(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 390 155**

(51) Int. CI.:
***G06F 1/00*** (2006.01)
***H04L 29/00*** (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **04806089 .1**
(96) Fecha de presentación: **16.12.2004**
(97) Número de publicación de la solicitud: **1700183**
(97) Fecha de publicación de la solicitud: **13.09.2006**

(54) Título: **Un método de operación segura de un dispositivo informático**

(30) Prioridad:
**23.12.2003 GB 0329835**

(45) Fecha de publicación de la mención BOPI:
**07.11.2012**

(45) Fecha de la publicación del folleto de la patente:
**07.11.2012**

(73) Titular/es:
**CORE WIRELESS LICENSING S.A.R.L. (100.0%)**
**16 Avenue Pasteur**
**2310 Luxembourg, LU**

(72) Inventor/es:
**HEATH, CRAIG y**
**CLARKE, LEON**

(74) Agente/Representante:
**URÍZAR ANASAGASTI, José Antonio**

**DESCRIPCIÓN**

UN MÉTODO DE OPERACIÓN SEGURA DE UN DISPOSTIVO INFORMÁTICO

[0001] La presente invención se refiere a un método para operar un dispositivo informático, y en particular, a un método para el funcionamiento seguro de un dispositivo informático en el que un usuario necesita ser autentificado, tal como introducuendo una frase de paso, antes de que el usuario sea capaz de llevar a cabo una operación solicitada en el dispositivo. La presente invención también se refiere a un dispositivo informático dispuesto para operar de acuerdo con el método anterior y también al programa informático para causar que un dispositivo informático funcione de acuerdo con el método anterior.

[0002] El término dispositivo informático como aquí se usa tiene que interpretarse ampliamente para cubrir cualquier forma de dispositivo eléctrico e incluye dispositivos de grabación de datos, tal como cámaras digitales y de video de cualquier factor de forma, ordenadores de cualquier tipo o forma, incluyendo ordenadores portátiles y personales, y dispositivos de comunicación de cualquier factor de forma, incluyendo teléfonos móviles, télefonos inteligentes, comunicadores que combinan comunicaciones, grabación y/o reproducción de imágenes, y funcionalidad informática dentro de un único dispositivo, y otras formas de dispositivos de información inalámbricos y por cable.

[0003] Cada vez más, los sistemas informáticos distribuidos se están convirtiendo en un aspecto prevalente de la vida diaria. Los dispositivos informáticos distribuidos están ahora conectados por redes de área local, redes de área amplia, y redes de redes, tal como las redes de zonas, tal como Internet. Muchas de tales redes se aseguran por una variedad de técnicas, incluyendo programa cortafuegos, limitaciones de enrutado, codificación, redes virtuales privadas, y/o otros medios. Los ordenadores dentro de un perímetro de seguridad pueden acceder fácilmente a datos almacenados en la red segura, normalmente sujetos a permisos al usuario y al grupo, listas de control de acceso, y similares, mientras a las máquinas fuera del perímetro se les niega el acceso sustancialmente o por completo.

[0004] Con el crecimiento de tales redes seguras y su contenido de información, existe una necesidad en aumento para soportar el acceso seguro por usuarios autorizados. Existe también una necesidad en aumento de autentificar a los usuarios porque incluso aunque un usuario pueda ser autorizado para acceder a una red existen ciertas comunicaciones en una red que se considera que son más sensibles que otros. El uso de técnicas de codificación y descodificación están siendo consideradas cada vez más como esenciales para llevar a cabo cualquier clase de transacción sensible, tal como una compra con tarjeta de cédito por Internet, o la discusión de información empresarial confidencial entre departamentos alejados en una organización.

