(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 733 362**

(51) Int. CI.:

H04L 9/06 (2006.01)
H04L 9/32 (2006.01)
G06F 21/42 (2013.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **06.06.2014 PCT/GB2014/051749**

(87) Fecha y número de publicación internacional: **18.12.2014 WO14199128**

(96) Fecha de presentación y número de la solicitud europea: **06.06.2014 E 14730967 (8)**

(97) Fecha y número de publicación de la concesión europea: **10.04.2019 EP 3008852**

(54) Título: **Sistema y método de cifrado**

(30) Prioridad:

12.06.2013 GB 201310468

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
28.11.2019

(73) Titular/es:

CRYPTOMATHIC LTD (100.0%)
327 Cambridge Science Park, Milton Road, Cambridge
Cambridgeshire CB4 0WG, GB

(72) Inventor/es:

FORGET, GUILLAUME;
PEDERSEN, TORBEN PRYDS y
LANDROCK, PETER

(74) Agente/Representante:

RIZZO , Sergio

DESCRIPCIÓN

Sistema y método de cifrado

CAMPO DE LA INVENCIÓN

[0001] Esta invención se refiere a un método y aparato para solicitar y proporcionar una firma digital.

ANTECEDENTES DE LA INVENCIÓN

[0002] Casi 40 años después de que se introdujera el concepto de firma digital, siguen existiendo varios desafíos en lo que se conoce como comercio electrónico. El objetivo es una configuración en la que un usuario pueda firmar digitalmente documentos y transacciones, y la infraestructura subyacente completa proporcione un marco legal seguro que presente la mayoría de las propiedades aceptadas tradicionalmente durante siglos antes de que el comercio se volviera electrónico. En resumen, los principales desafíos son proporcionar un sistema que

1) ofrezca lo que se conoce con la frase hecha de «What You See Is What You Sign» (Lo que se ve es lo que se firma) o «WYSIWYS» y permite que un usuario escoja firmar «lo que ve», de manera que:

2) sea posible aportar pruebas sustanciales y convincentes (sobre todo desde el punto de vista legal) de que esta firma digital específica en ese documento o transacción concreto se genere como un acto voluntario de ese usuario concreto identificado unívocamente.

[0003] El concepto de WYSIWYS lo introdujeron Peter Landrock y Torben Pedersen en «WYS/WYS? What you see is what you sign?» - *Information Security Technical Report*, Elsevier, vol. 3, n.º 2, 1998.

[0004] Otro artículo técnico fundamental es el de Fiat-Shamir titulado «How to Prove Yourself: Practical Solutions to Identification and Signature Problems», *Advances in Cryptology, CRYPTO'86: Proceedings, Lecture Notes in Computer Science,* Springer Verlag, 1986. Este artículo define los siguientes diversos esquemas vinculados con el transporte seguro de datos electrónicos:

Esquemas de autenticación: A puede demostrar a B que es A, pero otra persona no puede demostrar a B que sea A.

Esquemas de identificación: A puede demostrar a B que es A, pero B no puede demostrar a otra persona que sea A.

Esquemas de firma: A puede demostrar a B que es A, pero B no puede demostrar ni siquiera a sí mismo que sea A.

[0005] Se posibilita un esquema de autenticación simplemente al utilizar técnicas de cifrado simétrico con una clave compartida. En un protocolo basado en software, los esquemas de identificación más seguros requerían técnicas de clave pública. Estas técnicas demuestran que la clave privada de A estaba implicada, pero no necesita que su clave se aplique a un mensaje con un contenido elegido. Los esquemas de identificación denominados de conocimiento cero se incluyen en esta categoría. Por último, en el esquema de firma segura, el protocolo subyacente no puede ser simulado por B, al contrario que un esquema de identificación, en el que podría ser posible.

[0006] Un concepto para un esquema de firma era que cada usuario llevara su clave privada almacenada en un dispositivo local de creación de firma, como una tarjeta inteligente o un lápiz de firma que incluya un microchip. Este enfoque presenta algunos inconvenientes importantes, ya que precisa la disponibilidad de un puerto USB y/o un lector de tarjeta inteligente, la escasa idoneidad de utilizar dicho periférico en entornos basados en la red y posibles problemas de compatibilidad entre dispositivos antiguos y modernos o dispositivos que tengan distintas marcas. También resulta fundamental que el usuario mantenga el dispositivo de creación de firma en una ubicación segura que impida su movilidad y facilidad de uso. Este enfoque nunca tuvo éxito realmente en su implantación a nivel nacional, y las tasas de utilización elevadas y la implantación derivada se han limitado a entornos controlados con pocos usuarios.

[0007] En el documento EP 1364508 se describe un enfoque alternativo para un esquema de firma. Este esquema utiliza un dispositivo central (seguro) de creación de firma que almacena de manera centralizada claves privadas para la creación de una firma para un usuario, al mismo tiempo que garantiza que su usuario conserva el control único sobre las mismas. Este enfoque es utilizado ampliamente en la actualidad, p. ej., en Dinamarca, Noruega y Luxemburgo, por casi todos los ciudadanos, empresas y organizaciones de servicios públicos.

[0008] Durante los últimos 30 años, han evolucionado también otras varias soluciones comerciales, que se han vuelto cada vez más avanzadas, debido a que los ataques se han vuelto cada vez más complejos. Las soluciones menos seguras son soluciones que proporcionan cierto grado de seguridad de sesión, que únicamente tratan de identificar al usuario, pero no aseguran el propio mensaje. Por ejemplo, una solución rápida se basaba en el envío de una contraseña estática con el mensaje, y las últimas soluciones se han basado en las denominadas OTP, contraseñas de un solo uso que se envían con el mensaje (generadas, sin embargo,

independientemente del contenido del mensaje). Otras soluciones del estado de la técnica se describen en los documentos: US 2003/0140252 A1 y WO 2013/013262 A1.

[0009] Con la llegada de los teléfonos inteligentes, ha aparecido una gama de nuevas oportunidades. Estas se han aprovechado, por ejemplo, en los documentos EP1969880 y EP1959374, en los cuales, con *hardware* dedicado, cumplirán, de hecho, los dos requisitos anteriores en relación con la autenticación y la identificación, pero a costa de utilizar *hardware* bastante caro.

[0010] No obstante, ninguno de estos enfoques garantiza la propiedad WYSIWYS (que, a menudo, resulta crucial para cumplir su propósito) sin otras medidas, como la confirmación de voz o el uso de canales independientes.

[0011] Una importante forma de realización de WYSIWYS, aunque quizá no sea la más fácil de usar, es CAP, el programa de autenticación de chip (*Chip Authentication Program*), desarrollado por Mastercard y adoptado posteriormente por Visa como DPA (autenticación de contraseña dinámica, *Dynamic Passcode Authentication*), que precisa un lector de tarjetas independiente y una tarjeta de débito o de crédito con chip EMV. Una vez el usuario haya proporcionado los detalles de un pago, por ejemplo, en una estación de trabajo, se le solicita que acople su tarjeta de débito o tarjeta de crédito en el lector de tarjetas tecleando su PIN y eligiendo la función «Firmar». A continuación, se le pide que teclee la cantidad que debe pagar y la cuenta del beneficiario, y su tarjeta de crédito o de débito genera un código de autorización de mensajes (MAC) que se muestra en el lector. Posteriormente, lo teclea junto con su transacción en la estación de trabajo.

[0012] La criptografía tras este método es un sistema de cifrado simétrico con una clave compartida entre la tarjeta de pago y el servidor (*backend*) del banco. Por lo tanto, este parece ser un esquema de autenticación según la definición expuesta anteriormente. No obstante, como la clave de la tarjeta de pago y el *backend* del banco se protegen mediante *hardware* inviolable, presumiblemente, se trata, de hecho, de un esquema de firma, y presenta un uso generalizado en banca electrónica.

[0013] Por consiguiente, se puede conseguir WYSIWYS empleando una combinación de técnicas de cifrado simétrico y *hardware* inviolable. Sin embargo, los esquemas de firma basados en técnicas de clave pública resultan especialmente útiles, si no imprescindibles, en el comercio electrónico, donde muchas partes independientes se comunican con otras partes independientes, al contrario que en la banca electrónica, donde la comunicación es de muchas a una, a saber, el banco. Además, ninguno de los métodos y técnicas descritos anteriormente han abordado la necesidad de proporcionar una importante funcionalidad WYSIWYS dirigida a una firma electrónica legalmente vinculante llevada a cabo por un dispositivo local o central (seguro) de creación de firma, (S)SCD (por sus siglas en inglés), según se define en la Directiva del Parlamento Europeo sobre firma electrónica [Directiva 1999/93/EC] adoptada por todos los Estados miembros y tomada como referencia en muchos otros países del mundo.

[0014] Por el contrario, la principal contribución de la presente invención es cómo generar esta funcionalidad WYSIWYS con la tecnología más novedosa disponible, que actualmente incluye teléfonos inteligentes, tabletas y dispositivos similares.

SUMARIO DE LA INVENCIÓN

[0015] Se definen aspectos de la invención en las reivindicaciones adjuntas 1 a 15.

[0016] Según un primer aspecto de la invención, se proporciona un método para generar una firma en nombre de un usuario que presenta un primer y un segundo dispositivo de usuario, comprendiendo el método

recibir una solicitud desde dicho primer dispositivo de usuario para crear una firma para un primer mensaje M;

generar un desafío de validación utilizando un segundo mensaje M' basado en el primer mensaje M y una primera clave secreta compartida con dicho usuario;

enviar dicho desafío de validación a dicho usuario para permitir que dicho segundo dispositivo de usuario vuelva a generar dicho segundo mensaje M';

recibir un código de validación desde dicho segundo dispositivo de usuario, confirmando dicho código de validación la solicitud para crear una firma; y

generar la firma para el usuario para el primer mensaje M.

[0017] Según un segundo aspecto de la invención, se proporciona un servidor de firma para crear una firma en nombre de un usuario que presenta un primer y un segundo dispositivo de usuario, estando configurado el servidor para

recibir una solicitud desde dicho primer dispositivo de usuario para crear una firma para un primer mensaje M;

generar un desafío de validación utilizando un segundo mensaje M' basado en el primer mensaje M y una primera clave secreta compartida con dicho usuario;

enviar dicho desafío de validación a dicho usuario para permitir que dicho segundo dispositivo de usuario vuelva a generar dicho segundo mensaje M';

recibir un código de validación desde dicho segundo dispositivo de usuario, confirmando dicho código de validación la solicitud para crear una firma; y

generar la firma para el usuario para el primer mensaje M.

[0018] Por consiguiente, una característica fundamental de la invención es la interacción con el primer y el segundo dispositivo de usuario, que, preferiblemente, son independientes entre sí. La solicitud de una firma se recibe desde el primer dispositivo de usuario y se confirma desde el segundo dispositivo de usuario antes de que se cree la firma. Además, el desafío de validación se genera para que se pueda volver a crear el mensaje en el segundo dispositivo de usuario para que un usuario pueda ver el mensaje antes de confirmar la solicitud de firma. En consecuencia, se proporciona la funcionalidad «What You See Is What You Sign» (Lo que se ve es lo que se firma) (WYSIWYS).

[0019] El método es un método implementado en ordenador donde las etapas de generación se llevan a cabo en un procesador dentro de un servidor de firma, y las etapas de recepción y envío se llevan a cabo mediante un sistema de entrada/salida del servidor de firma.

[0020] El servidor de firma puede comprender un dispositivo de creación de firma, por ejemplo, un dispositivo de creación de firma segura, según se define en la Directiva del Parlamento Europeo sobre firma electrónica [Directiva 1999/93/EC]. El dispositivo de creación de firma (más en concreto, el procesador del dispositivo de creación de firma) puede recibir la solicitud para generar la firma y, en última instancia, generar la firma. Preferiblemente, la firma es una firma electrónica avanzada, esto es, una que está vinculada exclusivamente al signatario, que es capaz de identificar al signatario, que se crea utilizando medios que el signatario puede mantener bajo su control exclusivo, y que está vinculada a los datos con los que se le asocia, de modo que se puede detectar cualquier cambio posterior de los datos.

[0021] El servidor de firma puede ser local o remoto con respecto al usuario. Por local, se entiende que el dispositivo de creación de firma pertenece al usuario (esto es, lo maneja el usuario). Por remoto, se entiende que el dispositivo de creación de firma se encuentra físicamente separado del usuario, por ejemplo, en un servidor de firma central que puede ser manejado por una entidad independiente.

[0022] El dispositivo de creación de firma también puede generar el desafío de validación y, por lo tanto, una única entidad proporciona tanto el desafío de validación como la firma. Sin embargo, se requiere aún así la interacción con dos dispositivos de usuario para garantizar la seguridad. En esta configuración, el dispositivo de creación de firma puede ser local en relación con el usuario.

[0023] El servidor de firma puede comprender un servidor de autenticación y validación independiente. El servidor de autenticación y validación (más en concreto, el procesador del servidor de autenticación y validación) puede generar el desafío de validación. El servidor de autenticación y validación puede ser remoto o estar integrado en el dispositivo de creación de firma.

