(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 381 293**

(21) Número de solicitud: 200901024

(51) Int. CI.:
H04W 12/00 (2009.01)
H04L 9/32 (2006.01)
G06Q 30/00 (2012.01)

(12) PATENTE DE INVENCIÓN B1

(22) Fecha de presentación: **20.04.2009**

(43) Fecha de publicación de la solicitud: **24.05.2012**

Fecha de la concesión: **25.10.2012**

Fecha de modificación de las reivindicaciones: **05.10.2012**

(45) Fecha de anuncio de la concesión: **07.11.2012**

(45) Fecha de publicación del folleto de la patente: **07.11.2012**

(73) Titular/es:
ALTER CORE, S.L. (100.0%)
LUIS DE SALAZAR 12
28001 MADRID, ES

(72) Inventor/es:
PÉREZ SORIA, José María

(74) Agente/Representante:
CARVAJAL Y URQUIJO, Isabel

(54) Título: **SISTEMA Y MÉTODO DE ACREDITACIÓN PERSONAL MEDIANTE DISPOSITIVO MÓVIL.**

(57) Resumen:
Sistema y método de acreditación personal ante un proveedor de servicio mediante dispositivo móvil. El método comprende:
- proporcionar al usuario del dispositivo móvil (2) un código bidimensional (1), la información contenida en dicho código bidimensional (1) incluyendo datos originales cifrados que comprenden una clave de sesión cifrada para efectuar la acreditación del usuario ante el proveedor de servicio;
- obtener el dispositivo móvil (2), a través de medios de captura de imagen, una imagen con el código bidimensional (1)
- obtener el dispositivo móvil (2) a partir de dicha imagen el código bidimensional (1);
- convertir el código bidimensional (1) a un código de caracteres;
- obtener el dispositivo móvil (2), a partir de dicho código de caracteres y aplicando un proceso de descifrado, los datos originales incluyendo la clave de sesión para efectuar la acreditación del usuario ante el proveedor del servicio.

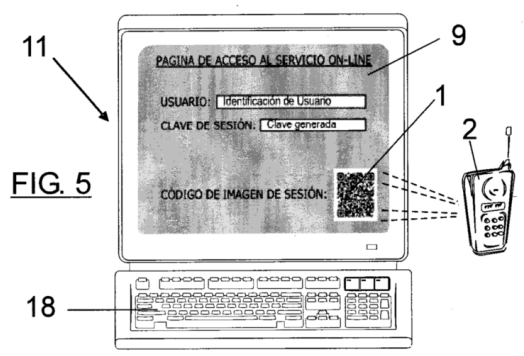


FIG. 5

ES 2 381 293 B1

DESCRIPCION

Sistema y método de acreditación personal mediante dispositivo móvil

Campo de la invención

La presente invención se engloba dentro del campo de los sistemas de acreditación personal empleando dispositivos móviles (por ejemplo, teléfonos móviles).

Antecedentes de la invención

En la actualidad, con las tecnologías aplicadas a los dispositivos móviles, aparte de utilizar los servicios básicos de telefonía y datos, se pueden disponer de otros servicios que nos pueden facilitar la realización de servicios de valor añadido. En la actualidad se vienen utilizando pictogramas o códigos bidimensionales para la realización de la decodificación de información relativa, principalmente, a direcciones de páginas web. Es decir, los códigos bidimensionales solamente ofrecen información codificada de texto a pictograma con el objeto de utilizar las cámaras de fotos de los dispositivos móviles para la captura de dicha información y su posterior decodificación y conversión a texto plano que posteriormente podrá ser tratado automáticamente por el dispositivo móvil para el acceso local (base de datos) o remoto (página web) a la información por referencia de dicho texto. Sin embargo, en ningún caso se ha aplicado para realizar funciones de autenticación.

La presente invención propone utilizar dispositivos móviles dotados con cámara de fotos para la realización de funciones de autenticación de datos a través del tratamiento de los fotogramas de los pictogramas o códigos bidimensionales de dichos datos.

Descripción de la invención

La invención se refiere a un método de acreditación personal ante un proveedor de servicio mediante dispositivo móvil de acuerdo con la reivindicación 1 y un sistema de acuerdo con la reivindicación 9. Realizaciones preferidas del sistema y del método se definen en las reivindicaciones dependientes.

El dispositivo móvil debe disponer de medios de captura de imagen. El método comprende:

- proporcionar al usuario del dispositivo móvil un código bidimensional, la información contenida en dicho código bidimensional incluyendo datos originales cifrados que comprenden una clave de sesión cifrada para efectuar la acreditación del usuario ante el proveedor de servicio;

- obtener el dispositivo móvil, a través de los medios de captura de imagen, una imagen con el código bidimensional;

- obtener el dispositivo móvil a partir de dicha imagen el código bidimensional;

- convertir el código bidimensional a un código de caracteres;

- obtener el dispositivo móvil, a partir de dicho código de caracteres y aplicando un proceso de descifrado, los datos originales incluyendo la clave de sesión para efectuar la acreditación del usuario ante el proveedor del servicio.

En una realización preferida el código bidimensional es previamente generado por el proveedor del servicio aplicando un proceso de cifrado sobre los datos originales que comprenden la clave de sesión y posteriormente una conversión de los caracteres obtenidos a código bidimensional.

El que el código bidimensional es preferentemente de doble cifrado, cifrado con clave pública de usuario y con clave privada del proveedor del servicio, comprendiendo el proceso de descifrado:

- obtener, a partir del código de caracteres, los datos originales cifrados incluyendo la clave de sesión cifrada;

- descifrar los datos originales con la clave pública del proveedor del servicio;

- descifrar el resultado anterior con la clave privada del usuario del dispositivo móvil, obteniendo los datos originales incluyendo la clave de sesión.

El proceso de generación del código bidimensional es preferentemente efectuado por parte del proveedor del servicio y comprende:

- generar aleatoriamente una clave de sesión;

- cifrar los datos originales que incluyen dicha clave de sesión con la clave pública del usuario;

- cifrar el resultado con la clave privada del proveedor del servicio;

- efectuar una codificación bidimensional del resultado anterior, obteniendo el código bidimensional que incluye los datos originales cifrados que a su vez comprenden la clave de sesión cifrada.

El método puede comprender adicionalmente mostrar al usuario en la pantalla del dispositivo móvil la clave de sesión obtenida y opcionalmente introducir la clave de sesión obtenida en un terminal conectado al proveedor del servicio para obtener la acreditación.

En una realización preferente el método comprende adicionalmente:

- establecer el dispositivo móvil una conexión segura con un servidor del proveedor del servicio;

- enviar el dispositivo móvil información para la acreditación del usuario, incluyendo en dicha información al menos la clave de sesión obtenida.

El proceso de descifrado puede ser también efectuado por una tarjeta criptográfica conectada al dispositivo móvil.

Los datos originales cifrados contenidos en el código bidimensional pueden comprender adicionalmente alguno de los siguientes datos:

- referencia del servicio o producto
- referencia del proveedor del servicio
- importe de la operación;
- fecha y hora de la operación;
- dirección web del proveedor del servicio.

Es objeto también de la presente invención un sistema de acreditación personal ante un proveedor de servicio mediante dispositivo móvil, disponiendo el dispositivo móvil de medios de captura de imagen. El sistema comprende dicho dispositivo móvil configurado para:

- obtener, a través de los medios de captura de imagen y a partir de un código bidimensional proporcionado al usuario del dispositivo móvil y que incluye datos originales cifrados que comprenden una clave de sesión cifrada para efectuar la acreditación del usuario ante el proveedor de servicio, una imagen que contiene dicho código bidimensional;
- obtener a partir de dicha imagen el código bidimensional;
- convertir el código bidimensional a un código de caracteres;
- obtener, a partir de dicho código de caracteres y aplicando un proceso de descifrado, los datos originales incluyendo la clave de sesión para efectuar la acreditación del usuario ante el proveedor del servicio.

El sistema puede comprender adicionalmente un servidor del proveedor del servicio configurado para generar el código bidimensional mediante un proceso de cifrado sobre los datos originales que comprenden la clave de sesión y una conversión de los caracteres obtenidos a código bidimensional.

El código bidimensional es preferentemente de doble cifrado, cifrado con clave pública de usuario y con clave privada del proveedor del servicio, estando el dispositivo móvil configurado, dentro del proceso de descifrado, para:

- obtener, a partir del código de caracteres, los datos originales cifrados incluyendo la clave de sesión cifrada;
- descifrar los datos originales con la clave pública del proveedor del servicio;

- descifrar el resultado anterior con la clave privada del usuario del dispositivo móvil, obteniendo los datos originales incluyendo la clave de sesión.

El servidor del proveedor del servicio está preferiblemente configurado, dentro del proceso de generación del código bidimensional, para:

- generar aleatoriamente una clave de sesión;
- cifrar los datos originales que incluyen dicha clave de sesión con la clave pública del usuario;
- cifrar el resultado con la clave privada del proveedor del servicio;
- efectuar una codificación bidimensional del resultado anterior, obteniendo el código bidimensional que incluye los datos originales cifrados que a su vez comprenden la clave de sesión cifrada.

El sistema puede comprender un terminal conectado al servidor del proveedor del servicio, con medios de visualización configurados para mostrar al usuario el código bidimensional y con medios de introducción de datos configurados para permitir la introducción de la clave de sesión para obtener la acreditación del usuario.

El dispositivo móvil puede estar configurado adicionalmente para:

- establecer una conexión segura con un servidor del proveedor del servicio;
- enviar información para la acreditación del usuario, incluyendo en dicha información al menos la clave de sesión obtenida.

El dispositivo móvil puede estar asimismo configurado para efectuar el proceso de descifrado mediante una tarjeta criptográfica conectada al dispositivo móvil.

