(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 263 344**

(21) Número de solicitud: 200401988

(51) Int. Cl.:
G07F 19/00 (2006.01)
G07F 7/10 (2006.01)

(12) PATENTE DE INVENCIÓN B1

(22) Fecha de presentación: **30.07.2004**

(43) Fecha de publicación de la solicitud: **01.12.2006**

Fecha de la concesión: **11.10.2007**

(45) Fecha de anuncio de la concesión: **16.11.2007**

(45) Fecha de publicación del folleto de la patente: **16.11.2007**

(73) Titular/es: **José Ignacio Bas Bayod**
Francisco Vitoria, 31 - 5º 2º
50008 Zaragoza, ES
Francisco Bas Bayod y
Fernando Bas Bayod

(72) Inventor/es: **Bas Bayod, José Ignacio;**
Bas Bayod, Francisco y
Bas Bayod, Fernando

(74) Agente: **No consta**

(54) Título: **Método para realizar transacciones de pago o cobro seguras, utilizando teléfonos móviles programables.**

(57) Resumen:
Método para realizar transacciones de pago o cobro seguras, utilizando teléfonos móviles programables. La utilización de teléfonos programables -como por ejemplo con tecnología Java-, en los cuáles se carga una aplicación (p. ej. aplicación Java), permite su uso como terminales de transacciones de cobro o pago seguras. La aplicación permite al y comprador/vendedor realizar la transacción, incluyendo la verificación, en una sola conexión. Los datos enviados son encriptados y transmitidos mediante GPRS u otro protocolo de transmisión de datos a un servidor de transacciones, donde las transacciones son verificadas y autorizadas. La seguridad del proceso la confiere principalmente el uso de hasta cinco elementos de identificación no relacionados, incluyendo una clave de acceso única para cada usuario, almacenada en el teléfono móvil.

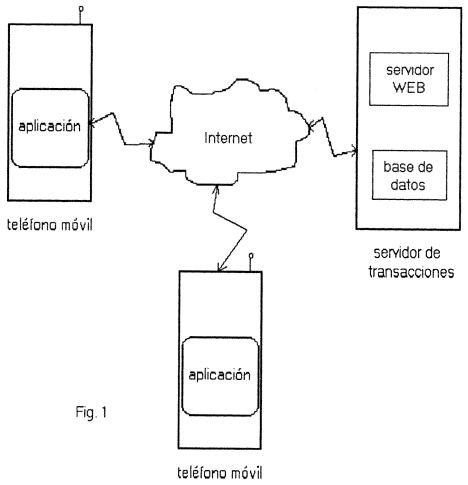


Fig. 1

ES 2 263 344 B1

DESCRIPCIÓN

Método para realizar transacciones de pago o cobro seguras, utilizando teléfonos móviles programables.

Descripción de la invención

Método para realizar transacciones de cobro o pago seguras, utilizando teléfonos móviles programables -como por ejemplo teléfonos móviles con tecnología Java-.

La presente invención se encuadra en el sector técnico de las telecomunicaciones y se refiere a un método válido para terminales basados en teléfonos móviles programables con conexión a Internet, para transacciones de cobro o pago, en el que el uso de hasta 5 elementos de verificación del usuario por el sistema, hacen que dichas transacciones sean seguras. Los 5 elementos utilizados por el sistema para identificar a un usuario pueden ser: 1) los datos de la tarjeta de crédito/débito, o cuenta bancaria de débito; 2) el número del teléfono móvil del usuario 3) el número de identificación personal del usuario (NIP); 4) la información sobre la tarjeta SIM del usuario que el terminal móvil envía como identificador cuando conecta a Internet, actualmente mediante cabeceras HTTP, información que puede ser leída por el servidor de transacciones; y 5) una clave de acceso (CA) que el servidor de aplicaciones asigna al nuevo usuario, siendo ésta almacenada en la memoria del teléfono móvil.

Asimismo, el uso de una aplicación específica cargada en el teléfono permite que la introducción y envío de datos, la autorización de la transacción y la verificación de ésta por el usuario se realicen en la misma conexión y de una manera sencilla, lo que flexibiliza el sistema. La universalidad de la aplicación permite además que el sistema sea usado sin cambios con cualquier teléfono móvil, en cualquier país y utilizando cualquier operador de telefonía móvil con servicio de acceso a Internet. Además, el uso de una aplicación específica y la robustez y seguridad del sistema permiten que el vendedor no requiera disponer de dispositivos lectores de tarjetas, ni otros elementos auxiliares, que no sean su propio teléfono móvil, para realizar sus cobros. Por otro lado, el comprador no requiere disponer de su teléfono móvil al realizar la compra, ya que el terminal del vendedor se puede utilizar para realizar íntegramente la transacción.

El sistema al que se aplica el método está compuesto por un servidor de transacciones y una pluralidad de teléfonos móviles programables, en los que previamente se ha descargado una aplicación al efecto (p. ej. escrita en Java). La aplicación para compras está diseñada para realizar pagos, siendo principalmente usada en transacciones de venta no presencial (por referencia, pagos en comercios virtuales o en máquinas vending). En este caso, en una ejecución preferida de la invención, el usuario inicia la aplicación, introduce la cantidad a pagar, el número de identificación personal (NIP), el número telefónico del vendedor (indicado por la máquina expendedora o el comercio virtual) y en su caso el número de referencia de la compra, y envía dichos datos al servidor de transacciones. Previamente, el servidor de transacciones envía una clave de encriptación de sesión diferente para cada conexión. La aplicación cargada en el teléfono encripta la clave de sesión con la clave de encriptación fija, asignada a cada usuario en el momento del alta, generando pues una clave de sesión modificada, añade a los datos introducidos por el usuario el número propio del teléfono y la clave de acceso (CA), extraídos ambos de la memoria del propio teléfono móvil, y los envía encriptados con la clave de sesión modificada, al servidor de transacciones. El servidor de transacciones recibirá los datos encriptados, encriptará la clave de sesión que previamente generó con la clave de encriptación fija, y con esta clave modificada desencriptará dichos datos. Otra opción sería utilizar el protocolo SSL, en cuyo caso no sería necesaria la generación de claves de encriptación para cada usuario, siendo dicho proceso de encriptación/desencriptación automáticamente realizado por el sistema.

Una vez validada la operación, mediante la comprobación de la identidad del usuario, disponibilidad de crédito y en su caso, de la existencia de una referencia válida asociada a un determinado importe, el usuario recibe un mensaje de aceptación.

La aplicación para ventas está diseñada para realizar cobros. En este caso, es el vendedor quién inicia la aplicación. En una ejecución preferida de la invención, el vendedor introduce la cantidad a cobrar y opcionalmente el número de referencia de la venta (RV), y pide al cliente que introduzca el número de teléfono móvil asignado al sistema de transacciones y su número de identificación personal. El servidor de transacciones enviará entonces la clave de encriptación de sesión. Dicha clave es a su vez encriptada por la aplicación cargada en el teléfono con la clave de encriptación fija, generando pues una clave de sesión modificada. Por último, estos datos, salvo el número de teléfono del comprador, que se envía sin encriptar, además del número telefónico propio del terminal del vendedor y de la clave de acceso (CA), recuperados por la aplicación de la memoria del teléfono, son encriptados con la clave de sesión modificada y enviados al servidor de transacciones. El servidor recuperará la clave de encriptación fija del comprador a partir de su número de teléfono móvil, encriptará la clave de sesión original utilizando dicha clave fija, generando la clave de sesión modificada y desencriptará los datos recibidos utilizando dicha clave modificada. La opción de utilización del protocolo SSL es aquí también aplicable.

