(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 369 654**

(51) Int. CI.:
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **99963605 .3**
(96) Fecha de presentación: **15.12.1999**
(97) Número de publicación de la solicitud: **1142194**
(97) Fecha de publicación de la solicitud: **10.10.2001**

(54) Título: **PROCEDIMIENTO Y SISTEMA DE IMPLEMENTACIÓN DE UNA FIRMA DIGITAL.**

(30) Prioridad:
16.12.1998 FI 982728

(45) Fecha de publicación de la mención BOPI:
02.12.2011

(45) Fecha de la publicación del folleto de la patente:
02.12.2011

(73) Titular/es:
TELIASONERA FINLAND OYJ
TEOLLISUUSKATU 15
00510 HELSINKI, FI

(72) Inventor/es:
VATANEN, Harri

(74) Agente: **Carpintero López, Mario**

DESCRIPCIÓN

Procedimiento y Sistema de Implementación de una Firma Digital

La presente invención se refiere sistemas de telecomunicaciones y a una técnica para firmar y cifrar información digital. En particular, la invención se refiere a un sistema que hace posible firmar un formulario electrónico, u otra información electrónica, y verificar la autenticidad de la firma y del firmante.

Antecedentes de la invención

En la técnica anterior, es conocido el uso de una estación móvil digital, por ejemplo una estación móvil en el sistema GSM (Sistema Global para comunicaciones Móviles, GSM), para las transacciones comerciales, tales como el pago de una factura o la realización de un pago por medios electrónicos. La solicitud de patente de los Estados Unidos Nº 5.221.838 presenta un dispositivo que puede usarse para realizar un pago. La memoria descriptiva describe un sistema de pago electrónico en el cual un dispositivo terminal capaz de transferir datos por cable o de forma inalámbrica se usa como un terminal de pago. El dispositivo terminal, de acuerdo con la memoria descriptiva, comprende un lector de tarjetas, un teclado, un lector de códigos de barras para la entrada de información y una unidad de pantalla para la presentación de la información de pago.

La memoria descriptiva de la patente WO 94/11849 desvela un procedimiento para el uso de servicios de telecomunicaciones y la ejecución de transacciones de pago a través de un sistema de telefonía móvil. La memoria descriptiva describe un sistema que comprende un dispositivo terminal que comunica sobre un sistema de telecomunicaciones con un ordenador central del proveedor del servicio que contiene el sistema de pago del proveedor de servicio. El dispositivo terminal usado en una red de telefonía móvil, es decir, la estación móvil, puede proporcionarse con un módulo de identidad del abonado que comprende información del abonado para la identificación del abonado y para el cifrado de las telecomunicaciones. La información puede leerse dentro del dispositivo terminal de modo que puede usarse en las estaciones móviles. La memoria descriptiva menciona el sistema GSM como ejemplo, en el cual se usa una tarjeta SIM (Módulo de Identidad de Abonado, SIM) como una unidad de identificación del abonado.

En el sistema de acuerdo con la patente WO 94/11849, la estación móvil comunica con una estación base comprendida en la red de telefonía móvil. De acuerdo con la memoria descriptiva, la conexión se establece además con el sistema de pago, y se transmite la cantidad a pagar así como los datos requeridos para la identificación del abonado, dentro del sistema de pago. En el servicio de banco descrito en la memoria descriptiva, el cliente coloca una tarjeta del servicio entregada por el banco y que contiene una unidad SIM dentro del dispositivo terminal usado en la red GSM. En el servicio del banco basado en el teléfono, el dispositivo terminal puede ser una estación móvil de GSM consistente con la normativa. Usado el procedimiento descrito en la memoria descriptiva, puede usarse una conexión de telecomunicaciones inalámbricas para realizar pagos y/o pagar facturas o implementar otros servicios de banco o de efectivo.

El problema con las soluciones mencionadas anteriormente es que no involucran ninguna consideración de la fiabilidad del pago desde el punto de vista del pagador y del beneficiario. Cuando se usa una estación móvil para realizar un pago, es importante tanto para el pagador como para el beneficiario poder confiar en el sistema. El pagador debe conocer exactamente por qué está pagando, cuánto está pagando, a quién está pagando, cómo está pagando, etc. El beneficiario debe también saber exactamente quién está pagando, para qué, y cuánto, etc.

Como es bien conocido, la transmisión de información en un formulario electrónico desde un lugar a otro es sencilla. Sin embargo, es más difícil asegurar que la información transmitida permanezca sin cambios durante la transmisión, y que, por ejemplo, la información presentada sobre la pantalla del teléfono móvil se transmita exactamente del mismo modo y sin cambios al receptor.

Una práctica conocida anteriormente es usar un código de huella digital, que es un campo de datos formado y calculado a partir de la información a transmitir. El código de huella digital se calcula generalmente usando un algoritmo que es una función de un sentido, en otras palabras, el código de huella digital no puede descifrarse de modo que se revele la información desde la cual se ha generado. Un algoritmo que puede usarse para este propósito es el SHA-1 (Algoritmo de Huella Digital Seguro).

Una firma digital, que se considera como un requisito general en el pago electrónico, se usa para verificar la integridad del material transmitido y el origen de remitente. La firma digital se genera por el cifrado de un código de huella digital calculado a partir del material a transmitir, usando la clave secreta del remitente. Como nadie más conoce la clave secreta del remitente, el receptor que descifra el material cifrado puede estar seguro de que el material no se ha cambiado y se generó por el remitente. Un ejemplo de un algoritmo usado en las firmas digitales es el algoritmo de cifrado RSA, que es un sistema de cifrado basado en una clave privada y una clave pública y que se usa también para el cifrado de mensajes.

El documento EP 0689316 desvela un procedimiento y un dispositivo para el envío de paquetes de datos por un dispositivo inalámbrico sobre una red de transmisión de datos. Cada uno de los mensajes transmitidos incluye tres segmentos, esto es, los datos de identificación del remitente, una parte de la firma digital y el paquete de datos real.

