(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 590 678**

(51) Int. CI.:

G06F 21/72 (2013.01)
G06F 21/34 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **06.09.2013 PCT/GB2013/052347**

(87) Fecha y número de publicación internacional: **13.03.2014 WO14037741**

(96) Fecha de presentación y número de la solicitud europea: **06.09.2013 E 13779326 (1)**

(97) Fecha y número de publicación de la concesión europea: **15.06.2016 EP 2732400**

(54) Título: **Método y sistema para verificar una solicitud de acceso**

(30) Prioridad:

06.09.2012 GB 201215951
07.12.2012 GB 201222090

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.11.2016

(73) Titular/es:

VISA EUROPE LIMITED (100.0%)
1 Sheldon Square
London W2 6TT, GB

(72) Inventor/es:

TARATINE, BORIS;
JOHNSON, MATTHEW;
RUST, SIMON PETER y
ROUNDS, ANDREW WARREN

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Método y sistema para verificar una solicitud de acceso

Campo técnico

La presente invención se refiere a un método y a un sistema para la verificación de una solicitud de acceso, y es particularmente, pero no exclusivamente, adecuado para la verificación de una solicitud de acceso a datos, servicios o activos.

Antecedentes

La demanda de acceso a datos confidenciales o específicos (o bienes o servicios) del usuario es cada vez mayor. Por ejemplo, facilitando el acceso a una cuenta bancaria y permitiendo la transferencia de dinero de esa cuenta se debe restringir a los usuarios autorizados, como el titular de una cuenta. Habitualmente, los usuarios se autentican al solicitar el acceso a los datos por medio de credenciales que identifican a la persona que solicita el acceso a los datos. El acceso remoto de datos presenta problemas particulares debido a que la persona que solicita datos, bienes o servicios es típicamente en una ubicación física diferente a la de la parte que responde a la solicitud. Como resultado, es muy difícil para la parte que atiende la solicitud saber si la entidad que realiza la solicitud es a) quien dice ser, b) tiene derecho a utilizar el dispositivo desde donde se origina la solicitud y c) está en posesión del dispositivo desde donde se origina la solicitud.

Por lo general, cuando una cuenta se establece entre una persona y una parte como un proveedor de datos, la persona va a establecer las credenciales antes mencionadas para ser utilizadas por el proveedor de datos de identificación y autenticación de la persona para futuras solicitudes. Las credenciales pueden incluir información que identifica de forma exclusiva a la persona (por ejemplo, información de identificación personal (PII)) y un secreto (por ejemplo, una contraseña) para su uso en la verificación de la identidad de la persona. Ahora también es común que el proveedor de datos requerirá a la persona registrarse como el propietario de un dispositivo que se utiliza para acceder a los datos. La asociación registrada entre el dispositivo y el propietario del dispositivo puede ser utilizada por el proveedor de datos como un factor de validación adicional. Por ejemplo, en el caso de que un proveedor de datos reciba una solicitud de acceso a una cuenta a nombre de una persona en particular desde un dispositivo particular que no es el dispositivo registrado para la persona, el proveedor de datos puede determinar confiar en que la solicitud se hizo por la persona registrada para la cuenta.

Puede ser relativamente fácil para una persona que desee acceder a los datos de un proveedor de datos en nombre de otra persona que tenga una cuenta con ese proveedor de datos obtener sus credenciales de usuario (es decir, PII, ID de usuario y contraseña) mediante la compra de los mercados en línea criminales en la sombra y, posteriormente, acceder de manera fraudulenta los datos de la otra persona. Además, es posible acceder de forma remota y controlar dispositivos, y por lo tanto solicitar los datos en nombre del propietario registrado de dichos dispositivos. A menudo no es posible determinar si la petición fue hecha por un usuario que esté en posesión física del dispositivo o si la solicitud se hizo de forma remota por un usuario utilizando otro dispositivo para controlar de forma remota el dispositivo desde el que se realiza la solicitud.

Las contraseñas de un solo uso (OTP) se utilizan comúnmente para aliviar estos problemas: un servidor de autenticación asigna de forma exclusiva una generación de claves OTP al propietario registrado de un dispositivo, la generación de claves OTP son para uso en la generación y validación de OTPs. Un servidor de autenticación normalmente tiene cientos o miles de claves de generación de OTP, cada una habiendo sido asignada de forma exclusiva, o registrada respecto a, una persona diferente. El servidor de autenticación configura un testigo OTP en posesión del propietario registrado con su clave de generación de OTP asignada. Estos testigos OTP pueden, por ejemplo, utilizar la tecla de generación de OTP para generar una contraseña diferente cada vez que una nueva contraseña es solicitada por el usuario registrado o como otro ejemplo, puede utilizar la tecla de generación de OTP para generar nuevas contraseñas a intervalos de tiempo regulares. El testigo OTP puede utilizar además la indicación de tiempo actual para generar una OTP, para evitar que la OTP sea almacenada y reproducida en un momento posterior.

Con el fin de acceder a los datos con restricción de usuario a través de un dispositivo, un usuario proporciona la OTP generada por el testigo OTP al proveedor de datos junto con las credenciales que identifican de forma única al propietario del dispositivo. Típicamente, el proveedor de datos a continuación, identifican al propietario del dispositivo y transmite la OTP recibida al servidor de autenticación. El servidor de autenticación buscará la clave de generación de OTP asociada con la persona identificada y utilizará la clave, y si se requiere el tiempo actual, para determinar si la OTP recibida corresponde a la OTP que se habría generado por el testigo OTP en poder del propietario del dispositivo en el momento actual, o al menos dentro de un período predeterminado del tiempo actual. El servidor de autenticación a continuación, indicará al proveedor de datos si la OTP recibida es válida. Si la OTP correcta se envía al proveedor de datos, entonces se puede determinar que el usuario del dispositivo está en posesión del testigo OTP. Sin embargo, los servidores de autenticación son vulnerables a la manipulación lo que facilita la distribución no autorizada a otras entidades y permitiendo que cualquier persona con acceso (ilegítimo) a

una clave de generación de OTP distribuida acceda a los datos en nombre de la persona asociada con esa clave.

El documento US 4998279 describe un sistema en el que una tarjeta genera un código que depende del tiempo que se valida mediante un módulo de control de acceso. Se describen los métodos por los cuales los relojes en la tarjeta y en el módulo de control de acceso se pueden mantener en sincronía. El documento US 2005/005114 describe un método de adquisición de forma segura de un valor para el tiempo desde un servidor remoto.

Sumario

De acuerdo con un primer aspecto de la presente invención, se proporciona un sistema para su uso en la verificación de una solicitud de acceso a los datos, comprendiendo el sistema: un primer módulo que tiene acceso a un segundo indicador de tiempo confiable; un segundo módulo que tiene acceso a un indicador de tiempo no confiable; y un dispositivo informático configurado para comunicarse con un primer indicador de tiempo confiable, en el que: el primer módulo está dispuesto para generar una contraseña utilizando al menos un valor del segundo indicador de tiempo confiable; el segundo módulo está dispuesto para: recibir la contraseña asociada a la solicitud de acceso a los datos; validar la contraseña recibida utilizando por lo menos un valor del indicador de tiempo no confiable; y hacer que, en el caso de que la contraseña recibida sea validada por el segundo módulo, un mensaje que se transmite al dispositivo informático, el mensaje comprendiendo datos indicativos del valor del indicador de tiempo no confiable utilizado para validar la contraseña recibida; y el dispositivo informático estando dispuesto para generar datos indicativos de una comparación entre los datos recibidos indicativos del valor del indicador de tiempo no confiable y un valor del primer indicador de tiempo confiable, en el que el dispositivo informático está dispuesto para proporcionar acceso a los datos almacenados en o generados por el dispositivo informático, en base a los datos generados.

En algunas situaciones, un segundo módulo puede no tener acceso a un indicador de tiempo confiable (sin comunicarse con un elemento externo). En consecuencia, las modificaciones en el tiempo no confiables pueden abrir un sistema a un ataque. Al verificar una contraseña utilizando el indicador de tiempo no confiable y, a continuación, haciendo que un mensaje se transmita a un dispositivo informático, en el que el tiempo no confiable se compara con un tiempo confiable, obviando la posibilidad de un ataque. Por otra parte, se reduce la cantidad de señalización para la verificación, dado que un único mensaje puede necesitar ser enviado desde el segundo módulo al dispositivo o sistema informático.

Ventajosamente, el mensaje transmitido al dispositivo informático puede comprender datos indicativos de la validación de la contraseña recibida utilizando por lo menos el indicador de tiempo no confiable por el segundo módulo.

En una disposición, el primer y segundo módulos comparten un secreto que ha sido asignado de forma única a la misma, el primer módulo está dispuesto para usar el secreto para generar la contraseña, y el segundo módulo está dispuesto para usar el secreto para validar la contraseña recibida. El secreto compartido puede ser almacenado en un elemento de seguridad del primer módulo. Alternativa o adicionalmente, el secreto puede ser almacenado en un elemento de seguridad del segundo módulo. En otras realizaciones, los primer y segundo módulos no comparten un secreto para uso en la generación y validación de contraseñas.

En una disposición, el primer módulo comprende hardware resistente a manipulación que comprende un reloj, el reloj estando dispuesto para proporcionar el segundo indicador de tiempo confiable.

En algunas disposiciones, el segundo módulo puede estar conectado comunicativamente a un dispositivo que tiene un reloj, el reloj estando dispuesto para proporcionar el indicador de tiempo no confiable.

Ventajosamente, en una disposición, el dispositivo informático puede estar dispuesto para enviar un mensaje que comprende los datos generados para un dispositivo informático adicional, y el dispositivo informático puede además estar dispuesto para proporcionar dicho acceso a los datos a la recepción de los datos generados.

