(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 534 478**

(51) Int. CI.:

G06F 1/00 (2006.01)
G07F 7/10 (2006.01)
G06Q 20/34 (2012.01)
G07F 7/08 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **17.05.2001 E 01936570 (9)**

(97) Fecha y número de publicación de la concesión europea: **05.11.2014 EP 1290528**

(54) Título: **Procedimiento de protección contra la modificación fraudulenta de datos enviados a un medio electrónico seguro**

(30) Prioridad:

31.05.2000 FR 0007041

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.04.2015

(73) Titular/es:

GEMALTO SA (100.0%)
6, RUE DE LA VERRERIE
92190 MEUDON, FR

(72) Inventor/es:

GIRARD, PIERRE y
GIRAUD, JEAN-LUC

(74) Agente/Representante:

ISERN CUYAS, María Luisa

DESCRIPCIÓN

Procedimiento de protección contra la modificación fraudulenta de datos enviados a un medio electrónico seguro.

La invención se refiere a un método de protección contra la modificación fraudulenta de datos enviados por un usuario en un medio seguro (una tarjeta inteligente, por ejemplo). Tales datos pueden estar constituidos por una orden y/o por un mensaje acompañado de una firma digital para su autenticación. La invención se sitúa en un contexto donde el medio seguro se acopla a un ordenador PC (Personal Computer en Inglés, que significa un ordenador personal) a través de un lector.

Con el desarrollo del comercio electrónico, ya sea de empresa a empresa o de empresa a particular, hay una necesidad de lograr un marco legal que permita resolver ante un tribunal cualquier conflicto que pueda aparecer. Este marco legal está empezando a tener lugar, ya sea en Europa o en Estados Unidos, con el reconocimiento de la firma electrónica como medio de prueba.

En estas condiciones, es importante tener en cuenta los medios técnicos a implementar para generar firmas electrónicas fiables, es decir, lo menos objetables posible. Se utilizan generalmente técnicas de cifrado de clave pública que permiten generar firmas digitales de documentos digitales. La mayor parte de los algoritmos de cifrado utilizados comúnmente, como el DSA, Schnorr y El Gamal por ejemplo, explotan una función de control en el proceso de generación de la firma electrónica. Tal función, pseudoaleatoria, consiste en transformar el texto inicial a firmar en un texto de control que rompe la linealidad de la generación de firmas.

Los algoritmos de generación de firma electrónica se implementan típicamente usando hardware y software, típicamente un ordenador tipo PC con el software y la clave pública, así como un soporte seguro que contiene la clave secreta del usuario y los algoritmos cifrados de firma.

Dependiendo de las aplicaciones, el soporte seguro puede ser una tarjeta inteligente o una tarjeta PCMCIA, por ejemplo. La mayoría de los ordenadores portátiles están equipados de un lector integrado PCMCIA. Algunas de estas tarjetas de formato PCMCIA pueden también ser lectores de tarjetas inteligentes.

Supongamos a continuación que la firma electrónica se genera a partir de una tarjeta inteligente que requiere el uso de un código de autenticación (PIN) y que el jugador es un acoplador sencillo del tipo GemPC420 que no dispone ni de teclado ni de pantalla. De hecho los lectores con tales entradas/salidas (tipo GCR500) son mucho más caros y rara vez se encuentran conectados a un PC porque son autónomos, pero la puesta en práctica de la invención, sin embargo, se vería facilitada por su uso.

Tradicionalmente, se considera que un proceso de generación de firma electrónica debe producir una firma con las siguientes propiedades:

- Autenticidad: una firma válida implica la voluntad deliberada del usuario de firmar el documento al que se asocia la firma. El protocolo de firma debe por tanto garantizar la participación activa del usuario y solo de él. Por ello es necesario autenticarse antes de firmar. En un sistema que utiliza una tarjeta inteligente, dos elementos

garantizan la presencia activa del usuario: la presencia de un elemento físico que sólo él posee (la tarjeta) y la entrada de un dato que sólo él conoce (un código PIN o contraseña).

- Infalsificabilidad: Únicamente el usuario debe estar en condiciones de generar una firma para un documento dado. Esta propiedad está garantizada por el uso de algoritmos criptográficos considerados como fiables y de una infraestructura de clave pública de confianza, y por el uso de un medio de almacenamiento de claves resistente a ataques físicos y lógicos (una tarjeta inteligente, por ejemplo).

- No reutilizabilidad: la firma asociada con un documento no puede ser reutilizada ni asociada con otro documento, es decir, que cualquier alteración del mensaje asociado a la firma debe poder ser detectado. Esta propiedad está garantizada por los métodos conocidos que utilizan una función de control y algoritmos de generación de firmas digitales aleatorias por el uso de los peligros regenerados entre cada firma.

- No repudio: el usuario del documento no puede negar haber firmado deliberadamente un documento después de haberlo hecho. Esta propiedad se basa en la seguridad global del sistema, y por lo tanto no es cierto que la probabilidad de ataque al sistema sea insignificante. De lo contrario, un usuario podría repudiar su firma con el argumento de la debilidad del sistema. Se han de tener en cuenta a este nivel usuarios de mala fe (conocidos por la expresión anglosajona de ataque de primera parte). De hecho, un usuario puede introducir deliberadamente un fallo en el sistema para, a posteriori, repudiar su firma. Por ejemplo, si el usuario genera por sí mismo su clave pública, puede elegir deliberadamente una clave frágil para pretender posteriormente haber elegido una clave aleatoria que ha demostrado ser débil y estar rota.

Se considera en general que los sistemas que utilizan un PC y las tarjetas inteligentes son lo suficientemente fiables para garantizar el no repudio de las firmas generadas. Sin embargo, los ataques por medio de caballos de Troya están lo suficientemente desarrollados en los últimos tiempos que uno tiene derecho a impugnar ese punto de vista.

Un caballo de Troya se define como una pieza de código malicioso que se esconde en un programa que efectúa tareas banales.

Los sistemas operativos utilizados en la actualidad en los PC domésticos y la falta de vigilancia de los usuarios hace que sea muy fácil introducir un programa con un troyano en el PC y que el caballo de Troya, una vez en su lugar, tiene todos los derechos posibles. Por ejemplo, los caballos de Troya pueden estar ocultos en programas populares y de libre disposición o compartido en la web (shareware en Internet), tales como protectores de pantalla, por ejemplo. También existen troyanos genéricos como "Back Orifice" que permiten tomar el control total de un PC de manera remota y modificar la totalidad o parte de su contenido, o troyanos que aprovechan un error (bug) en un programa de red (por ejemplo, Internet Explorer).