En el procedimiento, es posible calcular y enviar una huella digital, y enviar el mensaje real por un dispositivo inalámbrico a un receptor predefinido. Adicionalmente, la huella digital puede cifrarse antes de la transmisión. Además de la información recibida el dispositivo incluye una unidad de entrada de datos (referencia 160 en la figura 1) para introducir información al dispositivo. La unidad de entrada de datos puede ser por ejemplo un teclado separado conectado al dispositivo, un teclado fijado al dispositivo o cualquier otro aparato de entrada. El dispositivo puede ser por ejemplo un asistente digital personal (PDA) o un dispositivo de telecomunicaciones móviles (columna 3 líneas 42 – 45).

El documento US 5.018.196 desvela un procedimiento en el que se intercambian de forma bidireccional transacciones electrónicas con respecto a documentos de contratos y especialmente firmas digitales entre las partes contratantes. El sistema incluye una tercera parte que puede verificar el contrato y las firmas digitales en una situación de un posible problema.

Objetivo de la invención

El objetivo de la presente invención es eliminar los problemas referidos anteriormente. Un objetivo específico de la invención es desvelar un nuevo tipo de procedimiento y un sistema para la firma de un formulario o información correspondiente por medio de una estación móvil. En este contexto, "formulario" puede referirse a muchos tipos de mensajes, despacho o estructura de información con diversos contenidos. El formulario puede consistir de un tipo de objeto o información de tipos de objetos software que puede procesarse en una forma electrónica.

Un objetivo adicional de la invención es desvelar un procedimiento simple para implementar transacciones comerciales, tales como el pago de una factura y transacciones de negocios con un banco, usando una estación móvil, un procedimiento que es fácil de implementar con la tecnología actual.

Objeto de la invención

La invención concierne a un procedimiento para firmar digitalmente un formulario electrónico como se ha definido anteriormente con una firma digital usando una estación móvil o algún otro dispositivo equivalente y comparable. En el procedimiento, el material a firmar, que puede comprender al menos el formulario y/o su identificador y/o información compartida entre la estación móvil y una segunda parte, y/o la información en campos esenciales del formulario, se transfieren a la estación móvil. El material a firmar puede también generarse a partir de un identificador del formulario y la información en los campos esenciales del formulario; por ejemplo, en el caso de un formulario de transferencia bancaria, el material a firmar puede generarse a partir del identificador del formulario de la transferencia de banco y los datos en los campos esenciales en el mimo, tales como los campos del pagador, el beneficiario y la cantidad.

De acuerdo con la invención, a partir del material a firmar, se calcula un primer código de huella digital, preferentemente antes de que el material se transfiera dentro de la estación móvil. El primer código de huella digital se combina con el material a transferir con el mismo, permitiendo de este modo el uso del código de huella digital y una ayuda en la verificación. Después de que se ha transferido el material combinado dentro de la estación móvil, se firma de forma digital por medio de la estación móvil y, de acuerdo además con la invención, la autenticidad y conformidad del material firmado y transferido se verifican comparando el código de huella digital firmado con el primer código de huella digital calculado a partir del material antes de la firma. La firma también puede realizarse firmando tanto la información esencial como el código de huella digital, en cuyo caso se asegurará incluso que el material firmado a través de la estación móvil corresponde con el material transferido para la firma.

En el caso de ciertos tipos de aplicación, tales como las aplicaciones de pago, el material transferido desde una máquina de pago al interior de la estación móvil puede transferirse también desde la máquina de pago a la segunda parte, por ejemplo el banco, que puede calcular un código de huella digital a partir del material recibido. El material firmado en la estación móvil puede cifrarse adicionalmente y el material cifrado y firmado puede transferirse también desde la estación móvil a la segunda parte. La segunda parte descifra la información cifrada, verifica la firma, calcula un segundo código de huella digital a partir del material recibido desde la estación móvil y lo compara con el primer código de huella digital calculado a partir del material original. Si la segunda parte acepta la firma digital y si el primer y segundo códigos de huella digital se corresponden entre sí, entonces el banco aceptará la firma realizada a través de la estación móvil. Después de que el banco ha aceptado la firma, puede poner un sello de tiempo en el material firmado y cifrado y archivar la transacción de la firma del material combinado.

El caso descrito anteriormente es un procedimiento en el cual un cliente de un banco firma un formulario recibido desde el banco. El cliente o usuario de la estación móvil puede comunicar localmente con una máquina automatizada de pago o equivalente, en cuyo caso la máquina de pago transmite al cliente un formulario para el pago y la aprobación. En este caso, el cliente intercambia mensajes con la máquina de pago localmente y la máquina de pago transmite los datos de la firma digital adicionalmente. Sin embargo, la máquina de pago puede inferir a partir de la comunicación que está transmitiendo que el cliente ha aceptado el servicio y el formulario de pago ofrecido para ello. La máquina puede servir al cliente localmente en el modo deseado y el pago por el cliente sin esperar necesariamente la aprobación del banco del mismo. En la práctica, la situación corresponde a la práctica normal donde por ejemplo un cliente en una máquina de efectivo de una tienda paga por productos o servicios con

una tarjeta monedero y la tienda los proporciona al cliente sin verificar la autenticidad del pago contactando con el banco.

El material también puede cifrarse antes de transferirse dentro de la estación móvil, en cuyo caso el material tiene que descifrarse en la estación móvil antes de la firma. Este expediente puede usarse para asegurar que sólo la estación móvil deseada recibirá el material a transferir y garantizar la seguridad de la información.

El formulario puede generarse usando una plantilla de formulario acordada de antemano, una estructura de mensaje o cualquier otra estructura de información, proporcionada con un identificador, en el cual la información acordada de antemano en los campos esenciales del formulario se rellena antes de que el formulario se transfiera dentro de la estación móvil. El código de huella digital puede calcularse usando, por ejemplo, una función de huella digital. Para la firma y/o cifrado del mensaje y/o el formulario, puede usarse un procedimiento de clave pública y privada.

