(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 547 534**

(51) Int. CI.:

G06F 21/34 (2013.01)
G06F 21/84 (2013.01)
G06F 21/72 (2013.01)
G06F 21/64 (2013.01)
G06F 21/62 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **27.01.2009 E 09151451 (3)**

(97) Fecha y número de publicación de la concesión europea: **08.07.2015 EP 2088531**

(54) Título: **Procedimiento y dispositivo de firma electrónica móvil segura**

(30) Prioridad:

01.02.2008 DE 102008007367

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
07.10.2015

(73) Titular/es:

NOVOSEC AG (100.0%)
BERLINER STRASSE 44
60311 FRANKFURT AM MAIN, DE

(72) Inventor/es:

STOHN, MAIK

(74) Agente/Representante:

MORGADES MANONELLES, Juan Antonio

DESCRIPCIÓN

Procedimiento y dispositivo de firma electrónica móvil segura

La presente invención se refiere a un dispositivo personal móvil para firma electrónica segura, y al correspondiente procedimiento.

Sector de la invención

En las comunicaciones, y en especial en las comunicaciones de negocios, es frecuentemente imprescindible verificar la autenticidad de una información enviada y la identidad del ente de negocios asociado. Ello se puede conseguir con la ayuda de firmas electrónicas. El proceso de la firma electrónica comprende normalmente tres fases parciales: la transferencia de la información a firmar, preferentemente mediante una vía electrónica, la representación de la información a firmar y la generación de la firma electrónica propiamente dicha. En esta situación, se debe asegurar que la firma electrónica corresponde exactamente a la información o documento a firmar.

Por el carácter público de los canales preferentemente utilizados para el envío de informaciones, no se puede excluir que los datos enviados puedan ser vistos o incluso manipulados por terceros. De manera general, esto se soluciona mediante la codificación [1] de los datos sensibles en las redes públicas. Esto facilita, no obstante, solamente seguridad para la parte de la transferencia de la información.

Aparte de la transferencia de informaciones, existen, no obstante, otros puntos susceptibles de intrusión. Los sistemas que se utilizan para la visualización y recepción de informaciones, tales como, por ejemplo, sistemas de ordenadores o terminales, deben ser considerados de manera general como susceptible de manipulación. La existencia de lagunas de seguridad en sistemas operativos, virus, troyanos y ataques de “phishing” lo demuestran. Incluso cuando las informaciones transferidas en el envío de datos están protegidas por la codificación contra las manipulaciones, el usuario debe recibir la información en un momento determinado de forma no codificada para su elaboración o confirmación. Por lo tanto, se pueden dar posibilidades de manipulación del proceso en el caso de que el aparato de visualización o recepción de informaciones (por ejemplo, un ordenador) sea manipulado por terceros. En este caso, a pesar de la codificación de las informaciones transferidas, puede ocurrir que la información mostrada por un sistema manipulado no sea idéntica a la información realmente firmada. Esto puede tener lugar, por ejemplo, por los llamados programas troyanos, que generan en el usuario la impresión de que han comunicado con un ente de negocios asociado (por ejemplo, el banco), pero que en realidad han comunicado con/a través de un programa troyano, por lo que el troyano puede conseguir informaciones correspondientes tales como contraseñas de acceso y números de identificación (TAN).

La presente invención se refiere a un dispositivo y un procedimiento para firma digital segura. Mediante una arquitectura de nuevo tipo, se garantiza que la información mostrada corresponde también realmente a la información firmada. De esta manera, se pueden dificultar sustancialmente los intentos de manipulación con respecto a lo que ocurre en el estado de la técnica.

Estado de la técnica

A pesar de que existen múltiples aplicaciones de la firma electrónica, el estado de la técnica se explicará en base al ejemplo del pago electrónico de mercancías o servicios. La presente invención cubre esta zona de utilización, pero no está limitada a la misma.

En el pago electrónico, el usuario se debe identificar con respecto a la institución de crédito o a un proveedor de servicio. Posteriormente, se muestra el importe a pagar y, opcionalmente, otras informaciones. El usuario utiliza el proceso con la introducción de su número PIN y eventualmente un número opcional de transacción (TAN). En las nuevas arquitecturas, el usuario tiene eventualmente una tarjeta inteligente electrónica que contiene un código electrónico, codifica los mensajes electrónicos, pudiendo efectuar su firma. Frecuentemente, dichos procedimientos se basan en una “Public-Key-Infrastructure (PKI)” [2].

A continuación, se describirá el objetivo conseguido por la presente invención, en el que se explicará una posible manipulación teórica según el estado de la técnica actual.

En dispositivos de lectura de tarjetas de chip existen en la actualidad 4 tipos de seguridad, tal como se especifican en Alemania por la Autoridad Central de Crédito (“Zentralen Kreditausschuss”) (ZKA [3]) [4]:

Clase de seguridad 1	Los aparatos de esta clase no tienen ninguna característica especial de seguridad. El lector de las tarjetas actúa solamente como unidad de contacto para la tarjeta de chip.
Clase de seguridad 2	Este lector de tarjetas de chip presenta un teclado, mediante el cual se puede facilitar directamente, por ejemplo, el PIN para la Banca doméstica. De esta manera, se excluye prácticamente el descifrado del PIN (por ejemplo, mediante “Keylogger” o troyanos).
Clase de seguridad 3	Además del teclado, estos aparatos tienen una pantalla y una “inteligencia” incorporada, con la que es posible, por ejemplo, el pago con tarjetas de dinero por internet.
Clase de seguridad 4	Igual que la clase 3, no obstante, el terminal presenta una identidad propia que no puede ser manipulada. Esto se garantiza mediante una segunda tarjeta inteligente que es utilizada en el terminal.

