(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 363 268**

(51) Int. Cl.:
G06F 21/20 (2006.01)
H04L 29/06 (2006.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **06786402 .5**
(96) Fecha de presentación : **05.07.2006**
(97) Número de publicación de la solicitud: **1920380**
(97) Fecha de publicación de la solicitud: **14.05.2008**

(54) Título: **Dispositivo de almacenamiento masivo con carga automática de credenciales.**

(30) Prioridad: **08.07.2005 US 697906 P**
27.12.2005 US 319259
27.12.2005 US 319835

(45) Fecha de publicación de la mención BOPI:
28.07.2011

(45) Fecha de la publicación del folleto de la patente:
28.07.2011

(73) Titular/es: **SANDISK CORPORATION**
601 McCarthy Boulevard
Malpitas, California 95035-7932, US

(72) Inventor/es: **Gonzalez, Carlos J.;**
Ferchau, Joerg y
Jogand-Coulomb, Fabrice

(74) Agente: **Carpintero López, Mario**

DESCRIPCIÓN

Dispositivo de almacenamiento masivo con carga automática de credenciales

Campo de la invención

La presente invención se refiere en general a dispositivos portátiles de almacenamiento masivo, tales como tarjetas de memoria y unidades portátiles de memoria flash de bus serie universal ("USB"), utilizadas para almacenar y transferir archivos de gran tamaño a dispositivos digitales o desde ellos; y más concretamente, a los mecanismos de seguridad y control de acceso implementados en los dispositivos, para acceder a dispositivos y también a otras instituciones.

Antecedentes de la invención

Tener que recordar contraseñas es una molestia. El ordenador de la oficina necesita un nombre de usuario y una contraseña. Cada cuenta de correo electrónico necesita un nombre de usuario y una contraseña, como también cada una de las cuentas en línea. Si la seguridad no fuera un problema, cualquiera optaría por tener un solo nombre de usuario y una sola contraseña para todas las cuentas.

Pero la seguridad es un problema serio y consecuentemente, la gestión de las contraseñas y el acceso a las cuentas también lo es. Varios de los enfoques actuales enfrentan este serio problema en un intento de hacer las contraseñas más fáciles de recordar, o bien más fuertes y resistentes a la hora de resultar comprometidas.

Uno de estos enfoques es la contraseña de un solo uso ("OTP"). En general, una contraseña de un solo uso es un valor que puede utilizarse para acceder al sistema una vez, antes de que cambie. En otras palabras, se actualiza regularmente (a una cierta frecuencia definida) sin que el usuario tenga que cambiarla. Esto quiere decir que el usuario envía un único valor (contraseña), que se utiliza una sola vez, y el sistema al cual este quiere acceder, verifica que se trata del valor que debe ser. Normalmente esto se logra con un pequeño dispositivo o "token", que genera la contraseña del usuario basándose en un algoritmo predecible. La entidad validadora del sistema utiliza el mismo algoritmo predecible, y si a los algoritmos se les da el mismo valor semilla, el sistema "sabe" de esa manera cuál debe ser el valor en cada instante (o cuenta) de la contraseña de un solo uso del usuario, siempre cambiante. La manera más común de que se actualicen estos tokens requiere que el usuario lea el valor en una pantalla y lo introduzca en el ordenador. Otro mecanismo recientemente desarrollado permite al token transmitir el valor directamente al ordenador. Las dos implementaciones y en general, la contraseña de un solo uso, proporcionan un alto nivel de seguridad, pero necesitan que el usuario lleve encima un token para la generación de los valores de la contraseña de un solo uso. Los tokens son una forma de autenticación de dos factores, siendo uno de los factores el secreto del usuario (contraseña o pin) y el segundo factor, el valor OTP junto con el hardware (token) necesario para producirlo.

Otro enfoque utiliza un dispositivo de gestión de contraseñas. Tal dispositivo es capaz de realizar un seguimiento de varias contraseñas y números de cuenta de un usuario y enviar la(s) contraseña(s) adecuada(s) a cada cuenta de usuario. Por ejemplo, el usuario puede tener una contraseña maestra para acceder al dispositivo y cuando el dispositivo verifica la contraseña maestra del usuario, puede enviar la contraseña real para una cuenta determinada cuando se conecta a un ordenador de acogida. El usuario puede introducir sus distintas contraseñas o las contraseñas pueden insertarse en el dispositivo de gestión de contraseñas. Uno de estos dispositivos de SafeNet® (anteriormente, Rainbow Technologies) se conoce como iKey™ y también tiene capacidades de encriptado, con la generación de claves asociada.

Cada uno de estos enfoques carece de algo y por tanto, no ha logrado un alto nivel de aceptación en el gran público. Los tokens OTP se utilizan sobre todo para controlar el acceso a redes corporativas y no han tenido una amplia aceptación a la hora de usarse en sistemas de amplia disposición entre el gran público, p. ej. proveedores de correo electrónico o subastas en línea, etc. Los dispositivos de gestión de contraseñas actualmente disponibles carecen del nivel de seguridad de los tokens y sistemas OTP.

Cada uno de estos enfoques requiere la utilización de un dispositivo especializado, o en otro caso, no tiene capacidad de generar contraseñas de un solo uso para distintas instituciones al tiempo que mantiene la seguridad de las contraseñas, con sus algoritmos y semillas asociados. Por ejemplo, muchos incluyen un token o dispositivo USB de cadenas de claves para un solo fin. Llevar encima este dispositivo a todas partes supone un inconveniente y limita la aceptación del usuario, especialmente en el caso de un usuario versado en tecnología, que puede estar portando también un teléfono móvil, un reproductor musical, una PDA o Blackberry, una cámara digital u otros múltiples aparatos electrónicos.

Por tanto, se necesita un dispositivo práctico y multipropósito, que integre la generación de contraseñas de un solo uso como parte de un sistema sólido de gestión de seguridad y contraseñas.

La publicación de la patente de Estados Unidos US 2002/0145632 divulga la utilización de servicios de red desde un ordenador de acogida, con ayuda de software cargado desde un dispositivo de almacenamiento portátil, p. ej. un token USB. En esta solicitud de patente, el software cargado desde el dispositivo de almacenamiento portátil y que

se ejecuta en el ordenador de acogida está descrito como "keylet". Un keylet inicial se lanzará automáticamente, y ejecuta la autenticación entre el usuario y el propio dispositivo de almacenamiento portátil. Se pueden cargar otros keylets desde el dispositivo de almacenamiento portátil para ejecutarse en el PC de acogida. Los keylets de web pueden usarse para acceder a servicios web y para proporcionar automáticamente la información de registro correcta desde el dispositivo de almacenamiento portátil, para el servicio web al que se accede. Puede cargarse un navegador web propietario desde el dispositivo de almacenamiento portátil. Un keylet concreto puede instalar una barra publicitaria visible permanentemente, por ejemplo en el navegador web. Esta barra publicitaria puede proporcionar enlaces a otros keylets y servicios de red. Un keylet puede funcionar para descargar de la red contenido transferido y mostrarlo en la barra publicitaria. Se divulga un software de inicialización para llevar a cabo la configuración inicial de la clave, incluyendo la configuración de la información de autenticación de usuario y la adquisición de certificados encriptados que residirán en la clave. Sin embargo, el documento no especifica cómo tiene lugar la adquisición de los certificados.

El documento menciona que se pueden utilizar varias configuraciones de contraseña, pero no dice nada respecto a la autenticación de contraseñas de un solo uso. Además, el documento no sugiere la implementación de las funcionalidades del software de inicialización en una keylet descargada automáticamente.

