

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 668 396**

51 Int. Cl.:

H04W 12/02 (2009.01)

H04L 29/06 (2006.01)

H04L 12/58 (2006.01)

H04W 12/08 (2009.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **22.12.2009** **PCT/ES2009/000594**

87 Fecha y número de publicación internacional: **01.07.2010** **WO10072863**

96 Fecha de presentación y número de la solicitud europea: **22.12.2009** **E 09834150 (6)**

97 Fecha y número de publicación de la concesión europea: **14.02.2018** **EP 2378800**

54 Título: **Sistema de comunicación seguro**

30 Prioridad:

23.12.2008 ES 200803669

26.06.2009 ES 200930365

45 Fecha de publicación y mención en BOPI de la traducción de la patente:
17.05.2018

73 Titular/es:

FMF GESTIÓN, S.L. (100.0%)

Plaça Guillemo 3

AD500 Andorra la Vella, AD

72 Inventor/es:

TROYANO TIBURCIO, FERNANDO

74 Agente/Representante:

CARPINTERO LÓPEZ, Mario

ES 2 668 396 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Sistema de comunicación seguro

La presente invención se refiere a un sistema de comunicación.

5 En particular, la presente invención se refiere a un sistema de comunicación que pretende especialmente preservar la privacidad en la comunicación de mensajería telefónica, aunque la presente invención no necesariamente se limita a dicha aplicación.

La seguridad y, más particularmente, la privacidad de comunicaciones es uno de los problemas que surgen con comunicaciones a través de redes de telefonía móvil a través de protocolos de mensajería móvil. Específicamente, en comunicaciones a través de mensajería móvil, se producen los siguientes eventos:

- 10
- el terminal (normalmente un teléfono móvil) recibe el mensaje sin control de usuario;
 - el terminal envía una notificación de mensaje recibido que se visualiza en la interfaz de usuario (pantalla) del terminal móvil;
 - el terminal almacena físicamente el mensaje recibido en su dispositivo de memoria.

15 En consecuencia, cualquier tercera persona que acceda al terminal del usuario sabrá si hay nuevos mensajes y puede acceder a los mensajes almacenados en el dispositivo de memoria, incluyendo nuevos mensajes que aún no ha sido leídos por el usuario.

De hecho, diversos estudios concluyen que la mayoría de casos de infidelidad de pareja se descubren a través de teléfonos móviles.

20 La presente invención desvela nuevos medios técnicos de mantenimiento de la privacidad de mensajes de telefonía móvil.

El documento EP 1788771A desvela un sistema y un procedimiento de gestión de mensajes electrónicos. Los dispositivos emisores cifran los mensajes y se reciben mediante un servidor. El servidor aplica una serie de procedimientos de seguridad que determinan si el mensaje recibido se enviará o no al usuario final.

25 El documento EP 1921792 desvela un sistema de comunicación que habilita que se comuniquen datos entre un primer y un segundo dispositivo terminal a base de una contraseña compartida entre esos dispositivos terminal. Este sistema se caracteriza porque dicho primer dispositivo terminal usa un desencadenante para informar al otro terminal que ha comenzado comunicación de datos a través de un canal de comunicación y un procedimiento de comunicación. En respuesta a la transmisión y recepción del desencadenante de la comunicación de datos se establece un canal de comunicación, que usa un segundo procedimiento de comunicación entre el dispositivo y un

30 servidor de retransmisión que reenvía la contraseña cifrada, el canal de comunicación se cambia del primer canal de comunicación al segundo canal de comunicación, que usa un segundo medio de comunicación entre el segundo dispositivo y un segundo servidor de retransmisión que reenvía la contraseña cifrada, el canal de comunicación se cambia al canal de comunicación para el segundo procedimiento y dicha contraseña cifrada se comparte a través del canal entre los dispositivos terminales.

35 El documento WO 2007/107554 desvela un procedimiento de control de usuarios a través de un sistema de comunicación que incluye un servidor y un dispositivo de comunicación (por ejemplo, un teléfono móvil) que se comunica a través de una red de comunicación. En este caso, el servidor satisface el fin de mantener una base de datos que comprende datos de control del dispositivo de comunicación, habilitando códigos personales secretos y que la identidad de un usuario se verifique a base del mensaje recibido y los datos de control.

40 El documento WO 2007/006815 A2 desvela un procedimiento de cifrado y un sistema de transferencia de mensajes seguros a y desde teléfonos móviles de tal forma que esos mensajes seguros pueden no interceptarse por Terceras Partes, por ejemplo, accediendo al SMSC en el que siempre se hace una copia de un mensaje SMS antes de la transmisión hacia delante. Dicho sistema comprende un servidor de mensaje seguro que tiene una memoria y en el que se transmiten y almacenan mensajes seguros en la memoria de servidor de mensaje seguro para posterior

45 recogida del destinatario previsto. En dicho procedimiento de recogida, el usuario previsto del mensaje necesita comprobar periódicamente el servidor seguro para mensajes y en vista de que hay un mensaje almacenado en dicho servidor, dicho usuario descarga el mensaje a su teléfono móvil. En consecuencia, el mensaje se almacena en la memoria de dispositivo móvil y por lo tanto es accesible y/o recuperable por cualquier tercera persona.

50 El documento US 2002/107002 A1 desvela un sistema de envío de alertas de mensaje de texto a dispositivos de comunicaciones móviles en los que dicho mensaje de texto contiene únicamente un resumen y el usuario puede acceder a información adicional descargando una página web de respuesta. El sistema comprende: un proveedor de información que suministra a un servidor información relacionada con productos/servicios de interés a varios usuarios; un servidor que recibe, almacena y resume dicha información y envía la misma con un enlace de Internet a un dispositivo de comunicación de usuario quien puede descargar una página web de respuesta con la información

55 original. Este sistema forma claramente parte del estado de la técnica.

La invención se define mediante las reivindicaciones adjuntas. El objeto de la presente invención es divulgar un sistema (una combinación de medios técnicos y sus interrelaciones) que pueden mantener la privacidad sin la

necesidad de usar cifrado o almacenar mensajes en el terminal (aunque dichas posibilidades no se excluyen), y que evitan que una tercera persona conozca que incluso exista una comunicación privada. La presente invención también tiene la ventaja de que puede implementarse en sistemas de comunicación existentes.

De acuerdo con la presente invención el emisor de mensaje envía a través de un dispositivo de comunicación (habitualmente un teléfono móvil) un mensaje con una estructura que difiere del de un mensaje de telefonía móvil estándar. En particular, dicho mensaje tiene al menos una porción privada. Más preferentemente, dicho mensaje tiene dos porciones, al menos una de las cuales es confidencial. El mensaje modificado, a diferencia de lo que sucede en sistemas de comunicación conocidos, no se envía directamente al dispositivo de comunicación móvil del receptor, sino que se envía en su totalidad a un servidor con características especiales. Dicho servidor tiene una estructura de tal forma que puede diferenciar cada una de las dos porciones del mensaje y seleccionar el canal de transmisión de envío de cada una de dichas porciones dependiendo de su naturaleza. Las porciones no confidenciales se envían (habitualmente mediante SMS) al dispositivo móvil de recepción (habitualmente un teléfono móvil), por ejemplo, a través de los canales de transmisión convencionales. La porción pública del mensaje modificado puede actuar habitualmente como notificación de la existencia de una porción del mensaje confidencial (dicha notificación puede incluir una instrucción para el dispositivo móvil de recepción). Para su parte, la porción del mensaje confidencial se almacena preferentemente en el servidor hasta que el usuario del dispositivo móvil de recepción decide recuperar y leer dicha porción confidencial en su dispositivo (teléfono móvil), usando una aplicación provista en su dispositivo. Esta puede ser una aplicación de gestión de comunicaciones de tipo IP, pero también podría ser una aplicación especializada. Para hacer esto, debe enviarse una instrucción al servidor desde el dispositivo móvil para acceder desde el teléfono móvil. Por lo tanto, la porción del mensaje confidencial no se almacena en el dispositivo de memoria del dispositivo móvil de recepción (siempre se visualiza en el teléfono móvil pantalla, pero no se almacena) y, por lo tanto, es imposible que terceras personas accedan al contenido del mensaje confidencial o incluso sepan de su existencia.

