”) puede ser una clave para un archivo-contenedor.

Este método puede encontrarse a disposición después de la inicialización y autentificación satisfactorias. Se puede utilizar para solicitar la clave para decodificación de un archivo-contenedor. Esta petición puede ser hecha solamente por un cliente que es un solicitante que desea abrir un archivo-contenedor (programa-lector).

El cliente puede enviar el siguiente mensaje al servidor:

Conseguir-Clave <TAB> CódigoSegmentación
Se recuerda que esta transferencia puede ser codificada.
ConseguirClave-> puede definir la acción deseada
CódigoSegmentación-> puede ser el código de segmentación calculado del archivo-contenedor recibido.

El servidor puede recoger en primer lugar todas las direcciones de correo electrónico disponibles para el cliente-usuario autentificado en el momento (en este caso el receptor).

A continuación, el servidor puede solicitar a su base de datos una transacción que se pueda corresponder tanto con el código de segmentación como la dirección correcta de correo electrónico del receptor. Si esto falla, el servidor puede interrumpir la ejecución de esta función y puede devolver un mensaje de error al cliente.

Después de la correspondencia positiva del código de segmentación y de la dirección de correo electrónico, el servidor puede recuperar la clave de la base de datos.

El servidor puede crear una nueva entrada de la base de datos para archivar transacciones completas. Los siguientes valores pueden ser almacenados:

- Archivo-ID (puede ser creado automáticamente para cada nueva entrada)
- Receptor/Usuario-ID
- Dirección de correo electrónico del receptor
- Emisor/Usuario-ID
- Tema
- Código de segmentación
- Clave
- Fecha-Inicio (fecha en que ha empezado la transacción. Tomada de la tabla de transacción)
- Fecha de terminación (fecha en que termina esta transacción tal como se ha indicado en la tabla de transacción)
- Fecha de recogida (ésta puede ser la hora en que la clave ha sido recogida)
- Emisor-IP (puede ser la dirección IP del cliente- ordenador emisor; procedente de la tabla de transacción)
- Emisor- Nombre NT (puede ser el nombre de registro (“logon”) del usuario emisor; procedente de la tabla de transacción)
- Emisor- Nombre del ordenador NT (puede ser el nombre del ordenador del emisor procedente de la tabla de transacción)
- Receptor IP (puede ser la dirección IP del cliente- ordenador que ha recibido la clave)
- Receptor- Nombre NT (puede ser el nombre de registro (“logon”) del usuario actual en el lado que corresponde al cliente)
- Receptor- Nombre de ordenador NT (puede ser el nombre del ordenador del usuario actual en el lado que corresponde al cliente)

A continuación, el servidor puede transmitir la clave con el siguiente mensaje:

OK <PIPE> Clave
Se recuerda que esta transferencia puede ser codificada.
OK-> puede indicar la identificación correcta de este mensaje y transacción

<PIPE> puede ser ASCII- Char 124 (&H7C) para separar la clave de OK
Clave-> puede ser la clave necesaria para decodificar los archivos y contenido del archivo-contenedor.

Los aspectos definidos en lo anterior y otros aspectos de la invención quedarán evidentes de los ejemplos de realizaciones que se describirán a continuación y se explican con referencia a estos ejemplos de realizaciones.

La invención se describirá de manera más detallada a continuación con referencia a ejemplos de realizaciones pero a los que no queda limitada la invención.

La figura 1 muestra un sistema de comunicaciones, de acuerdo con una realización a título de ejemplo de la invención.

La figura 2 muestra un sistema de comunicaciones, de acuerdo con otro ejemplo de realización de la invención.

Las ilustraciones de los dibujos son esquemáticas.

A continuación, haciendo referencia a la figura 1, se describirá un sistema de comunicaciones 100 de acuerdo con una realización a título de ejemplo de la invención.

El sistema de comunicaciones 100 comprende una unidad emisora 101, una unidad receptora 102 y una unidad de control 103.

