(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 525 013**

(51) Int. CI.:

G06F 21/34 (2013.01)
G06F 21/35 (2013.01)
G06F 21/42 (2013.01)
G06F 21/43 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **31.03.2010 E 10712415 (8)**

(97) Fecha y número de publicación de la concesión europea: **22.10.2014 EP 2417550**

(54) Título: **Procedimiento para ejecutar una aplicación por medio de un soporte de datos portátil**

(30) Prioridad:

06.04.2009 DE 102009016532

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
17.12.2014

(73) Titular/es:

GIESECKE & DEVRIENT GMBH (100.0%)
Prinzregentenstrasse 159
81677 München, DE

(72) Inventor/es:

BAUER, SVEN

(74) Agente/Representante:

ARPE FERNÁNDEZ, Manuel

DESCRIPCIÓN

Procedimiento para ejecutar una aplicación por medio de un soporte de datos portátil

La invención se refiere a un procedimiento para ejecutar una aplicación por medio de un soporte de datos portátil, así como a un soporte de datos portátil correspondiente.

Los soportes de datos portátiles personales se emplean cada vez más para permitir a los usuarios la ejecución de aplicaciones prácticas basadas en software, mediante el empleo de un software al que el usuario tiene sólo acceso limitado. El fin de las aplicaciones prácticas basadas en software es normalmente la modificación de un conjunto de datos administrado por un tercero. Un ejemplo de tales aplicaciones prácticas basadas en software es en particular la realización de transacciones electrónicas, por ejemplo transacciones bancarias, por Internet. En la ejecución de aplicaciones prácticas basadas en software, en lo que sigue denominadas aplicaciones, intercalando una comunicación entre un equipo terminal y un servidor, existe la necesidad de proteger los correspondientes enlaces de comunicación contra manipulaciones de terceros. Esto es especialmente importante en la ejecución de aplicaciones en forma de transacciones electrónicas por Internet.

En el estado actual de la técnica se conocen distintos procedimientos para la protección contra la manipulación de transacciones. En la ejecución electrónica de transacciones bancarias se emplea especialmente el procedimiento PIN (NÚMERO DE IDENTIFICACIÓN PERSONAL)/TAN (NÚMERO DE AUTENTICACIÓN DE TRANSACCIÓN) en diferentes expresiones. En éste, un usuario inicia sesión con un PIN en el servidor de su banco por medio de su navegador y, mediante un enlace de datos correspondiente, que preferentemente está protegido criptográficamente, introduce los datos de la transacción a realizar. En el procedimiento TAN sencillo, el usuario recibe previamente una lista de números TAN de varios dígitos, estando los números TAN depositados también en el servidor del banco. Para concluir una transacción, el usuario debe introducir un número TAN correspondiente aún no utilizado de la lista. A continuación, el servidor del banco comprueba si el TAN es válido, es decir si procede de la lista del usuario y aún no ha sido utilizado por el usuario. Si es éste el caso, el servidor realiza finalmente la transacción bancaria correspondiente.

En un perfeccionamiento del procedimiento TAN antes mencionado, el, así llamado, procedimiento iTAN (TAN INDEXADO), la lista de números TAN que tiene presente el usuario está indexada. Para aumentar la seguridad se pide al usuario que, para concluir la transacción, introduzca un TAN con un número índice específico. Por consiguiente, un agresor que tenga un número TAN de la lista debe eventualmente efectuar múltiples intentos para realizar una transacción, hasta que finalmente el servidor pida el TAN con el índice del que dispone el estafador. Limitando correspondientemente el número de entradas erróneas puede aumentarse adecuadamente la seguridad.

En otra forma de realización de un procedimiento TAN electrónico, el, así llamado, procedimiento mTAN (TAN MÓVIL), el TAN a introducir no se le transmite al usuario previamente en forma de una lista, sino que el servidor envía el TAN como mensaje SMS (SERVICIO DE MENSAJE CORTO) a un equipo de radiotelefonía móvil personal del usuario. Para confirmar la transacción, el usuario introduce, mediante la interfaz de usuario del ordenador en el que está haciendo uso de la banca por Internet, el TAN transmitido a su equipo de radiotelefonía móvil, que se le muestra en la pantalla del equipo. Este procedimiento ofrece ventajas adicionales, ya que un agresor debe, mediante un software malintencionado correspondiente, conseguir control tanto sobre el ordenador en el que se está haciendo uso de la banca a distancia como sobre el teléfono móvil del usuario. Sin embargo, este procedimiento presenta la desventaja de que al introducir el TAN se producen retardos causados por el envío del SMS con el TAN al teléfono móvil. Además, con la transmisión del SMS se producen costes adicionales para el usuario, ya que por lo general las tasas por el envío del SMS se cargan al usuario.