RSA Security Inc ha publicado un conjunto de especificaciones en abierto para la integración de contraseñas de un solo uso en sistemas de empresa: "Open Specifications Integrate One-Time Passwords with Enterprise Applications", XP002415772; "Cryptographic Token Key Initialization Protocol V1.0 Draft 3", XP002416268; "OTP-WSS-Token: Web Services Security One-Time-Password (OTP) Token Profile, Version 1-0d3", XP002416269; "A CryptoAPI Profile for One-Time Password Tokens V1.0 Draft 2", XP002416270. El documento XP002416268 especifica cómo inicializar una contraseña de un solo uso con un secreto necesario para la autenticación. Sin embargo, XP002416268 no especifica cómo está provista la aplicación que funciona en el ordenador de acogida, necesario para la inicialización de la clave.

Resumen de la invención

La invención se define como se define en las reivindicaciones independientes anexas.

La presente invención integra una sólida seguridad y la comodidad de la gestión de contraseñas en un dispositivo portátil de almacenamiento masivo. Puesto que el usuario generalmente ya tiene un dispositivo portátil de almacenamiento masivo para su utilización en cámaras digitales, reproductores musicales, PDA o similares, la seguridad y comodidad añadidas no suponen una gran carga para el usuario. Ello facilita la gran penetración de esquemas de contraseñas de un solo uso muy seguros y da como resultado la reducción significativa del riesgo respecto a aplicaciones sensibles, como la banca en línea. Como un dispositivo portátil de almacenamiento masivo seguro puede almacenar programas y otros datos seguros, la generación de OTP *y* la gestión de contraseñas pueden integrarse en una cómoda plataforma.

Una de las barreras que tiene el adoptar un sistema de autenticación de dos niveles en el espacio de consumo es la necesidad de que el usuario transporte un token exclusivamente para llevar a cabo una operación de autenticación. Una manera de eliminar la carga que supone tener que transportar múltiples dispositivos especializados, es integrar estas funciones en un dispositivo que una persona pueda tener y/o llevar encima por otras razones. Ejemplos de tales dispositivos de almacenamiento masivo pueden ser: un dispositivo de almacenamiento masivo flash USB o una tarjeta de memoria flash de almacenamiento masivo, como una tarjeta flash compacta "CF", una tarjeta SD, una tarjeta MMC, una tarjeta XD, un lápiz de memoria, una tarjeta Trans-Flash, o similares, que se utilizan normalmente para guardar datos, y más recientemente, para guardar y transportar aplicaciones. Tal dispositivo, según la presente invención, lleva a cabo las funciones básicas de OTP y lleva una aplicación cliente que puede lanzarse desde el dispositivo de almacenamiento masivo y ejecutarse en el ordenador de acogida. La aplicación cliente es responsable de interactuar con el dispositivo para llevar a cabo la operación de OTP y extraer el valor de OTP del dispositivo. En otra realización, el propio cliente lleva a cabo las funciones OTP y guarda y recupera información como la cuenta hacia y desde el dispositivo, según sea necesario. En cada caso, la información estaría almacenada de forma segura, y protegida adecuadamente mediante encriptado, por ejemplo.

En una realización, se puede utilizar un dispositivo de almacenamiento masivo único para autenticar una serie de instituciones independientes, manteniendo una serie de semillas independientes y pares de cuentas en el dispositivo, cada uno de ellos para autenticar de forma independiente una institución determinada. De forma alternativa, la autenticación de múltiples instituciones puede lograrse con una sola semilla y una sola cuenta, empleando una ubicación central que verifique la información de autenticación. En cada caso, el valor semilla de las semillas puede cargarse en el dispositivo o en el cliente de manera segura, bien durante la fabricación del dispositivo o bien remotamente, con preferencia a través de un canal seguro. Los canales seguros son bien conocidos en el estado de la técnica y generalmente implican un protocolo de comunicación en el cual se encripta la comunicación entre dos entidades con una clave solo conocida por aquellas dos entidades. Normalmente, la clave es del tipo clave de sesión, que se establece con un protocolo de intercambio de claves predefinido entre las dos entidades.

Una de las preocupaciones que rodean a los sistemas de autenticación para uso particular tiene que ver con la facilidad en el uso y la simplicidad del sistema. Es típico que la seguridad añada un nivel de complejidad tal que

suponga una barrera a la hora de adoptarla. Uno de los objetivos en el diseño de tales sistemas es lograr un nivel de simplicidad tal que haga casi transparente al usuario los aspectos relacionados con la seguridad y la interacción del usuario. Para este propósito, en la presente invención la seguridad se trata en segundo plano, como parte de las actividades normales del usuario.

Esta invención implica la integración de las funciones de OTP directamente en el registro de usuario durante la operación, de manera que el usuario preferiblemente no participa en la ejecución de la autenticación OTP tras la inscripción y/o activación inicial. En concreto, en las realizaciones preferidas, las funciones OTP se integran en un dispositivo de almacenamiento flash USB u otro dispositivo de almacenamiento extraíble de uso común, y la aplicación cliente también se almacena en el propio dispositivo. La aplicación cliente se lanza desde el dispositivo de almacenamiento y se ejecuta en el ordenador de acogida. La aplicación puede lanzarse bien manualmente por el usuario o bien el sistema puede configurarse para lanzar automáticamente la aplicación, tras la inserción del dispositivo en el ordenador central. Una vez lanzada, la aplicación cliente lleva a cabo las tareas para obtener un valor OTP desde el dispositivo de almacenamiento masivo y proporciona la identidad del usuario, credenciales, y un valor OTP al servidor, con el cual el usuario se está autenticando. Idealmente, esto se lleva a cabo bien de manera automática, si la aplicación cliente está especializada para operar con una sola institución, o bien se realiza mediante un click, utilizando un dispositivo de interfaz humana, tal como un ratón o un teclado, seleccionando un icono de la institución (logotipo corporativo) o un nombre de entre una lista.

En otra realización, el cliente puede estar activo en el ordenador de acogida y detectar si el usuario accede a una página web que se encuentra en la lista de instituciones inscritas, para activar el registro de la secuencia. La lista de instituciones puede mostrarse en una interfaz gráfica de usuario ("GUI") en forma de lista, de lista desplegable, de grupo de iconos, de grupo de logotipos corporativos, u otras representaciones de este tipo. La identidad del usuario y sus credenciales, y el localizador uniforme de recursos ("URL") u otra forma de dirección web están también ya almacenadas, idealmente, en el dispositivo extraíble de almacenamiento masivo para autenticación, y se recuperan para la autenticación. Si el dispositivo es compatible con una serie de semillas OTP independientes, o incluso si es compatible con una serie de instituciones independientes que utilizan las mismas semillas OTP, la identidad del usuario, sus credenciales y URL se seleccionan, idealmente, de una lista almacenada en el dispositivo, según la institución en concreto para la cual la persona se está autenticando. El sistema combina a la perfección las funciones de un gestor tradicional de contraseñas con un sistema de autenticación OTP, y lleva a cabo el registro y la operación de autenticación conjuntamente, con la sola pulsación de un botón. Aunque la ejecución de todas estas acciones con un simple click puede ser preferible en ciertas situaciones, en otras puede ser preferible hacerlo mediante varios clicks o mediante la introducción de datos por parte de otro usuario.

Para asegurar que ninguna otra persona pueda utilizar el dispositivo para autenticarse en caso de pérdida o robo, el dispositivo de almacenamiento masivo de la presente invención es de un tipo tal que no funcionaría sin que el usuario introdujera cierta información que identifica únicamente a la persona, como un PIN o contraseña, al menos una vez cuando se lanza la aplicación cliente. Existe una serie de procedimientos de identificación de usuario, tales como la biometría, la contestación a preguntas, etc. En una realización, el sistema puede emplearse para proporcionar información de usuario para la autenticación más de dos factores general y/o operaciones de gestión de contraseñas; de entre esta información, algunos datos pueden ser más sensibles que otros. El sistema puede diseñarse para separar esta información más sensible y pedir verificación al usuario, introducción adicional de un PIN o contraseña, u otra acción para asegurar que el usuario es consciente y autoriza que esta información sea proporcionada al sistema. Un ejemplo de ello podría ser la autorización o pago con tarjetas de crédito.

