(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 393 220**

(51) Int. CI.:
G07F 7/10 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **07857942 .2**
(96) Fecha de presentación: **20.12.2007**
(97) Número de publicación de la solicitud: **2106605**
(97) Fecha de publicación de la solicitud: **07.10.2009**

(54) Título: **Método y sistema para el incremento de la seguridad en la elaboración de firmas electrónicas mediante tarjeta con chip**

(30) Prioridad:
29.12.2006 DE 102006062046

(45) Fecha de publicación de la mención BOPI:
19.12.2012

(45) Fecha de la publicación del folleto de la patente:
19.12.2012

(73) Titular/es:
NEC CORPORATION (100.0%)
7-1, Shiba 5-chome Minato-ku
Tokyo 108-8001, JP

(72) Inventor/es:
LO IACONO, LUIGI

(74) Agente/Representante:
DE ELZABURU MÁRQUEZ, Alberto

DESCRIPCIÓN

Método y sistema para el incremento de la seguridad en la elaboración de firmas electrónicas mediante tarjeta con chip.

La presente invención se refiere a un método, así como a un sistema para el incremento de la seguridad en la elaboración de firmas electrónicas mediante tarjeta con chip. El método según la invención contempla especialmente una verificación visual de los datos a firmar, a fin de garantizar una firma digna de confianza.

Las tarjetas con chip, denominadas a menudo también Smartcards, o bien Integrated Circuit Card (ICC), son tarjetas especiales de plástico con un chip integrado, el cual presenta normalmente una lógica de hardware, una memoria y/o un microprocesador. Existen tarjetas chip en distintos modelos.

La tarjetas con chip de memoria sirven fundamentalmente para el almacenamiento de datos, y tiene solamente una lógica sencilla, mientras que las tarjetas con chip con procesador están dotadas la mayoría de las veces con un sistema operativo propio, y tienen a menudo capacidades criptográficas. Las tarjetas con chip y capacidades criptográficas ofrecen, junto a la posibilidad de almacenar informaciones privadas, como por ejemplo claves criptográficas, además de ello también algoritmos criptográficos, de forma que el cifrado, o bien la creación de firmas electrónicas, tiene lugar solamente en el interior de la tarjeta con chip, y las claves criptográficas nunca pueden ser leídas directamente.

Dado que las claves secretas, o bien privadas, están almacenadas en la tarjeta con chip, y no abandonan la misma, el ver la clave es prácticamente imposible, por lo que la elaboración de firmas mediante una tarjeta con chip ha de considerarse principalmente como muy segura. Las firmas electrónicas ofrecen muchas ventajas para las transacciones sobre redes, por ejemplo conceden la autenticidad de una noticia. La mayoría de los estados miembros de la Unión Europea han aprobado entretanto leyes referentes a las firmas electrónicas, y cumplen con ello los requerimientos de la directiva europea 1999/93/EC. En Alemania y en Europa se equipara ampliamente la firma electrónica con la firma manuscrita. Debido al alto nivel de seguridad que ofrecen las tarjetas con chip para la elaboración de firmas electrónicas, las mismas están prescritas en la ley alemana de firmas (SigG), o bien la ordenanza de firmas (SigV) como las llamadas “unidades de elaboración de firmas“ para la elaboración de la pareja electrónica de la firma manuscrita.

Dado que las tarjetas con chip no presentan la mayoría de las veces ni alimentación de energía, ni teclado ni pantalla, se necesita constantemente un aparato de lectura/escritura, así como un terminal para la presentación de los datos, y para la interacción con una tarjeta con chip. De ello se desprende que para firmar y presentar documentos electrónicos han de transmitirse continuamente datos entre el terminal y las tarjetas con chip. De aquí, un firmante ha de confiar en una transmisión y una presentación de los datos dignas de confianza, a fin de estar seguro de que en los datos que se presentan en la pantalla del terminal, se trata de los datos que él quiere firmar con su tarjeta con chip, es decir, un usuario desearía firmar lo que él ve (WYSIWYS - "What You See Is What You Sign"). La comunicación de datos entre el terminal y la tarjeta con chip, así como la presentación de los datos a firmar en la pantalla del terminal, encierra no obstante un riesgo potencial, que es descrito a menudo como "problema del terminal“, y se discute brevemente a continuación.

