(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 527 632**

(51) Int. CI.:

G06Q 20/00 (2012.01)
G07F 7/10 (2006.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **18.11.2010 E 10793007 (5)**

(97) Fecha y número de publicación de la concesión europea: **22.10.2014 EP 2591463**

(54) Título: **Sistema y procedimiento de identificación y registro de identidad seguros**

(30) Prioridad:

08.07.2010 FR 1055573

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.01.2015

(73) Titular/es:

ABM TECHNOLOGIES (100.0%)
4 rue de Charenton
94140 Alfortville, FR

(72) Inventor/es:

BOULANOUAR, RYAD

(74) Agente/Representante:

LAZCANO GAINZA, Jesús

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 y procedimiento de identificación y registro de identidad seguros

La presente invención está relacionada con un sistema y un procedimiento de identificación y registro de identidad seguros.

Cuando un usuario desea registrar su identidad, por ejemplo, cuando desea abrir una línea de teléfono móvil desde un proveedor telefónico o proceder a una transferencia de dinero, el mismo debe llenar uno o varios formularios, entregar fotocopias de su tarjeta de identificación o de su pasaporte, lo que toma generalmente mucho tiempo. Los puntos de venta correspondientes no están siempre equipados correctamente con mesas y sillas que permitan a los usuarios llenar dichos formularios sin dificultad, de manera que es con frecuencia complicado y dilatado registrar su identidad. Por otra parte, el tiempo que transcurre entre los tenderos o vendedores que atienden al usuario durante esta fase de registro se pierde con respecto a otros usuarios, lo que demora el tiempo de espera y disminuye del mismo modo la rentabilidad de la tienda. Además, actualmente cuando un usuario se registra, por ejemplo, para abrir una línea telefónica, éste no puede utilizar este registro para otros servicios y por consiguiente debe comenzar esta fase de registro por cada servicio al que desea suscribirse.

El documento WO 2008/002979 describe un sistema y procedimiento de identificación y registro de identidad biométrica segura, que comprende un terminal de pago electrónico situado en un punto de venta, un teléfono celular del usuario a identificar, y un servidor para autenticar las informaciones sonoras relativas a la identidad del usuario que son comunicadas con dicho teléfono celular.

La presente invención tiene como objeto ofrecer un sistema y un procedimiento de registro de identidad y de identificación seguro que no reproduce los inconvenientes mencionados.

En particular, la presente invención tiene como objeto ofrecer un sistema y procedimiento tal que sea simple y rápido, a la vez de extremadamente confiable y seguro a fin de evitar al máximo los riesgos de fraude.

La presente invención tiene también como objetivo ofrecer un sistema y procedimiento tal que permita reutilizar varias veces el mismo registro de identidad, sin necesidad de comenzar nuevamente todo el procedimiento cada vez que una nueva identificación segura sea necesaria.

La presente invención tiene también como objetivo además ofrecer un sistema y procedimiento tal que sea simple y poco costoso de llevar a cabo.

La presente invención tiene por lo tanto como objetivo un sistema de identificación y registro de identidad seguros, que comprende:

- medios de copia para realizar una copia numérica de un documento de identidad del usuario a identificar,
- al menos un servidor,
- primeros medios de transmisión para transmitir dicha copia digital a dicho servidor,
- medios de reconocimiento de caracteres para analizar dicha copia numérica y extraer dicha copia numérica de las informaciones relativas a la identidad del usuario de dicha copia numérica,
- al menos una base de datos para almacenar dicha copia numérica y dichas informaciones relativas a la identidad del usuario,
- un terminal de pago electrónico, específicamente ubicado en un punto de venta,
- segundos medios de transmisión para transmitir dichas informaciones relativas a la identidad del usuario hacia dicho terminal de pago electrónico,
- un teléfono celular del usuario a identificar, asociado a un código secreto,
- terceros medios de transmisión para transmitir el número de dicho teléfono celular a partir del dicho terminal de pago electrónico hacia dicho servidor,
- medios que envían una melodía que reproducirá dicho servidor en dicho terminal de pago electrónico,
- medios para llamar que permiten a dicho servidor realizar una comunicación telefónica con dicho teléfono celular, y

- elementos de autenticación sonora por dicho servidor de dicha melodía reproducida por dicho terminal de pago electrónico a través de dicha comunicación telefónica con dicho teléfono celular.

Ventajosamente, dicho servidor comprende un módulo NSDT (Near Sound Data System) que permite llamar a dicho teléfono celular y reconocer una melodía reproducida por dicho terminal de pago electrónico.

Ventajosamente, un módulo de gestión garantiza la seguridad de todas las transmisiones.

Ventajosamente, los medios de transmisión emplean la red Internet.

Ventajosamente, un módulo de gestión del terminal de pago electrónico está asociado a dicho servidor para controlar las transmisiones entre dicho servidor y dicho terminal de pago electrónico.

Ventajosamente, dicho terminal de pago electrónico comprende un visualizador, un teclado, una impresora, un lector de tarjeta magnética, un alto parlante y un módulo de conexión a Internet.

Ventajosamente, dichos medios para copiar comprenden un escáner.

