(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 639 556**

(51) Int. CI.:

G06Q 20/38 (2012.01)
G06Q 40/02 (2012.01)
G06Q 30/06 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **15.10.2013 PCT/EP2013/071495**

(87) Fecha y número de publicación internacional: **22.05.2014 WO14075862**

(96) Fecha de presentación y número de la solicitud europea: **15.10.2013 E 13776812 (3)**

(97) Fecha y número de publicación de la concesión europea: **14.06.2017 EP 2920754**

(54) Título: **Procedimiento para la realización de transacciones**

(30) Prioridad:

14.11.2012 DE 102012220774

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
27.10.2017

(73) Titular/es:

GIESEN, HEINZ (100.0%)
Kettelerstrasse 24
48147 Münster, DE

(72) Inventor/es:

GIESEN, HEINZ

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Procedimiento para la realización de transacciones

La invención se refiere a un procedimiento para realizar transacciones entre un número de usuarios.

A partir del estado actual de la técnica, se conoce un elevado número de procedimientos para realizar transacciones, en particular para el sector financiero. Una debilidad frecuente de estos procedimientos es la posibilidad de manipulación de los datos limitadores de las transacciones, tales como conexiones bancarias de emisores y receptores de transferencias. Esto es particularmente problemático en el campo de la banca por Internet, debido a la accesibilidad del canal de las transacciones, por ejemplo, a través de ataques de intermediarios. Para evitar estos ataques, se ha introducido el uso de números de transacción específicos para cada transacción (procedimientos TAN), que sólo son conocidos por el emisor y por la entidad financiera y que deben transmitirse con cada orden de transacción. Este procedimiento ha sido mejorado, entre otras cosas, con el procedimiento iTAN, o con el chipTAN, en vista de su seguridad frente a manipulaciones, en particular el chipTAN que se caracteriza por un cambio de medios. En este caso, un cambio de medios significa la transición desde un medio, por ejemplo, Internet, a otro medio, por ejemplo, la detección visual de una imagen. Esto reduce la vulnerabilidad del procedimiento, ya que deberían ser atacados ambos medios para conseguir la manipulación del procedimiento.

Se conocen, por ejemplo, sistemas de pago y procedimientos correspondientes, así como sistemas para simplificar y autentificar transacciones, a partir de los documentos WO 02/19211 A1, EP 1 150 227 A1, WO 2004/036513 A1, así como del documento US 2012/0089519 A1.

El documento WO 2012/125531 A1 describe un sistema de pago móvil mediante la lectura de códigos QR.

Frente a ello, la invención se basa en la tarea de proporcionar un procedimiento mejorado para realizar transacciones.

Esta tarea en la que se basa la invención se consigue con las características de la reivindicación 1. Se proporcionan formas de realización de la invención en las reivindicaciones subordinadas.

Según una forma de realización de la invención, se proporciona un procedimiento para realizar transacciones entre un número de usuarios. A cada uno de los usuarios de una transacción se le asigna un alias único. La asignación de los alias a los usuarios respectivos se almacena en un servidor de autentificación. Además, los datos de la transacción de los usuarios se almacenan en el servidor de autentificación y se asignan unívocamente a los usuarios. Asimismo, se requiere un programa de aplicación y al menos un servidor de transacciones para realizar la operación.

Los datos de transacción en este caso son datos sin cuyo conocimiento no es posible realizar una transacción. En el caso de una transferencia, los datos de transacción serían, por ejemplo, las conexiones bancarias de los usuarios, en el caso de la transmisión de un mensaje, por ejemplo, direcciones de correo electrónico. Los datos de transacción permanecen iguales para una variedad de transacciones, por lo que pueden ser llamados datos maestros.

Un servidor de autentificación es, al igual que un servidor de transacciones, un equipo servidor. Este no tiene porqué representar necesariamente una entidad física, sino que también puede funcionar de manera completamente virtual, por ejemplo, como una unidad de computación remota en una red de ordenadores. Un servidor de autentificación está configurado de tal manera que los datos almacenados en el servidor de autentificación están protegidos contra el acceso de terceros y se proporcionan al servidor de transacciones sólo a petición de un servidor de transacciones.

En una primera etapa del procedimiento, el alias de un primer usuario es registrado por el programa de aplicación. La detección del alias se puede realizar, por ejemplo, mediante introducción manual o mediante lectura de una memoria de datos. En el ejemplo de una transacción financiera, el primer usuario sería el emisor o remitente. En una segunda etapa del procedimiento, el programa de aplicación detecta los alias de cualquier número de usuarios adicionales. La detección de los alias se realiza preferiblemente por un método sensorial, es decir, mediante la lectura de una tarjeta magnética o mediante la detección visual de un código de barras, de un código QR según la invención.

Utilizando el ejemplo de una transacción financiera, los usuarios adicionales citados serían los destinatarios de una transferencia. Una vez que el programa de aplicación ha recogido todos los usuarios implicados en la transacción, se notifican al programa de transacción los parámetros de la transacción. Utilizando de nuevo el ejemplo de una transacción financiera, los parámetros de la transacción serían la cantidad a transferir o el concepto de la transferencia. Por lo tanto, los parámetros de transacción pueden ser diferentes para cada transacción y se denominan datos del movimiento.

Después de que los alias de los usuarios, así como los parámetros de transacción, son adquiridos por el programa de aplicación, todo el registro de datos de transacción, que también contiene estos alias y los parámetros de transacción, se pasa a al menos un servidor de transacciones. El reenvío se puede realizar, por ejemplo, a través de Internet o de cualquier otro canal de comunicación. Tan pronto como el servidor de transacciones recibe un registro

de datos de transacción, extrae de éste los alias de los usuarios que intervienen y los notifica al servidor de autentificación. Dado que la asignación de los alias a los usuarios correspondientes se almacena en el servidor de autentificación, el servidor de autentificación está capacitado para identificar a cada usuario por su alias. Por lo tanto, el servidor de autentificación puede transmitir los datos de transacción al servidor de transacciones. Una vez que el servidor de transacciones ha recibido los datos de transacción de los usuarios, puede realizar o iniciar la transacción.

La forma de realización descrita resulta particularmente ventajosa, puesto que el registro de datos de transacción contiene únicamente los alias de los usuarios. Por lo tanto, no es posible manipular los datos de la transacción, tales como datos bancarios, en el registro de datos de transacción, salvo intercambiando completamente los alias. Sin embargo, esto supone que el posible atacante también está registrado en el servidor de autentificación. Esto hace que el atacante sea fácilmente identificable. Sólo los parámetros de transacción pueden ser manipulados, pero generalmente esto no causa ningún daño, ya que los participantes en la transacción pueden darse cuenta de ello y corregirlo. En el caso de una transacción financiera, por ejemplo, sólo se puede cambiar la cantidad a transferir entre los usuarios. No sería posible una desviación de la transacción de pago a una cuenta ajena sin revelar la identidad del atacante.

Según una forma de realización de la invención, a cada alias de usuario se le asigna una serie de datos. Para que se realice una transacción, primero deben almacenarse los datos de la transacción de cada usuario. Éstos se proporcionan, según se ha descrito más arriba, mediante una solicitud del servidor de autentificación al servidor de transacciones. Además de estos datos de transacción, se almacena información adicional que identifica de forma unívoca a un usuario. Esta puede ser, por ejemplo, nombre, dirección, lugar de nacimiento y fecha de nacimiento, número de identificación, o una combinación de estos datos. Además, se almacena una información unívoca del canal para cada usuario en el servidor de autentificación, que es adecuada para especificar un canal de comunicación entre el servidor de autentificación y el programa de aplicación. Esta puede ser, por ejemplo, una dirección de correo electrónico del usuario.

Los datos antes mencionados se pueden registrar, por ejemplo, en el caso de registro de un usuario en el servidor de autentificación, rellenando cada usuario un formulario con datos personales. Los datos proporcionados son posteriormente introducidos en el servidor de autentificación, o registrados por éste último. Los datos de los usuarios son conocidos únicamente por el servidor de autentificación y están protegidos contra el acceso de terceros. En el curso del registro, también se puede comprobar la identidad del usuario, por ejemplo, comprobando un documento de identificación.

