(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 396 965**

(51) Int. CI.:

G06F 21/00 (2006.01)
G07F 7/10 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **30.04.2003 E 03008899 (1)**

(97) Fecha y número de publicación de la concesión europea: **03.10.2012 EP 1365363**

(54) Título: **Procedimiento para la realización de una transacción de datos por medio de un dispositivo de transacción que comprende un componente principal y un componente auxiliar separable**

(30) Prioridad:

02.05.2002 DE 10219731

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
01.03.2013

(73) Titular/es:

GIESECKE & DEVRIENT GMBH (100.0%)
PRINZREGENTENSTRASSE 159
81677 MÜNCHEN, DE

(72) Inventor/es:

PUMBERGER, GÜNTER

(74) Agente/Representante:

DURÁN MOYA, Luis Alfonso

DESCRIPCIÓN

Procedimiento para la realización de una transacción de datos por medio de un dispositivo de transacción que comprende un componente principal y un componente auxiliar separable

La invención parte de un dispositivo de transacciones del tipo indicado en la reivindicación principal. Este dispositivo es descrito, por ejemplo, en la publicación “Geldinstitute 1-2/97”, página 88 a 89. De acuerdo con dicha publicación para la generación de una firma electrónica digital se dispone un sistema seguro, cerrado, el cual está dotado de un aparato de lectura con el formato de una tarjeta PC, así como una llamada Smartcard, es decir, tarjeta inteligente, o sea una tarjeta de plástico que tiene las dimensiones de un talonario para cheques dotada de un microprocesador. Utilizado en un PC o en un terminal de ordenador, el dispositivo constituido a base de un aparato de lectura y una tarjeta inteligente, sirve para la identificación del usuario, así como para la codificación de informaciones. En especial, el aparato de lectura sirve para la preparación de una firma digital por la realización de un procedimiento de codificación asimétrico. La clave secreta del usuario utilizada para ello, está dispuesta en la tarjeta inteligente.

El anteriormente mencionado dispositivo de transacción presenta una elevada seguridad contra el “espionaje” no deseado de la realización de la transferencia y, por lo tanto, contra falsificaciones indeseadas. El dispositivo de transacción está destinado, por lo tanto, para la realización de transacciones críticas en cuanto a seguridad. Un punto débil en cuanto a su manipulación lo constituye de todos modos el interfaz serie con respecto a la tarjeta inteligente. Cuanto mayor es la cantidad de datos a manipular por la tarjeta inteligente, mayor es el tiempo necesario para el intercambio de datos con el aparato de lectura. En relación con utilizaciones críticas en cuanto a seguridad, se observa el desarrollo de cantidades de datos cada vez mayores. Esto es válido, por ejemplo, para la clave utilizada o en especial para certificados para claves abiertas, que son utilizadas en un procedimiento de codificación asimétrico. Para el usuario de un dispositivo de transacciones, pueden resultar de ello tiempos de espera no deseables.

El concepto de firma digital se describe en múltiples publicaciones, entre otras en el “Handbuch der Chipkarten”, W. Rankl, W. Effing, 3ª Edición 1999, página 197 y siguientes (“Manual de las tarjetas de chip”). Una parte del concepto de firma digital es, según dicho documento, la preparación de un certificado administrado por un llamado centro de garantía (“Trustcenter”) que contiene la clave abierta que corresponde a la clave secreta del usuario.

El documento WO 00/28493 A1 describe un procedimiento para la generación de una firma en un conjunto de datos de usuario con ayuda de una tarjeta de chip, que codifica de forma simétrica los datos de usuario que se le han enviado y facilita el resultado a un terminal de ordenador. El resultado será finalmente combinado con el conjunto de datos del usuario.

Por el documento US 5.677.955 A se conoce un procedimiento para la transferencia electrónica de valores con utilización de tarjetas de firma que, con utilización de procedimientos asimétricos, generan firmas digitales. Las claves abiertas necesarias para la realización del procedimiento pueden estar almacenadas en estaciones de trabajo que están asociadas a las tarjetas de firma.

El documento EP 588 339 A2 da a conocer un procedimiento para la realización de un proceso de conteo asegurado, mediante una tarjeta de chip, con utilización de una técnica de codificación asimétrica. La tarjeta de chip y un terminal de tarjetas asociado a la misma se verifican mutuamente con ayuda de un par de claves asimétricas.

El documento WO 98/25220 describe la realización de una transacción de conteo electrónica asegurada con ayuda de una tarjeta de firma que genera una firma concatenada con utilización de técnicas de codificación asimétrica.

El documento US 6.021.202 A describe un procedimiento para la transmisión de informaciones críticas en cuanto a seguridad a través de una red electrónica, con utilización de tarjetas de firma.

Es un objetivo de la invención dar a conocer un procedimiento para la realización de una transacción de datos que es realizable mediante un dispositivo de transacción de seguridad con elevada velocidad.

