(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 962 886**

(51) Int. Cl.:

G06F 21/35 (2013.01)
H04L 9/08 (2006.01)
H04W 12/06 (2011.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **26.02.2018 PCT/FR2018/050450**

(87) Fecha y número de publicación internacional: **30.08.2018 WO18154258**

(96) Fecha de presentación y número de la solicitud europea: **26.02.2018 E 18709706 (8)**

(97) Fecha y número de publicación de la concesión europea: **11.10.2023 EP 3586258**

(54) Título: **Sistema de autenticación de clave segmentada**

(30) Prioridad:

27.02.2017 FR 1751535

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
21.03.2024

(73) Titular/es:

GASCUEL, JACQUES (100.0%)
Edifici Santa Maria de Coll de Caldes Escala A - Planta Cinquena Crta d'Engolasters
Escaldes-Engordany AD700, AD

(72) Inventor/es:

GASCUEL, JACQUES

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Sistema de autenticación de clave segmentada

1. Campo técnico de la invención

La invención se refiere a un sistema de autenticación en una o más aplicaciones. En particular, la invención se refiere a un sistema de autenticación en una o más aplicaciones accesibles a través de un ordenador y cuyo acceso está controlado por un dato de autenticación, que puede ser, por ejemplo, una identidad digital, un par identificador/contraseña, una clave de cifrado, un código de acceso, una clave de asociación de dos aparatos, etc.

2. Antecedentes tecnológicos

Los sistemas de autenticación actuales se basan generalmente en una autenticación débil de tipo identificador y/o contraseña. Este tipo de autenticación es uno de los más sencillos de implantar y requiere la intervención de un usuario que introducirá estos identificadores que conoce o que están anotados en otro documento.

Este tipo de autenticación tiene varios inconvenientes.

En primer lugar, se funda en la memoria del usuario y si este tiene que memorizar varios identificadores y/o contraseñas, es probable que olvide fácilmente los pares identificadores/contraseñas asociados a cada aplicación. Para solucionar este inconveniente, existen administradores de contraseñas, cuyo acceso está protegido por una contraseña principal. Sin embargo, si una persona se hace con la contraseña principal, tiene acceso a todos los pares identificadores/contraseñas del usuario, lo cual es muy perjudicial.

En segundo lugar, si una persona malintencionada roba el par identificador/contraseña de forma remota mediante pirateo o porque está escrito en un documento, esa persona malintencionada puede acceder a la aplicación sin que el usuario se dé cuenta de este robo. Para solucionar este inconveniente, existen objetos o aparatos físicos propiedad del usuario que permiten proporcionar el dato de autenticación, por ejemplo, una tarjeta inteligente, una memoria USB, un dispositivo móvil, etc., a través de un lector de tarjetas, por ejemplo. Sin embargo, si una persona malintencionada se hace con este objeto o aparato, puede acceder fácilmente a la aplicación en lugar del usuario o al menos hacerse con los datos que contiene.

Otra solución era optar por la llamada identificación fuerte, en la que se solicita una contraseña y se envía un código por SMS a un teléfono del usuario para verificar su identidad. En este caso, el inconveniente es que, si le roban el teléfono, este SMS lo recibe directamente la persona malintencionada y simplifica su autenticación ante la aplicación.

Por último, el par identificador/contraseña, incluso si se oculta lo suficiente a una persona malintencionada, debe introducirse en claro en la aplicación. Por lo tanto, una persona malintencionada puede hacerse con él, especialmente si ha instalado, en el ordenador utilizado por el usuario para acceder a la aplicación, un software de registro de teclas (*keylogger* en inglés).

Por tanto, el inventor ha buscado una solución a estos inconvenientes. Las solicitudes de patente US 2016/337863 A1 y US 2014/0208112 A1 dan a conocer métodos de protección de datos de autenticación mediante el uso compartido de claves.

3. Objetivos de la invención

La invención pretende subsanar al menos algunos de los inconvenientes de los sistemas de autenticación conocidos.

En particular, la invención pretende proporcionar, en al menos una realización de la invención, un sistema de autenticación que permita el almacenamiento de uno o más datos de autenticación con seguridad.

La invención también pretende proporcionar, en al menos una realización, un sistema de autenticación que utiliza objetos físicos para la autenticación con el fin de evitar un robo remoto de datos de autenticación.

La invención también pretende proporcionar, en al menos una realización de la invención, un sistema de autenticación que permita evitar los robos de contraseñas por parte de un registrador de teclas.

La invención también pretende proporcionar, en al menos una realización de la invención, un sistema de autenticación que permita protegerse contra los riesgos de autenticación por parte de una persona malintencionada en caso de robo de uno o varios de los equipos de este sistema de autenticación.

