(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 646 443**

(51) Int. CI.:

G06F 21/42 (2013.01)
G06F 21/60 (2013.01)
H04L 29/06 (2006.01)
G06Q 30/00 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **17.07.2012 PCT/EP2012/003008**

(87) Fecha y número de publicación internacional: **24.01.2013 WO13010665**

(96) Fecha de presentación y número de la solicitud europea: **17.07.2012 E 12740493 (7)**

(97) Fecha y número de publicación de la concesión europea: **06.09.2017 EP 2735129**

(54) Título: **Procedimiento para asegurar una transacción**

(30) Prioridad:

19.07.2011 DE 102011108069

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
13.12.2017

(73) Titular/es:

GIESECKE+DEVRIENT MOBILE SECURITY GMBH (100.0%)
Prinzregentenstrasse 159
81677 München , DE

(72) Inventor/es:

WEISS, DIETER y
BALDISCHWEILER, MICHAEL

(74) Agente/Representante:

DURAN-CORRETJER, S.L.P

DESCRIPCIÓN

Procedimiento para asegurar una transacción

La invención se refiere a un procedimiento, un producto de programa informático, un dispositivo terminal de comunicación, así como a un sistema para asegurar una transacción, en particular una transacción de pago entre un dispositivo terminal de comunicación y una instancia de servidor.

Los dispositivos terminales de comunicación son utilizados cada vez con mayor frecuencia en forma de un teléfono móvil, teléfono inteligente o asistente digital personal, abreviado PDA, con función de teléfono móvil para realizar transacciones como, por ejemplo, transacciones bancarias, transacciones de pago, consulta de contenidos de datos y similares. Para ello, el dispositivo terminal de comunicación se encuentra en comunicación de datos con una instancia de servidor.

Por instancia de servidor se entiende en esta solicitud una instancia localmente remota del dispositivo terminal de comunicación. Éste es el caso, por ejemplo, de instancias de servidor de hardware o software que ponen a disposición y ofrecen prestaciones y servicios. En el sentido de la solicitud, el término instancia de servidor comprende en particular un servicio electrónico, también denominado tienda online o tienda web. Por servicio electrónico se entiende todo servicio y actividad creado por ordenador y que se realiza y ofrece interactivamente a través de medios electrónicos como internet.

Un servicio electrónico pone a disposición, por ejemplo, artículos y productos digitales en internet. El servicio electrónico comprende un software con una funcionalidad de cesta de compra virtual. El comprador selecciona el producto deseado mediante su dispositivo terminal de comunicación. Éste es colocado en una cesta de compra virtual e identificado para el pago. Para llevar a cabo este servicio electrónico existe una tienda física que realmente se encarga del pedido correspondiente del usuario.

Todos estos servicios electrónicos requieren una transacción entre la instancia de servidor y el dispositivo terminal de comunicación. Esta transacción es o bien una transacción de pago, una transacción de identificación, una transacción de autentificación o similar. En este contexto, por transacción se entiende en particular una secuencia de pasos que puede considerarse una unidad lógica. En el curso de la transacción y con fines de identificación y autentificación, un usuario introduce frecuentemente datos de entrada críticos para la seguridad o confidenciales a través de un dispositivo de entrada como, por ejemplo, un teclado, en el dispositivo terminal del usuario. A continuación, estos datos de entrada son enviados a través de la red de comunicación de datos como datos relevantes para la transacción a la instancia de servidor. En el paso siguiente, la instancia de servidor libera el servicio o el producto, lo que debe entenderse a continuación como autorización de la transacción.

Principalmente existe el problema de que tanto los dispositivos terminales de comunicación móviles equipados con teclado y pantalla, personales o públicos, como, por ejemplo, los teléfonos inteligentes, móviles o similares, al igual que la red de comunicación de datos, generalmente son inseguros y por tanto vulnerables a software malicioso. Como software malicioso se conocen, por ejemplo, virus, gusanos, troyanos, programas espía o similares, que interceptan los datos relevantes para la transacción o incluso pueden manipularlos de forma que, en lugar de la transacción objetivo del usuario del dispositivo terminal, se realiza una transacción no deseada a favor de un tercero no autorizado, sin que el usuario, el dispositivo terminal de comunicación o la instancia del servidor puedan reconocerlo. Cuando una transacción de este tipo es manipulada se pueden producir daños considerables para el operador de la instancia de servidor y también para el usuario que paga.

Ante este problema, en el documento EP 1 260 077 B1 se describe un procedimiento con el cual el usuario de un dispositivo terminal de comunicación móvil confirma una transacción. Para ello se incluye en el sistema de transacción un servidor de autentificación que es utilizado para asegurar la transacción al enviar el dispositivo terminal automáticamente una oferta del proveedor de servicios al servidor de autentificación como confirmación de la transacción. Esto puede ser desventajoso porque en el teléfono móvil puede haberse instalado previamente un software malicioso que manipule la confirmación de la transacción de forma correspondiente. Además, el sistema se vuelve más complejo debido al servidor adicional de autentificación, por lo que se generan costes adicionales.

Para asegurar las transacciones a través de una red de comunicación de datos, desde hace algún tiempo se utilizan los denominados entornos de ejecución seguros, también denominados Trusted Execution Environment® o TrustZone®. Estos entornos de ejecución seguros se utilizan para ejecutar aplicaciones críticas para la seguridad en un entorno aislado y protegido contra la manipulación.

Las soluciones conocidas hasta el momento requieren por parte de las instancias de servidor modificaciones en su operación en internet para integrar el entorno de ejecución seguro en el desarrollo de transacciones. Estas modificaciones comprenden en particular la puesta a disposición de software y/o módulos de hardware adicionales o de servidores de certificación más complejos. Estas modificaciones a veces están vinculadas a costes considerables, razón por la cual las transacciones que utilizan entornos de ejecución seguros aún no están muy extendidas en la actualidad.

El documento US 6 092 202 A del estado de la técnica da a conocer un procedimiento para asegurar una transacción, en particular una transacción de pago entre un dispositivo terminal de comunicación (ordenador) y una instancia de servidor (servidor) (columna 1, líneas 20-32), comprendiendo el dispositivo terminal de comunicación un procesador con un entorno de ejecución no seguro (traditional computing environment 102, columna 7, líneas 31-32) y un entorno de ejecución seguro (security-coprocessor, columna 3, líneas 10-13, secure computing environment 104, columna 7, líneas 29-31). Mediante el entorno de ejecución seguro, en el procedimiento se extraen datos relevantes para la transacción de, por ejemplo, una tarjeta de chip, que son enviados a través de un canal interno al entorno de ejecución no seguro para ser reenviados desde allí para la autorización de la transacción.

El documento US 2003/223586 A1 del estado de la técnica da a conocer un ordenador con un entorno de ejecución no seguro de un procesador normal (D2, página 2, [0023], general purpose processor 203) y un entorno de ejecución seguro de un procesador de seguridad (D2, página 1, [0006], líneas 1-2; página 2, [0024], security processor 213).

La invención tiene por tanto el objetivo de simplificar las transacciones entre dispositivos terminales de comunicación e instancias de servidor. No obstante, también se deben proporcionar unas medidas elevadas de seguridad ante manipulación y en particular no debe ser necesaria ninguna adaptación de la infraestructura dentro del sistema de transacción.

El objetivo de la invención se consigue mediante las medidas descritas en las reivindicaciones independientes secundarias. En las correspondientes reivindicaciones dependientes se describen realizaciones ventajosas.

El objetivo se consigue en particular mediante un procedimiento para asegurar una transacción, en particular una transacción de pago, entre un dispositivo terminal de comunicación y una instancia de servidor. El dispositivo terminal de comunicación comprende un procesador con un entorno de ejecución no seguro y un entorno de ejecución seguro. Para el procedimiento, en primer lugar se establece un primer canal de comunicación entre el dispositivo terminal de comunicación y la instancia de servidor. Para terminar, se envían los datos relevantes para la transacción del dispositivo terminal de comunicación a la instancia de servidor a través del primer canal de comunicación. El procedimiento según la invención se caracteriza por que, antes del paso de envío, se establece un segundo canal de comunicación entre la aplicación de navegador en el entorno de ejecución no seguro y una aplicación de transacción en el entorno de ejecución seguro y al menos una parte de los datos introducidos relevantes para la transacción es enviada a través del segundo canal de comunicación a la aplicación de transacción. Antes del paso de envío, la aplicación de transacción genera una información de confirmación a partir de la parte recibida de los datos relevantes para la transacción. Esta información de confirmación es utilizada para la autorización de la transacción. El término autorización de la transacción se refiere en particular a un aviso de la instancia de banco a la instancia de servidor.