En una realización preferida de la invención, el material y/o parte del material se presenta en la estación móvil antes de la firma del material combinado. Por ejemplo, pueden presentarse el beneficiario, el pagador y la información de referencia y la cantidad a pagar. También es posible requerir que la estación móvil se arranque en el modo de firma antes de la transferencia de información a su interior. En la práctica, esto puede significar que el usuario de la estación móvil tiene que introducir otro código PIN predeterminado con el cual se ha configurado la estación móvil para arrancar en un modo de firma predeterminado. De este modo, es posible usar una clase de autenticación local.

La invención también concierne a un sistema para firmar de forma digital un formulario electrónico usando una estación móvil. El sistema preferentemente comprende una máquina de pago y, conectado a la misma, un medio para generar el material a firmar y transferir al interior de la estación móvil, siendo dicho material como se ha definido anteriormente. En este contexto, la "máquina de pago" puede referirse a cualquier máquina automatizada local u operada localmente capaz de comunicar sobre una red de telecomunicaciones con un proveedor de servicios, tal como un banco, tienda o equivalente.

La máquina de pago puede también implementarse localmente en un ordenador que comunica con el proveedor de servicios, por ejemplo, sobre la Internet, proporcionando el proveedor de servicios productos y servicios a través de la Internet. En este caso, el material a firmar se transfiere para la firma desde el ordenador al interior de la estación móvil usando una conexión local o directamente desde el propio servidor del proveedor del servicio sin usar un ordenador local y una conexión local.

De acuerdo con la invención, la máquina de pago comprende un medio para el cálculo de un primer código de huella digital a partir del material a firmar. Adicionalmente, la máquina de pago comprende un medio para combinar el primer código de huella digital con el material. Además, la estación móvil comprende un medio de firma para la firma del material combinado transferido a su interior. El medio de firma puede comprender una memoria en la cual están almacenados los algoritmos y las claves requeridas para la firma y el cifrado, y un procesador que está conectado a la memoria y que procesa el material, implementando la firma y posiblemente el cifrado. Además, la máquina de pago comprende un medio para verificar la autenticidad del material firmado y transferido comparando el código de huella digital firmado en la estación móvil con el primer código de huella digital calculado a partir del material antes de la firma.

El sistema puede comprender también un servidor que está conectado a la máquina de pago y/o a la estación móvil y que está controlado por una segunda parte, tal como un banco o una compañía de tarjetas de crédito. Tal servidor puede de este modo mantenerse, por ejemplo por un banco y puede usarse en la implementación de las transacciones de banco. El servidor también puede comprender un medio para la verificación de la autenticidad de la firma digital realizada por la estación móvil y medios de cifrado y descifrado para cifrar y/o descifrar el material transferido entre el servidor y la máquina de pago y/o la estación móvil.

La estación móvil también puede comprender medios para la presentación del material y/o parte del material en la estación móvil antes de la firma del material combinado.

El servidor también puede comprender medios para sellar el material firmado con un sello de tiempo y un medio para presentar una transacción de la firma del material combinado después de que la firma se ha autenticado. Estos pueden implementarse de un modo conocido por los especialistas en la técnica, de modo que no se describirán con más detalle en este punto.

En comparación con la técnica anterior, la presente invención proporciona la ventaja de facilitar la implementación de las aplicaciones de pago, verificación de transacciones y similares. Gracias a la invención, una estación móvil puede usarse de forma fiable para realizar una firma digital y puede incorporarse una firma digital en muchas aplicaciones diferentes.

Lista de ilustraciones

A continuación, se describirá la invención con la ayuda de unos pocos ejemplos de sus realizaciones preferidas con referencia a los dibujos adjuntos, en los que

la Fig. 1 presenta un sistema preferido de acuerdo con la presente invención:
la Fig. 2 presenta otro sistema preferido de acuerdo con la presente invención.
la Fig. 3 presenta una realización preferida de la presente invención en la forma de un diagrama de flujo; y
la Fig. 4 es una representación diagramática de un ejemplo preferido de la generación del material a firmar en conjunción con la presente invención.

El sistema presentado en la Fig. 1 comprende una máquina de pago local (LPM) 2 y, conectado a la misma, un medio para generar el material a firmar, que comprende un formulario, su identificador, datos compartidos y/o información esencial asociada con el mismo. Además, el medio 4 conectado a la misma para la transferencia del material a la estación móvil. En la forma correspondiente, la estación móvil comprende un medio 1 usado por la estación móvil (MS) para comunicar con la máquina de pago. En una realización, los medios 1 y 4 están implementados usando la tecnología Bluetooth. Una descripción más detallada de la tecnología Bluetooth se encontrará por ejemplo en la página WWW www.bluetooth.com. También pueden usarse otros protocolos de acceso de enlace conocidos, tales como la interfaz de infrarrojos.

El sistema presentado en la Fig. 1 comprende además un servidor 8 que está conectado a través de un enlace TCP/IP a la máquina de pago 2 y que en este ejemplo se gestiona por un banco. El servidor comprende además un medio 9 para verificar la autenticidad de la firma – en la práctica estos medios se usan para descifrar el mensaje cifrado recibido y para comparar las firmas digitales contenidas en los mismos con la información recibida del usuario. Además, el servidor comprende medios 11 y 12 para sellar el material firmado con un sello de tiempo y presentar la transacción de firma después de que se ha autenticado la firma. El medio de verificación correspondiente también puede estar comprendido en la máquina de pago, y en este ejemplo están indicados por el número 7. Los medios 7, 11 y 12 también pueden tener una característica para la búsqueda de las claves públicas requeridas a partir de servidores de gestión de claves universales, por ejemplo a través de la red TCP/IP.