Ventajosamente, en un punto de venta, un escáner, un pad y un TPE/POS/POS están unidos a una caja de gestión que controla las conexiones y enlaces de estos elementos entre ellos y con el servidor.

Ventajosamente, dicha caja de gestión, dicho escáner y dicho pad forman una única unidad global.

La presente invención tiene también como objeto un procedimiento de identificación y registro de identidad seguros, que comprende las etapas siguientes:

- realizar una copia numérica de un documento de identidad del usuario a identificar,
- transmitir dicha copia numérica a un servidor,
- realizar un reconocimiento de caracteres de dicha copia numérica para extraer de dicha copia numérica informaciones relativas a la identidad del usuario,
- almacenar dicha copia numérica y dichas informaciones relativas a la identidad del usuario en al menos una base de datos,
- transmitir a un terminal de pago electrónico, específicamente ubicado en un punto de venta, dichas informaciones relativas a la identidad del usuario,
- visualizar dichas informaciones relativas a la identidad del usuario en el visualizador de dicho terminal de pago electrónico,
- introducir en dicho terminal de pago electrónico el número de teléfono celular del usuario a identificar,
- introducir en dicho terminal de pago electrónico un código secreto asociado a dicho número de teléfono,
- transmitir dicho número de teléfono a dicho servidor si dicho código secreto es correcto,
- enviar de dicho servidor a dicho terminal de pago electrónico una melodía que se reproducirá,
- realizar un comunicación telefónica con dicho teléfono celular a partir de dicho servidor,
- transmitir a dicho servidor, a través de dicha comunicación telefónica, dicha melodía reproducida por el terminal de pago electrónico, y
- autenticar dicha melodía por dicho servidor.

Estas características y ventajas entre otras de la presente invención se mostrarán más claramente a lo largo de la descripción detallada siguiente, hecha con referencia a los dibujos adjuntos, ofrecidos a título de ejemplos no limitativos, y en los cuales

- la figura 1 representa un esquema funcional ilustrando los elementos del sistema y las etapas del procedimiento de la presente invención, según un modo de realización ventajoso de éstos, y
- las figuras 2 a 4 son variantes de configuración hardware utilizables para llevar a cabo la presente invención.

Con referencia a la figura 1, el sistema de registro de identidad e identificación seguros de la presente invención presenta varios elementos que forman parte de un centro de tratamiento de datos y varios otros elementos que forman parte o están

previstos al nivel del punto de venta, estos diferentes elementos estando unidos unos a los otros significativamente a través de la red Internet.

Más específicamente, el centro de tratamiento de datos comprende al menos un servidor A. Estos servidores están ventajosamente instalados en un centro de tratamiento de datos seguro y controlado. La continuación de la descripción será hecha con referencia a un solo servidor A, pero es obvio que pueden considerarse varios servidores.

Al nivel del punto de venta, donde se encuentra el usuario que desea registrarse y/o identificarse, se prevén medios de copia J para realizar una copia numérica del documento de identidad K del usuario a identificar. De preferencia, estos medios de copia J aparecen bajo la forma de un escáner. Este escáner contiene los primeros medios de transmisión para transmitir dicha copia digital a dicho servidor A. Ventajosamente, estos primeros medios de transmisión utilizan la red Internet G, específicamente a través de una conexión TCP/IP, PPP o GPRS. En una variante, el usuario pudiera también enviar, por ejemplo, por email, una copia numérica de su documento de identidad directamente al servidor, por ejemplo a través de un sitio de internet de registro dedicado. Al nivel del centro de tratamiento de datos, se prevén medios de reconocimiento de caracteres E para analizar dicha copia numérica recibida. Este análisis sirve específicamente para extraer de dicha copia numérica las informaciones relativas a la identidad del usuario. Ventajosamente, estos medios de reconocimiento de caracteres están formados por un módulo OCR (« Optical Character Recognition ») que se encuentra asociado a un servidor. Este módulo OCR puede descifrar específicamente la zona legible de las tarjetas de identidad o pasaportes modernos llamado MRZ (« Machine Readable Zone »). El mismo permite también recuperar la foto del documento de identidad así como las informaciones clásicas tales como el nombre, la fecha de nacimiento, la fecha de expiración, etc. La copia numérica del documento de identidad así como dichas informaciones relativas a la identidad del usuario son posteriormente transmitidas a una o varias base(s) de datos B para su almacenamiento. Estas bases de datos son entonces aseguradas y replicadas y el acceso a los datos es controlado.

Así, la copia numérica sólo es necesaria para el registro del usuario. Posteriormente, para identificarse, esta copia numérica almacenada en la base de datos y/o las informaciones relativas a la identidad que fueron extraídas podrán ser comparadas con el verdadero documento de identidad del usuario.

