(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 606 602**

(51) Int. CI.:

H04L 9/28 (2006.01)
H04L 9/32 (2006.01)
G06F 21/36 (2013.01)
G06F 21/42 (2013.01)
H04L 29/06 (2006.01)
G06Q 20/32 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **02.08.2012 E 12382313 (0)**

(97) Fecha y número de publicación de la concesión europea: **05.10.2016 EP 2693687**

(54) Título: **Método para la generación de un código, método y sistema de autorización de una operación**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
24.03.2017

(73) Titular/es:

BANCO BILBAO VIZCAYA ARGENTARIA, S.A. (100.0%)
C/ Azul, 4, La Vela. Planta 13ª. Secretaria General
28050 Madrid, ES

(72) Inventor/es:

FERNÁNDEZ DE TORRES, FRANCISCO;
VILLA MARTÍNEZ, JOSÉ MANUEL;
UGUINA CARRIÓN, LUIS y
TARRIÑO ESCUDERO, ALEJANDRO

(74) Agente/Representante:

ARIAS SANZ, Juan

DESCRIPCIÓN

Método para la generación de un código, método y sistema de autorización de una operación.

Objeto de la invención

La presente invención está dirigida a un método para la generación de un código, y método que comprende la autorización de una operación llevada a cabo por un cliente sobre un primer servidor. En la autorización interviene un segundo servidor que genera un código de autorización de acuerdo a un método de codificación. Las operaciones pueden ser transacciones, acceso a una página web, pagos usuario a usuario, pagos usuario a comercio, pagos usuario a comercio online, retirada de dinero en cajeros, firmado de operaciones, etc.

Antecedentes de la invención

El desarrollo y el impacto social de los dispositivos móviles han impulsado el desarrollo de aplicaciones para móviles en el entorno comercial, tales como aquellas que efectúan transacciones comerciales.

Algunos dispositivos móviles incluyen aplicaciones software que permiten capturar códigos QR, o quick response codes. La aplicación captura el código, lo decodifica y transmite la información decodificada a un servidor remoto como solicitud de información de por ejemplo materiales, como una orden de compra, etc. Este tipo de operaciones son meramente intercambio de información y no incluyen ningún tipo de operación de transacción comercial.

PayPalTM es un sistema de pago unidireccional de solo texto con capacidad para ser instalado en dispositivos móviles. El sistema funciona de tal forma que se envía, desde el dispositivo móvil a un servidor, información acerca del pagador y la cantidad a ser pagada. Tras el envío de esta información un operario telefonea al usuario del dispositivo móvil para que el usuario autorice la transacción.

ObopayTM es una aplicación de dispositivo móvil cuyo uso permite la transacción desde una cuenta de ObopayTM hasta un comercio. El uso depende de software propietario instalado en el dispositivo, con el inconveniente de que no todos los dispositivos están preparados para ejecutar el software de ObopayTM.

Otras formas de pago usando dispositivos móviles comprenden el uso de códigos de barras, comunicación con el comerciante mediante tecnología sin cables, como Bluetooth o infrarrojos, etc. El principal inconveniente es el requisito de utilizar hardware y software adicional, tanto en el cliente como en el comerciante.

Sin embargo, no existen aplicaciones que permitan el intercambio de fondos de una manera rápida y cómoda para el usuario y que garantice al cien por cien la seguridad de dichas operaciones y transacciones. Por otra parte, lo expuesto en esta invención permite, además de realizar transacciones, la identificación y firmado de operaciones en canales alternativos que evitan los ataques habituales usando los medios comunes hasta ahora.

El documento EP 1 705 594 A2 describe un método y dispositivo para la determinación de los receptores y de la manipulación de una cuenta de usuario, para resolver el problema técnico de identificación de usuario.

El documento WO 2011/069492 A1 se refiere a un método para proporcionar una red, especialmente a cuentas de usuario en línea (cuentas en línea), estas cuentas siendo especialmente cuentas de usuario de acceso restringido que requieren autorización.

Descripción de la invención

La presente invención soluciona los problemas técnicos descritos anteriormente mediante un método para la generación de un código según la reivindicación 1, un método de autorización de una operación según la reivindicación 5, y un sistema para la autorización de una operación según la reivindicación 15. En las reivindicaciones dependientes se definen realizaciones preferidas de la invención.

En un primer aspecto inventivo se presenta un método para la generación de un código según la reivindicación 1.

Cifrar o encriptar debe entenderse en el contexto de la presente invención por su acepción convencional, esto es, aplicar un algoritmo de conversión de la información original en una información secreta. Un mensaje que es susceptible de ser cifrado, sufre al menos una transformación mediante una clave. El mensaje original es transformado, mediante la clave, en una cadena binaria. Para obtener el mensaje original, la entidad que descifra debe poseer la clave de descifrado.

Codificado o codificar debe entenderse en el contexto de la presente invención por su acepción convencional, esto es,

aplicar un algoritmo de representación de la información. Para representar una serie de símbolos binarios en un carácter se puede utilizar, por ejemplo, el sistema de codificación Base64, en el que se toman grupos de 6 bits y se forman caracteres. Gráficamente se ve de la siguiente manera:

000110101110010101110011… ➔

000110 101110 010101 110011…➔

G u V 5

El método para la generación de un código genera un código a partir de una cadena de caracteres de información de manera que es seguro en el sentido de que no contiene información sensible o vulnerable que pueda ser utilizada por un tercero que intercepte el código. Este código puede ser utilizado en un método de autorización de una operación como el descrito a continuación en el segundo aspecto inventivo.

En un segundo aspecto inventivo, la invención presenta un método de autorización de una operación implementado en un sistema que comprende,

- un cliente,
- un primer servidor,
- un segundo servidor, en comunicación con el primer servidor, y en comunicación con el cliente, caracterizado porque comprende las etapas de un método según la reivindicación 4.

Finalmente, la autorización la envía el cliente al segundo servidor quien puede ejecutar la operación.

En un tercer aspecto inventivo se presenta un sistema para la autorización de una operación que comprende las siguientes entidades,

-un cliente,

-un primer servidor, y

-un segundo servidor, en comunicación con el primer servidor, y en comunicación con el cliente,

caracterizado porque

-las tres entidades están adaptadas para implementar las etapas de un método según el segundo aspecto inventivo,

-el segundo servidor está adaptado para implementar las etapas de un método de generación de un código según el primer aspecto inventivo, y

-el cliente está adaptado para llevar a cabo la decodificación de un código generado mediante un método según el primer aspecto inventivo.

En un cuarto aspecto inventivo se presenta un programa de ordenador según la reivindicación 15.

En un quinto aspecto inventivo se presenta un producto de programa de ordenador según la reivindicación 16.

Todas las características y/o las etapas de métodos descritas en esta memoria (incluyendo las reivindicaciones, descripción y dibujos) pueden combinarse en cualquier combinación, exceptuando las combinaciones de tales características mutuamente excluyentes.

Descripción de los dibujos

Estas y otras características y ventajas de la invención, se pondrán más claramente de manifiesto a partir de la descripción detallada que sigue de una forma preferida de realización, dada únicamente a título de ejemplo ilustrativo y no limitativo, con referencia a las figuras que se acompañan.

Figura 1 Esta figura muestra un ejemplo de un diagrama de bloques que implementa las etapas de un método de autorización de una operación según la invención.

Figura 2 Esta figura muestra un ejemplo de realización de un diagrama de bloques que representa la implementación de un método de generación de código según la invención.

Figura 3 Muestra un ejemplo particular de realización de un método según la invención, en donde se muestra un ejemplo del método implementado por las tres entidades principales de la comunicación en una transacción sobre QR realizado desde un dispositivo móvil hasta otro dispositivo móvil.

Figura 4 Muestra un ejemplo particular de realización de un método según la invención, en donde se muestra un ejemplo del método implementado por las tres entidades principales de la comunicación en una transacción sobre QR realizado desde un dispositivo móvil cliente en un comercio físico con un primer servidor como un TPV o terminal de punto de venta.

Figura 5 Muestra un ejemplo particular de realización de un método según la invención, en donde se lleva a cabo una firma o autorización de operaciones en un canal alternativo, o fuera de banda.

Figura 6 Muestra un ejemplo particular de realización de un método según la invención, en donde se lleva a cabo la retirada de dinero de un cajero automático.

Figura 7 Muestra un ejemplo particular de realización de un método de generación de un código según la invención.

Exposición detallada de la invención

Método para la generación de un código

Como se puede apreciar en la figura 7, un método para la generación de un código (108) según la invención comprende las etapas:
a.- proveer una primera cadena de caracteres (101) de W caracteres,
b.- cifrar (110) la primera cadena de caracteres (101) mediante un método de cifrado, obteniendo una cadena cifrada (102),
c.- codificar (111) la primera cadena cifrada (102) mediante un método de codificación, obteniendo una cadena de Y caracteres (103) cifrada y codificada,
d.- dividir (112) la cadena de Y caracteres (103) en:
- una cadena pública de M caracteres (104), y
- una cadena privada de Y-M caracteres (105),
e.- concatenar (113) al menos:
- la cadena pública de M caracteres (104), e
- información adicional (106),
obteniendo una segunda cadena de caracteres (107),
f.- codificar (114) la segunda cadena de caracteres (107) con un método de codificación, obteniendo el código (108).

Los métodos de cifrado (etapa b) y codificación (etapa c) son métodos conocidos en el estado de la técnica.

El código es un conjunto de signos y de reglas que permite formular y comprender un mensaje. En el ámbito de la presente invención el mensaje es la cadena de caracteres (101) de W caracteres que se pretende codificar y el código puede ser un código bidimensional, un código de barras, un código hexadecimal, un código en forma de imagen, etc.

En una realización particular del método para la generación de un código (108), el método de codificación de la etapa f.- es un método de generación de un código QR (quick response code), que ventajosamente puede utilizarse para ser capturado mediante captura de imagen, por ejemplo escaneando, desde un dispositivo que comprende un sensor de imagen.

En una realización de un método para generar un código según la invención la información adicional en la etapa e.- comprende al menos:
-un identificador de base de datos (301) que indica una dirección de memoria de una unidad de almacenamiento donde se almacena la cadena privada de Y-M caracteres (105),
-un prefijo (302).

