(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 530 467**

(51) Int. CI.:

H04L 9/32 (2006.01)
H04L 9/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **16.03.2011 E 11708480 (6)**

(97) Fecha y número de publicación de la concesión europea: **26.11.2014 EP 2548331**

(54) Título: **Sistema y procedimiento para la comunicación entre diferentes entidades mediante el uso de diferentes porciones de datos para diferentes canales**

(30) Prioridad:

29.10.2010 US 408056 P
19.03.2010 US 315616 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
02.03.2015

(73) Titular/es:

MR.QR10 GMBH & CO. KG (100.0%)
Lise-Meitner-Strasse 4
24941 Flensburg, DE

(72) Inventor/es:

PALZER, MARTIN;
STALS, LUC;
GELDERMANN, MARTIN y
HIRASAWA, SHINJI

(74) Agente/Representante:

PONTI SALES, Adelaida

DESCRIPCIÓN

Sistema y procedimiento para la comunicación entre diferentes entidades mediante el uso de diferentes porciones de datos para diferentes canales.

[0001] En la actualidad, la transferencia de datos está expuesta a fallos en la seguridad como, por ejemplo, el *phishing*, ataques de intermediarios o MitM (*man-in-the-middle*), robo de contraseñas, etc. En la siguiente solicitud de patente se describe una manera de asegurar las transmisiones de datos a través de una transferencia de datos multidireccional. La presente solicitud de patente ofrece varias ventajas. En primer lugar, la transmisión de dos vías independientes resulta muy difícil de atacar. En segundo lugar, en el caso de que utilicemos tecnologías de identificación automática, por ejemplo un código 2D, el atacante no tendrá ninguna posibilidad de descubrir de qué modo y a través de qué vía la segunda (o múltiple, en su caso) entidad está enviando los otros datos, ya que en la primera entidad no se conoce información acerca de la segunda entidad. Otras opciones para esta comunicación bidireccional consisten en la división del archivo cifrado, la división de la clave de cifrado o incluso ambas, dependiendo de la aplicación y las necesidades de seguridad.

[0002] En el documento WO 2009/144010 A1, se describe un dispositivo servidor para controlar una transacción, una primera entidad y una segunda entidad. La primera entidad puede ser, entre otros, un punto de servicio o una tienda *online* o incluso un coche que se quiera arrancar. La segunda entidad puede ser un usuario provisto de un teléfono móvil con una cámara digital, y la tercera entidad es el servidor. La primera entidad genera un código con información sobre la transacción y envía un primer mensaje a un servidor. La segunda entidad, por ejemplo un comprador de un producto o un usuario de un servicio, capta el código y transmite un segundo mensaje al servidor con información sobre la transacción, extraída del código. La transacción solo se autoriza cuando el servidor haya determinado que el primer mensaje y el segundo mensaje concuerdan entre sí. La transacción puede ser efectuar un pago mediante una transferencia, obtener el acceso a un servicio u obtener el acceso a un portal de Internet.

[0003] En el documento JP2005064984, se describe una primera entidad para la comunicación con otras entidades de comunicación que comprende un subdivisor de datos para subdividir una entidad de datos en diferentes porciones de datos, una interfaz de salida para transmitir a cada una de las entidades de comunicación mensajes que comprenden una porción de datos diferente, e información acerca del modo en que se ha subdividido la entidad de datos.

[0004] La invención se define en las reivindicaciones independientes. Las formas de realización particulares se exponen en las reivindicaciones dependientes.

[0005] La presente invención se basa en el descubrimiento de que se puede obtener una mejora en lo que respecta a la seguridad y/o eficiencia cuando los mensajes enviados desde la primera entidad y la segunda entidad al servidor no comprenden los mismos datos de transacción, que posteriormente son comparados por la tercera entidad/servidor para comprobar si son idénticos entre sí o no. En lugar de ello, los datos enviados desde la primera entidad al servidor son diferentes de los datos enviados desde la segunda o más entidades al servidor, pero estos dos o más bloques de datos o porciones de datos pertenecen a la misma entidad de datos. La entidad de datos puede comprender un archivo, que puede o no estar cifrado, o una clave. Esta entidad de datos se subdivide en la primera entidad en diferentes porciones de datos, y una interfaz de salida en la primera entidad transmite a la tercera entidad (o más) un mensaje que contiene la primera porción, pero sin la segunda porción (o más porciones). Además, la primera entidad genera un segundo mensaje que comprende la segunda porción (o más) de datos, pero no comprende la primera porción de datos y proporciona este segundo mensaje (o más mensajes) para que los reciba una segunda entidad. En concreto, el subdivisor de datos está configurado para subdividir la entidad de datos de una manera conocida por la tercera entidad. Otra posibilidad consiste en que el subdivisor de datos esté configurado para generar información de la subdivisión que indique la manera en que se subdivide la entidad de datos, y esta información de subdivisión se incluye en el primer mensaje o el segundo mensaje como información adicional o se envía a la tercera entidad como un mensaje individual.

[0006] Basándose en esta información, la tercera entidad, por ejemplo un servidor, puede (re)ensamblar las porciones de datos recibidas, procedentes de la primera entidad y la segunda entidad, para procesar la entidad de datos al completo tras reensamblarla.

[0007] Preferentemente, los canales de transmisión para transmitir el primer mensaje y el segundo mensaje son diferentes entre sí, y el primer canal de transmisión para transmitir el primer mensaje será, normalmente, un

canal de transmisión de alta capacidad, como un canal de Internet, un canal por cable o un canal de telefonía móvil. Sin embargo, el segundo canal puede ser un canal de baja capacidad que sea, preferentemente, un canal unidireccional como, por ejemplo, un canal consistente en la presentación de los datos en la pantalla y la captura de unos datos visualizados por parte de la segunda entidad.

[0008] Un modo preferido de hacerlo consiste en presentar el segundo mensaje en forma de código QR o cualquier otro código bidimensional en una pantalla o a través de cualquier tecnología de identificación automática, como por ejemplo RFID o NFC. De este modo, la segunda entidad dispondrá de una cámara digital y un lector de códigos QR o cualquier otro lector para leer el código bidimensional o de identificación automática con el fin de extraer la información del segundo mensaje. Como otra posibilidad, se podría implementar cualquier otra tecnología de identificación automática, como NFC o RFID.

[0009] A diferencia de lo que ocurre con la transmisión de los mismos datos a través de los dos o más canales de transmisión, la eficiencia del procedimiento de la invención mejora gracias al hecho de que solo se transmite, por ejemplo, el 50% de los datos a través de los canales, en comparación con un sistema que transmite los mismos datos a través de ambos canales.

[0010] Además, el concepto de la invención es flexible, ya que las porciones de datos pueden tener diferentes tamaños, de manera que una porción de datos grande se transmita en el mensaje para el canal de banda ancha y una porción de datos pequeña se transmita a través del canal con la menor capacidad de datos. Concretamente, la capacidad de datos de un canal formado por un código bidimensional es bastante baja. Por otra parte, este canal resulta muy atractivo, ya que se puede adaptar de manera sencilla y eficiente a aplicaciones de telefonía móvil, es decir, en el caso de que la segunda entidad sea una aplicación de telefonía móvil.

[0011] Además, la seguridad del proceso también mejora debido al hecho de que no existe ningún canal a través del cual se transmita la entidad de datos al completo. Para expresarlo de otro modo, en el sistema que transmite los mismos datos a través de ambos canales, un atacante podría atacar un solo canal y hacerse con la totalidad de los datos. No obstante, de acuerdo con la presente invención, si se ataca un único canal no se obtendrá la entidad de datos al completo, sino que se obtendrá la porción de datos que normalmente no tiene ninguna utilidad para el atacante. Por lo tanto, la seguridad mejora debido al hecho de que el atacante tendría que atacar ambos canales para recuperar la primera porción de datos y la segunda porción. Sin embargo, incluso estas porciones de datos resultarán insuficientes para que el ataque a dicho sistema sea completo, debido al hecho de que el atacante desconoce la manera en que se ensamblan las porciones de datos para recuperar la entidad de datos. Por lo tanto, el atacante tiene que obtener información adicional acerca de la manera de ensamblar las porciones de datos para poder completar un ataque al sistema de la invención.

[0012] Preferentemente, la entidad de datos se genera mediante el cifrado de datos de transmisión. Por tanto, incluso si se extraen únicamente varios bytes de los datos cifrado para el canal de baja capacidad y se deja la inmensa mayoría de los datos del primer mensaje para transmitirlos a través del canal de alta capacidad, sin embargo, se producirá una consecuencia positiva, ya que, aunque un atacante ataque la inmensa mayoría de los datos cifrados, estos datos resultarán inservibles debido al hecho de que la separación de las diferentes porciones de datos se ha llevado a cabo en el dominio cifrado y no en el dominio no cifrado. No es necesario aclarar que esa minoría de datos del segundo mensaje no sirve para recuperar los datos de la entidad de datos.

[0013] A continuación se describirán formas de realización preferidas de la invención, haciendo referencia a los dibujos adjuntos:

la fig. 1a es una secuencia de etapas llevadas a cabo por la primera entidad, la segunda entidad o el servidor en una forma de realización preferida;

la fig. 1b es una secuencia adicional de etapas llevadas a cabo entre el servidor y una compañía de pagos en el caso de que se dé un emparejamiento positivo entre ambos mensajes;

la fig. 2 es un diagrama de bloques de una forma de realización preferida de la primera entidad, como por ejemplo un punto de servicio;

la fig. 3a es un diagrama de bloques de una implementación preferida del servidor;

la fig. 3b es una secuencia de etapas seguidas por el servidor para llevar a cabo otra comprobación opcional de

seguridad basada en información tal como el número de dispositivo de servicio móvil (MSISDN/IMSI) y/o IMSI (identidad internacional de estación móvil o IIEM);

la fig. 4a es un diagrama de bloques de una aplicación preferida de la segunda entidad, como por ejemplo un teléfono móvil con cámara digital;

la fig. 4b es una secuencia de etapas llevadas a cabo por la segunda entidad, que incluye la petición de un secreto al usuario;

la fig. 5 es una tabla que ilustra seis diferentes aplicaciones ejemplares del concepto de la invención;

la fig. 6 ilustra un modelo de comunicación entre las tres entidades de acuerdo con una forma de realización en la que se identifican diferentes canales de transmisión;

la fig. 7 ilustra otra forma de realización de un modelo de transmisión entre las tres entidades con una clave generada por la primera entidad;

la fig. 8 ilustra otra aplicación del concepto de la fig. 7, pero con el uso de otra clave K1 entre la primera entidad y la tercera entidad;

la fig. 9 ilustra otra forma de realización, en la que el emparejamiento en la tercera entidad se lleva a cabo con datos procedentes de múltiples entidades, por ejemplo una cuarta entidad o incluso más entidades;

la fig. 10 ilustra una forma de realización en la que la entidad de datos es un archivo de datos cifrado mediante un algoritmo de cifrado y usando información de clave que permite una comunicación segura entre la primera entidad y la tercera entidad;

la fig. 11 ilustra otra implementación, en la que la entidad de datos es una clave separada en dos porciones de clave diferentes;

la fig. 12 ilustra una topología general en una aplicación de telefonía móvil/tienda web con un servidor de emparejamiento;

la fig. 13 ilustra varios detalles de la implementación del concepto de la fig. 12;

la fig. 14 ilustra más detalles relativos a la distribución de operaciones entre una parte móvil y una parte de servidor y entre la primera entidad (punto de servicio/tienda web) y la segunda entidad (teléfono móvil);

la fig. 15 ilustra algunos detalles del concepto de la fig. 14;

la fig. 16 ilustra una forma de realización en la que la entidad de datos es un archivo cifrado;

la fig. 17 ilustra más detalles relativos al concepto de la fig. 16;

la fig. 18 ilustra un diagrama de bloques de una primera entidad en una implementación preferida;

la fig. 19 ilustra un diagrama de bloques de una tercera entidad de acuerdo con una implementación preferida; y

la fig. 20 ilustra un diagrama de bloques de una segunda entidad de acuerdo con una implementación preferida.

[0014] La fig. 6 ilustra una vista general entre una primera entidad 11, una segunda entidad 12 y una tercera entidad 13. Concretamente, existen tres canales de comunicación 60a, 60b y 60c entre las diferentes entidades, en los que el canal de transmisión 60b se extiende entre la primera entidad 11 y la tercera entidad 13 y puede comprender un canal de transmisión de alta capacidad.

[0015] Además, la transmisión a través de este canal de transmisión 60b puede ser una comunicación cifrada en la que la información de clave usada para esta comunicación se ilustra como K1. Cuando se aplica un cifrado simétrico, la información de clave, tal como se emplea a lo largo de la presente memoria descriptiva, puede ser una clave simétrica conocida únicamente por la primera entidad y la tercera entidad, de modo que estas dos entidades

puedan usar esta clave secreta K1 para el cifrado y el descifrado. No obstante, la información de clave tal como se emplea a lo largo de la presente memoria también puede comprender un cifrado asimétrico, en el que para cada entidad exista un par de claves. Este par de claves comprende una clave pública conocida por todos y una clave privada conocida únicamente por la entidad concreta y desconocida para cualquier otra entidad. Así, la primera entidad cifraría los datos destinados a la tercera entidad usando la clave pública de la tercera entidad, y la tercera entidad podría descifrar estos datos usando su propia clave privada. El canal de transmisión entre la primera entidad y la segunda entidad, indicado como 60a, es preferentemente un canal de capacidad muy baja, como por ejemplo un canal de código QR, un canal de comunicación de campo próximo o cualquier canal similar. Por último, el tercer canal 60c es, preferentemente, un canal de telefonía móvil, ya que la implementación preferida de la segunda entidad es como teléfono móvil.

[0016] Opcionalmente, la segunda entidad y la tercera entidad también comparten información de clave, como por ejemplo una clave simétrica K2,o, de nuevo, la información de clave necesaria para el cifrado asimétrico, como por ejemplo un par de claves que comprende una clave pública conocida por todos y una clave privada conocida únicamente por la respectiva entidad. Si no se usa ningún cifrado (K2), se prefiere la aplicación de un canal seguro, como el https, entre la segunda y la tercera entidad.

[0017] La fig. 7 ilustra otra implementación del concepto de la fig. 6, en la que se ofrecen más detalles del cifrado mediante el uso de la información de clave K2. En particular, la primera clave es una clave creada en la primera entidad, tal como una clave dinámica ilustrada en 70. En una etapa 71, la primera entidad 11 presenta un código bidimensional que contiene la clave (K2) y datos adicionales, y particularmente la segunda porción de datos de una entidad de datos se indica en 71. Además, la primera entidad envía la clave K2 y otros datos, y específicamente la primera porción de los datos de la tercera entidad 13, tal como se indica en 72. En una etapa 73, la segunda entidad 12 lee el código bidimensional usando una cámara y el producto de *software* correspondiente y descodifica el código bidimensional para extraer la clave K2, tal como se ilustra en 73. A continuación, la segunda entidad 12 cifra la segunda porción de datos que se ha extraído del código bidimensional usando esta clave K2. Entonces, la segunda entidad envía la segunda porción de datos cifrada a la tercera entidad a través del canal de transmisión 60c tal como se indica en 75. En la etapa 76, la tercera entidad descifra el mensaje procedente de la segunda entidad usando la clave K2 enviada por la primera entidad. A continuación, se lleva a cabo en la tercera entidad 13 un emparejamiento de los datos usando la primera porción de datos procedente de la primera entidad 11 y usando la segunda porción de datos procedente de la segunda entidad 12, tal como se ilustra en 77. Si no se usa ningún cifrado, se prefiere la implementación de un canal seguro como el https entre la segunda y la tercera entidad.

[0018] La fig. 8 ilustra otra implementación del concepto de la fig. 7, pero ahora con una segunda información de clave indicada en la fig. 1 como K1. Tras haber creado la clave de cifrado K2 en la etapa 70, la primera entidad cifra la porción de datos (la primera porción de datos) destinada a la tercera entidad usando esta clave K2 y vuelve a cifrar el resultado del cifrado con K2 usando la información de clave K1, que es conocida por la tercera entidad y la primera entidad, en el caso de un algoritmo de cifrado simétrico, o usando la correspondiente clave pública en el caso de un cifrado asimétrico, tal como se indica en 80. Después, la primera entidad envía esta porción de datos doblemente cifrada al servidor, tal como se indica en 81. Además, la primera entidad cifra la clave K2 usando la clave K1 y presenta un código bidimensional que contiene el resultado del cifrado, además de contener la segunda porción de datos. No obstante, ahora se cifrará la segunda porción de datos con K1 y/o K2. Esto se indica en la etapa 82. A continuación, la segunda entidad 12 lee el código bidimensional usando una cámara y el producto de *software* y después extrae el resultado del cifrado, tal como se indica en 83. Después, la segunda entidad envía el resultado del cifrado a la tercera entidad, tal como se indica en la etapa 84 de la fig. 8, y la tercera entidad descifra (85) el resultado del cifrado procedente de la segunda entidad, usando K1, para obtener K2 y la segunda porción de datos. En la etapa 86, el servidor usa K2 para descifrar el archivo de datos recibido, es decir, la primera porción de datos procedente de la primera entidad, y descifra el resultado a partir de K1 para leer la primera porción de datos. A continuación, en la etapa 87, el servidor empareja los datos procedentes de la primera entidad y los datos procedentes de la segunda entidad y este emparejamiento comprende un ensamblado de las dos porciones de datos diferentes, tal como se explicará más adelante. Si no se usa ningún cifrado, se prefiere la implementación de un canal seguro, como el https, entre la segunda y la tercera entidad.

[0019] La primera entidad crea una clave de cifrado dinámica y transfiere esta clave dinámica, por ejemplo, a través de un código 2D a la segunda entidad. La segunda entidad toma la clave y cifra los datos extraídos a partir del código con esta clave (opción: cifrado). En paralelo, la primera entidad envía la clave de cifrado (opción: cifrado) a la tercera entidad. La tercera entidad descifra los datos cifrados (doblemente, de manera opcional) y continúa con la operación, por ejemplo, el emparejamiento de datos o la transferencia de datos (fig. 7).

[0020] Opción: La transmisión de la clave de cifrado también podría cifrarse.

1) La primera entidad crea una clave de cifrado y cifra un archivo de datos por primera vez y vuelve a cifrarlo con una clave ya conocida por la tercera entidad y envía este archivo de datos al servidor. La primera entidad cifra la clave de cifrado dinámica con la clave de cifrado ya conocida por el servidor y la entrega a la segunda entidad, por ejemplo, entre otras posibilidades, en forma de un código 2D. La segunda entidad transfiere la clave de cifrado cifrada al servidor. El servidor solo es capaz de descifrar el archivo de datos cuando dispone de ambos archivos (fig. 8).

2) La primera entidad crea un archivo de datos y cifra el archivo con una clave dada (esta clave se podría renovar para cada nueva transferencia de datos). Tras el cifrado, la primera entidad divide los datos cifrados en dos o más archivos y envía una parte del archivo (o archivos) a la tercera o más entidades y la otra parte a la segunda entidad a través de cualquier tecnología de transferencia conocida o futura, como: TCP/IP, códigos 1D o 2D, etc. La segunda entidad toma los datos y también los envía a la tercera entidad. La tercera entidad reensambla las partes recibidas, descifra los datos y continúa con la operación predefinida, por ejemplo: emparejamiento de datos, transferencia de datos, validación de datos, etc. (fig. 10).

[0021] Opción: La primera entidad, que divide el archivo de datos cifrado, añade a los datos enviados a la tercera entidad el orden de los paquetes enviados a la segunda entidad y añade el orden de los paquetes enviados a la segunda entidad a los datos enviados a la tercera entidad para reensamblar los datos enviados en la dirección correcta.

[0022] Opción 2: La clave de cifrado se divide y se envía por dos vías a la tercera entidad. Opción 3: La clave de cifrado dividida se vuelve a cifrar (doble cifrado).

[0023] Estas tres entidades llevan a cabo una comunicación específica con el fin de implementar una transacción segura. A continuación, se describe una secuencia de mensajes de acuerdo con una forma de realización preferida, en el contexto de la fig. 1a. En una primera etapa 20, la segunda entidad contacta con la primera entidad. Esta etapa puede consistir, por ejemplo, en un mensaje directo a la primera entidad que puede ser, por ejemplo, un punto de venta, y el usuario notifica que el usuario está interesado en adquirir un producto o acceder a un servicio. Esta etapa no requiere que la segunda entidad revele ningún secreto o datos personales al punto de servicio, lo cual es importante. Esta primera etapa de «activación» 20 ni siquiera requiere que la segunda entidad revele su nombre o su identificación.

[0024] Como respuesta a la etapa 20, la primera entidad crea información de la transacción, como se indica en 21. Esta información de transacción puede incluir cualquier tipo de información que identifique una transacción que finalmente se ha de llevar a cabo. La información de transacción puede ser una identificación de la transacción, una descripción de la segunda entidad y/o la primera entidad, una descripción del producto o servicio en cuestión, una descripción del precio en cuestión, sellos de tiempo, etc. Tras generar la información de transacción en la etapa 21, la primera entidad transmite el primer mensaje con la información de transacción al servidor, como se indica en la etapa 22. Además, la primera entidad genera un código de identificación que contiene la información de transacción, tal como se indica en 23. Otra posibilidad consiste en que la primera entidad además cifre un archivo, divida el archivo y lo transmita a través de diferentes medios de transmisión tales como GSM, UMTS, etc. (aunque no se ilustran explícitamente en la fig. 2). Por tanto, la entidad 111 de la fig. 2 también puede producir un archivo dividido o incluso una clave dividida, como se explicará en líneas generales más adelante.

