(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 972 228**

(51) Int. Cl.:

G06F 21/16 (2013.01)
G06F 21/36 (2013.01)
H04N 1/32 (2006.01)
G06F 21/64 (2013.01)
H04N 1/00 (2006.01)
G06F 16/2457 (2009.01)
G07C 9/35 (2010.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **07.02.2014 PCT/EP2014/052498**

(87) Fecha y número de publicación internacional: **14.08.2014 WO14122297**

(96) Fecha de presentación y número de la solicitud europea: **07.02.2014 E 14703103 (3)**

(97) Fecha y número de publicación de la concesión europea: **29.11.2023 EP 2954449**

(54) Título: **Autenticación de firma manuscrita digitalizada**

(30) Prioridad:

08.02.2013 FR 1351087

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.06.2024

(73) Titular/es:

BANKS AND ACQUIRERS INTERNATIONAL HOLDING (100.0%)
28-32 boulevard de Grenelle
75015 Paris, FR

(72) Inventor/es:

CECE, PHILIPPE

(74) Agente/Representante:

ARIAS SANZ, Juan

DESCRIPCIÓN

Autenticación de firma manuscrita digitalizada

1. Campo de la invención

La invención se refiere al campo de la autenticación. Más particularmente, la invención se refiere al campo de la autenticación de firmas manuscritas.

2. Técnica anterior

Durante determinados actos de vente, de contractualización o de suscripción, es necesario que el suscriptor aporte una firma manuscrita. Con el fin de facilitar la gestión de estos documentos, cada vez resulta más habitual desmaterializar, directamente o con posterioridad, los documentos así como la firma, con el uso de datos biométricos o no, para conservar únicamente un soporte digital.

Por tanto, desde un punto de vista legal y con frecuencia psicológico, siempre es necesario disponer de una firma manuscrita en un determinado número de documentos. Por tanto, existe una necesidad de proponer una solución que permita respetar las exigencias legales y tranquilizar a los usuarios preocupados por ver aparecer una firma manuscrita al tiempo que se garantice que esta firma respeta las disposiciones de la directiva 1999/93/CE.

A partir de la técnica anterior, se conocen métodos y dispositivos que permiten introducir la firma de un individuo en un soporte informático. Tales dispositivos se usan, por ejemplo, por agentes de los servicios postales o por transportistas para validar la recepción, por un destinatario, de un paquete o de una carta entregado en propia mano. El uso de tales dispositivos de firmas permite sustituir el resguardo en papel por un resguardo electrónico. Tal resguardo electrónico permite simplificar la gestión de los acuses de recibo para organismos que usan tales métodos. En cambio, en lo que se refiere a la seguridad, los dispositivos existentes no presentan buenas prestaciones. En efecto, estos dispositivos no están realizados para tener en cuenta exigencias legales de autenticación de firma. Por el contrario, los dispositivos existentes tienen como única función la toma de la firma y su digitalización. Dado que el objetivo de estos dispositivos es el de sustituir la firma en papel por una firma digitalizada, una protección de estas firmas solo se tiene en cuenta de manera poco frecuente.

Por el contrario, en el campo de la protección de los intercambios electrónicos (tal como, por ejemplo, entre un cliente y un servidor), existen numerosos mecanismos que garantizan que la información intercambiada es confidencial. Estos mecanismos se ponen en práctica por medio de claves asimétricas o de claves compartidas. A partir de estas claves, la información se intercambia de una manera cifrada. Evidentemente, existen numerosas variaciones y numerosos métodos que permiten garantizar que solo el depositario de una clave o de un par de claves puede cifrar o descifrar una información. Estos mecanismos permiten concretamente poner en práctica una firma denominada “digital” (también denominada firma electrónica) de documentos. De manera general, una firma digital permite garantizar la integridad de un documento electrónico y autenticar a su autor. Una firma digital presenta características que permiten al lector de un documento identificar a la persona o al organismo que ha estampado su firma y que garantizan que el documento no ha sido alterado entre el instante en el que lo ha firmado el autor y el momento en el que lo consulta el lector. Las características que deben cumplirse para que una firma digital sea conforme a las expectativas son las siguientes: la autenticidad de la identidad del firmante, el carácter infalsificable de la firma, la imposibilidad de reutilizar la firma para otro documento, la inalterabilidad del documento firmado y la irrevocabilidad de la firma.

Ahora bien, teniendo en cuenta el estado de la técnica, estas características no se cumplen con frecuencia en los dispositivos actuales de introducción de firma manuscrita. Por tanto, pocos dispositivos existentes permiten una introducción de firma manuscrita que responda a las características anteriores. Algunos sistemas existentes presumen de poder proporcionar una firma manuscrita digitalizada que cumple con la directiva del Parlamento europeo y del Consejo del 13 de diciembre de 1999 (1999/93/CE). Se trata, por ejemplo, de la sociedad Wacom™. No obstante, los sistemas existentes, entre ellos los de Wacom™, necesitan el uso de un dispositivo externo complementario (denominado “tableta” para firmas). Por otro lado, tal como se explica por Wacom™, la comunicación con el dispositivo de Wacom™ puede controlarse por medio de un entramado, que conoce todo el mundo y que permite, como mínimo, desarrollar un software malicioso para el acceso al dispositivo. Por tanto, hay un fallo de seguridad presente en los sistemas actuales. Además, las soluciones actuales ofrecen un acceso “en abierto” a los datos biométricos producidos (son las firmas de los clientes). Esto es contrario a las disposiciones de la directiva europea 95/46/CE, que estipula que tales datos biométricos no deben ser objeto de una difusión no controlada.

El documento WO 2010/037407 A1 (STEPOVER; GUENTHER ANDREAS) del 8 de abril de 2010 describe un método de captura de firma manuscrita que permite firmar un documento de manera biométrica y electrónica. El sistema (ilustrado en la figura 1 y en la figura 4) de firma del documento WO 2010/037407 comprende un ordenador que tiene un monitor configurado para visualizar un documento electrónico que va a firmarse, y un dispositivo de captura de firma que tiene un segundo monitor. El dispositivo de captura de firma permite capturar la firma y los datos biométricos de la firma. En cambio, el documento WO 2010/037407 no permite garantizar la inviolabilidad de la firma al tiempo que se conserve un aspecto visual de esta inviolabilidad: más particularmente, no se visualiza ningún factor aleatorio

en el documento WO 2010/037407.

El documento US 2005/132196 A1 (DIETL JOSEF [DE]), del 16 de junio de 2005, se refiere a la firma de documentos electrónicos. En una realización, se calcula un resumen criptográfico unidireccional para un documento electrónico y se incorpora una marca de agua digital que representa el resumen criptográfico unidireccional en un documento de firma. Basándose en una entrada de un usuario, se modifica el documento de firma que comprende la marca de agua digital integrada y se asocia el documento electrónico al documento de firma. El documento electrónico y el documento de firma constituyen juntos un documento electrónico firmado. La entrada del usuario puede incluir información biométrica, tal como una firma manuscrita o una grabación vocal. Para mayor seguridad, el resumen criptográfico unidireccional puede cifrarse antes de que se incorpore una representación del resumen criptográfico en el documento de firma. Por tanto, el documento US 2005/132196 A1 describe el uso de una imagen (documento electrónico), pero esta imagen se selecciona aleatoriamente en un banco de imágenes: no es posible evitar el uso de una misma imagen en repetidas ocasiones.