Como se mencionó anteriormente, a cada usuario se le asigna un alias único. Según una forma de realización de la invención, el registro de datos cifrado de un usuario se define como un alias. La clave utilizada para el cifrado se almacena exclusivamente en el servidor de autentificación, de modo que el alias puede ser descifrado únicamente por el servidor de autentificación. No se tiene que almacenar necesariamente el registro completo de datos de cada usuario en el servidor de autentificación, sino sólo una asignación de alias y claves. Se puede utilizar un procedimiento cualquiera para el cifrado. Además, en este caso es posible cifrar el registro de datos de forma simétrica utilizando una libreta de un solo uso (One-Time-Pad), para que se pueda evitar el descifrado del alias sin el conocimiento de la clave. Dado que el cifrado y descifrado del alias se realiza en la misma entidad, no puede ocurrir la problemática que conduciría a una transmisión de la clave.

Según una forma de realización de la invención, el código QR del registro de datos cifrado del usuario previamente descrito se define como el alias del usuario. El uso del alias en forma de un código QR facilita la adquisición de los alias en el futuro, ya que un código QR se puede capturar visualmente con poco esfuerzo, por ejemplo, con la cámara de un teléfono inteligente o con la de una tableta.

Como se ha descrito anteriormente, es posible manipular los parámetros de transacción contenidos en un registro de transacción. Sin embargo, según una forma de realización de la invención, esto se puede evitar cifrando un registro de datos de transacción con el software de aplicación antes de la transferencia desde el software de aplicación al servidor de transacciones. Entonces, el registro de datos de transacción se descifra con el servidor de transacciones. A través de una elección adecuada del procedimiento de cifrado, la seguridad del procedimiento descrito anteriormente se puede adaptar a los respectivos requisitos de seguridad.

El tipo de cifrado y la clave utilizada se pueden definir específicamente para cada tipo de transacción o para cada transacción individual, según una forma de realización de la invención. En este caso, se pueden utilizar procedimientos de cifrado simétricos, asimétricos o también híbridos. Además, es posible cifrar sólo parcialmente un registro de datos de transacción. Por ejemplo, pueden protegerse parámetros de transacción críticos, tales como el importe de una transferencia o información confidencial, mientras que los parámetros de transacción no críticos, tales como un texto adjunto, no precisan ser cifrados.

Según una forma de realización de la invención, se realiza una transacción sólo si al menos una parte de los participantes en la transacción ha sido autentificada por el servidor de transacciones o por el servidor de autentificación. En este caso, la autentificación de los participantes se realiza preferiblemente solamente después de que se haya recibido un registro de datos de transacción en un servidor de transacciones. El hecho de que los

participantes en la transacción se hayan autentificado mediante un servidor de transacciones o un servidor de autentificación asegura, antes de realizarse la transacción, que los alias de los usuarios contenidos en el registro de datos de transacción no se han intercambiado. De esta manera, la sustitución de los alias se reconocería, a más tardar, durante la autentificación de los usuarios, según esta forma de realización.

Según una forma de realización de la invención, los usuarios son autentificados a través de programas de aplicación, en cada uno de los cuales están registrados los usuarios, con el uso adicional de una ventana de tiempo de validez para un registro de datos de transacción. En este caso, a cada usuario se le asigna preferentemente un programa de aplicación separado y la asignación de los programas de aplicación a los usuarios se almacena en el servidor de autentificación. Si se va a transferir un registro de datos de transacción a un servidor de transacciones, primero se establece un período de validez para este registro de datos de transacción. Entonces, el registro de transacción es procesado por un servidor de transacciones, solamente cuando el tiempo de procesamiento queda dentro del período de validez del registro de transacción. Para ello, el programa de aplicación inserta una marca de tiempo en el registro de datos de transacción. Esta documenta el momento en el que se ha creado el registro de datos de transacción.

Si un registro de datos de transacción es introducido a un servidor de transacciones, éste comprueba si la hora actual se encuentra dentro de la ventana del período de validez, teniendo en cuenta la marca de tiempo del registro de datos de transacción. Si este es el caso, se solicita una confirmación de la orden de transacción mediante el programa de aplicación o los programas de aplicación de los usuarios. Esta solicitud puede ser enviada tanto por el servidor de transacciones como por el servidor de autentificación. Una solicitud de confirmación puede ser, por ejemplo, que se abra una ventana emergente en el programa de aplicación de los usuarios, lanzada por el servidor de transacciones o por el servidor de autentificación, e informar al usuario de que se ha recibido una solicitud de transacción. Esta solicitud de transacción puede ser confirmada o rechazada. Una transacción no se ejecuta hasta que se hayan recibido todas las confirmaciones solicitadas.

En el caso de que el tiempo para el procesamiento de un registro de datos de transacción esté fuera de la ventana del período de validez, el registro de datos de transacción es rechazado por el servidor de transacciones. Esto evita la retención de los registros de datos de transacción para su procesamiento posterior. La autentificación de los usuarios también evita que se realice una transacción a un destinatario erróneo. Por ejemplo, el remitente puede esperar a su vez con la confirmación de la solicitud de transacción hasta que los destinatarios hayan recibido la solicitud de confirmación. Una vez recibida la solicitud de confirmación por los destinatarios, se asegura que los alias de los destinatarios no se han manipulado.

Según una forma de realización de la invención, el programa de aplicación, que detecta los alias y al que se notifican los parámetros de transacción, se registra con uno de los usuarios. Esto significa que su alias es conocido por el programa de aplicación y no tiene que ser recogido de nuevo para cada solicitud de transacción. Si se envía un registro de transacción desde este programa de aplicación, el alias del usuario al que se ha registrado el programa de aplicación se inserta automáticamente en el registro de transacción. Además, al registrar el programa de aplicación en el usuario, es posible una asignación unívoca del programa de aplicación a este usuario por el servidor de autentificación o también por el servidor de transacciones. Esto permite que los registros de datos de transacción, que son enviados al servidor de transacciones por el programa de aplicación registrado, se asignen unívocamente a un primer usuario. De esta manera se descarta una posibilidad de manipulación no deseada del alias del primer usuario. Además, según la forma de realización descrita a continuación, el registro de un programa de aplicación a un usuario también puede contener una asignación del programa de aplicación a un terminal. Esto permite impedir que se extraiga el programa de aplicación del terminal del usuario y que se utilice en otro dispositivo terminal contra la voluntad del usuario.

Según una forma de realización de la invención, el registro de un programa de aplicación en un usuario comprende las siguientes etapas:

Primero, el alias del usuario al que se va a registrar el programa de aplicación es detectado sensorialmente por el programa de aplicación. Esto se puede realizar durante la instalación del programa de aplicación o después. Posteriormente, el programa de aplicación determina un parámetro que identifica unívocamente el dispositivo terminal en el que está instalado el programa de aplicación. Éste puede ser, por ejemplo, el identificador global único (GUID) del dispositivo terminal, que normalmente se almacena en el hardware del dispositivo terminal. Posteriormente, el programa de aplicación notifica el alias del usuario al que se va a registrar el programa de aplicación, así como el parámetro que identifica unívocamente el dispositivo terminal en el servidor de autentificación. Sin embargo, antes de que estos datos se almacenen en el servidor de autentificación, primero debe comprobarse que el usuario que desea registrar un software de aplicación en un alias es realmente el usuario asignado a este alias en el servidor de autentificación. Para este fin, además de los datos ya mencionados, se notifica al servidor de autentificación la información de usuario que puede ser asignada unívocamente al usuario por el servidor de autentificación. Esto puede ser, por ejemplo, una pregunta de seguridad, información personal que está contenida en el registro del usuario o cualquier número generado cuando el usuario inicia una sesión en el servidor de autentificación y es conocido únicamente por el usuario y por el servidor de autentificación. Tras la recepción de una solicitud de registro en el servidor de autentificación, éste comprueba si la información de usuario transmitida está contenida en el registro de datos del usuario al que está asignado el alias. Si este es el caso, al

registro de datos del usuario se añade adicionalmente información sobre el terminal en el que se ha registrado un programa de aplicación.

Según una forma de realización de la invención, se presenta un sistema que incluye al menos un servidor de transacciones y un servidor de autentificación. En este caso, un servidor de transacciones está adaptado para leer registros de datos de transacciones que contienen parámetros de transacciones y alias de usuarios, y para ejecutar y/o iniciar la transacción correspondiente. El servidor de autentificación contiene registros de los usuarios en el procedimiento, conteniendo los registros la siguiente información:

- el alias de un usuario,

- datos que identifiquen unívocamente al usuario,

- datos de transacción del usuario;

En el que el servidor de autentificación, a petición del servidor de transacciones, proporciona los datos relevantes para la transacción pertenecientes a un alias contenido en el registro de datos de transacción, al servidor de transacciones.

Según una forma de realización de la invención, el sistema descrito anteriormente incluye además un dispositivo terminal de usuario, en el que está instalado un programa de aplicación, que permite la implementación del procedimiento descrito anteriormente.