[0025] Cabe señalar que la etapa 22 de la fig. 1a puede comprender una subdivisión de datos llevada a cabo en la primera entidad con el fin de subdividir la entidad de datos, es decir, el conjunto completo de la información de transacción en una primera porción de datos que se introducirá en el primer mensaje y una segunda porción de datos que se introducirá en un segundo mensaje, tal como se menciona, por ejemplo, en la etapa 25 de la fig. 1A.

[0026] El orden de las etapas 22 y 23 se puede invertir y puede haber una cierta distancia temporal entre la generación del código de identificación y la transmisión del primer mensaje al servidor, de manera que la transmisión del primer mensaje al servidor tenga lugar en un momento determinado, posterior a la generación del código de identificación. Además, la transmisión del primer mensaje al servidor puede depender de otra condición más, de manera que la primera entidad reciba información que le permita saber si la segunda entidad realmente ha transmitido un mensaje al servidor o si la segunda entidad, aunque haya iniciado las operaciones de la primera entidad en la etapa 20, ha detenido todo el procedimiento debido a una falta de interés en el producto o servicio ofrecido.

[0027] En la etapa 24, la segunda entidad recibe el código procedente de la primera entidad a través de una comunicación unidireccional y extrae la información de transacción a partir del código. La etapa 24 se implementa preferentemente tomando una fotografía del código de identificación generado y presentando en pantalla por la primera entidad. No obstante, otra posibilidad es que el código de identificación también sea una transmisión de RF, en la que se haga uso, por ejemplo, de tecnología de comunicación de campo próximo o que se trate de una transmisión de audio en el espectro audible o inaudible, desde el punto de servicio al usuario. Esta transmisión también puede ser la transmisión de un correo electrónico o incluso la entrega de un papel con el código de identificación impreso, que el usuario pueda analizar mediante una cámara digital o un escáner.

[0028] Tras extraer la información de transacción a partir del código de identificación en la etapa 24, la segunda entidad transmite un segundo mensaje al servidor, tal como se indica en 25, y el segundo mensaje transmitido al servidor comprende la información de transacción y, preferentemente, información adicional, como se explicará más adelante. En la etapa 26, el servidor empareja ambos mensajes usando sellos temporales, un contador de tiempo, un emparejamiento de identificadores o cualquier otra forma de validar dos mensajes para comprobar si estos mensajes o la información contenida en estos mensajes guardan entre sí una relación predeterminada. Cuando la etapa 26 arroja un resultado negativo, es decir, cuando la comprobación ha puesto de manifiesto que la información contenida en los dos mensajes no guarda entre sí una relación predeterminada o que solo ha llegado uno de los dos mensajes al servidor, se genera una salida de emparejamiento fallido en 27. La acción ejecutada como respuesta a un resultado de emparejamiento fallido puede ser cualquiera de estas dos: transmitir realmente un mensaje de transacción rechazada a la primera entidad y/o la segunda entidad, o simplemente interrumpir el procedimiento sin dar ninguna otra indicación, o incluso puede tratarse de dar una información a la policía u otra autoridad similar en el caso de que se sospeche que se ha cometido un delito.

[0029] El emparejamiento del servidor llevado a cabo en la etapa 26 de la fig. 1A comprende, en una forma de realización de la invención, el reensamblado de las diferentes porciones de datos recibidas por el servidor, procedentes de las diferentes entidades, y el procesamiento adicional de los datos reensamblados. Un procesamiento adicional puede ser, por ejemplo, una operación de descifrado cuando la entidad de datos contenga datos cifrados, y el emparejamiento arrojará un resultado positivo cuando los datos cifrados sean correctos, ya que solo entonces un descifrado producirá un resultado que sea útil. El procesamiento adicional puede consistir en la lectura de un archivo de datos cuando la entidad de datos no esté cifrada. En tal caso, la lectura del archivo de datos solo producirá un contenido útil cuando las porciones de datos estén emparejadas unas con otras, es decir, cuando juntas formen la entidad de datos reensamblada. Un procesamiento adicional puede ser el uso de la entidad de datos como clave para el descifrado, y el descifrado solo producirá un resultado útil cuando la clave, es decir, la entidad de datos, se haya reensamblado correctamente, usando las porciones de datos correctas en un orden correcto.

[0030] Sin embargo, cuando la etapa 26 haya producido un resultado positivo, es decir, un resultado de emparejamiento correcto 28, la transacción identificada por la información de transacción se autorizará en la etapa 44. La etapa 44 puede dar lugar a un mensaje para la primera o la segunda entidad en el que se indique que la transacción ha sido autorizada, pero además de ello o como otra opción, puede dar lugar a otro modelo de comunicación como, por ejemplo, el que se ilustra en la fig. 1b. Tras un resultado de emparejamiento correcto, el servidor puede extraer u obtener de una base de datos información bancaria de la segunda entidad en la etapa 30 a partir de una base de datos alojada en el servidor, o bien del segundo mensaje procedente de la segunda entidad o un mensaje adicional enviado por la segunda entidad. Los datos bancarios, como por ejemplo la información de la cuenta, no se deberían incluir en los datos de transacción. Normalmente, la primera entidad no conocerá los datos bancarios. Por tanto, los datos bancarios se alojan en un servidor y se recuperan a partir de una base de datos local o a partir de un segundo servidor, en función de la información del usuario. Dependiendo de los datos bancarios extraídos, el servidor puede contactar con una compañía de pagos en la etapa 31, y el servidor puede iniciar una transferencia de dinero desde la segunda entidad a la primera entidad en la etapa 32. En el caso de que se obtenga un resultado positivo en la etapa 32, el servidor recibe la confirmación de la transferencia de dinero o cualquier otro mensaje de compensación que indique que con total seguridad se va a recibir una transferencia de dinero. Tras recibir dicha confirmación o mensaje de compensación en la etapa 33, el servidor puede enviar en la etapa 34 una confirmación a la primera y/o la tercera entidad de que todo ha resultado correcto y que la transacción de transferencia se ha efectuado de manera satisfactoria. A continuación, dependiendo de este mensaje enviado por el servidor tras la etapa 34, la primera entidad, finalmente, puede entregar el producto o permitir el acceso a un servicio, o puede llevar a cabo cualquier otra acción por la que se haya pagado con la transferencia de dinero iniciada por el servidor en la etapa 32.

[0031] Se han señalado correspondencias entre las etapas de la fig. 1a y la fig. 1b y la fig. 7a. Una implementación concreta de la etapa 22 consiste en un primer mensaje en el que la parte vendedora solicita a la parte compradora que efectúe el pago. Una implementación concreta de la etapa 24 consiste en que una transferencia de datos de un código de identificación automática tenga lugar sin que haya ningún vínculo entre ambas partes, por ejemplo, a través de una comunicación unidireccional y, preferentemente, a través de una captura óptica con la cámara desde la segunda entidad 12. Una implementación preferida de la etapa 25 consiste en un mensaje enviado por la parte compradora a la parte vendedora que indique que la parte compradora envía una solicitud de pago para pagar a la parte vendedora. Una implementación preferida de una acción como respuesta a la transacción autorizada de la etapa 29 o la acción de envío de confirmación 34 de la fig. 1b consiste en que la compañía de pagos envíe a la parte vendedora información que indique que se ha aceptado el pago o, en su caso, que se ha rechazado. Cuando la solicitud de pago/autenticación es aceptada, la parte vendedora entregará el producto o aceptará la autenticación, y, cuando el pago es rechazado, la parte vendedora no entregará el producto o rechazará la autenticación.

[0032] La fig. 2 ilustra un diagrama de bloques de una primera entidad 11 que puede ser, por ejemplo, un punto de servicio o un portal en línea 11, tal como se indica en la fig. 11, o puede ser un servidor en línea, tal como se indica en la fig. 10. La primera entidad 11 para llevar a cabo una transacción con una segunda entidad 12 bajo el control de un dispositivo servidor 13 comprende preferentemente un generador de información de transacción 110 para generar información acerca de la transacción. Además, se proporciona un generador de códigos de identificación 111, que recibe la información de transacción generada 112 y genera un código 113 que se emite preferentemente a través de una comunicación unidireccional. El código 113 puede ser un código QR o cualquier otro código o procedimiento de identificación automática, en el que el código puede implementarse bajo cualquier forma, por ejemplo: visual, a través de una transmisión de audio o a través de una transmisión de RF. Además, la primera entidad comprende un transmisor de mensajes 114 para transmitir un primer mensaje 115 al servidor, y el primer mensaje 115 comprende la información 112 acerca de la transacción. Además, la primera entidad 11 comprende un receptor de confirmaciones 116 para recibir una indicación de autorización 117 procedente del servidor. En función de la indicación de autorización 117, el receptor de confirmaciones volverá a comprobar si la indicación de autorización pertenece a una cierta información de transacción, lo cual se indica mediante un canal de conexión 118, y finalmente el receptor de confirmaciones autorizará o no una acción. Una acción autorizada puede consistir, por ejemplo, en la entrega de un producto o el permiso para acceder a un servicio, o una operación diferente. La acción autorizada por el receptor de confirmaciones no tiene que ser necesariamente la transacción en la que la información de transacción fue generada por el generador de información de transacción. Cuando la transacción es una transferencia de pago, el receptor de confirmaciones no autorizará esta transacción, ya que esta transacción deberá autorizarla el servidor. No obstante, cuando la transacción sea el acceso a un servicio en línea o un portal en línea, tal como se explicó en relación con la fig. 10 o la fig. 11, la acción autorizada por el receptor de confirmaciones 116 será, de hecho, la transacción identificada en la información de transacción 112. El generador de información de transacción 110 comprende preferentemente el subdivisor de datos para dividir la información de transacción en diferentes porciones de datos, en las que la primera porción de datos se proporciona al transmisor de mensajes 114 para transmitir el primer mensaje, y la segunda porción se proporciona al generador de códigos de identificación 111, de manera que esta porción de datos se pueda emitir a través de una comunicación unidireccional. Cabe señalar que la porción de datos emitida a través del bloque 111 no comprende la emisión de la porción de datos a través del bloque 114 y viceversa, de forma que el primer mensaje y el segundo mensaje comprenden diferentes datos a fin de lograr un concepto de comunicación que presente, por una parte, una seguridad mejorada y, por otra, una mayor eficiencia, y que además sea flexible, concretamente, en lo que respecta a la separación de la entidad de datos en las diferentes porciones de datos y a la determinación del tamaño de las porciones de datos.

[0033] La fig. 3a ilustra una implementación preferida de un dispositivo servidor 13 para controlar una transacción entre una primera entidad 11 y una segunda entidad 12. El dispositivo servidor comprende preferentemente un receptor de mensajes 130 para recibir el primer mensaje 115 procedente de la primera entidad 11, en el que dicho primer mensaje 150 comprende información relativa a una transacción, es decir, preferentemente, la información de transacción 112 generada por el generador de información de transacción de la fig. 2.

[0034] El receptor 130 recibe además el segundo mensaje 125 procedente de la segunda entidad 12, en donde el segundo mensaje comprende además información de transacción relativa a la transacción. Además, el servidor 13 comprende un emparejador 131 para comprobar si la primera información contenida en el primer mensaje 115 y la segunda información contenida en el segundo mensaje 125 guardan entre sí una relación predeterminada. El resultado de 132 de esta operación de comprobación llevada a cabo en el emparejador de mensajes 131 se envía a una interfaz de salida 133 para autorizar la transacción cuando la primera información y la segunda información guardan entre sí una relación predeterminada y para rechazar la transacción cuando la primera información y la segunda información no guardan entre sí una relación predeterminada. La autorización o el rechazo se pueden llevar

a cabo mediante la transmisión de mensajes a través de un canal de autorización/rechazo 134. Además, o como otra posibilidad, se puede activar una interfaz 135 con, por ejemplo, una compañía de pagos o cualquier otra entidad con el fin de llevar a cabo posteriores etapas para completar una transacción. Normalmente, la interfaz 135 solo se activará en el caso de un resultado positivo 132, generado por el emparejador de mensajes 131.

[0035] El emparejador de mensajes 131 comprende, de acuerdo con una forma de realización de la presente invención, un ensamblador de datos o reensamblador de datos para ensamblar la primera porción y la segunda porción con el fin de obtener la entidad de datos usando una regla de ensamblado predefinida o usando información de ensamblado enviada por la primera entidad. Otros detalles acerca del reensamblador o el ensamblador se explicarán en referencia a figuras posteriores.

[0036] Preferentemente, el emparejador de mensajes 131 dispondrá de un sello de tiempo, un contador de tiempo o cualquier otra funcionalidad relativa al tiempo 136, con el fin de llevar a cabo una cierta forma de emparejamiento de mensajes. Preferentemente, ambos mensajes, es decir, el primer mensaje 115 y el segundo mensaje 125 comprenden una identificación de transacción. Además, ambos mensajes pueden comprender una identificación de la primera entidad, pero no tienen que comprender necesariamente una identificación de la segunda entidad. En función de la identificación de transacción y/o la identificación de la primera entidad o en función de cierta identificación de un producto o servicio, por ejemplo, un identificador de producto o el precio de producto, el emparejador de mensajes buscará mensajes recibidos que contengan dicha información relacionada.

[0037] Además, se prefiere la implementación de una característica temporal adicional que garantiza que solo se aceptan como mensajes emparejados aquellos mensajes que ha recibido el servidor dentro de un determinado periodo de tiempo. En este caso, el receptor añadiría un sello temporal a un mensaje recibido que indicase el momento en el que se haya recibido realmente y el emparejador de mensajes podría estar preparado para determinar un emparejamiento únicamente cuando la diferencia de tiempo entre la instancia de tiempo de recepción de los dos mensajes sea menor que un cierto periodo de tiempo, como por ejemplo, una hora o, preferentemente, 30 minutos o, incluso más preferentemente, 5 minutos.

[0038] Como otra posibilidad, el transmisor de mensajes de la primera entidad y el transmisor de mensajes de la segunda entidad añadirán un sello temporal que indique el tiempo de transmisión real y el emparejador de mensajes evaluará una diferencia de tiempo entre estos sellos temporales que, para un emparejamiento positivo, debería ser inferior a un periodo de tiempo predeterminado, como por ejemplo, 60 minutos o, preferentemente, 30 minutos o, incluso más preferentemente, 5 minutos.

[0039] Otra posibilidad consiste en que el código de identificación comprenda de hecho un sello temporal que sea extraído por la segunda entidad y transmitido por la segunda entidad al servidor, en el que se pueda comparar un tiempo de recepción de este mensaje con el tiempo de generación del código de salida, con el fin de obtener un resultado positivo únicamente cuando la diferencia de tiempo entre ambas instancias sea menor que la cantidad predeterminada. Por lo tanto, en general, la funcionalidad temporal 136 del emparejador de mensajes estará preparada para evaluar la diferencia temporal entre dos eventos relacionados con la generación del código de identificación y/o la transmisión del primer mensaje con respecto a una transmisión y/o recepción del segundo mensaje.

[0040] Preferentemente, la aplicación que se ejecuta en un dispositivo móvil que constituye una implementación de la segunda entidad, tal como se explica con respecto a la fig. 4a, se implementará para añadir al segundo mensaje el número de dispositivo del servicio móvil, como por ejemplo el IMEI o MSISDN, IMSI o datos de GPS, para el que se ha registrado la aplicación. El número de dispositivo de servicio móvil es una combinación del número de identificación personal que incluye la tarjeta SIM y un número de serie del teléfono móvil. Por lo tanto, cuando se inserta una tarjeta SIM en un teléfono móvil distinto al teléfono móvil para el que se registró el IMEI o MSISDN o IMSI, un IMEI o MSISDN o IMSI transmitido a través de un segundo mensaje será distinto a un IMEI o MSISDN o IMSI que se transmite junto con el segundo mensaje, debido al protocolo de transmisión de la red de comunicación. Normalmente, cada comunicación, ya sea una llamada telefónica real o una comunicación por SMS, incluye este IMEI o MSISDN o IMSI obtenido, de hecho, a partir de la tarjeta SIM y el número de serie del teléfono móvil. Esta información también se podría obtener directamente de la red del proveedor de servicios de telefonía móvil. Por lo tanto, como se indica en la fig. 3b, el servidor recibirá, en la etapa 40, un primer número de unidad de la segunda entidad mediante la extracción del identificador a partir del segundo mensaje. Este puede ser un IMEI o MSISDN o IMSI, programado de manera fija en la aplicación que se ejecuta en el dispositivo móvil, para la que se registró todo el *software* de pago. También es posible emplear datos de GPS para crear una zona de uso alrededor de un dispositivo como un cajero automático, alrededor de un ordenador personal o de un coche. También es posible

establecer «geovallas» por GPS para zonas especiales, como alrededor de una ciudad, una provincia o un país, etc.

[0041] Además, el servidor recibe un segundo identificador único procedente de la transmisión a través de la red telefónica, que también puede ser un IMEI o MSISDN o IMSI, tal como se indica en la etapa 41. Sin embargo, el IMEI o MSISDN o IMSI extraído en la etapa 41 será diferente del IMEI o MSISDN o IMSI extraído en la etapa 40, cuando el usuario haya insertado una tarjeta SIM en un teléfono móvil diferente al teléfono móvil para el que se registró originalmente todo el servicio de pago.

[0042] El MSDN y/o MSISDN y/o IMEI y/o IMSI también se pueden comprobar por separado con el proveedor de la red de telefonía móvil, por ejemplo, preguntando el MSDN y/o MSISDN y/o IMEI y/o IMSI de la dirección IP de envío (segunda entidad) o simplemente preguntando si la combinación MSDN y/o MSISDN y/o IMEI y/o IMSI y la dirección IP de envío de la segunda entidad es correcta. Los proveedores de servicios de telefonía móvil también ofrecen servicios para introducir la identificación de usuario dentro de un flujo de datos. Es posible utilizar cualquier forma de comprobación a través de una tercera parte, si la información aportada es válida.

[0043] En la etapa 42, el servidor comparará el primer y el segundo identificador único y procederá a llevar a cabo un emparejamiento de mensajes en el elemento 141 de la fig. 3a, cuando ambos identificadores concuerdan, tal como se indica en 43. Sin embargo, cuando ambos identificadores no concuerdan, tal como se indica en 44, el servidor denegará la continuación del procedimiento y podrá adoptar contramedidas, tal como se indica en 45. Por lo tanto, esta comprobación consistirá en una comprobación previa llevada a cabo por el emparejador de mensajes 131, antes de que se lleve a cabo el verdadero emparejamiento de dos mensajes diferentes. Esta comprobación inicial proporciona un examen conveniente y sencillo del segundo mensaje, sin ninguna operación adicional, para rechazar en una fase temprana mensajes no permitidos e incluso ataques hostiles.

[0044] La fig. 4a ilustra la implementación preferida de la segunda entidad 12 para llevar a cabo una transacción con una primera entidad 11 bajo el control de un dispositivo servidor 13. La segunda entidad comprende preferentemente un lector de códigos de identificación 120 para leer un código de identificación generado y emitido por la primera entidad, en el que el código de identificación contiene información codificada acerca de la transacción. En una forma de realización, el lector de códigos de identificación comprende una cámara digital para hacer una fotografía del código 121. Además, la forma preferida de leer el código de identificación será una comunicación unidireccional 122, para lo cual una segunda entidad no tendrá que transmitir ninguna información a la primera entidad y la segunda entidad ejerce un control total sobre qué se transmite, desde qué entidad y a qué entidad. El código 121 se introduce en un proveedor de información 123 para proporcionar la información acerca de la transacción incluida en el código de identificación. En una forma de realización, el proveedor de información será un intérprete de códigos de identificación, como por ejemplo un descodificador de códigos de identificación. Otra posibilidad consiste en que el código de identificación sea descodificado por cualquier otro medio y que el código o la información del código, o al menos la información de transacción, se introduzca incluso manualmente en el sistema, de manera que el proveedor de información fuera un dispositivo de entrada tal como un teclado, un ratón, una bola rastreadora o cualquier otro dispositivo. El proveedor de información 123 generará la información de transacción 124 y remitirá la información de transacción a un transmisor de mensajes 126. El transmisor de mensajes 126 transmitirá el segundo mensaje 125 al servidor, y el segundo mensaje comprende la información de transacción 124.

[0045] Además, la segunda entidad comprende un receptor de confirmaciones 127 para recibir un mensaje de información 128 procedente del servidor, que indica que el segundo mensaje 125 guarda una relación predeterminada con el primer mensaje 115, enviado desde la primera entidad 11. El receptor de confirmaciones generará una salida de confirmación 129. La segunda entidad comprende preferentemente un almacenamiento de información adicional 150, con datos adicionales, como por ejemplo un identificador/IMEI o MSISDN o IMSI único, tal como se explica en relación con la fig. 3b o con información sobre los datos de pago, etc., que se puede remitir al transmisor de mensajes 126, de manera que el segundo mensaje 125 no solo incluya la información de transacción 124, sino también dicha información adicional que se proporciona desde el almacenamiento de información adicional 150.