El documento WO96/00485 A2 describe un procedimiento para la autenticación de un usuario en el acceso a un servicio prestado electrónicamente mediante un terminal, que se basa en el mismo principio que el procedimiento mTAN antes mencionado. Aquí se transmite al usuario, a través de un equipo personal separado, en particular un teléfono móvil, un código de autenticación proporcionado por una central de servicio que el usuario presenta al terminal, el cual lo envía a su vez a la central de servicio, donde se compara con el código de autenticación originalmente transmitido. En caso de coincidencia, el usuario obtiene el acceso a los servicios deseado.

Por el documento WO 95/19593 A1 y el documento WO 99/44114 A1 se conocen otras soluciones tipo mTAN basadas en el mismo principio, en las que, en particular mediante una red de radiotelefonía móvil, se transmite a un teléfono móvil un código de autenticación que lleva a una indicación en el mismo, que es introducida por el usuario en un terminal o en un PC. Ésta y las soluciones tipo mTAN antes mencionadas presentan las mismas ventajas y desventajas que el procedimiento mTAN. En particular ocasionan costes adicionales.

El documento DE 10 2004046847 A1 revela un procedimiento para la realización de una transacción que se lleva a cabo mediante una tarjeta chip, un PC y un servidor. Partiendo del PC se transmiten datos de transacción por una parte mediante un primer enlace de datos a un servidor y por otra parte mediante un segundo enlace de datos a la tarjeta chip. Mediante un tercer enlace de datos, el servidor envía además datos de autenticación a la tarjeta chip. La tarjeta chip lleva a cabo comprobaciones de seguridad con los datos obtenidos y visualiza datos contenidos en los datos de autenticación para que sean comprobados por un usuario. El procedimiento ofrece una gran seguridad,

pero presupone una visualización absolutamente digna de confianza. Ésta puede ponerse a disposición en un lector de tarjetas adecuado, pero ocasiona entonces un gasto adicional correspondiente. En una variante, el servidor envía los datos de autenticación parcialmente a un teléfono móvil, en cuya pantalla se reproducen datos contenidos en los datos de autenticación para que sean comprobados por un usuario. En caso favorable, el usuario transmite mediante el PC a la tarjeta chip una información de autenticación contenida en los datos de autenticación. Dado que una pantalla de teléfono móvil puede considerarse como digna de confianza, la variante aumenta aun más la seguridad. Sin embargo, requiere la disponibilidad y el uso de una red de radiotelefonía móvil. Debido a ello, por una parte se limita la aplicabilidad del procedimiento y por otra parte el uso de la red de radiotelefonía móvil ocasiona esfuerzo y gastos.

En la publicación WO 2008/046575 A1 se describe un procedimiento para ejecutar una aplicación por medio de un soporte de datos portátil, en el que la aplicación se ejecuta por medio de un primer y un segundo equipo terminal intercalando el soporte de datos. El procedimiento puede emplearse en particular también para la realización de transacciones bancarias electrónicas. La comunicación aquí llevada a cabo tiene lugar siempre intercalando el soporte de datos portátil. En el procedimiento, los datos de transacción se introducen en primer lugar mediante el primer equipo terminal, siendo el primer equipo terminal en particular un ordenador personal. A continuación se transmiten los datos al soporte de datos portátil, que los transfiere a un segundo equipo terminal, por ejemplo a un teléfono móvil. La transacción debe ser entonces autorizada por un usuario mediante una introducción en el segundo equipo terminal, transmitiéndose acto seguido los datos de transacción del soporte de datos a un servidor, que realiza la transacción.

En la publicación US 2003/0087601 A1 se describe la utilización de un testigo (token) de seguridad con dos interfaces para la transmisión de datos protegida entre un teléfono móvil y un PC. El testigo se comunica aquí con el teléfono móvil mediante una interfaz sin contacto, basada por ejemplo en Bluetooth o infrarrojos, y con el PC mediante una interfaz con contacto.

El objetivo de la invención es crear un procedimiento para ejecutar una aplicación por medio de un soporte de datos portátil, que permita fácilmente un intercambio de datos seguro durante la ejecución de la aplicación entre los componentes que participan en la aplicación.

Este objetivo se logra mediante el procedimiento según la reivindicación 1 o el soporte de datos portátil según la reivindicación 15. En las reivindicaciones dependientes se definen perfeccionamientos de la invención.

En el procedimiento según la invención para ejecutar la aplicación se utiliza un soporte de datos portátil personal que comprende dos interfaces de comunicación separadas. En el procedimiento, en primer lugar un usuario, mediante un primer equipo terminal, transmite a un servidor, a través de un primer enlace de datos entre el primer equipo terminal y el servidor, datos de entrada especificados que, por ejemplo, han sido introducidos mediante una interfaz de usuario correspondiente del primer equipo de entrada. Los datos de entrada están previstos aquí para el procesamiento por parte de la aplicación. A continuación, el servidor, mediante un segundo enlace de datos entre el servidor y el soporte de datos, que previamente se había conectado al primer equipo terminal mediante la primera interfaz de comunicación, transmite datos de autenticación para la autenticación de la aplicación a partir de los datos de entrada recibidos en el servidor. Por último, el soporte de datos envía los datos de autenticación al segundo equipo terminal a través de un tercer enlace de datos, mediante la segunda interfaz de comunicación. Al confirmar el usuario los datos de autenticación mediante el primer o el segundo equipo terminal, se transmiten al servidor datos de confirmación correspondientes mediante, al menos el primer o el segundo enlace de datos, ejecutando acto seguido el servidor la aplicación. Si los datos de autenticación se confirman mediante el primer equipo terminal, los datos de confirmación se transmiten al servidor, en particular a través del primer enlace de datos. Si los datos de autenticación se confirman mediante el segundo equipo terminal, los datos de confirmación se transmiten al servidor preferentemente a través del tercer y el segundo enlace de datos.