Según una realización de la invención, el servidor de autentificación del sistema descrito anteriormente está adaptado para asignar al usuario, unívocamente, el terminal en el que está instalado el programa de aplicación.

Según una realización de la invención, se presenta un producto de programa informático, que está adaptado para realizar las etapas del procedimiento descritas anteriormente.

Las formas de realización de la invención se explicarán con más detalle con referencia a los dibujos. Se muestran:

- la figura 1, un diagrama de flujo de una secuencia de procedimientos según la invención,

- la figura 2, un diagrama de flujo de una secuencia de procedimientos según la invención con un programa de aplicación registrado,

- la figura 3, un diagrama de flujo de una secuencia de procedimientos según la invención, con la etapa adicional de autentificación de los usuarios,

- la figura 4, un diagrama de flujo de una secuencia de procedimientos según la invención con un programa registrado y con autentificación de los usuarios,

- la figura 5, un diagrama de flujo de una secuencia de procedimientos según la invención para registrar un programa de aplicación en un usuario,

- la figura 6, un diagrama de bloques de un sistema que permite realizar un procedimiento según la invención.

A continuación, los elementos de las realizaciones posteriores que se corresponden o son idénticos entre sí se identifican, cada uno, con los mismos símbolos de referencia.

La figura 1 muestra un diagrama de flujo de una forma de realización del procedimiento según la invención. La viabilidad del procedimiento presupone, al menos, la presencia de un servidor de transacciones, un servidor de autentificación, un número de usuarios y un programa de aplicación. A cada usuario se le asigna un alias exclusivo, en el que la asignación de los alias a los usuarios se almacena en el servidor de autentificación. Además, los datos de transacción se asignan a los usuarios en el servidor de autentificación. Los datos de transacción de un usuario pueden, por ejemplo, ser sus datos bancarios o similares.

En una primera etapa 101, se registran los alias de los usuarios que están implicados en la transacción. Los alias son detectados por el programa de aplicación, por ejemplo, leyendo una memoria en la que se almacenan los alias o detectando visualmente un código de barras que contiene los alias. Después de que se hayan registrado los alias de los usuarios, los parámetros de transacción son registrados por el programa de aplicación 102. Los parámetros de transacción pueden ser, por ejemplo, una cantidad monetaria que se transfiere entre dos usuarios o un mensaje a transmitir.

La combinación de alias y parámetros de transacciones representa un registro de datos de la transacción. En la siguiente etapa 103, éste es transmitido por el programa de aplicación a un servidor de transacciones. Sin embargo, el servidor de transacciones no puede asignar los alias a los usuarios. Por lo tanto, en una cuarta etapa 104, los

alias, que están contenidos en el registro de datos de la transacción, son notificados al servidor de autentificación por el servidor de transacciones. A su vez, el servidor de autentificación puede asignar los alias que han sido notificados por el servidor de transacciones a los usuarios correspondientes 105 sobre la base de la asignación de usuarios y alias almacenados en el mismo. Dado que los datos de la transacción también se almacenan para cada usuario, éstos pueden ser notificados por el servidor de autentificación al servidor de transacciones 106, de manera que el servidor de transacciones pueda iniciar o ejecutar una transacción de acuerdo con el registro de datos de la transacción obtenido previamente 107.

La figura 2 muestra un diagrama de flujo de una forma de realización del procedimiento según la invención, extendiéndose el procedimiento mediante el registro del programa de aplicación que envía el registro de datos de la transacción a uno de los usuarios. En el curso del registro del programa del identificador global único (GUID) del dispositivo terminal en el que está instalado el programa de aplicación, el registro de datos del usuario que registra el programa de aplicación se asigna en el servidor de autentificación.

Dado que el programa de aplicación está registrado con uno de los usuarios, su alias es conocido por el programa de aplicación. Por lo tanto, en la primera etapa 201, sólo los alias de los usuarios adicionales son registrados por el programa de aplicación. El alias del primer usuario, que ha sido registrado por el programa de aplicación, es añadido a la base de datos por el programa de aplicación. En la segunda etapa 202, además de los parámetros de la transacción, el identificador global único (GUID) del dispositivo terminal es registrado por el programa de aplicación. En la tercera etapa 203, el registro de datos de transacción, que ha sido extendido mediante el GUID del dispositivo terminal utilizado respecto a la forma de la realización mostrada en la figura 1, es transmitido por el programa de aplicación al servidor de transacciones.

Análogamente al procedimiento anteriormente descrito, el servidor de transacciones extrae los alias de los usuarios del registro de datos de transacción y los notifica al servidor de autentificación. Además de los alias, el GUID, que está contenido en el registro de datos de la transacción, se notifica al servidor de autentificación. Entonces, el servidor de autentificación comprueba si el GUID obtenido está contenido en el registro de datos del primer usuario 205. Si este no es el caso, finaliza el procedimiento 206. Sin embargo, si la asignación del GUID corresponde al alias del usuario, las etapas del procedimiento 105-107 se realizan análogamente al procedimiento mostrado en la figura 1.

El uso de un programa de aplicación registrado impide una manipulación inadvertida del alias del primer usuario. Una vez manipulado el alias del primer usuario, la asignación del alias al GUID notificado no coincide con la información del servidor de autentificación, por lo que el procedimiento se interrumpe inmediatamente.

La figura 3 muestra un diagrama de flujo de una forma de realización del procedimiento según la invención, extendiéndose el procedimiento mediante la autentificación de los usuarios. La autentificación requiere que los participantes en el proceso ejecuten un programa de aplicación, que está registrado con ellos.

Las etapas de procedimiento 101-104 son idénticas a las de la figura 1. Después de que el servidor de autentificación haya recibido los alias contenidos en el registro de datos de la transacción del servidor de transacciones, se envía una solicitud de autentificación a los usuarios 305. Es necesario que cada usuario tenga un programa de aplicación registrado. El servidor de autentificación también debe tener la capacidad de comunicarse con los programas de aplicación de los usuarios.

Con fines de autentificación, por ejemplo, se puede enviar una solicitud al programa de aplicación de los usuarios, que debe ser confirmada manualmente por los usuarios. La solicitud puede contener, por ejemplo, la información de entre quiénes se va a realizar una transacción y qué parámetros de la transacción han sido notificados.

Si la solicitud de autentificación 306 no es confirmada por al menos un usuario, finaliza el procedimiento 307. Sin embargo, si todos los usuarios confirman la solicitud de autentificación, el procedimiento continúa de acuerdo con las etapas 105-107 descritas anteriormente.

En la etapa adicional de la solicitud de autentificación, por ejemplo, un primer usuario que desea realizar una transacción con los usuarios adicionales puede esperar con la confirmación de la solicitud de autentificación hasta que sepa que todos los demás usuarios también han realizado la solicitud de autentificación. Esto puede implementarse, por ejemplo, de modo que el primer usuario llama a los usuarios adicionales y pregunta si se ha recibido una solicitud de autentificación correspondiente a la transacción prevista. Si éste es el caso, se evita que la transacción que se va a realizar sea redirigida a otras personas.

La figura 4 es un diagrama de flujo de una forma de realización del procedimiento según la invención, extendiéndose el procedimiento mediante las etapas adicionales de registrar un programa de aplicación y solicitar autentificación.

Las etapas de procedimiento 201-204 son análogas a las de la figura 2. Una vez que el GUID contenido en el registro de datos de la transacción puede asignarse unívocamente al alias del primer usuario, se envía una solicitud de autentificación a los otros usuarios a través del servidor de autentificación o del de transacciones 305. Sólo después de la autentificación satisfactoria de los otros usuarios se realizan las etapas del procedimiento 105-107, de acuerdo con las descripciones de la figura 1.

Las consultas de seguridad 204 y 305 también se pueden intercambiar en su secuencia. En general, mediante esta forma de implementación del procedimiento, la identidad del primer usuario está asegurada mediante el registro, mientras que la identidad de los otros usuarios está asegurada debido a la solicitud de autentificación. Por lo tanto, se evita una manipulación no deseada de los alias de los usuarios de la transacción.

En las figuras 1 a 4, no se han tenido en cuenta ni el cifrado de un registro de datos de transacción por el programa de aplicación ni el descifrado posterior por el servidor de transacciones, para ofrecer una visión más clara.

La figura 5 es un diagrama de flujo de un procedimiento según la invención para registrar un programa de aplicación en un usuario.

