(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 820 434**

(51) Int. CI.:

G06F 21/31 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **16.12.2004 E 13157656 (3)**

(97) Fecha y número de publicación de la concesión europea: **03.06.2020 EP 2615570**

(54) Título: **Un procedimiento para la operación segura de un dispositivo informático**

(30) Prioridad:

23.12.2003 GB 0329835

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
21.04.2021

(73) Titular/es:

NOKIA TECHNOLOGIES OY (100.0%)
Karakaari 7
02610 Espoo, FI

(72) Inventor/es:

HEATH, CRAIG y
CLARKE, LEON

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Un procedimiento para la operación segura de un dispositivo informático

La presente invención se refiere a un procedimiento de operación de un dispositivo informático y, en particular, a un procedimiento para la operación segura de un dispositivo informático en el que un usuario necesita ser autenticado, por ejemplo, introducir una frase de contraseña, antes de que el usuario pueda llevar a cabo una operación solicitada en el dispositivo. La presente invención también se refiere a un dispositivo informático dispuesto para funcionar de acuerdo con el procedimiento anterior y también al software informático para hacer que un dispositivo informático funcione de acuerdo con el procedimiento anterior. El documento de la técnica anterior WO03/007570-A1 divulga un procedimiento y sistema para procesar mensajes cifrados en un dispositivo móvil en el que el dispositivo móvil recibe un mensaje cifrado que comprende contenido cifrado así como información cifrada para acceder al contenido cifrado. El documento de la técnica anterior US5913025 divulga un procedimiento para obtener derechos de un objeto de destino en el que los derechos comprenden un período de validez para una operación solicitada. El documento de la técnica anterior EP0580350-A1 divulga un sistema de control de acceso y un procedimiento para el sistema informático distribuido mediante el uso de credenciales de autenticación almacenadas localmente en cache.

El término dispositivo informático, como se usa en la presente memoria debe interpretarse ampliamente para abarcar cualquier forma de dispositivo eléctrico e incluye dispositivos de grabación de datos, como cámaras digitales fijas y de películas de cualquier factor de forma, ordenadores de cualquier tipo o forma, que incluye ordenadores portátiles y personales, y dispositivos de comunicación de cualquier factor de forma, que incluye teléfonos móviles, teléfonos inteligentes, comunicadores los cuales combinan comunicaciones, grabación y/o reproducción de imágenes, y funcionalidad informática dentro de un solo dispositivo, y otras formas de dispositivos de información inalámbricos y cableados.

Cada vez más, los sistemas informáticos distribuidos se convierten en un aspecto frecuente de la vida cotidiana. Los dispositivos informáticos distribuidos ahora se conectan por redes de área local, redes de área amplia y redes de redes, como Internet. Muchas de estas redes son protegidas por una variedad de técnicas, que incluyen software de firewall, limitaciones de enrutamiento, cifrado, redes privadas virtuales y/u otros medios. Los ordenadores dentro de un perímetro de seguridad pueden tener acceso inmediato a los datos almacenados en la red segura, normalmente sujetos a permisos de usuarios y grupos, listas de control de acceso y similares, mientras que a las máquinas fuera del perímetro se les niega sustancial o totalmente el acceso.

Con el crecimiento de estas redes seguras y su contenido de información, existe una creciente necesidad de apoyar el acceso seguro por parte de usuarios autorizados. También existe una creciente necesidad de autenticar a los usuarios debido a que aunque un usuario puede autorizarse a acceder a una red, hay ciertas comunicaciones a través de una red que se consideran más sensibles que otras. El uso de técnicas de cifrado y descifrado se considera cada vez más esencial a la hora de llevar a cabo cualquier tipo de transacción sensible, como una compra con tarjeta de crédito a través de Internet, o la discusión de la información confidencial de la empresa entre diferentes departamentos remotos de una organización.