Una vez validada la operación por el servidor de transacciones, ambos terminales, el del vendedor y el del comprador reciben, en su caso, sendos mensajes de la aceptación de la operación.

Tanto en la aplicación de compras, como en la de ventas, en una ejecución preferida de la invención, el servidor recibe la información, lee el contenido de las cabeceras HTTP (en dichas cabeceras se identifica cada tarjeta SIM), y desencripta, en su caso, los datos recibidos como se ha explicado (salvo el número del teléfono móvil del comprador, en el caso de una transacción de venta), usando toda esa información para identificar a los usuarios implicados en la transacción y realizar finalmente dicha transacción, o denegarla. La operación, una vez validada, consistirá en un traspaso monetario entre la cuenta asignada al usuario comprador y la cuenta del usuario vendedor, ambas identificadas por las cabeceras HTTP generadas por el terminal móvil para cada tarjeta SIM, o por los números de sus teléfonos móviles o por ambos a la vez. En caso de no utilizar las cabeceras HTTP en la identificación del usuario, los teléfonos móviles propios de los usuarios, tanto en modo compra como en modo venta, serían enviados sin encriptar. Ambas apli-

caciones (de compra y venta), pueden ser incluidas, por economía y uniformidad, en una sola aplicación, configurable por el usuario para operar en un modo u otro.

El alta de un usuario en el sistema, sin ser excluyente de un medio presencial, puede realizarse mediante el acceso del usuario a una página WEB en el servidor de transacciones, en donde se introducen los datos personales y de las tarjetas de crédito/débito u otras cuentas bancarias, y es identificada, mediante una referencia de alta, autentificándose ésta posteriormente, en una ejecución preferida de la invención, mediante el envío por el usuario de un mensaje corto SMS (en caso de utilizar el número de teléfono móvil como identificador) y una conexión HTTP a dicho servidor, los cuales deben incluir dicha referencia de alta en la comunicación. El servidor de transacciones extrae el número del teléfono móvil y las cabeceras HTTP y tras validar todos los datos de las tarjetas o cuentas bancarias, guarda toda esta información en su base de datos, para la posterior identificación del usuario que se da de alta.

Antecedentes de la invención

El pago electrónico es una modalidad que ha ido popularizándose a lo largo del tiempo. Existen multitud de sistemas conocidos que permiten realizar dicha modalidad de pago. En principio, estos sistemas se basaban completamente en las comunicaciones telefónicas tradicionales por cable y en lectores de tarjetas de banda magnética situados en los comercios. Pero con el advenimiento de Internet y de la telefonía móvil, nuevos métodos de pago a distancia han ido apareciendo. En concreto, es conocido un sistema de pago mediante teléfonos móviles, el cuál está basado en la asociación de un número de tarjeta de crédito/débito con un PIN y un número de teléfono móvil en el servidor de transacciones. El procedimiento seguido por este sistema es, básicamente, la autorización de la operación por el usuario, una vez recibidos los datos de la transacción en su teléfono móvil. La transacción no es realizada en tanto en cuanto el usuario no la confirme mediante su terminal, introduciendo su PIN secreto. La comunicación con el usuario, para autorizar dicha transacción, se realiza mediante una llamada de datos desde el servidor de transacciones, el cuál pasa a controlar la introducción de datos desde el teclado y la representación de información en la pantalla del teléfono. En compra presencial, un TPV es requerido y éste requiere estar preparado para pago con ese sistema, puesto que debe iniciar la transacción mediante una llamada especial a un número telefónico, gestionado por el servidor de transacciones.

Este sistema adolece de rigidez, debido a que la comunicación con el usuario se realiza a través de una llamada de datos, lo que dificulta que el sistema sea transnacional, debiendo tener servidores de transacciones en cada país. Por otro lado, debido a que el sistema requiere tomar el control del terminal móvil, y dicho control depende de las distintas marcas y modelos de teléfonos móviles, no estando dicho control estandarizado, se requiere disponer de módulos distintos para cada modelo existente, e incluir los de los nuevos modelos, lo que le resta universalidad. Además al usuario se le fuerza a aprender nuevas operatorias cuando usa distintos modelos. Una conexión a través del protocolo WAP, la cual permite lograr una mayor estandarización, encarecería notablemente el proceso para el usuario, debido a la gran cantidad de datos requeridos en las conexiones de dicho tipo. De otro lado, la utilización del limitado teclado del terminal móvil para la introducción de datos alfanuméricos requeridos en las transacciones, en una conexión WAP, haría lento el proceso de aquéllas, en caso de utilizarse el terminal móvil como terminal de compra/venta. Por último, la propia concepción actual del sistema requiere la presencia y uso de terminales TPV en los comercios.

Explicación de la invención

Para mejorar los sistemas antes mencionados, se ha desarrollado un nuevo método de cobro/pago mediante teléfono móvil, con las siguientes características:

1) Los terminales de compra/venta son los propios teléfonos móviles de los usuarios del sistema. Los teléfonos son programables y deben ser cargados con una aplicación específica (p. ej. escrita en Java), descargada por el usuario de un servidor de aplicaciones, o desde otro medio de almacenamiento, como por ejemplo un ordenador equipado con lectores de disco, o bien pre-cargada por el fabricante del teléfono.

2) Seguridad. La seguridad del sistema se consigue mediante la verificación del usuario, pudiendo usar hasta 5 elementos significativos (ES) de información no relacionada, o de difícil relación, como son a) los datos personales y de las tarjetas de crédito/débito, u otras cuentas financieras, b) el número de identificación personal (NIP), c) el número del teléfono móvil, d) las cabeceras HTTP de información de las tarjetas SIM, enviadas por los terminales móviles y e) una clave de acceso (CA), asignada a cada usuario por el servidor de transacciones y almacenada en la memoria del teléfono móvil al realizar la descarga de la aplicación, o en una configuración posterior.

3) Flexibilidad. La flexibilidad del sistema se debe a que todos los datos a introducir en una transacción pueden ser numéricos, lo que permite una cómoda introducción de éstos mediante el teclado del teléfono móvil.

4) Universalidad. Debida a la utilización de una aplicación específica en el teléfono móvil, lo que permite al teléfono ser usado como terminal de compra/venta en cualquier país y utilizando cualquier operador de telefonía móvil.

5) Coste. El coste de las transacciones para el usuario o para el gestor del servidor de transacciones es mínimo, debido una vez más a que la aplicación cargada en el teléfono permite un flujo óptimo de datos entre el terminal y el servidor de transacciones.

El alcance v contenido de la presente invención se mostrará con más claridad mediante dibujos, que muestran una ejecución preferida de la misma, donde:

La fig. 1 muestra una ejecución preferida de la patente para realizar transacciones tanto de compra como de venta.

La fig. 2 muestra una ejecución preferida del proceso de alta de un usuario en el sistema.

La fig. 3 muestra una ejecución preferida del proceso de descarga de la aplicación en el terminal móvil

La fig. 4 muestra una ejecución preferida del proceso de configuración del terminal móvil

La fig. 5 muestra una ejecución preferida de una transacción de compra

La fig. 6 muestra una ejecución preferida de una transacción de venta

En la fig. 1 se pueden ver varios terminales de compra/venta, cargados con la aplicación Java, lo que les permite transmitir los datos de identificación del usuario al servidor de transacciones, para que éste verifique y valide las transacciones. Asimismo, la aplicación les permite recibir y visualizar los resultados de las últimas transacciones realizadas.