A menudo, los ordenadores personales sirven como terminales, sirviendo la pantalla del ordenador como pantalla de terminal. Un usuario, o bien un signatario, no puede estar seguro, en terminales de ese tipo, si en el caso de los datos representados en la pantalla del ordenador, se trata en realidad de los datos que él quiere firmar. Así en el ordenador puede estar presente un software malicioso (programas dañinos, o bien malware, por ejemplo un "troyano“), modificando o cambiando el malware los datos en el ordenador, de forma que, aunque el usuario recibe los datos que desearía firmar representados en la pantalla del ordenador, se firman al final datos que no están representados en la pantalla del ordenador. El siguiente ejemplo ha de continuar aclarando esto.

Suponiendo que un usuario desee ejecutar una orden de transferencia desde su PC privado en casa, estando infectado el PC con malware sin que lo sepa el usuario. El malware puede capturar los datos a firmar y sustituirlos por una orden de transferencia modificada, por ejemplo una transferencia a un número de cuenta extranjero. No obstante, el malware muestra, en lugar de la transferencia engañosa, una señal de error en la pantalla del ordenador, de forma que el usuario no puede identificar que ya ha firmado la transferencia al número de cuenta en el extranjero, y con ello la ha ordenado, autorizado y aceptado.

En el estado de la técnica se proponen varios métodos y sistemas posibles para evitar este tipo de usos indebidos. Por ejemplo, terminales especificados especialmente para éste cometido podrían evitar que cualquier malware pueda alojarse en el terminal. No obstante, esto tiene el inconveniente de que los terminales de éste tipo sólo cumplen con un determinado objetivo, y son correspondientemente caros.

De aquí el que sea deseable el utilizar ordenadores personales como terminales con pantalla, pudiéndose evitar una manipulación engañosa, iniciada por un malware, a través de medidas de seguridad adicionales. Así, el documento DE 199 23 807 se refiere a un método para el incremento de la seguridad en las signaturas, o bien en las firmas

digitales, basándose el método fundamentalmente en el acoplamiento criptográfico entre un aparato externo de visualización y la tarjeta con chip. Para ello, entre el aparato externo de visualización y la tarjeta con chip se transmiten los datos sobre un canal cifrado de comunicación. La tarjeta con chip conoce especialmente el código abierto del aparato de visualización, y el aparato de visualización conoce el código abierto de la tarjeta con chip. De todas formas, este método no ofrece ninguna protección efectiva contra programas malignos como los troyanos. Cuando los mismos se han alojado en el PC, pueden desactivar el canal seguro entre el PC y la tarjeta con chip, dado que los programas de ese tipo pueden manipular prácticamente todo en el PC, y especialmente pueden actuar sobre el material de códigos que está almacenado allí para la formación del canal protegido. El método según la invención para el incremento de la seguridad de los datos se basa en la utilización de tarjetas con chip con un visualizador (display) integrado. La invención se refiere a un método mediante el cual un usuario recibe de forma segura los datos visualizados que él firma auténticamente con su tarjeta con chip, por ejemplo en un entorno potencialmente inseguro e indigno de confianza, es decir, el usuario firma los datos que él ve en realidad en el visualizador (auténtico "WYSIWYS"). Esto se logra, según la invención, al utilizar el visualizador de la tarjeta con chip como visualizador de confianza para la verificación de los datos a firmar. Con otras palabras, los datos a firmar con la tarjeta con chip se representan directamente con el visualizador de la tarjeta con chip. Dado que la tarjeta con chip controla directamente por sí misma al visualizador, y ningún malware puede alojarse en la tarjeta con chip, se trata, en el caso del visualizador de la tarjeta con chip, de un visualizador digno de confianza.

