(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 611 165**

(51) Int. CI.:

G06F 21/43 (2013.01)
G06Q 20/10 (2012.01)
G06Q 20/18 (2012.01)
G06Q 20/32 (2012.01)
G06Q 20/34 (2012.01)
G06Q 20/38 (2012.01)
G06Q 20/40 (2012.01)
G07F 7/10 (2006.01)
H04W 12/06 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **09.07.2009 PCT/EP2009/004986**

(87) Fecha y número de publicación internacional: **04.02.2010 WO10012362**

(96) Fecha de presentación y número de la solicitud europea: **09.07.2009 E 09777072 (1)**

(97) Fecha y número de publicación de la concesión europea: **19.10.2016 EP 2248083**

(54) Título: **Método de autentificación**

(30) Prioridad:

29.07.2008 DE 102008035391

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
05.05.2017

(73) Titular/es:

DEUTSCHE TELEKOM AG (100.0%)
Friedrich-Ebert-Allee 140
53113 Bonn, DE

(72) Inventor/es:

KRÄMLING, ANDREAS;
KOMPART, ANDREAS y
BAUSE, THOMAS

(74) Agente/Representante:

DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Método de autentificación

La invención se refiere a un método para la autentificación de un usuario en un punto de aceptación, siendo la autentificación realizada por la comparación de un número de transacción con un número de transacción calculado o almacenado.

Los métodos de autentificación de este tipo son conocidos y se usan, por ejemplo, en la banca en línea directa cuando se usan números de transacción indexados. Aquí, el índice, es decir un primer número de transacción, se notifica al usuario el cual responde con el TAN, es decir con el número de autentificación de la transacción que representa el segundo número de transacción o ID de la transacción. En este proceso los datos de transacción no están enlazados entre sí, y el TAN, es decir el número de autentificación de la transacción, sirve para firmar la transacción, la cual es a continuación activada por esta confirmación.

Una desventaja de los métodos conocidos es que requieren un registro previo del usuario en el punto de aceptación, es decir el usuario tiene que ser conocido en el punto de aceptación, con el resultado de que un método de este tipo no puede ser realizado anónimamente. Además, las listas de los TAN correspondientes tienen que ser hechas disponibles al usuario por adelantado, lo que en particular implica el riesgo de un mal uso si la lista de TAN cae en manos no apropiadas.

La solicitud de patente internacional WO01/48714 describe un método de transacción de pago en el que un centro de transacción compara una identificación de transacción recibida desde un dispositivo móvil de un cliente antes de solicitar un pago.

El objeto de la invención es proporcionar un método para la autentificación de un usuario en un punto de aceptación que ofrezca una seguridad de autentificación mayor y permita, en particular, la autentificación de un usuario anónimo, es decir un usuario que no ha sido registrado previamente en el punto de aceptación.

De acuerdo con la invención, este objeto se consigue mediante el método de autentificación expuesto en la reivindicación 1. Los desarrollos ventajosos de la invención están dados en las reivindicaciones dependientes.

Especialmente ventajoso en el método de acuerdo con la invención para la autentificación de un usuario en un punto de aceptación, siendo la autentificación realizada comparando un número de transacción con un número de transacción calculado o almacenado, es que el punto de aceptación y/o un terminal de usuario envía un mensaje de solicitud a un punto central y el punto central proporciona y transmite un número de transacción temporalmente válido por medio del cual se puede realizar la autentificación en el punto de aceptación, o que el punto de aceptación proporciona un número de transacción temporalmente válido por medio del cual se puede realizar la autentificación en un punto central, siendo realizada una autorización después de la autentificación con éxito en el punto central mediante la generación y transmisión de un mensaje de autorización desde el punto central al punto de aceptación.

Estos desarrollos de la invención hacen posible que un usuario anónimo se autentifique él mismo en un punto de aceptación tal como una máquina expendedora o un cajero automático, o en un servidor de Internet que ofrece programas o archivos para ser descargados, activando a continuación la autentificación con éxito una transacción o similar, en particular activando o confirmando una transacción de pago.

Unas aplicaciones apropiadas pueden ser proporcionadas para este fin en un terminal de usuario y/o una aplicación apropiada puede ser proporcionada en una caja/comprobador de pago en metálico, un PC o similar que sirve como una máquina expendedora o un cajero automático, etc.

A este respecto, el término “usuario anónimo” significa que el usuario no requiere ser previamente registrado en o conocido en el punto de aceptación ya que el procedimiento de autentificación se realiza llamando a un punto central.

Un punto central, es decir se puede proporcionar una aplicación central que sea responsable de controlar la activación de la transacción y, en particular, una transacción de pago que reúna las dos partes anónimas, es decir que en el desarrollo de la autentificación del usuario en el punto de aceptación de acuerdo con la invención sea posible de activar una transacción llamando a un punto central sin que el usuario tenga que registrarse primero en el punto de aceptación.

El punto de aceptación puede ser cualquier máquina expendedora o cajero automático o también un ofrecimiento en Internet. La autentificación puede entonces servir, por ejemplo, para comprobar si el usuario está conforme con cualquier límite de edad especificado para usar los ofrecimientos y/o para activar o confirmar una transacción de pago o similar.

La seguridad del proceso de autentificación está asegurada en particular por el hecho de que los números de transacción permanentemente válidos no tienen que ser proporcionados, extraídos y almacenados previamente sino que en cada caso se proporciona y transmite un número de transacción temporalmente válido por medio del cual se

puede realizar una autentificación. En una primera variante la autentificación es realizada directamente por el punto central en el punto de aceptación mediante la provisión y transmisión del número de transacción temporalmente válido.

La identificación personal (contraseña, por último también un TAN de un solo uso) puede adicionalmente ser solicitado al usuario. La solicitud de esta identificación personal puede tener lugar en cada caso o de una manera basada en reglas que dependen de la situación actual (por ejemplo, detección de un uso no debido, cantidad de la transacción, número de transacciones por intervalo de tiempo).

En la otra variante del método de acuerdo con la invención, el número de transacción temporalmente válido es proporcionado por el punto de aceptación para permitir la autentificación en el punto central, después de esto, tras la autentificación con éxito, este punto central genera a continuación un mensaje de autorización y lo transmite al punto de aceptación.

Esto asegura un nivel de seguridad muy alto del proceso de autentificación.

Preferiblemente, la solicitud de la provisión y/o la transmisión del número de transacción son enviadas por el punto de aceptación al punto central y/o por un terminal de usuario al punto de aceptación y/o al punto central, en particular por un terminal de telefonía móvil que tiene una aplicación de autentificación apropiada.

Preferiblemente, el proceso de autentificación es activado por un usuario mediante un código personal, en particular una contraseña, un número de transacción de un uso único (TrxID) o una identificación biométrica, en particular una huella digital o similar.

Preferiblemente, se requiere en cada caso la indicación de un código personal para activar el proceso de identificación o, alternativamente, se solicita dependiendo de la situación actual, en particular dependiendo del volumen de transacciones del usuario en un intervalo de tiempo, de la magnitud de la suma de la que se trata, del historial del cliente, del tipo de artículo y/o de otras características específicas del cliente.

De este modo se puede conseguir un mayor nivel de seguridad sin ser evidente al cliente que el nivel de seguridad del proceso de identificación es variable y, en particular, puede depender de parámetros predefinibles.

Preferiblemente, la comunicación entre el terminal de usuario, el punto de aceptación y el punto central tiene lugar por medio de conexiones de telefonía móvil y/o conexiones telefónicas o conexiones de comunicación temporales o permanentes, en particular vía Internet, y/o mediante una comunicación de corto alcance.

La comunicación entre el terminal de usuario, el punto de aceptación y el punto central puede así tener lugar por medio de diversos canales de comunicación alternativos o acumulativos, dependiendo de qué opción y cobertura de red está disponible así como en el nivel de seguridad requerido. En particular, la comunicación entre el terminal de usuario, el punto de aceptación y el punto central pueden tener lugar de una manera encriptada, es decir, con los datos transmitidos y/o los paquetes de datos, los datos de transacción y el número de transacción siendo transmitidos en una manera encriptada.

Igualmente, se pueden usar servicios diferentes, tales como el SMS (telefonía móvil) y/o enlaces de datos (telefonía móvil). La comunicación puede también tener lugar por línea de telefonía terrestre, DSL o similar, así como utilizando una combinación de diferentes servicios y tecnologías.

En una realización preferida la solicitud de provisión y/o transmisión del número de transacción es hecha por el punto de aceptación en el punto central y/o por un terminal de usuario en el punto de aceptación y/o por un terminal de usuario en el punto central. En particular, el terminal de usuario puede ser un terminal de telefonía móvil que tiene una aplicación de autentificación apropiada.

Hay por lo tanto varias posibilidades que pueden ser usadas alternativa o acumulativamente para realizar y aplicar el método de acuerdo con la invención. Las diferentes alternativas permiten la creación de una amplia variedad de aplicaciones, en particular cuando las rutas de transmisión tales como la telefonía móvil o las conexiones por Internet o similares están temporal o permanentemente no disponibles. Con una aplicación acumulativa de las diferentes variantes es posible establecer unos niveles de seguridad más altos, en particular en la forma de autentificaciones anidadas o verificadas.

En una realización preferida del método de acuerdo con la invención, el número de transacción es solicitado por medio de un terminal de telefonía móvil por medio de un primer mensaje corto y/o USSD, siendo transmitido el número de transacción por el punto central por medio de un segundo mensaje corto y/o USSD al terminal de telefonía móvil.

Mediante el uso de conexiones de telefonía móvil y de mensajes cortos (SMS, Servicio de Mensajes Cortos) se asegura un nivel de seguridad muy alto mientras que al mismo tiempo se permite la rápida realización del método de autentificación, ya que el punto central puede enviar una respuesta inmediata al primer mensaje corto de solicitud. A este respecto, el terminal de telefonía móvil transmite un único código de usuario, por ejemplo en la forma de

Número de Red Digital de Servicios Integrados de Abonados Móviles (MSISDN), es decir el número de abonado en el que un abonado de telefonía móvil puede ser conectado y por medio del cual un usuario puede ser claramente identificado, siendo posible en una base de datos apropiada del punto central asignar a este código de usuario una cuenta de usuario, por ejemplo, o verificación de la edad o similar.