En el ejemplo presentado en la Fig. 1, el material cifrado, que comprende un formulario de factura y un código de huella digital H1 calculado a partir del mismo, se transfiere desde la máquina de pago 2 al interior de la estación móvil MS, etapa 1. En la estación móvil, el material, es decir, el formulario de factura y el beneficiario, el pagador, la cantidad y el número de referencia del pago se presentan en la pantalla (10) del teléfono móvil, permitiendo al usuario de la estación móvil comprobar lo que está firmando. Usando la estación móvil, MS, el usuario firma a continuación el material y el código de huella digital H1 calculado a partir del mismo. El material con el código de huella digital firmado digitalmente $H1_{ds}$ añadido al mismo se transfiere dentro de la máquina de pago 2, etapa 2. Los mensajes transmitidos entre la máquina de pago 2 y la estación móvil MS pueden cifrarse usando claves públicas y privadas del usuario de la estación móvil y la máquina de pago. Después de que se ha verificado la autenticidad de la firma en la máquina de pago 2, se envía un mensaje de liquidación desde la máquina de pago al banco, etapa 3. La liquidación es una práctica conocida generalmente usada en las relaciones bancarias, de modo que no se describe en este punto con detalle.

Ahora se hace referencia a la Fig. 2, que presenta un sistema correspondiente a la Fig. 1, pero en este caso se usa el sistema en un modo algo diferente. En primer lugar, el material generado en la máquina de pago, por ejemplo, un formulario, se transfiere al banco, etapa 1. A continuación, en la máquina de pago, se calcula un código de huella digital H1 a partir del material y se transfiere a la estación móvil para la firma, etapa 2. La transferencia puede implementarse usando un enlace local, por ejemplo una conexión Bluetooth. En la estación móvil, el mensaje recibido se firma digitalmente, después de lo cual el material firmado y posiblemente cifrado se envía al banco, etapa 3. En el banco, el código de huella digital H1 calculado a partir del material recibido desde la máquina de pago se compara con el código de huella digital firmado digitalmente $H1_{ds}$ recibido desde la estación móvil, y si los dos códigos de huella digital coinciden, entonces se aprueba la transacción de firma. Después de esto, usando un servidor, se añade un sello de tiempo y se presenta la transacción de firma obtenida de este modo. El banco también puede ser algún otro proveedor de servicio correspondiente, tal como una compañía de tarjetas de crédito, en cuyo caso, además de la descripción anterior, se envía al banco una confirmación de la autenticidad de la firma, la máquina de pago u otro proveedor de servicio. En este caso, la compañía de tarjetas de crédito, después de confirmar la firma, toma la responsabilidad de la transacción.

Con referencia a la Fig. 3, se describirá una realización preferida de la invención. En primer lugar, se genera el material a firmar por medio de una estación móvil, bloque 31. A partir del material, se calcula un primer código de huella digital H1, bloque 32. A continuación, bloque 45, se realiza una comprobación para establecer si el material tiene que cifrarse antes de la transmisión. Si el material tiene que cifrarse, a continuación el procedimiento va al bloque 46 y el material se cifra usando la clave pública del usuario de la estación móvil. Después del cifrado, el procedimiento pasa al bloque 33. Si el material no necesita cifrado, a continuación la acción procede directamente al bloque 33, donde el material se transfiere a la estación móvil. A continuación, el procedimiento va al bloque 34, y el usuario comprueba el material o la información esencial en el mismo, presentada sobre la pantalla de la estación móvil, en otras palabras, el usuario comprueba si, por ejemplo, el beneficiario y el pago en la factura son correctos. Si el pagador está de acuerdo, en el bloque 35, a continuación la acción procede al bloque 37 y el material se firma. Si el pagador no está de acuerdo en el bloque 35, a continuación el procedimiento va al bloque 36, donde se envía un mensaje de rechazo al remitente del material, por ejemplo, una máquina de pago, y se para el procedimiento. Desde el bloque 37, la acción sigue al bloque 38, donde se generan los datos agregados a partir de la firma digital y el código de huella digital y posiblemente a partir del material recibido, que comprende, por ejemplo, la información

esencial contenida en el formulario, bloque 38. Después de esto, los datos agregados se transfieren a la máquina de pago, bloque 39, desde donde el procedimiento va al bloque 40, donde el código de huella digital calculado a partir del material transferido se compara con el código de huella digital firmado. Si los códigos de huella digital coinciden, bloque 41, entonces la firma se acepta y se realizan las acciones adicionales definidas.

Si en el bloque 40 los códigos de huella digital no coincidieron, entones puede repetirse el procedimiento. En este punto es posible usar un contador para comprobar que el material no se enviará más veces de las acordadas anteriormente. A partir del bloque 40, el procedimiento va al bloque 43, donde se incrementa en 1 el valor de un contador k = k + 1, después de lo cual la acción sigue en el bloque 44, donde se comprueba el valor del contador, indicando este valor el número de veces que se ha transferido el material a la estación móvil. Si el valor excede un límite acordado de antemano, entonces el procedimiento va al bloque 42 y se envía un mensaje de rechazo a la estación móvil. Si el valor del contador es más pequeño que el límite acordado anteriormente, entonces el procedimiento vuelve al bloque 31 y se repite el procedimiento.

La Fig. 4 ilustra un modo preferido de generar y firmar digitalmente el formulario o material. El material a transferir a la estación móvil comprende un identificador de formulario, bloque 51, todos los formularios usados tienen identificadores únicos. Asociado con el identificador de formulario existe una plantilla de formulario, bloque 52; en base a estos, las aplicaciones, el cliente y el proveedor de la aplicación conocen exactamente qué tipo de formulario se está usando en cada caso. Cuando se está generando el material, el identificador del formulario y la plantilla del formulario se encadenan secuencialmente como se ilustra en la Fig. 4, después de lo cual se calcula un primer código de huella digital a partir de los mismos, bloque 54.