[0046] La fig. 4b ilustra procesos preferidos llevados a cabo por la segunda entidad 12. En la etapa 50, la segunda entidad se dirige a una primera entidad y activa la primera entidad para generar un código de identificación. En la etapa 51, la segunda entidad lee el código y extrae la información de transacción a partir del código. En la etapa 52, la segunda entidad determina el servidor al que se debe enviar el segundo mensaje. La información contenida en el servidor se puede incluir en la lectura del código de identificación de la etapa 51, y se extrae a partir del código en esta forma de realización. En una forma de realización distinta, la dirección para el servidor al que se debe enviar el

segundo mensaje se puede instalar de manera fija y, por ejemplo, incluirla en el almacenamiento de información adicional 150 de la fig. 4a. En la etapa 53, la segunda entidad, por ejemplo el teléfono móvil o cualquier otro dispositivo móvil o fijo, requerirá que el usuario disponga de una autorización, por ejemplo una contraseña o un número PIN y, preferentemente, la confirmación de una determinada transacción, Además, o como otra posibilidad, la tercera entidad también requiere una autenticación por parte del usuario. A continuación, como respuesta a la etapa 53, el propio usuario humano introducirá la contraseña o el PIN, de manera que la segunda entidad continúe con el procedimiento. En la etapa 54, la segunda entidad generará el segundo mensaje que contendrá la información de transacción y, preferentemente, una identificación de la segunda entidad. La etapa 53 no tiene que llevarse a cabo necesariamente justo antes de la etapa 54, sino que se puede llevar a cabo en cualquier momento anterior a la generación o la propia transmisión del segundo mensaje al servidor. Esto garantiza que el segundo mensaje sea transmitido únicamente desde una segunda entidad que haya sido plenamente autorizada por el usuario humano. En la etapa 55, la segunda entidad recibirá una confirmación de un emparejamiento positivo y/o una confirmación de una transacción satisfactoria.

[0047] Tal como se explica en líneas generales más adelante, una forma de realización adicional comprende la petición del PIN realizada por el servidor en la segunda entidad. De manera simultánea, el servidor envía un nombre de usuario o nombre de cliente a la segunda aplicación en la segunda entidad. Si se ha instalado una aplicación fraudulenta en la segunda entidad y esta aplicación fraudulenta lleva a cabo la comunicación, esta aplicación fraudulenta estará en situación de solicitar el PIN, pero la aplicación fraudulenta no estará en situación de mostrar en pantalla el nombre de usuario o el nombre de cliente, lo cual constituye una característica de seguridad añadida.

[0048] La fig. 5 ilustra seis aplicaciones diferentes y las correspondientes transacciones y una recopilación preferida de información de transacción que se puede incluir en el código de identificación generado por la primera entidad y que también se puede incluir preferentemente en el primer mensaje o el segundo mensaje.

[0049] Posteriormente, se resumirá el procedimiento de la invención y se explicarán detalladamente implementaciones concretas que se resumen en la fig. 5.

[0050] Preferentemente, la información de transacción que se representa como un archivo de datos o que se considera como un archivo de datos comprende la entidad de datos que se va a subdividir en la primera porción de datos y la segunda porción de datos. Otra posibilidad consiste en que se incluya en la entidad de datos otra información pertinente para la tercera entidad o para la transacción deseada o para este el emparejamiento de datos y que se distribuya entre la primera porción de datos y la segunda porción de datos y, dependiendo de otras implementaciones, en otras porciones de datos.

[0051] Desde la introducción del pago electrónico y la autorización de cuentas, los criminales han estado buscando maneras de robar datos confidenciales de pago/cuentas para sus actividades criminales. El objetivo de la solución descrita en la presente patente consiste en reforzar la seguridad de la transacción o autorización de pago (por ejemplo proteger el acceso a un servicio en línea) evitando la necesidad de aportar ningún dato confidencial de pago de la parte compradora (por ejemplo, el número de tarjeta de crédito) a la parte vendedora, que pueda ser utilizado para actividades criminales, al mismo tiempo que se simplifica el uso del pago con móvil. Se puede usar el mismo procedimiento para cualquier otro tipo de autorización, como el acceso a servicios web (correo electrónico), entrada a redes de compañías, etc.

[0052] Como el procedimiento para autorizar el acceso a un servicio en línea es similar al procedimiento de pago, la parte vendedora también puede ser el proveedor de servicios web. La parte compradora puede ser la persona que desea acceder al servicio web. El servidor de pago es el servidor que procesa la autorización. Los datos de pago son similares a las credenciales de acceso. Cada una de las partes involucradas se beneficia de este procedimiento de pago/autorización. Las principales ventajas son:

- La parte compradora no tiene que revelar datos confidenciales, incluidos los datos de pago, a ninguna tercera parte.

- El riesgo de que se haga un mal uso de sus datos se reduce casi a cero.

- El riesgo de que las partes vendedoras revelen involuntariamente los datos confidenciales de pago de sus clientes se reduce de manera considerable, ya que no reciben esos datos. De esta manera se reducen sus esfuerzos dedicados a almacenar y proteger datos de usuario.

- El número de quejas a las compañías de pagos por motivos de fraude se pueden reducir al mínimo.

- Los compradores no necesitan introducir datos en su teléfono móvil, ya que esto lo realiza la aplicación mediante la lectura del código de identificación automática.

- En el caso de los procedimientos de autorización, la mayor ventaja es que, incluso si alguien robara los datos, nadie será capaz de usar los datos robados.

[0053] En los actuales modelos de pago/autorización, a menudo es necesario que la parte compradora aporte datos confidenciales de pago a la parte vendedora. En algunos casos, estos datos pueden ser copiados fácilmente y robados. Estos riesgos también se contemplan para los procedimientos de autorización. He aquí algunos ejemplos reales:

- Robo durante la transmisión de datos.

- Robo de los datos alojados en el servidor de la parte vendedora (por ejemplo, hacking, robo in situ, etc.).

- Manipulación fraudulenta de los dispositivos de lectura para captar los datos confidenciales de pago (por ejemplo, lectores de tarjetas manipulados, teclados manipulados, robo de datos para clonación de tarjetas o *skimming*, etc.).

- Actos delictivos perpetrados por personas durante procedimientos de pago de tipo CNP (sin presencia física de tarjeta).

- Copia de datos de la tarjeta de crédito en restaurantes, etc.

- Robo de credenciales de acceso.

[0054] Lo esencial de esta nueva solución es un concepto o procedimiento en el que la parte compradora no tiene que aportar datos confidenciales de pago (como números de tarjeta de crédito) a la parte vendedora para llevar a cabo la transacción de pago. Este concepto se podría utilizar también para cualquier otra acción en la que sea necesaria una autenticación/autorización. El identificador de transacción enviado por la parte compradora y vendedora es comparable al servidor (de pago/autorización).

[0055] En este nuevo concepto/método de pago/autorización, se usan tecnologías existentes, pero se hace de tal manera que las debilidades de los actuales procedimientos de pago/autorización se reducen sustancialmente.

[0056] Esto se logra mediante la captura/lectura de un código de identificación automática (por ejemplo, el código QR), proporcionado por la parte vendedora, con un dispositivo (por ejemplo, un teléfono móvil, etc.). Mediante la captura/lectura del código de identificación automática, los datos contenidos en el código de identificación automática son recibidos por la parte compradora (por ejemplo, la captura/lectura óptica con una cámara, etc.). Estos datos (o partes de los datos) se envían (por ejemplo, a través de una red de telefonía móvil, etc.) al servidor de pago seguro que está conectado con la compañía de pagos del comprador. Otra solución consiste en que el usuario (la parte compradora) lea el código de identificación automática y lo introduzca manualmente en el dispositivo (móvil).

[0057] Preferentemente, la información de transacción que se representa como un archivo de datos o que se considera como un archivo de datos comprende la entidad de datos que se va a subdividir en la primera porción de datos y la segunda porción de datos. Otra posibilidad consiste en incluir en la entidad de datos otra información pertinente para la tercera entidad o para la transacción deseada o para el emparejamiento de datos, y distribuirla entre la primera porción de datos y la segunda porción de datos, y, dependiendo de otras implementaciones, en otras porciones de datos.

[0058] La fig. 6 ilustra un modelo entre diferentes entidades, en el que la primera entidad es, por ejemplo, una tienda, la segunda entidad es, por ejemplo, un teléfono móvil y la tercera entidad es, por ejemplo, un servidor que empareja mensajes procedentes de la primera entidad y la segunda entidad, tal como se explica anteriormente, con el fin de llevar a cabo finalmente una determinada acción, que depende del resultado del emparejamiento. Cuando los mensajes concuerdan, se lleva a cabo una determinada acción y, cuando los mensajes no concuerdan, no se llevará a cabo una acción determinada, en la que esta acción puede ser, por ejemplo, una transacción de pago, etc.

[0059] En una forma de realización, la primera entidad y la tercera entidad comparten un secreto o, dicho de otro modo, una clave de cifrado K1. Esta clave es conocida por la primera entidad y la tercera entidad, pero no por la segunda entidad. Por otra parte, la segunda entidad y la tercera entidad comparten un secreto o, dicho de otro modo, una clave K2. Como es natural, este secreto o clave en común no tiene que ser necesariamente una clave de cifrado simétrica, los mismos procedimientos se pueden aplicar en el contexto del cifrado asimétrico en el que existe una clave pública y una privada. No obstante, en esta aplicación, es importante que la autenticación de la clave sea segura, la cual puede llevarse a cabo, por ejemplo, mediante un certificado emitido por una autoridad de autenticación acreditada.

[0060] La fig. 7 ilustra otra forma de realización, en la que la clave K2 es generada por la primera entidad y transmitida a la segunda entidad a través de un código 2D. Otra posibilidad distinta al procedimiento ilustrado en la fig. 7 consiste en que la transmisión entre la primera entidad y la tercera entidad se lleve a cabo empleando texto sin formato en lugar de estar cifrada mediante la clave K1 conocida por la primera entidad y la tercera entidad, pero desconocida para la segunda entidad. Resulta ventajoso para esta aplicación que las claves se puedan generar de manera descentralizada, es decir, por la primera entidad, que es, por ejemplo, un punto de servicio, tienda o similar. Este dispositivo solo precisa un simple generador de números aleatorios para generar una clave que después pueda transferirse desde la primera entidad a la segunda entidad. En esta implementación, la generación de la clave de manera descentralizada por la primera entidad es muy eficiente, ya que ni la segunda entidad, que suele ser un teléfono móvil, ni la tercera entidad deben llevar a cabo ningún tipo de gestión de claves que, en otro caso, sería necesaria. Debido a que este servicio está destinado a cualquier transacción de pago o transacción de servicio imaginable, tal como se define en la fig. 5, el número de usuarios puede ser extremadamente alto, y, por lo tanto, el número de claves que la tercera entidad o los teléfonos móviles deberían gestionar sería muy alto, lo cual se traduciría de nuevo en costes elevados. Todo esto no es necesario cuando las claves las genera la primera entidad, es decir, la tienda o un punto de servicio.

[0061] La fig. 8 ilustra otra forma de realización, en la que tiene lugar un doble cifrado, y en la que la clave K2 se genera de manera descentralizada.

[0062] La fig. 9 ilustra un modelo, en el que la tercera entidad lleva a cabo un emparejamiento con datos procedentes de múltiples entidades. Los datos procedentes de múltiples entidades se pueden emparejar usando preferentemente el procedimiento descrito en relación con la fig. 10. Para múltiples entidades, el mensaje mencionado en la fig. 10 o la clave de cifrado u otros datos que se vayan a transmitir por partes a través de diferentes canales de transmisión se deben dividir en un número de partes que sea al menos igual al número de entidades -1. Por lo tanto, cuando hay 5 entidades, en las que la tercera entidad es un servidor, el servidor debería emparejar los datos de cuatro entidades, es decir, la primera entidad, la segunda entidad, la cuarta entidad y la quinta entidad, lo cual significa que se tienen que generar al menos cuatro partes de un archivo o clave cuando se divide el archivo cifrado o la clave cifrada o la clave en texto sin formato o incluso el archivo de texto sin formato.

[0063] La fig. 11 ilustra otra forma de realización, en la que el archivo cifrado o la clave cifrada se divide en varias porciones. Se pone de manifiesto que la primera entidad, por ejemplo, divide la clave de cifrado, que ha sido generada por la primera entidad, en ocho porciones. Las porciones 3724 se transmiten junto con datos cifrados a la segunda entidad, preferentemente mediante un código de identificación automática. La segunda entidad simplemente usa estas porciones 3724 junto con los datos cifrados y envía este mensaje de datos a la tercera entidad. La tercera entidad recibe los datos cifrados enviados por la primera entidad junto con las porciones 6815, es decir, las otras cuatro porciones de la clave de cifrado. En este momento, la tercera entidad puede extraer las porciones 6815 y 3724 de los mensajes enviados desde la primera entidad a la segunda entidad con el fin de ensamblar la clave y, posteriormente, la tercera entidad puede descifrar los datos cifrados recibidos que proceden de la segunda entidad, haciendo uso de esta clave reensamblada. A continuación, la tercera entidad puede emparejar los datos descifrados a fin de averiguar si estos datos guardan entre sí una relación predeterminada, de manera que, al final, se pueda iniciar una transacción de pago o cualquier otra transacción tal como se explica en relación con la fig. 5, en el caso de que se produzca un emparejamiento positivo, o que se pueda denegar en el caso de un emparejamiento negativo. Un modo de emparejar los datos consiste en que los datos descifrados enviados por la primera entidad y los datos descifrados enviados por la segunda entidad sean idénticos entre sí.

[0064] Cabe destacar que la forma de realización de la fig. 11 solo requiere una única clave generada por la primera entidad de manera descentralizada. La primera entidad usa esta clave para cifrar datos a fin de obtener datos cifrados. La clave se transmite a la tercera entidad a través de los dos canales de comunicación diferentes y en porciones. De este modo, cualquier atacante que lea la comunicación entre la primera entidad y la segunda entidad o que lea la comunicación entre la segunda entidad y la tercera entidad o que solo lea la comunicación entre

la primera entidad y la tercera entidad no estará en situación de descifrar los datos cifrados, debido al hecho de que cada comunicación solo incluye una parte de la clave, en lugar de contener toda la clave. Es evidente que todas las partes de la clave están en forma de texto sin formato, pero una única porción de la clave en texto sin formato no será suficiente para descifrar los datos cifrados.

[0065] Este modelo resulta particularmente útil para aplicaciones de pago, ya que la primera entidad, que es preferentemente un punto de venta/punto de servicio/tienda, es la única que tiene que generar una única clave para cada transacción mediante un generador de números aleatorios, un generador de números pseudoaleatorios o un almacenamiento digital (de semiconductor) en el que se almacena un número determinado de claves generadas previamente. Además, la primera entidad debe estar en posesión de una funcionalidad de cifrado, pero la segunda entidad, que normalmente es un teléfono móvil, simplemente tiene que leer, en una forma de realización preferida, el código QR que contiene la porción de clave 3, 7, 2, 4 y los datos cifrados y extraer estos datos del código QR, de manera que estos datos se puedan retransmitir a la tercera entidad. De este modo, la segunda entidad no necesita ninguna clave en esta forma de realización.

[0066] Solo el servidor/tercera entidad necesita disponer de una capacidad de descifrado y necesita un conocimiento incluido en la transmisión, o bien acordado de antemano, acerca del modo en que se deben unir entre sí las diferentes porciones de la clave procedentes de la primera entidad y de la segunda entidad.

[0067] En una forma de realización, el mensaje enviado por la segunda entidad a la tercera entidad incluye además información acerca del modo en que se deben ensamblar las porciones de clave transmitidas desde la primera entidad a la tercera entidad, y el mensaje de la primera entidad a la tercera entidad comprende además información acerca del modo en que se deben ensamblar las porciones de clave incluidas en el mensaje de la segunda entidad a la tercera entidad.

[0068] Además, se podría cifrar una porción de clave, como la porción de clave 6815 transmitida desde la primera entidad a la tercera entidad, usando como clave las otras porciones de clave, como la 3724. En esta forma de realización, la transacción entre la primera entidad y la tercera entidad sería incluso una transacción cifrada con respecto a la porción de clave 6815, y la tercera entidad tendría que extraer en primer lugar las porciones de clave 3724 en forma de texto sin formato para descifrar la porción de clave cifrada 6815, de manera que, posteriormente, se recupere la clave completa para los datos cifrados y sea usada por la tercera parte para descifrar ambos datos a fin de estar en situación de llevar a cabo finalmente un emparejamiento de datos.

[0069] A continuación, se explica otra forma de realización preferida en relación con la fig. 6. En cuanto la tercera entidad haya determinado que los datos procedentes de la primera entidad y los datos procedentes de la segunda entidad concuerdan entre sí, el pago se puede autorizar. No obstante, a fin de obtener una mayor seguridad, la tercera entidad genera una petición a la segunda entidad mediante la cual se insta a la segunda entidad a que introduzca un número de identificación personal similar a los números de identificación personal que se introducen en el cajero automático de un banco. La tercera entidad cifra esta petición usando la clave K2 y la transmite a la segunda entidad de forma cifrada. En este momento, la segunda entidad descifra esta petición usando la clave K2 y presenta esta solicitud en la pantalla de un teléfono móvil. A continuación, el usuario introduce su PIN únicamente en su teléfono móvil, y su teléfono móvil recibe este número de identificación personal, cifra el número de identificación personal recibido y vuelve a enviar el número de identificación personal cifrado a la tercera entidad. Entonces, la tercera entidad comprueba si el número de identificación personal, que se ha obtenido descifrando el mensaje procedente de la segunda entidad usando la segunda clave, concuerda con un número de identificación personal almacenado previamente y gestionado por el servidor. Cuando este emparejamiento se determina de forma concluyente, la tercera entidad finalmente inicia una acción de pago o cualquier otra acción, tal como se explica en relación con la fig. 5. Por tanto, el emparejamiento entre mensajes se lleva a cabo como forma de comprobación previa, y solo cuando este emparejamiento es positivo, la tercera entidad solicitará a la segunda entidad una transmisión del PIN cifrado desde la segunda entidad. De este modo, se garantiza que cualquier transmisión de un PIN cifrado desde la segunda entidad a la tercera entidad acreditada solo tenga lugar cuando la comprobación previa haya arrojado un resultado positivo, es decir, cuando se pueda afirmar con una alta probabilidad que no se ha producido ningún ataque.

[0070] Además, se puede obtener una mayor seguridad cuando la tercera entidad, en el momento de preguntar a la segunda entidad el PIN, transmite también un nombre de usuario de la segunda entidad registrado en la tercera entidad. A continuación, la aplicación de *software* que se esté ejecutando en la segunda entidad presentará en pantalla este nombre de usuario y pedirá al usuario del teléfono móvil que introduzca el PIN. Cuando el nombre de usuario que se presenta en la pantalla del teléfono móvil no es el que el usuario esperaba, el usuario puede cancelar

todo el procedimiento, ya que es muy probable que se haya producido algún ataque, por ejemplo, en el *software* o el *hardware* del teléfono móvil o en la transacción. En dicho ataque, una aplicación fraudulenta que se esté ejecutando en el teléfono móvil podría presentar siempre, como nombre de usuario, el nombre de usuario que el usuario haya establecido para su teléfono móvil, como por ejemplo su nombre personal, pero cuando el usuario ha seleccionado un nombre de usuario diferente, como por ejemplo un apodo para un registro con la tercera entidad, se obtiene una mayor seguridad.

[0071] A continuación, se explicará otra forma de realización de la presente invención en relación con la fig. 9, que se puede usar no solo a efectos de pago, sino también para otros modelos de aplicación. Un modelo de este tipo consiste en que, para una determinada transacción, al superar una cantidad de dinero predeterminada, deben firmar al menos dos directores generales (CEO) de una compañía. Dicho de otro modo, el modelo se refiere al visto bueno a una operación con una cierta suma de dinero que requiere las firmas de al menos dos directores generales. Este modelo se refiere a cuatro entidades. La cuarta entidad, que es, por ejemplo, un banco o una institución de pago, pide una autorización del pago. Con este fin, la cuarta entidad genera un archivo de datos que se divide en tres porciones. La primera porción se transmite a una primera entidad, que se usa para generar códigos QR. La segunda porción se envía a una segunda entidad, que es, por ejemplo, el teléfono móvil de uno de los directores generales, y la tercera porción se envía a la tercera entidad, que es otro teléfono móvil del otro director general. La primera entidad genera un código QR para el primer director general, y el primer director general adquiere y descodifica este código QR a fin de obtener la segunda porción de los datos. Además, la primera entidad presenta en pantalla la primera porción de los datos al segundo director general (tercera entidad), y el segundo director general adquiere y descodifica la tercera porción de los datos. En este momento, el primer director general (segunda entidad) y el segundo director general (tercera entidad) vuelven a transmitir sus porciones de datos a la primera entidad o incluso al banco, en donde el banco también puede recibir la primera porción de nuevo procedente de la primera entidad. No obstante, cuando el primer director general (segunda entidad) y el segundo director general (tercera entidad) vuelven a enviar sus datos a la primera entidad, preferentemente, con una clave de cifrado dedicada que solo es conocida por la primera entidad y por el correspondiente director general y es desconocida para el otro director general, la primera entidad puede llevar a cabo un emparejamiento de datos en el que la primera entidad comprueba si los trozos de datos, es decir, la segunda porción enviada por el primer director general, concuerdan con la tercera porción enviada por el segundo director general y con la primera porción alojada en la primera entidad.