4. Presentación de la invención

Para ello, la invención se refiere a un sistema de autenticación para al menos una aplicación accesible por un usuario a través de un ordenador y cuyo acceso está controlado mediante un dato de autenticación, que comprende:

- un dispositivo móvil principal, que comprende un módulo de comunicación de campo cercano, una memoria no volátil y una memoria volátil, y configurado para comunicarse con el ordenador,

- un token principal, que comprende un módulo de comunicación de campo cercano y una memoria no volátil en la que está grabado al menos un dato de autenticación,

estando configurado el dispositivo móvil principal para recuperar, a través del módulo de comunicación de campo cercano, el dato de autenticación del token principal gracias a una clave de emparejamiento, y estando configurado el token principal para permitir el acceso al dato de autenticación solamente previa presentación de dicha clave de emparejamiento,

caracterizado por que la clave de emparejamiento está segmentada en varios segmentos, estando grabado un primer segmento en la memoria no volátil del dispositivo móvil principal y estando grabado al menos otro segmento adicional en una memoria no volátil de un dispositivo móvil secundario y/ o una memoria no volátil de un token secundario, estando configurado el dispositivo móvil principal para recuperar el o los segmentos adicionales mediante comunicación de campo cercano con dicho o dichos dispositivos móviles secundarios y/o dicho o dichos tokens secundarios, para recomponer la clave de emparejamiento y para presentar la clave de emparejamiento recompuesta al token principal,

y por que el o los segmentos adicionales recuperados por el dispositivo móvil principal se almacenan en la memoria volátil del dispositivo móvil principal.

Por lo tanto, el dispositivo móvil no guarda permanentemente el dato de autenticación para evitar que sea copiado por una persona malintencionada. La memoria volátil es, por ejemplo, una memoria de tipo RAM (por *Random Access Memory* en inglés).

Por lo tanto, un sistema de autenticación según la invención permite almacenar datos de autenticación en un token físico llamado token principal, que actúa así como administrador de autenticación, pero cuyo acceso depende de una clave de emparejamiento segmentada cuyos segmentos están distribuidos en varios equipos físicos, que pueden ser otros tokens y/o dispositivos móviles. Estos equipos físicos pueden estar disimulados o llevados por personas diferentes. En lugar de utilizar la memoria del usuario para memorizar una contraseña, el usuario memoriza por tanto qué equipos contienen los segmentos de la clave de emparejamiento y mantiene esta información en secreto. Así, una persona malintencionada que quiera acceder al dato de autenticación incluido en el token principal no podrá hacerlo hasta que haya recompuesto completamente la clave de emparejamiento con todos los segmentos. Pero estos segmentos de claves pueden estar disimulados, por ejemplo, un usuario en una oficina de una empresa puede recuperar un segmento de clave en un token disimulado debajo de su escritorio, y/o en un token disimulado en la entrada de su oficina y/o en otra sala de la empresa, y/o solicitar a un superior jerárquico un segmento grabado en su dispositivo móvil que de paso podrá autentificarlo visualmente, etc. Las interacciones del dispositivo móvil principal con el token principal y todas las recuperaciones de segmentos se realizan mediante comunicación de campo cercano, lo que requiere una proximidad física y evita los pirateos remotos. No hay conexión a una red de Internet que aumentaría el riesgo de pirateo remoto. Todas las comunicaciones se realizan en red local, incluida la conexión entre el ordenador y el dispositivo móvil principal (que puede conectarse por cable o de forma inalámbrica, por ejemplo, por Wi-Fi o Bluetooth).

El dispositivo móvil es, por ejemplo, un teléfono inteligente (*smartphone* en inglés), una tableta, etc. El token es un objeto físico, por ejemplo, de tipo tag (etiqueta) NFC (por *Near Field Communication* en inglés), alimentado únicamente a través de campo cercano o que tenga una fuente de energía limpia (una pila o batería, por ejemplo). La aplicación puede ser una página web, un software, una aplicación, etc. El ordenador puede ser cualquier equipo que comprenda un procesador, como un teléfono inteligente, un ordenador de escritorio/portátil, una tableta, un objeto inteligente, etc.

El primer segmento poseído por el dispositivo móvil principal puede ser poseído permanentemente por este dispositivo móvil principal, o quizás recibido de antemano, por ejemplo, enviado por un servidor externo.