El primer módulo puede, en algunas disposiciones, estar dispuesto para recibir, a través de una interfaz del primer módulo, un código de desafío generado por el segundo módulo o el dispositivo informático, y para generar la contraseña utilizando al menos el código de desafío.

En algunas disposiciones, el primer módulo puede estar dispuesto para generar una pluralidad de contraseñas, al menos una contraseña de la pluralidad de contraseñas siendo distinta a la otra contraseña de la pluralidad de contraseñas, y para proporcionar al menos una de las contraseñas generadas a un usuario a través de una interfaz del primer módulo.

Ventajosamente, el segundo módulo y el dispositivo informático pueden compartir un secreto adicional para su uso en comunicaciones entre ellas.

En una disposición, el segundo módulo puede estar dispuesto para almacenar dicha contraseña recibida, y para comparar dicha contraseña recibida a las contraseñas recibidas almacenadas previamente mediante las cuales validar la contraseña recibida.

En algunas disposiciones, el primer y segundo módulos pueden estar comunicativamente desconectados. Esto tiene la ventaja de que la contraseña generada por el primer módulo no se puede acceder de forma remota a través del segundo módulo. Por lo tanto, para que un usuario sea capaz de introducir correctamente una contraseña, que se ha generado por el primer módulo, en el segundo módulo, el usuario debe tener la posesión del primer módulo. En tales disposiciones, por lo tanto, se puede determinar si el usuario tiene la posesión del primer módulo. Esto puede ser útil, por ejemplo, para determinar si el usuario del primer módulo es un usuario humano.

En algunas disposiciones, dichos datos recibidos desde el dispositivo informático comprenden datos que indican si el indicador de tiempo no confiable está dentro de un rango predeterminado del primer indicador de tiempo confiable.

Los datos solicitados pueden, en algunas disposiciones, se contenidos por el segundo módulo, y el segundo módulo se puede configurar para utilizar dichos datos recibidos desde el dispositivo informático para determinar si se debe facilitar el acceso a dichos datos solicitados.

El segundo indicador de tiempo confiable puede ser un reloj del primer módulo, y el primer indicador de tiempo confiable puede ser un reloj que se sincroniza con el reloj del primer módulo.

Ventajosamente, el dispositivo informático y el segundo módulo pueden estar previamente configurados con claves criptográficas para su uso en la firma de datos enviados entre los mismos, y el segundo módulo puede estar dispuesto para firmar dicho mensaje transmitido al dispositivo informático y para verificar que dichos datos recibidos desde el dispositivo informático están firmados por el dispositivo informático utilizando dichas claves criptográficas.

En algunas disposiciones, el segundo módulo puede estar dispuesto para almacenar dicha contraseña recibida, y para comparar dicha contraseña recibida a las contraseñas recibidas almacenadas previamente mediante las cuales validar la contraseña recibida.

De acuerdo con un segundo aspecto de la presente invención, se proporciona un método de verificación de una solicitud de acceso a datos a través de un dispositivo informático que está configurado para comunicarse con un primer indicador de tiempo confiable, comprendiendo el método: generar en un primer módulo de una contraseña con al menos un valor de un segundo indicador de tiempo confiable; recibir en un segundo módulo de una contraseña asociada con la solicitud de acceso a los datos, validar en el segundo módulo la contraseña recibida utilizando por lo menos un valor de un indicador de tiempo confiable; haciendo que, en el caso de que la contraseña recibida es validada por el segundo módulo, se transmita un mensaje al dispositivo informático, el mensaje que comprende datos indicativos de un valor del indicador de tiempo no confiable utilizado para validar la contraseña recibida; y generar en el dispositivo informático los datos indicativos de una comparación entre los datos recibidos indicativos del valor del indicador de tiempo no confiable y un valor del primer indicador de tiempo confiable, y proporcionar el acceso al dispositivo informático a los datos almacenados en, o generados por el dispositivo informático, en base a los datos generados.

Otras características y ventajas de la invención resultarán evidentes a partir de la siguiente descripción de realizaciones preferidas de la invención, dada a modo de ejemplo solamente, que se hace con referencia a los dibujos adjuntos.

Breve descripción de los dibujos

La figura 1 muestra un diagrama de bloques de un sistema de acuerdo con una realización de la presente invención;
La figura 2 muestra esquemáticamente un método de acuerdo con una realización de la presente invención; y
La figura 3 muestra esquemáticamente un método de acuerdo con una realización adicional de la presente invención.

Descripción detallada

Las realizaciones de la invención se refieren a la determinación de si se debe habilitar el acceso a los datos, bienes o servicios solicitados. La figura 1 muestra un diagrama de bloques de un sistema 10 según una realización de la presente invención. El sistema 10 comprende un primer módulo 20 y un segundo módulo 30. El primer módulo 20 está dispuesto para generar contraseñas, y el segundo módulo 30 está dispuesto para recibir las contraseñas de un usuario del sistema 10 y validar las contraseñas recibidas. Tal como se representa por la línea de trazos 15, en la realización mostrada en la figura 1, el primer módulo 20 está comunicativamente desconectado del segundo módulo 30. En otras palabras, el sistema 10 está construido y configurado de tal manera que no hay medio de comunicación (excepto a través de un usuario humano) entre los dos módulos 20 y 30. En una realización particular, se impide la comunicación entre los dos módulos 20 y 30 al estar los módulos 20 y 30 desconectados físicamente unos de otros.

Se entenderá, sin embargo, que los dos módulos 20 y 30 podrían conectarse físicamente (es decir, ser integrados), mientras que estén desconectados de forma comunicativa, por ejemplo, si no comparten ninguna interfaz de circuitos o sistemas comunes o comprenden cualquier otro medio de intercambio de información entre sí.

En una realización alternativa, el primer y segundo módulos de 20,30 se pueden conectar de forma comunicativa.

El primer módulo 20 comprende una interfaz 21, que puede ser una interfaz de usuario. La interfaz 21 puede comprender al menos una entrada y/o salida. Una entrada de una interfaz de usuario de un dispositivo puede ser, por ejemplo, un botón, un teclado, un teclado numérico, un ratón, una pantalla táctil, un micrófono o cualquier otro componente que permita al usuario para proporcionar una entrada al dispositivo. Una salida de una interfaz de usuario de un dispositivo puede ser, por ejemplo, una pantalla, un altavoz, un codificador de Braille, o cualquier otro componente capaz de dar salida a la información del dispositivo a un usuario de la interfaz 21.

El primer módulo 20 puede comprender también un elemento de seguridad 22. Como se describirá en más detalle a continuación, en algunas realizaciones, el elemento de seguridad 22 puede almacenar un secreto que se asigna a los primer y segundo módulos. El elemento de seguridad 22 puede comprender también un reloj 23 que es capaz de proporcionar un indicador de tiempo confiable (denominado en lo sucesivo como el “segundo indicador de tiempo confiable”). El elemento de seguridad 22 puede ser a prueba de manipulación; es decir el elemento de seguridad 22 puede estar configurado de tal manera que el segundo indicador de tiempo confiable no puede ser alterado, y por lo tanto el segundo indicador de tiempo confiable es confiable. Igualmente, a prueba de manipulación significa que el secreto almacenado no puede ser leído, y por lo tanto se utiliza, sin la cooperación del primer módulo 20.

El segundo módulo 30 se muestra como parte de un dispositivo 35. El dispositivo 35 puede comprender una interfaz 31, que puede ser una interfaz de usuario, que puede comprender cualquiera o todas las características descritas anteriormente con referencia a la interfaz 21. Además, el dispositivo comprende un reloj capaz de proporcionar una indicación de tiempo. El segundo módulo 30 es capaz de comunicarse con la interfaz 31 y el reloj 33 del dispositivo, y, como tal, ser capaz de comunicarse con un usuario, en particular para recibir una contraseña proporcionada por el usuario, y ser capaz de acceder a una indicación de tiempo desde el reloj 33.

El segundo módulo 30 en sí puede contener un elemento de seguridad 32. Al igual que el elemento de seguridad 22, el elemento de seguridad 32 puede, en algunas realizaciones, almacenar un secreto asignado a los primer y segundo módulos. En algunas realizaciones, el segundo módulo y/o el elemento de seguridad 32 es extraíble del dispositivo 35. Cuando el reloj 33 del dispositivo 35 no es parte del elemento de seguridad 32, el indicador de tiempo proporcionado por el reloj 33 no es confiable, ya que puede ser alterado por un usuario, o por otras partes (por ejemplo, un adversario a distancia).

El segundo módulo está conectado comunicativamente a al menos un dispositivo o sistema informático adicional, por ejemplo, uno o ambos de los dispositivos informáticos 50 y 60. Estos dispositivos informáticos pueden ser servidores, conectados al dispositivo 35 a través de una red. Alternativamente, los dispositivos informáticos pueden ser otras formas de ordenador, tales como un ordenador de escritorio, al que el dispositivo 35 está conectado, por ejemplo, a través de conexiones 51 y 61. Los dispositivos informáticos pueden ser sistemas distribuidos, es decir, sistemas informáticos en la nube o similares. Los dispositivos informáticos 50 y 60 pueden estar conectados a través de una conexión 52. Como se describirá en más detalle a continuación, el dispositivo informático 50 comprende también un reloj 53, que es capaz de proporcionar un primer indicador de tiempo confiable. El segundo módulo 30 puede estar emparejado con el dispositivo informático 50. Por ejemplo, el segundo módulo 30 puede haber sido emparejado con el dispositivo informático 50 durante un proceso de configuración en el que se le asigna una clave criptográfica tanto para el segundo módulo 30 y el dispositivo informático 50 para su uso en comunicaciones seguras entre los mismos.