Los ataques que pueden conducir los troyanos son múltiples, pero conservamos tres principales:

- Robo del código PIN del usuario: El código PIN (del Inglés, Número de Identificación Personal) constituye un valor de autenticación para la autenticación del titular de la tarjeta.

Un troyano instalado en algún lugar del sistema operativo, en una aplicación de software, en los pilotos del lector de tarjetas o en los pilotos específicos de la tarjeta, es capaz de copiar el PIN que es introducido por el usuario y transmitirlo al autor del troyano. A partir de entonces, sólo faltará que éste último robe la tarjeta a su legitimo propietario y la utilice sin su conocimiento.

- Modificación de una orden emitida por el usuario con destino a la tarjeta.

Por ejemplo, un ataque de este tipo puede realizarse a una solicitud de generación de llave a bordo de la tarjeta por el PC. El troyano puede interceptar esta orden, generar una clave propia, personalizar la tarjeta con esta clave y transmitir una copia. En tal caso, está claro que las propiedades asociadas a la firma electrónica se pierden, ya que el propietario de la tarjeta no es el único que puede producir una firma válida.

- Modificación del documento a firmar entre su visualización por parte del usuario y su firma por la tarjeta.

Cuando el usuario introduce su código PIN para significar su aprobación, el software de la aplicación envía el documento a firmar a la tarjeta que lo controla antes de la firma (que va aquí en un contexto en que el volumen de datos a firmar no es incompatible con las capacidades de procesamiento de una tarjeta inteligente).

Sin embargo, un troyano puede interceptar los datos transmitidos a la tarjeta y modificarlos. El usuario habrá entonces firmado un documento que no sólo no ha aprobado, sino que nunca había visto. Está claro que tal situación no es aceptable. Se hace por tanto evidente que con la generalización del comercio electrónico y las firmas electrónicas, este tipo de ataques puede ser utilizado como argumento para la refutación de firmas.

El problema particular del robo del código PIN es a día de hoy tenido en cuenta y controlado en los sistemas que incorporan lectores de tarjetas inteligentes, como por ejemplo el GemPC420. Uno de dichos lector, que se muestra esquemáticamente en la figura 1, incluye un mecanismo especifico, comúnmente llamado "ruta de confianza" o camino seguro en seguridad informática, destinado a evitar el robo del código PIN por un caballo de Troya.

La figura 1 representa el principio de funcionamiento del GemPC420. Éste se coloca entre el PC y el teclado. Por lo tanto, está en posición de interrumpir todas las comunicaciones entre el teclado y el PC. El lector tiene tres modos de funcionamiento, correspondientes a tres circuitos de comunicación entre el PC, el teclado y el lector de la tarjeta inteligente. Estos circuitos están numeradas del 1 al 3 en la figura 1.

El circuito 1 corresponde a un modo de funcionamiento en el que la tarjeta no se utiliza y donde el PC dialoga con el teclado. El circuito 2 corresponde a un modo de funcionamiento en el que el PC dialoga con la tarjeta a través de la APDU (del Inglés Application Protocol Data Unit) definido por la norma ISO para estandarizar los intercambios entre un lector y una tarjeta. Por último, el circuito 3 corresponde a la ruta de

confianza: el lector corta la comunicación entre el PC y el teclado y las pulsaciones del teclado por parte del usuario se envían directamente a la tarjeta por el lector. El lector entra en el modo 3 por orden del PC y completa seguidamente la APDU enviada a la tarjeta por el PC con los códigos de las pulsaciones del teclado del usuario.

Para mayor seguridad y facilidad de uso, un diodo emisor de luz (LED) parpadea en el lector para significar que está en el modo 3, y sólo en ese caso.

Un troyano se encuentra por lo tanto con la imposibilidad de interceptar el PIN del usuario, ya que este código no transita en ningún momento por el PC. El usuario no debe introducir su código PIN cuando el lector está en modo ruta de confianza señalado mediante el parpadeo del LED. De hecho, un troyano puede mostrar en pantalla un mensaje invitando al usuario a que introduzca su PIN sin tener que cambiar el lector en modo de ruta de confianza.

En este caso, el lector no cortarla la comunicación teclado-lector y el troyano obtendría el código PI N.

En conclusión, está claro que el lector de tarjetas GemPC420 resuelve el problema del robo del PIN por parte de un troyano. También hay otros lectores, que utilizan otras tecnologías, que pueden lograr los mismos resultados.

Se pueden por ejemplo utilizar lectores que utilizan el protocolo de comunicación USB (del Inglés Universal Serial Bus) en un ordenador equipado con un teclado USB (como por ejemplo los ordenadores de Apple). El principio es muy similar al descrito anteriormente: el lector de tarjeta tiene dos conectores USB. El primero se conecta a uno de los puertos USB del ordenador y el segundo se utiliza para conectar el teclado. Normalmente, el lector transmite las informaciones intercambiadas entre el teclado y el ordenador. Al recibir una orden de aislamiento de su canal, el lector corta la conexión entre el teclado y el PC. Las informaciones que se pulsan a continuación en el teclado no se envían al ordenador sino que se utilizan directamente por el lector. Un PIN introducido de esta manera no regresa entonces nunca al PC y no tiene el riesgo de ser un objetivo de un troyano.

En lo sucesivo, partimos del principio de que nuestra solución utiliza un lector GemPC420, pero está claro que cualquier otro lector que disponga de una ruta de confianza, como por ejemplo un lector USB como el que acabamos de describir, también puede ser utilizado.

Además del problema del robo del PIN, falta por resolver el problema de la modificación de una orden y/o de un documento a firmar.

Actualmente, un troyano presente por ejemplo en un piloto del lector puede modificar el documento enviado a la tarjeta para su firma después de su aceptación por parte del usuario. Por ejemplo, el documento "Yo, el abajo firmante X reconozco deber 10 FF a Y" puede ser modificado por el troyano de manera que diga "Yo, el abajo firmante X reconozco deber 10.000 FF a Y".