Otras explicaciones con respecto a las clases de aparatos para dispositivos lectores de tarjetas de chip se encuentran también en las citas bibliográficas [5, 6]. En ellas, se puede leer que, en un teclado y pantalla de la clase de seguridad 3, como mínimo temporalmente, los terminales de las tarjetas de chip son controlados exclusivamente por el firmware y no existe ninguna posibilidad de interpretar las informaciones introducidas por el teclado mediante el sistema de computador que está conectado. El lector de tarjetas de chip no envía directamente a la tarjeta de chip petición alguna, sino que las comprueba en primer lugar. Exactamente, ahí se encuentra un punto débil: todos los dispositivos de lectura de tarjetas de chip que se basan en esta norma son controlables con un correspondiente código unitario para el firmware. Si este es conocido, todos los dispositivos de lectura de esta clase se deben considerar inseguros.

En la figura 1, se ha mostrado esquemáticamente un terminal de cliente de tarjeta inteligente de la clase de seguridad 3 para mostrar el estado de la técnica. El usuario 1 puede leer informaciones de la pantalla 7 y llevar a cabo introducciones de datos mediante la unidad de introducción de datos 5, que puede comprender un teclado y/o una pantalla táctil. La tarjeta inteligente 9 es controlada por el firmware 11. El firmware autoriza solamente los accesos a la tarjeta inteligente 9, que han sido comprobados con un código genérico para esta clase de terminal. La interfaz de comunicación 13 constituye una interfaz con el asociado de la comunicación (por ejemplo, el banco). La tarjeta inteligente 9 será introducida para diferentes procesos de firma en diferentes terminales 3.

Cuando un intruso consigue manipular el firmware 11 a través de la interfaz de comunicación 13 o del dispositivo mediante una modificación física, se pueden mostrar al usuario 1 contenidos distintos a los que él ha firmado realmente. Dado que además existen múltiples terminales constructivamente similares con idéntico firmware e idénticos algoritmos de preparación, en caso de que un intruso conozca el código para el firmware, todos los terminales de este tipo se deben considerar como comprometidos.

Muchos dispositivos de lectura de tarjetas inteligentes facilitan además la posibilidad de actualización del firmware o bien de la retrocarga de códigos para la comprobación de transacciones. Este mecanismo facilita por sí mismo de manera correspondiente la posibilidad de manipulación.

Además, en muchos casos, el dispositivo de lectura de tarjetas permanece en el lugar del pago y puede ser, por lo tanto, manipulado sin conocimiento del usuario. Incluso cuando el dispositivo de lectura de tarjetas permanece sellado en situación original, una posible manipulación podrá ser difícilmente advertida por parte del usuario.

Una manipulación del firmware y/o del hardware del dispositivo de lectura podría posibilitar, por lo tanto, que la información mostrada en la pantalla no sea la información firmada por el usuario.

En la literatura, se han dado a conocer muchos otros dispositivos para solucionar este problema que, no obstante, están afectados de inconvenientes específicos. Los terminales de tarjeta inteligente de la clase de seguridad 4 tienen, en general, otra tarjeta inteligente que, representa la identidad del correspondiente terminal [5]. En este caso, la complicación de la gestión es elevada, puesto que esta identidad debe ser gestionada adicionalmente a la del usuario y debe ser registrada. Además, el terminal de este tipo permanece en el distribuidor y podría, por lo tanto, ser manipulado sin conocimiento del usuario.

La solicitud de patente [7] describe la combinación inseparable de una tarjeta inteligente con una pantalla, pero se refiere ante todo a la integración de una pantalla en una tarjeta flexible y no se refiere a detalles para aumentar la seguridad del proceso de firma. En la solicitud de patente [8] para la firma segura, no se da a conocer de qué forma se puede evitar la manipulación de lo que representa el aparato de la firma. La solicitud de patente [9] describe la combinación de un indicador con una tarjeta inteligente, de manera que la unidad en su conjunto adopta un formato de tarjeta de chip. Un conmutador aplicado no se utiliza, no obstante, para la firma, sino para mostrar las informaciones almacenadas, tales como, por ejemplo, el saldo. En otra solicitud de patente [10] se describe una

tarjeta de chip con pantalla integrada y un teclado, que se puede utilizar para el movimiento de pagos. No obstante, en este documento no se facilitan detalles sobre la arquitectura de información con la que se debe proteger la tarjeta contra manipulaciones de terceros. En la comunicación de prensa [11] de la Sociedad Fraunhofer, se presenta una arquitectura que soluciona el problema de la manipulación del PC utilizado y sus periféricos. Esta disposición, al contrario de la presente invención, no es apropiada para la utilización en móviles. En la solicitud de patente [12] se describe un sistema portátil para la firma de informaciones. En este caso, el contenido principal se refiere, no obstante, a la codificación de informaciones en señales acústicas y a la implementación dentro de un aparato de radio móvil. En el escrito [13] se da a conocer igualmente una disposición y un método para la firma móvil. Este sistema funciona, no obstante, con un teléfono móvil y con utilización de redes telefónicas, lo cual muestra una limitación. Un teléfono móvil moderno es un sistema que puede ser manipulado mediante software; existen ya virus y programas agresivos para teléfonos móviles. En este sentido, un aparato de dicho tipo no es digno de confianza y se debe clasificar de manera similar a un PC. La solución del objetivo principal de la presente invención, es decir, la garantía de la correspondencia del mensaje mostrado y el mensaje firmado no se da a conocer [13].