Privacidad bastande buena (PGP) es un programa informático usado para cifrar y descifrar comunicaciones a través de grandes redes como Internet. También puede usarse para enviar una firma digital cifrada que permite a un receptor de una comunicación verificar la identidad de un remitente y saber que el mensaje no se ha cambiado en la ruta. PGP es uno de los programas de garantía de privacidad más usados. PGP usa una variación del sistema de claves públicas. En estos sistemas, cada usuario tiene una clave de cifrado conocida públicamente y una clave privada conocida solo por el usuario. Un mensaje enviado a un tercero se cifra mediante el uso de la clave pública de ese tercero. Cuando el mensaje cifrado es recibido por un tercero, se descifra mediante el uso de la clave privada de ese tercero. Dado que el cifrado de un mensaje completo puede llevar relativamente mucho tiempo, PGP usa un algoritmo de cifrado más rápido para cifrar el mensaje y a continuación usa la clave pública para cifrar la clave más corta que se usó para cifrar todo el mensaje. Tanto el mensaje cifrado como la clave corta se envían al receptor que primero usa la clave privada del receptor para descifrar la clave corta y a continuación usa esa clave para descifrar el mensaje. El uso de técnicas de cifrado/descifrado se considera especialmente importante en las comunicaciones inalámbricas debido a que los circuitos inalámbricos son a menudo más fáciles de "conectar" que sus contrapartes cableadas.

Sin embargo, es esencial autenticar a las personas que envían o acceden a los datos cifrados. La autenticación es el procedimiento de determinar si alguien o algo es, de hecho, quién o qué se declara que es. En redes informáticas privadas y públicas, incluida Internet, la autenticación se realiza comúnmente mediante el uso de contraseñas de inicio de sesión. Se supone que el conocimiento de la contraseña garantiza que el usuario es auténtico. Cada usuario puede registrarse inicialmente mediante el uso de una contraseña asignada o autodeclarada. En cada uso posterior, el usuario debe conocer y usar la contraseña declarada previamente. La debilidad de este sistema para las transacciones que son significativas, como el intercambio de dinero, es que las contraseñas a menudo pueden ser robadas, reveladas accidentalmente u olvidadas.

Para los programas de cifrado y descifrado como PGP, una frase de contraseña se usa, en esencia, como una firma digital para autenticar a una persona. La frase de contraseña, de hecho, realiza dos propósitos - permitir que el software del administrador de claves determine que el usuario autorizado del software está realmente presente (ya que solo ese usuario conoce el PIN o la frase de contraseña) y confirma que el usuario desea que se use la clave. Por lo tanto, la frase de contraseña se usa para probar que la persona que dice haber enviado un mensaje, o que trata de obtener acceso a un mensaje cifrado, o que trata de llevar a cabo una transacción segura, como una compra comercial, es de hecho esa persona. Dado que se requiere un nivel mejorado de seguridad en comparación con el proporcionado por una contraseña de acceso normal, la frase de contraseña típicamente tiene unos 16 caracteres de longitud y, con frecuencia, estos pueden tener una longitud de hasta unos 100 caracteres.

Si un software fraudulento intentara invocar al administrador de claves en un intento de firmar una transacción la cual el usuario no había solicitado, la aparición de la interfaz de usuario que solicita al usuario que se autentique alertaría al usuario de que un tercero intenta usar su clave, y el usuario se negaría a autenticarse.

Como se indicó anteriormente, la frase de contraseña suele ser una secuencia relativamente larga de caracteres alfanuméricos y la entrada repetida de la frase de contraseña cada vez que se requiere la autenticación del usuario no se considera conveniente. Si la frase de contraseña es una secuencia alfanumérica relativamente larga, o si se solicita la reintroducción de la frase de contraseña con demasiada frecuencia, la autenticación repetida con demasiada frecuencia puede incluso desalentar el uso del procedimiento de cifrado por parte de un usuario en ocasiones en las que su uso se consideraría particularmente beneficioso. Por lo tanto, para mejorar la experiencia del usuario del uso de estos sistemas, se sabe que no requiere que el usuario se autentique de nuevo si la clave se usa poco tiempo después de un uso previo de la clave. Esto se conoce como "almacenamiento en caché de frase de contraseña". El almacenamiento en caché de frase de contraseña es una manera de implementar la experiencia del usuario de tal manera que la clave se "desbloquea" durante un período de tiempo predeterminado. Es solo después de la expiración de este período de tiempo que el uso adicional de la clave requerirá que se repita el procedimiento de autenticación.

Con los esquemas de autenticación conocidos, la frase de contraseña se almacena en caché durante un período de tiempo predeterminado; por ejemplo 30 minutos. Por lo tanto, la siguiente secuencia de eventos puede, como ejemplo, ser necesaria de un usuario con el fin de llevar a cabo una serie de Operaciones seguras.