Un troyano también puede modificar una orden, por ejemplo, mediante la generación por si mismo de una clave de la que guarde una copia y envíe la orden a la tarjeta de

memorizar esta clave, en lugar de enviar la orden a la tarjeta de generar una clave a bordo.

La presente invención tiene por objeto remediar este problema y proponer una solución original para resolver este tipo de ataque.

Para este fin, la presente invención proporciona un procedimiento implementado por un sistema que consta de una tarjeta acoplada a un ordenador con un software especial. La tarjeta selecciona y memoriza un cierto número de datos enviados por el usuario y pide confirmación, en un modo seguro de comunicación que no transita través del PC, de la autenticidad de dichos datos.

Para ello, la tarjeta pide al usuario introducir la totalidad o parte de la orden emitida ó las palabras seleccionadas en el texto inicial a firmar, entonces se verifica que son idénticos a aquellos recibidos inicialmente.

El método de la invención consiste esencialmente en verificar que ningún ataque pueda cambiar una orden y/o un documento a firmar no es intervenido antes de proceder a la ejecución de la orden y/o a la generación de la firma electrónica de dicho documento.

La presente invención tiene más particularmente por objeto un método de protección contra la modificación de datos enviados por un usuario a un medio seguro a través de un lector, caracterizado porque consiste en seleccionar y memorizar ciertos datos y obtener confirmación de la autenticidad de dichos datos seleccionados verificando que son idénticos a los que figuren en la solicitud por parte del usuario en un modo de comunicación segura del lector.

Según una primera aplicación del método según la invención, los datos es un orden.

Según una variante, la orden es una orden de generación de clave.

Según una segunda aplicación del método de la invención, los datos son un documento firmado con una firma digital generada por el medio seguro.

Según una característica, el método consiste en seleccionar y memorizar algunas palabras del documento a firmar y obtener confirmación de la autenticidad de dicho documento verificando que dichas palabras seleccionadas son idénticas a las consignadas en la solicitud por parte del usuario en un modo de comunicación seguro del lector.

Según una característica, las palabras seleccionadas para la confirmación lo son por el usuario en un modo de comunicación seguro.

Según otra característica, las palabras seleccionadas para la confirmación lo son por el medio seguro.

Según una característica, las palabras seleccionadas por el medio seguro lo son de manera aleatoria.

Según otra característica, las palabras seleccionadas por el medio seguro lo son de manera determinista, el documento a firmar es un documento estructurado.

Según una variante de realización, el medio seguro selecciona para confirmación las palabras correspondientes a números.

Según una variante de realización, el método consiste además en solicitar confirmación de la ubicación en el documento de las palabras seleccionadas para confirmación.

Según una característica, la ubicación de las palabras seleccionadas se define por el número de filas y columnas del documento a firmar.

Según una variante de realización, el medio seguro selecciona como palabras de confirmación toda una columna y/o toda una línea del documento a firmar.

Según una característica, el documento a firmar está en formato ASCII.

La invención también concierne a un terminal capaz de comunicar con un soporte seguro por un lector que tiene un modo de comunicación seguro entre el medio y el lector, no haciendo pasar dicho modo seguro ninguna información por el terminal, comprendiendo dicho terminal un programa apto para llevar a cabo los siguientes pasos:

- envío de los datos al medio seguro,
- solicitar la entrada de datos de confirmación,
- envío de los datos de confirmación al medio seguro en un modo de comunicación seguro.

Según una característica, el terminal comprende al menos una tecla de función o una secuencia de teclas de función reservada para la activación del modo de seguridad.

Según una característica, el terminal comprende además un mini-escáner que incluye un modo de comunicación seguro con el terminal.

Según una realización, el terminal está constituido por un teléfono móvil (GSM).

Según otra realización, el terminal está constituido por un ordenador del tipo PC.

Según otra realización, el terminal está constituido por una tarjeta inteligente provista de una pantalla y un teclado incorporados.

Según otra realización, el terminal está constituido por un asistente digital personal (PDA).

Según una realización, el medio seguro está constituido por una tarjeta inteligente.

Según otra realización, el medio seguro está constituido por una tarjeta PCMCIA.

La invención se refiere además a una tarjeta inteligente capaz de comunicarse con un terminal a través de un lector que tiene un modo de comunicaciones seguro, caracterizado porque incluye un programa apto para implementar las siguientes etapas de:

- selección y memorización de datos recibidos del terminal en un modo de comunicación no segura,

- solicitud de confirmación de dichos datos,

- comparación de los datos memorizados con los recibidos en la confirmación del terminal en el modo de comunicación seguro.

La presente invención proporciona una solución eficaz a la alteración por parte de un troyano de órdenes o documentos firmados por una tarjeta inteligente. La crítica que se puede hacer con este método es su falta de facilidad de uso para el usuario, pero resulta extraño que un aumento de la seguridad se realice sin coacción y, además, el informe de seguridad/ergonomía se puede ajustar a voluntad.

Las características y ventajas de la invención se harán evidentes al leer la siguiente descripción, dada a modo de ejemplo ilustrativo y no limitativo, con referencia a las figuras adjuntas en las que:

la figura 1, ya descrita, es un esquema del lector de tarjeta GEMPC420;

la figura 2 muestra un ejemplo de texto a firmar estructurado;

la figura 3 muestra un ejemplo de un texto a firmar organizada en filas y columnas;

la figura 4 es un organigrama de la implementación del método según la invención, aplicado a la firma de un documento, con un lector de tipo GEMPC420.

la figura 5 es un organigrama de la implementación del método según la invención, aplicado a la firma de un documento, con un lector o una tarjeta que disponen de un teclado y una pantalla incorporados.

la figura 6 es un organigrama de la implementación del método según la invención, aplicado a la generación de una orden, con un lector de tipo GEMPC420.

la figura 7 es un organigrama de la implementación del método según la invención, aplicado a la generación de una orden con un lector o una tarjeta que disponen de un teclado y una pantalla incorporados.

Se describe en un primer momento el método de la invención en su aplicación a la protección contra la modificación de un documento a firmar.

Si tomamos el ejemplo anterior de un texto "Yo, el abajo firmante X certifico deber 10 francos a Y", y si debido a un ataque, el troyano modifica la palabra 10 por 10.000, el método según la invención debe ser capaz de desenmascararlo.