Los Datos del Servicio Suplementario No Estructurado (USSD) son un servicio de transmisión para redes GSM y soporta servicios suplementarios de telefonía móvil.

Preferiblemente, el número de transacción es transmitido por el punto central por medio de una conexión de telefonía móvil a un terminal de telefonía móvil o por medio de una conexión telefónica a un teléfono. Una transmisión de este tipo a un terminal de telefonía móvil o a un teléfono de línea terrestre puede, por ejemplo, ser hecha en la forma de un mensaje corto (SMS), como se ha descrito antes. Alternativa o acumulativamente, también es posible para el número de transacción que sea transmitido por un servicio de voz en la forma de un mensaje de voz que sea anunciado automáticamente, o en la forma de un correo electrónico o similar.

Alternativa o acumulativamente, el número de transacción puede también ser transmitido en la forma de un archivo de gráficos dentro de un mensaje multimedia (MMS, Servicio de Mensajería Multimedia) enviado al terminal de telefonía móvil. Representando el número de transacción como parte de un gráfico transmitido, se aumenta todavía más el nivel de seguridad del método de acuerdo con la invención ya que es más difícil para una tercera parte no autorizada espiar el número de transacción a partir del gráfico para acceder a un mensaje de voz u oírlo, incluso aunque sólo solamente sea por casualidad.

En una realización preferida del método de acuerdo con la invención, el número de transacción se calcula por medio de un algoritmo. En particular a este respecto, una palabra de código y/o un número de identificación del abonado, en particular los MSISDN, IMSI o TIMSI, pueden formar la base para el cálculo y/o un código transmitido por una comunicación de corto alcance pueden formar la base para el cálculo. El MSISDN es el número de telefonía móvil, es decir el Número de Red Digital de Servicios Integrados de Abonados Móviles (MSISDN), el cual es el número de abonado que hay que marcar que usa el que llama para conectar con un abonado de telefonía móvil. La IMSI es la Identidad del Abonado Móvil Internacional, y la TIMSI es, por consiguiente, una Identidad Temporal del Abonado Móvil Internacional. De este modo es posible una identificación clara de la identidad por medio de los MSISDN, IMSI o TIMSI.

Es especialmente ventajoso a este respecto que el nivel de seguridad del método de acuerdo con la invención pueda ser aumentado todavía más habiendo el algoritmo funcionado como un proceso oculto y calculando el número de transacción inmediatamente tras una solicitud de un número de transacción, es decir marcándolo innecesariamente para guardar y mantener un almacén de números de transacción, el cual posiblemente podría ser espiado.

En una realización posterior del método de acuerdo con la invención, el número de transacción es calculado por medio de un algoritmo por el punto de aceptación y por el punto central usando unos parámetros fijos. En particular a este respecto, la fecha y/o la hora de las solicitudes del número de transacción y/o los parámetros de una transacción de pago, en particular un número de orden y/o un número de artículo y/o un precio del artículo y/o un código del punto de aceptación y/o el número de transacciones activas pueden ser usados como parámetros y de este modo constituir la base para el cálculo del número de transacción por medio del algoritmo.

De este modo, usando una aplicación apropiada, los números de transacción se calculan usando un algoritmo en el punto de aceptación y en el punto central, con el algoritmo funcionando como un proceso oculto de modo que no hay necesidad de almacenar un almacén de números de transacción, lo que aumenta todavía más el nivel de seguridad.

La autentificación del usuario puede entonces ser realizada bien por el punto de aceptación que emite el número de transacción calculado, permitiendo al usuario autentificarse él mismo en el punto central, o bien por el punto central que proporciona el número de transacción calculado al usuario el cual puede entonces usar este número de transacción para autentificarse él mismo en el punto de aceptación.

En una realización preferida del método de acuerdo con la invención la autentificación se realiza usando una tupla del número de transacción que consta de al menos dos números de transacción A y B, siendo el primer número de transacción A proporcionado por el punto de aceptación, y el segundo número de transacción B siendo proporcionado por el punto central basado en el primer número de transacción A.

Preferiblemente, una lista de números de transacción no usados y/o de tuplas de números de transacción es almacenada temporal o permanentemente de una forma interrogable por el punto de aceptación.

Esto hace posible incluir en el método de acuerdo con la invención incluso aquellos puntos de aceptación que no pueden ser conectados en línea directa a un punto central por medio de un teléfono y/o una conexión por Internet y/o una conexión por telefonía móvil, haciendo disponibles una o más listas de números de transacción y/o de tuplas de números de transacción y almacenando estas listas temporal o permanentemente en el punto de aceptación de una forma interrogable cuando el punto de aceptación está siendo cargado. Esto hace posible conseguir una

completa independencia en la parte del punto de aceptación a partir de la presencia de un enlace de datos con el punto central.

En una realización preferida el método de acuerdo con la invención se desarrolla de modo que se autoriza y se realiza a través de la autentificación de una transacción, en particular que un envío o manejo de mercancías y/o una transacción de pago se activa y realiza en el punto de aceptación, es decir que a través de la realización de la autentificación una transacción de pago, por ejemplo, se lleva a cabo en un cajero automático o similar.

Preferiblemente, después de la transmisión de un mensaje de autorización por el punto central al punto de aceptación, el usuario obtiene acceso a los locales y/o a una celebración, en particular a un cine, a una piscina, a un concierto o similar.

El método también puede ser usado, una vez que un mensaje de autorización ha sido transmitido por el punto central al punto de aceptación, con el fin de permitir que el usuario utilice un servicio, en particular un servicio consular, gubernamental o similar.

Igualmente, un posible desarrollo consiste en, una vez que un mensaje de autorización ha sido transmitido por el punto central al punto de aceptación, permitiendo que el usuario acceda a datos analógicos o digitales, en particular medios tales como noticias, música, vídeo o similares.

Preferiblemente, el método se usa para realizar una verificación y/o asegurar la conformidad con las disposiciones legales, en particular las restricciones por la edad y/o restricciones voluntarias.

Por una parte, esto permite la verificación de la conformidad con las disposiciones legales obligatorias, tales como un límite de edad legal, por ejemplo, mayoría de edad. También permite la verificación de la conformidad con las restricciones fijadas por los cuerpos de autorregulación voluntaria, tales como los límites de edad para cines y similares. Igualmente, también pueden ser verificadas las autorrestricciones voluntarias que los usuarios se hayan impuesto a sí mismos, tales como un bloque para casinos de juego.

Preferiblemente, se usa un número de transacción numérico o alfanumérico (TrxID).

Preferiblemente, se usa un número de transacción (TrxID) para establecer un enlace de comunicación entre el punto de aceptación y el terminal de usuario.

Usando el número de transacción (TrxID) para establecer un enlace de comunicación entre el punto de aceptación y el terminal de usuario es posible establecer un enlace especialmente codificado de una manera simple y segura.

De acuerdo con la invención, el número de dígitos del número de transacción (TrxID) se adapta dinámicamente, en particular de acuerdo con el número de transacciones activas paralelas y/o de acuerdo con la carga de tráfico estimada.

Preferiblemente, la reutilización temporal del número de transacción (TrxID) se selecciona de acuerdo con el tipo de punto de aceptación.

Preferiblemente, la reutilización geográfica del número de transacción (TrxID) se selecciona dinámicamente de acuerdo con el código del país y/o las células de telefonía móvil y/o el lugar del punto de aceptación.

Preferiblemente, el usuario activa el proceso de autentificación bien enviando simplemente el número de transacción (TrxID) al punto central o bien introduciendo adicionalmente un identificador personal en una contraseña personal particular, TAN, ITAN, información biométrica, en particular una huella digital o similar.

Preferiblemente, el punto de aceptación comunica indirectamente con el punto central, en particular a través de uno o más agregadores, en particular un punto de recogida del distrito, el ordenador central en el supermercado o similar.

Por lo tanto, no es necesario que cada uno de los puntos de aceptación esté conectado directamente o que sea conectable directamente al punto central ya que existe la posibilidad de agrupar varios puntos de aceptación en unidades y comunicar indirectamente con el punto central.

Preferiblemente, los abonados usan una variedad de medios de comunicación, en particular Ethernet, Internet, líneas terrestres, radio o teléfonos móviles y/o diferentes servicios/protocolos, en particular USSD, IP, SMS, GPRS.

A este respecto, “abonado” significa cualquier componente implicado en el proceso de autentificación, en particular un terminal de usuario, un punto de aceptación, una base de datos, etc. Con respecto al terminal de usuario, éste puede ser en particular un terminal de telefonía móvil, aunque también puede ser un terminal de comunicaciones terrestres tal como un teléfono o un ordenador.

Alternativa o acumulativamente, en el caso de avería, la entrega incompleta del artículo / provisión de un servicio, el no acceso a los locales o similares, puede ser reembolsada la suma total o una suma parcial más una cantidad posible como compensación.

En el caso de una transacción de pago, se pueden deducir/añadir automáticamente diversos márgenes tales como un cargo por la conversión de moneda, un cargo para cubrir el riesgo de avería, los cargos por procesamiento, de modo que el punto de aceptación reciba una cantidad menor y/o que el usuario pague una cantidad mayor.

A este respecto, la cantidad de la moneda puede ya ser fijada al comienzo de la transacción o ser negociada entre las partes durante la transacción, permitiendo, si es necesario, la especificación de unos límites superiores y/o inferiores por uno o/y el otro abonado. También se puede incluir una gratificación por el servicio.

Inicialmente se puede reservar una cantidad durante un tiempo definido y la cantidad total o las cantidades parciales pueden ser finalmente enviadas durante este período de tiempo, con la cantidad restante siendo entregada automáticamente al final del período de tiempo, a menos que esto no haya sido hecho ya por el punto de aceptación por medio de un mensaje anterior.

Es posible para una o ambas partes seleccionar el medio de pago a partir de una lista específica de abonados (bien durante la transmisión de la solicitud del ID de la transacción o en el curso de una conversación).

Los medios posibles de pago pueden ser adaptados dinámicamente por el punto central para uno o ambos abonados y limitados según convenga, por ejemplo como una función del historial de pago, la solvencia, el riesgo de uso indebido, la cantidad de volumen de negocio, el número de transacciones, etc.