3. Sumario de la invención

La invención no presenta estos problemas de la técnica anterior. En efecto, la invención permite a la vez proporcionar una firma manuscrita digitalizada al tiempo que se garantizan las propiedades necesarias para su validación según las exigencias legales.

Más particularmente, la invención se presenta en forma de un procedimiento de creación de firma digitalizada. Según la invención, un procedimiento de este tipo comprende:

- una etapa de introducción de una firma, que suministra una firma digitalizada;

- una etapa de obtención de al menos un dato relativo a un contexto asociado a dicha firma digitalizada, que comprende una obtención de un dato aleatorio representativo de un fondo de imagen aleatorio;

- una etapa de combinación de dicha firma digitalizada y de dicho al menos un dato de contexto, que suministra una firma contextualizada.

Por tanto, la invención permite combinar, en una única firma, elementos que permiten identificar claramente el objeto de esta firma. Por tanto, el objeto de la firma está vinculado, de manera inalterable, a la propia firma. Por otro lado, dado que la imagen puede imprimirse, la invención también permite disponer de una prueba física de la firma del acto además de una prueba digital.

Según la invención, el procedimiento anteriormente mencionado se pone en práctica en el interior de un recinto protegido. Un recinto protegido de este tipo puede presentarse, por ejemplo, en forma de un terminal protegido, tal como un terminal de pago, que comprende un dispositivo o un mecanismo de digitalización de firma manuscrita.

Según una característica particular, la etapa de obtención de al menos un dato relativo a un contexto comprende al menos una etapa de obtención de un dato aleatorio.

Dado que el dato aleatorio también se obtiene en el momento de la obtención de los datos de contexto, también está vinculado al acto. Por tanto, un atacante que desea usurpar la firma también tendrá que recuperar este dato aleatorio, lo cual es muy complejo.

Según una característica particular, dicha etapa de obtención de dicho dato aleatorio comprende al menos una etapa de cálculo de un dato representativo de un fondo de imagen aleatorio.

Según una característica particular, dicha etapa de cálculo de dicho dato representativo de un fondo de imagen aleatorio comprende una etapa de aplicación, en una imagen sin procesar, de un ruido aleatorio.

Según una realización particular dicha etapa de obtención de firma comprende además una etapa de obtención de al menos un dato biométrico de dicho usuario.

Por tanto, este dato biométrico puede usarse en el marco de la creación del contexto. La etapa de obtención de firma también comprende una etapa de obtención de una imagen digitalizada y de otros parámetros, tales como, por ejemplo, el método empleado para realizar la captura de firma.

Según una realización particular, dicho procedimiento comprende además:

- una etapa de cálculo, con la ayuda de dicho al menos un dato relativo a un contexto y de dicha al menos una firma digitalizada, de al menos un dato oculto;

- una etapa de inserción, en el interior de dicha firma contextualizada, de dicho al menos un dato oculto.

El dato biométrico anteriormente obtenido puede usarse, según una realización particular, para calcular el dato oculto, haciendo de ese modo que la falsificación de la firma sea casi imposible.

Según una realización particular, dicha etapa de inserción en el interior de dicha firma contextualizada, de dicho al menos un dato oculto, comprende una etapa de cálculo de una marca de agua digital a partir de dicho al menos un dato oculto y en que dicha etapa de inserción de dicho al menos un dato oculto consiste en la aplicación, en el interior de dicha firma contextualizada, de dicha marca de agua digital.

Según una realización particular, dicha etapa de inserción en el interior de dicha firma contextualizada consiste en insertar dicho al menos un dato oculto, en el interior de metadatos de dicha firma contextualizada.

La invención también se refiere a un dispositivo de creación de firma digitalizada contextualizada, representativa de una firma realizada por un usuario.

Según la invención, un dispositivo de este tipo comprende:

- medios de obtención de al menos un dato relativo a un contexto;

- medios de obtención de una firma, que suministran una firma digitalizada;

- medios de combinación de dicha firma digitalizada y de dicho al menos un dato de contexto, que suministran una firma contextualizada.

Según una implementación preferida, las diferentes etapas de los procedimientos según la invención se ponen en práctica mediante uno o varios software o programas informáticos, que comprenden instrucciones de software destinadas a ejecutarse por un procesador de datos de un módulo de retransmisión según la invención y que está diseñado para controlar la ejecución de las diferentes etapas de los procedimientos.

Por consiguiente, la invención también se refiere a un programa, susceptible de ejecutarse por un ordenador o por un procesador de datos, comprendiendo este programa instrucciones para controlar la ejecución de las etapas de un procedimiento tal como se mencionó anteriormente.

Este programa puede usar cualquier lenguaje de programación y estar en forma de código fuente, código objeto o código intermedio entre código fuente y código objeto, tal como en una forma parcialmente compilada o en cualquier otra forma deseable.

La invención también se refiere a un soporte de información legible por un procesador de datos, y que comprende instrucciones de un programa tal como se mencionó anteriormente.

El soporte de información puede ser cualquier entidad o dispositivo que pueda almacenar el programa. Por ejemplo, el soporte puede comprender un medio de almacenamiento, tal como una ROM, por ejemplo un CD-ROM o una ROM de circuito microelectrónico, o incluso un medio de grabación magnético, por ejemplo un disquete (disco flexible) o un disco duro.

Por otro lado, el soporte de información puede ser un soporte transmisible tal como una señal eléctrica u óptica, que puede dirigirse mediante un cable eléctrico u óptico, por radio o mediante otros medios. En particular, el programa según la invención puede descargarse en una red de tipo Internet.

Alternativamente, el soporte de información puede ser un circuito integrado en el que está incorporado el programa, estando el circuito adaptado para ejecutar o para usarse en la ejecución del procedimiento en cuestión.

Según una realización, la invención se pone en práctica por medio de componentes de software y/o de hardware. En este sentido, el término “módulo” puede corresponder en este documento tanto a un componente de software como a un componente de hardware o a un conjunto de componentes de hardware y de software.

Un componente de software corresponde a uno o varios programas informáticos, uno o varios subprogramas de un programa, o, de manera más general, a cualquier elemento de un programa o de un software adecuado para poner en práctica una función o un conjunto de funciones, según lo que se describe a continuación para el módulo en cuestión. Un componente de software de este tipo se ejecuta por un procesador de datos de una entidad física (terminal, servidor, pasarela, descodificador, enrutador, etc.) y es susceptible de acceder a los recursos de hardware de esta entidad física (memorias, soportes de grabación, bus de comunicación, tarjetas electrónicas de entradas/salidas, interfaces de usuario, etc.).