1. Un usuario solicita descifrar un correo electrónico - Operación A.
2. El usuario introduce su frase de contraseña (se autentica a sí mismo) para descifrar y leer el correo.
3. Cinco minutos más tarde, el usuario descifra otro correo electrónico - Operación A.
4. No se pide al usuario que vuelva a introducir la frase de contraseña debido a que la frase de contraseña sigue almacenada en caché.
5. Un minuto más tarde, el usuario firma otro correo electrónico - Operación B.
6. No se pide al usuario que vuelva a introducir la frase de contraseña debido a que la frase de contraseña sigue almacenada en caché.
7. Un minuto más tarde, el usuario firma otro correo electrónico - Operación B.
8. No se pide al usuario que vuelva a introducir la frase de contraseña debido a que la frase de contraseña sigue almacenada en caché.
9. Cinco minuto más tarde, el usuario firma otro correo electrónico - Operación B.
10. No se pide al usuario que vuelva a introducir la frase de contraseña debido a que la frase de contraseña sigue almacenada en caché.
11. Una hora más tarde, el usuario intenta firmar otro correo electrónico - Operación B.
12. El usuario vuelve a introducir la frase de contraseña debido a que la frase de contraseña almacenada en caché ha expirado.
13. Una hora más tarde, el usuario solicita descifrar otro correo electrónico - Operación A.
14. El usuario vuelve a introducir la frase de contraseña debido a que la frase de contraseña almacenada en caché ha expirado.
15. Diez minutos más tarde, el usuario solicita llevar a cabo una transacción financiera - Operación C.
16. No se pide al usuario que vuelva a introducir la frase de contraseña debido a que la frase de contraseña sigue almacenada en caché.

Puede verse en el ejemplo anterior que, debido a que la frase de contraseña se almacena en caché durante un período de tiempo predeterminado, la Operación A, la Operación B o la Operación C pueden llevarse a cabo mientras el período de almacenamiento en caché de la frase de contraseña sea válido debido a que se adopta un período de almacenamiento en caché común independientemente de la operación que realice el usuario. Sin embargo, se apreciará que, en el ejemplo anterior, la Operación C, que implica gastos financieros, 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, la cual se limita a la lectura de un correo electrónico. Sin embargo, cada uno puede llevarse a cabo sin la reintroducción de la frase de contraseña, ya que la frase de contraseña ya está autenticada debido a que el período de almacenamiento en caché no ha expirado. Por lo tanto, hasta cierto punto, el almacenamiento en caché de una frase de contraseña durante un período el cual se considera apropiado para un tipo de operación puede comprometer la seguridad de otro tipo de operación.

Por lo tanto, es un objeto de la presente invención proporcionar un procedimiento mejorado para autenticar a un usuario que requiera realizar una operación en un dispositivo informático.

De acuerdo con un primer aspecto de la presente invención se proporciona un procedimiento de operación de un dispositivo informático, el procedimiento que comprende, en respuesta a una solicitud de un usuario para llevar a cabo una operación mediante el uso del dispositivo, determinar el período de tiempo desde que se autenticó la identidad del usuario y permitir la operación solicitada en dependencia del período de tiempo determinado y la finalidad de la operación solicitada.

De acuerdo con un segundo aspecto de la presente invención se proporciona un dispositivo informático dispuesto a operar de acuerdo con un procedimiento de acuerdo con el primer aspecto.

De acuerdo con un tercer aspecto de la presente invención se proporciona un software informático para hacer que un dispositivo informático de acuerdo con el segundo aspecto funcione de acuerdo con un procedimiento de acuerdo con el primer aspecto.

A continuación se describirá una realización de la presente invención, a manera de ejemplo adicional, con referencia a la Figura 1, la cual ilustra un diagrama de flujo de un procedimiento para autenticar a un usuario de acuerdo con la presente invención.

Con referencia a la Figura 1, en la etapa 2 un dispositivo informático recibe una solicitud para llevar a cabo una operación segura, la cual solo puede completarse si el usuario está autenticado actualmente, por ejemplo mediante la entrada de una frase de contraseña. En la etapa 4, el dispositivo informático determina el tipo de operación la cual el usuario ha solicitado. Por ejemplo, el usuario puede solicitar llevar a cabo la aprobación de un contrato de compra con obligaciones financieras significativas, en cuyo caso es imperativo identificar correctamente al usuario y de este modo asegurarse de que el usuario tiene la autoridad para comprometerse con las obligaciones financieras. Esto puede considerarse como una operación que requiere un alto nivel de seguridad. Alternativamente, el usuario puede solicitar llevar a cabo una operación de nivel de seguridad relativamente bajo, como la lectura de un correo electrónico. El tipo de operación que se solicita puede determinarse de varias maneras, por ejemplo al determinar el tipo de aplicación usada para llevar a cabo la operación, el tipo de archivo requerido, o incluso analizar el contenido de la propia solicitud. Muchas maneras de determinar el tipo de operación serán evidentes para las personas familiarizadas con esta técnica, y se considera que la presente invención puede aplicarse y, por lo tanto, abarca cualquier procedimiento el cual pueda usarse para clasificar las operaciones solicitadas.

