(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 784 008**

(51) Int. CI.:

H04L 29/06 (2006.01)
G06F 21/35 (2013.01)
G06F 21/43 (2013.01)
G06F 21/60 (2013.01)
H04L 9/08 (2006.01)
H04L 9/32 (2006.01)
H04W 12/00 (2009.01)
H04W 4/12 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **12.11.2012 E 18183257 (7)**

(97) Fecha y número de publicación de la concesión europea: **01.01.2020 EP 3432546**

(54) Título: **Mensajería segura**

(30) Prioridad:

11.11.2011 AU 2011904705

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
21.09.2020

(73) Titular/es:

SOPRANO DESIGN LIMITED (100.0%)
Level 11, 132 Arthur Street
North Sydney, NSW 2060, AU

(72) Inventor/es:

FAVERO, RICHARD FRANCIS

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Mensajería segura

Campo de la invención

La presente invención se refiere a una mensajería segura. En una forma, la mensajería segura de la presente invención se refiere a la transmisión y recepción de mensajes cifrados a un aparato telefónico. La invención se extiende también al almacenamiento seguro provisional de un mensaje en un servidor de mensajería, antes de transmitir el mensaje a un aparato telefónico.

Antecedentes de la invención

En algunas circunstancias es deseable la entrega segura de información privada a través de redes móviles. Un ejemplo de tal información privada es información sanitaria implícita, tal como el nombre del médico, la hora y la especialidad, que puede indicar una enfermedad que se esté tratando, formando dicha información parte de recordatorios de citas, u otro intercambio de información con profesionales sanitarios enviada a pacientes. Los bancos también pueden desear enviar información privada a sus clientes. La ubicuidad de los aparatos telefónicos móviles ha proporcionado medios eficaces para la entrega de información utilizando el servicio de mensajes cortos (SMS, por sus siglas en inglés) y otros canales de datos.

Las soluciones existentes que soportan mensajería segura cifran los mensajes en un servidor de mensajería intermedio, antes de reenviar el mensaje cifrado a un teléfono inteligente (*smartphone*). Típicamente se descarga al teléfono inteligente una aplicación (o ésta reside de forma nativa en el teléfono inteligente), que se utiliza para descifrar mensajes que han sido cifrados antes de la transmisión. El cifrado utiliza típicamente un cifrado de clave simétrica, por ejemplo el estándar de cifrado avanzado (*Advanced Encryption Standard* (AES)) con cifrado de 256 bits. Cuando se utiliza este tipo de solución, se usa la misma clave tanto para el cifrado como para el descifrado y ésta se almacena tanto en el aparato telefónico como en el servidor de mensajería que se utiliza para transferir el mensaje. Esto representa un riesgo para la seguridad en caso de que la clave se vea comprometida, bien en el servidor de mensajería, bien en el aparato telefónico. Si el servidor de mensajería o el aparato telefónico son hackeados, la clave utilizada para algunos de los aparatos telefónicos o para todos los aparatos telefónicos que reciben mensajes de este servidor puede verse comprometida y sería necesario facilitar a todos los aparatos telefónicos una nueva clave, lo que, considerando el gran número de aparatos telefónicos que puede soportar tal sistema, representaría un proceso de implementación complicado para muchos aparatos telefónicos.

Sigue existiendo la necesidad de una solución para proporcionar una mensajería cifrada o segura a aparatos telefónicos para recibir mensajes de forma segura que no adolezca de las desventajas de las soluciones existentes. Como alternativa, o adicionalmente, sería deseable proporcionar al público una opción útil.

Las referencias a cualquier técnica anterior en la especificación no son, ni deberían considerarse como, un reconocimiento o cualquier forma de insinuación de que esta técnica anterior forma parte del conocimiento general común en Australia o en cualquier otra jurisdicción o de que esta técnica anterior podría esperarse razonablemente que fuese establecida, entendida y considerada como relevante por un experto en la técnica.

El documento US2003/0204726 describe un procedimiento y sistema para la transmisión segura de información en la que un cliente envía a un servidor una petición de una contraseña de un solo uso con un único identificador, el servidor genera y cifra una respuesta que incluye una contraseña de un solo uso y la envía a un dispositivo móvil determinado desde el identificador único, y el dispositivo móvil transfiera la respuesta al cliente para su descifrado.

Compendio de la invención

La presente invención proporciona un procedimiento en un servidor de mensajería para registrar un aparato telefónico para permitir el envío seguro de un mensaje al aparato telefónico y un servidor de mensajería para ejecutar el procedimiento como se define en las reivindicaciones 1 a 8.

Según la invención, se utilizan canales de comunicación diferentes para proporcionar la contraseña temporal al aparato telefónico y recibir la contraseña de retorno del aparato telefónico.

La contraseña temporal se puede enviar al aparato telefónico como parte de un SMS, mientras que la contraseña de retorno se recibe desde el aparato telefónico utilizando una red móvil pública que soporta comunicación de datos.

El paso de comparar las contraseñas puede incluir además comparar un identificador de aparato telefónico recibido con la contraseña de retorno, con el identificador de aparato telefónico al que se ha enviado la contraseña temporal.

Tal como se utilizan en la presente memoria, excepto cuando el contexto requiera otra cosa, el término “comprenden” y las variaciones del término, tales como “que comprenden”, “comprende” y “comprendido”, no tienen por objeto excluir otros aditivos, componentes, números enteros u operaciones.

De la descripción siguiente, que se ofrece a modo de ejemplo y con referencia a los dibujos adjuntos, se desprenderán otros aspectos de la presente invención y otras realizaciones de los aspectos descritos en los párrafos precedentes.

Breve descripción de los dibujos

La Figura 1 es un diagrama esquemático de un sistema de mensajería segura que incluye un servidor de mensajería y un aparato telefónico;

la Figura 2 es un diagrama de flujo de las funciones globales realizadas por una aplicación del aparato telefónico de la Figura 1;

la Figura 3 es un diagrama de flujo de un ejemplo de funciones de registro del aparato telefónico de la Figura 1, que forma parte del diagrama de flujo de la Figura 2;

la Figura 4 es un diagrama de flujo de otro ejemplo de funciones de registro del aparato telefónico de la Figura 1, que forma parte del diagrama de flujo de la Figura 2;

la Figura 5 es una representación del flujo de mensajes del remitente al destinatario cuando el destinatario no está previamente registrado, de acuerdo con las funciones de registro de la realización ejemplar de la Figura 3;

la Figura 6 es una representación del flujo de mensajes del remitente al destinatario cuando el destinatario no está previamente registrado, de acuerdo con las funciones de registro de la realización ejemplar de la Figura 4;

la Figura 7 es una representación del flujo de mensajes del remitente al destinatario cuando el destinatario está previamente registrado; y

la Figura 8 es un diagrama de flujo de las funciones realizadas por el servidor de mensajería, de acuerdo con las funciones de registro de la realización ejemplar de la Figura 3.

Descripción detallada de las realizaciones

1. Sinopsis del sistema

La Figura 1 es un diagrama esquemático de un sistema 100 de mensajería segura para enviar mensajes seguros de un ordenador remitente 102 a un aparato telefónico destinatario 104 a través de un servidor 106 de mensajería. La comunicación entre el ordenador remitente 102 y el servidor 106 de mensajería se realiza a través de una red 108, que puede ser una red de datos privada o pública (por ejemplo, el ordenador puede utilizar una aplicación web a la que haya accedido a través de un sitio web y utilizando una conexión HTTP o HTTPS). La comunicación entre el servidor 106 de mensajería y el aparato telefónico 104 se realiza tanto a través de una red móvil pública 110, que soporta el envío/la recepción de mensajes SMS (sistema de mensajes cortos), como a través de una red móvil pública 112, que soporta la comunicación de datos utilizando, por ejemplo, un protocolo de comunicación 3G o 4G. El servidor 106 de mensajería se comunica mediante interfaz con uno o más dispositivos 114 de almacenamiento utilizados, entre otras cosas, para mantener una base de datos con información sobre usuarios registrados (destinatarios). La base de datos almacenada en el dispositivo 114 de almacenamiento puede utilizarse también para almacenar mensajes recibidos de uno o más remitentes antes de ser reenviados a uno o más destinatarios. En una realización, los mensajes que se almacenen en la base de datos pueden cifrarse (protegerse).

El ordenador remitente 102 y el servidor 106 de mensajería incluyen ambos unos componentes de *hardware* tales como un procesador, una memoria, un almacenamiento y una interfaz de red. El ordenador remitente 102 y el servidor 106 de mensajería pueden incluir también interfaces de entrada-salida (tales como un teclado y un monitor). El *hardware* estándar del ordenador remitente 102 y del servidor 106 de mensajería incluye también un bus para la comunicación entre componentes de *hardware*. El *hardware* informático funciona con un componente de *software* de una aplicación de mensajería segura (descrita posteriormente con mayor detalle), aplicación que está almacenada en la memoria y que es ejecutada por el procesador de cada máquina. El servidor 106 de mensajería se comunica mediante interfaz con los uno o más dispositivos 114 de almacenamiento, que pueden comprender también un disco duro, un sistema RAID u otro almacenamiento conectado directamente.

Se apreciará que hay muchas arquitecturas de ordenador posibles diferentes que pueden utilizarse para implementar la presente invención y que la descripción anterior es representativa de sólo una arquitectura ejemplar. El término “ordenador” se utiliza en la presente memoria en un sentido general e incluye, sin limitación, los dispositivos computacionales de ordenadores personales, asistentes digitales personales, teléfonos inteligentes, ordenadores tipo tableta y servidores. Los expertos en las técnicas pertinentes reconocerán cuáles de estas clases de ordenador pueden utilizarse para cada aspecto del sistema 100. Por ejemplo, los asistentes digitales personales, los teléfonos inteligentes y los ordenadores tipo tableta pueden ser alternativas adecuadas al ordenador remitente 102 mostrado en la Figura 1.