Del mismo modo, un componente de hardware corresponde a cualquier elemento de un conjunto físico (o de hardware) adecuado para poner en práctica una función o un conjunto de funciones, según lo que se describe a continuación

para el módulo en cuestión. Puede tratarse de un componente de hardware programable o con procesador integrado para la ejecución de software, por ejemplo un circuito integrado, una tarjeta de chip, una tarjeta de memoria, una tarjeta electrónica para la ejecución de un microsoftware (firmware), etc.

Evidentemente, cada componente del sistema anteriormente descrito pone en práctica sus propios módulos de software.

Las diferentes realizaciones mencionadas anteriormente pueden combinarse entre sí para la puesta en práctica de la invención.

4. Figuras

Otras características y ventajas de la invención se desprenderán más claramente de la lectura de la siguiente descripción de una realización preferible, facilitada únicamente a modo de ejemplo ilustrativo y no limitativo, y de los dibujos adjuntos, entre los que:

- la figura 1 es un ejemplo de firma contextualizada en el sentido de la invención;

- la figura 2 describe el método de creación de una firma contextualizada en el sentido de la invención;

- la figura 3 describe un método de verificación de firma contextualizada en el sentido de la invención

- la figura 4 ilustra un método de proporcionar una prueba de firma en el sentido de la invención

- la figura 5 ilustra un dispositivo adecuado para realizar una creación de una firma contextualizada.

5. Descripción de una realización

5.1. Recordatorio del principio de la invención

Tal como se describió anteriormente, se ha constatado que las soluciones actuales no permitían realmente garantizar la autenticidad de las firmas manuscritas digitalizadas para un acto dado y además no garantizan la confidencialidad de los datos personales (por ejemplo, biométricos) del usuario. En la actualidad, la desmaterialización de la firma corresponde habitualmente a una imagen. Por consiguiente, es posible para un comerciante o cualquier otra parte malintencionada copiar esta firma para estamparla en otro contrato, o en una modificación del contrato, o usar la firma obtenida en el marco de cualquier otra operación. Por otro lado, en los casos de desmaterialización de firma con datos biométricos, los sistemas de adquisición biométrica de firma proporcionan el conjunto de los datos a un software de tercero ejecutado en un sistema no protegido. Por tanto, es posible que software de tipo virus puedan recuperar esta información personal y usarla con fines fraudulentos.

La invención permite sellar la asociación de la firma del firmante y de los elementos que identifican el documento contractual en cuestión en el interior del equipo protegido de manera inalterable evitando los fallos anteriormente mencionados.

De manera general, la invención se refiere a la propia firma, a su procedimiento de creación y a los procedimientos que permiten verificar la validez de estas firmas. Para garantizar la confianza y la seguridad entre las dos partes, los inventores proponen usar un equipo dotado de un dispositivo de adquisición digital de la firma, con o sin datos biométricos, así como de un recinto criptográfico que le permite realizar algoritmos a base de una o de varias claves secretas y/o asimétricas. Más particularmente, los inventores se proponen usar terminal de pago por tarjeta y de captura de firma que responde, por ejemplo, a las normas de PCI-PTS. Por tanto, no es necesario disponer de un equipo de tercero para la captura de la firma y, por tanto, un único equipo con funciones de seguridad y de captura de firma es suficiente. Puede usarse un equipo existente (si comprende un dispositivo de captura/grabación de firma). Esto presenta varias ventajas. La primera es no depender de un proveedor de material particular. En efecto, los terminales de pago que responden, por ejemplo, a las normas de PCI-PTS están disponibles de varios fabricantes. El método propuesto es compatible con estos terminales. La segunda ventaja es disponer de un terminal muy protegido (con respecto a los terminales de las sociedades especializadas). En efecto, las “tabletas” de las sociedades especializadas están adaptadas a un uso convencional. Estas “tabletas” no disponen de las mismas medidas de protección que, por ejemplo, las de los terminales de pago de PCI-PTS (que comprenden mecanismos anti-intrusión, mecanismos de borrado de memoria, de clave de algoritmo criptográfico, etc.). Por tanto, en la actualidad, es posible dialogar con una “tableta” existente para obtener, por ejemplo, las claves criptográficas necesarias para el cifrado de la firma (para poder producir posteriormente firmas falsas) o para obtener una digitalización sin procesar de una firma existente.

En cambio, el uso, por ejemplo, de un terminal de PCI-PTS garantiza que este tipo de problema no puede suceder. Por tanto, según la invención, durante la petición de firma, el equipo (por ejemplo, un terminal de PCI-PTS) recibe los datos relativos al acto (de venta, del contrato o de la suscripción). El equipo calcula un certificado de operación relativo

a estos datos, después realiza la adquisición de la firma. Evidentemente, puede sustituirse el uso de un terminal de PCI-PTS por otro tipo de terminal siempre que este terminal garantice, por un lado, una protección de los datos introducidos y, por otro lado, comprenda medios de detección de intrusión y/o de fraude.

Para permitir la certificación de la firma en el punto de venta, de contractualización o de suscripción, el terminal proporciona una firma contextualizada del acto (de compra, de contractualización o de suscripción) en forma de imagen contextualizada (se trata de una imagen específica, tal como se mostrará a continuación). La enorme ventaja es que esta imagen puede imprimirse y servir de recibo de pago. En determinadas realizaciones, este recibo de pago también puede servir de prueba más adelante. Esta firma se describe en relación con la figura 1.

El certificado global 10 (o firma contextualizada o imagen contextualizada) comprende un factor aleatorio 11 (por ejemplo, un fondo aleatorio (por ejemplo, de tipo ruido blanco, habitualmente denominado “nieve”)) en el que están superpuestas al menos otras dos imágenes. La primera imagen 12 comprende los datos relativos al acto (se trata de datos de contexto o datos contextuales), agrupados en un certificado, denominado certificado de operación, calculado por el equipo y que identifica de manera indiscutible este acto. Esta primera imagen 12 también puede contener el conjunto de los datos necesarios para la verificación de este certificado de operación y, dado el caso, de la información legal de uso relativa a la firma contextualizada.

La segunda imagen 13 comprende una restitución gráfica de la firma.

Finalmente, la totalidad o parte de los datos recibidos o adquiridos por el equipo durante el acto así como el certificado de operación (los datos que sirven para la identificación del acto, tales como los identificadores, los importes, fechas y horas, etc.), los datos que sirven para su control y, opcionalmente, los datos legales de uso pueden cifrarse y ocultarse y/o grabarse en la firma contextualizada. Los parámetros biométricos de la firma recopilada pueden formar parte de estos datos así integrados y/o disimulados. Estos datos son invisibles (y, por tanto, no se representan en la figura 1). Pueden presentarse o bien en forma de una marca de agua digital o bien en forma de metadatos, incluidos en la imagen.