En una realización de la invención el método para la generación de un código comprende las siguientes etapas previas a la a.-:
-proveer una información (201), que preferentemente es información cifrada y codificada,
-decodificar y descifrar esta información si la información (201) es información cifrada y codificada,
-generar (210) un número aleatorio (202),
-concatenar (211) el número aleatorio a toda o parte de la información (201) provista, obteniéndose una cadena inicial (101).

La información puede ser proporcionada en una cadena de caracteres, un XML, etc…

La información (201) puede estar cifrada mediante un modo de cifrado CBC o cualquier otro modo de cifrado y puede estar codificada en Base32.

Al utilizar el modo de cifrado CBC, se obtiene un binario de bloques de 128 bits. Cuando posteriormente se codifica en Base32, se obtienen 25 caracteres por cada bloque de 128 bits.

Así, en una realización particular del método para la generación de un código según la invención en la etapa d.- relativa a la acción de dividir (112) la cadena de Y caracteres en una cadena pública de M caracteres y una cadena privada de Y-M caracteres, se escoge el número M = 26 que ventajosamente separa un bloque de 25 bits completo y algo más del resto de la cadena, lo que hace que la seguridad se incremente y no sea posible descifrar la información si no se

dispone de la parte pública y privada de la información. Si se tomase menos de un bloque completo, un tercero podría descodificar y descifrar la información.

Sistema para la generación de un código

En la figura 2 se muestra un ejemplo de realización de un sistema en diagrama de bloques que representa la implementación de un método de generación de código (108) según la invención. Estos bloques comprenden medios de procesamiento que están adaptados para implementar las etapas de un método para la generación de un código (108) según la invención.

Sistema para la autorización de una operación

Un sistema para la autorización de una operación según la invención comprende las siguientes entidades, representadas a modo de ejemplo en la figura 1:
-un cliente (1),
-un primer servidor (2), y
-un segundo servidor (3), en comunicación con el primer servidor (2), y en comunicación con el cliente (1),
caracterizado porque
-las tres entidades (1, 2, 3) están adaptados para implementar las etapas de un método según el segundo aspecto inventivo,
-el segundo servidor (3) está adaptado para implementar las etapas de un método de generación de un código (108) según el primer aspecto inventivo, y
-el cliente (1) está adaptado para llevar a cabo la decodificación de un código (108) generado mediante un método según el primer aspecto inventivo.

En un ejemplo particular el sistema está caracterizado porque el primer servidor (2) está en comunicación con el segundo servidor (3) a través de una primera red de comunicación (6) y el cliente (1) está en comunicación con el segundo servidor (3) a través de una segunda red de comunicación (7).

En un ejemplo particular el sistema está caracterizado porque el primer servidor (2) está en comunicación con el segundo servidor (3) a través de una primera red de comunicación (6) y el cliente (1) está en comunicación con el segundo servidor (3) a través de la misma primera red de comunicación (6).

Método de autorización de una operación
En la figura 1 se muestra una realización particular del método según la invención. Esta realización comprende las siguientes etapas:
a.- solicitar (401) un código (108) al segundo servidor (3), la solicitud comprendiendo una cadena con datos (4) de la operación,
b.- generar (402) un código (108) por parte del segundo servidor (3) a partir de una cadena con datos (4) de la operación según un método según el primer aspecto inventivo,
c.- enviar (403) el código (108) por parte del segundo servidor (3) al primer servidor (2),
d.- trasladar (404) el código (108), por parte del cliente (1) desde el primer servidor (2) hasta el cliente (1),
e.- decodificar (405) el código (108) por parte del cliente (1), obteniendo la segunda cadena de caracteres (107),
f.- finalizar (408) por parte del cliente (1) la autorización enviando una confirmación de autorización al segundo servidor (3),

En una realización particular, tras la etapa f.- se implementa la etapa g.- : ejecutar (409) la operación por parte del segundo servidor (3).

En un ejemplo de realización, en la etapa g.- la ejecución (409) de la operación se realiza si una clave de un solo uso (5) enviada desde el cliente (1) hasta el segundo servidor (3) es correcta donde una clave de un solo uso correcta (5) es una clave de un solo uso (5)
**conocida por el segundo servidor (3) y
**asociada a la operación a ejecutar.

En una realización particular la cadena con datos (4) de la operación es la cadena que se provee en la etapa a.- relativa a la acción de proveer una cadena de información (201), del método para la generación de un código según la invención.

En una realización particular de la invención el método de autorización comprende las etapas e1.- y e2.- entre las etapas e.- y f.-. Las etapas e1 y e2 comprendiendo:
e1.- solicitar (406) información de la operación por parte del cliente (1) al segundo servidor (3), y
e2.- proveer (407) la información de la operación por parte del segundo servidor (3).

Ventajosamente en este modo de realización particular se incrementa la seguridad del método al no enviar información vulnerable en el código (108) y recibiendo información relevante para llevar a cabo la operación sólo en el cliente (1).

En una realización particular, el método de generación de un código almacena la cadena privada de Y-M caracteres (105) que junto con la cadena pública de Y caracteres (104) representa información que permite al segundo servidor (3) obtener todos los datos necesarios de la operación tales que son suficientes para proveer (407) la información de la operación al cliente (1) para éste que finalice (408) la autorización de la operación.

Ventajosamente, el traslado (404) del código (108) por parte del cliente (1), desde el primer servidor (2) hasta el cliente (1), se implementa mediante la captura por parte del cliente (1), que puede ser una captura de imagen de un código (108) QR o captura mediante tecnología NFC de un código (108).

En una realización particular, la operación es una operación de transferencia bancaria desde una cuenta asociada al cliente (1) a una cuenta bancaria asociada al primer servidor (2). Ventajosamente en el ejemplo particular en el que las etapas e1 y e2 son implementadas, no es necesario enviar en el código (108) información relevante. De este modo es posible generar un código (108) que por sí solo no de información interpretable y de manera que la información relevante solo se envía al cliente (1) en la etapa e2.

En los ejemplos particulares de la invención el cliente (1), el primer servidor (2) y el segundo servidor (3) poseen las tablas de codificación y las claves de cifrado y descifrado evitando ser enviadas por un canal de comunicación.

En los ejemplos particulares que se exponen a continuación el cliente (1), puede ser uno cualquiera de una tableta, un robot, un ordenador, un smartphone, o cualquier otro dispositivo con capacidad de comunicación a través de una red de comunicación. En diferentes ejemplos el dispositivo está adaptado para la exploración de páginas web, la comunicación con el primer servidor (2) y la comunicación con el segundo servidor (3). El cliente (1) puede ser usado por un usuario o máquina.

Ejemplos particulares de realización del método según la invención

Ejemplo 1: Transacción desde un dispositivo móvil hasta otro dispositivo móvil
En la figura 3 se muestra un ejemplo particular de realización del método según la invención, en donde se muestra un ejemplo del método implementado por los tres elementos principales de la comunicación en una transacción sobre QR realizado desde un dispositivo móvil hasta otro dispositivo móvil.

En la transacción intervienen dos elementos o entidades:

- Cobrador o entidad primer servidor (2): entidad que recibe los fondos de la transacción. Para llevar a cabo la transacción se utiliza un dispositivo móvil que está adaptado para las transacciones de pago a través de un código QR. De este modo, el dispositivo móvil está adaptado para mostrar en una pantalla la imagen de un código QR a un usuario, desde donde es escaneada por el usuario que debe pagar.

- Pagador o entidad cliente (1): entidad que paga los fondos de la transacción a realizar. En este ejemplo particular el cliente (1) es un dispositivo móvil smartphone y utiliza un sensor de imagen instalado en el dispositivo móvil smartphone para escanear el código QR mostrado en la pantalla del cobrador o entidad primer servidor (2). Para ello, el pagador dispone de una aplicación para dispositivo móvil adaptada para realizar la transacción de pago sobre QR.

Este ejemplo de realización corresponde, por ejemplo, al ejemplo de un cobrador que solicita una transferencia a un pagador. Los dispositivos pagador y cobrador pueden ser utilizados por dos usuarios.

Flujo descriptivo del proceso:

3.0.- El primer servidor (2) dispositivo móvil cobrador inicia la transacción y la marca como una operación de pago con código QR.

3.1.- El primer servidor (2) dispositivo móvil cobrador genera un fichero XML (Extensible Markup Language) que comprende:

- un identificador de cobrador,
- un concepto,
- el importe solicitado,
- número de cuenta.

3.2.- El primer servidor (2) dispositivo móvil cobrador cifra el fichero XML generado utilizando un esquema de cifrado AES (advanced encryption estándar), en modo CBC (cipher-block chaining), conocida por el cliente (1) y el segundo

servidor (3).

3.3.- El primer servidor (2) dispositivo móvil cobrador codifica el resultado del paso anterior en Base64, obteniendo como resultado una cadena de caracteres de tamaño variable dependiendo de la información que se esté cifrando.

3.4.- El primer servidor (2) dispositivo móvil cobrador envía el fichero XML cifrado y codificado al segundo servidor (3), por ejemplo mediante el protocolo https, invocando un servicio web, por ejemplo un servicio REST (Representational State Transfer), de generación de código QR y enviando como parámetros:

- identificador interno de aplicación de dispositivo móvil cobrador,
- clave interna de aplicación,
- cadena de caracteres resultante del cifrado y codificado,
- prefijo (302) de la cadena que contendrá el código QR
- tamaño del QR,
- color del QR,
- nivel de redundancia del QR,
- formato de imagen.

El método se ejecuta en el cliente (1), primer servidor (2) y segundo servidor (3) gracias a una aplicación corriendo en cada uno. El identificador interno y la clave interna corresponden a identificador y clave internos y propios de la cada aplicación que corre en cada entidad (1, 2, 3).

3.5.- El segundo servidor (3):

- comprueba que el identificador interno de aplicación del segundo servidor (2) dispositivo móvil cobrador y la clave interna son correctas, donde correcta significa que los datos están comprendidos en una base de datos interna del segundo servidor (3),
- decodifica y descifra la información recibida y
- utiliza el identificador de cobrador para comprobar que quien solicita la generación del QR es correcto. Ventajosamente de este modo se incrementa la seguridad, ya que sólo entidades conocidas por el segundo servidor (3) podrán generar un código QR utilizando el segundo servidor (3),
- recibe el nombre y apellidos o razón social del cobrador, que será añadido a la información de la transacción antes de generar el código QR.