Como se indicó anteriormente, en la presente realización, el primer y segundo módulos están comunicativamente desconectados. Por lo tanto, en uso, la interfaz 21 del primer módulo 20 está configurada para proporcionar una contraseña generada a un usuario, que se muestra como el bloque 40, y la interfaz 31 accesible por el segundo módulo 30 está configurada para recibir una contraseña del usuario 40.

En algunas realizaciones, el primer módulo 20 y el segundo módulo 30 pueden ser dispositivos separados que se configuran colectivamente para determinar si es probable que una solicitud de acceso a los datos originada desde un usuario en posesión física del segundo módulo 30. A modo de ejemplo, los dos módulos 20 y 30 pueden fabricarse y venderse juntos, y estar en posesión de una persona en particular. El dispositivo 35 puede, en un ejemplo, ser un dispositivo de comunicaciones, tal como un teléfono móvil o un lector de tarjeta bancaria. Como tal, el segundo módulo puede ser una tarjeta SIM o una tarjeta bancaria capaz de ser insertada en el dispositivo 35. En realizaciones alternativas, el primer y segundo módulos 20 y 30 pueden ser componentes de un solo dispositivo.

El segundo módulo 30 puede operar bajo el control de un usuario que está en posesión del segundo módulo 30 a través de la interfaz 31 del dispositivo 35. Sin embargo, el segundo módulo 30 también puede operar bajo el control de una entidad remota que tiene un enlace de comunicaciones al segundo módulo 30. En la presente realización, como el primer módulo 20 está desconectado de forma comunicativa del segundo módulo 30, como se describe en

más detalle a continuación, no se puede controlar a través de la interfaz 31 del segundo módulo 31, ni por un enlace de comunicaciones a distancia.

El dispositivo 35 puede almacenar datos confidenciales asociados con una persona en particular. Como un ejemplo particular, el segundo módulo 30 puede almacenar claves criptográficas restringidas de usuario para desencriptar datos. Adicional o alternativamente, el segundo módulo 30 puede proporcionar o facilitar el acceso a datos confidenciales que se almacenan externamente por un tercero, por ejemplo, en uno o ambos de los dispositivos informáticos 50 y 60. En este último caso, la tercera parte solo puede permitir el acceso a los datos si se determina que los datos se proporcionan a una persona en particular, es decir, la persona en posesión física de los primer y segundo módulos 20 y 30 (en otras palabras, los datos pueden ser restringidos por el usuario). Antes de que un tercero otorgue acceso a los datos con restricción de usuario a través de un dispositivo en particular, la tercera parte podrá exigir que el propietario de un dispositivo registre una asociación entre el dispositivo y el propietario. En este caso, la tercera parte puede entonces enviar solo datos, que están destinados a ser recibidos por una persona en particular, al dispositivo que está asociado con esa persona. En otras realizaciones, el tercero puede tomar una acción, como el acceso a la información confidencial y/o datos de pago y el envío de la misma a una cuarta parte, si las instrucciones para hacerlo se reciben a través del segundo módulo 30. Por ejemplo, el dispositivo informático 50 puede enviar información confidencial a los dispositivos informáticos 60. Como tal, en el presente ejemplo, el segundo módulo 30 puede tener una asociación registrada con una persona en particular, y por lo tanto el segundo módulo 30 puede ser utilizado para identificar que se trata de la persona en particular, es decir, un titular de la cuenta, que está haciendo una solicitud.

Cuando el segundo módulo 30 comprende un módulo de comunicaciones, se apreciará que una persona no autorizada podría hacer una conexión con el segundo módulo 30 y controlar de forma remota el segundo módulo 30 para enviar una solicitud a la tercera parte. Si el segundo módulo 30 puede determinar si se hizo la solicitud de acceso a datos, ya sea por un usuario en posesión del segundo módulo 30 o por un usuario remoto desde el segundo módulo 30, se puede realizar una acción de respuesta apropiada, por ejemplo, no permitir el uso adicional del segundo módulo 30 cuando se determine que la solicitud fue hecha por un usuario remoto.

Como se explicará a continuación, las realizaciones proporcionan un medio de llevar a cabo dicha determinación. El primer módulo 20 comprende los circuitos y/o software que está construido y configurado para generar una contraseña basada en el indicador de tiempo confiable del reloj 23 (es decir, el segundo indicador de tiempo confiable anteriormente mencionado). Este circuito y/o software pueden, al menos en parte, estar contenidos dentro del elemento de seguridad 23.

Como se describió anteriormente, en una realización, el primer y segundo módulos 20, 30 pueden estar configurados con un secreto compartido para el uso en la generación y validación de contraseñas. En esta realización, el primer módulo 20 puede estar dispuesto para generar una contraseña basado también en el secreto compartido. El secreto puede, en una realización, ser asignado de forma exclusiva a los primer y segundo módulos 20, 30.

El secreto que se asigna a los primer y segundo módulos 20 y 30 puede ser una clave de generación de OTP y la contraseña que se genera por el primer módulo 20 es, pues, una contraseña de un solo uso (OTP). En esta realización, las contraseñas posteriores generadas por el primer módulo 20 son diferentes de las contraseñas generadas con anterioridad, y cada contraseña generada es válida para un solo intento de autenticación. En una disposición particular, la OTP generada es dependiente del tiempo y es válida por un período de tiempo predeterminado. En una disposición alternativa, el primer módulo 20 puede generar una contraseña en dependencia de una contraseña generada anteriormente y el segundo indicador confiable del tiempo usando una clave de generación de OTP.

La OTP se genera por el primer módulo 20 en función de una segunda indicación de tiempo confiable proporcionada por el reloj 23 del primer módulo 20 y la clave de la generación de OTP (es decir, el secreto). La OTP puede ser una función criptográfica de la clave de la generación de OTP y el tiempo actual. En el caso de que el primer módulo 20 y el segundo módulo 30 sean piezas de material compuesto de un solo dispositivo, la OTP, además, se puede generar en función de un identificador de dispositivo asociado de forma única con el dispositivo. Tal ID de un dispositivo puede ser, por ejemplo, una función hash de la ID de la CPU, una función hash de una ID GPU del dispositivo, o una combinación de las mismas. En este caso, la OTP puede ser una función criptográfica de la clave de la generación de OTP, la ID de dispositivo y el segundo indicador de tiempo confiable. El valor del segundo indicador de tiempo confiable será conocido aquí como el “tiempo de generación” T_G, y se entenderá que se ha medido con respecto al reloj 23 del primer módulo 20. En este caso, una OTP generada particular, solo se puede utilizar para validar una solicitud de acceso a los datos si se utiliza dentro de un período predeterminado de tiempo de generación T_G. En tales casos, la OTP generada puede ser validada si el tiempo T_{RU} está dentro de un período predeterminado de tiempo anterior o posterior al tiempo de generación T_G utilizado para generar la contraseña en el primer módulo 20 - aquí T_{RU} puede preceder a T_G debido a la deriva de tiempo entre los dos indicadores de tiempo.

Se apreciará que, a pesar del nombre, hay una posibilidad baja pero finita de que una OTP puede ser reutilizada. Sin embargo, la probabilidad de que una contraseña generada anteriormente será válida en un momento posterior es

efectivamente la misma que la posibilidad de que trabajo contraseña aleatoria funcione, y como tal, para los fines de este documento, se supondrá que una contraseña dada solo será válida una vez durante el curso de la vida de los módulos, y por lo tanto es una OTP. Además, si una OTP es utilizada dos veces dentro del período de tiempo predeterminado para el que es válida, será rechazada - esto impide que se reutilicen las contraseñas.

El segundo módulo 30 también comprende circuitos y/o software que está construido y configurado para determinar, basado en el indicador de tiempo no confiable de reloj 33 (y opcionalmente también el secreto compartido, si el segundo módulo 30 está configurado de esta forma), si una contraseña recibida desde el usuario 40 del segundo módulo 30 coincide con la contraseña que se habría generado por el primer módulo 20 en el momento que se indica por el indicador de tiempo no confiable desde el reloj 33. Una vez más, al menos una parte de la circuitería y/o software puede estar contenido dentro del elemento de seguridad 32.

En la realización particular mostrada en la figura 1, un secreto está asignado de forma exclusiva a los primer y segundo módulos 20 y 30. En otras palabras, el secreto puede estar asociado con los primer y segundo módulos 20 y 30 solamente. Sin embargo, esto no es un requisito esencial. En formas de realización, los elementos de seguridad 22 y 32 de los primer y segundo módulos 20 y 30 son a prueba de manipulaciones, es decir, el secreto y el algoritmo utilizado para generar la contraseña almacenada en el elemento de seguridad 23 y 33 no pueden ser alterados.

Como se mencionó anteriormente, la contraseña tal como se genera por el primer dispositivo 20 se genera utilizando un algoritmo apropiado y una indicación de tiempo, y por lo tanto es una OTP. El indicador de tiempo (es decir, el segundo indicador de tiempo confiable antes mencionado) puede ser, por ejemplo, un número entero, donde el número entero se incrementa a una frecuencia predeterminada (por ejemplo, cada 30 segundos o cada minuto). El número entero puede tener un valor de cero correspondiente a un punto conocido en el tiempo en el pasado, y puede ser dispuesto de tal manera que, durante la vida útil del dispositivo, el número entero no pasa – es decir que no alcanzará el valor máximo del registro que almacena el número entero, y por lo tanto volverá a cero. Esto asegura que el segundo indicador del tiempo confiable tiene un valor único que nunca se repite, y por lo tanto todas las contraseñas generadas usando el segundo indicador confiable no se repetirá. A pesar de lo anterior, será evidente que cualquier otro indicador de tiempo confiable puede ser utilizado en su lugar. El segundo indicador de tiempo confiable puede ser generado por un reloj contenido en el elemento de seguridad 23.