Aquí y en lo que sigue debe entenderse por un primer o un segundo o un tercer enlace de datos respectivamente un enlace de datos en el que está establecido un canal de datos continuo, de manera que durante el funcionamiento normal no se produce ninguna modificación de los datos transmitidos entre los dos componentes situados en los extremos del enlace de datos. Es decir que, siempre que haya componentes técnicos intercalados en la transmisión de datos, tienen únicamente una función de transferencia y no sirven para alterar o modificar los datos. En la transmisión de los datos a través del segundo enlace de datos, el primer equipo terminal, al que se conecta el soporte de datos, actúa en particular puramente de nodo de transferencia para transferir datos entre el soporte de datos y el servidor. Así pues, los enlaces de datos pueden calificarse también de enlaces de datos directos entre los componentes situados en los extremos respectivos del enlace de datos.

El procedimiento según la invención ofrece como ventaja que durante la ejecución de la aplicación participan una pluralidad de componentes en forma de un servidor, un primer equipo terminal y un segundo equipo terminal, así como un soporte de datos portátil. Esto dificulta la posibilidad de manipulaciones, ya que para un ataque de nivel crítico para la seguridad han de intervenirse, o se ha de influir en, varios componentes. Además, el procedimiento según la invención ofrece como ventaja que no se transporta a través del soporte de datos la totalidad de los datos a transmitir, sino únicamente datos de autenticación o, en caso dado, datos de confirmación, de manera que en la transmisión de datos puede utilizarse un soporte de datos con una funcionalidad sencilla. El procedimiento según la

invención resulta fácil de realizar, ya que para su preparación debe ponerse a disposición únicamente un soporte de datos configurado correspondientemente, mientras que todos los demás componentes están disponibles sin más. También se conocen ya en principio soportes de datos portátiles adecuados con dos interfaces de comunicación separadas.

El procedimiento según la invención se utiliza preferentemente para ejecutar aplicaciones a través de Internet, de manera que el primer y/o el segundo enlace de datos comprenden preferentemente un enlace de datos a través de Internet. Se logra una seguridad muy alta si para el primer o el segundo enlace de datos se emplean enlaces de datos protegidos criptográficamente, por ejemplo basados en el protocolo de codificación SSL/TLS, suficientemente conocido ya en el estado actual de la técnica.

En otra forma de realización especialmente preferida se utiliza como segundo enlace de datos un enlace de datos con intercalación de una interfaz con contacto como primera interfaz de comunicación, por ejemplo la interfaz USB, suficientemente conocida ya en el estado actual de la técnica. A diferencia de esto, para el tercer enlace de datos se utiliza preferentemente un enlace de datos mediante una interfaz sin contacto como segunda interfaz de comunicación, en particular una interfaz NFC de corto alcance (NFC = Near Field Communication [comunicación de campo cercano]) y/o una interfaz Bluetooth. Mediante la utilización de interfaces de corto alcance se reduce aun más el peligro de una manipulación de los datos transmitidos. En caso dado es además posible proteger el tercer enlace de datos criptográficamente, por ejemplo utilizando el protocolo SSL/TLS anteriormente mencionado.

El procedimiento según la invención puede emplearse en un primer o un segundo equipo terminal cualquiera, habiendo de entenderse por equipo terminal un equipo que soporta los correspondientes enlaces de datos anteriormente definidos. Es decir que el primer equipo terminal hace posible una comunicación a través de la primera interfaz de comunicación y el segundo equipo terminal hace posible una comunicación a través de la segunda interfaz de comunicación. Los equipos terminales presentan aquí una interfaz de usuario, a través de la cual el usuario puede comunicarse con el equipo. El primer equipo terminal es preferentemente un ordenador o computadora, en particular un ordenador personal. Por regla general, un ordenador personal presenta una interfaz de usuario de fácil manejo en forma de un teclado y una pantalla de gran tamaño, lo que tiene como ventaja que el usuario puede introducir los datos muy cómodamente. En cambio, el segundo equipo terminal es preferentemente un equipo móvil, por ejemplo un teléfono móvil, que un usuario lleva por lo general siempre consigo. El segundo equipo terminal dispone, como el primero, de una interfaz de usuario con medios de salida, preferentemente en forma de un *display* o pantalla, así como un dispositivo de introducción de datos en forma de un teclado. Además de la realización como teléfono móvil, el segundo equipo terminal puede estar configurado también como un ordenador portátil, un PDA y similares.