[0024] La primera clave secreta compartida puede estar almacenada en el dispositivo de creación de firma o en el servidor de autenticación y validación en función de cuál esté creando el desafío de validación. Por consiguiente, es necesario que el usuario registre el segundo dispositivo de usuario con el servidor de firma (más en concreto, el dispositivo de creación de firma o el servidor de autenticación y validación que esté creando el desafío de validación) para poder compartir la primera clave secreta compartida.

[0025] El desafío de validación se basa en el segundo mensaje M' que, a su vez, deriva del primer mensaje y, por lo tanto, el desafío de validación deriva del mensaje original. Por consiguiente, si el usuario es capaz de volver a generar el mensaje M' (o posiblemente el mensaje original M) a partir del desafío de validación, el usuario puede estar seguro de que este desafío de validación procede de una fuente fiable. Asimismo, el usuario se puede volver a asegurar de que el mensaje no haya sido modificado antes de presentarse al usuario para su validación como parte del proceso de generación de firma. Por consiguiente, el usuario puede confirmar la solicitud para firmar el mensaje. Esto proporciona la funcionalidad WYSIWYS.

[0026] El segundo mensaje M' puede ser idéntico al primer mensaje M o puede derivar del primer mensaje M. M' está diseñado para mostrarse en un dispositivo portátil. El segundo mensaje M' puede ser una versión abreviada del primer mensaje M para simplificar la visualización por parte del usuario para fines de validación. De manera alternativa, el segundo mensaje M' puede ser una versión distinta del primer mensaje M. El segundo mensaje M' comprende, preferiblemente, suficiente información del primer mensaje M, de modo que, cuando se muestra el segundo mensaje M' al usuario, el usuario puede confirmar que el segundo mensaje M' se refiere al primer mensaje M que se desea firmar. M puede ser, por ejemplo, una orden de compra y M' sería un resumen de esta, por ejemplo, con la referencia del pedido, el destinatario y la cantidad. El segundo mensaje M' se puede crear mediante el dispositivo de creación de firma o se puede crear mediante el primer dispositivo de usuario. Independientemente del lugar en el que se cree, M' se recibe, en última instancia, en el servidor de firma para crear el desafío de validación.

[0027] Preferiblemente, el desafío de validación se genera para que dicho segundo mensaje M' pueda derivar de dicho desafío de validación utilizando dicha primera clave secreta compartida. Por ejemplo, dicho desafío de validación se puede generar mediante cifrado simétrico cifrando dicho segundo mensaje M' con dicha primera clave secreta compartida, de modo que el descifrado de dicho desafío de validación con dicha primera clave secreta compartida vuelva a generar dicho segundo mensaje M'. De manrea alternativa, dicho desafío de validación se puede generar utilizando una primera clave secreta compartida en forma de un código de autenticación de mensajes (MAC). De manera alternativa, el desafío de validación puede ser una versión de M' firmada digitalmente, que se firma con una primera clave secreta compartida en forma de una clave privada asociada al usuario, encontrándose la parte pública de la clave privada en el segundo dispositivo de usuario. Por consiguiente, es necesario registrar previamente el dispositivo para intercambiar o acordar de otro modo la primera clave secreta compartida.

[0028] El desafío de validación se puede enviar de forma directa o indirecta al segundo dispositivo de usuario, por ejemplo, el desafío de validación se puede enviar a través del primer dispositivo de usuario. El método puede comprender, además, volver a formatear el desafío de validación como un código de barras (p. ej., código QR) que se pueda leer mediante el segundo dispositivo de usuario. Se puede mostrar el código de barras en el primer dispositivo de usuario para que se lea mediante el segundo dispositivo de usuario.

[0029] El código de validación se puede recibir de manera directa o indirecta desde el segundo dispositivo de usuario. El código de validación se puede verificar antes de crear la firma. La verificación comprueba que el código de validación ha sido recibido desde el segundo dispositivo de usuario. La verificación se puede llevar a cabo mediante cualquier proceso estándar. Por lo tanto, el código de validación se debe crear utilizando información, a saber, una segunda clave secreta compartida, que sea específica del usuario y, preferiblemente, distinta de la información utilizada para crear el desafío de validación.

[0030] Antes de crear la firma, el servidor de firma necesita verificar que el código de validación procede del usuario. La verificación del código de validación se puede llevar a cabo mediante el servidor de autenticación y validación (en caso de que se utilice uno), y el resultado de la verificación se puede enviar al dispositivo de creación de firma. En este caso, el dispositivo de creación de firma también puede verificar que el resultado procede del servidor de autenticación y validación. De manera alternativa, la verificación del código de validación se puede llevar a cabo mediante el propio dispositivo de creación de firma. Si se utiliza una segunda clave secreta compartida para crear el código de validación, esta se almacena también en el dispositivo que verifica el código de validación. Por consiguiente, es necesario intercambiar o acordar de otro modo la segunda clave secreta compartida como parte del registro previo del dispositivo.

[0031] Preferiblemente, el usuario posee al menos dos dispositivos: el primer dispositivo de usuario y el segundo dispositivo de usuario. Como alternativa, el usuario puede poseer un único dispositivo que combine la funcionalidad del primer y del segundo dispositivo de usuario. Así, el primer dispositivo de usuario puede ser también el segundo dispositivo de usuario. Este único dispositivo debe estar adaptado para proporcionar la doble funcionalidad; por ejemplo, el dispositivo único puede ser capaz de controlar dos canales independientes y/o presentar una interfaz gráfica de usuario fiable. El primer dispositivo de usuario envía la solicitud de firma. El segundo dispositivo de usuario vuelve a generar el segundo mensaje M' a partir del desafío de validación y crea un código de validación que confirma la solicitud para crear una firma. El primer dispositivo de usuario se puede denominar dispositivo de transacción inicial y el segundo dispositivo de usuario se puede denominar dispositivo de validación; estos términos se utilizan indistintamente a lo largo de la memoria descriptiva. El dispositivo de transacción inicial puede ser cualquier dispositivo electrónico, tal como una estación de trabajo, un ordenador portátil, una tableta o un teléfono inteligente. Del mismo modo, el dispositivo de validación puede ser cualquier dispositivo electrónico, aunque, preferiblemente, es un dispositivo electrónico distinto del dispositivo de transacción inicial.

[0032] Según otro aspecto de la invención, se proporciona un dispositivo de validación para que un usuario valide una solicitud de firma para un primer mensaje M, estando configurado el dispositivo de validación para

recibir un desafío de validación desde un dispositivo de creación de firma, habiéndose creado el desafío de validación utilizando un segundo mensaje M' que se basa en el primer mensaje M y una primera clave secreta compartida entre dicho dispositivo de creación de firma y dicho dispositivo de validación;

generar el segundo mensaje M' a partir del desafío de validación utilizando la primera clave secreta compartida;

mostrar el segundo mensaje M' al usuario;

recibir confirmación del usuario de que el segundo mensaje M' corresponde al primer mensaje M;

generar un código de validación que confirme la solicitud para crear la firma; y generar el código de validación.

[0033] Según otro aspecto de la invención, se proporciona un método para solicitar una firma para un primer mensaje M desde un dispositivo de creación de firma, comprendiendo el método

recibir un desafío de validación desde el dispositivo de creación de firma, habiéndose creado el desafío de validación utilizando un segundo mensaje M' que se basa en el primer mensaje M y una primera clave secreta compartida entre dicho dispositivo de creación de firma y dicho usuario;

generar el segundo mensaje M' a partir del desafío de validación utilizando la primera clave secreta compartida;

mostrar el segundo mensaje M' al usuario;

recibir confirmación de que el segundo mensaje M' corresponde al primer mensaje M;

generar un código de validación que confirme la solicitud para crear la firma; y generar el código de validación.

[0034] Las características descritas anteriormente en relación con el primer y el segundo aspecto de la invención se aplican también en estos aspectos de la invención que se refieren al dispositivo y a las etapas seguidas por el usuario. Por ejemplo, el desafío de validación y el segundo mensaje M' pueden habrse generado y transmitido según lo descrito anteriormente.

[0035] El segundo mensaje M' se puede generar a partir del desafío de validación mediante descifrado. Por ejemplo, la primera clave secreta compartida puede ser una clave simétrica. De manera alternativa, el desafío de validación se puede validar utilizando la primera clave secreta compartida mediante la verificación de un código de autenticación de mensajes (MAC) obtenido a partir del desafío de validación. De manera alternativa, la primera clave secreta compartida puede ser una clave privada asociada al usuario, encontrándose la parte pública de la clave privada en el segundo dispositivo de usuario. En este caso, el segundo mensaje M' se puede generar aplicando la parte pública de la clave privada al desafío de validación.

[0036] El código de validación se debe crear utilizando información que sea específica del usuario y, preferiblemente, distinta de la información utilizada para crear el desafío de validación, por ejemplo, una segunda clave secreta compartida. El código de validación se puede generar utilizando diversos métodos estandarizados, incluyendo el algoritmo desafío-respuesta OATH (OCRA, por sus siglas en inglés) [descrito en RFC 6287- ISSN 2070-1721] o tecnología propia equivalente, tal como CAP de MasterCard, CodeSure de Visa [WO2013013262] o mecanismos Digipass basados en desafío-respuesta de Vasco. El código de validación se puede generar utilizando cifrado, siendo la segunda clave secreta una clave simétrica compartida entre el dispositivo de validación y el servidor central de autenticación y validación o el dispositivo de creación de firma (en función del dispositivo que verifique el código de validación). El código de validación también puede ser una respuesta firmada con un número utilizado una sola vez (*nonce*) para evitar ataques de reproducción.

[0037] Según se ha descrito anteriormente, el servidor de firma puede comprender un dispositivo de creación de firma y/o un dispositivo de autenticación y validación. Cuando exista un dispositivo de autenticación y validación, el dispositivo de validación puede recibir el desafío de validación desde el dispositivo de autenticación y validación, y puede generar el código de validación para el dispositivo de autenticación y validación. En este caso, resulta necesario registrar previamente el dispositivo de validación con el dispositivo de autenticación y validación para garantizar que las claves secretas necesarias se han compartido. De manera alternativa, cuando la autenticación se lleve a cabo mediante el propio dispositivo de creación de firma, el dispositivo de validación puede recibir el desafío de validación desde el dispositivo de creación de firma y puede generar el código de validación para el dispositivo de creación de firma.

[0038] El sistema completo para la invención comprende un servidor de firma, un primer dispositivo de usuario (dispositivo de transacción inicial) y un segundo dispositivo de usuario (dispositivo de validación). Según otro aspecto de la invención, se da a conocer un sistema para proporcionar una firma para un mensaje M, comprendiendo el sistema un servidor de firma según se ha descrito anteriormente, un primer dispositivo de usuario según se ha descrito anteriormente y un segundo dispositivo de usuario según se ha descrito anteriormente.

[0039] Según otro aspecto de la invención, se proporciona un sistema que comprende un servidor de firma, un dispositivo de transacción inicial para un usuario y un dispositivo de validación para un usuario, estando configurado el dispositivo de transacción inicial para

mostrar un primer mensaje M; y

enviar una solicitud al servidor de firma para crear una firma para dicho primer mensaje M;

estando configurado el servidor de firma para

generar un desafío de validación utilizando un segundo mensaje M' que se base en dicho primer mensaje M' y una primera clave secreta compartida entre dicho usuario y dicho servidor de firma; y

enviar dicho desafío de validación al dispositivo de validación;

estando configurado el dispositivo de validación para

volver a generar dicho segundo mensaje M' utilizando dicha primera clave secreta compartida; y mostrar dicho segundo mensaje M';

recibir confirmación del usuario de que el segundo mensaje M' mostrado corresponde a dicho primer mensaje M;

generar un código de validación que confirme la solicitud para crear una firma; y enviar dicho código de validación a dicho servidor de firma;

a través de lo cual dicho servidor de firma genera la firma para el usuario para el primer mensaje M.

[0040] Del mismo modo, según otro aspecto de la invención, se proporciona un método que comprende

mostrar un primer mensaje M en un primer dispositivo de usuario;

enviar una solicitud desde dicho primer dispositivo de usuario a un servidor de firma para crear una firma para dicho primer mensaje M;

crear un segundo mensaje M' que se base en el primer mensaje M;

generar un desafío de validación utilizando dicho segundo mensaje M' y una primera clave secreta compartida entre dicho usuario y dicho servidor de firma;

enviar dicho desafío de validación a un segundo dispositivo de usuario;

volver a generar dicho segundo mensaje M' en dicho segundo dispositivo de usuario utilizando dicha primera clave secreta compartida;

mostrar dicho segundo mensaje M' en dicho segundo dispositivo de usuario;

recibir confirmación del usuario de que el segundo mensaje M' corresponde a dicho primer mensaje M;

generar un código de validación que confirme la solicitud para crear una firma;

enviar dicho código de validación desde dicho segundo dispositivo de usuario a dicho servidor de firma; y

generar la firma para el usuario para el primer mensaje M.

