(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 807 213**

(51) Int. CI.:

***H04L 9/08*** (2006.01)
***H04L 9/32*** (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **21.06.2017 PCT/EP2017/065199**

(87) Fecha y número de publicación internacional: **28.12.2017 WO17220636**

(96) Fecha de presentación y número de la solicitud europea: **21.06.2017 E 17730225 (4)**

(97) Fecha y número de publicación de la concesión europea: **22.04.2020 EP 3476077**

(54) Título: **Dispositivo de generación de contraseñas y dispositivo de verificación de contraseñas**

(30) Prioridad:

**23.06.2016 NL 2017032**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
**22.02.2021**

(73) Titular/es:

**MINDYOURPASS HOLDING B.V. (100.0%)**
**Treublaan 10**
**5644 DD Eindhoven, NL**

(72) Inventor/es:

**DE JONGE, MERIJN**

(74) Agente/Representante:

**CONTRERAS PÉREZ, Yahel**

## DESCRIPCIÓN

Dispositivo de generación de contraseñas y dispositivo de verificación de contraseñas

CAMPO DE LA INVENCIÓN

La invención se refiere a un dispositivo de generación de contraseñas, un procedimiento de generación de contraseñas y un programa informático.

ANTECEDENTES

Los usuarios de dispositivos informáticos tienen que recordar muchas contraseñas para acceder a diversos recursos informáticos. Incluso los sitios web de información o noticias, promueven cada vez más que los usuarios se registren para obtener una 'cuenta' con la que acceder a servicios como noticias personalizadas, etc. Al mismo tiempo, muchas aplicaciones que antes se ejecutaban localmente están siendo sustituidas por versiones en línea, por ejemplo, procesamiento de textos, almacenamiento de archivos y similares.

Para hacer frente a la proliferación de contraseñas, los usuarios han adoptado diversas estrategias de actuación. Por ejemplo, algunos usuarios simplemente usan la misma contraseña para todas sus cuentas en línea. Este procedimiento tiene la ventaja de añadir sólo una pequeña carga en la memoria del usuario, y probablemente no requiere que el usuario almacene localmente su contraseña. Por otra parte, este procedimiento tiene la desventaja de que, una vez que su contraseña se ha visto comprometida, todas sus cuentas en línea están en peligro. El hecho de que la contraseña se vea comprometida, ni siquiera tiene que ser causado por un error de usuario, sino que se puede deber a, por ejemplo, un sitio web que ha sido pirateado en el que el usuario tiene una cuenta.

Otro enfoque es usar un administrador de contraseñas. Un administrador de contraseñas es una aplicación informática que ayuda al usuario a administrar su conjunto de contraseñas. Normalmente, almacena contraseñas, por ejemplo, localmente o en la nube, y las encripta con una contraseña maestra. La aplicación inicia sesión en cuentas en línea y sincroniza las contraseñas en diversos navegadores y dispositivos.

En la práctica, todavía hay diversas desventajas con estos administradores de contraseñas. Por ejemplo, un sitio web que se ha visto comprometido significa todavía que se han visto comprometidas muchas contraseñas. Aunque un administrador de contraseñas facilita el uso de diferentes contraseñas, no hay garantía de que una contraseña sea única localmente, y mucho menos de que las contraseñas sean únicas globalmente. Además, un pirateo del administrador de contraseñas implica que todas las contraseñas locales se ven comprometidas. No hay forma de invalidar rápidamente todas estas contraseñas.

Las contraseñas no sólo causan problemas a los usuarios, sino también a los recursos informáticos, por ejemplo, a los propios sitios web. En particular, un sitio web no puede valorar la calidad de una contraseña. Por ejemplo, un sitio web no puede determinar si una contraseña se ha utilizado también para otro sitio web.

El documento de patente US 6 006 333 muestra una unidad de generación de contraseñas que comprende una unidad de entrada para recibir procedente de un aparato de usuario una dirección informática, una identificación de usuario y una contraseña, en el que la unidad comprueba si una identificación de usuario ya está registrada.

RESUMEN DE LA INVENCIÓN

Se proporciona un dispositivo de generación de contraseñas, que aborda algunas de las preocupaciones mencionadas en este documento. El dispositivo de generación de contraseñas comprende

- una unidad de entrada dispuesta para recibir procedente de un dispositivo de usuario
  - una dirección informática para acceder a un recurso informático,
  - un identificador de usuario que indica un usuario del dispositivo de usuario, y
  - una contraseña de usuario,
- una unidad de direcciones informáticas dispuesta para mapear la dirección informática con una dirección base, de modo que se mapean diversas direcciones informáticas con la misma dirección base,
- un gestor de identificadores dispuesto para
  - determinar si la dirección base está registrada con el gestor de identificadores, y
- en caso de no ser así: asignar a la dirección base un identificador de sistema de dirección base único y almacenar la dirección base junto con el identificador de sistema de dirección base,
- en caso de ser así: obtener el identificador de sistema de dirección base,
  - determinar si el identificador de usuario está registrado con el gestor de identificadores, y
- en caso de no ser así: asignar un identificador de sistema de usuario único al identificador de usuario, y almacenar el identificador de usuario junto con el identificador de sistema de usuario,
- en caso de ser así: obtener el identificador de sistema de usuario, y
- una unidad de contraseñas dispuesta para
  - determinar un primer identificador combinado a partir del identificador de sistema de dirección base, el identificador de sistema de usuario y la contraseña de usuario.

La contraseña generada por el dispositivo de generación de contraseñas puede ser el primer identificador combinado o derivado a partir del mismo, por ejemplo, a través del cálculo de un segundo identificador combinado. Las contraseñas generadas por el dispositivo de generación de contraseñas tienen una serie de ventajas según se indica en el presente documento. Por ejemplo, cambiando los identificadores de sistema se pueden invalidar clases enteras de contraseñas.

Como ventaja, el sistema de generación de contraseñas puede ser ampliado determinando un segundo identificador combinado, que también permite una invalidación individual. Si es necesario, se puede satisfacer una restricción de contraseña impuesta por un sitio web, derivando una contraseña final a partir del segundo identificador combinado y/o del primer identificador combinado que satisfaga la restricción de contraseña.

Además, teniendo un sistema central de generación de contraseñas se pueden obtener mejoras en la seguridad global. Por ejemplo, en una forma de realización, el dispositivo de generación de contraseñas comprende una unidad de verificación dispuesta para determinar si una contraseña recibida por un sitio web ha sido generada por el sistema de generación de contraseñas y, en particular, si ha sido generada para ese sitio web.

La generación de contraseñas es un dispositivo electrónico, por ejemplo, un dispositivo informático tal como un servidor, o similar.

Un procedimiento según la invención se puede implementar en un dispositivo informático como un procedimiento implementado en dispositivo informático, o en hardware dedicado, o en una combinación de ambos. El código ejecutable para un procedimiento según la invención puede ser almacenado en un producto de programa informático. Ejemplos de productos de programa informático incluyen dispositivos de memoria, dispositivos de almacenamiento óptico, circuitos integrados, servidores, software en línea, etc. Preferiblemente, el producto de programa informático comprende un código de programa no transitorio almacenado en un medio legible por dispositivo informático para realizar un procedimiento según la invención cuando dicho producto de programa es ejecutado en un dispositivo informático.

En una forma de realización preferida, el programa informático comprende un código de programa informático adaptado para realizar todas las etapas de un procedimiento según la invención cuando el programa informático es ejecutado en un dispositivo informático. Preferiblemente, el programa informático está incorporado en un medio legible por dispositivo informático.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Se describirán más detalles, aspectos y formas de realización de la invención, sólo a modo de ejemplo, con referencia a los dibujos. Se ilustran elementos en las figuras para mayor simplicidad y claridad y no han sido necesariamente dibujados a escala. En las figuras, elementos que corresponden a elementos que ya se han descrito pueden tener los mismos números de referencia. En los dibujos,

La Figura 1a muestra de forma esquemática un ejemplo de una forma de realización de un dispositivo de generación de contraseñas,
La Figura 1b muestra de forma esquemática un ejemplo de una forma de realización de una unidad de contraseñas,
La Figura 2 muestra de forma esquemática un ejemplo de derivación de contraseña final,
La Figura 3 muestra de forma esquemática un ejemplo de una forma de realización de un dispositivo de generación de contraseñas,
La Figura 4 muestra de forma esquemática un ejemplo de una forma de realización de un procedimiento de generación de contraseñas,
La Figura 5a muestra de forma esquemática un medio legible por dispositivo informático que tiene una parte escribible que comprende un programa informático según una forma de realización,
La Figura 5b muestra de forma esquemática una forma de realización de un sistema procesador según una forma de realización.

Lista de números de referencia, en las Figuras 1a – 3:

100,101 un dispositivo de generación de contraseñas
110 una unidad de entrada
120 una unidad de direcciones informáticas
130 un gestor de identificadores
132 una base de datos
140 una unidad de contraseñas
142 una unidad de primer identificador combinado
144 una unidad de segundo identificador combinado
146 una unidad de corrección de contraseñas

148 una unidad de restricción de contraseñas
150 una unidad proveedora de inicio de sesión
160 una unidad de verificación
170 una unidad de tickets
200 un dispositivo de usuario
210 un navegador web
250 un primer proveedor de inicio de sesión
260 un segundo proveedor de inicio de sesión
310 una dirección informática
312 una dirección base
315 un sistema de identificación de dirección base
320 un identificador de usuario
325 un identificador de sistema de usuario único
330 una contraseña de usuario,
340 un primer identificador combinado
345 un primer identificador de sistema combinado
350 un segundo identificador combinado
355 una contraseña final

DESCRIPCIÓN DETALLADA DE FORMAS DE REALIZACIÓN PREFERIDAS

Si bien esta invención es susceptible de ser realizada en muchas formas diferentes, en los dibujos se muestran y se describirán en detalle una o más formas de realización específicas, entendiendo que la presente divulgación se debe considerar como un ejemplo de los principios de la invención y no tiene por objeto limitar la invención a las formas de realización específicas que se muestran y se describen.

A continuación, por motivos de comprensión, se describen elementos de formas de realización durante su operación. Sin embargo, será evidente que los respectivos elementos están dispuestos para realizar las funciones que se describen como realizadas por los mismos.

La Figura 1a muestra de forma esquemática un ejemplo de una forma de realización de un dispositivo de generación de contraseñas 100. En la siguiente descripción se hace referencia además a la Figura 2 que ilustra una posible relación entre algunos de los elementos de datos utilizados en una forma de realización de un dispositivo de generación de contraseñas.

El dispositivo de generación de contraseñas 100 se puede utilizar con un dispositivo de usuario 200. El dispositivo de generación de contraseñas 100 está dispuesto para generar una contraseña que puede ser utilizada para acceder a un recurso informático. El dispositivo de generación de contraseñas 100 ofrece muchas ventajas en este sentido. Por ejemplo, el dispositivo de generación de contraseñas 100 genera contraseñas más fuertes que las que suelen generar usuarios no asistidos, reduciendo así la probabilidad de que un atacante descubra la contraseña de un usuario. Además, todas las contraseñas de un usuario determinado o de un sitio web determinado pueden ser desactivadas rápidamente. Así pues, si un usuario o un sitio web se ve comprometido, las contraseñas que el atacante pueda haber obtenido se pueden deshabilitar fácilmente. Curiosamente, esta funcionalidad se puede implementar sin almacenar las propias contraseñas.

El dispositivo de generación de contraseñas 100 comprende una unidad de entrada 110 dispuesta para recibir una dirección informática 310 procedente del dispositivo de usuario 200, un identificador de usuario 320 que indica un usuario del dispositivo de usuario, y una contraseña de usuario 330. Por lo general, la contraseña de usuario es un valor hash de una contraseña de usuario original para evitar la transmisión de la contraseña de usuario original. Sin embargo, esto último no es necesario, por ejemplo, si la transmisión entre el dispositivo de usuario y el dispositivo de generación de contraseñas es segura.

