(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 801 902**

(51) Int. CI.:

H04L 12/58 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **25.07.2018 E 18185617 (0)**

(97) Fecha y número de publicación de la concesión europea: **08.04.2020 EP 3435601**

(54) Título: **Sistema de mensajería certificado y método**

(30) Prioridad:

25.07.2017 IT 201700085021

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
14.01.2021

(73) Titular/es:

INFOCERT S.P.A. (100.0%)
Piazza Sallustio, 9
00187 Roma, IT

(72) Inventor/es:

RUGGIERO, ALESSIO ANTONIO;
MARCOLONGO, IGOR;
PONZI, FLORENTINA y
VERATELLI, ALBERTO

(74) Agente/Representante:

CARVAJAL Y URQUIJO, Isabel

DESCRIPCIÓN

Sistema de mensajería certificado y método

Campo técnico de la invención

La presente invención se relaciona con un método para certificar mensajes intercambiados a través de un sistema/servicio de mensajería entre dos o más usuarios, o entre un usuario y un agente de software inteligente, o entre dos agentes de software inteligentes. Adicionalmente, la presente invención también se relaciona con un sistema y servicio de mensajería certificado.

Estado de la técnica

Como es conocido, hoy en día hay innumerables sistemas y servicios disponibles que permiten el intercambio de mensajes entre usuarios a través de redes de telecomunicaciones, en particular las redes de Internet y/o telefonía móvil. Ejemplos universalmente conocidos de tales sistemas/servicios de mensajería son el servicio provisto por redes de telefonía móvil comúnmente conocidos como SMS (del inglés "Short Message Service"), el servicio de correo electrónico y sistemas/servicios de mensajería instantánea (por ejemplo, WhatsApp Messenger).

Todos estos sistemas/servicios de mensajería permiten el intercambio de mensajes de texto; muchos también permiten el intercambio de mensajes de audio y/o vídeo, así como el envío de contenido multimedia (tales como imágenes, fotos, vídeos, audio, archivos de música, enlaces, ubicaciones geográficas, tarjetas de presentación electrónicas, documentos de texto o incluso otros documentos, etc.).

Típicamente, los sistemas/servicios de mensajería antes mencionados requieren el uso de programas o aplicaciones de software específicos (las denominadas Apps) que los usuarios deben instalar en sus dispositivos de comunicación electrónica (tal como, por ejemplo, teléfonos inteligentes, tabletas, ordenadores portables, PCs de escritorio, televisores inteligentes, relojes inteligentes, etc.).

Algunos sistemas/servicios de mensajería también están disponibles a través de la web a través de aplicaciones web específicas (las denominadas apps web) accesibles a través de programas/aplicaciones de software para la navegación web (los denominados navegadores web o simplemente navegadores).

Hoy en día, también se conocen sistemas/servicios de mensajería en los cuales son usados los denominados agentes de software inteligentes (en general conocidos como *bots de conversación*, *bots de charla*, *bots conversacionales*, o simplemente *Bots*) capaces de mantener conversaciones inteligentes con humanos intercambiando mensajes de texto y/o mensajes de audio y/o mensajes de audio y vídeo. Estos agentes de software inteligentes (de aquí en adelante simplemente denominados como agentes inteligentes) son usados típicamente con propósitos de asistencia remota, para la provisión de información/datos de manera automática y también con propósitos comerciales.

En vista del uso creciente de sistemas/servicios de mensajería, en los últimos años se han desarrollado diversas soluciones tecnológicas que buscan certificar, de manera más o menos efectiva, el intercambio de mensajes entre dos usuarios.

Por ejemplo, en Italia el denominado Correo Electrónico Certificado (PEC) es usado ampliamente para certificar el envío y suministro de un mensaje.

Se proporcionan ejemplos de cómo puede tener lugar el intercambio de mensajes entre dos partes en el documento US 2016/0191513 A1 que describe métodos y sistemas para vincular una transacción de datos a una identidad de la persona usando biometría. De hecho, aunque el documento US 2016/191513 A1 se relaciona con un tema totalmente diferente al de la presente invención, este documento describe muchas características conocidas en el campo de la mensajería, tal como intercambiar datos en forma encriptada desde y enviar mensajes y resúmenes correspondientes desde los dispositivos de cliente a un servidor.

Objeto y resumen de la invención

El Solicitante ha indicado que hoy en día no hay sistema/servicio capaz de certificar de manera efectiva el intercambio de mensajes entre dos o más partes, por ejemplo, entre dos o más usuarios, o entre uno o más usuarios y uno o más agentes inteligentes, o entre dos o más agentes inteligentes.

En particular, no hay sistema/servicio capaz de certificar de manera efectiva la identidad de aquellos que intercambian mensajes a través de un sistema/servicio de mensajería, la integridad del contenido intercambiado, la fecha y hora de envío, recepción y lectura de mensajes, así como el orden de envío de mensajes intercambiados.

El Solicitante sintió así la necesidad de desarrollar tal sistema/servicio, llegando de esa manera a la presente invención.

Por consiguiente, un objeto general de la presente invención es proporcionar un método y un sistema para certificar de manera efectiva un intercambio de mensajes entre dos o más partes a través de un sistema de mensajería, por

ejemplo, entre dos o más usuarios, o entre uno o más usuarios y uno o más agentes inteligentes, o entre dos o más sistemas que interactúan entre sí a través de agentes inteligentes.

En particular, un objeto específico de la presente invención es proporcionar un método y un sistema para certificar de manera efectiva los contenidos (es decir, la integridad de los contenidos) de mensajes intercambiados entre dos o más partes a través de un sistema/servicio de mensajería, así como el orden exacto de los mensajes intercambiados.

Además, un objeto secundario de la presente invención es proporcionar un método y un sistema para certificar de manera efectiva la identidad de aquellos que intercambian mensajes, así como la fecha y hora de envío, recepción y lectura de mensajes.

Estos y otros objetos son logrados mediante la presente invención en cuanto a lo que se relaciona con un método para certificar mensajes intercambiados entre dos o más partes a través de un sistema de mensajería, como está definido en las reivindicaciones anexas.