[0041] La invención proporciona, además, un código de control de procesador para implementar los sistemas y métodos anteriormente descritos, por ejemplo, en un sistema informático de uso general o en un procesador de señal digital (DSP). El código se proporciona en un soporte físico de datos, tal como un disco, CD-ROM o DVD-ROM, memoria programada, tal como una memoria no volátil (p. ej., *flash*) o memoria de solo lectura (*firmware*). El código (y/o datos) para implementar formas de realización de la invención puede comprender código fuente, código objeto o código ejecutable en un lenguaje de programación habitual (interpretado o compilado), tal como C, o código de ensamblado. Como podrán observar los expertos en la materia, dicho código y/o datos se puede(n) distribuir entre una pluralidad de componentes acoplados en comunicación entre sí.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

[0042] La invención se representa, a título ilustrativo, mediante diagramas en los dibujos adjuntos, en los cuales:

la figura 1a es un diagrama de flujo de las etapas seguidas por los diversos dispositivos en el sistema;

la figura 1b es un mensaje de muestra;

la figura 2a es un diagrama esquemático para una configuración del sistema que muestra el flujo de información a través del sistema;

las figuras 2b y 2c son un diagrama de flujo para la implementación que se muestra en la figura 2a;

la figura 3a es un diagrama esquemático del sistema para otra configuración del sistema;

las figuras 3b y 3c son un diagrama de flujo para la implementación que se muestra en la figura 3a;

la figura 4a es un diagrama esquemático del sistema para otra configuración del sistema;

las figuras 4b y 4c son un diagrama de flujo para la implementación que se muestra en la figura 4a;

la figura 5a es un diagrama de bloques esquemático que muestra los componentes de un dispositivo de usuario; y

la figura 5b es un diagrama de bloques esquemático que muestra los componentes de un servidor central de autenticación y validación o de un dispositivo de creación de firma.

DESCRIPCIÓN DETALLADA DE LOS DIBUJOS

[0043] La figura 1a es un diagrama de flujo que muestra cómo proporciona esta nueva invención una importante funcionalidad «WYSIWYS» utilizando múltiples dispositivos. El sistema comprende tres dispositivos fundamentales: un dispositivo de creación de firma (SCD, por sus siglas en inglés) y, preferiblemente, dos dispositivos manejados por un usuario denominados en el presente documento un dispositivo de transacción inicial y un dispositivo de validación. Según se ha explicado más detalladamente en referencia a las figuras 2a a 4a; es en el dispositivo de creación de firma donde se lleva a cabo la generación real de la firma digital. El dispositivo de creación de firma puede ser un SCD central, tal como un servidor de firma o un dispositivo local de creación de firma, tal como una tarjeta inteligente o un lápiz de firma. El dispositivo de transacción inicial puede ser cualquier dispositivo electrónico, tal como una estación de trabajo, un ordenador portátil, una tableta o un teléfono inteligente. Del mismo modo, el dispositivo de validación puede ser cualquier dispositivo electrónico, aunque, preferiblemente, es un dispositivo electrónico distinto del dispositivo de transacción inicial. Existen dos canales de comunicación independientes, uno con cada uno del dispositivo de transacción inicial y el dispositivo de validación para conseguir WYSIWYS con un nivel adecuado de seguridad para evitar que se modifique el mensaje sin una detección inmediata. Si se utilizara únicamente un dispositivo de usuario, debería presentar características adicionales inviolables, tales como una GUI fiable (interfaz gráfica de usuario).

[0044] Al principio, en la etapa S100, el usuario utiliza el dispositivo de transacción inicial para identificar un mensaje específico M al que está preparado para comprometerse con una firma digital. El mensaje puede ser una transacción, documento u orden de compra en formato electrónico. En la figura 1b se muestra un ejemplo de un mensaje en forma de una orden de compra.

[0045] Debido a que el dispositivo de transacción inicial puede ser una plataforma poco segura, normalmente, el usuario no puede comprometerse a firmar el mensaje en este dispositivo, ya que un ataque en el dispositivo de transacción inicial puede sustituir el mensaje por otro. Por lo tanto, una vez el usuario haya aceptado el mensaje M (S102) y desee firmar el mensaje, se solicita una creación de firma al dispositivo de creación de firma (S104).

[0046] Una vez el SCD haya recibido una solicitud para firmar un mensaje M (S106), el SCD no creará la firma hasta que haya recibido pruebas de que el usuario se ha comprometido a firmar este mensaje concreto. En definitiva, esto se consigue enviando el mensaje (o partes del mismo) al dispositivo de validación. Por consiguiente, en la etapa S108, se crea una versión M' derivada del mensaje. M' puede ser la totalidad del mensaje M o se puede crear a partir de extractos de la información contenida en el mensaje M. Así, para el ejemplo de la figura 1b, los campos resaltados 11 se pueden utilizar para formar M'.

[0047] En la figura 1a, se muestra M' creado por el dispositivo de creación de firma, pero se podría crear mediante el dispositivo de transacción u otro dispositivo del sistema, según se muestra en las figuras 2b, 3b y 4b incluidas más adelante. Únicamente, se precisa que se reciba en el dispositivo de creación de firma para la generación del desafío de validación (S110). Según se explica con más detalle más adelante, el desafío de validación se basa también en el mensaje o deriva del mensaje.

[0048] El desafío de validación se envía al dispositivo de validación (S112). Mediante la creación de un desafío de validación derivado del mensaje original, el usuario se puede asegurar de que este mensaje derivado procede de una fuente fiable con motivos aceptables para creer que no ha sido modificado antes de presentarse al usuario para su validación como parte del proceso de generación de firma. El dispositivo de validación (que puede incluir una aplicación específica que se ejecute en el dispositivo) muestra la versión derivada del mensaje M' (S114). Si el usuario reconoce la transacción, la aprueba en el dispositivo de validación (S116), en cuyo caso se genera un código de validación único (S118). Este código de validación se recibe en el dispositivo de creación de firma (S120) y se debe verificar antes de que la transacción se firme mediante el SCD central o local (S122). La verificación garantiza que la firma se puede generar únicamente si esta verificación se ha completado con éxito.

[0049] La innovación posibilita varias formas de realización en función de si el SCD es un servidor de firma central o un dispositivo local (tarjeta inteligente, lápiz USB de firma). En el último caso, resultan posibles diversas formas de realización para verificar el código de validación único.

[0050] Se deben configurar procesos para inscribir el dispositivo de validación y para personalizarlo con algunas claves simétricas o asimétricas. Se trata de una técnica estándar que es muy conocida en la técnica y, por lo tanto, no se describe detalladamente.

[0051] Las figuras 2a a 2c muestran una configuración para proporcionar una importante funcionalidad «WYSIWYS» utilizando múltiples dispositivos. Como se muestra en la figura 2a, esta configuración comprende los dispositivos de usuario: un dispositivo de transacción inicial 10 y un dispositivo de validación 12. Estos dispositivos son independientes entre sí, como parte de la funcionalidad «WYSIWYS». La configuración también comprende un sistema central que se localiza de forma remota con respecto a los dispositivos de usuario y que comprende un dispositivo central de creación de firma 14 y un servidor central de autenticación y validación 16. El dispositivo central de creación de firma 14 está conectado al dispositivo de transacción inicial 10 y el servidor central de autenticación y validación 16 está conectado al dispositivo de validación 12. Por consiguiente, cada

uno de los dispositivos de usuario 12,14 presenta un canal de comunicación independiente separado de la parte central del sistema.

[0052] En la figura 2a, el dispositivo de creación de firma 14 y el servidor central de autenticación y validación 16 se muestran como dos entidades separadas que están conectadas entre sí, preferiblemente, por medio de una conexión segura. Este hecho indica únicamente que cada entidad desempeña una función o un papel distinto en el proceso. Se observa que las funciones separadas del dispositivo de creación de firma 14 y el servidor central de autenticación y validación 16 se pueden proporcionar también a través de una única entidad, por ejemplo, un único servidor de firma.

[0053] El flujo de información en torno al sistema se indica por medio de los números 1 a 8, y se explica más detalladamente en relación con las figuras 2b y 2c. Inicialmente, como muestra la flecha 1, el usuario acuerda el contenido y acepta un mensaje M que se muestra en su dispositivo de transacción inicial (S200). Su aceptación implica su disposición para comprometerse con el mensaje con una firma digital. Dicho mensaje M se puede presentar, opcionalmente, en un navegador de cliente del dispositivo de transacción inicial que recibe páginas web HTML desde un servidor web remoto controlado por un proveedor de aplicaciones.

[0054] Según indica la flecha 2a, el usuario pone en contacto el SCD central o servidor de firma para solicitar una firma para un mensaje M o una versión con *hash* del mismo (S202). Se crea una versión derivada del mensaje, denominada M'. M' puede ser idéntico a M o derivar de M, aunque, fundamentalmente, presenta el mismo contenido. M puede ser, por ejemplo, una orden de compra y M' sería un resumen de esta, por ejemplo, con la referencia del pedido, el destinatario o la cantidad. Según se muestra en las etapas S204a, S204b, S206c, M' se calcula mediante el dispositivo de transacción inicial, el SCD o el servidor central de autenticación y validación. Independientemente de dónde se cree, como indica la flecha 2b, existe comunicación entre el SCD central y el servidor central de autenticación y validación para asegurar que el servidor central de autenticación y validación recibe finalmente M' (S206).

[0055] Según indican la flecha 3 y S208, se genera un desafío de validación $VC_{M',\ User}$ mediante el servidor central de autenticación y validación para el mensaje M' y el usuario asociado a M' (y, por lo tanto, para el mensaje original M). Este desafío de validación es una función de cifrado seguro de M' y se puede generar utilizando cualquier técnica estándar conocida. El desafío de validación necesita proteger el mensaje M' con información que sea única para el usuario y para el servidor central de autenticación y validación, de manera que el usuario pueda estar seguro de que el desafío de validación se basa en el mensaje original M y procede de una fuente fiable. Además, el dispositivo de validación ha de ser capaz de recuperar M' a partir del desafío de validación. Por ejemplo, el desafío de validación se puede generar utilizando cifrado con una clave simétrica que compartan tanto el servidor de autenticación y validación como el dispositivo de validación. Del mismo modo, el desafío de validación se puede generar utilizando un código de autenticación de mensajes (MAC) que compartan tanto el servidor de autenticación y validación como el dispositivo de validación. De manera alternativa, el desafío de validación puede ser una versión de M' firmada digitalmente que se firma con una clave privada asociada al usuario, encontrándose la parte pública de la clave privada en el dispositivo de validación. Se observará que el hecho de generar el desafío de validación precisa que el dispositivo de validación se haya registrado o vinculado de otro modo al servidor central de autenticación y validación para compartir la información única (por ejemplo, clave simétrica, clave pública/privada o MAC) en una etapa más temprana para permitir que se genere el desafío de validación.

[0056] Como muestran la flecha discontinua 4 y la etapa S210, el desafío de validación $VC_{M',\ User}$ se envía al dispositivo de validación. La línea discontinua indica que la conexión entre el dispositivo de validación puede ser indirecta, por ejemplo, por medio del dispositivo de transacción inicial, o puede ser directa, según se describe más adelante. Además, el desafío de validación se puede volver a formatear antes de su transmisión. Por ejemplo, el desafío de validación se puede volver a formatear como un código estandarizado de respuesta rápida (código QR, por sus siglas en inglés) [ISO/IEC18004] o un código de barras similar que sea legible mediante un dispositivo apropiado. El desafío de validación reformateado $VC_{M',\ User}$ se puede enviar al dispositivo de transacción inicial y mostrarse en la pantalla, de manera que se pueda capturar y leer mediante el dispositivo de validación, por ejemplo, en una cámara controlada por la aplicación personalizada que se encuentra en el dispositivo de validación.

[0057] De manera alternativa, el desafío de validación se puede transmitir directamente a través de la red, por ejemplo, cuando exista una aplicación personalizada ubicada en el dispositivo de validación, un usuario puede ser capaz de introducir una inserción de comando que asegure que el desafío de validación $VC_{M',\ User}$ llega al dispositivo de validación. En tal caso, puede resultar valioso para proteger el acceso a la aplicación mediante un PIN o una contraseña o un patrón de autenticación para garantizar que el usuario está presente físicamente en el momento de la validación. Un modo para asegurar que el usuario está físicamente presente es enviar una solicitud a través de la red con el objetivo de que el usuario inicie la aplicación para que el desafío de validación $VC_{M',\ User}$ se pueda recuperar desde el servidor central de autenticación y validación y se ponga a disposición de la aplicación del dispositivo de validación.

[0058] Independientemente de la manera en que se transmita el desafío de validación, una vez recibido en el dispositivo de validación, el desafío de validación se utiliza para volver a crear el mensaje M' para que M' se

pueda mostrar en la pantalla del dispositivo de validación (S212). El método para recuperar M' depende del método de creación del desafío de validación. Por ejemplo, M' se puede recuperar mediante una validación correcta de MAC o mediante descifrado utilizando técnicas de criptografía simétrica o asimétrica.