Para este fin, se selecciona la palabra 10 para su confirmación. La tarjeta pide entonces la aplicación destacar (por ejemplo, en rojo o negrita) la palabra a introducir para su verificación por el usuario y mostrar un mensaje del tipo "Introduzca la palabra resaltada en para confirmación". El troyano, que recibe la palabra 10.000 de la tarjeta, destacará la palabra 10 en el texto que aparece en la pantalla del usuario que va a introducir 10. Si la introducción se realiza en modo normal (modo 1 del GEMPC420), el troyano tendrá la

oportunidad de reemplazar las teclas pulsadas por el usuario por 10.000 y la tarjeta efectuará, con éxito, la comparación entre 10.000 y 10.000. Si la entrada aprovecha la seguridad del lector (modo 3 del GemPC420), el troyano no podrá cambiar las teclas pulsadas por el usuario y la tarjeta comparará 10 y 10.000, detectando así la modificación del documento.

Se hace entonces evidente que la solución propuesta por la presente invención no detecta con seguridad un ataque. Si en el ejemplo anterior, la tarjeta selecciona para verificación una palabra del documento que no ha sido modificado por el troyano (por ejemplo, "el que suscribe"), no detectará el ataque y firmará el documento modificado. Es, por ello, importante implementar la solución de la invención de manera que un ataque, aún cuando sea todavía posible, tenga una probabilidad despreciable de tener éxito.

Parece que la elección de las palabras a confirmar y su número tienen una importancia determinante.

En lo que concierne al número de palabras a confirmar, es esencialmente un compromiso entre el grado deseado de seguridad y la dificultad ocasionada por la entrada de la confirmación. Una seguridad máxima se obtiene cuando el usuario reúne el texto completo del documento a firmar. En la práctica, el número de palabras de confirmación dependerá del grado de seguridad deseado y las cuestiones del contexto de aplicativo.

En lo que concierne a la elección de las palabras a confirmar, deben tenerse en cuenta varias limitaciones. Por un lado, las palabras a confirmar son seleccionadas por el usuario y/o por la tarjeta, y por el otro lado, esas palabras son elegidas al azar y/o de manera determinista.

Además, es necesaria una observación preliminar en cuanto a la elección de las palabras a confirmar. Se ha considerado, de hecho, hasta la fecha que el documento a firmar fuera un texto en un formato inteligible para la tarjeta y cuyas palabras fueran directamente comparables con la entrada del teclado.

Un texto en formato ASCII cumple con creces estos criterios. Un documento en un formato propietario (por ejemplo, Microsoft Word) no es utilizable de manera directa. Por contra, es muy posible exportar una versión ASCII de un documento de Microsoft Word para firmar. Esta versión deberá ser visualizada por el usuario, ya que será a la que hará referencia en caso de litigio de la transacción o del contrato. Una solución intermedia podría ser utilizar el formato RTF (Rich Text Format) que permite añadir los atributos de presentación al texto (negrita, subrayado), manteniendo una codificación ASCII. El precio a pagar es un analizador RTF en la tarjeta.

La presente invención en realidad se puede aplicar a cualquier formato de texto, pero se ha de decir que algunos formatos son más prácticos que otros. Uno puede imaginar, por ejemplo (aunque las tecnologías son más difíciles de implementar) formatos de mapa de bits (por ejemplo, obtenido mediante el escaneo de un documento en papel) en comparación con una entrada en una pantalla táctil (pantalla táctil) del teclado o de un dispositivo del tipo de tableta gráfica. Este dispositivo permitiría, por ejemplo, la firma de dibujos para los casos en que el usuario no confirmara palabras, sino partes de dibujos que reproduciría.

A continuación consideraremos que tenemos un texto en formato ASCII.

En la siguiente descripción, con referencia a las figuras 2 y 3, se considera un ejemplo de un texto escrito de la siguiente manera: "Yo el abajo firmante Pierre Girard certifico que debo la suma de noventa francos al Señor Jean-Luc Giraud. Hecho el 31 de enero 2000 en Gémenos".

Un primer punto importante en la implementación del método según la invención es determinar si la elección de las palabras a confirmar es realizada por la tarjeta y/o por el usuario.

La elección, por la tarjeta, de palabras a confirmar que puedan recaer sobre términos insignificantes de un contrato o de un documento (como "el abajo firmante" en nuestro ejemplo), podría hacer pensar que el usuario es el mismo que designa los términos importantes del documento. Puede indicar a la tarjeta, en el modo 3 del lector, las palabras que desea confirmar antes de que reciba el documento. Cuando la tarjeta recibe el documento y pide confirmación, el usuario confirma, en el modo 3 del lector, las palabras previstas.

Sin embargo, este método no defiende al sistema contra usuarios de mala fe (llamados ataque de primera parte) que pueden solicitar a la tarjeta que confirme palabras insignificantes en el documento ("el abajo firmante" en nuestro ejemplo), y repudiar seguidamente su firma pretendiendo haber sido víctima de un troyano.

Para obtener un nivel de seguridad máximo, resulta ventajoso lograr un compromiso en el que las palabras a confirmar son seleccionadas a partes iguales por el usuario (defensa contra troyanos) y por la tarjeta (defensa contra los usuarios de mala fe).

Un segundo punto importante en la implementación del método de la invención es determinar si la elección de palabras a confirmar es aleatoria o determinista

Cuando el usuario elige las palabras a confirmar, su comportamiento no es, a priori, predecible y usará su sentido común para elegir las palabras esenciales del documento. Un troyano tendrá pues muy pocas posibilidades de llevar a cabo un ataque.

En cuanto a la elección por parte de la tarjeta de las palabras a confirmar, se puede elegir entre una estrategia aleatoria o un algoritmo de selección determinista. La estrategia aleatoria es, por definición, impredecible para un troyano. Sin embargo, si la relación de la cantidad de palabras insignificantes y el número de palabras de confirmación es muy importante en el documento, la tarjeta, eligiendo las palabras al azar, tendrá muy pocas posibilidades de escoger una palabra que sea un objetivo potencial para un troyano o un usuario de mala fe.

Para evitar este problema, la tarjeta puede tratar de determinar las palabras importantes del documento. Uno puede pensar inmediatamente en todas las cantidades y las fechas, por ejemplo. Sin embargo, un algoritmo de este tipo es relativamente difícil de aplicar como tal.