Por tanto, la imagen contextualizada final proporcionada por el equipo constituye una firma electrónica en el sentido de la directiva del Parlamento europeo y del Consejo del 13 de diciembre de 1999 (1999/13/EC).

En efecto, la identidad del proveedor del acto, también denominado cocontratante, se garantiza mediante el uso de un terminal y la del suscriptor, también denominado firmante, mediante su firma, de la que él es el único que dispone de los medios de elaboración. La integridad de la firma contextualizada se garantiza mediante el certificado de operación y los datos de la firma manuscrita que se presentan y graban en la imagen. Además, en el caso del uso de datos biométricos, se respeta la protección de estos datos biométricos (que son datos personales), mediante cifrado, según la directiva europea 95/46/CE.

Debido a ello, la invención no necesita un sistema de tercero no controlado (es decir, un tercero que no es de confianza), para producir una firma contextualizada con valor de firma electrónica en el sentido de la directiva 99/13/EC. En cambio, según la invención, tal como se explica a continuación, la presencia de un tercero de confianza puede resultar útil para establecer la prueba de la firma en caso de litigio.

Esta imagen se transmite al dispositivo solicitante o de tercero, si es necesario, con vistas a una eventual impresión, a una copia de seguridad o a un archivado.

5.2. Creación de la firma contextualizada.

En relación con la figura 2, se presentan las diferentes etapas que conducen a la creación de una firma contextualizada en el sentido de la invención. Se recuerda que una firma contextualizada es una firma vinculada a un acto dado, ya se trate de un acto de compra, de venta, de suscripción. Más generalmente, una firma contextualizada es una firma que está relacionada con un contrato o con un compromiso.

Según la invención, en esta realización, la creación de una firma contextualizada comprende una etapa de obtención 200 de una imagen aleatoria 20 (en una realización particular, la imagen aleatoria es una imagen de fondo blanco en la que se aplica un ruido monocromo aleatorio, que a su vez está definido por un factor aleatorio representado en forma de una serie alfanumérica de caracteres). Una vez obtenida esta imagen aleatoria, el procedimiento comprende una etapa de obtención 201 de una firma digitalizada 21. Esta etapa de obtención comprende la introducción de la firma por parte de un usuario en el terminal y/o la obtención de un archivo de firma (archivo SIG que contiene datos biométricos). La etapa de obtención de firma también comprende una etapa de obtención de una imagen digitalizada y de otros parámetros, tales como, por ejemplo, el método empleado para realizar la captura de firma (2D, 3D, tasa de muestreo, etc.). El procedimiento también comprende una etapa de obtención 202 de datos de transacción 22 (o datos transaccionales). Estos datos de transacción corresponden al contexto para el que se realiza la firma. En el caso en el que se trata de una compra, estos datos transaccionales comprenden, por ejemplo, el identificador del vendedor, la fecha y la hora, el importe de la transacción, el identificador del cliente (firmante), el tipo de firma que se realiza para validar la transacción.

Esta última característica está directamente vinculada al contexto. En efecto, en función de los terminales, es posible captar una firma según diversos métodos. Determinadas capturas pueden realizarse únicamente en dos dimensiones. Otras firmas pueden captarse en tres dimensiones. Dado que el comerciante (o el propietario del terminal) conoce el tipo de firma que se capta por el terminal, este tipo de firma está integrado, según la invención, en los datos transaccionales. Esto permite vincular aún más la firma a un contexto particular.

La siguiente etapa consiste en fusionar 203 la imagen aleatoria 20, la firma 21 y una representación gráfica 23 de los datos transaccionales 22 en una única imagen combinada 24. Esta imagen combinada 24 forma, según una primera realización, la firma contextualizada en el sentido de la invención. Según una característica particular, el método comprende además una etapa de construcción 204 de datos ocultos 25 y una etapa de inserción 205, en forma de una marca de agua digital 26 (o de metadatos), de los datos ocultos en dicha imagen combinada 24 para formar una imagen con marca de agua 27. En esta segunda realización, la imagen con marca de agua 27 forma la firma contextualizada.

Según una característica particular, los datos ocultos 25 comprenden datos biométricos y/o los datos transaccionales y/o los datos de construcción de la imagen (por ejemplo, la cadena digital que representa el factor aleatorio usado). Los datos biométricos son datos representativos de la firma capturada 21. En función del método empleado para capturar los datos (por ejemplo, captura de firma en 2D o captura en 3D, con o sin datos de presión) comprendiendo los datos biométricos información de naturaleza más o menos diferente. Por tanto, según la invención, los datos biométricos se integran en la firma contextualizada. En cambio, para cumplir con las disposiciones legislativas en vigor (con la directiva 95/46/CE concretamente), estos datos biométricos, además de ocultarse, no se integran en abierto en la firma. Por el contrario, los datos biométricos se cifran previamente a su integración, en una forma oculta, en la firma contextualizada. Más específicamente, los datos ocultos se cifran previamente usando el material criptográfico del terminal (por ejemplo, del terminal de pago cuando se usa este tipo de terminal). Dado que el terminal está protegido y es seguro, se garantiza de ese modo que solo el propietario del material criptográfico del terminal (el propietario del material criptográfico es, por ejemplo el fabricante del terminal) puede descifrar estos datos cifrados y responder a las necesidades de autenticaciones que pueden surgir tras la firma.

5.3. Determinación de la prueba del acto

Después de haberse creado la firma contextualizada, pueden producirse dos situaciones. La primera situación es la petición, transmitida por un establecimiento de tercero, solicitante, que intenta obtener la prueba de la firma por el contratante (puede ser, por ejemplo, una prueba de pago solicitada por un banco). Según la invención, esta petición se satisface mediante la transmisión de una aserción de validación de la firma contextualizada. El método de entrega de esta aserción se describe en relación con la figura 3.

Pueden producirse dos casos en esta primera situación. En un primer caso 301, el cocontratante 30 (por ejemplo, el comerciante) usa directamente el archivo de imagen protegido (se trata de la firma contextualizada 24, 27) del que dispone. En este caso, puede transmitirlo al solicitante 31 (por ejemplo, a un establecimiento financiero que desea obtener una prueba de la compra o del acto). En un segundo caso, si el establecimiento financiero 31 desea tener la prueba de la autenticidad de esta firma contextualizada 27, el cocontratante 30, que dispone de esta firma contextualizada 27, la transmite 302 a un tercero de confianza 32 encargado de autenticarla. Este tercero de confianza 32, a partir únicamente de esta firma contextualizada 27, va a realizar las operaciones necesarias para la recreación de la firma. En esta realización, se considera que el tercero de confianza 32 dispone del material criptográfico necesario para el descifrado de los datos ocultos 25 de la firma contextualizada 27 (por ejemplo, el tercero de confianza dispone de la clave privada que permite descifrar los datos ocultos 25). Este tercero de confianza 32 puede ser el constructor del terminal que se ha usado para construir la firma contextualizada.