La unidad emisora 101 está adaptada para generar un mensaje electrónico 104 que puede ser designado también como archivo-contenedor. Además, la unidad emisora 101 puede enviar el mensaje electrónico 104 directamente a un cliente de correo 105 de la unidad receptora 102 (en la que el cliente de correo 105 puede formar parte de la unidad receptora 102). Además, la unidad emisora 101 puede enviar un mensaje de envío de información 106 a la unidad de control 103 indicando que la unidad emisora 101 ha enviado el mensaje electrónico 104 a la unidad receptora 102.

Además, la unidad receptora 102 puede recibir el mensaje electrónico 104 directamente de la unidad emisora 101 y puede enviar un mensaje de información de recepción 107 a la unidad de control 103, de manera que el mensaje 107 de información de recepción indica que un usuario de la unidad receptora 102 ha recibido el mensaje electrónico 104.

Un usuario de la unidad emisora 101 crea un correo electrónico 108 y decide enviar el correo electrónico 108 por medio del sistema de comunicación 100. Una entidad creadora de la unidad emisora 101 puede generar entonces un correo electrónico con el archivo-contenedor incorporado 104. Este archivo-contenedor 104 comprende el correo electrónico completo 108 de forma codificada. Para este objetivo, se utiliza una clave de codificación 109 en la unidad de usuario 101. El archivo-contenedor 104 contiene el mensaje incluyendo las incorporaciones. Para permitir la comprobación de la integridad de un documento, la entidad creadora puede calcular un código de segmentación del archivo-contenedor completo 104.

Además, la entidad creadora de la unidad emisora 101 establece una conexión con la unidad de control 103 (servidor) y autentifica con el nombre de usuario y contraseña del usuario de la unidad emisora 101. En este contexto, el mensaje 106 puede incluir la transmisión del código de segmentación del archivo-contenedor, un receptor, un tema, una clave de codificación 109 y cualquier otra información necesaria.

El mensaje de información de emisor 106 es enviado al servidor 103 conteniendo todas las informaciones necesarias para una transacción. La unidad de control 103 autentifica el usuario de la unidad emisora101 y/o de la unidad receptora 102 y comprueba los códigos de segmentación y contraseñas correctas. La unidad de control 103 puede enviar además la clave 109 a la unidad receptora 102 para decodificar los archivos-contenedor al receptor legítimo.

Después de la recepción del correo electrónico 104 por el cliente de correo 105 de la unidad receptora 102, la unidad receptora 102 recibe el correo electrónico que contiene el archivo-contenedor incorporado 104 que ahora puede abrir el usuario de la unidad receptora 102. Una vez que el usuario de la unidad receptora 102 abre el archivo 104, se puede poner en marcha automáticamente un lector. Antes de la primera utilización, es posible que el lector tenga que ser instalado localmente en la unidad receptora 102.

Después de que el usuario de la unidad receptora 102 ha abierto el archivo-contenedor 104, el lector se conecta al servidor 103 y autentifica al usuario de la unidad receptora 102. A continuación, el lector de la unidad receptora 102 puede calcular el código de segmentación del archivo-contenedor recibido 104 y puede pedir al servidor 103 la clave 109 para decodificar.

Cuando la autentificación de la unidad receptora 102 es aceptada por la unidad de control 103, la clave 109 es enviada desde la unidad de control 103 a la unidad receptora 102.

Además, la unidad de control 103 puede enviar un mensaje de confirmación 110 a la unidad emisora 101. Después del suministro de la clave 109, el servidor 103 envía el correo electrónico 110 a la unidad emisora 101 que confirma el suministro de la clave de decodificación 109 a la unidad receptora 102. Esto confirma que la unidad receptora 102 ha recibido y ha abierto el correo electrónico completo y no manipulado 104.

Después de recibir la clave 109, el archivo-contenedor 104 puede ser decodificado por la unidad receptora 102 y su contenido puede ser extraído. Finalmente, el archivo-contenedor 104 y los mensajes contenidos en el mismo pueden ser abiertos para tener acceso al contenido 111 del archivo 104.

A continuación, se describirá haciendo referencia a la figura 2, un sistema proveedor 200 para un correo electrónico asegurado de acuerdo con una realización a título de ejemplo de la invención.