Durante la autentificación y el procesamiento de las transacciones de pago, los abonados (punto de aceptación y/o usuario) pueden usar las mismas o diferentes monedas.

También es posible dirigir la comunicación con el abonado (punto de aceptación y/o usuario) en diferentes idiomas.

En una realización preferida, cuando se autoriza la transacción el punto central calcula una clave que es única y permanentemente asignada al usuario, en particular adicionalmente al punto de aceptación, e informa al punto de aceptación de esta clave para que las transacciones previas del usuario puedan ser claramente asignadas al usuario.

A este respecto, la clave es única y permanente, al menos en cuanto al usuario y posiblemente con respecto a la combinación del usuario y el punto de aceptación.

Una puesta en práctica y aplicación a modo de ejemplo de esta variante sería que el cliente descargase un artículo pagadero de un portal de Internet, por ejemplo, Test.de.

Mediante la “clave permanente” el usuario es reconocido y así le es dado acceso a los artículos previamente comprados y puede descargarlos.

Además, Test.de, por ejemplo, puede reconocer que el cliente está principalmente interesado en “electrónica de entretenimiento” y presentar los artículos apropiados (el cliente propiamente dicho, no obstante, tiene que ser conocido).

En una posterior realización preferida, el valor de la transacción es igual a 0, en particular la cantidad de dinero de la transacción es igual a 0, y por lo tanto se da acceso al usuario a una cuenta de usuario libre de cargas.

Por ejemplo, esto permite el acceso repetido a artículos previamente comprados y pagados a través de una red informática tal como la Internet.

En las Figuras se ilustran varias realizaciones a modo de ejemplo del método de acuerdo con la invención y se explican más adelante con referencia a las figuras, en las que:

la Figura 1 muestra una primera realización de un método de acuerdo con la invención para autentificación de un usuario en un punto de aceptación;

la Figura 2 muestra una segunda realización de un método de acuerdo con la invención para autentificación de un usuario en un punto de aceptación;

la Figura 3 muestra una tercera realización de un método de acuerdo con la invención para autentificación de un usuario en un punto de aceptación;

la Figura 4 muestra una cuarta realización de un método de acuerdo con la invención para autentificación de un usuario en un punto de aceptación;

la Figura 5 muestra una quinta realización de un método de acuerdo con la invención para autentificación de un usuario en un punto de aceptación.

Las Figuras 1 a 5 ilustran diversas realizaciones y variantes del método de autentificación de acuerdo con la invención en cada caso como un ejemplo en la forma de la autentificación de un usuario 1 en un punto de aceptación en la forma de una máquina expendedora 3, con una transacción que es autorizada por medio del método de autentificación. En los ejemplos ilustrados se designan los mismos componentes con los mismos símbolos de referencia en cada caso.

La realización a modo de ejemplo ilustrada en la Figura 1 se refiere a la autentificación de un usuario 1 en un punto de aceptación en la forma de una máquina expendedora 3, el vendedor y el comprador estando reunidos por medio de un ID temporal de la transacción, es decir un número de transacción TrxID. Este ID TrxID de la transacción se usa para comunicación de modo que no requiere ser conocido un identificador permanente, por ejemplo número de cuenta, etc, es decir, que el usuario 1 no tiene que registrase primero en el punto de aceptación 3.

Con fines de claridad, por ejemplo, la transacción puede ser identificada a largo plazo por medio del sello del momento de la transacción y el ID temporal de la transacción o por un ID único de largo plazo. El ID de la transacción de largo plazo, es decir el número de la transacción se emite durante la transacción, siendo preferido un número de transacción de largo plazo por razones técnicas.

En la Figura 1 se ilustra la secuencia del método de acuerdo con la invención. En la forma de la máquina expendedora 3 se hace disponible una oferta para la distribución de los artículos, el usuario 1 realiza la correspondiente elección seleccionando el artículo apropiado en la máquina expendedora 3, es decir, en el punto de aceptación, por ejemplo introduciendo un número de código para identificar el artículo o similar. Esto hace que la máquina expendedora 3 comience el proceso de autentificación y la transacción.

Como el usuario 1, el cual posee un terminal 2 de telefonía móvil, que le identifica claramente a través del número de identificación de abonado MSISDN, no ha sido registrado previamente en la máquina expendedora 3, la máquina expendedora 3 no conoce el MSISDN del terminal 2 de telefonía móvil.

Habiendo comenzado la transacción, la máquina expendedora 3 solicita un número de transacción temporal TrxID al punto central 4, que indica la categoría de la suma y las mercancías a medida que lo hace. En el ejemplo de acuerdo con la Figura 1 el número de transacción TrxID “8823” es transmitido desde el punto central 4 al punto de aceptación 3. El punto de aceptación 3 y el punto central 4 están conectados para este fin mediante un enlace de datos para intercambiar datos, es decir el punto de aceptación 3 y el punto central 4 tienen un canal de comunicación. Esto puede, por ejemplo, conseguirse por medio de una conexión de Internet, una conexión de telefonía terrestre o una conexión de telefonía móvil. En el ejemplo ilustrado el enlace entre el punto de aceptación 3 y el punto central 4 es, a modo de ejemplo, una conexión de Internet.

Cuando se usa una conexión de telefonía móvil se pueden usar diferentes servicios tales como enlaces de datos, SMS, USSD, etc.

De este modo el punto central proporciona el ID “8823” temporal de la transacción e informa de esto al punto de aceptación 3, es decir al punto de venta 3, a su vez el punto de aceptación 3 transmite este ID TrxID 8823 temporal de transacción al usuario 1. Esta transmisión al usuario 1 puede ser hecha verbalmente y/o por medio de una presentación visual y/o por medio de Internet o similar. Alternativamente, el TrxID puede ser transmitido por radio (Bluetooth, NFC) o por señales infrarrojas.

El usuario 1 tiene así la posibilidad, usando el terminal 2 de telefonía móvil y el número de transacción TrxID “8823”, de transmitir lo último al punto central 4, por ejemplo enviando al punto central un mensaje corto SMS con un texto predefinido apropiado tal como “999#8823”, como en el ejemplo ilustrado. Este mensaje corto desde el terminal 2 de telefonía móvil al punto central 4 naturalmente comprende también el número de identificación del abonado MSISDN además del número de transacción TrxID “8823”. Este SMS es recibido por el punto central 4 y procesado posteriormente.

En el ejemplo ilustrado esto se hace por medio de una solicitud de USSD usando el terminal 2 de telefonía móvil. Los Datos de Servicio Suplementario No Estructurado (USSD) son un servicio de transmisión normalizado para redes GSM que soporta unos servicios suplementarios de telefonía móvil aplicados por medio de la señalización GSM. Los números de acceso para servicios de este tipo que tienen que ser marcados con el fin de utilizar tales servicios tienen el formato *1NN#, solicitando los “*” y # el servicio apropiado. A través de los servicios USSD es posible, por ejemplo, obtener acceso a servicios preconfigurados que son específicos del operador de la respectiva red de telefonía móvil.

El número de transacción TrxID transmitido por el punto central 4 al punto de aceptación 3 depende del número total de números de transacción TrxID, el cual depende nuevamente del número de transacciones paralelas. Por ejemplo, el número de transacción hecho disponible puede comprender 4 dígitos como en el ejemplo descrito. El número de transacción TrxID es válido para un período de tiempo limitado.

La longitud del TrxID se calcula dinámicamente dependiendo de las transacciones paralelas / transacciones paralelas previstas.

Usando el ID proporcionado de la transacción (por ejemplo 8823), el ofrecimiento puede ahora ser solicitado al punto central 4, estando el ofrecimiento identificado por la transacción ID.

Los datos de la oferta tales como el precio, designación del producto y el comerciante son después visualizados como un resultado del punto 4 que accede a los datos almacenados en la base de datos 5. El usuario 1 tiene ahora la posibilidad de aceptar o rechazar la oferta. Si el cliente 1 confirma la transacción, la suma es autorizada y enviadas a través de la plataforma de la transacción. El punto central 4 confirma a continuación la autorización al punto de aceptación 3, tras lo cual las mercancías son entregadas y el punto de aceptación 3 envía un correspondiente mensaje al punto central 4. Si es necesario, mientras se realiza la transacción se puede hacer al suministrador 3 o al usuario 1 una solicitud para especificar el medio de pago deseado. Una vez que el artículo ha sido enviado y realizada la transacción, la suma es adeudada, como se muestra en la Figura 1, y termina el proceso, es decir la transacción.

Son posibles unas posteriores variantes del método de acuerdo con su invención y su realización, por ejemplo en la forma en la que la transacción es activada o comenzada por el usuario 1.

También es posible que la transacción sea comenzada por el deudor 1, es decir el cliente, o el acreedor 3, es decir el suministrador, sin indicar un precio o indicando solamente un límite de precio superior dado. Cuando se ha establecido el enlace de comunicación puede tener lugar la negociación del precio. Solamente se activa la transacción del pago y solamente tiene lugar una vez que se ha acordado un precio.

También es posible comenzar la transacción del pago usando el punto central 4, pero con sus similares comunicándose directamente entre sí, por ejemplo para descargar los términos y condiciones generales y para entregar la mercancía, por ejemplo en la forma de transmisión de archivos electrónicos a través de Internet.

Es posible usar idiomas diferentes al deudor 1 y al acreedor 3 durante la autentificación y realización de la transacción debido a que el punto central 4 y la base de datos 5 están implicados como intermediarios.

El intervalo de reutilización de números de transacción, es decir los IDs de la transacción, pueden ser reducidos usando una información adicional, tal como el país, la célula de telefonía móvil, etc, lo cual permite usar unos números de transacción más cortos. El deudor 1 (cliente) y el acreedor 3 (suministrador) pueden establecer su transacción por medio de diferentes redes o servicios de comunicación, por ejemplo línea terrestre, LAN, W-LAN, GPRS, USSD (radio), canal de voz (radio), etc.

A este respecto las características de los números de identificación de la transacción generados dinámicamente son tales que el número de puntos de aceptación es mayor que el número de transacciones simultáneas. Ya que no todos los puntos de aceptación tienen su propio identificador único sino que les es asignado un identificador temporal, éste puede ser más corto. Como resultado, la introducción manual en el terminal se hace más simple. Por ejemplo, hay más de 600.000 máquinas de pago en la forma de máquinas expendedoras para bebidas y cigarros, pero solamente se realizan simultáneamente unos pocos cientos de transacciones en la República Federal de Alemania.