En la etapa 6, el dispositivo informático determina el tiempo transcurrido desde el cual el usuario se autenticó por última vez al introducir su frase de contraseña. Con la presente invención, el dispositivo informático determina el tiempo transcurrido desde que la autenticación es aceptable para la operación que se solicita. Esto se muestra como la etapa 8 en la Figura 1. Al tomar los ejemplos de aprobación del contrato y la lectura de un correo electrónico, como se mencionó anteriormente, la lectura del correo electrónico es una operación segura de nivel relativamente bajo y por lo tanto el período de almacenamiento en caché 'estándar', digamos una hora, se considera aceptable. El período de tiempo transcurrido desde la última autenticación se determina que es inferior a una hora y la frase de contraseña, y de este modo la identidad del usuario, se considera auténtica. Por tanto, la operación se habilita y esto se muestra como la etapa 10 en la Figura 1. Sin embargo, para la operación de aprobación de contrato, el sistema se ha dispuesto de manera que para este tipo de operación el período de almacenamiento en caché expire al finalizar la operación anterior del mismo tipo. Por tanto, en este ejemplo, el dispositivo informático determina en la etapa 8 que el tiempo transcurrido desde la última autenticación no es válido para la operación solicitada y solicita, en la etapa 12 de la Figura 1, para que el usuario vuelva a introducir su frase de contraseña con el fin de autenticar al usuario para la operación de aprobación de contrato en particular. Si la frase de contraseña se introduce correctamente, el usuario se autentica y se determina que el período de tiempo es aceptable en la etapa 8 y a continuación se habilita esta operación segura de alto nivel. Después de habilitar la operación solicitada, el procedimiento finaliza en la etapa 14. Puede verse que el procedimiento anterior proporciona un entorno más seguro, pero todavía permite que una frase de contraseña controle el uso de todas las claves.

En el ejemplo siguiente se muestra cómo puede usarse la presente invención para dos operaciones similares pero obviamente más distintas. La Operación A es "descifrar y ver mis entradas de calendario para hoy", y la Operación B es "firmar una transacción para comprar un libro". La Operación A va a solicitarse por el usuario muchas veces durante cada día laboral y por lo tanto sería muy molesto si el usuario tuviera que escribir su frase de contraseña cada vez que el usuario desea consultar las entradas del calendario para el día en cuestión. En esencia, el usuario solo debe obligarse a introducir su frase de contraseña una o posiblemente dos veces al día para llevar a cabo esta operación. Por otro lado, la Operación B cuesta dinero, por lo que el usuario querrá asegurarse de que un tercero que pueda acceder al dispositivo informático, el cual puede ser en forma de teléfono móvil, no pueda llevar a cabo ninguna transacción financiera, como la compra de libros, por lo que se establece un tiempo de almacenamiento en caché relativamente corto para este tipo de operación. Pero, supongamos que el usuario desea comprar tres libros de tres proveedores en una sucesión relativamente rápida, entonces el usuario no quiere tener que introducir su frase de contraseña para cada transacción, pero sin embargo requiere tener un mayor nivel de seguridad que el proporcionado por el tiempo de almacenamiento en caché establecido para su calendario. De hecho, el usuario

puede querer que su frase de contraseña permita el uso de la Operación B durante un tiempo relativamente corto, digamos 3 minutos. Por tanto, en la presente invención, las operaciones anteriores pueden llevarse a cabo de la siguiente manera:

1. El usuario pide ver su calendario - Operación A.
2. El usuario introduce su frase de contraseña.
3. Cinco minutos más tarde, el usuario ve otro día en el calendario - Operación A.
4. Dado que la frase de contraseña se introdujo hace menos de un día y está dentro del período de almacenamiento en caché, no se solicita al usuario su frase de contraseña.
5. Un minuto más tarde, el usuario solicita comprar un libro - Operación B.
6. Dado que la frase de contraseña se introdujo por última vez hace más de 3 minutos, al usuario se le pide que vuelva a introducir la frase de contraseña. Este es un comportamiento diferente y es una buena seguridad.
7. Un minuto más tarde el usuario compra otro libro - Operación B.
8. No se le pide al usuario que vuelva a introducir la frase de contraseña debido a que la frase de contraseña se introdujo por última vez hace menos de 3 minutos.
9. Cinco minutos más tarde el usuario compra otro libro - Operación B.
10. Se le pide al usuario volver a introducir la frase de contraseña porque se introdujo por última vez hace más de 3 minutos - comportamiento diferente para 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 que vuelva a introducir la frase de contraseña.
13. Una hora más tarde, el usuario solicita ver las entradas del calendario - Operación A.
14. NO se solicita al usuario que vuelva a introducir la frase de contraseña porque se introdujo por última vez hace menos de un día) - comportamiento diferente a la Operación B, que proporciona un nivel de seguridad necesario con una buena comodidad para el usuario.

En resumen, se solicita al usuario su frase de contraseña solo cuando se considere necesario de acuerdo con la seguridad de la operación que está a punto de llevarse a cabo y el tiempo transcurrido desde que se introdujo la última vez la frase de contraseña, y no mecánicamente un período de tiempo fijado para un período de almacenamiento en caché el cual no se refiere a las operaciones las cuales pueden llevarse a cabo durante el período de almacenamiento en caché. Se prevé que el usuario seleccionará las categorías de operaciones y los períodos de tiempo transcurridos asociados para que el usuario pueda disponer nunca tener que volver a introducir la frase de contraseña en rápida sucesión.

Aunque la presente invención se ha descrito con referencia a una realización particular, se apreciará que las modificaciones pueden efectuarse sin dejar de estar dentro del ámbito de la presente invención tal como se define en las reivindicaciones anexas. Por ejemplo, en la realización descrita anteriormente, el tiempo transcurrido se determina a partir de la última o inmediatamente anterior entrada de la frase de contraseña. Sin embargo, este tiempo transcurrido también puede determinarse a partir de una entrada anterior de la frase de contraseña la cual no es necesariamente la última entrada. Además, la invención se ha descrito con referencia al uso de frases de contraseña. Sin embargo, también pueden emplearse otros procedimientos para autenticar al usuario, como el uso de contraseñas o PIN (números de identificación personal) y/o datos biométricos, como el reconocimiento de huellas dactilares o iris.

La divulgación adicional de la invención se proporciona en las siguientes cláusulas numeradas.

1. Un procedimiento de funcionamiento de un dispositivo informático, el procedimiento que comprende, en respuesta a una solicitud de un usuario para llevar a cabo una operación mediante el uso del dispositivo, determinar el período de tiempo desde que se autenticó la identidad del usuario y habilitar la operación solicitada en dependencia del período de tiempo determinado y la finalidad de la operación solicitada.

2. Un procedimiento de acuerdo con la cláusula 1 en el que la identidad del usuario se autentica mediante el uso de una frase de contraseña.

3. Un procedimiento de acuerdo con la cláusula 1 en el que la identidad del usuario se autentica mediante el uso de información biométrica.

4. Un procedimiento de acuerdo con cualquiera de las cláusulas 1 a 3 que comprende determinar el período de tiempo desde que se autenticó por última vez la identidad del usuario.

5. Un procedimiento de acuerdo con cualquiera de las cláusulas anteriores en el que se habilita la operación solicitada si el período de tiempo determinado es menor o igual a un período de tiempo establecido por el usuario.

6. Un procedimiento de acuerdo con la cláusula 5 en el que el período de tiempo establecido para un tipo de operación es un múltiplo de un período de tiempo establecido para otro tipo de operación.

7. Un procedimiento de acuerdo con la cláusula 5 en el que el período de tiempo para un tipo de operación se dispone para expirar una vez finalizada la operación inmediatamente anterior del mismo tipo.

8. Un procedimiento de acuerdo con cualquiera de las cláusulas anteriores en las que el usuario establece categorías de operaciones usadas para determinar el propósito de una operación solicitada.

9. Un dispositivo informático dispuesto para funcionar de acuerdo con un procedimiento definido en cualquiera de las cláusulas 1 a 8.