Este objetivo se consigue mediante un procedimiento que posee las características de la reivindicación principal. El procedimiento según la invención, se basa en el concepto de que las transacciones parciales, que serán llevadas a cabo mediante los componentes separables en forma de un soporte de datos portátil con un dispositivo procesador, contendrán habitualmente para cada realización sucesiva operaciones de asociación repetidas sin variación con una codificación y/o la realización de una firma, en las que los elementos secundarios de datos que no son críticos en cuanto a seguridad son elaborados en forma de un código abierto y/o uno o varios certificados. De acuerdo con la invención, la realización de estas operaciones de asociación estará separada en los componentes principales en forma de un aparato de lectura. De este modo, para la primera realización de una transacción parcial se transferirán los elementos secundarios de datos necesarios para ello a los componentes principales y se almacenarán en los mismos. Para la siguiente realización sucesiva de la misma transacción parcial, el componente principal conduce la operación de asociación con acceso a los elementos secundarios de datos almacenados. Este procedimiento, según la invención tiene la ventaja de que los elementos secundarios de datos no deben ser transferidos cada vez desde el

elemento auxiliar al elemento principal.

A causa del tiempo de transferencia ahorrado de este modo, el tiempo global para la realización de la transacción, se puede reducir. Desaparecen los tiempos de espera para el usuario, o bien, como mínimo, se reducen.

Una ventaja específica del procedimiento de la invención es que se puede realizar directamente mediante componentes conocidos.

En una disposición ventajosa, el procedimiento contiene medidas que aseguran que un elemento de datos secundario necesario para la operación de asociación realizada por el componente principal presenta la versión más actualizada correspondiente. Esto permite, modificar los elementos secundarios de datos del componente principal con independencia del componente principal y conduce, por lo tanto, a mejoras adicionales de la seguridad de manipulación de las transacciones a realizar.

La actualización de los elementos secundarios de datos, tiene lugar ventajosamente en base a la entrada de una actuación predeterminada, por ejemplo, con separaciones temporales predeterminadas, o mediante una señal de inicio generada por un usuario.

En una utilización preferente, el procedimiento de la invención sirve para la realización de aplicaciones PKI (Public Key Infrastructure) (Infraestructura de claves públicas) en ordenadores domésticos (PC) con utilización de tarjetas de chip. Las tarjetas de chip facilitan, en este caso, entre otros, firmas digitales. Mediante el almacenamiento de los elementos de datos secundarios en el PC del usuario se puede compensar de manera eficaz la velocidad de transferencia, habitualmente lenta, entre la tarjeta de chip y el lector de tarjetas.

Haciendo referencia a los dibujos se describirá de manera más detallada una realización de la invención.

En los dibujos:

La figura 1: muestra la constitución básica de un dispositivo para la realización del procedimiento,

La figura 2: muestra un diagrama de flujo de la realización de una transacción.

La figura 1 muestra la estructura básica de un dispositivo apropiado para la realización de un procedimiento de transacción. Comprende una instalación de proceso de datos -10-, un componente principal -20- asociado a la instalación de proceso de datos -10-, así como, un componente auxiliar separado -40-, que está asociado nuevamente al componente principal -20-. El componente principal -20- y el componente auxiliar -40- constituyen un dispositivo de transacciones -18-.

La estructura mostrada sirve para la realización, como mínimo, de una aplicación que contiene una transacción de datos incorporada, la cual será realizada por el dispositivo de transacciones. La aplicación adopta forma de un programa de aplicación con el que de manera autónoma o con la actuación de un usuario se procesarán datos. Son ejemplos de utilizaciones la realización de correos electrónicos o la realización de transacciones bancarias mediante el ordenador doméstico de un usuario. Mediante una transacción de datos incorporada, o bien una transacción incorporada se comprenderán procesos de datos que son realizados desde el punto de vista organizativo y/o técnico por un dispositivo separado de transacciones -18-. Un ejemplo típico de una transacción incorporada son operaciones relevantes en cuanto a seguridad, que son llevadas a cabo por componentes específicos especializados para ello.

Como instalación de proceso de datos -10- se considerará cualquier dispositivo deseado que es apropiado para la realización de programas de aplicaciones. Habitualmente, contiene los elementos básicos de un ordenador, es decir, en especial una unidad de proceso central para la realización de operaciones lógicas, medios de memoria para recibir programas y datos, así como, un interfaz de usuario -11- con medios para la reproducción y la introducción de datos mediante el usuario. En la práctica, la instalación de proceso de datos -10- puede ser, por ejemplo, un ordenador doméstico accesible solamente por un usuario único o un terminal libremente accesible, tal como se encuentran, por ejemplo, en bancos o en centros oficiales. Dado que la constitución y funcionamiento de estas instalaciones de proceso de datos -10- son sobradamente conocidos, no se hará referencia a ellos de forma adicional. Para la siguiente descripción se supondrá solamente que la instalación de proceso de datos -10- está preparada para la realización de, como mínimo, un programa de aplicación -12- que se designará de forma simplificada a continuación como aplicación, cuya realización contiene la realización de una transacción de datos a realizar por un dispositivo de transacciones -18-.

Para comunicación con el dispositivo de transacciones -18-, la instalación de proceso de datos -10-, contiene un interfaz -14-, puede ser de cualquier tipo deseado y puede trabajar por contacto o sin contacto.