La longitud de los números de transacción depende del nivel de tráfico. Fuera de los períodos de pico, por ejemplo por la noche, se puede usar un número de transacción muy corto, que consta por ejemplo de solamente dos dígitos, es decir que la longitud de los números de transacción puede variar de acuerdo con el nivel de tráfico, por ejemplo, la hora del día.

Como el número de transacción en el ejemplo explicado antes con referencia a la Figura 1 tiene que ser solicitado para cada transacción de pago, se requiere un enlace desde el punto de aceptación a la plataforma de transacción. Por lo tanto, tiene que establecerse un enlace específico o tiene que haber un enlace permanente.

Los pasos individuales del proceso de la secuencia de acuerdo con la Figura 1 son:

11 El cliente 1 selecciona el objeto deseado en una máquina expendedora 3. La máquina expendedora 3 comienza la transacción del pago (MSISDN desconocido).

12 Se transmite el ID (TrxID) temporal de la transacción. La longitud del TrxID depende del número total de números de transacción TrxID, que depende del número de transacciones paralelas (por ejemplo 4 dígitos). El número de transacción TrxID es válido durante un tiempo limitado y es visualizado.

13 El cliente 1 comienza una solicitud de USSD, los MSISDN y TrxID son recibidos por el punto central 4.

14 Selección de transacción/oferta basada en el TrxID. Se visualizan los detalles. El cliente 1 debe confirmar la transacción. La suma es autorizada y enviada (por medio de la plataforma de transacción).

15 El cliente 1 es notificado de la autorización con éxito y se adeuda la suma (respuesta a la solicitud de USSD). La máquina expendedora 3 recibe información de la autorización, el artículo es entregado.

16 Transacción terminada.

En la variante ilustrada en la Figura 2 para la realización de una transacción de pago por medio de tuplas de números de transacción almacenados no es necesario un enlace en línea directa permanente o el establecimiento de un enlace específico entre la máquina expendedora 3 y la plataforma de transacción 4, es decir que la máquina 3 en el ejemplo mostrado no tiene la posibilidad de establecer un enlace en línea directa permanente, por ejemplo debido a que la tecnología apropiada no está disponible o no existe conexión de radio, si no hay cobertura telefónica en la zona del punto de aceptación 3.

La transacción, es decir la transacción de pago ilustrada en el ejemplo de la Figura 2 está controlada por medio de tuplas del número de transacción que consta de dos IDs de transacción. Estas tuplas son llevadas al punto de venta 3 de antemano, por ejemplo manualmente como parte del proceso para dar servicio y/o cargar la máquina expendedora 3 o por medio de establecer un enlace una sola vez por medio de una conexión de comunicación.

Uno de estos IDs es dado a conocer por el acreedor 3 (suministrador) al deudor 1 (cliente), y el deudor 1 lo usa para realizar una autorización usando este primer número de transacción TrxID A de la tupla del número de transacción que consta de dos números de transacción A y B.

Después de la autorización y ejecución con éxito de la transacción de pago, el deudor 1 es notificado del segundo ID TrxID B que él notifica al acreedor 3. Si éste corresponde con el segundo TrxID B almacenado, el artículo puede ser entregado. Un tupla del número de transacción que consta de los IDs A y B de la transacción identifica claramente el precio y, posiblemente, la categoría de la mercancía, es decir que la transacción y/o la oferta es seleccionada sobre la base del número de transacción TrxID. Como está ilustrado en la Figura 2, los detalles son visualizados y la transacción es confirmada indicando el primer número A de la transacción, en particular la suma es adeudada con la participación de la base de datos 5 y el punto central 4 por intermedio del cual se ejecuta la transacción.

Después de la provisión por el punto central 4 del segundo número de transacción TrxID B, que es requerido para completar la tupla del número de transacción que consta de A y B, a través de la transmisión al terminal 2 de telefonía móvil del usuario 1, la entrega del artículo puede ser activada usando el segundo número de transacción TrxID B pasándolo a la máquina expendedora 3, tras lo cual la máquina expendedora 3 envía una confirmación correspondiente de la entrega del artículo al punto central 4 como verificación de la transacción realizada. Alternativamente, si la transacción falla, se envía una notificación para comunicar que la transacción ha fallado, seguida por el reembolso de la suma enviada.

El vendedor, es decir el acreedor 3, busca por adelantado uno o más bloques de tuplas de números de transacción. Necesita un bloque por categoría de precios y mercancías.

Cuando hace una oferta, el acreedor 3 informa al comprador, es decir al deudor 1, de un ID A de transacción de una tupla que concuerda con la categoría/precio de la mercancía, por ejemplo visualizándola en la máquina expendedora 3.

El deudor 1 realiza una autorización de la transacción indicando el ID A de la transacción notificado. Al hacerlo, recibe una información sobre la oferta, por ejemplo precio, categoría de la mercancía, vendedor, etc.

Si el deudor 1 acepta la oferta, recibe un segundo ID B de la transacción desde el punto central 4 por medio del cual puede autentificarse él mismo en el acreedor 3 informando al acreedor 3 del segundo ID B de la transacción, por ejemplo a través del envío automático desde el terminal de usuario 2 a la máquina expendedora 3.

El acreedor 3 comprueba si el segundo ID B notificado de la transacción coincide con su primer ID A de transacción, es decir si éste es una tupla correcta del número de transacción que consta de A y B. Si la respuesta es sí, la mercancía es entregada.

En una variante del método de acuerdo con la invención el acreedor 3 es claramente identificado a través del ID de la transacción, o alternativamente, el deudor 1 tiene que introducir adicionalmente en la aplicación un código de identificación del comerciante. El intervalo de reutilización de los números de identificación puede ser reducido usando información adicional tal como el país, la célula de telefonía móvil, etc, que permite usar unos números de identificación y tuplas de números de identificación más cortos.

En una variante posterior la transacción, es decir la autentificación, se realiza por medio de una tupla del número de transacción, pero a diferencia del ejemplo anterior las tuplas del número de transacción no están almacenadas en listas, sino que se calculan en una base caso por caso tras la solicitud, es decir tras la activación de un proceso de un proceso de autentificación, por medio de un algoritmo.

Aquí, el comprador (deudor) informa al punto central de los datos de transacción tales como el comerciante, el punto de aceptación, la categoría de la mercancía usando la aplicación apropiada en su terminal de telefonía móvil. Basándose en los datos de la transacción, tanto el punto de aceptación y el punto central cada uno calcula una clave. El punto central envía al deudor la clave que ha calculado, es decir al cliente, el cual la envía al acreedor, por ejemplo introduciéndola en el teclado del terminal de telefonía móvil, o similar. Si las dos claves coinciden, la mercancía puede ser entregada. Para calcular la clave no solamente se usan los datos de transacción sino también,

en particular, datos secretos tales como un código personal ha de ser introducido, o también datos variables tales como la hora en la que se activó la transacción.

Una secuencia a modo de ejemplo de un proceso de autorización y transacción de este tipo podría ser como sigue: El deudor 1 selecciona un artículo e introduce los datos de la transacción con detalles sobre el comerciante, el punto de aceptación y la categoría de la mercancía en la correspondiente aplicación de la transacción de su terminal 2 de telefonía móvil. Esta aplicación de transacción o aplicación de pago transmite los datos al punto central 4 que calcula la clave TrxID y la transmite de vuelta a la aplicación de pago del terminal 2 de telefonía móvil. Usando la clave recibida desde el punto central 4 el cliente 1 puede autentificarse él mismo en el punto de aceptación 3 por medio de su terminal 2 de telefonía móvil. El punto de aceptación 3 a su vez calcula la clave TRxID para comprobar la clave, es decir el número de transacción.

Si las claves coinciden, es decir la clave enviada por el punto central 4 es idéntica a la clave calculada por el punto de aceptación 3, el artículo es entregado.

Los pasos individuales del proceso de la secuencia de acuerdo con la Figura 2 son:

20 Solicitud de los números de transacción TrxID de cada combinación (precio y categoría). Los TrxID A y TrxID B son recibidos.

21 El cliente 1 selecciona el artículo deseado en una máquina expendedora 3 o similar.

22 La máquina expendedora 3 selecciona un TrxID A no usado para coincidir con el artículo seleccionado. Se visualiza el TrxID A.

23 El cliente 1 comienza la solicitud de USSD con el TrxID A (el TrxID A tiene que ser único, es decir muy largo o, alternativamente, se tiene que usar un identificador adicional para identificar la máquina expendedora 3).

24 Selección de la transacción/oferta basada en el TrxID A.

25 Se visualizan los detalles. Se confirma la transacción.

26 Se adeuda la suma.

27 La respuesta del USSD contiene el TrxID B. El TrxID B puede ser más corto que el TrxID A, precisamente lo suficientemente largo para asegurar que el TrxID B no pueda ser adivinado.

28 El TrxID B es transmitido a la máquina expendedora 3. Si el TrxID B coincide con el TrxID A, el artículo es enviado. Si es necesario, se realiza de nuevo la introducción del ID, 10 segundos de tiempo de espera en el caso de una introducción equivocada del ID.

29 Solicitud de nuevos números de transacción (TrxID A, TrxID B), notificación de transacciones fallidas → reembolso, información sobre transacciones con éxito (para verificación).

En la Figura 3 se muestra un posterior ejemplo en el que por medio de una única autentificación se produce un registro sistemático, y ya tras el registro sistemático una suma está reservada para el pago de sumas parciales individuales. En el ejemplo mostrado, ésta es 50 €. Si el cliente utiliza ahora diversos servicios del punto de aceptación 3, las sumas parciales individuales son enviadas por medio de un medio de pago interno a partir de una cuenta prepagada en un microcircuito 3a de RFID (Identificación de Radiofrecuencia) al punto de aceptación 3. Cuando se hace la verificación, la suma usada, que es 35 € en el ejemplo mostrado, es enviada como la cantidad final. Después de esto tanto el terminal 2 de telefonía móvil que fue usado para la autentificación en el punto de aceptación 3 y el punto central 4 y la base de datos 5 conectados al mismo son informados sobre los envíos, de modo que una transacción de pago pueda ser realizada para completar el proceso.