En la realización de la figura 2, la unidad de control 103 está subdividida en una primera entidad de control 202 (un primer servidor de proveedor) acoplado con capacidad de comunicación a la unidad emisora 101 en una forma en la que la transmisión del mensaje de información de envío 106 (que comprende una clave de decodificación 109 adaptada para decodificar el mensaje electrónico codificado 104) desde la unidad emisora 101 a la primera entidad de control 202 es indicativa de la identidad del usuario de la unidad emisora 101.

La unidad de control 103 comprende además una segunda entidad de control 201 (servidor de comprobación) acoplado con capacidad de comunicación a la primera entidad de control 202. La primera entidad de control 202 está adaptada para enviar un mensaje de información de envío anónimo 204 a la segunda entidad de control 201 de manera tal que la segunda entidad de control 201 no está enterada de la identidad del usuario de la unidad emisora 101.

Además, la unidad de control 103 comprende una tercera entidad de control 203 (un segundo servidor del proveedor) acoplado con capacidad de comunicación a la unidad receptora 102 de manera tal que una transmisión de un mensaje 107, 109 de un receptor entre la unidad receptora 102 y la tercera entidad de control 203 es indicativa de la identidad de un usuario de la unidad receptora 102. El mensaje del receptor 107, 109 puede comprender una clave de decodificación adaptada para decodificar el mensaje electrónico codificado 104.

La tercera entidad de control 203 está acoplada con capacidad de comunicación a la segunda entidad de control 201, de manera que la segunda entidad de control 201 está adaptada para intercambiar datos 205 con la tercera entidad de control 203, de manera tal que la segunda entidad de control 201 no está enterada de la identidad del usuario de la unidad receptora 102.

De este modo, el sistema de comunicación 200 es un sistema de gestión de transacción anónimo, más particularmente un sistema de comprobación anónimo.

La unidad de comprobación 201 permite la gestión de la transacción de la clave de manera anónima. Los datos de la clave son transmitidos de manera anónima después del recepción desde la primera entidad de control 202 o después de la petición desde la tercera entidad de control 203. Solamente los servidores de proveedor 202, 203 que pueden ofrecer sus servicios independientemente desde la unidad de comprobación que realiza la intermediación 201 conocen las identidades de sus respectivos clientes 101, 102. Por lo tanto, el intercambio de clave controlado por la unidad de comprobación 201 es anónimo, mientras que la primera entidad de control 202 conoce datos que caracterizan su cliente 101 y la tercera entidad de control 203 conoce datos que caracterizan su cliente 102. La unidad de comprobación 201 es un “socio de confianza” que lleva a cabo transacciones relacionadas sin saber la identidad de los elementos que se encuentran en comunicación 101, 102.

Una transmisión satisfactoria de la clave de decodificación desde la segunda entidad de control 201 a la tercera entidad de control 203 y desde allí a la unidad receptora 102 puede tener como resultado la transmisión de un mensaje notificador o de confirmación desde la tercera entidad de control 203 o desde la unidad receptora 102 a la segunda entidad de control 201 o a la primera entidad de control 202 o a la unidad emisora 101.

Un historial de transacción indicador de cualquier comunicación entre la primera entidad de control 202 y la segunda entidad de control 201 puede estar almacenado en memorias de ambas entidades 202, 201 de manera que cualquier comunicación puede ser objeto de seguimiento más tarde. De acuerdo con ello, un historial de transacción que indica cualquier comunicación entre la tercera entidad de control 203 y la segunda entidad de control 201 puede ser almacenado en memorias de ambas entidades 201, 203 de manera que se puede efectuar el seguimiento de cualquier comunicación más tarde. Por lo tanto, cuando se consideran los historiales de transacción, será posible reconstruir cualquier comunicación incluyendo la identidad de la unidad emisora 101 almacenada en la primera entidad de control 202 y/o la identidad de la unidad receptora 102 almacenada en la tercera unidad de control 203.

A continuación, se describirán de manera más detallada varios aspectos del sistema de comunicaciones 200.