El visualizador en la tarjeta con chip puede mostrar solamente, debido a su pequeño tamaño, predeterminado a través del tamaño de la tarjeta, relativamente pocas informaciones, y, especialmente, el visualizador no puede mostrar al mismo tiempo, en la mayoría de las ocasiones, todos los datos a firmar. Según la invención, los datos a firmar se reducen –en caso de necesidad – a datos específicos esenciales, y solo se representan en el visualizador esos datos específicos esenciales. Este planteamiento, según la invención, está basado en la observación de que cuando algunos datos esenciales no pueden ser manipulados inadvertidamente por el atacante – una manipulación es advertida por el usuario legal en el visualizador digno de confianza de la tarjeta con chip – ya no existe el fundamento y la motivación para un ataque. Esto puede representarse nuevamente de forma visible con el ejemplo de una transferencia bancaria. Aquí pueden verse, como datos esenciales, el receptor de la transferencia, así como la cantidad de la misma. Si el atacante ya no está en condiciones de modificar inadvertidamente en su beneficio estos datos, el atacante ya no tiene motivación alguna. Que datos se representan en el visualizador, y como se seleccionan esos datos por la tarjeta con chip, dependen del contexto de aplicación respectivo.

El documento DE 10 2004 046847 describe un sistema, un método y un soporte de datos portátil para la elaboración de una firma digital, y aquí especialmente la protección de una elaboración de una firma autorizada por un usuario mediante el soporte de datos portátil. Aquí se utiliza una tarjeta con chip, con la finalidad de la firma, que puede presentar un visualizador. El ordenador utilizado aquí, el cual puede ser potencialmente inseguro, se encarga de los principales cometidos del método conocido de firmar. Un usuario define especialmente los datos que desearía firmar, a través de introducción de datos en el ordenador. Además, el ordenador determina un valor de control a partir de los datos de la transacción, el cual ha de ser firmado por la tarjeta con chip. En este método conocido se le asignan al servidor unos pasos esenciales de la transacción, determinando asimismo el servidor, a partir de los datos de la transacción, un valor de control y adicionalmente datos de visualización para la visualización del usuario. Además son necesarios otros pasos para la verificación de la firma del servidor, así como otro paso para la comparación de los valores de control en la tarjeta con chip. Este método conocido requiere modificaciones de los procesos de firmado existentes, tanto del lado del usuario como del lado del servidor.

El documento WO 2004/032414 describe un firmado digital de datos con una tarjeta con chip con visualizador integrado. El marcado y la selección de datos esenciales desde los datos a firmar, mediante un dispositivo de selección, y la representación posterior de los datos seleccionados en el visualizador de la tarjeta con chip, no están previstos aquí

El objetivo de la presente invención es proporcionar un método, una tarjeta con chip, así como un sistema para el incremento de la seguridad en la elaboración de firmados digitales mediante tarjetas con chip, y soslayar preferentemente los inconvenientes del estado de la técnica descritos anteriormente. El objetivo de la presente invención se alcanza a través de las reivindicaciones independientes. Las reivindicaciones dependientes describen otras formas de ejecución preferidas, y variantes de la presente invención.

A continuación se utilizan como sinónimos los conceptos de firma digital, o bien de firma digital o firma electrónica, haciendo referencia de forma reforzada sobre las definiciones y conceptos de la ley alemana de firmas (SigG). Aquí se utiliza el concepto “firma electrónica“, y se diferencian tres tipos de firmas. Para el método según la invención, y para el sistema, son relevantes fundamentalmente los tipos de firmas, que se basan en métodos matemáticos, o bien criptográficos, o algoritmos, y especialmente la llamada “firma cualificada”, que parte del efecto del derecho

Además existe el concepto de „datos esenciales“ para los datos que son especialmente importantes para el proceso de firmado. Los datos esenciales son datos parciales de los datos a firmar, los cuales son especialmente indicados para caracterizar de forma significativa a los datos a firmar. Aquí es necesario observar que el término datos “parciales” no está limitado a una parte, sino que también el conjunto de los datos a firmar pueden ser elegidos como datos parciales, especialmente cuando en los datos a firmar se trata de relativamente pocos datos, que pueden ser

representados en el visualizador de la tarjeta con chip. En una transferencia bancaria se pueden elegir como datos característicos esenciales, por ejemplo, el número de cuenta, el número de identificación del banco, y el importe. Otros datos que describen el proceso de transferencia, como por ejemplo una referencia pueden no ser considerados en la selección de los datos característicos esenciales, es decir, esos datos no han de ser considerados como esenciales, sino solamente como complementarios. Con otras palabras, como datos esenciales han de observarse los datos que sean esenciales, significativos, o bien específicos para el proceso de firmado

A continuación se describen más detalladamente dos formas de ejecución preferidas del método según la invención.