Especialmente ventajoso en el método ilustrado para la autentificación y en particular para la ejecución y activación de las transacciones de pago es que el cliente no tiene que revelar su identidad al vendedor. En este caso el vendedor puede ser una máquina expendedora, un cajero automático, un taxi, cualquier punto de venta, una tienda de Internet o similar.

Una ventaja adicional es la alta seguridad del proceso de autentificación, ya que los datos del cliente no pueden ser mal usados, tal como sería posible, por ejemplo, con el número de una tarjeta de crédito o en el caso de manipulación del terminal de la tarjeta EC en un punto de aceptación tal como un supermercado o similar. La autorización es realizada en línea directa de una manera especialmente ventajosa y con un nivel de seguridad muy alto.

La seguridad se aumenta además usando diferentes medios de comunicación. Es decir, se evitan los ataques de “hombre en el medio”, Troyanos, con un alto nivel de probabilidad, ya que ambos medios de comunicación tendrían que ser infectados.

No pueden producirse duplicados a este respecto ya que el ID de la transacción es único dentro de un período de tiempo y solamente es temporalmente válido.

El deudor, y posiblemente el acreedor, pueden seleccionar diversos medios de pago. No es necesario a este respecto para la otra parte conocer el medio de pago elegido. Por ejemplo, se puede hacer una distinción entre una cuenta prepagada privada y una cuenta prepagada de una compañía. Es decir, el medio de pago usado puede, en particular, ser también un valor almacenado (prepagado) o una tarjeta de débito o una tarjeta de crédito. También es posible manejar el pago mediante un débito directo, teniendo el cliente solamente que registrarse primeramente en el punto central en este caso, aunque, como antes, no en el punto de aceptación, asegurando así el anonimato del cliente con respecto al punto de aceptación.

La autentificación y la transacción son autorizadas centralmente para reducir la posibilidad de un mal uso por robo (introducción de PIN, información biométrica) o cuentas por cobrar incobrables, es decir la transacción no es autorizada por la máquina o por un empleado en el punto de venta sino a través del sistema central. Es posible facilitar una restricción con respecto al medio de pago, es decir un límite personal o similar. Al mismo tiempo, que la conformidad con las condiciones de venta, tal como un límite de edad, es posible verificar los datos del cliente y/o introducir un PIN personal / información biométrica o similar.

Además de la transacción de pago real, temas con respecto a gratificaciones o similares pueden ser propuestos durante el diálogo del cliente. Si se confirma, tal gratificación, lleva a una segunda transacción de pago, posiblemente limitada, la segunda transacción de pago, por ejemplo una transacción que es enviada independientemente, por ejemplo para la “cuenta del personal de servicio”. En otra variante solamente se ejecuta un único pago de la transacción, es decir la suma que hay que pagar se aumenta en la cantidad de la gratificación, como es conocido a partir de las transacciones con tarjeta de crédito.

Dependiendo del proceso del negocio, el comprador (cliente) puede, no obstante, revelar su identidad, si por ejemplo, consiente en la transmisión de su número de identificación de abonado MSISDN por el punto central al punto de aceptación cuando se usa un terminal de telefonía móvil para la autorización. A este respecto, la identidad puede ser su “identidad real” o una entidad ficticia.

Es posible reducir la suma de la transacción si una suma máxima ha sido fijada por el acreedor al comienzo de la transacción. Una autorización posterior, es decir aumentando la suma del pago, puede solamente ser realizada mediante una confirmación posterior por el deudor, es decir el cliente. En tal caso, se tiene que activar una segunda transacción mediante una segunda autorización. Es posible para sumas no usuales, o sumas que no han sido cargadas como final, que sean reembolsadas, tal como se muestra en el tercer ejemplo en la Figura 3, en el que al principio fue autorizada una cantidad total de 50 €, de la que solamente se ha usado una suma parcial de 35 €.

Por medio del número de transacción único, es decir un ID temporal de la transacción más un sello de tiempo o un ID a largo plazo de la transacción asignado durante la transacción, la transacción puede ser reproducida. El número de transacción a largo plazo es notificado a ambas partes, por ejemplo en reseñas de las transacciones o en una declaración de cuenta mensual o similar. Esta información puede también ser usada para posteriores verificaciones, tales como una liquidación.

Los pasos individuales del proceso de la secuencia de acuerdo con la Figura 3 son:

31 El cajero automático comienza la “reserva”, la suma para ser reservada siendo especificada y generado un ID temporal de la transacción.

32 El TrxID es visualizado al cliente. A su vez, él comienza una transacción declarando el ID y recibe más detalles (cuánto, quién, etc). El cliente confirma la transacción y la suma es reservada.

33 Notificación de la reserva y asignación con éxito de un TrxID a largo plazo. El medio de pago interno es cargado.

34 El cliente “consume”. Se declara el tiempo.

35 Cuando la “verificación”, como final se carga la suma usada.

36 El cliente y el cajero automático son informados sobre el envío con éxito.

En las Figuras 4 y 5 se ilustran dos realizaciones más del método de autentificación de acuerdo con la invención por medio de las cuales un cliente 1 puede autentificarse él mismo en una máquina expendedora 3 y puede autorizar y realizar una transacción de pago por medio del punto central 4.

El proceso de autentificación es activado por el cliente 1 usando un terminal 2 de telefonía móvil usando los datos transmitidos por la máquina expendedora 3 al terminal 2. Estos datos incluyen el número de transacción TrxID proporcionado por la máquina expendedora 3. Los datos son transmitidos desde la máquina expendedora 3, es decir desde el punto de aceptación 3, al terminal 2 por medio de una comunicación de corto alcance. El mensaje para comenzar la transacción es enviado al punto central 4, es decir a la plataforma de transacción. Los datos transmitidos por el terminal 2 de telefonía móvil a la plataforma de transacción, es decir el punto central 4

comprenden por una parte el número de transacción TrxID proporcionado por la máquina expendedora 3, así como, adicionalmente, el MSISDN que sirve para identificar al usuario 1. El número de transacción TrxID y el MSISDN que identifica al usuario 1 son transmitidos por el terminal 2 al punto central 4 por medio de la red de telefonía móvil.

Los datos de transacción son después procesados según sea apropiado por el punto central 4 y la base de datos conectada 5. La cuenta del cliente 1 es por consiguiente adeudada y, una vez que el punto central 4 ha recibido una confirmación correspondiente desde la unidad de procesamiento y la base de datos 5 genera un mensaje de confirmación que es transmitido, nuevamente, por medio de la red de telefonía móvil, al terminal 2 del usuario 1 para su visualización y posterior procesamiento.

Al mismo tiempo un mensaje de confirmación es generado por el punto central 4 y es transmitido al punto de aceptación 3, después de lo cual el punto de aceptación 3, es decir la máquina expendedora 3, entrega el artículo. La máquina expendedora 3 envía de vuelta una confirmación al punto central 4 declarando que la mercancía ha sido entregada. Esta notificación por el punto de aceptación 3 al punto central 4 relativa a la realización con éxito de la transacción es enviada por el punto central 4 a la unidad de procesamiento 5 de datos conectados, la cual lo confirma de nuevo al punto central 4.

Los pasos individuales del proceso de la secuencia de acuerdo con la Figura 4 son:

41 El cliente 1 selecciona el artículo deseado en una máquina expendedora 3. La máquina expendedora 3 comienza la transacción.

42 El cliente comienza la transacción de pago (autentificación) usando los datos transmitidos por la máquina al terminal (por ejemplo, por medio de NFC, RFID). El mensaje para comenzar la transacción es enviado al punto central, es decir a la plataforma de transacción.

43 La cuenta del cliente es adeudada y el cliente recibe un mensaje de confirmación adicional con respecto a la transacción con éxito.

44 La máquina recibe una confirmación de la transacción la cual puede claramente relacionar con la transacción original ya que, por ejemplo, se usó una clave que se calculó basada en el ID original de la transacción.

45 Dependiendo del proceso del negocio, es decir si la entrega del artículo puede fallar, la máquina envía un mensaje al punto central declarando que el artículo fue entregado con éxito.

El proceso ilustrado en la Figura 5 difiere del de la Figura 4 en que, después de recibir el número de transacción TrxID y el MSISDN por medio de un mensaje desde el terminal 2 para identificar la transacción prevista por una parte, y el usuario 1 por otra parte, el punto central 4 genera un mensaje de confirmación que también está firmado por el punto central 4 por medio de una confirmación con firma. Esta confirmación firmada es transmitida por el punto central 4 directamente al terminal 2, después de lo cual el terminal 2 puede usar esta confirmación de la transacción firmada por el punto central 4 para autentificarse él mismo en el punto de aceptación 3 a través de un enlace de comunicación de corto alcance, de modo que el punto de aceptación 3, en este caso la máquina expendedora 3, pueda entregar el artículo.

Los pasos individuales del proceso de la secuencia de acuerdo con la Figura 5 son:

51 El cliente 1 selecciona el artículo deseado en una máquina expendedora 3. La máquina expendedora 3 comienza la transacción.

52 El cliente comienza la transacción de pago usando los datos transmitidos por la máquina al terminal 2 (por ejemplo, por medio de NFC, RFID). El mensaje para comenzar la transacción es enviado al punto central 4, es decir a la plataforma de transacción.

53 La cuenta del cliente es adeudada y el cliente recibe un mensaje de confirmación opcional con respecto a la transacción con éxito.

54 Además, una confirmación de la transacción con éxito firmada por el punto central 4(plataforma de transacción) es enviada al terminal 2 del usuario. El usuario o el terminal 2 del usuario transmite la información por NFC o RFID al punto de aceptación 3 (firmado: por ejemplo método de clave pública/privada, algoritmo “secreto”.

55 La confirmación de la transacción es enviada a la máquina 3 (punto de aceptación), que entrega el artículo.

En los ejemplos mostrados en las Figuras 4 y 5 la comunicación entre el terminal 2 del usuario y el punto central 4 tiene lugar de este modo por medio de la red de telefonía móvil. La comunicación entre el terminal 2 de usuario y el punto de aceptación 3, por otra parte, tiene lugar por una comunicación de corto alcance tal como NFC o RFID.