En esta realización de la invención, la siguiente etapa es una etapa de extracción 303 de los datos ocultos 25 seguida por una etapa de descifrado 304 de los datos ocultos 25 que suministra datos biométricos y datos contextuales (DB-DC). Por su parte, el solicitante 31 transmite 305 los datos transaccionales (DT) de los que dispone. A continuación se comparan 306 al menos algunos de los datos (DB-DC) con al menos algunos de los datos transaccionales (DT) y se transmite 307 una aserción A cuando los datos concuerdan. Alternativamente, el tercero de confianza 32 puede recibir los datos transaccionales DT de parte del cocontratante 31 (si éste dispone de los mismos). Alternativamente, el tercero de confianza 32 puede tener ya una copia de los datos transaccionales DT. La invención también se refiere a los programas informáticos y a los dispositivos que permiten poner en práctica el procedimiento que acaba de describirse.

5.4. Verificación de la validez de la firma contextualizada

La segunda situación es aquella en la que es necesario demostrar que una firma no se ha falsificado artificialmente, fuera del método de creación de la firma contextualizada y/o que los datos transaccionales no se han modificado.

El método de verificación se describe en relación con la figura 4.

Este método comprende:

- una etapa de recepción (400), procedente de un depositario (40), por parte de un tercero de confianza (TC), de datos transaccionales (41) que se supone que dan origen a una firma contextualizada (42) de la que se desea verificar la autenticidad (el depositario puede ser el comerciante, la entidad que tiene la calidad de cocontratante o un tercero de confianza en el que se conservan los datos transaccionales);

- una etapa de recepción (401), procedente de un depositario (43), de la firma contextualizada que va a verificarse (42). Puede tratarse del mismo depositario que anteriormente, aunque esto no es obligatorio;

- una etapa de búsqueda (402), en el interior de la firma contextualizada que va a verificarse (42), de una marca de agua digital o de metadatos (44), suministrando un dato de presencia de marca de agua digital o de metadatos; y

  - cuando dicho dato de presencia de una marca de agua digital es positivo, una etapa de obtención (403) de datos ocultos (45);

  - cuando dicho dato de presencia de una marca de agua digital es negativo, una etapa de rechazo (R) de dicha firma contextualizada;

- una etapa de control (404) de los datos ocultos (45); y cuando algunos de dichos datos ocultos corresponden a al menos algunos de dichos datos transaccionales (41) correspondientes,

  - una etapa de cálculo 405 de una firma, que comprende una etapa de descifrado de los datos biométricos, una etapa de construcción, a partir de los datos biométricos comprendidos en los datos ocultos descifrados, de una firma (SG);

  - una etapa de construcción 406, a partir de dichos datos anteriores de una firma contextualizada de referencia (SCR). La construcción comprende, dado el caso, la puesta en práctica del factor aleatorio comprendido en los datos ocultos;

  - una etapa de comparación de dicha firma de referencia SCR y de dicha firma contextualizada 42;

  - cuando las dos firmas son diferentes, una etapa de rechazo (R) de la firma contextualizada;

  - cuando las dos firmas son idénticas, una etapa de verificación 408 de la autenticidad de los datos biométricos (esta verificación se realiza mediante otros medios no descritos en este caso) y, cuando los datos biométricos son correctos, una etapa (409) de transmisión de una información de autenticidad de la firma.

Por tanto, tal como se desprende claramente de la lectura anterior, la firma contextualizada comprende a la vez una firma manuscrita visible e identificable directamente por un usuario y los datos necesarios para la reconstrucción de esta firma para control posterior de su propia autenticidad. Puede realizarse una analogía remota con una célula viva que comprende a la vez sus caracteres propios y los medios para duplicarse para obtener una célula idéntica. La invención también se refiere a los programas informáticos y a los dispositivos que permiten poner en práctica el procedimiento que acaba de describirse.

5.5. Contenido de los datos ocultos

En una realización meramente ilustrativa, los datos ocultos comprenden las siguientes grabaciones de datos:

- al menos un dato de identificación del firmante;

- al menos un dato de identificación del cocontratante (por ejemplo, el comerciante, la entidad emisora del contrato o del acto);

- al menos un dato de datación de la firma;

- al menos un dato de identificación de la firma;

- un dato de identificación de un tercero de confianza,

- un dato de identificación de una clave de cifrado,

- un dato de identificación de una versión de clave;

- un dato de identificación de una derivación de clave;

- una materialización de un factor aleatorio (se trata, por ejemplo, de una serie alfanumérica de una longitud predeterminada);

- datos biométricos cifrados.

Evidentemente, es posible completar o sustituir estos datos ocultos por otros datos que pueden resultar pertinentes en función de un contexto dado.

5.6. Dispositivo de creación de firma contextualizada

En relación con la figura 5, se describe un dispositivo 50 de creación de una firma contextualizada en el sentido de la invención. Un dispositivo de este tipo comprende medios de captura de firma 51. Tales medios son, por ejemplo, una pantalla táctil adecuada para grabar una firma. También puede tratarse de un bloque de firma separado de la visualización de la firma introducida.

En cualquier caso, este dispositivo comprende:

- medios de obtención 52 de al menos un dato relativo a un contexto. Estos medios pueden presentarse en forma de un módulo de software o hardware o incluso de un módulo de red de recepción de información procedente de otro dispositivo. También puede tratarse de todos estos medios a la vez para permitir combinar datos procedentes de varias fuentes;

- medios de introducción de una firma 51, que suministran una firma digitalizada, o bien estos medios integran medios de obtención de datos biométricos (es decir que a partir de la firma realizada, se calculan los datos biométricos mediante estos medios de introducción de firma), o bien estos medios están encargados únicamente de la captura de los datos, que a continuación se procesan y se analizan por otro módulo 53, para producir los datos biométricos;

- medios de combinación 54 de dicha firma digitalizada y de dicho al menos un dato de contexto, que suministran una firma contextualizada. Estos medios de combinaciones, que están integrados en el dispositivo, comprenden, por ejemplo, memorias protegidas que comprenden claves de cifrado, medios de generación de factor aleatorio cuando es necesario, medios de cifrado, medios de formateo de datos, etc. Estos medios pueden ser módulos de software puestos en práctica por un procesador, módulos de hardware, por ejemplo módulos de hardware programables, o incluso un procesador especializado que realiza el conjunto de estas tareas.

Por otro lado, el dispositivo comprende además interfaces (55, 56), por ejemplo interfaces de red R que permiten transmitir y recibir datos informáticos a otros dispositivos, tales como servidores, para permitir, por un lado, la recepción de petición de proporcionar firmas contextualizadas, la transmisión de tales firmas, únicamente de los contextos, etc.