Según una primera forma de ejecución preferida del método según la invención, una tarjeta con chip es utilizada con un solo propósito prefijado (por ejemplo negocios bancarios). Los formatos de los datos están prefijados, a través de ello, específicamente para el sistema, y con ello también los datos esenciales, que son visualizados por la tarjeta con chip. Los datos esenciales (reducidos) podrían ser aquí el número de cuenta, el código bancario y la cantidad.

Según una segunda forma de ejecución preferida del método, la tarjeta con chip es utilizable de forma versátil para varios propósitos, por ejemplo para negocios bancarios, como sustitutivo para la firma manuscrita, etc. Las características esenciales de los datos están definidas por ello de forma diferente para diferentes utilizaciones de la tarjeta con chip. En esa segunda forma de ejecución preferida del método según la invención, los datos esenciales de los datos a firmar, y que han de ser representados por el visualizador de la tarjeta con chip, son marcados y seleccionados según la utilización. El marcaje y la selección pueden ser realizados automáticamente, o bien por un usuario.

En ambos casos están previstos en la tarjeta con chip un dispositivo de procesamiento, o bien un dispositivo de selección, por ejemplo en forma de hardware, o bien de software, a fin de filtrar los datos relevantes, o bien los datos esenciales del flujo de datos a firmar, y representarlos en el visualizador de la tarjeta con chip.

Según la segunda forma de ejecución, se mantiene aquí una determinada secuencia y forma del proceso, de forma que la elaboración de la firma tenga lugar de forma correcta y según los estándares de firmado, y con ello la firma generada por la tarjeta con chip pueda ser verificado, también fuera de la tarjeta con chip, por componentes de verificación de firmas distribuidos previamente.

El método y sistema según la invención tiene la ventaja de que la autorización de la firma, por ejemplo a través de la introducción de un código de firmado, solo tiene lugar tras una verificación visual de los datos esenciales visualizados.

La presente invención se refiere también a una tarjeta con chip para ejecutar el método mejorado, según la invención, para el incremento de la seguridad en la elaboración de firmas electrónicas, o bien para el firmado digital de datos. La tarjeta con chip según la invención puede estar configurada como una tarjeta con chip que precisa contacto, o bien como una tarjeta con chip sin contacto, o como una tarjeta con chip que pueda ser consultada tanto por una interfase que precisa contacto como por una sin contacto.

La tarjeta con chip según la invención presenta un visualizador integrado en la tarjeta con chip, o bien la misma, que ha de estar configurado lo más grande posible, a fin de poder visualizar al mismo tiempo la mayor cantidad posible de informaciones. El visualizador puede estar previsto sobre el lado delantero y/o sobre el lado trasero. En las tarjetas con chip que precisa contacto, en las que los típicos contactos de oro del módulo de la tarjeta con chip están situados en la parte delantera, puede colocarse en la parte posterior un visualizador más grande. El visualizador puede estar basado, por ejemplo, en una tecnología de visualización orgánica, o bien en una tecnología de material sintético. Están indicados todos los visualizadores que sean lo suficientemente pequeños como para ser colocados sobre/en una tarjeta con chip. El incremento de la seguridad se alcanza especialmente a través de que la única interfase hacia el visualizador es manejada con el microprocesador de la tarjeta con chip. De aquí, se visualizan solamente datos que son procesados por el microprocesador sobre la tarjeta con chip. Como consecuencia de ello, el visualizador integrado sobre/en la tarjeta con chip es un visualizador digno de confianza.