En los ejemplos mostrados en las Figuras 4 y 5 el número de transacción TrxID es proporcionado por el punto de aceptación 3 después de que el proceso de autentificación ha comenzado, siendo la autentificación en el punto central 4 realizada por la generación de un correspondiente mensaje por el terminal 2. Este mensaje procedente del

terminal 2 contiene no sólo el número de transacción TrxID sino también el número de identificación MSISDN del abonado, por medio del cual el usuario 1 puede ser identificado.

REIVINDICACIONES

1. Un método para la autentificación de un usuario (1) en un punto de aceptación (3), siendo realizada la autentificación comparando un número de transacción (TrxID) con un número de transacción (TrxID) calculado o almacenado, en donde el punto de aceptación (3) y/o un terminal (2) del usuario envía un mensaje de solicitud a un punto central (4) y el punto central (4) proporciona y transmite un número de transacción (TrxID) temporalmente válido por medio del cual se puede realizar la autentificación del usuario (1) en el punto de aceptación (3), o en donde el punto de aceptación (3) proporciona un número de transacción (TrxID) temporalmente válido por medio del cual se puede realizar la autentificación del usuario (1) en el punto de aceptación (4), siendo realizada una autorización después de la autentificación con éxito en el punto central (4) por la generación y transmisión de un mensaje de autorización desde el punto central (4) al punto de aceptación (3) **caracterizado por que** el número de dígitos del número de transacción (TrxID) es adaptado dinámicamente de acuerdo con el número de transacciones activas paralelas y/o de acuerdo con una carga de tráfico estimada.

2. Un método de acuerdo con la reivindicación 1, **caracterizado por que** la solicitud para la provisión y/o transmisión del número de transacción (TrxID) es enviada por el punto de aceptación (3) al punto central (4) y/o por un terminal (2) del usuario al punto de aceptación (3) y/o al punto central (4), en particular por un terminal (2) de telefonía móvil que tiene una aplicación de autentificación apropiada.

3. Un método de acuerdo con la reivindicación 1 o 2, **caracterizado por que** el proceso de autentificación es activado por un usuario a través de un código personal, en particular una contraseña, un número de transacción (TrxID) de un único uso o una identificación biométrica, en particular una huella digital o similar.

4. Un método de acuerdo con cualquiera de las anteriores reivindicaciones, **caracterizado por que** en cada caso se requiere la indicación de un código personal para activar el proceso de autentificación o por que la solicitud se hace dependiendo de la situación actual, en particular dependiendo del volumen de negocio del usuario (1) dentro de un intervalo de tiempo, de la magnitud de la suma de la que se trata, del historial del cliente, del tipo de artículo y/o de otras características específicas del cliente.

5. Un método de acuerdo con cualquiera de las anteriores reivindicaciones, **caracterizado por que** la comunicación entre el terminal (2) del usuario, el punto de aceptación (3) y el punto central (4) tiene lugar por medio de conexiones de telefonía móvil y/o conexiones telefónicas y/o conexiones telefónicas o conexiones de comunicación temporales o permanentes, en particular a través de Internet, y/o a través de una comunicación de corto alcance.

6. Un método de acuerdo con cualquiera de las anteriores reivindicaciones, **caracterizado por que** el número de transacción (TrxID) es solicitado por medio de un terminal (2) de telefonía móvil en un primer mensaje corto y/o por USSD, y por que el número de transacción (TrxID) es transmitido por el punto central (4) en un segundo mensaje corto y/o por USSD al terminal (2) de telefonía móvil.

7. Un método de acuerdo con cualquiera de las anteriores reivindicaciones, **caracterizado por que** el número de transacción (TrxID) es transmitido por el punto central (4) por medio de una conexión de telefonía móvil a un terminal (2) de telefonía móvil o por medio de una conexión telefónica a un teléfono de línea terrestre.

8. Un método de acuerdo con cualquiera de las anteriores reivindicaciones, **caracterizado por que** el número de transacción (TrxID) es calculado por medio de un algoritmo, por el que en particular una palabra de un código y/o un número de identificación de un abonado (1) de telefonía móvil, en particular MSISDN, IMSI o TIMSI, forma la base para el cálculo y/o un código transmitido por una comunicación de corto alcance forma la base para el cálculo.

9. Un método de acuerdo con cualquiera de las anteriores reivindicaciones, **caracterizado por que** el número de transacción (TrxID) es calculado por medio de un algoritmo, tanto por el punto de aceptación (3) como por el punto central (4) usando unos parámetros fijos, en particular por que los parámetros usados son los datos y/o el momento de la solicitud y/o los parámetros de una transacción de pago, en particular un número de orden y/o un número de artículo y/o el precio del artículo, y/o un código del punto de aceptación (3) y/o el número de transacciones activas.

10. Un método de acuerdo con cualquiera de las anteriores reivindicaciones, **caracterizado por que** se usa la autentificación de una tupla del número de transacción (TrxID A, TrxID B) que consta de al menos dos números de transacción (TrxID A, TrxID B), siendo proporcionado un primer número de transacción (TrxID A) por el punto de aceptación (3) y siendo proporcionado un segundo número de transacción (TrxID B) por el punto central (4) basado en el primer número de transacción (TrxID A).

11. Un método de acuerdo con cualquiera de las anteriores reivindicaciones, **caracterizado por que** el punto de aceptación (3) tiene una lista de números de transacción (TrxID) no usados y/o de tuplas de números de transacción (TrxID A, TrxID B) almacenados temporal o permanentemente de una manera interrogable.

12. Un método de acuerdo con cualquiera de las anteriores reivindicaciones, **caracterizado por que** por medio de la autentificación se autoriza y realiza una transacción, en particular por que se activa y se realiza un envío de artículos y/o entrega de artículos en el punto de aceptación (3) y/o la transacción de pago.

13. Un método de acuerdo con cualquiera de las anteriores reivindicaciones, **caracterizado por que** tras un mensaje de autorización transmitido por el punto central (4) al punto de aceptación (3), se da acceso al usuario (1) a los locales y/o a una celebración, en particular a un cine, a una piscina, a un concierto o similar.

14. Un método de acuerdo con cualquiera de las anteriores reivindicaciones, **caracterizado por que** tras un mensaje de autorización transmitido por el punto central (4) al punto de aceptación (3), se permite al usuario (1) utilizar un servicio, en particular un servicio consular, gubernamental o similar.

15. Un método de acuerdo con cualquiera de las anteriores reivindicaciones, **caracterizado por que** tras un mensaje de autorización transmitido por el punto central (4) al punto de aceptación (3), se da acceso al usuario (1) a datos analógicos o digitales, en particular medios tales como noticias, música, vídeo o similares.

16. Un método de acuerdo con cualquiera de las anteriores reivindicaciones, **caracterizado por que** el método se usa para realizar una verificación y/o asegurar la conformidad con las provisiones legales, en particular limitaciones de edad y/o limitaciones voluntarias.

17. Un método de acuerdo con cualquiera de las anteriores reivindicaciones, **caracterizado por que** se usa un número de transacción (TrxID) numérico o alfanumérico.

18. Un método de acuerdo con cualquiera de las anteriores reivindicaciones, **caracterizado por que** usando el número de transacción (TrxID) se establece un enlace de comunicación entre el punto de aceptación (3) y el terminal (2) del usuario.

19. Un método de acuerdo con cualquiera de las anteriores reivindicaciones, **caracterizado por que** se selecciona el uso de nuevo del número de transacción (TrxID) de acuerdo con el tipo de punto de aceptación.

20. Un método de acuerdo con cualquiera de las anteriores reivindicaciones, **caracterizado por que** el uso de nuevo geográfico del número de transacción (TrxID) se selecciona dinámicamente de acuerdo con el código del país y/o las células de telefonía móvil y/o el lugar del punto de aceptación.

21. Un método de acuerdo con cualquiera de las anteriores reivindicaciones, **caracterizado por que** el usuario (1) activa el proceso de autentificación bien enviando simplemente el número de transacción (TrxID) al punto central (4) o introduciendo adicionalmente un identificador personal, en particular una contraseña personal TAN, ITAN, información biométrica, en particular una huella digital o similar.

22. Un método de acuerdo con cualquiera de las anteriores reivindicaciones, **caracterizado por que** el punto de aceptación (3) comunica indirectamente con el punto central (4), en particular por medio de uno o más agregadores, en particular un punto de recogida del distrito, un ordenador central en el supermercado o similar.

23. Un método de acuerdo con cualquiera de las anteriores reivindicaciones, **caracterizado por que** los abonados (2, 3, 4, 5) usan una variedad de medios de comunicación, en particular Ethernet, Internet, líneas terrestres, radio o teléfonos móviles y/o diferentes servicios/protocolos, en particular USSD, IP, SMS, GPRS.

24. Un método de acuerdo con cualquiera de las anteriores reivindicaciones, **caracterizado por que** cuando se autoriza la transacción el punto central (4) calcula una clave que es única y asignada permanentemente al usuario, en particular adicionalmente en el punto de aceptación, e informa al punto de aceptación de esta clave de modo que las transacciones previas del usuario puedan ser claramente asignadas al usuario.

25. Un método de acuerdo con cualquiera de las anteriores reivindicaciones, **caracterizado por que** el valor de la transacción, en particular la cantidad de dinero de la transacción es igual a 0 y de este modo se da acceso a una cuenta de usuario libre de cargas.