En particular, la presente invención comprende un sistema de comunicación que comprende

- un dispositivo de comunicación de envío,
- un servidor de mensajería móvil, y
- un dispositivo de comunicación de recepción (que preferentemente será un dispositivo móvil),

en el que el dispositivo de comunicación de envío envía un mensaje a través de una red de comunicación al servidor de mensajería móvil para el envío al dispositivo de comunicación móvil a través de un red de comunicación de telefonía móvil, estando el servidor provisto de un módulo de comunicación de recepción y envío del mensaje, estando el dispositivo de comunicación de recepción provisto de una memoria electrónica de almacenamiento de mensajes de telefonía móvil, una pantalla de interfaz de usuario y un módulo para visualizar mensajes almacenados en la pantalla de interfaz, en el que

- el mensaje enviado mediante el dispositivo de comunicación contiene al menos una porción privada (preferentemente, contendrá una porción pública y una porción privada), siendo dicho mensaje enviado a un servidor seguro, y
- el sistema comprende un servidor seguro que tiene un módulo de reconocimiento y gestión de las porciones pública y privada del mensaje recibido, de tal forma que el módulo de comunicación del servidor envía únicamente la porción pública del mensaje a través de la red de comunicación de telefonía móvil, estando el servidor seguro disponible para consulta en el mismo, y envía la porción privada a través de un canal de comunicación diferente. De acuerdo con la presente invención, la última fase preferentemente tiene lugar dejando la porción privada del mensaje enviado mediante el dispositivo de envío almacenada en un dispositivo de memoria especializada, estando el dispositivo de comunicación móvil también provisto de un módulo de comunicación que habilita que el mismo acceda a la porción privada del mensaje almacenado en el servidor seguro para visualizar el mismo en la pantalla de interfaz sin la necesidad de almacenamiento en el dispositivo de memoria del dispositivo móvil de recepción.

Para hacer esto, de acuerdo con un aspecto de la presente invención, el dispositivo de comunicación de recepción tiene un módulo de comunicación que habilita que dicho dispositivo acceda a la porción privada del mensaje almacenado en el servidor seguro, teniendo dicho módulo de comunicación submódulos para operar en los recursos del dispositivo de comunicación de recepción, comprendiendo dichos submódulos un submódulo de interfaz para visualizar el mensaje gráficamente en la pantalla y un submódulo de control de la memoria no volátil del dispositivo de comunicación de recepción, de modo que el mensaje privado no se almacena de forma accesible en la memoria no volátil del dispositivo de comunicación de recepción.

La representación gráfica (no alfanumérica) del mensaje que sigue en la pantalla permite que no sea almacenado de forma accesible en la memoria no volátil del dispositivo de comunicación que recibe el mensaje, de modo que una tercera persona no puede detectar la existencia de un mensaje seguro al que él/ella no puede acceder. Para que esto se produzca con máxima seguridad, el submódulo de control de memoria preferentemente borra la información relacionada con la porción privada una vez que el submódulo de interfaz ha visualizado dicha porción privada gráficamente en la pantalla.

Donde el mensaje enviado mediante el dispositivo de envío tiene una porción pública y otra porción privada, el módulo de reconocimiento y gestión del servidor seguro debe diferenciar entre la porción pública y la porción

privada. Si no contiene una porción pública (o si esta porción está vacía), el módulo puede generar una porción pública automáticamente si es necesario. La porción pública del mensaje enviada al dispositivo de comunicación de recepción contiene un desencadenante para que el dispositivo de comunicación móvil inicie comunicación con el servidor a través del módulo de comunicación del dispositivo de comunicación de recepción.

- 5 También es posible que el mensaje público no contenga una instrucción y es la responsabilidad del usuario receptor iniciar comunicación con el servidor seguro en recepción de la porción pública.

Preferentemente, el servidor seguro envía la porción pública al servidor de mensajería móvil.

También es posible, en una realización preferida, que el servidor seguro contenga el servidor de mensajería móvil como un módulo integrado.

- 10 Para realizar interrelaciones del sistema de acuerdo con la invención, el servidor seguro preferentemente también comprende

- un módulo de procesamiento de mensajes para distinguir la porción pública y porción privada de los mensajes, y
- un módulo de gestión de comunicaciones seguras con los dispositivos móviles de recepción.

- 15 Adicionalmente, y con el mismo objeto, preferentemente tanto el dispositivo de comunicación de recepción móvil como el dispositivo de envío comprenden un módulo de comunicación de comunicación con el servidor seguro.

Preferentemente, el módulo de comunicación comprende un submódulo de compresión de datos, un submódulo de comunicación IP (por ejemplo, HTTP) y un submódulo de comunicación de mensajería de telefonía móvil (por ejemplo, SMS).

- 20 Particularmente preferentemente para la presente invención, el dispositivo de comunicación de envío es un dispositivo de telefonía móvil y el dispositivo de comunicación de recepción es también un dispositivo de telefonía móvil.

Para aumentar la seguridad, preferentemente se cifran comunicaciones con el servidor seguro relacionadas con mensajes que comprende porciones privadas. También preferentemente, el servidor seguro requiere identificación de usuario y contraseña para recibir o enviar mensajes que comprenden porciones privadas.

- 25 Comunicaciones de mensajes privados entre el dispositivo de comunicación de recepción y el servidor seguro son preferentemente comunicaciones HTTP.

Definiciones

- 30 Dispositivo: cualquier dispositivo capaz de recibir cualquier tipo de mensaje a través de una red de comunicación, interpretar dicho mensaje, almacenar el mismo en su propio dispositivo de memoria y visualizar el mismo en una interfaz de usuario.

Dispositivo móvil: cualquier dispositivo capaz de recibir cualquier tipo de mensaje a través de una red de comunicación inalámbrica, interpretar dicho mensaje, almacenar el mismo en su propio dispositivo de memoria y visualizar el mismo en una interfaz de usuario.

Teléfono móvil: dispositivo portátil de acceso a diversos medios de teléfono móvil y transmisión de datos.

- 35 Mensaje: cualquier tipo de información digital, incluyendo texto de SMS, MMS, fotografías, videos, correos electrónicos y voz que puede recibirse, almacenarse y visualizarse en un dispositivo móvil.

Aplicación: conjunto de instrucciones y procedimientos para un dispositivo que determina y controla al menos parte de la operación de un dispositivo.

- 40 Servidor: conjunto de dispositivos IT capaces de recibir, almacenar, coordinar y enviar datos a través de canales de transmisión diferentes.

Canal: cualquier red o canal de envío, transmisión y/o recepción de datos.

Para un mejor entendimiento, los dibujos adjuntos muestran como un ejemplo una realización preferida explicativa pero no limitante de la presente invención.

- 45 La Figura 1 muestra esquemáticamente la estructura física básica de una realización de la presente invención, consistente en una plataforma de envío de mensajes de mensajería telefónica privados en una estructura pública preexistente que usa tecnología celular.

La Figura 2 muestra esquemáticamente la estructura física básica con detalle del servidor de una realización de la presente invención en la que todas las comunicaciones entre emisor y receptor pasan a través del mismo servidor.

- 50 La Figura 3 muestra esquemáticamente la función de envío de un mensaje privado.

La Figura 4 muestra esquemáticamente la función de envío por el emisor y la función de acceso por el receptor de un mensaje privado.

La Figura 5 muestra esquemáticamente las funciones de envío y recepción para las porciones públicas de los mensajes, y las funciones de envío y acceso para las porciones privadas desde diversos emisores a un receptor.

5 La Figura 6 muestra esquemáticamente una estructura física similar a la mostrada en la Figura 2 en la que se establecen flujos de comunicación entre el servidor y el emisor y entre el servidor y el receptor.

La Figura 7 muestra en mayor detalle las acciones, instrucciones y flujos de datos establecidos entre servidor y receptor en el ejemplo de la Figura 6.

10 La Figura 8 es un diagrama de los módulos de un dispositivo de comunicación móvil adecuado para operar como el receptor en la realización de las Figuras 6 y 7.

La Figura 9 es un diagrama de flujo principal para el ejemplo de las Figuras 6 a 8.

La Figura 10 es un diagrama de flujo para un módulo de datos de una realización de acuerdo con las Figuras 6 a 9.

15 La Figura 11 es un diagrama que muestra la arquitectura de gestión del dispositivo para la recepción de comunicaciones para no tener que almacenar la porción privada del mensaje.

La Figura 1 muestra esquemáticamente la estructura física básica de una realización de la invención, consistente en un sistema o plataforma de envío de mensajes de mensajería telefónica privados en una estructura pública preexistente o sistema que usa tecnología celular.

20 La estructura pública (a la izquierda de la línea de separación) comprende un dispositivo de comunicación de envío, en este caso particular un terminal 1 móvil, un servidor 60 de mensajería de telefonía móvil (por ejemplo, una pasarela de SMS) y un dispositivo de comunicación de recepción móvil, en este caso un teléfono móvil u organizador 3 personal. En operación normal, el dispositivo 1 de comunicación de envío envía un SMS al dispositivo 3 de comunicación de recepción móvil a través de la red de telefonía móvil. De acuerdo con tecnologías existentes, el mensaje se envía 61 a la pasarela 60 de SMS que a su vez envía el mismo 62 al dispositivo de comunicación de recepción móvil, que almacena el mensaje en un dispositivo de memoria y visualiza una notificación de mensaje recibido en una pantalla, mientras espera una pulsación de tecla antes de visualizar en la pantalla el mensaje almacenado en la memoria.

25 En una posible implementación de una realización de la presente invención, mostrada en la figura del ejemplo, se proporciona un servidor 2 para mensaje móviles privados o servidor PMMP (Plataforma de Mensajes Móviles Privados) además de la pasarela 60 de SMS.