Los datos relevantes para la transacción son preferentemente datos de transacción bancaria, en particular número de cuenta, código bancario, número de tarjeta de crédito, fecha de vencimiento de tarjeta de crédito, nombre del titular de la tarjeta de crédito, código de comprobación de la tarjeta de crédito, conexiones bancarias, importe de transferencia y similares. Estos datos relevantes para la transacción son solicitados por la instancia de servidor e introducidos por el usuario en el dispositivo terminal de comunicación y/o generados por la aplicación de transacción o leídos desde un área de almacenamiento seguro del entorno de ejecución seguro.

La instancia de banco es una instancia que recibe los datos relevantes para la transacción de la instancia de servidor y los compara con la información de confirmación. Tras la comparación, la instancia de banco genera un mensaje para la instancia de servidor con el resultado de la comparación. A consecuencia de ello, la instancia de servidor puede decidir si pone a disposición del usuario el servicio o el artículo correspondiente a la transacción.

La instancia de banco es, por ejemplo, una entidad de crédito que ofrece servicios retribuidos para operaciones/transacciones de pago, crédito y capital.

Además, estos datos relevantes para la transacción pueden ser datos críticos para la seguridad o confidenciales, o datos que son solicitados por la instancia de servidor para realizar la transacción, por ejemplo, números de identificación personal (PIN), números de transacción (TAN) u otros datos de transacción, como importe o número de pedido de un producto.

Por comunicación entre dispositivo terminal e instancia de servidor se entiende en este contexto una transmisión de señal caracterizada por el modelo de emisor-receptor. La información es codificada en caracteres y transferida de un emisor a un receptor a través de un canal de comunicación.

El primer canal de comunicación es en particular una red de telefonía móvil. Por red de telefonía móvil se entiende en este contexto una infraestructura técnica en la que tiene lugar la transmisión de señales para la telefonía móvil. En esta definición debe entenderse comprendida esencialmente la red de conmutación móvil, en la que tiene lugar la transmisión y conmutación de las señales entre dispositivos fijos y plataformas de la red de telefonía móvil, así como la red de acceso (también denominada interfaz aérea), en la que tiene lugar la transferencia de señales entre una

antena de telefonía móvil y un dispositivo terminal móvil. Por ejemplo, el "Global System for Mobile Communications", abreviado GSM, como representante de la denominada segunda generación, o el “General Packet Radio Service”, abreviado GPRS, y el “Universal Mobile Telecommunications System”, abreviado UMTS, como representantes de la denominada tercera generación de redes de telefonía móvil, se mencionan aquí a modo de ejemplo, estando ampliada la red de conmutación móvil de la tercera generación con la capacidad de una transferencia de datos orientada a paquetes, manteniéndose no obstante la red de radio invariable.

Para realizar una transacción se envían datos relevantes para la transacción desde el dispositivo de comunicación a la instancia de servidor.

Los datos relevantes para la transacción pueden ser en particular la fecha, el importe, un número de transacción que referencia inequívocamente la transacción u otro dato similar. Estos datos relevantes para la transacción pueden haber sido puestos a disposición por la instancia de servidor al menos parcialmente a través del primer canal de comunicación. Estos datos relevantes para la transacción son enviados antes del paso de envío al menos parcialmente a través del segundo canal de comunicación a la aplicación de transacción.

En una realización alternativa según la invención, al menos una parte de los datos relevantes para la transacción son puestos a disposición y/o generados por la aplicación de transacción.

En una realización preferente según la invención, los datos relevantes para la transacción pueden ser introducidos por el usuario en una aplicación de navegador en el entorno de ejecución no seguro, siendo enviada al menos una parte relevante para la transacción de los datos introducidos a través del segundo canal de comunicación a la aplicación de transacción antes del paso de envío. Para ello, el usuario introduce en particular el nombre de usuario, el número de tarjeta de crédito, el periodo de validez de la tarjeta de crédito, el código de comprobación CVV de la tarjeta de crédito y/o la empresa emisora de la tarjeta de crédito.

Para enviar los datos relevantes para la transacción a la instancia de servidor está prevista una aplicación de navegador. Puesto que la aplicación de navegador fue iniciada dentro del entorno de ejecución no seguro, la aplicación de navegador corre riesgo de manipulación por lo que los datos relevantes para la transacción deben ser, en cierta forma, supervisados y confirmados. Para ello se establece el segundo canal de comunicación al entorno de ejecución seguro, los datos relevantes para la transacción son puestos a disposición, al menos parcialmente, del entorno de ejecución seguro y se genera una información de confirmación dentro de un entorno protegido contra la manipulación.

La aplicación de navegador presenta en particular un módulo de extensión, un denominado complemento (plug-in) de navegador. Este módulo de extensión establece el segundo canal de comunicación entre la aplicación de navegador en el entorno de ejecución no seguro y la aplicación de transacción en el entorno de ejecución seguro, de forma que la aplicación de transacción en el entorno de ejecución seguro recibe, dado el caso complementa o comprueba, la parte relevante para la transacción de los datos introducidos con el fin de asegurar la transacción. El segundo canal de comunicación discurre exclusivamente dentro del procesador. El módulo de extensión supervisa la entrada en el entorno de ejecución no seguro y pone estos datos a disposición del entorno de ejecución seguro. El TEE presenta, de acuerdo con los requisitos, un módulo a nivel de la capa de protocolo que puede traspasar datos del entorno de ejecución no seguro al entorno de ejecución seguro. Un módulo de este tipo se diferencia del módulo de extensión, ya que el módulo de extensión consiste en una extensión de la propia aplicación de navegador, es decir, un módulo a nivel de la capa de aplicación.

Para asegurar la transacción, la aplicación de transacción accede a un elemento de entrada del dispositivo terminal de comunicación en el entorno de ejecución seguro. El envío de los datos relevantes para la transacción a la instancia de servidor tiene lugar sólo tras una entrada de confirmación del usuario, protegida contra la manipulación.

En una realización preferente, la aplicación de transacción comprueba en el entorno de ejecución seguro los datos introducidos relevantes para la transacción, en particular en relación a la consistencia con los datos almacenados en el entorno de ejecución seguro. Estos datos almacenados pueden estar almacenados en un área de almacenamiento seguro o también dentro de un elemento de seguridad, estando conectado el elemento de seguridad con el entorno de ejecución seguro para la comunicación de datos. Esta comunicación puede ser alámbrica o inalámbrica. El elemento de seguridad puede ser un soporte de almacenamiento de datos portátil con la correspondiente funcionalidad de seguridad como, por ejemplo, una tarjeta inteligente, tarjeta de chip, token, tarjeta de almacenamiento masivo, tarjeta multimedia o módulo de identificación de suscripción, abreviado SIM, o alternativamente un soporte de almacenamiento de datos de identificación como, por ejemplo, un pasaporte o documento de identidad electrónico con datos de identificación del usuario almacenados en un chip y legibles mediante máquinas. El elemento de seguridad está configurado en particular como componente de hardware e instalado como componente integrado de forma fija en el dispositivo terminal móvil, no siendo posible extraerlo del dispositivo terminal móvil en esa forma, por ejemplo, como módulo M2M, coprocesador. Alternativamente, el elemento de seguridad es un componente de software en forma de un área de almacenamiento seguro en el entorno de ejecución seguro.

Si se constata una inconsistencia entre los datos relevantes para la transacción y los datos del elemento de seguridad, la aplicación de transacción muestra al usuario un mensaje de aviso correspondiente a través de un elemento de salida del dispositivo terminal de comunicación. Alternativa o adicionalmente, impide el envío de los datos relevantes para la transacción a la instancia de servidor. De este modo, el usuario es informado de una forma protegida contra la manipulación o se evita la transacción en caso de un posible ataque de software malicioso.