Breve descripción de los dibujos

Para un mejor entendimiento de la presente invención, algunas realizaciones preferidas, proporcionadas puramente a modo de un ejemplo explicativo y no limitante, se ilustrarán ahora con referencia a los dibujos acompañantes (no a escala), en donde las figuras 1 y 2 ilustran esquemáticamente un sistema de mensajería certificado de acuerdo con una realización preferida de la presente invención.

Descripción detallada de realizaciones preferidas de la invención

La siguiente descripción se proporciona para permitir a una persona experimentada en la técnica hacer y usar la invención. Diversas modificaciones a las realizaciones presentadas serán inmediatamente evidentes para la persona experimentada en la técnica y los principios generales descritos pueden ser aplicados a otras realizaciones y aplicaciones mientras que permanezcan dentro del alcance de protección de la presente invención, como está definido en las reivindicaciones anexas.

Por lo tanto, la presente invención no debe considerarse limitada a las realizaciones descritas y mostradas, sino que se le da un alcance más amplio de protección de acuerdo con los principios y características presentados y definidos en las reivindicaciones anexas.

La presente invención se relaciona, en primer lugar, con un método para certificar un intercambio de mensajes entre al menos dos partes (las cuales de manera conveniente conversan a través de un sistema/servicio de mensajería), en donde cada mensaje es intercambiado:

• enviando el mensaje desde un remitente respectivo a un servidor, en donde dicho remitente respectivo es

- un primer usuario que usa un primer dispositivo de comunicación electrónica, o

- un primer agente de software inteligente; y

• enviando el mensaje desde el servidor a al menos un receptor respectivo, en donde dicho receptor respectivo es

- un segundo usuario que usa un segundo dispositivo de comunicación electrónica, o

- un segundo agente de software inteligente.

Además, para cada mensaje intercambiado, el remitente respectivo también envía al servidor un resumen correspondiente calculado aplicando una primera función de direccionamiento predefinida al mensaje.

De acuerdo con la presente invención, el servidor almacena los mensajes intercambiados y los resúmenes correspondientes en el orden en el cual son intercambiados dichos mensajes.

Además, el servidor, para cada mensaje intercambiado, calcula un resumen acumulativo aplicando una segunda función de direccionamiento predefinida

• al resumen que corresponde a dicho mensaje y

• a los resúmenes que corresponden a mensajes previamente intercambiados.

De esta forma, el servidor está provisto con la capacidad de certificar los contenidos y el orden de intercambio de los mensajes. De hecho, gracias al almacenamiento mediante el servidor de los mensajes intercambiados y los resúmenes correspondientes en el orden en el cual son intercambiados dichos mensajes y al uso del resumen acumulativo, se asegura que ni los contenidos de los mensajes intercambiados, ni el orden de intercambio de los mensajes, ni los resúmenes de los mensajes puedan ser manipulados (por ejemplo, con propósitos fraudulentos). Para la aplicación de la segunda función de direccionamiento predefinida a la lista de resúmenes mediante el servidor, el método para

la gestión dinámica y segura de una tabla relacional autentificada en una base de datos, descrito en la solicitud internacional del Solicitante WO 2008/035390 A2 puede ser usado de manera conveniente.

A la luz de lo que se acaba de explicar sobre la capacidad de certificación del servidor, el servidor de aquí en adelante será denominado un servidor de certificación.

De manera conveniente, el servidor de certificación:

• almacena una lista de los resúmenes que corresponden a los mensajes intercambiados actualizando dicha lista de resúmenes en cada nuevo mensaje intercambiado con el resumen que corresponde a dicho nuevo mensaje intercambiado; y

• calcula, para cada nuevo mensaje intercambiado, un nuevo resumen acumulativo aplicando la segunda función de direccionamiento predefinida a la lista actualizada de resúmenes.

De manera conveniente, el servidor de certificación firma electrónicamente la lista de resúmenes.

Preferiblemente, el servidor de certificación identifica a las partes que intercambian mensajes; adicionalmente, para cada mensaje intercambiado, el receptor respectivo envía al servidor de certificación:

• una notificación de recibo cuando es recibido el mensaje; y

• una notificación de lectura cuando es leído el mensaje.

Además, el servidor de certificación también almacena:

• las identidades de las partes que intercambian mensajes; y

• hora y fecha de envío, recepción y lectura de los mensajes intercambiados.

De esta forma, el servidor de certificación está provisto con la capacidad de certificar también las identidades de las partes que intercambian los mensajes y la hora y fecha de envío, recepción y lectura de los mensajes intercambiados.

De manera conveniente, para cada mensaje intercambiado, el remitente respectivo envía el mensaje y el resumen correspondiente al servidor de certificación en forma encriptada usando una tecnología de encriptado predefinida y el servidor de certificación envía el mensaje al receptor respectivo usando dicha tecnología de encriptado predefinida (la cual puede, por ejemplo, estar basada en claves simétricas).

Preferiblemente, el método comprende, además: tras una solicitud del remitente de un mensaje, llevar a cabo una primera función de bloqueo que, cuando está activada, no permite que el receptor responda hasta que el remitente desactive dicha primera función de bloqueo.

Preferiblemente, el método también comprende realizar una segunda función de bloqueo que, cuando está activada, no permite que un remitente de un mensaje envíe otro mensaje hasta que se haya recibido la respuesta del receptor.

Antes de proceder con la descripción de la invención, es importante especificar que en el presente documento (y, por lo tanto, dentro del alcance de la presente invención) el término "mensaje" significa cualquier tipo de mensaje o contenido digital y/o multimedia (por ejemplo, un mensaje de texto y/o audio y/o audio y/o vídeo y/o una imagen, una foto, un vídeo, un audio, un archivo de música, un enlace, una ubicación geográfica, una tarjeta de presentación electrónica, un documento/archivo de texto o incluso de otra naturaleza, etc.) que puede ser intercambiado entre dos o más usuarios, o entre uno o más usuarios y uno o más agentes inteligentes, o entre dos o más agentes inteligentes a través de un sistema/servicio de mensajería (por ejemplo SMS, correo electrónico, mensajería instantánea, mensajería de PEC, etc.).

Para un mejor entendimiento de la presente invención, las figuras 1 y 2 ilustran esquemáticamente un ejemplo de arquitectura de un sistema de mensajería certificado (denotado globalmente por el número de referencia 1) de acuerdo con una realización preferida (pero no vinculante, ni limitante) de la presente invención.