Para que el sistema pueda ser usado, se requiere que el usuario se dé de alta en el sistema. En la fig. 2 se puede ver cómo el usuario comienza el proceso de alta en el servidor de transacciones. Esta alta. según se ve en esta ejecución preferida, puede ser realizada en una página WEB diseñada al efecto, y consiste en la introducción de sus datos personales y los datos de las tarjetas de crédito/débito o cuentas financieras. El sistema genera una referencia de alta. Posteriormente, el usuario envía al servidor de transacciones un SMS (mensaje corto) conteniendo dicha referencia de alta. El servidor lee el SMS y extrae el número de teléfono móvil y la referencia de alta, adjuntando dicho número telefónico a los datos del usuario ya introducidos, e identificados por dicha referencia. El hecho de utilizar el número de teléfono móvil podría potenciar la seguridad en el futuro, además de simplificar su memorización. Finalmente, el usuario, utilizando un teléfono móvil con la misma tarjeta SIM con la que ha enviado el SMS anterior, en su caso, realiza una conexión HTTP a una página WEB del servidor, y envía asimismo la anterior referencia de alta. El servidor de transacciones lee la referencia de alta y la cabecera HTTP relativa a la identificación de la tarjeta SIM del usuario. Finalmente almacena dicha cabecera junto con los datos de usuario ya introducidos, identificados por la referencia de alta previamente enviada mediante el SMS (mensaje corto). En este mismo proceso, el servidor genera una clave de encriptación fija, asociada a cada usuario, la almacena en la base de datos, en el registro asociado al usuario, y la muestra a éste mediante la página WEB de altas, página que será descargada en el sistema informático del usuario utilizando un protocolo seguro. El usuario deberá copiar dicha clave de encriptación en su teléfono móvil a la hora de configurar el terminal, utilizando el teclado de éste. Esta clave de encriptación podría ser también cargada automáticamente en el teléfono en el proceso de configuración, utilizando un protocolo seguro, como SSL. Finalmente, el servidor de transacciones generará una clave de acceso (CA) distinta para cada usuario y la almacenará asimismo en la base de datos. Una vez realizado este proceso, el usuario puede descargar la aplicación en su terminal, según se ve en la fig. 3, sin más que acceder a una página WEB del servidor e iniciar la descarga. El servidor de transacciones leerá el número de teléfono móvil y la clave de acceso (CA) asociados al usuario, encriptará ambos datos con la clave de encriptación fija y añadirá ambos datos al fichero a descargar, junto con la propia aplicación. Finalmente, el fichero será descargado en el teléfono móvil. Los datos adjuntados a la aplicación son almacenados en la memoria del teléfono móvil para su posterior uso. Esos datos serán posteriormente desencriptados y almacenados por la aplicación, cuando el usuario configure y almacene la clave de encriptación fija en el terminal. La carga del número de teléfono móvil y de la clave alfanumérica (CA) podría también realizarse de forma manual, utilizando el teclado del propio teléfono móvil, o de forma remota, mediante conexión segura posterior a Internet (por ejemplo utilizando el protocolo SSL), o usando cualquier otro tipo de comunicación electrónica, en el proceso de configuración.

Una vez ha sido instalada la aplicación, el usuario puede iniciarla y acceder a un menú en el que hay varias opciones. Entre ellas están las siguientes: (1) configuración, (2) compra, (3) venta, (4) verificación de transacciones. Inicialmente, sólo la opción de configuración está habilitada. En la figura 4 se puede ver como la aplicación permite configurar el terminal bien en modo COMPRA o bien en modo VENTA. Una vez el terminal ha sido configurado, las opciones de COMPRA (2) o VENTA (3), y la opción de verificación de transacciones (4) se habilitarán, y el terminal quedará listo para realizar transacciones.

Para iniciar una transacción de compra, el usuario deberá iniciar la aplicación y seleccionar la opción de COMPRA (2) en el menú. Según se ve en la fig. 5, al acceder a la opción de compra, la aplicación muestra 3 campos vacíos en los que el usuario debe introducir la cantidad a pagar, el número de identificación personal y el número de teléfono móvil del vendedor. La aplicación interrogará entonces al usuario sobre la necesidad de utilización de referencia de compra (RC) en la transacción. Si la respuesta es afirmativa, aparecerá un cuarto campo vacío, donde el usuario introducirá dicha referencia de compra (RC), asignada por el vendedor. Tras la conexión, el servidor de transacciones enviará al terminal una clave de encriptación de sesión. Dicha clave será encriptada por la aplicación mediante la clave de encriptación fija, almacenada en la memoria del terminal, obteniéndose pues una clave de sesión modificada. Una vez introducidos, dichos datos, junto con la clave de acceso (CA) y el número del propio teléfono móvil, recuperados de la memoria del terminal, son encriptados por la aplicación con la clave de sesión modificada, y enviados mediante GPRS, UMTS u otro protocolo celular de transmisión de datos, al servidor de transacciones, a través de Internet. En la figura 5 se puede ver cómo el servidor recibe dichos datos encriptados, así como, en su caso, las cabeceras HTTP de identificación de la tarjeta SIM. El servidor de transacciones accede a la base de datos asociada, donde realiza la búsqueda del registro identificado por la cabecera HTTP correspondiente, o por el número del teléfono móvil propio del usuario, en su caso, que se enviaría sin encriptar. Si no existiera dicho registro, la transacción se dará por finalizada, enviándose un mensaje al usuario en este sentido, usando la conexión todavía abierta. Si el registro existe, se encriptará la clave de sesión original con la clave de encriptación fija, obteniéndose la clave de sesión modificada. La información recibida es desencriptada usando dicha clave de encriptación de sesión modificada, y se comparará el número de identificación personal enviado con el existente en la base de datos. Si no coinciden, la transacción se dará por finalizada, enviándose asimismo un mensaje de aviso al usuario mediante la conexión establecida. Si coinciden, se compararán el número de teléfono móvil y la clave de acceso (CA) enviados con los existentes en la base de datos. Si alguna comparación es fallida, la transacción finaliza, enviándose el mensaje de aviso correspondiente al usuario. Si todos los datos coinciden, la transacción será considerada correcta. En este caso se procederá a realizar una transferencia de fondos entre la cuenta asociada al usuario referido en el registro identificado y la cuenta pertenecien-

te al usuario referido mediante el número de teléfono móvil del vendedor, introducido previamente por el comprador y enviado por el terminal móvil, y correspondiente a la compra referenciada en el campo opcional de referencia de compra (RC) que fue enviada previamente desde el terminal, o cuantificada por el campo de cantidad de la transacción, enviado asimismo desde el terminal. Una vez realizada la transferencia, la transacción se dará por finalizada, y un mensaje de confirmación será enviado al usuario, utilizando la misma conexión, todavía abierta, y encriptado usando la clave de sesión modificada. En este mensaje se mostrarán los datos más relevantes de la transacción. El servidor de transacciones guardará un histórico de todas las transacciones realizadas por el sistema, ya sean correctas o erróneas. El protocolo SSL podría ser utilizado en este caso de manera equivalente.