[0005] Pretty Good Privacy (PGP) es un programa de ordenador usado para codificar y descodificar comunicaciones por grandes redes tal como internet. Puede también usarse para enviar una firma digital codificada que permita a un destinatario de una comunicación verificar la identidad de un remitente y saber que el mensaje no se cambió en ruta. PGP es uno de los programas aseguradores de privacidad más ampliamente utilizados. PGP utiliza una variación del sistema de clave pública. En tales sistemas, cada usuario tiene una clave de codificación públicamente conocida y una clave privada conocida unicamente por ese usuario. Un mensaje enviado a una tercera parte se encripta utilizando la clave pública para esa parte. Cuando el mensaje codificado se recibe por la tercera parte, se desencripta utlizando la clave privada para esa parte. Puesto que el codificar todo un mensaje puede llevar tiempo, PGP utiliza un algoritmo más rápido de codificación para codificar el mensaje y luego utiliza la clave pública para codificar la clave más corta que se utilizó para codificar todo el mensaje. Tanto el mensaje codificado como la clave corta se envian al destinatario que primero utiliza la clave privada del destinatario para descodificar la clave corta y luego utiliza esa clave para descodificar el mensaje. La utilización de técnicas de codificación/descodificaión se considera especialmente importante en comunicaciones inalámbricas porque los circuitos inalámbricos son a menudos más fáciles de "pinchar" que sus homólogos por cable.

[0006] Sin embargo, es imprescindible autentificar a las personas que envían o acceden a datos codificados. La autentificación es el proceso para determinar si alguien o algo es, de hecho, quien o que declara ser. En las redes informáticas privadas y públicas, incluyendo internet, la autentificación se hace normalmente a través del uso de contraseñas de comienzo de sesión. El conocimiento de la contraseña se asume que garantiza que el usuario es auténtico. Cada usuario puede registrarse inicialmente utilizando una contraseña asignada o autodeclarada. En cada uso posterior, el usuario debe conocer y utilizar la contraseña previamente declarada. La debilidad de este sistema para transacciones que son importantes, como el intercambio de dinero, es que las contraseñas a menudo pueden robarse, revelarse accidentalmente, u olvidarse.

[0007] Para programas de codificación y descodificación tales como PGP, se utiliza una palabra de paso, en esencia, como una firma digital para autentificar a una persona. La palabra de paso tiene, de hecho, dos fines- permite al programa gestor de claves determinar que el usuario autorizado del programa está presente en realidad (ya que solamente el usuario conoce el PIN o palabra de paso) y confirma que el usuario desea que la clave se use. Por lo tanto, la palabra de paso se usa para probar que la persona que reivindica haber enviado un mensaje, o que trata de conseguir acceso a un mensaje codificado, o que intenta llevar a cabo una transacción segura tal como una compra comercial, es de hecho esa persona. A causa de que se requiere un nivel mejorado de seguridad en comparación con el provisto por una contraseña normal de acceso, la palabra de

paso es normalmente de unos 16 caracteres de longitud, y frecuentemente pueden ser de hasta unos 100 caracteres de longitud.

[0008] Si software malintencionado intentara invocar al administrador de claves en un intento de firmar una transacción que el usuario no ha solicitado, entonces la apariencia de la interfaz de usuario que solicita al usuario autentificarse alertaria al usuario de que un tercero está intentando utilizar su clave, y el usuario rehusaría autentificarse.

[0009] Como se ha descrito antes, la palabra de paso es normalmente una secuencia relativamente larga de caracteres numéricos y la entrada repetida de la palabra de paso cada vez que la autentificación se requiere no se considera conveniente. Si la palabra de paso es una secuencia alfanumérica relativamente larga, o si la reentrada de la palabra de paso se solicita demasiado a menudo, la autentificación repetida con demasiada frecuencia puede incluso desanimar el uso del proceso de codificación por un usuario en ocasiones donde su uso se consideraría de otro modo particularmente beneficioso. Por ello, para mejorar la experiencia del usuario del uso de tales sistemas, se conoce no requerir al usuario que se autentifique de nuevo si la clave se utiliza en un corto período despues de un uso previo de la clave. Se hace referencia a esto como "cache de palabra de paso". El cache de palabra de paso es un modo de implementar la experiencia del usuario de un modo tal que la clave se “desbloquee” durante un período predeterminado de tiempo. Es solamente tras la caducidad de este período de tiempo cuando el uso adicional de la clave requerirá que se repita el proceso de autentificación.