El dato de autenticación puede ser, por ejemplo, una identidad digital, un par identificador/contraseña, una clave de cifrado, un código de acceso, una clave de asociación de dos aparatos (de tipo asociación Wi-Fi o Bluetooth), etc. El dato de autenticación puede asociarse a una denominación (un nombre o una referencia, por ejemplo), permitiendo encontrarlo en el token principal. El token principal es similar a un administrador de contraseñas pero más completo, porque permite más tipos de autenticación, y a un objeto físico como se describe en el estado de la técnica, pero con una capa adicional de seguridad. De hecho, no presenta los inconvenientes descritos anteriormente, en particular:

- no existe una contraseña principal que permita el acceso a todos los datos de autenticación en caso de robo. Todos los datos están protegidos por los segmentos de clave que ofrecen una protección mucho más robusta, especialmente porque no están disponibles de forma remota;

- un robo del token principal no permite el acceso a los datos de autenticación, porque el acceso a estos datos almacenados en la memoria está sujeto a la presentación de la clave de emparejamiento. Sin la clave de

emparejamiento, el token principal es inútil. Además, los datos que contiene están cifrados (por ejemplo, cifrado AES 256) y el token puede incluir protecciones internas para evitar el robo de datos, de tipo supresión de datos (en particular, seguida de la reescritura de datos aleatorios) o destrucción física, en particular después de uno o más intentos de presentación de una clave de emparejamiento. Además, aunque los futuros avances tecnológicos permitan romper la clave de cifrado utilizada para los datos, estos datos serán inaccesibles sin la clave de emparejamiento completa. Asimismo, el descifrado de un segmento de clave no permite encontrar la clave en defecto de los otros segmentos que pueden estar en objetos físicamente ocultos;

- un robo del dispositivo móvil tampoco permite acceder a la aplicación, ni recuperar los datos de autenticación del token principal, ya que se debe estar en poder de la totalidad de los segmentos de clave y, por tanto, conocer la existencia, la identidad y la ubicación del o los dispositivos móviles secundarios y/o del o los tokens secundarios.

El dispositivo móvil principal puede además estar previamente emparejado con el token principal, de modo que la clave de emparejamiento solo pueda ser proporcionada por ese dispositivo móvil principal, en cuyo caso se rechaza. Este emparejamiento previo refuerza la seguridad en el caso muy improbable de que una persona malintencionada consiguiera recomponer la clave con todos los segmentos.

El sistema de autenticación se describe desde el punto de vista del acceso a una única aplicación, cuyo dato de autenticación está incluido en un token, que es por tanto el token principal, ya que contiene este dato. Sin embargo, el token principal para una aplicación puede ser un token secundario para otra aplicación, es decir, puede incluir un segmento de clave de emparejamiento para otro token principal de otra aplicación. Asimismo, un token secundario para la aplicación descrita en la invención puede incluir datos de autenticación para otra aplicación. Lo mismo ocurre con el dispositivo móvil principal, que puede incluir otro segmento de clave o un dispositivo secundario puede comunicarse con un ordenador para otra aplicación.

Según determinadas variantes de la invención, el token principal (o un token secundario) puede comprender un microcontrolador. El microcontrolador puede permitir mejorar la seguridad del sistema, en particular controlando internamente determinados mecanismos de seguridad, en particular el cifrado AES256/SHA256 y/o RSA2048 y/o RSA4096. El microcontrolador permite una gestión de aplicaciones de determinadas funciones que son soportadas por el dispositivo móvil principal cuando el token no incluye este microcontrolador. En particular, se mejoran determinados mecanismos de seguridad permitiendo la manipulación de la memoria internamente, el recuento del número de intentos de emparejamiento, la gestión de autenticación, la gestión del tiempo mediante un reloj de tiempo real, la gestión de sensores, etc.

Según determinadas variantes de la invención, el token principal está configurado de manera que es accesible a través de dos perfiles de persona diferentes:

- un perfil administrador, que puede configurar el token principal, en particular el tipo de aleatorización, el número de intentos permitidos, los mecanismos de protección, las contraseñas de usuario, la segmentación de la clave de emparejamiento, el dispositivo móvil principal que se puede utilizar, los privilegios de acceso a los datos por parte de usuarios, etc. Además, el administrador puede consultar todas las denominaciones de los datos de autenticación presentes en el token;

- al menos un perfil usuario, que debe someterse a las limitaciones predefinidas por el administrador, y pudiendo únicamente comprobar la presencia de la denominación del dato de autenticación que desea recuperar sin poder consultar todas las denominaciones.

Las contraseñas del administrador y del o los usuarios están cifradas y almacenadas en el token.

En un funcionamiento preferente de la invención, el dato de autenticación está presente en la memoria volátil durante solo una fracción de segundo (del orden de un milisegundo), solo el tiempo para transferir este dato al ordenador, luego se borra (o libera para ser sustituido por otro tipo de dato). También preferentemente, el propio ordenador almacena el dato de autenticación en una memoria volátil.

Dado que el dato de autenticación se almacena en una memoria volátil durante un tiempo muy corto, es difícil o incluso imposible para una persona malintencionada recuperarlo. Además, generalmente se trata de un dato pequeño (unos pocos bytes), por lo que una persona malintencionada que analizara la memoria tendría que encontrar este pequeño dato entre varios megabytes, gigabytes o terabytes de datos.

Ventajosamente y según la invención, el dato digital es una contraseña, por que el token principal comprende un módulo de aleatorización adaptado para aleatorizar dicha contraseña añadiendo caracteres en posiciones particulares de la contraseña, siendo dichos caracteres y dichas posiciones predeterminados y conocidos por el usuario.