[0072] Tras este emparejamiento, la primera entidad puede comenzar una comunicación con el primer director general y con el segundo director general, tal como se explica más arriba, de manera que el primer director general y el segundo director general puedan introducir su PIN en sus respectivos teléfonos móviles para iniciar una transmisión cifrada para confirmar finalmente un pago o un procedimiento de aprobación. De nuevo, esta petición del PIN y su transmisión solo se llevan a cabo después de que se haya producido un emparejamiento positivo.

[0073] Otra implementación para obtener dos firmas de directores generales residentes en lugares distintos sería la siguiente. La primera entidad 11 de la fig. 9 tiene un cierto contrato que precisa la firma de dos diferentes directores generales de una compañía. Un director general está representado por la segunda entidad y el otro director general está representado por la entidad xxx 90. Otra posibilidad consiste en que la entidad de datos no tenga que ser necesariamente un contrato, sino que pueda ser también una instrucción de procesamiento de pago para iniciar una acción de pago, o cualquier otra instrucción para iniciar cualquier tipo de transacción distinta a una transacción de pago. La primera entidad dividiría entonces esta entidad de datos, es decir, el contrato o el documento con la instrucción de transacción, en tres porciones diferentes. La primera entidad transmitiría la primera porción directamente a la tercera entidad 13. Además, la primera entidad 11 se encargaría de presentar en pantalla la segunda porción con respecto a la segunda entidad en forma de, por ejemplo, un código QR y la segunda entidad 12 capturaría esta segunda porción. La tercera porción también se presentaría en pantalla a la tercera entidad 90, preferentemente también como un código QR, de manera que la tercera entidad 90 también pueda capturar este QR. Esto se puede obtener, por ejemplo, cuando la segunda entidad 12 y la tercera entidad 90 acceden a una página web bajo el control de la primera entidad 11, pero la segunda entidad y la tercera entidad, que corresponden a los teléfonos móviles de los respectivos directores generales, residen en distintos puntos geográficos.

[0074] A continuación, la segunda entidad 12 intentaría enviar su porción de datos a la tercera entidad 13. Tras enviar la porción de datos o antes de enviar la porción de datos, la tercera entidad pediría a la segunda entidad una identificación personal y, en cuanto se verificase la identificación personal de la segunda identidad 12, la segunda entidad transmitiría la segunda porción de datos, o si la segunda porción de datos ya se ha transmitido, la tercera entidad continuaría procesando la segunda porción de datos recibida. Para reforzar la seguridad de la verificación o autorización, la tercera entidad enviaría un nombre de usuario registrado por el director general que procesa la segunda entidad previamente. Entonces, el segundo director general, al que se le solicita que introduzca la

información de identificación personal, también podría verificar el nombre de usuario presentado en pantalla para comprobar si el nombre de usuario presentado en pantalla es el nombre de usuario esperado o se trata de cualquier otro nombre de usuario. Si aparece cualquier otro nombre de usuario, podría ser una indicación de que se ha producido cualquier tipo de ataque, bien en el *software* del teléfono móvil o bien en el canal de transmisión desde la tercera entidad a la segunda entidad.

[0075] Con la tercera entidad 90 se lleva a cabo el mismo procedimiento y, en cuanto ambas entidades 12, 90 han recibido la autorización, la tercera entidad empareja las porciones de datos procedentes de estas entidades mediante el reensamblado de las porciones de datos. Entonces se obtiene una entidad de datos reensamblada, que se continúa procesando, por ejemplo mediante un lector de documentos, un almacenamiento de documentos, una activación de una instrucción o similares. Tras leer el documento reensamblado, se pondrá de manifiesto si las tres diferentes porciones de datos forman una unidad o concuerdan entre sí. Si no es el caso, el contenido del documento resultará inservible. Otras operaciones de procesamiento adicionales son el descifrado del archivo de datos cifrado consistente en las tres porciones de datos, en el que el descifrado revelará si las porciones de datos procedentes de las diferentes entidades fueron recibidas correctamente, ya que de no ser así, el resultado del descifrado sería un error o un documento inservible que no contendría ninguna información útil.

[0076] Las figs. 12 a 17 ilustran formas de realización para otra implementación y requisitos y funcionalidades de las tres entidades de acuerdo con un aspecto de la invención.

[0077] La fig. 12 ilustra una topología en la que la primera entidad es un punto de servicio/tienda web, la segunda entidad es un teléfono móvil y la tercera entidad es un servidor de emparejamiento, y en la que la entidad de datos se ha subdividido en el punto de servicio/tienda web 11 y se ha reensamblado en el servidor de emparejamiento 13. La fig. 13 ilustra detalles de cifrado para procedimientos de cifrado entre las diferentes entidades. Preferentemente, el archivo de datos/entidad de datos usado por la tienda web 11 para la subdivisión con el fin de obtener la primera y la segunda porción de datos es un archivo cifrado, preferentemente mediante un cifrado AES. Para ello, se usa una clave de cifrado simétrico conocida por la primera entidad 11 y por la tercera entidad 13 y desconocida para la segunda entidad. La segunda entidad 12 transmite la segunda porción de datos recibida, procedente de la primera entidad 11, a la tercera entidad de forma cifrada tras haber sido autorizada usando un PIN de información de identificación personal.

[0078] La fig. 14 ilustra las diferentes tareas llevadas a cabo por la primera entidad 11 y la segunda entidad 12, en las que la primera entidad 11 posee dos partes diferentes de generación de datos, en la que una parte de generación de datos sirve para generar y cifrar datos destinados específicamente al teléfono móvil 12, y en la que la otra parte de generación de datos sirve para generar y cifrar datos destinados al servidor 13. Ambas partes se incluyen en un código QR, tal como se ilustra en la fig. 14. La primera entidad 11 presenta en pantalla el código QR, el cual es adquirido por el teléfono móvil y procesado por el teléfono móvil, en donde los datos para el servidor, es decir, la porción de datos de la entidad de datos, se envía desde el teléfono móvil al servidor, y en donde la porción de datos destinada al teléfono móvil es descifrada por el teléfono móvil 12. Por lo tanto, los bloques de cifrado en el bloque 11 de la fig. 14 usan diferentes claves, y se usa una primera información de clave K1 para la comunicación segura entre la primera entidad y la tercera entidad, y se usa una segunda información de clave K2 para la comunicación segura entre el teléfono móvil 12 y el servidor 13.

[0079] La fig. 15 ilustra una información de implementación para el procedimiento que se muestra en la fig. 14.

[0080] La fig. 16 y la fig. 13 ilustran implementaciones preferidas de la presente invención, en las que la entidad de datos es una entidad de datos cifrada generada como salida por el bloque 160 y alojada en la primera entidad. La entidad de datos se ilustra específicamente en 161 y la primera porción de datos se indica en 162 como los «bytes restantes» dentro del archivo cifrado, y la segunda porción de datos se indica en 163. La segunda porción de datos se procesa para obtener un código QR 164 y el teléfono móvil adquiere el código QR 164. Además, la primera porción de datos 162 se transmite como primer mensaje 165 al servidor, mientras que la segunda porción de datos se incluye en el segundo mensaje 166. Preferentemente, la entidad de datos comprende los datos de transacción o los datos de clave generados por un generador de datos 167.

[0081] En la fig. 17, los números de referencia similares indican elementos similares con respecto a la fig. 16. Como se pone de manifiesto particularmente en la fig. 16, el servidor 13 (tercera entidad) sabe qué bytes se han quitado y en qué dirección se han quitado los bytes. El servidor 13 reensambla los datos y solo cuando se han reensamblado los datos correctos en el orden correcto, se pueden descifrar los datos o el descifrado da lugar a un texto sin formato que resulta útil. El resultado de la información del ensamblado llevado a cabo en el servidor, que

puede ser controlado por una información de subdivisión/ensamblado transmitida específicamente desde la primera entidad, es el reensamblado de los datos, es decir, que se obtiene la entidad de datos 168, que después se puede seguir procesando, por ejemplo descifrándola o procesándola de cualquier otro modo descrito anteriormente.

[0082] El aspecto está relacionado con un procedimiento y un aparato para reducir el tráfico de datos y mejorar la seguridad mediante una transmisión bidireccional, una primera entidad, una segunda entidad y una tercera entidad.

[0083] En la actualidad, la transferencia de datos está expuesta a fallos de seguridad como el *phishing*, ataques de intermediarios, robo de contraseñas, etc. El aspecto ilustrado indica la manera de reducir el tráfico de datos mediante una transmisión bidireccional o multidireccional.

[0084] En una forma de realización, se quitan 1-x bytes del conjunto de datos, en donde x es menor que la cantidad total de datos, de manera que uno tenga al menos 2 partes (pero sin limitarse a este número). La primera parte restante se enviará al servidor directamente. La otra parte se enviará a través de la tercera entidad, por ejemplo un teléfono móvil mediante cualquier tecnología de transmisión, preferentemente mediante una tecnología de identificación automática como los códigos 1D, 2D o NFC. En especial, el uso de códigos 2D mejora la seguridad y protege la privacidad del usuario del teléfono móvil, ya que la primera entidad en este caso no conoce nada acerca de la segunda entidad. Debido a que las partes individuales resultan inservibles sin la otra u otras partes, solo el servidor es capaz de reensamblar los datos después de que haber recibido todas las partes. Un potencial atacante tiene que captar todos los datos a través de todas las vías de comunicación y además tiene que saber cómo reensamblarlos y quizás también cómo descifrarlos y con qué clave. Al quitar algunos bytes de los datos originales, ya no hay necesidad de usar tecnologías de compresión.

[0085] Además, se prefiere distribuir las porciones de datos de manera desigual en ambas «direcciones». En cambio, más del 50 por ciento de todos los datos se envía desde la entidad al servidor directamente, y menos del 50 por ciento se incluye en la representación de tecnología de identificación automática, como por ejemplo códigos 1D, 2D o NFC. Esto ofrece la ventaja de que se pueden introducir menos datos en los códigos 1D, 2D o NFC. Esto se traducirá inmediatamente en una mejora en la velocidad de generación de códigos 1D, 2D o NFC y además, lo que es aún más importante, se traducirá en una mejora de la velocidad de lectura de, por ejemplo, una lectura de un código QR realizada por un teléfono móvil. Aunque los datos se distribuyan de manera desigual, no se produce una reducción en la seguridad.

[0086] Una secuencia de etapas preferida es:

El punto de servició generó un registro de datos.

Este registro de datos se cifra mediante, por ejemplo, un cifrado AES.

[0087] A partir del registro de datos cifrado, se quitan x bytes. Por ejemplo, el registro de datos contiene 512 bytes, y se quitan 20 bytes. El servidor sabe qué bytes se han quitado y en qué orden se ha hecho.

[0088] El resto de los bytes se envían directamente al servidor.

[0089] Los bytes restantes (por ejemplo, los 20 bytes) se empaquetan en un código QR, son presentados en pantalla por el punto de servicio, leídos por el teléfono móvil y enviados desde el teléfono móvil al servidor.

[0090] El servidor reconstruye el registro de datos cifrado y descifra el registro de datos reconstruido. Aunque el cifrado aumenta la seguridad, otra forma de realización también puede usar solo una versión comprimida (y no cifrada) del registro de datos o incluso el propio registro de datos sin ninguna comprensión y/o cifrado.

[0091] Algunas ventajas son que las manipulaciones se pueden detectar inmediatamente, que ambos registros de datos resultan ilegibles individualmente incluso para alguien que tuviera la clave, y que se mejora la velocidad de lectura debido a la distribución desigual.

[0092] Se prefiere introducir menos del 40% de un registro de datos e incluso menos del 20% o incluso menos del 10% o incluso menos del 5% del registro de datos en el código y enviar la mayoría del registro de datos restante directamente al servidor.

[0093] La fig. 18 ilustra un diagrama de bloques detallado de una primera entidad para comunicarse con una

segunda entidad y una tercera entidad de acuerdo con una forma de realización de la invención. La primera entidad comprende un subdivisor 180 para subdividir una entidad de datos 182 en una primera porción de datos 162 y una segunda porción de datos 162 y, preferentemente, otras porciones de datos 183. Además, el subdivisor de datos está configurado para generar información de la subdivisión 184 que indica la manera de subdividir la entidad de datos, en la que la información de subdivisión/ensamblado 184 se puede transmitir a la tercera entidad a través de un mensaje dedicado o se puede adjuntar al primer mensaje 165 y/o el segundo mensaje 166 como información adicional o información complementaria. Además, la primera entidad comprende una interfaz de salida 181 para transmitir el primer mensaje 165 a la tercera entidad, en la que el primer mensaje no comprende la segunda porción de datos. Además, la interfaz de salida 182 está configurada para emitir un segundo mensaje 166, lo cual puede producirse a través de una presentación de un código QR, pero también puede producirse a través de cualquier otro tipo de interfaz de salida. El segundo mensaje 166 comprende la segunda porción de datos 163 y no comprende la primera porción de datos 162.

[0094] En una forma de realización en la que la información de subdivisión/ensamblado se transmite desde el subdivisor de datos 184 a la tercera entidad, no es necesario acordar previamente entre la primera entidad y la tercera entidad el modo en que se lleva a cabo la subdivisión. No obstante, en otras formas de realización, la primera entidad y la tercera entidad acuerdan un tipo específico de modo de subdivisión correspondiente a un modo de ensamblado específico, de manera que no haya que generar ninguna información de subdivisión/ensamblado o no haya que transmitirla.

[0095] Dependiendo de las formas de realización específicas, la entidad de datos puede ser un archivo de datos o una clave, y se prefiere transmitir el primer mensaje a través de un canal de alta capacidad tal como Internet, un canal telefónico, una conexión dedicada o similar, mientras que el segundo mensaje comprende un canal de baja capacidad, como por ejemplo una adquisición de código QR, una comunicación de campo próximo o cualquier otro canal de comunicación relacionado que solo disponga de una capacidad más pequeña que el canal a través del cual se transmite el mensaje 165.

[0096] Preferentemente, el segundo mensaje que comprende la segunda porción solo contiene un pequeño porcentaje de los bytes de toda la entidad de datos, y se prefieren por ejemplo valores inferiores al 10% de los bytes de la entidad de datos para la segunda porción de datos y más del 90% de los bytes de la entidad de datos para la primera porción de datos, de manera que se obtenga una excelente adaptación de la cantidad de datos transmitidos a la capacidad del canal de datos. Además, la capacidad de procesamiento de la segunda interfaz, que normalmente sería un teléfono móvil, es decir, el receptor, para el segundo mensaje se puede implementar fácilmente y toda la potencia de procesamiento requerida para procesar la segunda porción de datos también es baja. Debido a que la segunda entidad de datos es preferentemente un dispositivo móvil, la reducción de la carga de procesamiento en este dispositivo ofrece muchas ventajas, desde los costes para el usuario a una reducción en el consumo de baterías, etc.

[0097] En una forma de realización, la entidad de datos es una clave, de manera que el generador de datos 167 es un generador de claves 167 en la primera entidad. El generador de claves puede generar la clave dinámica K2, tal como se explica en el contexto de la fig. 7 y la fig. 8, y puede proporcionar la clave al cifrador 160 con el fin de cifrar datos tales como los datos/información de transacción, tal como se explica en el contexto de la fig. 5, que también se proporciona al cifrador 160, tal como se ilustra en la fig. 18. Entonces, la salida del cifrador 160 será la entidad de datos cifrada.

[0098] Además, o como otra posibilidad, el cifrador 160 puede recibir la información generada no localmente en la primera entidad, en la que la información de clave puede ser una clave simétrica conocida únicamente por la tercera entidad y la primera entidad o puede ser una clave pública de la tercera entidad en el contexto de un algoritmo de cifrado asimétrico. Dependiendo de la implementación, el subdivisor de datos también puede estar configurado para aleatorizar bytes de la entidad de datos seleccionados para la segunda porción de datos mediante el uso de información de aleatorización/codificación que permite un descifrado en la tercera entidad y que no permite un descifrado en la segunda entidad.

[0099] La fig. 19 ilustra una forma de realización preferida de una tercera entidad para la comunicación con una primera entidad y una segunda entidad, en la que la tercera entidad comprende una interfaz de entrada 193 para recibir un primer mensaje 165 procedente de la primera entidad y un segundo mensaje 166 procedente de la segunda entidad, en la que el primer mensaje comprende una primera porción de una entidad de datos y en la que el segundo mensaje comprende la segunda porción de la entidad de datos. Además, se proporciona un procesador de mensajes 192 para procesar el primer mensaje y el segundo mensaje, con el fin de obtener la primera porción de

la entidad de datos y la segunda porción de la entidad de datos extraída de los mensajes. La primera porción y la segunda porción obtenidas mediante el bloque 192 se introducen en un ensamblador de datos 194 que ensambla la primera porción y la segunda porción para obtener la entidad de datos 168. El ensamblador de datos 190 está configurado para usar una regla de ensamblado predefinida o para usar información de ensamblado proporcionada a través de la línea 195 de la interfaz de entrada 193, cuando la información de subdivisión/ensamblado se transmite a través de un mensaje distinto desde la primera entidad a la tercera entidad. No obstante, cuando la información de subdivisión/ensamblado 195a se adjunta al primer mensaje 165 o al segundo mensaje 162, el procesador de mensajes 192 extrae la información de subdivisión/ensamblado y proporciona esta información a través de la línea 195b al ensamblador de datos 190. Dependiendo de la implementación, la interfaz de entrada está configurada para recibir más mensajes de otras entidades y, por lo tanto, el procesador de mensajes 192 extraerá más de dos porciones de datos, tal como se indica a través de la línea 196.

[0100] La entidad de datos 168 se introduce preferentemente en un procesador de entidades de datos 197, que se implementa como un emparejador de datos específico para emparejar datos idénticos en el primer mensaje y el segundo mensaje, cuando la entidad de datos es una clave, tal como se explica en el contexto de la fig. 11. Como otra posibilidad, el procesador de entidades de datos 197 será un emparejador de datos general implementado específicamente como un descifrador, un lector de datos o, en el otro procesador de datos para comprobar si las porciones de datos concuerdan entre sí en el sentido de que las siguientes operaciones de procesamiento son simplemente la lectura, el descifrado, etc., y proporcionan una salida útil, tal como se explica anteriormente.

[0101] Dependiendo del resultado del procesador de entidades de datos, se inicia cualquier acción que se vaya a controlar. En concreto, la acción se inicia únicamente con un resultado útil/positivo de una operación de descifrado de un archivo, lectura de un archivo o emparejamiento de identidades de datos. No obstante, cuando estas operaciones no producen un resultado útil o positivo, es decir, cuando estas acciones producen un resultado inservible/negativo, no se inicia la acción concreta.

[0102] Además, la tercera entidad comprende un autorizador 191 para solicitar una identificación personal a la segunda entidad como respuesta a la recepción del segundo mensaje, para validar una información de personalización procedente de la segunda entidad y para controlar el ensamblador de datos 190 a través de la línea de control 198 como respuesta a una identificación personal validada de forma positiva, y no ensamblar los datos como respuesta a una identificación personal validada negativamente. El autorizador 191 puede estar configurado para usar, en el procedimiento de validación, otra información de teléfono móvil o un SMS procedente de la segunda entidad. Además, el autorizador puede transmitir a la segunda entidad un nombre de usuario de la segunda entidad registrada con respecto a la tercera entidad, de manera que la segunda entidad pueda verificar este nombre de usuario que preferentemente han acordado de antemano la tercera entidad y la segunda entidad.

[0103] La fig. 20 ilustra una segunda entidad para la comunicación con una primera entidad y una tercera entidad, en la que la segunda entidad comprende una interfaz de entrada para adquirir un mensaje de entrada generado por la primera entidad. La interfaz de entrada se indica en 200 y el mensaje de entrada es, en el contexto de la fig. 18 y la fig. 19, el segundo mensaje generado por la primera entidad.

[0104] La segunda entidad comprende además una interfaz de salida 202 para transmitir un mensaje de salida a la tercera entidad, y este mensaje de salida corresponde al segundo mensaje 166, por ejemplo, de la fig. 19.

[0105] Además, se proporciona un procesador 201 para generar el mensaje de salida basándose en el mensaje de entrada. La segunda entidad comprende además un autorizador 203 para recibir una petición de identificación personal procedente de una tercera entidad antes de la transmisión del mensaje de salida a la tercera entidad o como respuesta a dicha transmisión, y para enviar a la tercera entidad la información de identificación personal introducida por un usuario en la segunda entidad.

[0106] La segunda entidad es, preferentemente un teléfono móvil, el mensaje de entrada es un código QR generado por la primera entidad, y el procesador 201 está adaptado para descodificar el código QR y para introducir información extraída del código QR en el mensaje de salida.

[0107] Además, el autorizador 203 está configurado para presentar al usuario un nombre de usuario enviado por la tercera entidad, que se presenta junto con una solicitud para introducir el número de identificación personal.

[0108] En una forma de realización, el mensaje de entrada recibido por la interfaz de entrada 200 comprende una información de clave, y el mensaje de entrada comprende además una parte de entidad de datos cifrada o no

cifrada. Después se configura el procesador 201 para extraer la clave a partir del mensaje de entrada y para cifrar la porción de la entidad de datos con el fin de obtener el mensaje de salida.