Por ejemplo, la unidad de entrada 110 puede recibir la información a través de una red informática, por ejemplo, Internet, una LAN, una WAN, etc. La red informática puede ser total o parcialmente alámbrica o inalámbrica, etc.

En una forma de realización, el dispositivo de usuario 200 es un dispositivo informático que ejecuta un navegador web 210. La dirección informática 310 puede ser un URL (Uniform Resource Locator), por ejemplo, un primer URL denominado URL1. La dirección informática 310 puede ser usada para acceder a una página de inicio de sesión de una página web. Por ejemplo, el URL1 puede ser: https://myaccount.nytimes.com/auth/login.

En una forma de realización, el navegador web 210 está dispuesto para obtener la contraseña de usuario, el identificador de usuario y la dirección informática de la página web, por ejemplo, una página web en la que se detecta un campo de contraseña. El navegador web 210 está dispuesto para enviar la contraseña de usuario 330, el identificador de usuario 320 y la dirección informática 310 al dispositivo de generación de contraseñas 100, por ejemplo, a través de la red informática. Por ejemplo, la funcionalidad anterior se

puede implementar en el navegador web en forma de lo que se denomina un "plug-in". El navegador web 210 puede utilizar cualquier otro medio de comunicación que se desee, por ejemplo, el protocolo https para una mayor protección de la comunicación entre el navegador web 210 y el dispositivo de generación de contraseñas 100.

En una forma de realización, se impide que una contraseña de usuario original obtenida y/o almacenada en el dispositivo de usuario 200, por ejemplo, por el navegador web 210, sea enviada en claro al dispositivo de generación de contraseñas 100. Por ejemplo, el navegador web 210 puede recibir la contraseña de usuario directamente del usuario, por ejemplo, mediante escritura de la contraseña, pero en cambio el navegador web 210 puede recibir una contraseña de usuario original y aplicar una función hash a la contraseña original para obtener la contraseña de usuario. Las funciones hash son preferiblemente funciones hash unidireccionales, en particular, funciones hash criptográficas. Ejemplos de funciones hash criptográficas incluyen la suite SHA-2. Una salida de hash puede ser truncada si se desea, por ejemplo, a 64 bits o más, etc. El navegador web 210 está dispuesto para enviar la contraseña de usuario, la dirección informática y el identificador de usuario al dispositivo de generación de contraseñas 100, pero no la contraseña original.

En una forma de realización, el dispositivo de usuario 200, por ejemplo, el navegador web 210, recibe una contraseña final procedente del dispositivo de generación de contraseñas. El dispositivo de usuario 200 puede entonces utilizar la contraseña final para acceder al recurso informático. Por ejemplo, el navegador web 210 puede introducir la contraseña final en el campo de contraseña. El dispositivo de usuario 200, por ejemplo, el navegador web 210, envía entonces la contraseña al recurso informático para obtener acceso. La comunicación de contraseñas puede ser encriptada, por ejemplo, utilizando https. A continuación se presenta una forma de realización en la que la contraseña no pasa por el dispositivo de usuario 200, sino que se comunica directamente entre el dispositivo de generación de contraseñas 100 y el recurso informático, por ejemplo, utilizando tickets.

No es necesario que el dispositivo de generación de contraseñas 100 sea un dispositivo informático externo conectado con el dispositivo de usuario 200 a través de una red informática. Por ejemplo, el dispositivo de generación de contraseñas 100 puede estar comprendido en el dispositivo de usuario 200. El recurso informático puede ser un recurso accesible por el dispositivo de usuario 200 a través de la red informática, por ejemplo, un servicio web, por ejemplo, un servicio bancario, un editor en línea, un servicio de noticias, un sitio de redes sociales y similares. El recurso informático puede ser también un recurso accesible localmente en el dispositivo de usuario 200; por ejemplo, una aplicación informática protegida por una contraseña. Para explicar la invención, se asumirá a continuación que el dispositivo de generación de contraseñas 100 es un dispositivo externo al dispositivo de usuario 200, con la condición de que no es necesario.

En una forma de realización, el dispositivo de usuario 200 tiene acceso a múltiples recursos informáticos, por ejemplo, múltiples sitios web o múltiples aplicaciones locales, o una combinación de los mismos. Un recurso diferente con una dirección informática diferente, por ejemplo, un URL diferente, suele hacer que el dispositivo de generación de contraseñas 100 calcule una contraseña diferente.

En una forma de realización, el identificador de usuario puede identificar el usuario y/o el dispositivo de usuario 200 en el dispositivo de generación de contraseñas 100. Por ejemplo, el identificador de usuario puede ser único para todos los usuarios del dispositivo de generación de contraseñas 100. Alternativamente, el identificador de usuario puede ser un identificador de usuario utilizado para identificar al usuario con el recurso informático. En este caso, el dispositivo de generación de contraseñas 100 puede estar dispuesto de modo que la combinación de la dirección base y el identificador de usuario sea única, por ejemplo, única para el dispositivo de generación de contraseñas 100.

A continuación se supondrá que el mismo usuario utilizará el mismo identificador de usuario, o un número limitado de identificadores de usuario, para acceder a un mayor número de recursos informáticos. El dispositivo de generación de contraseñas 100 puede estar dispuesto para identificar al usuario en base al identificador de usuario.

En una forma de realización, el dispositivo de generación de contraseñas 100 almacena una lista de identificadores de usuario 320 de usuarios registrados. El dispositivo de generación de contraseñas 100 también puede almacenar una lista de identificadores de dispositivo de los dispositivos de usuario registrados. Por ejemplo, las listas se pueden almacenar, por ejemplo, en un archivo informático, en una base de datos, en la nube, etc. La unidad de entrada 110 puede estar dispuesta para recibir un identificador de dispositivo de usuario, además del identificador de usuario. La unidad de entrada 200 puede estar dispuesta para rechazar generar una contraseña si el identificador de dispositivo de usuario recibido no está registrado o está bloqueado. Asimismo, el dispositivo de usuario 200 puede estar dispuesto para rechazar generar una contraseña si el identificador de usuario recibido no está registrado o está bloqueado. Por ejemplo, el dispositivo de usuario 200 puede almacenar una lista blanca, con identificadores de usuario y/o de dispositivo aceptados. Por ejemplo, el dispositivo de usuario 200 puede almacenar una lista negra, con identificadores de usuario y/o de dispositivo bloqueados. También es posible una combinación de listas

blancas y negras. Por ejemplo, se puede utilizar una dirección MAC o una dirección IP del dispositivo de usuario 200 como identificador del dispositivo de usuario.

En una forma de realización, la contraseña de usuario comprende unos atributos asociados con el usuario o con el dispositivo de usuario, por ejemplo, un identificador biométrico obtenido a partir de un sensor biométrico. Por ejemplo, el dispositivo de usuario 200 puede comprender un sensor biométrico dispuesto para producir un identificador reproducible. Los sensores biométricos incluyen sensores de huellas dactilares y sensores biométricos faciales, por ejemplo, dispuestos para mapear una huella dactilar o un rostro con un identificador. Los atributos asociados con un dispositivo de usuario pueden incluir, por ejemplo, un perfil de dispositivo, números de serie de dispositivo y similares. Los atributos asociados con un usuario pueden incluir una contraseña, una identificación biométrica, una autenticación de dos factores y similares.

El dispositivo de generación de contraseñas 100 comprende además una unidad de direcciones informáticas 120 dispuesta para mapear la dirección informática con una dirección base 312, de modo que se mapean múltiples direcciones informáticas con la misma dirección base. Esto puede provocar que el mismo recurso informático sea accesible bajo diferentes direcciones informáticas. Por ejemplo, si una primera dirección informática (URL1) es https://myaccount.nytimes.com/auth/login, una segunda dirección informática (URL2) es https://nytimes.com/auth/login, una tercera dirección informática (URL3) es https://nytimes.com/login, entonces todas estas tres direcciones informáticas proporcionan acceso al mismo recurso informático, por ejemplo, un sitio web; en este caso, una página de inicio de sesión para acceder a un sitio web de noticias. Aunque las dos direcciones informáticas son diferentes, aceptan las mismas credenciales de inicio de sesión. La unidad de direcciones informáticas 120 mapea diferentes direcciones informáticas con una dirección base común, de modo que se generará la misma contraseña para las mismas direcciones informáticas. En una forma de realización, la unidad de direcciones informáticas 120 está dispuesta para seleccionar uno o más elementos de la dirección informática como dirección base. Por ejemplo, la unidad de direcciones informáticas 120 puede seleccionar el nombre de dominio de un URL como la dirección base. En el ejemplo anterior, la unidad de direcciones informáticas 120 puede estar dispuesta para adoptar nytimes.com como dirección base.

Por otra parte, en una forma de realización, la unidad de direcciones informáticas 120 puede estar dispuesta para eliminar uno o más elementos de la dirección informática para obtener la dirección base. Por ejemplo, la unidad de direcciones informáticas 120 puede eliminar una parte seleccionada de la dirección informática para obtener la dirección base. Por ejemplo, la unidad de direcciones informáticas puede eliminar un indicador de protocolo (por ejemplo, https en el ejemplo anterior), y/o eliminar partes comunes, tales como www, etc. Por ejemplo, con este último procedimiento se puede disponer que el URL1 y el URL2 sigan apuntando a la misma dirección base, por ejemplo, nytimes.com/auth/login, pero no el URL3.

El dispositivo de generación de contraseñas 100 comprende además un gestor de identificadores 130. El gestor de identificadores 130 está dispuesto para mapear diversos elementos de datos con identificadores de sistema. Por ejemplo, un elemento de datos se puede registrar con el gestor de identificadores 130 para obtener un identificador de sistema. Si el elemento de datos no se ha registrado anteriormente, se asigna un nuevo identificador de sistema. Si el elemento de datos se ha registrado anteriormente, se recupera un nuevo identificador de sistema. Los identificadores de sistema son preferiblemente únicos, por ejemplo, únicos dentro de los elementos de datos de un tipo particular registrados en el sistema, o únicos dentro de todos los identificadores asignados por el gestor de identificadores 130. Esto se puede conseguir utilizando un número de serie, un sello de tiempo, posiblemente modificado por una función resistente a colisiones, por ejemplo, encriptado o codificado con una función hash, etc. Un requisito más estricto es que los identificadores de sistema sean globalmente únicos. Esto último se puede conseguir asignando un número aleatorio de longitud suficiente; por ejemplo, un número aleatorio de 80 bits, 128 bits, etc. Una longitud suficiente se puede calcular estimando el número máximo de identificadores de sistema utilizados globalmente durante la vida útil del sistema. Se espera que los identificadores de sistema aleatorios sean suficientes para que sean únicos globalmente. Por ejemplo, los identificadores de sistema pueden ser los denominados "identificadores globalmente únicos", también conocidos como GUID. Un generador de números aleatorios puede estar incluido en el sistema de generación de contraseñas 100.

En una forma de realización, el gestor de identificadores 130 se utiliza para obtener un identificador de sistema para la dirección base y para el identificador de usuario.

Por ejemplo, el gestor de identificadores 130 está dispuesto para determinar si la dirección base está registrada con el gestor de identificadores, y
- en caso de no ser así: asignar a la dirección base un identificador de sistema de dirección base único 315, y almacenar la dirección base junto con el identificador de sistema de dirección base,
- en caso de ser así: obtener el identificador de sistema de dirección base 315.

Por ejemplo, el gestor de identificadores 130 está dispuesto para determinar si el identificador de usuario recibido está registrado con el gestor de identificadores, y

- en caso de no ser así: asignar un identificador de sistema de usuario único 325 al identificador de usuario, y almacenar el identificador de usuario junto con el identificador de sistema de usuario,
- en caso de ser así: obtener el identificador de sistema de usuario 325.