[0059] Según indica la flecha 5, en este momento del proceso, el usuario puede leer el mensaje M' en su dispositivo de validación y verificar que coincide con el mensaje M que se ha comprometido a firmar (S214). A título ilustrativo, en el ejemplo anterior, donde M es una orden de compra y M' sería un resumen de la misma con información acerca de campos importantes, por ejemplo, la referencia del pedido, el destinatario, la cantidad; se le presentaría al usuario la información de los campos para identificar M. Una correcta visualización del mensaje M' en el dispositivo de validación proporciona al usuario tanto evidencias de que el contenido del mensaje no ha sido modificado desde que se recibió en el SCD central como evidencias de que el desafío de validación procede de una fuente fiable, debido a que la recuperación de M' se ha completado de manera satisfactoria. Si, efectivamente, este es el caso, el usuario puede aprobar o validar M' y la aplicación del dispositivo de validación calculará un código de validación único (S216). Si M' no coincide, el proceso termina sin que se cree una firma. El código de validación se puede generar utilizando diversos métodos estandarizados, incluyendo el algoritmo desafío-respuesta OATH (OCRA) [descrito en RFC 6287- ISSN 2070-1721] o tecnología propia equivalente, tal como CAP de MasterCard, CodeSure de Visa [WO2013013262] o mecanismos Digipass basados en desafío-respuesta de Vasco. Por lo tanto, el código de validación se genera, preferiblemente, utilizando cifrado simétrico empleando otra clave específica del dispositivo compartida entre el dispositivo de validación y el servidor central de autenticación y validación. El código de validación también puede ser una respuesta firmada con un número utilizado una sola vez (*nonce*) para evitar ataques de reproducción. El código de validación se debe crear utilizando información que sea específica del usuario y, preferiblemente, distinta de la información utilizada para crear el desafío de validación. El servidor central de autenticación y validación se debe asegurar de que el código de validación procede del dispositivo de validación. No obstante, al contrario que en el desafío de validación, no es fundamental que el servidor central de autenticación y validación vuelva a crear alguna parte de la información contenida en el código de validación. Por consiguiente, se pueden utilizar también esquemas asimétricos.

[0060] Como indica la flecha discontinua 6 y la etapa S218, el código de validación se envía de vuelta al servidor central de autenticación y validación. Esto se puede llevar a cabo de manera indirecta, por ejemplo, mediante el dispositivo de transacción inicial. En un supuesto, el usuario teclea manualmente el código de validación en el dispositivo de transacción inicial para que se vuelva a distribuir al servidor central de autenticación y validación a través del SCD central. De manera alternativa, el código de validación se puede enviar directamente a través de la red desde el dispositivo de validación al servidor central de autenticación y validación, evitando así que el usuario vuelva a teclear el código.

[0061] En la etapa S220, el código de validación se verifica mediante el servidor central de autenticación y validación. La verificación se lleva a cabo empleando cualquier técnica estándar, por ejemplo, utilizando OCRA de OATH, según se describe en RFC 6287. Como indica la flecha 7 y S222, el resultado de esta verificación se envía a continuación de manera segura al SCD central (si los dos son físicamente distintos).

[0062] Por último, como indica la flecha 8, el SCD central comprueba el resultado de la verificación del código de validación (S224). Esta comprobación incluye confirmar que la respuesta del servidor central de autenticación y validación se autentifica correctamente y confirmar que el resultado de la verificación es positivo. Si esta comprobación no es correcta, el proceso termina sin firmar el mensaje. De manera alternativa, si todo está en orden, se genera la firma digital para el mensaje M utilizando el SCD central del usuario (S226).

[0063] Como etapa final, la firma generada puede ser verificada por el usuario o cualquier persona de confianza utilizando métodos heredados (S228). En caso de conflictos, el registro del servidor central de autenticación y validación se puede utilizar para crear una prueba de sistema de que el usuario se ha comprometido a firmar utilizando el dispositivo de validación.

[0064] La figura 3a muestra una variación de la configuración de la figura 2a, en la que el dispositivo central de creación de firma se sustituye por un dispositivo local de creación de firma 24. Por local, se entiende que el dispositivo de creación de firma pertenece al usuario (esto es, lo maneja el usuario), por ejemplo, un lápiz o llave USB. Todos los otros dispositivos son iguales y, por consiguiente, se utiliza la misma numeración. Asimismo, como se explica con más detalle más adelante, muchas de las etapas del proceso son similares y, por lo tanto, las etapas comunes a ambos se describen menos detalladamente en relación con la presente forma de realización. El flujo de información en torno al sistema se indica por medio de los números 1 a 10, y se explica más detalladamente en relación con las figuras 3b y 3c.

[0065] Al igual que en la configuración anterior, como muestra la flecha 1, el usuario acuerda el contenido y acepta un mensaje M que se muestra en su dispositivo de transacción inicial (S300). Del mismo modo, al igual en la configuración anterior, como muestra la flecha 2, el usuario contacta con el dispositivo de creación de firma para solicitar una firma para el mensaje M (S302). La diferencia fundamental se basa en que la solicitud se envía al dispositivo local de creación de firma.

[0066] De nuevo, se crea una versión derivada del mensaje, denominada M', mediante el dispositivo de transacción inicial (S304a), el SCD (S304b) o el servidor central de autenticación y validación (S304c). Sin

embargo, al contrario que en la configuración anterior, si M' se genera mediante el dispositivo de transacción inicial (S304a) o el SCD (S304b), el mensaje M' se autentifica mediante el SCD local (S305) antes de enviarse al servidor central de autenticación y validación para garantizar que el servidor central de autenticación y validación (S306) puede confiar en el mensaje M'. La autenticación se puede llevar a cabo empleando cualquier técnica conocida, por ejemplo, firmando. En esta configuración, no existe conexión segura entre el SCD y el servidor central de autenticación y validación. Por consiguiente, la autenticación garantiza que el servidor central de autenticación y validación puede confiar en que el mensaje M' ha sido recibido desde el SCD local.

[0067] Antes de crear el desafío de validación según indica la flecha 5, el servidor central de autenticación y validación puede llevar a cabo, por lo tanto, varias verificaciones opcionales para garantizar que M' procede del SCD del usuario (S307). Estas etapas opcionales se pueden llevar a cabo mediante el módulo de seguridad de *hardware* (HSM) o el compuesto de seguridad del servidor central de autenticación y validación. Estas verificaciones pueden garantizar que el usuario ha seleccionado el certificado correcto, que el certificado es válido y que el SCD local está conectado y es funcional antes de llevar a cabo la firma. Una vez completadas estas verificaciones opcionales, se genera un desafío de validación $VC_{M', User}$ (S308) mediante el servidor central de autenticación y validación para el mensaje M' y el usuario asociado a M'. Este desafío de validación se genera según lo descrito anteriormente.

[0068] Las etapas siguientes corresponden a lo descrito anteriormente. Así, como muestra la flecha discontinua 6 y la etapa S310, el desafío de validación $VC_{M', User}$ se envía de manera directa o indirecta al dispositivo de validación. Independientemente de la manera en que se transmita el desafío de validación, una vez recibido en el dispositivo de validación, el desafío de validación se utiliza para volver a crear el mensaje M' para que M' se pueda visualizar en la pantalla del dispositivo de validación (S312). Según indica la flecha 7, en este punto del proceso, el usuario puede leer el mensaje M' en su dispositivo de validación y verificar que coincide con el mensaje M que se ha comprometido a firmar (S314). El dispositivo de validación calculará, a continuación, un código de validación único (S316), según se ha descrito anteriormente. Como indican la flecha discontinua 8 y la etapa S318, el código de validación se vuelve a enviar de manera directa o indirecta al servidor central de autenticación y validación.

[0069] Al igual que en la configuración anterior, en la etapa S320, el código de validación se verifica mediante el servidor central de autenticación y validación. No obstante, como indican la flecha 9 y S322, el resultado de esta verificación se envía a continuación de manera segura al SCD local (en lugar de al SCD central de la figura 2a). Se puede conseguir la transmisión segura mediante técnicas conocidas, por ejemplo, firmando y/o cifrando el resultado de la verificación. Por último, como indica la flecha 10, el SCD central comprueba el resultado de la verificación del código de validación (S324). Esta comprobación incluye confirmar que la respuesta del servidor central de autenticación y validación se autentifica correctamente y confirmar que el resultado de la verificación es positivo. Si esta comprobación no es correcta, el proceso termina sin firmar el mensaje. De manera alternativa, si todo está en orden, el usuario puede estar seguro de que realmente corresponde al mensaje M' que ha aprobado en el dispositivo de validación para que el mensaje M (o un *hash* del mismo) se pueda firmar en última instancia.

[0070] Así, la firma digital se genera para el mensaje M utilizando el SCD local (S326). De manera opcional, la respuesta del servidor central de autenticación y validación y/o el código de validación se pueden adjuntar como atributo firmado de firma. Al igual que antes, la firma generada puede ser verificada por el usuario o cualquier persona de confianza utilizando métodos heredados. En caso de que haya conflicto, el registro del servidor central de autenticación y validación se puede utilizar para crear una prueba de sistema de que el usuario se ha comprometido con la firma utilizando el dispositivo de validación.

[0071] La configuración anterior presenta el inconveniente de que, a pesar de presentar un dispositivo local de creación de firma, se precisa un servidor central de autenticación y validación. La figura 4a muestra una variación de la configuración de la figura 3a en la que el dispositivo local de creación de firma 24 ofrece la funcionalidad del servidor central de autenticación y validación. En esta configuración, todas las operaciones se completan localmente sin necesitar ninguna conexión de red. El dispositivo de creación de firma 24 valida el código de validación antes de efectuar la firma en M. Este hecho garantiza que el dispositivo local de creación de firma se puede utilizar únicamente para crear firmas en mensajes que se hayan mostrado y aprobado en el dispositivo de validación 12. Por local, se entiende que el dispositivo de creación de firma pertenece al usuario (esto es, lo maneja el usuario), por ejemplo, un lápiz o llave USB. Los dispositivos de transacción inicial y de validación son iguales que antes y, por consiguiente, se utiliza la misma numeración. Asimismo, como se explica con más detalle más adelante, muchas de las etapas del proceso son similares y, por lo tanto, las etapas comunes a ambos se refieren simplemente a la descripción anterior. El flujo de información en torno al sistema se indica por medio de los números 1 a 8 y se explica más detalladamente en relación con las figuras 4b y 4c.

[0072] Al igual que en la disposición anterior, como muestra la flecha 1, el usuario acuerda el contenido y acepta un mensaje M que se muestra en su dispositivo de transacción inicial (S400). Del mismo modo, al igual en la configuración anterior, como muestra la flecha 2, el usuario contacta con el dispositivo local de creación de firma para solicitar una firma para el mensaje M (S302). De nuevo, se crea una versión derivada del mensaje, denominada M', mediante el dispositivo de transacción inicial (S404a) o el SCD (S404b).

[0073] Al contrario que en las configuraciones anteriores, como indica la flecha 3, el SCD local, en lugar del servidor central de autenticación y validación, genera un desafío de validación $VC_{M', User}$ (S408) para el mensaje M' y el usuario asociado a M'. Este desafío de validación se genera utilizando los mismos mecanismos descritos anteriormente; la única diferencia radica en que se llevan a cabo en el SCD local, en lugar de en el servidor central de autenticación y validación.

[0074] Al igual que en la configuración anterior, y según muestran la flecha discontinua 4 y la etapa S410, el desafío de validación $VC_{M', User}$ se envía de manera directa o indirecta al dispositivo de validación. Independientemente de la manera en que se transmita el desafío de validación, una vez recibido en el dispositivo de validación, el desafío de validación se utiliza para volver a crear el mensaje M' para que M' se pueda mostrar en la pantalla del dispositivo de validación (S412). Según indica la flecha 5, en este punto del proceso, el usuario puede leer el mensaje M' en su dispositivo de validación y verificar que coincide con el mensaje M que se ha comprometido a firmar (S414). El dispositivo de validación calculará, a continuación, un código de validación único (S416), según se ha descrito anteriormente.

[0075] En esta configuración, no existe un servidor central de autenticación y validación y, por lo tanto, el código de validación no se puede enviar a este para su verificación. Por consiguiente, en lugar de enviarse el código de validación directamente desde el dispositivo de validación al SCD local, el código de validación se muestra en el dispositivo de validación y un usuario introduce el código de validación en el dispositivo de transacción inicial. Esto se muestra mediante la flecha discontinua 6 y S418. La flecha 7 y S420 muestran que el código de validación se envía a continuación desde el dispositivo de transacción inicial al SCD local. Así, el código de validación se envía de manera indirecta desde el dispositivo de validación al SCD local. El código de validación se puede enviar como parte de la solicitud al SCD local para firmar el mensaje M.

[0076] Al igual que en las configuraciones anteriores, en la etapa S424, el código de validación se verifica mediante el SCD local. Por consiguiente, en esta configuración, el dispositivo de validación y el SCD local han de registrarse entre sí para que compartan una clave privada o clave secreta similar que se pueda utilizar para que el SCD local pueda confirmar que el código de validación procede del dispositivo de validación. La autenticación entre el SCD local y el dispositivo de validación puede emplear cualquier método conocido. Por ejemplo, la clave privada puede ser una clave simétrica, esto es, una clave que se pueda utilizar tanto para cifrar texto plano para crear texto cifrado como para descifrar el texto cifrado para volver a convertirlo en el texto plano. La clave privada se puede intercambiar en una fase de inicialización introduciendo una contraseña preferiblemente larga o secuencia de paso tanto en el SCD local como en el dispositivo de validación. Sin embargo, otros intercambios de la clave privada son posibles. Una vez se haya almacenado la clave privada, la solicitud de firma puede incluir también un código de acceso (p. ej., PIN) requerido para utilizar la clave privada en el SCD local.

[0077] Si todo está en orden tras el proceso de verificación, el usuario puede estar seguro de que el código de validación corresponde realmente al mensaje M' que ha aprobado en el dispositivo de validación para que, en última instancia, se pueda firmar el mensaje M (o un *hash* del mismo). Así, la firma digital se genera para el mensaje M utilizando el SCD local (S426). De manera opcional, M' y/o el código de validación se pueden adjuntar como un atributo firmado de firma.