10. Un dispositivo informático de acuerdo con la cláusula 9 que comprende un teléfono móvil.

11. El software informático dispuesto para hacer que un dispositivo informático como se define en la cláusula 9 o 10 funcione de acuerdo con un procedimiento como se define en cualquiera de las cláusulas 1 a 8.

REIVINDICACIONES

1. Un procedimiento de operación de un dispositivo informático, comprendiendo el procedimiento:
en respuesta a una solicitud (2) de un usuario para llevar a cabo una operación mediante el uso del dispositivo:
determinar (6) un período de tiempo transcurrido que ha transcurrido desde que se autenticó la identidad del usuario;
determinar un período de tiempo asociado a un tipo de operación solicitada; y
habilitar la operación solicitada si el período de tiempo transcurrido está dentro del período de tiempo asociado con el tipo de operación solicitada,
caracterizado porque
el período de tiempo asociado con un tipo de operación solicitada se dispone para expirar una vez finalizada la operación inmediatamente anterior del mismo tipo.

2. Un procedimiento de acuerdo con la reivindicación 1, en el que la identidad del usuario se autentica mediante el uso de una frase de contraseña.

3. Un procedimiento de acuerdo con la reivindicación 1, en el que la identidad del usuario se autentica mediante el uso de información biométrica.

4. Un procedimiento de acuerdo con cualquiera de las reivindicaciones anteriores, en el que el período de tiempo asociado con el tipo de operación solicitada es un período de tiempo establecido por el usuario.

5. Un procedimiento de acuerdo con cualquiera de las reivindicaciones anteriores, en el que el período de tiempo asociado con un tipo de operación es un múltiplo de un período de tiempo establecido para otro tipo de operación.

6. Un procedimiento de acuerdo con cualquiera de las reivindicaciones anteriores, que comprende además solicitar la autenticación de la identidad del usuario con el fin de habilitar la operación solicitada si el período de tiempo transcurrido no está dentro del período de tiempo asociado con el tipo de operación solicitada.

7. Un dispositivo informático que comprende medios para realizar:
en respuesta a una solicitud (2) de un usuario para llevar a cabo una operación mediante el uso del dispositivo:
determinar (6) un período de tiempo transcurrido que ha transcurrido desde que se autenticó la identidad del usuario;
determinar un período de tiempo asociado a un tipo de operación solicitada; y
habilitar la operación solicitada si el período de tiempo transcurrido está dentro del período de tiempo asociado con el tipo de operación solicitada,
caracterizado porque
el período de tiempo asociado con un tipo de operación solicitada se dispone para expirar una vez finalizada la operación inmediatamente anterior del mismo tipo.

8. El dispositivo informático de acuerdo con la reivindicación 7, en el que la identidad del usuario se autentica mediante el uso de una frase de contraseña o en el que la identidad del usuario se autentica mediante el uso de información biométrica.

9. El dispositivo informático de acuerdo con la reivindicación 7 u 8, en el que el período de tiempo asociado con el tipo de operación solicitada es un período de tiempo establecido por el usuario.

10. El dispositivo informático de acuerdo con cualquiera de las reivindicaciones 7 a 9, comprendiendo el dispositivo informático medios adicionales para realizar:
solicitar la autenticación de la identidad del usuario con el fin de habilitar la operación solicitada si el período de tiempo transcurrido no está dentro del período de tiempo asociado con el tipo de operación solicitada.

11. Un dispositivo informático de acuerdo con cualquiera de las reivindicaciones 7 a 10, que comprende al menos uno de un teléfono móvil, un dispositivo de grabación de datos, una cámara fija digital, una cámara de cine, un ordenador, un ordenador portátil, un ordenador personal y un dispositivo de comunicación.

12. Un software informático dispuesto para hacer que un dispositivo informático como se define en cualquiera de las reivindicaciones 7 a 11 realice:
en respuesta a una solicitud (2) de un usuario para llevar a cabo una operación mediante el uso del dispositivo:
determinar (6) un período de tiempo transcurrido que ha transcurrido desde que se autenticó la identidad del usuario;
determinar un período de tiempo asociado a un tipo de operación solicitada; y
habilitar la operación solicitada si el período de tiempo transcurrido está dentro del período de tiempo asociado con el tipo de operación solicitada,
caracterizado porque

el período de tiempo asociado con un tipo de operación solicitada se dispone para expirar una vez finalizada la operación inmediatamente anterior del mismo tipo.