Por el sistema de comprobación 200, se puede soportar un número esencialmente no imitado de proveedores 202, 203 (dos, tres o más):

- esto permite la disponibilidad global de este sistema de correo electrónico asegurado 200 con intermedio de distintos usuarios 101, 102 (dos, tres o más)
- el primer usuario 101 puede enviar un correo electrónico asegurado 104 al segundo usuario 102 que puede tener acceso al mismo aunque el primer usuario 101 y el segundo usuario 102 utilicen el servicio de diferentes proveedores de servicio 202, 203.
- los proveedores de servicio 202, 203 mantienen la privacidad de sus relaciones con los clientes (emisor 101, receptor 102)
- la unidad de servicio de comprobación 201 controla solamente datos de transacción anónimos 204, 205 y no tiene acceso a ningún dato de cliente.

El sistema de comprobación 200 puede estar organizado en tres capas:

En una capa de usuario 101, 102,_ se pueden utilizar las solicitudes “creador” y “lector” para crear, enviar y leer los mensajes 104, 106, 107, 109 .

En una capa de proveedor, un proveedor 202, 203 pone en marcha las aplicaciones de servidor a las que se conectan todos los usuarios 101, 102 (proveedor-servidor). El proveedor 202, 203 organiza también y controla los datos de cliente y todos los datos necesarios para el sistema 200.

Los proveedores 202, 203 pueden comunicar con la capa 201 de comprobación para intercambiar información de transacción. Cada proveedor 202, 203 envía (o recibe) información 204, 205 necesaria para gestionar una nueva transacción anónima al servicio de comprobación 201.

En la capa de comprobación 201, las transacciones anónimas de cada proveedor 202, 203 son gestionadas para garantizar el intercambio de información de transacción a través de los proveedores 202, 203.

El sistema de comprobación 201 puede contener las siguientes informaciones:

- código de segmentación del contenedor de transacción para verificar la transmisión y mensaje correctos
- clave para decodificar el mensaje (clave de transacción)
- código de segmentación de la dirección de correo del receptor para verificar que el receptor es correcto
- código de identificación para controlar la gestión de transacciones
- fecha para el fin de la transacción
- información respecto al emisor (autentificación-estado)
- código de identificación del proveedor emisor

A continuación, se describirá la forma en la que el receptor 102 de un correo electrónico tendrá acceso a este correo electrónico.

Si un servidor 203 del proveedor recibe la petición de una clave de transacción del usuario receptor 102, enviará una petición 205 al servidor de comprobación 201 al someter el código de segmentación del mensaje. El servidor de comprobación 201 facilitará la clave, códigos de segmentación, códigos de segmentación del receptor y otras informaciones con respecto a cada transacción activa que corresponden al código de segmentación sometido por el proveedor 203 del receptor 102. El proveedor 203 comprueba estos resultados y compara los códigos de segmentación de las direcciones de correo del receptor con los códigos de segmentación devueltos por el servidor de comprobación 201. Si existe correspondencia, el proveedor 203 del receptor 102 facilitará la clave al receptor 102 y confirmará el compromiso de suministro al servidor de comprobación 201. El servidor de comprobación 201 almacena este compromiso en una tabla de notificación especial asignada a cada uno de los proveedores 202, 203.

Cada proveedor 202, 203 pide su tabla de notificación actual en un intervalo reducido. Si el proveedor-servidor 202, 203 recibe esta notificación, puede poner en marcha una notificación al usuario emisor 101 sobre el suministro satisfactorio de la transacción.

A continuación, se explicará una característica relativa a la puesta en vigor de incorporaciones de documentos.

El sistema 200, más particularmente el proveedor-servidor 202 puede ofrecer opcionalmente la posibilidad de forzar al creador 101 para que añada incorporaciones.

De acuerdo con una realización a título de ejemplo, esto se puede evitar por el usuario y es controlado por el administrador del proveedor- servidor 202. Utilizando este mecanismo, el creador 101 puede ser forzado a añadir certificados de legitimidad firmados digitalmente.

En la realidad, puede ser el proveedor-servidor 202 que obligue a la adición de la incorporación. Además, la característica de una incorporación obligatoria es opcional y puede ser activada o desactivada por el usuario o un administrador del sistema. Opcionalmente, un proveedor puede dejarlo a la disposición de un usuario para activar o desactivar la característica de una incorporación obligatoria (con intermedio de un interfaz de web). Además, un usuario puede definir un sub-usuario (usuario secundario). Entonces, es posible asignar los documentos al sub-usuario que no puede evitar la incorporación ni alterar su correspondiente colocación.