[0078] Según se ha descrito anteriormente, el dispositivo de validación y el dispositivo de transacción inicial pueden encontrarse en cualquier forma de dispositivo electrónico que haya sido modificado (p. ej., programado o configurado) mediante *software* para ser un ordenador con finalidad específica para llevar a cabo las funciones descritas en el presente documento. La figura 5a muestra de manera esquemática los componentes del dispositivo de validación o del dispositivo de transacción inicial. Cada uno comprende un procesador 52 unido a una memoria de códigos y datos 54, un sistema de entrada/salida 56 (por ejemplo, que comprende interfaces para una red y/o medios de almacenamiento y/u otras comunicaciones), una interfaz de usuario 58 que comprende, por ejemplo, un teclado y/o ratón y una pantalla de usuario 62. Puede haber también una cámara opcional 64 que se puede utilizar cuando se cree una versión legible de código de barras o similar del desafío de validación, según se ha desrito anteriormente en relación con la etapa S210 de la figura 2b. El código y/o datos almacenado(s) en la memoria 54 se puede(n) proporcionar en un medio de almacenamiento extraíble 60.

[0079] Para el dispositivo de validación, el sistema de entrada/salida 56 se puede utilizar para recibir el desafío de validación o, de manera alternativa, se puede utilizar la cámara 64 para capturar el desafío de validación de un código de barras que se muestre en el dispositivo de transacción inicial. El procesador 52 se puede utilizar para volver a generar el mensaje M' a partir del desafío de validación y se puede utilizar la pantalla de usuario 62 para mostrar el mensaje M'. A continuación, un usuario puede utilizar la interfaz de usuario 58 para aprobar el mensaje M' si es correcto y para calcular un código de validación. La pantalla 62 puede mostrar el código de validación al usuario y el sistema de entrada/salida 56 puede comunicar este código de validación a la parte apropiada del sistema. Los datos almacenados en la memoria 54 pueden incluir las claves secretas necesarias compartidas que se requieran para la verificación y/o el descifrado de cualquier dato de entrada, por ejemplo, un par de claves secretas que se compartan únicamente con el SCD local en la configuración de la figura 4a o con el servidor central de autenticación y validación en las configuraciones de la figura 2a y 3a. Preferiblemente, el par de claves secretas comprenden dos elementos de información distintos, uno para descifrar y/o verificar el desafío de validación entrante para volver a generar el mensaje M' y otro para generar el código de validación.

[0080] Para el dispositivo de transacción inicial, la pantalla de usuario 62 se puede utilizar para visualizar el mensaje original M y, a continuación, un usuario puede utilizar la interfaz de usuario 58 para solicitar la firma para el mensaje M. La pantalla de usuario 62 se puede utilizar también para mostrar el desafío de validación, por ejemplo, en forma de un código de barras. La interfaz de usuario 58 se puede utilizar para introducir el código de validación de manera que el código de validación se pueda transmitir al dispositivo de creación de firma.

[0081] La figura 5b muestra de manera esquemática los componentes del dispositivo de creación de firma (local o central) o bien del servidor central de autenticación y validación. Cada uno comprende un procesador 72 unido a una memoria de códigos y datos 74 y un sistema de entrada/salida 76 (por ejemplo, que comprende interfaces para una red y/o medios de almacenamiento y/u otras comunicaciones). El código y/o datos almacenado(s) en la memoria 74 se puede(n) proporcionar en un medio de almacenamiento extraíble. El dispositivo también comprende una base de datos de usuario 78 que comprende el par de claves secretas compartidas con el dispositivo de validación. La base de datos de usuario se muestra como un componente separado, aunque puede estar integrado en el mismo dispositivo. El dispositivo también comprende un módulo de seguridad de *hardware* 80. El HSM se puede utilizar para proteger y utilizar las claves de firma en el caso del SCD. El HSM se puede utilizar para proteger y utilizar las claves que protegen el desafío de validación y el código en el servidor de autenticación y validación.

[0082] En las configuraciones de las figuras 2a y 3a, el procesador 72 para el servidor central de autenticación y validación puede generar el desafío de validación y el sistema de entrada/salida puede enviarlo al dispositivo de validación. Se puede recibir un código de validación a través del sistema de entrada/salida 76 y verificarse mediante el procesador 72. A continuación, los resultados de la verificación se pueden enviar al dispositivo de creación de firma.

[0083] En todas las configuraciones, para el dispositivo de creación de firma, el procesador 72 puede crear la firma utilizando información privada almacenada en la base de datos del usuario 78. Además, en las configuraciones de la figura 4a, el procesador 72 para el dispositivo de creación de firma puede generar el desafío de validación y el sistema de entrada/salida 76 puede enviarlo al dispositivo de validación. Se puede recibir un código de validación a través del sistema de entrada/salida 76 y verificarse mediante el procesador 72.

[0084] La figura 5b muestra un único dispositivo informático con múltiples componentes internos que se pueden implementar desde una única o múltiples unidad(es) de procesamiento, por ejemplo, microprocesador(es). Se observará que la funcionalidad del dispositivo se puede distribuir a través de varios dispositivos informáticos. Se observará también que los componentes individuales se pueden combinar en uno o varios componentes que proporcionan la funcionalidad combinada. Además, cualquiera de los módulos, bases de datos o dispositivos mostrados en la figura 5b se pueden implementar en un ordenador para fines generales modificado (p. ej., programado o configurado) mediante *software* para ser un ordenador con finalidad específica para llevar a cabo las funciones descritas en el presente documento.

[0085] No cabe duda de que a los expertos en la materia se les ocurrirán muchas otras alternativas efectivas. Se comprenderá que la invención no se limita a las formas de realización descritas y abarca modificaciones evidentes para los expertos en la materia que se incluyen dentro del alcance de las reivindicaciones adjuntas a la misma.

[0086] Otras características de la presente invención pueden incluir las siguientes.

[0087] Volver a formatear el desafío de validación como un código de barras que sea legible mediante el segundo dispositivo de usuario y enviar el desafío de validación reformateado al usuario.

[0088] Verificar el código de validación utilizando una segunda clave secreta compartida.

[0089] Ser la segunda clave secreta compartida distinta de la primera clave secreta compartida.

[0090] Generar dicho código de validación utilizando cifrado, siendo la segunda clave secreta una clave simétrica.

[0091] Recibir el desafío de validación desde un dispositivo de autenticación y validación.

[0092] Generar el código de validación para el dispositivo de autenticación y validación.

[0093] Recibir el desafío de validación desde un dispositivo de creación de firma.

[0094] Verificar el código de validación antes de generar la firma.

[0095] Ser el dispositivo de creación de firma local con respecto al usuario.

[0096] Generar el desafío de validación mediante el dispositivo de creación de firma.

[0097] Almacenar la primera clave secreta compartida mediante el dispositivo de creación de firma y el segundo dispositivo de usuario.

[0098] Ser el servidor de autenticación y validación remoto con respecto al usuario.

[0099] Ser dicho segundo mensaje M' idéntico a dicho primer mensaje M.

[0100] Configurarse el dispositivo de validación para generar dicho código de validación utilizando una segunda clave secreta que se comparta con el dispositivo de creación de firma y que se almacene en el dispositivo de validación.

[0101] Configurarse el dispositivo de validación para generar dicho código de validación utilizando métodos criptográficos, siendo la segunda clave secreta una clave simétrica.

[0102] Configurarse el dispositivo de validación para recibir el desafío de validación desde un dispositivo de autenticación y validación.

[0103] Configurarse el dispositivo de validación para generar el código de validación para el dispositivo de autenticación y validación.

[0104] Configurarse el dispositivo de validación para recibir el desafío de validación desde un dispositivo de creación de firma.

REIVINDICACIONES

1. Método para generar una firma en nombre de un usuario que presenta un primer y un segundo dispositivo de usuario, comprendiendo el método

recibir una solicitud desde dicho primer dispositivo de usuario para crear una firma para un primer mensaje M;

generar un desafío de validación utilizando un segundo mensaje M' que se basa en el primer mensaje M y una primera clave secreta compartida con dicho usuario, donde dicho desafío de validación se genera cifrando dicho segundo mensaje M' utilizando dicha primera clave secreta compartida;

enviar dicho desafío de validación a dicho usuario para permitir que dicho segundo dispositivo de usuario vuelva a generar dicho segundo mensaje M';

recibir un código de validación desde dicho segundo dispositivo de usuario, confirmando dicho código de validación la solicitud para crear una firma y generándose dicho código de validación tras la confirmación por parte del usuario de que el segundo mensaje M' mostrado en el segundo dispositivo de usuario corresponde al primer mensaje M, donde el segundo mensaje M' mostrado en el segundo dispositivo de usuario se genera descifrando dicho desafío de validación utilizando dicha primera clave secreta compartida; y

generar la firma para el usuario para el primer mensaje M.

2. Método según cualquier reivindicación anterior, comprendiendo además verificar el código de validación antes de generar la firma.

3. Método según cualquier reivindicación anterior, comprendiendo además registrarse previamente con el segundo dispositivo de usuario para obtener la primera clave secreta compartida y/o la segunda clave secreta compartida.

4. Método de validación de una solicitud de firma para un primer mensaje M desde un dispositivo de creación de firma, comprendiendo el método

recibir un desafío de validación desde el dispositivo de creación de firma, habiéndose creado el desafío de validación utilizando un segundo mensaje M' que se basa en el primer mensaje M y una primera clave secreta compartida entre dicho dispositivo de creación de firma y dicho usuario, donde dicho desafío de validación se genera cifrando dicho segundo mensaje M' utilizando dicha primera clave secreta compartida;

generar el segundo mensaje M' a partir del desafío de validación descifrando dicho desafío de validación utilizando dicha primera clave secreta compartida;

mostrar el segundo mensaje M' al usuario;

recibir confirmación de que el segundo mensaje M' mostrado corresponde al primer mensaje M;

generar un código de validación que confirme la solicitud para crear la firma; y

generar el código de validación.

5. Método según la reivindicación 4, donde dicho segundo mensaje M' es idéntico a dicho primer mensaje M.

6. Método según cualquiera de las reivindicaciones 4 o 5, comprendiendo generar dicho código de validación utilizando una segunda clave secreta compartida con el dispositivo de creación de firma.

7. Método para generar una firma en nombre de un usuario, comprendiendo el método

mostrar un primer mensaje M en un primer dispositivo de usuario;

enviar una solicitud desde dicho primer dispositivo de usuario a un servidor de firma para crear una firma para dicho primer mensaje M;

crear un segundo mensaje M' que se basa en el primer mensaje M;

generar un desafío de validación utilizando dicho segundo mensaje M' y una primera clave secreta compartida entre dicho usuario y dicho servidor de firma, donde dicho desafío de validación se genera cifrando dicho segundo mensaje M' utilizando dicha primera clave secreta compartida;

enviar dicho desafío de validación a un segundo dispositivo de usuario;

volver a generar dicho segundo mensaje M' en dicho segundo dispositivo de usuario utilizando dicha primera clave secreta compartida donde dicho segundo mensaje M' se genera descifrando dicho desafío de validación utilizando dicha primera clave secreta compartida;

mostrar dicho segundo mensaje M’ en dicho segundo dispositivo de usuario;

recibir confirmación del usuario de que el segundo mensaje M' mostrado corresponde a dicho primer mensaje M;

generar un código de validación que confirme la solicitud para crear una firma;

enviar dicho código de validación desde dicho segundo dispositivo de usuario a dicho servidor de firma; y

generar la firma para el usuario para el primer mensaje M.

8. Soporte que presenta un código de control de procesador para que, al ejecutarse en un procesador, implemente el método según cualquiera de las reivindicaciones anteriores.

9. Servidor de firma para crear una firma en nombre de un usuario, teniendo el usuario un primer y un segundo dispositivo de usuario, estando configurado el servidor para

recibir una solicitud desde dicho primer dispositivo de usuario para crear una firma para un primer mensaje M;

generar un desafío de validación utilizando un segundo mensaje M' que se basa en el primer mensaje M y una primera clave secreta compartida con dicho usuario, donde dicho desafío de validación se genera cifrando dicho segundo mensaje M' utilizando dicha primera clave secreta compartida;

enviar dicho desafío de validación a dicho usuario para permitir que dicho segundo dispositivo de usuario vuelva a generar dicho segundo mensaje M';

recibir un código de validación desde dicho segundo dispositivo de usuario, confirmando dicho código de validación la solicitud para crear una firma y generándose dicho código de validación tras la confirmación por parte del usuario de que el segundo mensaje M' mostrado en el segundo dispositivo de usuario corresponde al primer mensaje M, donde el segundo mensaje M' mostrado en el segundo dispositivo de usuario se genera descifrando dicho desafío de validación utilizando dicha primera clave secreta compartida; y

generar la firma para el usuario para el primer mensaje M.

10. Servidor de firma según la reivindicación 9, comprendiendo un dispositivo de creación de firma para generar la firma para el usuario.

11. Servidor de firma según la reivindicación 9 o 10 comprendiendo un servidor de autenticación y validación para generar el desafío de validación.