El aparato telefónico 104 es el tipo de aparato telefónico que puede recibir mensajes SMS y puede también comunicarse a través de una red de datos tal como una red 3G o 4G. Los aparatos telefónicos adecuados incluyen, por ejemplo, asistentes digitales personales, teléfonos inteligentes, ordenadores tipo tableta o similares.

2. Aplicación de aparato telefónico

El sistema 100 soporta el envío de mensajes seguros del ordenador remitente 102 al aparato telefónico destinatario 104 a través del servidor 106 de mensajería, tanto cuando el destinatario está previamente registrado en el servidor 106 de mensajería como cuando el destinatario no está previamente registrado en el servidor 106 de mensajería. Si un destinatario no está registrado, significa que el servidor 106 de mensajería no tiene credenciales de cifrado del aparato telefónico destinatario 104 (concretamente una clave de cifrado de aparato telefónico tal como una clave pública de aparato telefónico), lo que típicamente significa que el aparato telefónico destinatario 104 no tiene activada una aplicación de aparato telefónico. La aplicación de aparato telefónico se utiliza para el registro del aparato telefónico destinatario 104, para generar claves de cifrado/descifrado y para descifrar mensajes cortos protegidos recibidos del servidor 106 de mensajería.

Para el registro de un destinatario en el servidor 106 de mensajería, la aplicación de aparato telefónico presente en el aparato telefónico 104 envía una clave de cifrado de aparato telefónico al servidor 106 de mensajería y entonces la clave se almacena en el servidor de mensajería (en la memoria del servidor y/o en el dispositivo 114 de almacenamiento del servidor) para utilizarla cuando sea necesario enviar un mensaje al aparato telefónico en particular. Con este fin, el aparato telefónico destinatario 104 instala una aplicación de aparato telefónico y configura la aplicación de aparato telefónico para recibir mensajes seguros. Configurar la aplicación de aparato telefónico de manera que se registre el aparato telefónico destinatario 104 y se permita al mismo descifrar mensajes puede suponer además, por ejemplo, autenticar el aparato telefónico 104 emparejando el identificador de aparato telefónico del aparato telefónico en forma del número de móvil/número MSISDN asociado con el aparato telefónico y verificando una contraseña temporal tal como una contraseña de un solo uso (*one time password* (OTP)). Adicionalmente, la configuración incluye la creación de claves de cifrado y descifrado utilizadas para mensajes enviados al aparato telefónico 104. Tal como se utilizan en la presente memoria, los términos “autenticar” y “validar” se utilizan de manera intercambiable para describir la comparación entre la contraseña enviada al identificador de un aparato telefónico y la contraseña introducida por un usuario del aparato telefónico.

Adicionalmente, un experto en la técnica apreciará que un aparato telefónico debe identificarse siempre mediante un identificador de aparato telefónico en forma de, por ejemplo, un número MSISDN, y que las notificaciones y toda otra correspondencia se enviarán a un aparato telefónico que incluya una tarjeta de identificación, por ejemplo una tarjeta SIM, con el identificador de aparato telefónico en particular.

La aplicación de aparato telefónico es una aplicación cliente ejecutada en el aparato telefónico 104, aplicación que el destinatario obtiene, por ejemplo, de una tienda de aplicaciones. Tales tiendas de aplicaciones pueden incluir tiendas específicas para aparatos telefónicos tales como las tiendas de aplicaciones Apple, Android, Windows, Blackberry o J2ME. La funcionalidad proporcionada por la aplicación de aparato telefónico incluye proporcionar autenticación y registro del aparato telefónico destinatario 104 en el servidor 106 de mensajería y soportar una mensajería segura entre el servidor 106 de mensajería y el aparato telefónico 104 por el método de a) generar y proporcionar una clave de cifrado al servidor 106 de mensajería y b) proporcionar la capa de aplicación para SMS y comunicación de datos (por ejemplo 3G) entre el servidor 106 de mensajería y el aparato telefónico 104 a través de las redes móviles públicas 110, 112. Se apreciará que la aplicación de aparato telefónico puede también ser nativa para el aparato telefónico estando preinstalada en el aparato telefónico 104.

a. Autenticación y registro

La Figura 2 muestra un diagrama 200 de flujo de las funciones globales realizadas por la aplicación de aparato telefónico. Una vez que se ha instalado la aplicación de aparato telefónico en el aparato telefónico 104, la aplicación de aparato telefónico autentica en el paso 202 el aparato telefónico 104.

Durante el proceso de autenticación se comparan parejas de contraseñas temporales y números de móvil y, si estas parejas coinciden, la aplicación de aparato telefónico puede autenticar el aparato telefónico destinatario 104 en el servidor 106 de mensajería y entonces se registra también el aparato telefónico 104 en el servidor 106 de mensajería (véase el paso 204). Preferiblemente, las contraseñas temporales han de recibirse a través de canales de comunicación separados. Los datos de registro para el aparato telefónico 104 que el servidor 106 de mensajería mantiene incluyen el identificador de aparato telefónico 104, es decir el número de móvil (número MSISDN) asociado con el aparato telefónico, el tipo de dispositivo (tal como el tipo de teléfono inteligente), así como la clave pública de cifrado que la aplicación de aparato telefónico envía al servidor 106 de mensajería.

A continuación se tratan, con referencia a las Figuras 3 y 4, más funciones detalladas realizadas por el aparato telefónico 104 durante el proceso de registro.

Centrándonos en primer lugar en la Figura 3, se describe un proceso 220 de registro en el que se genera una contraseña temporal en el servidor 106 de mensajería. En el paso 222, se solicita a la aplicación de aparato telefónico que pida al usuario el identificador de aparato telefónico, es decir el número de móvil (MSISDN). La

aplicación de aparato telefónico obtiene el número de móvil asociado con el aparato telefónico 104 del usuario del aparato telefónico, quien introduce el número a través de la interfaz de usuario de la aplicación (por ejemplo una interfaz gráfica de usuario (GUI, por sus siglas en inglés)), como se muestra en el paso 224. Entonces, la aplicación de aparato telefónico envía el número de móvil, por ejemplo a través de una conexión HTTP o HTTPS, al servidor 106 de mensajería en el paso 226. En el paso 228, el servidor 106 de mensajería genera una contraseña temporal, en forma de una contraseña de un solo uso (OTP), que está asociada con el número de móvil del aparato telefónico 104. La OTP puede ser una cadena de caracteres creada aleatoriamente por el servidor 106 de mensajería. Se entenderá que la longitud y la composición de caracteres pueden configurarse de varias maneras diferentes, de modo que la OTP puede ser una cadena alfanumérica de cualquier longitud. En una realización, la OTP contiene 6 números. La OTP es válida durante un periodo de tiempo limitado, por ejemplo cinco minutos, una hora, un día o una semana.

El servidor 106 de mensajería envía una copia de la OTP al aparato telefónico 104 enviando un SMS al identificador del aparato telefónico (por ejemplo al número MSISDN/de móvil del aparato telefónico). Puede utilizarse un solo identificador para registrar múltiples dispositivos portátiles (por ejemplo un iPhone y un iPad asociado), de manera que es posible utilizar los múltiples dispositivos portátiles para ver mensajes seguros enviados al identificador.

En el paso 230, la aplicación de aparato telefónico solicita al usuario del aparato telefónico 104 que introduzca la OTP (que el servidor 106 de mensajería ha enviado al número de móvil del aparato telefónico 104) a través de la interfaz de usuario de la aplicación de aparato telefónico.

La aplicación de aparato telefónico envía la OTP introducida al servidor 106 de mensajería a través de una conexión HTTP o HTTPS. Después, el servidor 106 de mensajería compara la pareja número de móvil/OTP requerida con la pareja número de móvil/OTP introducida por el usuario.

El proceso de autenticación se realiza en el paso 232, que está indicado en líneas discontinuas en la Figura 3, dado que este paso se lleva a cabo en el servidor 106 de mensajería. Si las parejas número de móvil/OTP no coinciden, la aplicación de aparato telefónico puede dar al usuario una oportunidad de introducir de nuevo una OTP. Si las parejas siguen sin coincidir, la aplicación de aparato telefónico puede estar configurada para informar al servidor 106 de mensajería de que no es posible autenticar o registrar el aparato telefónico 104 y la aplicación concluye (paso 234).

Si las parejas coinciden, se autentica el aparato telefónico y se envía un acuse de recibo a la aplicación de aparato telefónico en el paso 236. Luego, en el paso 238, sigue el registro del aparato telefónico 104, que es igual que el paso 204 de registro mostrado en la Figura 2.

En una variación de esta realización, la autenticación se produce en el aparato telefónico. En este escenario, además de la OTP que se envía al aparato telefónico a través de SMS, el servidor 106 de mensajería envía también la OTP a la aplicación de aparato telefónico utilizando una conexión HTTP o HTTPS. Entonces, la aplicación de aparato telefónico tiene dos copias de la OTP, una recibida a través de SMS y una recibida a través de conexión HTTP o HTTPS, es decir a través de canales de comunicación diferentes. Ahora, la aplicación de aparato telefónico autentica el aparato telefónico comparando las OTP recibidas, validando de este modo el aparato telefónico.

Con referencia ahora a la Figura 4, se describe un proceso 240 alternativo de registro en el que se genera una contraseña temporal en la aplicación de aparato telefónico 104. En el paso 242 se solicita a la aplicación de aparato telefónico que inicie el proceso de registro. La aplicación de aparato telefónico genera, en el aparato telefónico 104, una OTP (paso 244). La OTP puede tener características similares a las descritas anteriormente con referencia a la Figura 3. En respuesta a la solicitud, la aplicación de aparato telefónico está configurada también para hacer que el aparato telefónico envíe un SMS que contenga la OTP al servidor 106 de mensajería, como se muestra con el paso 246. Este SMS es en efecto un SMS automático, que no requiere ninguna introducción por parte del usuario. Utilizando la funcionalidad de “identificación de llamada” inherente del mensaje SMS, el servidor 106 de mensajería puede obtener el número de móvil (MSISDN) del aparato telefónico a partir del SMS. La OTP se extrae también del mensaje SMS. En el paso 248, la aplicación de aparato telefónico solicita al usuario del aparato telefónico 104 que introduzca el identificador del aparato telefónico (número de móvil), número que se envía, con la OTP, a través de una red móvil pública que soporte comunicación de datos, tal como una conexión HTTP o HTTPS, al servidor 106 de mensajería (véase el paso 250).