El documento WO 02/091669 A1 muestra un procedimiento para la firma de documentos, que se visualizan sobre una pantalla del aparato, y que se deben firmar, pudiendo ser destacado si los documentos han sido modificados.

El documento EP 1055 989 muestra un ordenador reforzado, cuyo procesador de la pantalla es inmune contra modificaciones no autorizadas.

El documento EP 1 035 461 muestra un procedimiento, en el que se aseguran ordenadores, que están conectados mediante una interfaz, antes de la introducción de software no autorizado. El documento WO 99/08415 muestra un dispositivo para conseguir firmas seguras que mediante un aparato externo, en el que se deben autorizar estas firmas antes de su impresión.

El documento EP 1054 364 A2 muestra un procedimiento en el que se aumenta la seguridad en la realización de firmas digitales. En este caso, existe un íntimo acoplamiento entre el dispositivo de visualización y tarjeta de chip, cuya comunicación está protegida mediante firmas.

Descripción de la invención

Es un objetivo de la presente invención el aseguramiento de la correspondencia del mensaje mostrado y del mensaje firmado.

La presente invención se refiere a un dispositivo y a un procedimiento para la firma segura, realizado mediante un aparato para autorizar informaciones o bien para liberar transacciones, que se designará también a continuación como dispositivo de firma.

El dispositivo o aparato de firma contiene una tarjeta inteligente, una unidad enchufable para la misma y que está dotado, como mínimo, de una pantalla. La tarjeta inteligente puede estar incorporada también como módulo funcional inseparable en el aparato de firma.

Es un objetivo de la invención excluir la diferencia entre la información mostrada (por ejemplo, la información de la transacción) y la información realmente firmada en el aparato de firma. Ello se consigue de acuerdo con la invención mediante una combinación de dos medidas técnicas:

En primer lugar, el hardware es construido de manera tal que la visualización del aparato muestra solamente contenidos que están firmados para la correspondiente e individual identidad de diferentes usuarios. Esto se consigue por el hecho de que el aparato de firma muestra solamente las informaciones apropiadas para la tarjeta inteligente utilizada y, por lo tanto, para el usuario específico. Esto puede ser garantizado por el hecho de que el ente de comunicación asociado del dispositivo de firma (por ejemplo, la institución de crédito) envía una información que puede ser decodificada solamente por la tarjeta inteligente del usuario real, la cual es mostrada en la pantalla bajo control directo o con la colaboración de la tarjeta inteligente. Una característica determinante del dispositivo es que el aparato de firma muestra solamente informaciones conseguidas del exterior, cuando estas han sido autorizadas por la tarjeta inteligente específica del usuario.

Esta primera medida solamente no sería suficiente puesto que, en este caso, sería posible además una manipulación del hardware del aparato de firma y, de este modo, de la información visualizada y firmada. Por esta razón, de acuerdo con la invención, se combina con una segunda medida: la conexión entre la tarjeta inteligente y la pantalla, que muestra informaciones de la transacción no se separará habitualmente y se encuentra bajo el control del usuario. El usuario no tiene interés alguno en la manipulación de sus propias transacciones. La interfaz entre tarjeta inteligente y pantalla solamente puede ser manipulada de forma muy difícil por un tercero, puesto que en su conjunto no es accesible por parte del distribuidor o vendedor del servicio u otros terceros. De acuerdo con la invención, la tarjeta inteligente y la pantalla constituyen una unidad que tiene el usuario bajo su control y que puede utilizar en diferentes lugares. Si bien la tarjeta inteligente, por ejemplo para la primera utilización, es dispuesta en el

aparato de firma, de manera habitual permanece para otros procesos sucesivos de firma apareada con el aparato de firma.

En caso de que un tercero consiguiera, a pesar de todo, manipular la interfaz entre la tarjeta inteligente y la pantalla y además llegar a conseguir la posesión del número PIN, entonces puede tener lugar solamente una utilización no apropiada con la propia identidad del usuario (una tarjeta inteligente propia). Al contrario de ello, en el estado actual de la técnica, en un aparato de lectura estacionario sería posible por parte del distribuidor, mediante manipulación de un único hardware (pantalla y teclado de introducción del PIN), la manipulación de transacciones de diferentes identidades de usuario.

La realización de acciones de firma y, en especial, la visualización de informaciones de transacción se puede llevar a cabo solamente de manera correspondiente en la presente invención cuando el ente asociado en la comunicación (por ejemplo, la institución de crédito) dispone del código adecuado para la tarjeta inteligente específica.

El aparato de firma correspondiente de la invención contiene, como mínimo, una pantalla y una tarjeta inteligente. Además, puede existir una posibilidad de introducción de datos para el número PIN en el aparato de firma. Esto puede ser realizado en forma de un teclado o también mediante una pantalla sensible al tacto (pantalla táctil) o por un lector de huellas digitales. El número PIN será verificado con ayuda de la tarjeta inteligente. La introducción del número PIN puede tener lugar igualmente a través de componente de hardware a través de un sistema principal conectado (por ejemplo, un PC). Este sistema debe ser considerado, en general, como inseguro, siendo teóricamente posible un ataque al PIN a través de un programa troyano. Un ataque de este tipo no sería, no obstante, satisfactorio, puesto que para la realización de una acción de firma se requiere simultáneamente la disposición física de la tarjeta inteligente.

Descripción de las figuras:

A continuación, se describirán brevemente las figuras:

Se muestra:

La figura 1, la construcción esquemática de un terminal de cliente con tarjeta inteligente de la clase de seguridad 3 para ilustración del estado de la técnica

La figura 2, la estructura de un aparato de firma, de acuerdo con la invención;

Las figuras 3a, 3b, una vista en planta y la figura 3b una vista en alzado de un dispositivo para la implementación de la presente invención;

Las figuras 4a y 4b, otros ejemplos de realización.