El componente principal -20- del dispositivo de transacciones -18-, está conectado a través de un interfaz -24- correspondiente al interfaz -14- de la instalación de proceso de datos. De esta manera, el componente principal -20-

está preparado para la realización de, como mínimo, una transacción incorporada, en la que elabora los datos alimentados desde la instalación de proceso de datos -10-, los modifica y los devuelve a la instalación de proceso de datos -10-.

El componente principal -20- dispone para ello habitualmente, igualmente, de todos los elementos de un ordenador. De manera correspondiente, presenta una unidad de proceso central -22- que realiza, de acuerdo con un programa de trabajo, como mínimo, una transacción incorporada. Además, presenta un dispositivo de memoria -26- que está unido con la unidad de proceso central -22- y que presenta las memorias -28-, -30-, -32- para almacenamiento no volátil de datos.

En una primera memoria -28- del dispositivo de memoria -26- se encuentran los programas para el funcionamiento del componente principal -20- propiamente dicho y también para la realización de las transacciones incorporadas a realizar por el componente principal -20-. En una segunda memoria -30- se encuentran elementos secundarios de datos que se utilizarán en el ámbito de la realización de una transacción incorporada.

En los elementos de datos secundarios se trata de datos o de informaciones que son insensibles contra espionaje y que están asociados en el ámbito de una transacción incorporada mediante una operación conocida, no crítica en cuanto a seguridad, preferentemente lineal, con los datos de la transacción. Un elemento de datos secundario podría ser, por ejemplo, un certificado sobre una clave pública que está introducida en un conjunto de datos de una transacción.

En una tercera memoria -32- se han dispuesto características de compensación, que corresponden a los elementos secundarios de datos y que posibilitan la comprobación de la actualidad de los elementos secundarios de datos dispuestos en la memoria -30-. Como característica de compensación, puede servir en una realización especialmente simple, un número sucesivo. Además, se toman en consideración como característica de compensación otras muchas características, así como, otras características almacenadas de manera fija en el componente auxiliar -40-, tal como un número de serie, un número de identidad del componente auxiliar, una información sobre el propietario de un componente auxiliar o una fecha de evento asociada a un componente auxiliar, igual que características variables, determinadas de forma dinámica, tales como un número de sucesos, una marca horaria, una suma de comprobación constituida mediante otras de las características antes mencionadas o un valor “hash“ constituido mediante otras características. En la utilización de características de compensación variables dinámicas, se puede prever que su cálculo tiene lugar en el componente principal -20-.

Además, el componente principal -20- posee un interfaz -34- para comunicación con el componente auxiliar -40-. El interfaz -34- puede ser, de modo correspondiente, de un tipo deseado y puede funcionar sin contacto o con contacto. Si el componente auxiliar -40- presenta la estructura de un soporte de datos portátil, por ejemplo en forma de una tarjeta de chip, el interfaz -34- tiene, de manera típica, la forma constructiva de un aparato de lectura habitual.

Todos los elementos de un componente principal -20- están unidos entre sí mediante uniones apropiadas de datos.

El componente principal -20- puede estar constituido como elemento de hardware independiente, que está dispuesto en una instalación de proceso de datos -10-, o puede estar asociado mediante una unión permanente apropiada. De manera alternativa, se pueden realizar elementos del componente principal -20-, de manera completa o parcial, mediante los elementos existentes en la instalación de proceso de datos -10-. Esto es válido para el dispositivo de almacenamiento -26-; que puede quedar realizado por ejemplo sobre una placa fija existente sobre la instalación de proceso de datos, pero también sobre un medio de almacenamiento separado acoplado a dicha instalación de proceso de datos. El componente principal -20- puede ser realizado de manera correspondiente parcialmente en forma de software.

El componente auxiliar -40- sirve para la realización de manera segura contra manipulaciones y contra acciones espía de operaciones sensibles dentro del marco de una transacción a realizar. Está constituido como unidad independiente separable del componente principal -20- y presenta un interfaz -44- que se corresponde con el interfaz -34- del componente principal -20-. De modo correspondiente, puede ser de tipo sin contactos o con contactos. Un elemento esencial del componente auxiliar -40- constituye un dispositivo procesador -42- que presenta los elementos esenciales de un sistema de ordenador habitual, es decir, en especial una unidad de proceso central, así como, un medio de memoria -50- para el almacenamiento no volátil de datos y programas. El componente auxiliar -40- presenta la forma de un soporte de datos portátil, preferentemente con la estructura de una tarjeta de chip. El chip comprende, en este caso, el dispositivo procesador -42-, el interfaz -44- estará constituido por una tarjeta de chip que funciona con contacto, a través del campo de contacto del chip en un tipo sin contactos a través de la bobina.

En el dispositivo de memoria -50- del dispositivo procesador -42- se encuentra el programa de trabajo para la realización de las operaciones sensibles, así como, datos fijos y variables utilizados para las mismas. Son datos fijos típicos, en este caso, por ejemplo, una clave cliptográfica para la realización de codificaciones, un número de serie asociado al componente principal -40-, un número de identificación asociado al dispositivo procesador -42-, o bien una información que designa un usuario del componente principal -40-. Los datos almacenados variables pueden

ser, por ejemplo, un número al azar, una indicación de tiempo, una suma de comprobación o un valor “hash” constituido con intermedio de múltiples datos. Básicamente, los datos introducidos en el dispositivo de memoria -50-, no son accesibles y en todo caso lo son bajo condiciones especiales, por ejemplo, después de haber realizado con éxito procesos de autentificación especiales. Se puede prever que en un dispositivo de memoria -50- se encuentren dispuestos diferentes elementos de datos secundarios asociados a diferentes componentes principales -20-.