Dicho sistema 1 de mensajería certificado es propiedad, controlado y operado por un proveedor de un servicio de mensajería certificado. En resumen, dicho proveedor de servicio de mensajería certificado está indicado en las figuras 1 y 2 y de aquí en adelante en la descripción con las iniciales CMSP, abreviatura de "Proveedor de Servicio de Mensajería Certificado".

El sistema 1 de mensajería certificado incluye al menos un servidor 11 de certificación. Las figuras 1 y 2 muestran un único servidor 11 de certificación solamente, exclusivamente para facilidad de ilustración. De hecho, el sistema 1 de mensajería certificado podría incluir de manera conveniente una pluralidad de servidores 11 de certificación.

Dicho servidor 11 de certificación está programado para implementar una pluralidad de módulos lógicos, cada uno de los cuales está dedicado a una función respectiva. En particular, las figuras 1 y 2 ilustran los siguientes módulos lógicos

implementados, en uso, por el servidor 11 de certificación: un módulo 111 Autentificador, un módulo 112 de Direccionamiento, un módulo 113 de Seguimiento de Auditoría y un módulo 114 de Mensajero.

Además, el sistema 1 de mensajería certificado incluye, para cada usuario habilitado para usar el servicio de mensajería certificado, un programa de software predefinido o una App predefinida instalada en un dispositivo de comunicaciones electrónicas respectivo (por ejemplo un teléfono inteligente, una tableta, un ordenador portable, un ordenador de escritorio, un televisor inteligente, un reloj inteligente, etc.) de dicho usuario, en donde dicho dispositivo de comunicaciones electrónicas respectivo está configurado para permitir que dicho programa/app predefinido se conecte a, y se comunique con, el servidor 11 de certificación en modo inalámbrico y/o por cable, a través de una o más redes de telecomunicaciones, preferiblemente una o más redes basadas en Protocolo de Internet (IP), de manera conveniente la red de Internet (posiblemente, a través de una o más redes locales, domésticas, comerciales, públicas, privadas, etc.). Por ejemplo, dicho dispositivo de comunicaciones electrónicas respectivo puede ser de manera conveniente un teléfono inteligente, tableta o reloj inteligente que usa una o más de las siguientes tecnologías de comunicación inalámbrica: GPRS, EDGE, HSPA, UMTS, LTE, LTE Avanzada, Wi-Fi, WiMAX, etc.

En el ejemplo que se muestra en las figuras 1 y 2, un usuario A y un usuario B del sistema 1 de mensajería certificado usan, respectivamente, un primer teléfono inteligente 2 y un segundo teléfono inteligente 3 en los cuales ambos han instalado la App predefinida de dicho sistema 1 de mensajería certificado (en la figura 1, App A instalada en el primer teléfono inteligente 2 del usuario A, App B instalada en el segundo teléfono inteligente 3 del usuario B).

De manera conveniente, el sistema 1 de mensajería certificado puede usar programas/apps de tipo independiente, y/o versiones de SDK (acrónimo de la expresión bien conocida en inglés "*Software Development Kit*"), es decir como módulo para ser integrado en sistemas de mensajería tradicionales no certificados preexistentes (por ejemplo, SMS, correo electrónico, sistemas de mensajería instantánea, etc.), o en modo extra a las solicitudes/productos del Solicitante.

Más en general, el CMSP podría ser de manera conveniente un proveedor de un servicio de mensajería no certificado que se equipa por sí mismo con la presente invención para proporcionar, tras solicitud, también el servicio de mensajería certificado de acuerdo con la presente invención. De lo contrario, el CMSP podría ser un tercero que, cuando sea requerido, proporciona el servicio de mensajería certificado de acuerdo con la presente invención para certificar los mensajes intercambiados a través de sistemas/servicios de mensajería de otros proveedores.

El funcionamiento del sistema 1 de mensajería certificado se describirá en detalle a continuación.

En particular, primero se realiza una etapa de identificación y registro de los usuarios. En el ejemplo que se muestra en la figura 1, los usuarios A y B usan directamente las Apps A y B para realizar la identificación y registro a través del módulo 111 Autentificador del servidor 11 de certificación. De acuerdo con una realización alternativa de la invención, la identificación y registro de usuario también podrían ser realizadas a través de un sitio web de CMSP/portal de Internet usando un navegador web.

Como se ilustra en la figura 1, el módulo 111 autentificador está de manera conveniente conectado a los sistemas 4 de identificación y autentificación con los cuales se comunica y coopera con el fin de realizar tanto la identificación de usuarios A y B como luego, una vez completada la identificación y registro de usuarios A y B, también la autentificación de estos últimos siempre que tengan la intención de usar el servicio de mensajería certificado proporcionado por el sistema 1.

Con el fin de identificar a un nuevo usuario, se pueden explotar de manera conveniente diferentes métodos de identificación, por ejemplo: el Sistema Público de Identidad Digital (SPID), la Tarjeta Nacional de Servicios (CNS), la Tarjeta de Identidad Electrónica emitida por un Estado, sistemas de identidad digital públicos o privados, métodos de identificación *de visu*, identificación basada en sistemas de videoconferencia italianos (tal como, por ejemplo, las técnicas de identificación descritas en la patente Italiana No. 1418080 y en EP3455765), etc.

Al final del proceso de identificación, los usuarios A y B pueden elegir, para el acceso subsecuente al servicio, un sistema de autentificación de ordenador ya usado previamente (por ejemplo SPID), o elegir usar un conjunto de credenciales de autentificación fuertes (por ejemplo identificación con Tarjeta de Identidad Electrónica y autentificación con credenciales elegidas por el usuario más contraseñas de único uso ("Contraseña de Una Vez" - OTP)), o incluso elegir usar sistemas de autentificación basados en biometría (huella digital, huella facial, voz, etc.). Para la autentificación de usuario, también podría usarse de manera conveniente una integración de modo de inicio de sesión único (SSO) con sistemas de autentificación comunes.

La fase de autentificación es realizada cuando el usuario A o B desea usar la App A/B para utilizar el servicio de mensajería certificado. La fase de autentificación, llevada a cabo en cooperación con el módulo 111 Autentificador del servidor 11 de certificación, puede involucrar el uso de OTP (por ejemplo, de tipo de impulso, a través de SMS, contraseña física o virtual (es decir tipo de App), etc.).