Para facilitar la interpretación del texto por la tarjeta y la elección de las palabras pertinentes para confirmación, se puede transmitir de forma ventajosa a la tarjeta el texto estructurado, por ejemplo en XML (Extended Mar-kup Language), que implica tener en la tarjeta el analizador correspondiente. Un de estos textos estructurados se ilustra en la

figura 2. La tarjeta puede así seleccionar para confirmar elementos importantes como fechas o cantidades.

Se pueden también imaginar textos estándar "con blancos" donde sólo la información personal, fechas y cantidades, por ejemplo, falten por completar.

Por último destacar que la tarjeta puede tener una estrategia mixta, complementando su elección determinista con palabras seleccionadas aleatoriamente.

Además de la elección y el número de palabras a confirmar, es importante designar con precisión estas palabras.

De hecho, es obvio que la confirmación de la presencia de un número de palabras en un documento no es suficiente para establecer su significado. También debemos aseguramos de que el orden de las palabras es respetado. Por ejemplo, es importante asegurarse de que la palabra "ciento" no ha sido agregada entre las palabras "de" y "cuatro". Será importante designar con precisión la ubicación respectiva de las palabras "de" y "cuatro".

Esto se puede lograr usando un texto organizado en filas y columnas, como el ilustrado en la figura 3, a fin de designar con precisión la ubicación de las palabras a confirmar.

Al entrar las palabras de confirmación, la tarjeta puede también pedir al usuario que introduzca para confirmación las palabras 4 a 7 de línea 2 y también la palabra 1 de la línea 3. El usuario introducirá entonces las palabras solicitadas y su emplazamiento en el texto. Un acuerdo podría ser "12m4 de" para confirmar la palabra "de" en la posición 4 de la línea 2.

Para evitar las supresiones, inserciones y desplazamiento de palabras, una posible estrategia consiste en solicitar confirmación de columnas de texto. En nuestro ejemplo, si la tarjeta solicita confirmación de la columna 14, el usuario introducirá "c14 Pmin".

La implementación del método de acuerdo con la invención se resume en el siguiente ejemplo completo, con referencia al organigrama de la figura 4:

El método se implementa mediante un software adecuado almacenado en un PC que puede comunicarse con una tarjeta inteligente mediante un lector del tipo GEMPC420.

1. El software muestra en la pantalla del usuario el documento a firmar (siempre usamos el ejemplo de las figuras 2 y 3).

2. El software cambia el GemPC420 a modo 3. El usuario verifica que el LED verde parpadea.

3. El usuario indica a la tarjeta las palabras que quiere introducir en la confirmación mediante la introducción de "12m4-7 de noventa 13m1 francos".

4. El software cambia el GemPC420 a modo 2, luego transmite el texto a firmar a la tarjeta. Si el volumen de texto a firmar es importante, la tarjeta puede cortar sobre la marcha, efectuando las dos etapas siguientes.

5. La tarjeta verifica que la entrada del usuario es coherente con el texto recibido, de lo contrario, se termina el protocolo (evitando así ataques por un troyano).

6. La tarjeta elige las palabras que el usuario deberá introducir para su confirmación. Por ejemplo, la tarjeta selecciona la fecha, a continuación, la columna 21 al azar y la palabra "Pierre". La tarjeta transmite esta elección al software.

7. El software pone en rojo o subraya las palabras a confirmar y cambian el GemPC420 a modo 3. El usuario verifica que el LED verde parpadea.

8. El usuario introduce los datos solicitados por la tarjeta para confirmación: "14m3-5 31 enero 2000 c21 Gua0 11m3 Pierre".

9. La tarjeta verifica que los datos de confirmación son compatibles con el documento recibido, sino el protocolo se termina (evitando asilos ataques de un troyano y/o por parte de un usuario de mala fe).

10. El software le pide al usuario que introduzca su PIN para confirmar su voluntad de firmar el documento (estando el GemPC420 en modo 3). El usuario verifica que el LED verde parpadea.

11. El usuario introduce su PIN.

12. La tarjeta verifica el PIN y, si es correcto, firma el documento y devuelve la firma al software.

En el caso de que se dispusiera de un lector de tarjetas o de una tarjeta que incorporara una pantalla y un teclado integrados, el procedimiento de firma se simplifica de la siguiente forma en referencia al organigrama de la figura 5:

1. El software muestra en la pantalla del usuario el documento a firmar (siempre usamos el ejemplo de las figuras 2 y 3).

2. El usuario indica las palabras que desea introducir para confirmar introduciendo en el teclado del lector (de la tarjeta) "12m4-7 13m1".

3. El software transmite el texto a firmar a la tarjeta. Si el volumen de texto a firmar es importante, la tarjeta puede cortar sobre la marcha, efectuando las dos etapas siguientes.

4. El lector (la tarjeta) muestra las palabras que el usuario ha solicitado confirmar "12m4-7 de noventa 13m1 francos".

5. El usuario verifica que las palabras de confirmación se corresponden con al texto que desea firmar, de lo contrario el protocolo se termina (evitando así los ataques de un troyano).

6. La tarjeta elige las palabras que el usuario deberá introducir para su confirmación. Por ejemplo, la tarjeta selecciona la fecha, a continuación, la columna 21 al azar y la palabra "Pierre". Esta opción se visualiza en la pantalla del lector o de la tarjeta.

7. El usuario Introduce en el teclado del lector (de la tarjeta) las palabras a confirmar: "14m3-5 31 enero 2000 c21 Guao 11m3 Pierre".

8. La tarjeta verifica que los datos de confirmación son compatibles con el documento recibido, sino el protocolo se termina (evitando asilos ataques de un troyano y/o por parte de un usuario de mala fe).

9. El software le pide al usuario que introduzca su PIN para confirmar su voluntad de firmar el documento.

10. El usuario introduce su PIN.

11. La tarjeta verifica el PIN y, si es correcto, firma el documento y devuelve la firma al software.

El método de la invención también puede implementarse en terminales del tipo GSM (teléfonos móviles) o PDA (Personal Digital Assistant) con la condición de que tengan al menos una tecla o una secuencia de teclas de función para activar un modo seguro y una salida que permita saber si el modo de seguridad está activado o no.