Breve descripción de los dibujos

A continuación se pasa a describir de manera muy breve una serie de dibujos que ayudan a comprender mejor la invención y que se relacionan expresamente con una realización de dicha invención que se presenta como un ejemplo no limitativo de ésta.

La Figura 1 muestra el proceso de obtención de código bidimensional utilizando datos con doble cifrado.

La Figura 2 representa el proceso de obtención de datos a partir de código bidimensional con doble cifrado.

La Figura 3 representa el esquema de generación en el servidor del proveedor del código bidimensional de clave dinámica de sesión con doble cifrado.

La Figura 4 muestra un ejemplo de pantalla de acceso al servicio de proveedor on-line mediante clave dinámica de sesión.

La Figura 5 muestra el acceso a servicio de proveedor on-line mediante clave dinámica de sesión, en concreto la captura del código bidimensional por parte del dispositivo móvil.

La Figura 6 representa un esquema de obtención en el dispositivo móvil de la clave dinámica de sesión a partir de código bidimensional.

Las Figuras 7A, 7B y 7C muestran la operativa de acreditación por presentación de clave.

Las Figuras 8A y 8B muestran la operativa de acreditación con conexión móvil-servidor.

Las Figuras 9A y 9B muestran la operativa de acreditación utilizando el DNI electrónico.

Las Figura 10 muestra el servicio de pago presencial con presentación de código bidimensional en el terminal punto de venta.

LA Figura 11 muestra el servicio de pago presencial con código bidimensional en recibo de compra.

La Figura 12 representa el servicio de pago de facturación electrónica con código bidimensional en pantalla.

La Figura 13 muestra un servicio de pago de facturación con código bidimensional en factura de papel.

La Figura 14 muestra un servicio de control de accesos con código bidimensional en dispositivo de acceso.

La Figura 15 muestra el acceso a servicios en cajero automático con acreditación personal utilizando clave dinámica de sesión generada por el dispositivo móvil.

Descripción de una realización preferida de la invención

El sistema y método que se propone consiste en la utilización de pictogramas o códigos bidimensionales codificados en forma de representación visual de la información pero cuyo contenido no son textos planos, sino información cifrada utilizando criptografía de clave pública o asimétrica (ej. RSA); es decir, permite cifrar la información con una clave y ser descifrada con otra diferente, pareja de la anterior (pareja de claves privada/pública).

Para la aplicación del método y sistema propuesto se puede utilizar cualquier tipo de representación visual de datos o información, incluyendo los códigos

bidimensionales, códigos de barras bidimensionales o cualquier tipo de pictograma que pueda ser capturada y decodificado por un dispositivo digital móvil.

Los códigos bidimensionales son símbolos formados por una matriz de datos que permite el escaneo rápido de la información que contiene. Pueden ser reconocidos e interpretados por dispositivos digitales de captura de imagen y posteriormente utilizados para diferentes aplicaciones.

Hay múltiples tipos de códigos bidimensionales: Datamatrix, QR codes, Semacodes, Shotcodes, Bidi codes, Beetag, etc.

La cantidad máxima de información (caracteres) que pueden contener los códigos bidimensionales dependen del tamaño del código y de su nivel de redundancia.

La combinación de los pictogramas o códigos bidimensionales con la criptografía de clave pública supone una doble codificación: en primer lugar se codifica la información utilizando los procedimientos criptográficos de clave pública realizando un doble cifrado (cifrado con clave pública de usuario y con clave privada de proveedor) y, a continuación, se codifica el resultado para la obtención de un código bidimensional.

Es decir, para la realización de la codificación de la información con doble cifrado, se deberán realizar los siguientes pasos, tal como se muestra en la **Figura 1**:

- Tomar los datos originales y realizar el cifrado con la clave pública del usuario.

- Cifrar el resultado con la clave privada del proveedor del servicio.

- Realizar la codificación bidimensional del resultado, obteniendo un código bidimensional 1.

Para obtener la información cifrada, se deberán realizar los siguientes pasos, tal como se muestra en la **Figura 2**:

- El primer paso consiste en la decodificación visual del código bidimensional 1 para convertirlo en código de caracteres (por ejemplo, código hexadecimal, alfanumérico, ASCII, etc.).

- El resultado será descifrado con la clave pública del proveedor del servicio.

- Los datos originales, que solamente serán conocidos por el proveedor del servicio y por el usuario, serán la consecuencia de descifrar el resultado anterior con la clave privada del usuario.

De esta manera, se realiza un doble cifrado que garantiza la autenticación mutua entre el proveedor del servicio y el usuario del mismo, garantizándose la

seguridad de extremo a extremo del sistema de acreditación (de aplicación tanto para servicios presenciales como para servicios remotos o mixtos)

Existen distintos ejemplos de aplicaciones del sistema objeto de la invención:

1. Sistema de acreditación de usuarios para accesos seguros a servicios on-line.

2. Sistema de acreditación de usuarios para servicios de pagos presenciales.

3. Sistema de acreditación de usuarios para la facturación.

4. Sistema de acreditación de usuarios para controles de accesos presenciales.

5. Sistema de acreditación de usuarios para realizar operaciones en cajeros automáticos.

6. Sistema de acreditación de usuarios para pagos de recibos de servicios, entradas de espectáculos, multas, tasas, impuestos, etc.

1. Sistema de acreditación de usuarios para accesos seguros a servicios on-line.

Los servicios on-line ofrecidos a través de redes abiertas como Internet adolecen del problema de la autenticación de los usuarios que acceden a dichos servicios. La mayoría de los sistemas utilizados (por ejemplo banca electrónica) realizar la identificación de los usuarios se fundamentan en solicitar a los mismos ciertos datos que solamente deberían ser conocidos por el propio usuario y por el proveedor del servicio. Este es el caso de solicitar los datos relativos a la identificación de usuario y una palabra clave de acceso o clave secreta.

Sin embargo, de acuerdo con las actuales normativas que regulan el uso de las firmas electrónicas (en España, la Ley 59/2003 de Firma Electrónica), existe la posibilidad de retrocesión de cualquier operación on-line que no utilice la firma electrónica reconocida, como método de autenticación de la transacción. Esto quiere decir que aquellas operaciones que utilicen métodos de identificación de usuarios basado en datos relacionados con palabras secretas o passwords pueden ser repudiadas por los usuarios que aseguren no haberlas realizado. En caso de disputa, judicialmente, la carga de la prueba de la realización efectiva de la transacción, deberá ser realizada por el proveedor del servicio.

En el caso de utilización de autenticación basada en el uso de la firma electrónica reconocida para la realización de operaciones on-line, de acuerdo con la Ley de Firma Electrónica, la transacción se presume realizada por el usuario firmante, a no ser que dicho usuario demuestre fehacientemente que no ha realizado la operación. Es decir, en caso de disputa, judicialmente, la carga de la prueba de

repudio de la transacción, deberá ser aportada por el usuario del servicio. Por otra parte, existe una creciente tendencia de fraude utilizando técnicas de usurpación de la identidad (phishing).

El sistema consiste en la utilización de un modelo de autenticación robusta basado en la criptografía de clave pública y, en concreto, en la utilización del doble cifrado como método de acreditación del usuario para la realización de operaciones online.

Es decir, para la generación del código bidimensional de la clave de sesión de doble cifrado se propone la realización de un primer cifrado de los datos únicos de sesión (comprendiendo al menos un número aleatorio como clave única de sesión, y pudiendo comprender la dirección de la página web para evitar las técnicas de usurpación de identidad -phishing-, la fecha y la hora para controlar el tiempo de validez de la operación y su prescripción por time-out, por seguridad) con la clave pública del usuario y a continuación, la realización de un segundo cifrado del resultado de la operación anterior, con la clave privada del proveedor del servicio. Este resultado será codificado para la obtención del código bidimensional que incluye la clave de sesión de doble cifrado.

La generación del código bidimensional de clave dinámica de sesión requiere la realización de un doble cifrado de los datos (incluyendo el número aleatorio o clave de sesión) con criptografía de clave pública previamente a la realización de la codificación del código bidimensional. El diagrama de bloques del sistema de acreditación propuesto para la generación del código bidimensional es el representado en la **Figura 3**.

En la página de acreditación del usuario el proveedor del servicio presentará, en forma de código bidimensional 1, la clave dinámica de sesión doblemente cifrada para la acreditación en el sistema, según se muestra en la **Figura 4**,por ejemplo a través del monitor 9 de un ordenador 11.

La obtención de la clave dinámica de sesión requiere la captura del código bidimensional 1 por la cámara da fotos del dispositivo móvil 2, según se representa en la **Figura 5**, realización de la decodificación del código bidimensional 1 previamente al doble descifrado con criptografía de clave pública de los datos conteniendo dicha clave de sesión, tal como se puede observar en la **Figura 6**. El certificado digital del proveedor del servicio de la Figura 6, al igual que el certificado digital del usuario de la Figura 3, tienen la función de acreditar la veracidad de las claves públicas por parte de

una tercera parte confiable en el contexto de un Sistema de PKI (Public Key Infrastructure).

Aparte de la clave de sesión como información básica, los datos cifrados en el código bidimensional 1 podrán contener cierta información adicional que complemente el modelo de seguridad del sistema propuesto, como:

- Número aleatorio (clave de sesión), generado por el servidor.
- Dirección de página web del proveedor del servicio
- Fecha de la transacción (sello de tiempo para control de time-out)
- Hora de la transacción (sello de tiempo para control de time-out)
- Otros datos (ej.: importe de la transacción, datos de usuario, etc.)

La acreditación del usuario en el sistema se realiza mediante la presentación de la clave dinámica de sesión decodificada en pantalla y descifrada por el dispositivo móvil 2.