3.6.- El segundo servidor (3) genera un número aleatorio.

3.7.- El segundo servidor (3) genera una cadena concatenando

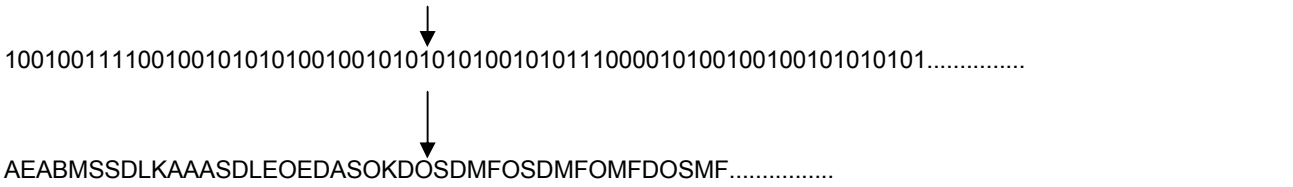
- el número aleatorio generado,
- importe,
- concepto,
- nº de cuenta del cobrador,
- nombre y apellidos o razón social del cobrador, y
- moneda,

obteniendo una cadena como por ejemplo:
“Num=1234567890&nombre=Fernando Fernández&concepto=Cena del miercoles&importe=35&moneda=euro&num_cc=43530049884993829384”.

Ventajosamente, el número aleatorio incluido permite que la cadena sea siempre diferente del resto, incluso para operaciones del mismo titular y misma cuantía y cuenta. El número aleatorio que se genera y añade al principio de la cadena, en un ejemplo particular tiene una longitud de 10 dígitos.

3.8.- El segundo servidor (3) cifra la cadena generada utilizando un esquema de cifrado AES (advanced encryption estándar), en modo CBC (cipher-block chaining) y el resultado es codificado en Base32 con una tabla de conversión propia, que ventajosamente aumenta la seguridad del codificado.

En un ejemplo de realización cifrar y codificar la cadena del punto 3.7 se representa de la siguiente manera:
“Num=1234567890&nombre=Fernando Fernández&concepto=Cena del miercoles&importe=35&moneda=euro&num_cc=43530049884993829384”.



3.9.- El segundo servidor (3) divide la cadena obtenida en 2 partes:

- una parte contendrá los primeros 30 caracteres de la cadena y será la parte “pública” de la información, y
- el resto de la cadena se almacena en la base de datos del segundo servidor (3), siendo la parte “privada” de la información.

La parte pública será la que se envía en un código QR, mientras que la parte privada reside en el segundo servidor (3). Ventajosamente de este modo, aunque un tercero intente decodificar y descifrar el contenido de la cadena del código QR, no puede, ya que no tiene la cadena completa a decodificar y descifrar, sólo los 30 primeros caracteres.

3.10.- El segundo servidor (3) genera un identificador de base de datos utilizado para localizar la información privada almacenada en la base de datos.

3.11.- El segundo servidor (3) genera una cadena con los siguientes datos:

- prefijo (302), que preferiblemente es por ejemplo bbvaqr://bbva?,
- cadena de 30 caracteres obtenida o parte pública de la información,
- identificador de base de datos generado.

Esta cadena en un ejemplo de realización es la siguiente:
“bbvaqr://bbva?pp=ADFKERORMVMOECALSPPORJWIDOLSKM&id_base_datos=329873”.

Ventajosamente, el prefijo al ser reconocido por el receptor del código (108) QR accede directamente a la aplicación que corre en el cliente (1) para la correcta interpretación del código (108) QR.

En un caso en el que el código (108) se lee desde el cliente (1) utilizando una aplicación estándar de lectura de códigos BIDI y la aplicación está instalada, la aplicación se ejecuta en ese momento.

3.12.- El segundo servidor (3) genera un código QR con la cadena del punto anterior, por ejemplo:

- fijando el formato de imagen a formato bmp, o bitmap,
- estableciendo el tamaño adecuado para el dispositivo móvil cobrador, y
- con un nivel de redundancia a cero que ventajosamente obtiene la mínima densidad posible, siendo el nivel de redundancia el número de bits de corrección de errores utilizado y la densidad el número de bits utilizado para generar el código.

Ventajosamente en este modo de realización, el código QR siempre contiene la misma cantidad de información, y por lo tanto, la densidad del mismo no varía nunca, independientemente del tamaño de la información completa, ya que siempre se envían los 30 primeros caracteres y el resto está almacenado en la base de datos. El código QR, por lo tanto, no contiene datos sensibles de la transacción.

3.13.- El segundo servidor (3) envía la imagen del código QR al dispositivo móvil cobrador y éste la presenta en la pantalla. En este ejemplo de realización, el QR tiene una validez de un tiempo predeterminado, por ejemplo de 48 horas, que ventajosamente impide que el código pueda ser reutilizado.

3.14.- El dispositivo móvil pagador o cliente (1) escanea la imagen del código QR, utilizando el sensor de imagen. En un ejemplo de realización alternativo, el código QR en lugar de ser escaneado es enviado al correo electrónico de un usuario pagador que manipula el cliente (1) o dispositivo móvil pagador.

3.15.- El dispositivo móvil pagador o cliente (1) obtiene el contenido del código QR.

3.16.- El dispositivo móvil pagador o cliente (1) aplica al contenido un método URL encode y lo envía como parámetro en una llamada a un servicio web, por ejemplo un servicio REST (Representational State Transfer) de petición de validación en el segundo servidor (3) con los siguientes parámetros:

- contenido del QR tras el URL encode,
- identificador interno de entidad cliente (1),
- clave interna de entidad cliente (1),
- modo de recepción de la información, por ejemplo, json (JavaScript Object Notation) o XML.

El modo de recepción es la forma en la que el segundo servidor (3) le envía los datos de la transacción al dispositivo o entidad cliente (1) o pagador una vez validado el código QR.

El identificador interno y la clave interna son propios del cliente (1) y sirven para identificar de manera única al cliente. De manera homóloga, el primer servidor (2) o dispositivo móvil cobrador también comprende un identificador interno y una clave interna para identificarlo de manera única.

3.17.- El segundo servidor (3):
- recibe la petición de validación de la información de un código QR,
- comprueba que el identificador de entidad cliente (1) y la clave de entidad cliente (1) son correctas,
- utilizando el identificador de base de datos, accede a la cadena privada almacenada en base de datos y la recupera para unirla a los otros 30 caracteres,
- concatena los 30 caracteres recibidos en la petición de validación con la cadena privada de la base de datos y los decodifica y descifra, obteniendo toda la información relativa a la operación,
- genera un json o XML con información de la transacción y se lo envía a la entidad cliente (1) o pagador de manera segura o mediante el protocolo https.

En esta realización particular, el método de generación de un código almacena la cadena privada de Y-M caracteres (105) que junto con la cadena pública de Y caracteres (104) representa información que permite al segundo servidor (3) obtener todos los datos necesarios de la operación para proveer (407) la información de la transacción al cliente (1) para que autorice (408) la operación.

3.18.- La entidad dispositivo móvil pagador o cliente (1):
- recibe los datos de la transacción,
- revisa los datos de la transacción,
- en caso de estar de acuerdo, autoriza la operación mediante la clave de operaciones,
- si la clave de operaciones es correcta, recibe una clave de un solo uso, que en un ejemplo particular es enviada mediante un sms,
- se completa la transacción enviando al segundo servidor (3) la clave de un solo uso.

3.19.- El primer servidor (2) o cobrador recibe una confirmación de la correcta finalización de la transacción.

3.20.- El dispositivo móvil pagador o cliente (1) recibe la confirmación de la correcta finalización de la transacción y de los detalles correspondientes a la misma.

Ejemplo 2: Transacción desde un dispositivo móvil cliente con TPV
En la figura 4 se muestra un ejemplo particular de realización del método según la invención, en donde se muestra un ejemplo del método implementado por las tres entidades principales de la comunicación en una transacción sobre QR realizado desde un dispositivo móvil cliente (1) en un comercio físico con un primer servidor (2) como TPV o terminal de punto de venta.

En la transacción intervienen dos elementos o entidades:

- Cobrador o entidad primer servidor (2): entidad que recibe los fondos de la transacción. Para llevar a cabo la transacción se utiliza un dispositivo TPV. El TPV está adaptado para las transacciones de pago a través de un código QR. De este modo, el TPV, como alternativa a la ranura conocida en el estado de la técnica para deslizar la banda de las tarjetas de débito o crédito, está adaptado para mostrar en una pantalla la imagen de un código QR, desde donde es escaneada por la entidad cliente (1).
- Pagador o entidad cliente (1): entidad que paga los fondos de la transacción a realizar. En este ejemplo particular el cliente (1) es un dispositivo móvil pagador o cliente (1) smartphone y utiliza un sensor de imagen comprendido en el dispositivo móvil cliente (1) para escanear el código QR mostrado en la pantalla del TPV.

Flujo descriptivo del proceso:

4.0.- El primer servidor (2) o cobrador TPV inicia la transacción y la marca como una operación de pago con código QR.

4.1.- El primer servidor (2) o cobrador TPV se conecta al segundo servidor (3), enviando
- el identificador del comercio y
- el importe solicitado.

4.2.- El segundo servidor (3) comprueba en su base de datos, a partir del identificador del comercio,
- la razón social del comercio
- el número de cuenta del comercio y
- CIF del comercio.

4.3.- El segundo servidor (3) genera un número aleatorio.

4.4.- El segundo servidor (3) genera una cadena concatenando
- el número aleatorio generado y

- la razón social del comercio,
- el concepto de la operación,
- el importe de la operación,
- la moneda de la operación, y
- el número de cuenta del comercio

obteniendo una cadena como por ejemplo:
"Num=43252&nombre=CarnicerÍaGómez&concepto=Varios&importe=35&moneda=euro&num_cc=43530049884993829384"

4.5.- El segundo servidor (3) codifica la cadena generada utilizando un esquema de cifrado AES (advanced encryption estandar) en modo CBC (cipher-block chaining) y el resultado es codificado en Base32 con una tabla de conversión propia, que ventajosamente aumenta la seguridad del codificado.