Figura 1

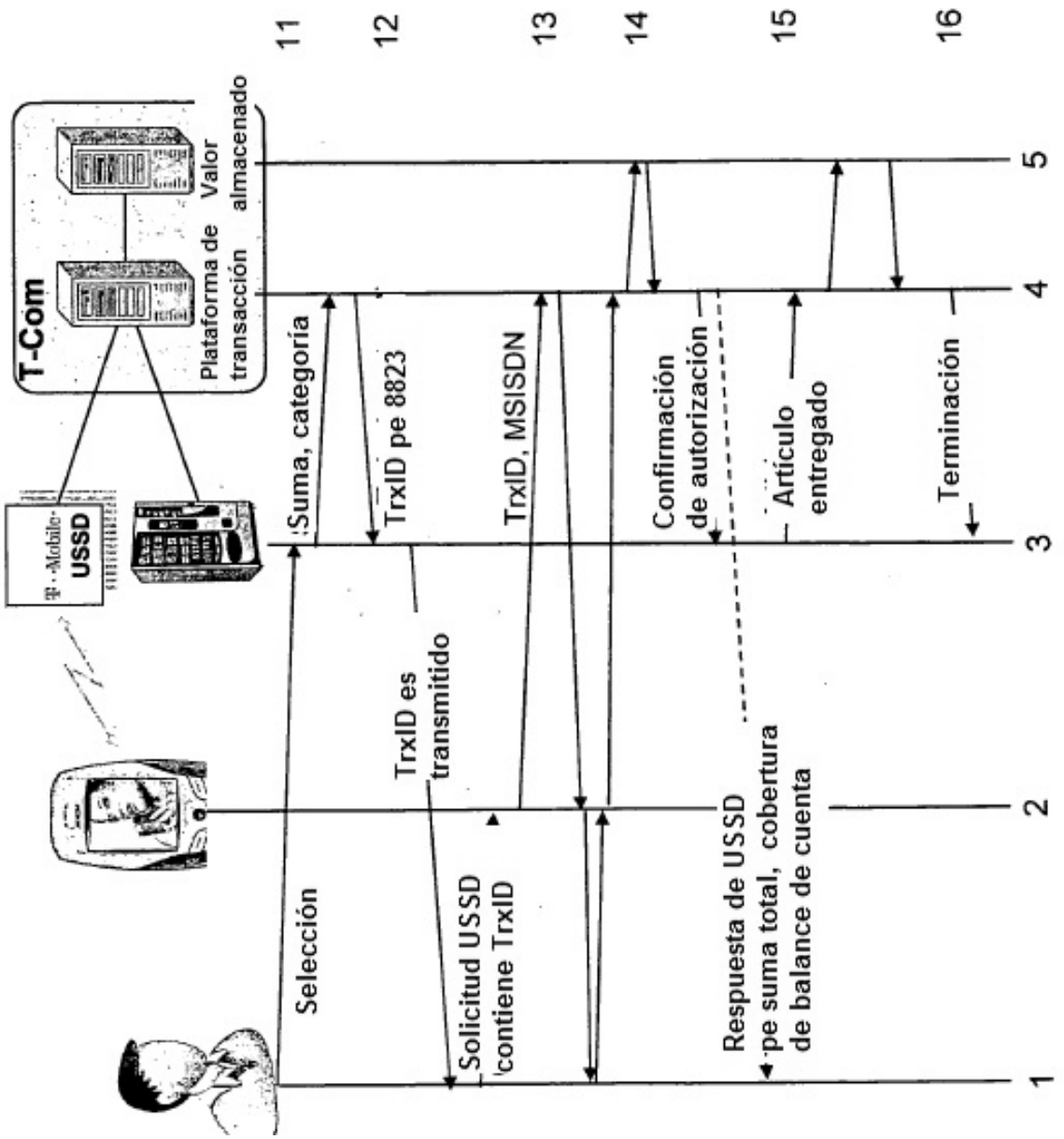

T-Com
Plataforma de transacción
Valor almacenado
T-Mobile
USSD
Selección
Solicitud USSD contiene TrxID
TrxID es transmitido
Suma, categoría
TrxID pe 8823
TrxID, MSISDN
Respuesta de USSD pe suma total, cobertura de balance de cuenta
Confirmación de autorización
Artículo entregado
Terminación
1
2
3
4
5
11
12
13
14
15
16

Figura 2

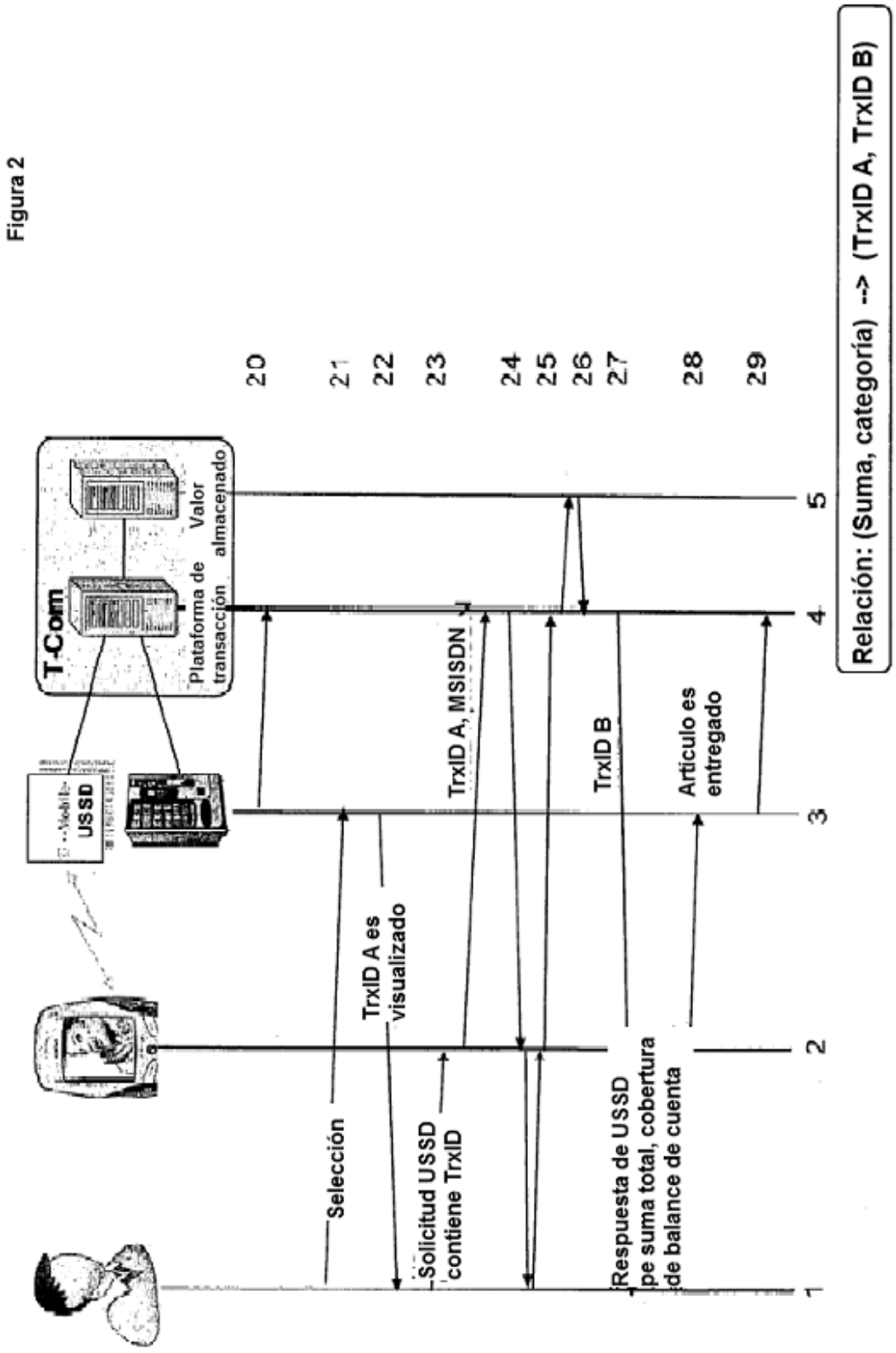

Relación: (Suma, categoría) --> (TrxID A, TrxID B)
T-Com
Plataforma de transacción
Valor almacenado
USSD
Selección
TrxID A es visualizado
Solicitud USSD contiene TrxID
TrxID A, MSISDN
TrxID B
Artículo es entregado
Respuesta de USSD pe suma total, cobertura de balance de cuenta
1
2
3
4
5
20
21
22
23
24
25
26
27
28
29