Los pasos a seguir para realizar la autenticación requerida para el acceso al servicio on-line, mostrados en las Figuras 7A, 7B y 7C, son los siguientes:

1. Introducir en el campo requerido la apropiada opción de identificación de usuario (**Figura 7A**):

a) Número de teléfono móvil

b) Número de Documento de Identidad Personal

c) Dirección de correo electrónico

d) Código de Usuario suministrado por el Proveedor del Servicio

e) Cualquier otro código de Identificación de Usuario

2. Realizar un fotograma mediante el teléfono móvil 2 del código bidimensional 1 de sesión recibido del servidor del proveedor del servicio (**Figura 7B**). La aplicación criptográfica instalada en el dispositivo móvil 2 se encarga de generar una clave única de sesión, que se muestra en pantalla.

3. Introducir la clave de sesión generada por la aplicación del teléfono móvil, en el campo requerido (**Figura 7C**) en la pantalla 9 del ordenador 11, por ejemplo a través de un teclado 18 conectado al ordenador.

La acreditación del usuario en el sistema se puede realizar también mediante conexión móvil-servidor, esto es, mediante la transmisión de la información de la operación, incluyendo la clave dinámica de sesión decodificada y descifrada, desde el dispositivo móvil al servidor del proveedor del servicio a través de una conexión on-line.

Los pasos a seguir para realizar la autenticación requerida para el acceso al servicio on-line, son los siguientes, mostrados en las Figuras 8A y 8B:

1. Introducir en el campo requerido la apropiada opción de Identificación de Usuario (**Figura 8A**):

a) Número de teléfono móvil

b) Número de Documento de Identidad Personal

c) Dirección de correo electrónico

d) Código de Usuario suministrado por el Proveedor del Servicio

e) Cualquier otro código de Identificación de Usuario

2. Realizar un fotograma mediante el dispositivo móvil 2 del código bidimensional 1 de sesión recibido del servidor del proveedor del servicio. La aplicación ejecutada por el dispositivo desencadenará una conexión segura on-line con el servidor del proveedor del servicio, a quien enviará la información relativa a la operación de acreditación, incluyendo la clave única de sesión (**Figura 8B**).

3. El servidor del proveedor del servicio verificará los datos recibidos del usuario a través de la conexión en tiempo real con su dispositivo móvil y, una vez realizada la autenticación de los mismos por el servidor, permitirá el acceso al servicio.

La acreditación del usuario en el sistema la realiza en los casos anteriormente descritos el dispositivo móvil 2 (en concreto la aplicación de acreditación), pero se puede realizar también utilizando una tarjeta criptográfica 3 externa al dispositivo, como por ejemplo el DNI electrónico (a través de la apropiada interfaz directa, cableada o inalámbrica de la tarjeta criptográfica 3 con el dispositivo móvil 2) para la gestión de claves y la ejecución de los procesos criptográficos, tal como se muestra en las **Figuras 9A** y **9B**, con el objeto de realizar la acreditación del usuario ante el proveedor del servicio, ya sea mediante la presentación de la clave dinámica de sesión, o por transmisión de la información de la operación, incluyendo la clave dinámica de sesión, desde el dispositivo móvil al servidor del proveedor del servicio.

Los pasos a seguir para realizar la autenticación requerida para el acceso al servicio on-line, son los siguientes:

1. Introducir en el campo requerido la apropiada opción de Identificación de Usuario (Figura 9A):

a) Número de teléfono móvil

b) Número de Documento de Identidad Personal

c) Dirección de correo electrónico

d) Código de Usuario suministrado por el Proveedor del Servicio

e) Cualquier otro código de Identificación de Usuario

2. Realizar un fotograma mediante el teléfono móvil 2 del código bidimensional 1 de sesión recibido del servidor del proveedor del servicio. La aplicación ejecutada por el dispositivo utiliza la gestión de claves y algoritmos criptográficos de la tarjeta criptográfica 3, y genera una clave única de sesión para su presentación al sistema o bien desencadena una conexión segura on-line con el servidor del proveedor del servicio, a quien enviará la información relativa a la operación de acreditación, incluyendo la clave única de sesión (Figura 9B).

3. Se introduce la clave de sesión generada por la aplicación del teléfono móvil 2 en el campo requerido o bien se transmite al servidor del proveedor del servicio los datos de la operación, incluida la clave de sesión, para su verificación en tiempo real.

2. Sistema de acreditación de usuarios para servicios de pagos presenciales

El sistema propuesto basado en la utilización de pictogramas o códigos bidimensionales también puede ser utilizado para efectuar la acreditación de los clientes de establecimientos con el objeto de realizar pagos electrónicos presenciales seguros.

Con el objeto de facilitar el pago electrónico presencial en el establecimiento, se habilitará el terminal punto de venta 4 (TPV) para mostrar el código dinámico bidimensional 1 ligado a la transacción de pago (incluyendo el importe, fecha y hora, número de establecimiento y código dinámico de doble cifrado emitido por la entidad financiera).

El cliente tomará un fotograma del código bidimensional 1 mostrado en la pantalla 5 del TPV 4 (**Figura 10**), o bien del recibo impreso 6 en el que figurará el pictograma (**Figura 11**), aparte de los pertinentes datos de la operación de compra (importe, fecha y hora, número de establecimiento, descripción de los artículos comprados, etc.).

A continuación, la aplicación de acreditación o de autenticación del dispositivo móvil 2 generará una clave de sesión para ser presentada por teclado 7 al TPV 4 o bien se conectará en tiempo real con el servidor de la entidad financiera para la resolución de la solicitud de autorización del pago.

La resolución de la solicitud de autorización del pago presencial será enviada al TPV 4 del establecimiento y, en el caso de que el dispositivo móvil se haya conectado al servidor de la entidad financiera el usuario recibirá también la resolución de la operación en el propio dispositivo móvil 2.

De igual manera, el modelo propuesto para el pago presencial es compatible con la utilización de la tarjeta criptográfica 3 (ej.: DNI electrónico) según se ha descrito anteriormente.

3. Sistema de acreditación de usuarios para la facturación

Otra aplicación de referencia del sistema propuesto consiste en la utilización del código bidimensional 1 con doble cifrado para la identificación inequívoca de una factura 8 y, de esta manera, poder permitir el pago automático de la misma, facilitando una conexión al sistema de banca electrónica del cliente utilizando el procedimiento descrito previamente para la acreditación de usuarios para accesos seguros a servicios on-line.

La factura puede ser visualizada tanto en pantalla de un terminal mostrado en la **Figura 12** (como por ejemplo un monitor 9 de un ordenador 11) como en papel impreso 10 (**Figura 13**), de forma que el código bidimensional con doble cifrado pueda ser capturado por el dispositivo móvil y, una vez ejecutada la aplicación de acreditación, se realice la presentación de la clave de sesión o bien sean enviado los datos relativos a la operación al servidor en tiempo real para su autorización.

De igual manera, el modelo propuesto para el pago de facturas será compatible con la utilización de la tarjeta criptográfica 3 (DNI electrónico), tal como se ha descrito anteriormente.

4. Sistema de acreditación de usuarios para controles de accesos presenciales

El sistema de utilización de códigos bidimensionales con doble cifrado puede ser utilizado para realizar la gestión del control de accesos físicos con la presentación de la clave dinámica, o bien con la transmisión de los datos de autenticación al sistema de gestión del control del acceso físico.

De manera similar a los pagos presenciales en el terminal punto de venta, se presenta en la pantalla 13 del terminal de acceso 12 el código bidimensional 1 ligado al acceso, que incluirá el código dinámico de doble cifrado emitido por la entidad se seguridad encargada del control de acceso. El usuario tomará una fotografía del código bidimensional 1 mostrado en la pantalla 13 (**Figura 14**). A continuación, la aplicación de acreditación o de autenticación del dispositivo móvil 2 generará una clave de sesión para ser presentada por teclado 14 al terminal de acceso 12 o bien se conectará en tiempo real con el servidor de la entidad de seguridad para la resolución de la solicitud de autorización del acceso, permitiendo o denegando el acceso.

De igual manera, el modelo propuesto para el control de accesos físicos, será compatible con la utilización de la tarjeta criptográfica 3 (DNI electrónico) según se ha descrito anteriormente.

5. Sistema de acreditación de usuarios para realizar operaciones en cajeros automáticos

Tal como se muestra en la **Figura 15**, el sistema descrito se puede utilizar como procedimiento de acreditación personal para realizar operaciones en cajeros automáticos 15, tales como reintegros de dinero, transferencias, recargas de tarjetas telefónicas, pagos de recibos, etc.

De forma similar al procedimiento utilizado para accesos seguros a servicios on-line, el código bidimensional 1 (entre cuyos datos figura una clave de sesión doblemente cifrada por la clave pública del usuario y la clave privada de la entidad financiera) generado por la entidad financiera será mostrado en la pantalla 16 del cajero automático 15. Dicho código bidimensional 1 será tratado por el dispositivo móvil 2 y, una vez decodificado el código bidimensional 2 y descifrados los datos utilizando la clave pública de la entidad financiera y la clave privada del usuario para obtener la clave de sesión, ésta será presentada directamente al cajero automático, por ejemplo mediante el teclado 17, o bien transmitida por conexión on-line desde el dispositivo móvil 2 a la entidad financiera, para su verificación y aceptación de la solicitud de acceso a los servicios a través del cajero automático.

El sistema de utilización de códigos bidimensionales con datos cifrados puede ser utilizado para acceder a servicios bancarios en cajeros automáticos con la presentación de la clave dinámica, o bien con la transmisión de los datos de autenticación al sistema de gestión del servidor de la entidad financiera.