Una vez que se han realizado la identificación, registro (con aceptación relativa de los términos contractuales del servicio de mensajería certificado) y autentificación, el módulo 111 Autentificador también registra los teléfonos inteligentes 2 y 3 de usuarios A y B y envía a las Apps A y B una "siembra" respectiva para inicializar un generador de

números pseudoaleatorio (PRNG) respectivo el cual genera las claves que serán usadas para encriptar las comunicaciones con el servidor 11 de certificación. En esta etapa, el usuario A puede asociar de manera única el primer teléfono inteligente 2 con la App A y el usuario B puede asociar de manera única el segundo teléfono inteligente 3 con la App B.

Cuando el usuario A desea tener una conversación certificada con el usuario B, él abre la App A y se autentifica él mismo, luego la App A le pide al usuario A (por ejemplo, a través de una interfaz gráfica de usuario) que elija el tipo de conversación deseada: certificada, o en modo estándar en donde no se proporcionan mecanismos de certificación.

Si el usuario A elige el modo certificado, la App A permite al usuario A intercambiar mensajes de texto y/o contenido multimedia (tal como, por ejemplo, imágenes, fotos, vídeos, audio, archivos de música, enlaces, ubicaciones geográficas, tarjetas de presentación electrónicas, documentos/archivos de texto o incluso otros tipos de archivos, etc.) con el usuario B a través del servidor 11 de certificación el cual certifica la conversación.

A este respecto, la App A podría configurarse de manera conveniente para permitir que el usuario A envíe su ubicación geográfica (calculada de manera conveniente mediante el primer teléfono inteligente 2 por medio de un receptor de GNSS respectivo) (acrónimo de la expresión bien conocida en inglés "*Global Navigation Satellite System*"), por ejemplo, del tipo de GPS, GALILEO, GLONASS, etc.) para el usuario B, implementando de manera ventajosa un método de geolocalización certificado.

En particular, con referencia a la figura 2, para cada mensaje que el usuario A desea enviar al usuario B durante una conversación certificada, la App A está configurada para:

• aplicar una primera función de direccionamiento predefinida (es decir algoritmo) al mensaje, generando de esa manera un resumen correspondiente; y

• enviar al servidor 11 de certificación el mensaje y el resumen correspondiente en forma encriptada (de manera conveniente, usando una clave de encriptado generada por el PRNG respectivo).

El servidor 11 de certificación también incluye un PRNG que corresponde al de la App A e inicializado sobre la base de la misma siembra, siendo así capaz de desencriptar los mensajes y resúmenes correspondientes recibidos de la App A. Lo mismo se aplica a la App B. Como resultado, las comunicaciones entre el servidor 11 de certificación y las Apps A y B tienen lugar a través de canales de comunicación respectivos protegidos mediante técnicas de encriptado respectivas. Se pueden usar de manera conveniente mecanismos de encriptado y derivación de siembra (es decir del tipo de "peritazgo") para asegurar la seguridad del canal de transmisión. Donde estén presentes, las claves pueden ser historizadas de manera conveniente con un sistema de archivo seguro.

En uso, el módulo 112 de Direccionamiento almacena:

• una lista (por ejemplo, en la forma de un arreglo) de resúmenes que se relacionan con los mensajes intercambiados por los usuarios A y B durante la conversación certificada y que son enviados al servidor 11 de certificación mediante las Apps A y B junto con los mensajes a los cuales se refieren; y

• un resumen acumulativo calculado aplicando una segunda función de direccionamiento predefinida (es decir algoritmo) a dicha lista de resúmenes (la cual puede ser igual a, o diferente de, la primera función de direccionamiento predefinida).

Además, para cada nuevo mensaje y resumen correspondiente enviado desde la App A al servidor 11 de certificación, el módulo 112 de Direccionamiento está configurado para:

• actualizar la lista de resúmenes incluyendo, en dicha lista, el nuevo resumen recibido de la App A; y

• aplicar dicha segunda función de direccionamiento predefinida a la lista actualizada de resúmenes, generando así un nuevo resumen acumulativo correspondiente.

Preferiblemente, el módulo 112 de Direccionamiento está configurado, cada vez que es actualizada la lista de resúmenes, para firmar electrónicamente la lista actualizada (es decir el archivo relativo que contiene dicha lista actualizada) y/o cada nuevo resumen acumulativo generado. Para este fin, el módulo 112 de Direccionamiento puede usar de manera conveniente una función predefinida de Firma Electrónica Calificada (QES) o Firma Electrónica Avanzada (AES), y/o una función predefinida de Sello Electrónico Calificado (QSEAL) o Sello Electrónico Avanzado (ASEAL), con base en una infraestructura de clave pública (PKI) o no. Por ejemplo, el módulo 112 de Direccionamiento podría configurarse de manera conveniente para implementar el método avanzado de firma electrónica basado en voz descrito en el documento EP3316162.

Además, para cada nuevo mensaje y resumen correspondiente enviado por la App A al servidor 11 de certificación, el módulo 114 de Mensajero está configurado para enviar a la App B dicho nuevo mensaje en forma encriptada (de manera conveniente, usando una clave de encriptado generada por el PRNG que corresponde a la de la App B e inicializada sobre la base de la misma siembra).

En uso, el módulo 114 de Mensajero almacena:

• una lista de mensajes intercambiados por los usuarios A y B durante la conversación certificada; y,

• para cada mensaje, una marca de tiempo correspondiente que indica la hora y fecha en que el mensaje fue enviado por el usuario A (es decir por la App A), la hora y la fecha en que el mensaje fue recibido por el usuario B (es decir por la App B) y la hora y fecha en que el mensaje fue leído por el usuario B.

En esencia, el módulo 114 de Mensajero es el componente que permite el desacoplamiento del servicio de certificación del servicio de mensajería.