Preferentemente, la tarjeta con chip según la invención presenta elementos de control y de manejo, como por ejemplo teclas para pasar página (Scroll buttons) o un campo táctil (Scroll pad). Loe elementos de control posibilitan a un usuario el hojear los datos, o bien las informaciones visualizados en el visualizador. La presente invención se refiere también a un sistema para el incremento de la seguridad en el firmado digital de datos. El sistema según la invención comprende preferentemente una tarjeta con chip, según la invención, y un aparato de lectura/escritura adaptado para ello, preferentemente con un terminal, o bien con un indicador terminal, o bien con un visualizador terminal. Un aparato lector/escritor de tarjetas con chip, según la invención, es preferentemente de tal forma que el visualizador sobre la tarjeta chip permanece visible también durante el transcurso de la comunicación entre el aparato de lectura/escritura y la tarjeta con chip. En las tarjetas con chip que precisan contacto, esto se puede lograr configurando en forma transparente partes del aparato de lectura/escritura, de forma que el visualizador que está situado debajo también permanece visible todavía cuando el aparato de lectura está unido con los contactos de la tarjeta con chip. Según otra ejecución, el aparato de lectura/escritura puede presentar también un entrante que posibilite la observación sobre el visualizador de la tarjeta con chip, en una tarjeta con chip introducida en el aparato

de lectura/escritura.

Debido al visualizador relativamente pequeño en la tarjeta con chip, solamente se pueden representar sobre el mismo una cantidad limitada de datos, o bien de informaciones. Un aspecto esencial de la presente invención consiste por ello en una selección inteligente de los datos, es decir, de una gran cantidad de datos de información se elige una pequeña parte, la cual sea no obstante suficiente para visualizar todos los aspectos importantes de los datos a firmar para un usuario. En los datos elegidos, o bien seleccionados, se trata preferentemente de partes esenciales de los datos a firmar. Según una forma de ejecución, un usuario puede seleccionar él mismo los datos que a él le parezcan esenciales. Según otra forma de ejecución preferida, la selección de los datos esenciales se lleva a cabo de forma automática. Esto es especialmente ventajoso cuando en la tarjeta con chip se trata de una tarjeta con chip que está prevista para un único proceso determinado, por ejemplo operaciones bancarias. Dado que para ese determinado proceso los datos esenciales están previamente definidos, estos datos esenciales predefinidos pueden ser seleccionados automáticamente. Y representados a continuación en el visualizador de la tarjeta con chip.

La selección se basa preferentemente en un marcaje de datos, es decir, los datos marcados se seleccionan y se visualizan en el visualizador de la tarjeta con chip. El marcaje, es decir, el fundamento de la selección, tiene lugar preferentemente mediante marcadores predefinidos, preferentemente marcadores basados en texto. Especialmente se prefieren idiomas estructurados basados en textos, como por ejemplo XML.

A continuación se describe detalladamente una forma de ejecución preferida de la presente invención, con referencia a la(s) figura(s). Se muestran:

En la figura 1 un sistema según la invención para la realización del proceso de firmado según la invención.

Según la figura 1 se describe el proceso de transferencia bancaria citado anteriormente en el estado de la técnica, pero no obstante esta vez con la utilización del método según la invención. En una transferencia bancaria se contemplan, o bien se eligen como datos esenciales, por ejemplo, el destinatario, número de cuenta, código bancario, cantidad y la fecha. El visualizador 5 integrado en la tarjeta con chip no ha de representar con ello todos los datos que son necesarios para la realización del proceso de transferencia, sino que bastan los datos esenciales que caractericen adecuadamente exactamente a un usuario el proceso de transferencia. Con estos datos esenciales puede verificar con ello un usuario que la cantidad correcta ha sido transferida a la persona correcta en la fecha deseada. Un usuario puede por tanto, tras un control visual de los datos esenciales para él, firmar la transferencia, es decir, autorizarla/ordenarla. En el caso de que, por algún motivo, halla sido realizada una manipulación en los datos, por ejemplo a través de un malware en el terminal, esos datos manipulados se muestran, según el método según la invención, en el visualizador 5. Un usuario reconocerá esto, y no firmará correspondientemente los datos manipulados.