Según este aspecto de la invención, la aleatorización permite combatir los registradores de teclas añadiendo caracteres en posiciones predeterminadas y conocidas por el usuario mediante medios nemotécnicos. Luego, el usuario borra estos caracteres añadidos en el campo de texto destinado a la contraseña. De este modo, cuando el usuario va a copiar la contraseña en el campo, la contraseña que se muestra será una contraseña aleatorizada, que

puede ser recuperada por un registrador de teclas o incluso leída directamente en la pantalla por una persona malintencionada. Cuando el usuario borra los caracteres añadidos con ayuda de un teclado, un registrador de teclas solo detectará la pulsación de una tecla de borrado, sin saber dónde se encuentra el cursor y, por lo tanto, sin saber qué carácter se ha borrado.

En las otras variantes de la invención, por ejemplo cuando el dato de autenticación no es una contraseña para introducir, no es necesaria la aleatorización porque un registrador de teclas no puede detectar nada y la autenticación se lleva a cabo automáticamente, previa presentación del dato de autenticación, sin intervención del usuario.

Ventajosamente y según la invención, la clave de emparejamiento está segmentada en un primer segmento y al menos dos segmentos adicionales, y por que los segmentos adicionales están ordenados, de modo que la recomposición de la clave de emparejamiento solo es posible si los segmentos adicionales son recuperados por el dispositivo móvil principal en un orden predeterminado.

Según este aspecto de la invención, la recomposición de la clave de emparejamiento está sujeta a la vez al conocimiento de la posición y de la identidad de los equipos secundarios que comprenden los segmentos adicionales, lo que ya garantiza una primera seguridad como se explicó anteriormente, pero también al orden en que se recuperan estos segmentos. Por ejemplo, el usuario primero debe recuperar un segmento adicional n.º 1 de un token secundario cerca de la entrada de su oficina, un segmento adicional n.º 2 de un token secundario debajo de su escritorio y un segmento adicional n.º 3 de un dispositivo móvil secundario llevado por su superior. Si los segmentos adicionales no son recuperados en orden (por ejemplo, n.º 3, luego n.º 1, luego n.º 2), la clave recompuesta con los segmentos desordenados no forma la clave de emparejamiento y el dispositivo móvil principal no puede recuperar el dato de autenticación. Si los segmentos son recuperados en orden, se recompone la clave de emparejamiento.

Ventajosamente y según la invención, el token principal comprende una pluralidad de datos de autenticación identificados cada uno de ellos por una denominación, y por que el dispositivo móvil principal solicita un dato de autenticación proporcionando dicha denominación al token principal.

Según este aspecto de la invención, un mismo token principal puede contener datos de autenticación para varias aplicaciones y las denominaciones permiten encontrar un dato de autenticación en el token principal. Las denominaciones también pueden permitir que el dispositivo móvil principal verifique previamente que el dato efectivamente está en el token principal y no en otro token.

La invención también se refiere a un procedimiento implementado por un sistema de autenticación según la invención, caracterizado por que comprende los siguientes pasos:

- un paso de solicitud de un dato de autenticación por parte de la aplicación,
- un paso de transmisión de la solicitud desde el ordenador al dispositivo móvil principal,
- un paso de comunicación de campo cercano del dispositivo móvil principal con el token principal,
- un paso de verificación de la clave de emparejamiento recompuesta presentada por el dispositivo, y:
    - mientras la clave de emparejamiento no esté completa, un paso de recuperación de al menos un segmento de clave de emparejamiento por parte del dispositivo móvil principal, seguido de un nuevo paso de verificación de la clave de emparejamiento recompuesta,
    - si la clave de emparejamiento es correcta, un paso de transmisión del dato de autenticación por el token principal al dispositivo móvil principal,
- un paso de almacenamiento del dato de autenticación por el dispositivo móvil principal en su memoria volátil,
- un paso de transmisión del dato de autenticación por el dispositivo móvil principal al ordenador,
- un paso de autenticación en la aplicación a través del dato de autenticación.

Por tanto, un procedimiento según la invención permite un control total de la autenticación de un usuario que desea acceder a una aplicación en el ordenador. El dato de autenticación, almacenado en el token principal, solo se proporciona en presencia de todos los segmentos de la clave de emparejamiento. Los segmentos de la clave de emparejamiento pueden ser recuperados previamente por el dispositivo móvil principal y luego proporcionarse al token principal, o el dispositivo móvil principal puede intentar acceder al token principal, en cuyo caso el token principal deniega el acceso e indica que la clave presentada no está completa.

Preferiblemente, el número de pasos de verificación puede ser limitado (de uno a varios pasos) y, si se excede este número, el token principal inicia un paso de protección de los datos que contiene, por ejemplo mediante borrado de los datos y reescritura de los mismos para evitar que una persona malintencionada acceda a ellos. Este número de

pasos de verificación es preconfigurable en el token principal y una persona malintencionada no puede saber cuántos pasos de verificación se permiten y, por lo tanto, no puede prever un ataque múltiple en función del número de intentos posibles (puede haber solo uno).