Descripción de las formas de realización:

La estructura de un aparato de firma según la invención se ha mostrado en la figura 2. La tarjeta inteligente 9 está conectada directamente con el puerto de comunicación 13 y permanece de forma habitual en el aparato de firma 15. La arquitectura está implementada de forma tal que la información es mostrada en la pantalla 7, solamente en el caso de que ha sido autorizada por la tarjeta inteligente 9 mediante un código específico para el correspondiente usuario. La manipulación directa de la pantalla 7 o de la unidad de introducción de datos 5 sin autorización por la tarjeta inteligente, queda excluida.

Otra característica del dispositivo de la invención es un mecanismo de firma que se puede utilizar de manera especialmente simple y segura. En el aparato de firma se encuentra un pulsador como parte del dispositivo de introducción de informaciones 5, de manera que este aparato puede ser controlado exclusivamente por el usuario del aparato de firma y en ningún caso desde el exterior. Simultáneamente, este pulsador está realizado constructivamente de forma tal que no puede ser accionado erróneamente. Preferentemente, dicho pulsador tiene solamente la misma función para la firma o autorización. Si es accionado, pone en marcha la firma o bien la confirmación de la información mostrada en este momento en la pantalla, a través del usuario con ayuda de su tarjeta inteligente. Es determinante en este caso que la operación de firma es llevada a cabo, preferentemente, solamente con un único accionamiento. En formas de realización alternativas, se pueden presionar varios pulsadores o combinaciones de los mismos.

Un aparato de lectura de clase 2 dispone, para una posibilidad de recepción segura de un PIN, de manera que la disposición técnica es de tipo tal que la manipulación o violación de los datos introducidos por el teclado queda excluida por diseño técnico del dispositivo o queda muy dificultada. Esta disposición que corresponde al estado de la técnica presenta, no obstante, un inconveniente, puesto que el teclado para la introducción del PIN y para la confirmación difícilmente puede ser construido de pequeñas dimensiones y transportable. De acuerdo con la invención, es suficiente la existencia de un elemento material o de hardware único, asegurado y no manipulable tal

como, por ejemplo, un pulsador para la autorización o firma. La introducción del PIN puede tener lugar también mediante otros aparatos de introducción de datos que, eventualmente, se deben considerar como inseguros. Si un programa troyano llegara a poseer el PIN, ello no sería suficiente. Incluso con el conocimiento y representación del PIN por un programa troyano, no puede tener lugar una utilización no autorizada, puesto que el accionamiento o manipulación del pulsador para la firma del mensaje visualizado no puede tener lugar por software sin acceso físico al aparato. La eliminación de un teclado completo para la introducción del PIN no constituye por lo tanto un riesgo de seguridad más elevado, puesto que es suficiente un único elemento de hardware físicamente no manipulable, es decir, el pulsador, para la autorización de la firma. Esta realidad posibilita la construcción de acuerdo con la invención de aparatos de firma muy pequeños, portátiles, y a pesar de ello, seguros. Mediante la miniaturización, es fácilmente realizable el transporte del aparato de firma por el usuario, y ello dificulta la manipulación del hardware dado que el aparato de firma es objeto de transporte.

Además, un proceso de firma puede ser interrumpido también de manera simple y rápida. En caso de que el aparato de firma no intercambie informaciones de forma inalámbrica, el proceso de firma puede ser interrumpido simplemente por la terminación de la conexión física (por ejemplo, por separación del puerto USB). En caso de acoplamiento inalámbrico, que es realizado preferentemente mediante una conexión inalámbrica de corto alcance, el proceso de firma puede ser interrumpido de manera correspondiente por la separación del terminal previsto para ello.

A continuación, se explicarán dispositivos y también procedimientos relacionados correspondientes a la invención a base de ejemplos. La disposición posible de la invención está constituida por un aparato de firma portátil que se describe para la autorización de procesos de pago o bien otros tipos de transacciones. La presente invención no está limitada, no obstante, a estas utilizaciones.

La figura 3a muestra una vista en planta y la figura 3b una vista en alzado lateral de un dispositivo para la implementación de la presente invención. El aparato de firma 15 presenta una pantalla 17 y un puerto de comunicación 21. En este ejemplo de realización, el puerto de comunicación está realizado en forma de interfaz USB. No obstante, son posibles también conexiones inalámbricas (IRDA, WLAN, Bluetooth, USB-Wireless) o combinaciones de conexiones por cables e inalámbricas. El puerto de comunicación 21 puede estar eventualmente protegido por una tapa de recubrimiento, que no se ha representado en la figura 3. En la vista en alzado lateral de la figura 3b, se puede apreciar la tarjeta inteligente 23. En este caso, se puede tratar de la introducción de una tarjeta inteligente, una tarjeta inteligente en la primera utilización del aparato de firma 15 instalada en su interior, o una tarjeta inteligente aplicada de manera fija en el aparato de firma. Es importante que la tarjeta inteligente para la limitación de las posibilidades de manipulación permanezca en el funcionamiento habitual dentro del aparato de firma 15.

El elemento de servicio 19 del aparato de firma sirve para el inicio simple del proceso de firma, de manera que por presionado de este elemento de servicio, realizado preferentemente en forma de pulsador, se firman las informaciones mostradas en aquel momento en la pantalla con ayuda de la identidad de usuario contenida en la tarjeta inteligente. En este caso, es importante que el hardware del elemento de servicio 19 no pueda ser manipulado desde el exterior mediante software, sino que es necesario para ello un accionamiento físico. Para conseguir este efecto, la memoria de trabajo del aparato está realizada en una forma preferente con protección de escritura, o puede estar conectada en una modalidad de protección de escritura. Para el proceso de firma, se puede utilizar una infraestructura de clave pública (“Public Key Infrastructure”) [2] de acuerdo con el estado de la técnica.