30 En segundo lugar, el terminal 1 móvil de emisión tiene una aplicación que habilita que el usuario del terminal 1 móvil de emisión genere un mensaje a través de la interfaz de terminal móvil (por ejemplo, una pantalla o teclado numérico) para el dispositivo 3 de comunicación de recepción móvil que contiene una porción pública y una porción privada, y que se envía 41 al servidor 2 PMMP. Para enviar el mensaje, puede usarse teléfono móvil o como alternativa protocolos IP bien soportados en redes inalámbricas o no inalámbricas. Si se usa una aplicación especializada, la comunicación puede seguir procedimientos de seguridad similares a los explicados a continuación para el acceso a mensajes mediante el dispositivo móvil de recepción. La PMMP realiza acciones en el mensaje recibido y envía 47 un mensaje SMS público, que sirve como una notificación, al terminal 3 de comunicación móvil de recepción a través de la pasarela 60 de SMS.

35 El SMS público puede contener una instrucción para una aplicación 35 que reside en la memoria volátil del dispositivo móvil de recepción. Dicha instrucción puede añadirse al mensaje mediante el servidor 2 PMMP. Dicha aplicación 35 puede ser similar a la del dispositivo 1 móvil de emisión o puede tener diferentes características. Dicha instrucción provocará, a través de los diferentes mecanismos explicados a continuación, por ejemplo, que el terminal 3 móvil de recepción acceda 43 al servidor 2 PMMP a través de un protocolo de comunicación para visualizar el mensaje almacenado en un dispositivo de memoria de la PMMP en la pantalla, sin almacenar dicho mensaje en el dispositivo de memoria del terminal 3 móvil de recepción.

40 La Figura 2 muestra un diagrama similar en el que el servidor 2 PMMP comprende una pasarela 22 de SMS en lugar de la pasarela de SMS estándar. La figura muestra un dispositivo 1 móvil de emisión enviando un mensaje 12 de telefonía móvil que contiene una porción 121 pública (por ejemplo, una notificación o texto codificado) y una porción 122 privada, cuya privacidad debe preservarse. El mensaje 12 se envía al servidor 2 PMMP. El servidor 2 PMMP tiene un módulo 21 de procesamiento de mensaje que distingue entre la porción 121 pública y la porción 122 privada del mensaje 12. La porción 122 privada se almacena en un dispositivo 24 de memoria del servidor 2 PMMP, mientras que la porción 121 pública se envía al módulo 22 de pasarela de SMS (u otra pasarela de mensajería móvil). Antes de enviarse, el módulo 21 de procesamiento de mensajes puede alterar el contenido de la porción 121 pública, por ejemplo, añadiendo un texto o incluyendo una instrucción para una aplicación que reside en el dispositivo 3 móvil de recepción, si es apropiado. El módulo 22 de pasarela de SMS envía la porción 121 pública a

través de un primer canal 901 determinado, preferentemente un canal de mensajería móvil, por ejemplo, un canal de SMS. El usuario 31 recibe el SMS 121 público en su dispositivo 3 móvil de recepción y se envía una notificación de SMS recibido a la pantalla 34 de visualización. Como ya se ha mencionado, el SMS 121 público puede contener una instrucción o puede actuar como una notificación que puede reconocerse únicamente por el usuario 21 receptor, dándole acceso, desde el terminal 3 móvil de recepción y a través de un segundo canal 902, por ejemplo, un canal de HTTP, a un módulo de gestión para comunicaciones seguras con los dispositivos móviles de recepción, por ejemplo, un módulo 23 de HTTP del servidor 2 PMMP. A través del canal de HTTP y a continuación de una instrucción desde el terminal 3 móvil de recepción, el módulo 23 de HTTP transforma el mensaje 122 privado a un formato que puede visualizarse en la pantalla 34 del terminal 3 móvil de recepción sin la necesidad de almacenamiento previo en su dispositivo de memoria no volátil como un mensaje. Para hacer esto, puede requerirse identificación previa del usuario 21 receptor a través de identificación de cuenta y una contraseña.

La Figura 3 muestra el flujo seguido por los mensajes públicos y las porciones privadas del mensaje.

En particular, el mensaje se envía 41 desde el dispositivo 1 de comunicación de envío al servidor 2 PMMP, que a su vez envía el mismo 43 al dispositivo 3 móvil de recepción.

En contraste, la Figura 4 muestra el flujo para las porciones privadas de los mensajes.

La porción privada se envía desde el dispositivo 1 de comunicación de envío al servidor 2 PMMP, pero es el terminal 3 móvil de recepción el que accede 46 al contenido de la porción privada almacenada en el servidor 2 PMMP.

Para aumentar la privacidad, se recomienda que el dispositivo móvil de recepción solicite que se envíen un usuario y una contraseña o PIN (inicio de sesión). Una petición similar también puede hacerse al dispositivo 1 de envío antes de enviar el mensaje, o la porción privada del mismo.

Se entenderá que el sistema mostrado tiene la ventaja de que la identificación del dispositivo 1 de envío puede ocultarse o alterarse según se ve mediante el dispositivo 3 móvil de recepción en la porción pública del mensaje, produciéndose la correcta identificación en la comunicación de la porción privada.

Adicionalmente, la existencia de un módulo 21 de procesamiento de mensaje de acuerdo con la presente invención, en combinación con el resto del sistema, tiene otras ventajas. Por ejemplo, un receptor 31 que tiene diversos dispositivos de recepción móviles puede seleccionar el dispositivo en el que recibir el mensaje de acuerdo con los atributos de mensaje (por ejemplo, el emisor), que mejora la privacidad. Además, también es posible enviar un único mensaje público para diversos mensajes públicos/privados recibidos en el servidor 2 PMMP una vez que se han cumplido condiciones preestablecidas (por ejemplo, tiempo, hora o número de mensajes recibidos).

Otra ventaja del servidor 2 PMMP en comparación con servidores conocidos de mensajería móvil (por ejemplo, pasarela de SMS) es que habilita que mensajes desde diferentes emisores 1, 1', 1" se almacenen en un dispositivo 24 de memoria que está continuamente disponible para el usuario 21 receptor incluso después de que se hayan leído.

Las Figuras 6 a 10 muestran la arquitectura, estructura física, módulos, relaciones y comunicaciones establecidas en otra realización de la presente invención.

En esta realización, el usuario 21 receptor recibe 43 un mensaje privado o notificación y puede aceptar o rechazar la comunicación simplemente enviando 46 un mensaje de "aceptar" o "rechazar" garantizando la validez de las comunicaciones e identidades del usuario 11 generador y el usuario 21 receptor.

El usuario 11 emisor envía 41 una propuesta o mensaje como se ha descrito anteriormente a través de un dispositivo 1 de comunicación. En respuesta, el servidor 2 PMMP puede enviar 42 una respuesta, por ejemplo, un acuse de recibo de recibo, un acuse de recibo de recepción por el receptor o más preferentemente una petición de validación / identificación (véase la Figura 6).

El servidor 2 PMMP procesa el mensaje enviado desde el dispositivo 1 de envío y envía 43 un SMS público al dispositivo 3 móvil de recepción, que visualiza 431 la notificación en la pantalla 34 de interfaz (véase la Figura 7).

El dispositivo 3 de recepción móvil en el ejemplo mostrado, además, está provisto de un módulo 35' de comunicación que a su vez tiene un compresor 36, un submódulo 37 de comunicación SMS, un submódulo 38 de comunicación HTTP junto con otros submódulos 39 de comunicación que se consideren apropiados y/o necesarios (véase la Figura 8). Además, también pueden existir submódulos especiales para firma 463 digital, autenticación 465 y gestión 464 de configuración.

La función del módulo 35' de comunicación que consiste en gestionar y llevar a cabo la comunicación entre el dispositivo 3 móvil de recepción y el servidor 2 PMMP. El submódulo 36 de compresión reduce el tamaño de la información enviada para bajar el coste y duración de la comunicación tanto como sea posible. El submódulo 38 de HTTP se usa durante la comunicación con el servidor 2 PMMP iniciada por el dispositivo 3 móvil de recepción, excluyendo, por ejemplo, el envío de documentos firmados electrónicamente.

El submódulo 37 de SMS puede usarse si una comunicación HTTP no está disponible. En este caso, el submódulo 37 de SMS empaqueta la comunicación como mensajes SMS para habilitar la realización de los procedimientos de comunicación que deben completarse mediante el sistema, por ejemplo, el flujo de datos mostrado en la Figura 7

(inicio de sesión, etc.).

Una vez que la notificación se ha visualizado en la pantalla 34 de interfaz, el usuario 21 receptor lee 461 el SMS público enviado (visualizado en la pantalla) y puede aceptar 462 o rechazar el mismo, por medio de una acción en la interfaz (presionando una tecla, por ejemplo). En esta realización particular, esto provoca que un mensaje de aceptación se envíe 46, que puede acompañarse mediante una firma 463 para la aceptación. Una vez que la aceptación se ha recibido, el servidor 2 PMMP puede descargar 45 la porción privada del mensaje en un formato que puede leerse mediante la aplicación 35 que reside en el dispositivo móvil. En algunos casos, la porción privada del mensaje puede almacenarse en un dispositivo 33 de memoria del dispositivo 3 móvil de recepción, no automáticamente, pero de una manera controlada por el usuario a través de la aplicación 35 (véase la Figura 7).