Por otra parte, se podría utilizar los documentos impresos por el cajero automático para la acreditación del usuario y la realización de accesos a servicios, pagos, etc.

De igual manera, el modelo propuesto de acreditación personal para realizar operaciones en cajeros automáticos, será compatible con la utilización de de la tarjeta criptográfica 3 (ej.: DNI electrónico) según se ha descrito anteriormente.

6. Sistema de acreditación de usuarios para pagos de recibos de servicios, entradas de espectáculos, multas, tasas, impuestos, etc.

Otra aplicación de referencia del sistema propuesto consiste en la utilización del código bidimensional con doble cifrado para la identificación inequívoca de un recibo de servicios, entrada de espectáculo, multa, tasa, impuesto, o cualquier otro documento que esté relacionado con un pago.

De esta manera, se puede realizar el pago del importe asociado, bien por presentación de la clave de pago, generada por el dispositivo móvil 2, bien a través de una conexión on-line del dispositivo móvil al sistema de banca electrónica del cliente utilizando el procedimiento descrito previamente para la acreditación de usuarios para accesos seguros a servicios on-line.

El recibo o cualquier otro documento de pago puede ser visualizado tanto en pantalla como en papel impreso, de forma que el código bidimensional con doble cifrado pueda ser capturado por el dispositivo móvil y, una vez ejecutada la aplicación de acreditación, se realice la presentación de la clave de sesión o bien sean enviado los datos relativos a la operación al servidor en tiempo real para su autorización.

El método propuesto puede ser empleado para el pago de servicios, tasas, impuestos, etc. cuyo documento de pago esté emitido en papel. Simplemente se deberá incluir el código bidimensional ligado al pago, que incorpore, juntos con los datos de acreditación, entre otra información, la relativa a los datos requeridos para el pago, es decir: importe, fecha, hora, referencia de producto y referencia de proveedor o vendedor.

De esta manera, a través de la captura de la imagen del código bidimensional impreso en el papel, y su posterior tratamiento, se realizará la acreditación del usuario y se facilitará la conexión on-line con el proveedor del servicio y a través de los correspondientes sistemas de medios de pago, para la acreditación y posterior realización del pago del servicio o producto.

De igual manera, el modelo propuesto para el pago de recibos, será compatible con la utilización de de la tarjeta criptográfica 3 (ej.: DNI electrónico) según se ha descrito anteriormente.

REIVINDICACIONES

1. Método de autenticación personal ante un proveedor de servicio mediante dispositivo móvil, disponiendo dicho dispositivo móvil (2) de medios de captura de imagen, el método comprendiendo:

- proporcionar al usuario del dispositivo móvil (2) un código bidimensional (1);

- obtener el dispositivo móvil (2), a través de los medios de captura de imagen, una imagen con el código bidimensional (1);

- obtener el dispositivo móvil (2) a partir de dicha imagen el código bidimensional (1);

- convertir el código bidimensional (1) a un código de caracteres;

caracterizado por que la información contenida en dicho código bidimensional (1) incluyen datos originales cifrados que comprenden una clave de sesión dinámica cifrada para efectuar la autenticación del usuario ante el proveedor de servicio;

por que la información contenida en el código bidimensional (1) está cifrada mediante criptografía de clave pública;

y por que el método comprende adicionalmente:

- aplicar el dispositivo móvil (2) un proceso de descifrado sobre dicho código de caracteres para obtener la clave de sesión dinámica para efectuar la autenticación del usuario ante el proveedor del servicio.

2. Método según la reivindicación 1, **caracterizado porque** el código bidimensional (1) es previamente generado por el proveedor del servicio aplicando un proceso de cifrado sobre los datos originales que comprenden la clave de sesión dinámica y posteriormente una conversión de los caracteres obtenidos a código bidimensional.

3. Método según cualquiera de las reivindicaciones anteriores, en el que el código bidimensional (1) es de doble cifrado, cifrado con clave pública de usuario y con clave privada del proveedor del servicio, **caracterizado porque** el proceso de descifrado comprende:

- obtener, a partir del código de caracteres, los datos originales cifrados incluyendo la clave de sesión dinámica cifrada;

- descifrar los datos originales con la clave pública del proveedor del servicio;

- descifrar el resultado anterior con la clave privada del usuario del dispositivo

móvil (2), obteniendo los datos originales incluyendo la clave de sesión dinámica.

4. Método según la reivindicación anterior, **caracterizado porque** el proceso de generación del código bidimensional (1) es efectuado por parte del proveedor del servicio y comprende:

- generar aleatoriamente una clave de sesión dinámica;
- cifrar los datos originales que incluyen dicha clave de sesión dinámica con la clave pública del usuario;
- cifrar el resultado con la clave privada del proveedor del servicio;
- efectuar una codificación bidimensional del resultado anterior, obteniendo el código bidimensional (1) que incluye los datos originales cifrados que a su vez comprenden la clave de sesión dinámica cifrada.

5. Método según cualquiera de las reivindicaciones anteriores, **caracterizado porque** comprende adicionalmente:

- mostrar al usuario en la pantalla del dispositivo móvil (2) la clave de sesión dinámica obtenida,
- introducir la clave de sesión dinámica obtenida en un terminal (4,11,12,15) encargado de permitir la autenticación para el proveedor del servicio.

6. Método según cualquiera de las reivindicaciones anteriores, **caracterizado porque** comprende adicionalmente:

- establecer el dispositivo móvil (2) una conexión segura con un servidor del proveedor del servicio;
- enviar el dispositivo móvil (2) información para la autenticación del usuario, incluyendo en dicha información al menos la clave de sesión dinámica obtenida.

7. Método según cualquiera de las reivindicaciones anteriores, **caracterizado porque** el proceso de descifrado es efectuado por una tarjeta criptográfica (3) conectada al dispositivo móvil (2).

8. Método según cualquiera de las reivindicaciones anteriores, **caracterizado porque** los datos originales cifrados contenidos en el código bidimensional (1) comprenden adicionalmente alguno de los siguientes datos:

- referencia del servicio o producto;

- referencia del proveedor del servicio;
- importe de la operación;
- fecha y hora de la operación;
- dirección web del proveedor del servicio.

9. Sistema de autenticación personal ante un proveedor de servicio mediante dispositivo móvil, disponiendo el dispositivo móvil (2) de medios de captura de imagen, el sistema comprendiendo:

dicho dispositivo móvil (2) configurado para:

- obtener, a través de los medios de captura de imagen y a partir de un código bidimensional (1) proporcionado al usuario del dispositivo móvil (2), una imagen que contiene dicho código bidimensional (1);
- obtener a partir de dicha imagen el código bidimensional (1);
- convertir el código bidimensional (1) a un código de caracteres;

un servidor del proveedor del servicio configurado para generar el código bidimensional (1);**caracterizado por que** la información contenida en el código bidimensional (1) incluye datos originales cifrados que comprenden una clave de sesión dinámica cifrada para efectuar la autenticación del usuario ante el proveedor de servicio;

por que la información contenida en el código bidimensional (1) está cifrada mediante criptografía de clave pública;

y por que el dispositivo móvil (2) está adicionalmente configurado para:

- aplicar un proceso de descifrado sobre dicho código de caracteres para obtener la clave de sesión dinámica para efectuar la autenticación del usuario ante el proveedor del servicio.

10. Sistema según reivindicación 9, **caracterizado porque** el servidor del proveedor del servicio está configurado para generar el código bidimensional (1) mediante un proceso de cifrado sobre los datos originales que comprenden la clave de sesión dinámica y una conversión de los caracteres obtenidos a código bidimensional.

11. Sistema según cualquiera de las reivindicaciones 9-10, en el que el código bidimensional (1) es de doble cifrado, cifrado con clave pública de usuario y con clave privada del proveedor del servicio, **caracterizado porque** el dispositivo móvil está configurado, dentro del proceso de descifrado, para:

- obtener, a partir del código de caracteres, los datos originales cifrados incluyendo la clave de sesión dinámica cifrada;

- descifrar los datos originales con la clave pública del proveedor del servicio;

- descifrar el resultado anterior con la clave privada del usuario del dispositivo móvil (2), obteniendo los datos originales incluyendo la clave de sesión dinámica.

12. Sistema según las reivindicaciones 10 y 11, **caracterizado porque** el servidor del proveedor del servicio está configurado, dentro del proceso de generación del código bidimensional (1), para:

- generar aleatoriamente una clave de sesión dinámica;

- cifrar los datos originales que incluyen dicha clave de sesión dinámica con la clave pública del usuario;

- cifrar el resultado con la clave privada del proveedor del servicio;

- efectuar una codificación bidimensional del resultado anterior, obteniendo el código bidimensional (1) que incluye los datos originales cifrados que a su vez comprenden la clave de sesión dinámica cifrada.

13. Sistema según cualquiera de las reivindicaciones 10 ó 11-12 cuando dependen de la 10, **caracterizado porque** comprende un terminal (4,11,12,15) encargado de permitir la autenticación para el proveedor del servicio, con medios de visualización (5,9,13,16) configurados para mostrar al usuario el código bidimensional (1) y con medios de introducción de datos (7,14,17,18) configurados para permitir la introducción de la clave de sesión dinámica para obtener la autenticación del usuario.

14. Sistema según cualquiera de las reivindicaciones 10-13, **caracterizado porque** el dispositivo móvil (2) está configurado adicionalmente para:

- establecer una conexión segura con un servidor del proveedor del servicio;

- enviar información para la autenticación del usuario, incluyendo en dicha información al menos la clave de sesión dinámica obtenida.

15. Sistema según cualquiera de las reivindicaciones 10-14, **caracterizado porque** el dispositivo móvil (2) está configurado para efectuar el proceso de descifrado mediante una tarjeta criptográfica (3) conectada al dispositivo móvil (2).