Algunos datos introducidos en el dispositivo de memoria -50-, están destinados, no obstante, expresamente para su envío al exterior, no son secretos y, por lo tanto, son fácilmente accesibles. Estos datos se designarán en esta descripción como elementos de datos secundarios. Los datos de este tipo son una clave pública a utilizar en el ámbito de un proceso de codificación asimétrico, o bien, uno o varios certificados distintos, por ejemplo, un certificado respecto a un código público o una cadena de certificados con certificados de diferentes puntos de certificación. Los elementos secundarios de datos pueden ser además informaciones de estructura públicamente accesibles con respecto al sistema de archivo utilizado en el componente auxiliar -40-, con respecto a las aplicaciones realizables con elemento auxiliar -40- o con respecto a determinados elementos de datos existentes en el componente auxiliar -40-. Otros elementos de datos secundarios posibles son además, informaciones legibles de manera libre, por ejemplo, el nombre y dirección, por parte del propietario o del suministrador del componente auxiliar -40-.

Los elementos de datos secundarios son combinados frecuentemente mediante operaciones lineales simples, por ejemplo mediante añadidos con los datos de la transacción sin excluir en modo alguno la aplicación de operaciones complejas. Las operaciones de combinación o encadenamiento no son en sí mismas críticas en cuanto a seguridad ni secretas y pueden ser llevadas a cabo también fuera del componente auxiliar -40-.

Los elementos de datos secundarios no sensibles, son leídos regularmente antes de la realización de una transacción de manera completa o parcial. En este caso, los elementos de datos secundarios pueden tener una dimensión tal que solamente pueden ser transferidos en un tiempo detectable para el usuario que, típicamente se encuentra en un rango de unos segundos, a través de los interfaces -44-, -34- al componente principal -20-.

Mediante el procedimiento propuesto, se consigue que los elementos de datos secundarios se deban transferir de manera menos frecuente y el tiempo para la realización de una transacción incorporada disminuye de manera correspondiente.

La figura 2 muestra el funcionamiento conjunto de los elementos de la estructura mostrada en la figura 1, en la realización de una aplicación en la que se lleva a cabo una transacción incorporada mediante el dispositivo de transacción -18-.

El diagrama de flujo empieza con el inicio de la aplicación en la instalación de proceso de datos -10-, fase -100-. En la aplicación se puede tratar, por ejemplo, de la realización de un correo electrónico que finalmente es firmado con utilización de una tarjeta de chip que funciona como dispositivo auxiliar -40-.

En la etapa inicial -100-, se comprenden habitualmente, en principio, etapas de procedimiento -102- en el ámbito de la aplicación iniciada que deben ser llevadas a cabo en la instalación de tratamiento de datos -10-. En el ejemplo de la realización de un correo electrónico, éstas pueden ser por ejemplo, fases para la introducción de texto o para la realización de una comprobación de autenticidad de escritura. En la realización de la aplicación, en un punto determinado por la propia aplicación o por el usuario, tiene lugar el inicio de una transacción incorporada, que será llevada a cabo mediante el dispositivo de transacción -18-, etapa -104-.

La realización de la transacción incorporada, será realizada en primer lugar por la unidad de proceso central -22- del componente principal -20-. Después de conseguir los datos de la transacción a manipular de la aplicación -12- y de la realización correspondiente de las etapas de preparación previstas, la unidad central de proceso -22-, comprueba si los elementos de datos secundarios a manipular por el componente auxiliar -40-, los cuales deben ser combinados en el ámbito de la transacción incorporada con los datos de la transacción, se encuentran ya en la memoria -30- del componente principal -20-, etapa -106-. Esta comprobación, puede tener lugar de manera que la unidad de proceso -22- comprueba solamente en principio si existe en la memoria -32- una característica de correspondencia de ajuste correspondiente al elemento de datos secundario.

La comprobación de existencia en la etapa -106- puede tener lugar previamente a una etapa mediante la cual la unidad de proceso -22- determina si por parte del componente principal -40- se ha llevado a cabo una variación de los elementos de datos secundarios. Esta comprobación puede ser realizada mediante una correspondiente consulta simple. De manera alternativa, puede tener lugar, de manera que la unidad de proceso -22- evalúa la característica de ajuste.

Si existen los elementos de datos secundarios necesarios, la unidad de proceso central prepara los elementos de datos secundarios, etapa -128-, envía al componente auxiliar -40- los datos de transacción a manipular, etapa -130- y pone en marcha la realización de las operaciones a realizar por el componente auxiliar -40-.

El componente auxiliar -40- lleva a cabo a continuación, todas las operaciones sensibles previstas en el ámbito de la transacción incorporada, etapa -132- y envía los datos de transacción resultantes en retorno al componente principal -20-, etapa -134-. Las etapas -130- a -134- pueden ser realizadas en caso necesario varias veces una después de otra para llevar a cabo en el ámbito de una transacción incorporada diferentes operaciones sensibles previstas.