En una forma de realización especialmente preferida, el soporte de datos portátil es una tarjeta chip o un testigo (token). Un testigo es un componente de hardware que forma parte de un sistema para la identificación o autenticación de un usuario. Un testigo puede estar configurado aquí en particular como una tarjeta chip. Como tarjetas chip se emplean preferentemente las, así llamadas, tarjetas de interfaz dual, que tienen tanto una interfaz con contacto como una interfaz sin contacto, que en el procedimiento según la invención se emplean como primera y segunda interfaz de comunicación.

Un campo de aplicación especialmente preferido del procedimiento según la invención es la realización de una transacción electrónica, en particular la realización de operaciones bancarias electrónicas. Como datos de entrada se transmiten a través del primer enlace de datos preferentemente datos de transacción destinados a especificar la transacción a realizar, por ejemplo datos correspondientes relativos al beneficiario de una transferencia bancaria y el importe a transferir.

En una variante del procedimiento propuesto se transmite una identificación, como datos de autenticación, a través del segundo y el tercer enlace de datos, transmitiéndose además de la identificación preferentemente también un resumen de los datos de aplicación recibidos por el servidor. En el caso de uso de la realización de una transacción electrónica, la identificación es en particular un número TAN para la autenticación de la transacción, como ya se mencionaba al principio.

En otra variante del procedimiento según la invención, la identificación se muestra al usuario en el segundo equipo terminal, y en particular la identificación se muestra al usuario visualmente en la pantalla del equipo terminal. El usuario confirma los datos de autenticación introduciendo mediante el primer equipo terminal la identificación mostrada. La identificación introducida se transmite como datos de confirmación, a través del primer enlace de datos, al servidor, que ejecuta la aplicación si la identificación recibida coincide con la identificación enviada originalmente por él a través del segundo enlace de datos.

En otra variante del procedimiento según la invención, la confirmación de los datos de autenticación por parte del usuario se realiza mediante una introducción en el segundo equipo terminal, transmitiéndose acto seguido datos de confirmación al servidor a través del tercer y el segundo enlace de datos. Esta variante tiene como ventaja que el usuario ya no tiene que introducir ningún dato en el primer equipo terminal. En particular es posible asegurar, mediante un software adecuado, que el usuario sólo tenga que introducir en el segundo equipo terminal una tecla de

confirmación predeterminada, de manera que puede prescindirse por completo de la introducción de un TAN por parte del usuario.

En otra forma de realización preferida del procedimiento según la invención, la aplicación se ejecuta por medio de una rutina de software almacenada en el soporte de datos portátil, comprendiendo en este caso dicho soporte de datos una memoria de masa correspondiente para guardar la rutina de software. El usuario puede arrancar la rutina de software tras la conexión del soporte de datos al primer equipo terminal a través de la primera interfaz de comunicación. De este modo se hace posible para un usuario ejecutar la aplicación en cualesquiera primeros equipos terminales con el entorno al que está acostumbrado.

Además del procedimiento anteriormente descrito, la invención se refiere a un soporte de datos portátil, en particular a una tarjeta chip, que comprende una primera interfaz de comunicación y una segunda interfaz de comunicación, estando el soporte de datos preparado para llevar a cabo cualquier variante del procedimiento según la invención antes descrito.

A continuación se describen detalladamente ejemplos de realización de la invención por medio de la figura adjunta.

La figura 1 muestra una representación esquemática de las etapas llevadas a cabo en una forma de realización del procedimiento según la invención y de los componentes utilizados para ello.

Para la siguiente descripción de la invención se toma por base una forma de realización en la que la aplicación ejecutada es la realización segura de una transacción por Internet. Los componentes empleados comprenden un soporte de datos portátil personal 1, un, así llamado, testigo, con dos interfaces de comunicación 101, 102 independientes entre sí. En el ejemplo de realización, el testigo 1 está configurado como una tarjeta chip o una tarjeta inteligente (*smartcard*). Aquí se utiliza ventajosamente una, así llamada, tarjeta de interfaz dual, que presenta por una parte una interfaz de comunicación con contacto 101 y por otra parte una interfaz de comunicación sin contacto 102. La interfaz con contacto 101 puede estar configurada por ejemplo como una interfaz USB según la norma ISO 7816. En el ejemplo de realización de la figura 1, la interfaz sin contacto 102 es una interfaz para la comunicación NFC (NFC = Near Field Communication [comunicación de campo cercano]), con la que es posible intercambiar datos a corto alcance sin contacto mediante campos electromagnéticos de alta frecuencia. La interfaz sin contacto 102 se basa aquí en la norma ISO 14443. Aunque la utilización de una interfaz sin contacto y una interfaz con contacto es conveniente, las dos interfaces de comunicación 101, 102 pueden por supuesto estar realizadas también según otras normas o en otras combinaciones. Por ejemplo existe la posibilidad de que ambas interfaces de comunicación 101, 102 estén realizadas como interfaces sin contacto.