[0010] Con esquemas conocidos de autentificación, la palabra de paso se cachea durante un período predeterminado de tiempo; por ejemplo 30 minutos. Por ello, como un ejemplo, puede requerirse de un usuario la siguiente secuencia de sucesos con el fin de llevar a cabo una serie deOperaciones seguras

1. Un usuario necesita descodificar un correo electrónico-Operación A
2. El usuario introduce su palabra de paso (se autentifica) para descodificar y leer el correo.
3. Cinco minutos más tarde, el usuario descodifica otro correo electrónico - Operación A.
4. No se pide al usuario que reintroduzca la palabra de paso porque la palabra de paso está todavía memorizada.
5. Un minuto más tarde, el usuario firma otro correo electrónico-Operación B.
6. No se pide al usuario que reintroduzca la palabra de paso porque la palabra de paso está todavía memorizada.
7. Un minuto más tarde, el usuario firma otro correo electrónico -Operación B
8. No se pide al usuario que reintroduzca la palabra de paso porque la palabra de paso está todavía memorizada.
9. Cinco minutos más tarde, el usuario firma otro correo electrónico -Operación B

10. No se pide al usuario que reintroduzca la palabra de paso porque la palabra de paso está todavía memorizada.

11. Una hora más tarde, el usuario intenta firmar otro correo electrónico - Operación B.

12. El usuario reintroduce la palabra de paso porque la la palabra de paso en cache ha expirado.

13. Una hora más tarde, el usuario solicita descodificar otro correo electrónico - Operación A.

14. El usuario reintroduce la palabra de paso porque la palabra de paso en cache ha caducado.

15. Diez minutos más tarde, el usuario solicita llevar a cabo una transacción financiera-Operación C.

16. No se pide al usuario que reintroduzca la palabra de paso porque la palabra de paso está todavía en cache.

[0011] Puede verse del ejemplo anterior que, dado que la palabra de paso está en cache durante un período predeterminado de tiempo, la Operación A, Operación B u Operación C puede llevarse a cabo en tanto en cuanto el período de cache para la palabra de paso es válido porque se adopta un período común de cache independientemente de la Operación a realizar por el usuario. Sin embargo, se apreciará que, en el ejemplo anterior, la Operación C, que implica un gasto financiero, es más sensible comercialmente que la Operación B. Además, la Operación B, que implica la generación de un correo electrónico, es más sensible que la Operación A, que se limita a leer un correo electrónico. Sin embargo, cada una de ellas puede llevarse a cabo sin reintroducir la palabra de paso ya que la palabra de paso ya está autentificada porque el período de cache no ha expirado. Por ello, en cierta medida, el cache de una palabra de paso durante un período que se considera apropiado para un tipo de operación puede comprometer la seguridad para otro tipo de operación.

[0012] Es por tanto un objeto de la presente invención proporcionar un método mejorado para autentificar a un usuario que requiere realizar una operación en un dispositivo informático.

[0013] WO 03007570 revela un método y sistema proporcionados para procesar mensajes codificados en un dispositivo móvil. Un dispositivo móvil recibe un mensaje codificado que comprende contenido codificado asi como información de codificación para acceder al contenido codificado. En el dispositivo móvil, la información de acceso a la codificación se obtiene y se almacena en memoria. La información de acceso a la codificación se recupera de la memoria con el fin de descodificar el contenido codificado cuando se accede posteriormente al mensaje.

[0014] US 5913025 revela un método para que una fuente obtenga los derechos de un objeto objetivo. La fuente obtiene primero los derechos de un objeto de origen, en donde los derechos

incluyen la autorización para acceder a un objeto objetivo y modificar los datos de autentificación del objeto objetivo. Despues, el objeto de origen genera nuevos datos de autentificación. Tras acceder al objeto objetivo usando los derechos del objeto fuente, la fuente modifica los datos de auntentificación del objeto objetivo para incluir los nuevos datos de autentificación. Utilizando los nuevos datos de autentificación, la fuente obtiene los derechos del objeto objetivo, por lo que la fuente se vuelve un proxy para el objeto objetivo. Como proxy, la fuente utiliza los derechos del objeto objetivo.