De forma ventajosa, la información de confirmación también contiene datos de la aplicación de navegador, en particular datos sobre el primer canal de comunicación y/u otros datos específicos de la transacción. La información de confirmación puede ser, por ejemplo, una URL o la dirección IP de la instancia de servidor. Adicionalmente, la información de confirmación también puede incluir el lugar, la fecha y otros datos que identifican la transacción.

En una realización preferente, la información de confirmación contiene al menos parcialmente una información que identifica el entorno de ejecución seguro. Esta información puede ser, por ejemplo, un número de identificación asignado inequívocamente al entorno de ejecución seguro que se ha dado a conocer a la instancia de banco. Alternativamente, la información de confirmación es cifrada con una clave criptográfica, siendo capaz la instancia de servidor de volver a descifrar esta información de confirmación. Alternativamente, una fecha relevante para la transacción es vinculada inequívocamente al entorno de ejecución seguro, habiendo sido comunicada esta vinculación a la instancia de servidor antes de la transacción.

En una realización preferente, la aplicación de transacción establece un tercer canal de comunicación con la instancia de banco en el entorno de ejecución seguro y envía la información de confirmación a la instancia de banco antes de que los datos relevantes para la transacción sean enviados a la instancia de servidor. Esta información de confirmación es solicitada por la instancia de servidor. La instancia de servidor compara la información de confirmación con los datos enviados relevantes para la transacción y autoriza o evita el servicio asociado a la transacción en función de la comparación.

En una realización alternativa, la aplicación de transacción incluye la información de confirmación de forma codificada en los datos relevantes para la transacción. A continuación, los datos relevantes para la transacción con la información de confirmación incluida de forma codificada son puestos a disposición de la aplicación de navegador. Los datos relevantes para la transacción con la información de confirmación incluida de forma codificada son enviados a la instancia de servidor como datos relevantes para la transacción. En particular, la información de confirmación está incluida de forma codificada en una parte del número de tarjeta de crédito específica del usuario, por lo que se genera un número de tarjeta de crédito modificado. En particular, el número de tarjeta de crédito modificado es enviado a la instancia de servidor como parte de los datos relevantes para la transacción, en lugar del número de tarjeta de crédito. Puesto que el usuario ya ha realizado la entrada de los datos relevantes para la transacción, es innecesario volver a mostrar el número de tarjeta de crédito modificado porque confundiría al usuario. La instancia de servidor reconoce mediante el número modificado que el número de tarjeta de crédito contiene una información de confirmación y descifra el número de tarjeta de crédito correspondientemente.

La idea de la invención incluye además un producto de programa informático que se puede cargar directamente en la memoria de un procesador dentro de un dispositivo terminal de comunicación digital y comprende partes del código de software con las que se ejecutan los pasos del procedimiento aquí descrito cuando el producto de programa informático es ejecutado en el procesador.

El objetivo se consigue además mediante un dispositivo terminal de comunicación con medios para realizar el procedimiento descrito. El dispositivo terminal presenta para ello una unidad de procesador con un entorno de ejecución no seguro y un entorno de ejecución seguro; una unidad de entrada para introducir datos relevantes para la transacción; una unidad de salida para emitir datos relevantes para la transacción; así como una primera interfaz para establecer un primer canal de comunicación y enviar datos relevantes para la transacción. El dispositivo terminal presenta en particular una aplicación de navegador en el entorno de ejecución no seguro con un módulo de extensión, presentando este módulo de extensión una segunda interfaz para establecer un segundo canal de comunicación con una aplicación de transacción en el entorno de ejecución seguro. La aplicación de transacción accede al menos a parte de los datos introducidos relevantes para la transacción a través del segundo canal de comunicación para generar una información de confirmación para asegurar la transacción.

El objetivo se consigue además mediante un sistema con medios para realizar el procedimiento descrito. El sistema presenta un dispositivo terminal de comunicación aquí descrito, una instancia de servidor y una instancia de banco. En particular, el dispositivo terminal de comunicación presenta un entorno de ejecución seguro. Este entorno de ejecución seguro es inequívocamente identificable mediante una clave criptográfica en el sistema.

A continuación se describen la invención u otros modos de realización y ventajas de la invención en detalle en base a las figuras, aunque las figuras únicamente describen ejemplos de realización de la invención. Los componentes iguales en las figuras se caracterizan con los mismos números de referencia. Las figuras no deben considerarse a escala, algunos elementos de las figuras pueden estar representados con un tamaño exageradamente grande o de forma exageradamente simplificada.

Muestran:

La figura 1, una representación esquemática de un procesador configurado en un dispositivo de comunicación según la invención

La figura 2, una representación esquemática de un sistema según la invención

La figura 3, una representación esquemática de un primer ejemplo de realización del procedimiento según la invención

La figura 4, una representación esquemática de un ejemplo de realización alternativo al de la figura 3 del procedimiento según la invención

La figura 1 muestra un procesador -P- configurado en un dispositivo terminal de comunicación -1- según la invención. La generación de la información de confirmación tiene lugar según la invención dentro de un entorno de ejecución seguro -TZ-. Este entorno de ejecución seguro -TZ- es, por ejemplo, una ARM TrustZone® en un dispositivo terminal de telefonía móvil -1-. La ARM TrustZone® representa una tecnología conocida, con la que se genera una zona protegida en el procesador -P-, que es utilizada como entorno de ejecución seguro -TZ- para realizar aplicaciones críticas para la seguridad, denominadas trustlet -TL-. Con este fin, la ARM TrustZone® está implementada en una plataforma de hardware -HW- de un dispositivo de comunicación móvil -1-. Esta plataforma de hardware -HW- ofrece la posibilidad de acceso a una pantalla -D-, un teclado -KB- y, dado el caso, a un elemento de seguridad -SE-, por ejemplo, una SIM o una tarjeta de almacenamiento masivo con funcionalidad de seguridad.

Un área de almacenamiento en el dispositivo terminal de comunicación -1- está subdividida en un área de almacenamiento no seguro y un área de almacenamiento seguro e incluye un entorno de ejecución. El entorno de ejecución carga aplicaciones -AL-, también denominadas Applet, y las ejecuta en la plataforma de hardware -HW-. Las funciones básicas y principales de un entorno de ejecución son la lectura, escritura, clasificación y búsqueda de archivos, transferencia de datos a través de una red de comunicación, control de elementos de entrada, por ejemplo, del teclado -KB- o un micrófono, así como control de elementos de salida, por ejemplo, de la pantalla -KB- o un altavoz.

En el área de almacenamiento no seguro se ejecuta un entorno de ejecución no seguro -NZ-, también denominado zona normal, mientras que en el área de almacenamiento seguro se ejecuta un entorno de ejecución seguro -TZ-. En el entorno de ejecución no seguro están almacenadas una o varias aplicaciones -AL-, también denominadas Applet, que son iniciadas desde el entorno de ejecución normal -NZ-. Uno o varios controladores (= TZ System Driver y TZ API), así como un sistema operativo ("Rich OS"), también están dispuestos en el área de almacenamiento no seguro. En un escenario de ataque, en el entorno de ejecución no seguro -NZ- se encuentran, además de las aplicaciones -AL-, también aplicaciones maliciosas que son capaces de espiar y modificar los datos introducidos mediante el elemento de entrada -KB-. Para que el usuario no advierta el ataque, dado el caso, también el elemento de salida -D- puede estar afectado por el ataque, de forma que al usuario se muestra información falsa.

En el área de almacenamiento seguro -TZ- se ejecuta el sistema operativo del entorno de ejecución seguro -TRE- (= Trustzone Runtime Environment), así como una o varias aplicaciones relevantes para la seguridad, denominadas trustlet -TL-.

Además de la tecnología ARM TrustZone® representada en la figura 1, en el procedimiento aquí descrito también se pueden utilizar otras tecnologías para el aislamiento de entornos de ejecución seguros. Por ejemplo, se puede realizar una virtualización en un denominado sistema embebido. Por ejemplo, se pueden utilizar productos de las empresas Trango® y Open Kernel Labs®.