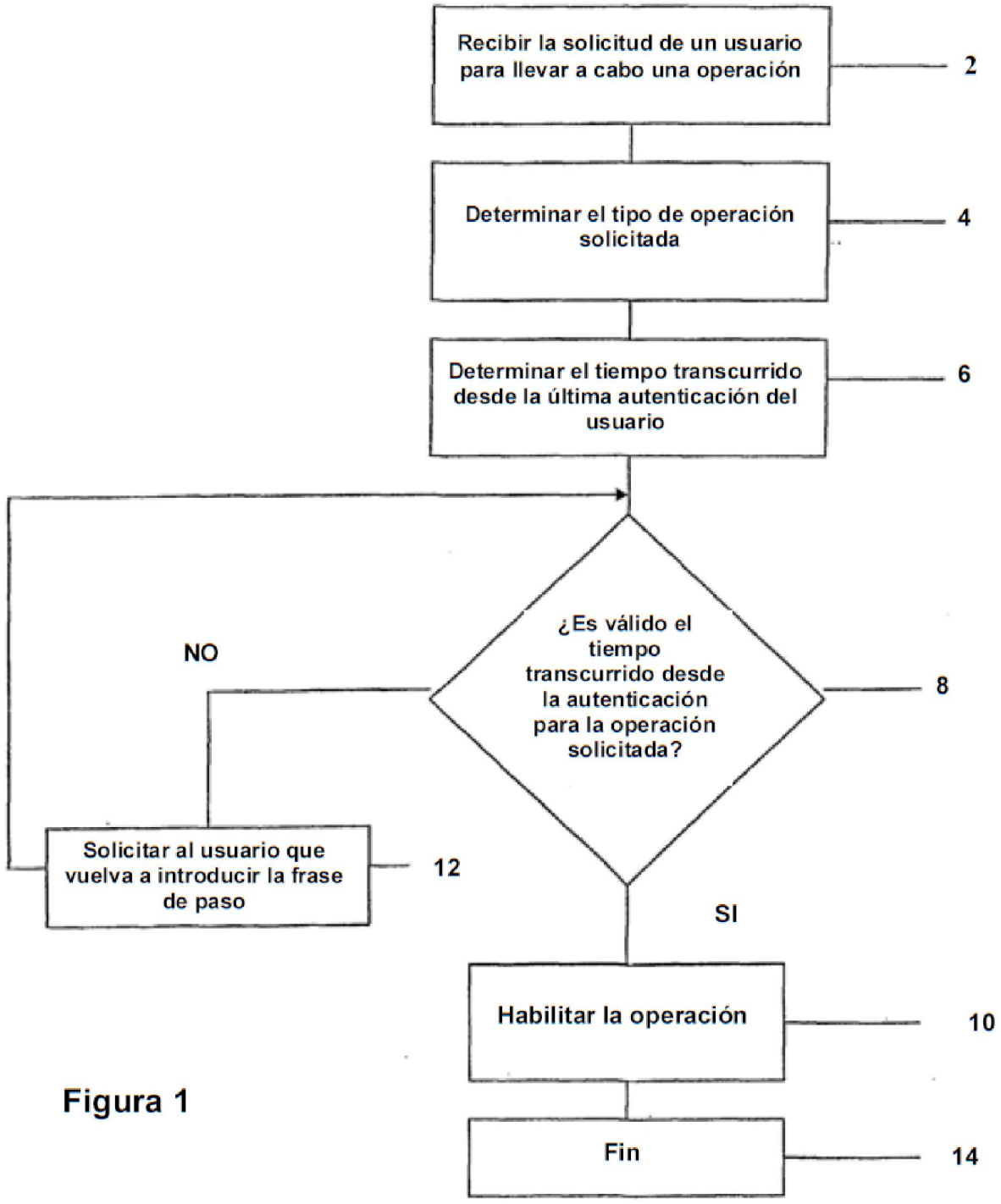
Recibir la solicitud de un usuario para llevar a cabo una operación
2
Determinar el tipo de operación solicitada
4
Determinar el tiempo transcurrido desde la última autenticación del usuario
6
¿Es válido el tiempo transcurrido desde la autenticación para la operación solicitada?
8
NO
Solicitar al usuario que vuelva a introducir la frase de paso
12
SI
Habilitar la operación
10
Fin
14

Figura 1