Después de conseguir los datos de transacción resultantes, la unidad central de proceso -22-, utiliza los elementos de datos secundarios preparados, y lleva a cabo la realización de la transacción incorporada, de manera que combina los datos de la transacción conseguidos del componente auxiliar -40- con los elementos de datos secundarios, etapa -136-.

Los datos de transacción procesados, de los que se dispone entonces, son enviados por el componente principal -20- mediante las interfaces -24-, -14- en retorno a la aplicación -12-, etapa -140-.

Si la comprobación realizada en la etapa -106- indica que los elementos de datos secundarios necesarios no se encuentran en la memoria -30-, el componente principal -20- requiere que el componente auxiliar -40- envíe los elementos de datos secundarios necesarios, etapa -120-. El componente auxiliar -40- lee entonces los elementos de datos secundarios solicitados de su dispositivo de memoria -50- y los envía al componente principal -20-, etapa -122-, recogiéndolos en su dispositivo de memoria -30-, etapa -124-.

Si los elementos de datos secundarios necesarios están preparados, el componente principal -20- sigue con la realización de la transacción, es decir, con la realización de las etapas -128- y -130-.

De manera ventajosa, el componente principal -20-, lleva a cabo, en conexión con la etapa -106-, antes de utilizar los elementos de datos secundarios existentes en el elemento de memoria -30-, una comprobación de si el elemento de datos secundarios es válido. Para ello, la unidad de proceso central -22- provoca que el elemento auxiliar -40-, etapa -108- lea de su dispositivo de memoria -50- una o varias características de ajuste y que las envíe al componente principal -20-, etapa -110-. Además, la unidad de proceso central -22- lee la memoria -32- de su propio dispositivo de memoria -26-, etapa -112-, para determinar de esta manera, las características de ajuste correspondientes solicitadas por el componente auxiliar -40-. En la etapa sucesiva -112- la unidad de proceso central -22- evalúa la característica de ajuste conseguida del elemento auxiliar -40- con respecto a la que se ha conseguido de la memoria -32-, etapa -114-. A efectos de simplicidad se debe considerar que la característica de ajuste se trata de un número sucesivo. La unidad central de proceso -22- comprueba entonces, si el número sucesivo leído de la memoria -32- como elemento de dato secundario coincide con aquel que le fue enviado por el elemento auxiliar -40-. En caso de coincidencia lleva a cabo la transacción incorporada con utilización del elemento de datos secundario dispuesto en la memoria -30-, etapa -130-.

Si no se corresponden las características de compensación, el correspondiente elemento secundario de la memoria -30- ya no es válido. La unidad de proceso central -22- sigue en ese caso con la etapa -120- y provoca que el elemento auxiliar -40- envíe en el momento el o los elementos de datos secundarios necesarios para la transacción incorporada.

En una variante ventajosa del procedimiento mostrado en la figura 2, la unidad central de proceso -22- solicita al componente principal -20- los elementos de datos secundarios necesarios para una transacción incorporada y las correspondientes características de compensación del componente auxiliar -40-, es decir, se realizan las etapas -120- y -108-, incluso antes de comprobar la existencia de los elementos de datos secundarios necesarios en la memoria -30-. Las solicitudes correspondientes tienen lugar, en este caso, por ejemplo, directamente después del inicio de una transacción incorporada en la etapa -104-. A pesar de la realización previa de las etapas -116-, o bien -108-, la unidad central de proceso -22- lleva a cabo la etapa -106-. Si la comprobación de existencia indica, en este caso, que en la memoria -30- se encuentran ya los elementos de datos secundarios necesarios, y éstos son válidos, se interrumpirá el proceso de petición anteriormente introducido, es decir, la realización de las etapas -120- o -108-.

Si la prueba de validez de la etapa -114- ha indicado que un elemento de datos secundario no es válido, éste será anulado por la unidad central de proceso -22-, o dotado de una anotación de falta de validez. Para el aumento de la protección contra manipulaciones o fallos funcionales, se puede prever que elementos de datos secundarios, después de haber transcurrido un periodo de tiempo predeterminado, o después de la introducción de acciones definidas, sean anulados con la independencia de su validez, o marcados como no válidos.

Se puede prever además, una anulación manual y actualización de un elemento de datos secundario por parte de un usuario. De manera ventajosa, el usuario consigue, en este caso, a través del interfaz de usuario -11- de la instalación de proceso de datos -10-, peticiones correspondientes generadas por la unidad central de proceso -22-, las cuales le conducen a realizar las necesarias acciones.