Preferiblemente, el módulo 114 de Mensajero está configurado para hacer interfaz con (y por lo tanto usar) diversos sistemas de mensajería (por ejemplo, SMS, correo electrónico, mensajería instantánea, PEC, etc.). En particular, el módulo 114 de Mensajero podría configurarse de manera conveniente para recibir mensajes de los usuarios A y B en uno o más canales de mensajería diferentes (SMS, correo electrónico, mensajería instantánea, PEC, etc.), por ejemplo ,en el caso en el cual las Apps A y B no reciben confirmación de recibo de un mensaje enviado al servidor 11 de certificación.

Además, el módulo 114 de Mensajero también puede configurarse de manera conveniente para enviar mensajes a los usuarios A y B (y/o las notificaciones relativas) usando uno o más canales de mensajería diferentes (SMS, correo electrónico, mensajería instantánea, PEC, etc.), por ejemplo, en el caso en el cual el servidor 111 de certificación no recibe confirmación de recibo y/o lectura de un mensaje enviado a la App A o B.

En otras palabras, el módulo 114 de Mensajero puede ser de manera conveniente un módulo de mensajería multiplataforma capaz de usar diversos canales de llegada y diversos canales de salida para enviar/recibir mensajes y/o las notificaciones relativas, de tal manera que se asegure siempre el intercambio de mensajes entre los usuarios A y B.

Una vez que la App B ha recibido, desde el módulo 114 de Mensajero, un nuevo mensaje de la App A (es decir del usuario A) y el usuario B ha recibido la notificación relevante (por ejemplo, una notificación de impulso y/o a través de SMS, correo electrónico, etc.), dicho usuario B abre la App B y autentifica y procede con la lectura del mensaje. Una vez que el usuario B lee el mensaje, la App B envía una notificación de lectura relacionada al módulo 114 de Mensajero.

Por supuesto, cuando el usuario A inicia una conversación certificada con el usuario B, el usuario B debe proporcionar, a través de la App B, su consentimiento para la certificación de la conversación.

El usuario B puede luego responder a los mensajes de usuario A usando los mismos mecanismos descritos anteriormente para enviar mensajes del usuario A al usuario B.

Una sesión de certificación puede finalizar tras alcanzar un tiempo de espera predefinido o establecido por el usuario que inició la conversación certificada (en el ejemplo descrito anteriormente, el usuario A), o acordado por los dos usuarios (es decir, en el ejemplo de la figura 2, los usuarios A y B).

En particular, al final de una sesión de certificación, el módulo 113 de Seguimiento de Auditoría recolecta toda la evidencia generada (es decir, identidad de los usuarios A y B, la lista completa de mensajes intercambiados, hora y fecha de envío, recepción y lectura de cada mensaje (marca de tiempo), la lista completa de resúmenes relacionados con los mensajes intercambiados y el resumen acumulativo generado para el último mensaje intercambiado en la conversación certificada, o todos los resúmenes acumulativos generados durante la conversación certificada) y envía tal evidencia a un sistema de archivo documental seguro. De manera conveniente, los datos recolectados y enviados para archivar pueden ser firmados electrónicamente por el módulo 113 de Seguimiento de Auditoría usando una función de QES/AES y/o QSEAL/ASEAL predefinida, basada en PKI o no.

En otras palabras, el módulo 113 de Seguimiento de Auditoría es el módulo que permite, en caso de litigación o verificación, acceder a los datos certificados almacenados por el sistema 1 de mensajería certificado. En particular, todos los datos relevantes para certificar el tránsito, autenticidad e integridad de la información y contenido intercambiado son enviados a uno o más sistemas de archivo documental seguros y pueden estar disponibles a solicitud de un usuario o una autoridad (por ejemplo, la autoridad judicial).

De manera conveniente, el sistema 1 de mensajería certificado cierra sesión de un usuario tras alcanzar un tiempo de espera predefinido o en respuesta a una acción del usuario (por ejemplo una acción indicativa del deseo del usuario de desconectarse del servicio de mensajería certificado).

Es importante anotar que, aunque hasta ahora la operación del sistema 1 de mensajería certificado se ha descrito en relación con una conversación certificada entre dos usuarios solamente (por ejemplo, los usuarios A y B), dicho sistema 1 de mensajería certificado también puede ser usado de manera conveniente, *mutatis mutandis*, para certificar conversaciones entre más de dos usuarios.

Además, el sistema 1 de mensajería certificado también puede explotarse de manera conveniente, *mutatis mutandis*, para certificar conversaciones entre uno o más usuarios humanos y uno o más agentes inteligentes configurados para mantener conversaciones inteligentes con humanos (por ejemplo, con propósitos de asistencia remota, para la provisión de información/datos de manera automática y/o con propósitos comerciales).

Por último, el sistema 1 de mensajería certificado también podría explotarse de manera ventajosa, *mutatis mutandis*, para certificar conversaciones entre dos o más agentes inteligentes configurados para mantener conversaciones entre ellos.

Preferiblemente, el sistema 1 de mensajería certificado puede configurarse para realizar una primera función de bloqueo la cual, si es activada por el remitente de un mensaje, no permite que el receptor responda hasta que el remitente haya desactivado dicha primera función de bloqueo. Por ejemplo, dicha primera función de bloqueo puede ser útil si un remitente desea enviar una secuencia de mensajes sin el riesgo de que el receptor responda antes de que el remitente haya finalizado de enviar todos los mensajes.

De nuevo preferiblemente, el sistema 1 de mensajería certificado también se puede configurar para realizar una segunda función de bloqueo la cual, si está activada, no permite que un usuario que acaba de enviar un mensaje envíe mensajes adicionales hasta que él/ella haya recibido la respuesta del otro usuario.

Estas funciones de bloqueo permiten a los usuarios gestionar el orden en el cual son intercambiados los mensajes dentro de la misma conversación, manteniéndolos en orden.

Con referencia a lo que se ilustra en las figuras 1 y 2, la solicitud a los usuarios A y B de activar o no la primera función de bloqueo y/o la segunda función de bloqueo, así como la implementación de dicha primera/segunda función de bloqueo (cuando está activada) son tareas que se pueden confiar de manera conveniente a las Apps A y B.

Además, las Apps A y B podrían estar equipadas de manera conveniente con un módulo de composición de documentos que permite a los usuarios A y B componer dinámicamente documentos de ordenador asociados con el intercambio de información con base en un conjunto de metadatos acordado. Los documentos de ordenador así creados se pueden luego ofrecer a usuarios (personas físicas) para aceptación y firma con firma electrónica, firma electrónica calificada o firma electrónica avanzada.