Al nivel del punto de venta, un terminal de pago electrónico I, a continuación denominado TPE/POS, comprende ventajosamente un visualizador, un teclado, una imprenta, un lector de tarjeta magnética, un alto parlante y un módulo de conexión a Internet. Ventajosamente, el TPE/POS comprende un lector de tarjeta inteligente que permite la lectura de informaciones (por ejemplo a partir de las tarjetas sésame, vitale, tarjeta de identidad electrónica, etc.), así como un lector sin contacto RFID, que permite leer por ejemplo los pasaportes biométricos inteligentes RFID. Éstos entonces pueden aprovecharse para adquirir y enriquecer el perfil del usuario. El visualizador comprende típicamente varias líneas, por ejemplo cuatro, y el teclado puede ser numérico o alfanumérico. La conexión a la red Internet puede igualmente hacerse por conexión TCP/IP o GPRS. El escáner y el TPE/POS pudieran enlazarse para compartir la conectividad. Segundos medios de transmisión se emplearán para transmitir las informaciones relativas a la identidad del usuario a partir de la base de datos B hacia dicho TPE/POS. Esta transmisión se realiza de preferencia a través de la red Internet. Al nivel del centro de tratamiento, se prevé un módulo de gestión D de transacciones o transmisiones TPE/servidor para asegurar la gestión y la autenticación de la plataforma TPE/POS así como la interfaz con la ventanilla (o « front office ») del centro de tratamiento. En efecto, el centro de tratamiento de datos comprende de preferencia un módulo de gestión de ventanilla que asegura la concentración de las conexiones, el control de coherencia de los datos y el aseguramiento de los intercambios.

Cuando las informaciones relativas a la identidad son transmitidas al TPE/POS, éstas se visualizarán en el visualizador de dicho TPE/POS. El responsable del TPE/POS, es decir, el vendedor del punto de venta, va a entonces poder efectuar un primer control comparando la visualización en su TPE/POS con el documento de identidad que el usuario le va a mostrar. Se debe observar que esta etapa de verificación visual por el vendedor no es absolutamente esencial para el buen funcionamiento del sistema y procedimiento de la presente invención.

Para garantizar la identificación segura del usuario, un teléfono H de dicho usuario a identificar se pone a disposición, de preferencia su teléfono celular o móvil. Por ejemplo, este número de teléfono puede ser comunicado en el punto de venta, o transmitido por email juntos con la copia numérica del documento de identidad. El número de dicho teléfono está asociado a un código secreto, previamente comunicado al usuario. Ventajosamente, este código secreto, que puede por ejemplo comprender cuatro o seis cifras, puede ser escogido confidencialmente por el usuario, en el registro o ulteriormente si lo desea cambiar. La función de este código secreto es cifrar las informaciones confidenciales del usuario en la base de datos, y es por ende necesario para la identificación y/o la transferencia de informaciones hacia servicios terceros. En caso de pérdida de este código, el registro será realizado nuevamente de preferencia por razones de seguridad. El usuario va entonces a introducir su número de teléfono en el teclado de dicho TPE/POS. Del mismo modo va a introducir dicho código

secreto asociado. Si dicho código secreto es correcto, es decir, si corresponde al código secreto asociado al número de teléfono, entonces los terceros medios de transmisión van a transmitir dicho número de teléfono introducido de dicho TPE/POS en dicho servidor. Nuevamente, esta transmisión se hace preferencialmente a través de Internet. De retorno, el servidor va a enviar a dicho TPE/POS, a través de los medios de envío apropiados, una melodía aleatoria, para que la misma sea reproducida por dicho TPE/POS. Este envío de la melodía es realizado igualmente de manera ventajosa a través de la red Internet.

El servidor comprende medios de llamar C a dicho teléfono, permitiendo a dicho servidor llamar a dicho teléfono. Ventajosamente, estos elementos de llamada están formados por un módulo NSDT (« Near Sound Data System »). La llamada telefónica al teléfono del usuario por dicho servidor se realiza justo después del envío de la melodía a dicho TPE/POS. El usuario descuelga su teléfono cuando recibe la llamada del servidor y acerca su teléfono a dicho TPE/POS para transmitir a través de dicha comunicación telefónica dicha melodía reproducida por dicho TPE/POS. Dicho servidor autentica entonces dicha melodía como la que se trasmitió precedentemente al TPE/POS, lo que le permite identificar claramente el número de teléfono asociado a las informaciones relativas a la identidad de la base de datos. Los elementos de autenticación sonoras del servidor forman parte ventajosamente de dicho módulo NSDT.

De este modo, la invención ofrece un sistema y un procedimiento de registro de identidad e identificación seguros que permite en muy poco tiempo, típicamente de dos a tres minutos, no solamente registrarse sino también identificarse de manera totalmente segura. En efecto, para violar el sistema de la invención, se necesitaría no solamente presentar una falsa tarjeta de identidad sino igualmente lograr sustraer el teléfono y el código secreto asociado a dicho teléfono para eventualmente encontrar un fallo en el sistema. Una etapa opcional de verificación de las informaciones relativas a la identidad visualizadas en el TPE/POS con el verdadero documento de identidad del usuario refuerza aún más la seguridad del sistema. Es evidente que con la futura generación de los TPE/POS, o con el pad descrito a continuación con referencia a las figuras de la 2 a la 4, la totalidad o casi la totalidad de la copia numérica del documento de identidad, incluyendo la foto, podrá aparecer en la pantalla de los TPE/POS y/o del pad, lo que facilitará aún más la verificación de identidad.