4.6.- El segundo servidor (3) divide la cadena obtenida en 2 partes:

- una parte contendrá los primeros 30 caracteres de la cadena y será la parte "pública" de la información, y
- el resto de la cadena se almacena en la base de datos del segundo servidor (3), siendo la parte "privada" de la información.

La parte pública será la que se envía en un código QR, mientras que la parte privada reside en el segundo servidor (3). Ventajosamente de este modo, aunque alguien intente decodificar y descifrar el contenido de la cadena del código QR, no puede, ya que no tiene la cadena completa a decodificar y descifrar, sólo los 30 primeros caracteres.

4.7.- El segundo servidor (3) genera un identificador de base de datos utilizado para localizar la información privada almacenada en la base de datos.

4.8.- El segundo servidor (3) genera una cadena con los siguientes datos:

- prefijo (302), que preferentemente es por ejemplo bbvaqr://bbva?,
- cadena de 30 caracteres obtenida o parte pública de la información,
- identificador de base de datos generado.

Esta cadena en un ejemplo de realización es la siguiente:
"bbvaqr://bbva?pp=ADFKERORMVMOECSKDOOEIWUURMWKWJ&id_base_datos=329873"

4.9.- El segundo servidor (3) genera un código QR con la cadena del punto anterior, por ejemplo:

- fijando el formato de imagen a formato bmp, o bitmap,
- estableciendo el tamaño adecuado para el TPV, y
- con un nivel de redundancia a cero que ventajosamente obtiene la mínima densidad posible, siendo el nivel de redundancia el número de bits de corrección de errores utilizado y la densidad el número de bits utilizado para generar el código.

Ventajosamente en este modo de realización, el código QR siempre contiene la misma cantidad de información, y por lo tanto, la densidad del mismo no varía nunca, independientemente del tamaño de la información completa, ya que siempre se envían los 30 primeros caracteres y el resto está almacenado en la base de datos. El código QR, por lo tanto, no contiene los datos de la transacción.

4.10.- El segundo servidor (3) envía la imagen del código QR al TPV del comercio y éste la presenta en la pantalla. En este ejemplo de realización, el QR tiene una validez de un tiempo predeterminado, por ejemplo 5 minutos, que ventajosamente impide que el código pueda ser reutilizado. El segundo servidor (3) verifica si se ha realizado el pago hasta que se efectúe, o como máximo hasta que pasen el tiempo predeterminado.

4.11.- El dispositivo móvil pagador o cliente (1) escanea la imagen del código QR, utilizando el sensor de imagen.

4.12.- El dispositivo móvil pagador o cliente (1) obtiene el contenido del código QR.

4.13.- El dispositivo móvil pagador o cliente (1) aplica al contenido un método URL encode y lo envía como parámetro en una llamada un servicio web, por ejemplo un servicio REST (Representational State Transfer) de petición de validación en el segundo servidor (3) con los siguientes parámetros:

- contenido del QR tras el URL encode,
- identificador interno aplicación de de entidad cliente (1),
- clave interna de aplicación de entidad cliente (1),
- modo de recepción de la información, por ejemplo, json o XML.

El método se ejecuta en el cliente (1), primer servidor (2) y segundo servidor (3) gracias a una aplicación corriendo en éstos. El identificador interno y la clave interna corresponden a identificador y clave internos y propios de la aplicación que corre en cada entidad (1, 2, 3).

El modo de recepción es la forma en la que el segundo servidor (3) le envía los datos de la transacción al dispositivo o entidad cliente (1) o pagador una vez validado el código QR.

4.14.- El segundo servidor (3):

- recibe la petición de validación de la información de un código QR,
- comprueba que el identificador de entidad cliente (1) y la clave de entidad cliente (1) son correctas,
- utilizando el identificador de base de datos, accede a la información privada almacenada en base de datos y la recupera para unirla a los otros 30 caracteres,
- concatena los 30 caracteres recibidos en la petición de validación con los obtenidos de base de datos y los decodifica y descifra, obteniendo toda la información relativa a la operación,
- genera un json o XML con información de la transacción y se la envía a la entidad cliente (1) o pagador de manera segura o mediante el protocolo https.

En esta realización particular, el método de generación de un código almacena la cadena privada de Y-M caracteres (105) que junto con la cadena pública de Y caracteres (104) representa información que permite al segundo servidor (3) obtener todos los datos necesarios de la operación para proveer (407) la información de la transacción al cliente (1) para que éste autorice (408) la operación. Ventajosamente, la información vulnerable como el número de cuenta, etc se envía exclusiva y directamente al cliente (1) mediante el protocolo https de manera que un posible tercero que pretenda interceptar la información no es capaz de leerla.

4.15.- El dispositivo móvil pagador o cliente (1) recibe los datos de la transacción y comprueba que son correctos,

4.16.- El dispositivo móvil pagador o cliente (1)

- recibe los datos de la transacción,
- revisa los datos de la transacción,
- en caso de estar de acuerdo, autoriza la operación mediante el envío de la clave de operaciones al segundo servidor (2).

4.17.- El dispositivo móvil pagador o cliente (1):

- si la clave de operaciones es correcta, recibe una clave de un solo uso que en un ejemplo particular es enviada mediante un sms,
- finaliza la autorización enviando la clave de un solo uso.

4.18.- El primer servidor (2) o cobrador TPV recibe una confirmación de la correcta finalización de la transacción.

4.19.- El dispositivo móvil pagador o cliente (1) recibe la confirmación de la correcta finalización de la transacción y de los detalles correspondientes a la misma.

Ejemplo 3: Firma de operaciones

En la figura 5 se muestra un ejemplo particular de realización del método según la invención, en donde se lleva a cabo una firma de operación en una página de banca online a través de un canal alternativo, o fuera de banda.

En este ejemplo el primer servidor (2) es un ordenador para conectarse a internet y el cliente (1), por ejemplo un dispositivo móvil tipo smartphone, accede a una página web alojada en el segundo servidor (3) a través del ordenador. El dispositivo móvil smartphone puede ser usado por un usuario. El cliente (1), puede ser uno cualquiera de tablet, robot, ordenador, o cualquier otro dispositivo adaptado para la exploración de páginas web. El cliente (1) puede ser usado por un usuario o máquina.

En este ejemplo, ventajosamente se aumenta la seguridad del cliente (1) en el contexto de las operaciones electrónicas realizadas a través de internet.

Se utilizan los códigos QR como medio de transmisión de información sensible o vulnerable en el proceso de firma o autorización de operaciones y evitar así que un usuario que manipula el primer servidor (2) deba introducir contraseñas con el riesgo de ser tomadas y copiadas por terceros.

En este ejemplo de realización, se cierra y completa la autorización de la operación en un dispositivo alternativo y ventajosamente se evitan los problemas que puedan derivarse de una situación en la que el primer servidor (2) u ordenador que se utiliza para conectarse a internet y desarrollar la relación principal de un usuario del ordenador o

primer servidor (2) y del cliente (1) con el segundo servidor (3), por ejemplo un banco, se encuentre comprometido de algún modo por virus, man in the middle, etc.

Como alternativa adicional, para más seguridad, el usuario puede introducir un código pin en el dispositivo móvil smartphone para completar la firma en el sistema.

Flujo descriptivo del proceso:
5.0.- El primer servidor (2) ordenador inicia una operación de firma de operaciones y la marca como una operación de firma con código QR.

5.1.- El primer servidor (2) ordenador se conecta al segundo servidor (3), enviando
- el identificador de un usuario que utiliza el primer servidor (2) ordenador,
- identificador interno de aplicación de primer servidor (2),
- clave interna de aplicación de primer servidor (2) y
- los detalles de la operación que se está realizando.

5.2.- El segundo servidor (3) comprueba en su base de datos, a partir del identificador del usuario y el identificador y clave de primer servidor (2) que el usuario está autorizado por el segundo servidor (2).

5.3.- El segundo servidor (3) genera un número aleatorio.

5.4.- El segundo servidor (3) genera una cadena concatenando
- el número aleatorio generado,
- los datos de la operación,

obteniendo una cadena como por ejemplo:
"Num=43252&operacion=Transferencia&Destinatario=Nombre y apellidos&concepto=Varios&importe=35&moneda=euro"

5.5.- El segundo servidor (3) codifica la cadena generada utilizando un esquema de cifrado AES (advanced encryption estandar) en modo CBC (cipher-block chaining) y el resultado es codificado en Base32 con una tabla de conversión propia, que ventajosamente aumenta la seguridad del codificado.

5.6.- El segundo servidor (3) divide la cadena obtenida en 2 partes:
- una parte contendrá los primeros 30 caracteres de la cadena y será la parte "pública" de la información, y
- el resto de la cadena se almacena en la base de datos del segundo servidor (3), siendo la parte "privada" de la información.

La parte pública será la que se envía en un código QR, mientras que la parte privada reside en el segundo servidor (3). Ventajosamente de este modo, aunque un tercero intente decodificar y descifrar el contenido de la cadena del código QR, no puede, ya que no tiene la cadena completa a decodificar y descifrar, sólo los 30 primeros caracteres.

5.7.- El segundo servidor (3) genera un identificador de base de datos utilizado para localizar la información privada almacenada en la base de datos.

5.8.- El segundo servidor (3) genera una cadena con los siguientes datos:
- prefijo (302), que preferiblemente es por ejemplo bbvaqr://bbva?,
- cadena de 30 caracteres obtenida o parte pública de la información,
- identificador de base de datos generado.

Esta cadena en un ejemplo de realización es la siguiente:
"bbvaqr://bbva?pp=ADFKERORMVMOEC&token=329873"

5.9.- El segundo servidor (3) genera un código QR con la cadena del punto anterior, por ejemplo:
- fijando el formato de imagen a formato bmp, o bitmap,
- estableciendo el tamaño adecuado para el primer servidor (2) ordenador, y
- con un nivel de redundancia a cero que ventajosamente obtiene la mínima densidad posible, siendo el nivel de redundancia el número de bits de corrección de errores utilizado y la densidad el número de bits utilizado para generar el código.

Ventajosamente en este modo de realización, el código QR siempre contiene la misma cantidad de información, y por lo tanto, la densidad del mismo no varía nunca, independientemente del tamaño de la información completa, ya que siempre se envían los 30 primeros caracteres y el resto está almacenado en la base de datos. El código QR, por lo tanto, no contiene los datos de la transacción.