En la figura 3(a), se ha mostrado una forma de cuerpo en las proximidades del elemento de servicio o de accionamiento, que como ventaja de la disposición de la presente invención, hace impensable el accionamiento erróneo del elemento de servicio. En este ejemplo de realización, no se aprecian posibilidades de introducción de datos para el número PIN. Este puede ser facilitado mediante teclas separadas que pueden ser leídas a través del puerto de comunicación 21. Alternativamente a ello, la pantalla 17 puede estar realizada en forma de pantalla táctil, puede ser utilizada para la introducción de un número PIN o para el reconocimiento de una huella dactilar.

Otro ejemplo de realización se ha mostrado en la figura 4. La figura 4(a) muestra una vista en planta, y la figura 4(b) una vista en alzado lateral de un dispositivo para la implementación de la presente invención. El aparato de firma 15 presenta una pantalla 17, que está implementada preferentemente en forma de pantalla táctil y que puede ser utilizada también para la introducción de números PIN. El elemento de accionamiento 19 pone en marcha la firma de la información mostrada en la pantalla. El aparato puede estar acoplado con el exterior con intermedio de una bobina de inducción o bien una antena 25. Esto posibilita el intercambio de datos y/o el suministro de corriente. De acuerdo con la invención, la operación de firma puede ser realizada por disposición del aparato de firma 15 sobre un lugar previsto para ello y preferentemente marcado. Esto tiene lugar mediante acoplamiento con una segunda bobina de inducción (no mostrada en la figura 4), que alimenta el aparato con energía y/o datos. El usuario puede anular en todo momento una operación de firma no deseada por retirada del aparato o bien por desacoplamiento de la bobina de inducción por retirada del aparato de firma. La función del elemento de accionamiento 19 puede ser implementada igualmente sobre la pantalla 17, cuando se trata de una versión de pantalla táctil. Tal como en el ejemplo anterior, puede tener lugar la introducción de un número PIN igualmente a través de un aparato de introducción de datos, con el que comunica el aparato de firma con intermedio de una interfaz de comunicación.

También se puede utilizar un sensor de huellas dactilares, que reconoce adicionalmente la identidad. En la vista en alzado lateral 4(b) se puede apreciar la tarjeta inteligente 23. En este caso, se puede tratar de un alojamiento para la introducción de una tarjeta inteligente, una tarjeta inteligente instalada en la primera utilización del aparato de firma 15 en el interior del mismo, o una tarjeta inteligente aplicada de manera fija en el aparato de firma. También en este ejemplo de realización, la arquitectura del aparato de firma 15 está establecida de forma tal que, solamente se muestran informaciones por la pantalla 17, que han sido autorizadas o decodificadas por la tarjeta inteligente 23.

El procedimiento se basa preferentemente en el dispositivo antes descrito. En este, el dispositivo de firma móvil según la invención será conectado en una primera fase a través de la interfaz (por ejemplo, USB) con un PC o con un terminal de pago. Estos últimos están conectados a su vez con un servidor, que recibe habitualmente las tarjetas o las transacciones bancarias en línea, o las realiza. El dispositivo de la invención será conectado a continuación, por ejemplo, a través del puerto USB con el ordenador. Además, se aplican también iniciadores o informaciones de programa en una zona de memoria de almacenamiento (que puede estar constituida en forma de disco duro o USB y puesto en marcha mediante Autostart), de manera que el dispositivo personal móvil de firma pueda recibir o bien intercambiar informaciones con el PC y/o el servidor. Mediante el añadido para Autostart los iniciadores pueden ser puestos en marcha automáticamente en la conexión por los iniciadores o bien las informaciones de programa necesarias. En un terminal de pago, el terminal detecta en base al aparato conectado de manera inmediata, que la firma ha tenido lugar a través del dispositivo objeto de la invención, y guía la comunicación correspondiente a un servidor en caso de que sea posible la comunicación directa del dispositivo de la invención con el servidor. En las variantes de banca en línea orientadas a PC, la aplicación reconoce, comunicando con un navegador interno, que se encuentra a disposición un dispositivo de firma. De esta manera se controlará, o bien de forma automática la autorización de la transacción a través del dispositivo de firma, sin necesidad de facilitar un TAN, o se preparará la selección mediante un diálogo, de manera que el usuario puede decidir en qué forma se puede autorizar la transacción. Este programa puede ser, por ejemplo, un Applet-JAVA o similar, que se carga por petición en la página de banca doméstica de internet. El usuario tiene en este caso la posibilidad de selección de si desea trabajar con el dispositivo de firma o con un TAN. Si se escoge, por ejemplo, el dispositivo de firma, las informaciones facilitadas se transmitirán al servidor. El servidor puede modificar las informaciones de manera tal que pueden ser descodificadas por la tarjeta inteligente. Esto puede tener lugar mediante una firma o mediante decodificación.

Las informaciones elaboradas y/o decodificadas de este modo serán recibidas a través del servidor en el dispositivo de firma personal móvil. Esto puede tener lugar directamente o con el intermedio del PC. Así, por ejemplo, el dispositivo objeto de la invención puede recibir los datos a través del NAT como aparato de red propio. De manera alternativa, también puede enviar el PC los datos a través del iniciador instalado o bien a través del programa instalado al dispositivo objeto de la invención.