[0015] EP 0580350 revela un sistema informático distribuido que tiene un número de ordenadores acoplados al mismo en distintos nodos. El ordenador en cada nodo del sistema distribuido tiene una base informática acreditada que incluye un agente de autentificación para autentificar solicitudes recibidas de los principales en otros nodos en el sistema. Las solicitudes se transmiten a servidores como mensajes que incluyen un primer identificador provisto por el solicitante y un segundo identificador provisto por el agente de autentificación del nodo del solicitante. Cada proceso del servidor se proporciona con un cache local de datos de autentificación que identifica a solicitantes cuyos mensajes de solicitud previos se han autentificado. Cuando se recibe una solicitud, el servidor revisa los primeros y segundos identificadores de solicitud contra las entradas en su caché local. Si hay una correspondencia, entonces se sabe que la petición es auténtica. De otro modo, el agente de autentificación del nodo del servidor es llamado para obtener credenciales de autentificación del nodo de los solicitantes para autentificar el mensaje de solicitud. El identificador principal del solicitante y las credenciales recibidas son almacenadas en un caché local por el agente de autentificación del nodo del servidor. El proceso del servidor también almacena un registro en su caché local indicando que se sabe que los mensajes de solicitud del solicitante especificado son auténticos.

[0016] Según un primer aspecto de la presente divulgación se proporciona un método para operar un dispositivo informático, comprendiendo el método, en respuesta a una solicitud de un usuario para realizar una operación usando el dispositivo, determiner el período de tiempo desde que se autentificó la identidad del usuario, y habilitar la operación solicitada en dependencia del período de tiempo determinado y el propósito de la operación solicitada.

[0017] Según un segundo aspecto de la presente divulgación se provee un dispositivo informático dispuesto para operar conforme a un método según el primer aspecto..

[0018] Según un tercer aspecto de la presente divulgación se provee un programa de ordenador para hacer que dispositivos informáticos según el segundo aspecto operen conforme a un método según el primer aspecto.

[0019] Una realización de la presente revelación se describirá ahora, por medio de un ejemplo adicional únicamente, con referencia a la figura 1, que ilustra un diagrama de flujo de un método para autentificar un usuario según la presente invención.

[0020] La invención se define según la reivindicación 1.

[0021] Haciendo referencia a la figura 1, en el paso 2 un dispositivo informático recibe una solicitud para llevar a cabo una operación segura, que unicamente puede completarse si el usuario es realmente autentificado, tal como por entrada de una palabra de paso. En el paso 4, el dispositivo informático determina el tipo de operación que el usuario ha solicitado. Por ejemplo, el usuario puede estar solicitando llevar a cabo la aprobación de un contrato de compra con importantes obligaciones financieras, en cuyo caso es imperativo identificar correctamente al usuario y así asegurar que el usuario tiene la autoridad de comprometerse con las obligaciones financieras. Esto puede verse como una operación que requiere un nivel alto de seguridad. Alternativamente, el usuario puede estar solicitando llevar a cabo una operación de nivel de seguridad relativamente bajo, tal como leer un correo electrónico. El tipo de operación que se solicita puede determinarse de una serie de formas, tal como determinando el tipo de aplicación utilizada para llevar a cabo la operación, el tipo de archivo requerido, o incluso analizando el contenido de la propia petición. Muchos modos de determinar el tipod de operación serán evidentes para personas familiarizadas con esta técnica, y se considera que la presente invencion puede aplicarse a y por tanto engloba cualquier método que puede utilizarse para categorizar las operaciones solicitadas.

[0022] En el paso 6, el dispositivo informático determina el tiempo que ha transcurrido desde que el usuario fue autentificado por última vez introduciendo su palabra de paso. Con la presente invención, el dispositivo informático entonces determina si el tiempo transcurrido desde la autentificación es aceptable para la operación que se solicita. Esto se muestra como paso 8 en la figura 1. Tomando los ejemplos de aprobación de contrato y lectura de un correo electrónico, como se ha referido antes, la lectura del correo electrónico es una operación segura de nivel relativamente bajo y por ello el período de cache normal, digamos una hora, se considera que es aceptable. El período de tiempo transcurrido desde la última autentificación se determina que es menos de una hora y la palabra de paso, y por ello la identidad del usuario, se considera que es auténtica. Por tanto, la operación es habilitada y esto se muestra como paso 10 en la figura 1. Sin embargo, para la operación de aprobación de contrato, el sistema se ha dispuesto de tal modo que para este tipo de operación el período de cache expira tras la finalización de la operación previa del mismo tipo. Por ello, en este ejemplo el dispositivo informático determina en el paso 8 que el tiempo transcurrido desde la última autentificación no es válido para la operación solicitada y pide, en el paso 12 de la figura 1, que el usuario reintroduzca su palabra de paso con el fin de autentificar al usuario para la operación particular de aprobación de contrato. Si la palabra de paso