Otros componentes mostrados en la figura 1 son un primer equipo terminal 2 configurado como un ordenador en la forma de un PC 2 (PC = Personal Computer [ordenador personal]), un servidor 3 y un segundo equipo terminal 4 en forma de un teléfono móvil apto para NFC, es decir provisto de una interfaz NFC.

El PC 2 tiene una interfaz opuesta 201 correspondiente a la interfaz de comunicación 101 de la tarjeta inteligente 1, mediante la cual se conecta a la tarjeta inteligente 1, a través de la interfaz de comunicación 101. Además, tiene una interfaz de usuario con un teclado 22 y una pantalla 21. El PC 2 está además conectado al servidor 3 mediante una red de datos 23. En el ejemplo de realización, la red de datos 23 es Internet, pero también entran en consideración sin más otras redes, como redes privadas de acceso restringido, por ejemplo de bancos u otras organizaciones gubernamentales.

El segundo equipo terminal 4 tiene, de manera correspondiente a la segunda interfaz de comunicación 102 de la tarjeta inteligente 1, una interfaz 402 para establecer enlaces de datos a través de una vía de transmisión de datos 14 independiente de la red de datos 23. La vía de transmisión de datos 14 está configurada convenientemente en forma de una red de datos local y preferentemente está realizada en forma de una comunicación NFC. La utilización de una comunicación NFC tiene como ventaja que, debido al poco alcance de campo de la comunicación, el riesgo de interceptación durante una transmisión de datos es muy pequeño. En el ejemplo de realización, la interfaz 402 está realizada como una interfaz de comunicación NFC y la red de datos 14 como un enlace NFC. El segundo equipo terminal 4 dispone además, como el primero, de una interfaz de usuario con medios de salida 41, preferentemente en forma de un *display* o una pantalla, así como un dispositivo de introducción de datos en forma de un teclado 42. La tarjeta inteligente 1 está conectada al segundo equipo terminal 4, es decir al teléfono móvil 4, mediante la interfaz de comunicación 102 a través la vía de transmisión de datos separada 14, es decir el enlace NFC. Para aumentar la protección, la transmisión de datos entre la tarjeta inteligente 1 y el teléfono móvil 4 puede realizarse además de manera codificada.

El fin del procedimiento es la ejecución de una aplicación, explicándose el procedimiento a modo de ejemplo en la realización de una transacción bancaria mediante banca por Internet. Para realizar tal transacción, en primer lugar un usuario inicia sesión con su PC 2 mediante su navegador en el servidor 3 de su banco, de manera que se establece un enlace de datos D1 entre el PC 2 y el servidor del banco 3 a través Internet. Aquí se establece en particular un enlace de datos protegido criptográficamente por medio del suficientemente conocido protocolo SSL/TLS.

Para realizar la transacción a través del servidor del banco 3, el usuario introduce en el navegador del PC 2 mediante la interfaz de usuario, es decir mediante un teclado en combinación con una pantalla, datos de entrada especificados, es decir datos de transacción. Los datos de transacción pueden tratarse por ejemplo de datos bancarios de un beneficiario de una transferencia, una cantidad a transferir y un concepto. Los datos de transacción introducidos se transmiten al servidor mediante el primer enlace de datos D1.

Para confirmar los datos de transacción introducidos es necesaria la presentación, por parte del usuario, de una identificación secreta específica de transacción que esté asignada de manera inequívoca a esta transacción y basada en los datos de transacción transmitidos. La identificación, por ejemplo un TAN, la pone a disposición el servidor 3 y debe transmitirse al usuario. Con este fin, el usuario conecta la tarjeta inteligente 1, mediante la interfaz de comunicación 101, a la interfaz opuesta correspondiente 201 del PC 2. Acto seguido se establece otro enlace de datos protegido D2, mediante la misma red de datos 23 a través de la cual se estableció el primer enlace de datos D1, en el ejemplo de realización a través de Internet, entre la tarjeta inteligente 1 y el servidor 3. El PC 2 implicado en el segundo enlace de datos protegido actúa aquí únicamente de *router (dispositivo encaminador)*, que sólo transfiere datos, sin modificarlos. Para conseguir esto y para proteger el enlace de datos D2 se emplea preferentemente de nuevo una codificación basada en el protocolo SSL/TLS. La codificación del segundo enlace de datos D2, tiene la ventaja de que un software malintencionado presente en el PC 2 no puede ni interceptar esta conexión ni manipular de manera encauzada los contenidos que circulen por la misma.

A través del segundo enlace de datos D2, el servidor del banco 3 envía después una identificación correspondiente, o sea por ejemplo un TAN, a la tarjeta inteligente 1. Junto con la identificación, el servidor del banco 3 transmite a la tarjeta inteligente 1 además convenientemente un resumen de los datos de transacción recibidos previamente a través del primer enlace de datos D1.