Una parte de la invención consiste en un módulo de extensión -PI- de una aplicación de navegador. Este módulo de extensión, también denominado complemento (Plug-In), proporciona un segundo canal de comunicación -5- entre la aplicación de navegador -AL- y la aplicación de transacción -TL- para asegurar la transacción.

En la figura 2 está representado un sistema según la invención, con el que se pueden asegurar las transacciones. Aquí está representado nuevamente el dispositivo terminal de comunicación -1-, según la invención, descrito en la figura 1. Como ya se ha descrito en la figura 1, el dispositivo terminal -1- presenta un procesador -P- con un entorno de ejecución seguro y uno no seguro -TZ-, -NZ-. Además está previsto un elemento de entrada -KB- y un elemento de salida -D-. A su vez, para el aseguramiento de una transacción está prevista, según la invención, una aplicación de navegador -AL- con un módulo de extensión -PI- que puede establecer un segundo canal de comunicación -5-. Adicionalmente, el dispositivo terminal -1- está equipado con un elemento de seguridad -SE-, pudiendo el entorno de ejecución seguro establecer un cuarto canal de comunicación -7- para tomar medidas de seguridad adicionales, por ejemplo, la comprobación de un PIN introducido por un usuario, almacenado como PIN de referencia en el -SE-.

El sistema comprende además una instancia de servidor -2-, en este caso en forma de una tienda web y una instancia de banco -3-.

La instancia de servidor -2- ofrece, por ejemplo, servicios de información y formación, como educación en línea, aprendizaje en línea, enseñanza en línea, publicaciones digitales, libros electrónicos, revistas en línea y catálogos en línea, o servicios de adquisición, comercio y pedidos, como negocio electrónico, comercio electrónico, aprovisionamiento electrónico, tarjeta virtual de pago, tiendas en línea, intermediarios en línea, subastas en línea, o servicios culturales y administrativos, como cultura en línea, gobierno electrónico o voto electrónico, que el usuario quisiera utilizar con su dispositivo terminal -1-. Para ello, el usuario inicia la aplicación de navegador -AL- para establecer un primer canal de comunicación -4- con la instancia de servidor -2-, que tiene lugar, por ejemplo, en forma de una consulta de http a través de la aplicación de navegador -AL-.

La aplicación de navegador -AL-, también denominada navegador web, es en este caso una aplicación especial para representar páginas web en internet. Mientras el navegador web -AL- es ejecutado en el entorno de ejecución no seguro -NZ-, la aplicación de transacción -TL- se encuentra dentro del entorno de ejecución seguro -TZ-. De este modo, la aplicación de transacción -TL- no puede ser atacada por software malicioso que pudiera encontrarse en el dispositivo terminal de comunicación -1-.

Un usuario que quisiera utilizar la aplicación de transacción según la invención mediante un entorno de ejecución seguro -TZ- debe haber instalado el módulo de extensión -PI-. Esto puede tener lugar simultáneamente, por ejemplo, con la instalación por parte del propio usuario de una aplicación (app) en el dispositivo terminal de comunicación -1-, que el usuario puede descargar en una instancia de servidor -2- desde la que quisiera adquirir servicios, o en una instancia de banco -3- a través de la cual se realiza físicamente la transacción de pago.

Preferentemente, esta "app" es puesta a disposición por el proveedor del procedimiento de pago, en adelante denominado instancia de banco -3-. En el marco de la descarga de la "app", o tras su instalación, la instancia de banco -3- es informada sobre qué datos relevantes para la transacción son vinculados a qué entorno de ejecución seguro -TZ-. Los datos relevantes para la transacción, en particular los datos de la tarjeta de crédito, son identificados en este caso mediante los datos habituales de las tarjetas, como titular, número, fecha de vencimiento, código de comprobación, etc. A su vez, el entorno de ejecución seguro es identificado inequívocamente mediante una clave criptográfica K_{Applet} que ha sido generada en el entorno de ejecución seguro y comunicada a la instancia de banco -3- o, alternativamente, ha sido generada por la instancia de banco y puesta a disposición del entorno de ejecución seguro -TZ-.

Tras la instalación del módulo de extensión -PI-, en la instancia de banco queda establecida una clasificación de datos relevantes para la transacción y una identificación inequívoca del entorno de ejecución seguro -TZ-. El entorno de ejecución seguro -TZ- también conoce los datos relevantes para la transacción.

La instancia de banco -3- también tiene conocimiento de que las transacciones realizadas con el dispositivo terminal -1- del usuario están aseguradas con el entorno de ejecución seguro. Esto es importante para que las solicitudes de pago de la instancia de servidor -2- que llegan a la instancia de banco -3- sean procesadas correctamente en la instancia de banco -3-.

A continuación se describe en detalle un primer ejemplo de realización de la invención según la figura 3. Una aplicación de navegador -AL- establece un primer canal de comunicación -4- con la instancia de servidor -2-.

Para el usuario, la compra a través de internet mediante el dispositivo terminal -1- tiene lugar de la forma habitual: El usuario selecciona el servicio, el producto o el artículo en la página web de la instancia de servidor -2-. La instancia de servidor -2- solicita entonces al usuario en el paso -A- que pague el artículo seleccionado, para lo que emite un formulario HTML en el que el usuario debe introducir los datos relevantes para la transacción, en particular, los datos de la tarjeta de crédito. Alternativamente, el usuario puede permitir la introducción automática de datos por parte de la trustlet o del navegador mediante la función de "autocompletar".

El complemento (Plug-In) de navegador -PI- reconoce en el paso -B- que se ha activado un proceso de pago y establece un segundo canal de comunicación -5- para supervisar los datos relevantes para la transacción, introducidos en los campos del formulario HTML. Esto puede tener lugar de forma continua, es decir, tras cada pulsación sobre el elemento de entrada -KB-, o, preferentemente, al enviar el formulario HTML, es decir, cuando el usuario ha activado el botón "enviar" en la aplicación de navegador. Si el formulario HTML se cumplimenta primero en su totalidad y a continuación se activa el complemento de navegador -PI- para la transferencia de los datos introducidos relevantes para la seguridad al entorno de ejecución seguro -TZ- (paso -B-), estos datos ya se encuentran en su forma definitiva y el usuario ya ha indicado que no quiere realizar ningún cambio.

El complemento de navegador -PI- busca entonces los datos relevantes para la transacción, que deben ser comprobados/supervisados en los campos del formulario HTML. Para ello, los datos relevantes para la transacción buscados/supervisados, por ejemplo, el número de tarjeta de crédito, pueden estar almacenados en el propio complemento de navegador -PI-, es decir, en el entorno de ejecución no seguro -NZ-, o en el entorno de ejecución seguro -TZ-. En este último caso, el complemento de navegador -PI- activa, para cada envío de un formulario HTML, la aplicación de transacción -TL- del entorno de ejecución seguro -TZ-, para que esta aplicación de transacción -TL- pueda examinar los campos del formulario HTML buscando los correspondientes datos relevantes para la transacción.

Si los datos relevantes para la transacción son encontrados en un campo del formulario HTML, el complemento de navegador -PI- impide el envío de los datos del formulario HTML. A continuación, la aplicación de transacción -TL- inicia las medidas para asegurar la transacción, lo que en la figura 3 también se representa en el paso -B-. Además de los datos introducidos relevantes para la transacción, la aplicación de transacción -TL- recibe del complemento de navegador -PI- otros datos de la aplicación de navegador, por ejemplo, la URL, es decir, la página web mostrada en el navegador, o la dirección IP de la instancia de servidor -2-. Adicionalmente, el complemento de navegador puede poner a disposición del entorno de ejecución seguro -TL- también el lugar, la fecha y otros datos que identifican la transacción.

En el caso más sencillo, la aplicación de transacción -TL- muestra entonces un cuadro de diálogo no manipulable, por ejemplo:

"¿Desea realmente realizar la transacción en www.serverinstanz.de?"