El dispositivo de generación de contraseñas 100 comprende una unidad de contraseñas 140. La unidad de contraseñas 140 está dispuesta para calcular la contraseña. La unidad de contraseñas 140 está dispuesta para determinar un primer identificador combinado 340 a partir del identificador de sistema de dirección base, el identificador de sistema de usuario y la contraseña de usuario recibida. Por ejemplo, la unidad de contraseñas 140 puede estar dispuesta con una función de primer identificador combinado, que la unidad de contraseñas 140 aplica al identificador de sistema de dirección básica, al identificador de sistema de usuario y a la contraseña de usuario. La función es preferiblemente resistente a colisiones y unidireccional. Por ejemplo, la función puede comprender una función hash criptográfica. Se puede calcular una contraseña final directamente a partir del primer identificador combinado 340, por ejemplo, por parte de una unidad de restricción de contraseñas 148 (que se explica posteriormente). El primer identificador combinado 340 también se puede utilizar directamente como contraseña. Téngase en cuenta que, en general, los números se pueden expresar como una cadena de bits, cadenas de caracteres, etc., según se desee. La restricción de contraseña puede incluir unos límites en el número de caracteres, el número de letras, el número de dígitos, el número de signos de puntuación, etc.

A causa de que la contraseña está compuesta por diversos elementos, los elementos individuales no necesitan ser tan fuertes. Por ejemplo, se puede generar una contraseña segura mientras que el usuario sólo necesita recordar una contraseña relativamente fácil. Además, puede incluso reutilizar esta contraseña para todos los recursos informáticos, por ejemplo, para todas sus cuentas. Descubrir una contraseña es difícil para un atacante, ya que no tiene acceso a los identificadores de sistema.

Derivar una contraseña final a partir del primer identificador combinado 340, por ejemplo, según se ha divulgado anteriormente, o a través de un segundo identificador combinado, según se muestra a continuación, tiene una serie de ventajas. Todas las contraseñas para un determinado recurso informático, por ejemplo, un determinado sitio web, por ejemplo, nytimes.com, se pueden restablecer conjuntamente cambiando el identificador de sistema de dirección base. De modo similar, todas las contraseñas de un usuario particular se pueden restablecer conjuntamente cambiando el identificador de sistema de usuario. En una forma de realización, el administrador de identificadores está dispuesto para cambiar el identificador de sistema de dirección base, renovando de este modo todas las contraseñas para el recurso informático, y/o cambiar el identificador de sistema de usuario, renovando de este modo todas las contraseñas para el identificador de usuario. Por ejemplo, el dispositivo de generación de contraseñas 100 puede comprender una interfaz de gestor de identificadores para efectuar dichos cambios. La interfaz de gestor de identificadores está preferiblemente protegida. Por ejemplo, la interfaz de gestor de identificadores puede estar protegida por una contraseña, ser accesible sólo localmente (no a través de una red informática), etc.

Por ejemplo, una vez que un sitio se ha visto comprometido, todas las contraseñas de ese sitio pueden ser invalidadas al mismo tiempo. Como el primer identificador combinado 340 se calcula utilizando una función resistente a colisiones, no es probable que el dispositivo de generación de contraseñas 100 vuelva a generar una contraseña invalidada.

Téngase en cuenta que para cambiar todas las contraseñas para un determinado recurso y/o para un determinado usuario no es necesario cambiar ninguno de los componentes recibidos (por ejemplo, el identificador de usuario, la dirección informática y la contraseña de usuario). Esto permite invalidar las contraseñas sin afectar al usuario.

En una forma de realización, el gestor de identificadores 130 se utiliza también para que el primer identificador combinado 340 obtenga un primer identificador de sistema combinado 345. Por ejemplo, el gestor de identificadores 130 puede estar dispuesto para determinar si el primer identificador combinado 340 está registrado con el gestor de identificadores, y
- en caso de no ser así: asignar un primer identificador de sistema combinado único 345 al primer identificador combinado 340, y almacenar el primer identificador combinado 340 junto con el primer identificador de sistema combinado 345,
- en caso de ser así: obtener el primer identificador de sistema combinado 345 asignado al primer identificador combinado 340.

La unidad de contraseñas 140 está dispuesta además para determinar un segundo identificador combinado 350 a partir de al menos el primer identificador de sistema combinado 345. La unidad de contraseñas 140 puede utilizar entradas adicionales para determinar el segundo identificador combinado 350. En una forma de realización, la unidad de contraseñas 140 utiliza uno o más de entre el identificador de usuario, la dirección base y la contraseña de usuario como entrada adicional. Por ejemplo, la unidad de contraseñas 140 puede estar dispuesta con una función de segundo identificador combinado, que la unidad de contraseñas 140 aplica a sus entradas. La función de segundo identificador combinado puede tener los mismos requisitos que la función de primer identificador combinado. Por ejemplo, las dos funciones pueden

ser las mismas. Por ejemplo, la función de segundo identificador combinado puede comprender una función hash criptográfica. En una forma de realización, la función de segundo identificador combinado recibe como entrada al menos el primer identificador de sistema combinado 345 y la contraseña de usuario. En una forma de realización, la unidad de contraseñas 140 puede utilizar como entrada adicional el primer identificador combinado 340, posiblemente además de las entradas anteriores, tal como la contraseña de usuario.

En una forma de realización, almacenar el primer identificador combinado 340, si aún no se ha registrado ninguno, se realiza almacenando el valor hash del primer identificador combinado 340. Esto mejora la seguridad en caso de que la base de datos se vea comprometida. Por ejemplo, el gestor de identificadores 130 puede estar dispuesto para determinar si el primer identificador combinado 340 está registrado con el gestor de identificadores, calculando un valor hash del primer identificador combinado 340 y utilizando el valor hash como clave para encontrar el primer identificador de sistema combinado 345 en un almacenamiento, por ejemplo, un almacenamiento local, una base de datos 132, un almacenamiento en la nube, etc. Si el valor hash del primer identificador combinado 340 no se encuentra como clave, por ejemplo, no se ha asignado previamente el correspondiente primer identificador de sistema combinado 345, entonces se asigna un primer identificador de sistema combinado único 345 al primer identificador combinado 340. En este caso, el primer identificador de sistema combinado 345 se puede almacenar en el almacenamiento asociado con el valor hash del primer identificador combinado 340 como clave. Una clave también se denomina a veces clave de base de datos. En lugar de una base de datos, también se puede utilizar una matriz asociativa para almacenar pares de claves, valores. Por ejemplo, se pueden almacenar pares (h(x), y) en los que x es el primer identificador combinado 340, y es el primer identificador de sistema combinado 345, y h es una función hash (posiblemente salada).

El cálculo de la contraseña en etapas que utilizan entradas de usuario e identificadores de sistema recibidos tiene el efecto de que las contraseñas pueden ser canceladas de manera más selectiva. En una forma de realización, el gestor de identificadores 130 está dispuesto para cambiar el primer identificador de sistema combinado 345, renovando de este modo el segundo identificador combinado 350 y/o la contraseña final para el identificador de usuario y el recurso informático. Esto permite cambiar únicamente la contraseña para un recurso informático determinado, sin restablecer todas las contraseñas para ese usuario o para ese recurso informático.

En una forma de realización, el dispositivo de generación de contraseñas 100 comprende una unidad de restricción de contraseñas 148. La unidad de restricción de contraseñas 148 está dispuesta para obtener, por ejemplo, recuperar, restricciones de contraseña para el recurso informático. Por ejemplo, las restricciones de contraseña se pueden recuperar de un almacenamiento local, por ejemplo, de una base de datos 132, o se pueden recuperar del recurso informático, etc.

La unidad de restricción de contraseñas 148 determina una contraseña final a partir del segundo identificador combinado 350 (o a partir del primer identificador combinado 340 si no se utiliza un segundo identificador combinado) que satisfaga las restricciones de contraseña. Por ejemplo, el segundo identificador combinado 350 puede ser una cadena de 512 bits, por ejemplo, como la salida de una función hash. Una restricción de contraseña puede ser la longitud de la contraseña. La restricción de contraseña puede ser que se utilice un máximo de 8 caracteres alfanuméricos en la contraseña. Esta restricción se puede recuperar y se puede generar una contraseña que cumpla esta condición. Por ejemplo, el segundo identificador combinado 350 puede ser mapeado con un número en base 62 (26 + 26 + 10) que a su vez es mapeado con una cadena alfanumérica. La cadena puede entonces ser truncada a 8 caracteres. Se pueden adoptar muchas restricciones de esta manera. Se observa que en lugar de una unidad de restricción, el recurso informático puede estar adaptado para aceptar una cadena de bits directamente como contraseña, por ejemplo, una cadena de 512 bits. Otra restricción puede ser que la contraseña final contenga al menos un dígito. Esto se puede conseguir seleccionando primero un dígito y una posición, en base al segundo identificador combinado 350, y luego llenando las posiciones restantes en base al segundo identificador combinado 350. Lo mismo se puede utilizar para letras, puntuaciones, etc. prescritas.

La satisfacción de la restricción adicional de que la contraseña final contenga al menos un dígito también se puede conseguir seleccionando primero un carácter del segundo identificador combinado 350 en base a la frecuencia con la que este carácter aparece en el identificador y sustituyéndolo luego por un dígito. El carácter seleccionado determina qué dígito se elige, por ejemplo, utilizando una función de módulo. Este procedimiento se puede utilizar para cumplir con todas las letras, puntuaciones, etc. prescritas, y se puede repetir en caso de que se requiera más de un dígito, etc.

En la forma de realización, que se muestra en la Figura 1a, el gestor de identificadores 130 utiliza una base de datos 132. Por ejemplo, el gestor de identificadores 130 puede almacenar en la base de datos 132 registros que contienen un elemento de datos y un identificador de sistema, y posiblemente otra información tal como un tipo de datos. Los tipos de datos pueden incluir, por ejemplo, una dirección base y un identificador de usuario, etc. En una forma de realización, la base de datos 132 utiliza una o más matrices asociativas, que asocian un elemento de datos con un identificador de sistema. Por ejemplo, la base de

datos 132 puede comprender una matriz asociativa para direcciones base, para identificadores de usuario, etc.

La Figura 1b muestra de forma esquemática un ejemplo de una forma de realización de una unidad de contraseñas 140.

La unidad de contraseñas 140 comprende una unidad de primer identificador combinado 142 dispuesta para recibir una entrada procedente de la unidad de entrada 110, por ejemplo, la contraseña de usuario 330, y procedente del gestor de identificadores 130, por ejemplo, el identificador de sistema de dirección base 315 y el identificador de sistema de usuario 325. La unidad de primer identificador combinado 142 puede estar dispuesto para aplicar una función de primer identificador combinado. La unidad de contraseñas 140 comprende además una unidad de segundo identificador combinado 144. La unidad de segundo identificador combinado 144 está dispuesta para recibir una entrada procedente del gestor de identificadores 130, por ejemplo, el primer identificador de sistema combinado 345. La unidad de segundo identificador combinado 144 puede recibir entradas adicionales, por ejemplo, el primer identificador combinado 340, o entradas procedentes de la unidad de entrada 110, por ejemplo, la contraseña de usuario, etc. La unidad de contraseñas 140 puede comprender además una unidad de restricción de contraseñas 148 para calcular una contraseña final que satisfaga las restricciones impuestas por el recurso informático.

En una forma de realización, el dispositivo de generación de contraseñas 100 puede estar dispuesto para almacenar un factor de corrección para contraseña. La unidad de contraseñas 140 puede comprender una unidad de corrección de contraseñas 146 dispuesta entre la unidad de segundo identificador combinado 144 y la unidad de restricción de contraseñas 148, y dispuesta para aplicar el factor de corrección para contraseña al segundo identificador combinado 350 para mapearlo con un segundo identificador combinado adicional generado previamente para un identificador de usuario diferente. Por ejemplo, el factor de corrección para contraseña se puede almacenar en la base de datos 132, por ejemplo, junto con el segundo identificador de sistema combinado, etc. A partir del factor de corrección no es posible determinar identificador combinado alguno.