De manera similar al proceso mostrado en la Figura 3, el proceso de autenticación se lleva a cabo en el paso 252, indicado de nuevo mediante líneas discontinuas porque este paso se lleva a cabo en el servidor 106 de mensajería. Si las parejas número de móvil/OTP coinciden, se autentica el aparato telefónico 104 y se envía un acuse de recibo a la aplicación de aparato telefónico en el paso 254. Después, en el paso 256, sigue el registro del aparato telefónico 104, que el igual que el paso 204 de registro mostrado en la Figura 2.

b. Generar claves de cifrado/descifrado

Volviendo ahora a las funciones después del paso 204 de registro mostrado en la Figura 2, la aplicación de aparato telefónico se muestra como configurada para generar claves de cifrado y descifrado. Se crea una clave nueva y diferente para cada aparato telefónico sobre la base del número de móvil de ese aparato telefónico, que se utiliza

para sembrar un generador de números aleatorios. Esto significa que, en caso de que la aplicación de aparato telefónico sea hackeada y una clave privada se vea comprometida, sólo se ve afectado un aparato telefónico.

En el paso 208, la aplicación de aparato telefónico genera la clave de cifrado y la clave de descifrado asociada con el aparato telefónico 104. La aplicación de aparato telefónico utiliza el número de móvil (MSISDN) del aparato telefónico para sembrar un generador de números aleatorios con el fin de generar las claves. En una realización, el cifrado es asimétrico y las claves son claves RSA 1024. En otra realización, si el aparato telefónico 104 tiene la potencia de cálculo suficiente para soportar la longitud de clave de una clave RSA 2048, entonces las claves son claves RSA 2048. Se entenderá que existen diversos tipos de cifrado que pueden utilizarse. Se apreciará que la longitud de la clave de cifrado aumentará con el paso del tiempo según aumente la potencia de cálculo.

Cuando se utiliza un cifrado asimétrico, la clave de cifrado se denomina clave pública y la clave de descifrado se denomina clave privada. Después de generar las claves, la aplicación de aparato telefónico envía la clave pública al servidor 106 de mensajería (paso 210), preferiblemente a través de un uso por parte de la aplicación de aparato telefónico de un canal seguro tal como HTTPS, y no comparte la clave privada. Después, el servidor 106 de mensajería utilizará la clave pública del aparato telefónico para cifrar todos los mensajes dirigidos a ese aparato telefónico 104 específico. La clave privada se almacenará en la aplicación de aparato telefónico en el aparato telefónico 104 del destinatario y será utilizada por la aplicación de aparato telefónico para descifrar los mensajes enviados al aparato telefónico 104 desde el servidor 106 de mensajería a través de la aplicación de aparato telefónico.

c. Comunicación aparato telefónico servidor

Si el servidor 106 de mensajería recibe un mensaje del ordenador remitente 102 cuyo destino sea el aparato telefónico destinatario 104, entonces el servidor 106 de mensajería envía un mensaje SMS al aparato telefónico para notificar al aparato telefónico 104 que hay un mensaje en espera. Esta comunicación se realiza a través de la red móvil pública 110 que soporta la mensajería SMS. Una vez que el destinatario haya visto el mensaje SMS, el destinatario sabrá que ha de acceder a la aplicación de aparato telefónico para ver el mensaje protegido que está en espera. Como alternativa, la aplicación de aparato telefónico puede abrirse automáticamente a través de una configuración concreta del aparato telefónico. La aplicación de aparato telefónico proporciona la capa de aplicación para la conexión de red entre el servidor 106 de mensajería y el aparato telefónico destinatario 104 a través de la red móvil pública 112 de datos (por ejemplo 3G). La aplicación de aparato telefónico proporciona una interfaz de usuario en la que se visualizan los mensajes que se hayan recibido del servidor de mensajería (por ejemplo a través de una conexión HTTP o HTTPS), de manera que el destinatario pueda verlos.

La aplicación de aparato telefónico proporciona también una interfaz de usuario que el destinatario puede utilizar para enviar una respuesta al mensaje. Las respuestas del aparato telefónico 104 al servidor 106 de mensajería pueden utilizar un protocolo de comunicación tal como HTTP, HTTPS, SMPP, correo electrónico, WSDL, etc. En algunas realizaciones, el servidor 106 de mensajería reenvía los mensajes de respuesta al ordenador remitente 102.

En una realización, cuando el destinatario realiza una de las acciones siguientes: iniciar la aplicación de aparato telefónico, abrir la bandeja de entrada de la aplicación de aparato telefónico, actualizar la bandeja de entrada de la aplicación de aparato telefónico o seleccionar un mensaje de una lista en la bandeja de entrada de la aplicación de aparato telefónico, entonces se provoca que la aplicación de aparato telefónico se ponga en contacto con el servidor 106 de mensajería (paso 212) y que lleve a cabo en el paso 214 lo siguiente:

recuperar uno o más mensajes cifrados aún por recibir del servidor 106;

descifrar el mensaje; y

visualizar el mensaje en la interfaz de usuario de la aplicación de aparato telefónico para que el destinatario vea el mensaje.

El mensaje cifrado recibido ha sido cifrado por el servidor 106 utilizando la clave pública del aparato telefónico. En el servidor 106 de mensajería permanece una copia de este mensaje cifrado después de que el mensaje cifrado haya sido enviado al aparato telefónico. La copia del mensaje puede permanecer en el servidor durante un periodo de tiempo predeterminado (por ejemplo un día), o la copia del mensaje puede guardarse en el almacenamiento 114 durante un periodo de tiempo más largo (por ejemplo una semana, o hasta que el usuario pida al servidor que elimine la copia del mensaje). Se entenderá que la gestión y el almacenamiento de los mensajes en el servidor 106 pueden realizarse de múltiples maneras, por ejemplo dependiendo de la cantidad de memoria o almacenamiento utilizado por el servidor o el tipo de servicio prestado al destinatario.

3. Flujo de mensajes entre remitente, servidor de mensajería y destinatario

Las Figuras 5 a 7 representan el flujo de mensajes del ordenador remitente 102 al aparato telefónico destinatario 104 a través del servidor 106 de mensajería cuando el destinatario no está previamente registrado (Figuras 5 y 6) y cuando el destinatario está previamente registrado (Figura 7).

Remitiéndonos en primer lugar a la Figura 5, que muestra la comunicación en términos de la funcionalidad de la aplicación de aparato telefónico anteriormente descrita con referencia a las Figuras 2 y 3, en el paso 302 el ordenador remitente 102 utiliza una aplicación de cliente para enviar un mensaje ("Msg1") al servidor 106 de mensajería, que se ha de entregar cifrado al aparato telefónico 104. El ordenador remitente 102 envía al servidor 106 el mensaje Msg1 junto con un identificador de aparato telefónico. Como se ha mencionado anteriormente, el identificador de aparato telefónico puede ser una dirección de red pública tal como un número de guía para un aparato telefónico móvil que utilice un plan de numeración nacional para teléfonos móviles (por ejemplo un número de móvil MSISDN).

El servidor 106 de mensajería determina si el aparato telefónico está registrado en el paso 304 comprobando la base 114 de datos de registro para determinar si en la misma existe una clave de cifrado de aparato telefónico (tal como una clave pública de aparato telefónico) asociada con el identificador (por ejemplo dirección de red pública) del aparato telefónico 104.

Para el escenario mostrado en la Figura 5, el aparato telefónico 104 no está registrado en esta fase; en otras palabras: el servidor 106 de mensajería no tiene una clave de cifrado que pueda utilizar para reenviar un mensaje cifrado al aparato telefónico 104. En el paso 306, el servidor 106 de mensajería cifra por lo tanto el mensaje recibido ("Msg1") temporalmente en la plataforma utilizando una clave de cifrado ("serv.cif") de servidor de mensajería. El mensaje cifrado ("Msg2") se almacena en el servidor 106 y/o en el almacenamiento 114 del servidor. Por lo tanto, en esta realización, el mensaje recibido Msg1 no está almacenado en el servidor 104.

Este cifrado intermedio puede ser un cifrado simétrico o asimétrico. Los ejemplos de tipos de cifrado que pueden utilizarse incluyen RSA con longitud de clave 1024, RSA con longitud de clave 2048 o AES con longitud de clave 256.

En el paso 308, el servidor 106 de mensajería envía una notificación al aparato telefónico 104, que indica que hay un mensaje cifrado en espera y que proporciona detalles para descargar la aplicación de aparato telefónico requerida, por ejemplo proporcionando un hipervínculo a un sitio web de una tienda de aplicaciones. En una realización, esta notificación se envía a través de SMS.

En otra realización, el paso 308 de notificación puede preceder al paso 306 de cifrado intermedio.

En el paso 310, el usuario descarga e instala la aplicación de aparato telefónico desde la tienda de aplicaciones apropiada. Si la aplicación de aparato telefónico ya se halla en el aparato telefónico (por ejemplo si el usuario la ha descargado previamente o si está preinstalada en el aparato telefónico), o como alternativa después de que el usuario haya descargado ahora la aplicación de aparato telefónico, el usuario inicia la aplicación de aparato telefónico en el aparato telefónico 104 y, cuando se le solicite, introduce el número de móvil del aparato telefónico utilizando la interfaz de usuario de la aplicación de aparato telefónico.