Inicialmente el usuario recibe, por ejemplo, una información sobre la falta de validez de une elemento de datos secundario, así como, la indicación de que se debe solicitar un elemento de datos secundario válido del componente auxiliar -40-. Además, recibe indicaciones para la anulación o invalidación de elementos de datos secundarios no válidos que se encuentran en la memoria -30-. Por esta razón, será conducido a poner en marcha la actualización

del elemento de datos secundario. En vez de la conducción de un diálogo del usuario sobre acciones individuales sucesivas, se puede también evidentemente prever una función de programa individual que solamente debe ser activada por el usuario. Además, se puede prever también que la anulación/actualización manual sea realizada a través de otras rutas de comunicación, por ejemplo, mediante el correo habitual. Para la protección contra manipulaciones, los elementos secundarios de datos y las características de compensación serán almacenadas en las memorias -30- ó -32- del componente principal -20-, ventajosamente de forma codificada. La codificación puede tener lugar en este caso, mediante utilización de claves generadas en el componente principal -20- y administradas también en el mismo. De manera alternativa, la codificación tiene lugar con utilización de un código preparado por el componente auxiliar -40-. Un código de este tipo, será solicitado después del inicio de una transacción introducida en la etapa -102- por la unidad central de proceso -22- del componente auxiliar -40-, en una variante adicional, la codificación tiene lugar con utilización de una clave de reunión ("session key"), que será codificada de manera correspondiente y almacenada en el dispositivo de memoria -26- del componente principal -20-. La utilización de un código de reunión es especialmente apropiado cuando éste será de todos modos generado para el intercambio de datos entre el componente principal -20- y el componente auxiliar -40-. Dado que será también almacenado en el componente auxiliar, puede actuar también como característica de compensación. Como alternativa o para mejora adicional de la protección contra manipulaciones se puede prever además, la utilización de números de comprobación, por ejemplo, en forma de valores "hash".

De acuerdo con el concepto principal, de acelerar el acceso de un componente principal -20- a un componente auxiliar -40-, de manera que elementos de datos secundarios no críticos en cuanto a seguridad utilizados en una transacción incorporada, son almacenados en el componente principal -20- teniendo lugar de esta manera el acceso a este último, la solución anteriormente descrita permite múltiples realizaciones ampliadas. Esto es válido para la estructura interna de los componentes utilizados en el sistema. De este modo, tanto el elemento principal -20- como el elemento auxiliar -40-, como también la instalación de proceso de datos -10-, pueden contener otros elementos funcionales o elementos funcionales adicionales, en las que están distribuidas de otro modo las funcionalidades descritas. Como características de compensación utilizables se pueden determinar, aparte de las indicadas, otras sin dificultad. Además, se consiguen amplias posibilidades funcionales para la manipulación de elementos de datos secundarios y características de compensación del elemento componente principal -20-. En este caso, se pueden prever en especial, otros mecanismos para evitar que elementos de datos secundarios almacenados en la memoria -30-, pero que ya no son actuales, puedan ser utilizados en una transacción incorporada. Por ejemplo, se puede prever que regularmente los elementos de datos secundarios más viejos o utilizados con menor frecuencia o escogidos de manera casual sean anulados y, a continuación, deben ser solicitados de nuevo. Es ventajoso también constituir una gestión de almacenamiento para administración específicamente de las memorias -30-, -32-. Para el control de la ocupación de las memorias se puede prever o se puede disponer prever o se puede disponer un espacio de almacenamiento máximo de manera que regularmente se anulen los elementos de datos secundarios mayores o los utilizados menos frecuentemente.

REIVINDICACIONES

1. Procedimiento para la realización de una transacción de datos dentro de una infraestructura de clave pública, por medio de un dispositivo de transacción (18), que consiste en un componente principal (20) en forma de un dispositivo de lectura y un componente auxiliar separable (40) en forma de un soporte de datos portátil con un dispositivo procesador (42), de manera que la transacción de datos comprende, como mínimo, una transacción parcial que es llevada a cabo por el componente auxiliar (40) y, que comprende una operación de combinación, que comporta una codificación y/o la formación de una firma, de manera que los datos de la transacción son combinados con un elemento de datos secundario no crítico en cuanto a seguridad, en forma de una clave pública y/o de uno o varios certificados que es almacenado en el componente auxiliar (40), **caracterizado porque** la operación de combinación en la que, el elemento de datos secundario no crítico en cuanto a seguridad es combinado con los datos de la transacción, es desplazado al componente principal (20) mediante, para la realización por primera vez de la transacción parcial, la transferencia del elemento de datos secundario utilizado al componente principal (20) y almacenándolo en el mismo y en la siguiente realización de la transacción parcial, el componente principal (20) que lleva a cabo la operación de combinación en la que el elemento secundario no crítico en cuanto a seguridad, es combinado con los datos de la transacción, mientras se accede al elemento de datos secundarios almacenados en el componente principal (20).

2. Procedimiento, según la reivindicación 1, **caracterizado porque** un elemento de datos secundario es comprobado en cuanto a validez (114), antes de ser procesado por el componente principal (20) en una operación de combinación.

3. Procedimiento, según la reivindicación 2, **caracterizado porque** la comprobación de validez es efectuada en base a una característica de comparación que es facilitada por el componente auxiliar (40).

4. Procedimiento, según la reivindicación 2, **caracterizado porque** la comprobación de validez es llevada a cabo después de que haya tenido lugar una actuación predeterminada.

5. Procedimiento, según la reivindicación 2, **caracterizado porque** la comprobación de validez es puesta en marcha por el usuario.