En el diagrama de flujo de la Figura 7 también se muestra la posibilidad de que el dispositivo 3 móvil de recepción se descargue 44 una aplicación 32 desde el servidor 2 PMMP. Una vez que la aplicación 372 se descarga, el usuario puede crear preferentemente una cuenta 441, acceder 442 al servidor PMMP voluntariamente a través de dicha aplicación 35 (inicio de sesión) y leer de nuevo 443 mensajes privados almacenados en el servidor PMMP usado.

Para acceder a la aplicación, dicha aplicación solicitará preferentemente en la realización mostrada identificación 451 a través de la pantalla de visualización del dispositivo 3 móvil. Para verificar la identidad, la aplicación se conecta (habitualmente a través de HTTP o HTTPS) al servidor 2 PMMP y efectúa una búsqueda en una base de datos de la PMMP 2. Si el resultado de búsqueda es positivo (inicio de sesión satisfactorio), la aplicación 35 recupera del servidor 2 PMMP la lista de mensajes privados que no se ubican en el dispositivo de memoria del dispositivo 3 móvil de recepción, visualiza 464 la lista en la pantalla y, si es apropiado 462, descarga el mensaje o mensajes en la memoria del dispositivo 3 móvil de recepción.

La aplicación 35 también puede usarse para escribir mensajes 12 que contienen una porción 121 pública y una porción 122 privada. Para hacer esto, la aplicación solicita contenido para las diferentes porciones del mensaje y solicita identificación desde el receptor (por ejemplo, por medio de un nombre de usuario o número de teléfono). La aplicación almacena el mensaje en una base de datos en el dispositivo de memoria, posiblemente cifrando y/o comprimiendo el mensaje, se conecta al servidor (por ejemplo, a través de HTTP o HTTPS) y envía 41 el mensaje, junto con información de inicio de sesión, por ejemplo.

Para el envío, el módulo de datos de la aplicación 35 puede usar medios de conexión alternativos.

Por lo tanto, de acuerdo con el ejemplo mostrado en la Figura 9, después de la instrucción 701 de envío, y compresión, cifrado y/o almacenamiento 702, el dispositivo comprueba 703 si está disponible la comunicación HTTP. Si lo está, envía 704 el mensaje y espera 705 una respuesta desde el servidor 2 PMMP. Si HTTP no está disponible, calcula 708 el número de mensajes SMS necesarios para enviar el mensaje 12, prepara 709 el dispositivo 1, 3 para los envíos múltiples y establece un bucle que se repite siempre que existan todavía datos 713 que enviar, y genera 710, números 711 y envía 712 el SMS (véase la Figura 9).

Una vez que se ha recibido una respuesta 706 desde el servidor 2 PMMP, se visualiza un correspondiente mensaje 707 en la pantalla del dispositivo 1, 3.

Una vez que un mensaje 12 se ha recibido, el servidor 2 PMMP habitualmente:

- verifica la identificación del emisor 1;
- busca al receptor 3 en una base de datos (nombre, número de teléfono, etc.);
- si la búsqueda no es satisfactoria, solicita al emisor 1 confirmación 42 y si recibe dicha confirmación, añade al nuevo receptor a su base de datos;
- si la búsqueda es positiva (el usuario existe), almacena el mensaje en un dispositivo de memoria, modifica las bases de datos de mensajes existentes y envía la porción pública (modificada o no) al receptor por medio de una API apropiada dependiendo de la pasarela (habitualmente una pasarela de SMS).

La porción o porciones públicas, que pueden actuar o no como una notificación de la existencia de una porción confidencial, se reciben mediante el dispositivo de comunicación de recepción móvil, y ejecutando la aplicación de dispositivo, después de pasar los controles de seguridad (identificación, inicio de acceso), el usuario receptor puede acceder a los mensajes.

La Figura 10 muestra un diagrama de flujo que en algunas realizaciones puede considerarse un flujo principal de datos que puede extraerse del diagrama de flujo de datos mostrado en la Figura 7. En la Figura 10, elementos similares o equivalentes a los descritos anteriormente se han indicado con números de referencia idénticos y, por lo tanto, el diagrama en la Figura 10 no se describirá en profundidad.

El diagrama muestra cómo, después de enviar 43 la notificación en la que el submódulo 37 de comunicación SMS participa, se instala la aplicación 32 y/o enciende (si es necesario). Dependiendo 372 de si el usuario está registrado o no, se crea y/o accede 442 una cuenta 441. Recibiendo una petición para leer el mensaje 443, el módulo 35 de comunicación puede visualizar una propuesta 451 que, si es aceptada 462 por el usuario, conduce, usando el procedimiento de gestión de configuración, a un campo 469 que se visualiza para introducir la aceptación, a la propuesta con aceptación que se firma a través del módulo 463 de firma digital, y a la propuesta 46 que se envía, solamente por medio de un ejemplo y como una realización particular.

Un ejemplo de arquitectura diseñada para mantener la seguridad de la porción privada del mensaje se ha ilustrado en la Figura 11.

Los mensajes se procesan mediante diversos submódulos 351, 352, 353, etc. Los módulos son intercambiables (complementos) para ocuparse de diferentes clases y tipos de mensajes. Un mensaje de texto, por lo tanto, procesado adecuadamente por el correspondiente complemento 351 visualizará el texto en la pantalla 34. Esto también se producirá si el mensaje es de un tipo diferente (por ejemplo, una imagen y/o video). Un submódulo 352 de microcódigo contendrá una serie de instrucciones de operación en los recursos del dispositivo 3 de comunicación de recepción (memoria 33 no volátil, pantalla 34, teclado 342 numérico de interfaz, etc.), que en combinación permiten que se realicen operaciones en el mismo. Por lo tanto, es posible visualizar la pantalla, solicitar datos al usuario, modificar campos en un mensaje, borrar o crear un mensaje y solicitar o enviar información adicional al servidor, entre otras aplicaciones. En particular, los submódulos pueden tomar decisiones sobre la gestión de los dispositivos 33 de memoria para evitar el almacenamiento de las porciones privadas de los mensajes, excepto cuando existe una instrucción explícita en contra desde el usuario. Por lo tanto, cuando se accede al dispositivo 3 móvil, se evita que una tercera persona conozca que se almacenan mensajes privados a los que él/ella no puede acceder.

Como se entenderá, a través de la presente invención, se evita que las porciones no públicas sean vistas por terceras personas que tienen acceso al dispositivo de comunicación de recepción móvil sin la necesidad de cifrado de las comunicaciones (aunque esto también puede producirse) y sin la necesidad de almacenar los mensajes privados en la memoria del dispositivo móvil, que alertarían a terceras personas de la existencia de un mensaje privado y/o cifrado.

Aunque la invención se ha descrito con respecto a realizaciones preferidas, estas no deberían considerarse como que limitan la invención, que se definirá mediante la interpretación más amplia de las siguientes reivindicaciones.

REIVINDICACIONES

1. Sistema de comunicación que comprende

- un dispositivo (1) de comunicación de envío,
- un servidor (60, 22) de mensajería móvil, y

5 - un dispositivo (3) de comunicación de recepción, siendo dicho sistema de comunicación del tipo en el que el dispositivo (1) de comunicación de envío envía (61) un mensaje de telefonía móvil a través de una red de comunicación al servidor (60) de mensajería móvil, que a su vez envía el mismo al dispositivo (3) de comunicación de recepción a través de una red de comunicación de telefonía móvil,

estando el servidor (60, 22) provisto de un módulo de comunicación de recepción y envío de dicho mensaje de telefonía móvil,

estando el dispositivo (3) de comunicación de recepción provisto de una memoria (33) electrónica no volátil para el almacenamiento de dicho mensaje de telefonía móvil, una pantalla de interfaz de usuario (34) y un módulo para visualizar dicho mensaje de telefonía móvil almacenado en la pantalla de interfaz (34), en el que el dispositivo (1) de comunicación de envío envía un mensaje (12), que contiene al menos una porción (122) privada, siendo dicho mensaje (12) enviado a un servidor (2) seguro comprendido dentro del sistema, comprendiendo dicho servidor (2) seguro un módulo (21) de procesamiento de mensajes de reconocimiento y gestión de las porciones del mensaje (12) públicas (121) y privadas (122) recibidas, de tal forma que el módulo de comunicación del servidor envía únicamente la porción (121) pública del mensaje (12) a través del servidor (60, 22) de mensajería móvil al dispositivo (3) de comunicación de recepción, dejando la porción (121) privada en el servidor (2) seguro disponible para consulta a través de un canal de comunicación diferente, en el que el dispositivo (3) de comunicación de recepción tiene un módulo (35') de comunicación que habilita que dicho dispositivo (3) acceda a la porción (122) privada del mensaje (12) almacenado en el servidor (2) seguro, teniendo dicho módulo (35') de comunicación submódulos (351, 352, 353) para operar en los recursos del dispositivo (3) de comunicación de recepción, comprendiendo dichos submódulos un submódulo de interfaz para visualizar el mensaje (12) gráficamente en la pantalla (34) y un submódulo de control de la memoria (33) electrónica no volátil del dispositivo (3) de comunicación de recepción, de modo que la porción (122) privada del mensaje no se almacena en la memoria (33) electrónica no volátil del dispositivo (3) de comunicación de recepción y en el que la porción (121) pública del mensaje (12) enviada al dispositivo (3) de comunicación de recepción contiene un desencadenante para que el módulo de comunicación del dispositivo (3) de comunicación de recepción inicie comunicación con el servidor (2) a través del módulo de comunicación del dispositivo (3) de comunicación de recepción móvil, siendo el desencadenante una instrucción para una aplicación que reside en el dispositivo móvil de recepción (3) y provocando que el dispositivo móvil de recepción (3) acceda al servidor, sin la necesidad de que el usuario inicie la comunicación.