Después de que la aplicación de aparato telefónico haya reenviado el número de móvil introducido al servidor 106 de mensajería como se ha descrito anteriormente (paso 312), el servidor 106 de mensajería genera y envía una OTP al aparato telefónico 104 a través de SMS en el paso 314.

El usuario proporciona la OTP a la aplicación de aparato telefónico con el fin de validar el aparato telefónico 104. En la realización mostrada en la Figura 5, la aplicación de aparato telefónico solicita al usuario la OTP y luego envía la OTP introducida por el usuario al servidor 106 (paso 316). Entonces, el servidor 106 compara la pareja número de móvil/OTP requerida con la pareja número de móvil/OTP introducida por el usuario, habiéndose de señalar que el usuario sólo ha introducido la OTP, pero la aplicación habrá enviado el número de móvil del aparato telefónico con la OTP al servidor 106 de mensajería. Si las parejas coinciden, el servidor 106 autentica el aparato telefónico destinatario en el servidor 106 (véase el paso 318) y después también se registra el aparato telefónico 104 en el servidor 106. Típicamente se enviará un acuse de recibo de autenticación a la aplicación de aparato telefónico (paso 320).

En otra realización (no mostrada), el servidor 106 de mensajería puede enviar la OTP a la aplicación de aparato telefónico y luego la aplicación compara la pareja número de móvil/OTP requerida por el servidor con la pareja número de móvil/OTP introducida por el usuario.

En el paso 322, la aplicación de aparato telefónico crea una clave pública de aparato telefónico y una clave privada de aparato telefónico para el aparato telefónico 104. En el paso 324, la aplicación de aparato telefónico proporciona la clave pública de aparato telefónico al servidor 106 de mensajería. En este paso, la aplicación de aparato telefónico puede enviar al servidor 106 también otros datos (por ejemplo datos relativos al tipo de dispositivo), que se guardarán en el almacenamiento 114 del servidor junto con otros datos de registro relacionados con el aparato telefónico específico. En una realización, los datos de registro se mantienen en el almacenamiento 114 del servidor para su futuro uso, de modo que si es necesario enviar un segundo mensaje al aparato telefónico 104 se determinará que el aparato telefónico 104 ya está registrado, con lo que el segundo mensaje puede a) cifrarse utilizando la clave pública de aparato telefónico guardada y b) enviarse de forma segura al aparato telefónico 104.

En una realización, cuando el usuario abre la bandeja de entrada de la aplicación de aparato telefónico para recuperar el mensaje protegido, esto proporciona un disparador (o activador) a la aplicación de aparato telefónico para que envíe una petición al servidor 106 de mensajería con el fin de solicitar al servidor 106 de mensajería que envíe el mensaje. Esto se muestra en el paso 326.

En el paso 328, el servidor 106 de mensajería descifra el mensaje cifrado Msg2 intermedio utilizando la clave de descifrado de servidor de mensajería. En el paso 330, el servidor 106 de mensajería cifra el mensaje utilizando la clave pública de aparato telefónico y este mensaje cifrado ("Msg4") se entrega a la aplicación de aparato telefónico. En una realización, el mensaje cifrado Msg4 se almacena también en la base de datos.

En el paso 332, la aplicación de aparato telefónico descifra el mensaje utilizando la clave privada de aparato telefónico y visualiza el mensaje en la interfaz de usuario de la aplicación para que el destinatario lo vea.

Remitiéndonos ahora a la Figura 6, se muestra la comunicación en términos de la funcionalidad de la aplicación de aparato telefónico anteriormente descrita con referencia a las Figuras 2 y 4. Dado que sólo los pasos de autenticación son diferentes entre los procesos de comunicación descritos en términos de las Figuras 5 y 6, se han utilizado los mismos números de referencia para los pasos que son iguales y no se repite a continuación una descripción de estos pasos.

Comenzando así en el paso 310 en la Figura 6, el usuario descarga e instala la aplicación de aparato telefónico desde la tienda de aplicaciones apropiada.

En el paso 340, la aplicación de aparato telefónico genera una OTP. La aplicación de aparato telefónico está configurada para hacer que el aparato telefónico 104 envíe automáticamente, es decir sin introducción por parte del usuario, un mensaje SMS al servidor 106 de mensajería (paso 342), que contiene la OTP generada. En el paso 344, la aplicación de aparato telefónico solicita al usuario que introduzca el número de móvil del usuario (es decir la ID del aparato telefónico), que es enviado por la aplicación de aparato telefónico, junto con la OTP generada, a través de la red 112 de datos privada o pública (por ejemplo a través de una conexión HTTP o HTTPS) al servidor 106 de mensajería (véase el paso 346).

Se apreciará que la OTP se envía de nuevo del aparato telefónico al servidor 106 de mensajería a través de canales de comunicación diferentes.

Al recibir al mensaje SMS, el servidor 106 de mensajería obtiene el identificador de aparato telefónico a través de la funcionalidad de identificación de llamada del SMS. De manera similar al proceso de comunicación anteriormente descrito con referencia a la Figura 5, el servidor 106 compara las parejas número de móvil/OTP y, si las parejas coinciden, se realizan a continuación la autenticación y el registro.

Remitiéndonos a la Figura 7, en el paso 302 el ordenador remitente 102 utiliza una aplicación de cliente para enviar un mensaje ("Msg1") al servidor 106 de mensajería, que se ha de entregar cifrado al aparato telefónico 104. El servidor 106 de mensajería determina en el paso 304 si el aparato telefónico está registrado. Para el escenario mostrado en la Figura 7, el aparato telefónico 104 ya está registrado en esta fase y el servidor 106 de mensajería tiene por lo tanto la clave pública del aparato telefónico.

En el paso 350, el servidor 106 de mensajería envía una notificación a través de SMS al aparato telefónico, que indica que hay un mensaje en espera de ser entregado.

En una realización, cuando el usuario abre la bandeja de entrada de la aplicación de aparato telefónico para recuperar el mensaje protegido, esto proporciona un disparador (o activador) a la aplicación de aparato telefónico para que envíe una petición al servidor 106 de mensajería con el fin de solicitar al servidor 106 de mensajería que envíe el mensaje. Esto se muestra en el paso 352.

En el paso 354, el servidor 106 de mensajería cifra el mensaje utilizando la clave pública de aparato telefónico, y este mensaje cifrado ("Msg4") se entrega a la aplicación de aparato telefónico. En otra realización, el servidor 106 de mensajería cifra el mensaje utilizando la clave pública de aparato telefónico para generar el mensaje cifrado Msg4 antes de enviarse una notificación al aparato telefónico 104, y este mensaje cifrado Msg4 se almacena en el servidor 106 de mensajería y/o el almacenamiento 114 del servidor de mensajería hasta que el disparador induzca al servidor 106 de mensajería (paso 356) a enviar el mensaje cifrado Msg4 al aparato telefónico 104.

4. Funciones realizadas por el servidor de mensajería

La funcionalidad soportada por el servidor 106 de mensajería puede entenderse con referencia a la Figura 8, que muestra un diagrama 400 de flujo de los pasos llevados a cabo en el servidor 106 de mensajería, con referencia a la realización ejemplar de la Figura 3.

En el paso 402, el servidor 106 de mensajería recibe un mensaje no cifrado de un ordenador remitente 102, junto con el número de móvil del aparato telefónico destinatario 104 al que se ha de enviar el mensaje. En el paso 404, el servidor 106 de mensajería comprueba la base de datos que el servidor 106 de mensajería mantiene para

determinar si el aparato telefónico destinatario 104 asociado con el número de móvil ya está registrado. Si el aparato telefónico ya está registrado, entonces, en el paso 406, el servidor 106 de mensajería cifra el mensaje sin cifrar recibido (Msg1) utilizando la clave pública de aparato telefónico que el servidor 106 de mensajería ya ha guardado junto con los datos de registro asociados con el aparato telefónico previamente registrado. En el paso 408, el servidor 106 de mensajería envía un SMS al aparato telefónico 104 para notificar al destinatario que hay un mensaje en espera. Una vez que el destinatario intenta acceder al mensaje en espera, se envía un disparador al servidor 106 de mensajería en el paso 410 para inducir al servidor 106 de mensajería a enviar el mensaje. En el paso 412, el mensaje cifrado (Msg4) se entrega a la aplicación de aparato telefónico.

En una variación, el mensaje se cifra (paso 406) después de que se haya notificado al usuario que hay un mensaje en espera (paso 408). En otra variación más, el mensaje se cifra (paso 406) después de que se haya notificado al usuario (paso 408), pero antes de que el servidor 106 de mensajería reciba el disparador para enviar el mensaje cifrado (paso 410).

Si, en el paso 404, el servidor 106 de mensajería comprueba la base de datos que el servidor 106 de mensajería mantiene para determinar si el aparato telefónico destinatario 104 asociado con el número de móvil ya está registrado y determina que no lo está, entonces el servidor 106 de mensajería proporciona un cifrado intermedio al mensaje. En el paso 414, el mensaje sin cifrar recibido (Msg1) se cifra utilizando la clave de cifrado de servidor de mensajería. En el paso 416, el servidor 106 de mensajería envía una notificación al aparato telefónico 104, que indica que hay un mensaje cifrado en espera y que proporciona detalles para descargar la aplicación de aparato telefónico requerida. En el paso 418, el servidor 106 de mensajería envía una OTP al aparato telefónico 104 a través de SMS.

La autenticación del aparato telefónico 104 puede producirse en el servidor 106 de mensajería, en cuyo caso la aplicación de aparato telefónico debe solicitar al usuario que introduzca la OTP recibida a través de SMS, o puede producirse en el aparato telefónico, en cuyo caso la OTP debe enviarse a la aplicación de aparato telefónico a través de una red de comunicación de datos.