La unidad de corrección de contraseñas 146 permite a dos usuarios diferentes compartir una cuenta de forma segura. No es raro que usuarios compartan sus contraseñas, por ejemplo, para utilizar conjuntamente la misma cuenta. Si los dos usuarios tienen un identificador de usuario diferente, el sistema, según se ha descrito anteriormente, calculará una contraseña diferente para los dos usuarios. Por ejemplo, si un primer usuario tiene un primer segundo identificador combinado calculado para éste, mientras que un segundo usuario tiene un segundo segundo identificador combinado calculado para éste. Almacenando, por ejemplo, la diferencia entre el primer segundo identificador combinado y el segundo segundo identificador combinado como factor de corrección, la unidad de corrección de contraseñas 146 puede mapear, por ejemplo, el segundo segundo identificador combinado con el primer segundo identificador combinado. Eliminando el factor de corrección se elimina el vínculo entre las cuentas. La diferencia se puede calcular de diversas maneras, por ejemplo, como una diferencia aritmética, un XOR, etc.

La unidad de corrección de contraseñas 146 también se puede utilizar para hacer que una contraseña siga siendo la misma aunque, por ejemplo, cambie la dirección base de un recurso informático, el identificador de usuario o la contraseña de usuario.

La Figura 2 muestra de forma esquemática un ejemplo de derivar una contraseña final. En la Figura 2 se muestran una dirección informática 310, un identificador de usuario 320 y una contraseña de usuario 330. Éstas se pueden recibir, por ejemplo, procedentes del dispositivo de usuario 200.

La dirección informática 310 es mapeada con la dirección base 312, que a su vez es mapeada con un identificador de sistema de dirección base único 315. El identificador de usuario 320 es mapeado con un identificador de sistema de usuario único 325. Los tres elementos de datos: el identificador de sistema de dirección base 315, el identificador de sistema de usuario 325 y la contraseña de usuario 330 son mapeados con un primer identificador combinado 340. El primer identificador combinado 340 es mapeado con un primer identificador de sistema combinado 345. Téngase en cuenta que cambiando cualquiera de los mapeos de los identificadores de sistema se puede invalidar la contraseña o contraseñas correspondientes.

El primer identificador de sistema combinado 345 es mapeado con el segundo identificador combinado 350 posiblemente junto con otra entrada. Por ejemplo, la Figura 2 muestra que también se utiliza la contraseña de usuario 330 en este mapeo. Finalmente, el segundo identificador combinado 350 es mapeado con una contraseña final 355 que satisface las restricciones de contraseña.

La Figura 3 muestra de forma esquemática un ejemplo de una forma de realización de un dispositivo de generación de contraseñas 101. El dispositivo de generación de contraseñas 101 es una mejora del dispositivo de generación de contraseñas 100 y comprende una serie de características opcionales adicionales.

El dispositivo de generación de contraseñas 101 comprende una unidad proveedora de inicio de sesión 150 dispuesta para interactuar entre un primer proveedor de inicio de sesión 250 y un dispositivo de usuario 200. El primer proveedor de inicio de sesión 250 está dispuesto para proporcionar un primer identificador de usuario original. Por ejemplo, el primer proveedor de inicio de sesión puede ser un proveedor de inicio de sesión como Google, Facebook, LinkedIn, etc., por ejemplo, que utiliza el protocolo OpenID Connect. La unidad proveedora de inicio de sesión 150 está dispuesta para obtener el identificador de usuario a partir del primer identificador de usuario original y enviarlo al dispositivo de usuario. Por ejemplo, la unidad proveedora de inicio de sesión 150 puede aplicar una función de identificador de usuario al identificador de usuario original. La función de identificador de usuario puede comprender una función hash, por ejemplo, un hash criptográfico.

El uso del protocolo OpenID Connect puede operar de la siguiente manera. Primero el usuario intenta acceder a (o iniciar sesión en) la unidad proveedora de inicio de sesión 150. Si no hay ningún inicio de sesión anterior que siga siendo válido, la unidad proveedora de inicio de sesión (o de acceso) 150 redirige el intento de inicio de sesión al primer proveedor de inicio de sesión 250. En el proveedor de inicio de sesión 250, por ejemplo, Google, el usuario inicia sesión con sus credenciales de inicio de sesión habituales. A continuación, es redirigido de nuevo a la unidad proveedora de inicio de sesión 150. En la unidad proveedora de inicio de sesión 150, se recibe un identificador de usuario original, según lo ha proporcionado el proveedor de inicio de sesión 250. El identificador de usuario se obtiene a partir del identificador de usuario original. Por ejemplo, este mapeo puede ser una función, por ejemplo, que utiliza un hash, pero también puede utilizar el gestor de identificadores 130. El identificador de usuario se envía entonces al dispositivo de usuario 200. En consecuencia, el dispositivo de usuario 200 utiliza el identificador de usuario para obtener contraseñas procedentes del dispositivo de generación de contraseñas 101.

Nótese que, si ningún acceso (o inicio de sesión) anterior es todavía válido, la unidad proveedora de inicio de sesión 150 también puede redirigir el usuario a un menú en el que puede elegir un proveedor de inicio de sesión. Después de que el usuario haya seleccionado, la unidad proveedora de inicio de sesión 150 redirige el usuario al proveedor de inicio de sesión seleccionado.

Utilizando el estándar OpenID Connect se obtiene un identificador de usuario sin que se requiera el dispositivo de generación de contraseñas 101 para almacenar cuentas y credenciales de usuario. En efecto, un usuario no necesita crear una cuenta en el dispositivo de generación de contraseñas 101. El protocolo OpenID Connect permite utilizar la infraestructura de esos denominados proveedores de inicio de sesión para autenticar a un usuario. Al dispositivo de generación de contraseñas 101 se le proporciona un identificador de usuario único del proveedor de inicio de sesión que entonces se utiliza en forma de valor hash o en forma encriptada, etc., como uno de los tres componentes, por ejemplo, el identificador de usuario 320, de la contraseña generada. Así pues, no es necesario almacenar la contraseña de usuario, ni el identificador de usuario original proporcionado por el proveedor de inicio de sesión 250.

Este procedimiento aumenta la confianza del usuario, porque no necesita confiar al dispositivo de generación de contraseñas 101 el almacenamiento de una contraseña o de un identificador de usuario original. Además, se pueden utilizar diversos proveedores de inicio de sesión y el usuario puede elegir el que quiere utilizar. En la actualidad, por ejemplo, Google, Facebook, LinkedIn y Microsoft ofrecen servicios de inicio de sesión que se pueden utilizar con el dispositivo de generación de contraseñas 101. El dispositivo de generación de contraseñas 101 puede, por lo tanto, estar incluido en la infraestructura de seguridad del proveedor de inicio de sesión. Por ejemplo, la autenticación de dos factores proporcionada por Google, por ejemplo, está disponible para el dispositivo de generación de contraseñas 101. Los múltiples proveedores de inicio de sesión se pueden conectar a través de un protocolo de inicio de sesión adecuado, por ejemplo, el protocolo OpenID Connect.

En una forma de realización, la unidad proveedora de inicio de sesión 150 está dispuesta para trabajar con múltiples proveedores de inicio de sesión, por ejemplo, el primer proveedor de inicio de sesión 250 y el segundo proveedor de inicio de sesión 260. Por ejemplo, si un usuario inicia sesión (o accede) utilizando el segundo proveedor de inicio de sesión 260, el dispositivo de generación de contraseñas 101 recibirá un identificador de usuario original adicional. Si a este segundo identificador de usuario original se le aplicara una función hash para producir un identificador de usuario adicional, entonces todas las contraseñas de ese usuario serían diferentes. En una forma de realización, el gestor de identificadores 130 está dispuesto para almacenar un factor de corrección para identificador de usuario, que el dispositivo de generación de contraseñas 101 aplica al identificador de usuario adicional para mapearlo con el identificador de usuario, por ejemplo, en la unidad de entrada, la unidad de generación de contraseñas, etc. Al igual que el factor de corrección para contraseña, el factor de corrección para identificador de usuario puede ser una diferencia entre el identificador de usuario adicional y el identificador de usuario. Al igual que con el factor de corrección para contraseña, no es posible determinar ninguno de los identificadores de usuario a partir del factor de corrección.

Un efecto del factor de corrección para identificador de usuario es que un usuario no necesita mantener un registro de qué proveedor de inicio de sesión ha utilizado para qué sitios. Además, un usuario puede utilizar

un proveedor de inicio de sesión de su elección, aunque el recurso informático no admita un proveedor de inicio de sesión determinado. Basta con que el dispositivo de generación de contraseñas 101 admita un proveedor de inicio de sesión determinado. De esta manera, muchos proveedores de inicio de sesión pueden ser admitidos por los sitios web a través del dispositivo de generación de contraseñas 101, aunque los mismos sólo admitan inicios de sesión con contraseñas simples. Por ejemplo, el sitio web A puede admitir el proveedor de inicio de sesión 250 además del inicio de sesión manual con una contraseña, y el sitio web B puede admitir el proveedor de inicio de sesión 260 además del inicio de sesión manual con una contraseña. Sin embargo, el proveedor de inicio de sesión 150 puede admitir tanto el proveedor de inicio de sesión 250 como el proveedor de inicio de sesión 260. Esto significa que un usuario puede iniciar sesión con el proveedor de inicio de sesión 250 o 260 según lo desee, recibir un identificador de usuario (original) y recibir una contraseña para el sitio web A o el sitio web B. Además, utilizando un factor de corrección, el usuario obtendrá la misma contraseña con independencia de que el inicio de sesión se realice con el proveedor de inicio de sesión 250 o 260. Esto significa que un usuario puede utilizar el proveedor de inicio de sesión 260 aunque utilice el sitio web A, o el proveedor de inicio de sesión 250 aunque utilice el sitio web B. En ambos casos se utiliza la opción de inicio de sesión manual de los sitios web A y B para introducir la contraseña generada por el dispositivo de generación de contraseñas. Así pues, el dispositivo de generación de contraseñas 101 actúa como un intermediario entre el recurso informático, por ejemplo, el sitio web, y el usuario. Un usuario sólo tiene que dar permiso al dispositivo de generación de contraseñas 101 para iniciar la sesión a través del proveedor de inicio de sesión.

En una forma de realización, el gestor de identificadores 130 está dispuesto para almacenar un valor hash de una contraseña generada, opcionalmente salada con una sal aleatoria. Este valor hash se denomina en este documento la firma de la contraseña generada. La firma sirve como clave para almacenar información adicional sobre la contraseña generada. Esto puede incluir la correspondiente dirección informática o la dirección base, las restricciones de contraseña aplicadas, etc. En consecuencia, tener la contraseña generada o un valor hash de la misma permite encontrar la información asociada y, por ejemplo, permite verificar si la correspondiente dirección informática o la dirección base es correcta.

Por ejemplo, en una forma de realización, el dispositivo de generación de contraseñas 101 puede comprender una unidad de verificación 160. La unidad de verificación 160 comprende una interfaz dispuesta para recibir una contraseña y, opcionalmente, una dirección informática. La unidad de verificación 160 está dispuesta para determinar si la contraseña se ha almacenado en forma de valor hash y, opcionalmente, si la dirección recibida se corresponde con la dirección base asociada con la contraseña en forma de valor hash almacenada. La unidad de verificación 160 puede recibir contraseñas en la interfaz en forma de valor hash o no codificada con función hash, siendo preferible la primera. Así pues, un recurso informático puede consultar la unidad de verificación 160 a través de la interfaz para verificar si se ha generado una contraseña determinada para ese recurso en particular. Por ejemplo, la unidad de verificación 160 puede operar de la siguiente manera. Si la contraseña se ha recibido en la interfaz en forma no codificada con función hash, a la contraseña se le aplica una función hash para obtener la firma; si la contraseña se ha recibido en forma de valor hash, entonces la contraseña recibida en forma de valor hash puede formar directamente la firma. A continuación, la unidad de verificación 160 verifica si la contraseña ha sido almacenada previamente por el gestor de identificadores 130, buscando la contraseña recibida en forma de valor hash, por ejemplo, buscando la firma. Si se encuentra una firma, se recupera la información adicional asociada, que incluye la dirección informática o la dirección base. Si no se encuentra una firma, la contraseña recibida no ha sido generada por el generador de contraseñas. A continuación, la dirección informática recuperada es comparada con la dirección informática recibida. Si ambas direcciones son iguales, la contraseña generada recibida ha sido generada para la dirección informática; de lo contrario, la contraseña generada recibida se está utilizando en un sitio web incorrecto, lo que puede ser indicativo de un ataque, o de un error en el sistema, etc.