El procedimiento es particularmente simple, el usuario que desee identificarse se presenta en un punto de venta, éste muestra su tarjeta de identidad al vendedor y teclea en el TPE/POS su número de teléfono y su código secreto. El TPE/POS transmite el número de teléfono al servidor si el código secreto es correcto. Dicho servidor envía entonces la melodía aleatoria al TPE/POS y llama inmediatamente al teléfono. El usuario descuelga, acerca el teléfono al TPE/POS que reproduce dicha melodía previamente enviada, y el servidor valida la autenticación si reconoce la melodía reproducida como la que fue previamente enviada. Típicamente, el teléfono estará ventajosamente distante al menos 30 cm de dicho TPE/POS en el momento donde el reconocimiento sonoro se realice, para evitar posibles ruidos parásitos.

La plataforma de registro de la invención permite registrar clientes en dos o tres minutos, en puntos de venta equipados con terminales de pago electrónicas, y escáneres que poseen la funcionalidad de enviar correos electrónicos. El registro con la autenticación fuerte realiza el almacenamiento seguro de la copia numérica del documento de identidad del cliente en un centro de tratamiento de datos, el registro del número de teléfono móvil del cliente como « dato público », el registro del código confidencial del cliente como « dato confidencial », y el reconocimiento del teléfono móvil del cliente por autenticación sonora, con la finalidad de validar que el número de teléfono introducido es el del teléfono cuyo cliente realmente posee.

Una ventaja de la presente invención es que una vez que el usuario es registrado, y que su registro fue autenticado, éste puede utilizar esta « identificación electrónica » cada vez que desee identificarse para cualquier servicio. De esta forma, si se identifica la primera vez de manera electrónica según la invención para por ejemplo abrir una línea telefónica, puede luego, si se dirige a un punto de venta proponiendo un servicio de transferencia de dinero, identificarse de la misma manera empleando el procedimiento de identificación de la presente invención, lo que le permite utilizar los diferentes servicios que reconocen esta identificación electrónica. La presente invención permite entonces ofrecer un ahorro de tiempo muy importante, evita los registros repetitivos, demorados e incómodos para los usuarios, simplifica el trabajo de los vendedores y lo hace más eficaz, y presenta una alta confiabilidad. La presente invención se aplica entonces a todo tipo de servicio que necesite una determinada identificación, como las aperturas de cuentas bancarias, transferencias de dinero, etc.

Ventajosamente, el perfil del usuario puede ser enriquecido con nuevos documentos, tales como la licencia de conducción, la tarjeta gris, una factura EDF, etc. Esto permite facilitar un perfil completo, cuyas informaciones o parte de las mismas podrán ser transmitidas a terceros servicios.

Las figuras 2 a 4 ilustran configuraciones hardware posibles para llevar a cabo la presente invención. Así, en la configuración ilustrada esquemáticamente en la figura 2, un escáner 9, una terminal electrónica de pago (TPE/POS) 11 y un pad 10 están unidos a una caja (Box) 8 que asegura la interconexión y los enlaces entre estos elementos y el o los

servidores del sistema. Las conexiones pueden ser alámbricas o inalámbricas. Una configuración típica es aquella donde el usuario /cliente es separado del vendedor que lo recibe en el punto de venta, típicamente por una ventanilla con eventualmente una parte inferior abierta permitiendo el paso de documentos. La caja y el escáner pueden entonces estar ubicados al lado del vendedor, mientras que el pad puede estar al lado del usuario, el TPE/POS pudiendo pasar de un lado al otro de la separación. El usuario pasa su documento de identidad al vendedor que la escanea, y el pad, de preferencia dotado de un visualizador, visualiza informaciones que pueden leerse por el usuario, por ejemplo la copia escaneada de su documento de identidad para verificación y validación. El pad puede también servir para recoger la firma del usuario, con la ayuda de un lápiz apropiado. En una variante, el pad puede comprender una cámara, por ejemplo del tipo de una webcam, para hacer una foto numérica del usuario durante la fase de registro. Éste pudiera también comprender un micrófono para capturar una frase pronunciada por el usuario para un reconocimiento vocal ulterior. El pad pudiera inclusive comprender altavoces adaptados para reproducir sonidos, por ejemplo la melodía que reproducirá el servidor. Según la utilización concebida, el pad puede entonces ser la interfaz principal del usuario, más que el TPE/POS. En el ejemplo de la figura 3, el escáner y la caja/box son reunidos en una sola y misma unidad global, y en el ejemplo de la figura 4, el pad está también integrado a esta unidad global. Estas prácticas de las figuras 3 y 4 simplifican la conectividad y los enlaces, alámbricos o no, entre los diferentes componentes del sistema. Sin embargo, para determinaciones aplicaciones, puede ser preferible mantener cada componente separado de los otros, como en el ejemplo de la figura 2. Las figuras de la 2 a la 4 ilustran ejemplos de tipos de uniones y/o conexiones posibles (USB, Serie, RJ45, RJ11, Bluetooth, Wi-Fi, etc.).