Se pueden prever varias posibles implementaciones del método de acuerdo con la invención.

El primero consiste en realizar una interfaz entre el sistema propuesto por la invención (el software que implementa el método de acuerdo con la invención que es capaz de conducir el lector de tarjetas y proporcionar instrucciones al usuario) y los softwares como el Word o Excel que son extensibles. En este marco, se debe codificar en Visual Basic una interfaz con las API (Application Programming Interface) de firma y se recuperan las funcionalidades de subrayar en el texto las palabras.

Otra posible implementación de este sistema se puede obtener mediante la integración del software de implementación de la invención en una página Web por medio de una aplicación Java.

Además, uno de los inconvenientes del método de la invención reside en el esfuerzo requerido para la introducción de ciertas palabras por parte del usuario, lo que va en contra de la evolución de los interfaces para facilidad de uso. Una solución a este problema puede consistir en añadir al sistema que implementa la invención un mini-escáner seguro conectado al mismo puerto de comunicación que el lector o directamente en el lector mismo. En caso de que el lector y el mini-escáner estén conectados a un mismo puerto, el lector estará obviamente dispuesto entre el PC y el mini-escáner, como en el caso del teclado para el GemPC420. El mini-escáner permite al usuario introducir palabras que se muestran en la pantalla o impresas, evitando así una nueva entrada.

El proceso de protección de acuerdo con la invención también puede aplicarse al problema de la modificación de órdenes enviadas a la tarjeta por un troyano.

La invención proporciona para este propósito un procedimiento de protección contra la modificación de la orden enviada al medio seguro (la tarjeta inteligente en el ejemplo considerado). Este método implementa las mismos pasos que se describen en referencia a la protección contra la modificación de un documento firmado.

Después de recibir la orden de, por ejemplo, generación de claves a bordo, la tarjeta pedirá al usuario que confirme esta orden.

En el caso en que el medio seguro esté acoplado a un lector del tipo GemPC420, el método procede de acuerdo con las siguientes etapas en referencia a la figura 6:

1. Se invita al usuario a confirmar su orden de un mensaje que aparece en la pantalla del PC.

2. El software cambia el GemPC420 a modo 3. El usuario verifica que el LED verde parpadea.

3. El usuario confirma su orden (por ejemplo, mecanografiando GENK para la generación de clave a bordo).

4. La tarjeta compara la entrada del usuario con la orden recibida. Si la comparación es negativa, el protocolo se termina, de lo contrario la tarjeta ejecuta la orden (generando la clave).

En el caso en que se utilice un terminal o una tarjeta con pantalla y teclado integrados, el método procede de acuerdo con las siguientes etapas con referencia a la figura 7:

1. La orden recibida por la tarjeta se visualiza en la pantalla del terminal.

2. El usuario verifica que se trata de la orden que desea producir y posteriormente confirma mediante una tecla de función en el terminal o termina el protocolo.

REIVINDICACIONES

1. Método de protección contra la modificación de datos enviados por un usuario a un medio seguro a través de un lector, y recibidos en un modo de comunicación no seguro, **caracterizado** porque consiste en seleccionar y almacenar algunos de los datos recibidos en un modo de comunicación no seguro y obtener confirmación de la autenticidad de dichos datos seleccionados verificando que son idénticos a los entrados a petición por el usuario en un modo de comunicación seguro del lector.

2. Método de protección de acuerdo con la reivindicación 1, **caracterizado** porque los datos consisten en una orden.

3. Método de protección de acuerdo con la reivindicación 2, **caracterizado** porque la orden es una orden de generación de clave.

4. Método de protección de acuerdo con la reivindicación 1, **caracterizado** porque los datos consisten en un documento a firmar con una firma electrónica generada por el medio seguro.

5. Método de protección de acuerdo con la reivindicación 4, **caracterizado** porque consiste en seleccionar y memorizar ciertas palabras del documento a firmar y obtener confirmación de la autenticidad de dicho documento verificando que las citadas palabras seleccionadas son idénticas a las entradas a petición del usuario en un modo de comunicación seguro del lector.

6. Método de protección de acuerdo con la reivindicación 5, **caracterizado** porque las palabras seleccionadas para la confirmación, son seleccionadas por el usuario en un modo de comunicación seguro.

7. Método de protección de acuerdo con una de las reivindicaciones 5-6, **caracterizado** porque las palabras seleccionadas para la confirmación, son seleccionadas por el medio seguro.

8. Método de protección de acuerdo con la reivindicación 7, **caracterizado** porque las palabras seleccionadas por el medio seguro, son seleccionadas de manera aleatoria.

9. Método de protección de acuerdo con la reivindicación 7, **caracterizado** porque las palabras seleccionadas por el medio seguro, son seleccionadas de manera determinista, siendo el documento a firmar un documento estructurado.

10. Método de protección de acuerdo con la reivindicación 9, **caracterizado** porque el medio seguro selecciona para confirmación palabras que son números.

11. Método de protección de acuerdo con cualquiera de las reivindicaciones 4 a 10, **caracterizado** porque consiste además en solicitar confirmación de la ubicación en el documento de las palabras seleccionadas para su confirmación.

12. Método de protección de acuerdo con la reivindicación 11, **caracterizado** porque la ubicación de las palabras seleccionadas se define por el número de filas y columnas del documento a firmar.

13. Método de protección de acuerdo con la reivindicación 12, **caracterizado** porque el medio seguro selecciona como palabras de confirmación toda una columna y/o toda una línea del documento a firmar.

14. Método de protección de acuerdo con cualquiera de las reivindicaciones 4 a 13, **caracterizado** porque el documento a firmar está en formato ASCII.

15. Terminal capaz de comunicar con un medio seguro por medio de un lector que incluye un modo de comunicación seguro entre el medio y el lector, no haciendo transitar dicho modo ninguna información por el terminal, **caracterizado** porque comprende un programa capaz de implementar las siguientes etapas:

- envío de los datos al medio seguro en un modo de comunicación no seguro,
- petición de una introducción de datos de confirmación en un modo seguro que no transita por el terminal,
- envío de los datos de confirmación al medio seguro en modo de comunicación seguro.

16. Terminal de acuerdo con la reivindicación 15, **caracterizado** porque comprende al menos una tecla de función o una secuencia de teclas de función reservada para la activación del modo seguro.