A continuación, la tarjeta inteligente 1 transmite al teléfono móvil 4 perteneciente al usuario la identificación y, si está presente, el resumen de los datos de transacción, por medio de la segunda interfaz 102. Con este fin, la tarjeta inteligente 1 establece, mediante la segunda interfaz de comunicación 102, a través de la vía de transmisión de datos separada 14 configurada como comunicación NFC, un tercer enlace de datos sin contacto D3 con el teléfono móvil 4. Acto seguido, la tarjeta inteligente 1 transmite los datos al teléfono móvil 4 a través de este tercer enlace de datos sin contacto D3. A continuación, el usuario puede comprobar los datos de transacción en la pantalla 41 del teléfono móvil 4 para, en caso dado, detectar errores por él introducidos o manipulaciones realizadas durante la transmisión e interrumpir la transacción. En la pantalla se muestra al usuario además la identificación, o sea por ejemplo el TAN, para la transacción.

Si los datos de transacción visualizados en la pantalla del teléfono móvil 4 son correctos, el usuario puede introducir como confirmación en la página de Internet correspondiente del servidor del banco 3, mediante el navegador del PC 2, la identificación visualizada en el teléfono móvil 4, o sea por ejemplo el TAN, transmitiéndose acto seguido la identificación al servidor 3 a través del enlace de datos D1. Una vez que el servidor 3 establece la coincidencia entre la identificación previamente enviada a través del enlace de datos D2 con la identificación ahora recibida a través del enlace de datos D1, el servidor 3 ejecuta definitivamente la aplicación deseada, en el ejemplo de realización la transacción electrónica. El usuario obtiene un acuse de recibo correspondiente a través de la ventana del navegador.

Al igual que en procedimiento mTAN ya conocido, en el que el TAN se transmite al teléfono móvil mediante SMS, la seguridad del procedimiento según la invención se basa en que para un agresor es muy difícil manipular dos equipos terminales independientes, o sea por ejemplo no sólo un ordenador personal 2, sino además un teléfono móvil 4. En el procedimiento según la invención la seguridad es además mayor, porque se emplea como componente adicional una tarjeta inteligente 1 asignada al usuario. Además, el procedimiento descrito tiene la ventaja de que la identificación, o sea el TAN, no llega al teléfono móvil 4 mediante el envío de un SMS, y por lo tanto mediante una red de datos adicional, de manera que no se ocasionan gastos adicionales para el usuario y/o el operador del servidor por el uso de una segunda red de datos. Más bien se utiliza sólo una única red de datos y se realiza una conexión adicional por medio de un soporte de datos portátil personal que, mediante una interfaz de comunicación adicional, hace accesible un enlace de datos local, existente de todos modos, con un segundo equipo terminal, también existente de todos modos. El procedimiento aquí descrito puede además llevarse a cabo con mayor rapidez, ya que no se da el retardo temporal habitualmente existente en el envío de SMS hasta la recepción del SMS, de manera que el usuario puede concluir la transacción más rápidamente.

El procedimiento descrito por medio de la figura 1 puede ampliarse y complementarse adecuadamente. Así, la tarjeta inteligente 1 puede contener adicionalmente una memoria de masa en la que esté almacenado un software correspondiente para la realización de las operaciones bancarias por Internet. Este software puede entonces arrancarse una vez conectada la tarjeta inteligente 1 mediante la primera interfaz 101 al PC 2 y permite al usuario visualizar su entorno de trabajo acostumbrado también en otros PC 2 que no utilice regularmente para realizar operaciones bancarias por Internet. Además, para procesar los datos de transacción recibidos en el teléfono móvil 4 puede utilizarse una aplicación separada, en lugar del software ya existente en el teléfono móvil. Con tal aplicación existe por ejemplo la posibilidad de que la transacción no se confirme ya introduciendo un TAN correspondiente en el PC 2, sino pulsando el usuario una tecla o una combinación de teclas correspondiente en su teléfono móvil 4. En este caso se suprime la necesidad de escribir un TAN.

El procedimiento anteriormente descrito tiene además como ventaja que a través de la tarjeta inteligente 1 sólo circula información relacionada con el TAN. Por lo tanto, el software presente en la tarjeta inteligente 1, puede presentar una funcionalidad pequeña, ya que en esencia pasa datos al teléfono móvil 4. Para ello sólo es necesario también efectuar unas modificaciones insignificantes en las páginas de Internet del servidor del banco 3. Al transmitirse los datos de autenticación, el servidor 3 debe únicamente saber que ha de enviar los datos de transacción y un correspondiente TAN a la tarjeta inteligente 1. Al mismo tiempo, también existe en caso dado la posibilidad de que puedan realizarse a través del servidor 3 tanto transacciones con listas TAN usuales transmitidas previamente al usuario como transacciones intercalando la tarjeta inteligente 1. Según esta variante, el servidor 3 únicamente ha de comprobar si el usuario que ha iniciado sesión en el mismo utiliza el procedimiento TAN usual mediante una lista o la transmisión del TAN a través de la tarjeta inteligente 1. En el primer caso el servidor 3 pide un TAN correspondiente de la lista y en el segundo caso el servidor 3 transmite un TAN a la tarjeta inteligente 1.