Ventajosamente y según la invención, en la variante del sistema de autenticación en donde el token principal comprende un módulo de aleatorización, el paso de autenticación en la aplicación comprende un subpaso de copia de la contraseña aleatorizada en un campo de texto de la aplicación, y un subpaso de borrado por parte del usuario de los caracteres añadidos por el módulo de aleatorización, de modo que la contraseña mostrada corresponda a la contraseña de la aplicación.

En otra variante de la invención, el usuario también puede añadir caracteres para recomponer la contraseña.

La invención también se refiere a un sistema de autenticación y a un procedimiento de autenticación caracterizados en combinación por todas o parte de las características mencionadas anteriormente o a continuación.

5. Lista de figuras

Otros objetivos, características y ventajas de la invención aparecerán con la lectura de la siguiente descripción que se hace únicamente con carácter no limitativo y que hace referencia a las figuras adjuntas, en donde:

- la figura 1 es una vista esquemática de un sistema de autenticación según una realización de la invención,

- la figura 2 es una vista esquemática de un procedimiento de autenticación según una realización de la invención.

6. Descripción detallada de una realización de la invención

Las siguientes realizaciones son ejemplos. Aunque la descripción se refiere a una o más realizaciones, esto no significa necesariamente que cada referencia se refiera a la misma realización, o que las características solo se apliquen a una única realización. También se pueden combinar características individuales de diferentes realizaciones para proporcionar otras realizaciones. En las figuras no se respetan estrictamente escalas y proporciones por motivos de ilustración y claridad.

La figura 1 representa esquemáticamente un sistema de autenticación 10 según una realización de la invención. El sistema de autenticación 10 permite controlar el acceso a una aplicación 12 accesible a través de un ordenador 14. El sistema de autenticación comprende un dispositivo móvil principal 16 y un token principal 18. El dispositivo móvil principal comprende un módulo de comunicación de campo cercano 20, una memoria no volátil 22 y una memoria volátil 24.

El token principal 18 también comprende un módulo de comunicación de campo cercano 26 y una memoria no volátil 28, en la que se almacena (de forma cifrada) al menos un dato de autenticación 30. El token principal puede comprender una sujeción 34 para transportarse como llavero.

Para acceder a la aplicación, un usuario necesita este dato de autenticación 30. Para recuperarlo, el dispositivo móvil principal 16 debe presentar una clave de emparejamiento 32 que permita el acceso al dato de autenticación 30, siendo transmitido dicho dato de autenticación 30 por el token principal 18 solo en presencia de esta clave de emparejamiento 32. Esta clave de emparejamiento es preferiblemente una clave de tipo clave de cifrado y es un dato compuesto por una serie de valores hexadecimales sucesivos. Sin embargo, la clave de emparejamiento 32 se almacena en varios segmentos, de los cuales un primer segmento 32a se almacena en la memoria no volátil 22 del dispositivo móvil principal 16. Uno o más segmentos adicionales, aquí dos segmentos adicionales, son almacenados por otros equipos: por ejemplo, un dispositivo móvil secundario 116, similar al dispositivo móvil principal 16, posee un segmento adicional 32b, y un token secundario 118, similar al token principal 18, posee un segmento adicional 32c. Para recomponer la clave de emparejamiento 32, el dispositivo móvil 16 debe recuperar estos segmentos adicionales gracias a una comunicación de campo cercano. La recomposición de la clave de emparejamiento 32 puede requerir que los segmentos sean recuperados en un orden preciso.

El procedimiento de autenticación 40 implementado por este sistema de autenticación 10 se representa esquemáticamente con referencia a la figura 2.

El procedimiento de autenticación 40 comprende un paso 42 de solicitud de un dato de autenticación por parte de la aplicación, un paso 44 de transmisión de la solicitud desde el ordenador al dispositivo móvil principal y un paso 46 de comunicación de campo cercano del dispositivo móvil principal con el token principal.

Antes de proporcionar el dato de autenticación, el token principal procede a una etapa 48 de verificación de la clave de emparejamiento recompuesta presentada por el dispositivo. Mientras esta no esté completa, el dispositivo móvil principal procede a al menos un paso 50 de recuperación de al menos un segmento de clave de emparejamiento por el dispositivo móvil principal, y luego el token principal procede a un nuevo paso de verificación de la clave de emparejamiento recompuesta.

El número de pasos 48 de verificación llevados a cabo puede ser limitado.

Si la clave de emparejamiento está completa, el token principal procede a un paso 52 de transmisión del dato de autenticación por el token principal al dispositivo móvil principal.