5.10.- El segundo servidor (3) envía la imagen del código QR al primer servidor (2) ordenador y éste la presenta en la pantalla. En este ejemplo de realización, el QR tiene una validez de un tiempo predeterminado, por ejemplo 5 minutos, que ventajosamente impide que el código pueda ser reutilizado. El segundo servidor (3) verifica si se ha realizado la firma de la operación hasta que se efectúe, o como máximo hasta que pase el tiempo predeterminado.

5.11.- El cliente (1) dispositivo móvil smartphone escanea la imagen del código QR, utilizando el sensor de imagen.

5.12.- El cliente (1) dispositivo móvil smartphone obtiene el contenido del código QR.

5.13.- El cliente (1) dispositivo móvil smartphone aplica al contenido un método URL encode y lo envía como parámetro en una llamada un servicio web, por ejemplo un servicio REST (Representational State Transfer) de petición de validación en el segundo servidor (3) con los siguientes parámetros:

- contenido del QR tras el URL encode,
- identificador de aplicación de cliente (1),
- clave de aplicación de cliente (1),
- modo de recepción de la información, por ejemplo, json o XML.

El método se ejecuta en el cliente (1), primer servidor (2) y segundo servidor (3) gracias a una aplicación corriendo en éstos. El identificador interno y la clave interna corresponden a identificador y clave internos y propios de la aplicación que corre en cada entidad (1, 2, 3).

El modo de recepción es la forma en la que el segundo servidor (3) le envía los datos de la operación de acceso a la página web al cliente (1) dispositivo móvil smartphone una vez validado el código QR.

5.14.- El segundo servidor (3):

- recibe la petición de validación de la información de un código QR,
- comprueba que el identificador de cliente (1) y la clave de cliente (1) son correctas,
- utilizando el identificador de base de datos, accede a la información privada almacenada en base de datos y la recupera para unirla a los otros 30 caracteres,
- concatena los 30 caracteres recibidos en la petición de validación con los obtenidos de base de datos y los decodifica y descifra, obteniendo toda la información relativa a la operación,
- genera un json o XML con la información de la operación a firmar y se la envía al cliente (1) de manera segura o mediante el protocolo https.

En esta realización particular, el método de generación de un código almacena la cadena privada de Y-M caracteres (105) que junto con la cadena pública de Y caracteres (104) representa información que permite al segundo servidor (3) obtener todos los datos necesarios de la operación tales que son suficientes para proveer (407) la información de la operación al cliente (1) para éste que autorice (408) la operación. En este ejemplo particular estos datos son todos los detalles de la operación que se quiere firmar. Ventajosamente, al recibir los datos de la operación a firmar en el cliente (1), el usuario del cliente (1) tendrá conocimiento de que se ha iniciado una operación de firma, pudiendo no finalizarla si dicha operación no hubiera sido iniciada por él. Por tanto, se aumenta la seguridad.

5.15.- El cliente (1) dispositivo móvil smartphone:

- recibe los datos de la operación a firmar,
- revisa los datos de la operación y,
- en caso de estar de acuerdo, acepta la operación enviando un PIN de 4 dígitos,
- opcionalmente se podría enviar un sms comprendiendo una clave de un solo uso como en ejemplos anteriores.

5.16.- El primer servidor (2) ordenador recibe una confirmación del firmado de la operación por parte del cliente (1).

5.17.- El cliente (1) dispositivo móvil smartphone recibe la confirmación de la correcta firma de la operación.

Ejemplo 4: Retirada de dinero en un cajero

La ventaja de este ejemplo de método es ofrecer a un usuario un medio para optimizar el tiempo que tiene disponible en transacciones u operaciones que necesitan de una interacción física como las retiradas e ingresos de efectivo en cajeros automáticos.

El cliente (1) da de alta operaciones que quedan listas y pendientes de ser completadas en el segundo servidor (3) y que, una vez el cliente (1) opera con un primer servidor (2) o cajero, el proceso de finalización de la operación se desencadena a través de un código QR.

El primer servidor (2) o cajero deberá ser adaptado para que muestre en algún medio de visualización un código QR generado por el segundo servidor (3).

De este modo, se realizarán los siguientes pasos, representados en la figura 6, para generar el QR de cada segundo servidor (2) o cliente:

6.0 Se genera un XML o cadena con la siguiente información:

- Identificador único de primer servidor (2) o cajero.
- Localización.
- Coordenadas geográficas.

6.1.- Se solicita al segundo servidor (3) la generación de un código QR con la información del punto 6.0.

En un ejemplo particular esta solicitud (6.1) se envía desde el cajero (2), en otro ejemplo particular y no limitativo, esta solicitud (6.1) se realiza desde un servidor central y no representado en la figura 6.

6.2.-El segundo servidor (3) realiza las siguientes operaciones:

- Genera un número aleatorio que concatenado al resto de información, sirve para que la cadena que contendrá el QR sea siempre diferente del resto.

- Genera una cadena concatenando el número generado y el resto de parámetros de la operación, obteniendo una cadena del siguiente estilo:
  "Num=43252&identificador_cajero=11223344455&localizacion=Plaza Maria Soledad Torres Acosta&coordenadas=3453454564645,4565436456456"

- La cadena generada es cifrada utilizando el esquema AES en modo CBC y el resultado es codificado en Base32 con una tabla de conversión propia, lo que aumenta la seguridad del codificado.

- Divide la cadena obtenida en 2 partes. Una parte contiene los primeros 30 caracteres y será la parte "pública" de la información, y el resto de la cadena se almacena en base de datos, siendo la parte "privada" de la información. La parte pública será la que se enviará en el QR, mientras que la parte privada siempre residirá en el segundo servidor (3). De este modo, aunque alguien intentara decodificar y descifrar el contenido de la cadena del QR, no podría, ya que no tendría la cadena completa a decodificar y descifrar, sólo los 30 primeros caracteres.

- Se genera un identificador de base de datos que servirá para localizar la información privada almacenada en base de datos.

- Se genera una cadena con los siguientes datos:

✓prefijo (302) por ejemplo bbvaqr://bbva?
✓cadena de 30 caracteres obtenida (parte pública de la información).
✓Identificador de base de datos generado.

Esta cadena será del estilo de la siguiente:
"bbvaqr://bbva?pp=ADFKERORMVMOEC&token=329873"

- El segundo servidor (3) llama al servicio de generación de QR, que contiene la cadena obtenida en el punto anterior. Al utilizarse este método, el QR siempre contiene la misma cantidad de información, y por lo tanto, la densidad del mismo no varía nunca, independientemente del tamaño de la información que contenga, ya que siempre se enviarán los 30 primeros caracteres y el resto estará almacenado en base de datos. El QR, por lo tanto, no contiene los datos completos del primer servidor (2) o cajero.

6.3- El segundo servidor (3) envía el código QR al segundo servidor (2) o cajero.

En este punto, el código (108) queda visible en el cajero automático, bien en unos medios de visualización o impreso en una carcasa exterior del cajero (2). A partir del momento en el que el código (108) está disponible y visible, un cliente (1) puede escanearlo o capturarlo sin restricciones de tiempo.

6.4- El cliente (1), en algún momento, utilizando la aplicación, inicia una operación de retirada de efectivo que queda pendiente en el servidor (3).

6.5- El cliente (1) en algún momento, por ejemplo no superior a 2 horas, captura el código (108) QR del cajero (2) con el sensor de imagen. Esta acción desencadena el inicio del proceso de finalización de la operación que el cliente (1) inició

en el punto 6.4 y que quedó en estado pendiente.

6.6.- El cliente (1) obtiene el contenido del código (108). Le aplica el método URL encode y lo envía como parámetro en una llamada al servicio REST de validación correspondiente en el segundo servidor (3) con los siguientes parámetros:

- ✓identificador de un usuario que utiliza el cliente (1),
- ✓contenido del QR tras el URL encode,
- ✓identificación interna de aplicación de cliente,
- ✓clave interna de aplicación, y
- ✓modo de recepción de la información (json/xml).

El modo de recepción es la forma en la que el servidor le enviará los datos de la operación al dispositivo del usuario una vez validado el QR.

6.7.- El servidor recibe la petición de validación de la información de un QR y efectúa las siguientes operaciones:

✓Comprueba que la identificación interna de aplicación de cliente y la clave son correctas.

✓Utilizando el identificador de base de datos, accede a la información privada almacenada en base de datos y la recupera para unirla a los otros 30 caracteres.

✓Concatena los 30 caracteres recibidos en la llamada con los obtenidos de base de datos y los decodifica y descifra.

✓Utilizando el identificador de usuario de cliente (1), el segundo servidor (3) comprueba que éste tiene pendiente una operación de retirada de efectivo y recupera la cuantía a retirar.

✓genera un json o xml con la información de la operación (importe y datos del cajero).

6.8.- El segundo servidor (3) envía al cliente (1) de manera segura (https) la información de la operación como por ejemplo importe y datos del cajero (2).

6.9.- El cliente (1) verifica que se encuentra en del cajero correcto.

6.10.-En caso de ser correcto, el cliente (1) envía un PIN de 4 dígitos para completar el proceso al segundo servidor (3).

6.11.- El segundo servidor (3) verifica que el PIN introducido es correcto y envía al primer servidor (2) o cajero un orden para que entregue el efectivo solicitado.

6.12.-El cajero entrega el efectivo, dándose por finalizada la operación.

Ventajosamente en este ejemplo de realización se evita la introducción de credenciales en el cajero automático que puedan ser interceptadas por un tercero.

REIVINDICACIONES

1.- Método para la generación de un código (108) que comprende las etapas:
a.- proveer una primera cadena de caracteres (101) de W caracteres,
b.- cifrar (110) la primera cadena de caracteres (101), obteniendo una cadena cifrada (102),
c.- codificar (111) la primera cadena cifrada (102), obteniendo una cadena de Y caracteres (103) cifrada y codificada,
d.- dividir (112) la cadena de Y caracteres (103) en:
- una cadena pública de M caracteres (104), y
- una cadena privada de Y-M caracteres (105),
e.- concatenar (113) al menos:
- la cadena pública de M caracteres (104),
- un identificador de base de datos (301) que indica una dirección de memoria de una unidad de almacenamiento donde se almacena la cadena privada de Y-M caracteres (105),
- un prefijo (302) e
- información adicional (106),
obteniendo una segunda cadena de caracteres (107),
f.- codificar (114) la segunda cadena de caracteres (107) , obteniendo el código (108)
en el que el identificador se usa para acceder a información privada almacenada en la base de datos de un segundo servidor (3) y el prefijo se usa para acceder directamente a una aplicación ejecutada en un cliente.