[0109] Las formas de realización de la primera entidad descritas hasta el momento se refieren a un subdivisor de datos 180 (fig. 18) en la primera entidad. No obstante, en otras formas de realización, la subdivisión de datos se puede realizar de antemano y la primera entidad solo está en posesión de una porción de datos, y la segunda entidad está en posesión de la segunda porción de datos perteneciente a la primera porción de datos. Por tanto, la distribución de la segunda porción de datos a la segunda entidad no ha tenido lugar desde la primera entidad, sino que la segunda entidad ha recibido la segunda porción de datos a través de otro canal que no tiene su origen en la primera entidad. Este procedimiento se puede emplear para llevar a cabo un control a distancia de un dispositivo que tenga, por ejemplo, una dirección de tipo IPv4 o IPV6. El dispositivo del tipo, por ejemplo, de un interruptor de corriente o un frigorífico posee, como primera entidad, una parte de código QR cifrado como primera porción de datos. Para controlar a distancia la primera entidad, la segunda entidad lee el código. Además, la segunda entidad está en la posición de la segunda parte del código QR cifrado, o expresado de forma general, la segunda porción de datos. En este momento, la segunda entidad lee el código procedente de la primera entidad y añade su propia información, como un certificado o su propia parte del código QR cifrado, a los datos transmitidos al servidor y envía ambas partes al servidor.

[0110] El servidor comprueba ambas partes mediante cualquier tipo de emparejamiento de datos, como por ejemplo ensamblando las dos partes del código QR y comprobando posteriormente si los códigos QR ensamblados producen una salida que resulte útil. Si la salida obtenida por el emparejamiento del ensamblado de datos constituye un resultado positivo, el servidor permite a la segunda entidad controlar a distancia la primera entidad. Otra posibilidad consiste en que el servidor acceda directamente a la primera entidad.

[0111] Este modelo resulta particularmente útil para dispositivos alimentados que tengan una dirección IP. En particular, tales direcciones IP, como las IPv6, son bastante complicadas de manejar para los usuarios, ya que estas direcciones son bastante largas y, por tanto, no resultan cómodas de procesar para un usuario.

[0112] Otro ejemplo de control a distancia podría ser el encendido y apagado de un interruptor de corriente, para encender y apagar un radiador o para encender y apagar un aparato de aire acondicionado o cualquier otro dispositivo eléctrico en un entorno doméstico o de oficina. Esta forma de realización hace que el control a distancia resulte mucho más cómodo y añade más características de seguridad al control a distancia debido al emparejamiento de datos.

[0113] Aunque algunos aspectos se han descrito en el contexto de un aparato, es evidente que estos aspectos también representan una descripción del procedimiento correspondiente, en el que un bloque o dispositivo corresponde a una etapa de un procedimiento o una característica de una etapa de un procedimiento. De forma análoga, los aspectos descritos en el contexto de una etapa de un procedimiento también representan una descripción de un correspondiente bloque o elemento o característica de un correspondiente aparato.

[0114] Por lo tanto, la presente invención se refiere a un aparato, procedimiento y programa informático para operar una primera entidad, una segunda entidad o una tercera entidad y las correspondientes entidades que se describen anteriormente, y en los que una mayoría de los datos de un registro de datos se transmiten desde la primera entidad a la tercera entidad directamente, y una minoría de los datos del registro de datos son procesados por la primera entidad para que los reciba la segunda entidad, son recibidos por la segunda entidad y transmitidos desde la segunda entidad al servidor.

[0115] Preferentemente, el registro de datos es un registro de datos comprimido y/o cifrado.

[0116] Además, la invención se refiere a un sistema de comunicación que comprende al menos dos o tres entidades o más entidades, tal como se explica anteriormente.

[0117] Dependiendo de ciertos requisitos de implementación, se pueden implementar ejemplos de la invención tales como la primera entidad, la segunda entidad o la tercera entidad en forma de *hardware* o de *software*. La implementación se puede llevar a cabo a través de un medio de almacenamiento digital, por ejemplo un disco flexible, un DVD, un CD, una memoria ROM, PROM, EPROM, EEPROM o FLASH, que tenga almacenadas señales de control de lectura electrónica, que cooperen (o sean capaces de cooperar) con un sistema informático programable de manera que se lleve a cabo el respectivo procedimiento.

[0118] Algunos ejemplos de acuerdo con la invención comprenden un soporte de datos con señales de control de lectura electrónica, que son capaces de cooperar con un sistema informático programable, de manera que se lleve a cabo uno de los procedimientos descritos en la presente memoria.

[0119] Por lo general, se pueden implementar ejemplos de la presente invención en forma de producto de programa informático con un código de programa, en el que el código de programa se puede emplear para llevar a cabo uno de los procedimientos cuando el producto de programa informático se ejecuta en un ordenador. El código de programa puede, por ejemplo, estar almacenado en un soporte de lectura mecánica.

[0120] Otros ejemplos comprenden el programa informático para llevar a cabo uno de los procedimientos descritos en la presente memoria, almacenado en un soporte de lectura mecánica.

[0121] Dicho de otro modo, un ejemplo del procedimiento de la invención consiste, por tanto, en un programa informático con un código de programa para llevar a cabo uno de los procedimientos descritos en la presente memoria, cuando el programa informático se ejecuta en un ordenador.

[0122] Otro ejemplo del procedimiento de la invención consiste, por tanto, en un soporte de datos (o un medio de almacenamiento digital, o medio de lectura informática) que comprende, grabado en el mismo, el programa informático para llevar a cabo uno de los procedimientos descritos en la presente memoria.

[0123] Otro ejemplo del procedimiento de la invención consiste, por tanto, en un flujo de datos o una secuencia de señales que representan el programa informático para llevar a cabo uno de los procedimientos descritos en la presente memoria. El flujo de datos o secuencia de señales puede estar configurado, por ejemplo, para transferirlo a través de una conexión de comunicación de datos, por ejemplo a través de Internet.

[0124] Otro ejemplo comprende unos medios de procesamiento, por ejemplo un ordenador, o un dispositivo lógico programable, configurados o adaptados para llevar a cabo uno de los procedimientos descritos en la presente memoria.

[0125] Otro ejemplo comprende un ordenador que tiene instalado el programa informático para llevar a cabo uno de los procedimientos descritos en la presente memoria.

[0126] En algunos ejemplos, se puede usar un dispositivo lógico programable (por ejemplo una matriz de puertas programables en campo o FPGA, por sus siglas en inglés) para llevar a cabo algunas de las funcionalidades, o todas, de los procedimientos descritos en la presente memoria. En algunos ejemplos, una FPGA puede cooperar con un microprocesador para llevar a cabo uno de los procedimientos descritos en la presente memoria. Por lo general, los procedimientos se llevan a cabo preferentemente mediante cualquier aparato de *hardware*.

[0127] Los ejemplos descritos más arriba tienen un carácter meramente ilustrativo de los principios de la presente invención. Se entiende que las modificaciones y variaciones de las disposiciones y los detalles descritos en la presente memoria resultarán evidentes para otros expertos en la materia. Por lo tanto, las limitaciones vendrán impuestas únicamente por el alcance de las siguientes reivindicaciones de patente y no por los detalles concretos presentados a modo de descripción y explicación de los ejemplos incluidos en la presente memoria.

REIVINDICACIONES

1. Primera entidad (11) para la comunicación con una segunda entidad (12) y una tercera entidad (13), que comprende:

un subdivisor (180) para subdividir una entidad de datos en al menos una primera porción de datos y una segunda porción de datos (162, 163);

una interfaz de salida (181) para transmitir un primer mensaje (165) a la tercera entidad, teniendo que el primer mensaje comprende la primera porción de datos (162) y no comprende la segunda porción de datos (163), y para emitir un segundo mensaje (166) para ser recibido por la segunda entidad (12), teniendo que el segundo mensaje comprende la segunda porción de datos (163) y no comprende la primera porción de datos (162), en la que la interfaz de salida (181) está configurada para transmitir el primer mensaje (165) a través de un primer canal de transmisión, para transmitir el segundo mensaje (166) a través de un segundo canal de transmisión, en la que la capacidad de transmisión del segundo canal es menor que la capacidad de transmisión del primer canal de transmisión,

en la que el subdivisor de datos (180) está configurado para subdividir la entidad de datos de manera que una cantidad de datos en la primera porción de datos sea mayor que una cantidad de datos en la segunda porción de datos, y en la que el subdivisor de datos (180) está configurado para subdividir la entidad de datos de una manera conocida por la tercera entidad, o en la que el subdivisor de datos (180) está configurado para generar información de la subdivisión (184) que indica la manera de subdividir la entidad de datos y el primer mensaje (165) o el segundo mensaje (166) comprende la información de subdivisión, o en la que la interfaz de salida (181) está configurada para transmitir a la tercera entidad (13) otro mensaje que comprende la información de subdivisión.

2. Primera entidad de acuerdo con la reivindicación 1, en la que la entidad de datos es un archivo de datos o una clave.

3. Primera entidad de acuerdo con una cualquiera de las reivindicaciones 1 a 2, en la que la interfaz de salida (181) está configurada para presentar el segundo mensaje como un código óptico bidimensional en una pantalla.

4. Primera entidad de acuerdo con una de las reivindicaciones precedentes, en la que la entidad de datos es una clave,

en la que la primera entidad comprende un cifrador para cifrar (160) un mensaje de datos usando la clave para obtener un mensaje cifrado, y

en la que la interfaz de salida (181) está configurada para generar el primer mensaje usando el mensaje cifrado y solo una porción de la clave como primera porción de datos o para generar el segundo mensaje usando el mensaje cifrado y solo una segunda porción de la clave como segunda porción de datos, y en la que la segunda porción de la clave es diferente a la primera porción de la clave.

5. Primera entidad de acuerdo con la reivindicación 1, en la que la entidad de datos es una clave, en la que la primera entidad comprende además un cifrador (160), y en la que el cifrador está configurado para cifrar una porción de la clave usando la otra porción de la clave.

6. Primera entidad de acuerdo con una de las reivindicaciones precedentes, en la que el subdivisor de datos (180) está configurado para subdividir la entidad de datos de manera que la primera porción de datos contenga diez veces, o más, cantidad de datos que la segunda porción de datos.

7. Primera entidad de acuerdo con la reivindicación 1 o 2, que además comprende un cifrador (160) para cifrar un archivo de datos usando una información de cifrado que permite un descifrado en la tercera entidad y no permite un descifrado en la segunda entidad para obtener un archivo de datos cifrado, en la que el archivo de datos cifrado es la entidad de datos.

8. Primera entidad de acuerdo con una de las reivindicaciones precedentes, en la que el subdivisor de datos (180) está configurado para aleatorizar o cifrar bytes de la entidad de datos seleccionados para la segunda porción de datos usando información de aleatorización o cifrado que permite una desaleatorización o descifrado en

la tercera entidad y no permite una desaleatorización o descifrado en la segunda entidad.

9. Primera entidad de acuerdo con una de las reivindicaciones precedentes, que además comprende un generador de claves (167) para generar localmente una clave como entidad de datos.

10. Primera entidad de acuerdo con una de las reivindicaciones precedentes, en la que la entidad de datos comprende un archivo de datos cifrado o no cifrado, en la que el subdivisor de datos (180) está configurado para subdividir la entidad de datos en al menos tres porciones de datos, en la que la interfaz de salida está configurada para transmitir a la tercera entidad el primer mensaje que comprende la primera porción, para emitir el segundo mensaje que comprende la segunda porción con destino a la segunda entidad, y para emitir un tercer mensaje que comprende la tercera porción de datos y no comprende la segunda porción y la primera porción, dirigido a una cuarta entidad.

11. Procedimiento de comunicación con una segunda entidad (12) y una tercera entidad (13) por parte de una primera entidad (11), que comprende:

la subdivisión (180) de una entidad de datos en al menos una primera porción de datos y una segunda porción de datos (162, 163);

la transmisión (181) de un primer mensaje (165) a la tercera entidad, en la que el primer mensaje comprende la primera porción de datos (162) y no comprende la segunda porción de datos (163), y la emisión de un segundo mensaje para ser recibido por la segunda entidad (12), en la que el segundo mensaje no comprende la primera porción de datos (162),

en el que el primer mensaje (165) se transmite a través de un primer canal de transmisión, en el que el segundo mensaje (166) se transmite a través de un segundo canal de transmisión, en el que la capacidad de transmisión del segundo canal de transmisión es menor que la capacidad de transmisión del primer canal de transmisión,

en el que la subdivisión (180) se lleva a cabo de manera que una cantidad de datos en la primera porción de datos sea mayor que una cantidad de datos en la segunda porción de datos, y

en el que la subdivisión de la entidad de datos se lleva cabo de una manera conocida por la tercera entidad, o en el que se genera información de la subdivisión (184) que indica la manera de subdividir la entidad de datos, y se proporciona al primer mensaje (165) o al segundo mensaje (166) la información de subdivisión o en el que se transmite otro mensaje que comprende la información de subdivisión.

12. Programa informático con un código de programa para llevar a cabo, cuando se ejecuta en un ordenador, un procedimiento de acuerdo con la reivindicación 11.

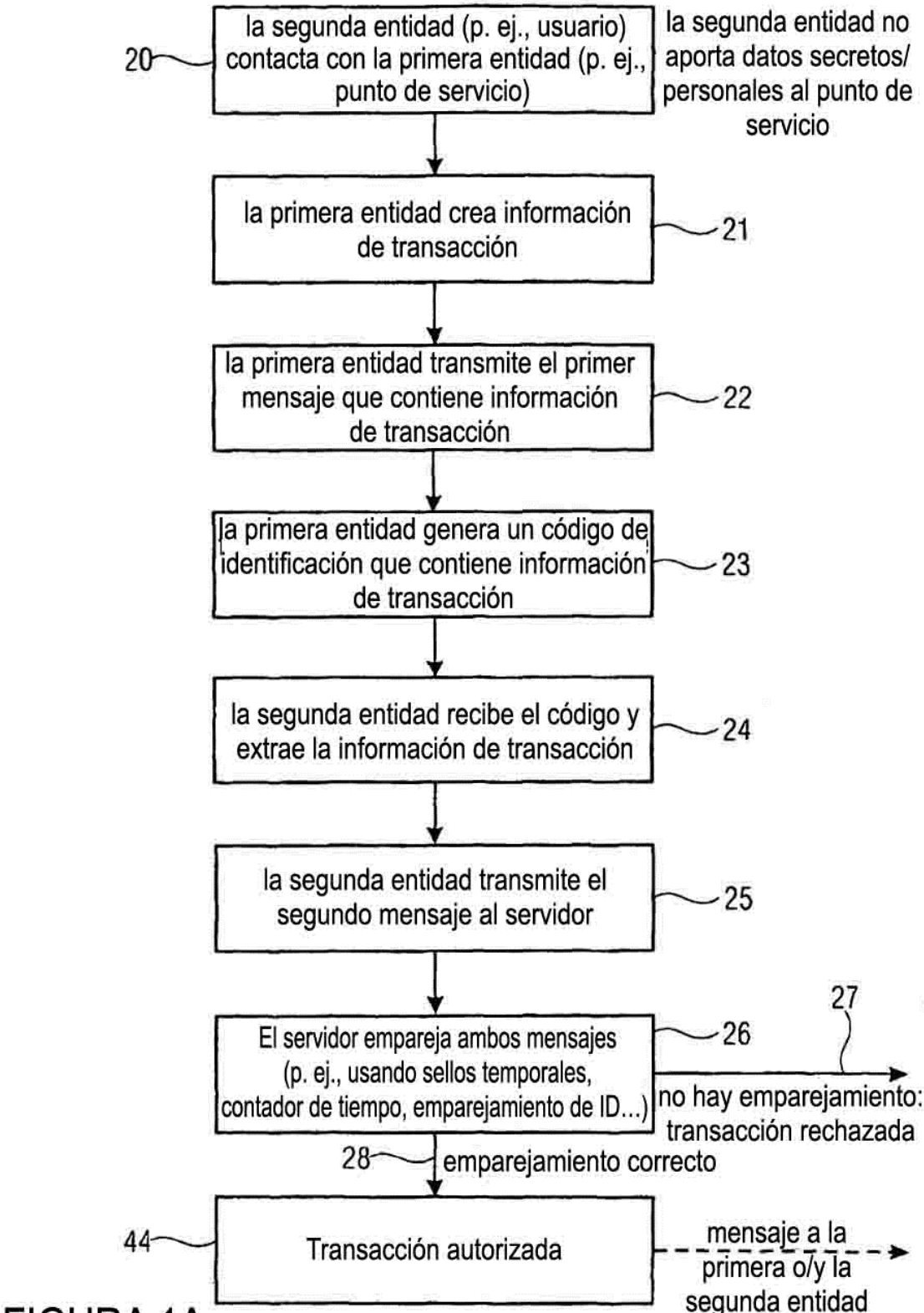
20
la segunda entidad (p. ej., usuario) contacta con la primera entidad (p. ej., punto de servicio)
la segunda entidad no aporta datos secretos/ personales al punto de servicio
la primera entidad crea información de transacción
21
la primera entidad transmite el primer mensaje que contiene información de transacción
22
la primera entidad genera un código de identificación que contiene información de transacción
23
la segunda entidad recibe el código y extrae la información de transacción
24
la segunda entidad transmite el segundo mensaje al servidor
25
27
El servidor empareja ambos mensajes (p. ej., usando sellos temporales, contador de tiempo, emparejamiento de ID...)
26
no hay emparejamiento: transacción rechazada
28
emparejamiento correcto
44
Transacción autorizada
mensaje a la primera o/y la segunda entidad

FIGURA 1A

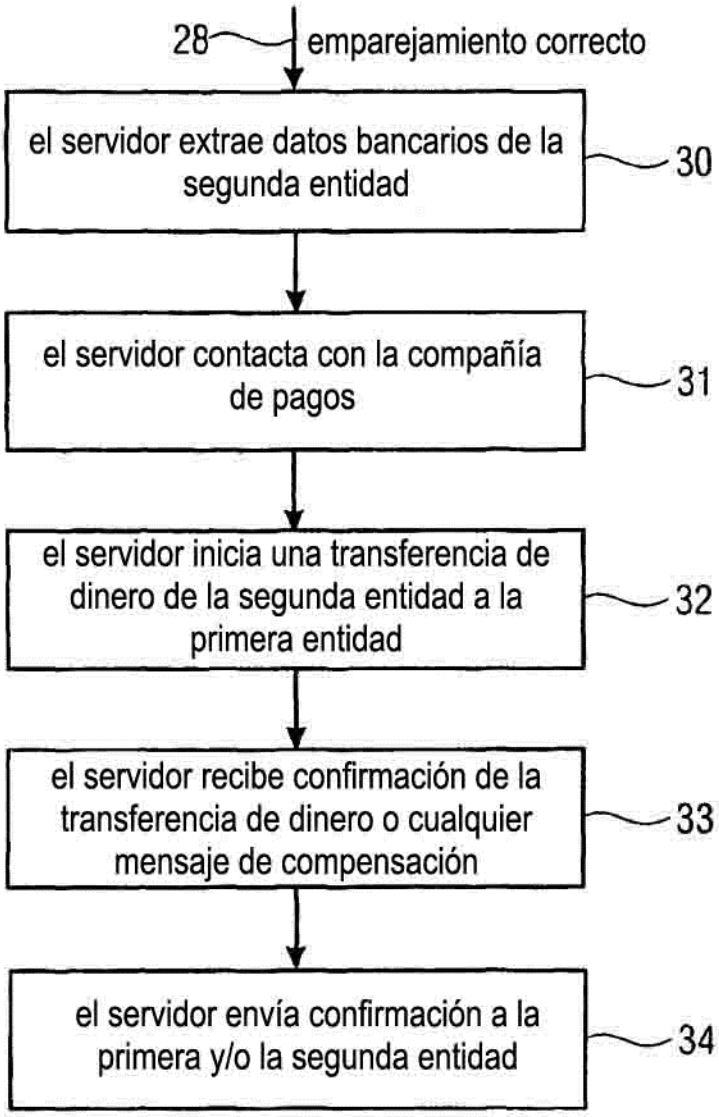
28
emparejamiento correcto
el servidor extrae datos bancarios de la segunda entidad
30
el servidor contacta con la compañía de pagos
31
el servidor inicia una transferencia de dinero de la segunda entidad a la primera entidad
32
el servidor recibe confirmación de la transferencia de dinero o cualquier mensaje de compensación
33
el servidor envía confirmación a la primera y/o la segunda entidad
34