Luego, el dispositivo procede a un paso 54 de almacenamiento del dato de autenticación por el dispositivo móvil principal en su memoria volátil.

Luego, el procedimiento comprende un paso 56 de transmisión del dato de autenticación por el dispositivo móvil principal al ordenador.

Finalmente, el procedimiento comprende un paso 58 de autenticación en la aplicación a través del dato de autenticación.

El token principal también puede comprender un módulo de aleatorización (no representado), y el paso de autenticación comprende entonces un subpaso de copia de la contraseña aleatorizada en un campo de texto de la aplicación, y un subpaso de borrado por parte del usuario de los caracteres añadidos por el módulo de aleatorización, de modo que la contraseña mostrada corresponda a la contraseña de la aplicación. Un ejemplo de aleatorización de la contraseña podría ser el siguiente:

La contraseña para la aplicación es motdepasse. Cuando el dispositivo móvil principal solicita esta contraseña, tras la presentación de la clave de emparejamiento completa y válida, el módulo de aleatorización aleatoriza esta contraseña. Además, puede almacenarse directamente aleatorizada y cifrada. La contraseña aleatorizada es, por ejemplo, &mo@tdep%as^se. El usuario, conociendo la aleatorización predeterminada, en particular la posición de la aleatorización, sabe que los caracteres añadidos son los caracteres 1º, 4º, 9º y 12º. Puede introducir la contraseña aleatorizada en la aplicación, ya sea escribiéndola de nuevo, o bien mediante copiar-pegar. Luego borra los caracteres añadidos, posicionándose delante o detrás de los caracteres añadidos usando un ratón o mediante pulsación táctil, y los borra mediante una tecla "borrado" (por ejemplo, "Supr" o "Retroceso") del teclado para permitir el envío de la verdadera contraseña a la aplicación.

Por lo tanto, un registrador de teclas que estuviera instalado en el ordenador que ejecuta la aplicación registraría las siguientes pulsaciones de teclas: «&» «m» «o» «@» «t» «d» «e» «p» «%» «a» «s» «^» «s» «e» «Tecla de borrado» «Tecla de borrado» «Tecla de borrado» «Tecla de borrado». Así pues, no está en condiciones de leer la contraseña. La ventaja es la misma si una persona malintencionada lee la contraseña aleatorizada antes de que el usuario la corrija: la persona malintencionada cree que tiene la contraseña correcta, pero es incorrecta.

Esta contraseña y esta aleatorización se presentan, por supuesto, con fines ilustrativos, siendo preferentemente la contraseña y la aleatorización elegidas, obviamente, más complejas, en particular, la contraseña generalmente no se compone de una palabra del diccionario, es más larga y la aleatorización debería ser más difícil de adivinar porque, por ejemplo, se mezcla con caracteres complejos de la contraseña y los caracteres añadidos lo son en gran cantidad.

La invención no se limita a las realizaciones descritas. En particular, más allá de los sistemas de seguridad aquí descritos, las memorias de los elementos del sistema y las comunicaciones entre los diferentes elementos del sistema están preferentemente cifradas y protegidas mediante principios de seguridad conocidos, en particular cifrado AES, SSL, etc., para añadir la máxima seguridad a cada elemento y para cada transmisión de datos.

REIVINDICACIONES

1. Sistema de autenticación en al menos una aplicación (12) accesible por un usuario a través de un ordenador (14) y cuyo acceso está controlado por un dato de autenticación, que comprende:

- un dispositivo móvil principal (16), que comprende un módulo de comunicación de campo cercano (20), una memoria no volátil (22) y una memoria volátil (24), y configurado para comunicarse con el ordenador (14),

- un token principal (18), que comprende un módulo de comunicación de campo cercano (26) y una memoria no volátil (28) en la que está grabado al menos un dato de autenticación (30),

estando configurado el dispositivo móvil principal (16) para recuperar, a través del módulo de comunicación de campo cercano (22), el dato de autenticación (30) del token principal gracias a una clave de emparejamiento (32), y estando configurado el token principal (18) para permitir el acceso al dato de autenticación (30) solamente previa presentación de dicha clave de emparejamiento (32),

caracterizado por que la clave de emparejamiento (32) está segmentada en varios segmentos, estando grabado un primer segmento (32a) en la memoria no volátil (22) del dispositivo móvil principal (16) y estando grabado al menos otro segmento adicional (32b, 32c) en una memoria no volátil de un dispositivo móvil secundario (116) y/o una memoria no volátil de un token secundario (118), estando configurado el dispositivo móvil principal (16) para recuperar el o los segmentos adicionales (32b, 32c) mediante comunicación de campo cercano con dicho o dichos dispositivos móviles secundarios (116) y/o dicho o dichos tokens secundarios (118), para recomponer la clave de emparejamiento (32) y para presentar la clave de emparejamiento recompuesta (32) al token principal (18),

y por que el o los segmentos adicionales (32b, 32c) recuperados por el dispositivo móvil principal (16) se almacenan en la memoria volátil (24) del dispositivo móvil principal.