En la fig. 6 se muestra el proceso seguido en una transacción de venta. En este caso. el vendedor debe iniciar la aplicación y seleccionar en el menú la opción de VENTA (3). Al hacer esto, obtiene una pantalla con cuatro campos, relativos a la cantidad de la transacción, la referencia de venta (RV), el número de teléfono móvil del comprador y el número de identificación personal de éste. Los dos primeros deben ser rellenados por el vendedor, aunque el campo de referencia de venta (RV) es opcional. Una vez introducidos dichos datos, el vendedor pide al comprador que introduzca su número de teléfono móvil y su número de identificación personal, lo que concluirá la introducción de datos. La aplicación finalmente recuperará el número propio del teléfono móvil del vendedor y la clave de acceso (CA), de la memoria del terminal. La aplicación conecta entonces con el servidor de transacciones mediante una conexión GPRS, UMTS u otro protocolo de transmisión de datos. Tras la conexión, dicho servidor de transacciones envía la clave de encriptación de sesión. La aplicación encripta la clave de sesión mediante la clave de encriptación fija, almacenada en la memoria del terminal, generando una clave de sesión modificada, encripta los anteriores datos utilizando dicha clave modificada y los envía al servidor. Todos los datos son encriptados, excepto el número de teléfono móvil del comprador (y el teléfono móvil del vendedor, en su caso), que se envía sin encriptar. El servidor de transacciones recibe pues ciertos datos del vendedor y del comprador encriptados, el número de teléfono móvil del comprador, así como las cabeceras HTTP de identificación de la tarjeta SIM. Al igual que en la transacción de compra, el servidor de transacciones comprueba si tanto el registro referenciado por la cabecera HTTP correspondiente (o por el número propio del teléfono móvil del vendedor, en su caso), como el referenciado por el número de teléfono móvil del comprador existen. Si alguno de esos registros es inexistente, la transacción finaliza, enviándose un mensaje de error al terminal del vendedor, mediante la conexión todavía abierta. Si los dos registros existen, se encripta la clave de sesión con la clave de encriptación fija, asignada a cada usuario (en este caso al vendedor), obteniéndose la clave de sesión modificada, la cuál se utiliza para desencriptar los datos de la transacción. Si el número de identificación personal del comprador así desencriptado no coincide con el NIP que está asociado al registro de comprador mediante el número de teléfono móvil recibido en la conexión, la transacción finaliza, y un mensaje de error es enviado al terminal del vendedor. Si ambos NIP coinciden, se leerá (en su caso) el número del teléfono móvil del vendedor asociado a la cabecera HTTP de identificación y la clave de acceso (CA). Si dichos datos coinciden con los recientemente desencriptados, pertenecientes al vendedor, la transacción se considera correcta y se realiza la transferencia de fondos entre la cuenta del comprador. referenciada por su número de teléfono móvil, y la cuenta del vendedor, referenciada por la cabecera HTTP correspondiente (o por su número de teléfono móvil). El servidor de transacciones guarda un histórico de todas las transacciones realizadas, ya sean válidas o erróneas, incluyendo la referencia de venta (RV), adjuntada si ésta ha sido introducida por el vendedor en el terminal. Un mensaje de confirmación será enviado al terminal del vendedor, utilizando la conexión todavía abierta, siendo encriptado previamente mediante la clave de sesión modificada. Si el comprador quiere saber el resultado de la transacción, deberá usar la opción (4) de su menú de transacciones. Una vez iniciada la aplicación. debe introducir su número de identificación personal (NIP) y hacer la petición al servidor de transacciones. La aplicación enviará en su caso, el número propio del teléfono móvil del comprador. El servidor de transacciones recibirá la cabecera HTTP de identificación de tarjeta SIM, o en su caso, el número de teléfono móvil del comprador, leerá el registro asociado al usuario en la base de datos, generará y enviará al terminal la clave de encriptación de sesión, encriptará dicha clave con la clave de encriptación fija asociada al comprador (obteniendo la clave de sesión modificada) y enviará el mensaje de confirmación encriptado con dicha clave de sesión modificada. El servidor encriptará y enviará también el NIP correspondiente al usuario. La aplicación encriptará la clave de sesión con la clave de encriptación fija, almacenada en la memoria del terminal, obteniendo la clave de sesión modificada, desenciptará el mensaje de confirmación, desencriptará el NIP enviado, lo comparará con el NIP introducido y si ambos coinciden, mostrará el mensaje de confirmación en la pantalla del terminal. En este caso la opción de usar el protocolo seguro SSL podría utilizarse de manera equivalente.

Si se desea dotar al sistema de mayor seguridad, al producirse tres conexiones erróneas conteniendo una misma cabecera HTTP de identificación (o un mismo número de teléfono móvil, en su caso), el registro de usuario asociado a dicha cabecera HTTP podría ser bloqueado.

Naturalmente, la invención no se limita a las realizaciones antes descritas y mostradas en las figuras, sino que se puede modificar dentro del alcance de las reivindicaciones anexas.

REIVINDICACIONES

1. Método para realizar transacciones de compra/venta utilizando teléfonos móviles programables (p. ej. con tecnología Java), que convierte un teléfono móvil programable (p. ej. con tecnología Java) en un terminal de compra/venta, y que comprende los pasos de:

a) Dar de alta al usuario, almacenando hasta 5 elementos significativos (ES), en la base de datos del servidor de transacciones, que conforman la información principal del usuario. En este proceso de alta, se generará también una clave de encriptación, diferente para cada usuario. Este paso se realiza una única vez por cada usuario y puede realizarse de forma presencial o no presencial, a través de Internet. Los datos quedan almacenados en la base de datos del servidor de transacciones.

b) Descargar la aplicación específica (p. ej. escrita en Java) para convertir el teléfono móvil del usuario en un terminal de compra/venta, mediante un servidor WEB alojado o conectado con el servidor de transacciones, aplicándose una vez para cada usuario.

c) Encriptar y descargar en el terminal móvil el número propio del teléfono móvil del usuario y la clave de acceso (CA) única para cada usuario, generada por el servidor de transacciones, para que puedan ser utilizados por la aplicación en cada transacción realizada. Este paso es realizado una única vez por el servidor de transacciones.

d) Introducir en el terminal la clave de encriptación fija, única para cada usuario. Este paso será realizado por el usuario del sistema, utilizando los medios suministrados por el mencionado teléfono móvil programable, controlados por la aplicación (escrita en Java, por ejemplo) residente en éste, siendo dicho paso realizado sólo una vez.

e) Desencriptar y almacenar en la memoria del teléfono móvil, el número propio del teléfono móvil y la clave de acceso (CA) previamente descargadas. Este paso será realizado automáticamente por la aplicación cargada en el teléfono móvil, y será realizado sólo una vez.

f) Iniciar la aplicación en el teléfono móvil. Este paso será realizado por el usuario, utilizando los medios suministrados por el teléfono móvil programable, controlados por la aplicación residente en éste, cada vez que dicho usuario quiera efectuar una transacción.

g) En el caso de que el terminal, controlado por la aplicación, opere en modo de compra, introducir el número de teléfono del vendedor, el número personal de identificación (NIP). la cantidad a pagar, y la referencia de compra (RC), si existe, en los campos correspondientes generados por dicha aplicación. Este paso será realizado por el usuario, utilizando los medios suministrados por el teléfono móvil programable, controlados por la aplicación residente en éste, cada vez que dicho usuario quiera efectuar una transacción de compra.

h) En el caso de que el terminal, controlado por la aplicación, opere en modo de venta, introducir la cantidad a cobrar, en su caso la referencia de venta (RV), el número de teléfono móvil del comprador y el número de identificación personal (NIP) de éste, en los correspondientes campos. Este paso será realizado por los usuarios -comprador y vendedor-, utilizando los medios suministrados por el teléfono móvil programable, controlados por la aplicación residente en éste, cada vez que dichos usuarios quieran efectuar una transacción.

i) Recuperar el número de teléfono móvil y la clave de acceso (CA) de la memoria del teléfono móvil que inicia la operación de compra o venta. Este paso será realizado automáticamente por la aplicación (escrita en Java, por ejemplo) sobre el teléfono móvil.

j) Encriptar dichos datos, salvo los necesarios para la identificación de los usuarios implicados en la transacción, por parte del servidor de transacciones. Este paso será realizado automáticamente por la mencionada aplicación (escrita en Java, por ejemplo) sobre el teléfono móvil.