La figura 2 muestra esquemáticamente un método de ejemplo de acuerdo con la presente realización. En este método, el usuario 40 realiza una solicitud de acceso a los datos, tal como se representa por la flecha 74. La solicitud de acceso a los datos puede ser, por ejemplo, una solicitud de acceso a una página web restringida, una solicitud de acceso a información confidencial, o una solicitud de acceso a los datos para su uso en permitir el acceso a un servicio. La solicitud puede ser presentada en el dispositivo 35, y por lo tanto a través del segundo módulo 30, alternativamente, la solicitud podrá realizarse por el usuario a cualquiera de los dispositivos informáticos 50 y 60. En general, los datos a los que el usuario 40 desea acceder podrían ser los datos almacenados o generados por cualquiera de los componentes del sistema 10, o pueden ser datos que se almacenan en, o generados por una entidad que es externa al sistema 10 (por ejemplo, una base de datos o un servidor externo). Los datos a los que el usuario 35 del segundo módulo 30 desea acceder pueden ser, por ejemplo, una página web restringida alojada en un servidor, que es externo al sistema 10, y en este caso, el acceso a la página web puede ser activado por el servidor enviando datos al segundo módulo 30. La información contenida en los datos enviados por el segundo módulo 30 se explicará en más detalle a continuación.

En respuesta a la solicitud de acceso a los datos en la etapa 74, el segundo módulo 30, en la etapa 76, solicita al usuario 40 introducir una contraseña que se ha generado por el primer módulo 20. El usuario, en la etapa 78, a continuación, puede hacer que el primer módulo 20 genere una contraseña, por ejemplo, pulsando un botón de la interfaz 21 del primer módulo o indicando de otro modo al primer módulo 20 que se requiere una contraseña.

En la etapa 80, el primer módulo 20 utiliza el secreto que se asigna de forma única a los primer y segundo módulos 20 y 30, así como la segunda indicación de tiempo confiable proporcionada por el reloj 33, para generar una contraseña, que a continuación se proporciona en la etapa 82 al usuario 40. La contraseña generada puede ser, por ejemplo, una serie de números, una serie de letras, una combinación de letras, números y otros caracteres o una imagen y puede por ejemplo ser presentada al usuario 40 en una pantalla de la interfaz 21.

Alternativamente, el primer módulo 20 puede generar contraseñas (en dependencia del secreto compartido y el segundo indicador de tiempo confiable) a intervalos de tiempo regulares y puede presentar automáticamente la contraseña generada más recientemente en la interfaz 21 del primer módulo 20. En tales situaciones, la etapa 78 no se requeriría dado que el primer módulo 30 presenta la contraseña sin petición.

En cualquier caso, el usuario 40 puede entonces proporcionar, en la etapa 84, la contraseña generada por el primer módulo 20 al segundo módulo 30. Esto puede ser hecho por el usuario que introduce la contraseña en la interfaz 31 del dispositivo 35, a través de la que se proporciona al segundo módulo 30. En la etapa 86, el segundo módulo 30 a continuación, utiliza el secreto que se asigna de forma única a los primer y segundo módulos 20 y 30, y el indicador de tiempo no confiable desde el reloj 33 del dispositivo 35, para verificar si la contraseña recibida del usuario 40 es la misma que la contraseña que se habría generado por el primer módulo 20.

Se apreciará que cuando se introduce una contraseña que se genera por el primer módulo 20 en el segundo módulo 30, la contraseña debe haberse recuperado anteriormente del primer módulo 20. Como, en esta realización, el primer módulo 20 está comunicativamente desconectado del segundo módulo 30, es muy probable que el usuario 40 es un humano que está en posesión de, o al menos tiene acceso a, el primer módulo 20, así como por lo tanto al segundo módulo 30, y es capaz de recuperar la contraseña del primer módulo 20 y proporcionarla de forma manual al segundo módulo 30.

Como se indicó anteriormente, el primer módulo 20 y el segundo módulo 30 pueden comprender cada uno un elemento de seguridad respectivo 22 y 32 en el que se almacena un secreto. El secreto puede ser asignado de forma única a los primer y segundo módulos 20 y 30 y almacenados en los elementos de seguridad 22 y 32. En otras palabras, el secreto que se asigna únicamente a la primera y segunda módulos 20 y 30 se almacena en partes de los primer y segundo módulos 20 y 30 que no se puede accedido por un usuario, tal como el usuario 40, e igualmente cualquier otra parte que pueden tener acceso a los primer y segundo módulos 20 y 30.

En este caso, el secreto puede ser provisto a los elementos de seguridad 22 y 32 de los primer y segundo módulos 20 y 30 en la fabricación. En una realización, los elementos de seguridad 22 y 32 se fabrican por separado de los demás componentes de los módulos 20 y 30 y por lo tanto la asociación entre los módulos 20 y 30 y el secreto almacenado en los elementos de seguridad 22 y 32 no puede ser conocida por cualquier entidad externa al sistema 10. El almacenamiento del secreto dentro de elementos seguros 22 y 32 evita que cualquier usuario con acceso a cualquiera de los módulos 20 y 30 descubra el secreto y por lo tanto sea capaz de descubrir la contraseña que debe ser introducida en el segundo módulo 30 con el fin de acceder a los datos solicitados. También evita que cualquier usuario altere el algoritmo para la generación de contraseñas, que de este modo podrían hacer que el primer módulo 20 o el segundo módulo 30 generen una respuesta falsa. Por ejemplo, el algoritmo en el segundo módulo se puede alterar para aceptar cualquier entrada como válida.

Una ventaja particular de la presente realización surge del hecho de que el secreto para generar y validar la contraseña está asignado de forma exclusiva a los primer y segundo módulos 20 y 30. Más específicamente, porque hay una asignación uno a uno entre el secreto y el módulo 30 que utiliza el secreto para validar la contraseña, y también una asignación uno a uno entre el secreto y el módulo 20 que utiliza el secreto de generar la contraseña, por lo tanto, en el caso de que el secreto se vea comprometido, los módulos 20 y 30 solo tienen que ser reconfigurados con un nuevo secreto (que es de nuevo asignado de forma exclusiva a los módulos 20 y 30). Esto se puede lograr, por ejemplo, mediante la sustitución de los elementos de seguridad 22 y 32 de los módulos 20 y 30 con nuevos elementos seguros que tienen el nuevo secreto almacenado en el mismo. Alternativamente, cuando los módulos son artículos de coste relativamente bajo, tales como un SIM de teléfono (segundo módulo 30) y un módulo generador de contraseña asociada (primer módulo 20), los dos módulos pueden ser reemplazados.

Esto puede ser contrastado con el sistema de OTP conocido descrito en la sección de antecedentes, en el que una clave de OTP dada está asociada de forma única a un usuario en particular en lugar de a un par de módulos 20 y 30. En este sistema conocido, no puede haber una relación de uno a muchos entre la clave OTP y los dispositivos que utilizan la clave OTP para generar una contraseña. Siendo ese el caso, si se compromete una clave OTP, los datos pueden ser accedidos en nombre de ese usuario a través de cualquier dispositivo que utiliza la clave OTP. Como normalmente se almacena la clave OTP tanto en el número de testigos de OTP y también en el servidor de autenticación, establecer una nueva clave OTP puede ser bastante oneroso en el servidor de autenticación, ya que se requiere tanto que el servidor de autenticación vuelva a asignar una nueva generación de claves OTP a ese usuario y configurar un nuevo conjunto de testigos OTP con la nueva generación de claves OTP.

El segundo módulo 30 utiliza el indicador de tiempo no confiable del reloj 33 y la clave de la generación de OTP (es decir, el secreto compartido) para determinar si la contraseña es la misma que una contraseña que se habría generado por el primer módulo 20 en un tiempo dentro un tiempo predeterminado desde el momento en que la contraseña fue recibida por el segundo módulo 30. El valor del indicador de tiempo no confiable en el que la contraseña fue recibida por el segundo módulo 30 se dará a conocer en el presente documento como el “tiempo de recepción no confiable” T_{RU}.

El método utilizado por el segundo módulo 30 para validar la contraseña recibida dependerá del método utilizado por el primer módulo 20 para generar la contraseña. Muchos de estos métodos ya son conocidos y el método específico se considera fuera del ámbito de la presente invención.

Si el segundo módulo 30 determina que la contraseña recibida coincide con una OTP que fue/se habría generado por el primer módulo 20 en un momento T_G es decir dentro de un período predeterminado de tiempo de recepción T_{RU}, entonces el segundo módulo 30 valida la contraseña recibida.

Sin embargo, esta contraseña puede haber sido generada por el primer módulo 20 en un momento anterior, y reproducida al segundo módulo 30. Esto puede ocurrir si el dispositivo 35 ha sido comprometido, y por lo tanto la contraseña introducida a través de la interfaz 31 puede ser interceptada. Como se mencionó anteriormente, la contraseña es una contraseña de un solo uso (OTP) que se generó con una indicación de tiempo. Por lo tanto, el retardo de tiempo entre que se genera la contraseña por el primer módulo 20 y es recibida por el segundo módulo 30

típicamente sería suficiente para que la OTP ya no sea válida.