Figura 3

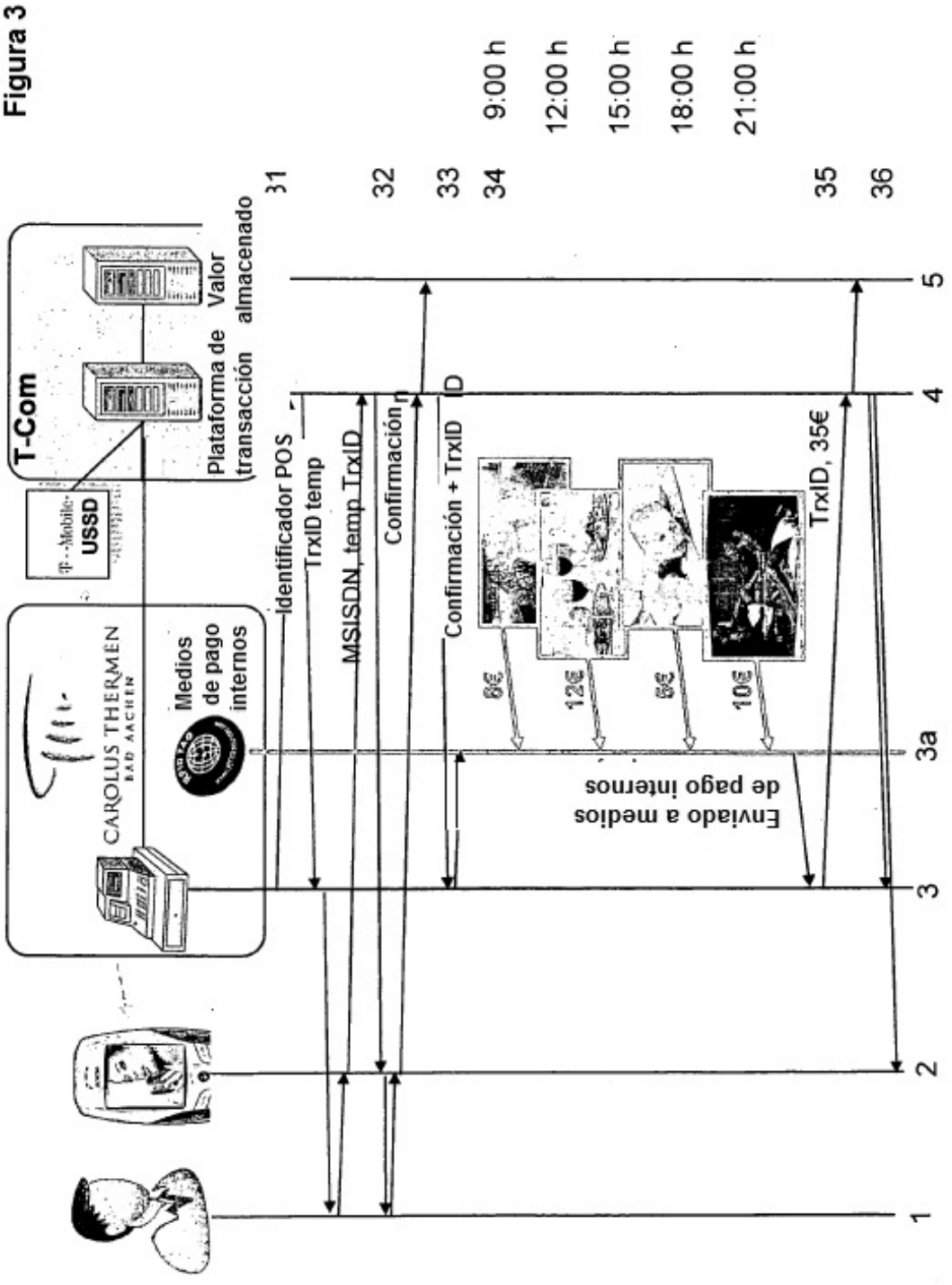

T-Com
Plataforma de transacción
Valor almacenado
T-Mobile
USSD
CAROLUS THERMEN
BAD AACHEN
Medios de pago internos
Identificador POS
TrxID temp
MSISDN, temp TrxID
Confirmación
Confirmación + TrxID
6€
12€
6€
10€
TrxID, 35€
Enviado a medios de pago internos
9:00 h
12:00 h
15:00 h
18:00 h
21:00 h
1
2
3
3a
4
5
31
32
33
34
35
36

Figura 4

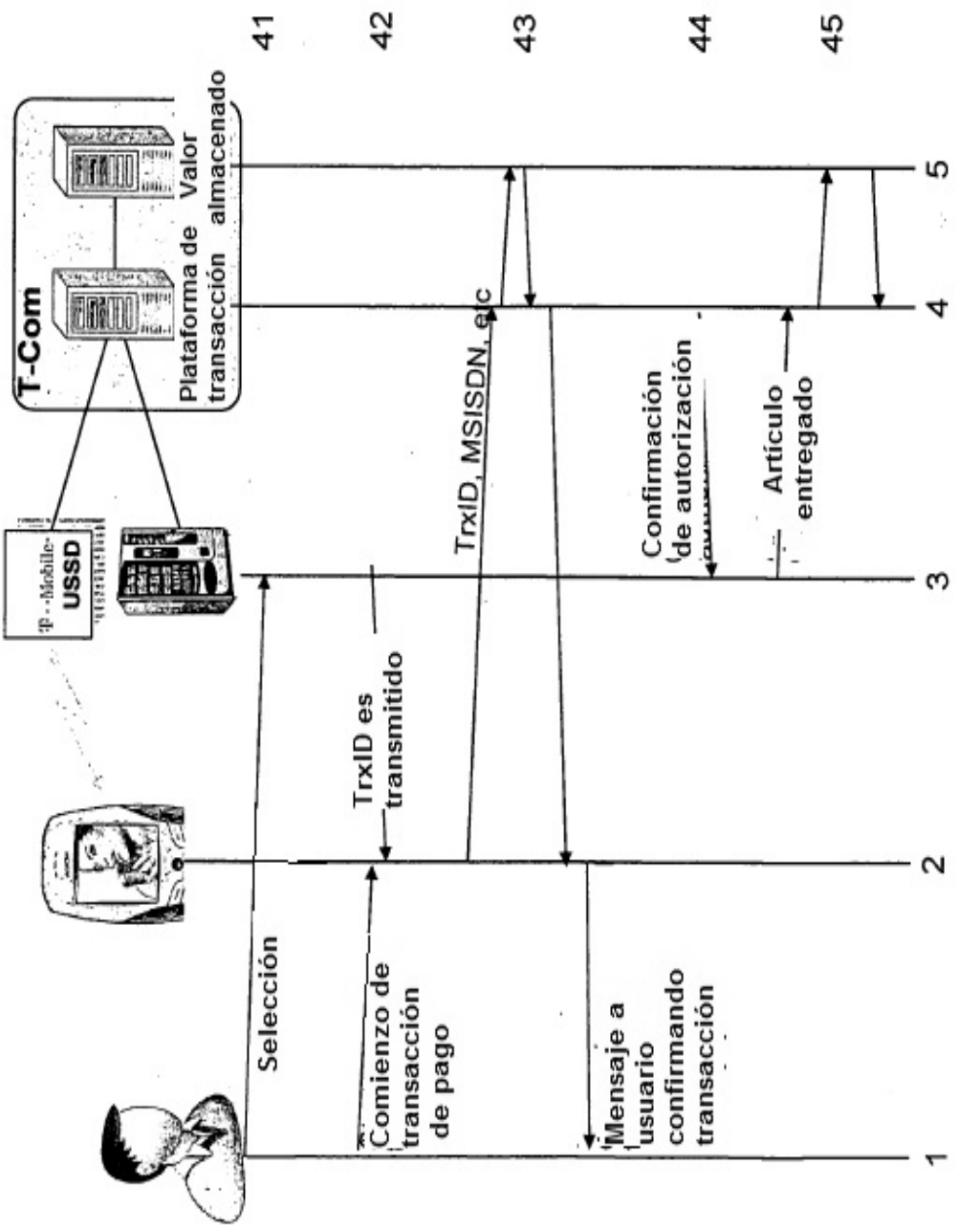
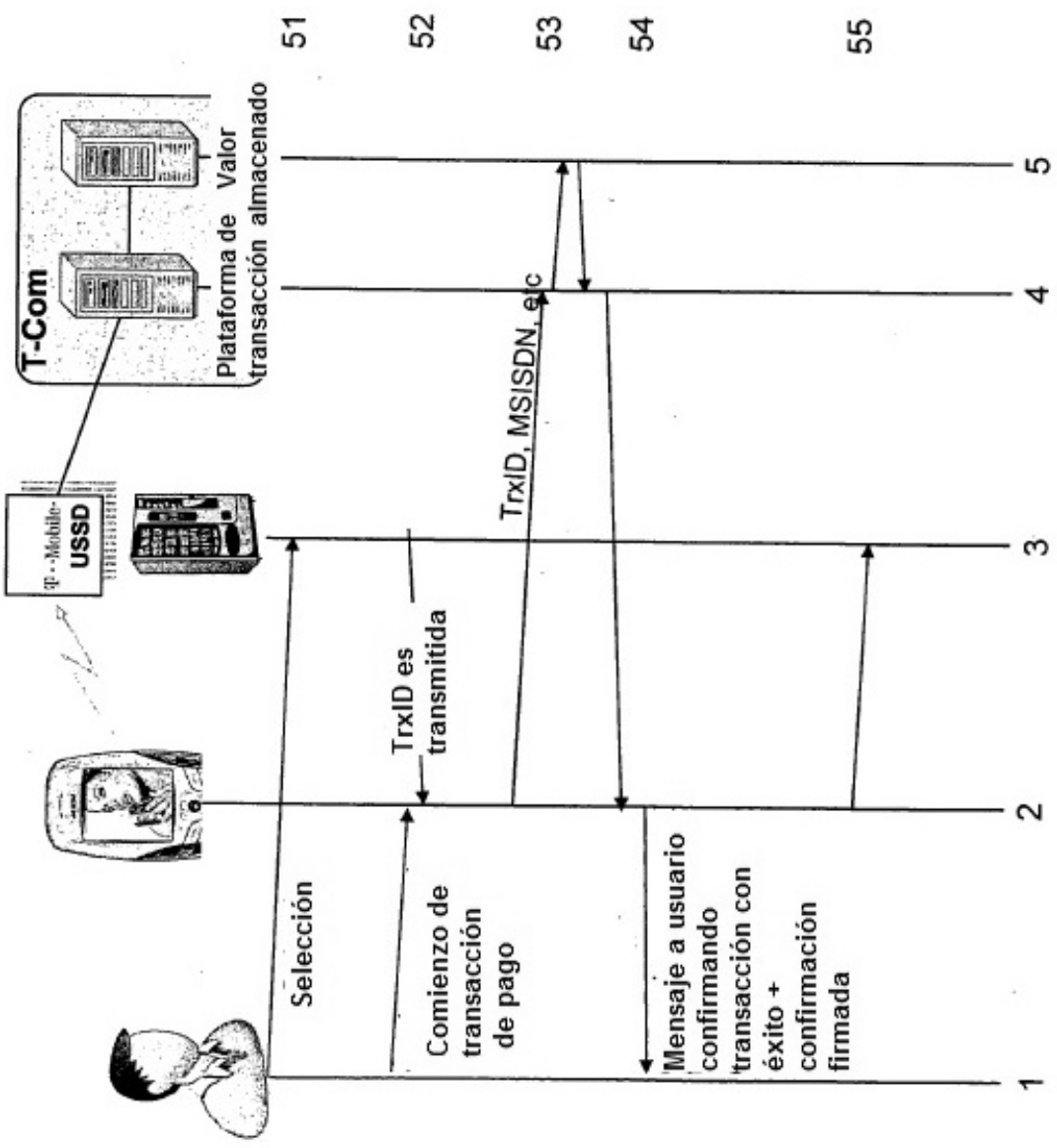

41
42
43
44
45
T-Com
Plataforma de transacción
Valor almacenado
USSD
Selección
Comienzo de transacción de pago
TrxID es transmitido
TrxID, MSISDN, etc
Confirmación de autorización
Artículo entregado
Mensaje a usuario confirmando transacción
1
2
3
4
5

Figura 5


T-Com
Plataforma de Valor transacción almacenado
USSD
Selección
Comienzo de transacción de pago
TrxID es transmitida
TrxID, MSISDN, etc
Mensaje a usuario confirmando transacción con éxito + confirmación firmada
51
52
53
54
55
1
2
3
4
5