En el proceso de transferencia representado en la figura 1, a título de ejemplo, se dispone un terminal 2 y un visualizador 1 del terminal. Esto puede pasar, por ejemplo, en un banco o en una estación de tren, o bien el ordenador doméstico sirve como terminal 2 y la pantalla del ordenador sirve como visualizador 1 del terminal. Además se dispone de un lector/grabador 4 de tarjetas con chip par leer la tarjeta con chip 5. Un usuario introduce entonces la tarjeta con chip 5 en el lector/grabador 4. Aquí basta con que solamente la parte delantera de la tarjeta con chip 5, con los típicos contactos de oro, sea introducida en el lector/grabador 4, a fin de establecer una comunicación entre el lector/grabador 4 y la tarjeta con chip. La parte posterior de la tarjeta con chip presenta un visualizador 51, el cual permanece visible también cuando la tarjeta con chip está en unión de comunicación con el lector/grabador

Un usuario comienza su proceso de transferencia, estando representados en la pantalla del terminal los datos detallados del proceso de transferencia. Con ello se transfieren datos, según el método de la invención, a la tarjeta 3 con chip, y se calcula un valor criptográfico de control, mediante una función criptográfica de control, a través de los datos introducidos. Un valor de control es un valor escalar de longitud fija y corta, el cual es calculado de los datos de introducción de longitud discrecional, y que es denominado de vez en cuando también como huella dactilar de la noticia, dado que el valor de control identifica la noticia de forma inequívoca, debido a las propiedades de las funciones criptográficas de control.

Una vez que el usuario se ha autentificado como usuario autorizado para la tarjeta con chip, por ejemplo a través de la introducción de un número de identificación personal (PEN), o bien a través del escaneado de una característica biométrica, se calcula la firma electrónica (mediante el valor de control) en la tarjeta con chip. Esta firma electrónica es enviado de vuelta al terminal 2 por el lector 4 de tarjetas con chip. En el caso de que hayan de visualizarse todos los datos en el visualizador 51 de la tarjeta con chip. No se marca ningún dato, o bien se marca el conjunto de los datos, y se representa en el visualizador de la tarjeta con chip.

En el caso de que se halla de representar solamente una parte esencial de los datos a firmar, el procesador busca marcas en el conjunto de datos en la tarjeta 5 con chip, y los datos esenciales se seleccionan según las marcas. Los datos no marcados se remiten directamente a la función de control, y no se representan en el visualizador de la

tarjeta 51 con chip. Cuando dentro del conjunto de datos se encuentra una parte marcada, se retira la marca (por ejemplo “moneyorder” o “iban”) y los datos marcados son seleccionados, a fin de ser representados sobre el visualizador, y se remiten a la función de control sin la marca. Con otras palabras, el valor de control que es firmado finalmente, está basado en los datos sin texto de marca. El método según la invención garantiza especialmente, en este contexto, el orden en el que los datos son memorizados en la función de control, a fin de conservar y apoyar la compatibilidad con componentes estándar de verificación de firmas.

El método según la invención puede ser utilizado también, por supuesto, en otros procesos a firmar. Así pueden, por ejemplo, en el caso de un contrato entre dos partes, representarse solamente los datos esenciales, como por ejemplo los nombres de las partes contratantes, el título del contrato, la fecha, y quizás prescripciones importantes del contrato.

REIVINDICACIONES

1. Método para el incremento de la seguridad en la elaboración de firmas electrónicas con una tarjeta (5) con chip, con las fases:

a) preparación de una tarjeta (5) con chip, con visualizador integrado (51),
b) preparación de un terminal (29 y un aparato de lectura, o bien escritura (4) para tarjetas con chip, para la transferencia de los datos a firmar desde la tarjeta (5) con chip al terminal (2), o bien desde el terminal a la tarjeta con chip,
c) establecimiento de una transmisión de datos entre la tarjeta (5) con chip y el terminal (2), siendo sustancialmente visible para un usuario el visualizador (51) durante la transmisión de datos entre la tarjeta (5) con chip y el terminal (2),
d) iniciación de un proceso de firmado,
e) transmisión de los datos a firmar a la tarjeta (5) con chip, en los que los datos esenciales están señalizados mediante marcas,
f) selección automática de los datos esenciales entre los datos a firmar, sobre la base de las marcas, mediante un dispositivo de selección en la tarjeta con chip,
g) representación de los datos seleccionados en el visualizador (51) de la tarjeta con chip, y
h) firmado de los datos a firmar, siendo transmitido la firma desde la tarjeta (5) con chip al terminal (2).