Sin embargo, el segundo módulo 30 solo tiene acceso a un indicador de tiempo no confiable. Esto es típicamente debido a que el indicador de tiempo es proporcionado por el reloj 33 del dispositivo 35. Como tal, el reloj puede haberse ajustado, por ejemplo, manipulando el dispositivo 35, a través del acceso remoto del dispositivo, o de forma legítima, simplemente ajustando el reloj 33 a través de una preferencia del usuario. Esto significa que el indicador de tiempo no confiable podría ser ajustado para corresponder al tiempo en el que la contraseña se ha generado por el primer módulo 20 y por lo tanto a un tiempo que corresponde a una contraseña que fue recibida anteriormente por un adversario. Esto a su vez puede hacer que el segundo módulo determine correctamente que la contraseña reproducida es válida.

El segundo módulo 30 solo puede tener acceso a un tiempo no confiable, porque no es práctico proporcionar el segundo módulo 30, o el elemento de seguridad 32, con un tiempo seguro, y por lo tanto confiable. Por ejemplo, cuando el elemento de seguridad es una tarjeta SIM o tarjeta bancaria, la energía puede ser retirada del segundo módulo 30, y como tal cualquier reloj que se ejecuta en el módulo puede perder el tiempo. Esto hace que el segundo módulo 30 dependa del reloj 33 del dispositivo 35, que como se ha dicho es no confiable.

Como tal, una vez que el segundo módulo 30 ha validado una contraseña recibida utilizando el indicador de tiempo no confiable T_{RU}, el segundo módulo 30 envía un mensaje en la etapa 88 al dispositivo informático 50. Este mensaje contiene datos indicativos de que el indicador de tiempo se utiliza para validar la contraseña recibida (es decir, la marca de tiempo no confiable T_{RU}). El mensaje también puede contener datos indicativos de la validación de la contraseña recibida (utilizando el tiempo no confiable) por el segundo módulo 30.

Como se mencionó anteriormente, el dispositivo informático 50 tiene acceso a un primer indicador de tiempo confiable, por ejemplo, a través de un reloj 53. Este reloj 53 puede ser sincronizado con el reloj 23 del primer módulo 20. Aquí, ser sincronizado significa que es posible que el dispositivo informático 50 acceda a un indicador de tiempo (T'_G) que está dentro de un rango predeterminado (para permitir la deriva entre los relojes) del tiempo T_G utilizado por el primer módulo 20 para generar la contraseña. Además, la confianza puede haber sido establecida entre el dispositivo informático 50 y el segundo módulo 30 por el intercambio de claves criptográficas para su uso en la firma y por lo tanto en la autenticación de los mensajes enviados entre los mismos, como se discutirá en más detalle a continuación.

Al recibir el mensaje que contiene el indicador de tiempo no confiable, el dispositivo informático 50 compara el indicador de tiempo no confiable T_{RU} indicado en el mensaje recibido con el primer indicador de tiempo confiable T'_G tal como se determina por el reloj 53 del dispositivo informático 50. Si el tiempo no confiable T_{RU} se determina para estar dentro del rango predeterminado del primer tiempo T'_G confiable y el mensaje indica que la contraseña recibida por el segundo módulo 30 es válida, el dispositivo informático 50 determina confiar en que el usuario 40 tiene acceso a ambos primer y segundo módulos 20 y 30. En consecuencia, el dispositivo informático 50 puede generar datos indicativos de esta comparación, y el uso de los datos generados para proporcionar acceso a los datos, según lo solicitado inicialmente en la etapa 74.

Esto es porque, si el segundo módulo 30 ha validado positivamente una contraseña recibida utilizando la marca de tiempo T_{RU}, entonces el usuario 40 debe haber proporcionado una contraseña que se habría generado por el primer módulo 20 en un tiempo confiable T_G que está cerca de T_{RU}. Se deduce entonces que, si T_{RU} está cerca del tiempo T'_G confiable tal como se determina por el dispositivo informático 50, entonces T_G también debe estar cerca del tiempo actual y por lo tanto se puede determinar que el usuario 40 debe haber proporcionado una contraseña que era/habría generado por el primer módulo 20 en algún momento T_G cerca de, es decir, dentro de un rango predeterminado del tiempo actual, como se indica por T'_G. Por lo tanto, el usuario 40 es probable que esté actualmente en posesión de, o al menos tenga acceso a, el primer módulo 20. Como no hay manera de transferir automáticamente una contraseña generada por el primer módulo 20 al segundo módulo 30, es muy probable que la persona en posesión del segundo módulo 20 también esté en posesión del primer módulo 30 y por lo tanto puede transferir la contraseña generada por el primer módulo 20 al segundo módulo 30 manualmente.

Ventajosamente, si el dispositivo informático 50 determina que la marca de tiempo no confiable T_{RU} no está dentro del intervalo predeterminado de tiempo confiable T'_G, y por lo tanto se obtuvo de una fuente de tiempo que no está sincronizada con el reloj del primer módulo 20, el dispositivo informático 50 puede denegar el acceso a los datos.

En consecuencia, como se muestra en la etapa 92, el dispositivo informático 50 puede comunicarse con los otros elementos del sistema para efectuar el acceso a los datos, utilizando para ello los datos generados por la comparación anterior. Por ejemplo, el dispositivo informático 50 puede enviar un mensaje al segundo módulo 30 que indica si el tiempo T_R está dentro del intervalo de tiempo predeterminado. Si el tiempo T_R está dentro del intervalo de tiempo predeterminado, el segundo módulo 30 puede habilitar el acceso a los datos solicitados. Alternativamente, si el tiempo T_R está fuera del rango de tiempo predeterminado, el segundo módulo puede negar el acceso a los datos solicitados.

El usuario 40 puede haber solicitado el acceso a los datos contenidos externamente por el dispositivo informático 50. En este caso, el dispositivo informático 50 puede responder o bien mediante el envío de los datos solicitados al segundo módulo 30 o denegar el acceso.

Alternativamente, en un ejemplo adicional, el dispositivo informático 50 puede permitir el acceso, por el dispositivo informático 60, a los datos almacenados en uno o ambos del dispositivo informático 50 o el segundo módulo 30. En un ejemplo adicional más, la validación satisfactoria se puede utilizar para permitir que el dispositivo informático 50, y/o el segundo módulo 30, accedan a datos en el dispositivo informático 60.

En los ejemplos anteriores, el segundo módulo 30 puede almacenar OTP recibidas anteriormente y anular cualquier OTP que se haya recibido previamente. Esto es particularmente útil en situaciones en las que se accede al segundo módulo 30 al mismo tiempo tanto por un adversario remoto como por un usuario en posesión de ambos primer y segundo módulos 20 y 30 (es decir, un usuario local 40). Suponiendo que los intentos de los usuarios remotos de acceder a los datos mediante la replicación de una OTP que fue inscrita en el segundo módulo 30 por el usuario local 40, el segundo módulo 30 rechazará la OTP replicada como un duplicado. En una disposición, el segundo módulo 30 puede almacenar un número limitado de OTPs recibidas previamente de manera que sea capaz de rechazar duplicados. El número de duplicados almacenados puede ser tal que si una OTP particular, que ya no es almacenada por el segundo módulo 30, se replica, la tercera parte 100 es probable que rechace la OTP ya que se asocia con una marca de tiempo que está fuera el intervalo predeterminado del tiempo actual.

El mensaje que contiene la marca de tiempo no confiable T_{RU} utilizada por el segundo módulo 30 para validar una contraseña recibida puede ser firmado por el segundo módulo 30 (por ejemplo, usando una clave(s) criptográfica asociada con el segundo módulo 30 y el dispositivo informático 50), permitiendo así que el dispositivo informático 50 verifique el origen del mensaje. Esto significa que, si el usuario remoto intenta alterar un mensaje enviado por el segundo módulo 30 que contiene el tiempo no confiable, el dispositivo informático 50 reconocerá que el mensaje ha sido alterado, ya que no contendrá la firma correcta del segundo módulo, y negará el acceso a los datos solicitados asociados. Del mismo modo, los mensajes reproducidos, es decir, los mensajes previamente enviados por el segundo módulo 30, que se vuelven a enviar al dispositivo informático 50 contendrán un indicador de tiempo no confiable T_{RU} que está en el pasado, y serán rechazados.

Además, si el dispositivo informático 50 está configurado para enviar un mensaje al segundo módulo 30 que indica si una marca de tiempo recibida es válida, ese mensaje puede también ser firmado. Esto permite que el segundo módulo 30 identifique los mensajes enviados al segundo módulo 30 por una parte que no sea el dispositivo informático 50, que puede no ser confiable.

Lo anterior puede ser contrastado con un sistema en el que el segundo módulo 30 recupera una marca de tiempo de un tercero. En tal sistema es posible que un usuario remoto pueda observar una OTP introducida por un usuario 40 en posesión de ambos primer y segundo módulos 20 y 30 y también puede observar la marca de tiempo recibida de la tercera parte. Ese usuario remoto puede, en algún momento posterior, suministrar el segundo módulo 30 con la marca de tiempo observada y la OTP observada. En este caso, el segundo módulo 30 puede validar la contraseña del usuario remoto. Sin embargo, en un sistema configurado de acuerdo con la realización anterior, el segundo módulo 30 envía la marca de tiempo que se utiliza para validar la contraseña al dispositivo informático 50, el dispositivo informático 50 siendo capaz de identificar que cualquier marca de tiempo está fuera de fecha y en consecuencia denegará el acceso a los datos que se solicitan.

Un sistema configurado de acuerdo con la forma de realización anterior tiene la ventaja de que el segundo módulo es capaz de tomar la primera etapa en la verificación de la contraseña proporcionada sin tener que acceder a una marca de tiempo remota. Esto acelera el tiempo para la verificación, ya que solo un único mensaje (etapa 88) puede necesitar ser transmitido al sistema en su conjunto para completar la verificación. Por el contrario, un sistema en el que se proporciona una marca de tiempo confiable al segundo módulo 30 requiere al menos dos mensajes, una petición de tiempo confiable y una respuesta.