2. Sistema de acuerdo con la reivindicación 1, **caracterizado porque** el submódulo de control de memoria borra la información relacionada con la porción (122) privada una vez que el submódulo de interfaz ha visualizado dicha porción (122) privada gráficamente en la pantalla (34).

3. Sistema, de acuerdo con la reivindicación 1 o 2, en el que dicha instrucción se añade mediante el módulo (21) de procesamiento de mensajes.

4. Sistema de acuerdo con una cualquiera de las reivindicaciones 1 a 3, **caracterizado porque** el mensaje (12) enviado mediante el dispositivo de comunicación de envío contiene una porción (121) pública y una porción (122) privada.

5. Sistema de acuerdo con una cualquiera de las reivindicaciones 1 a 4, **caracterizado porque** el servidor (2) seguro envía la porción (121) pública a un servidor (60, 22) de mensajería móvil.

6. Sistema de acuerdo con una cualquiera de las reivindicaciones 1 a 4, **caracterizado porque** el servidor (2) seguro comprende el servidor (60, 22) de mensajería móvil como un módulo integrado.

7. Sistema de acuerdo con una cualquiera de las reivindicaciones 1 a 6, **caracterizado porque** el servidor (2) seguro también comprende un módulo (23) de gestión de comunicaciones seguras con dispositivos móviles de recepción.

8. Sistema de acuerdo con una cualquiera de las reivindicaciones 1 a 7, **caracterizado porque** el dispositivo (1) de envío comprende un módulo de comunicación de comunicación con el servidor (2) seguro.

9. Sistema de acuerdo con la reivindicación 8, **caracterizado porque** el módulo o módulos de comunicación comprenden un submódulo (36) de compresión de datos, un módulo (38) de comunicación IP y un submódulo (37) de comunicaciones de mensajería de telefonía móvil.

10. Sistema de acuerdo con una cualquiera de las reivindicaciones 1 a 9, **caracterizado porque** el dispositivo (3) de comunicación de recepción es un dispositivo de comunicación de recepción móvil.

11. Sistema de acuerdo con una cualquiera de las reivindicaciones 1 a 10, **caracterizado porque** el dispositivo (1) de comunicación de envío es un dispositivo de telefonía móvil.

12. Sistema de acuerdo con una cualquiera de las reivindicaciones 1 a 11, **caracterizado porque** comunicaciones con el servidor (2) seguro relacionadas con mensajes que comprenden porciones (122) privadas están encriptadas.

13. Sistema de acuerdo con una cualquiera de las reivindicaciones 1 a 12, **caracterizado porque** el servidor (2) seguro requiere identificación de usuario y contraseña para recibir o enviar mensajes que comprenden porciones (122) privadas.

5 14. Sistema de acuerdo con una cualquiera de las reivindicaciones 1 a 13, **caracterizado porque** comunicaciones de mensajes privados entre el dispositivo (3) de comunicación de recepción y el servidor (2) seguro son del tipo HTTP.