En una forma de realización, la interfaz de la unidad de verificación 160 está dispuesta para recibir una contraseña en forma no codificada con función hash, por ejemplo, procedente de un recurso informático que utiliza la unidad de verificación 160 para verificar una contraseña. En esta forma de realización, el gestor de identificadores 130 puede almacenar tuplas $(h(p_i), a_j,..., a_k)$. En estas fórmulas, $p_i$ denota una contraseña generada, h denota una función hash (que incluye posiblemente una sal), $a_j,.., a_k$ denota atributos asociados con la contraseña generada. Los atributos pueden incluir la dirección informática o la dirección base. En estas fórmulas, la primera entrada es la firma que sirve de clave. Después de que la unidad de verificación 160 haya recibido una contraseña p y una dirección informática ca, puede calcular una firma h(p), recuperar los atributos asociados almacenados y comparar la dirección informática recibida con la dirección informática recuperada para verificar si son iguales.

En una forma de realización, la interfaz de la unidad de verificación 160 está dispuesta para recibir la contraseña en forma de valor hash, por ejemplo, procedente de un recurso informático dispuesto para verificar una contraseña. En esta forma de realización, el gestor de identificadores 130 puede almacenar tuplas $(h(p_i), a_j,..., a_k)$. Después de que la unidad de verificación 160 haya recibido una contraseña h(p) en forma de valor hash y una dirección informática ca, puede utilizar la firma h(p) como una clave y recuperar los atributos asociados almacenados y comparar la dirección informática recibida con la dirección

informática recuperada para verificar si son iguales. En las formas de realización anteriores, los atributos pueden almacenar una dirección base, y se mapea una dirección informática recibida con la dirección base antes de la comparación.

La primera opción es utilizable si la contraseña es recibida en la interfaz de la unidad de verificación 160 en claro, la segunda opción es utilizable si la contraseña es recibida en la interfaz de la unidad de verificación 160 en forma de valor hash ($h(p_i)$).

La unidad de verificación 160 puede determinar si un atacante está usando una contraseña capturada en un sitio web incorrecto para ver si la contraseña funciona. Si se realiza dicha determinación, la contraseña puede ser inhabilitada, por ejemplo, cambiando el primer identificador de sistema combinado, o incluso el identificador de sistema de usuario y/o el identificador de sistema de dirección base asociado con la contraseña en forma de valor hash almacenada; por ejemplo, en función de un nivel de escalada. La contraseña en forma de valor hash puede ser almacenada por el gestor de identificadores 130, por ejemplo, junto con el primer identificador de sistema combinado. Las contraseñas en forma de valor hash pueden ser almacenadas aunque los correspondientes identificadores de sistema hayan cambiado, de modo que también se puede detectar el abuso de contraseñas antiguas. Las formas de realización que se proporcionan en este documento son de ejemplo, pero se hace énfasis en que de esta manera se pueden identificar diferentes patrones de uso y se pueden adoptar medidas de diferentes maneras según proceda.

El dispositivo de generación de contraseñas 101 no almacena contraseñas en sí. Pero la unidad de verificación 160 puede almacenar una firma de la contraseña. La firma puede ser un valor hash sobre la contraseña que ha generado el dispositivo de generación de contraseñas 101 opcionalmente en combinación con una sal. Una firma puede estar asociada con información adicional. La información adicional puede incluir el sitio web para el que se ha generado la contraseña. La firma de la contraseña generada se puede utilizar como una clave para recuperar la información adicional. Dado que el valor hash es unidireccional, no es posible obtener la propia contraseña producida, o la contraseña de usuario, o el identificador de usuario del proveedor de inicio de sesión, a partir de la firma.

Un recurso informático, por ejemplo, un sitio web, puede enviar una contraseña, preferiblemente en forma de valor hash al dispositivo de generación de contraseñas 101 y la unidad de verificación 160 puede validar:
1. Si la firma de la contraseña recibida corresponde a una contraseña generada por el dispositivo de generación de contraseñas 101. En caso de ser así, se sabe que el sitio web ha recibido del usuario una contraseña fuerte y globalmente única. En caso de no ser así, el sitio web puede rechazar la contraseña, por ejemplo, porque no se puede dar ninguna garantía de calidad para la contraseña. Por ejemplo, el sitio web puede alertar al usuario y/o proporcionarle información de que debe utilizar el dispositivo de generación de contraseñas 101.
2. Si la firma de la contraseña recibida corresponde a una contraseña generada para ese sitio web en particular. En caso de no ser así, entonces se debe tratar un abuso o un error de usuario.
3. Si la firma de la contraseña recibida corresponde a una contraseña que está activa, por ejemplo, que no está bloqueada. En caso de ser así, la contraseña es fuerte, y está destinada al sitio y está activa. En caso de no ser así, entonces es probable que se trate de un abuso, o puede corresponder a un usuario que almacenó su antigua contraseña en algún lugar y la utiliza ahora. Dicho usuario puede ser informado directamente por la unidad de verificación 160.

En una forma de realización, el dispositivo de generación de contraseñas puede ser utilizado de forma anónima y puede no haber forma de contactar con un usuario. Sin embargo, la unidad de verificación 160 puede estar dispuesta para informar al propietario de la contraseña del abuso o error de usuario, por ejemplo, por correo electrónico. Por ejemplo, un usuario puede tener la opción de registrar su información de contacto durante el registro inicial, por ejemplo, una dirección de correo electrónico. Una firma puede estar asociada con un usuario registrado de modo que la unidad de verificación 160 pueda obtener la información de contacto de un usuario a través de una firma.

Por consiguiente, la unidad de verificación 160 proporciona una capacidad de validación de contraseñas con la opción de proporcionar una retroalimentación directa al usuario. El uso de contraseñas incorrectas o inactivas puede ser monitorizado por la unidad de verificación 160. Tanto el sitio web para el que se ha generado una contraseña como el sitio web que ha informado de la contraseña en la interfaz de la unidad de verificación 160 pueden ser informados por la unidad de verificación 160 del intento de contraseña incorrecta.

De este modo, el dispositivo de generación de contraseñas 101 puede validar la fortaleza de una contraseña más allá de los límites de los sitios web. Esto hace que las restricciones de contraseña según se aplican en algunos sitios web, sean redundantes. Los sitios web pueden estar seguros de que si la contraseña es generada por el dispositivo de generación de contraseñas 101, entonces la contraseña es fuerte y globalmente única. Se debe señalar que las actuales restricciones de contraseña no pueden verificar si una contraseña es globalmente única. En efecto, un sitio web que utiliza el dispositivo de generación de contraseñas 100 o 101, no necesita utilizar un identificador de usuario para inicios de sesión. Dado que las

contraseñas son fuertes y únicas, al menos para el sitio web, y preferiblemente globalmente únicas, el usuario puede ser identificado de manera única por su contraseña.

En una forma de realización, el dispositivo de generación de contraseñas 101 comprende una unidad de tickets 170. La unidad de tickets 170 está dispuesta para asignar un identificador de ticket a una contraseña generada, y para almacenar el identificador de ticket, una restricción de ticket y la contraseña generada. La unidad de tickets 170 está dispuesta para enviar el identificador de ticket al dispositivo de usuario 200.

La unidad de tickets 170 está dispuesta para
- recibir procedente del recurso informático un identificador de ticket recibido y una dirección informática recibida, y
- verificar que el identificador de ticket ha sido asignado por la unidad de tickets 170 y que la dirección informática recibida se corresponde con la dirección base asociada con la contraseña generada, y la restricción de ticket, y en caso de ser así, enviar la contraseña generada al recurso informático.

Usando un ticket, se impide que la contraseña final tenga que pasar por el dispositivo de usuario. El dispositivo de usuario y la conexión entre el dispositivo de usuario y el recurso son probablemente la principal fuente de malware, y por lo tanto el punto en el que es más probable que se vean comprometidas las contraseñas. De esta manera, se aumenta la seguridad de la contraseña.

En este procedimiento de autenticación, el dispositivo de generación de contraseñas 101 genera una contraseña final de forma habitual, pero no envía la contraseña al dispositivo de usuario 200. El identificador de ticket puede ser un número aleatorio. El ticket es almacenado (al menos temporalmente). Cuando el recurso informático envía el identificador de ticket, el dispositivo de generación de contraseñas 101 verifica diversas restricciones, por ejemplo, si el ticket aún no ha sido utilizado, si el ticket ha sido generado para ese sitio, si el ticket ha sido recibido en una ventana de tiempo asociada con el ticket, etc. Los tickets y/o sus contraseñas pueden ser comunicados en forma encriptada, por ejemplo, utilizando https.

En una forma de realización, tanto el ticket como la contraseña generada almacenada tienen una fecha de expiración. Después de la fecha de expiración la contraseña se borra del sistema. Esto significa que los tickets no se pueden usar después de la fecha de expiración. También significa que la exposición de la contraseña es limitada. En una forma de realización, la contraseña se almacena en forma encriptada, por ejemplo, utilizando una clave almacenada en el sistema, por ejemplo, en una memoria volátil.

En una forma de realización, se amplía adicionalmente una unidad de tickets para que gestione información personal del usuario. Por ejemplo, el dispositivo de generación de contraseñas puede almacenar uno o más elementos de información personal asociados con el usuario. La unidad de tickets 170 está dispuesta para generar un identificador de ticket adicional y para asociar el identificador de ticket adicional con el usuario. En cierto sentido, se crean dos tickets, por ejemplo, junto con la generación de la contraseña. El primer ticket se utiliza para transmitir la contraseña al recurso informático correcto, por ejemplo, el sitio web, sin pasar por el dispositivo de usuario; el segundo ticket se utiliza para gestionar la información personal. Inicialmente sólo el primer ticket es transmitido al recurso informático, por ejemplo, a través del dispositivo de usuario.

Cuando se utiliza el primer ticket, por ejemplo, verificado satisfactoriamente según se ha indicado anteriormente, la contraseña generada es enviada (posiblemente después de una desencriptación y/o encriptación local para su transmisión) al recurso informático. El segundo ticket, por ejemplo, el identificador de ticket adicional, también es enviado al recurso informático, por ejemplo, junto con la contraseña generada.

Más tarde, si el recurso informático necesita acceder a un elemento de información personal, el recurso informático puede enviar el segundo ticket, por ejemplo, el identificador de ticket adicional, al sistema 100. La unidad de tickets 170 está dispuesta para recibir el identificador de ticket recibido adicional, y para verificar que el identificador de ticket recibido adicional se corresponde con el identificador de ticket adicional almacenado. Si esta última verificación es satisfactoria, la información personal asociada con el usuario es enviada al recurso informático.

El segundo ticket se puede utilizar para solicitar información adicional sobre un usuario. Por ejemplo, una dirección de correo electrónico o un número de teléfono, etc. De esta manera, un usuario puede gestionar los sitios que pueden recuperar información sobre él. El usuario puede hacer un seguimiento de esta información en una ubicación, por ejemplo, el dispositivo 100. Si un usuario deja de utilizar un recurso informático, puede denegar el acceso a su información en el dispositivo 100.