El cuadro de diálogo puede volver a mostrar parte de los datos relevantes para la transacción. Para este cuadro de diálogo, el elemento de salida -D- únicamente puede ser controlado a través del entorno de ejecución seguro -TZ-, de forma que cualquier salida es generada por el entorno de ejecución seguro -TZ-. Por lo tanto, el usuario puede estar seguro de que la nueva salida está protegida contra la manipulación. El usuario puede comprobar entonces la nueva salida con los datos relevantes para la transacción introducidos previamente en el formulario HTML y en caso de datos inconsistentes impedir la transacción en este punto. La salida de datos protegida contra la manipulación en un elemento de salida mediante un entorno de ejecución seguro -TZ- se describe, por ejemplo, en el documento DE 102011018431, con fecha de solicitud de patente del 21 de abril de 2011 del mismo solicitante, a cuya descripción completa se hace referencia aquí explícitamente.

Ahora se solicita al usuario del dispositivo terminal -1- que responda al cuadro de diálogo. La respuesta tiene lugar a través de una entrada mediante el elemento de entrada -KB-. Para este cuadro de diálogo, el elemento de entrada -KB- únicamente puede ser controlado a través del entorno de ejecución seguro -TZ-, de forma que cualquier entrada en relación a este cuadro de diálogo es verificada por el entorno de ejecución seguro -TZ-. De este modo, el cuadro de diálogo únicamente puede ser respondido por el usuario a través de una entrada protegida contra la manipulación. La entrada de datos protegida contra la manipulación mediante un entorno de ejecución seguro -TZ- se describe, por ejemplo, en el documento DE 102010052666.5, con fecha de solicitud de patente del 26 de noviembre de 2010 del mismo solicitante, a cuya descripción completa se hace referencia aquí explícitamente.

En lugar de una respuesta sí/no para responder al cuadro de diálogo, también se puede solicitar al usuario volver a introducir parte de los datos relevantes para la transacción, por ejemplo, el importe y código de comprobación de la tarjeta de crédito. Esto tiene dos ventajas. En primer lugar, el usuario es consciente del importe que va a pagar. Si el dispositivo terminal -1- ya estuviera correspondientemente protegido de otra manera, dado el caso podría prescindirse de la entrada de un PIN o similar. En segundo lugar, no es trivial filtrar partes de los datos relevantes para la transacción de la pluralidad de diferentes páginas web de instancias de servidor -2- individuales. De este modo, este cuadro de diálogo con una nueva entrada supondría un método elegante para que la aplicación de transacción -TL- obtenga parte de los datos relevantes para la transacción.

Alternativamente se puede solicitar al usuario la introducción de un PIN o una información equivalente, especialmente una contraseña, o una huella dactilar biométrica.

A partir de los datos relevantes para la transacción, obtenidos mediante el segundo canal de comunicación -5-, la aplicación de transacción -TL- genera una información de confirmación que es cifrada con la clave criptográfica K_{Applet} del entorno de ejecución seguro -TZ-. Una información de confirmación puede estar estructurada, por ejemplo, como sigue:

Información de confirmación = $enc(URL_{Tienda\ web} \mid\mid Importe, K_{Applet}) \mid\mid$ Número de tarjeta de crédito

El número de tarjeta de crédito se adjunta sin cifrado. Alternativamente, la propia información de confirmación puede ser nuevamente cifrada para que nadie pueda leer el número de tarjeta de crédito durante la transferencia de datos.

La aplicación de transacción -TL- envía entonces la información de confirmación a la correspondiente instancia de banco -3-, por ejemplo, un proveedor de tarjeta de crédito. Para ello, la aplicación de transacción -TL- establece un tercer canal de comunicación -6-. Este canal -6- puede realizarse de cualquier modo, por ejemplo, por SMS o a través del protocolo de internet. Esto está representado en la figura 3 como paso -C-. La instancia de banco -3- se puede determinar fácilmente en base al número de tarjeta de crédito disponible, gracias a lo cual el dispositivo terminal puede establecer el canal de forma precisa.

Para establecer el canal -6- se utiliza, por ejemplo, el número de identificación del banco, abreviado BIN, también denominado número de identificación del emisor IIN. El BIN se utiliza, por ejemplo, para identificar tarjetas de crédito y débito en el enrutamiento dentro de redes de cajeros automáticos. En base al BIN se pueden identificar el tipo de

tarjeta utilizado y la instancia de banco -3- que ha emitido la tarjeta de pago correspondiente. El BIN tiene validez internacional. El formato exacto del BIN está descrito en la norma ISO 7812. En un número de tarjeta de crédito de 16 dígitos, los primeros 6 representan el BIN. Alternativamente existen buscadores de BIN para poder determinar, por ejemplo, el BIN de una tarjeta EC/Maestro. Pero esta información también se puede almacenar al instalar la trustlet -TL- en la -TL-. Esto permite prescindir de la búsqueda.

De este modo, la aplicación de transacción -TL- dispone de una lista de los números de teléfono de las instancias de banco -3- para transferir un SMS con la información de confirmación a través del tercer canal de comunicación -6-. Si el canal -6- se establece alternativamente mediante protocolo de internet -IP-, la aplicación de transacción -TL- dispone, a través del BIN, de una lista de las URL o las direcciones IP de las instancias de banco -3-.

Si la información de confirmación ha sido enviada a la instancia de banco, el complemento de navegador activa el envío de los datos relevantes para la transacción a la instancia de servidor según el paso -D-, a través de lo cual se envía, por ejemplo, la consulta de http a través del primer canal de comunicación -4-. Tras recibir los datos relevantes para la transacción, el operador de la instancia de servidor -2- contacta con la instancia de banco -3- según el paso -E- de la figura 3 para poder comprobar los datos relevantes para la transacción y recibir el importe pendiente.

Entonces, en el paso -F-, la instancia de banco -3- comprueba si para el número de tarjeta de crédito correspondiente es necesaria una información de confirmación de un entorno de ejecución seguro -TZ-. Si este es el caso, la instancia de banco -3- comprueba si se dispone de una información de confirmación de un entorno de ejecución seguro -TZ- con los mismos datos relevantes para la transacción, por ejemplo, nombre y URL de la instancia de servidor -2-, y el mismo importe. Si la comparación resulta en una coincidencia, la transacción es autorizada por la instancia de banco -3-. Para ello, la instancia de servidor recibe en el paso -H- el resultado de la comparación, por lo cual la instancia de servidor pone a disposición del usuario del dispositivo terminal -1- el producto, el artículo o el servicio.

Si el resultado de la comparación del paso -F- indica que los datos relevantes para la transacción de la instancia de servidor no coinciden con los datos de la información de confirmación, la instancia de banco -3-, según el paso -G-, puede realizar consultas a través del canal -6- aún establecido o, alternativamente, volver a contactar con un tercer canal de comunicación -6- a través del número de teléfono transferido con el SMS o, alternativamente, la dirección IP obtenida, para realizar consultas según el paso -G-.

En la figura 4 está representado un procedimiento alternativo al de la figura 3 para asegurar una transacción. Los pasos -A- y -B- son idénticos con los pasos -A- y -B- de la figura 3.

Al igual que en la figura 3, la aplicación de transacción -TL- genera la información de confirmación en el entorno de ejecución seguro -TZ-. Sin embargo, esta información de confirmación no es enviada directamente a la instancia de banco -3- (paso -C- de la figura 3) sino que es incluida de forma codificada en los datos relevantes para la transacción, por ejemplo, el número de tarjeta de crédito.

Un número de tarjeta de crédito está compuesto por una parte de 10 dígitos específica del titular y un BIN de 6 dígitos. La parte de 6 dígitos del número de tarjeta de crédito debería mantenerse invariable para que sea posible realizar de forma invariable una comprobación de veracidad de los datos relevantes para la transacción, por ejemplo, errores tipográficos, en la instancia de servidor -2-.

La parte del número de la tarjeta de crédito específica del titular se utiliza entonces para incluir la información de confirmación de forma codificada. Si se utilizan los diez dígitos decimales de la parte específica del titular de la tarjeta de crédito para la codificación, la información de codificación se puede incluir de forma codificada con un volumen de datos de aproximadamente 32 bits.

En representación de muchas posibilidades de codificación de datos relevantes para la transacción como información de confirmación en 32 bits, a continuación se describe una posibilidad, en la que la información de confirmación está compuesta, por ejemplo, por el importe a pagar y la URL de la instancia de servidor -2-. Esta inclusión de forma codificada se corresponde con el paso -I- de la figura 4.