En muchos casos, los datos del formulario se añaden al formulario, bloque 53, incluso antes de que el formulario se transfiera a la estación móvil para la firma. En este caso, el identificador del formulario y los datos del formulario se concatenan en el orden indicado en la Fig. 4 y la secuencia de bits obtenida a partir de los mismos se concatena adicionalmente con los dieciséis bytes aleatorios, bloque 55. El primer código de huella digital del bloque 54 se combina con estos datos.

En este punto, el material está listo para transmitirse a la estación móvil, después de lo cual se calcula un segundo código de huella digital a partir del mismo, bloque 56. En la práctica, el segundo código de huella digital se calcula en la estación móvil y se añade al mensaje a firmar, bloque 57. Del mismo modo, los datos de usuario, que el usuario de la estación móvil puede haber completado con información personal cuando se necesite, se han añadido al mensaje a firmar. A este mensaje a firmar preferentemente también se añaden los 16 bytes aleatorios desde el bloque 55, haciendo posible de este modo la verificación de la autenticidad del mensaje firmado generado por la parte que transfiere el material y el usuario de la estación móvil. Después de que se han puesto en secuencia los bytes aleatorios, los datos de usuario y el segundo código de huella digital, el mensaje se firma digitalmente en la estación móvil del usuario. Después de esto, el mensaje puede transmitirse además a una segunda parte, a la máquina de pago o a otra fuente de origen del material.

En resumen, se ha establecido además que la invención pretende implementar un procedimiento y un sistema en el cual un usuario, un proveedor de servicios y un banco, que se han mencionado como un ejemplo, pueden verificar la autenticidad de una firma digital. El objetivo es posibilitar que el material a firmar se ligue a algunos datos de usuario, el formato y la firma digital realizados por el usuario. En otras palabras, debe ser posible enlazar la firma con cierta clase de cadena, que en la práctica corresponde con la cadena usada actualmente en la cual el usuario confirma una compra por su propia firma manual. De forma similar, el objetivo del procedimiento es identificar al firmante de una forma fiable como se requiere y se intenta por el legislador.

La invención no está restringida a los ejemplos mencionados anteriormente, sino que son posibles muchas variaciones dentro de los límites de la esfera de protección definida por las reivindicaciones.

REIVINDICACIONES

1. Un procedimiento para firmar digitalmente un formulario electrónico por medio de una estación móvil, comprendiendo dicho procedimiento las etapas de
transferir el material a firmar, el cual comprende el formulario y/o su identificador y/o información compartida y/o información en campos esenciales del formulario, a la estación móvil,
calcular un primer código de huella digital (H1) a partir del material a firmar;
verificar la autenticidad del material firmado y transferido comparando el código de huella digital firmado con el primer código de huella digital calculado a partir del material antes de la firma, **caracterizado porque**
el primer código de huella digital se combina con el material a firmar; y **porque**
el material combinado transferido a la estación móvil se firma digitalmente por medio de la estación móvil.

2. El procedimiento como se define en la reivindicación 1, **caracterizado porque** el material a firmar se genera a partir de un identificador del formulario y la información en los campos esenciales del formulario.

3. El procedimiento como se define en una cualquiera de las reivindicaciones anteriores 1 – 2, **caracterizado porque**
el material transferido desde una máquina de pago a la estación móvil para la firma también se transfiere desde la máquina de pago a la segunda parte; y el material firmado se transfiere desde la estación móvil a la segunda parte, después de lo cual la segunda parte verifica la autenticidad de la firma.

4. El procedimiento como se define en una cualquiera de las reivindicaciones anteriores 1 – 2, **caracterizado porque**
el material combinado a firmar y el material firmado se cifran antes de transferirse entre una máquina de pago y la estación móvil; y
el material cifrado se descifra antes de la firma y antes de la verificación de la autenticidad.

5. El procedimiento como se define en la reivindicación 3, **caracterizado porque** el material firmado se cifra antes de transferirse entre la estación móvil y la segunda parte; y
el material cifrado se descifra en la segunda parte antes de la verificación de la autenticidad.

6. El procedimiento como se define en una cualquiera de las reivindicaciones anteriores 1 – 5, **caracterizado porque**
el formulario se genera usando una plantilla de formulario acordada con anterioridad provista con un identificador, rellenándose la información en los campos esenciales del formulario en la plantilla del formulario antes de transferirse a la estación móvil.

7. El procedimiento como se define en una cualquiera de las reivindicaciones anteriores 1 – 5, **caracterizado porque**
el código de huella digital se genera usando una función de huella digital.

8. El procedimiento como se define en una cualquiera de las reivindicaciones anteriores 1 – 7, **caracterizado porque**
la firma y/o el cifrado del mensaje se implementa usando un procedimiento de una clave pública y una privada.

9. El procedimiento como se define en una cualquiera de las reivindicaciones anteriores 1 – 8, **caracterizado porque**
el material y/o parte del material se presentan en la estación móvil antes de que se firme el material combinado.

10. El procedimiento como se define en una cualquiera de las reivindicaciones anteriores 1 – 9, **caracterizado porque**
la estación móvil se arranca en un modo de firma antes de la transferencia del material dentro de la estación móvil.

11. El procedimiento como se define en una cualquiera de las reivindicaciones anteriores 1 – 10, **caracterizado porque**
el material firmado se sella con un sello de tiempo, y
se presenta una transacción de la firma del material combinado después de que la firma se ha autenticado.

12. Un sistema para firmar digitalmente un formulario electrónico por medio de una estación móvil (MS), comprendiendo dicho sistema
una máquina de pago (2);
un medio (3) conectado a la máquina de pago para la generación del material a firmar, comprendiendo dicho material un formulario y/o su identificador y/o la información compartida
y/o información en campos esenciales del formulario; y un medio (4) conectado a la máquina de pago para la transferencia del material al interior de la estación móvil (MS);
comprendiendo la máquina de pago un medio para calcular un primer código de huella digital (H1) a partir del material a firmar;
comprendiendo la máquina de pago un medio (7) para la verificación de la autenticidad del material firmado y

transferido comparando el código de huella digital firmado ($H1_{da}$) con el primer código de huella digital (H1) calculado a partir del material antes de la firma, **caracterizado porque**
la máquina de pago comprende un medio para la combinación del primer código de huella digital con el material a firmar; y
la estación móvil comprende un medio de firma para la firma del material combinado transferido a su interior.