Además, el servidor 11 de certificación y las Apps A y B también se pueden proporcionar de manera conveniente con un módulo de firma que permite la firma electrónica, o a través de una solución de QES o AES, de un archivo producido por el servidor 11 de certificación o enviado por un usuario (persona física o agente inteligente). Por ejemplo, para este propósito, podría usarse de manera conveniente el método avanzado de firma electrónica basado en voz descrito en el documento EP3316162.

El sistema 1 de mensajería certificado y, más en general, el método, sistema y servicio de certificación de acuerdo con la presente invención pueden explotarse de manera ventajosa en diversas aplicaciones, por ejemplo, para certificar mensajes intercambiados, a través de un sistema de mensajería, entre:

• pilotos y controladores de tráfico aéreo;

• un usuario en necesidad de asistencia y un proveedor de un servicio de asistencia remota (en este caso, la segunda parte puede ser de manera conveniente un operador humano o un agente inteligente), por ejemplo para el mantenimiento/reparación de dispositivos/sistemas (tales como radar, sistemas de comunicación, sistemas de medición, etc.) instalados en lugares inaccesibles o de difícil acceso (por ejemplo a bordo de un barco en medio de un océano, en una base científica/militar ubicada en la Antártida, etc.); y

• usuarios remotos y proveedores de productos y/o servicios tangibles y/o intangibles (por ejemplo, tiendas físicas o virtuales, bancos, compañías de seguros, hoteles, agencias de viajes, compañías de transporte, etc.).

En particular, en el último caso la presente invención podría explotarse de manera ventajosa:

• con propósitos de asesoramiento financiero (por ejemplo como un medio de comunicación entre un asesor financiero y un cliente para obtener el consentimiento del cliente para propuestas de inversión);

• como parte de procesos de ventas (por ejemplo, para comunicaciones entre un departamento de ventas de la empresa y un cliente para acordar cambios contractuales);

• como parte de un proceso de aprobación (por ejemplo, para acordar cambios en documentos que necesitan ser firmados electrónicamente);

• en el sector de la salud (por ejemplo, para el intercambio seguro de información entre médicos y pacientes); en particular, la presente invención podría ser integrada de manera ventajosa en sistemas de información que permiten a los pacientes interactuar con médicos y/o gestionar/consultar sus registros médicos electrónicos;

• en el sector de seguros (por ejemplo, para la firma y/o para la gestión posventa de pólizas de seguros).

A partir de la descripción anterior las innumerables ventajas técnicas de la presente invención son inmediatamente evidentes.

En particular, es importante enfatizar que la presente invención hace posible certificar de una manera verdaderamente efectiva el intercambio de mensajes entre dos o más usuarios, o entre uno o más usuarios y uno o más agentes inteligentes, o entre dos o más agentes inteligentes. En particular, la presente invención hace posible certificar de manera efectiva la identidad de aquellos que intercambian mensajes a través de un sistema/servicio de mensajería, la integridad del contenido intercambiado, la fecha y hora de envío, recepción y lectura de mensajes, así como el orden exacto de envío de mensajes intercambiados.

Con más detalle, es importante anotar que la presente invención hace posible:

• concatenar el intercambio de contenido de información textual y/o multimedia (por ejemplo, imágenes, fotos, vídeos, audio, archivos de música, enlaces, ubicaciones geográficas, tarjetas de presentación electrónicas, documentos de texto o incluso otros documentos, etc.) calculando un resumen de cada contenido, certificando así la integridad del contenido intercambiado entre dos o más usuarios (o entre un usuario y un agente inteligente, o entre dos o más agentes inteligentes);

• certificar el orden en el cual son enviados los mensajes en una conversación, gracias al cálculo de resumen acumulativo el cual, como se explicó anteriormente, concatena el resumen de cada nuevo mensaje enviado con los de los mensajes previos;

• certificar mediante marca de tiempo la fecha y hora de envío, recepción y lectura de cada mensaje intercambiado;

• enviar una conversación completa y evidencia relacionada para el archivo digital seguro (sujeto a un acuerdo entre las partes, cuando están las personas físicas); y

• producir a solicitud (por ejemplo, en el contexto de procedimientos judiciales) un documento que certifique la integridad y concatenación, en el cual el CMSP presenta toda la evidencia reunida en relación con una conversación.

Ventajas adicionales de la presente invención son:

• alta velocidad de comunicación entre sujetos que requieren mensajes certificados;

• alternativa simple, rápida, segura para intercambiar a través de PEC o correo electrónico;

• integrabilidad en plataformas de PEC, con el objetivo de extender su funcionalidad;

• posibilidad de certificar la solución de acuerdo con la presente invención como un servicio de suministro calificado de acuerdo con la Regulación de eIDAS (Autentificación y Firma de IDentificación Electrónica) - Regulación de la Unión Europea (UE) No. 910/2014 sobre identidad digital y servicios de confianza.

En conclusión, está claro que se pueden hacer diversas modificaciones a la presente invención, todas que caen dentro del alcance de protección de la invención como está definido en las reivindicaciones anexas.

REIVINDICACIONES

1. Un método para certificar mensajes intercambiados entre dos o más partes (Usuario A, Usuario B) a través de un sistema de mensajería, en donde cada mensaje es intercambiado:

• enviando el mensaje desde un remitente respectivo a un servidor (11) de certificación, en donde dicho remitente respectivo es

- un primer usuario (Usuario A) que usa un primer dispositivo (2) de comunicación electrónica, o

- un primer agente de software inteligente; y

• enviando el mensaje desde el servidor (11) de certificación a al menos un receptor respectivo, en donde dicho receptor respectivo es

- un segundo usuario (Usuario B) que usa un segundo dispositivo (3) de comunicación electrónica, o

- un segundo agente de software inteligente;

en donde, para cada mensaje intercambiado, el remitente respectivo también envía al servidor (11) de certificación un resumen correspondiente calculado aplicando una primera función de direccionamiento predefinida al mensaje;

en donde el servidor (11) de certificación almacena los mensajes intercambiados y una lista de los resúmenes que corresponden a los mensajes intercambiados;

caracterizado porque el servidor (11) de certificación:

• almacena los mensajes intercambiados y los resúmenes correspondientes en el orden en el cual son intercambiados los mensajes; y,

• por cada mensaje intercambiado,

- actualiza la lista de resúmenes con el resumen que corresponde a dicho mensaje intercambiado, por lo que la lista actualizada de resúmenes incluye el resumen que corresponde a dicho mensaje intercambiado y los resúmenes que corresponden a mensajes intercambiados previamente, y

- calcula un resumen acumulativo aplicando una segunda función de direccionamiento predefinida a la lista actualizada de resúmenes;

por lo que el servidor (11) de certificación está provisto con capacidad para certificar contenidos y orden de intercambio de los mensajes.