El importe a pagar se expresa de forma binaria. Los valores numéricos superiores a 42 millones se pueden codificar en una palabra de datos de 32 bits, debiéndose tener en cuenta dos posiciones decimales, ya que se cumple que

Valor numérico máximo = 2*exp(32)/100.

Se aplica una función hash de 32 bits a la URL de la instancia de servidor -2-. El resultado es cifrado con la clave criptográfica K_{Applet} del entorno de ejecución seguro -TZ-.

Información de confirmación = enc(Parte del número de tarjeta de crédito específica del titular EXOR Importe EXOR Hash($URL_{Tienda\ web}$), K_{Applet})

Al contrario que en el procedimiento según la figura 3, en este caso no se requiere ningún otro cifrado de la información de confirmación.

La información de confirmación generada dispone a su vez de 32 bits, lo que se expresa en 10 dígitos decimales. La parte de 10 dígitos del número de la tarjeta de crédito específica del titular es sustituida entonces con la información de confirmación de diez dígitos, por lo que se obtiene un número de tarjeta de crédito modificado. A continuación se vuelve a calcular la cifra de comprobación de la tarjeta de crédito.

En el paso -K- de la figura 4, el complemento de navegador -PI- obtiene el número de tarjeta de crédito modificado de la aplicación de transacción -TL- del entorno de ejecución seguro -TZ- y sustituye el número de tarjeta de crédito introducido por el número de tarjeta de crédito modificado en el lugar correspondiente del campo del formulario HTML de la aplicación de navegador -AL-. Puesto que el usuario ya ha presionado el botón "enviar", es razonable ocultar el número de tarjeta de crédito modificado según el paso -L- para que el usuario no vea el número de tarjeta de crédito modificado. De este modo no se confunde al usuario del dispositivo terminal -1-.

Ahora, según el paso -D-, la instancia de servidor -2- obtiene los datos relevantes para la transacción con la información de confirmación incluida de forma codificada a través del primer canal de comunicación -4-. La instancia de servidor -2- redirige estos datos obtenidos a la instancia de banco -3- de la forma habitual, según el paso -E-. En base a los datos relevantes para la transacción, por ejemplo, el nombre del titular, la instancia de banco -3- reconoce que los datos relevantes para la transacción podrían haber sido generados por una aplicación de transacción -TL- de un entorno de ejecución seguro -TZ- y especialmente que el número de tarjeta de crédito contiene una confirmación incluida de forma codificada. La instancia de banco -3- también calcula el número de tarjeta de crédito modificado con la clave criptográfica K_{Applet} recibida previamente y los datos relevantes para la transacción (URL, importe) recibidos de la instancia de servidor -2-. Si el número de tarjeta de crédito modificado calculado coincide con el número de tarjeta de crédito modificado recibido de la instancia de servidor -2-, se autoriza la transacción y la instancia de servidor -2- es informada sobre la consistencia de los datos, véase paso -H-.

Listado de números de referencia

1 Dispositivo terminal de comunicación móvil, teléfono inteligente
P Procesador
NZ Entorno de ejecución no seguro
TZ Entorno de ejecución seguro, Trustzone
TZ-ID Número de identificación del TZ, K_{Applet}
OS Sistema operativo del entorno de ejecución no seguro
TRE Sistema operativo del entorno de ejecución seguro, MobiCore
TL Trustlet, aplicación dentro del TZ
AL Applet, aplicación dentro del NZ
PI Complemento, módulo de extensión de un AL
HW Plataforma de hardware
SE Elemento de seguridad
KB Teclado, elemento de entrada
DP Pantalla, elemento de salida

2 Instancia de servidor, tienda web
3 Instancia de banco, proveedor de servicio de pago
4 Primer canal de comunicación, red de telefonía móvil
5 Segundo canal de comunicación, dentro del procesador
6 Tercer canal de comunicación, red de telefonía móvil
7 Cuarto canal de comunicación, fuera del procesador

A Inicio del proceso de pago
B Reconocimiento de la transacción mediante complemente de navegador y activación de la comprobación mediante TZ
C Información de confirmación al proveedor de servicios de pago
D Envío de los datos relevantes para la transacción, datos de la tarjeta de crédito
E Reenvío de los datos relevantes para la transacción y datos de la tienda web
F Comparación entre los datos relevantes para la transacción/datos de la tienda web e información de confirmación
G Consultas en caso de datos inconsistentes
H Información sobre proceso de pago realizado con éxito
I Codificación del número de tarjeta de crédito con información de confirmación (importe, receptor, TZ-ID del TZ) y recepción de un número de tarjeta modificado
K Utilización del número de tarjeta de crédito modificado en el navegador (web)
L Ocultación del número de tarjeta de crédito modificado
M Cálculo del número de tarjeta de crédito modificado en base a los datos de la tienda web y TZ-ID

REIVINDICACIONES

1. Procedimiento para asegurar una transacción, en particular una transacción de pago, entre un dispositivo terminal de comunicación (1) y una instancia de servidor (2), tal que el dispositivo terminal de comunicación (1) comprende un procesador (P) con un entorno de ejecución no seguro (NZ) y un entorno de ejecución seguro (TZ), con los pasos de procedimiento:

- establecimiento de un primer canal de comunicación (4) entre el dispositivo terminal de comunicación (1) y la instancia de servidor (2);
- envío (D) de datos relevantes para la transacción del dispositivo terminal de comunicación (1) a la instancia de servidor (2) a través del primer canal de comunicación (4), **caracterizado por que:**

- antes del paso de envío se establece un segundo canal de comunicación (5) entre la aplicación de navegador (AL) en el entorno de ejecución no seguro (NZ) y una aplicación de transacción (TL) en el entorno de ejecución seguro (TZ);
- antes del paso de envío, al menos una parte de los datos relevantes para la transacción es enviada a través del segundo canal de comunicación (5) a la aplicación de transacción (TL);
- antes del paso de envío, la aplicación de transacción (TL) genera una información de confirmación a partir de la parte recibida de los datos relevantes para la transacción con el fin de asegurar la transacción; y
- esta información de confirmación es utilizada para autorizar la transacción en la instancia de servidor (2).

2. Procedimiento, según la reivindicación 1, en el que la información de confirmación también contiene datos de la aplicación de navegador (AL), en particular datos sobre el primer canal de comunicación y/u otros datos específicos de la transacción.

3. Procedimiento, según cualquiera de las reivindicaciones 1 o 2, tal que los datos relevantes para la transacción son introducidos por el usuario en una aplicación de navegador (AL) en el entorno de ejecución no seguro (NZ), siendo enviada al menos una parte relevante para la transacción de los datos introducidos a través del segundo canal de comunicación (5) a la aplicación de transacción (TL) antes del paso de envío.

4. Procedimiento, según cualquiera de las reivindicaciones 1 o 2, en el que al menos una parte de los datos relevantes para la transacción son puestos a disposición por la instancia de servidor (2) a través del primer canal de comunicación y al menos una parte relevante para la transacción de los datos introducidos es enviada a través del segundo canal de comunicación (5) a la aplicación de transacción (TL) antes del paso de envío.

5. Procedimiento, según cualquiera de las reivindicaciones 1 o 2, tal que al menos una parte de los datos relevantes para la transacción son puestos a disposición y/o generados por la aplicación de transacción (TL).

6. Procedimiento, según cualquiera de las reivindicaciones anteriores, en el que la aplicación de transacción (TL):

- comprueba los datos relevantes para la transacción en el entorno de ejecución seguro (TZ);
- en caso de constatar una inconsistencia de partes de los datos relevantes para la transacción durante la comprobación:

- muestra al usuario un mensaje de advertencia a través de un elemento de salida (D) del dispositivo terminal de comunicación (1); y/o
- impide el envío (D) de los datos relevantes para la transacción a la instancia de servidor (2).

7. Procedimiento, según cualquiera de las reivindicaciones anteriores, en el que la información de confirmación contiene una información (TZ-ID, K_{Applet}) que identifica inequívocamente al entorno de ejecución seguro (TZ).