2. Sistema de autenticación según la reivindicación 1, caracterizado por que el dato de autenticación (30) es una identidad digital, una contraseña, un par identificador/contraseña, una clave de cifrado o un código de acceso.

3. Sistema de autenticación según la reivindicación 2, caracterizado por que el dato digital (30) es una contraseña, por que el token principal (18) comprende un módulo de aleatorización adaptado para aleatorizar dicha contraseña añadiendo caracteres en posiciones particulares de la contraseña, siendo dichos caracteres y dichas posiciones predeterminados y conocidos por el usuario.

4. Sistema de autenticación según una de las reivindicaciones 1 a 3, caracterizado por que la clave de emparejamiento (32) está segmentada en un primer segmento (32a) y al menos dos segmentos adicionales (32b, 32c), y por que los segmentos adicionales (32a, 32b) están ordenados, de modo que la recomposición de la clave de emparejamiento (32) solo es posible si los segmentos adicionales (32b, 32c) son recuperados por el dispositivo móvil principal (16) en un orden predeterminado.

5. Sistema de autenticación según una de las reivindicaciones 1 a 4, caracterizado por que el token principal (18) comprende una pluralidad de datos de autenticación identificados cada uno de ellos por una denominación, y por que el dispositivo móvil principal (16) solicita un dato de autenticación proporcionando dicha denominación al token principal (18).

6. Procedimiento de autenticación implementado por un sistema de autenticación según una de las reivindicaciones 1 a 5, caracterizado por que comprende los siguientes pasos:

- un paso (42) de solicitud de un dato de autenticación por parte de la aplicación,

- un paso (44) de transmisión de la solicitud desde el ordenador al dispositivo móvil principal,

- un paso (46) de comunicación de campo cercano del dispositivo móvil principal con el token principal,

- un paso (48) de verificación de la clave de emparejamiento recompuesta presentada por el dispositivo, y:

  - mientras la clave de emparejamiento no esté completa, un paso (50) de recuperación de al menos un segmento de clave de emparejamiento por parte del dispositivo móvil principal, seguido de un nuevo paso de verificación de la clave de emparejamiento recompuesta,

  - si la clave de emparejamiento es correcta, un paso (52) de transmisión del dato de autenticación por el token principal al dispositivo móvil principal,

- un paso (54) de almacenamiento del dato de autenticación por el dispositivo móvil principal en su memoria volátil,

- un paso (56) de transmisión del dato de autenticación por el dispositivo móvil principal al ordenador,

- un paso (58) de autenticación en la aplicación a través del dato de autenticación.

7. Procedimiento de autenticación implementado por un sistema de autenticación según la reivindicación 6, caracterizado por que el paso (58) de autenticación en la aplicación comprende un subpaso de copia de la contraseña aleatorizada en un campo de texto de la aplicación, y un subpaso de borrado por parte del usuario de los caracteres añadidos por el módulo de aleatorización, de modo que la contraseña mostrada corresponda a la contraseña de la aplicación.