k) Conectar con el servidor de transacciones. Este paso será realizado automáticamente por la mencionada aplicación (escrita en Java, por ejemplo) entre el teléfono móvil y el servidor de transacciones.

l) Enviar los datos recolectados al servidor de transacciones. Este paso será realizado automáticamente por la aplicación (escrita en Java, por ejemplo) entre el teléfono móvil y el servidor de transacciones, mediante una conexión GPRS, UMTS, u otro protocolo de conexión a Internet.

m) Recibir los datos recolectados, más la cabecera de identificación de la tarjeta SIM del terminal del usuario conectado, en su caso, en el servidor de transacciones. Este paso será realizado automáticamente por el servidor de transacciones.

n) Utilizar la cabecera de identificación de SIM, o el número del teléfono móvil de el/los usuarios, para localizar los registros correspondientes a los usuarios implicados en la transacción. Este paso será realizado automáticamente por el servidor de transacciones.

o) Desencriptar y procesar el resto de los datos para comprobar la correcta identidad de los usuarios, contra tos datos almacenados en la base de datos. Este paso será realizado automáticamente por el servidor de transacciones.

p) Validar y realizar, en su caso, la transacción entre comprador y vendedor. Este paso será realizado automáticamente por el servidor de transacciones.

q) Encriptar y enviar un mensaje de confirmación al terminal móvil del usuario que está conectado. Este paso será realizado automáticamente por el servidor de transacciones entre dicho servidor de transacciones y el terminal móvil del usuario conectado a aquél, mediante una conexión GPRS, UMTS, u otro protocolo de conexión a Internet.

r) Almacenar la transacción en un histórico. Este paso será realizado automáticamente por el servidor de transacciones.

s) Encriptar y enviar al terminal del usuario que no ha iniciado la transacción, y a petición de éste, un informe de la última transacción efectuada. Este paso será realizado automáticamente por el servidor de transacciones entre dicho servidor de transacciones y el terminal de usuario conectado a aquél, mediante una conexión GPRS, UMTS, u otro protocolo de conexión a Internet.

2. Método de acuerdo con la reivindicación 2, **caracterizado** porque el paso b) también puede realizarse mediante la descarga de la aplicación desde cualquier dispositivo de almacenamiento de datos, una vez el usuario se ha dado de alta, o ser realizado por el propio fabricante del teléfono móvil.

3. Método de acuerdo con la reivindicación 2, **caracterizado** porque el paso d) también puede realizarse de manera automática, mediante la comunicación segura de la clave de encriptación fija al teléfono móvil, por el servidor de transacciones, en el proceso de configuración.

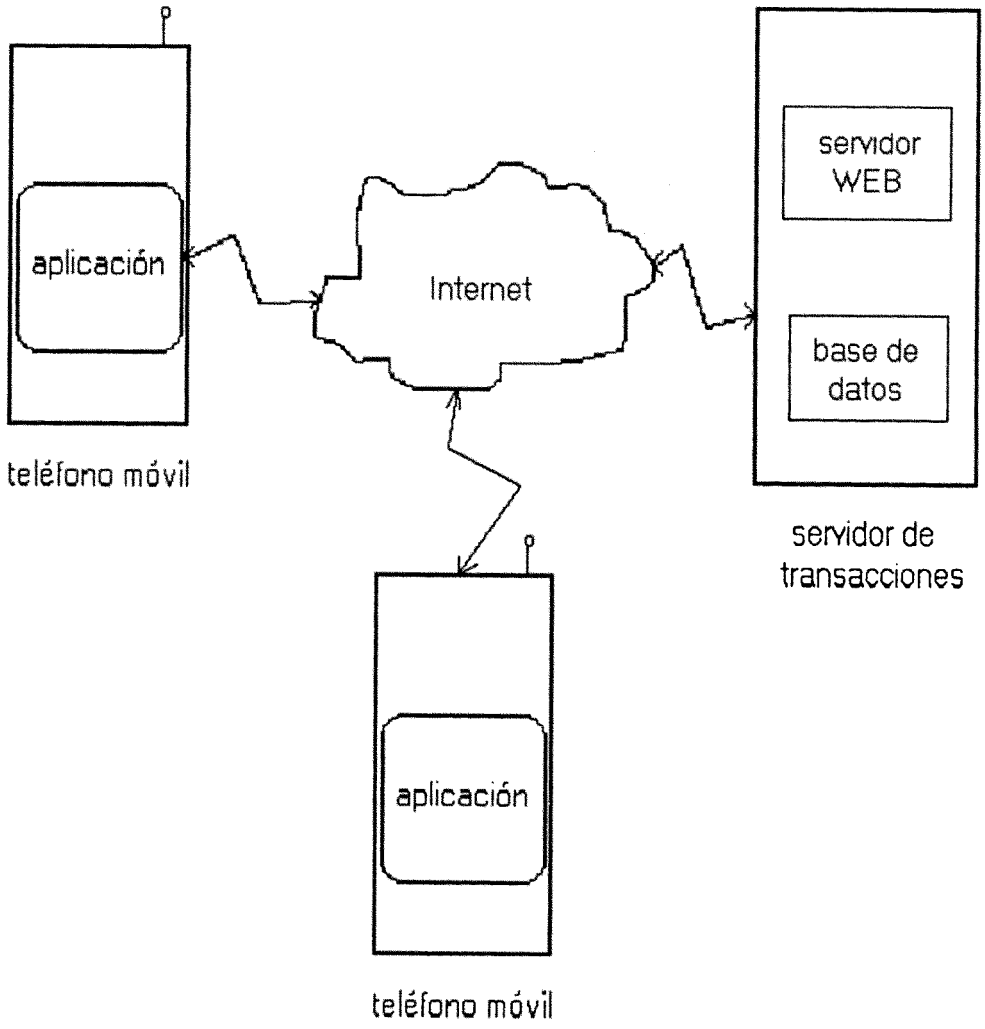

aplicación
teléfono móvil
Internet
servidor WEB
base de datos
servidor de transacciones
aplicación
teléfono móvil