REIVINDICACIONES

1. Procedimiento de creación de firma digitalizada contextualizada, representativa de una firma realizada por un usuario en un dispositivo de introducción de firma para un acto dado, estando el procedimiento caracterizado porque comprende:

- una etapa de obtención de al menos un dato relativo a un contexto, que comprende una obtención de un dato aleatorio representativo de un fondo de imagen calculado de manera aleatoria;

- una etapa de obtención de una firma, que suministra una firma digitalizada;

- una etapa de combinación de dicha firma digitalizada y de dicho al menos un dato de contexto, que suministra una firma contextualizada.

2. Procedimiento según la reivindicación 1, caracterizado porque dicha etapa de obtención de dicho dato representativo de un fondo de imagen aleatorio comprende una etapa de aplicación, en una imagen sin procesar, de un ruido aleatorio.

3. Procedimiento según la reivindicación 1, caracterizado porque dicha etapa de obtención de firma comprende además una etapa de obtención de al menos un dato biométrico de dicho usuario.

4. Procedimiento según la reivindicación 1, caracterizado porque comprende además:

- una etapa de cálculo, con la ayuda de dicho al menos un dato relativo a un contexto y de dicha al menos una firma digitalizada, de al menos un dato oculto;

- una etapa de inserción, en el interior de dicha firma contextualizada, de dicho al menos un dato oculto.

5. Procedimiento según la reivindicación 4, caracterizado porque dicha etapa de inserción en el interior de dicha firma contextualizada, de dicho al menos un dato oculto, comprende una etapa de cálculo de una marca de agua digital a partir de dicho al menos un dato oculto y porque dicha etapa de inserción de dicho al menos un dato oculto consiste en la aplicación, en el interior de dicha firma contextualizada, de dicha marca de agua digital.

6. Procedimiento según la reivindicación 4, caracterizado porque dicha etapa de inserción en el interior de dicha firma contextualizada consiste en insertar dicho al menos un dato oculto en el interior de metadatos de dicha firma contextualizada.

7. Dispositivo de creación de firma digitalizada contextualizada, representativa de una firma realizada por un usuario, caracterizado porque comprende:

- medios de obtención de al menos un dato relativo a un contexto, que comprenden una obtención de un dato aleatorio representativo de un fondo de imagen calculado de manera aleatoria;

- medios de obtención de una firma, que suministran una firma digitalizada;

- medios de combinación de dicha firma digitalizada y de dicho al menos un dato de contexto, que suministran una firma contextualizada.

8. Producto de programa informático descargable desde una red de comunicación y/o almacenado en un soporte legible por ordenador y/o ejecutable por un microprocesador, caracterizado porque comprende instrucciones de código de programa para la puesta en práctica del procedimiento de determinación según una cualquiera de las reivindicaciones 1 a 6.