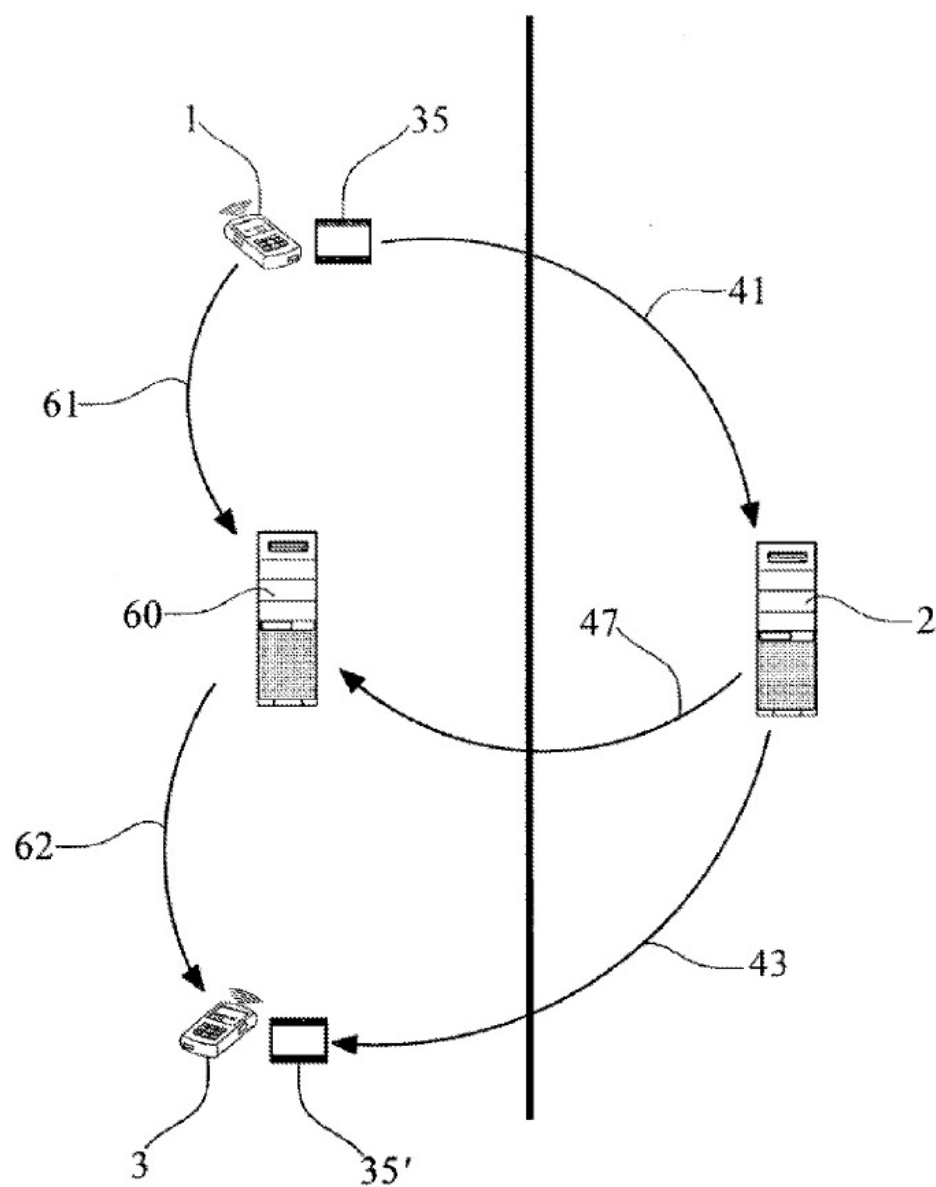


FIG.1

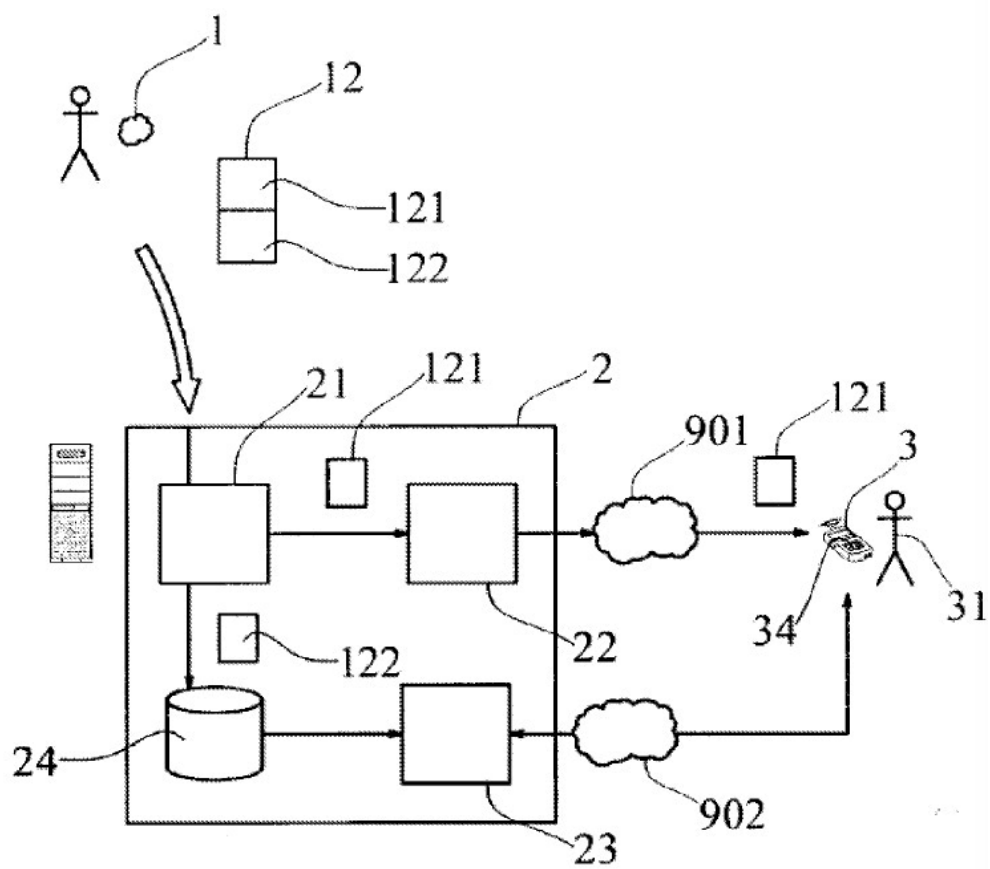


FIG.2

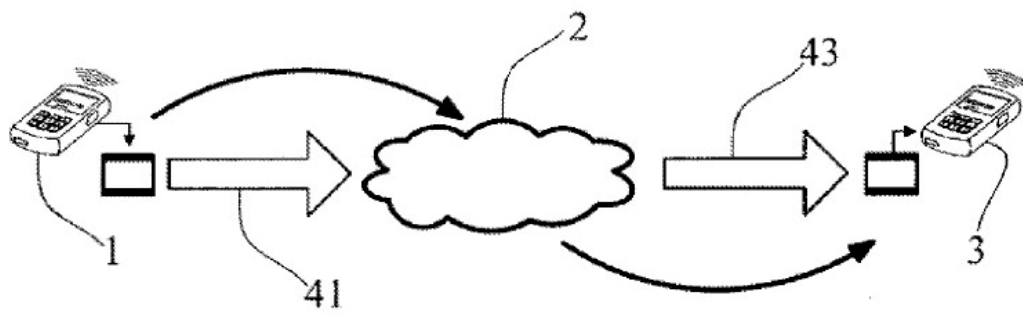


FIG.3

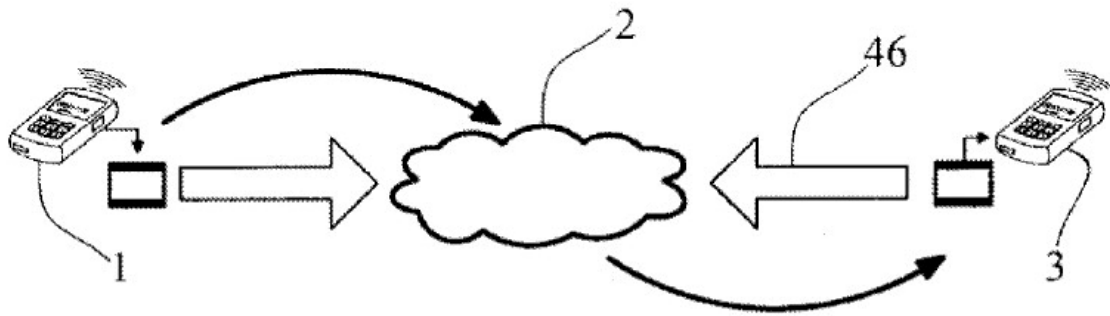