En una primera etapa 501, el programa de aplicación se instala en el terminal del usuario. El terminal puede ser, por ejemplo, un teléfono inteligente, un ordenador personal, una tableta o similar. En una segunda etapa 502, el alias del usuario, que desea registrar el programa de aplicación, es registrado por el programa de aplicación. Los alias se pueden introducir alternativamente durante la instalación del programa de aplicación o después. La detección del alias mismo puede efectuarse, por ejemplo, leyendo un código de barras o leyendo un medio de almacenamiento. El alias del usuario es almacenado por el programa de aplicación después de su adquisición. Posteriormente, la aplicación identifica el identificador global único del dispositivo terminal 503. Este se almacena, usualmente, en el hardware del dispositivo terminal. Después de que se han registrado el alias y el GUID, éstos se notifican al servidor de autentificación 504. El servidor de autentificación identifica al usuario por medio de su alias después de la introducción del alias y del GUID, y pide una información de usuario adicional del usuario a través de un canal de comunicación, especificado durante el registro, mediante un canal de información desde 504. El canal de comunicación correspondiente se puede definir, por ejemplo, mediante una dirección de correo electrónico.

Una información de usuario puede ser, por ejemplo, la fecha de nacimiento, la dirección, el número de identificación del usuario o similar. En este caso, es necesario que la información de usuario haya sido almacenada inicialmente en el registro de datos del usuario cuando el usuario se conecta al servidor de autentificación, y puede ser asignada al usuario por el servidor de autentificación. Después de que se ha recibido la información de usuario, el servidor de autentificación comprueba si la información de usuario transmitida está contenida en el registro de datos que está asignado al alias en el servidor de autentificación 506. Si este es el caso, se asigna el GUID del dispositivo terminal en el que se instaló el programa de aplicación 507, al registro de datos del alias. Si la información de usuario no está contenida en el registro de datos del alias, se descarta el registro y se descarta el registro 508.

El registro del programa de aplicación en un usuario permite al servidor de autentificación enviar una solicitud de autentificación a este programa de aplicación. De acuerdo con lo anterior, esto contribuye a la seguridad del procedimiento. Además, el registro del programa de aplicación mejora la facilidad de uso, ya que el alias del usuario al que está registrado el programa de aplicación no tiene que volver a introducirse en cada transacción, sino que es agregado automáticamente por el programa de aplicación al registro de transacciones.

La figura 6 muestra un sistema 600 que permite realizar un procedimiento según una forma de realización de la invención. Con este propósito, son necesarios esencialmente un servidor de autentificación 610, un servidor de transacciones 620, así como el dispositivo terminal de un usuario 630.

El servidor de autentificación 610 contiene una base de datos 611, en la que se almacenan al menos la asignación de alias a usuarios, así como los datos de transacción de los usuarios. En el caso de que, según la realización anterior, el alias de un usuario sea el registro cifrado de datos de éste, el servidor de autentificación comprende además medios para cifrar y descifrar 612 registros de datos de los usuarios.

Estos pueden ser, por ejemplo, un procesador con almacenamiento de datos asociado, conteniendo el almacén de datos un código de programa ejecutable por un procesador que contiene instrucciones ejecutables por ordenador que están adaptadas para cifrar y descifrar un registro de datos de acuerdo con un procedimiento de cifrado específico.

El servidor de transacciones 620 incluye medios para iniciar una transacción 621, que puede ser, por ejemplo, una conexión de comunicaciones con un banco en el caso de una transacción financiera. En el caso de que los registros de datos de transacciones sean cifrados por el programa de aplicación para mejorar la seguridad del procedimiento, el servidor de transacciones 620 comprende además medios para descifrar 622 los registros de datos de transacciones que pueden ejecutarse análogamente a 612.

El terminal de un usuario 630 contiene una base de datos 631, en la que el alias del usuario se almacena, por ejemplo, después del registro de un programa de aplicación. Además, el dispositivo terminal de un usuario 630 contiene una cadena de números o caracteres que identifica unívocamente el dispositivo terminal 632, por ejemplo, el GUID del dispositivo terminal. En el caso de que los registros de datos de transacción se transmitan cifrados al servidor de transacciones, el dispositivo terminal de usuario también contiene medios para cifrar registros de datos 633, que se pueden ejecutar análogamente a 612. Además, el dispositivo terminal 630 incluye el programa de aplicación 634 que se requiere para realizar las transacciones. Esto permite acceder al GUID 632, a la base de datos 631, así como a los medios de cifrado 633. Además, el dispositivo terminal 630 contiene un sensor 635, con el que se pueden detectar alias de usuarios. Este sensor está acoplado operativamente al programa de aplicación para

que el programa de aplicación pueda recibir información del sensor.

Hay canales de comunicación entre el dispositivo terminal 630 y el servidor de autentificación 610, que pueden usarse para autentificar un usuario 604 y para registrar un programa de aplicación en un usuario 605.

Además, existe un canal de comunicación entre el dispositivo terminal 630 y el servidor de transacciones 620, a través del cual se notifican los registros de datos de transacciones 603 desde el dispositivo terminal al servidor de transacciones. Dado que el servidor de transacciones 620 no puede procesar inicialmente alias, existe también un enlace de comunicación entre el servidor de transacciones 620 y el servidor de autentificación 610, a través del cual el servidor de transacciones 620 puede solicitar datos de usuarios 601, tras lo cual el servidor de autentificación 610 puede proporcionar datos 602 correspondientes al servidor de transacciones 620.

El procedimiento de acuerdo con la figura 4 se explica a continuación con referencia al sistema 600. Se supone que el programa de aplicación está registrado en uno de los usuarios. Por razones de claridad, sólo se utiliza un servidor de transacciones. Además, sólo se muestra un dispositivo terminal de usuario, que debe representar, de manera representativa, una pluralidad de dispositivos terminales de usuarios.

En primer lugar, los alias de los usuarios de la transacción son detectados por el sensor 635 y notificados al programa de aplicación 634. Además, los parámetros de transacción son registrados por el programa de aplicación 634 y es registrado el GUID 632 del dispositivo terminal 630. El alias del primer usuario contenido en la base de datos 631 también es leído por el programa de aplicación 634 y añadido al registro de datos de transacción. El registro de datos así creado, que contiene el alias del primer usuario, los alias de los demás usuarios, el GUID del dispositivo terminal, así como los parámetros de la transacción, está a partir de ese momento cifrado 633. El registro de datos de la transacción cifrado se notifica ahora a través del canal de comunicación 603 al servidor de transacciones 620. Este realiza el descifrado 622 del registro de datos de la transacción. Posteriormente, el servidor de transacciones extrae del registro de datos de la transacción los alias de los usuarios, así como el GUID del dispositivo terminal, en el que se creó el registro de datos de la transacción a partir del registro de datos de la transacción. Los datos de la transacción que forman parte de los alias son ahora consultados 601 desde el servidor de transacciones 620 al servidor de autentificación 610. El GUID extraído previamente también se notifica al servidor de autentificación. El servidor de autentificación 610 comprueba ahora si el GUID recibido está almacenado en el registro de datos del primer usuario. Si no es así, el procedimiento finaliza, porque se debe suponer que el programa de aplicación se utiliza contra la voluntad del primer usuario, por ejemplo, debido a una extracción del programa de aplicación desde el terminal del primer usuario. Sin embargo, si el GUID recibido corresponde al GUID que está contenido en el registro de datos del primer usuario, se envía una solicitud de autentificación 604 a los dispositivos terminales 630 de los demás usuarios. Si la solicitud de autentificación no es confirmada por al menos un usuario, el procedimiento finaliza porque debe suponerse que el alias del usuario ha sido manipulado. Sin embargo, si la solicitud de autentificación es confirmada por todos los usuarios, el servidor de autentificación asigna los usuarios correspondientes con los datos de la transacción respectivos por los alias y notifica los datos de la transacción de los usuarios 602 al servidor de transacciones 620. Este último realiza ahora la transacción a través de 621 utilizando los parámetros de la transacción previamente realizados o iniciados.