Independientemente de esto, una vez autenticado y registrado el aparato telefónico destinatario 104, entonces, en el paso 420, el servidor 106 de mensajería recibe de la aplicación de aparato telefónico la clave pública de aparato telefónico. En el paso 422, el servidor 106 de mensajería recibe un disparador de la aplicación de aparato telefónico, que induce al servidor 106 de mensajería a enviar el mensaje al aparato telefónico 104. Después, el servidor 106 de mensajería descifra el mensaje cifrado intermedio Msg2 utilizando la clave de descifrado de servidor, y cifra de nuevo el mensaje utilizando esta vez la clave pública de aparato telefónico (paso 410). En el paso 412, el mensaje cifrado (Msg4) se entrega a la aplicación de aparato telefónico.

En otra realización, el mensaje cifrado intermedio Msg2 se descifra (paso 424) y se cifra utilizando la clave pública de aparato telefónico (paso 510) para proporcionar el mensaje cifrado Msg4, después de que el servidor 106 de mensajería reciba la clave pública de aparato telefónico del servidor de aplicación (paso 520). En tal realización, el servidor 106 de mensajería almacena el mensaje en la forma cifrada final (Msg4) hasta recibir un disparador (paso 422).

Aunque no se muestra, se deduce de todas las descripciones anteriores que el paso 418 descrito con referencia a la Figura 8 puede sustituirse por un paso consistente en recibir del aparato telefónico un SMS que comprenda la OTP y recibir, a través de una red de comunicación de datos, un identificador de aparato telefónico introducido por el usuario con la OTP generada por la aplicación de aparato telefónico. Con toda esta información a mano, el servidor 106 de mensajería está equipado para comparar parejas de OTP/números de móvil para así autenticar y registrar el aparato telefónico 104. Esto está de acuerdo con las descripciones anteriores.

El sistema y el procedimiento descritos en la presente memoria tienen varias ventajas, incluyendo:

si el servidor de mensajería se ve comprometido, los mensajes enviados a todos los aparatos telefónicos no pueden descifrarse, porque las claves privadas no son conocidas en el servidor 106 de mensajería;

si un aparato telefónico 104 se ve comprometido, sólo se ven comprometidos los mensajes del destinatario, y la aplicación puede restablecer una nueva clave pública/privada para ese destinatario (por ejemplo utilizando una semilla diferente para el generador de números aleatorios para obtener las claves, en lugar de utilizar el número de móvil);

todos los aparatos telefónicos se validan a través de una contraseña temporal, tal como una contraseña de un solo uso, asociada con el aparato telefónico, mejorando así la seguridad del sistema;

el ordenador remitente no necesita indicar previamente a un destinatario que se requiere una aplicación de aparato telefónico para recibir el mensaje cifrado; y

no es necesario que un aparato telefónico esté previamente registrado para que un ordenador remitente envíe un mensaje cifrado al aparato telefónico. Como tales, los destinatarios de mensajes no necesitan descargar ni registrar la aplicación de aparato telefónico hasta que haya de recuperarse un mensaje cifrado.

Se entenderá que la invención descrita y definida en esta especificación se extiende a todas las combinaciones alternativas de dos o más de las características individuales mencionadas o que resulten evidentes por el texto o los dibujos. Todas estas combinaciones diferentes constituyen diversos aspectos alternativos de la invención.

REIVINDICACIONES

1. Un procedimiento en un servidor (106) de mensajería para registrar un aparato telefónico (104) para permitir el envío seguro de mensajes seguros al aparato telefónico (104), comprendiendo el método los pasos secuenciales de:

recibir un identificador de aparato telefónico que identifique el aparato telefónico (104) desde el aparato telefónico (104);

generar una contraseña temporal;

transmitir la contraseña temporal al aparato telefónico (104);

recibir una contraseña de retorno desde el aparato telefónico (104);

comparar la contraseña temporal con la contraseña de retorno; y

en el caso en el que la contraseña temporal y la contraseña de retorno coincidan:

transmitir un acuse de recibo de autenticación al aparato telefónico (104);

recibir una clave de cifrado desde aparato telefónico (104); y

almacenar la clave de cifrado de aparato telefónico contra el identificador de aparato telefónico del aparato telefónico (104) para registrar el aparato telefónico (104) para permitir el envío seguro de mensajes seguros al aparato telefónico (104);

en donde los canales de comunicación diferentes se utilizan para proporcionar la contraseña temporal al aparato telefónico (104) y recibir la contraseña de retorno desde el aparato telefónico (104).

2. El procedimiento de la reivindicación 1, en el que el identificador de aparato telefónico comprende un MSISDN del aparato telefónico (104).

3. El procedimiento de la reivindicación 1 o reivindicación 2, en el que la clave de cifrado de aparato telefónico comprende una clave pública generada por generación de clave asimétrica por el aparato telefónico (104) y una clave de descifrado privada correspondiente generada por generación de clave asimétrica por el aparato telefónico (104) no se comparte por el aparato telefónico (104).

4. El procedimiento de cualquier reivindicación precedente, en donde la contraseña temporal se envía al aparato telefónico (104) como parte de un mensaje SMS, mientras que la contraseña de retorno se recibe del aparato telefónico (104) utilizando una red móvil pública que soporta comunicación de datos.

5. El procedimiento de cualquier reivindicación precedente, que incluye recibir el identificador del aparato telefónico (104) con una contraseña de retorno, y en donde el paso de comparar las contraseñas incluye comparar el identificador del aparato telefónico recibido con la contraseña de retorno, con el identificador del aparato telefónico del aparato telefónico (104) al que se había enviado la contraseña temporal.

6. El procedimiento de cualquier reivindicación precedente, en donde la contraseña temporal comprende una contraseña de un solo uso que es válida por un periodo de tiempo limitado.

7. El procedimiento de la reivindicación 6, en el que la contraseña temporal contiene 6 números.

8. Un servidor (106) de mensajería que comprende:

un procesador; y

una memoria con instrucciones, que cuando se ejecutan por el procesador, provocan que el servidor (106) de mensajería lleve a cabo el procedimiento de una cualquiera de las reivindicaciones 1 a 7.