2. El método de la reivindicación 1, en donde el servidor (11) de certificación firma electrónicamente la lista de resúmenes.

3. El método de acuerdo con la reivindicación 1 o 2, en donde el servidor (11) de certificación identifica a las partes (Usuario A, Usuario B) que intercambian los mensajes; en donde, para cada mensaje intercambiado, el receptor respectivo envía al servidor (11) de certificación:

• una notificación de recibo cuando es recibido el mensaje; y

• una notificación de lectura cuando es leído el mensaje;

y en donde el servidor (11) de certificación también almacena:

• las identidades de las partes (Usuario A, Usuario B) que intercambian mensajes; y

• hora y fecha de envío, recepción y lectura de los mensajes intercambiados;

por lo que dicho servidor (11) de certificación está provisto con capacidad de certificar también las identidades de las partes (Usuario A, Usuario B) que intercambian los mensajes y la hora y fecha de envío, recepción y lectura de los mensajes intercambiados.

4. El método de acuerdo con cualquier reivindicación 1-3, en donde para cada mensaje intercambiado:

• el remitente respectivo envía el mensaje y el resumen correspondiente al servidor (11) de certificación en forma encriptada usando una tecnología de encriptado predefinida; y

• el servidor (11) de certificación envía el mensaje al receptor respectivo usando dicha tecnología de encriptado predefinida.

5. El método de acuerdo con cualquier reivindicación precedente, que comprende además: tras una solicitud del remitente de un mensaje, llevar a cabo una primera función de bloqueo que, cuando está activada, no permite que el receptor responda hasta que el remitente desactive dicha primera función de bloqueo.

6. El método de acuerdo con cualquier reivindicación precedente, que comprende además llevar a cabo una segunda función de bloqueo que, cuando está activada, no permite que un remitente de un mensaje envíe otro mensaje hasta que se haya recibido la respuesta del receptor.

7. Un servidor (11) de certificación configurado para llevar a cabo el método como se reivindica en cualquier reivindicación precedente para certificar mensajes intercambiados entre dos o más partes (Usuario A, Usuario B) a través de un sistema de mensajería, en donde cada mensaje es intercambiado enviando el mensaje desde un remitente respectivo a dicho servidor (11) de certificación, en donde dicho remitente respectivo es un primer usuario (Usuario A) que usa un primer dispositivo (2) de comunicación electrónica o un primer agente de software inteligente;

en donde, para cada mensaje intercambiado, el remitente respectivo también envía al servidor (11) de certificación un resumen correspondiente calculado aplicando una primera función de direccionamiento predefinida al mensaje;

en donde el servidor (11) de certificación está configurado para:

• almacenar los mensajes intercambiados y una lista de los resúmenes que corresponden a los mensajes intercambiados en el orden en el cual son intercambiados los mensajes; y,

• por cada mensaje intercambiado,

- enviar el mensaje recibido del remitente respectivo a al menos un receptor respectivo, en donde dicho receptor respectivo es un segundo usuario (Usuario B) que usa un segundo dispositivo (3) de comunicación electrónica o un segundo agente de software inteligente,

- actualizar la lista de resúmenes con el resumen que corresponde a dicho mensaje intercambiado, por lo que la lista actualizada de resúmenes incluye el resumen que corresponde a dicho mensaje intercambiado y los resúmenes que corresponden a mensajes intercambiados previamente, y

- calcular un resumen acumulativo aplicando una segunda función de direccionamiento predefinida a la lista actualizada de resúmenes;

por lo que el servidor (11) de certificación está provisto con capacidad para certificar contenidos y orden de intercambio de los mensajes.

8. El servidor de certificación de la reivindicación 7, configurado además para firmar electrónicamente la lista de resúmenes.

9. El servidor de certificación de acuerdo con la reivindicación 7 u 8, configurado además para identificar a las partes (Usuario A, Usuario B) que intercambian los mensajes; en donde, para cada mensaje intercambiado, el receptor respectivo envía al servidor (11) de certificación:

• una notificación de recibo cuando es recibido el mensaje; y

• una notificación de lectura cuando es leído el mensaje;

estando el servidor (11) de certificación configurado además para almacenar:

• las identidades de las partes (Usuario A, Usuario B) que intercambian los mensajes; y

• hora y fecha de envío, recepción y lectura de los mensajes intercambiados;

por lo que dicho servidor (11) de certificación está provisto con capacidad para certificar también las identidades de las partes (Usuario A, Usuario B) que intercambian los mensajes y la hora y fecha de envío, recepción y lectura de los mensajes intercambiados.