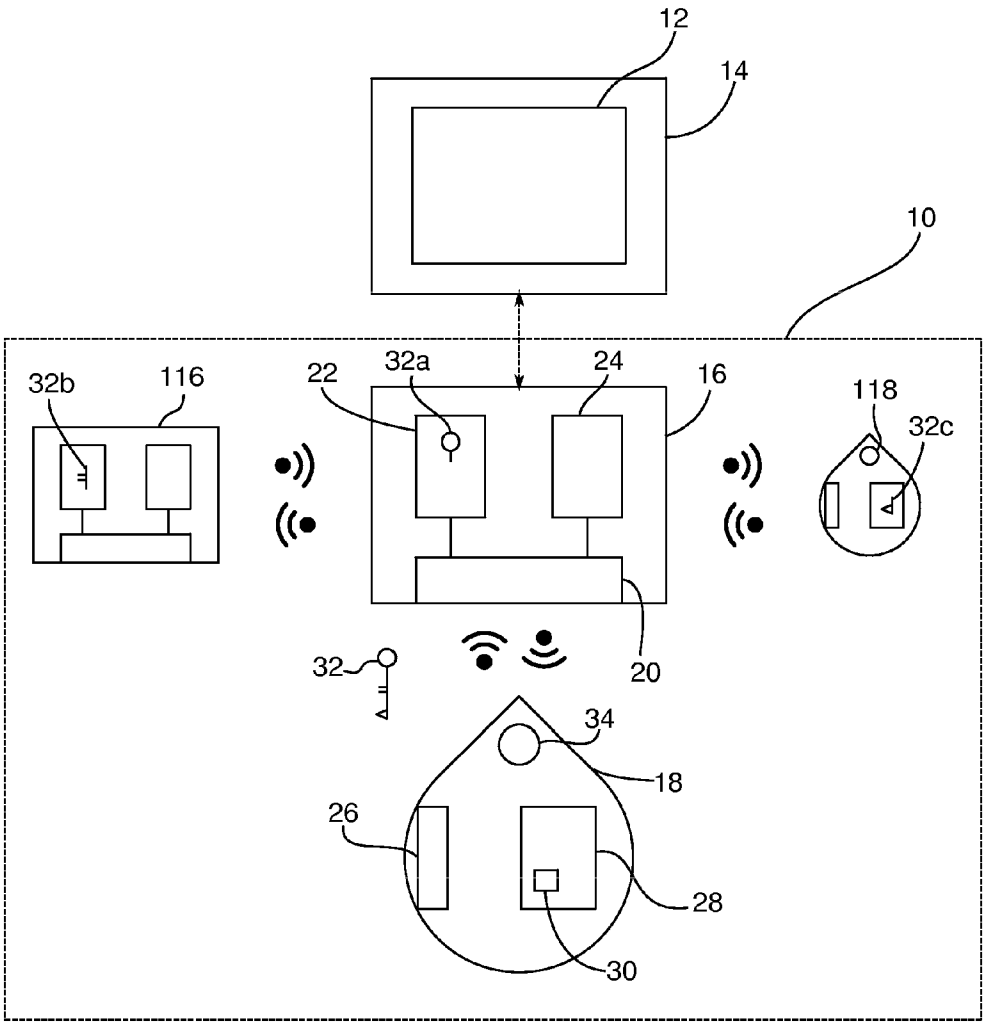

Fig.1

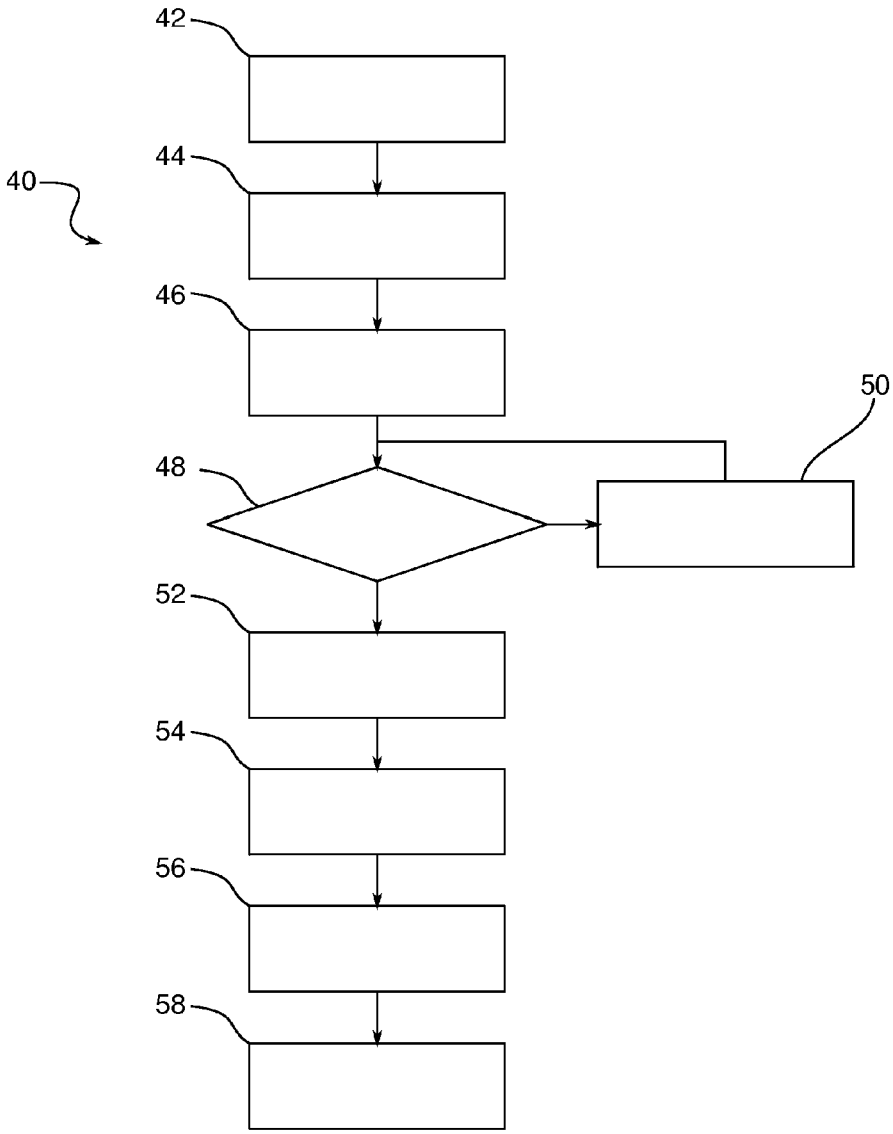

Fig.2