Estos certificados pueden incluir derechos y restricciones mantenidos por las organizaciones de las que es miembro el usuario 101, por ejemplo, para órdenes o restricciones de competencia del usuario 201, tal como “el usuario está autorizado a comprar artículos hasta un valor de…”

Una ventaja es que ningún usuario de este proveedor-servidor 202 necesita software para gestionar certificados, bloquear listas o hardware para leer tarjetas inteligentes para firma digital. En realidad, el usuario 101 no necesita siquiera reunir un certificado legalmente vinculante PKI. Cada mensaje enviado por el usuario 101 es firmado de forma legalmente vinculante por la empresa mediante el certificado de legitimidad añadido y firmado digitalmente.

Se debe observar que el término “comprende” no excluye otros elementos o etapas y el “un” o “uno” no excluye varios. Asimismo, se pueden combinar elementos descritos en asociación con diferentes realizaciones.

Se debe observar que los signos de referencia en las reivindicaciones no estarán considerados como limitativos del alcance de las mismas.

REIVINDICACIONES

1. Sistema de comunicaciones que comprende
una unidad emisora (101);
una unidad receptora(102); y
una unidad de control (103)
en el que la unidad emisora (101) está adaptada para generar un mensaje electrónico (104) a transmitir a la unidad receptora (102) y para enviar un mensaje de información de envío (106) a la unidad de control (103) indicando que la unidad emisora ha enviado el mensaje electrónico (104) a la unidad receptora (102):
en el que la unidad receptora (102) está adaptada para recibir el mensaje electrónico (104) y enviar un mensaje (107) de información de recepción a la unidad de control (103), indicando el mensaje de información de recepción(107) que un usuario de la unidad receptora (102) ha recibido el mensaje electrónico (104):
en el que la unidad emisora (101) está adaptada para generar el mensaje electrónico como mensaje electrónico codificado al codificar datos electrónicos, utilizando una clave;
en el que la unidad emisora (101) está adaptada para generar una huella dactilar del mensaje electrónico, permitiendo a la huella dactilar la identificación no ambigua del mensaje electrónico y para enviar la huella dactilar a la unidad de control (103), como mínimo, como parte del mensaje de información de envío;
en el que la unidad emisora (101) está adaptada para enviar la clave a la unidad de control, como mínimo, como parte del mensaje de información de envío, estando adaptada la clave para decodificar el mensaje electrónico codificado;
en el que la unidad receptora (102) está adaptada para generar una huella dactilar del mensaje electrónico, permitiendo a la huella dactilar la identificación no ambigua del mensaje electrónico, y para enviar la huella dactilar a la unidad de control;
en el que la unidad de control (103) está adaptada para comparar la huella dactilar generada por la unidad receptora y la huella dactilar generada por la unidad emisora, y
en el que la unidad de control (103) está adaptada para poner en marcha el envío de la clave a la unidad receptora solamente cuando hay correspondencia positiva de las huellas dactilares.

2. Sistema de comunicaciones, según la reivindicación 1,
en el que la unidad emisora (101) está adaptada para notificar un evento en el que un usuario de la unidad receptora (102) ha tenido acceso al mensaje electrónico (104).

3. Sistema de comunicaciones, según cualquiera de las reivindicaciones 1 a 2,
en el que la unidad emisora (101) está adaptada para notificar un evento en el que un usuario de la unidad receptora (102) no ha tenido acceso al mensaje electrónico (104) durante un intervalo de tiempo que supera un intervalo de tiempo umbral predeterminado.

4. Sistema de comunicaciones, según cualquiera de las reivindicaciones 1 a 3,
en el que la unidad de control (103) comprende una primera entidad de control (202) acoplada con capacidad de comunicación a la unidad emisora (101) de manera que una transmisión de un mensaje de emisor desde la unidad emisora (101) a la primera entidad de control (202) es indicativa de la identidad de la unidad emisora (101);
en el que la unidad de control (103) comprende una segunda entidad de control (201) acoplada con capacidad de comunicación a la primera entidad de control (202); y
en el que la primera entidad de control (202) está adaptada para enviar el mensaje de emisor a la segunda entidad de control (201) de manera que la segunda entidad de control (201) no está enterada de la identidad de la unidad emisora (101).