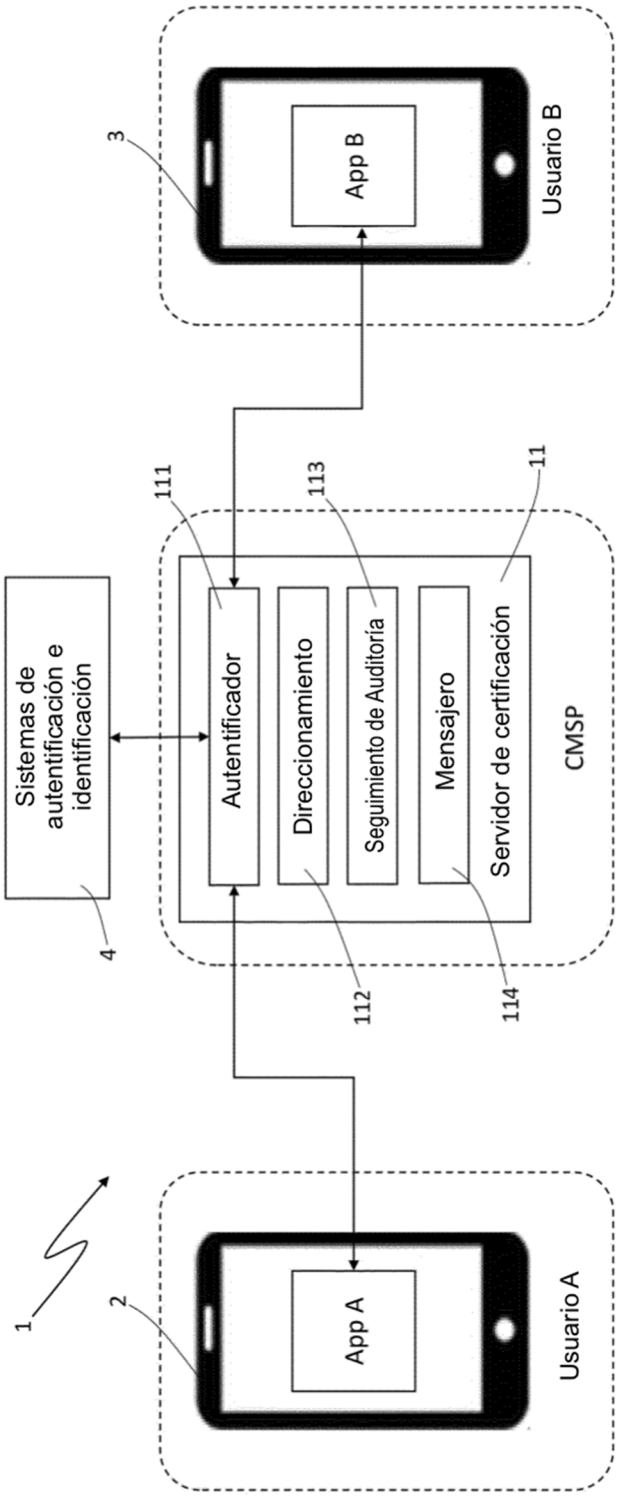
Usuario B
App B
3
111
113
11
Sistemas de autentificación e identificación
Autentificador
Direccionamiento
Seguimiento de Auditoría
Mensajero
Servidor de certificación
CMSP
4
112
114
1
2
App A
Usuario A

Fig. 1

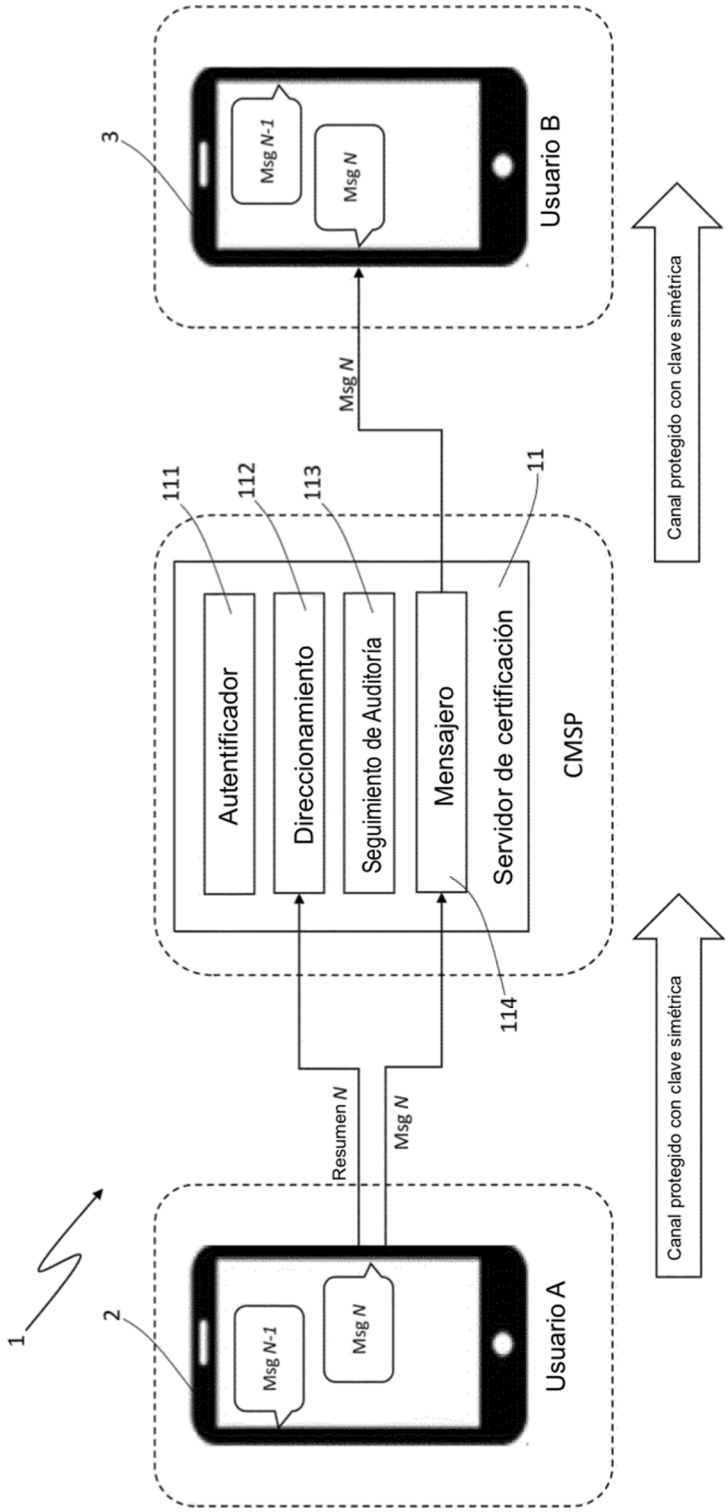
1
2
Usuario A
Msg N-1
Msg N
3
Usuario B
Msg N-1
Msg N
Resumen N
Msg N
Msg N
111
112
113
11
114
Autentificador
Direccionamiento
Seguimiento de Auditoría
Mensajero
Servidor de certificación
CMSP
Canal protegido con clave simétrica
Canal protegido con clave simétrica

Fig. 2