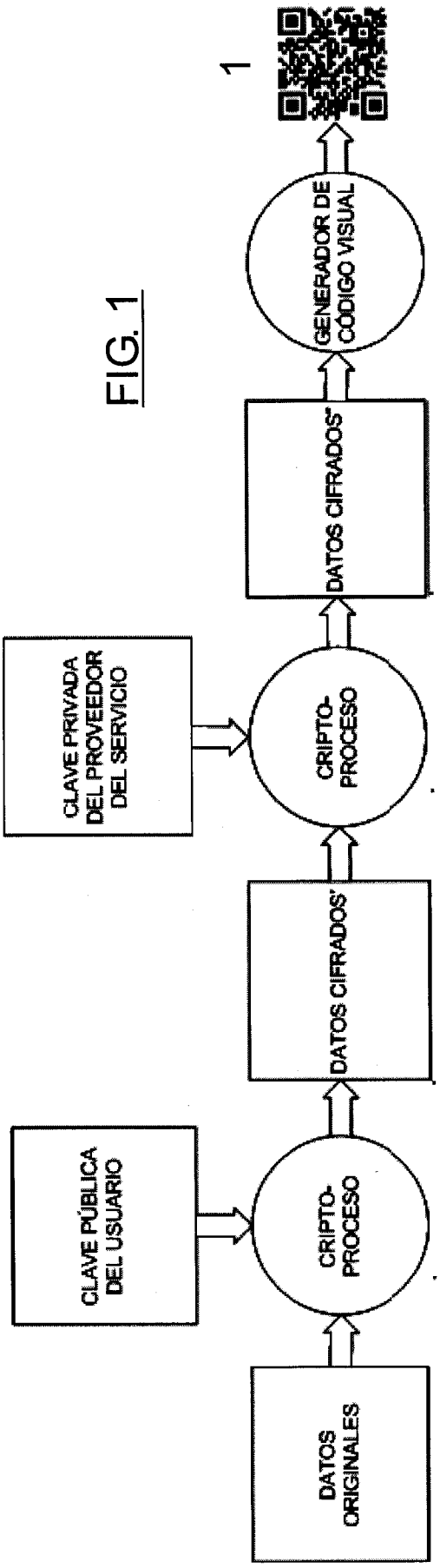

DATOS ORIGINALES
CLAVE PÚBLICA DEL USUARIO
CRIPTO-PROCESO
DATOS CIFRADOS'
CLAVE PRIVADA DEL PROVEEDOR DEL SERVICIO
CRIPTO-PROCESO
DATOS CIFRADOS"
GENERADOR DE CÓDIGO VISUAL
1

FIG. 1

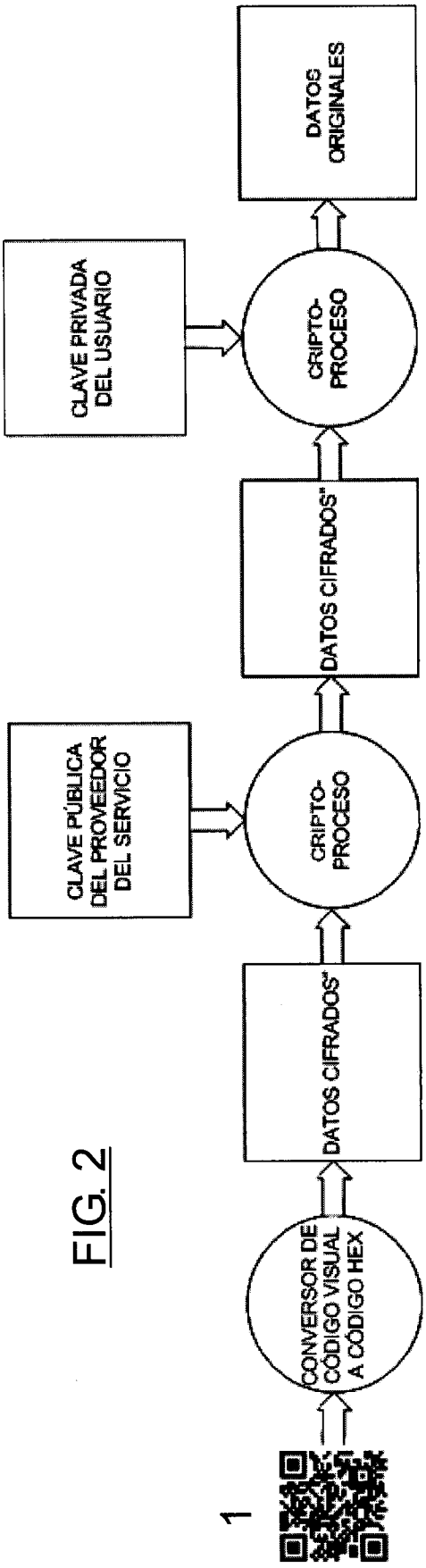

1
CONVERSOR DE CÓDIGO VISUAL A CÓDIGO HEX
DATOS CIFRADOS'
CLAVE PÚBLICA DEL PROVEEDOR DEL SERVICIO
CRIPTO-PROCESO
DATOS CIFRADOS"
CLAVE PRIVADA DEL USUARIO
CRIPTO-PROCESO
DATOS ORIGINALES

FIG. 2

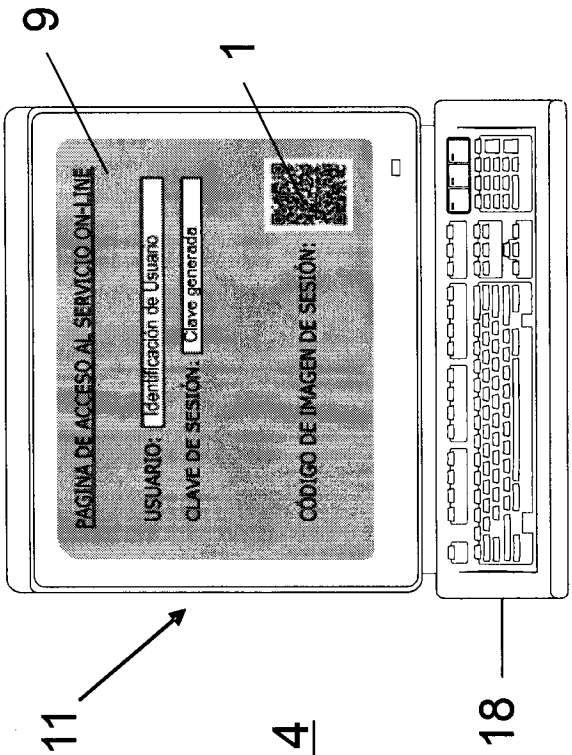

9
1
PÁGINA DE ACCESO AL SERVICIO ON-LINE
USUARIO: Identificación de Usuario
CLAVE DE SESIÓN: Clave generada
CÓDIGO DE IMAGEN DE SESIÓN:
11
18

FIG. 4

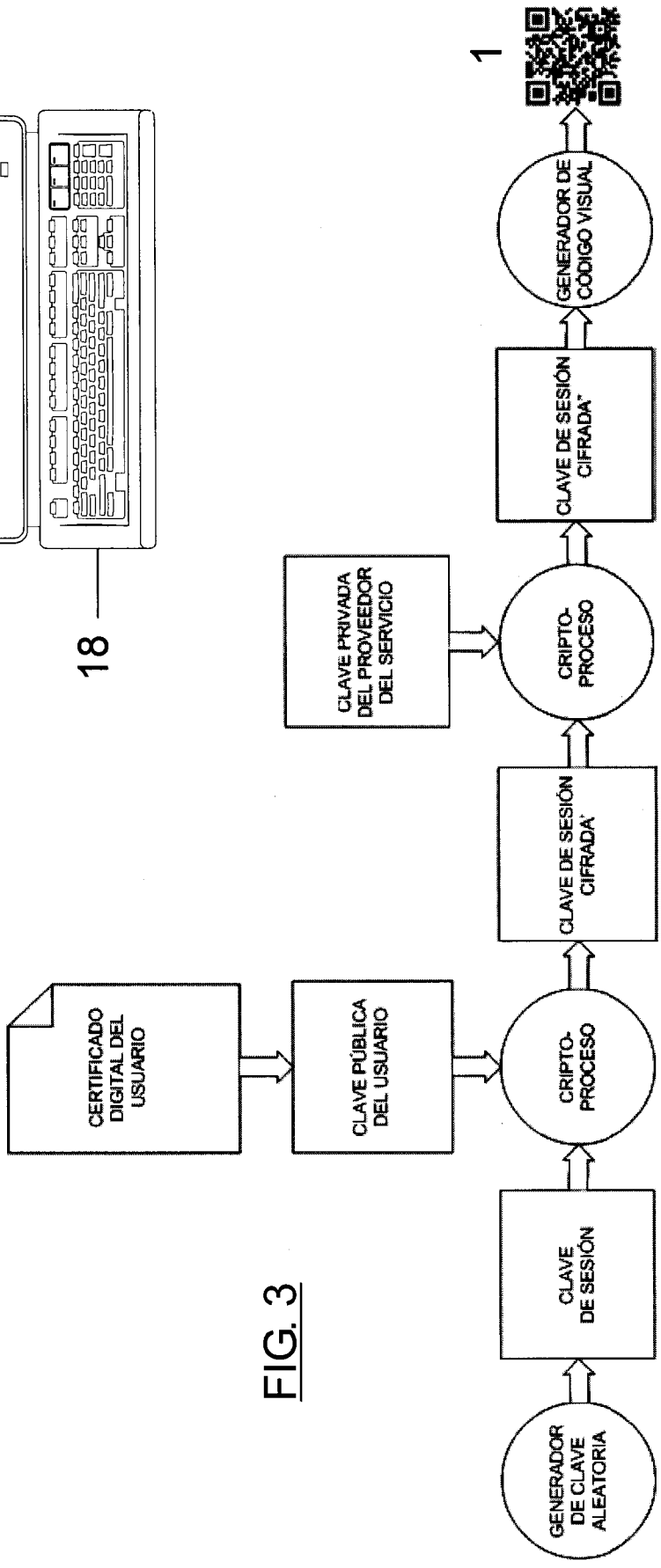

1
GENERADOR DE CÓDIGO VISUAL
CLAVE DE SESIÓN CIFRADA'
CRIPTO-PROCESO
CLAVE PRIVADA DEL PROVEEDOR DEL SERVICIO
CLAVE DE SESIÓN CIFRADA'
CRIPTO-PROCESO
CERTIFICADO DIGITAL DEL USUARIO
CLAVE PÚBLICA DEL USUARIO
CLAVE DE SESIÓN
GENERADOR DE CLAVE ALEATORIA