REIVINDICACIONES

1. Procedimiento para ejecutar una aplicación por medio de un soporte de datos portátil (1), comprendiendo el soporte de datos una primera interfaz de comunicación (101) y una segunda interfaz de comunicación (102) y siendo necesaria para ejecutar la aplicación una comunicación con un servidor (3), en el que:
- se establece un primer enlace de datos (D1) entre un primer equipo terminal (2) y el servidor (3) mediante una red de datos (23),
- un usuario transmite al servidor (3) mediante el primer equipo terminal (2), a través del primer enlace de datos (D1), datos de entrada especificados para el procesamiento por parte de la aplicación;
- se conecta el soporte de datos (1) al primer equipo terminal (2) mediante la primera interfaz de comunicación (101) y se establece un segundo enlace de datos (D2) entre el soporte de datos (1) y el servidor (3) a través de la red de datos (23),
- a través del segundo enlace de datos (D2) se transmiten, entre el servidor (3) y el soporte de datos (1), datos de autenticación para la autenticación de la aplicación a partir de los datos de entrada del servidor (3);
- se establece un tercer enlace de datos (D3) entre el soporte de datos (1) y un segundo equipo terminal (4) mediante la segunda interfaz de comunicación (102),
- el soporte de datos (1) transmite los datos de autenticación al segundo equipo terminal (102) a través del tercer enlace de datos (D3);
- el segundo equipo terminal (4) da salida a datos contenidos en los datos de autenticación para que sean comprobados por el usuario;
- en caso de confirmación de los datos de autenticación por parte del usuario mediante el primer o el segundo equipo terminal (2, 4), se transmiten datos de confirmación al servidor (3) mediante, al menos, el primer o el segundo enlace de datos (D1, D2), ejecutando acto seguido el servidor (3) la aplicación.

2. Procedimiento según la reivindicación 1, caracterizado porque el primer y/o el segundo enlace de datos (D1, D2) comprende un enlace de datos por Internet, en particular un enlace de datos protegido criptográficamente.

3. Procedimiento según la reivindicación 1 o 2, caracterizado porque el segundo enlace de datos (D2) es un enlace de datos con intercalación de una interfaz con contacto como primera interfaz de comunicación (101), en particular una interfaz USB.

4. Procedimiento según una de las reivindicaciones precedentes, caracterizado porque el tercer enlace de datos (D3) es un enlace de datos por medio de una interfaz sin contacto como segunda interfaz de comunicación (102), en particular una interfaz NFC y/o una interfaz Bluetooth.

5. Procedimiento según una de las reivindicaciones precedentes, caracterizado porque el tercer enlace de datos (D3) está protegido criptográficamente.

6. Procedimiento según una de las reivindicaciones precedentes, caracterizado porque como primer equipo terminal (2) se emplea un ordenador, en particular un ordenador personal.

7. Procedimiento según una de las reivindicaciones precedentes, caracterizado porque como segundo equipo terminal (4) se emplea un equipo terminal móvil, en particular un teléfono móvil.

8. Procedimiento según una de las reivindicaciones precedentes, caracterizado porque como soporte de datos portátil (1) se emplea una tarjeta chip y/o un testigo (token).

9. Procedimiento según una de las reivindicaciones precedentes, caracterizado porque la aplicación es una transacción electrónica, en particular una transacción bancaria electrónica.

10. Procedimiento según la reivindicación 9, caracterizado porque como datos de entrada se transmiten a través del primer enlace (D1) datos de transacción destinados a especificar la transacción a realizar.

11. Procedimiento según una de las reivindicaciones precedentes, caracterizado porque a través del segundo y el tercer enlace de datos (D2, D3) se transmite, como datos de autenticación, una identificación, transmitiéndose además de la identificación preferentemente un resumen de los datos de entrada recibidos en el servidor (3).

12. Procedimiento según la reivindicación 11, caracterizado porque la identificación se muestra al usuario en el segundo equipo terminal (4), confirmando el usuario los datos de autenticación mediante la introducción a través del primer equipo terminal (2) de la identificación mostrada y transmitiéndose la identificación introducida como datos de confirmación, a través del primer enlace de datos (D1), al servidor (3), que ejecuta la aplicación si la identificación recibida coincide con la identificación enviada originalmente a través del segundo enlace de datos (D2).

13. Procedimiento según una de las reivindicaciones precedentes, caracterizado porque la confirmación de los datos de autenticación por parte del usuario, se realiza mediante una entrada en el segundo equipo terminal (4),

transmitiéndose acto seguido datos de confirmación al servidor (3) a través del tercer y el segundo enlace de datos (D3, D2).