En otra realización, el cliente puede proporcionar la información de autenticación y del usuario a un servidor web que, cuando reciba las credenciales de usuario y la información de autenticación válidas, rellene automáticamente la las entradas típicas de la página web de registro, que se utilizan normalmente para registrarse sin esta autenticación de dos factores. Esta realización haría posible que una institución determinada mantuviera una única página web de registro, añadiendo un componente de sistema distinto para manejar la autenticación de dos factores. En este caso, la autenticación de dos factores puede ser diversas formas de autenticación que no se prestan fácilmente a un relleno tipo formulario, como hace la OTP, sino que en su lugar serían esquemas de autenticación, como una infraestructura de clave pública ("PKI"), que suelen involucrar operaciones de tipo pregunta-respuesta.

Como mejora del sistema, el dispositivo puede contener una lista de instituciones en las cuales se quiere inscribir el usuario para ser autenticado. Esta lista puede actualizarse de manera remota, bien a requerimiento del usuario o bien automáticamente, mediante la aplicación cliente. La lista puede estar organizada de tal forma que proporcione una posición preferente para las instituciones de pago, o el posicionamiento en la propia lista puede estar reservado solo a instituciones de pago. El sistema también puede rellenar las credenciales del usuario por él, si detecta que se ha abierto una página web concreta para la cual se han almacenado credenciales. Esto puede realizarse con un programa o rutina que monitorice el puerto utilizado para comunicarse con Internet o la WWW. El programa monitoriza al navegador instalado en el ordenador, y configura el navegador para realizar todas las comunicaciones de datos con Internet o WWW a través de un puerto específico que se monitoriza. La monitorización tendría lugar automáticamente en cualquier momento que el dispositivo de acogida se utilizara, y mantendría un archivo de todos los sitios web que están siendo visitados. Si se trata de un sitio web para el cual el sistema mantiene los credenciales del usuario, éste registrará al usuario.

Un procedimiento habitual de pirateo, normalmente conocido como "pishing" consiste en que al usuario se le engaña para que proporcione información confidencial en un sitio web que se enmascara como un sitio web auténtico. Hay una serie de maneras de contrarrestar esta forma de pirateo. La lista de instituciones participantes puede utilizarse como medio de proporcionar información adicional al sistema, como las URL válidas que pertenecen a una institución dada, la forma de autenticación o protocolos específicos empleados para la autenticación, etc. En una realización, la URL insertada en la lista de instituciones participantes puede utilizarse para limitar las URL en las cuales un usuario pueda inscribirse con el sistema. En una implementación de este tipo, la lista se descargaría al dispositivo preferiblemente desde un servidor remoto, por medio de un canal seguro, para evitar espionaje por parte de terceros. En otra implementación, el cliente puede requerir validación de una URL estableciendo un enlace con un servidor remoto y, preferiblemente, a través de un canal seguro, pidiendo la validación de la URL. El servidor remoto puede ser también, en otra realización, un servidor de autoridad o una entidad de validación tal como las que se pueden ver en las figs. 1 a 3. En otra realización más, la validación del sitio web puede llevarse a cabo mediante alguna forma de autenticación que utilice un procedimiento habitual, como PKI con certificados, etc. En una implementación, se añade seguridad al servidor web para asegurar que esté conectado un dispositivo válido, antes de iniciar el procedimiento de autenticación. En otra realización, la página web puede activar servicios en el PC, que si se trata de un Microsoft Windows OS puede ser tecnología ActiveX, para interactuar con el cliente de autenticación a la hora de determinar la presencia en el dispositivo. En una solución preferida, toda la validación tiene lugar de forma lógica entre el servidor remoto y el propio dispositivo, ejecutando el cliente local la facilitación de la comunicación.

Todos los sistemas antes mencionados incluyen un mecanismo simple para transferir los derechos de autenticación de un dispositivo a otro, así como la información y credenciales del usuario de un dispositivo a otro. La transferencia de los derechos de autenticación, que en una realización puede consistir en un identificador (ID) y semilla de dispositivo, y en otros, un certificado, clave u otra forma de información, puede llevarse a cabo añadiendo la información a una lista de dispositivos inactivos en el servidor, una eliminación de dicha información del dispositivo por medio de un protocolo seguro, y la provisión otra vez a un nuevo dispositivo, por medio de un protocolo seguro, si tiene éxito la identificación del usuario, con una eliminación de la lista de dispositivos inactivos. Se puede emplear un procedimiento similar en caso de que el usuario pierda el dispositivo, lo que conllevaría la invalidación de los antiguos ID y semilla del dispositivo en el servidor, y la provisión otra vez del mismo o un nuevo ID y semilla de dispositivo a un nuevo dispositivo.

Breve descripción de las figuras

La fig. 1 es una ilustración esquemática de un primer sistema según la presente invención.

La fig. 2 es una ilustración esquemática de un segundo sistema según la presente invención.

La fig. 3A es un diagrama de bloques de un dispositivo de almacenamiento masivo 100.

La fig. 3B es una ilustración del espacio de memoria de la memoria flash de almacenamiento masivo de la fig. 3A.

La fig. 3C es un diagrama del cliente y un generador de contraseñas de un solo uso del dispositivo de almacenamiento masivo 100.

La fig. 4 es una ilustración de las funciones del dispositivo de almacenamiento masivo 100.

La fig. 5A es una ilustración de las entidades e interacciones implicadas en la vinculación de ranuras del dispositivo y la activación de ranuras del dispositivo.

La fig. 5B es una ilustración de las entidades e interacciones implicadas en la autenticación de un dispositivo con una ranura vinculada.

La fig. 5C es una ilustración de las entidades e interacciones involucradas en la autenticación con una infraestructura de clave pública.

La fig. 6 es un diagrama de flujo de un procedimiento de uso del dispositivo de almacenamiento masivo 100 para inscribirse en instituciones, según una realización de la presente invención.

La fig. 7 es un diagrama de flujo de un procedimiento de uso del dispositivo de almacenamiento masivo 100 para registrarse en instituciones, según una realización de la presente invención.

La fig. 8 es un diagrama de flujo de un procedimiento de uso del dispositivo de almacenamiento masivo 100 para inscribirse en instituciones, según una realización de la presente invención.

La fig. 9 es un diagrama de flujo de un procedimiento de uso del dispositivo de almacenamiento masivo 100 para inscribirse en instituciones, según una realización de la presente invención.

La fig. 10A es un diagrama de flujo de una vinculación de ranuras de dispositivo, tal como se ve en la fase 905 de la fig 9.

La fig. 10B es un diagrama de flujo de la activación de ranuras del dispositivo, tal como se ve en la fase 910 de la fig 9.

La fig. 10C es un diagrama de flujo de la autenticación tal como se ve en la fase 915 de la fig 9.

Las figs. 11A-I son pantallas de la interfaz de usuario del cliente 320 según una realización de la presente invención.

Las figs. 12A-B son pantallas de la interfaz de usuario del cliente 320 según una realización de la presente invención.

Descripción

Los dispositivos de almacenamiento masivo son muy utilizados para almacenar contenido digital tal como fotografías, música, vídeos y documentos. También son lo suficientemente amplios como para almacenar aplicaciones de software extensas. Es típico que los dispositivos portátiles de almacenamiento masivo en la actualidad utilicen memoria flash con fines de almacenamiento, y tengan un factor de forma de una tarjeta de memoria o unidad USB. Estos dispositivos de almacenamiento masivo se distinguen de otros dispositivos portátiles en que están concebidos para almacenar muy poca información, tal como la que se requiere para propósitos de transacción o identificación. Los dispositivos de almacenamiento masivo también se distinguen de otros dispositivos con un propósito especializado, tales como las tarjetas de clave y los tokens utilizados para la autenticación, en que mientras los dispositivos especializados pueden tener pequeñas cantidades de memoria para almacenar información pertinente para la identificación del usuario, no están diseñados para almacenar frecuentemente y transferir lo que son archivos comparativamente grandes y a menudo encriptados de una manera rápida, fiable y repetible.