El dispositivo recibe o bien elabora las informaciones solamente cuando las informaciones han sido correctamente decodificadas. De esta manera, se puede evitar que el dispositivo se vea dificultado o atacado por informaciones no deseadas. En caso de que las informaciones hayan sido modificadas o decodificadas correctamente, estas se mostraran en la pantalla y se esperará que tenga lugar la autorización por parte del usuario. En este caso, se mostrarán las informaciones de transacción completas. Estas comprenden, por ejemplo, el importe, la cuenta inicial y la cuenta de destino.

Después de una introducción por el usuario con intermedio de la unidad de introducción de datos tiene lugar la firma de las informaciones a través del dispositivo de firma personal móvil y, a continuación, la transmisión al servidor. En este caso, se debe tener en cuenta que la introducción solamente puede tener lugar mediante una tecla o mediante una pantalla táctil, o bien un lector de huellas digitales.

Los datos para las huellas digitales pueden estar integrados, por ejemplo, en la tarjeta de chip/tarjeta inteligente.

El control del dispositivo está constituido de manera tal, que las informaciones mostradas sobre la pantalla no serán firmadas, y las acciones no serán interrumpidas, cuando el dispositivo está separado de la interfaz, en especial del puerto USB.

En la forma de realización preferente, se lleva a cabo la conexión mediante una interfaz estándar-PC (USB, Fire Wire) o con intermedio de una interfaz inalámbrica, tal como Bluetooth o WLAN. En este caso, la suministro de corriente tiene lugar a través de una batería integrada, la interfaz USB/Fire Wire o por radio, por ejemplo, mediante RFID.

También el proceso de firma se interrumpirá por la separación del suministro de corriente, de manera que este suministro de corriente puede estar implementado por una conexión eléctrica directa o por un acoplamiento inductivo, de manera que se puede utilizar este tipo opcional de acoplamiento también para el envío de datos.

Además, la introducción de un número PIN para la autorización de un proceso de firma puede no formar parte del aparato de firma propiamente dicho, sino que puede tener lugar mediante un aparato conectado o en disposición de comunicación. La autorización tiene que tener lugar, no obstante, en el propio aparato.

Referencias Bibliográficas

[1] Steve Burnett, Stephen Paine: "RSA Security's Official Guide to Cryptography", Mcgraw-Hill Professional (2002)
[2] Carlisle Adams, Steve Lloyd:"Understanding Public-Key Infrastructure: Concepts, Standards, Deployment Considerations", Macmillan Technical Publishing (1999)
[3] Zentraler Kreditausschuss http://www.zentraler-kreditausschuss.de
[4] http://de.wikipedia.org/wiki/Chipkarte (Stand 21.11.2007)
[5] Kobil Systems GmbH, Worms. www.kobil.de/index.php?id=135&type=2&L=1 (Stand 21.11.2007)
[6] Initiative Geldkarte e.V. http://www.initiative-geldkarte.de/ www/de/pub/geldkarte initiative/initiative geldkarte/aktuelles/hintergr undtext chipkartenles.php (Stand 22.11.07)
[7] DE10210606, GIESECKE & DEVRIENT GMBH (2003): "Display module credit card/payment card/money payment having display module and chip module with conductor track conjugate contact zones and electronic control chip tracks connected/encapsulated"
[8] WO9908415, Siemens AG (1999), "SYSTEM FOR GENERATING ELECTRONIC SIGNATURES IN ABSOLUTE SECURITY"
[9] DE10221496, GIESECKE & DEVRIENT GMBH (2004), "Datenträger"
[10] DE10008076, FREUDENBERG CARL FA (DE), (2001), "Chipkarte"
[11] Fraunhofer Gesellschaft, Pressemitteilung 2003: "Sicheres Signierterminal nutzt PC-Peripherie", http://idw-online.de/pages/de/news59463 (Stand 23.11.2007)
[12] US2007143622, Isaac Labaton (2007), METHODS AND PORTABLE DEVICE FOR DIGITALLY SIGNING DATA
[13] DE19747603C2 Brokat GmbH, Verfahren zum digitalen Signieren einer Nachricht.

REIVINDICACIONES

1. Procedimiento para la firma electrónica segura de información sobre un pago o una transacción bancaria en línea, que se origina desde un servidor, con un dispositivo de firma personal móvil (15), en el que el procedimiento comprende:

- como mínimo, una pantalla (7) para la visualización de informaciones,
- una tarjeta inteligente integrada (9) o un medio de conexión para una tarjeta inteligente, que está diseñado de manera tal que la tarjeta inteligente está integrada permanentemente, de manera que el dispositivo móvil personal, la tarjeta inteligente y la pantalla forman una unidad pequeña y compacta, portátil modular, que tiene bajo su control el usuario;
- una unidad de introducción de datos (5) para interacción;
- una interfaz (13), que permite una conexión desacoplable en diferentes lugares, que se puede utilizar para la firma de información en diferentes lugares, sobre la cual se reciben las informaciones a firmar, y sobre la cual se devuelven las informaciones firmadas,
- con un controlador, configurado y adaptado para visualizar solamente información en las pantallas, que ha sido decodificada por la tarjeta inteligente y, por lo tanto, está destinada a un ID específico de usuario, que está determinado por la tarjeta inteligente, refiriéndose una acción de firma a la información visualizada, solicitando obligatoriamente una introducción por la unidad de introducción;
- un suministro de corriente que tiene lugar a través de la interfaz o a través de una batería integrada,

que comprende las etapas de

- conexión del dispositivo de firma personal móvil a través de la interfaz con un PC o un terminal de pago que, a su vez, están conectados con un servidor, de manera que el dispositivo personal móvil puede comprender información del servidor;
- recepción de las informaciones a firmar del pago o de la transacción bancaria en línea en el PC o el terminal de pago;
- transmisión de las informaciones al servidor, que pueden ser descodificadas por la tarjeta inteligente con el ID específico del usuario;
- envío de las informaciones codificadas a través del servidor al dispositivo de firma personal móvil;
- recepción de las informaciones codificadas a través del PC o del terminal de pago, cuando la información está codificada correctamente;
- visualizar las informaciones sobre la pantalla y esperar la autorización del usuario;
- después de una introducción por parte del usuario en la unidad de introducción de datos, firmar las informaciones para su liberación a través del dispositivo personal móvil de firma y enviar la información al servidor que ejecuta la transacción si la firma es correcta.