Fig. 1

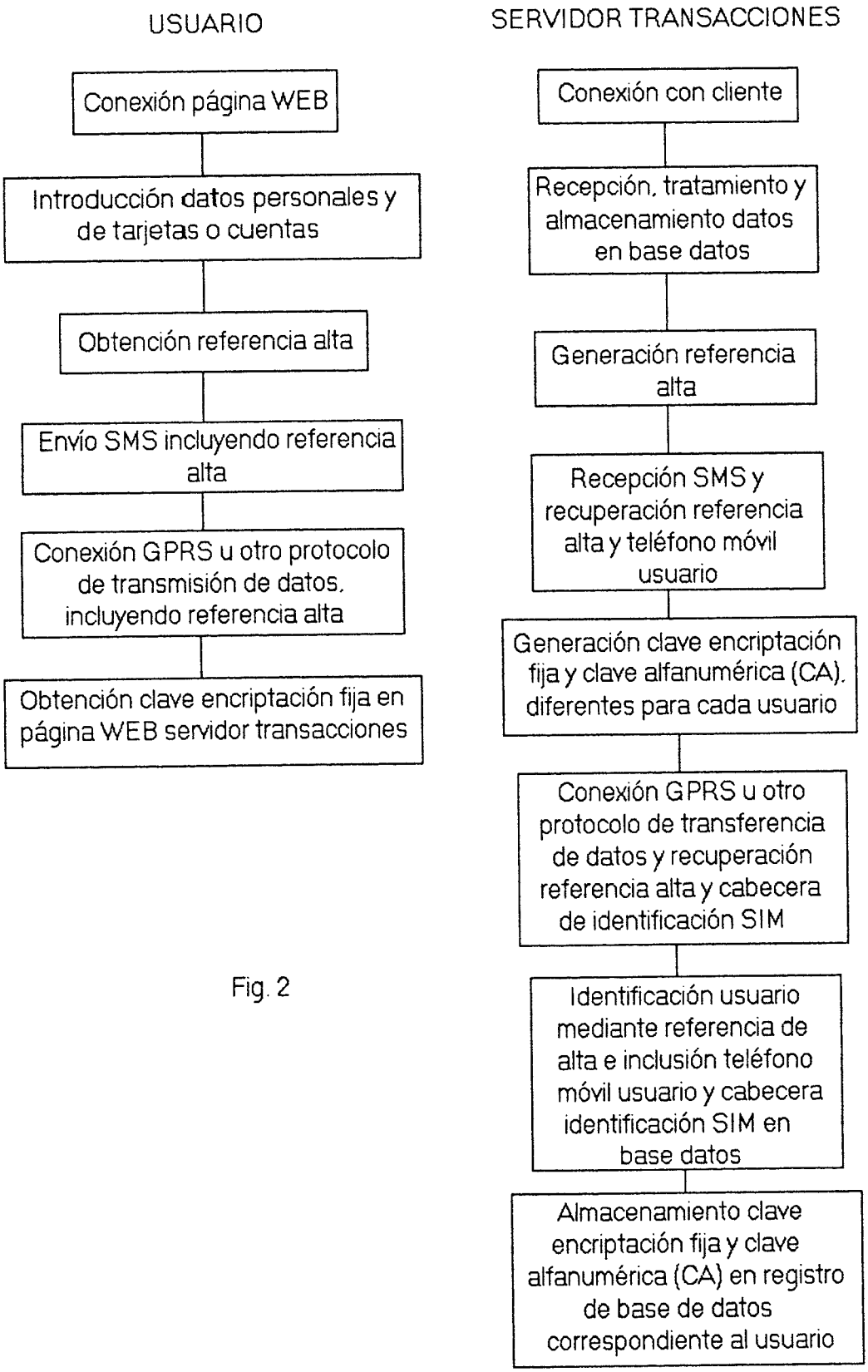

USUARIO
SERVIDOR TRANSACCIONES
Conexión página WEB
Introducción datos personales y de tarjetas o cuentas
Obtención referencia alta
Envío SMS incluyendo referencia alta
Conexión GPRS u otro protocolo de transmisión de datos, incluyendo referencia alta
Obtención clave encriptación fija en página WEB servidor transacciones
Conexión con cliente
Recepción, tratamiento y almacenamiento datos en base datos
Generación referencia alta
Recepción SMS y recuperación referencia alta y teléfono móvil usuario
Generación clave encriptación fija y clave alfanumérica (CA), diferentes para cada usuario
Conexión GPRS u otro protocolo de transferencia de datos y recuperación referencia alta y cabecera de identificación SIM
Identificación usuario mediante referencia de alta e inclusión teléfono móvil usuario y cabecera identificación SIM en base datos
Almacenamiento clave encriptación fija y clave alfanumérica (CA) en registro de base de datos correspondiente al usuario

Fig. 2

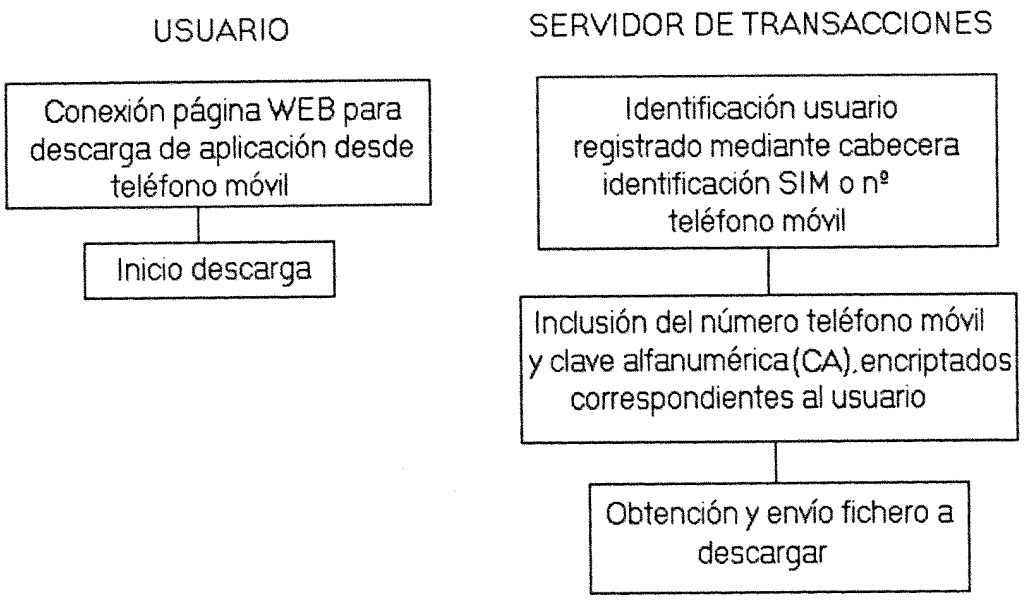
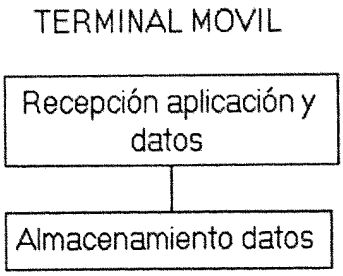

USUARIO
SERVIDOR DE TRANSACCIONES
Conexión página WEB para descarga de aplicación desde teléfono móvil
Inicio descarga
Identificación usuario registrado mediante cabecera identificación SIM o nº teléfono móvil
Inclusión del número teléfono móvil y clave alfanumérica (CA), encriptados correspondientes al usuario
Obtención y envío fichero a descargar

Fig. 3


TERMINAL MOVIL
Recepción aplicación y datos
Almacenamiento datos

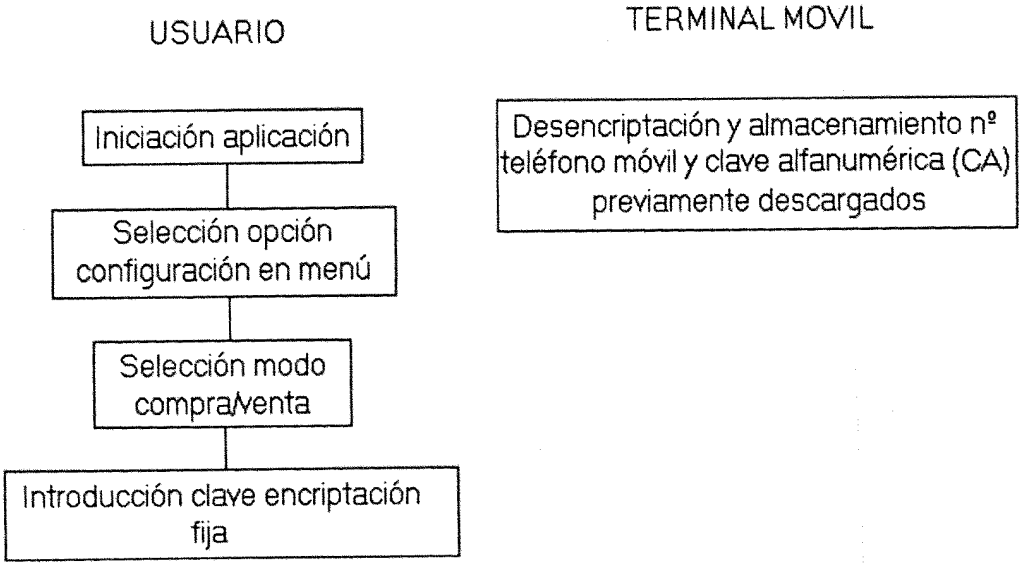

USUARIO
TERMINAL MOVIL
Iniciación aplicación
Selección opción configuración en menú
Selección modo compra/venta
Introducción clave encriptación fija
Desencriptación y almacenamiento nº teléfono móvil y clave alfanumérica (CA) previamente descargados