Por ejemplo, una tarjeta de memoria, realización de un dispositivo portátil de almacenamiento masivo, tiene que ser capaz de almacenar rápidamente imágenes con unas dimensiones de 5-20 megabytes o más. Una sola imagen obtenida en cámara digital puede necesitar un almacenamiento mayor en órdenes de magnitud del que tiene un dispositivo con propósito especializado como pueda ser una tarjeta inteligente, una tarjeta de claves o un token. Además, un dispositivo con un propósito especializado generalmente no es capaz de leer y escribir archivos con rapidez, ni mucho menos los archivos relativamente grandes utilizados en las cámaras y reproductores musicales, etc. Los dispositivos de almacenamiento masivo tienen controladores y firmware con rutinas que están optimizadas para leer y escribir muy rápido en los bancos de memoria. Además, muchos de los dispositivos portátiles de almacenamiento masivo poseen rutinas de seguridad y encriptado para malograr la copia no autorizada del contenido frecuentemente actualizado. Mientras que los tokens especializados pueden tener alguna forma de seguridad (para proteger la semilla y/o algoritmo), los datos de un token son normalmente estáticos y la seguridad no está diseñada para la protección contra la copia no autorizada o los archivos de usuario frecuentemente actualizados. El dispositivo de almacenamiento masivo de la presente invención también puede almacenar las semillas y otra información necesaria para la validación y autenticación en una zona de la memoria de almacenamiento masivo que no esté sujeta a mapeo lógico o físico, para que la información sea más fiable y pueda recuperarse con rapidez.

Las semillas también pueden cargarse en particiones ocultas del dispositivo. La carga de las semillas, dondequiera que estén almacenadas, solo tiene que ser posible si la entidad que desea cargar las semillas tiene los permisos y/o credenciales adecuados para hacerlo. En ciertas realizaciones, este permiso está contenido en una grabación de control de acceso, que será explicada más tarde.

La presente invención utiliza un dispositivo de almacenamiento masivo con fines de seguridad. El dispositivo dispone de características de seguridad integradas en el mismo que i) limitan el acceso a la información almacenada en el dispositivo, y ii) hacen que el dispositivo funcione como una especie de "clave" que permite el acceso a otros sistemas y datos de seguridad. La presente invención también incluye un sistema que utiliza un dispositivo de almacenamiento masivo para verificar las credenciales de un usuario. Una vez verificadas, al usuario se le permite el acceso a información a la cual no sería capaz de acceder de otra manera.

Normalmente, se han utilizado contraseñas estáticas para verificar las credenciales de un usuario. Sin embargo, una contraseña estática es fácil de hurtar y apenas proporciona protección, en especial teniendo en cuenta lo extendido del "pishing" de contraseñas y otra información personal hoy día. Como se ha comentado anteriormente en los antecedentes de la invención, también se han implementado sistemas con token OTP especializado. Llevar encima estos tokens especializados supone una carga, son costosos y no han tenido una amplia aceptación en el mercado. Estos tokens tampoco disponen de las funciones de almacenamiento masivo que tiene una tarjeta de memoria o una unidad USB.

Hoy en día, casi todo el mundo que posee una cámara digital, grabador de vídeo, PDA, reproductor musical portátil u ordenador personal, tiene una tarjeta de memoria o una unidad USB tamaño bolsillo, llamado algunas veces "lápiz de memoria". La presente invención elimina la barrera de entrada que supone necesitar un token especializado separado (u otro dispositivo especializado) para implementar una OTP. Si un usuario no tiene que llevar encima varios dispositivos, sino que en su lugar utiliza algo que ya posee, debería aumentar significativamente la aceptación y utilización de la autenticación de OTP y de dos factores. Esto trae como resultado mejores medidas de seguridad y menos riesgo de fraude en el comercio electrónico y en otros sectores.

Las realizaciones de esta invención comprenden un dispositivo de almacenamiento masivo, como un dispositivo de almacenamiento flash USB, con funciones de OTP y un cliente en el dispositivo, que cuando es seleccionado por el usuario, enlaza automáticamente con la página web de la institución adecuada, introduce las credenciales del usuario, lleva a cabo la transacción de OTP con el dispositivo, e introduce el valor OTP en la página web, llevando a cabo toda la operación perfectamente y con un solo click por parte del usuario.

El aumento de las medidas de seguridad tiene una importancia crucial, pues el robo de identidades y el fraude se están convirtiendo cada vez más en una amenaza para el crecimiento de la actividad económica en internet. Los bancos, corredurías y otras instituciones financieras buscan soluciones que les permitan generar más actividad en línea, dado que los costes pueden ser tan reducidos como del 0,5% por transacción, comparados con la misma transacción realizada en una oficina sucursal. Del mismo modo, también se están desarrollando otros programas alrededor de las transacciones mercantiles en línea, la navegación segura para niños, etc. La necesidad fundamental de todas ellas es un medio que proporcione una sólida autenticación individual, que supere las formas más comunes de robo de identidad, que son el pishing y pirateo para obtener la identidad y credenciales del usuario y el robo físico o la copia de información en las tarjetas de crédito.

Una de las soluciones al problema, y uno de los aspectos de la presente invención, es proporcionar a los consumidores un medio o sistema para llevar a cabo una autenticación de dos factores, a la hora de registrarse o llevar a cabo transacciones en internet. La autenticación de dos factores, como queda implícito en su nombre, requiere que una persona se halle en posesión de los dos componentes del sistema, uno de los cuales es normalmente un dispositivo físico que identifica de forma única a la persona, y el otro es cierta información (un secreto) que solo es conocido por dicha persona y la entidad ante la cual la persona quiere autenticarse.

La entidad de autenticación o validación dispone habitualmente de una base de datos que contiene las credenciales de la persona, así como medios para verificar que la persona está en posesión de ambos componentes del sistema de autenticación de dos factores. La persona queda autenticada solo si es capaz de probar que posee ambos componentes, y de esta manera se malogra la forma más común de fraude, en la que un pirata puede saber la identidad de la persona y su secreto, dado que el pirata, que normalmente no es nunca una persona física, no está en posesión del componente físico. Del mismo modo, si la persona perdiera el dispositivo, o este fuera robado, nadie podría utilizar el componente físico para autenticarse falsamente sin conocer el secreto.

La presente invención incluye funciones criptográficas. En una realización preferida, incluye un motor criptográfico basado en hardware, aunque la función criptográfica pueda también basarse principalmente en un firmware. Tiene ventajas incluir algún mecanismo de criptografía para hacer mayor el esfuerzo que supondría piratear el sistema. Una de las ventajas que tiene el utilizar un motor criptográfico basado en hardware es que el firmware puede estar ligado al motor criptográfico, de tal manera que el firmware no se ejecute a menos que esté firmado por el hardware. Esto quiere decir que tanto el firmware como el hardware auténticos tienen que estar presentes para que funcione el dispositivo. Ni uno ni otro pueden ser reemplazados por piezas diseñadas para comprometer la seguridad del dispositivo y permitir la copia no autorizada de los contenidos.