2. Método según la reivindicación 1, siendo configurado un valor de control a partir de los datos a firmar, el cual es firmado a su vez.

3. Método según la reivindicación 2, estando basado el valor de control sobre los datos a firmar, sin las marcas.

4. Método según la reivindicación 3, siendo retiradas las marcas para la formación del valor de control.

5. Método según una de las reivindicaciones precedentes, teniendo lugar la fase del marcado y/o la selección automáticamente para un proceso de firmado predeterminado.

6. Método según una de las reivindicaciones 1 a 5, siendo ejecutada la fase del escaneado de los datos transferidos, según las marcas, entre la fase de iniciación y selección, y la selección se basa en las marcas.

7. Método según la reivindicación 6, estando basadas las marcas en un lenguaje estructurado, basado en texto, como por ejemplo XML.

8. Tarjeta (5) con chip, con visualizador (51) integrado, para el incremento de la seguridad en la elaboración de firmas digitales, estando adaptada la tarjeta con chip para firmar datos mediante un método según una de las reivindicaciones precedentes.

9. Tarjeta con chip según la reivindicación 8, seleccionando el dispositivo de selección los datos esenciales basándose en marcas.

10. Tarjeta con chip según la reivindicación 8 ó 9, presentando adicionalmente la tarjeta con chip elementos de control (6), con los cuales puede ser controlado la sucesión de las imágenes del visualizador (51) sobre la tarjeta con chip.

11. Sistema para el incremento de la seguridad en la elaboración de firmas electrónicos, configurado con:

a) una tarjeta (5) con chip, según una de las reivindicaciones 8 a 10, y
b) un aparato de lectura/escritura (4) para tarjetas con chip, de forma que durante una transmisión de datos entre el aparato de lectura/escritura (4) para tarjetas con chip y la tarjeta con chip (5), el visualizador (51) de la tarjeta con chip (5) es visible al menos parcialmente.

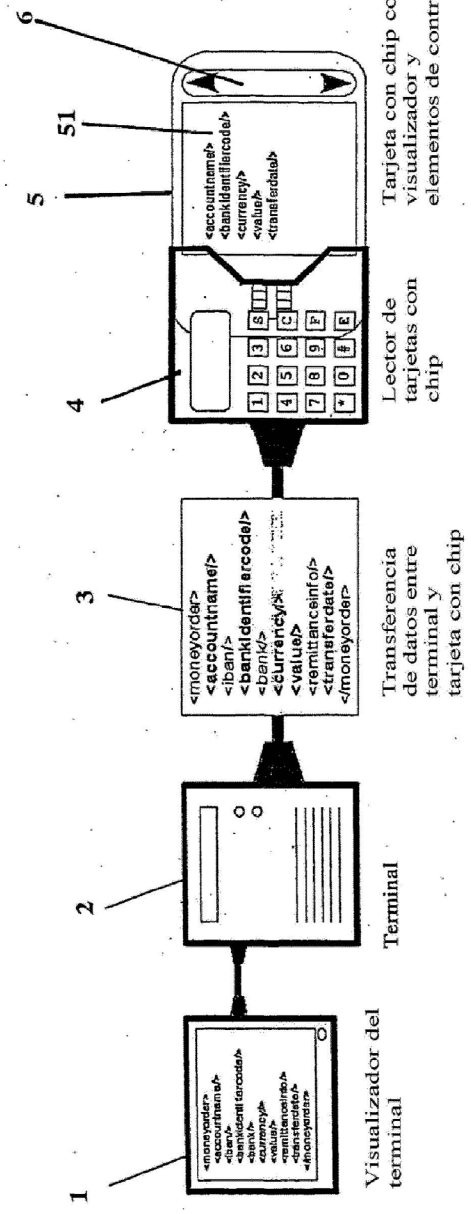
1
2
3
4
5
51
6
Visualizador del terminal
Terminal
Transferencia de datos entre terminal y tarjeta con chip
Lector de tarjetas con chip
Tarjeta con chip con visualizador y elementos de control

Fig. 1