2.- Método según la reivindicación 1 caracterizado porque el método de codificación de la etapa f.- es un método de codificación de códigos QR, obteniéndose como código (108) un código QR.

3.- Método según cualquiera de las reivindicaciones anteriores caracterizado porque la primera cadena de caracteres (101) de W caracteres es una cadena obtenida mediante las siguientes etapas:
- proveer una cadena de información (201), que preferentemente es información cifrada y codificada,

- decodificar y descifrar esta información si la información (201) es información cifrada y codificada,
- generar (210) un número aleatorio (202),
- concatenar (211) el número aleatorio a toda o parte de la cadena de información (201) provista, obteniéndose una cadena inicial (101).

4.- Método de autorización de una operación implementado en un sistema que comprende,
- un cliente (1),
- un primer servidor (2),
- un segundo servidor (3), en comunicación con el primer servidor (2), y en comunicación con el cliente (1),
el método comprende las etapas de:
a.- solicitar (401) un código (108) al segundo servidor (3), la solicitud comprendiendo una cadena con datos (4) de operación,
b.- generar (402) un código (108) por parte del segundo servidor (3) a partir de una cadena con datos (4) de operación según un método según cualquiera de las reivindicaciones 1 a 3,
c.- enviar (403) el código (108) por parte del segundo servidor (3) al primer servidor (2),
d.- trasladar (404) el código (108), por parte del cliente (1) desde el primer servidor (2) hasta el cliente (1),
e.- decodificar (405) el código (108) por parte del cliente (1), obteniendo la segunda cadena de caracteres (107),
e1.- solicitar (406) información de operación por parte del cliente (1) al segundo servidor (3), y
e2.- proveer (407) información de operación por parte del segundo servidor (3),
f.- finalizar (408) por parte del cliente (1) la autorización enviando una confirmación de autorización al segundo servidor (3).

5.- Método según la reivindicación 4 caracterizado porque tras la etapa f.- se ejecuta la etapa g:
g.- ejecutar (409) la operación por parte del segundo servidor (3).

6.- Método de autorización según cualquiera de las reivindicaciones 4 o 5 caracterizado porque la operación es una operación de transferencia desde una cuenta bancaria asociada al cliente (1) hasta una cuenta bancaria asociada al primer servidor (2).

7.- Método según cualquiera de las reivindicaciones 4 a 6 caracterizado porque
- el código (108) es una imagen QR, o código bidimensional, y
- en la etapa d.- el traslado se realiza captando del código (108).

8.- Método según cualquiera de las reivindicaciones 4 a 6 caracterizado porque el código (108) es trasladado vía tecnología NFC desde el primer servidor (2) hasta el cliente (1).

9.- Método según cualquiera de las reivindicaciones 4 a 8 caracterizado porque
- en la etapa e1.- la solicitud (406) de información de operación se realiza junto con un identificador de aplicación y una clave de aplicación de cliente (1), y
- en la etapa e2.- la provisión (407) de información de operación se realiza si el identificador de aplicación y la clave de aplicación de cliente (1) son correctas, donde un identificador y una clave de cliente (1) correctas son un identificador de aplicación y una clave de aplicación de cliente (1):
- conocida por el segundo servidor (3) y
- que corresponde con el cliente (1) desde el que se recibe.

10.- Método según cualquiera de las reivindicaciones 4 a 9 caracterizado porque,
- tras la etapa e2.- se implementan las etapas:
e3.- enviar por parte del cliente (1) una clave de operaciones,
e4.-recibir en el cliente (1) una clave de un solo uso (5), preferentemente mediante un servicio de mensajes cortos, mensaje sms,
- en la etapa f.- la finalización (408) por parte del cliente (1) de la autorización se realiza enviando la clave de un solo uso (5).

11.- Método según cualquiera de las reivindicaciones 4 a 10 caracterizado porque,
-en la etapa a.- la solicitud (401) comprende un fichero XML o Extensible Markup Language con los datos (4) de operación cifrados mediante un cifrado AES y codificados mediante una codificación en Base64, el fichero XML comprendiendo información de operación.

12.- Método según cualquiera de las reivindicaciones 4 a 11 caracterizado porque
-en la etapa e1.-,
**la solicitud (406) de información adicional comprende los datos obtenidos en la etapa e.- codificados mediante una codificación URL y
**la solicitud (406) de información adicional se realiza con una llamada a un servicio web del segundo servidor (3), preferentemente un servicio REST, o Representational State Transfer, de petición de validación en el segundo servidor (3) y preferentemente la llamada comprende los parámetros,
-resultado de la codificación de los datos (500) obtenidos en la etapa e.- tras codificar mediante una codificación URL,
-identificador interno de cliente (1),
-clave interna de cliente (1),
-modo de recepción de la información, preferentemente, json o XML,

-en la etapa e2.- la información solicitada (406) comprende información de operación que es obtenida por parte del segundo servidor (3) tras haber implementado un método que comprende las etapas:
**recibir la llamada a un servicio web del segundo servidor (3), preferentemente una petición de validación de la información en el segundo servidor (3),
**comprobar (411) que el identificador de cliente (1) y la clave de cliente (1) son correctos,
**utilizar el identificador de base de datos (301) para acceder a la cadena privada de Y-M caracteres (105) almacenada en memoria de una unidad de almacenamiento y recuperarla para unirla a los datos obtenidos en la etapa e1.- recibidos en la llamada a un servicio web,
**concatenar (410) los datos (500) obtenidos en la etapa e1.- recibidos en la llamada a un servicio web con la cadena privada de Y-M caracteres (105),
**descodificar y descifrar la cadena resultante, obteniendo la información de operación por parte del segundo servidor (3),
**proveer (407) una información de operación, preferentemente en el modo de recepción seleccionado en la etapa e1.- y preferentemente de manera segura mediante el protocolo https.

13.- Sistema para la autorización de una operación que comprende las siguientes entidades,
-un cliente (1),
-un primer servidor (2), y
-un segundo servidor (3), en comunicación con el primer servidor (2), y en comunicación con el cliente (1),
en el que,
-las tres entidades (1, 2, 3) están adaptados para implementar las etapas de un método según cualquiera de las reivindicaciones 4 a 12,
-el segundo servidor (3) está adaptado para implementar todas las etapas de un método de generación de un código (108) según cualquiera de las reivindicaciones 1 a 3, y
-el cliente (1) está adaptado para llevar a cabo la decodificación de un código (108) generado mediante todas las etapas de un método según cualquiera de las reivindicaciones 1 a 3.

14.- Sistema según la reivindicación 13 caracterizado porque el cliente (1) es un dispositivo que comprende un sensor de imagen o es un dispositivo que comprende una antena adaptada para trabajar con la tecnología NFC, o es un

dispositivo que comprende un sensor de imagen y una antena adaptada para trabajar con la tecnología NFC.

15.- Programa de ordenador que comprende
- código de programa de ordenador, el cual cuando se ejecuta por un segundo servidor (3), causa que el segundo servidor (3) lleve a cabo todas las etapas del método de cualquiera de las reivindicaciones 1 a 3, o
- código de programa de ordenador, el cual cuando se ejecuta por un cliente (1), causa que el cliente (1) lleve a cabo todas las etapas del método de cualquiera de las reivindicaciones 4 a 12, o
- código de programa de ordenador, el cual cuando se ejecuta por un primer servidor (2), causa que el primer servidor (2) lleve a cabo todas las etapas del método de cualquiera de las reivindicaciones 4 a 12, o
- código de programa de ordenador, el cual cuando se ejecuta por un segundo servidor (3), causa que el segundo servidor (3) lleve a cabo todas las etapas del método de cualquiera de las reivindicaciones 4 a 12.

16.- Producto de programa de ordenador almacenado en un soporte legible por un ordenador,
que comprende medios de código de programa de ordenador adaptados para realizar todas las etapas de un método de cualquiera de las reivindicaciones 1 a 3, cuando las etapas las implementa un segundo servidor (3), o
que comprende medios de código de programa de ordenador adaptados para realizar todas las etapas de un método de cualquiera de las reivindicaciones 4 a 12 cuando las etapas las implementa un cliente (1), o
que comprende medios de código de programa de ordenador adaptados para realizar todas las etapas de un método de cualquiera de las reivindicaciones 4 a 12, cuando las etapas las implementa un primer servidor (2), o
que comprende medios de código de programa de ordenador adaptados para realizar todas las etapas de un método de cualquiera de las reivindicaciones 4 a 12 cuando las etapas las implementa el segundo servidor (3).