13. El sistema como se define en la reivindicación 12, **caracterizado porque** el sistema comprende
un servidor (8) conectado a la máquina de pago (2) y la estación móvil (MS) y controlado por una segunda parte; y
la estación móvil comprende un medio para el cifrado del material firmado.

14. El sistema como se define en las reivindicaciones 12 ó 13, **caracterizado porque** el servidor (8) comprende
un medio (9) para la verificación de la autenticidad de la firma digital.

15. El sistema como se define en una cualquiera de las reivindicaciones anteriores 12 – 14, **caracterizado porque** la estación móvil comprende
un medio (10) para presentar el material y/o parte del material de la estación móvil (MS) antes de la firma del material combinado.

16. El sistema como se define en una cualquiera de las reivindicaciones anteriores 12 – 15, **caracterizado porque** el servidor (8) comprende
un medio (11) para el sellado del material combinado firmado con un sello de tiempo; y
un medio (12) para presentar una transacción de la firma del material combinado después de que la firma se ha autenticado.

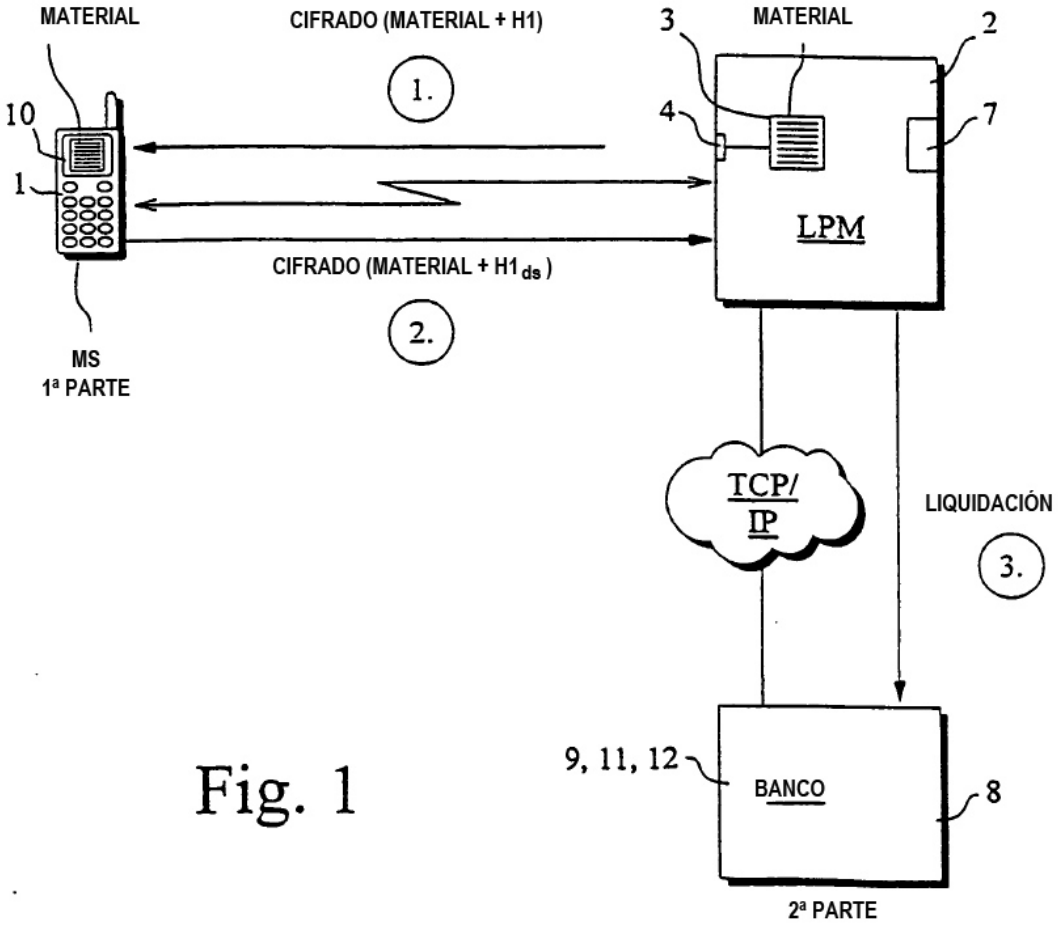
MATERIAL
CIFRADO (MATERIAL + H1)
1.
3
MATERIAL
2
10
4
7
1
LPM
CIFRADO (MATERIAL + H1 ds)
2.
MS
1ª PARTE
TCP/
IP
LIQUIDACIÓN
3.
9, 11, 12
BANCO
8
2ª PARTE