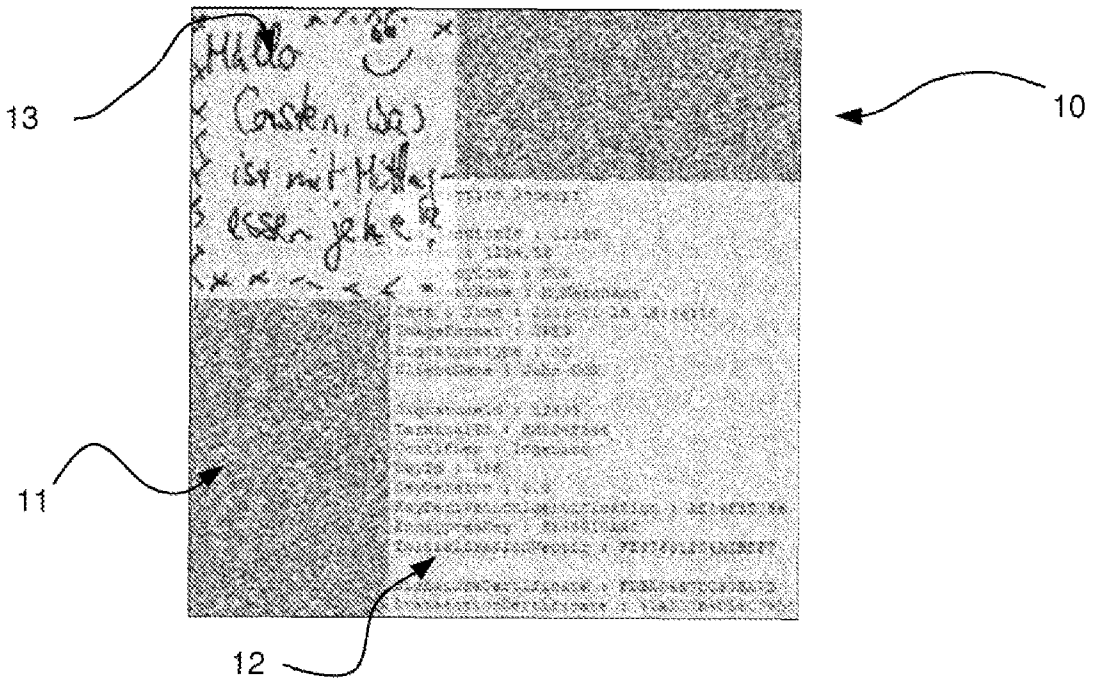

Figura 1

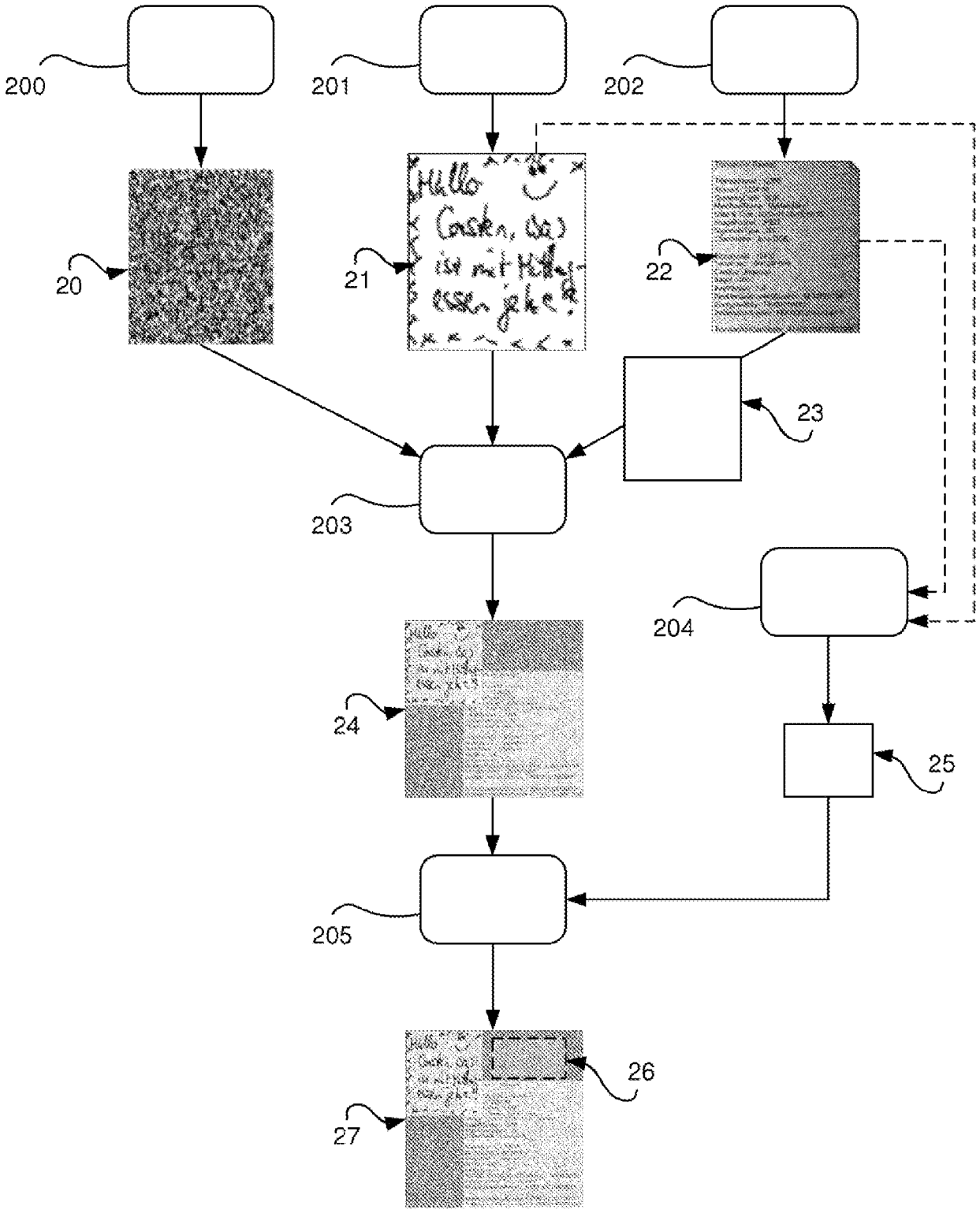

Figura 2

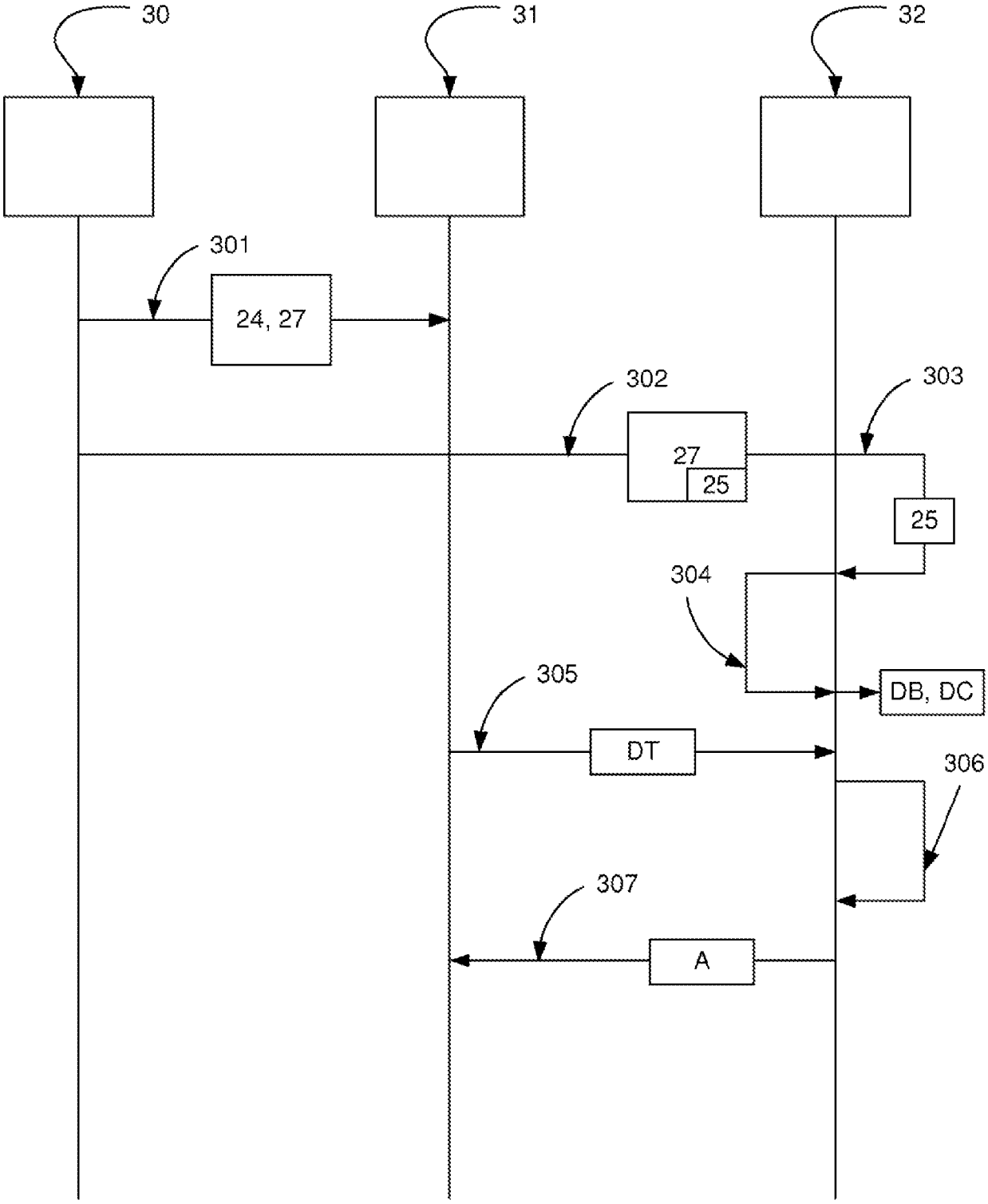

Figura 3

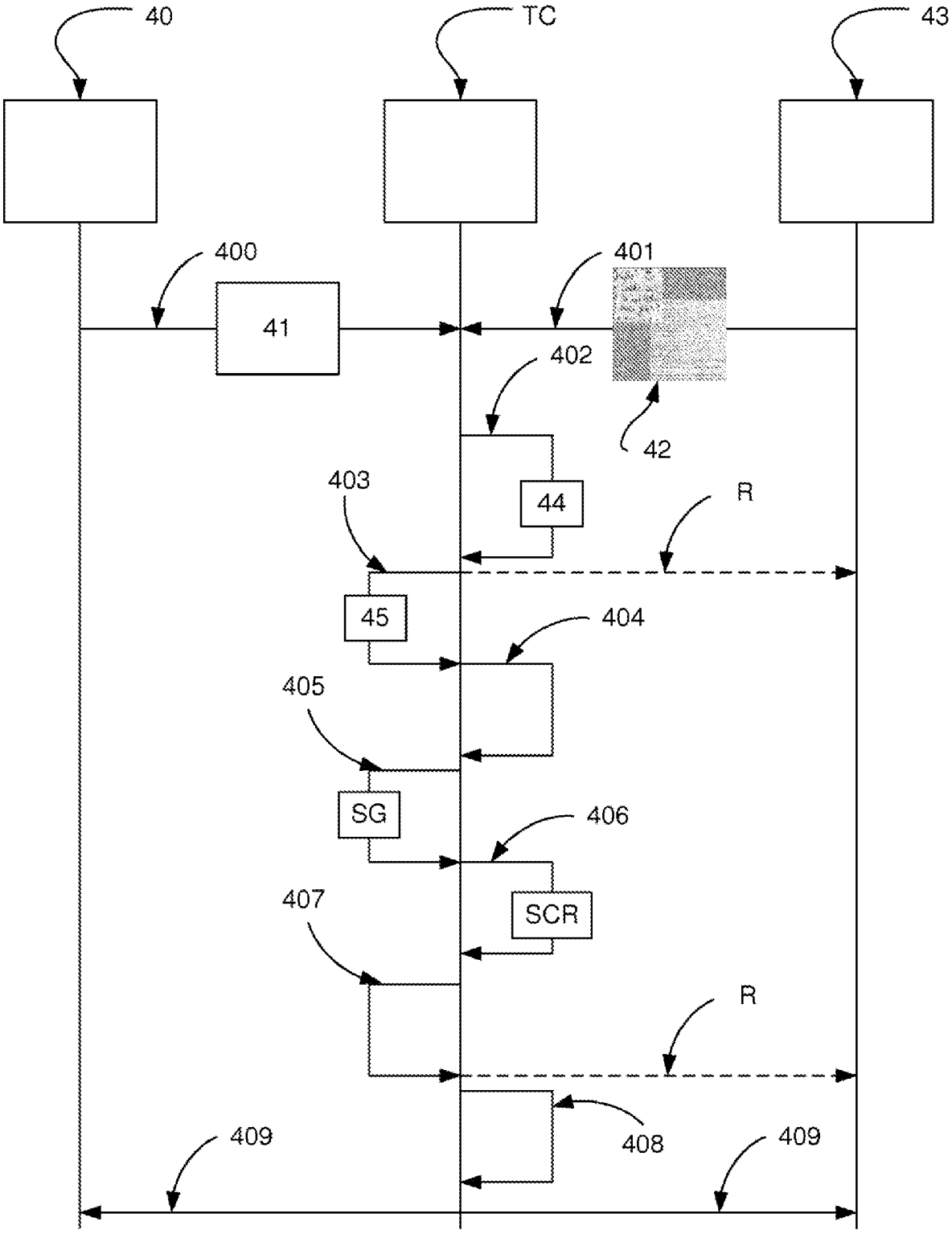
40
TC
43
400
41
401
402
42