14. Procedimiento según una de las reivindicaciones precedentes, caracterizado porque la aplicación se ejecuta por medio de una rutina de software que está almacenada en el soporte de datos portátil (1) y que el usuario puede arrancar tras la conexión del soporte de datos (1) al primer equipo terminal (2) a través de la primera interfaz de comunicación.

15. Soporte de datos portátil, en particular testigo (token) o tarjeta chip, con una primera interfaz de comunicación (101) y una segunda interfaz de comunicación (102), estando el soporte de datos (1) preparado para ejecutar un procedimiento según una de las reivindicaciones precedentes.

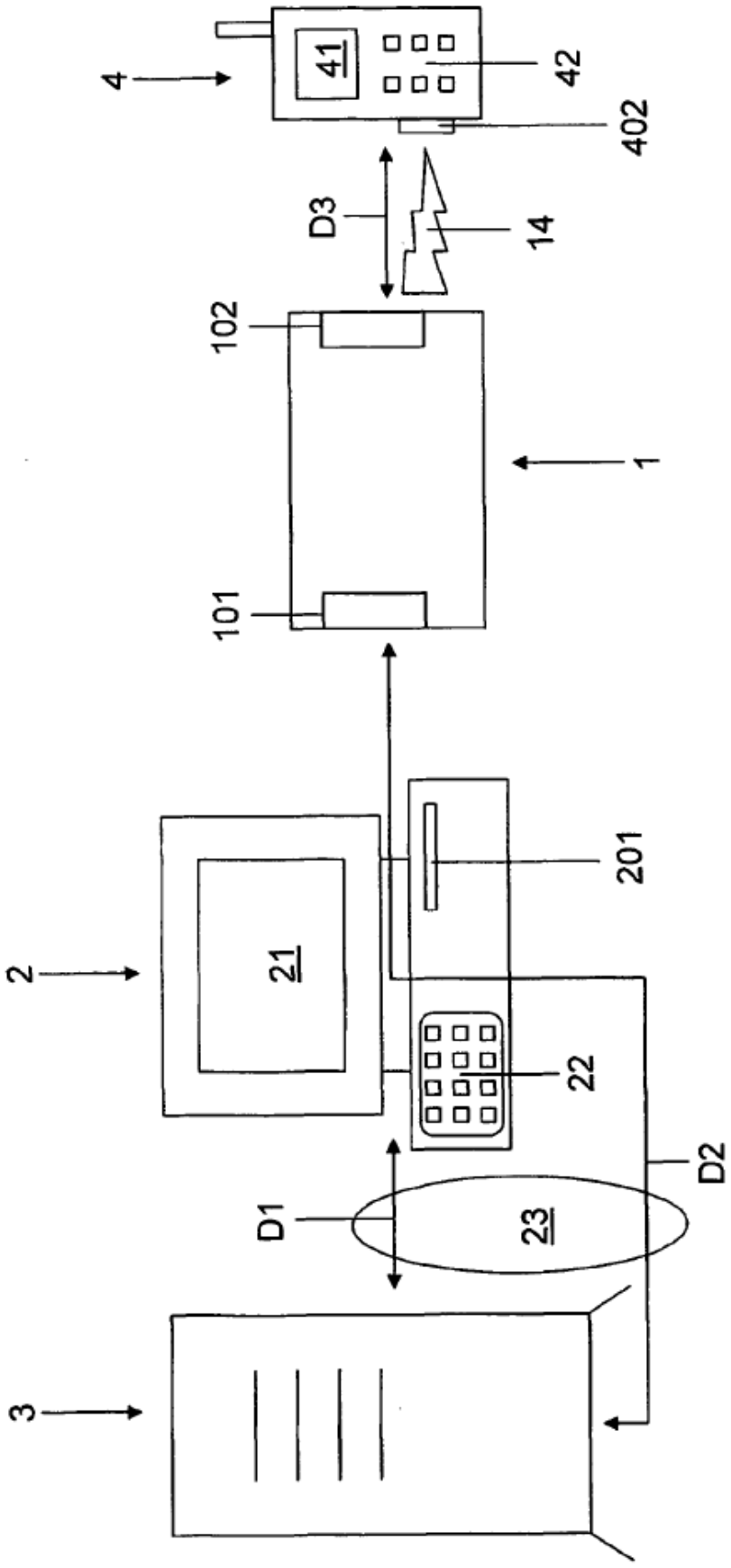

Fig. 1

REFERENCIAS CITADAS EN LA DESCRIPCIÓN

La lista de referencias citada por el solicitante lo es solamente para utilidad del lector, no formando parte de los documentos de patente europeos. Aún cuando las referencias han sido cuidadosamente recopiladas, no pueden excluirse errores u omisiones y la OEP rechaza toda responsabilidad a este respecto.

Documentos de patente citados en la descripción

- WO 9600485 A2 **[0006]**
- WO 9519593 A1 **[0007]**
- WO 9944114 A1 **[0007]**
- DE 102004046847 A1 **[0008]**
- WO 2008046575 A1 **[0009]**
- US 20030087601 A1 **[0010]**