FIG. 3

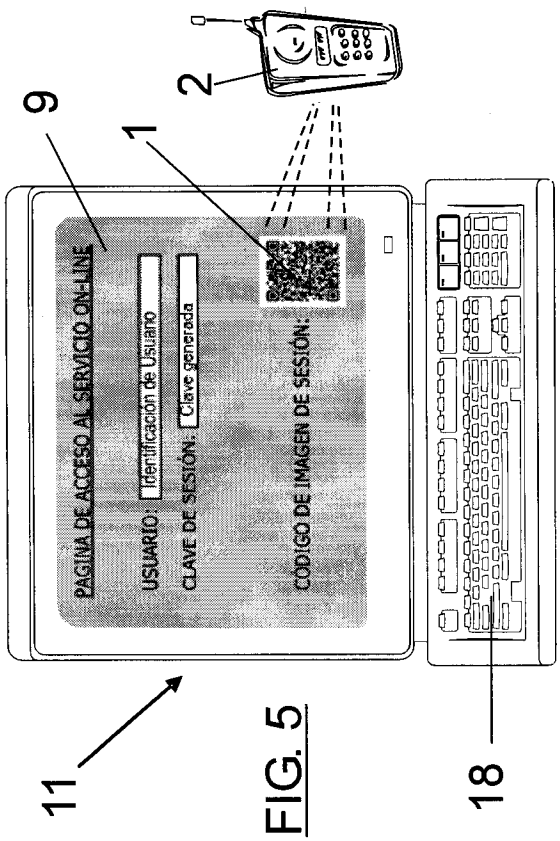

PÁGINA DE ACCESO AL SERVICIO ON-LINE
USUARIO: Identificación de Usuario
CLAVE DE SESIÓN: Clave generada
CÓDIGO DE IMAGEN DE SESIÓN:
9
1
2
11
18

FIG. 5

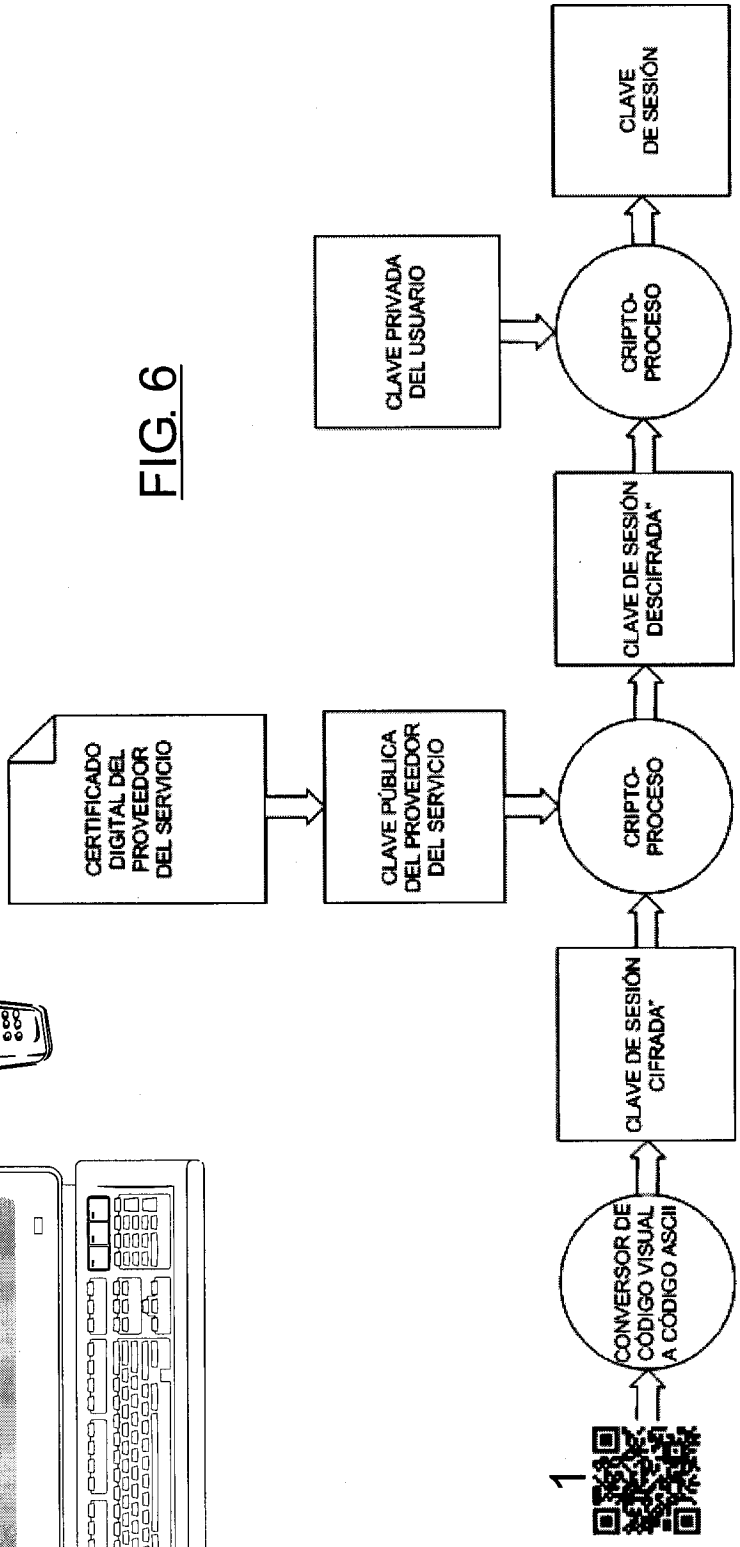

CERTIFICADO DIGITAL DEL PROVEEDOR DEL SERVICIO
CLAVE PÚBLICA DEL PROVEEDOR DEL SERVICIO
CLAVE PRIVADA DEL USUARIO
CRIPTO-PROCESO
CRIPTO-PROCESO
CONVERSOR DE CÓDIGO VISUAL A CÓDIGO ASCII
CLAVE DE SESIÓN CIFRADA"
CLAVE DE SESIÓN DESCIFRADA"
CLAVE DE SESIÓN
1