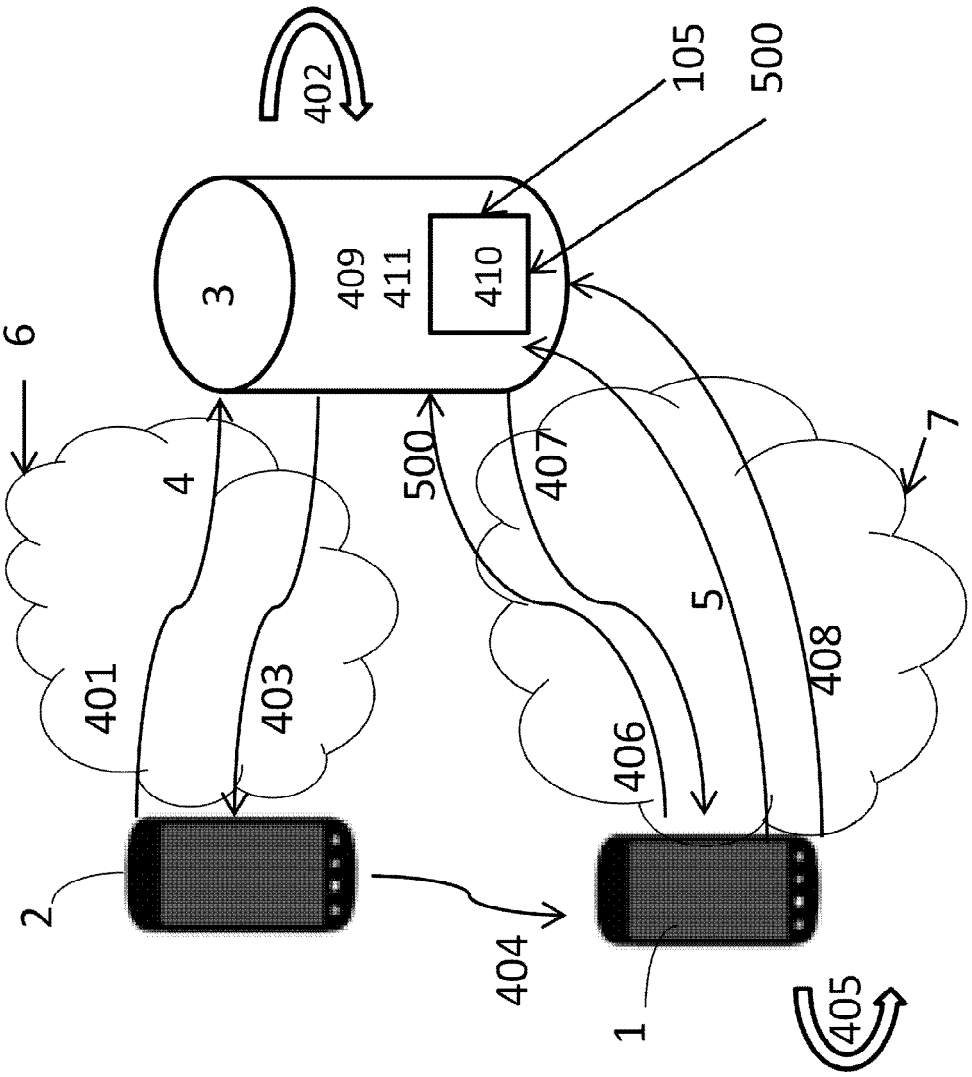


FIG. 1

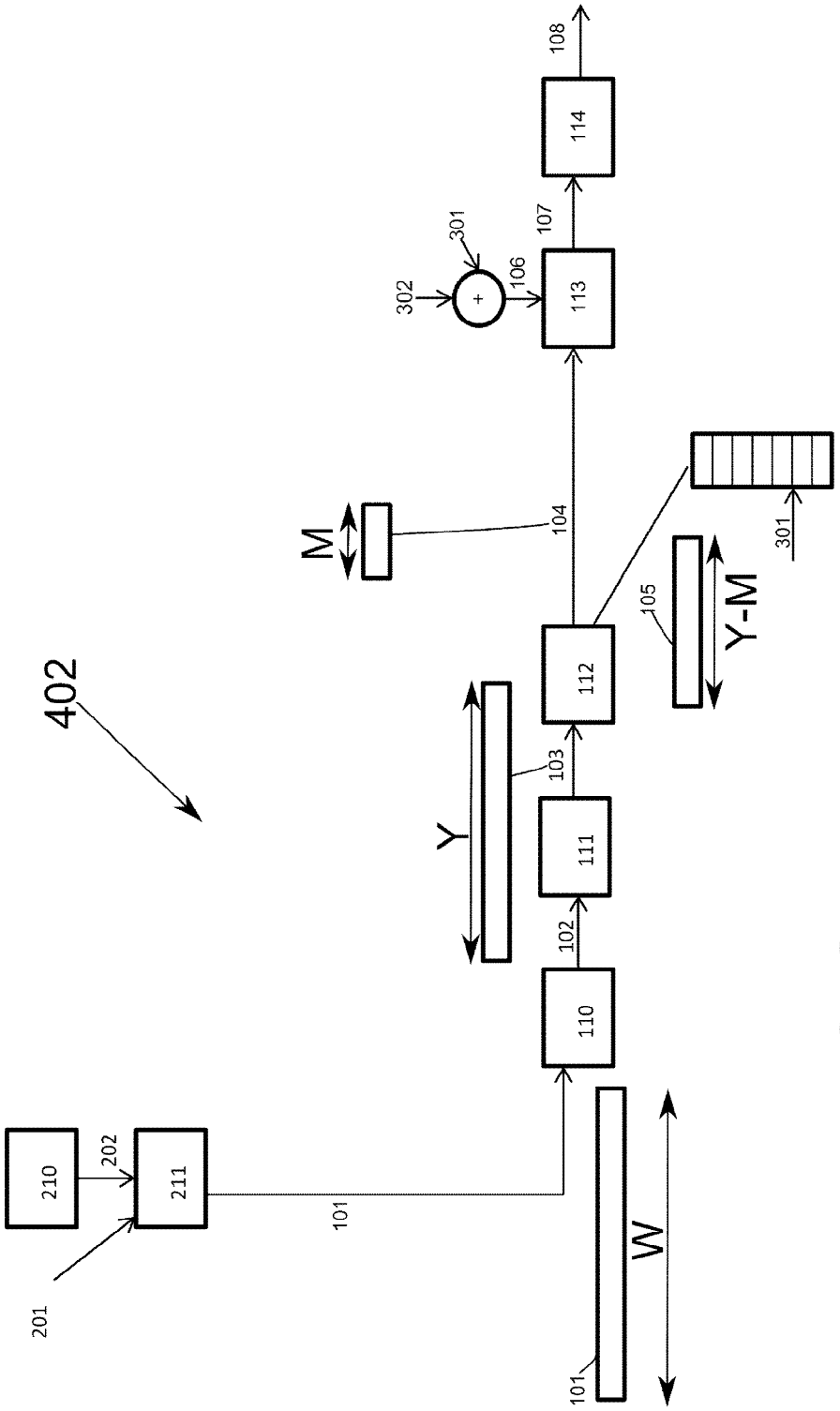

402
201
210
211
202
101
110
102
111
103
Y
112
105
Y-M
301
M
104
113
106
107
302
301
114
108
W
101

FIG. 2

FIG. 3

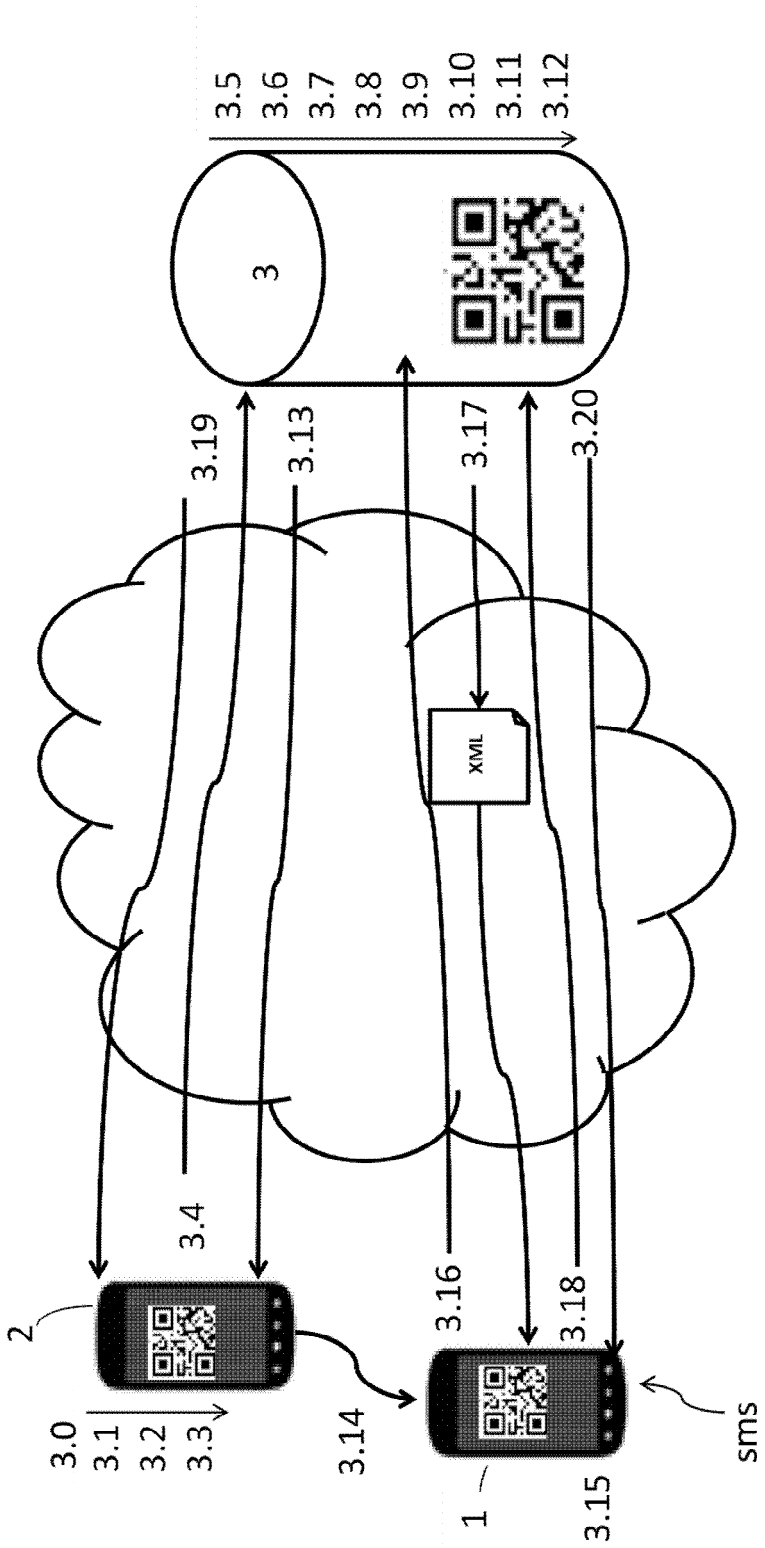
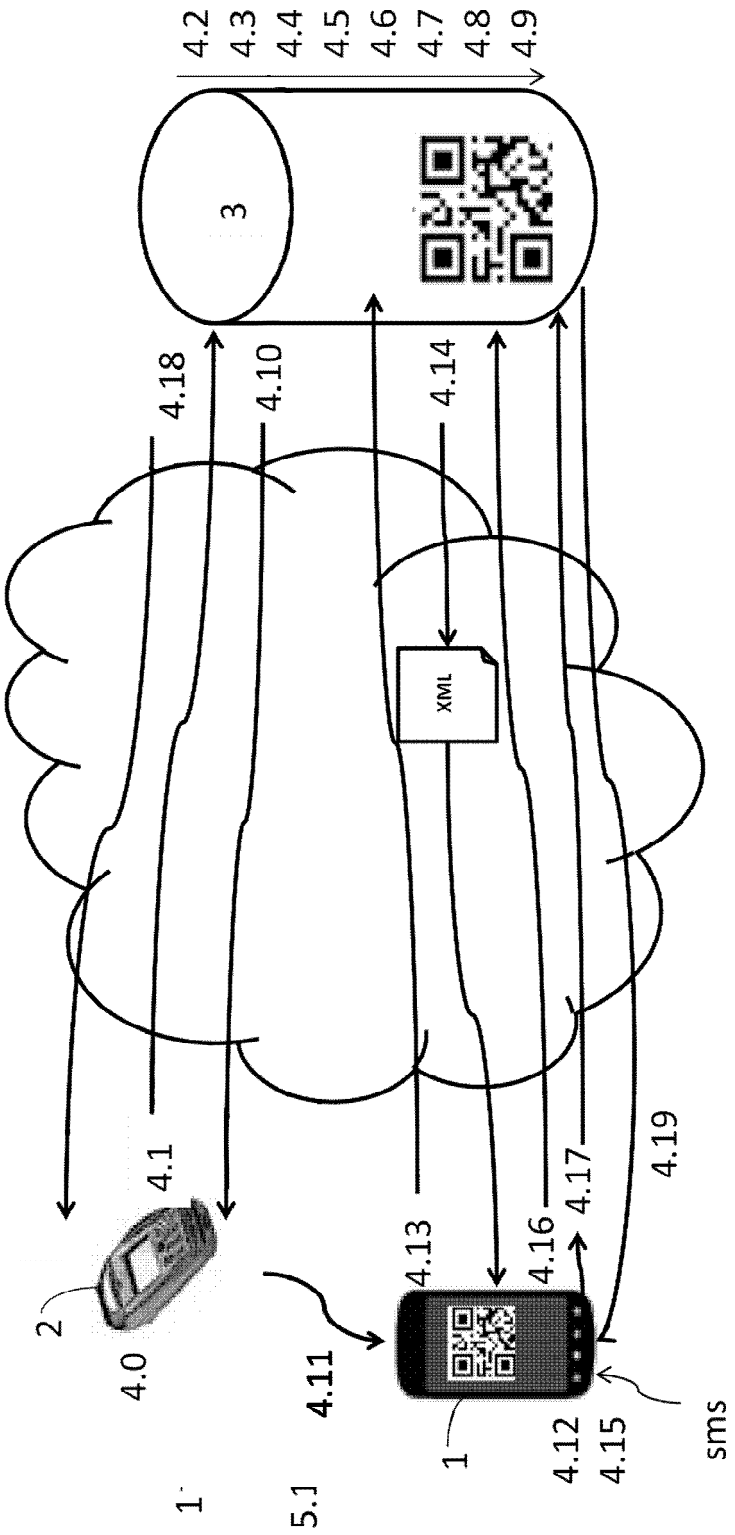