FIGURA 1B

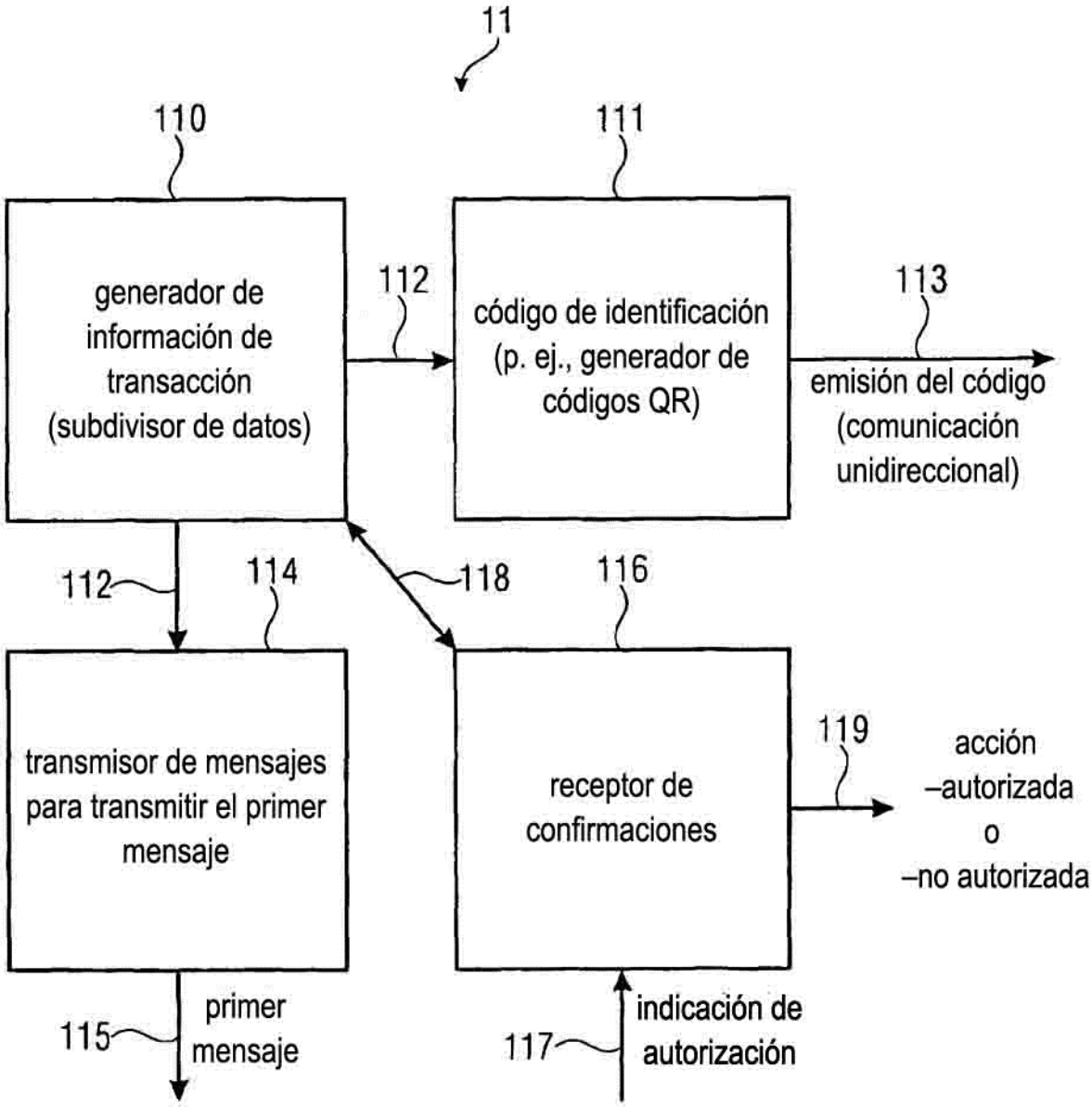

FIGURA 2

PRIMERA ENTIDAD (P. EJ., PUNTO DE SERVICIO)

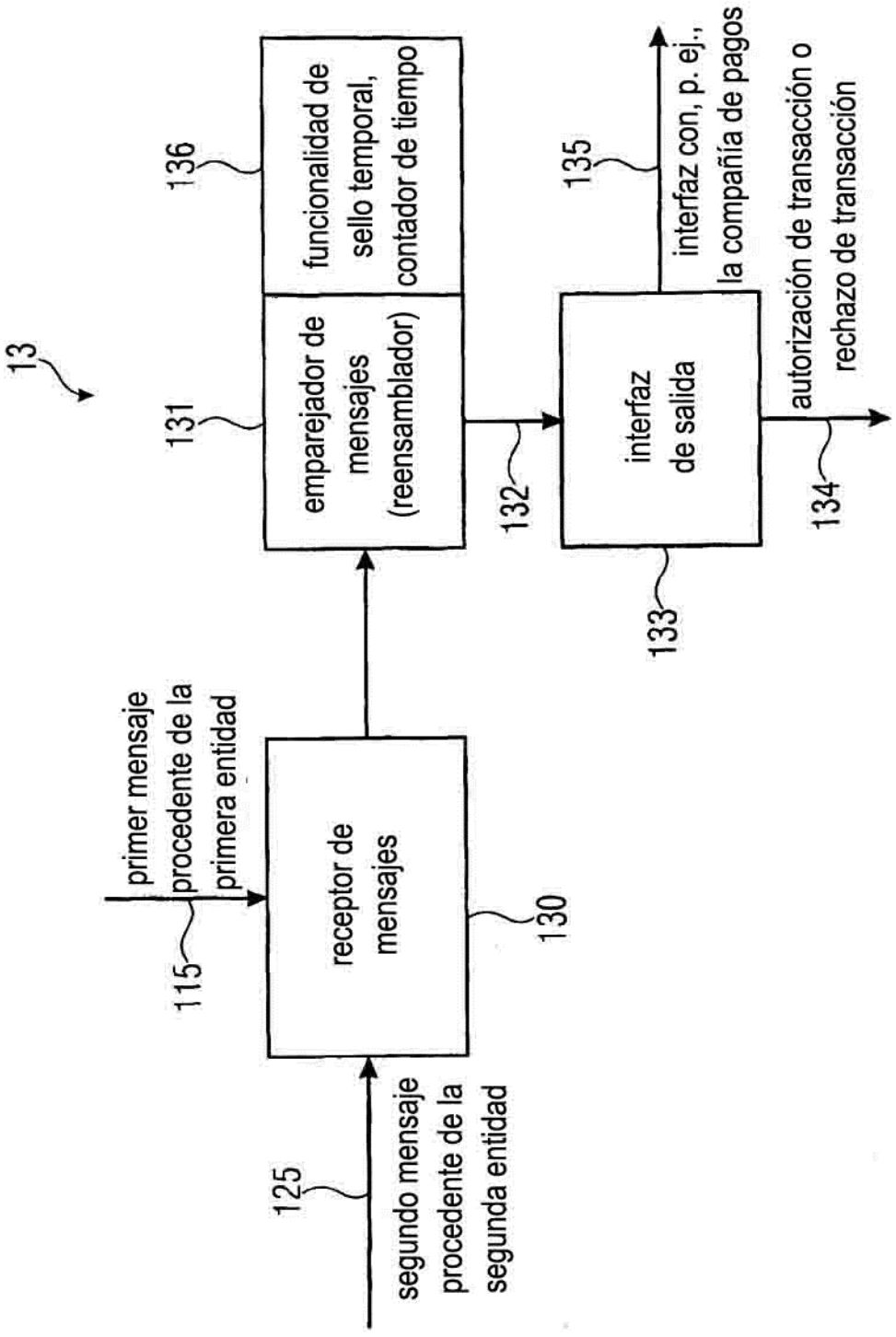

FIGURA 3A
SERVIDOR

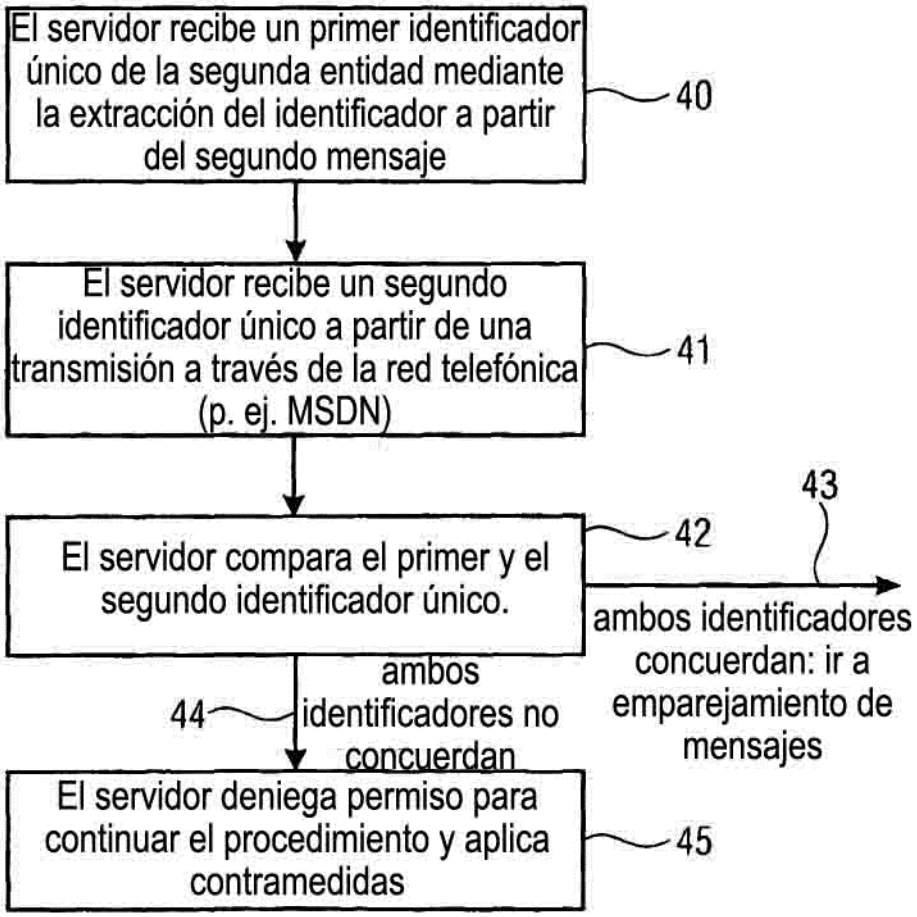
El servidor recibe un primer identificador único de la segunda entidad mediante la extracción del identificador a partir del segundo mensaje
40
El servidor recibe un segundo identificador único a partir de una transmisión a través de la red telefónica (p. ej. MSDN)
41
El servidor compara el primer y el segundo identificador único.
42
43
ambos identificadores concuerdan: ir a emparejamiento de mensajes
44
ambos identificadores no concuerdan
El servidor deniega permiso para continuar el procedimiento y aplica contramedidas
45

FIGURA 3B

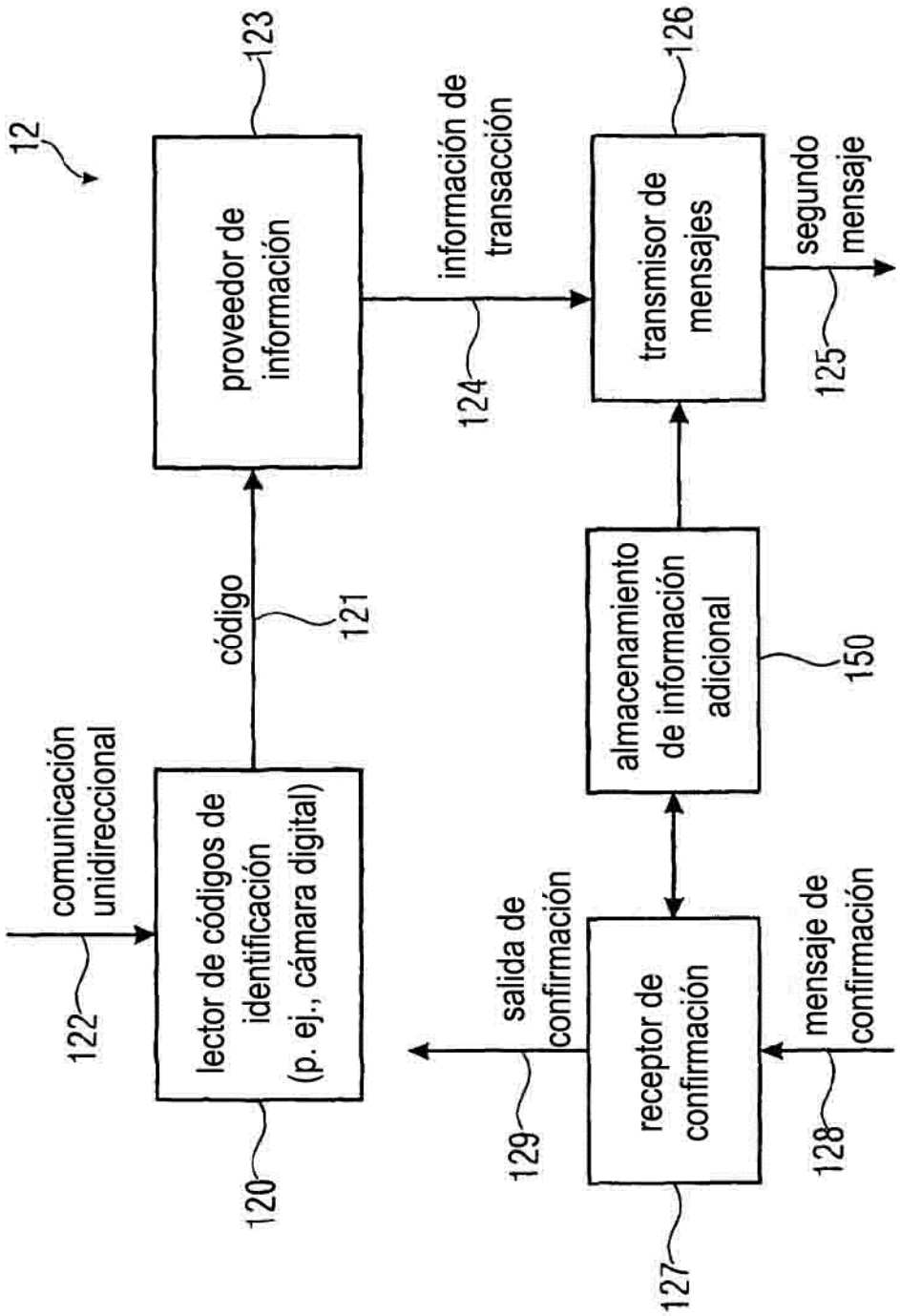

FIGURA 4A
SEGUNDA ENTIDAD
(P. EJ., TELÉFONO MÓVIL CON CÁMARA DIGITAL)

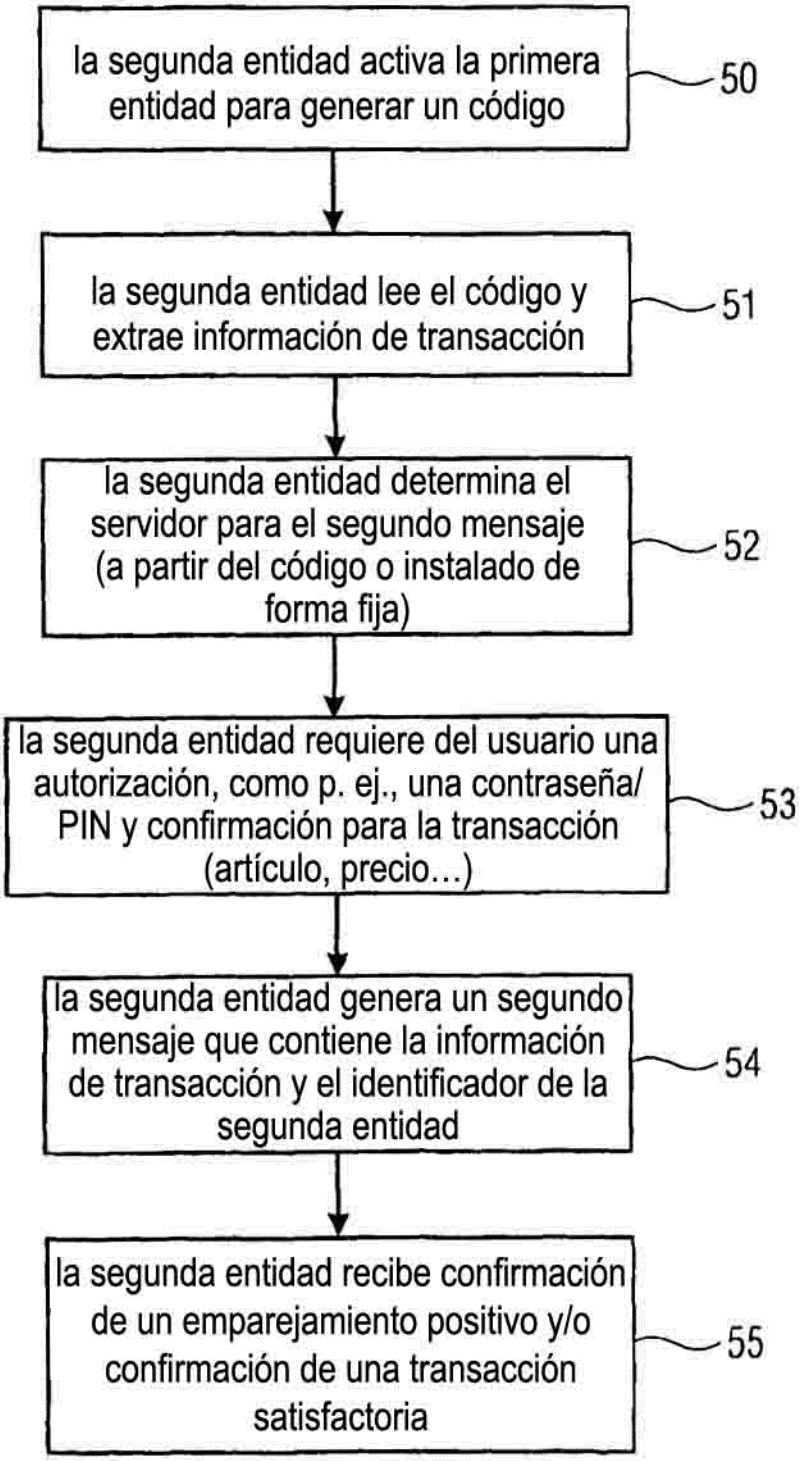
la segunda entidad activa la primera entidad para generar un código
50
la segunda entidad lee el código y extrae información de transacción
51
la segunda entidad determina el servidor para el segundo mensaje (a partir del código o instalado de forma fija)
52
la segunda entidad requiere del usuario una autorización, como p. ej., una contraseña/ PIN y confirmación para la transacción (artículo, precio...)
53
la segunda entidad genera un segundo mensaje que contiene la información de transacción y el identificador de la segunda entidad
54
la segunda entidad recibe confirmación de un emparejamiento positivo y/o confirmación de una transacción satisfactoria
55

FIGURA 4B

tipo de aplicación	transacción	información de transacción
1. Pago en línea	procedimiento de pago para transferir/garantizar el pago a la primera entidad	ID de transacción, ID de punto de servicio, artículo, precio
2. Retirada de efectivo	cargar a la cuenta la cantidad retirada y/o entregar dinero	ID de transacción, ID de terminal de cajero, cantidad requerida
3. Pago del recibo	procedimiento de pago para transferir/garantizar el pago a la primera entidad	ID de transacción, ID de punto de servicio, cantidad
4. Aplicaciones sin presencia de tarjeta (CND)	procedimiento de pago para transferir/garantizar el pago a la primera entidad	ID de transacción, ID de parte vendedora, artículo, precio
5. Pago de móvil a móvil	procedimiento de pago para transferir/garantizar el pago a la primera entidad	ID de transacción, ID de entidad compradora/ receptora precio/cantidad
6. Autorización	la segunda entidad puede acceder a un servicio proporcionado por una primera entidad (un portal de Internet)	ID de transacción, ID de primera entidad

FIGURA 5

- la primera entidad (p. ej., TIENDA) y la tercera entidad (servidor) comparten un secreto (K1) o han obtenido una autenticación segura para el cifrado asimétrico; K1 es desconocido para la segunda entidad (teléfono móvil).

- la segunda entidad (teléfono móvil) y la tercera entidad (servidor) comparten un secreto (K2) o han obtenido una autenticación segura para el cifrado asimétrico; K2 es desconocido para la primera entidad (tienda).