Lista de símbolos de referencia

601 Solicitud de datos

602 Suministro de datos

603 Notificación de un registro de transacción

604 Autentificación

605 Registro

610 Servidor de autentificación

611 Base de datos

612 Cifrado y descifrado

620 Servidor de transacciones

621 Inicio de una transacción

622 Descifrado

630 Dispositivo terminal de usuario

631 Base de datos

632 GUID

633 Cifrado

634 Programa de aplicación

635 Sensor

REIVINDICACIONES

1. Procedimiento para la realización de transacciones entre un número de usuarios, en el que se asigna un alias unívoco a cada uno de los usuarios, en el que el alias incluye los datos de la transacción cifrados del usuario, en el que los datos de la transacción de un usuario son datos limitadores de la transacción, sin cuyo conocimiento no se puede realizar una transacción y que permanecen iguales para cada transacción del usuario, en el que se asigna un alias a un usuario, así como la clave necesaria para descifrar los datos de la transacción como un registro de datos de usuario almacenado en un servidor de autentificación (610), que comprende la provisión de un programa de aplicación (634) instalado en un dispositivo terminal (630) de un primer usuario y al menos un servidor de transacciones (620), en el que el programa de aplicación (634) está registrado (605) en el primer usuario, para que su alias sea conocido por el programa de aplicación (634), en el que el parámetro (632) que identifica unívocamente el dispositivo terminal (630) del primer usuario está contenido en el registro de datos de usuario del primer usuario, en el que el programa de aplicación puede determinar el parámetro (632) que identifica unívocamente el dispositivo terminal (630) del primer usuario, en el que el procedimiento comprende las etapas de:

- detección óptica de un código QR que contiene el alias de un segundo usuario mediante el programa de aplicación (634),

- registro de los parámetros de la transacción mediante el programa de aplicación (634),

- notificación (603) de los alias de los usuarios primero y segundo, de los parámetros de la transacción y de los parámetros (632) para identificar unívocamente el dispositivo terminal (630) desde el programa de aplicación (634) a uno de los servidores de transacciones (620) a través de Internet,

- notificación (601) de los alias y de los parámetros (632) para identificar unívocamente el dispositivo terminal (630) desde el al menos un servidor de transacciones (620) al servidor de autentificación (610),

- identificación de los usuarios sobre la base de los alias desde el servidor de autentificación (610),

- comprobación de si el parámetro (632), que identifica unívocamente el dispositivo terminal (630), está contenido en el registro de datos de usuario del primer usuario,

- si el parámetro (632) que identifica unívocamente el dispositivo terminal (630) está contenido en el registro de datos del primer usuario, descifrado de los datos de la transacción contenidos en el alias del usuario,

- notificación (602) de los datos de la transacción de los usuarios al al menos un servidor de transacciones (620) desde el servidor de autentificación (610),

- realización de la transacción entre el primer usuario y el al menos un usuario adicional sobre la base de los parámetros de la transacción mediante el al menos un servidor de transacciones (620).

2. Procedimiento según la reivindicación 1, en el que los parámetros de transacción son datos que pueden ser diferentes para cada transacción del usuario y no limitan la transacción.

3. Procedimiento según una de las reivindicaciones precedentes, en el que el parámetro que identifica unívocamente un dispositivo terminal es un parámetro que se almacena en el hardware del dispositivo terminal.

4. Procedimiento según una de las reivindicaciones precedentes, en el que se asignan al alias del primero y/o segundo de los usuarios los siguientes datos:

- información que identifique unívocamente al usuario,

- información de canal asignada unívocamente al usuario para especificar un canal de comunicación entre el servidor de autentificación (610) y el programa de aplicación (634),

- datos de transacción del usuario,

en el que los datos con el alias asociado se almacenan en el servidor de autentificación (610).

5. Procedimiento según una de las reivindicaciones precedentes, en el que al menos una parte del registro de datos de la transacción (603), que contiene los alias de los usuarios y los parámetros de la transacción, es cifrada por el programa de aplicación (634) antes de la notificación desde el programa de aplicación (634) al al menos un servidor de transacciones (620), y es descifrada de nuevo por el al menos un servidor de transacciones (620) después de recibir el registro de datos de la transacción (603).

6. Procedimiento según la reivindicación 5, en el que cada tipo de transacción y/o cada transacción en sí misma tiene asignado un procedimiento de cifrado y/o la clave utilizada para cifrar el registro de datos de la transacción (603).

7. Procedimiento según una de las reivindicaciones precedentes, en el que una transacción se realiza únicamente si el al menos un usuario adicional y/o todos los demás usuarios adicionales participantes, después de recibir el registro de datos de la transacción (603) en un servidor de transacciones (620), son autentificados (604) por un servidor de transacciones (620) y/o por un servidor de autentificación (610).

8. Procedimiento según la reivindicación 7, en el que cada usuario tiene al menos un programa de aplicación (634) registrado en el usuario respectivo, en el que la autentificación (604) del al menos un usuario adicional comprende las siguientes etapas:

- establecimiento de una ventana de tiempo de validez para un registro de datos de la transacción (603),

- inserción de una marca de tiempo en el registro de datos de la transacción (603) mediante el programa de aplicación (634),

- comprobación, por medio del servidor de transacciones (620), de si la recepción y/o el procesamiento del registro de datos de la transacción (603) en el servidor de transacciones (620) queda dentro de la ventana de tiempo de validez del registro de datos de la transacción (603),

- en este caso: solicitud de confirmación de la orden de transacción mediante el programa de aplicación (634) del al menos un usuario adicional,

- de lo contrario, cancelación del registro de datos de transacción (603).

9. Procedimiento según una de las reivindicaciones precedentes, en el que el registro (605) del programa de aplicación (634) en un usuario comprende las siguientes etapas:

- detección sensorial del alias del usuario mediante el programa de aplicación (634),

- determinación de un parámetro (632) que identifica unívocamente el dispositivo terminal (630) en el que está instalado el programa de aplicación (634),

- notificación al servidor de autentificación (610) del alias del usuario y del parámetro (632) que identifica unívocamente el terminal (630),

- notificación al servidor de autentificación (610) de la información de usuario que puede ser asignada unívocamente al usuario desde el servidor de autentificación (610),

- comprobación por el servidor de autentificación (610), de si la información a asignar al usuario está contenida en el registro de datos al que está asignado el alias del usuario.

10. Sistema para realizar transacciones entre un número de usuarios, incluyendo el sistema al menos un servidor de transacciones (620), un servidor de autentificación (610) y un dispositivo terminal (630) de un primer usuario,

en el que se asigna un alias unívoco a cada uno de los usuarios, en el que el alias incluye los datos de la transacción cifrados del usuario, en el que los datos de la transacción de un usuario son datos que limitan la transacción, sin el conocimiento de los cuales no se puede realizar una transacción y que permanecen iguales para cada transacción del usuario, en el que la asignación de un alias a un usuario, así como la clave necesaria para descifrar los datos de la transacción se almacenan como un registro de datos de usuario en el servidor de autentificación (610),

en el que un programa de aplicación (634) está instalado en el terminal (630) del primer usuario, estando registrado (605) el programa de aplicación (634) en el primer usuario, de manera que su alias sea conocido por el programa de aplicación (634), en el que un parámetro (632) que identifica unívocamente el terminal (630) del primer usuario está contenido en el registro de datos de usuario del primer usuario, en el que el programa de aplicación es capaz de determinar el parámetro (632) que identifica unívocamente el dispositivo terminal (630) del primer usuario,

en el que el programa de aplicación (634) instalado en el dispositivo terminal (630) del primer usuario está configurado para:

- detectar ópticamente un código QR que contiene el alias de un segundo usuario,

- registrar los parámetros de la transacción, y

- notificar a través de Internet los alias del primer y del segundo usuario, los parámetros de la transacción y el parámetro (632) que identifica unívocamente el dispositivo terminal (630), al servidor de transacciones (620),

en el que el servidor de transacciones (620) está configurado para transmitir los alias y el parámetro que identifica unívocamente el dispositivo terminal (630) al servidor de autentificación (610),

en el que el servidor de autentificación está configurado para:

- identificar a los usuarios en base a los alias,

- comprobar si el parámetro (632) para identificar unívocamente el dispositivo terminal (630) está contenido en el registro de datos de usuario del primer usuario,

- si el parámetro (632) para identificar unívocamente el terminal (630) está contenido en el registro de datos del primer usuario, para descifrar los datos de transacción contenidos en los alias de los usuarios, y

- notificar los datos de la transacción de los usuarios al al menos un servidor de transacciones (620),

en el que el servidor de transacciones (620) está configurado además para realizar la transacción entre el primer usuario y el al menos un usuario adicional en base a los parámetros de la transacción.

11. Producto de programa informático, que está adaptado para realizar las etapas del procedimiento descritas anteriormente de una de las reivindicaciones 1-9.