403
44
R
45
404
405
SG
406
SCR
407
R
408
409
409

Figura 4

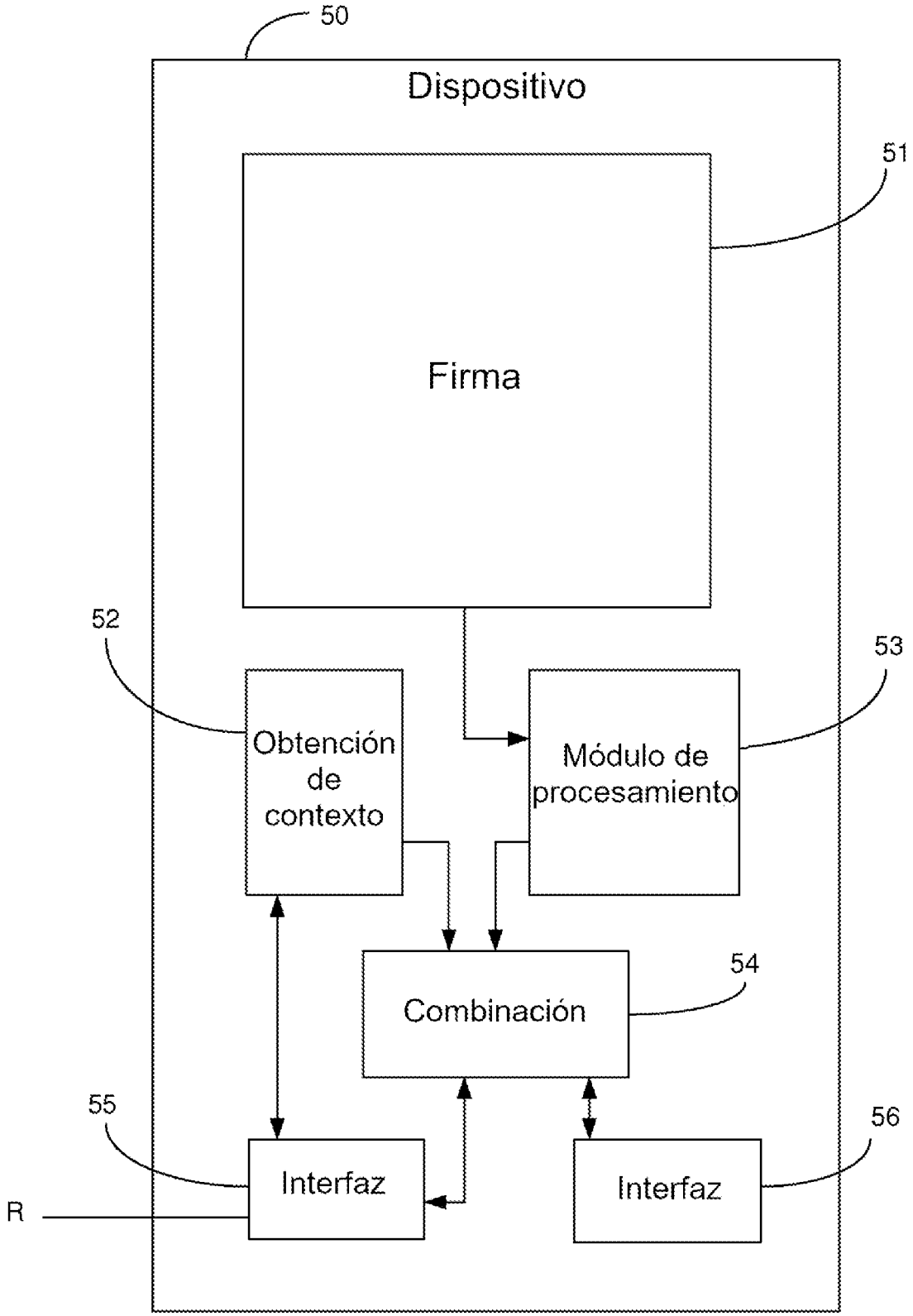
50
Dispositivo
51
Firma
52
Obtención de contexto
53
Módulo de procesamiento
54
Combinación
55
Interfaz
R
56
Interfaz

Figura 5