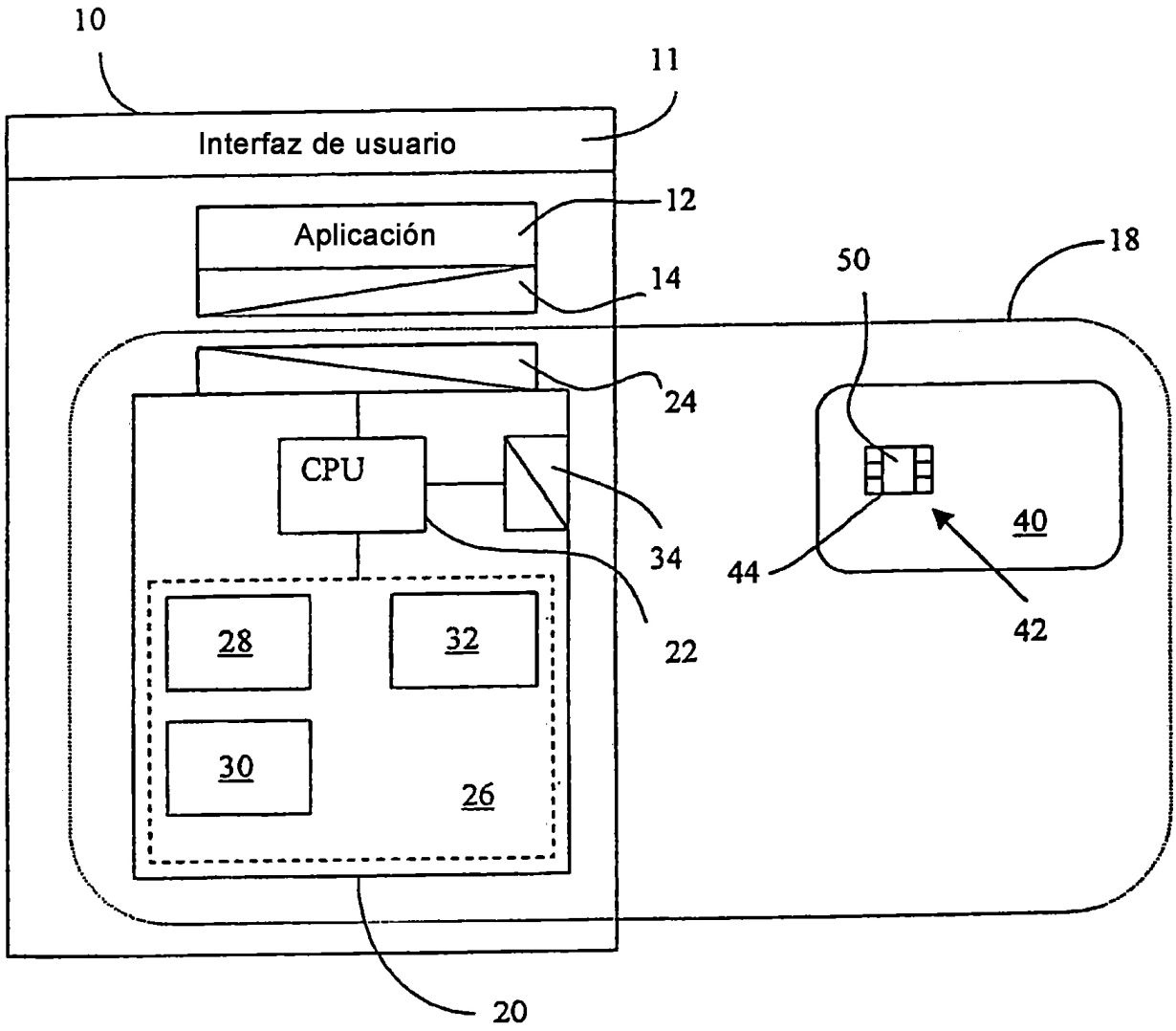
6. Procedimiento, según la reivindicación 3, **caracterizado porque** la petición de una característica de comparación es efectuada antes de llevar a cabo la comprobación de validez.

7. Procedimiento, según la reivindicación 1, **caracterizado porque** un elemento de datos secundario transferido al componente principal (20) es dispuesto en una memoria (30) del componente principal (20) de forma codificada.

8. Procedimiento, según la reivindicación 7, **caracterizado porque** la clave para llevar a cabo la codificación se pone a disposición por el componente auxiliar (40).

9. Dispositivo de transacción (18), para la realización de una transacción de datos, dentro de una infraestructura de clave pública, que consiste en un componente principal (20) en forma de un dispositivo de lectura y un componente auxiliar separable (40) en forma de soporte de datos portátil que tiene un dispositivo procesador (42), de manera que la transacción de datos comprende, como mínimo, una transacción parcial que es llevada a cabo por el componente auxiliar (40) y comprende una operación de combinación que comporta una codificación y/o la formación de una firma, de manera que se combinan datos de la transacción con un elemento de datos secundario no crítico en cuanto a seguridad, en forma de una clave pública y/o de uno o varios certificados almacenados en el componente principal (40), **caracterizado porque** el dispositivo de transacción está configurado para la operación de combinación, en la que el elemento de datos secundarios no crítico en cuanto a la seguridad, es combinado con los datos de transacción desplazados al componente principal (20), para la ejecución por primera vez de la transacción parcial, siendo transferido el elemento de datos secundario utilizado al componente principal (20) y almacenado en el mismo y cuando tiene lugar la siguiente realización de la transacción parcial, el componente principal (20) lleva a cabo la operación de combinación en la que el elemento de datos secundario no crítico en cuanto a seguridad es combinado con los datos de la transacción, mientras accede al elemento de datos secundario almacenado en el componente principal (20).