2. Procedimiento, según la reivindicación anterior, en el que la interfaz está conectada a un medio de comunicación, que en el lugar de realización de la acción de firma permite una conexión directa o indirecta del dispositivo mencionado con un canal de comunicación tal como, por ejemplo, internet, una conexión telefónica, o una conexión de tipo celular, para obtener la información a firmar del servidor.

3. Procedimiento, según una o varias de las reivindicaciones anteriores, en el que la interfaz estándar puede estar configurada como una interfaz de PC cableado (USB, FireWire) o como una interfaz inalámbrica, tal como Bluetooth o WLAN.

4. Procedimiento, según una o varias de las reivindicaciones anteriores, en el que la unidad de introducción de datos actúa para la autorización de la firma de las informaciones visualizadas en la pantalla, consistiendo, preferentemente, en un pulsador, y que lleva a cabo una operación de firma con respecto a la información visualizada sobre la pantalla solamente con un accionamiento, y/o
en el que la unidad de introducción de datos está implementada para poner en marcha la operación de firma con ayuda de una pantalla táctil, y/o
en el que la unidad de introducción de datos está prevista para poner en marcha la operación de firma con un lector de huellas dactilares.

5. Procedimiento, según una o varias de las reivindicaciones anteriores, en el que el controlador está implementado de forma tal que la información mostrada en la pantalla no será firmada, y toda acción es anulada, cuando el dispositivo está separado de la interfaz, en particular del puerto USB,
y/o cuando se produce interrupción por fallo de suministro de corriente, en el que el suministro de corriente puede estar implementado por una conexión eléctrica directa o por acoplamiento inductivo, pudiendo ser utilizado también este último opcionalmente para la transmisión de datos.

6. Procedimiento, según una o varias de las reivindicaciones anteriores, que comprende una zona portadora de datos para un programa, iniciándose el programa cuando se establece conexión con la interfaz, de manera que tiene lugar una comunicación con un servidor a través de la interfaz mediante la red, y de manera que solamente se reciben datos tales del servidor que son decodificados por la tarjeta inteligente y, por lo tanto, están destinados a un ID de usuario específico, que está determinado por la tarjeta inteligente.

7. Procedimiento, según una o varias de las reivindicaciones anteriores, en el que la interfaz, y preferentemente el programa, están implementados de forma tal que permite una comunicación con o a través de un PC y/o un terminal de pago,
y/o de manera que el dispositivo de hardware para la introducción de un número PIN para la autorización del proceso de firma no necesita ser, en sí mismo, parte del aparato de firma móvil, sino que tiene lugar en un aparato conectado o que se encuentre en comunicación, pero la autorización deberá tener lugar en el propio aparato.