12. Servidor de firma según la reivindicación 11, donde el servidor de autenticación y validación o el dispositivo de creación de firma, y el segundo dispositivo de usuario almacenan, ambos, la primera clave secreta compartida.

13. Dispositivo de validación para que un usuario valide una solicitud de firma para un primer mensaje M, estando configurado el dispositivo de validación para

recibir un desafío de validación desde un dispositivo de creación de firma, habiéndose creado el desafío de validación utilizando un segundo mensaje M' que se basa en el primer mensaje M y una primera clave secreta compartida entre dicho dispositivo de creación de firma y dicho dispositivo de validación, donde dicho desafío de validación se genera cifrando dicho segundo mensaje M' utilizando dicha primera clave secreta compartida;

generar el segundo mensaje M' a partir del desafío de validación utilizando la primera clave secreta compartida donde dicho segundo mensaje M' se genera descifrando dicho desafío de validación utilizando dicha primera clave secreta compartida;

mostrar el segundo mensaje M' al usuario;

recibir confirmación del usuario de que el segundo mensaje M' corresponde al primer mensaje M;

generar un código de validación que confirme la solicitud para crear la firma; y generar el código de validación.

14. Sistema para generar una firma para un usuario que comprende un servidor de firma según lo expuesto en cualquiera de las reivindicaciones 9 a 12 y un dispositivo de validación según lo expuesto en la reivindicación 13.

15. Sistema que comprende un servidor de firma, un dispositivo de transacción inicial para un usuario y un dispositivo de validación para un usuario, estando configurado el dispositivo de transacción inicial para

mostrar un primer mensaje M; y

enviar una solicitud al servidor de firma para crear una firma para dicho primer mensaje M;

estando configurado el servidor de firma para

generar un desafío de validación utilizando un segundo mensaje M' que se basa en dicho primer mensaje M' y una primera clave secreta compartida entre dicho usuario y dicho servidor de firma, donde dicho desafío de validación se genera cifrando dicho segundo mensaje M' utilizando dicha primera clave secreta compartida; y

enviar dicho desafío de validación al dispositivo de validación;

estando configurado el dispositivo de validación para

volver a generar dicho segundo mensaje M' utilizando dicha primera clave secreta compartida donde dicho segundo mensaje M' se genera descifrando dicho desafío de validación utilizando dicha primera clave secreta compartida;

mostrar dicho segundo mensaje M';

recibir confirmación del usuario de que el segundo mensaje M' mostrado corresponde a dicho primer mensaje M;

generar un código de validación que confirme la solicitud para crear una firma; y

enviar dicho código de validación a dicho servidor de firma;

a través de lo cual dicho servidor de firma genera la firma para el usuario para el primer mensaje M.

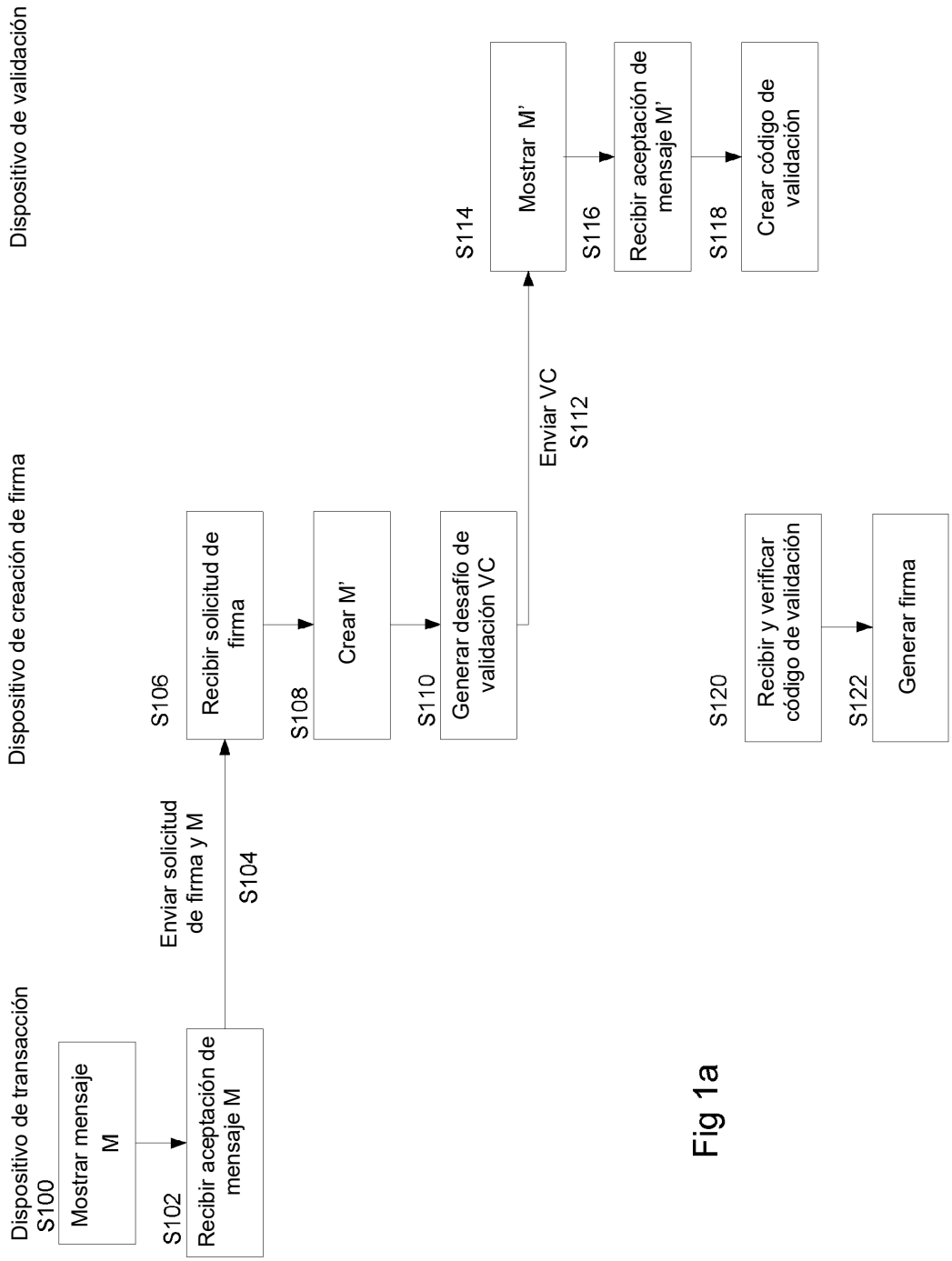
Dispositivo de transacción
Dispositivo de creación de firma
Dispositivo de validación
S100
Mostrar mensaje M
S102
Recibir aceptación de mensaje M
Enviar solicitud de firma y M
S104
S106
Recibir solicitud de firma
S108
Crear M'
S110
Generar desafío de validación VC
Enviar VC
S112
S114
Mostrar M'
S116
Recibir aceptación de mensaje M'
S118
Crear código de validación
S120
Recibir y verificar código de validación
S122
Generar firma

Fig 1a

11

Paul Smith
The Best Company Ltd.
Random Street 30
66666 PROFITOWN
PAÍS

ORDEN DE COMPRA

N.º de pedido #004 / Fecha: 6 de junio de 2013

Tu referencia de presupuesto: F68498Y67
Fecha 08.03.2013
Versión

Se indica a continuación la descripción de los artículos solicitados, junto con las coordenadas de la factura.

Artículo	Descripción	Cantidad	Precio (€)
934-000010	Artículo adquirido con funciones avanzadas	1	3750,00 €
Descuento de distribución 25 %			(937,50 €)
En función de nuestro último acuerdo (firmado en 2010)			
	Valor total (sin IVA)		2812,50 €

Dirección de entrega
Mutterunternehmen GmbH
Freudestrasse 7 D – 85630 Glückstadt - ALEMANIA
Número de identificación fiscal / USt-IdNr: de 81403858

Condiciones de pago
Como máximo, 30 días desde el envío

Dirección de facturación
Mutterunternehmen GmbH
Happiness Strasse 7 D – 85630 Glückstadt - ALEMANIA
Número de identificación fiscal / USt-IdNr: de 81403858

Una vez recibido, rogamos envíen confirmación del pedido incluyendo la fecha estimada de entrega.
Saludos cordiales,

Mister Mustermann
Director de compras

Fig 1b

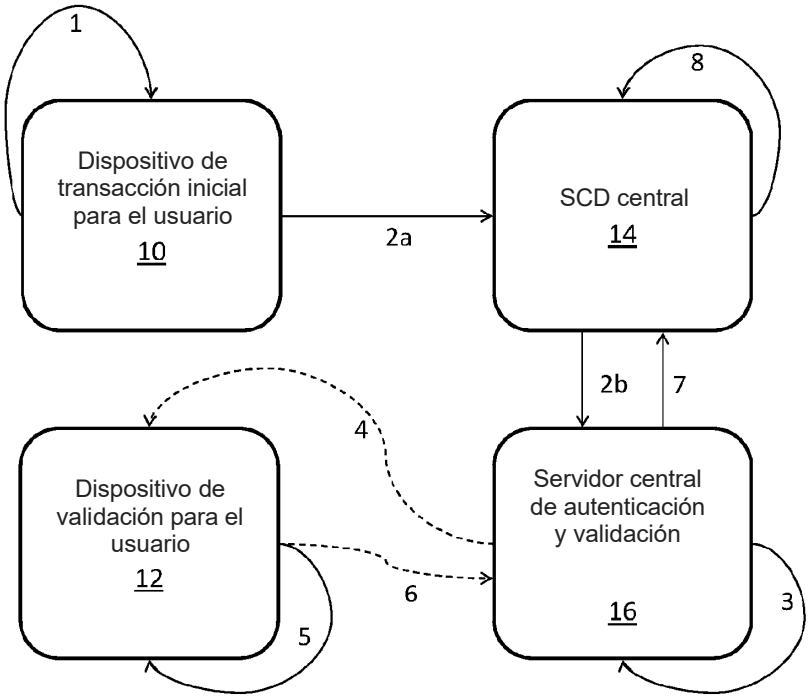
1
8
Dispositivo de transacción inicial para el usuario
10
2a
SCD central
14
2b
7
4
Dispositivo de validación para el usuario
12
6
Servidor central de autenticación y validación
16
3
5

Fig 2a

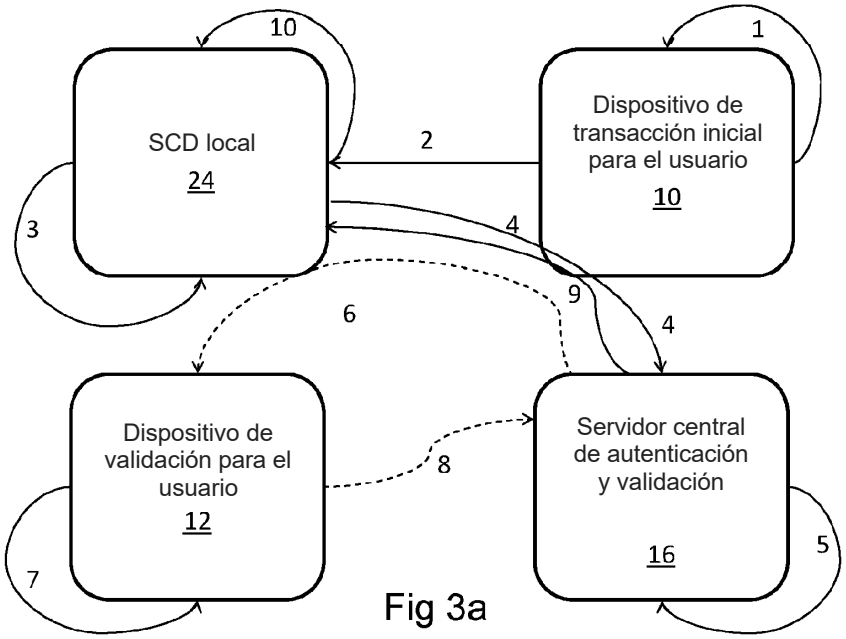
10
1
SCD local
24
2
Dispositivo de transacción inicial para el usuario
10
3
4
9
6
4
Dispositivo de validación para el usuario
12
8
Servidor central de autenticación y validación
16
5
7