Un PC o teléfono móvil tiene una arquitectura abierta que es vulnerable a toda forma de pirateo. Una ventaja de la presente invención es que instalando las capacidades criptográficas en el dispositivo de almacenamiento masivo, se puede utilizar una API muy segura y limitada, comparada con la que estaría presente en un ordenador personal ("PC") o un dispositivo electrónico típico, como un teléfono móvil. La API segura del dispositivo de almacenamiento masivo está diseñada de tal manera, que no existe forma de que los piratas utilicen una interfaz lógica normal a la hora de descubrir los secretos criptográficos que contiene el dispositivo de almacenamiento masivo. En esencia, el dispositivo de almacenamiento masivo de la presente invención está hecho para ser mucho más seguro que el dispositivo de acogida al que se acopla.

El dispositivo de almacenamiento masivo seguro trabaja en paralelo con un servidor o servidores ubicados remotamente, utilizando el dispositivo de acogida básicamente como pasarela. Aunque en ciertas realizaciones, el procesador del dispositivo de acogida ejecuta un cliente que está almacenado en el dispositivo de almacenamiento masivo, en las realizaciones preferidas, las operaciones criptográficas y de OTP solo se encuentran en el dispositivo de almacenamiento masivo, que puede fabricarse, tanto desde el punto de vista físico como el lógico, de una forma mucho más protegida. El dispositivo de almacenamiento masivo seguro trabaja conjuntamente con una entidad o entidades seguras ubicadas remotamente para conformar un sistema seguro. También son seguras las conexiones entre el dispositivo de almacenamiento masivo y las entidades seguras. La entidad segura ubicada remotamente es o comprende uno o más servidores remotos, que normalmente están protegidos físicamente contra el acceso, y tienen contramedidas de seguridad que limitan los tipos de interacciones que pueden llevarse a cabo a pesar de la interfaz externa.

A continuación se hará referencia a las figuras. La fig. 1 ilustra un sistema con el que se puede utilizar el dispositivo de almacenamiento masivo ("MSD") para la autenticación y gestión de contraseñas. El MSD 100 está conectado a un dispositivo informático de acogida 110 mediante la conexión 102. La conexión 102 puede ser cualquier tipo de conexión directa o inalámbrica. Algunos ejemplos de conexión inalámbrica son: OTA (over the air, en inglés), que utiliza enlaces de comunicación telefónica estándar; radiofrecuencias, algunas de las cuales implican rangos seleccionados y protocolos tales como wi-fi (802.11x) y Bluetooth; comunicaciones inductivas de campo cercano

("NTC") e infrarrojos. En las realizaciones preferidas actualmente, el MSD 100 toma forma como una unidad USB o una tarjeta de memoria, y por tanto, la conexión es directa y el MSD se interconectará con un receptáculo 104 del dispositivo de acogida. Como se discutirá más tarde con profusión de detalles más tarde, el MSD 100 tiene una memoria de almacenamiento masivo que se utiliza para almacenar y recuperar frecuente y rápidamente archivos de usuario de gran tamaño. Estos archivos de usuario pueden ser cualquier tipo de archivo y por lo común incluyen fotografías y música digital, como también programas ejecutables de software. En el caso de una conexión inalámbrica 102, el receptáculo 104 no sería un receptáculo físico sino un transceptor inalámbrico.

El dispositivo informático de acogida 110 puede ser cualquier tipo de dispositivo electrónico inteligente, y por razones de comodidad nos referiremos a él simplemente como dispositivo de acogida. Algunos ejemplos de dispositivo de acogida 110 serían un ordenador personal, un teléfono móvil o un dispositivo organizador y de correo electrónico ("PDA"). De hecho, el dispositivo de acogida puede ser cualquier dispositivo electrónico que pueda utilizarse para acceder a las cuentas del usuario y/o sitios de interés. El dispositivo de acogida 110 está conectado a una red, que a su vez está conectada con varias instituciones 118, y con otras entidades. Para simplificar, solo se muestra una institución 118. La red puede ser cualquier tipo de red de área amplia como Internet, y varios tipos de redes de teléfono móvil. Ciertas redes pueden utilizar también comunicaciones por satélite. Un tipo de entidad conectada a la red es una entidad validadora o de autenticación 124. La entidad 124 comprende uno o más servidores. En el caso de que el dispositivo de acogida 110 sea un PC, se puede establecer si se desea una conexión con una red privada virtual ("VPN") Además de la conexión de red 114, que conecta el dispositivo de acogida con la institución 118, y la conexión de red 116, que conecta el dispositivo de acogida con la entidad validadora 124, también puede existir una conexión no de red separada 122 entre la institución 118 y la entidad validadora 124. Por supuesto, las instituciones 118 también pueden comunicarse con entidades 124 a través de la red.

El dispositivo de acogida 110 y los componentes que interactúan con él se describirán a continuación con referencia a sus realizaciones actualmente preferidas, pero esta descripción no debería limitar de ninguna manera el alcance de la invención, que se definirá en las reivindicaciones anexas. En una realización preferida, el dispositivo de acogida 110 es un PC y el MSD 100 es un lápiz de memoria USB. Como se ha mencionado previamente, el ordenador de acogida también puede ser un organizador portátil, comúnmente conocido como PDA, o un teléfono móvil, una cámara digital o un dispositivo híbrido capaz de todas estas funciones, al que pueda acoplarse un dispositivo extraíble de almacenamiento. En una realización, el dispositivo de almacenamiento o subsistema puede estar insertado en el ordenador de acogida. Si un usuario desea acceder a una institución concreta, por ejemplo su banco en línea, conecta su MSD 100 a un puerto USB, se lanza el cliente que reside en el MSD en su PC y el cliente inscribe al usuario en su cuenta o cuentas bancarias. La entidad validadora 124 trabaja conjuntamente con la institución, el cliente, el PC y el MSD, para validar o autorizar al usuario y su MSD antes de permitir el acceso del usuario a la institución y registrarlo o inscribirlo en la institución. Por supuesto, cada institución 118 mantiene varias bases de datos de sus usuarios y sus números de cuenta y secretos (p.ej. contraseñas o números PIN). Del mismo modo, las entidades validadoras mantienen bases de datos que se necesitan para validar o autorizar a los usuarios y sus dispositivos. Estos procedimientos se explicarán más tarde en detalle. La aplicación cliente que reside en el MSD 100 puede ejecutarse mediante el procesador de un dispositivo de acogida 110 o MSD 100, y ello dependerá del nivel de seguridad requerido y de las configuraciones de ambos dispositivos 110 y MSD 100, así como la conexión 102 entre ellos. En el caso de que el dispositivo de acogida 110 sea un PC, se prefiere por el momento que el PC ejecute la aplicación cliente.

La fig. 2 es similar a la fig. 1, pero deja claro que la entidad validadora, que comprende uno o más servidores, puede basarse en las mismas premisas que la institución y sus equipos. Además, ilustra una autoridad 126. La autoridad es una entidad que proporciona información al MSD 100, necesaria para la validación o autorización y la inscripción del usuario. La autoridad 126 también será referida como servidor de autoridad 126. Por ejemplo, la autoridad 126 puede proporcionar las semillas necesarias para la generación OTP en el MSD 100. La autoridad 126 se muestra conectada al dispositivo de acogida 110 a través de la conexión de red 128. En esta situación, la autoridad puede cargar las semillas en el MSD 100 en cualquier momento durante la vida útil del MSD 100. También puede cambiar o eliminar las semillas si es necesario. En el caso de que las semillas estén cargadas de fábrica, la autoridad 126 podría conectarse directamente al MSD sin tener que conectarse por medio de una red y el dispositivo de acogida. La autoridad 126 podría ser gestionada por cualquier número de empresas u otras entidades. Una de estas entidades podría ser el fabricante o proveedor del dispositivo. Por ejemplo, si es SanDisk quien produce el MSD, el titular de la presente invención, la autoridad puede ser también SanDisk o un agente suyo. En otro ejemplo, la autoridad 126 puede ser un distribuidor de dispositivos, como un empleador. Asimismo, la institución 118 o la entidad validadora 124 puede proporcionar la información necesaria para la validación o autorización (p. ej. semillas OTP), directamente en vez de la autoridad 126 o en colaboración con ella.