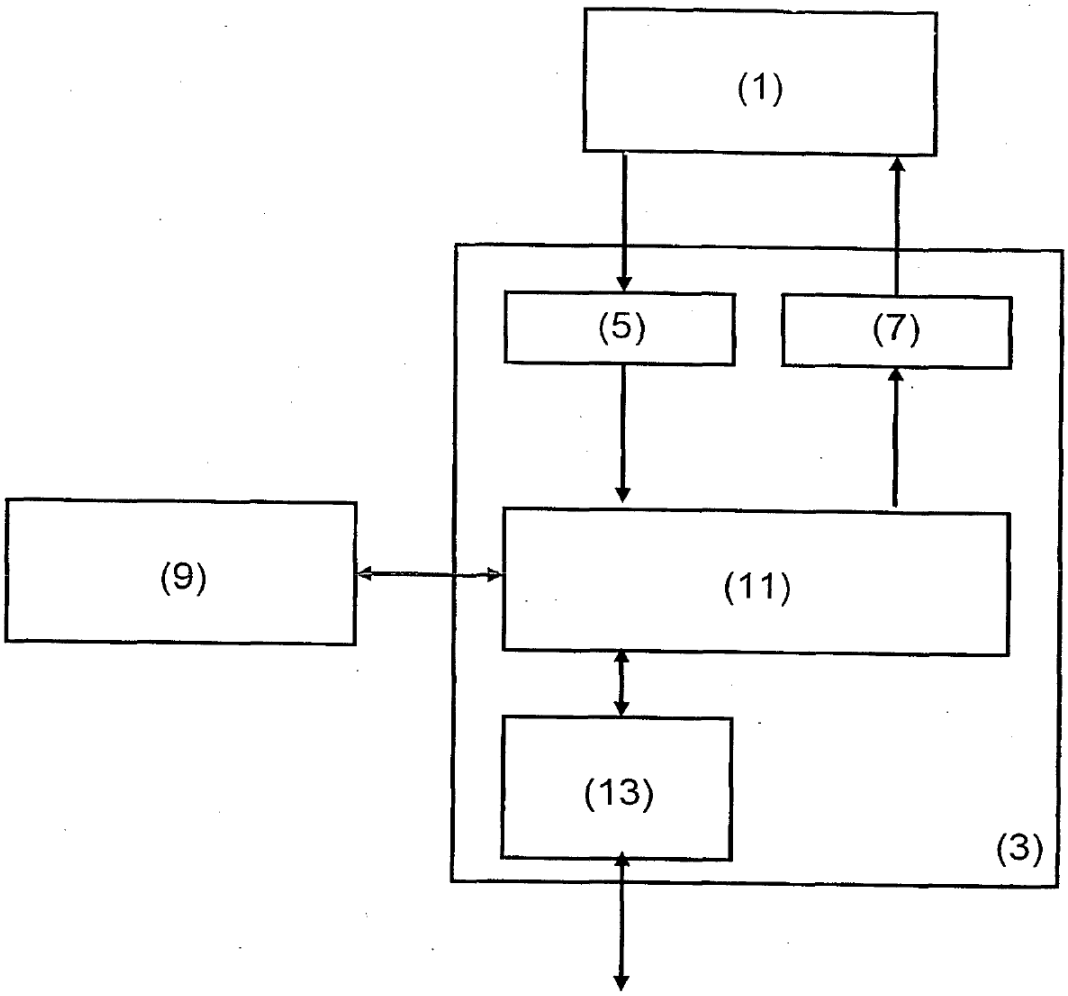

Figura 1

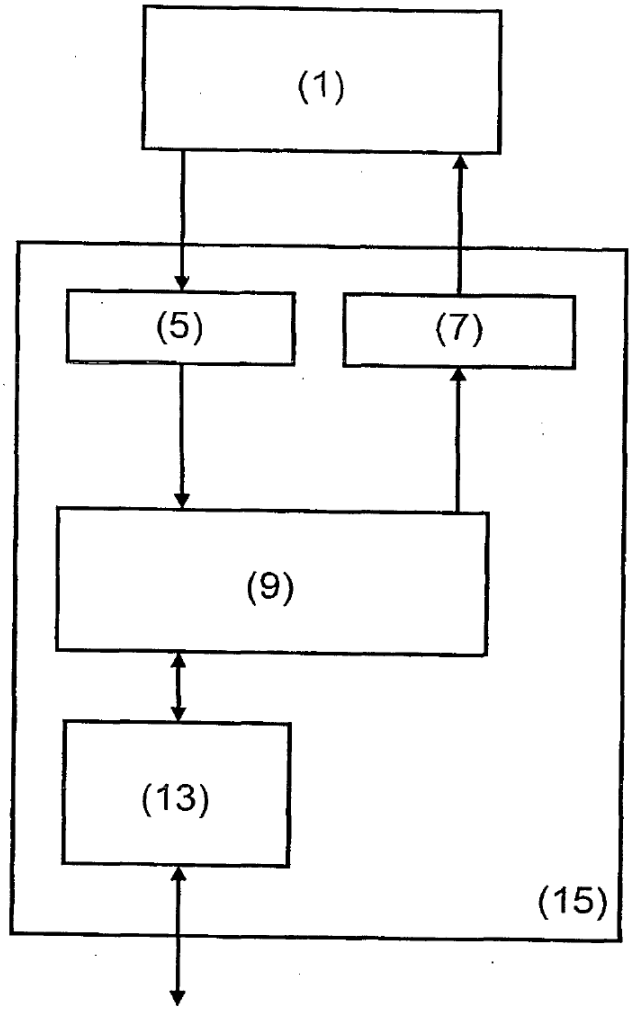

Figura 2

Figura 3

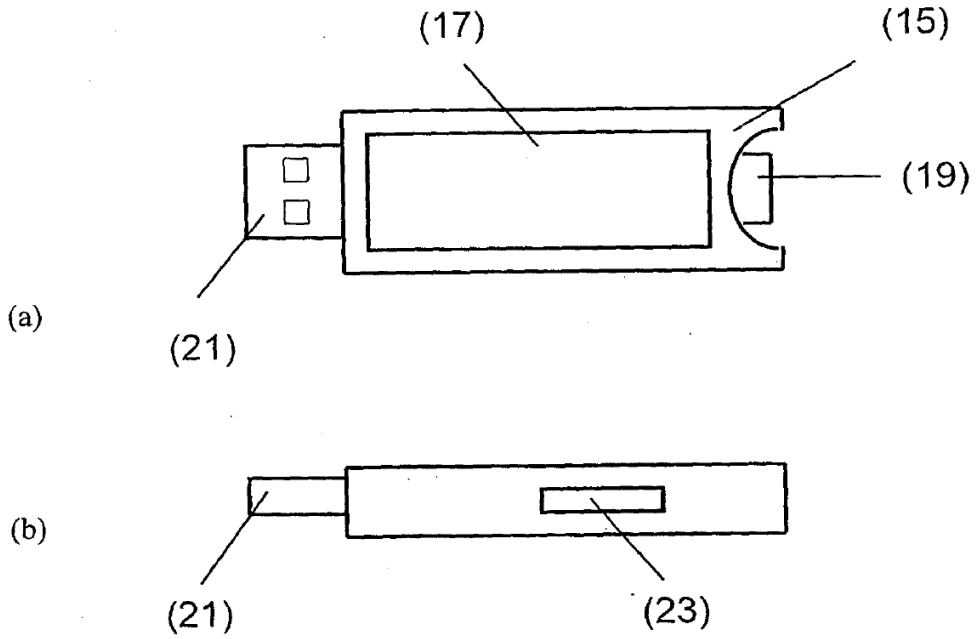

Figura 4