FIG. 6

PAGINA DE ACCESO AL SERVICIO ON-LINE

USUARIO: Identificación de Usuario

FIG. 7A

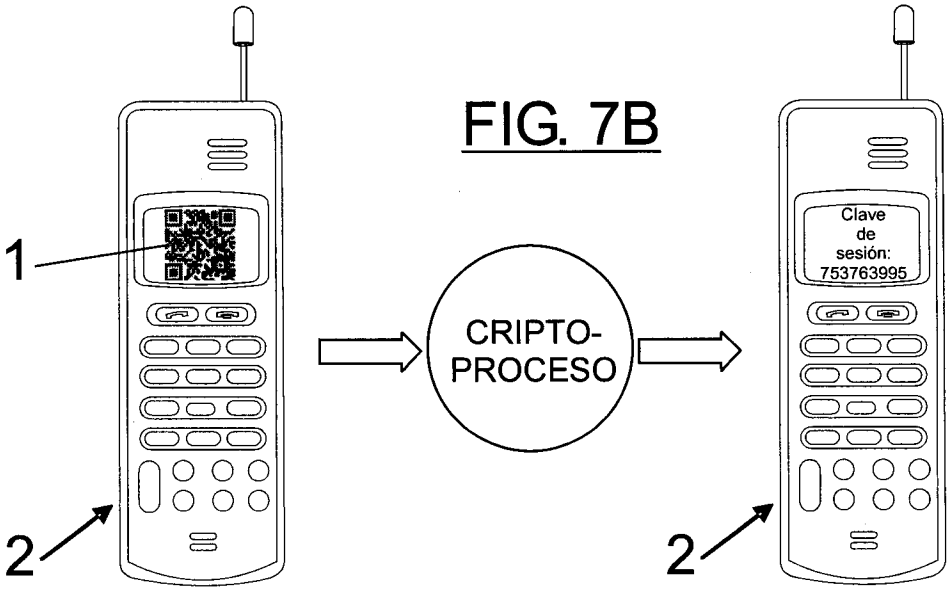


FIG. 7B

PAGINA DE ACCESO AL SERVICIO ON-LINE

USUARIO: Identificación de Usuario

CLAVE DE SESIÓN: Clave generada

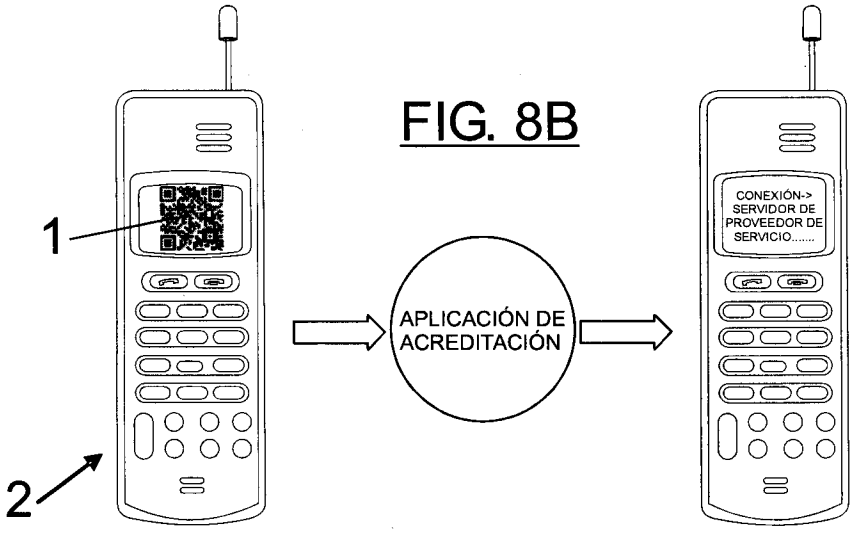
FIG. 7C

PAGINA DE ACCESO AL SERVICIO ON-LINE

USUARIO: Identificación de Usuario

FIG. 8A

FIG. 8B

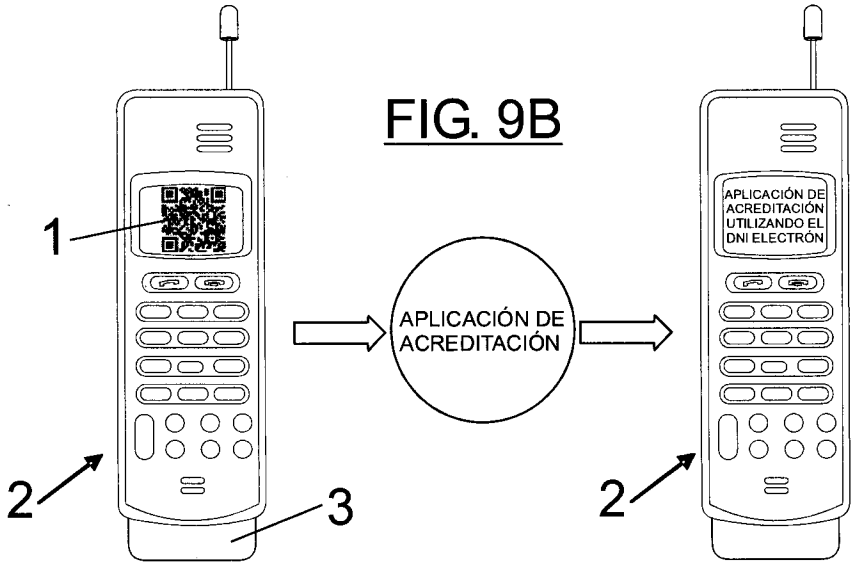


PAGINA DE ACCESO AL SERVICIO ON-LINE

USUARIO: Identificación de Usuario

FIG. 9A

FIG. 9B



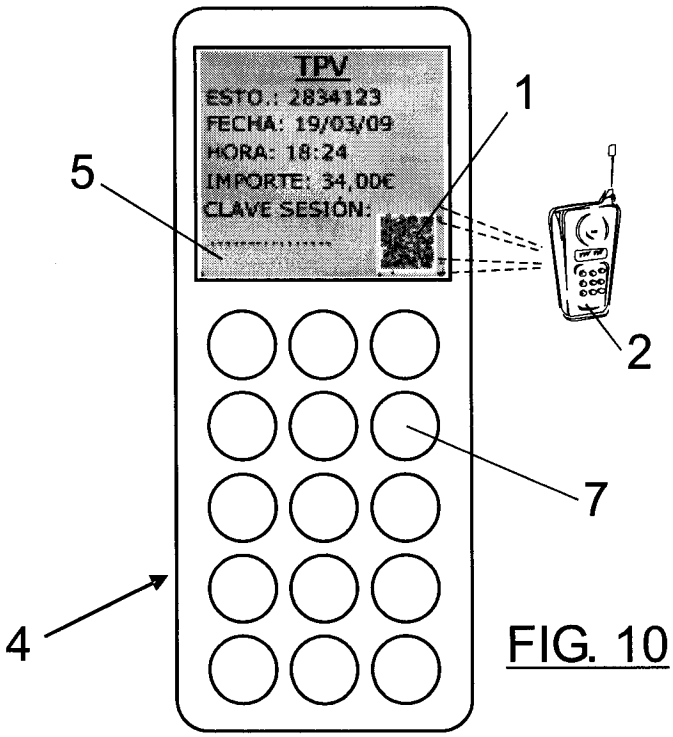

TPV
ESTO.: 2834123
FECHA: 19/03/09
HORA: 18:24
IMPORTE: 34,00€
CLAVE SESIÓN:
1
2
4
5
7

FIG. 10

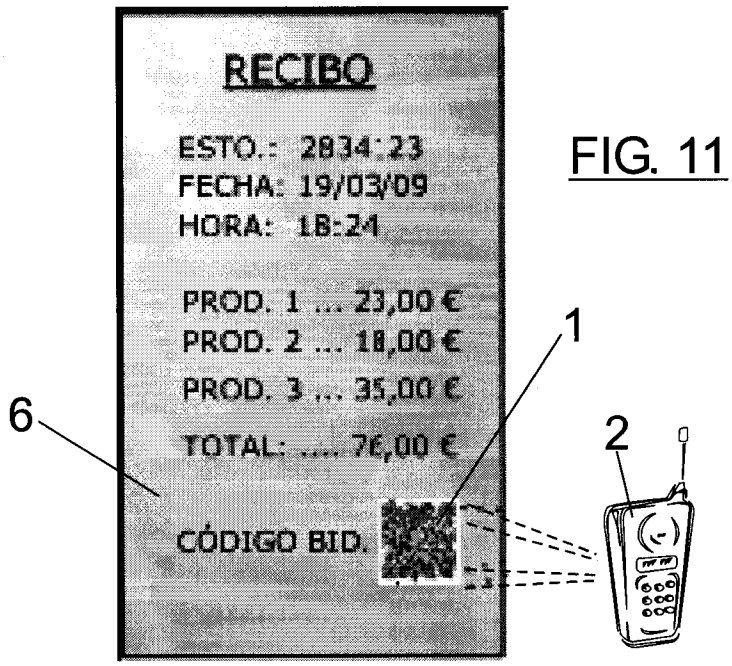

RECIBO
ESTO.: 2834123
FECHA: 19/03/09
HORA: 18:24
PROD. 1 ... 23,00 €
PROD. 2 ... 18,00 €
PROD. 3 ... 35,00 €
TOTAL: .... 76,00 €
CÓDIGO BID.
1
2
6