Fig. 4

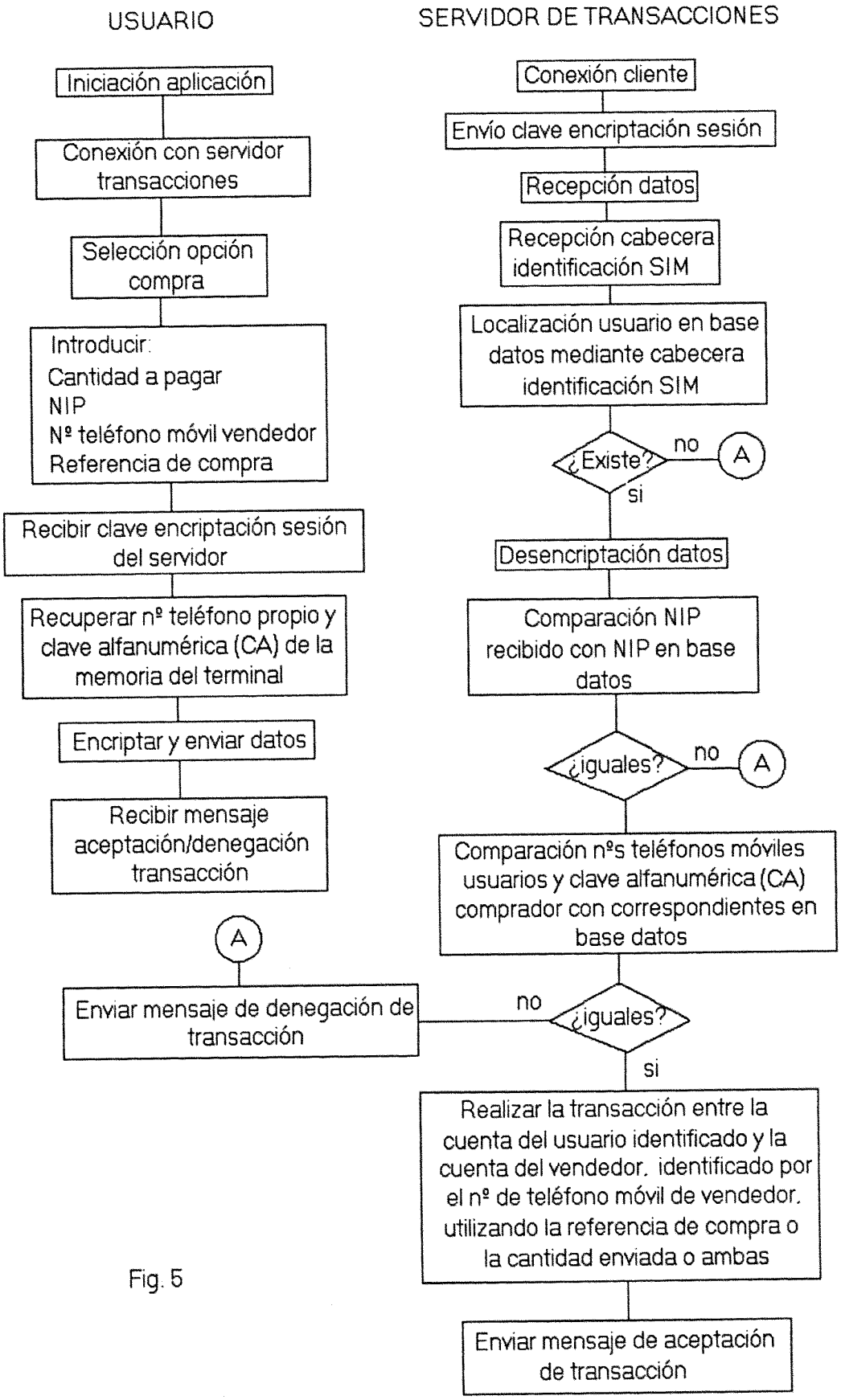

USUARIO
SERVIDOR DE TRANSACCIONES
Iniciación aplicación
Conexión con servidor transacciones
Selección opción compra
Introducir:
Cantidad a pagar
NIP
Nº teléfono móvil vendedor
Referencia de compra
Recibir clave encriptación sesión del servidor
Recuperar nº teléfono propio y clave alfanumérica (CA) de la memoria del terminal
Encriptar y enviar datos
Recibir mensaje aceptación/denegación transacción
A
Enviar mensaje de denegación de transacción
Conexión cliente
Envío clave encriptación sesión
Recepción datos
Recepción cabecera identificación SIM
Localización usuario en base datos mediante cabecera identificación SIM
¿Existe?
no
A
si
Desencriptación datos
Comparación NIP recibido con NIP en base datos
¿iguales?
no
A
Comparación nºs teléfonos móviles usuarios y clave alfanumérica (CA) comprador con correspondientes en base datos
¿iguales?
no
si
Realizar la transacción entre la cuenta del usuario identificado y la cuenta del vendedor, identificado por el nº de teléfono móvil de vendedor, utilizando la referencia de compra o la cantidad enviada o ambas
Enviar mensaje de aceptación de transacción