Por lo general, cada uno de los dispositivos 100, 101, 200, 250 y 260 comprende un microprocesador (que no se muestra por separado) que ejecuta software apropiado almacenado en el dispositivo; por ejemplo, ese software se puede haber descargado y/o almacenado en una memoria correspondiente, por ejemplo, una memoria volátil tal como una RAM o una memoria no volátil tal como una Flash (que no se muestra por

separado) del dispositivo. Alternativamente, los dispositivos pueden, en su totalidad o en parte, ser implementados en lógica programable, por ejemplo, como una matriz de puertas programables de campo (FPGA). Los dispositivos se pueden implementar, total o parcialmente, como un denominado circuito integrado de aplicación específica (ASIC), es decir, un circuito integrado (IC) personalizado para su uso particular. Por ejemplo, los circuitos se pueden implementar en CMOS, por ejemplo, utilizando un lenguaje de descripción de hardware tal como Verilog, VHDL, etc.

En una forma de realización, el dispositivo de generación de contraseñas 101 comprende un circuito de entrada, un circuito de dirección informática, un circuito de gestión de identificadores, un circuito de contraseñas, un circuito de proveedor de inicio de sesión, un circuito de verificación, un circuito de tickets, etc. Los circuitos implementan las correspondientes unidades que se describen en el presente documento. Los circuitos pueden ser un circuito procesador y un circuito de almacenamiento, en el que el circuito procesador ejecuta instrucciones representadas electrónicamente en los circuitos de almacenamiento. Los circuitos también pueden ser, FPGA, ASIC o similares.

La Figura 4 muestra de forma esquemática un ejemplo de una forma de realización de un procedimiento de generación de contraseñas 400 en forma de un diagrama de flujo.

El procedimiento de generación de contraseñas 400 comprende
- recibir 410 procedente de un dispositivo de usuario
  - una dirección informática 310, URL1 para acceder a un recurso informático,
  - un identificador de usuario 320 que indica un usuario del dispositivo de usuario, y
  - una contraseña de usuario 330,
- mapear 420 la dirección informática con una dirección base 312, de modo que se mapean múltiples direcciones informáticas URL1, URL2 con la misma dirección base,
- determinar 430 si la dirección base está registrada con el gestor de identificadores, y
  - en caso de no ser así: asignar 432 un identificador de sistema de dirección base único 315 a la dirección base, y almacenar la dirección base junto con el identificador de sistema de dirección base,
  - en caso de ser así: obtener 434 el identificador de sistema de dirección base,
- determinar 440 si el identificador de usuario está registrado con el gestor de identificadores, y
  - en caso de no ser así: asignar 442 un identificador de sistema de usuario único 325 al identificador de usuario, y almacenar el identificador de usuario junto con el identificador de sistema de usuario,
  - en caso de ser así: obtener 444 el identificador de sistema de usuario, y
- determinar 450 un primer identificador combinado 340 a partir del identificador de sistema de dirección base, el identificador de sistema de usuario y la contraseña de usuario.
- determinar 460 si el primer identificador combinado 340 está registrado con el gestor de identificadores, y
  - en caso de no ser así: asignar 462 un primer identificador de sistema combinado único al primer identificador combinado 340, y almacenar el primer identificador combinado 340 junto con el primer identificador de sistema combinado,
  - en caso de ser así: obtener 464 el primer identificador de sistema combinado asignado al primer identificador combinado 340, y
- determinar 470 un segundo identificador combinado a partir de al menos el primer identificador de sistema combinado, y
- determinar 480 una contraseña final a partir del segundo identificador combinado 350 que satisfaga las restricciones de contraseña del recurso.

Obsérvese que el procedimiento 400 incluye unas etapas opcionales 460 – 480.

Son posibles muchas formas diferentes de ejecutar el procedimiento, como será evidente para un experto en la materia. Por ejemplo, el orden de las etapas puede ser variado o algunas etapas pueden ser ejecutadas en paralelo. Además, entre las etapas se pueden insertar otras etapas de procedimiento. Las etapas insertadas pueden representar refinamientos del procedimiento como los que se describen en el presente documento, o pueden no estar relacionados con el procedimiento. Por ejemplo, las etapas 430 – 434 y 440 – 444 pueden ser revertidas o ejecutadas, al menos parcialmente, en paralelo. Además, es posible que una determinada etapa no haya terminado completamente antes de que se inicie la siguiente.

Un procedimiento según la invención puede ser ejecutado utilizando un software, que comprende instrucciones para hacer que un sistema procesador realice el procedimiento 400. Programas informáticos o software pueden incluir sólo las etapas adoptadas por una sub-entidad particular del sistema. El software se puede almacenar en un medio de almacenamiento adecuado, tal como un disco duro, un disquete, una memoria, un disco óptico, etc. El programa informático puede ser enviado como una señal a través de un cable, o de forma inalámbrica, o utilizando una red de datos, por ejemplo, Internet. El software puede estar disponible para su descarga y/o para su uso remoto en un servidor. Un procedimiento según la invención se puede ejecutar utilizando un flujo de bits dispuesto para configurar una lógica programable, por ejemplo, una matriz de puertas programables de campo (FPGA), para realizar el procedimiento.

Se apreciará que la invención se extiende también a programas informáticos, en particular a programas informáticos en o dentro de una portadora, adaptados para poner en práctica la invención. El programa puede ser en forma de código fuente, código objeto, código fuente intermedio, y código objeto tal como en una forma parcialmente compilada, o en cualquier otra forma adecuada para su uso en la implementación del procedimiento según la invención. Una forma de realización relativa a un producto de programa informático comprende instrucciones ejecutables por un dispositivo informático que corresponden a cada una de las etapas de procesamiento de al menos uno de los procedimientos que se describen. Estas instrucciones pueden subdividirse en subrutinas y/o almacenarse en uno o más ficheros que pueden estar enlazados estática o dinámicamente. Otra forma de realización relativa a un producto de programa informático comprende instrucciones ejecutables por un dispositivo informático correspondientes a cada uno de los medios de al menos uno de los sistemas y/o productos que se describen.

La Figura 5a muestra un medio legible por dispositivo informático 1000 que tiene una parte escribible 1010 que comprende un programa informático 1020, comprendiendo el programa informático 1020 unas instrucciones para hacer que un sistema procesador realice un procedimiento de generación de contraseñas, según una forma de realización. El programa informático 1020 puede estar incorporado en el medio legible por dispositivo informático 1000 como marcas físicas o mediante magnetización del medio legible por dispositivo informático 1000. Sin embargo, también se puede concebir cualquier otra forma de realización adecuada. Además, se apreciará que, aunque el medio legible por dispositivo informático 1000 se muestra en este documento como un disco óptico, el medio legible por dispositivo informático 1000 puede ser cualquier medio legible por dispositivo informático adecuado, tal como un disco duro, una memoria de estado sólido, una memoria flash, etc., y puede ser no grabable o grabable. El programa informático 1020 comprende instrucciones para hacer que un sistema procesador realice dicho procedimiento de generación de contraseñas.

La Figura 5b muestra en una representación esquemática un sistema procesador 1140 según una forma de realización. El sistema procesador comprende uno o más circuitos integrados 1110. La arquitectura del uno o más circuitos integrados 1110 se muestra de forma esquemática en la Figura 5b. El circuito 1110 comprende una unidad de procesamiento 1120, por ejemplo, una CPU, para ejecutar componentes de programa informático para ejecutar un procedimiento según una forma de realización y/o implementar sus módulos o unidades. El circuito 1110 comprende una memoria 1122 para almacenar código de programación, datos, etc. Parte de la memoria 1122 puede ser de sólo lectura. El circuito 1110 puede comprender un elemento de comunicación 1126, por ejemplo, una antena, conectores o ambos, y similares. El circuito 1110 puede comprender un circuito integrado dedicado 1124 para realizar parte del o todo el procesamiento definido en el procedimiento de generación de contraseñas. El procesador 1120, la memoria 1122, el circuito integrado dedicado 1124 y el elemento de comunicación 1126 pueden estar conectados entre sí a través de una interconexión 1130, es decir, un bus. El sistema procesador 1110 puede estar dispuesto para una comunicación por contacto y/o sin contacto, utilizando una antena y/o conectores, respectivamente.

Se debe señalar que las formas de realización mencionadas anteriormente ilustran la invención en lugar de limitarla, y que los expertos en la materia podrán diseñar muchas formas de realización alternativas.

En las reivindicaciones, cualesquiera signos de referencia puestos entre paréntesis no se interpretarán como limitantes de la reivindicación. El uso del verbo "comprender" y sus conjugaciones no excluye la presencia de elementos o etapas distintos de los indicados en una reivindicación. El artículo "un" o "una" que precede a un elemento no excluyen la presencia de una pluralidad de dichos elementos. La invención se puede implementar a través de hardware que comprende diversos elementos distintos y a través de un dispositivo informático debidamente programado. En la reivindicación de dispositivo que enumera diversos medios, varios de estos medios pueden ser implementados por un y el mismo elemento de hardware. El mero hecho de que se reciten ciertas medidas en reivindicaciones dependientes diferentes entre sí no indica que una combinación de estas medidas no se pueda utilizar para obtener un beneficio.

En las reivindicaciones, las referencias entre paréntesis se refieren a signos de referencia en dibujos de formas de realización o a fórmulas de formas de realización, lo que aumenta la inteligibilidad de la reivindicación. Estas referencias no se interpretarán como una limitación de la reivindicación.

**REIVINDICACIONES**

1. Un dispositivo de generación de contraseñas (100) que comprende
- una unidad de entrada (110) dispuesta para recibir procedente de un dispositivo de usuario
  - una dirección informática (310, URL1) para acceder a un recurso informático,
  - un identificador de usuario (320) que indica un usuario del dispositivo de usuario, y
  - una contraseña de usuario (330),

**caracterizado por**
- una unidad de direcciones informáticas (120) dispuesta para mapear la dirección informática con una dirección base (312), de modo que se mapean múltiples direcciones informáticas (URL1, URL2) con la misma dirección base,
- un gestor de identificadores (130) dispuesto para
  - determinar si la dirección base está registrada con el gestor de identificadores, y
  - en caso de no ser así: asignar a la dirección base un identificador de sistema de dirección base único (315) y almacenar la dirección base junto con el identificador de sistema de dirección base,
  - en caso de ser así: obtener el identificador de sistema de dirección base,
- determinar si el identificador de usuario está registrado con el gestor de identificadores, y
  - en caso de no ser así: asignar un identificador de sistema de usuario único (325) al identificador de usuario, y almacenar el identificador de usuario junto con el identificador de sistema de usuario,
  - en caso de ser así: obtener el identificador de sistema de usuario, y
- una unidad de contraseñas (140) dispuesta para
  - determinar un primer identificador combinado (340) a partir del identificador de sistema de dirección base, el identificador de sistema de usuario y la contraseña de usuario.

2. Un dispositivo de generación de contraseñas según la reivindicación 1, en el que
- el gestor de identificadores está dispuesto para
  - determinar si el primer identificador combinado está registrado con el gestor de identificadores, y
    - en caso de no ser así: asignar un primer identificador de sistema combinado único al primer identificador combinado, y almacenar el primer identificador combinado junto con el primer identificador de sistema combinado,
    - en caso de ser así: obtener el primer identificador de sistema combinado asignado al primer identificador combinado, y
- la unidad de contraseñas está dispuesta además para determinar un segundo identificador combinado a partir de al menos el primer identificador de sistema combinado.

3. Un dispositivo de generación de contraseñas según la reivindicación 2, en el que
- la unidad de contraseñas está dispuesta además para recuperar restricciones de contraseña para el recurso informático y para determinar una contraseña final a partir del segundo identificador combinado y/o el primer identificador combinado, satisfaciendo la contraseña final las restricciones de contraseña recuperadas.