5. Sistema de comunicaciones, según la reivindicación 4,
en el que el mensaje de emisor es el mensaje de información de envío (106), particularmente, es un mensaje de información de envío que comprende la clave (109) adaptada para decodificar el mensaje electrónico codificado (104).

6. Sistema de comunicaciones, según las reivindicaciones 4 ó 5,
en el que la unidad de control (103) comprende una tercera entidad de control (203) acoplada con capacidad de comunicación a la unidad receptora (102) de manera que una transmisión de un mensaje de receptor entre la unidad receptora (102) y la tercera entidad de control (203) es indicativa de la identidad de la unidad receptora (102);
en el que la tercera entidad de control (203) está acoplada con capacidad de comunicación a la segunda entidad de control (201);
en el que la tercera entidad de control (203) está adaptada para intercambiar datos con la segunda entidad de control (201) de manera que la segunda entidad de control (201) no está enterada de la identidad de la unidad receptora (102).

7. Sistema de comunicaciones, según la reivindicación 6;

en el que el mensaje del receptor comprende, como mínimo, uno del grupo que consiste en el mensaje de información de recepción (107) y la clave (109) adaptada para decodificar el mensaje electrónico codificado (104).

8. Sistema de comunicaciones, según cualquiera de las reivindicaciones 4 a 7, en el que, como mínimo, uno del grupo que consiste en la primera entidad de control (202) y la tercera entidad de control (203) es una unidad proveedora.

9. Sistema de comunicaciones, según cualquiera de las reivindicaciones 4 a 8, en el que la primera entidad de control (202) y la tercera entidad de control (203) son unidades proveedoras distintas.

10. Sistema de comunicaciones, según cualquiera de las reivindicaciones 4 a 9, adaptado como sistema de gestión de transacción anónima, particularmente como sistema de comprobación anónimo.

11. Sistema de comunicaciones, según cualquiera de las reivindicaciones 1 a 10, en el que, como mínimo, uno del grupo que consiste en la unidad emisora (101), la unidad receptora (102) y la unidad de control (103) está adaptado para impedir accesibilidad a la información incluida en el mensaje electrónico (104) en el caso en que falte una incorporación predeterminada al mensaje electrónico (104).

12. Sistema de comunicaciones, según cualquiera de las reivindicaciones 1 a 10, en el que la unidad emisora (101) está adaptada para la incorporación obligatoria de una incorporación predeterminada al mensaje electrónico (104).

13. Sistema de comunicaciones, según la reivindicación 11 ó 12, en el que la incorporación predeterminada comprende, como mínimo, uno del grupo que consiste en una identificación de un usuario de una unidad emisora (101), una autentificación de un usuario de la unidad emisora (101), una obligación de un usuario de la unidad emisora (101) y un logotipo que caracteriza un usuario de la unidad emisora (101).

14. Sistema de comunicaciones, según cualquiera de las reivindicaciones 1 a 13, en el que la huella digital es un código de segmentación.