Fig. 1


10
11
Interfaz de usuario
12
Aplicación
14
18
50
24
CPU
34
40
44
42
22
28
32
30
26
20

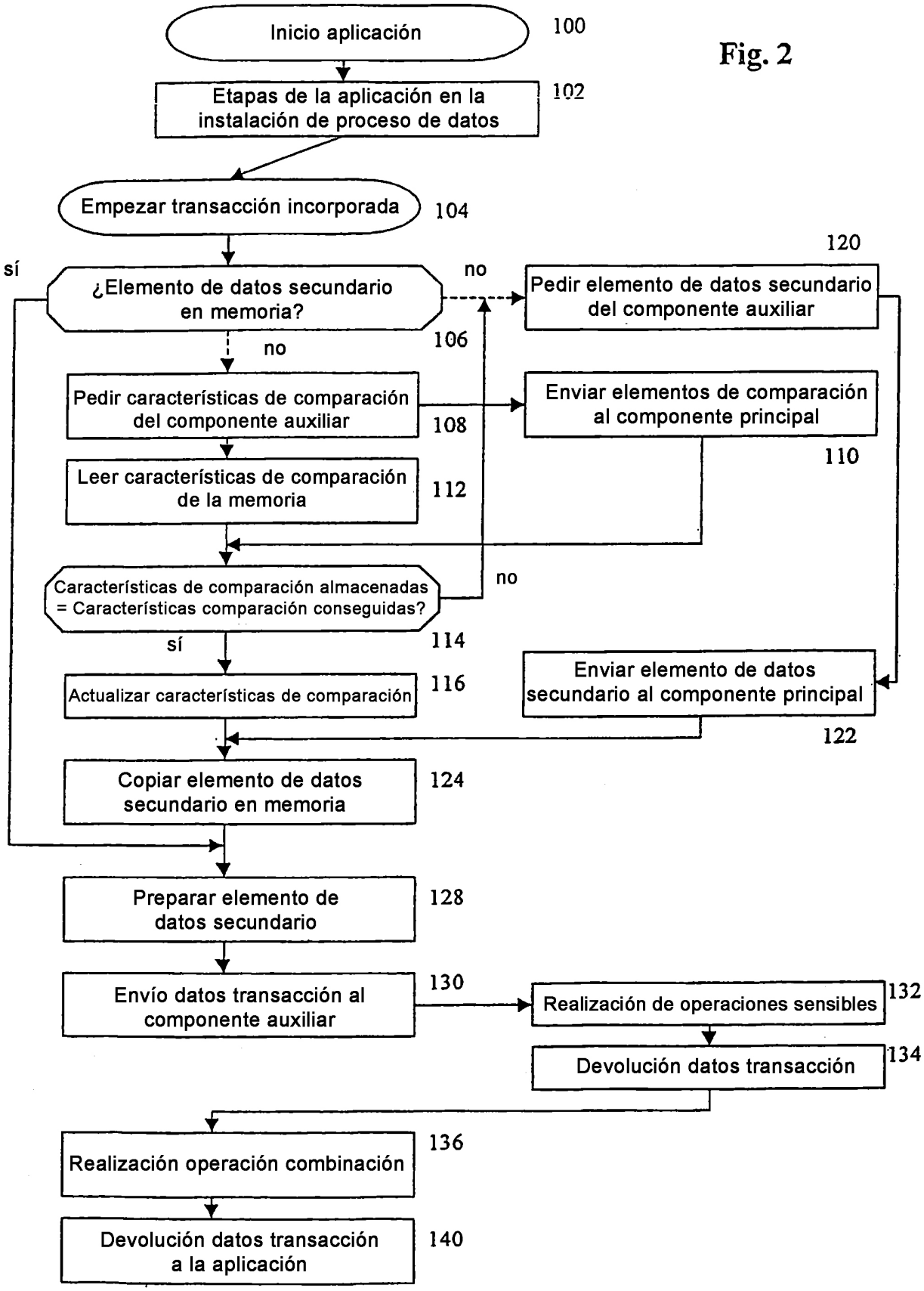

Inicio aplicación
100
Etapas de la aplicación en la instalación de proceso de datos
102
Empezar transacción incorporada
104
sí
¿Elemento de datos secundario en memoria?
no
106
120
Pedir elemento de datos secundario del componente auxiliar
no
Pedir características de comparación del componente auxiliar
108
Enviar elementos de comparación al componente principal
110
Leer características de comparación de la memoria
112
Características de comparación almacenadas = Características comparación conseguidas?
no
sí
114
Actualizar características de comparación
116
Enviar elemento de datos secundario al componente principal
122
Copiar elemento de datos secundario en memoria
124
Preparar elemento de datos secundario
128
Envío datos transacción al componente auxiliar
130
Realización de operaciones sensibles
132
Devolución datos transacción
134
Realización operación combinación
136
Devolución datos transacción a la aplicación
140

Fig. 2