Fig. 1

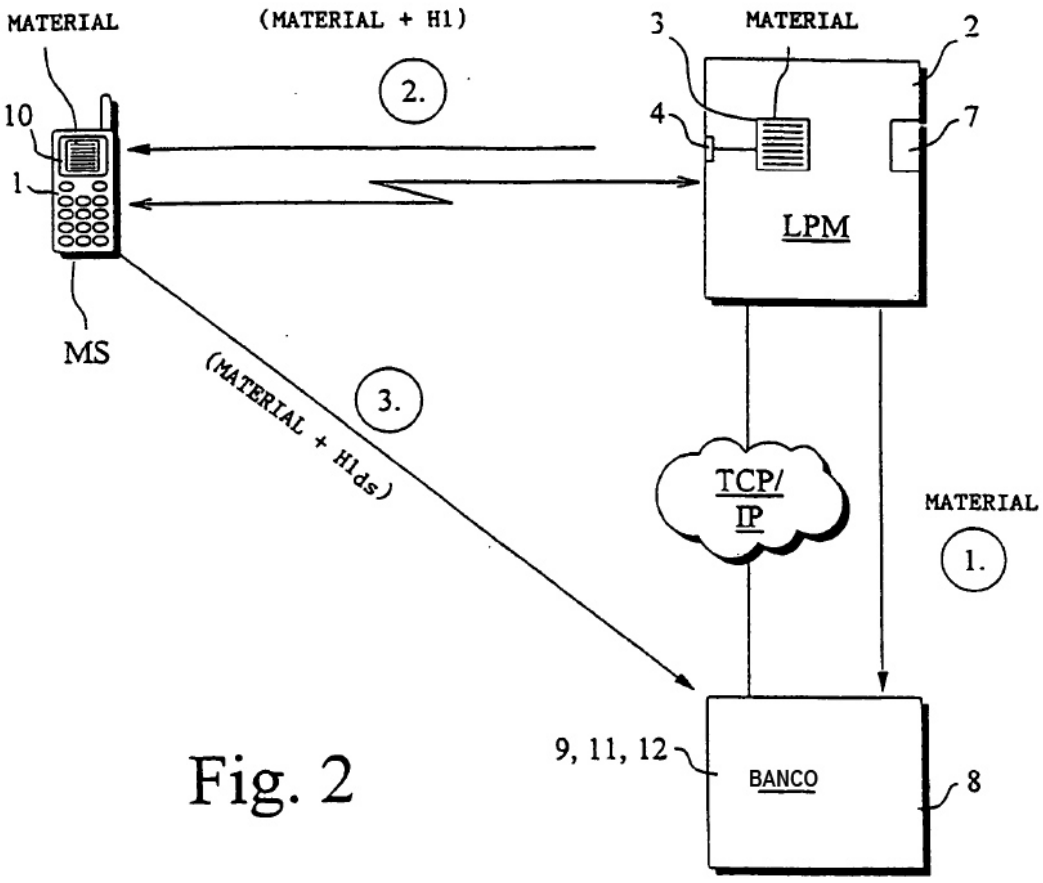
MATERIAL
(MATERIAL + H1)
2.
3
MATERIAL
2
10
4
7
1
LPM
MS
(MATERIAL + H1ds)
3.
TCP/
IP
MATERIAL
1.
9, 11, 12
BANCO
8

Fig. 2

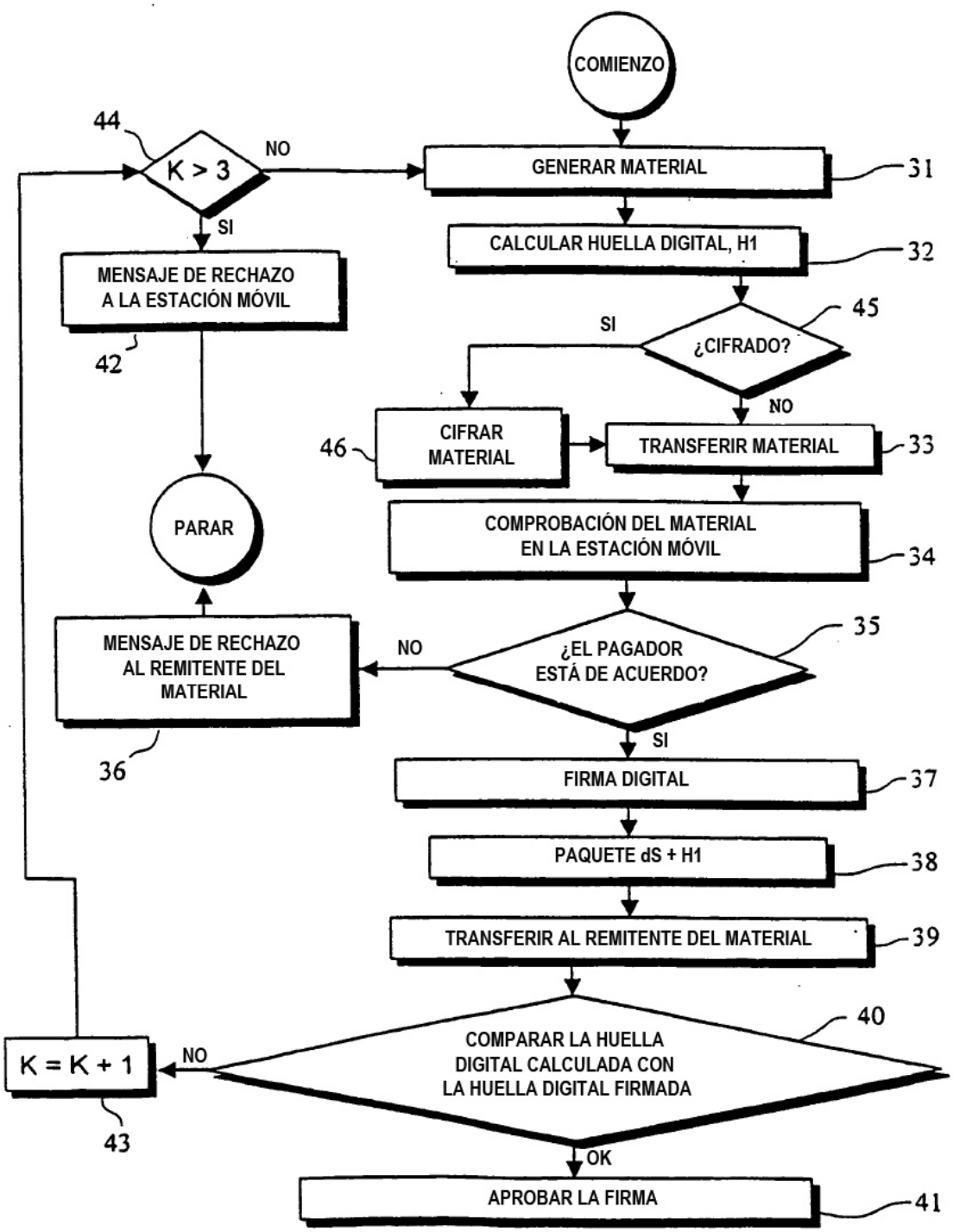
COMIENZO
GENERAR MATERIAL
31
CALCULAR HUELLA DIGITAL, H1
32
¿CIFRADO?
45
SI
NO
CIFRAR MATERIAL
46
TRANSFERIR MATERIAL
33
COMPROBACIÓN DEL MATERIAL EN LA ESTACIÓN MÓVIL
34
¿EL PAGADOR ESTÁ DE ACUERDO?
35
NO
SI
MENSAJE DE RECHAZO AL REMITENTE DEL MATERIAL
36
FIRMA DIGITAL
37
PAQUETE dS + H1
38
TRANSFERIR AL REMITENTE DEL MATERIAL
39
COMPARAR LA HUELLA DIGITAL CALCULADA CON LA HUELLA DIGITAL FIRMADA
40
OK
APROBAR LA FIRMA
41
K > 3
44
NO
SI
MENSAJE DE RECHAZO A LA ESTACIÓN MÓVIL
42
PARAR
K = K + 1
43
NO