15. Procedimiento de comunicaciones que comprende:
generar un mensaje electrónico (104) como mensaje electrónico codificado al codificar datos electrónicos por medio de una unidad emisora (101) utilizando un clave.
generar, por medio de la unidad emisora, una huella dactilar del mensaje electrónico, permitiendo la huella dactilar la identificación no ambigua del mensaje electrónico; transmitiendo el mensaje electrónico (104) a una unidad receptora (102),
enviar un mensaje de envío de información (106) desde la unidad emisora (101) a una unidad de control (103) indicando que la unidad emisora ha enviado el mensaje electrónico (104) a la unidad receptora (102);
enviar la clave desde la unidad emisora (101) a la unidad de control (103) como una parte, como mínimo, del mensaje de información de envío, estando adaptada la clave para decodificar el mensaje electrónico codificado;
enviar la huella dactilar generada por la unidad emisora (101) desde la unida emisora (101) a la unidad de control (103) como parte, como mínimo, del mensaje de información de envío;
recibir, por medio de la unidad receptora (102), el mensaje electrónico (104);
generar, por medio de la unidad receptora (102), una huella dactilar del mensaje electrónico, permitiendo la huella dactilar la identificación no ambigua del mensaje electrónico;
enviar la huella dactilar generada por la unidad receptora (102) desde la unidad receptora (102) a la unidad de control (103);
enviar un mensaje de información de recepción(107) desde la unidad receptora (102) a la unidad de control (103), indicando el mensaje de información de recepción(107) que un usuario de la unidad receptora (102) ha recibido el mensaje electrónico (104);
comparar, por medio de la unidad de control (103) la huella dactilar generada por la unidad receptora (102) y la huella dactilar generada por la unidad emisora (101) por medio de la unidad de control (103), poniendo en marcha el envío de la clave desde la unidad de control (103) a la unidad receptora (102) solamente después de correspondencia positiva de las huellas dactilares.

16. Elemento de programa que cuando es llevado a cabo por el sistema de comunicaciones de las reivindicaciones 1 a 14, está adaptado para controlar o llevar a cabo el procedimiento de comunicaciones de la reivindicación 15.

17. Soporte que puede ser leído por ordenador, en el que se ha almacenado un programa de ordenador que, cuando es llevado a cabo por el sistema de comunicaciones de las reivindicaciones 1 a 14, está adaptado para controlar o llevar a cabo el procedimiento de comunicaciones de la reivindicación 15.

18. Unidad de control para un sistema de comunicaciones,
en el que la unidad de control (103) está adaptada para recibir un mensaje de información de envío desde una unidad emisora (101), indicando el mensaje de información de envío (106) que un mensaje electrónico (104) ha sido enviado a una unidad receptora (102) y está adaptado para recibir un mensaje de información de recepción desde la unidad receptora (102), indicando el mensaje de información de recepción que un usuario de la unidad receptora (102) ha recibido el mensaje electrónico (104), de manera que el mensaje electrónico es generado como mensaje electrónico codificado al codificar datos electrónicos utilizando una clave
en el que la unidad de control (103) está adaptada para recibir desde la unidad emisora (101), como mínimo, como parte del mensaje de información de envío, una huella dactilar del mensaje electrónico, permitiendo la huella dactilar la identificación no ambigua del mensaje electrónico;
en el que la unidad de control (103) está adaptada para recibir desde la unidad emisora (101), como mínimo, como parte del mensaje de información de envío la clave, estando adaptada la clave para decodificar el mensaje electrónico codificado;
en el que la unidad de control (103) está adaptada para recibir desde la unidad receptora (102) una huella dactilar del mensaje electrónico, permitiendo la huella dactilar la identificación no ambigua del mensaje electrónico;
en el que la unidad de control (103) está adaptada para comparar la huella dactilar generada por la unidad receptora y la huella dactilar generada por la unidad emisora, y
en el que la unidad de control (103) está adaptada para poner en marcha el envío de la clave a la unidad receptora solamente después de una correspondencia positiva de las huellas dactilares.