- Diferentes canales de comunicación (con respecto al medio, protocolo, tipo…)
  de la primera entidad a la tercera entidad, p. ej., INTERNET (no orientada a la conexión)
  de la segunda entidad a la tercera entidad, p. ej., conexión telefónica (orientada a la conexión)

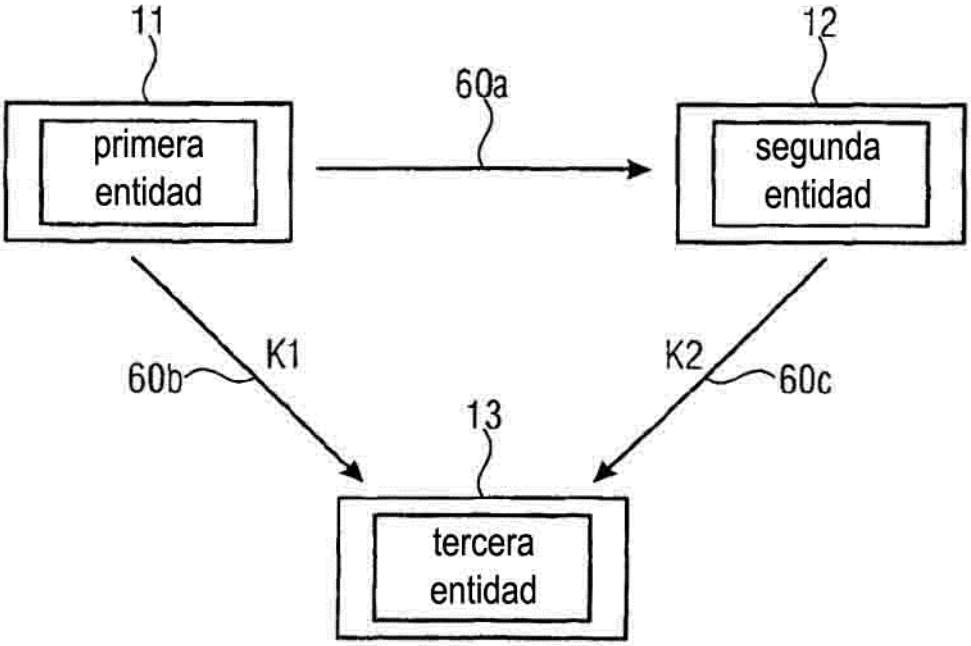

FIGURA 6

- la primera entidad crea, p. ej., una clave dinámica — 70
- la primera entidad presenta en pantalla un código 2D que contiene la clave y otros datos opcionales; — 71

- la primera entidad envía la clave y los otros datos a la tercera entidad; — 72
- la segunda entidad lee el código 2D mediante una cámara y la aplicación del *software* correspondiente y descodifica el código para extraer la clave; — 73
- la segunda entidad cifra los otros datos extraídos del código 2D usando la clave; — 74

- la segunda entidad envía los otros datos cifrados a la tercera entidad; — 75
- la tercera entidad descifra el mensaje procedente de la segunda entidad usando la clave enviada por la primera entidad; — 76

- emparejamiento de datos en la tercera entidad; — 77

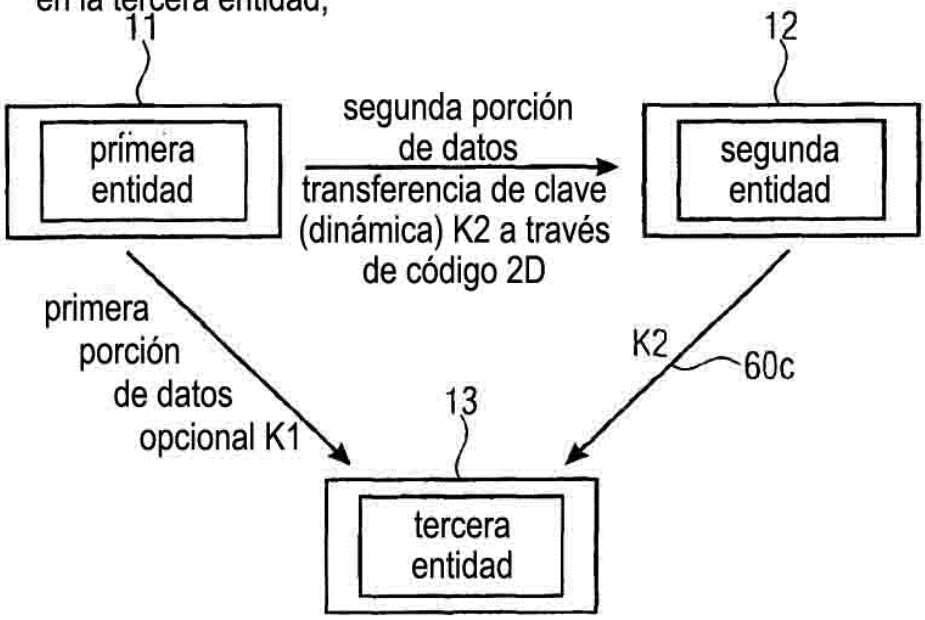

FIGURA 7

- la primera entidad crea una clave de cifrado K2; 70
- la primera entidad cifra un archivo de datos usando K2 y vuelve a cifrar el resultado del cifrado con K2 usando la clave K1 (conocida por la tercera entidad y la primera entidad); 80

- la primera entidad envía estos datos (doblemente) cifrados al servidor (tercera entidad); 81

- la primera entidad cifra la clave K2 usando la clave K1 y presenta un código 2D que contiene el resultado del cifrado (opcionalmente los datos del archivo de datos se cifran con K1 y/o K2 y también se incluyen en el código 2D); 82
- la segunda entidad lee el código 2D mediante una cámara y un *software* extrae el resultado del cifrado; 83

- la segunda entidad envía el resultado del cifrado a la tercera entidad; 84
- la tercera entidad descifra el resultado del cifrado procedente de la segunda entidad usando K1 para obtener K2 y, opcionalmente, los datos; 85
- el servidor usa K2 para descifrar el archivo de datos recibido, procedente de la primera entidad, y descifra el resultado con K1 para leer datos procedentes de la primera entidad; 86
- el servidor (tercera entidad) empareja datos de la primera entidad y datos de la segunda entidad; 87

FIGURA 8

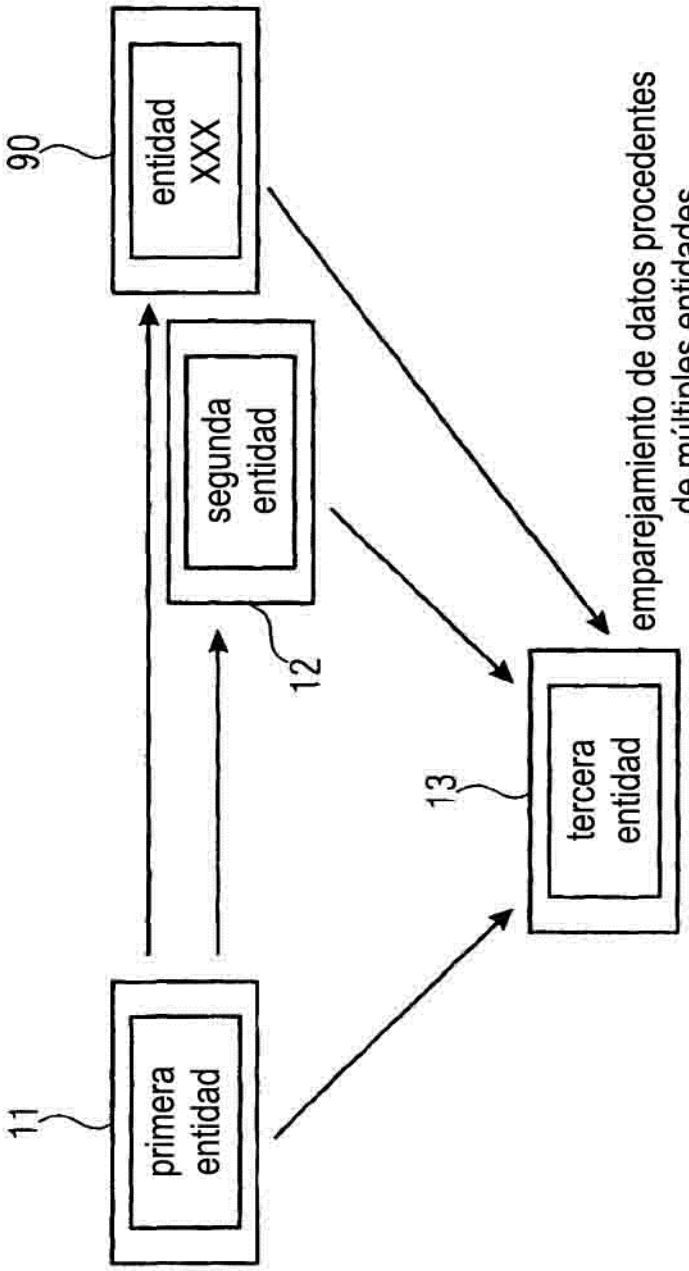
90
entidad XXX
segunda entidad
12
13
tercera entidad
11
primera entidad
emparejamiento de datos procedentes de múltiples entidades

FIGURA 9

- la primera entidad crea un archivo de datos y una clave K1 (conocida por la primera entidad y la tercera entidad, y desconocida para la segunda entidad) y cifra el archivo de datos usando K1;

- la primera entidad divide el archivo de datos (cifrado) en dos o más archivos y transmite una primera parte a la tercera entidad y una segunda parte a la segunda entidad, p. ej., a través de un código 2D;

- la segunda entidad lee el código 2D, p. ej., mediante una cámara y una aplicación de software y extrae la segunda parte a partir del código;

- la segunda entidad envía la segunda parte al servidor (tercera entidad);

- la tercera entidad reensambla y descifra ambas partes usando K1 y continúa con una operación predeterminada, si los datos descifrados tienen sentido/cumplen una condición predeterminada.

FIGURA 10

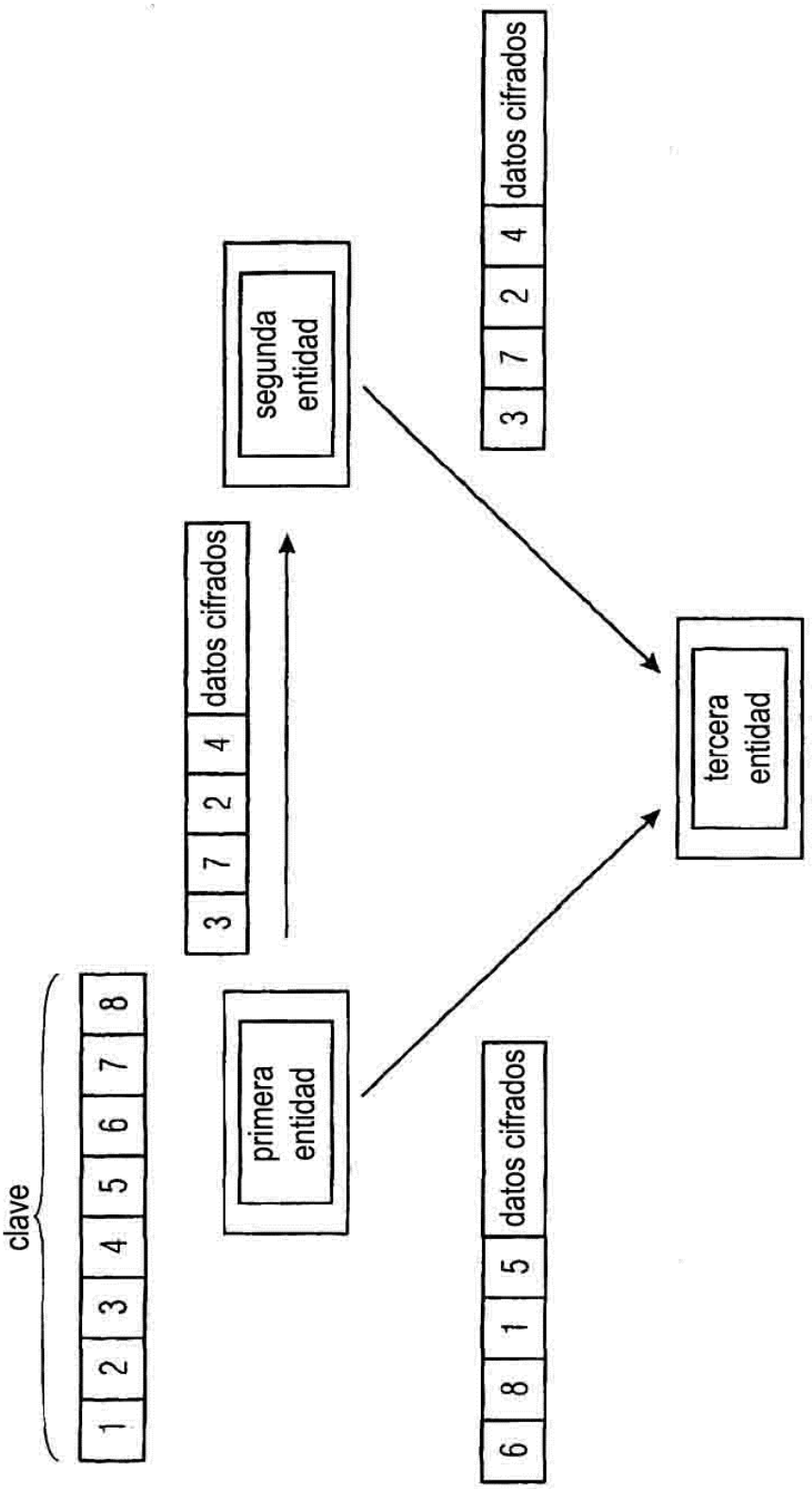
clave
1
2
3
4
5
6
7
8
primera entidad
segunda entidad
tercera entidad
3
7
2
4
datos cifrados
6
8
1
5
datos cifrados
3
7
2
4
datos cifrados

FIGURA 11

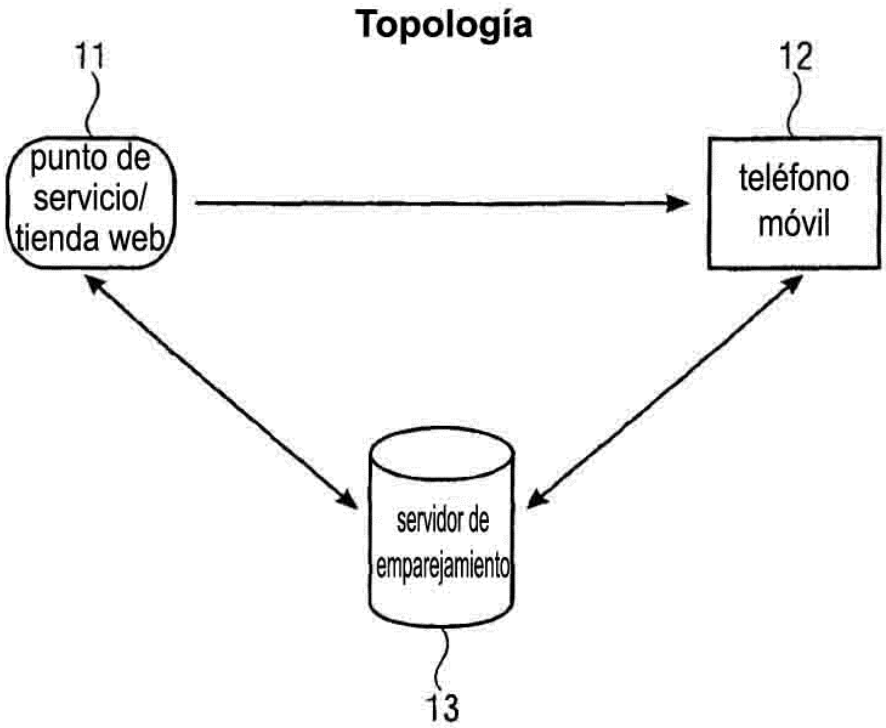

FIGURA 12

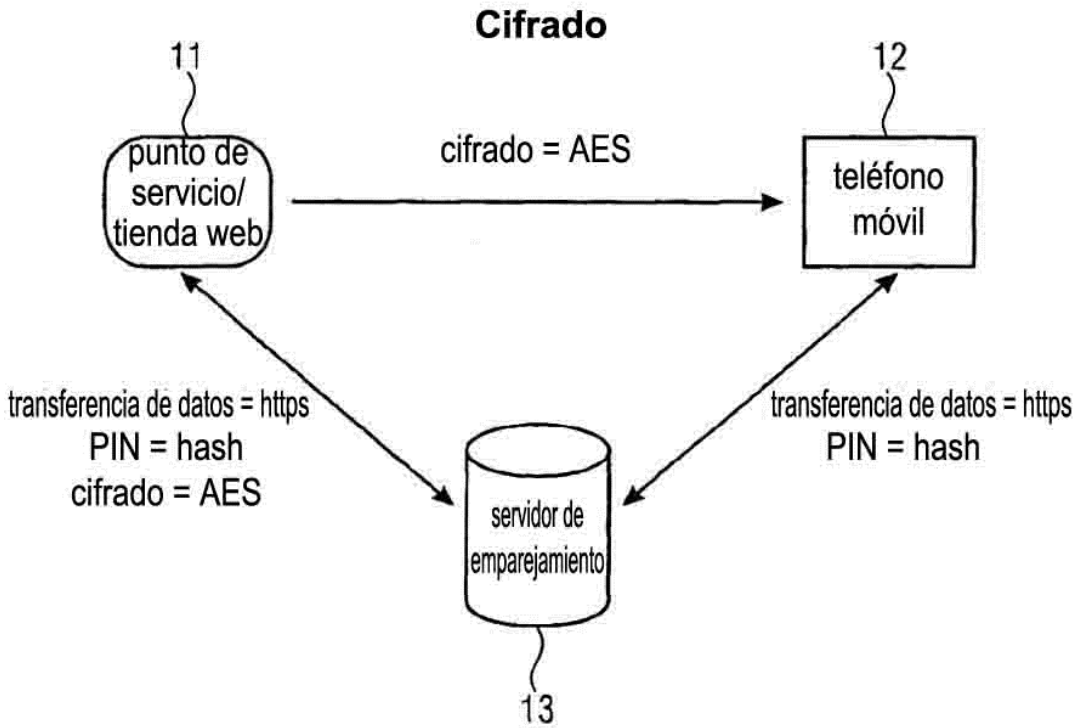

FIGURA 13

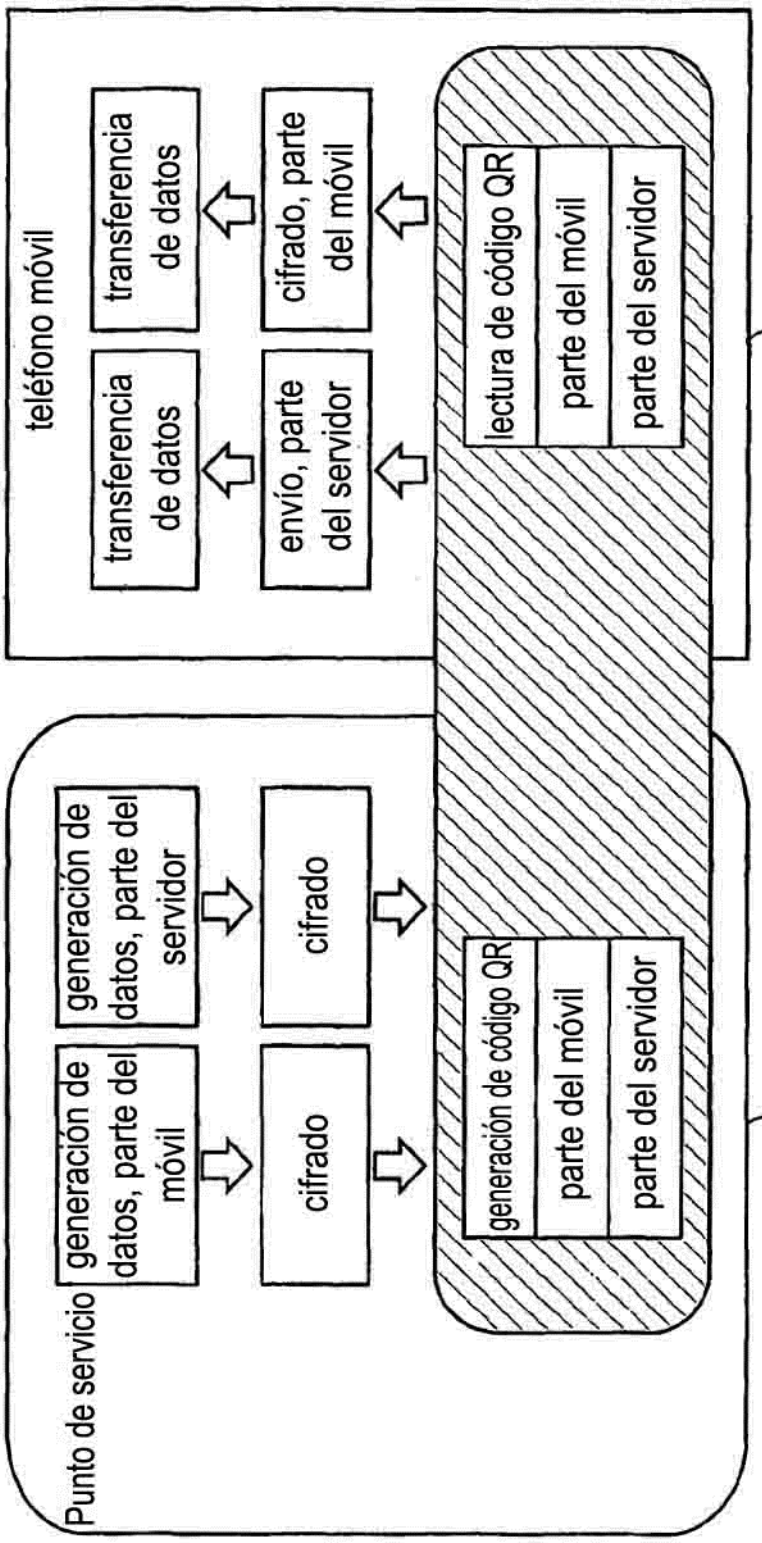

FIGURA 14

Es necesario un separador entre la parte del móvil y la del servidor, el generador de códigos QR solo obtiene un archivo

- No es necesario ningún cifrado porque los datos ya está cifrados
- El código solo será legible con un cierto lector
- El código tiene dos tipos de contenidos
  1. parte del teléfono móvil, que será descifrada por el teléfono móvil
  2. parte del servidor, que será enviada por el teléfono móvil al servidor
- Longitud de código para secuencia piloto
  - Parte del teléfono móvil: 4 bytes
  - Parte del servidor: hasta 94 bytes
- El buen rendimiento en la lectura es la clave del éxito