Fig 3a

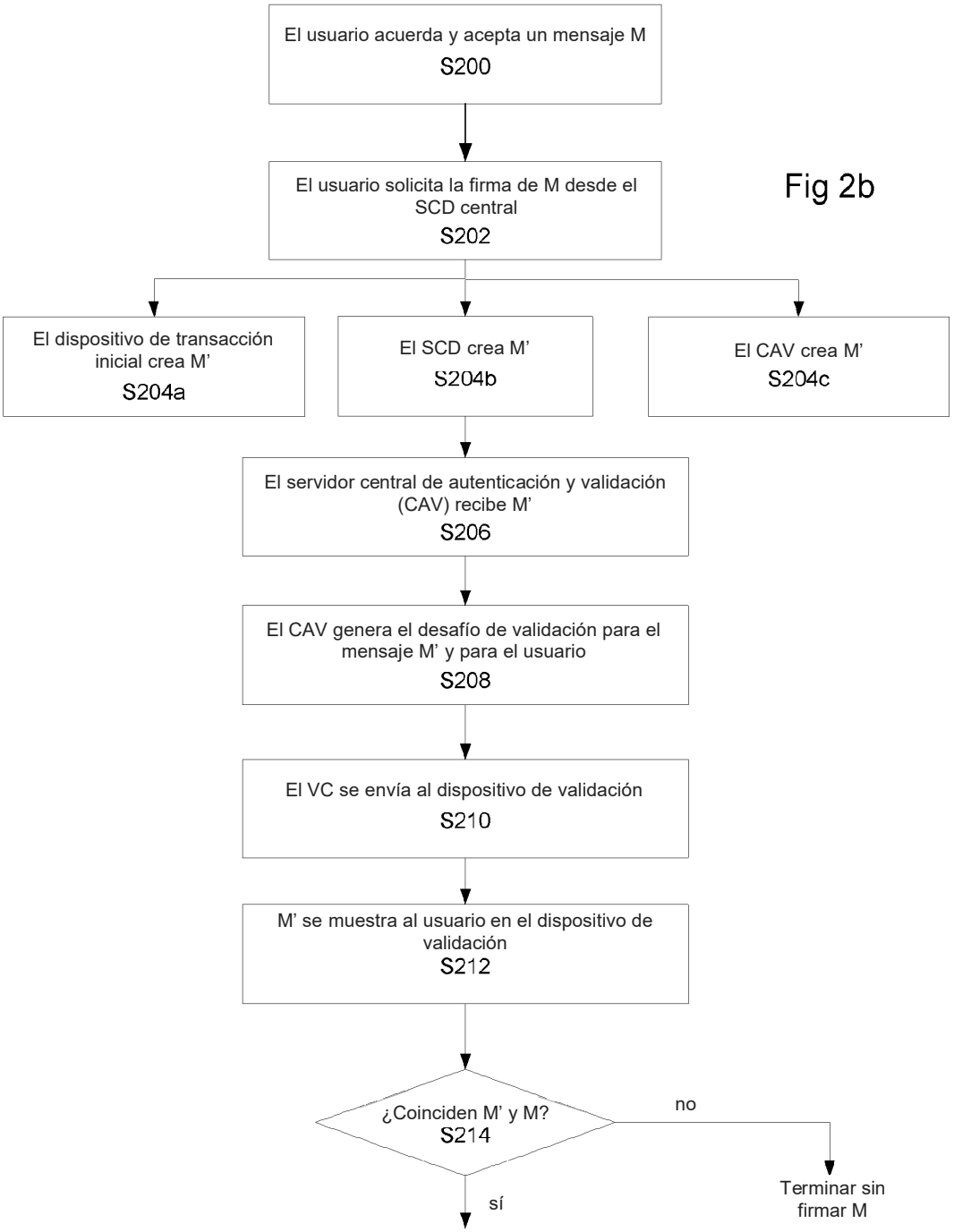

Fig 2b

Figura 2c

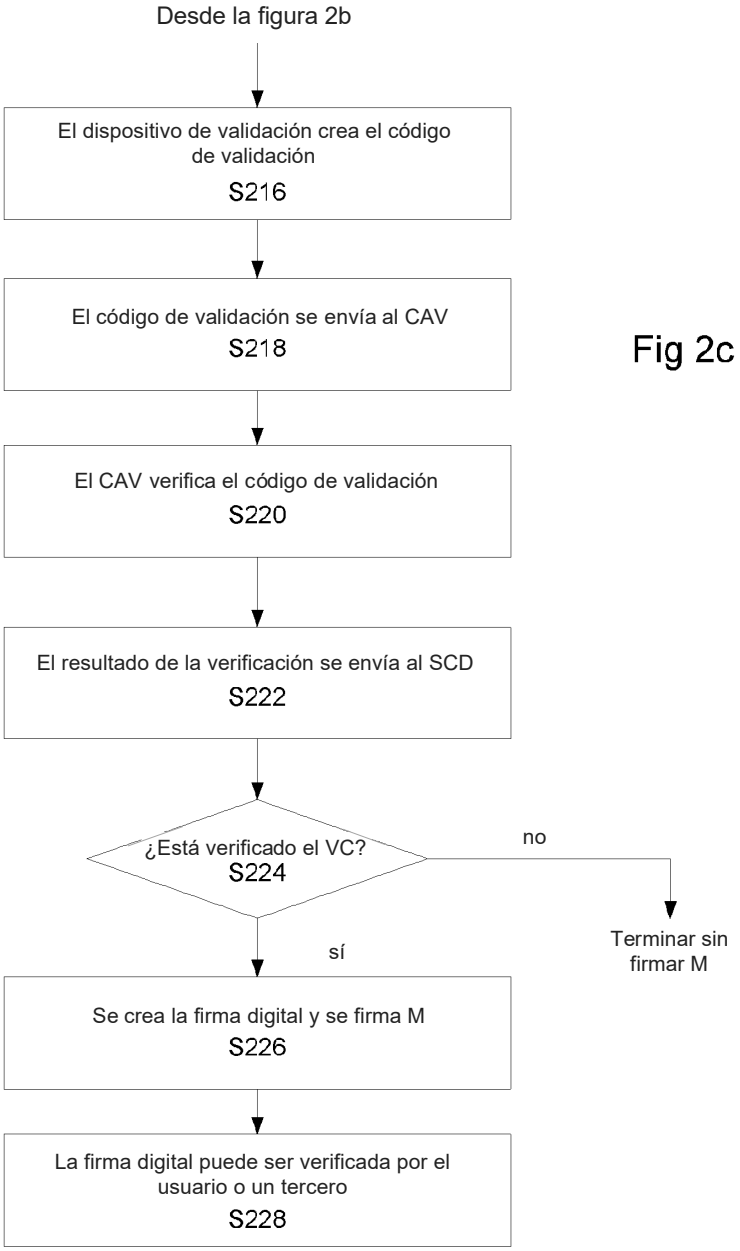
Desde la figura 2b
El dispositivo de validación crea el código de validación
S216
El código de validación se envía al CAV
S218
El CAV verifica el código de validación
S220
El resultado de la verificación se envía al SCD
S222
¿Está verificado el VC?
S224
no
Terminar sin firmar M
sí
Se crea la firma digital y se firma M
S226
La firma digital puede ser verificada por el usuario o un tercero
S228

Fig 2c

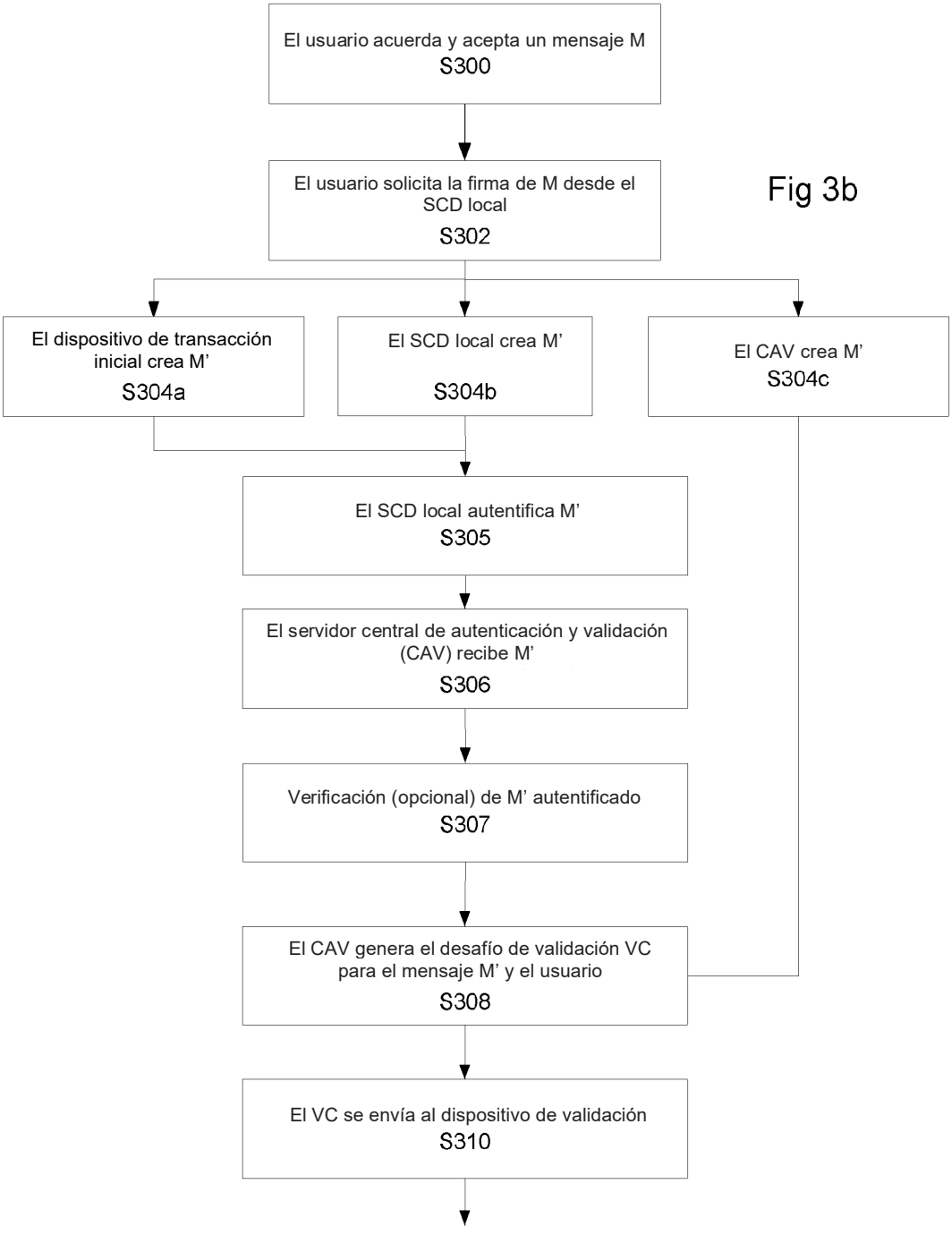

Fig 3b

A la figura 3c

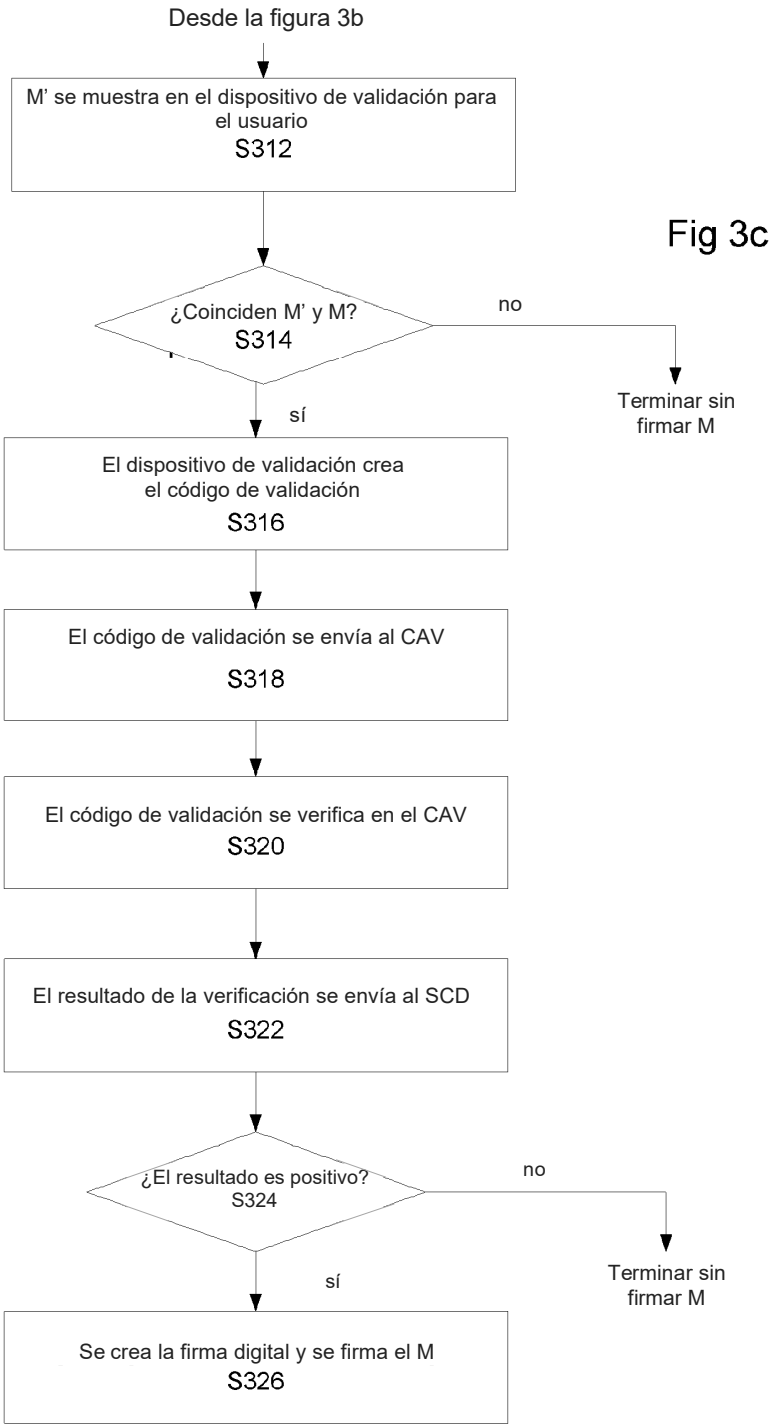
Desde la figura 3b
M' se muestra en el dispositivo de validación para el usuario
S312
¿Coinciden M' y M?
S314
no
Terminar sin firmar M
sí
El dispositivo de validación crea el código de validación
S316
El código de validación se envía al CAV
S318
El código de validación se verifica en el CAV
S320
El resultado de la verificación se envía al SCD
S322
¿El resultado es positivo?
S324
no
Terminar sin firmar M
sí
Se crea la firma digital y se firma el M
S326