Fig. 5

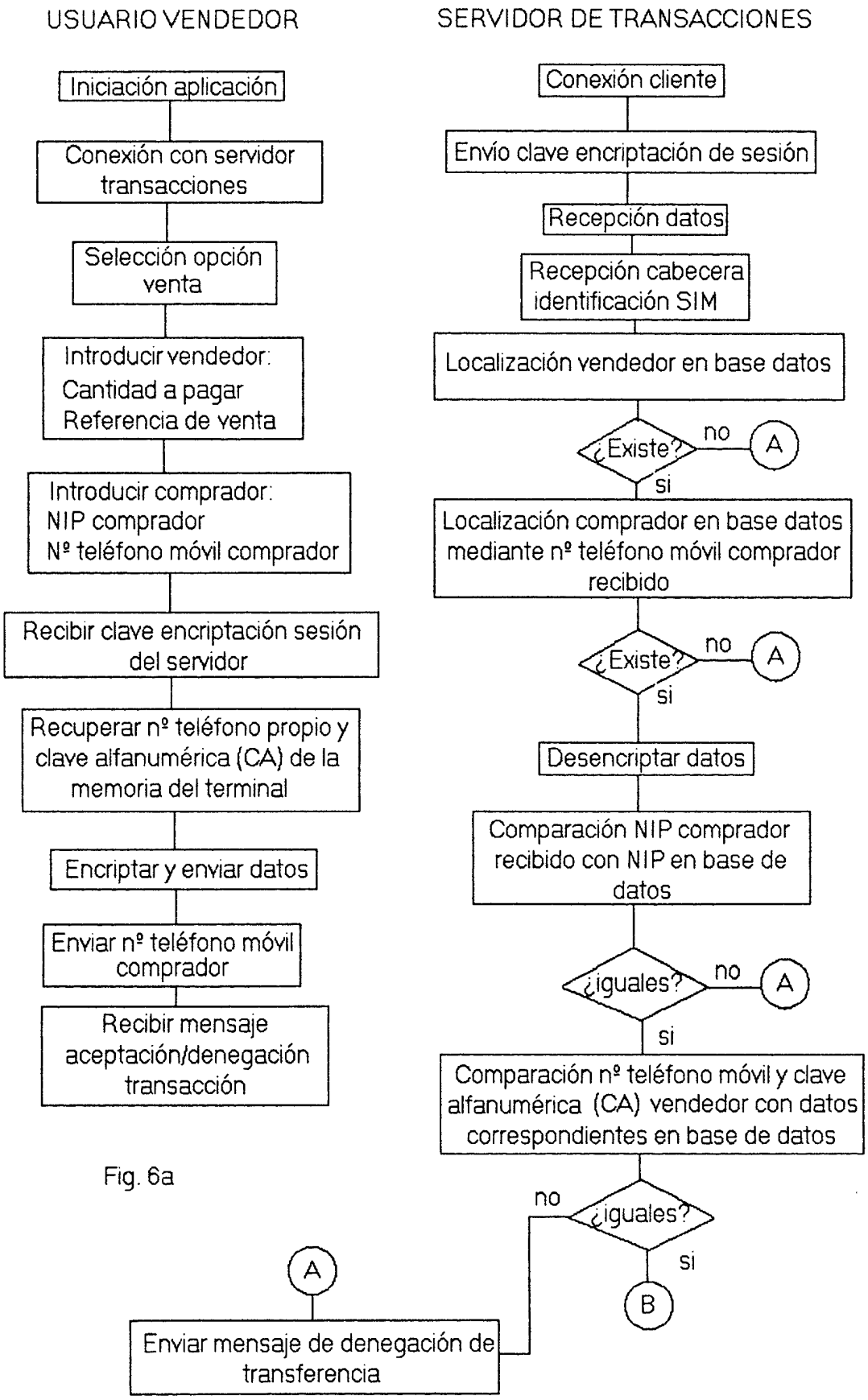

USUARIO VENDEDOR
Iniciación aplicación
Conexión con servidor transacciones
Selección opción venta
Introducir vendedor:
Cantidad a pagar
Referencia de venta
Introducir comprador:
NIP comprador
Nº teléfono móvil comprador
Recibir clave encriptación sesión del servidor
Recuperar nº teléfono propio y clave alfanumérica (CA) de la memoria del terminal
Encriptar y enviar datos
Enviar nº teléfono móvil comprador
Recibir mensaje aceptación/denegación transacción
SERVIDOR DE TRANSACCIONES
Conexión cliente
Envío clave encriptación de sesión
Recepción datos
Recepción cabecera identificación SIM
Localización vendedor en base datos
¿Existe?
no
A
si
Localización comprador en base datos mediante nº teléfono móvil comprador recibido
¿Existe?
no
A
si
Desencriptar datos
Comparación NIP comprador recibido con NIP en base de datos
¿iguales?
no
A
si
Comparación nº teléfono móvil y clave alfanumérica (CA) vendedor con datos correspondientes en base de datos
¿iguales?
no
si
B
A
Enviar mensaje de denegación de transferencia

Fig. 6a

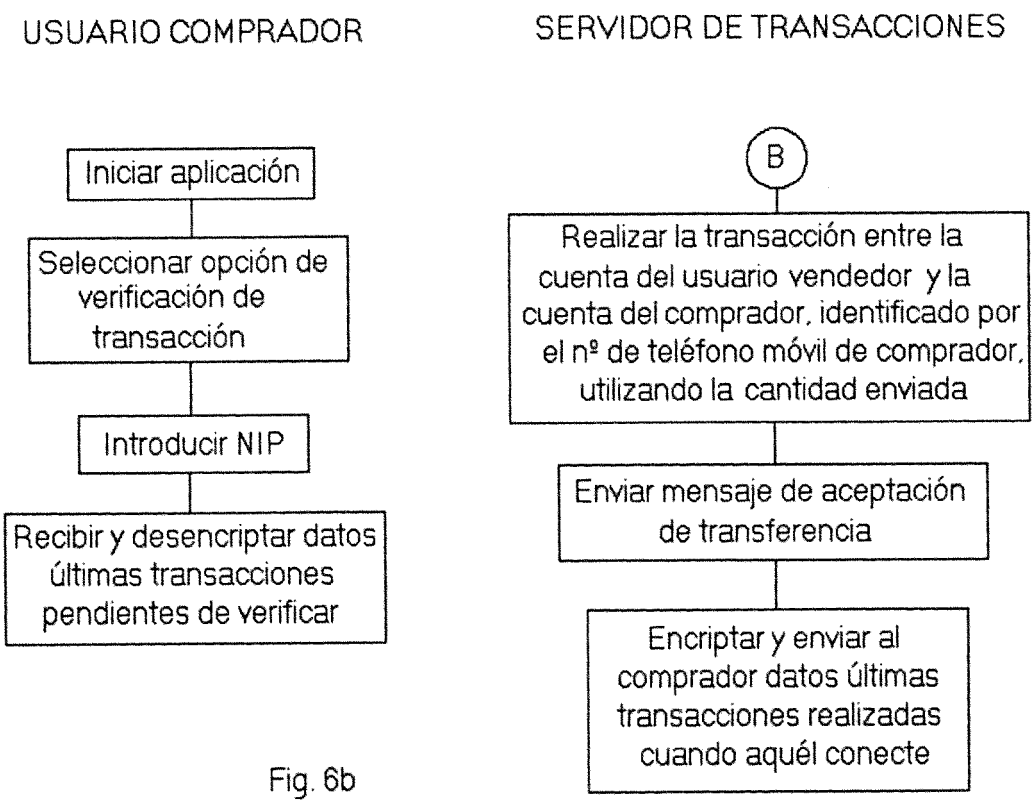

USUARIO COMPRADOR
SERVIDOR DE TRANSACCIONES
Iniciar aplicación
Seleccionar opción de verificación de transacción
Introducir NIP
Recibir y desencriptar datos últimas transacciones pendientes de verificar
B
Realizar la transacción entre la cuenta del usuario vendedor y la cuenta del comprador, identificado por el nº de teléfono móvil de comprador, utilizando la cantidad enviada
Enviar mensaje de aceptación de transferencia
Encriptar y enviar al comprador datos últimas transacciones realizadas cuando aquél conecte

Fig. 6b

OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) ES 2 263 344

(21) Nº de solicitud: 200401988

(22) Fecha de presentación de la solicitud: **30.07.2004**

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TÉCNICA

(51) **Int. Cl.:** ***G07F 19/00*** (2006.01)
G07F 7/10 (2006.01)

DOCUMENTOS RELEVANTES

Categoría	Documentos citados	Reivindicaciones afectadas
X	WO 0241271 A1 (HAIDAR) 23.05.2002, página 4, líneas 20-28; página 6, línea 21 - página 8, línea 11; página 11, línea 9 - página 13, línea 7; página 15, línea 23 - página 18, línea 3; figuras.	1-3
X	WO 0031699 A1 (LIPTON et al.) 02.06.2000, todo el documento.	1-3

Categoría de los documentos citados

X: de particular relevancia
Y: de particular relevancia combinado con otro/s de la misma categoría
A: refleja el estado de la técnica
O: referido a divulgación no escrita
P: publicado entre la fecha de prioridad y la de presentación de la solicitud
E: documento anterior, pero publicado después de la fecha de presentación de la solicitud

El presente informe ha sido realizado

☒ para todas las reivindicaciones ☐ para las reivindicaciones nº:

Fecha de realización del informe	Examinador	Página
10.11.2006	M. Alvarez Moreno	1/1