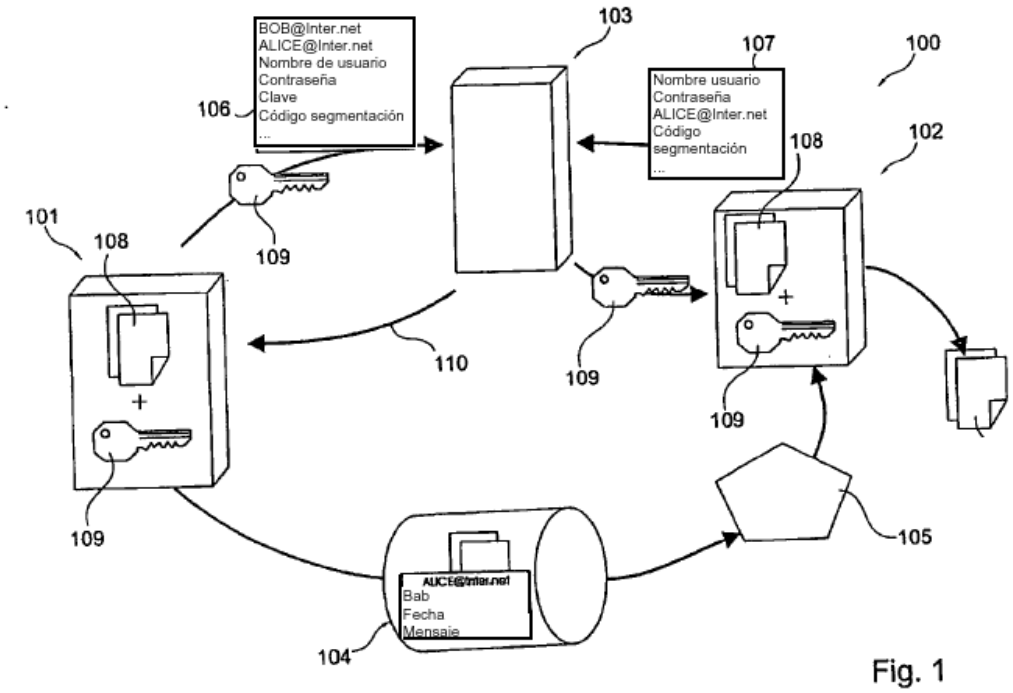
BOB@Inter.net
ALICE@Inter.net
Nombre de usuario
Contraseña
Clave
Código segmentación
...
106
103
107
Nombre usuario
Contraseña
ALICE@Inter.net
Código
segmentación
...
100
102
108
101
108
109
110
109
109
109
105
ALICE@Inter.net
Bab
Fecha
Mensaje
104

Fig. 1

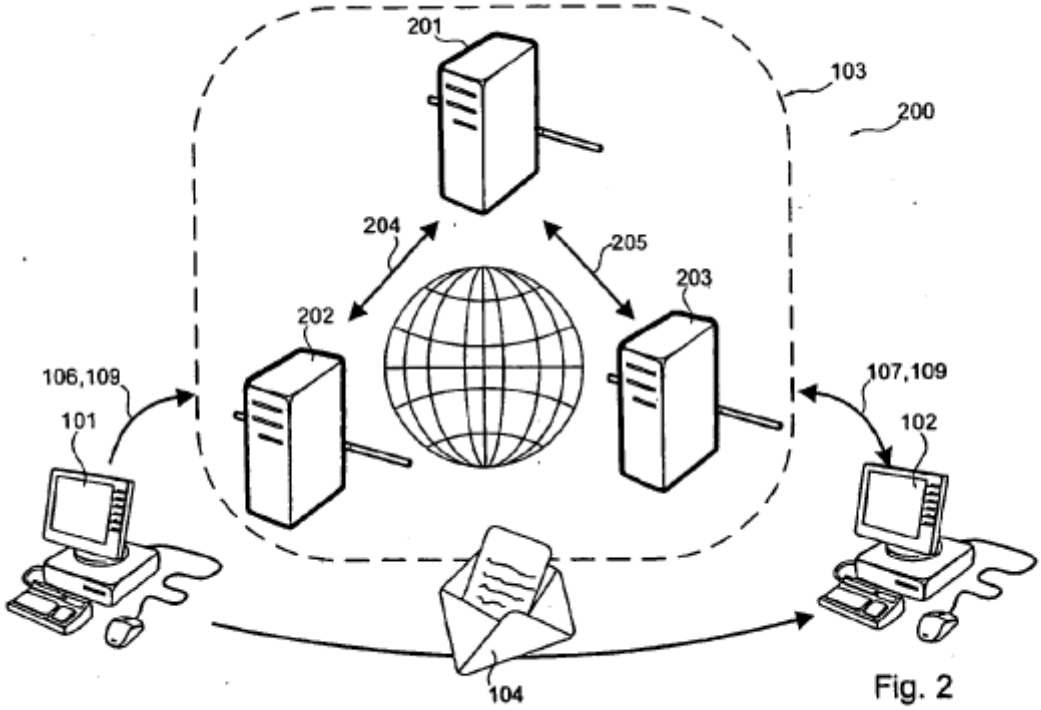

Fig. 2