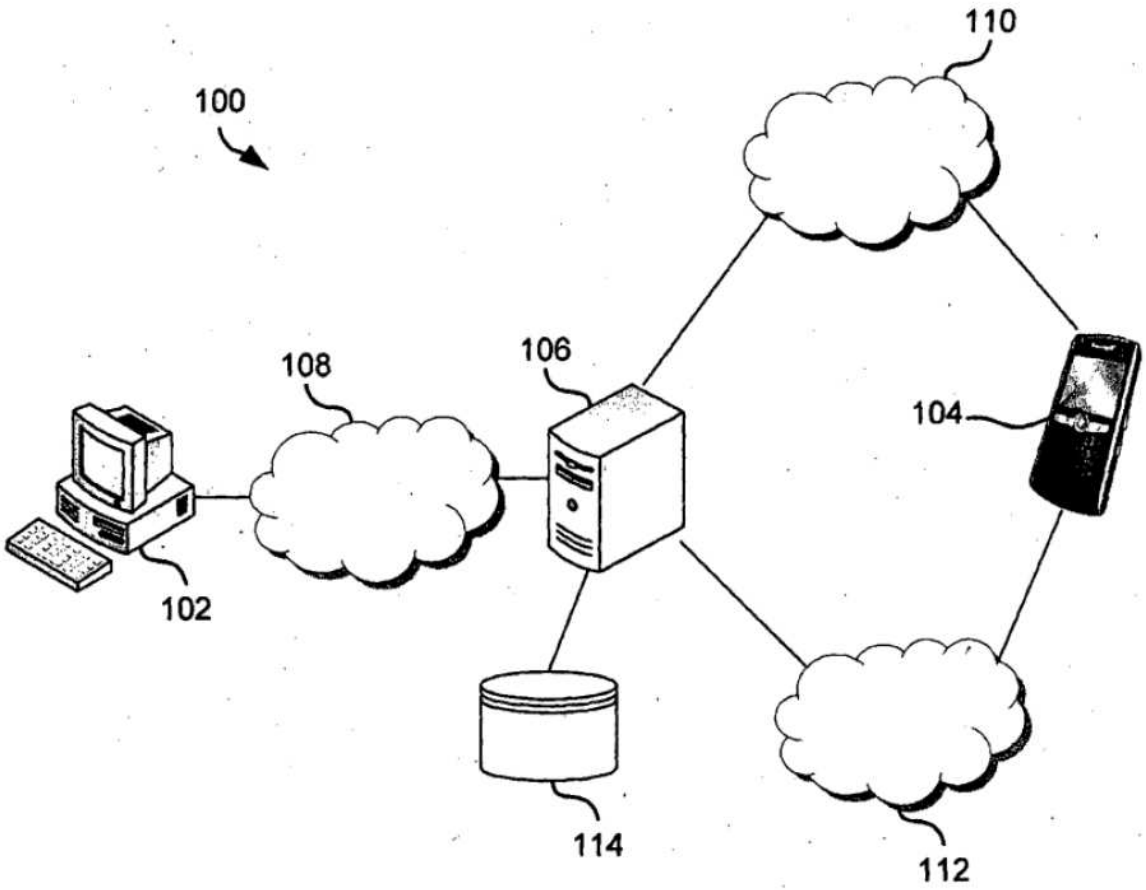

Figura 1

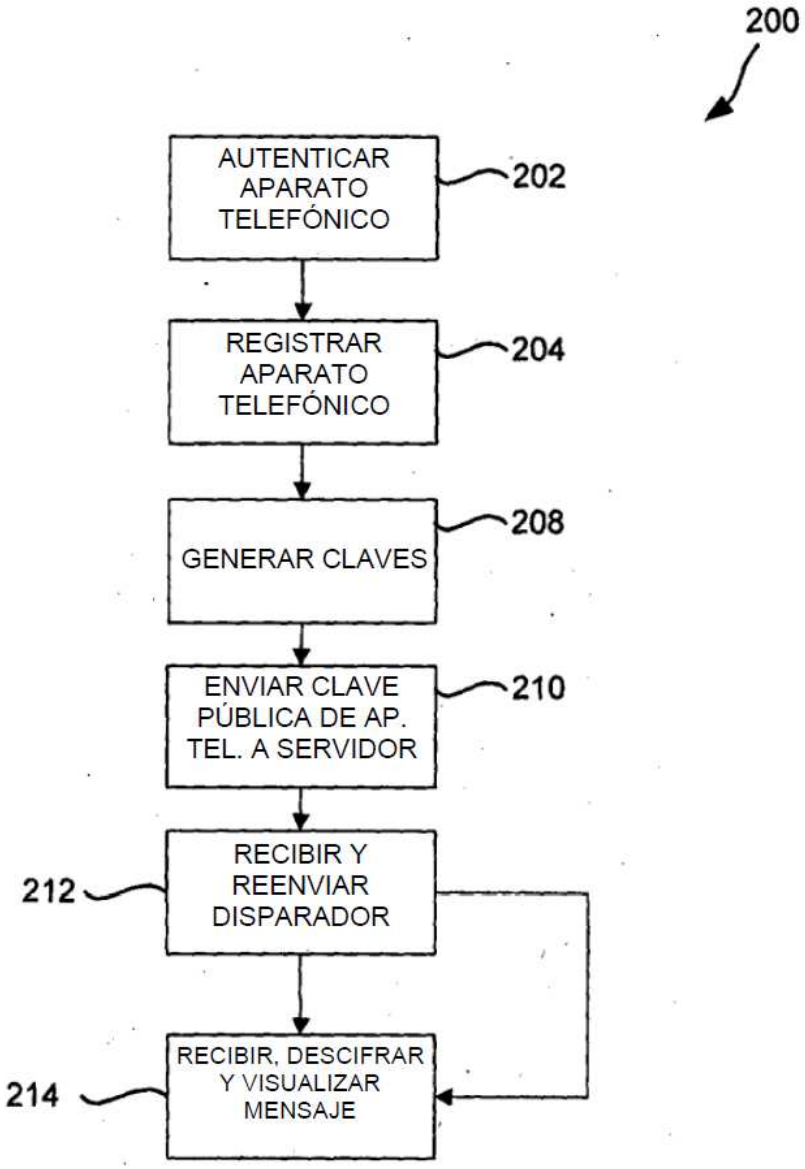
200
AUTENTICAR APARATO TELEFÓNICO
202
REGISTRAR APARATO TELEFÓNICO
204
GENERAR CLAVES
208
ENVIAR CLAVE PÚBLICA DE AP. TEL. A SERVIDOR
210
RECIBIR Y REENVIAR DISPARADOR
212
RECIBIR, DESCIFRAR Y VISUALIZAR MENSAJE
214

Figura 2

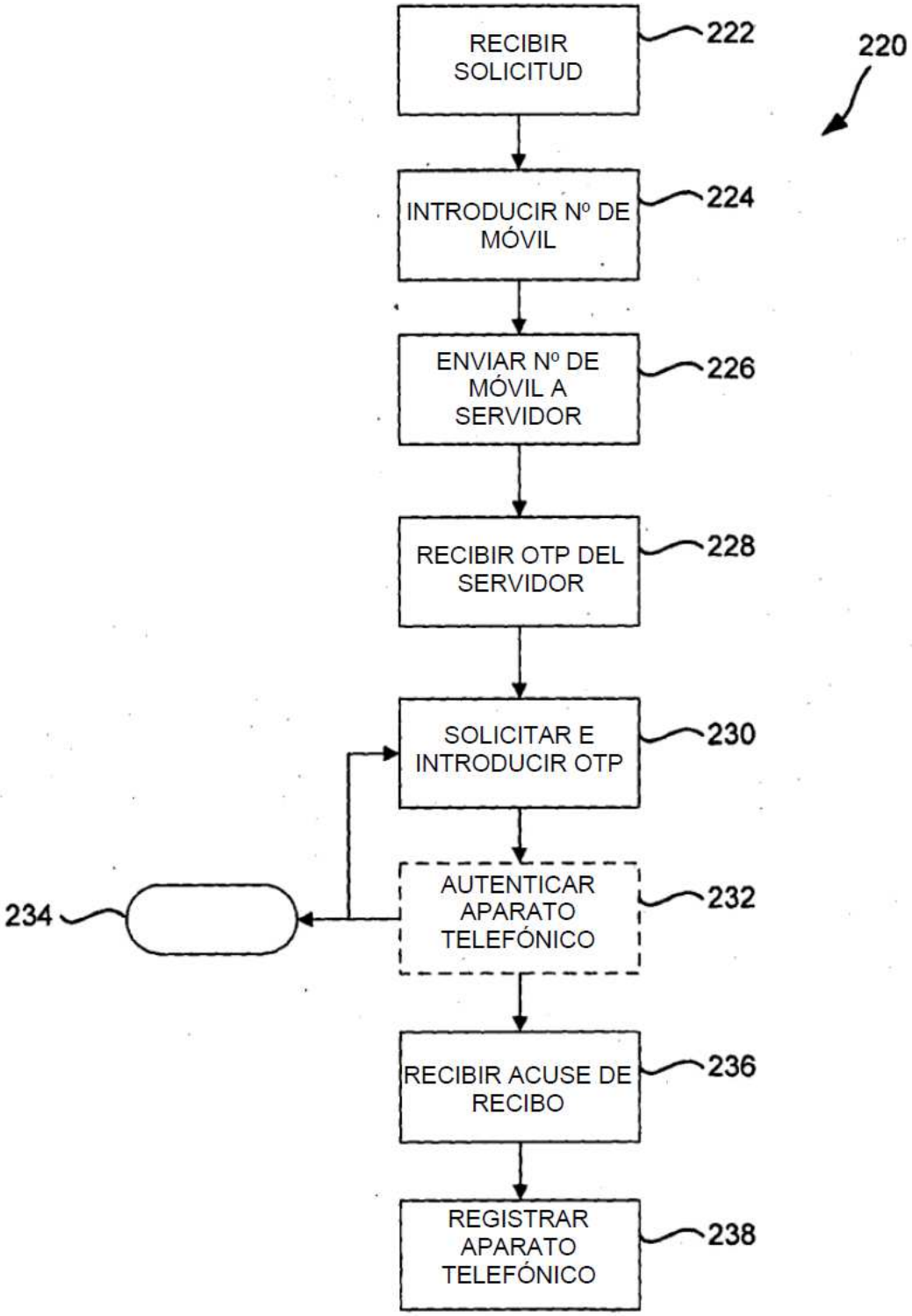
220
RECIBIR SOLICITUD
222
INTRODUCIR Nº DE MÓVIL
224
ENVIAR Nº DE MÓVIL A SERVIDOR
226
RECIBIR OTP DEL SERVIDOR
228
SOLICITAR E INTRODUCIR OTP
230
AUTENTICAR APARATO TELEFÓNICO
232
234
RECIBIR ACUSE DE RECIBO
236
REGISTRAR APARATO TELEFÓNICO
238

Figura 3

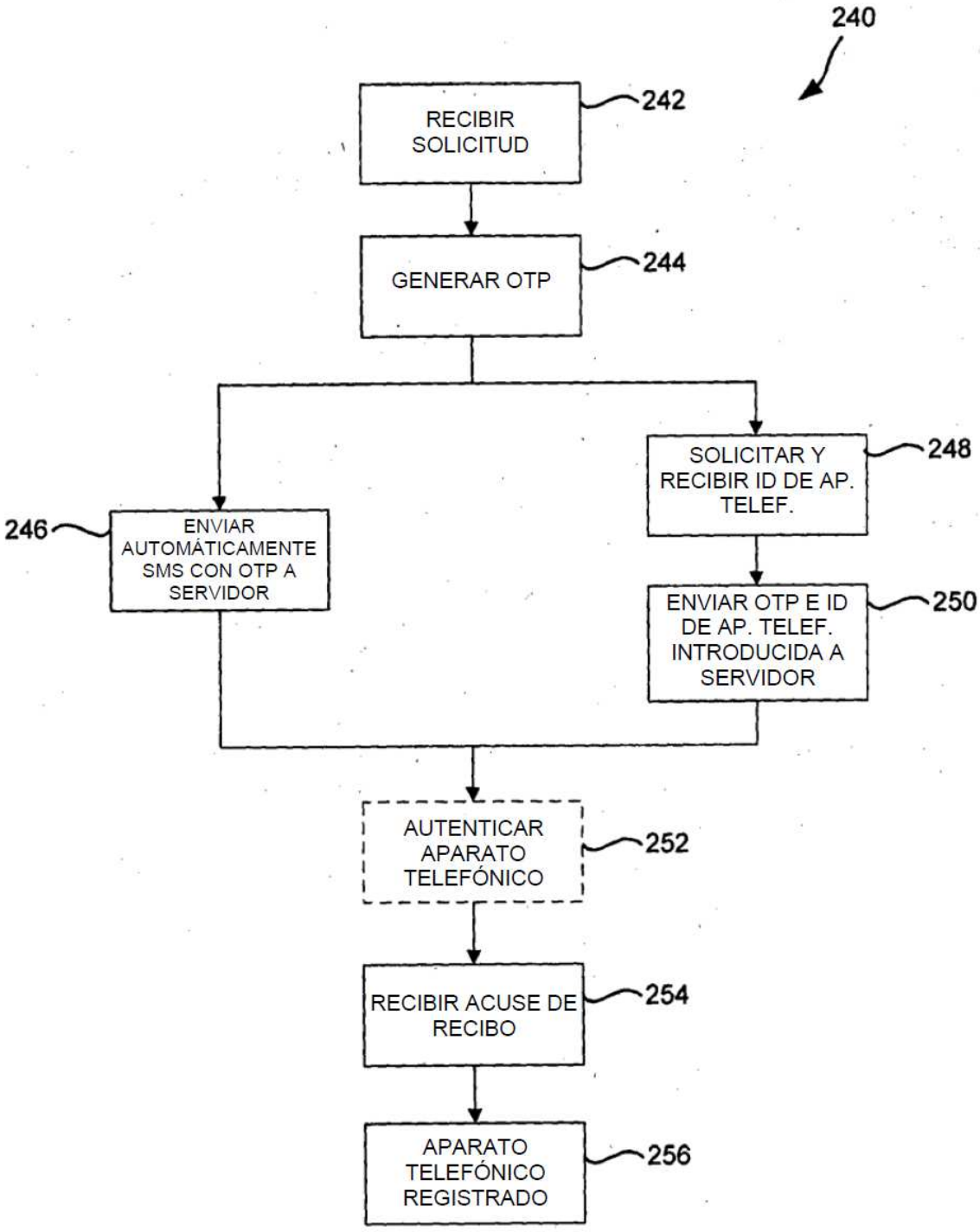
240
RECIBIR SOLICITUD
242
GENERAR OTP
244
246
ENVIAR AUTOMÁTICAMENTE SMS CON OTP A SERVIDOR
SOLICITAR Y RECIBIR ID DE AP. TELEF.
248
ENVIAR OTP E ID DE AP. TELEF. INTRODUCIDA A SERVIDOR
250
AUTENTICAR APARATO TELEFÓNICO
252
RECIBIR ACUSE DE RECIBO
254
APARATO TELEFÓNICO REGISTRADO
256