FIG.4

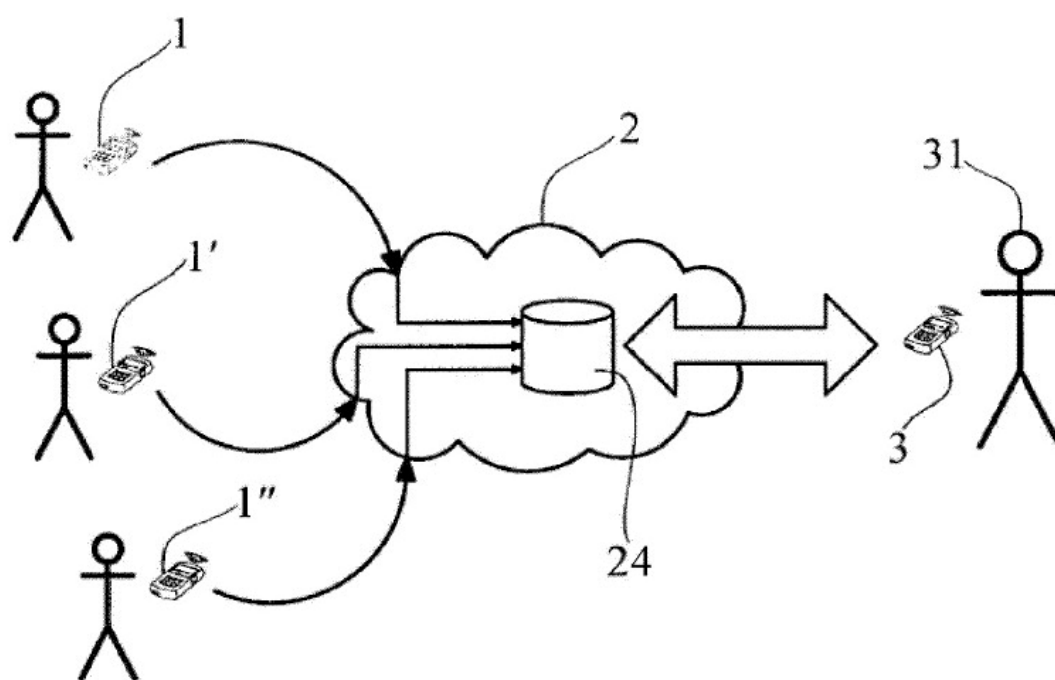


FIG.5

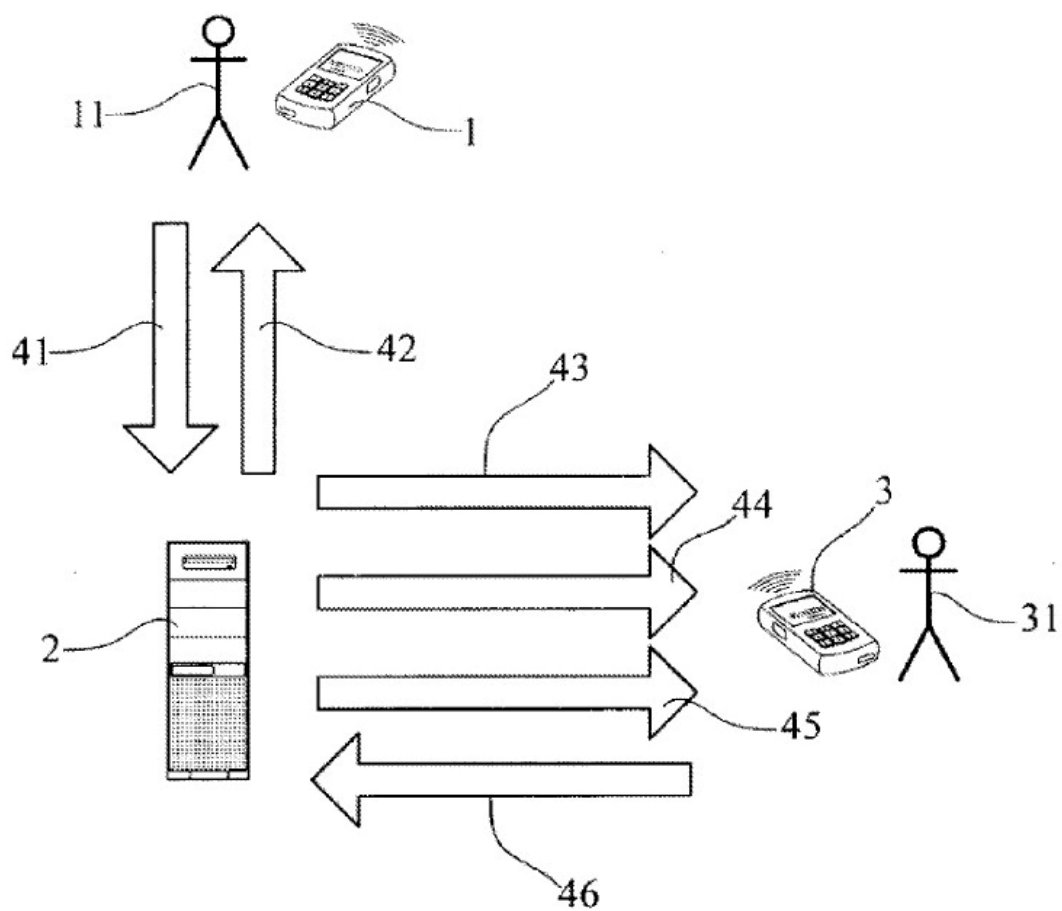


FIG.6

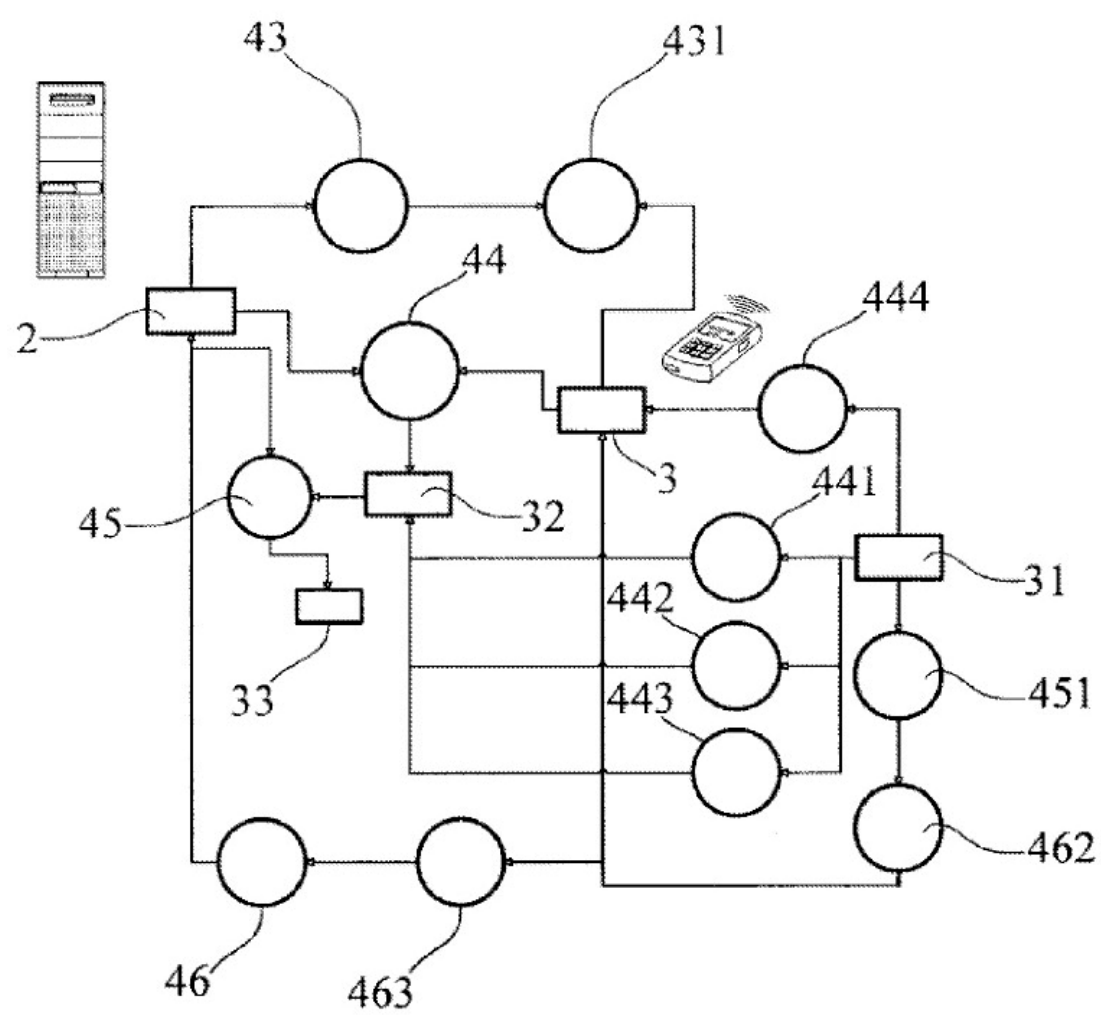


FIG.7