se introduce correctamente, el usuario es autentificado y se determina que el período de tiempo es aceptable en el paso 8 y entonces se habilita esta operación de alto nivel de seguridad. Despues de habilitar la operación solicitada, el proceso finaliza en el paso 14. Se puede ver que el proceso anterior provee un medio más seguro, pero aún permite que un palabra de paso controle el uso de todas las claves.

[0023] El siguiente ejemplo muestra cómo la presente invención puede utilizarse para dos operaciones similares pero más obviamente distintas. La Operación A es "descodificar y ver mis entradas en el calendario para hoy", y la Operación B es "firmar una transacción para comprar un libro". La Operación A va a ser con toda probabilidad solicitada por el usuario muchas veces durante cada dia laboral y por ello sería muy molesto que el usuario tenga que teclear su palabra de paso cada vez que el usuario desee consultar las entradas del calendario para el día relacionado. En esencia, al usuario solamente se le debería requerir introducir su palabra de paso una vez o posiblemente dos al día para llevar a cabo esta operación. Por otro lado, la Operación B cuesta dinero, de modo que el usuario querrá asegurarse de que un tercero que pueda conseguir acceso al dispositivo informático, lo que puede ser en forma de un teléfono móvil, no pueda llevar a cabo transacción financiera alguna, tal como la compra de libros, de modo que se fija un tiempo de cache relativamente corto para este tipo de operación, Pero supongamos que el usuario desea compar tres libros de tres proveedores en sucesión reltivamente rápida, entonces el usuario no quiere tener que introducir su palabra de paso para cada transacción, pero sin embargo requiere tener un nivel de seguridad mayor que el proporcionado por el tiempo de cache fijado para su calendario. De hecho el usuario puede querer que su palabra de paso permita el uso de la Operación B durante un tiempo relativamente corto, digamos 3 minutos. Así, en la presente invención, las operaciones anteriores pueden conducirse como sigue:

1. El usuario pide ver su calendario– Operación A.
2. El usuario introduce su palabra de paso.
3. Cinco minutos más tarde, el usuario ve otro día en el calendario- Operación A.
4. Dado que la palabra de paso se introdujo hace menos de un día y está dentro del período de cache, el usuario no es urgido a introducir su palabra de paso.
5. Un minuto más tarde, el usuario solicita comprar un libro- Operación B.
6. Dado que la palabra de paso se introdujo por última hace más de 3 minutos, se pide al usuario reintroducir la palabra de paso. Este es un comportamiento diferente y es buena seguridad.
7. Un minuto más tarde el usuario compra otro libro - Operación B
8. No se pide al usuario reintroducir la palabra de paso porque la palabra de paso se introdujo por ultima hace vez menos de 3 minutos.

9. Cinco minutos más tarde el usuario compra otro libro- Operación B.

10. Al usuario se le pide reintroducir la palabra de paso porque se introdujo por última vez hace más de 3 minutos- comportamiento diferente a la Operación B, con seguridad mejorada con el uso de la misma contraseña.

11. Una hora más tarde el usuario compra otro libro– Operación B.

12. Se solicita al usuario reintroducir la palabra de paso.

13. Una hora más tarde el usuario solicita ver las entradas del calendario- Operación A.

14. NO se solicita al usuario reintroducir la palabra de paso porque se introdujo por última vez hace menos de un día)- comportamiento distinto a la Operación B, que proprociona un requisito de nivel de seguridad con buena convenciencia para el usuario.

[0024] En resumen, se pide al usuario su palabra de paso únicamente cuando se considera necesario de acuerdo a la seguridad de la función que está a punto de llevarse a cabo y el tiempo que ha pasado desde que la palabra de paso se introdujo por última vez, y no mecánicamente tras un período de tiempo fijado para un período de cache que no se tiene relación con las funciones que pueden llevarse a cabo durante el período de cache. Se prevé que el usuario seleccionará las categorias de las operaciones y los períodos de tiempo transcurridos de modo que el usuario puede disponer que nunca tenga que reintroducir la palabra de paso en sucesión rápida.