4. Un dispositivo de generación de contraseñas según las reivindicaciones 2 o 3, en el que
- el gestor de identificadores está dispuesto para
  - cambiar el identificador de sistema de dirección base, renovando de este modo todas las contraseñas para el recurso informático, y/o
  - cambiar el identificador de sistema de usuario, renovando de este modo todas las contraseñas para el identificador de usuario, y/o
  - cambiar el primer identificador de sistema combinado, renovando de este modo el segundo identificador combinado y/o la contraseña final para el identificador de usuario y el recurso informático.

5. Un dispositivo de generación de contraseñas según una cualquiera de las reivindicaciones anteriores, en el que el dispositivo de generación de contraseñas comprende
- una unidad proveedora de inicio de sesión (150) dispuesta para hacer de interfaz entre un primer proveedor de inicio de sesión (250) y el dispositivo de usuario, proporcionando el primer proveedor de inicio de sesión un primer identificador de usuario original, estando la unidad proveedora de inicio de sesión dispuesta para obtener el identificador de usuario a partir del primer identificador de usuario original y enviarlo al dispositivo de usuario.

6. Un dispositivo de generación de contraseñas según una cualquiera de las reivindicaciones anteriores, en el que la unidad proveedora de inicio de sesión está dispuesta para hacer de interfaz entre un segundo proveedor de inicio de sesión (260) y el dispositivo de usuario, proporcionando el segundo proveedor de inicio de sesión un segundo identificador de usuario original, estando la unidad proveedora de inicio de sesión dispuesta para obtener un identificador de usuario adicional a partir del segundo identificador de usuario original y enviarlo al dispositivo de usuario, estando el gestor de identificadores dispuesto para almacenar un factor de corrección para identificador de usuario, en el que el dispositivo de generación de contraseñas aplica el factor de corrección para identificador de usuario al identificador de usuario adicional para mapearlo con el identificador de usuario.

7. Un dispositivo de generación de contraseñas según una cualquiera de las reivindicaciones anteriores, en el que el gestor de identificadores almacena un factor de corrección para contraseña, en el que el dispositivo de generación de contraseñas aplica el factor de corrección para contraseña al segundo identificador combinado para mapearlo con un segundo identificador combinado adicional generado anteriormente para un identificador de usuario diferente.

8. Un dispositivo de generación de contraseñas según una cualquiera de las reivindicaciones anteriores, en el que el gestor de identificadores está dispuesto para almacenar un valor hash de una contraseña generada, opcionalmente junto con la dirección informática o la dirección base, comprendiendo el dispositivo de generación de contraseñas
- una unidad de verificación (160),
  - comprendiendo la unidad de verificación una interfaz dispuesta para recibir una contraseña y opcionalmente una dirección informática,
  - estando la unidad de verificación dispuesta para
    - determinar si la contraseña se ha almacenado en forma de valor hash y, opcionalmente, si la dirección recibida se corresponde con la dirección base asociada con la contraseña en forma de valor hash almacenada.

9. Un dispositivo de generación de contraseñas según una cualquiera de las reivindicaciones anteriores, en el que la unidad de verificación está dispuesta además para
- almacenar la contraseña en forma de valor hash y opcionalmente la dirección informática,
- determinar si se recibe la misma contraseña varias veces.

10. Un dispositivo de generación de contraseñas según una cualquiera de las reivindicaciones anteriores, que comprende
- una unidad de tickets (170) dispuesta para asignar un identificador de ticket a una contraseña generada, y para almacenar el identificador de ticket, una restricción de ticket y la contraseña generada, estando la unidad de tickets dispuesta para enviar el identificador de ticket al dispositivo de usuario,
- estando la unidad de tickets dispuesta para
  - recibir un identificador de ticket recibido y una dirección informática recibida procedente del recurso informático,
  - verificar que el identificador de ticket ha sido asignado por la unidad de tickets y que la dirección informática recibida se corresponde con la dirección base asociada con la contraseña generada, y la restricción de ticket, y en caso de ser así, enviar la contraseña generada al recurso informático.

11. Un dispositivo de generación de contraseñas según la reivindicación 10, en el que el dispositivo de generación de contraseñas almacena una información personal asociada con el usuario,
- la unidad de tickets (170) está dispuesta para generar un identificador de ticket adicional y para asociar el identificador de ticket adicional con el usuario, y está dispuesta para enviar el identificador de ticket adicional al recurso informático después de una verificación satisfactoria,
- estando la unidad de tickets dispuesta para
  - recibir un identificador de ticket recibido adicional, verificar que el identificador de ticket recibido adicional se corresponde con el identificador de ticket adicional almacenado y, en caso de ser así, enviar la información personal asociada con el usuario al recurso informático.

12. Un dispositivo de generación de contraseñas según una cualquiera de las reivindicaciones anteriores, que almacena una lista de identificadores de dispositivo registrados, estando la unidad de entrada dispuesta además para recibir un identificador de dispositivo de usuario, y estando el dispositivo de generación de contraseñas dispuesto para rechazar generar una contraseña si el identificador de dispositivo de usuario no está registrado o está bloqueado.

13. Un dispositivo de generación de contraseñas según una cualquiera de las reivindicaciones anteriores, en el que la contraseña de usuario comprende unos atributos asociados con el usuario o el dispositivo de usuario, por ejemplo, un identificador biométrico obtenido a través de un sensor biométrico.

14. Un sistema de generación de contraseñas que comprende un dispositivo de generación de contraseñas según una cualquiera de las reivindicaciones anteriores y un dispositivo de usuario, comprendiendo el dispositivo de usuario un navegador web dispuesto para
- recibir una contraseña de usuario original,
- aplicar una función hash a la contraseña original, para obtener la contraseña de usuario,
- detectar un campo de contraseña en una página web,
- enviar el identificador de usuario, la dirección de la página web y la contraseña de usuario al dispositivo de generación de contraseñas.

15. Un procedimiento de generación de contraseñas (400) que comprende
- recibir (410) procedente de un dispositivo de usuario

- una dirección informática (310, URL1) para acceder a un recurso informático,
- un identificador de usuario (320) que indica un usuario del dispositivo de usuario, y
- una contraseña de usuario,

**caracterizado por**

- mapear (420) la dirección informática con una dirección base (312), de modo que se mapean múltiples direcciones informáticas (URL1, URL2) con la misma dirección base,
- determinar (430) si la dirección base está registrada con el gestor de identificadores, y
- en caso de no ser así: asignar a la dirección base un identificador de sistema de dirección base único (315) y almacenar la dirección base junto con el identificador de sistema de dirección base,
- en caso de ser así: obtener el identificador de sistema de dirección base,
- determinar (440) si el identificador de usuario está registrado con el gestor de identificadores, y
- en caso de no ser así: asignar un identificador de sistema de usuario único (325) al identificador de usuario, y almacenar el identificador de usuario junto con el identificador de sistema de usuario,
- en caso de ser así: obtener el identificador de sistema de usuario, y
- determinar (450) un primer identificador combinado (340) a partir del identificador de sistema de dirección base, el identificador de sistema de usuario y la contraseña de usuario.

16. Un programa informático (1020) que comprende instrucciones de programa informático dispuestas para realizar el procedimiento de la reivindicación 15 cuando el programa informático es ejecutado en un dispositivo informático.