8. Procedimiento, según cualquiera de las reivindicaciones anteriores, en el que:

- la aplicación de transacción (TL) establece en el entorno de ejecución seguro (TZ) un tercer canal de comunicación (6) con la instancia de banco (3); y
- la información de confirmación es enviada (D) a la instancia de banco (3) utilizando partes de los datos relevantes para la transacción, antes de que los datos relevantes para la transacción sean enviados a la instancia de servidor (2).

9. Procedimiento, según la reivindicación 8, en el que

- la instancia de servidor (2) envía al menos parcialmente los datos relevantes para la transacción recibidos del dispositivo terminal de comunicación (1) a la instancia de banco (3);
- la instancia de banco compara la información de confirmación con los datos relevantes para la transacción enviados por la instancia de servidor (2); y
- la instancia de banco (2) autoriza o impide la transacción en función de la comparación.

10. Procedimiento, según cualquiera de las reivindicaciones 1 a 7, en el que la aplicación de transacción (TL):

- incluye la información de confirmación de forma codificada en los datos relevantes para la transacción;
- pone a disposición de la aplicación de navegador (AL) los datos relevantes para la transacción con la información de confirmación incluida de forma codificada; y
- los datos relevantes para la transacción con la información de confirmación incluida de forma codificada son enviados a la instancia de servidor (2).

11. Procedimiento, según la reivindicación 10, en el que la información de confirmación se incluye de forma codificada en una parte del número de tarjeta de crédito específico del titular, mediante lo cual se genera un número de tarjeta de crédito modificado.

12. Procedimiento, según la reivindicación 11, en el que el número de tarjeta de crédito modificado es enviado a la instancia de servidor (2) como parte de los datos relevantes para la transacción, en lugar del número de tarjeta de crédito.

13. Procedimiento, según cualquiera de las reivindicaciones anteriores, en el que la aplicación de transacción (TL) en el entorno de ejecución seguro (TZ) cifra los datos relevantes para la transacción mediante una clave criptográfica asignada a este entorno de ejecución seguro (TZ).

14. Procedimiento, según cualquiera de las reivindicaciones anteriores, en el que a la instancia de banco (3) le fue comunicada la correspondencia de al menos partes de los datos relevantes para la transacción, en particular del número de tarjeta de crédito, con el entorno de ejecución seguro (TZ) antes de ejecutar por primera vez el procedimiento.

15. Producto de programa informático que se puede cargar directamente en la memoria de un procesador (P) dentro de un dispositivo terminal de comunicación (1) digital y comprende partes del código de software con las que se ejecutan los pasos, según cualquiera de las reivindicaciones 1 a 11, cuando el producto de programa informático es ejecutado en el procesador (P).

16. Dispositivo terminal de comunicación (1) con medios para realizar el procedimiento, según cualquiera de las reivindicaciones 1 a 14, que presenta:

- una unidad de procesador (P) con un entorno de ejecución no seguro (NZ) y un entorno de ejecución seguro (TZ);
- una unidad de entrada (KB) para introducir los datos relevantes para la transacción;
- una unidad de salida (DP) para emitir los datos relevantes para la transacción;
- una primera interfaz para establecer un primer canal de comunicación (4) y enviar (D) datos relevantes para la transacción;

caracterizado por que:

- una aplicación de navegador (AL) en el entorno de ejecución no seguro (NZ) presenta un módulo de extensión (PI) y este módulo de extensión (PI) presenta una segunda interfaz para establecer un segundo canal de comunicación (5) con una aplicación de transacción (TL) en el entorno de ejecución seguro (TZ), y
- la aplicación de transacción (TL) puede acceder al menos a parte de los datos introducidos relevantes para la transacción a través del segundo canal de comunicación (5) para generar una información de confirmación para asegurar la transacción.

17. Sistema con medios para realizar el procedimiento, según cualquiera de las reivindicaciones 1 a 14, que presenta:

- un dispositivo terminal de comunicación (1) según la reivindicación 16;
- una instancia de servidor (2); y
- una instancia de banco (3)

caracterizado por que:

- el dispositivo terminal de comunicación (1) presenta un entorno de ejecución seguro (TZ) y este entorno de ejecución seguro (TZ) es inequívocamente identificable (TZ-ID) mediante una clave criptográfica en el sistema.