[0025] Aunque la presente invención se ha descrito con referencia a una particular realización, se apreciará que pueden efectuarse modificaciones mientras que zcan dentro del ámbito de la presente invención como se define por las reivindicaciones adjuntas. Por ejemplo, en la realización antes descrita, el tiempo transcurrido se determina desde la última o inmediatamente precedente entrada de la palabra de paso. Sin embargo, este tiempo transcurrido puede también determinarse a partir de una entrada previa de la palabra de paso que no es necesariamente la última entrada. Además, la invención se ha descrito con referencia al uso de palabras de paso. Sin embargo, puede también emplearse otros métodos para autentificar al usuario, tal como el uso de contraseñas o PiNs (Números de Identificación Personal), y/o datos biométricos, tales como reconocimiento de huellas dactilares o de iris.

**REIVINDICACIONES**

1. Un método de operar un dispositivo informático, el método comprendiendo:

   autentificar una identidad;

   habilitar la solicitud de múltiples operaciones utilizando el disposiivo informático, cada operación teniendo un período de tiempo de nivel de seguridad asociado diferente respectivo; y

   determinar si, o no, la autentificación es valida para cada una de las múltiples operaciones solicitadas, en base a si el tiempo entre la autentificación y la operación que se está solicitando está dentro del período de tiempo del nivel de seguridad asociado diferente respectivo.

2. Un método según la reivindicación 1 en el que la identidad es autentificada utilizando una palabra de paso.
3. Un método según la reivindicación 1 en el que la identidad es autentificada utilizando información biométrica.
4. Un método según cualquiera de las reivindicaciones 1 a 3 que comprende determinar que el tiempo entre la última autentificación y la operación que se está solicitando está dentro del período de tiempo del respectivo nivel de seguridad asociado .
5. Un método según cualquiera de las reivindicaciones precedentes en el que la operación solicitada se habilita si el período de tiempo determinado es menor que o igual a un período de tiempo de nível de seguridad fijado por el usuario.
6. Un método según la reivindicación 6 en el que el período de tiempo del nivel de seguridad fijado para un tipo de operación es un múltiplo de un período de tiempo de nivel de seguridad fijado para otro tipo de operación.
7. Un método según la reivindicación 5 en el que el período de tiempo de nivel de seguridad para un tipo de operación se dispone para expirar tras la finalización de la operación del mismo tipo inmediatamente anterior.
8. Un método según cualquiera de las reivindicaciones precedentes, en el que las categorias de operaciones utilizadas para determinar el período de tiempo de nivel de seguridad para una operación solicitada son establecidas por el usuario.
9. El método según cualquiera de las reivindicaciones precedentes, en el que, en respuesta a que la autentificación se determina como no válida para las operaciones solicitadas, el método comprende:

   solicitar autentificación de la identidad.

10. El método según cualquiera de las reivindicaciones precedentes, en el que, en respuesta a que la autentificación se determina como válida para las operaciones solicitadas, el método comprende:

realizar la operación solicitada.

11. Un método según cualquiera de las reivindicaciones precedentes, en el que el nivel de seguridad asociado con una operación corresponde al propósito de la operación.

12. Un método según cualquiera de las reivindicaciones precedentes, en el que cada una de las múltiples operaciones se solicita en un momento diferente.

13. Un método según cualquiera de las reivindicaciones precedentes, en el que la identidad es una identidad de usuario asociado con un usuario.

14. Un dispositivo informático dispuesto para operar según un método como se reivindica en cualquiera de las reivindicaciones 1 a 13.

15. Un dispositivo informático según la reivindicación 14 que comprende un teléfono móvil, unos dispositivos de grabación de datos, un cámara digital, una cámara de video, un ordenador, un ordenador portátil, un ordenador personal, un dispositivo de comunicación, un teléfono movil o un teléfono inteligente.

16. Un programa de ordenador dispuesto para causar que un dispositivo informativo como se reivindica en la reivindicación 14 o 15 opere según un método como se reivindcia en cualquiera de las reivindicaciones 1 a 13.