La fig. 3A ilustra algunos de los componentes físicos de la MSD 100. La interfaz 304 envía y recibe datos y órdenes hacia el MSD 100 y desde éste, y comunica la información con el controlador 306. Como se ha mencionado anteriormente, la interfaz 304 en algunas realizaciones comprende los contactos eléctricos y/o un conector para el dispositivo de almacenamiento masivo, mientras que en otras realizaciones comprende un transceptor inalámbrico. En ciertas realizaciones, el suministro eléctrico para el MSD 100 también puede recibirse a través de la interfaz 304. El controlador 306 comprende un microprocesador y controla todas las operaciones de almacenamiento de los datos del MSD 100. Esto quiere decir que dirige todas las operaciones de lectura y escritura hacia la memoria de

almacenamiento masivo 308 y desde ella. Esta memoria es preferiblemente de tipo flash. Aunque el controlador y la memoria de almacenamiento masivo están representadas como conexión en serie, en realidad se conectan normalmente mediante un bus. También puede haber varios componentes en el bus, incluyendo memoria solo de lectura ("ROM") y memoria de acceso aleatorio ("RAM"). El MSD 100 es capaz de leer y escribir archivos encriptados en la memoria de almacenamiento masivo 308, lo cual, en las realizaciones preferidas se logra con un motor de encriptado en el controlador 306. El controle ejecuta el firmware para que funcione el MSD y est firmware puede estar ubicado en una ROM especializado, o alternativamente, almacenado en la memoria flash 308. El firmware se almacena preferiblemente en la memoria de almacenamiento masivo 308, para eliminar el coste que tiene que una ROM almacene el firmware. Almacenar el firmware que hace funcionar al MSD en la memoria flash 308, que carece de la protección intrínseca de una ROM, requiere de complejos mecanismos de protección para el MSD 100 que garanticen que las rutinas de protección anti-copia no pueden ser manipuladas o que no es posible sustituir el firmware completo con otro malintencionado o no seguro.

Como se aprecia en la fig. 3B, la memoria flash 308 tiene un área segura 308A donde se ubica el firmware y otra información esencial para el funcionamiento del MSD. En algunas realizaciones, el firmware está encriptado y no se ejecutará a menos que primero se determine que es auténtico.

En algunas realizaciones además, solo se puede escribir en el área segura 308 durante ciertos estados operativos del dispositivo. En general, esto también sirve para proteger al firmware de su manipulación o reemplazo, y para una mayor información sobre los estados operativos del dispositivo de almacenamiento masivo.

Estas protecciones necesitan tener lugar, pues el dispositivo de almacenamiento masivo se utiliza para el almacenamiento de archivos con fines generales, y en especial, para almacenar obras con derechos de autor que no pueden ser puestas a libre disposición para la copia. Por ejemplo, la música del MSD debe protegerse contra la copia no autorizada (lo cual no es un problema para los tokens especializados, que no se pueden utilizar para almacenar archivos de usuario). Esto tiene especial importancia si el firmware para controlar el dispositivo reside en la misma memoria que los archivos de usuario, más que en un dispositivo de almacenamiento especializado como un ROM, que es intrínsecamente más difícil de piratear.

Las ranuras lógicas 310A, 310B ... 310x se ubican en el área segura 308A. Estas ranuras también pueden estar en el área de almacenamiento de archivos 308B. Una ranura es un área de memoria lógica protegida que se utiliza para almacenar la información necesaria para registrar a un usuario en una institución. La información se encripta como medida de seguridad. Esto puede incluir la información de identificación del usuario, como su nombre, dirección, número de cuenta, etc., el secreto del usuario, como una contraseña o PIN, y la información necesaria para generar los valores de OTP, incluyendo los algoritmos y valores semilla para cada institución.

Cada institución tendrá su propia ranura. En ciertas realizaciones, cada cuenta dentro de una institución puede tener su propia ranura. El registro y la utilización de las ranuras se explicará más tarde en detalle. En una realización de la invención, las ranuras del MSD pueden estar ubicadas en un área del sistema de la memoria de almacenamiento masivo que no esté sujeta a mapeo físico o lógico, para que la información sea más fiable y pueda recuperarse rápidamente. Las semillas utilizadas para la generación de OTP también pueden almacenarse en un área de la memoria 308 que esté oculta respecto a un ordenador con acceso a los archivos del área de almacenamiento de archivos 308B. Esto puede hacerse dentro de una partición oculta ubicada en cualquier parte de la memoria 308.

Como se ha mencionado previamente, las semillas pueden cargarse en el MSD 100 en diferentes momentos. Es importante que una entidad que desee cargar semillas en la tarjeta sea verificada antes de que dicha carga tenga lugar. En una realización, esto se gestiona con una aplicación de almacenamiento segura ("SSA"), que es un módulo de seguridad del dispositivo de almacenamiento masivo. Esto puede interactuar con la aplicación cliente 320, a través de una capa de gestión en el dispositivo. El sistema SSA se asienta sobre el sistema de almacenamiento del MSD y añade una capa de seguridad para los archivos almacenados y otros datos, que en una realización incluye a las semillas.

Las particiones SSA son particiones ocultas (para el sistema operativo del dispositivo de acogida o el SO y el resto de las entidades) a las que solo puede accederse mediante el SSA. El sistema SSA preferiblemente no permitirá al dispositivo de acogida o a otra entidad el acceso a una partición SSA de otra forma que no sea mediante una sesión establecida al registrarse con un registro de control de acceso ("ACR"). De manera similar, preferiblemente el SSA no proporcionará información relativa a la existencia, tamaño y permiso de acceso de una partición SSA, a menos que esta petición venga a través de una sesión establecida por una autoridad o entidad adecuada.

Los derechos de acceso a las particiones se derivan de una lista de permisos que se encuentra en el ACR. Un ACR también puede contener el algoritmo de registro, las credenciales y un procedimiento de autenticación de una entidad o que se vaya a utilizar con una entidad. Cuando se crea una partición, el dispositivo de acogida proporciona un nombre de referencia o ID para dicha partición. Esta referencia se utiliza para las siguientes órdenes de lectura y escritura de la partición. Por tanto, en una realización de este tipo, cuando una entidad desee cargar una semilla en el MSD, necesitará el permiso adecuado y/o el algoritmo de registro, credenciales y procedimiento de autenticación adecuados.

La fig. 3C ilustra las funciones divididas de las realizaciones preferidas del MSD 100. En las realizaciones preferidas, la aplicación cliente 320 lleva a cabo muchas funciones, pero no la generación de OTP. En las realizaciones preferidas, como se ha explicado anteriormente, el cliente se ejecuta en el dispositivo de acogida (aunque esté almacenado en el MSD), mientras que la generación de OTP se lleva a cabo en el MSD. El generador OTP 330 está mejor protegido en el entorno seguro del MSD 100, cuando se compara con los entornos relativamente abiertos y potencialmente inseguros que pueden estar presentes en diversos dispositivos de acogida. El cliente 320 pedirá y después recogerá el valor OTP generado por el generador de OTP 330. El generador de OTP 330 puede utilizar múltiples algoritmos diferentes para proporcionar más seguridad y funciones que los anteriores tokens OTP, solo capaces de utilizar un algoritmo sencillo introducido en el momento de la fabricación. Por ejemplo, el generador de OTP 330 puede utilizar un único valor que genera un algoritmo para cada institución. El generador de OTP puede implementarse en la lógica del controlador 306, en un dispositivo lógico programable o en una circuitería especializada separada. La circuitería especializada puede implementarse en un ASIC o con componentes de circuitería a nivel de placa.