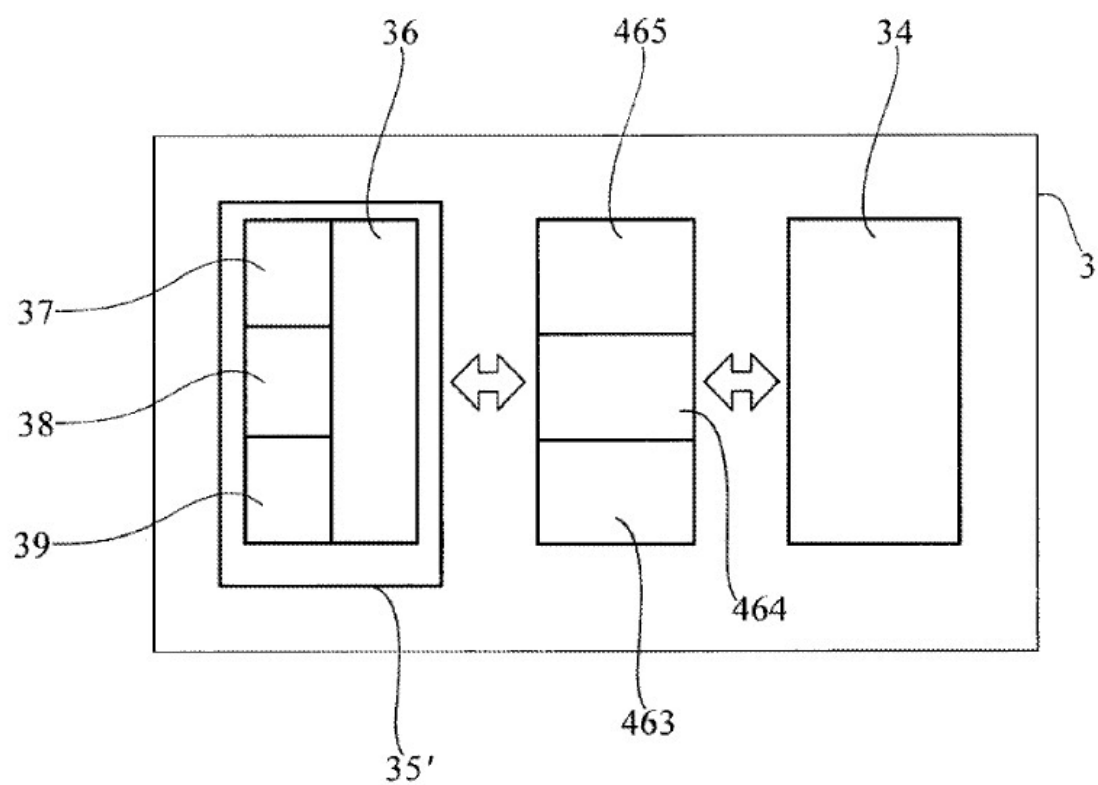


FIG. 8

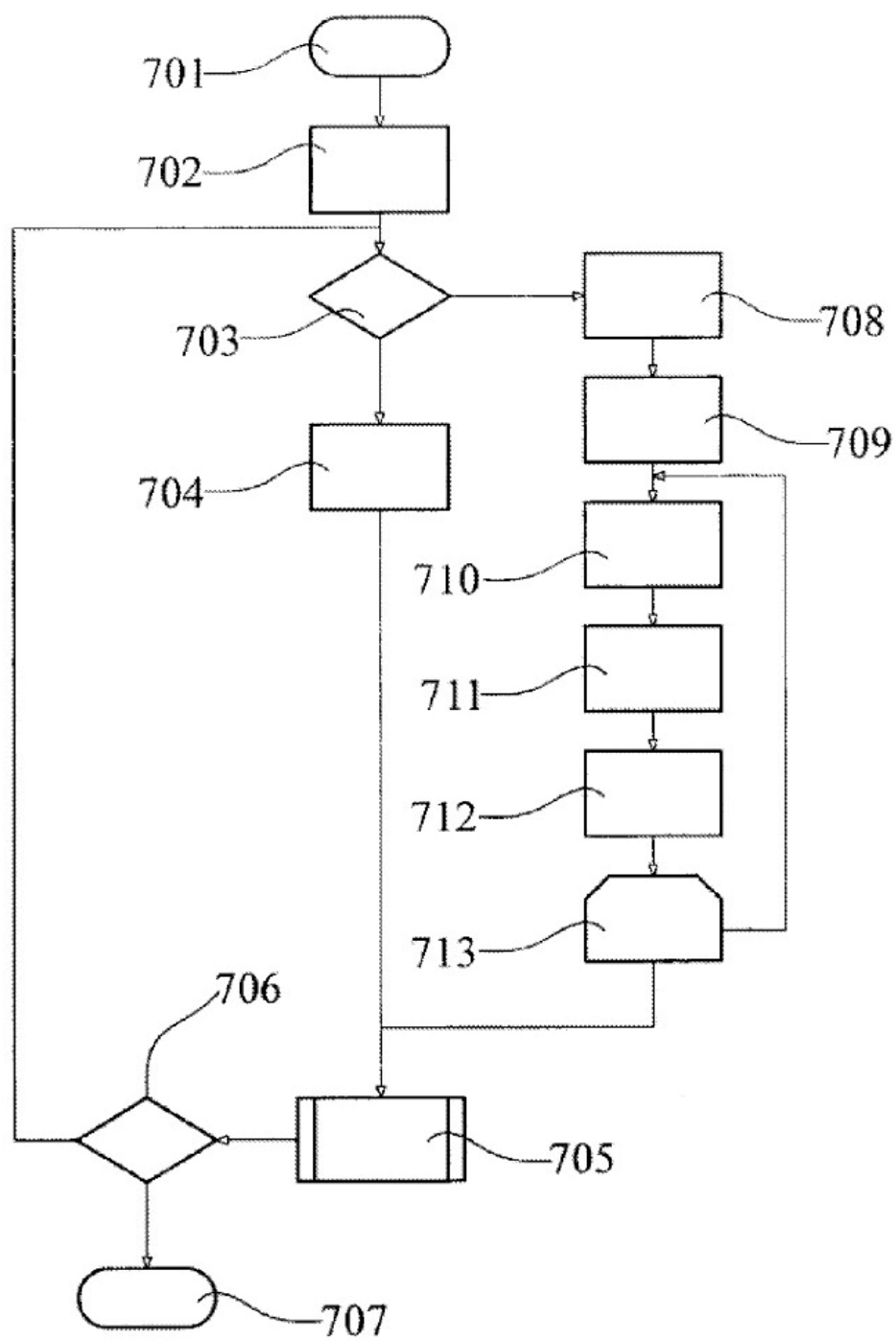


FIG.9

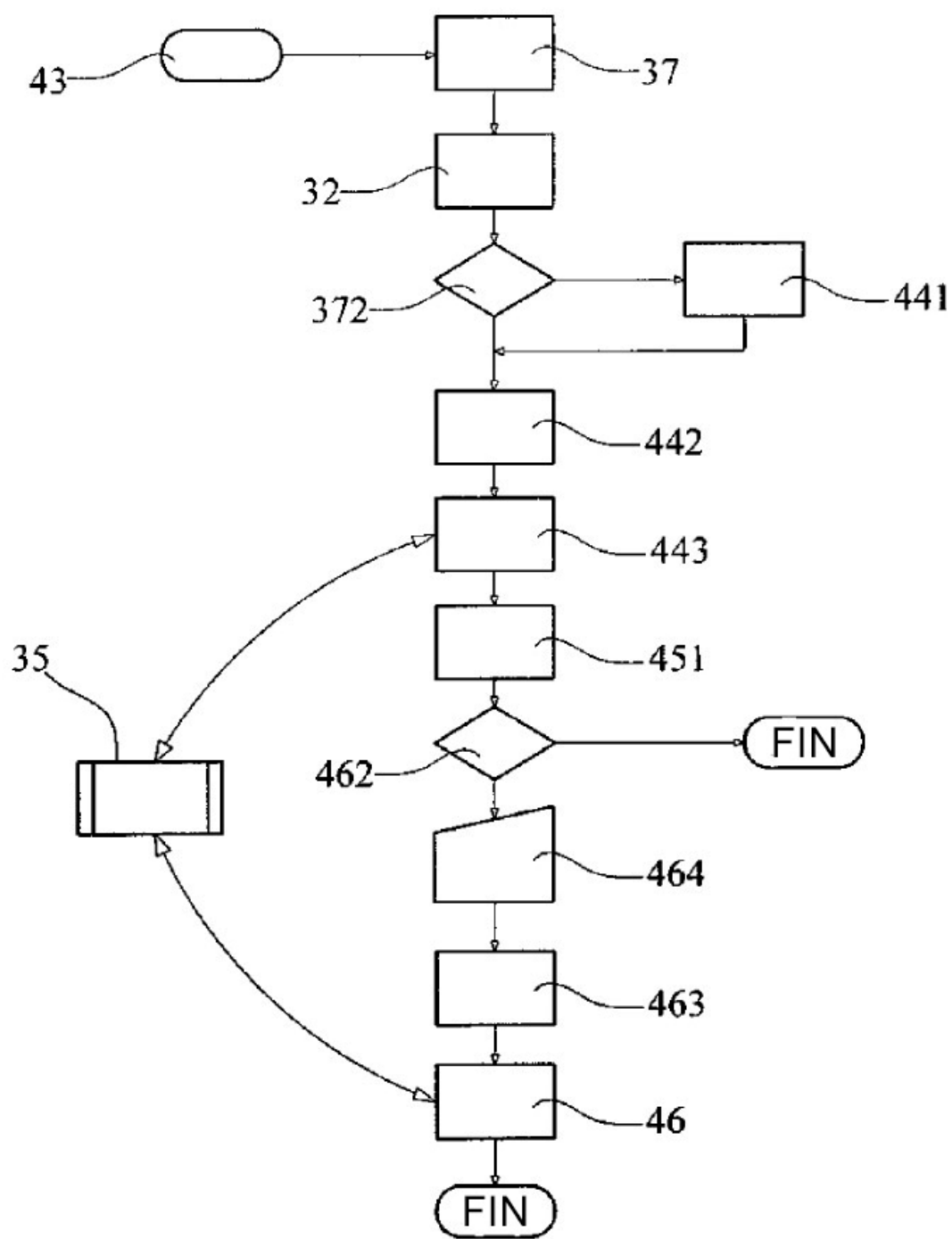


FIG.10

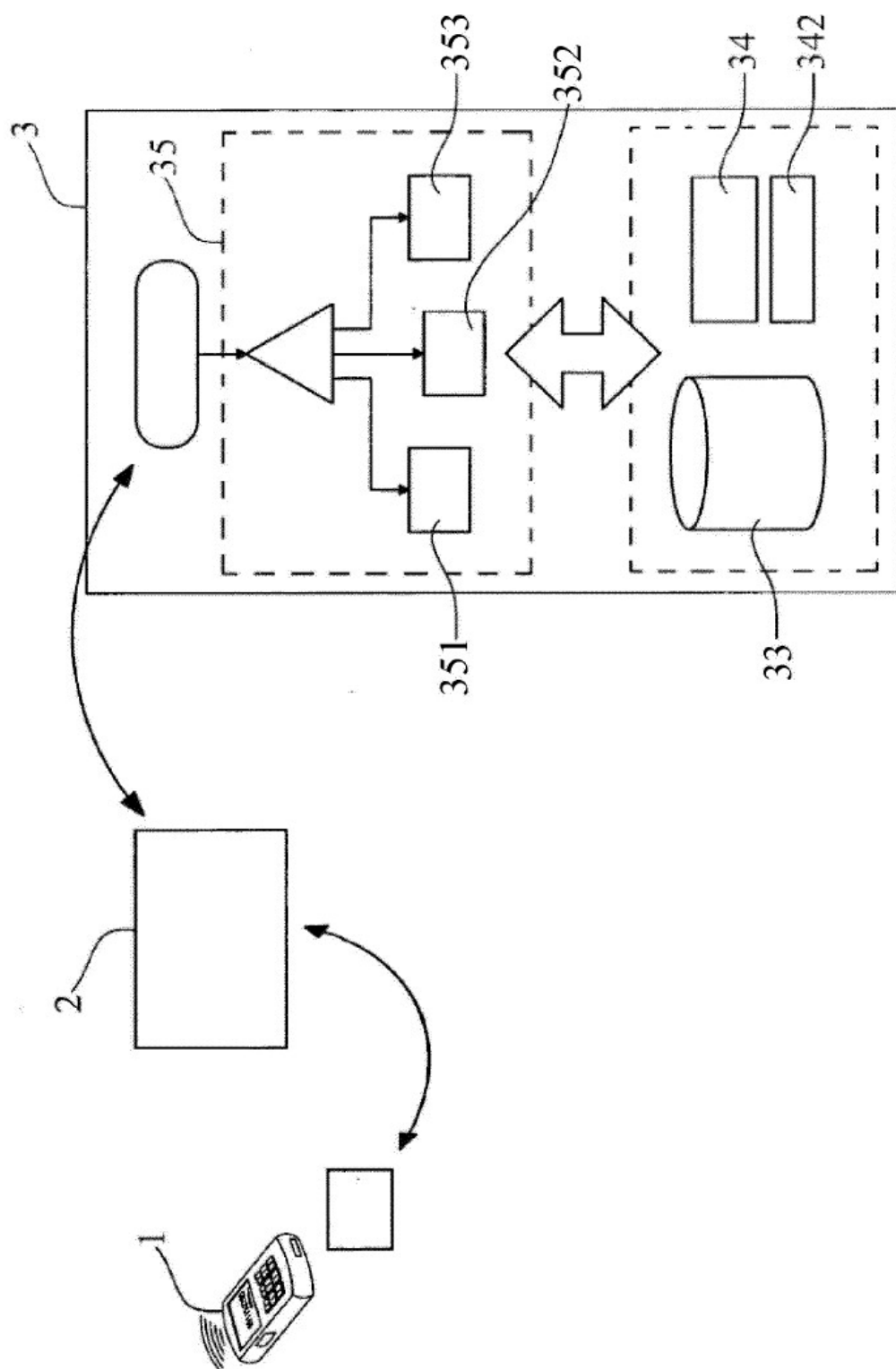


FIG.11