Fig. 3

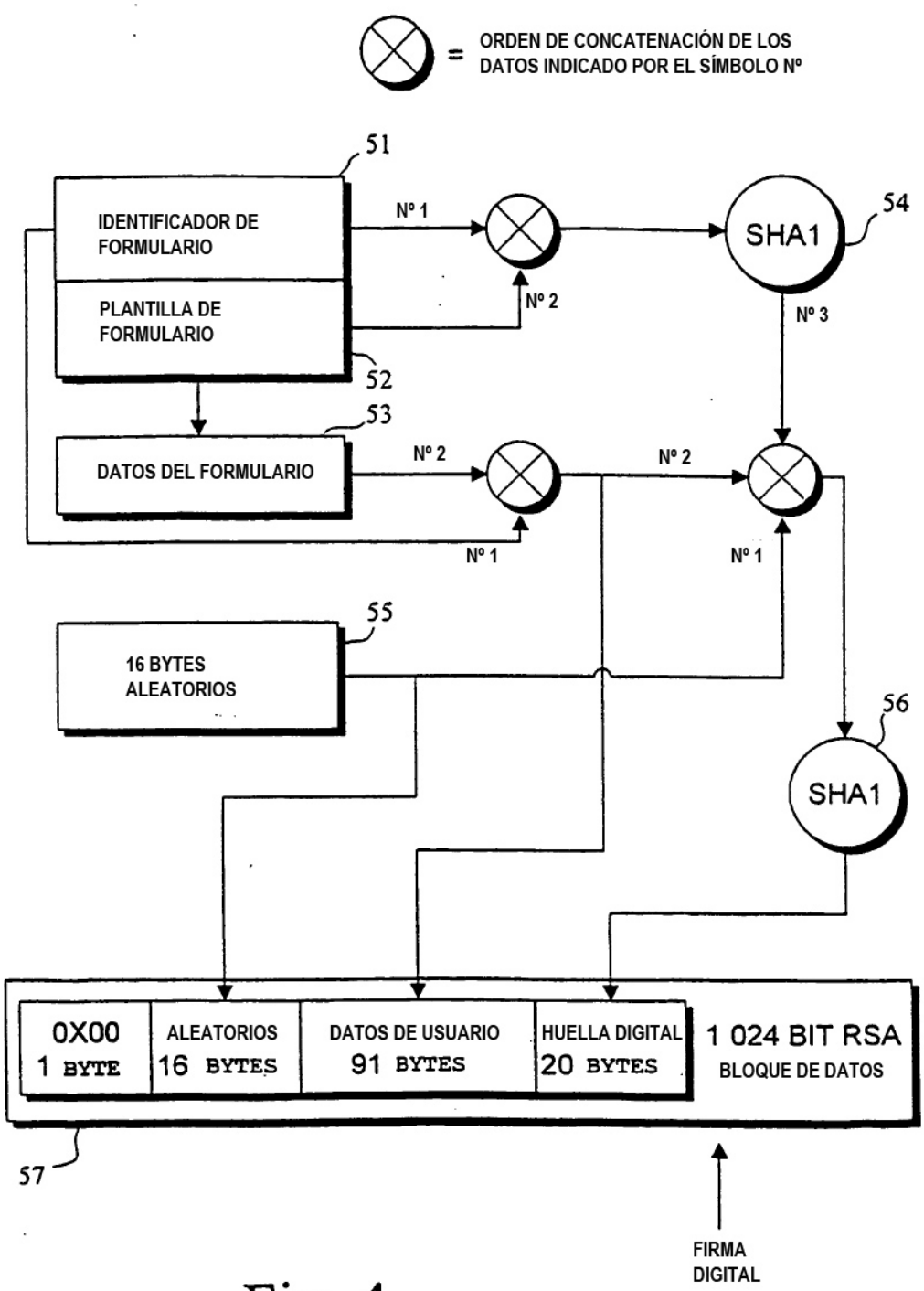
= ORDEN DE CONCATENACIÓN DE LOS DATOS INDICADO POR EL SÍMBOLO Nº
51
IDENTIFICADOR DE FORMULARIO
PLANTILLA DE FORMULARIO
52
Nº 1
Nº 2
SHA1
54
Nº 3
53
DATOS DEL FORMULARIO
Nº 2
Nº 2
Nº 1
Nº 1
55
16 BYTES ALEATORIOS
56
SHA1
0X00
1 BYTE
ALEATORIOS
16 BYTES
DATOS DE USUARIO
91 BYTES
HUELLA DIGITAL
20 BYTES
1 024 BIT RSA
BLOQUE DE DATOS
57
FIRMA DIGITAL

Fig. 4