17. Terminal de acuerdo con una de las reivindicaciones 15 a 16, **caracterizado** porque comprende además un mini-escáner que incluye un modo de comunicación seguro con el terminal.

18. Terminal de acuerdo con una de las reivindicaciones 15 a 17, **caracterizado** porque está constituido por un teléfono móvil (GSM).

19. Terminal de acuerdo con una de las reivindicaciones 15 a 17, **caracterizado** porque está constituido por un ordenador tipo PC.

20. Terminal de acuerdo con una de las reivindicaciones 15 a 17, **caracterizado** porque está constituido por una tarjeta inteligente provista de una pantalla y un teclado integrados.

21. Terminal de acuerdo con una de las reivindicaciones 15 a 17, **caracterizado** porque está constituido por un asistente digital personal (PDA para Personal Digital Assistant).

22. Terminal de acuerdo con una de las reivindicaciones 15 a 21, **caracterizado** porque el medio seguro está constituido por una tarjeta inteligente.

23. Terminal de acuerdo con una de las reivindicaciones 15 a 21, **caracterizado** porque el medio seguro está constituido por una tarjeta PCMCIA.

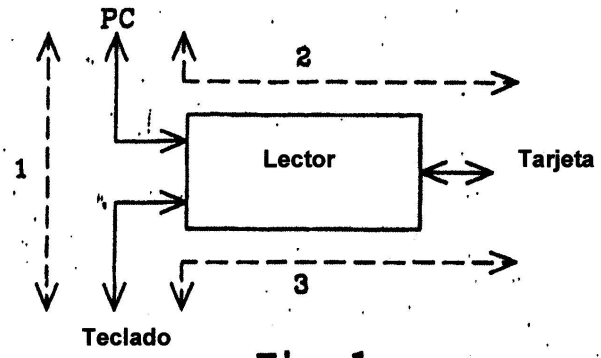


Fig. 1

<contract>
je soussigné <signer>Pierre Girard</signer> <object>certifie devoir</object> la somme de <amount>quatre vingt dix <currency>francs</currency></amount> à <party>Monsieur Jean-Luc Giraud</party>. Fait le <date>31 Janvier 2000</date> <where>à Gémenos</where>.
</contract>

Fig. 2

```
                    11111111112222222222333333
          123456789012345678901234567890123456
        1 Je soussigné Pierre Girard certifie
        2 devoir la somme de quatre vingt dix
        3 francs à Monsieur Jean-Luc Giraud.
        4 Fait le 31 Janvier 2000 à Gémenos.
```

Fig. 3

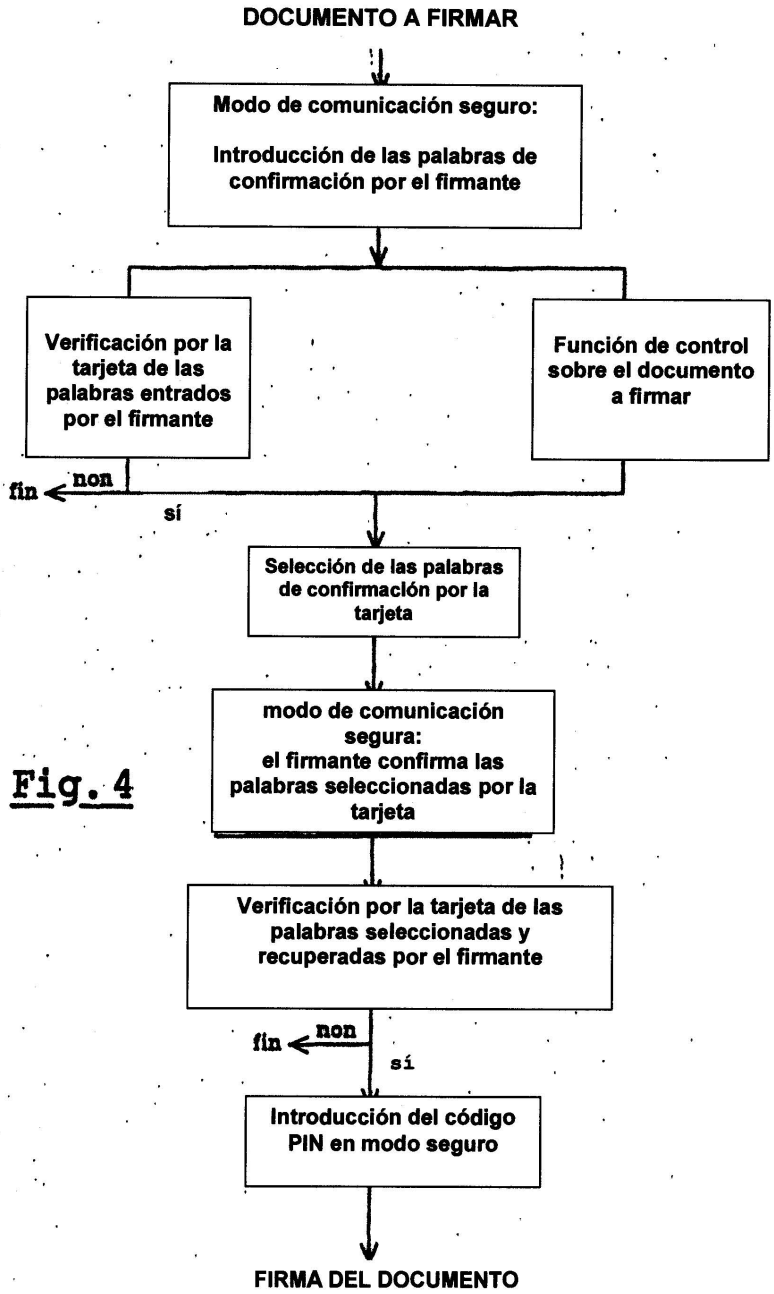

DOCUMENTO A FIRMAR
Modo de comunicación seguro:
Introducción de las palabras de confirmación por el firmante
Verificación por la tarjeta de las palabras entrados por el firmante
Función de control sobre el documento a firmar
fin
non
sí
Selección de las palabras de confirmación por la tarjeta
modo de comunicación segura:
el firmante confirma las palabras seleccionadas por la tarjeta
Verificación por la tarjeta de las palabras seleccionadas y recuperadas por el firmante
fin
non
sí
Introducción del código PIN en modo seguro
FIRMA DEL DOCUMENTO