Aunque la presente invención haya sido descrita con referencia a modos de realización particulares, es obvio que la misma no está limitada por los ejemplos representados en los dibujos sino por el contrario un experto puede aportarle todas las modificaciones útiles sin salirse del marco de la presente invención tal como lo definen las reivindicaciones anexadas.

Reivindicaciones

1. Sistema de identificación y registro de identidad seguros, que comprende:
- medios de copia (J) para realizar una copia numérica de un documento de identidad (K) del usuario a identificar,
- al menos un servidor (A),
- primeros medios de transmisión para transmitir dicha copia digital a dicho servidor,
- medios de reconocimiento de caracteres (E) para analizar dicha copia numérica y extraer dicha copia numérica de las informaciones relativas a la identidad del usuario de dicha copia numérica,
- al menos una base de datos (B) para almacenar dicha copia numérica y dichas informaciones relativas a la identidad del usuario,
- un terminal de pago electrónico (I), situado en un punto de venta,
- segundos medios de transmisión para transmitir dichas informaciones relativas a la identidad del usuario hacia dicho terminal de pago electrónico,
- un teléfono celular (H) del usuario a identificar, asociado a un código secreto,
- terceros medios de transmisión para transmitir el número de dicho teléfono celular a partir de dicho terminal de pago electrónico hacia dicho servidor,
- medios de envío de una melodía a reproducir por dicho servidor a dicho terminal de pago electrónico,
- medios para llamar (C) que permiten a dicho servidor realizar una comunicación telefónica con dicho teléfono celular, y
- medios de autenticación sonora (C) por dicho servidor de dicha melodía reproducida por dicho terminal de pago electrónico a través de dicha comunicación telefónica con dicho teléfono celular.

2. Sistema según la reivindicación 1, en el cual dicho servidor comprende un módulo NSDT o sistema Near Sound Data que permite llamar a dicho teléfono celular y reconocer una melodía reproducida por dicho terminal de pago electrónico.

3. Sistema según la reivindicación 1 ó 2, en el cual un módulo de gestión (F) asegura la confiabilidad de todas las transmisiones.

4. Sistema según una de las reivindicaciones precedentes, en el cual los medios de transmisión emplean la red Internet (G)

5. Sistema según una de las reivindicaciones precedentes, en el cual un módulo de gestión (D) del terminal de pago electrónico es asociado a dicho servidor para controlar las transmisiones entre dicho servidor y dicho terminal de pago electrónico.

6. Sistema según una cualquiera de las reivindicaciones precedentes, en el cual dicho terminal de pago electrónico comprende un visualizador, un teclado, una imprenta, un lector de tarjeta magnética, un alto parlante y un módulo de conexión a Internet.

7. Sistema según una cualquiera de las reivindicaciones precedentes, en el cual dichos elementos de copia comprenden un escáner.

8. Sistema según una cualquiera de las reivindicaciones precedentes, en el cual en un punto de venta un escáner, un pad y un TPE/POS están unidos a una caja de gestión que controla las conexiones y los enlaces de estos elementos entre ellos y con el servidor.

9. Sistema según la reivindicación 8, en el cual dicha caja de gestión, dicho escáner y dicho pad forman una sola unidad global.

10. Procedimiento de identificación y registro de identidad seguros, que comprende las etapas siguientes:
- realizar una copia numérica (1) de un documento de identidad (K) del usuario a identificar,
- transmitir (2) dicha copia numérica a un servidor (A),
- realizar un reconocimiento de caracteres de dicha copia numérica para extraer de dicha copia numérica sólo las informaciones relativas a la identidad del usuario,
- almacenar (3) dicha copia numérica y dichas informaciones relativas a la identidad del usuario en al menos una base de datos (B),

- transmitir (4) a un terminal de pago electrónico (I), situado en un punto de venta, dichas informaciones relativas a la identidad del usuario,
- visualizar (5) dichas informaciones relativas a la identidad del usuario en el visualizador de dicho terminal de pago electrónico,
- introducir en dicho terminal de pago electrónico el número de teléfono de un teléfono celular (H) del usuario a identificar,
- introducir en dicho terminal de pago electrónico un código secreto asociado a dicho número de teléfono,
- transmitir (6) dicho número de teléfono a dicho servidor si dicho código secreto es correcto,
- enviar (7) de dicho servidor a dicho terminal de pago electrónico una melodía a reproducir,
- realizar una comunicación telefónica (8) con dicho teléfono celular a partir de dicho servidor,
- transmitir (9) a dicho servidor, a través de dicha comunicación telefónica, dicha melodía reproducida por dicho terminal de pago electrónico, y
- autenticar dicha melodía por dicho servidor.