La figura 3 muestra esquemáticamente un método de ejemplo para el intercambio de claves criptográficas temporales, como una forma de proporcionar acceso a los datos, entre un proveedor de servicios bancarios, que puede ser el dispositivo informático 50, y el segundo módulo 30. En este ejemplo, el proveedor de servicios bancarios 50 ha compartido claves criptográficas temporales con otro proveedor de servicios, que pueden estar asociadas con el dispositivo informático 60. Juntas, las claves criptográficas compartidas con el proveedor de servicios 60 y las claves criptográficas compartidas con el segundo módulo 30 se pueden usar en la autenticación y/o cifrado/descifrado de los mensajes enviados entre el segundo módulo 30 y el proveedor de servicios 60, como se discutirá en más detalle a continuación.

El segundo módulo 30 y el proveedor de servicio bancarios 50 ya han preasignado claves criptográficas para su uso en la codificación y la autenticación de los mensajes enviados entre los mismos, como se discutió anteriormente. Además, el proveedor de servicios bancarios 50 puede almacenar una asociación entre el segundo módulo 30 y el titular de una cuenta bancaria particular.

Como se describió anteriormente, el segundo módulo 30 no tiene un reloj que se sincronice con el reloj del primer módulo 20. Sin embargo, el proveedor de servicios bancarios 50 tiene un reloj que se sincroniza con el reloj del primer módulo 20 (por ejemplo, los dos relojes pueden ejecutar en tiempo universal, o el proveedor de servicios bancarios 50 puede ser capaz de derivar la marca de tiempo en el primer módulo 20).

En este ejemplo concreto, un usuario 40 solicita, en la etapa 96, una clave criptográfica temporal del proveedor de servicios bancarios 50 a través del segundo módulo 30 y el dispositivo 35. Al solicitar el acceso a la clave de cifrado temporal, el usuario 40 puede proporcionar información al segundo módulo 30 y/o el dispositivo 35 que identifica al titular de la cuenta bancaria particular, respecto de la cual el usuario 40 quiere obtener una clave de cifrado temporal.

Al recibir la petición de una clave criptográfica temporal, es decir, la solicitud de datos, el segundo módulo 30 envía un mensaje (etapa 98) al proveedor de servicios bancarios 50 que indica que una solicitud de acceso a una clave criptográfica temporal se ha realizado por un usuario 40 y que indica que los módulos 20 y 30 están disponibles para generar y validar las contraseñas. Este mensaje (enviado en la etapa 98) informa al proveedor de servicios bancarios 50 que será capaz de determinar si la solicitud (en la etapa 98) para el acceso a una clave criptográfica temporal se originó a partir de un usuario en posesión física de los primer y segundo módulos 20 y 30.

En consecuencia, como se muestra en la etapa 74', el proveedor de servicios bancarios 50 podrá solicitar que el segundo módulo proporcione una indicación de que se ha proporcionado la contraseña correcta. En esta realización, el procedimiento continúa generalmente como se describe anteriormente con referencia a las etapas 76 a 88, con una contraseña que se solicita desde el primer módulo, y es validada por el segundo módulo.

Sin embargo, además, un código de desafío puede ser utilizado para proporcionar aún más la seguridad. El código de desafío puede ser generado por el segundo módulo 30, o puede ser recibido por el segundo módulo 30 desde el proveedor de servicios bancarios 50 en la etapa 74'. El código de desafío se proporciona al usuario 40 en la etapa 76, y se proporciona al primer módulo 30 por el usuario 40 en la etapa 78. El código de desafío es utilizado por el primer módulo 20 en la generación de la contraseña en la etapa 80, y, posteriormente, en la validación de la contraseña por el segundo módulo en la etapa 86.

En una etapa adicional (no referenciada) el usuario 40 puede ser obligado a introducir las credenciales (como un nombre de usuario y un PIN o contraseña) que han sido acordadas previamente entre el proveedor de servicios bancarios 50 y el titular de la cuenta bancaria (es decir, el usuario 40). Esto tiene la ventaja de que el proveedor de servicios bancarios 50 es capaz de verificar si el usuario 40 del segundo módulo 30 es el titular de la cuenta bancaria identificado o si el usuario es una persona diferente (que pueden haber robado los módulos 20 y 30, por ejemplo).

Como se describió anteriormente, el segundo módulo 30 determina en la etapa 86 si la contraseña recibida desde el usuario 40 es válida basado en la indicación de tiempo no confiable disponible para el segundo módulo 30 y, en su caso, cualquier código de desafío que pueda haber sido proporcionado. Posteriormente, en la etapa 88 el segundo módulo 30 envía un mensaje proporcionando la indicación de tiempo no confiable utilizada para verificar esa OTP recibida. El mensaje puede contener, además, datos indicativos de que la OTP recibida se encontró que era válida, y que el código de desafío correcto fue utilizado para generar la contraseña. La respuesta puede ser encriptada y/o firmada, por ejemplo, mediante el uso de las claves criptográficas compartidas entre el segundo módulo 30 y el dispositivo informático 50. La respuesta también puede contener cualquier nombre de usuario, contraseña y similares proporcionados por el usuario 40.

Si, por el contrario, el segundo módulo 30 no valida correctamente la contraseña recibida, el segundo módulo 30 puede enviar un mensaje firmado con el proveedor de servicios bancarios 50 que indica que la OTP recibida se encontró que era no válida.

Si el mensaje enviado en la etapa 88 indica que la OTP recibida fue validada a continuación, el proveedor de servicios bancarios 50 puede comparar el tiempo indicado en la marca de tiempo no confiable enviada en la etapa 88 con el primer indicador de tiempo confiable. Esta etapa puede incluir cualquier otra forma de autenticación, por ejemplo, la validación de un nombre de usuario y contraseña como se describe anteriormente. Si el proveedor de servicios bancarios 50 determina que el tiempo no confiable (proporcionado en la etapa 88) se encuentra dentro del intervalo de tiempo predeterminado y, si es necesario, que cualquier otra credencial de autenticación (es decir, nombre de usuario y contraseña) es válida, el proveedor de servicios bancarios 50 puede enviar (en la etapa 100) la clave criptográfica temporal solicitada al segundo módulo 30, donde entonces se almacena.

En un ejemplo alternativo, en lugar de que proveedor de servicios bancarios 50 genere y distribuya la clave criptográfica temporal, la clave criptográfica temporal podría ser generada por el proveedor de servicios 60, y se envía al proveedor de servicios bancarios 50, que a continuación, determinar si desea compartir que clave con el segundo módulo 30 como en el caso de que la clave criptográfica temporal es generada por el proveedor de servicios bancarios 50. Alternativamente, la clave criptográfica temporal podría ser generada por el segundo módulo 30, y puede ser enviada al proveedor de servicios bancarios 50 en el mensaje 88, por ejemplo. En esta disposición,

el proveedor de servicios bancarios 50 puede luego compartir esa clave de cifrado temporal con un proveedor de servicios 60.

Como se mencionó anteriormente, el segundo módulo 30 se ha registrado en un proveedor de servicios bancarios 50 como propiedad de un titular de la cuenta bancaria particular. El proveedor de servicios bancarios 50 comparte claves criptográficas temporales con el segundo módulo 30 y el proveedor de servicios 60. El proveedor de servicios 60 puede que ya sepa que el titular de la cuenta bancaria es el propietario registrado del segundo módulo 30, y en este caso, cuando las claves criptográficas temporales son compartidas con el proveedor de servicios 60, el titular de la cuenta bancaria que se asocia con dichas claves está identificado para el proveedor de servicios 60. Alternativamente, si el titular de la cuenta bancaria no es aún conocido por el proveedor de servicios 60, el proveedor de servicios bancarios 50 puede enviar al proveedor de servicios 60 información para su uso en la identificación y prestación de un servicio al titular de la cuenta bancaria cuando las claves criptográficas temporales asociadas son compartidas.

En el presente ejemplo, un usuario puede solicitar el acceso 40 (etapa 102) a un proveedor de servicios adicional 60 para su uso en la realización de un pago o la transferencia de fondos de la cuenta del titular de la cuenta bancaria

En algunas formas de realización, en lugar de una solicitud de acceso a datos que están siendo recibidos en cualquiera del segundo módulo 30, el dispositivo informático 50 o el dispositivo informático 60 de un usuario 40, una solicitud de acceso a los datos puede ser generada por cualquiera del segundo módulo 30, el dispositivo informático 50 o el dispositivo informático 60 sin intervención del usuario. Por ejemplo, una tercera parte que opera el dispositivo informático 50 puede desear determinar si hay un usuario 40 del segundo módulo 30 que está en posesión física del segundo módulo 30 y por lo tanto el dispositivo informático 50 envía un mensaje al segundo módulo 30 que indica el mismo. Tras la recepción de este mensaje, el segundo módulo 30 solicita a un usuario 40 del segundo módulo 30 introducir una contraseña que se ha generado por el primer módulo 20 en el segundo módulo 30, y el procedimiento continúa como se describió anteriormente.

Las realizaciones de la invención pueden ser contrastadas con un sistema en el que el secreto utilizado por el primer módulo 20 para generar una contraseña no es conocido por el segundo módulo 30, sino que se comparten entre un servidor de autenticación, tal como el dispositivo informático 50, y el primer módulo 20. Mientras que el segundo módulo 30 en dicha forma de realización no requiere tener acceso a una indicación de tiempo, ya sea confiable o no, el sistema puede perder la seguridad de tener el secreto compartido de forma única entre el primero y segundo módulo, cuando el secreto es comparte entonces entre el primer módulo 20 y el dispositivo informático 50. De hecho, si el dispositivo informático 50 se viera comprometido, muchos secretos pueden llegar a ser conocidos, en contraste con el sistema anterior, en el que solo un único secreto puede llegar a ser conocido a través de un primero o segundo módulo que quedara comprometido.