FIGURA 15

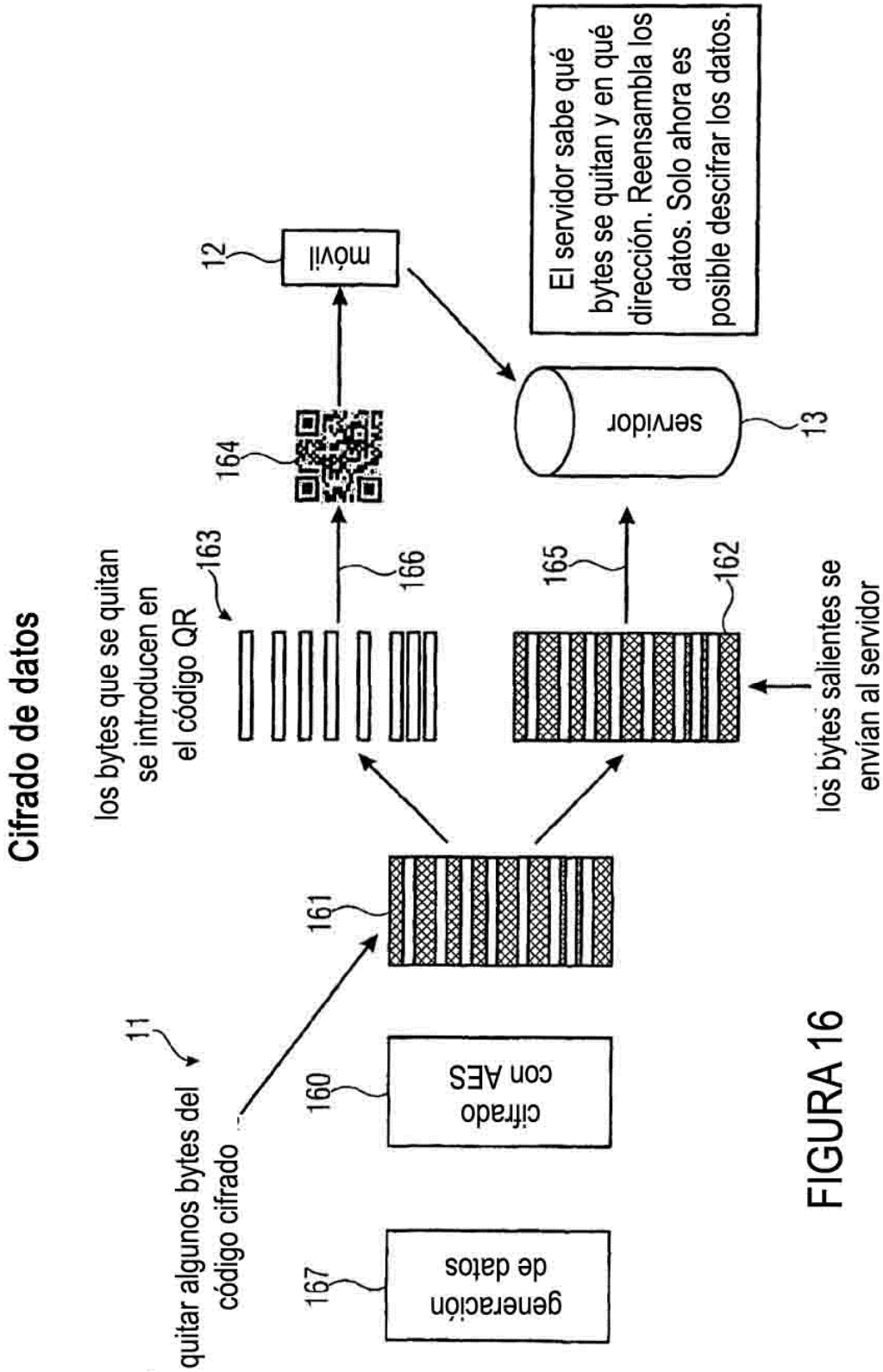
Cifrado de datos
quitar algunos bytes del código cifrado
11
generación de datos
167
cifrado con AES
160
161
los bytes que se quitan se introducen en el código QR
163
166
164
165
162
los bytes salientes se envían al servidor
12
móvil
servidor
13
El servidor sabe qué bytes se quitan y en qué dirección. Reensambla los datos. Solo ahora es posible descifrar los datos.

FIGURA 16

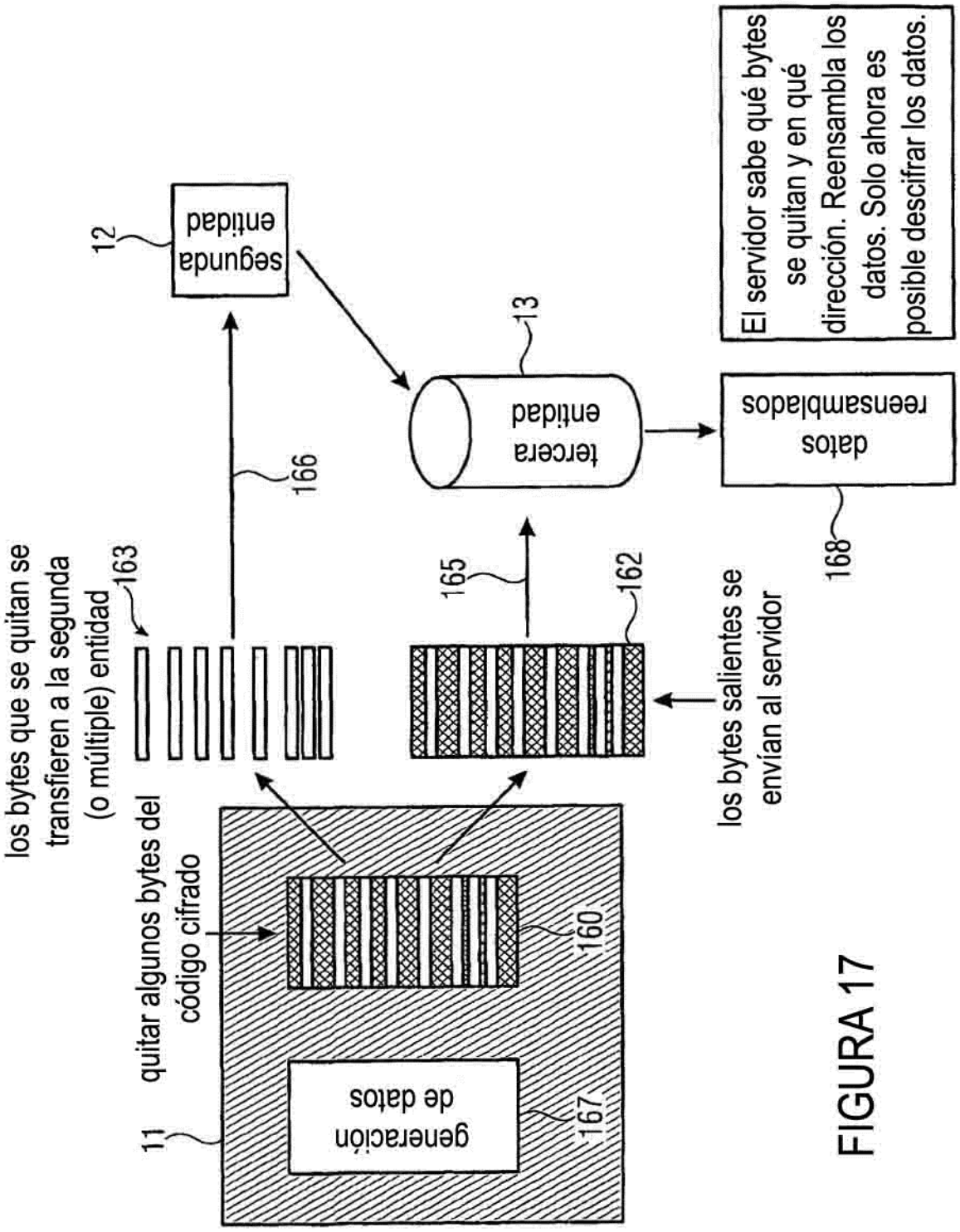
El servidor sabe qué bytes se quitan y en qué dirección. Reensambla los datos. Solo ahora es posible descifrar los datos.
12
segunda entidad
13
tercera entidad
datos reensamblados
168
166
165
162
los bytes salientes se envían al servidor
los bytes que se quitan se transfieren a la segunda (o múltiple) entidad
163
quitar algunos bytes del código cifrado
11
generación de datos
160
167

FIGURA 17

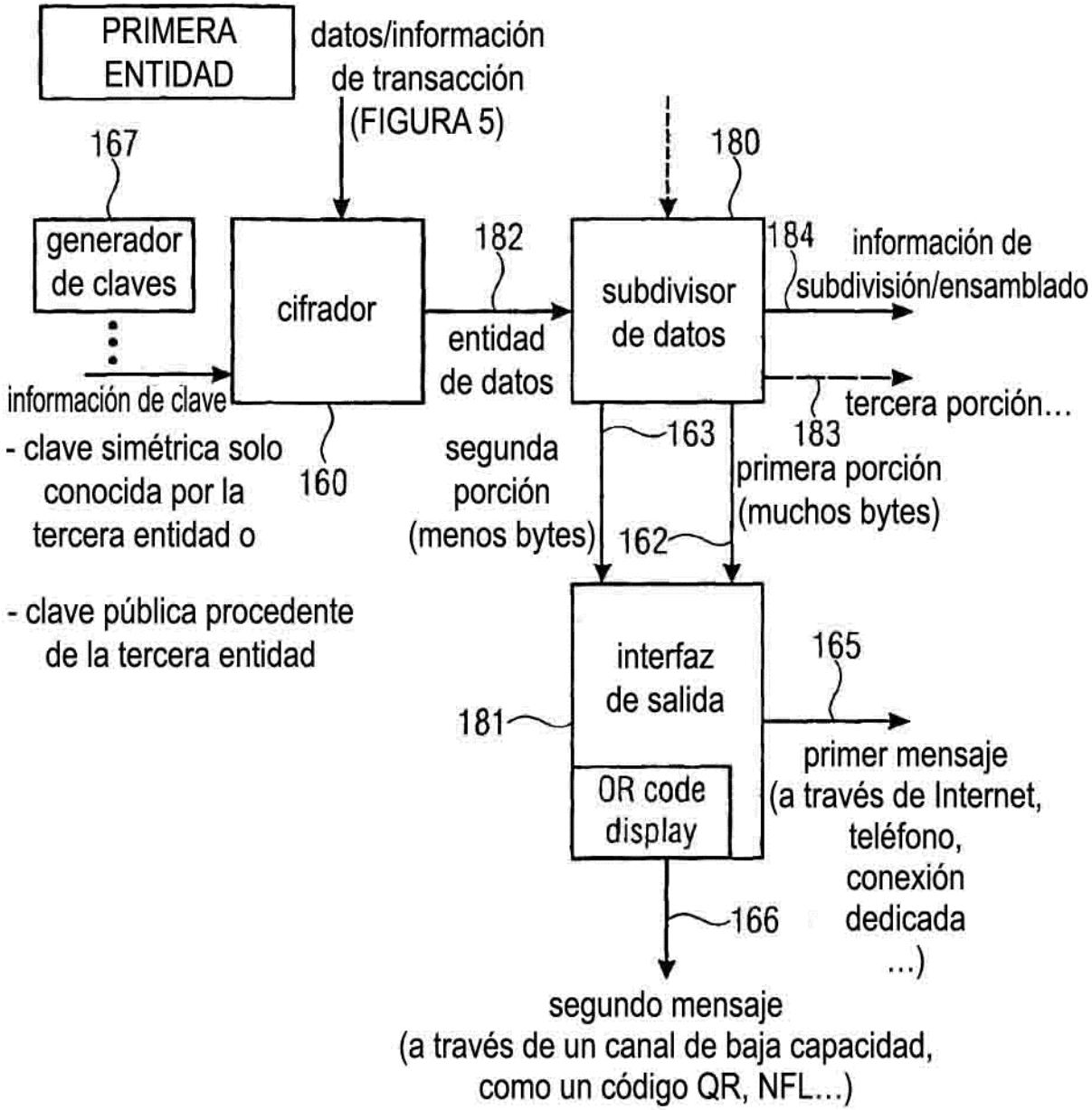
PRIMERA ENTIDAD
datos/información de transacción (FIGURA 5)
167
180
generador de claves
cifrador
182
subdivisor de datos
184
información de subdivisión/ensamblado
información de clave
- clave simétrica solo conocida por la tercera entidad o
- clave pública procedente de la tercera entidad
160
entidad de datos
segunda porción (menos bytes)
163
183
tercera porción...
primera porción (muchos bytes)
162
interfaz de salida
165
181
OR code display
primer mensaje (a través de Internet, teléfono, conexión dedicada ...)
166
segundo mensaje (a través de un canal de baja capacidad, como un código QR, NFL...)

FIGURA 18

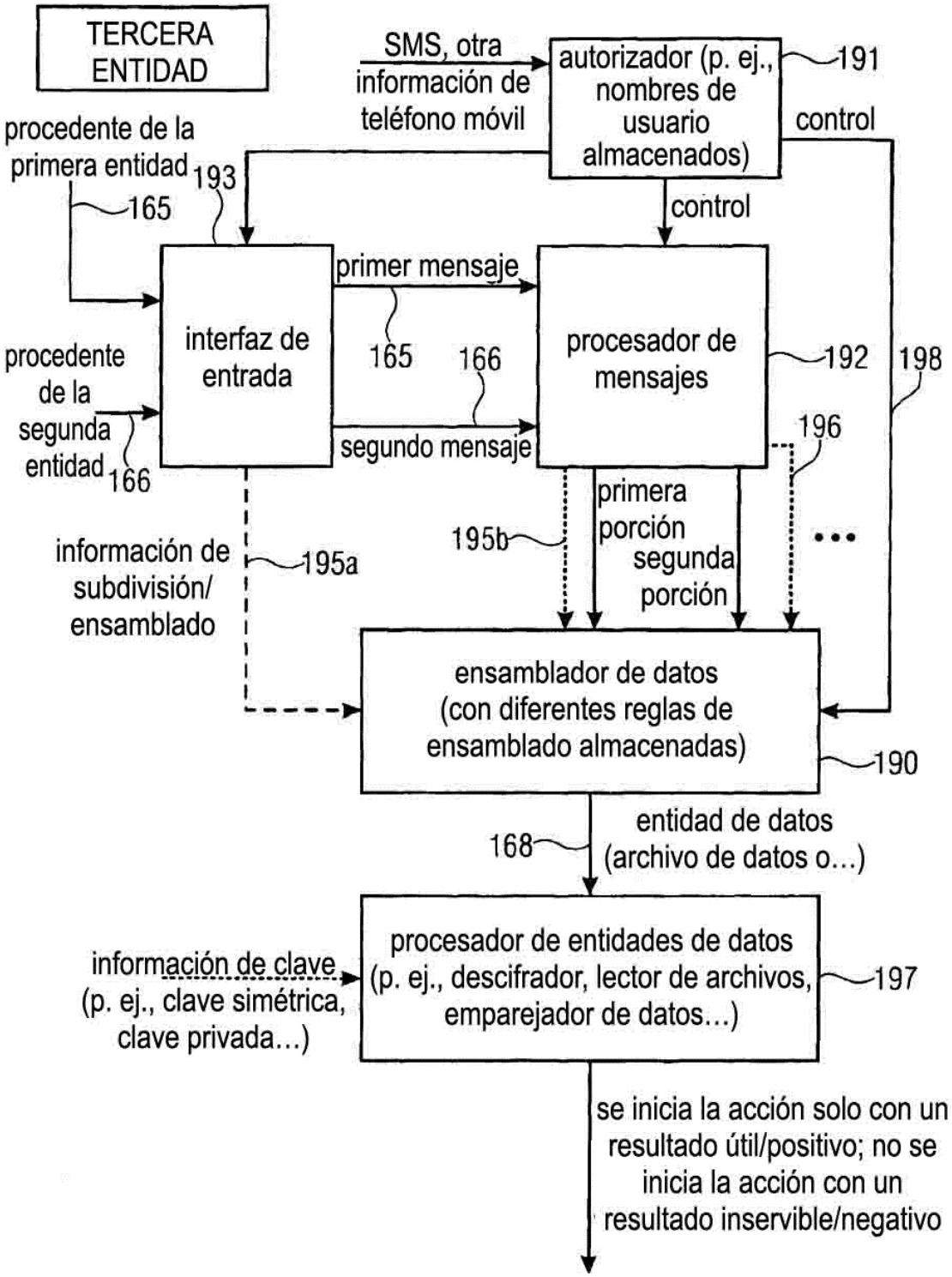
TERCERA ENTIDAD
SMS, otra información de teléfono móvil
autorizador (p. ej., nombres de usuario almacenados)
191
control
procedente de la primera entidad
193
165
control
primer mensaje
interfaz de entrada
165
166
procesador de mensajes
192
198
procedente de la segunda entidad
166
segundo mensaje
196
primera porción
segunda porción
información de subdivisión/ ensamblado
195a
195b
ensamblador de datos (con diferentes reglas de ensamblado almacenadas)
190
168
entidad de datos (archivo de datos o...)
información de clave (p. ej., clave simétrica, clave privada...)
procesador de entidades de datos (p. ej., descifrador, lector de archivos, emparejador de datos...)
197
se inicia la acción solo con un resultado útil/positivo; no se inicia la acción con un resultado inservible/negativo

FIGURA 19

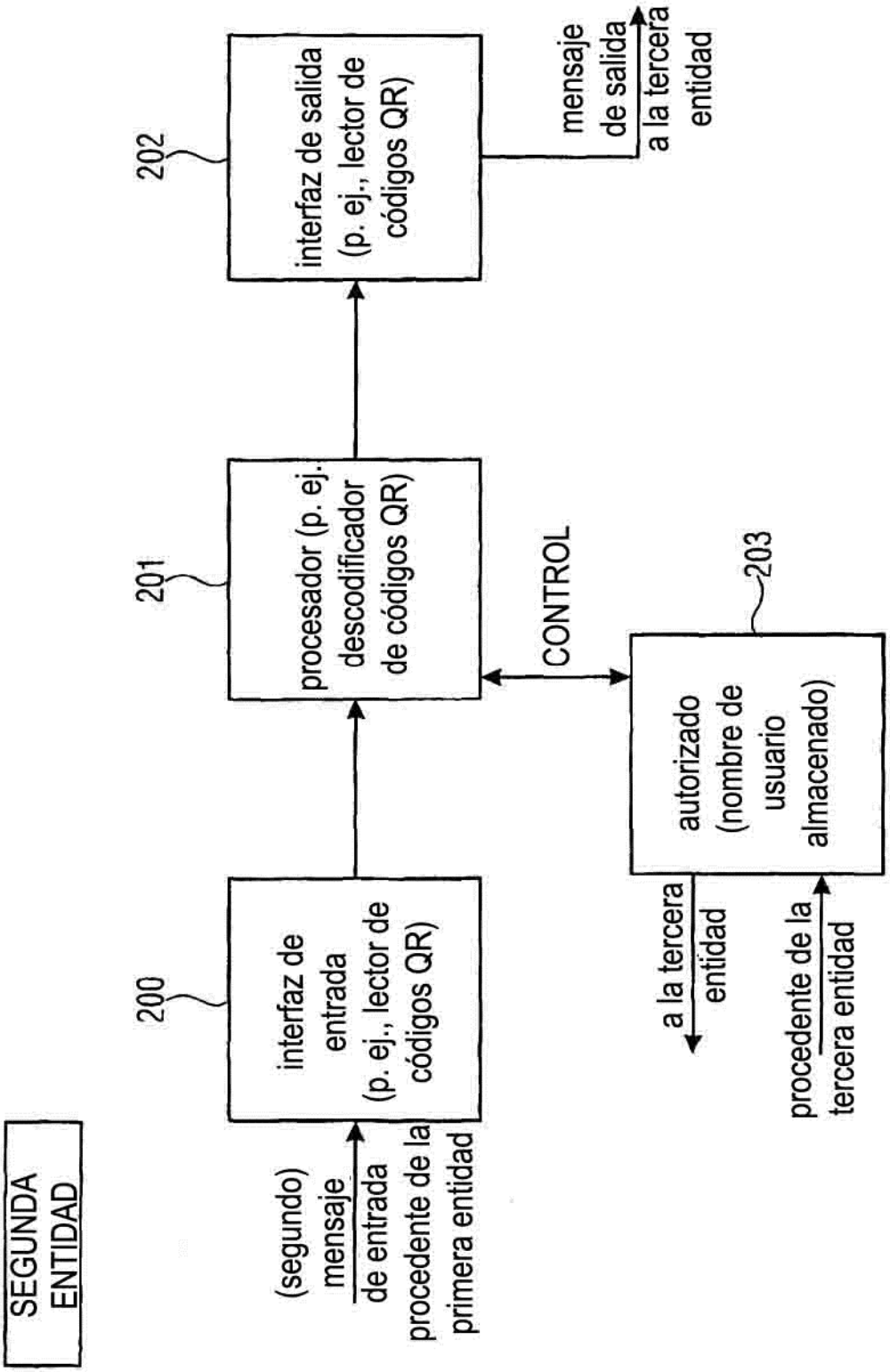
SEGUNDA ENTIDAD
(segundo) mensaje de entrada procedente de la primera entidad
200
interfaz de entrada (p. ej., lector de códigos QR)
201
procesador (p. ej. descodificador de códigos QR)
CONTROL
203
autorizado (nombre de usuario almacenado)
a la tercera entidad
procedente de la tercera entidad
202
interfaz de salida (p. ej., lector de códigos QR)
mensaje de salida a la tercera entidad

FIGURA 20