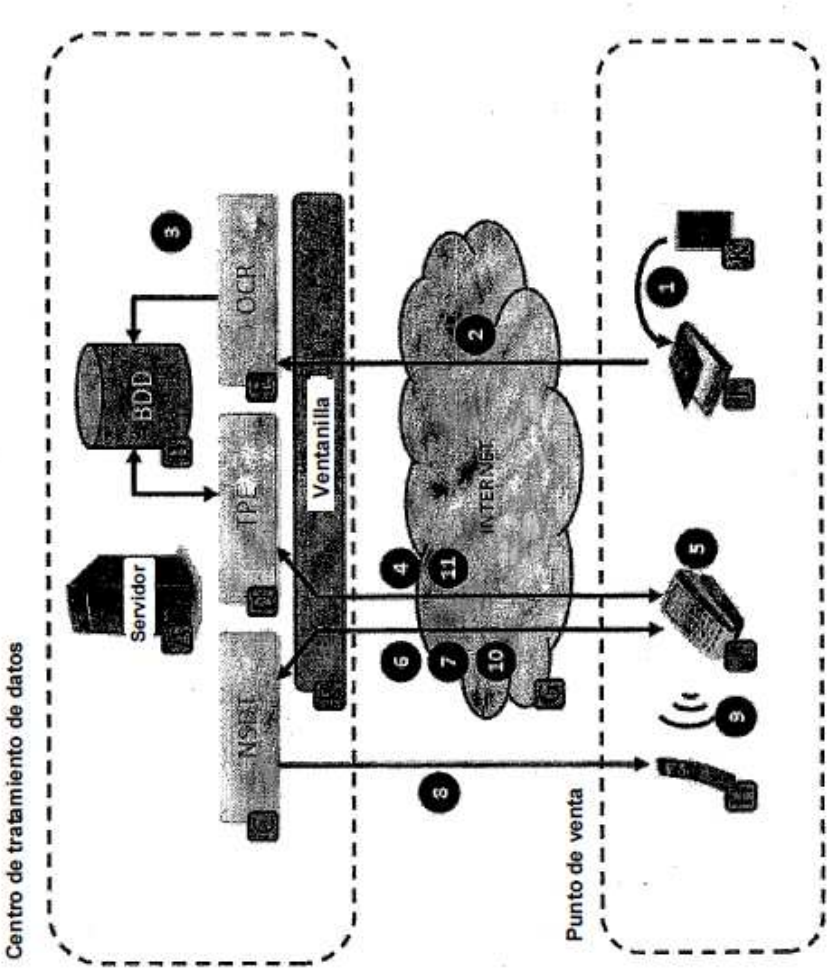

Centro de tratamiento de datos
Servidor
BDD
OCR
TPE
NSBL
Ventanilla
INTERNET
Punto de venta
1
2
3
4
5
6
7
8
9
10
11