El cliente 320 también comprende la interfaz del dispositivo 320A, la interfaz de usuario 320B, el gestor de autenticación 320C y el gestor de provisión 320D. El cliente 320 registra perfectamente a un usuario en las instituciones que este elige, basándose en la interacción del usuario con la interfaz de usuario 320A. La interfaz de usuario acciona la interfaz del dispositivo, el gestor de autenticación y el gestor de provisión, sin que el usuario tenga que conocerlo o intervenir.

La fig. 4 ilustra las funciones multipropósito del dispositivo 100. El MSD 100 posee funciones de almacenamiento masivo. Esta es la razón por la cual un usuario normalmente tiene un MSD 100, para almacenar sus archivos en un cómodo dispositivo del tamaño de un bolsillo. Ahora, la presente invención añade la comodidad de un gestor de cuentas y la inscripción. Esto involucra tanto la gestión de contraseñas como la gestión de autenticación. La gestión de autenticación incluye verificar que tanto el usuario como el dispositivo son quienes pretenden ser y están autorizados a acceder a instituciones seguras. La gestión de autenticación implica el uso de identificadores de dispositivo específicos y también las contraseñas de un solo uso generadas por el generador de OTP 330. El que se añada la seguridad de la generación de OTP y la autenticación de dos factores a un dispositivo que el usuario ya posee debería aumentar mucho la adopción del uso de OTP. El que se añada la comodidad de gestionar las múltiples contraseñas que una persona suele tener, también debería hacer mucho más interesante y valioso un dispositivo de este tipo al usuario. El aumento de la seguridad, las funciones y la comodidad dará como resultado un nivel de aceptación más alto para la autenticación de dos factores en las instituciones seguras, así como entre los usuarios.

La complejidad de los procedimientos se describirá en detalle a continuación, en relación con las figs 5A – 10C.

La fig. 6C describe dos fases principales. Primero, en la fase 604, el MSD 100 recibe una o más semillas de OTP mientras el dispositivo está sobre el terreno, o en otras palabras, cuando ha sido vendido y está en posesión del usuario. En una realización, en la tarjeta se recibe una semilla por institución. En otras realizaciones, se utiliza una semilla para generar valores para dos o más instituciones. Aunque se pueden pre-cargar varias semillas en el dispositivo antes de que sea vendido al usuario o a un intermediario, se prefiere que las semillas se carguen sobre la marcha. Más tarde, en la fase 608, se utilizan la(s) semilla(s) recibida(s) para inscribirse en diversas instituciones con el dispositivo de almacenamiento masivo 100. Antes de que se carguen las semillas sobre la marcha, en ciertas realizaciones, el cliente puede verificar que el MSD conectado al dispositivo de acogida es capaz de llevar a cabo la necesaria generación de OTP. Una manera de hacerlo es con ActiveX.

Las figs. 5A y 5B y los diagramas de flujo de las figs. 7 – 10C deben ser vistas en conjunto. La fig. 5A muestra la interacción entre cada una de las entidades involucradas en la vinculación de ranuras del dispositivo y la activación de ranuras del dispositivo: usuario final 99, MSD 100, cliente 320, institución 118 y entidad validadora 124. Antes de que el MSD 100 pueda utilizarse para acceder a una institución en concreto, se lleva a cabo la vinculación y activación de ranuras del dispositivo. La fig. 5B muestra la interacción entre cada una de las entidades involucradas en el acceso a una institución, una vez que una ranura del MSD 100 ya está vinculada y activada. Las entidades mostradas en las figs. 5A y 5B son básicamente las mismas, pero se utiliza y muestra una función distinta del cliente 320. Por ejemplo, en la fig 5B, el gestor de autenticación 320C y la interfaz de usuario 320B del cliente están involucrados en los procedimientos, al tiempo que el manager de provisión 320D del cliente 320 está activo durante la vinculación de las ranuras del dispositivo y su activación, que se ven en la fig. 5A . La base de datos institucional 120 de la institución 118 también se muestra como una entidad lógica separada, aunque es parte de la institución 118.

La fig. 7 es un diagrama de flujo que ilustra las fases principales que utilizan el MSD 100 para acceder a una institución, a alto nivel. En la fase 704, tras conectarse el MSD 100 al ordenador, se lanza el cliente. El cliente puede lanzarse por el usuario o bien puede lanzarse automáticamente cuando se detecte la conexión con el ordenador. Después, en la fase 708, el usuario selecciona la institución a la que desea acceder a pesar de la interfaz de usuario del cliente. Algunas de las pantallas de la interfaz de usuario pueden verse en las figs. 11-12 y se describirán más adelante. En general, la selección se hará por medio de los dispositivos de interfaz humana del ordenador, cada vez que se lance el cliente. Sin embargo, el usuario puede configurar el MSD 100 para que acceda automáticamente a la institución cuando se detecte la conexión y se lance el cliente.

En la fase 712, el MSD 100 genera un valor OTP para cada una de las instituciones seleccionadas. Cada institución puede tener una única semilla y algoritmo para la generación de OTP. En la fase 716, el cliente se conecta a las instituciones seleccionadas. Una vez conectado, el cliente entonces presenta la información necesaria para registrar al usuario en las instituciones seleccionadas. Esta información comprende la información de identificación del usuario, tal como el nombre, número de cuenta o ID de usuario; la información del secreto del usuario como su cuenta o PIN y el valor de OTP para la institución en concreto, si esta institución es una de las que requieren un valor de OTP para registrarse en ella. La información puede recopilarse desde una página de la interfaz de usuario del cliente que el usuario rellena, o puede recopilarse al monitorizar las acciones de un usuario en el momento en que introduce información en la página web de la institución. En otra realización, el cliente puede proporcionar la información de autenticación y del usuario a un servidor web que, cuando reciba las credenciales de usuario y la información de autenticación válidas, rellene automáticamente la las entradas típicas de la página web de registro, que se utilizan normalmente para registrarse sin esta autenticación de dos factores. Esta realización haría posible que una institución determinada mantuviera una única página web de registro, añadiendo un componente de sistema distinto para manejar la autenticación de dos factores. En ciertas realizaciones, también puede ser necesario el ID de dispositivo del MSD 100 para registrarse. En la fase 724, el usuario 99 y el dispositivo 100 son autenticados o validados y se registran al usuario/dispositivo en cada institución seleccionada. Por último, una vez ha sido registrado el usuario, puede acceder a la institución. En el caso de que el usuario acceda al sitio web de una institución, se presentan al usuario las páginas web de la institución en la fase 728. Por supuesto, las interfaces de la institución no se limitan a las páginas web, y el acceso a otras interfaces se encuentra dentro del alcance de la presente invención. Esto se hace especialmente relevante si el dispositivo de acogida 110 no es un PC.

La fig. 8 es un diagrama de flujo similar al de la fig. 7, pero en la fig. 8 una tercera parte, que es una parte distinta de la institución y el usuario/dispositivo, juega un papel en el registro del usuario dentro de la institución. Solo se describirán las fases que difieran de las de la fig. 7. En la fase 714 el cliente conecta el usuario / dispositivo / dispositivo de acogida con una 3ª parte en vez de con una institución, como en la fase 716 de la fig. 7. Esta 3ª parte mantiene las bases de datos de los usuarios, dispositivos, instituciones y toda la información necesaria para verificar la autenticidad y validez de un usuario y su dispositivo. Esto puede incluir la verificación de los valores de OTP generados por el MSD. En la fase 717, la 3ª parte autentica/valida al usuario/dispositivo. Una vez que esto tiene lugar, la 3ª parte presenta la información apropiada que se necesita para registrar al usuario en las instituciones seleccionadas en la fase 717. A 3ª parte puede presentar los valores de OTP generados bien al nivel de MSD o por la propia 3ª parte. El usuario es entonces registrado en la institución, en la fase 722.