Fig. 4

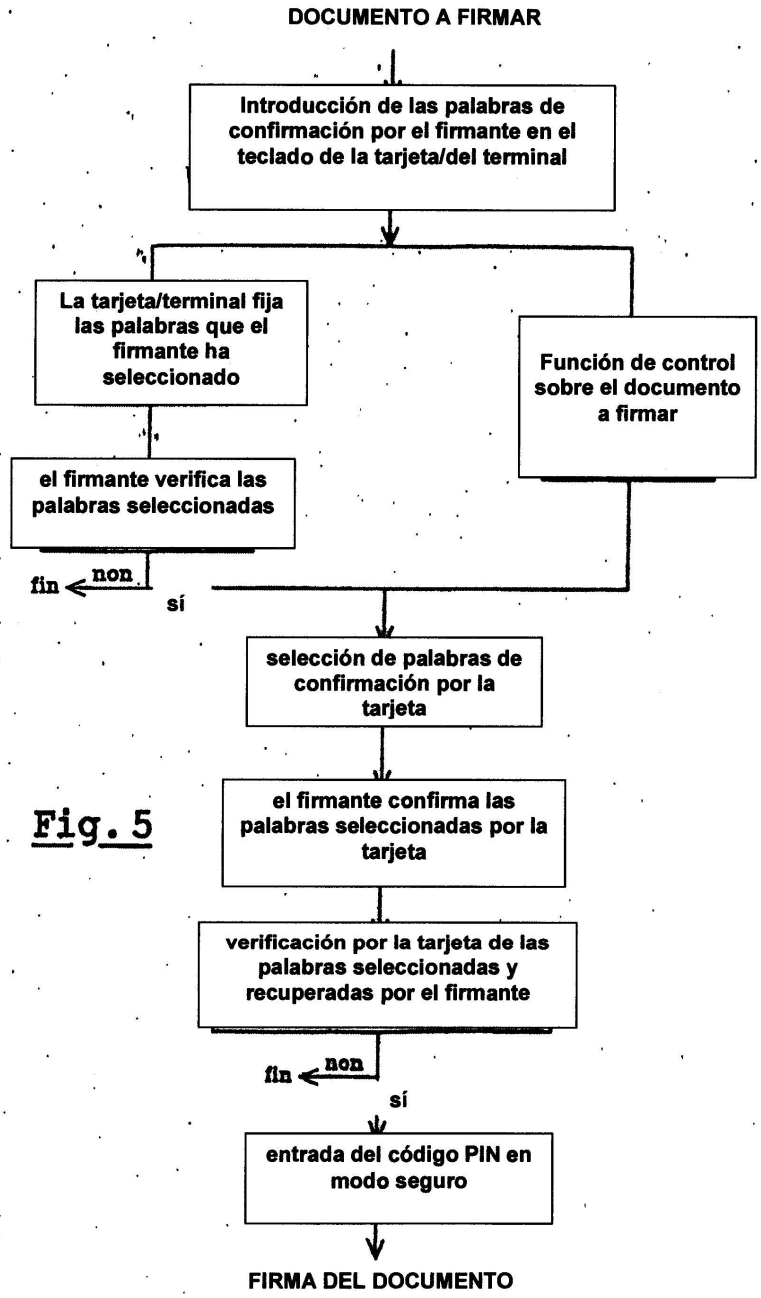

DOCUMENTO A FIRMAR
Introducción de las palabras de confirmación por el firmante en el teclado de la tarjeta/del terminal
La tarjeta/terminal fija las palabras que el firmante ha seleccionado
Función de control sobre el documento a firmar
el firmante verifica las palabras seleccionadas
fin
non
sí
selección de palabras de confirmación por la tarjeta
el firmante confirma las palabras seleccionadas por la tarjeta
verificación por la tarjeta de las palabras seleccionadas y recuperadas por el firmante
fin
non
sí
entrada del código PIN en modo seguro
FIRMA DEL DOCUMENTO

Fig. 5

Fig. 6

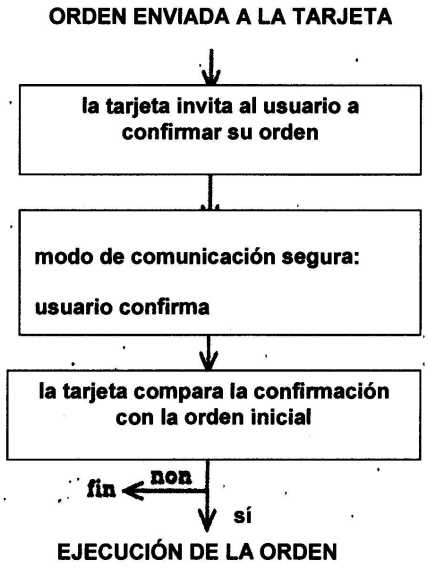
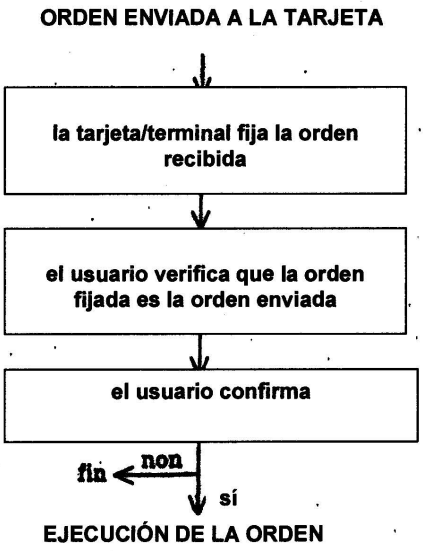

ORDEN ENVIADA A LA TARJETA
la tarjeta invita al usuario a confirmar su orden
modo de comunicación segura:
usuario confirma
la tarjeta compara la confirmación con la orden inicial
non
fin
sí
EJECUCIÓN DE LA ORDEN

Fig. 7


ORDEN ENVIADA A LA TARJETA
la tarjeta/terminal fija la orden recibida
el usuario verifica que la orden fijada es la orden enviada
el usuario confirma
non
fin
sí
EJECUCIÓN DE LA ORDEN