Fig. 1

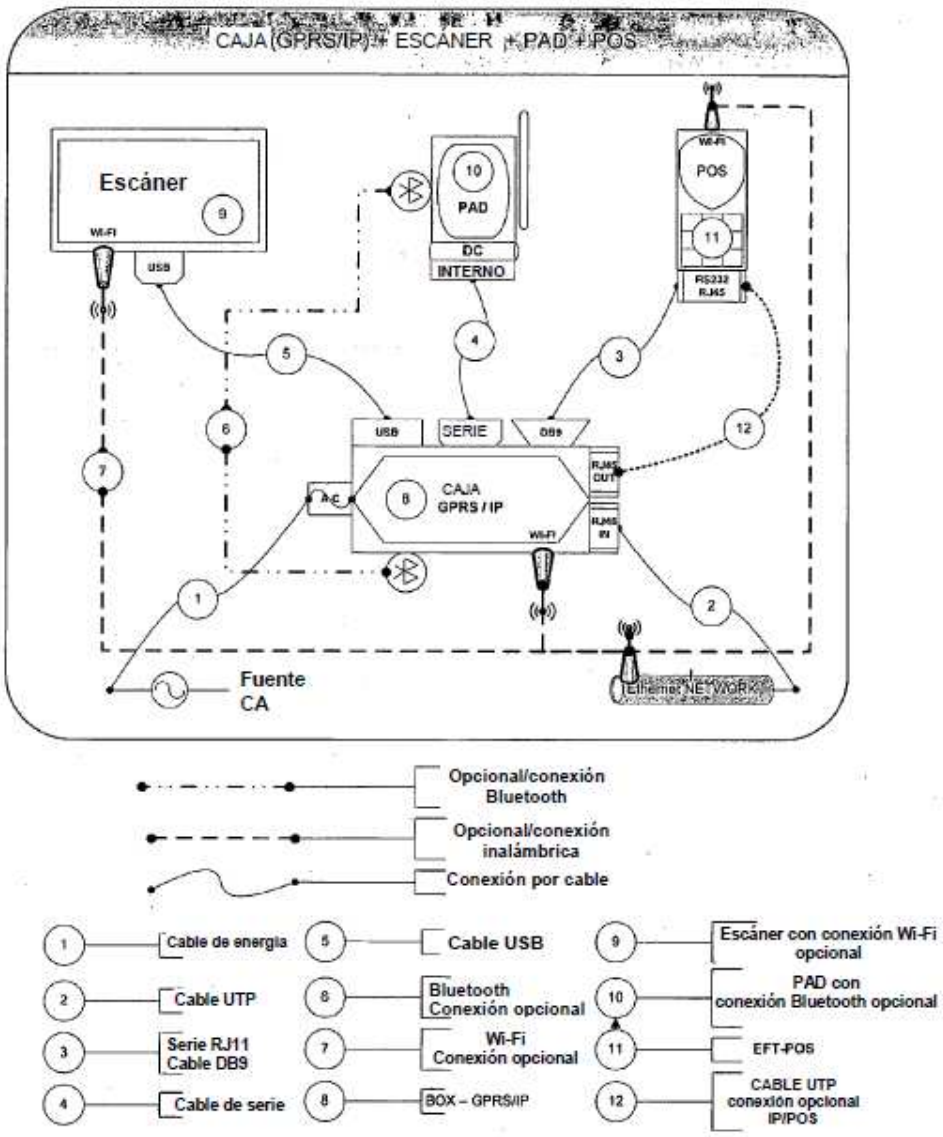

CAJA (GPRS/IP) + ESCÁNER + PAD + POS
Escáner
9
Wi-Fi
USB
10
PAD
DC
INTERNO
Wi-Fi
POS
11
RS232
RJ45
5
4
3
6
USB
SERIE
DB9
12
7
8
CAJA
GPRS / IP
RJ45
OUT
RJ45
IN
Wi-Fi
1
2
Fuente
CA
Ethernet NETWORK
Opcional/conexión Bluetooth
Opcional/conexión inalámbrica
Conexión por cable
1 Cable de energía
2 Cable UTP
3 Serie RJ11 Cable DB9
4 Cable de serie
5 Cable USB
6 Bluetooth Conexión opcional
7 Wi-Fi Conexión opcional
8 BOX – GPRS/IP
9 Escáner con conexión Wi-Fi opcional
10 PAD con conexión Bluetooth opcional
11 EFT-POS
12 CABLE UTP conexión opcional IP/POS