Como se ha indicado anteriormente, los primer y segundo módulos 20 y 30 pueden ser piezas compuestas del mismo dispositivo y pueden ser desconectados de manera comunicativa entre sí dentro de ese dispositivo. En estas realizaciones, la única forma (realista probable) en que un usuario 40 es capaz de recuperar una contraseña desde el primer módulo 20 e insertarla en el segundo módulo 30 es si el usuario 40 está en posesión del primer módulo 20. Por lo tanto, se deduce que, en este caso, el usuario 40 es muy probable que esté en posesión del dispositivo y por lo tanto es un usuario humano. Por lo tanto, si el segundo módulo 30 valida la contraseña recibida del usuario 40, el segundo módulo 30 puede determinar hasta un nivel de confianza muy alto que la solicitud de acceso a los datos se originó de un humano que está en posesión del dispositivo (y por lo tanto, no es una entidad remota). Permitiendo el acceso a los datos solicitados puede incluir permitir el acceso a datos restringidos contenidos en el dispositivo o, en el caso de que los datos solicitados estén contendidos por un tercero (tal como el dispositivo informático 50), puede incluir el envío de datos a la tercera parte para utilizarlos para permitir el acceso a los datos solicitados.

Se apreciará que el usuario 40 como se describe anteriormente puede no ser una sola persona física, y como tal, un primer usuario de este tipo puede proporcionar la contraseña a un segundo usuario, desde el cual la contraseña es recibida por la interfaz 31.

La interfaz 21 del primer módulo 20 y la interfaz 31 del dispositivo 35 pueden ser interfaces de usuario como se describió anteriormente. Sin embargo, en algunas formas de realización, las interfaces pueden proporcionar una interfaz de entrada/salida que se conecta a una interfaz de usuario adecuada. Esto puede hacerse para permitir que el primer módulo 30 o el dispositivo 35 sean distribuidos, de tal manera que las interfaces de usuario a través de las que se proporciona la contraseña pueden estar físicamente separadas.

Las realizaciones anteriores han de entenderse como ejemplos ilustrativos de la invención. Se prevén realizaciones adicionales de la invención. Por ejemplo, el segundo módulo 30 puede ser utilizado para permitir el acceso a los datos, los bienes o servicios que se encuentren o suministrados por una pluralidad de terceros, por ejemplo, los dispositivos informáticos 50 y 60 y otros sistemas que no se muestran. Se apreciará que, mientras que, en muchas de las realizaciones descritas anteriormente, el primer y segundo módulos se han descrito como que están conectados de forma comunicativa, esta característica no es una característica esencial de la invención, y en otras realizaciones, el primer y segundo módulos 20, 30 pueden estar conectados de forma comunicativa. Del mismo

modo, a la vez que ventajosa, los primer y segundo módulos 20, 30 no están obligados a compartir un secreto para su uso en la generación y validación de contraseñas. Es de entenderse que cualquier característica descrita en relación con cualquier forma de realización puede ser utilizada sola, o en combinación con otras características descritas, y también se puede usar en combinación con una o más características de cualquier otra de las realizaciones, o cualquier combinación de cualquier otra de las formas de realización. Además, equivalentes y modificaciones no descritas anteriormente también se pueden emplear sin apartarse del alcance de la invención, que se define en las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un sistema para su uso en la verificación de una solicitud de acceso a datos, comprendiendo el sistema:

un primer módulo (20) que tiene acceso a un segundo indicador de tiempo confiable;
un segundo módulo (30) que tiene acceso a un indicador de tiempo no confiable; y
un dispositivo informático (50) configurado para comunicarse con un primer indicador de tiempo confiable,

en el que:

el primer módulo (20) está dispuesto para generar una contraseña utilizando al menos un valor del segundo indicador de tiempo confiable;
el segundo módulo (30) estando dispuesto para:

recibir la contraseña asociada a la solicitud de acceso a los datos;
validar la contraseña recibida utilizando por lo menos un valor del indicador de tiempo no confiable; y
hacer que, en el caso de que la contraseña recibida sea validada por el segundo módulo, se transmita un mensaje al dispositivo informático (50), comprendiendo el mensaje datos indicativos del valor del indicador de tiempo no confiable utilizado para validar la contraseña recibida; y

el dispositivo informático (50) está dispuesto para generar datos indicativos de una comparación entre los datos recibidos indicativos del valor del indicador de tiempo no confiable y un valor del primer indicador de tiempo confiable,

en el que el dispositivo informático (50) está dispuesto para proporcionar acceso a los datos almacenados en, o generados por el dispositivo informático (50), sobre la base de los datos generados.

2. Un sistema de acuerdo con la reivindicación 1, en el que el mensaje transmitido al dispositivo informático (50) comprende datos indicativos de la validación de la contraseña recibida utilizando por lo menos el indicador de tiempo no confiable por el segundo módulo.

3. Un sistema de acuerdo con cualquiera de las reivindicaciones anteriores, en el que el primer y segundo módulos comparten un secreto que ha sido asignado de forma única a los mismos, estando dispuesto el primer módulo para usar el secreto para generar la contraseña, y estando dispuesto el segundo módulo para utilizar el secreto para validar la contraseña recibida.

4. Un sistema de acuerdo con cualquiera de las reivindicaciones anteriores, en el que el primer módulo (20) comprende hardware resistente a manipulación (22) que comprende un reloj (23), estando dispuesto el reloj (23) para proporcionar el segundo indicador de tiempo confiable.

5. Un sistema de acuerdo con cualquiera de las reivindicaciones anteriores, en el que el segundo módulo (30) está conectado en comunicación con un dispositivo que tiene un reloj (33), estando dispuesto el reloj (33) para proporcionar el indicador de tiempo no confiable.

6. Un sistema de acuerdo con cualquiera de las reivindicaciones anteriores, en el que el dispositivo informático (50) está dispuesto para enviar un mensaje que comprende los datos generados a un dispositivo informático adicional (60), estando dispuesto el dispositivo informático adicional (60) para proporcionar dicho acceso a los datos a la recepción de los datos generados.

7. Un sistema de acuerdo con cualquiera de las reivindicaciones anteriores, en el que el primer módulo (20) está dispuesto para recibir, a través de una interfaz (21) del primer módulo, un código de desafío generado por el segundo módulo (30) o el dispositivo informático (50), y para generar la contraseña utilizando al menos el código de desafío.

8. Un sistema de acuerdo con cualquiera de las reivindicaciones anteriores, en el que el segundo módulo (30) y el dispositivo informático (50) comparten un secreto adicional para su uso en comunicaciones entre ellos.

9. Un método de verificación de una solicitud de acceso a los datos utilizando un dispositivo informático (50) que está configurado para comunicarse con un primer indicador de tiempo confiable, comprendiendo el método:

generar en un primer módulo (20) una contraseña utilizando al menos un valor de un segundo indicador de tiempo confiable;
recibir en un segundo módulo (30) la contraseña asociada a la solicitud de acceso a los datos,
validar en el segundo módulo (30) la contraseña recibida utilizando por lo menos un valor de un indicador de tiempo no confiable;
hacer que, en el caso de que la contraseña recibida sea validada por el segundo módulo, se transmita un

mensaje al dispositivo informático (50), el mensaje comprendiendo datos indicativos de un valor del indicador de tiempo no confiable utilizado para validar la contraseña recibida;

generar en el dispositivo informático (50) datos indicativos de una comparación entre los datos recibidos indicativos del valor del indicador de tiempo no confiable y un valor del primer indicador de tiempo confiable; y

proporcionar en el dispositivo informático acceso a los datos almacenados en, o generados por el dispositivo informático (50), sobre la base de los datos generados.