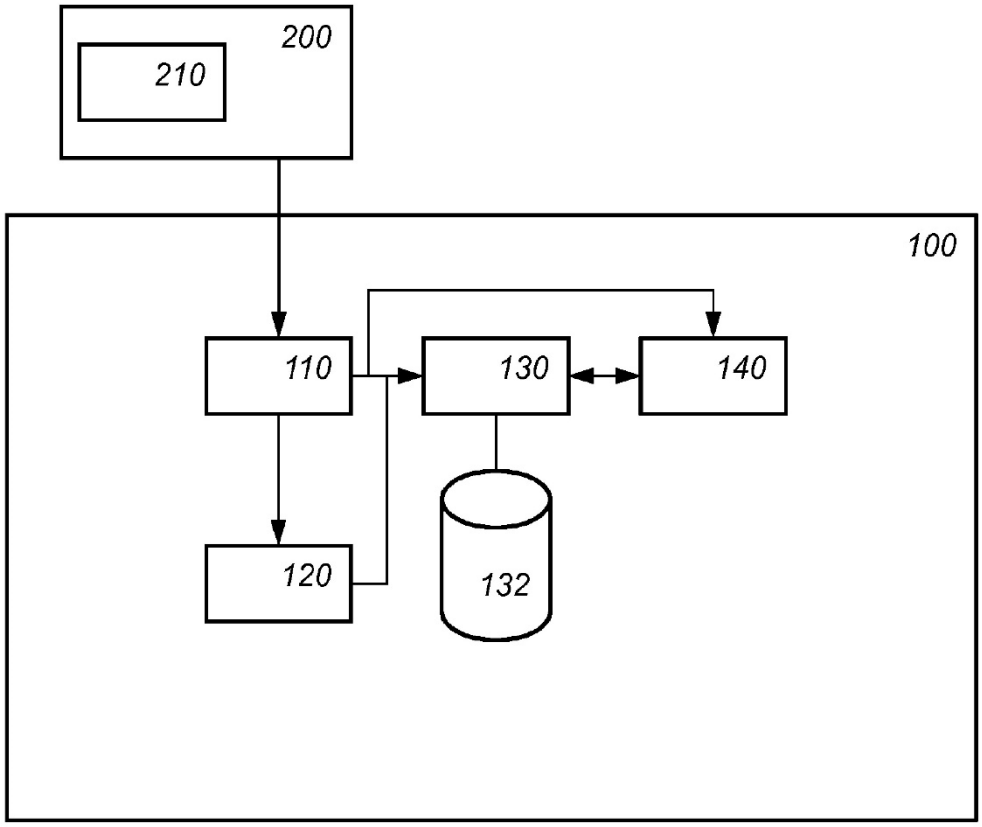


Fig. 1a

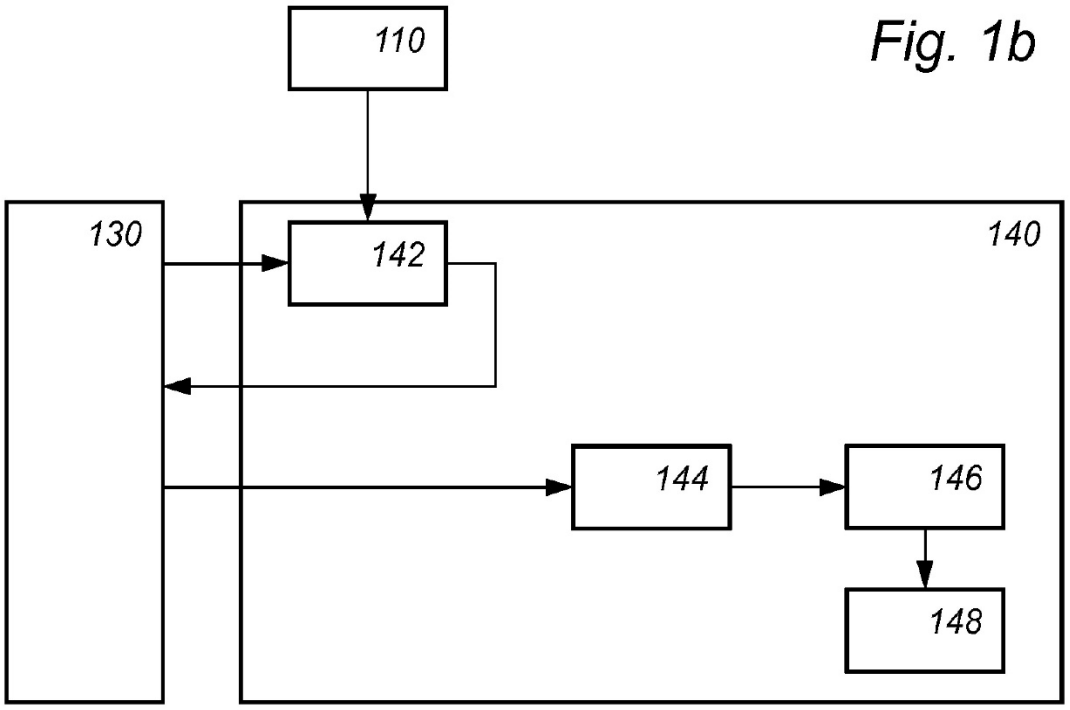


Fig. 1b

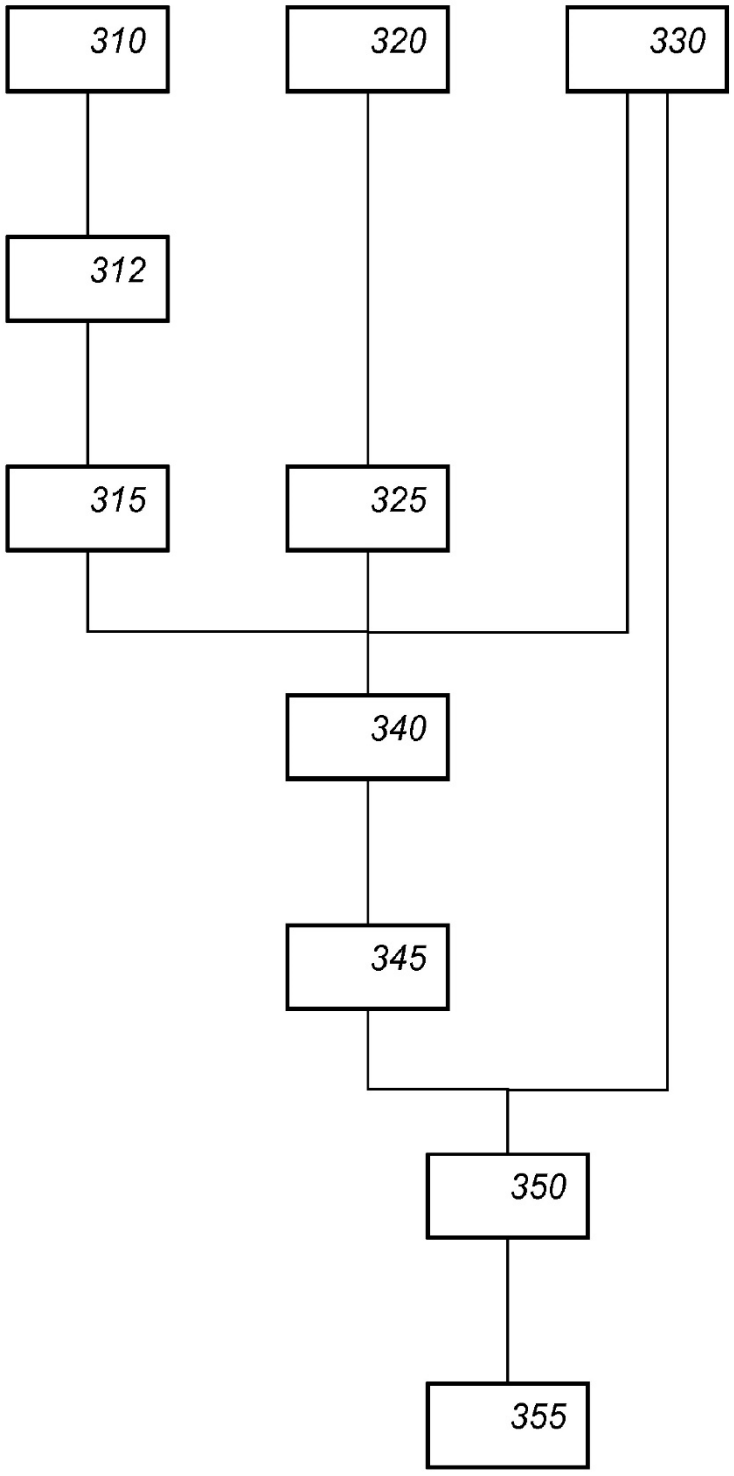


Fig. 2

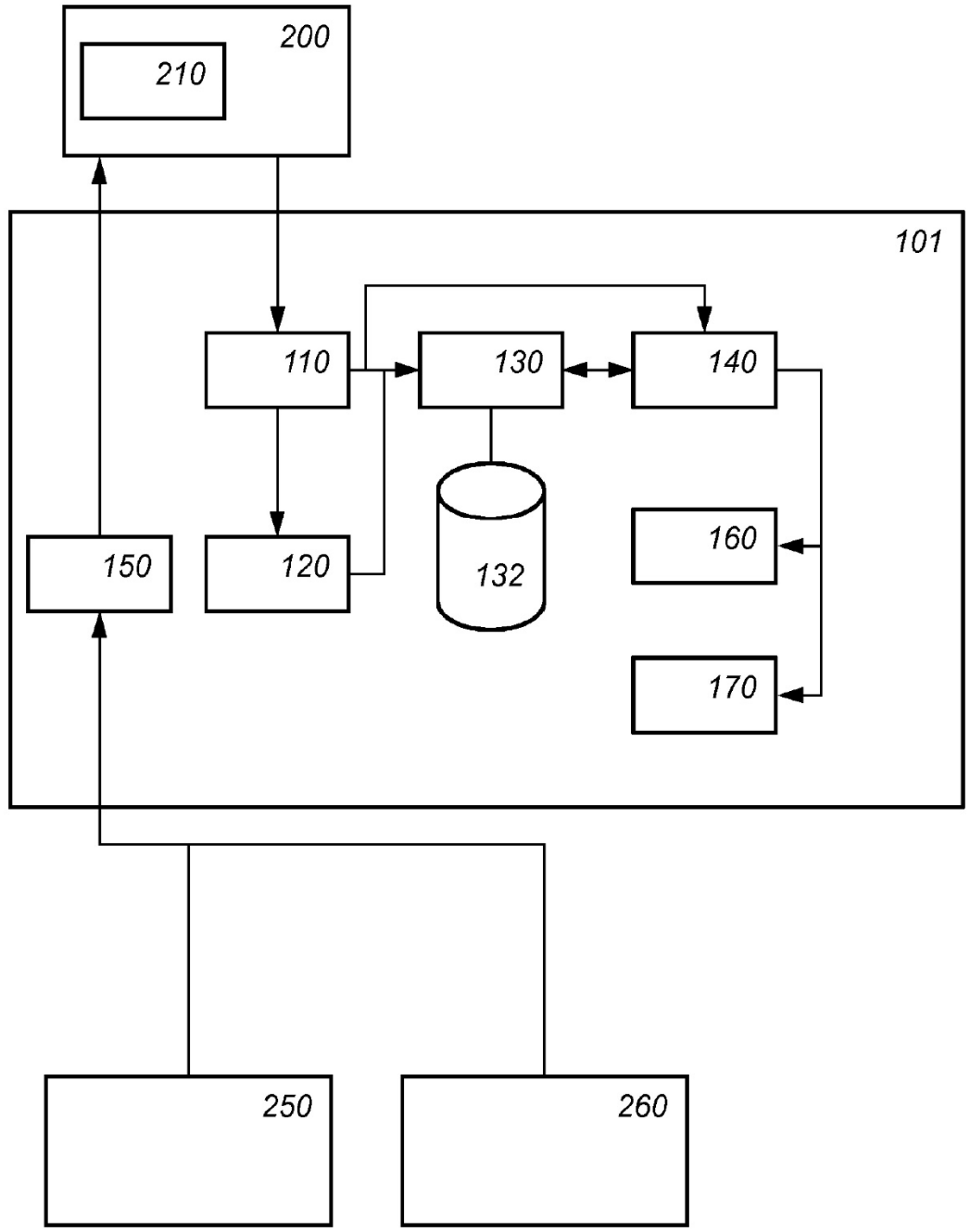


Fig. 3

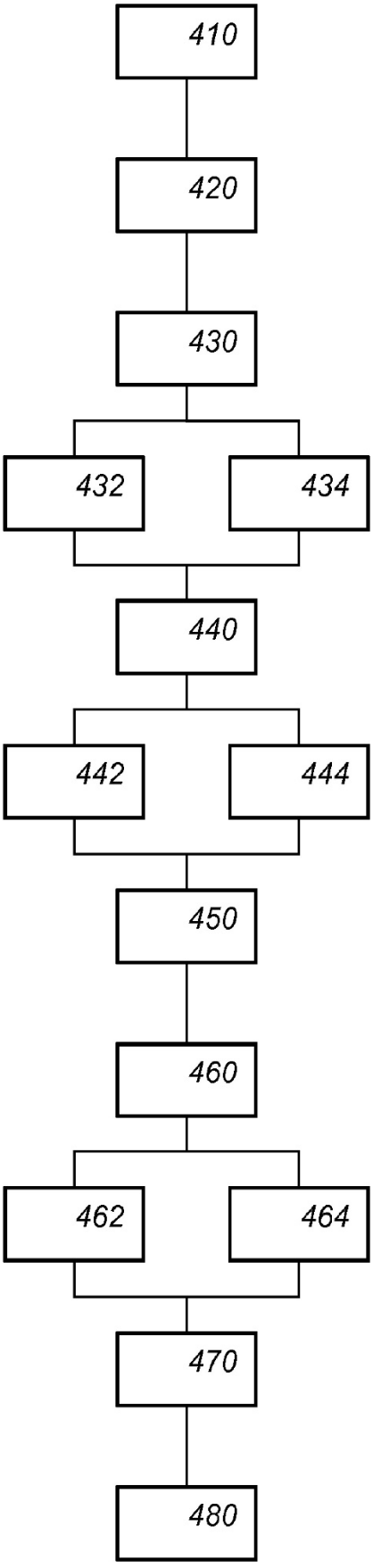


Fig. 4

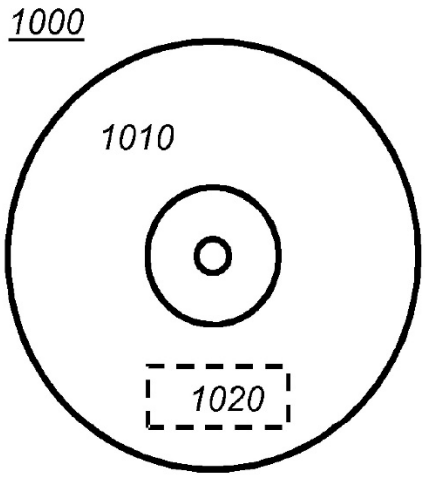


Fig. 5a

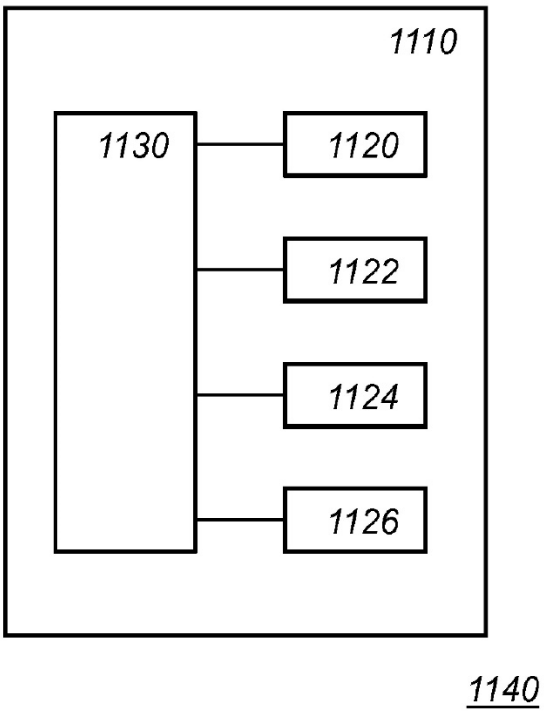


Fig. 5b