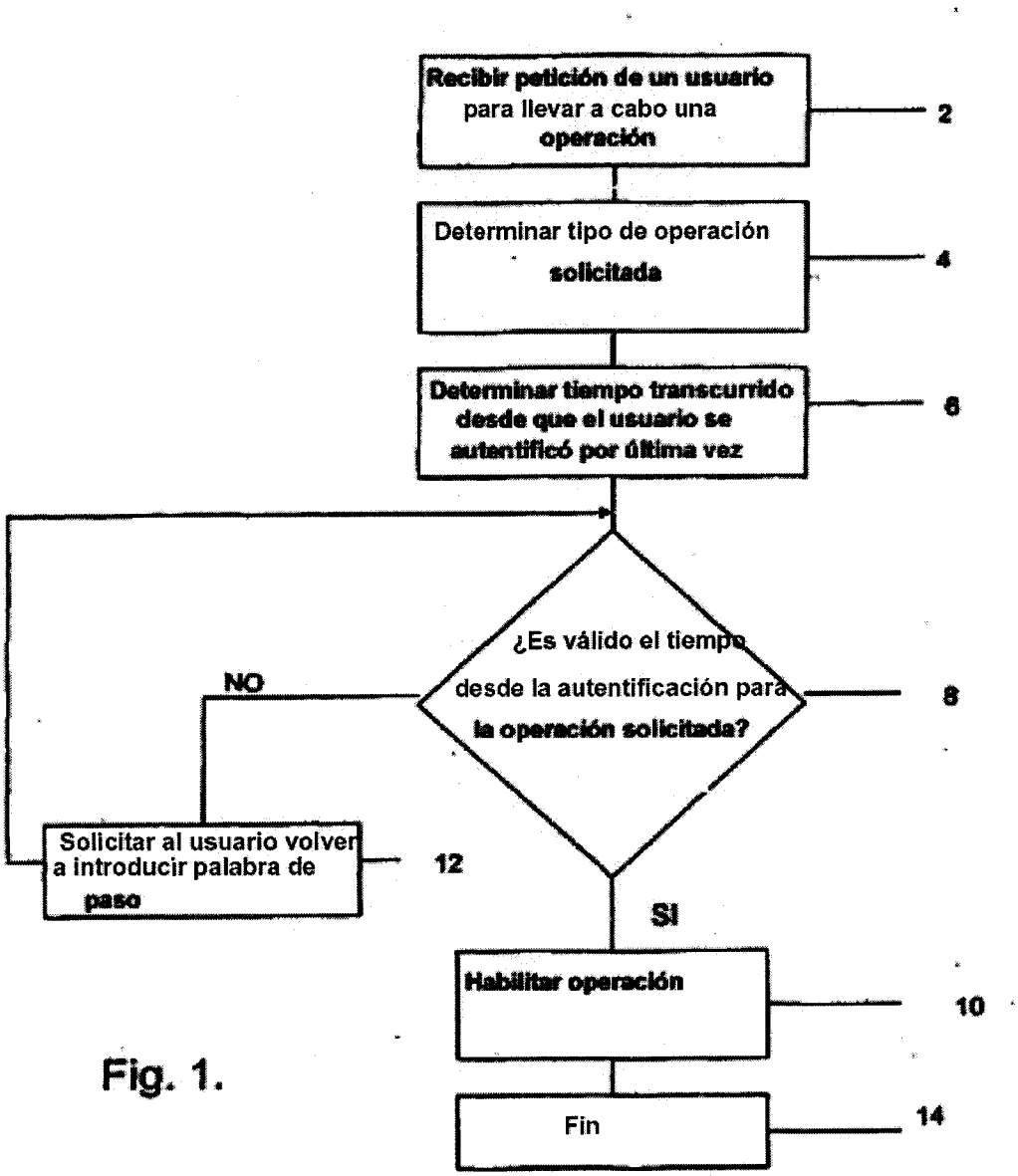
Recibir petición de un usuario para llevar a cabo una operación
2
Determinar tipo de operación solicitada
4
Determinar tiempo transcurrido desde que el usuario se autentificó por última vez
6
¿Es válido el tiempo desde la autentificación para la operación solicitada?
8
NO
SI
Solicitar al usuario volver a introducir palabra de paso
12
Habilitar operación
10
Fin
14

Fig. 1.