Fig 3c

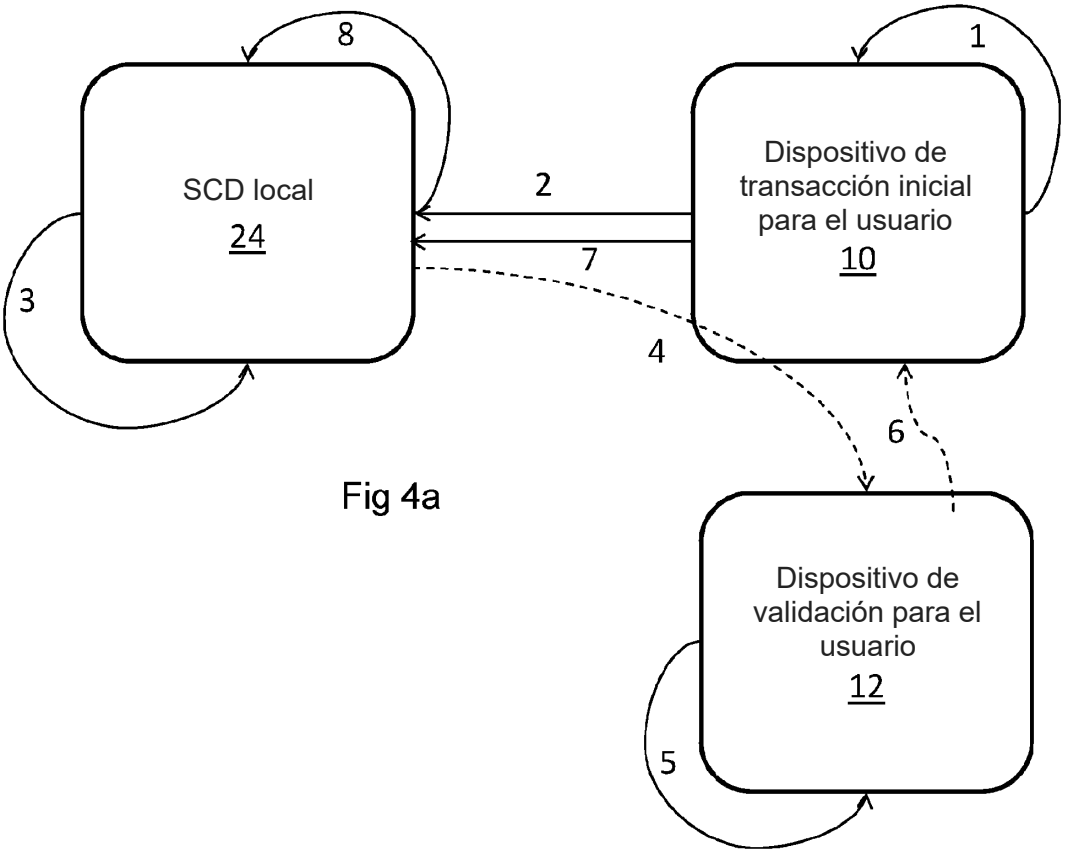
8
1
SCD local
24
2
Dispositivo de transacción inicial para el usuario
10
7
3
4
6
Dispositivo de validación para el usuario
12
5

Fig 4a

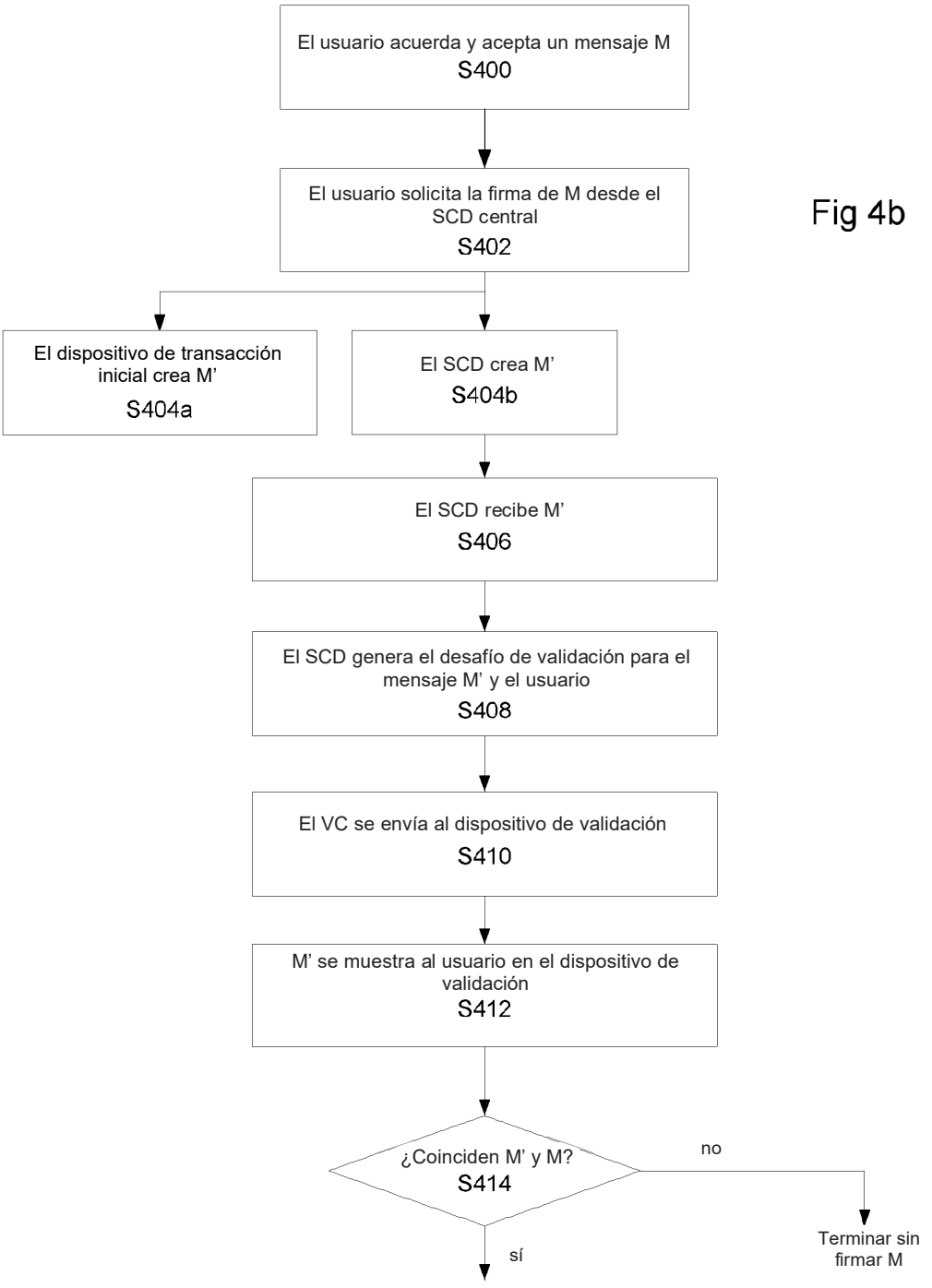
El usuario acuerda y acepta un mensaje M
S400
El usuario solicita la firma de M desde el SCD central
S402
El dispositivo de transacción inicial crea M'
S404a
El SCD crea M'
S404b
El SCD recibe M'
S406
El SCD genera el desafío de validación para el mensaje M' y el usuario
S408
El VC se envía al dispositivo de validación
S410
M' se muestra al usuario en el dispositivo de validación
S412
¿Coinciden M' y M?
S414
no
Terminar sin firmar M
sí

Fig 4b

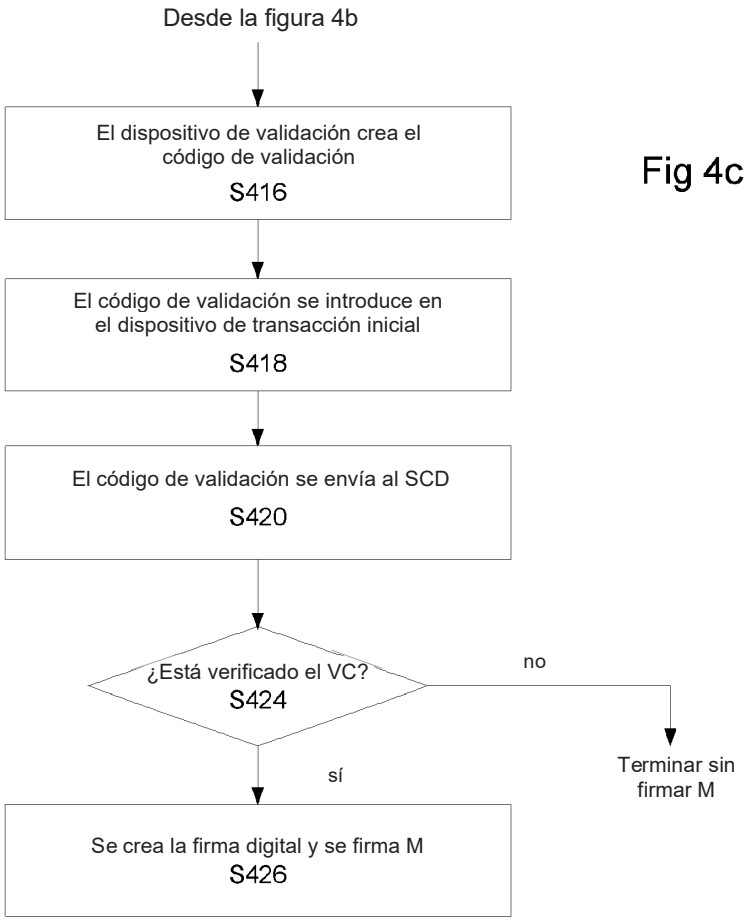
Desde la figura 4b
El dispositivo de validación crea el código de validación
S416
El código de validación se introduce en el dispositivo de transacción inicial
S418
El código de validación se envía al SCD
S420
¿Está verificado el VC?
S424
no
Terminar sin firmar M
sí
Se crea la firma digital y se firma M
S426

Fig 4c

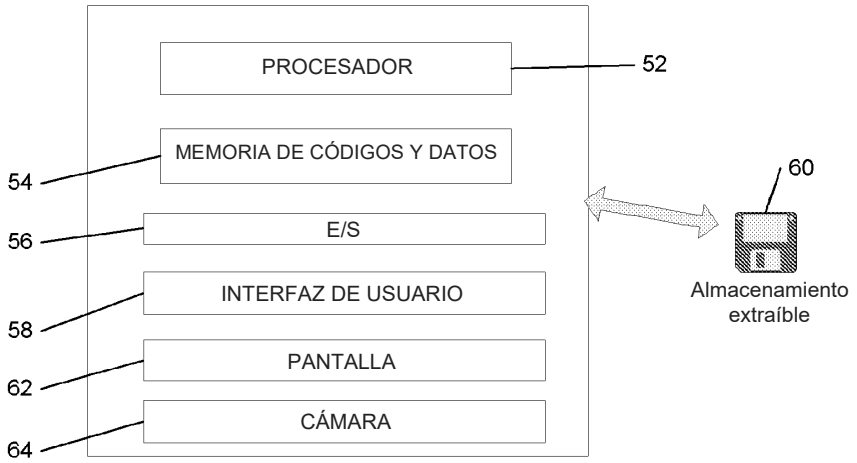
PROCESADOR
52
MEMORIA DE CÓDIGOS Y DATOS
54
E/S
56
INTERFAZ DE USUARIO
58
PANTALLA
62
CÁMARA
64
60
Almacenamiento extraíble

Fig 5a

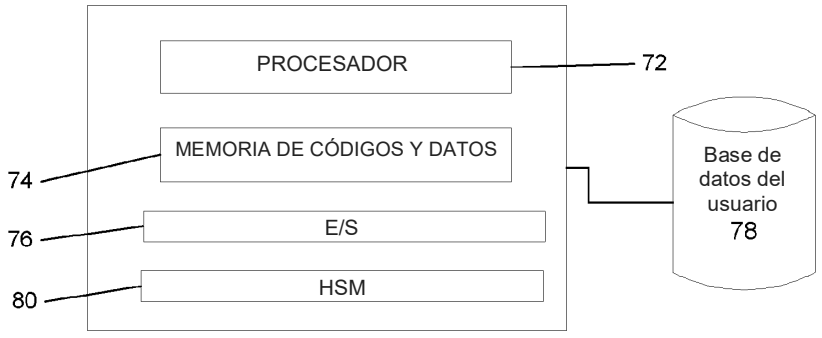
PROCESADOR
72
MEMORIA DE CÓDIGOS Y DATOS
74
E/S
76
HSM
80
Base de datos del usuario
78

Fig 5b