Fig. 2

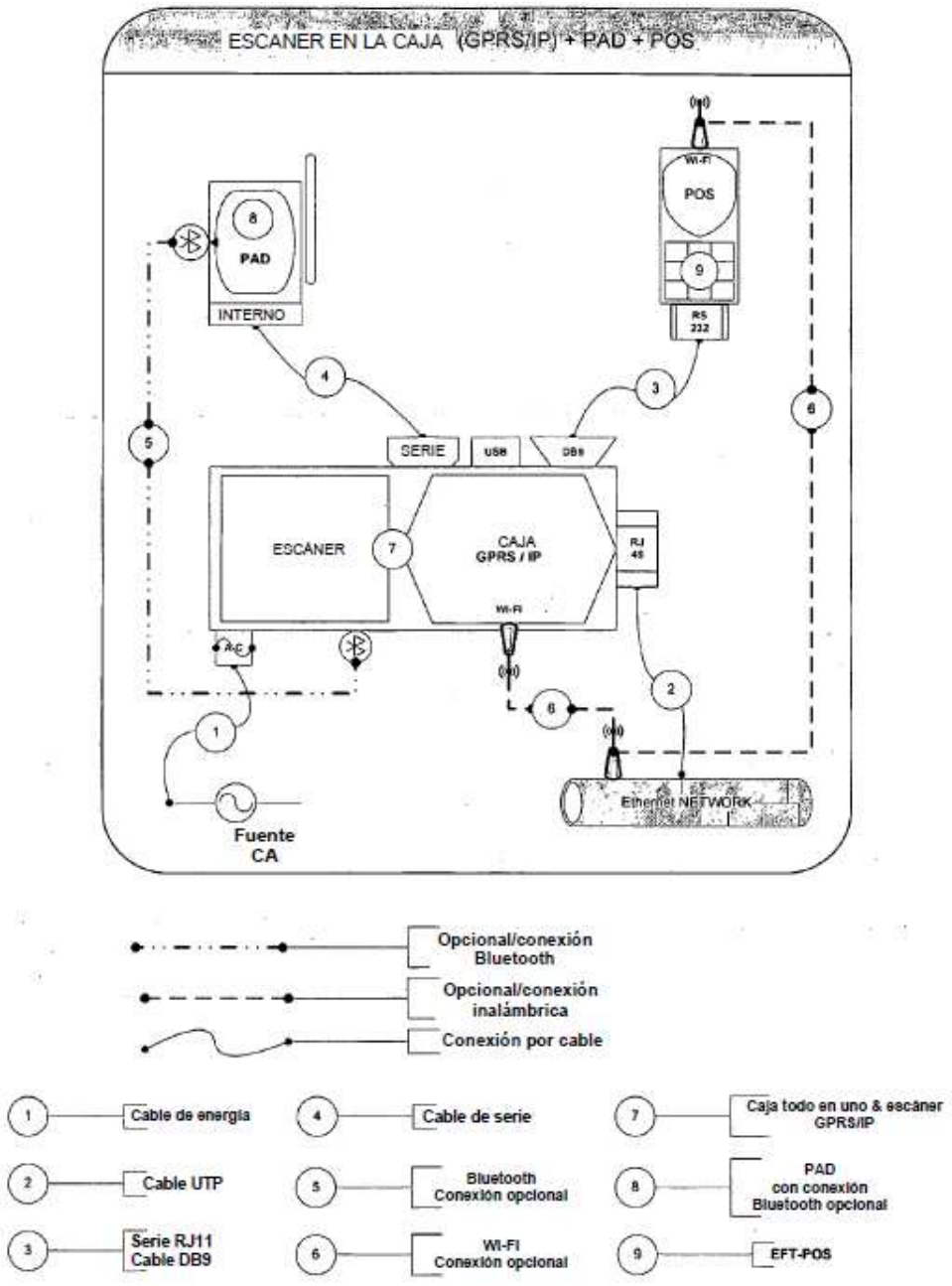

ESCANER EN LA CAJA (GPRS/IP) + PAD + POS
Wi-Fi
POS
9
RS 232
8
PAD
INTERNO
4
3
6
5
SERIE
USB
DB9
ESCANER
7
CAJA
GPRS / IP
RJ 45
Wi-Fi
2
6
1
Ethernet NETWORK
Fuente CA
Opcional/conexión Bluetooth
Opcional/conexión inalámbrica
Conexión por cable
1 Cable de energía
2 Cable UTP
3 Serie RJ11 Cable DB9
4 Cable de serie
5 Bluetooth Conexión opcional
6 WI-FI Conexión opcional
7 Caja todo en uno & escáner GPRS/IP
8 PAD con conexión Bluetooth opcional
9 EFT-POS

Fig. 3

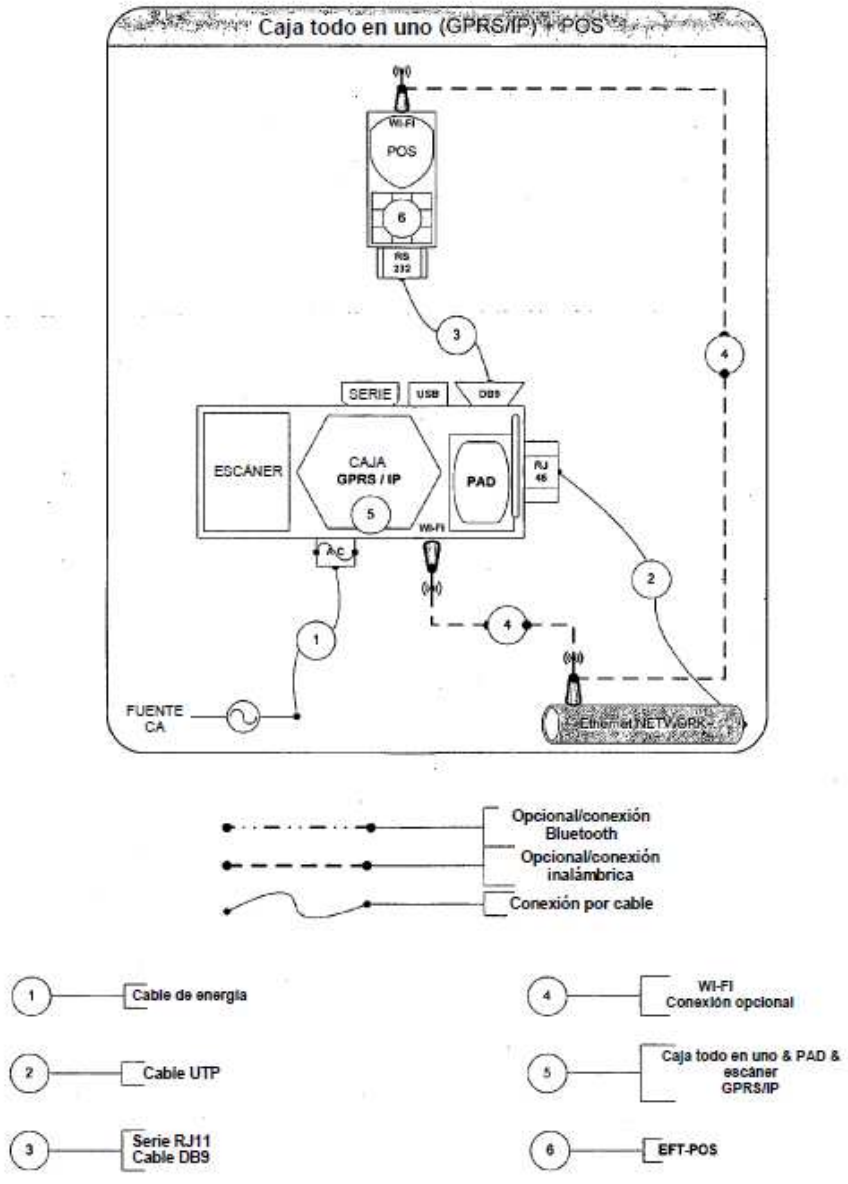

Caja todo en uno (GPRS/IP) + POS
Wi-Fi
POS
6
RS 232
3
4
SERIE
USB
DB9
ESCÁNER
CAJA
GPRS / IP
5
PAD
RJ 45
Wi-Fi
AC
2
1
4
FUENTE
CA
Ethernet/NETV/GPRS
Opcional/conexión Bluetooth
Opcional/conexión inalámbrica
Conexión por cable
1
Cable de energía
2
Cable UTP
3
Serie RJ11
Cable DB9
4
WI-FI
Conexión opcional
5
Caja todo en uno & PAD & escáner
GPRS/IP
6
EFT-POS

Fig. 4