3.5
3.6
3.7
3.8
3.9
3.10
3.11
3.12
3
3.19
3.13
3.17
3.20
XML
3.4
3.16
3.18
2
3.0
3.1
3.2
3.3
3.14
1
3.15
sms

FIG. 5


5.16
5.1
2
5.0

FIG. 4


4.2
4.3
4.4
4.5
4.6
4.7
4.8
4.9
3
4.18
4.10
4.14
XML
4.1
2
4.0
4.13
4.16
4.17
4.19
4.11
1
4.12
4.15
sms
1
5.1

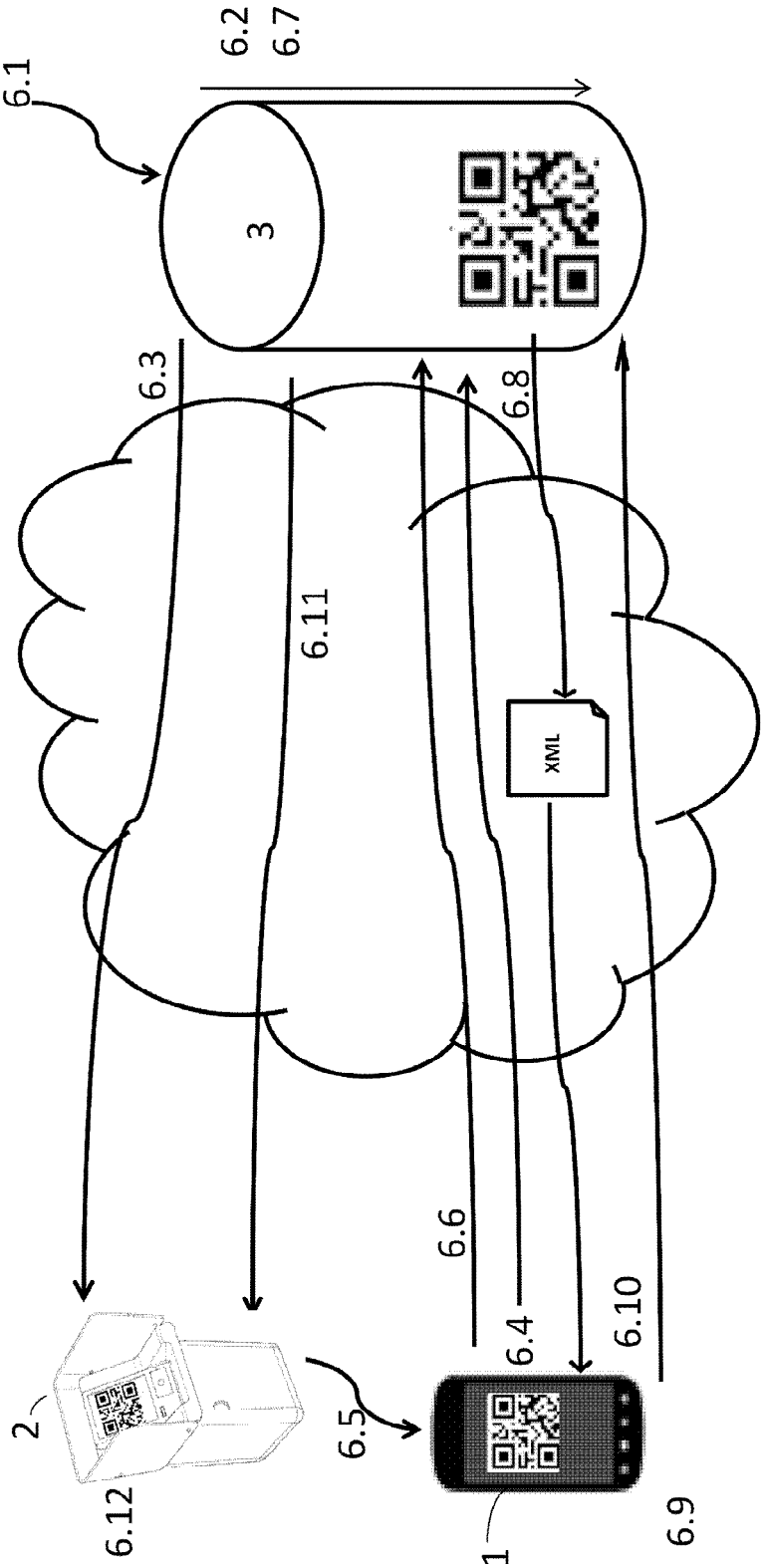


FIG. 6

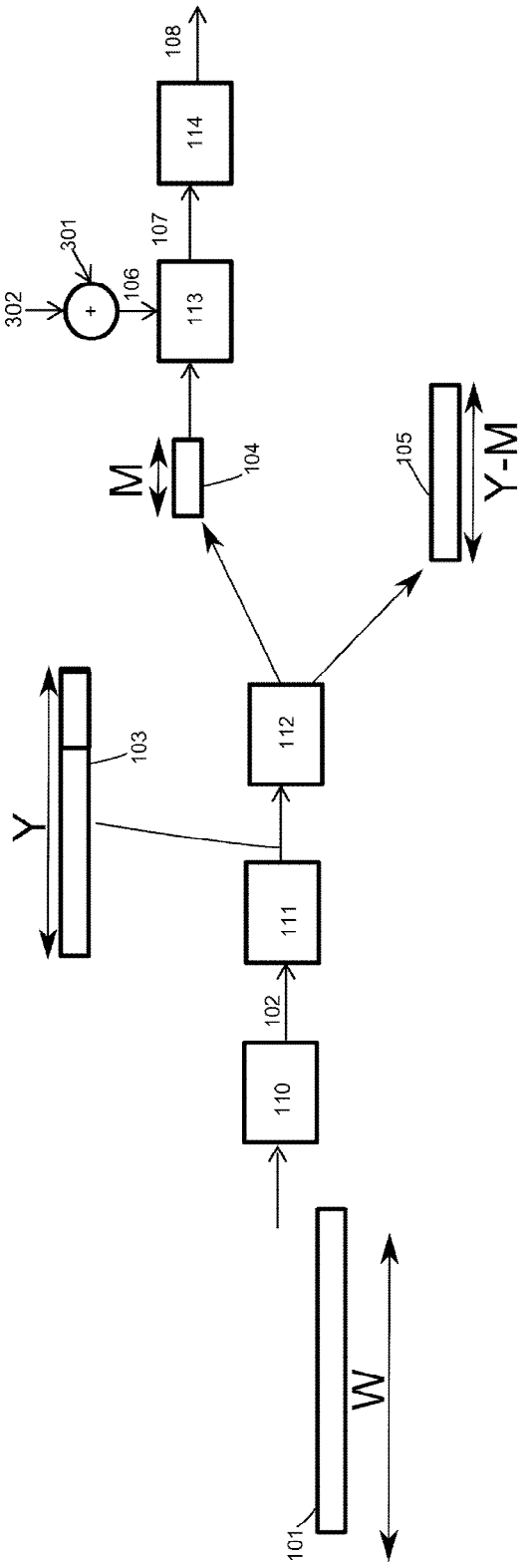

108
114
107
301
106
302
113
M
104
105
Y-M
112
103
Y
111
102
110
W
101

FIG.7