Figura 4

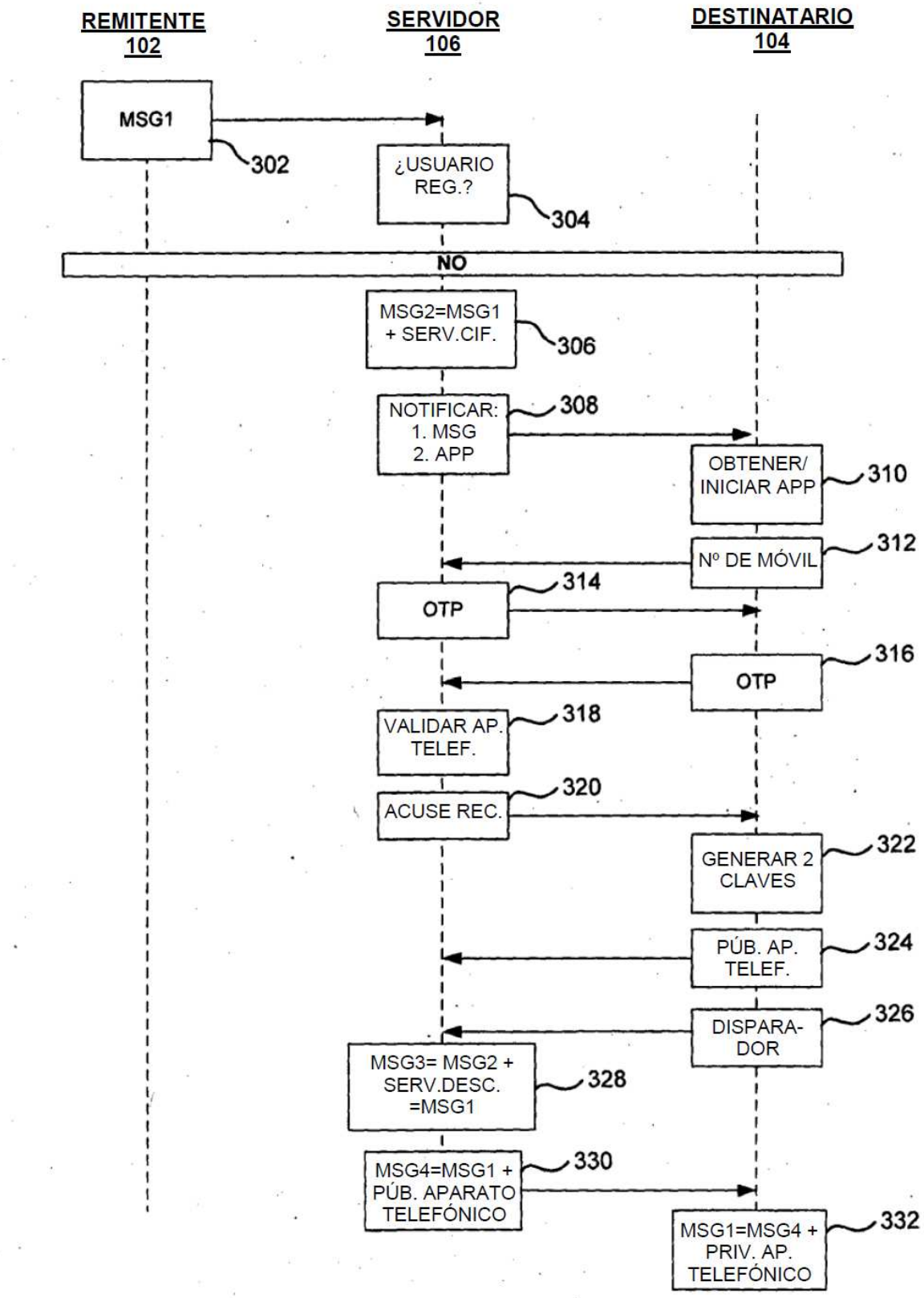
REMITENTE
102
SERVIDOR
106
DESTINATARIO
104
MSG1
302
¿USUARIO REG.?
304
NO
MSG2=MSG1 + SERV.CIF.
306
NOTIFICAR: 1. MSG 2. APP
308
OBTENER/ INICIAR APP
310
Nº DE MÓVIL
312
OTP
314
OTP
316
VALIDAR AP. TELEF.
318
ACUSE REC.
320
GENERAR 2 CLAVES
322
PÚB. AP. TELEF.
324
DISPARA-DOR
326
MSG3= MSG2 + SERV.DESC. =MSG1
328
MSG4=MSG1 + PÚB. APARATO TELEFÓNICO
330
MSG1=MSG4 + PRIV. AP. TELEFÓNICO
332

Figura 5

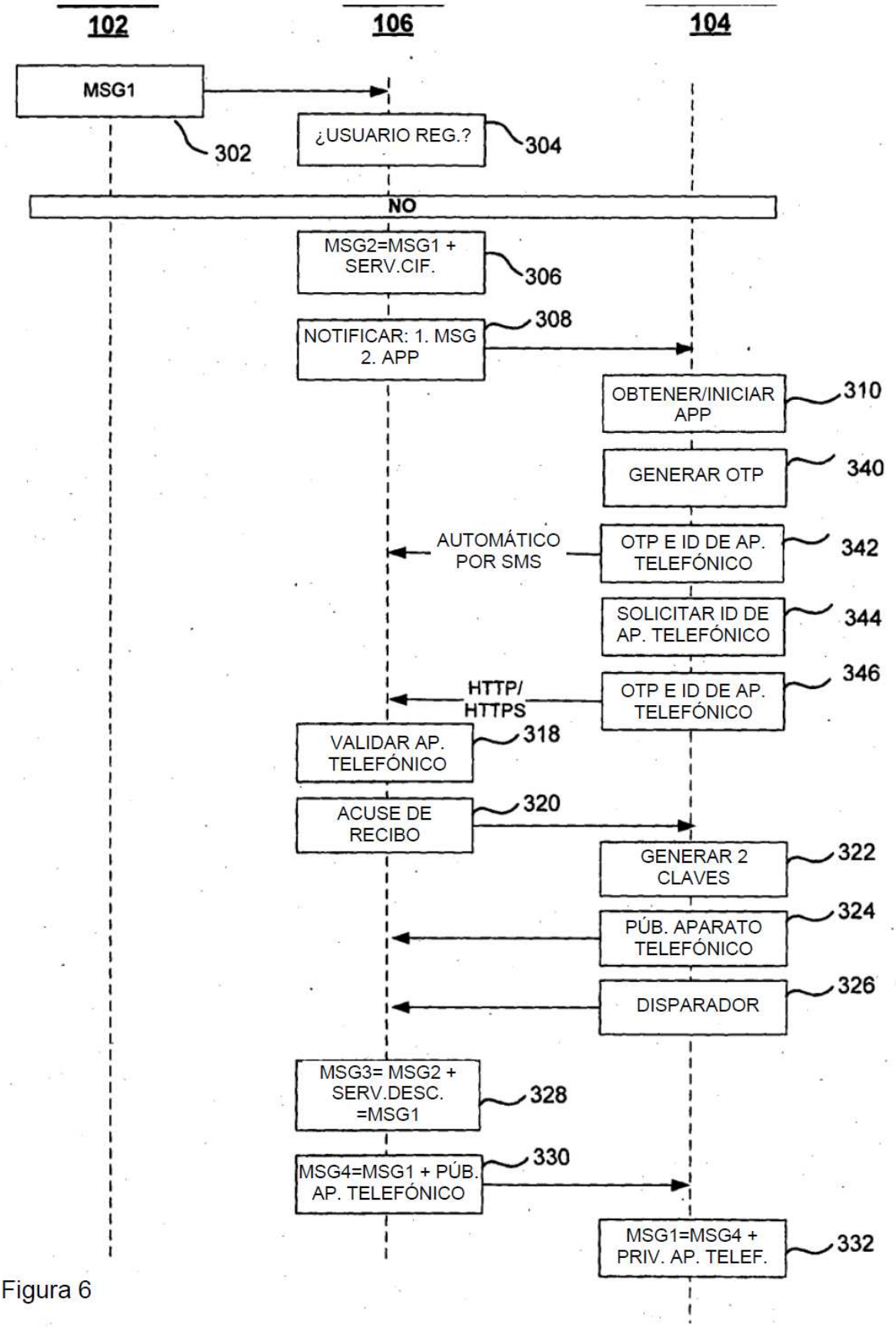
102
106
104
MSG1
302
¿USUARIO REG.?
304
NO
MSG2=MSG1 + SERV.CIF.
306
NOTIFICAR: 1. MSG 2. APP
308
OBTENER/INICIAR APP
310
GENERAR OTP
340
AUTOMÁTICO POR SMS
OTP E ID DE AP. TELEFÓNICO
342
SOLICITAR ID DE AP. TELEFÓNICO
344
HTTP/ HTTPS
OTP E ID DE AP. TELEFÓNICO
346
VALIDAR AP. TELEFÓNICO
318
ACUSE DE RECIBO
320
GENERAR 2 CLAVES
322
PÚB. APARATO TELEFÓNICO
324
DISPARADOR
326
MSG3= MSG2 + SERV.DESC. =MSG1
328
MSG4=MSG1 + PÚB. AP. TELEFÓNICO
330
MSG1=MSG4 + PRIV. AP. TELEF.
332