FIGURA 1

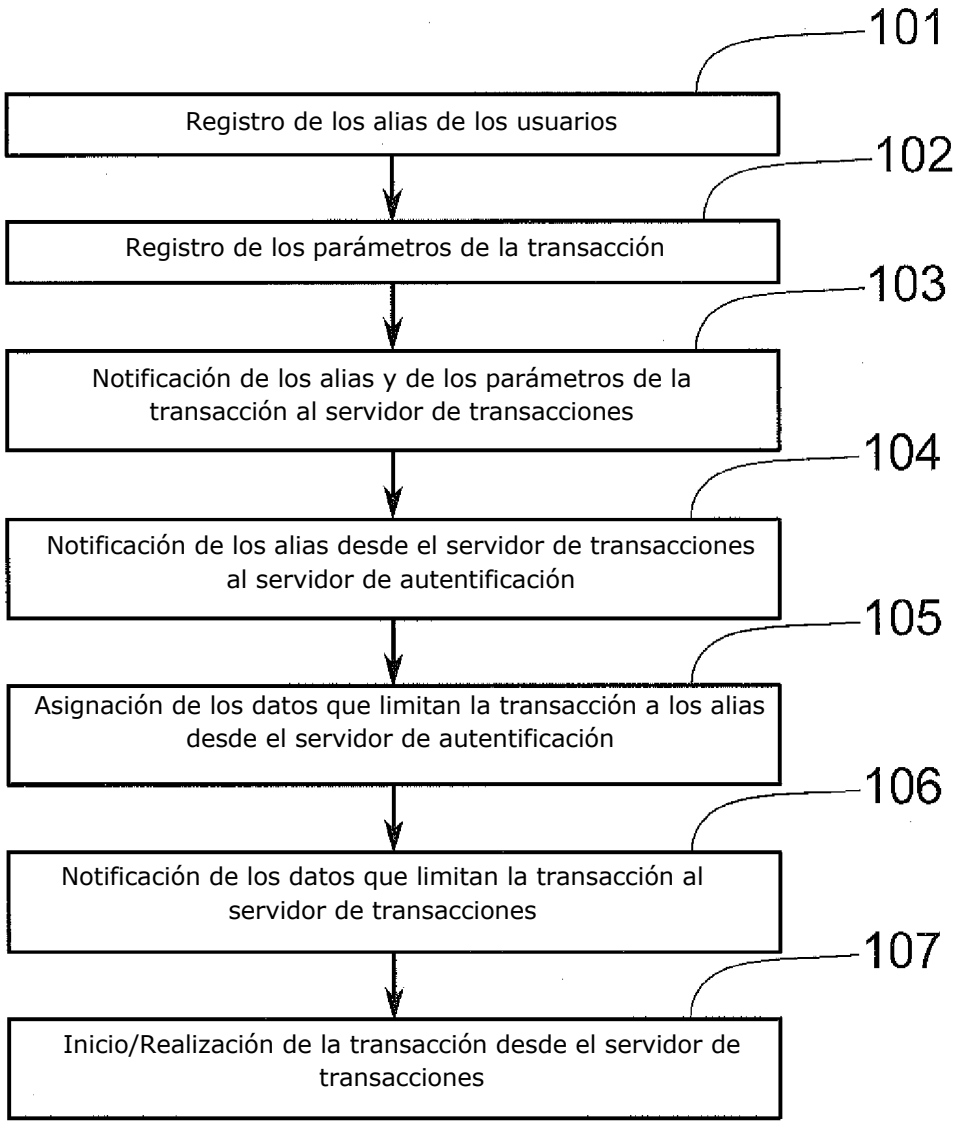

101
Registro de los alias de los usuarios
102
Registro de los parámetros de la transacción
103
Notificación de los alias y de los parámetros de la transacción al servidor de transacciones
104
Notificación de los alias desde el servidor de transacciones al servidor de autentificación
105
Asignación de los datos que limitan la transacción a los alias desde el servidor de autentificación
106
Notificación de los datos que limitan la transacción al servidor de transacciones
107
Inicio/Realización de la transacción desde el servidor de transacciones

FIGURA 2

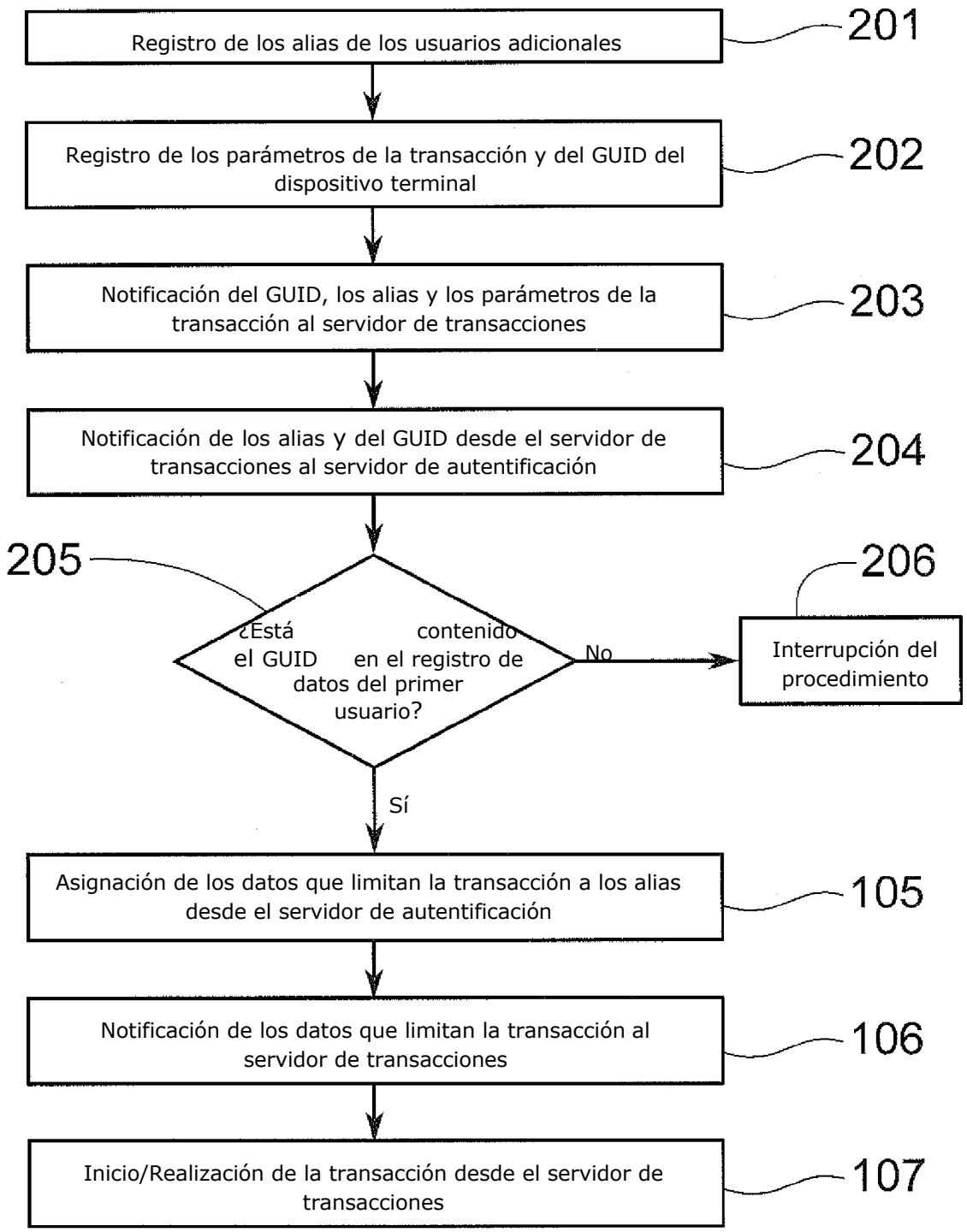

Registro de los alias de los usuarios adicionales
201
Registro de los parámetros de la transacción y del GUID del dispositivo terminal
202
Notificación del GUID, los alias y los parámetros de la transacción al servidor de transacciones
203
Notificación de los alias y del GUID desde el servidor de transacciones al servidor de autentificación
204
205
¿Está contenido el GUID en el registro de datos del primer usuario?
No
206
Interrupción del procedimiento
Sí
Asignación de los datos que limitan la transacción a los alias desde el servidor de autentificación
105
Notificación de los datos que limitan la transacción al servidor de transacciones
106
Inicio/Realización de la transacción desde el servidor de transacciones
107