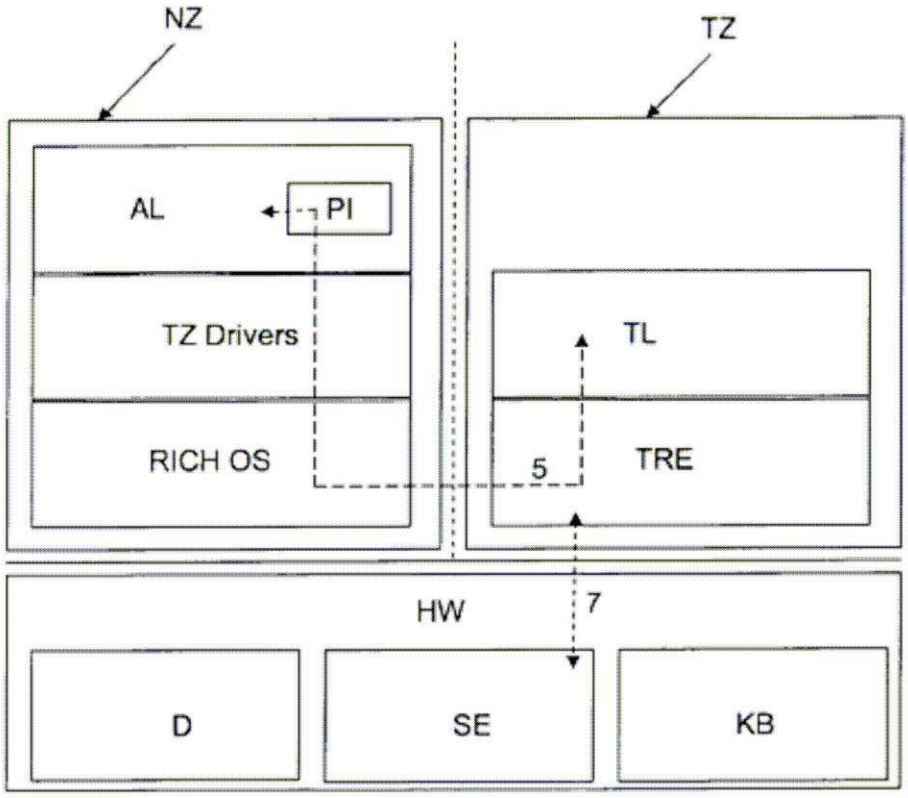

Fig 1

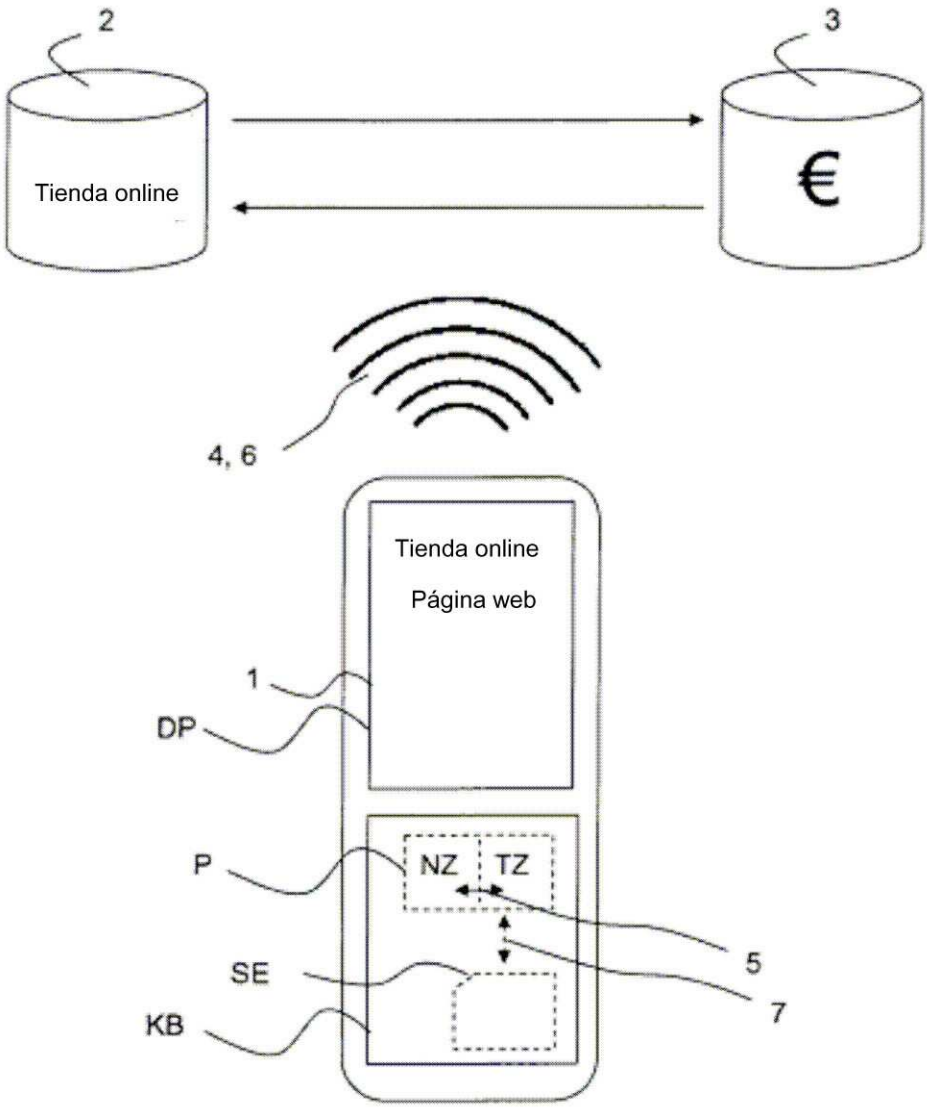
2
3
Tienda online
€
4, 6
Tienda online
Página web
1
DP
P
NZ
TZ
5
SE
7
KB

Fig 2

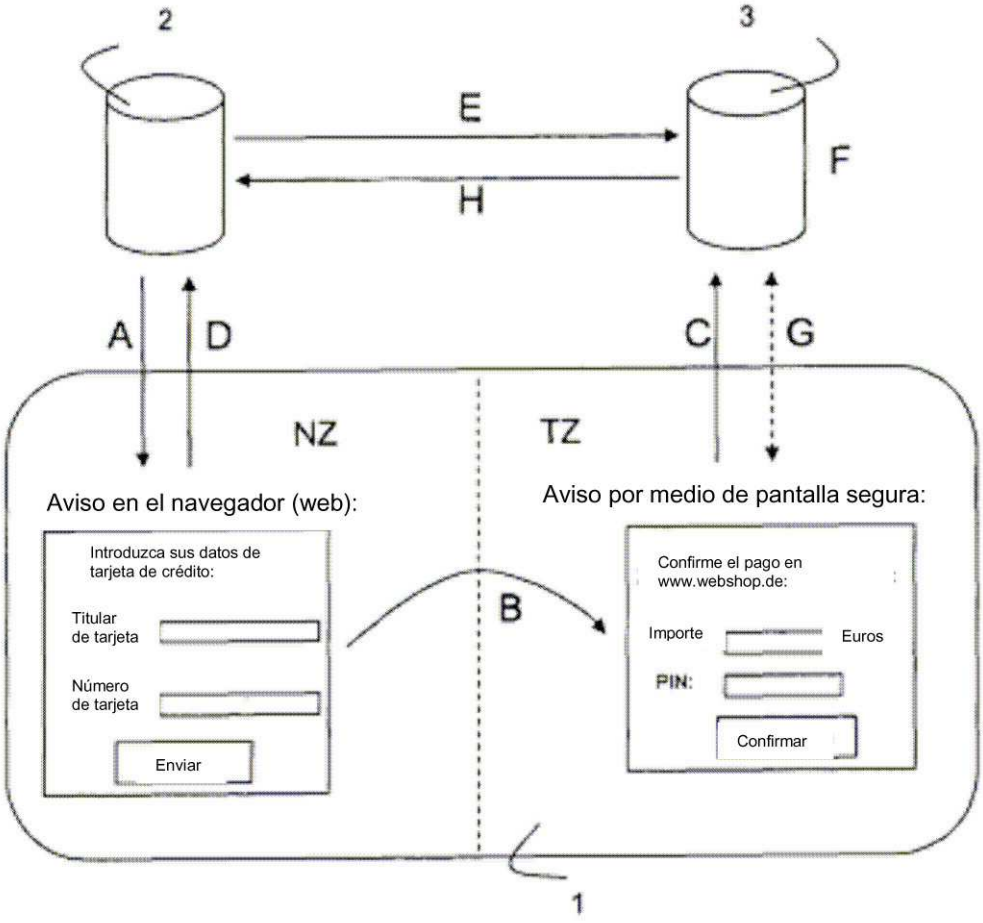
2
3
E
H
F
A
D
C
G
NZ
TZ
Aviso en el navegador (web):
Introduzca sus datos de tarjeta de crédito:
Titular de tarjeta
Número de tarjeta
Enviar
B
Aviso por medio de pantalla segura:
Confirme el pago en www.webshop.de:
Importe
Euros
PIN:
Confirmar
1

Fig 3

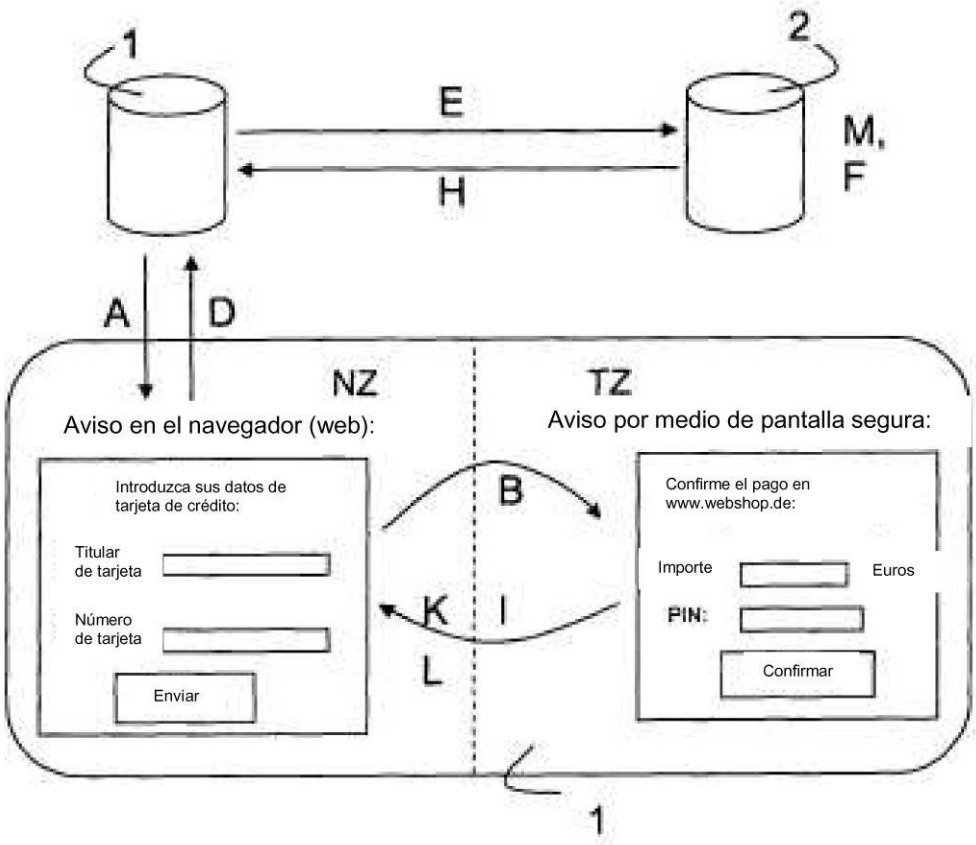
1
2
E
H
M,
F
A
D
NZ
TZ
Aviso en el navegador (web):
Aviso por medio de pantalla segura:
Introduzca sus datos de tarjeta de crédito:
Titular de tarjeta
Número de tarjeta
Enviar
B
K
I
L
Confirme el pago en www.webshop.de:
Importe
Euros
PIN:
Confirmar
1

Fig 4