Figura 6

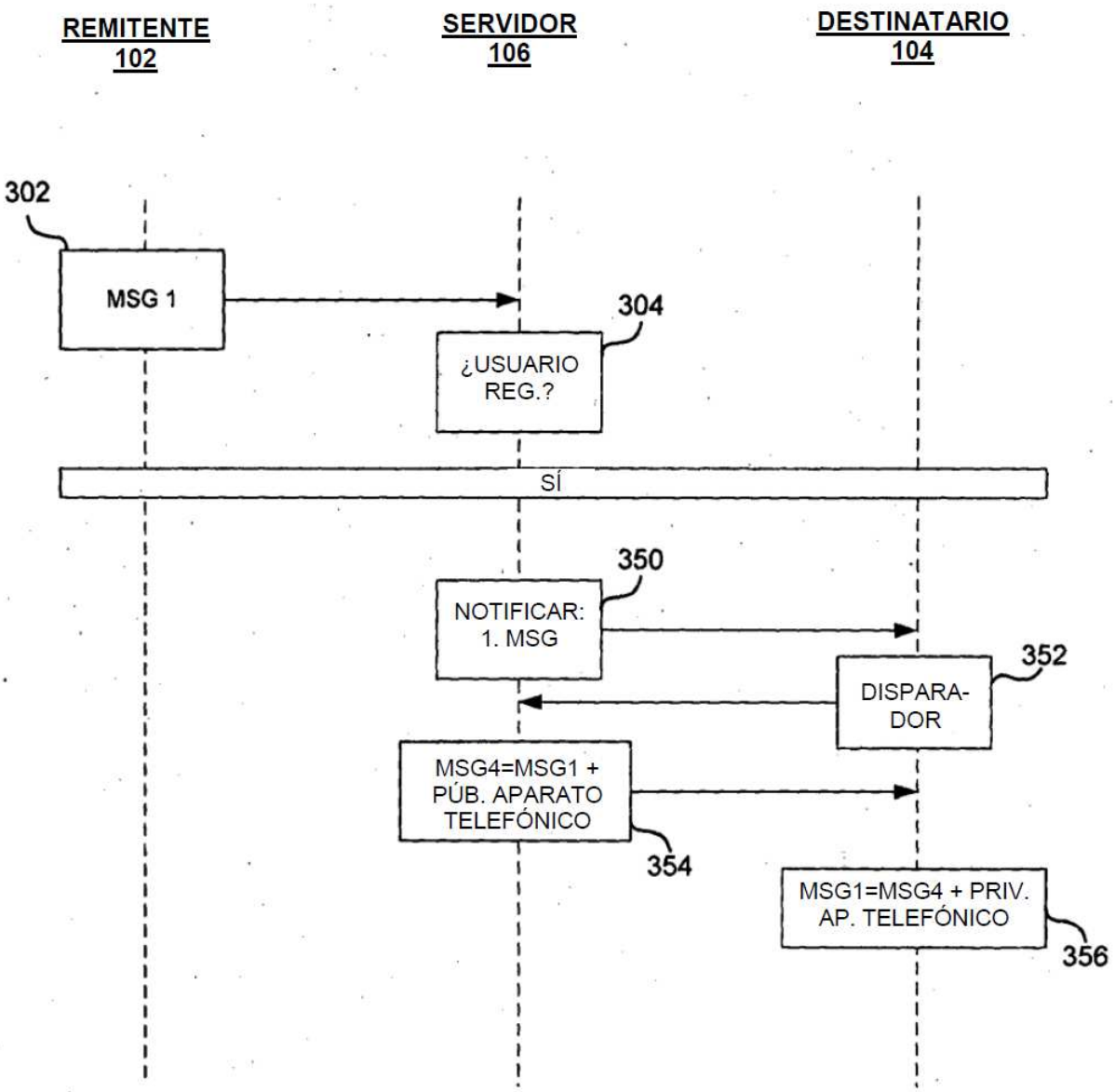
REMITENTE
102
SERVIDOR
106
DESTINATARIO
104
302
MSG 1
304
¿USUARIO REG.?
SÍ
350
NOTIFICAR: 1. MSG
352
DISPARA-DOR
MSG4=MSG1 + PÚB. APARATO TELEFÓNICO
354
MSG1=MSG4 + PRIV. AP. TELEFÓNICO
356

Figura 7

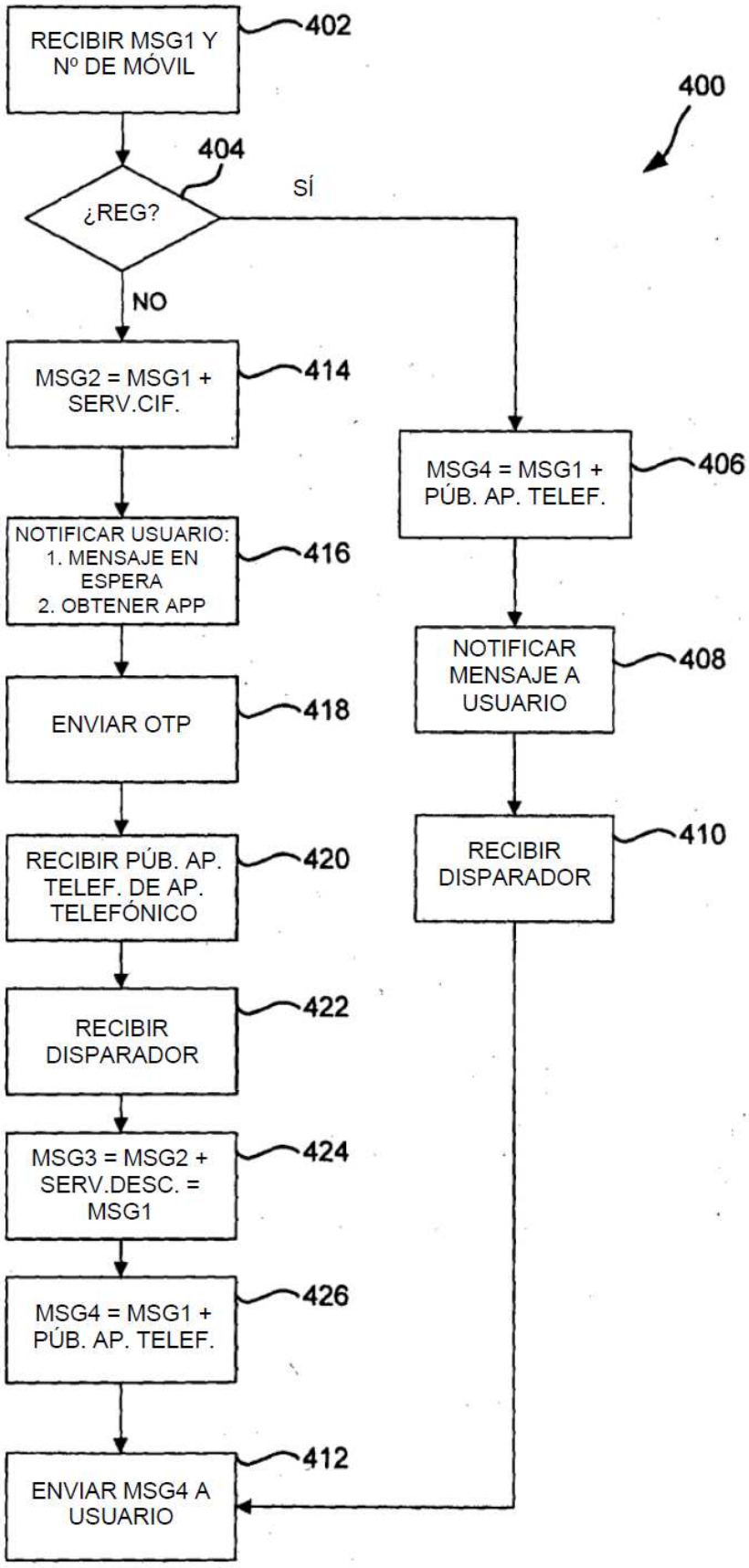
RECIBIR MSG1 Y Nº DE MÓVIL
402
400
404
¿REG?
SÍ
NO
MSG2 = MSG1 + SERV.CIF.
414
MSG4 = MSG1 + PÚB. AP. TELEF.
406
NOTIFICAR USUARIO: 1. MENSAJE EN ESPERA 2. OBTENER APP
416
NOTIFICAR MENSAJE A USUARIO
408
ENVIAR OTP
418
RECIBIR PÚB. AP. TELEF. DE AP. TELEFÓNICO
420
RECIBIR DISPARADOR
410
RECIBIR DISPARADOR
422
MSG3 = MSG2 + SERV.DESC. = MSG1
424
MSG4 = MSG1 + PÚB. AP. TELEF.
426
ENVIAR MSG4 A USUARIO
412

FIGURA 8