FIGURA 3

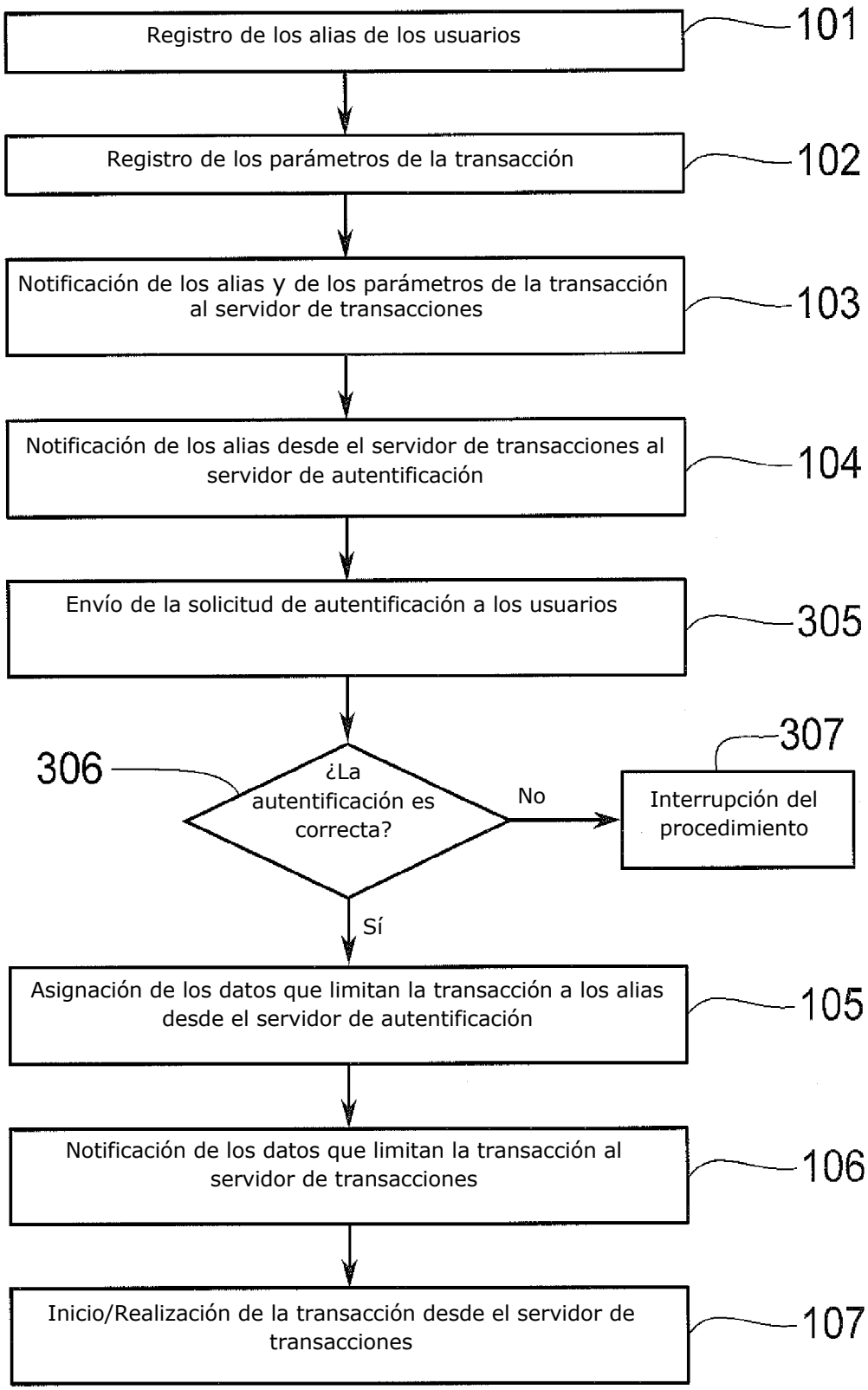

Registro de los alias de los usuarios
101
Registro de los parámetros de la transacción
102
Notificación de los alias y de los parámetros de la transacción al servidor de transacciones
103
Notificación de los alias desde el servidor de transacciones al servidor de autentificación
104
Envío de la solicitud de autentificación a los usuarios
305
306
¿La autentificación es correcta?
No
307
Interrupción del procedimiento
Sí
Asignación de los datos que limitan la transacción a los alias desde el servidor de autentificación
105
Notificación de los datos que limitan la transacción al servidor de transacciones
106
Inicio/Realización de la transacción desde el servidor de transacciones
107

FIGURA 4

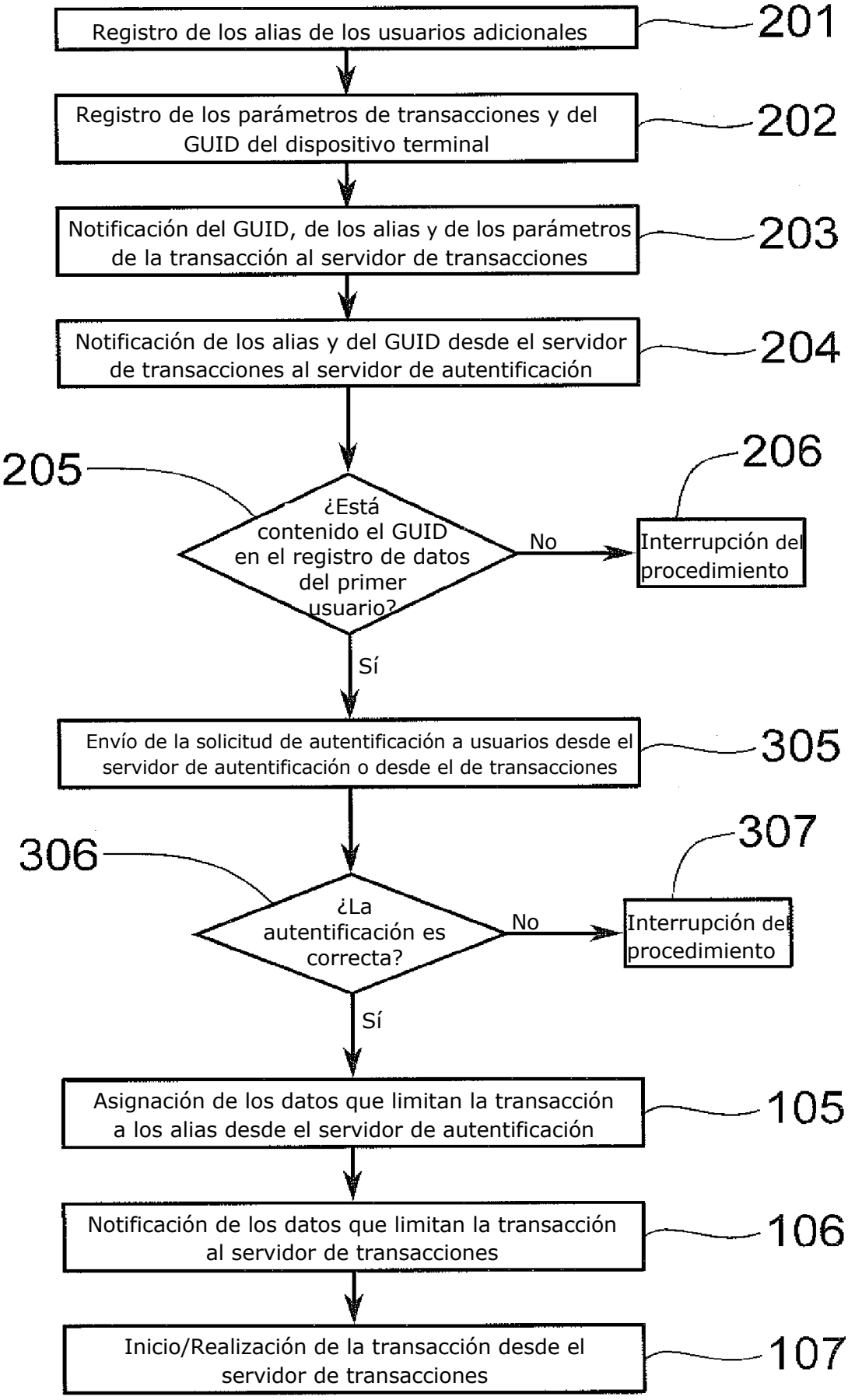

Registro de los alias de los usuarios adicionales
201
Registro de los parámetros de transacciones y del GUID del dispositivo terminal
202
Notificación del GUID, de los alias y de los parámetros de la transacción al servidor de transacciones
203
Notificación de los alias y del GUID desde el servidor de transacciones al servidor de autentificación
204
205
¿Está contenido el GUID en el registro de datos del primer usuario?
No
206
Interrupción del procedimiento
Sí
Envío de la solicitud de autentificación a usuarios desde el servidor de autentificación o desde el de transacciones
305
306
¿La autentificación es correcta?
No
307
Interrupción del procedimiento
Sí
Asignación de los datos que limitan la transacción a los alias desde el servidor de autentificación
105
Notificación de los datos que limitan la transacción al servidor de transacciones
106
Inicio/Realización de la transacción desde el servidor de transacciones
107