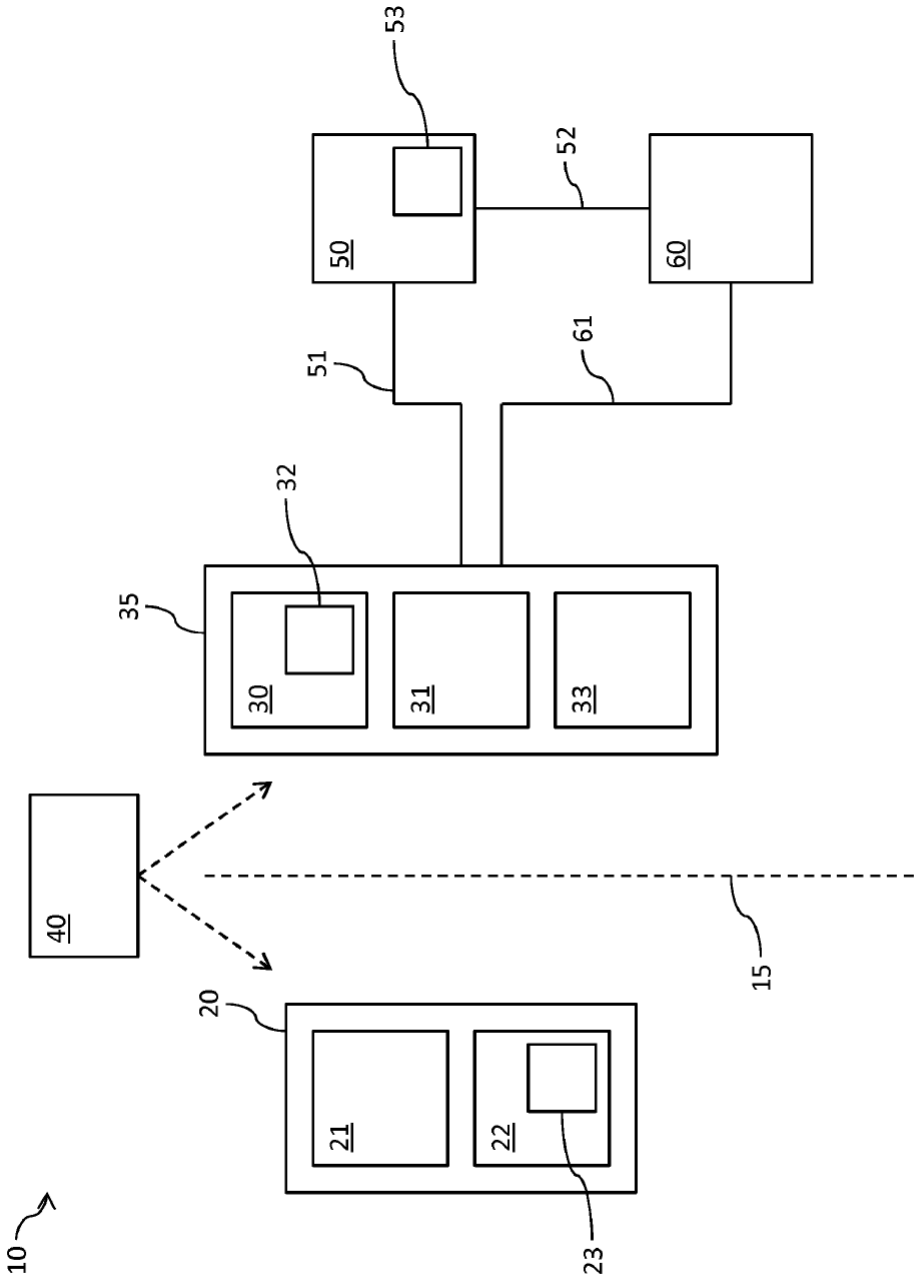

Fig 1

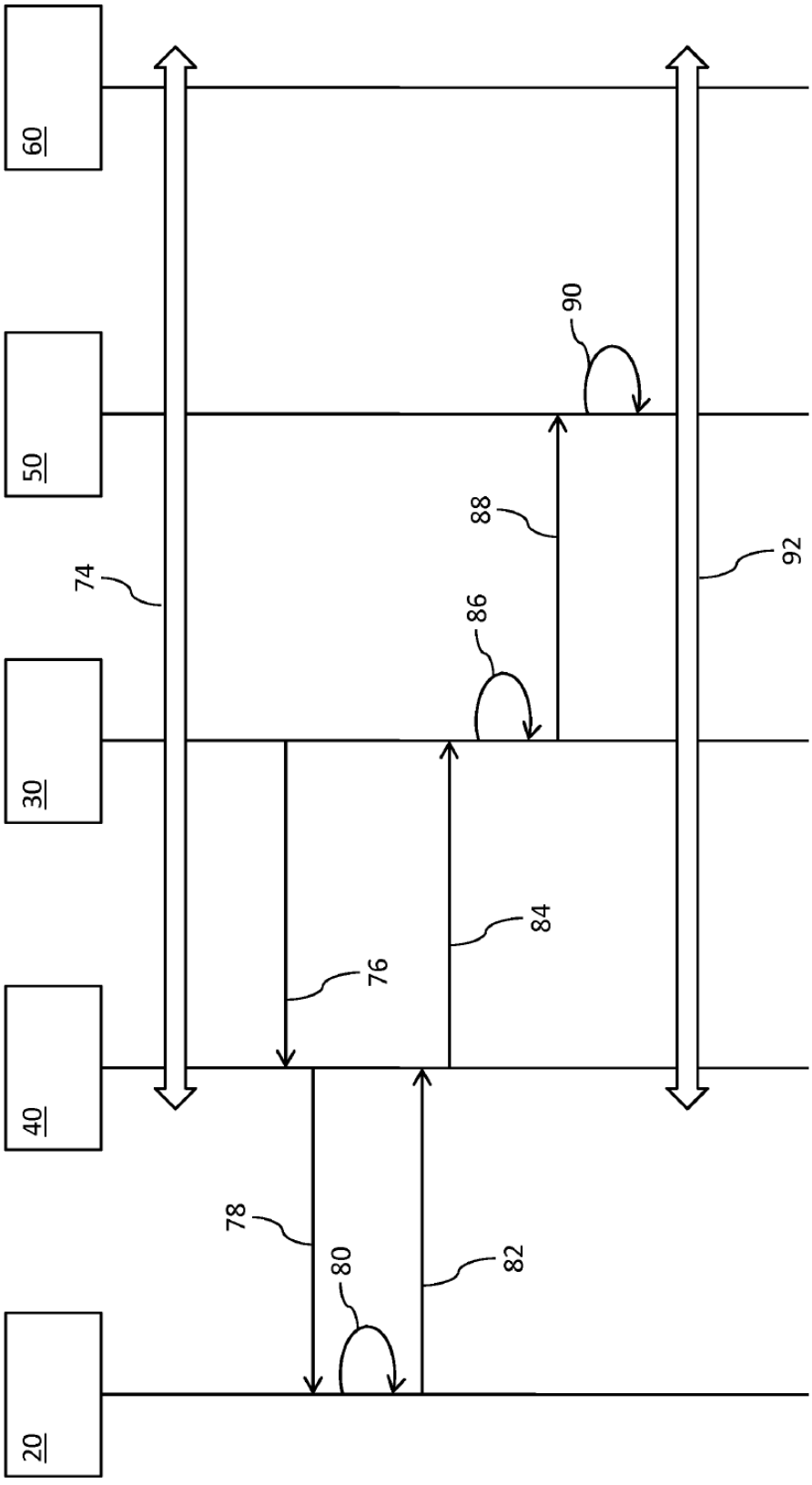

Fig 2

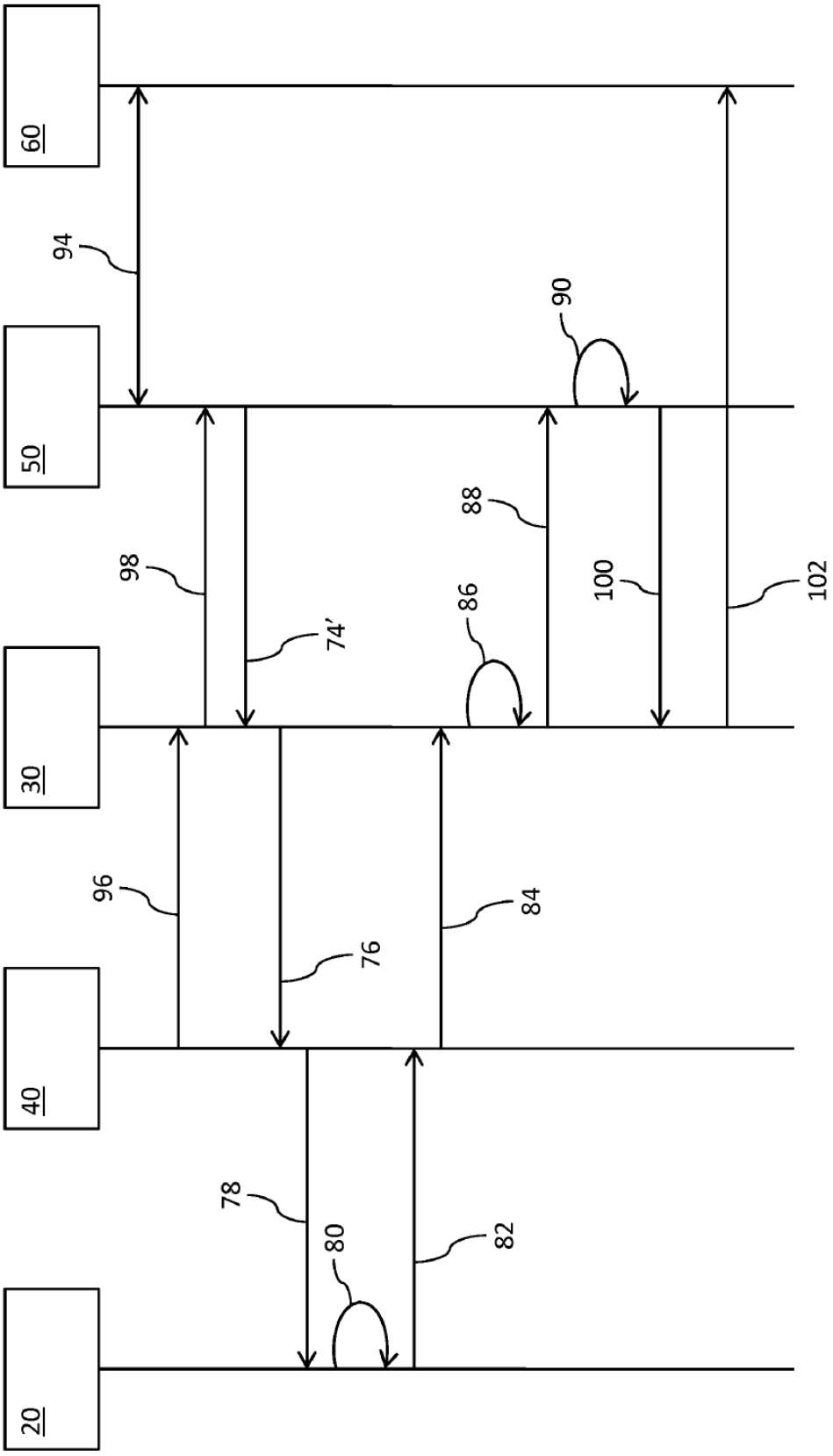

Fig 3