FIG. 11

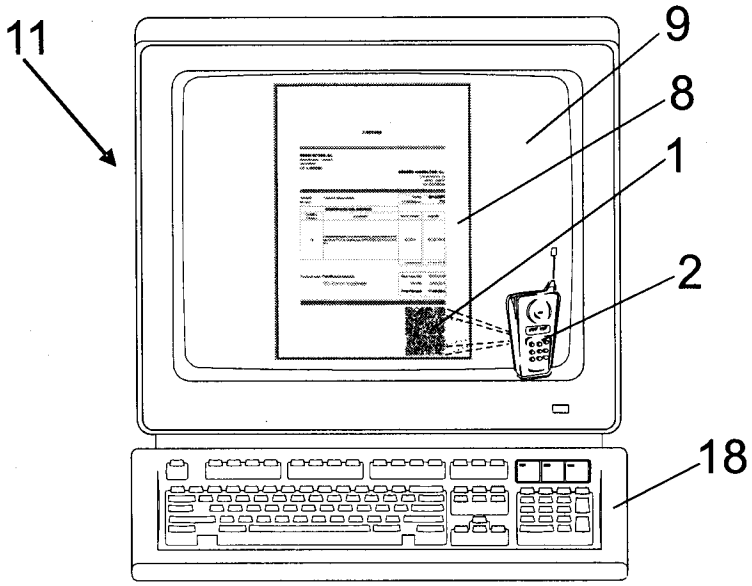


FIG. 12

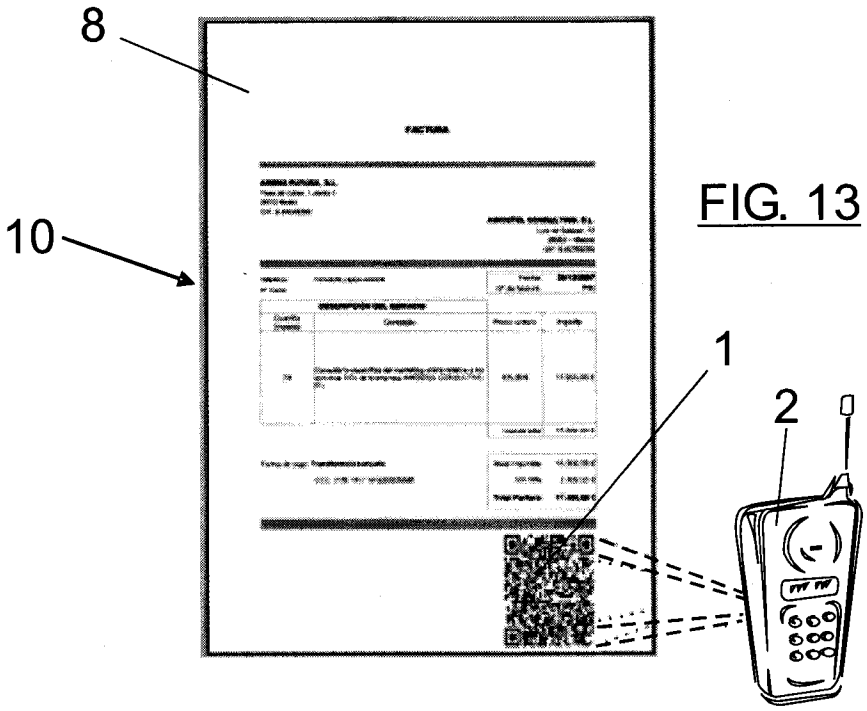


FIG. 13

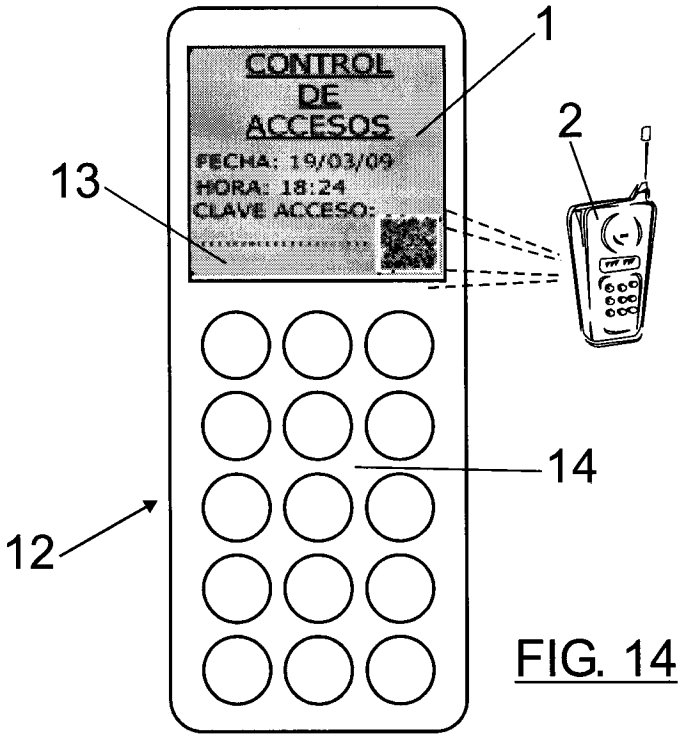

CONTROL
DE
ACCESOS
FECHA: 19/03/09
HORA: 18:24
CLAVE ACCESO:
1
2
13
14
12

FIG. 14

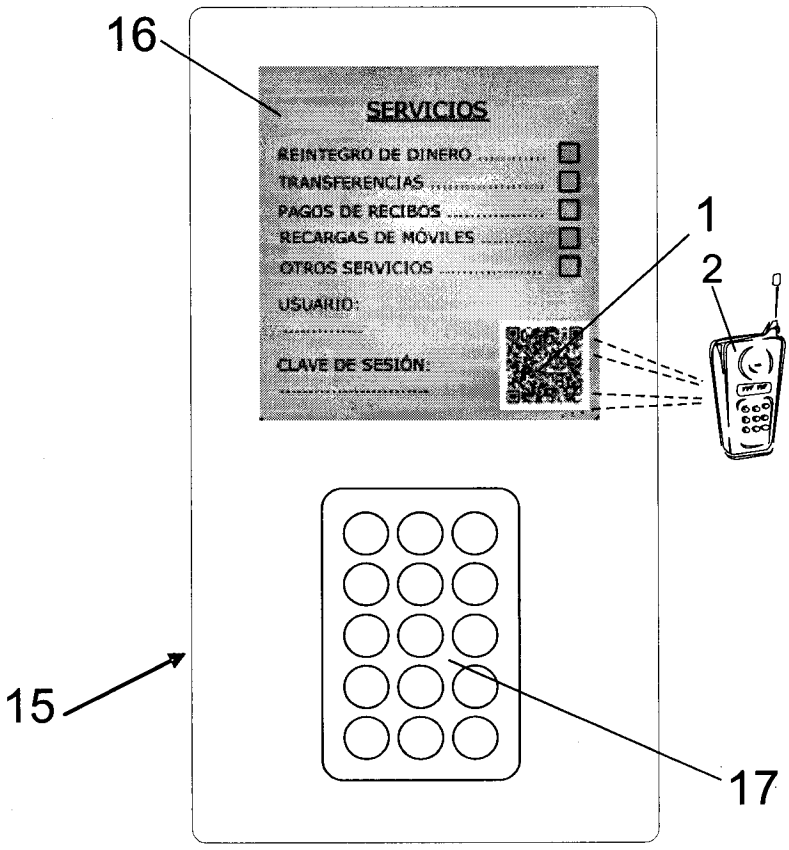

SERVICIOS
REINTEGRO DE DINERO
TRANSFERENCIAS
PAGOS DE RECIBOS
RECARGAS DE MÓVILES
OTROS SERVICIOS
USUARIO:
CLAVE DE SESIÓN:
16
1
2
15
17

FIG. 15

OFICINA ESPAÑOLA
DE PATENTES Y MARCAS

ESPAÑA

(21) N.º solicitud: 200901024

(22) Fecha de presentación de la solicitud: 20.04.2009

(32) Fecha de prioridad:

INFORME SOBRE EL ESTADO DE LA TECNICA

(51) **Int. Cl. :** Ver Hoja Adicional

DOCUMENTOS RELEVANTES

Categoría	(56) **Documentos citados**	**Reivindicaciones afectadas**
Y	US 2007174198 A1 (TOSHIBA KK) 26.07.2007, resumen; reivindicaciones; figuras.	1-15
Y	EP 0859341 A2 (NEOPOST LTD) 19.08.1998, página 2, columna 1, líneas 15-19.	1-15
A	GB 2434947 A (IDENTUM LTD) 08.08.2007	2-4,6

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**
02.04.2012	M. Muñoz Sanchez	1/4

CLASIFICACIÓN OBJETO DE LA SOLICITUD

H04W12/00 (2009.01)
H04L9/32 (2006.01)
G06Q30/00 (2012.01)

Documentación mínima buscada (sistema de clasificación seguido de los símbolos de clasificación)

H04W, H04L, G06Q

Bases de datos electrónicas consultadas durante la búsqueda (nombre de la base de datos y, si es posible, términos de búsqueda utilizados)

INVENES, EPODOC, WPI

Fecha de Realización de la Opinión Escrita: 02.04.2012

Declaración

Novedad (Art. 6.1 LP 11/1986)	Reivindicaciones	1-15	**SI**
	Reivindicaciones		**NO**
Actividad inventiva (Art. 8.1 LP11/1986)	Reivindicaciones		**SI**
	Reivindicaciones	1-15	**NO**

Se considera que la solicitud cumple con el requisito de aplicación industrial. Este requisito fue evaluado durante la fase de examen formal y técnico de la solicitud (Artículo 31.2 Ley 11/1986).

Base de la Opinión.-

La presente opinión se ha realizado sobre la base de la solicitud de patente tal y como se publica.

1. Documentos considerados.-

A continuación se relacionan los documentos pertenecientes al estado de la técnica tomados en consideración para la realización de esta opinión.

Documento	Número Publicación o Identificación	Fecha Publicación
D01	US 2007174198 A1 (TOSHIBA KK)	26.07.2007
D02	EP 0859341 A2 (NEOPOST LTD)	19.08.1998
D03	GB 2434947 A (IDENTUM LTD)	08.08.2007

2. Declaración motivada según los artículos 29.6 y 29.7 del Reglamento de ejecución de la Ley 11/1986, de 20 de marzo, de Patentes sobre la novedad y la actividad inventiva; citas y explicaciones en apoyo de esta declaración

Se considera D01 el documento del estado de la técnica más próximo al objeto de la invención.

Reivindicaciones independientes

Reivindicación 1: Siguiendo la redacción del documento de solicitud el documento D01 divulga un método de acreditación personal ante un proveedor de servicio para recibir de éste contenidos de pago. Dicha acreditación se realiza en los siguientes pasos:

- Se le proporciona al usuario un código bidimensional, incluyendo datos originales
- Se captura mediante un dispositivo móvil una imagen de dicho código
- Dicho código bidimensional se decodifica, se obtienen los datos originales para proceder a la autenticación y tras un resultado positivo de esta se ofrece el servicio a dicho usuario.

La diferencia entre el documento D01 y el documento de solicitud es la encriptación de los datos originales. Esta diferencia se recoge el documento D02.
Por tanto la combinación de D01 y D02 afecta a la actividad inventiva de la reivindicación 1 según el artículo 8.1 de la Ley de Patentes.
Reivindicación 9: La constitución de un sistema que implemente el método reivindicado se deriva de forma evidente para el experto en la materia a partir del método reivindicado.
Por tanto la combinación de D01 y D02 afecta a la actividad inventiva de la reivindicación 9 según el artículo 8.1 de la Ley de Patentes.

Reivindicaciones dependientes

Reivindicación 2-4: La encriptación con clave de proveedor (verificación de firmas) y con un esquema de clave privada-clave pública de usuario es evidente para el experto en la materia.
Reivindicaciones 5,7 y 8: Se trata de opciones de diseño.
Reivindicación 6: El establecimiento de una conexión segura usando una clave de sesión es ampliamente conocido.
Reivindicaciones: 10-15: Las características adicionales del sistema están en directa relación con las del método y por ello, de lo comentado anteriormente resultan evidentes para el experto en la materia.
Por tanto la combinación de D01 y D02 afecta a la actividad inventiva de las reivindicaciones 2-8 y 10-15 según el artículo 8.1 de la Ley de Patentes.