FIGURA 5

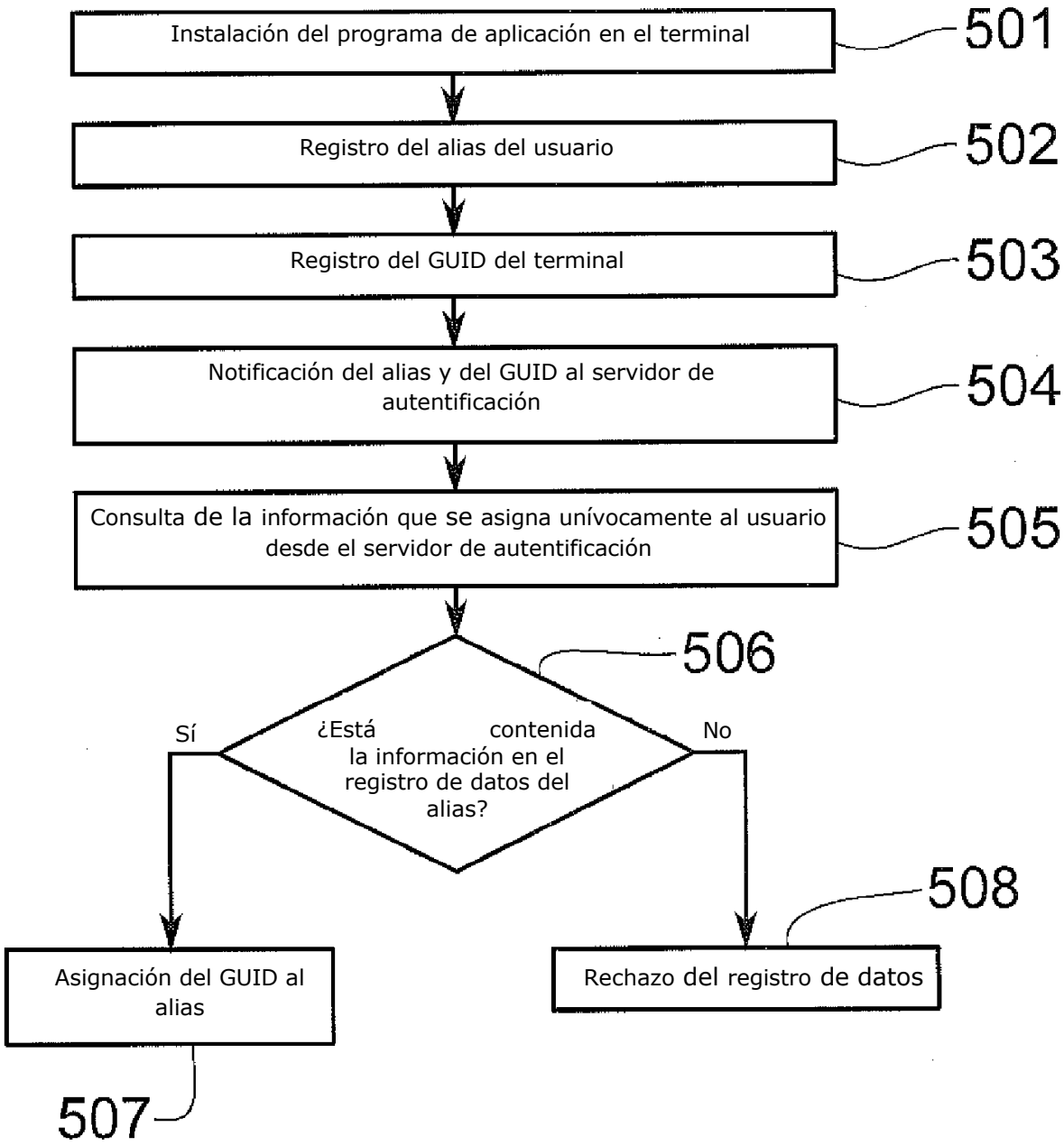
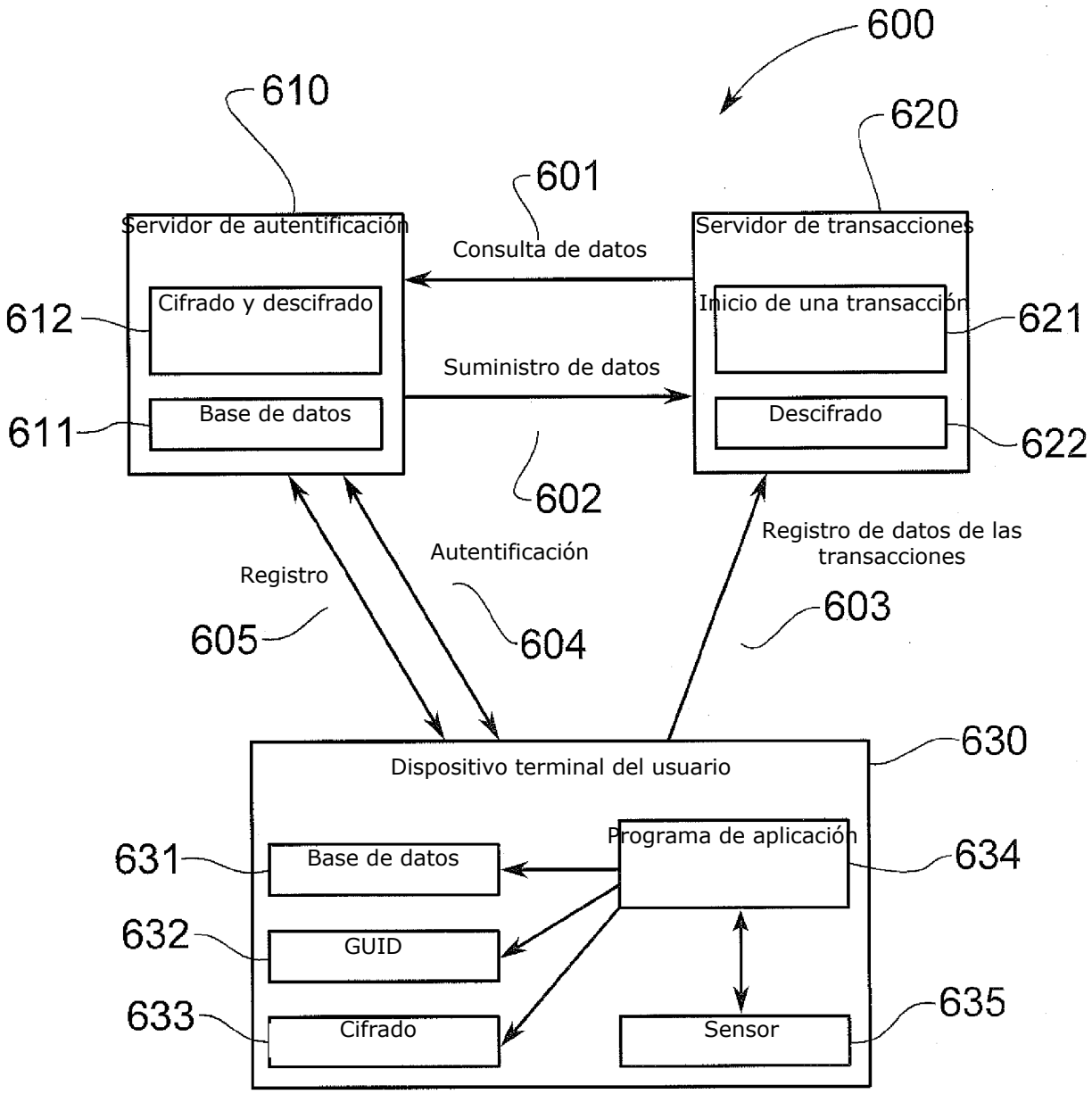

Instalación del programa de aplicación en el terminal
501
Registro del alias del usuario
502
Registro del GUID del terminal
503
Notificación del alias y del GUID al servidor de autentificación
504
Consulta de la información que se asigna unívocamente al usuario desde el servidor de autentificación
505
506
¿Está contenida la información en el registro de datos del alias?
Sí
No
Asignación del GUID al alias
507
Rechazo del registro de datos
508

FIGURA 6


600
610
620
601
Servidor de autentificación
Consulta de datos
Servidor de transacciones
612
Cifrado y descifrado
Inicio de una transacción
621
Suministro de datos
611
Base de datos
Descifrado
622
602
Registro de datos de las transacciones
Autentificación
Registro
603
605
604
630
Dispositivo terminal del usuario
Programa de aplicación
631
Base de datos
634
632
GUID
633
Cifrado
Sensor
635