Como se ha mencionado anteriormente, antes de que el MSD 100 pueda utilizarse para registrar a un usuario en los sitios que este seleccione, las ranuras del dispositivo deben estar vinculadas y activadas. El usuario y dispositivo deben autenticarse antes de que se complete el registro, como se ve en la fig.9 En la fase 905 se vincula una ranura 310 del MSD 100 con un servidor de la entidad validadora 124, que también puede ser referida como servidor de validación 124. Esta fase se describe en más detalle en el diagrama de flujo de la fig 10 y también se muestra en la fig. 5A. Después, en la fase 910 se activa la ranura. Este procedimiento de activación se describe en más detalle en el diagrama de flujo de la fig 10B y también se muestra en la fig. 5A. En la fase 915 se autentica el usuario y la ranura del MSD 100. Este procedimiento de autenticación o validación se describe en más detalle en el diagrama de flujo de la fig 10C y también se muestra en la fig. 5B.

La fig. 10A ilustra el procedimiento vinculación en detalle (fase 905 de la fig. 9). En la fase 918, la MSD primero se conecta al dispositivo de acogida 110. En la fase 920 se lanza el cliente. Después, en la fase 922 el usuario selecciona una institución en la cual se quiere inscribir. De nuevo, el usuario puede hacerlo él mismo en este momento o las instituciones pueden estar preseleccionadas desde la sesión previa del usuario. En la fase 924, se adjudica una ranura dentro del MSD 100 a la institución o cuenta seleccionada. En la fase 926 el cliente recupera el ID del dispositivo del MSD 100. Entonces, en la fase 928, un identificador único, que es referido como el ID del token, se crea a partir del ID del dispositivo y del ID de la ranura. En la fase 930, el MSD 100, en concreto, la ranura apropiada del MSD 100, se vincula al servidor de validación 128, utilizando el ID del token. En la fase 932 se recibe una semilla para la institución seleccionada, y entonces, esta se asigna a la ranura adjudicada en la fase 934. Las fases 924-934 se repiten para cada institución seleccionada en la fase 922.

La fig. 10B ilustra en detalle el procedimiento de activación de ranuras del dispositivo (fase 910 de la fig. 9). Una ranura de dispositivo puede activarse después de haberse vinculado. En la fase 940, el usuario introduce su nombre de usuario u otra información identificativa, y su contraseña u otro secreto. Después, en la fase 942, el generador de OTP 330 del MSD 100 genera uno o más valores de contraseña de un solo uso para la ranura que se está activando. En la fase 944, la ranura del MSD se activa con la institución, y entonces en la fase 946, la institución y/o el cliente piden la validación de la ranura/MSD/usuario al servidor de validación 124. Al mismo tiempo, la institución 118 y el servidor de validación 124 validan la ranura/MSD/usuario en las fases 948 y 950. Entonces y de manera optativas, en la fase 952 se les notifica al cliente y al usuario el éxito de la activación.

La fig. 10C ilustra en más detalle el procedimiento de autenticación de usuario y del dispositivo (fase 915 de la fig. 9). Esto también se muestra en la fig 5B. Cuando el dispositivo se activa, se vincula y asocia con una institución o cuenta. Esto se hace utilizando el ID del dispositivo y la información de la ranura. Ahora la institución necesita asociar el dispositivo y su contenido al nombre de usuario y contraseña, para poder autenticar al usuario con la información presentada en el dispositivo, además de la información específica del usuario (información identificativa

y secreto del usuario). En la fase 960, e MSD se conecta al dispositivo de acogida si es que no está ya conectado. A continuación, en la fase 962, se lanza el cliente si no está ya abierto y funcionando, y en la fase 964, el usuario introduce su información de identificación (p. ej. nombre de usuario, número de cuenta, etc.) y su secreto (p. ej. contraseña y PIN). Después, en la fase 966, el generador de OTP del MSD 100 genera un valor OTP para cada una ranura concreta. En la fase 968, el valor OTP, la información identificativa de usuario y el secreto del usuario se envían a la institución. Entonces, en la fase 970, la institución valida que el usuario tenga acceso a dicha institución. Esto involucra a las fases 970A y 970B. En la fase 970A, la institución valida la información identificativa del usuario y el secreto, con la(s) base(s) de datos de las instituciones. También en la fase 970B, valida el valor de OTP y el ID del token del MSD 100 con el servidor de validación 124. Si el usuario ha sido validado con éxito en la fase 970, en la fase 974 se le registra en la institución.

Como se ha mencionado, en otra realización, el cliente puede proporcionar la información de autenticación y del usuario a un servidor web que, cuando reciba las credenciales de usuario y la información de autenticación válidas, rellene automáticamente las entradas típicas de la página web de registro, que se utilizan normalmente para registrarse sin esta autenticación de dos factores. Esta realización haría posible que una institución determinada mantuviera una única página web de registro, añadiendo un componente de sistema distinto para manejar la autenticación de dos factores. En este caso, la autenticación de dos factores pueden ser diversas formas de autenticación que no se prestan fácilmente a un relleno tipo formulario, como hace la OTP, sino que en su lugar serían esquemas de autenticación, como una PKI, que suelen involucrar operaciones de tipo pregunta-respuesta.

La fig. 5C muestra una posible implementación de la realización que utiliza la infraestructura de clave pública para la verificación/autorización de credenciales. Puesto que las transacciones no pueden ser más seguras que el sistema en el que tienen lugar, el elemento más importante llega a ser el establecer una manera de que los corresponsales se localicen unos a otros y tengan confianza en que la clave pública que usan pertenece verdaderamente a la persona (o máquina) con quien o con la que quieren comunicarse. Una infraestructura de clave pública está diseñada para proporcionar esta confianza. Utilizando un elemento de datos llamado certificado digital o certificado de clave pública, que vincula una clave pública para identificar información sobre su propietario, la infraestructura está diseñada para crear el vínculo y gestionarlo para el beneficio de todos los miembros de la comunidad usuaria.

La PKI es una tecnología de autenticación. Utilizando la combinación de una clave secreta y la criptografía para una clave pública, PKI posibilita un conjunto de servicios de seguridad distintos que incluyen confidencialidad de los datos, integridad de los datos y gestión de claves. El fundamento o marco para la PKI se define en la recomendación ITU-T X.509 [X.509].

Las entidades finales se conciben a veces como usuarios finales. Aunque a menudo este resulta ser el caso, el término "entidad final" pretende ser mucho más genérico. Una entidad final puede ser un usuario final, un dispositivo como un router o un servidor, un procedimiento o algo que pueda ser identificado con el nombre del sujeto de un certificado de clave pública. Las entidades finales también pueden concebirse como los consumidores de los servicios relacionados con el PKI. En la presente invención, como se ve en la realización mostrada en la fig. 5, la entidad final es el dispositivo de almacenamiento masivo 100 o su usuario.

Las claves públicas se distribuyen en forma de certificados de clave pública por la autoridad certificadora ("CA") 550. El MSD 100 podría requerir un certificado, de modo que una institución 118 o una entidad validadora permitiera al usuario del MSD 100 inscribirse. Un certificado de una institución 118 también podría utilizarse para probar que la institución es auténtica, antes de que el MSD inscribiera al usuario en la institución. Los certificados de clave pública son firmados digitalmente por la CA 520 que los emite (que vincula de manera efectiva el nombre del sujeto con la clave pública). Las CA también son responsables de emitir listas de revocación de certificados ("CRLs") a menos que esta función haya sido delegada en un emisor de CRL aparte. Las CA también pueden estar involucradas en una serie de tareas administrativas tales como el registro de usuario final, pero a menudo estas se delegan a una autoridad de registro ("RA") separada, que es opcional y no se muestra en la fig. 5C. En la práctica, la CA 520 u otra CA también puede servir como respaldo de clave y utilidad de recuperación, aunque esta función también puede delegarse en un componente aparte. Las CA se conciben a menudo como la "fuente de confianza" en una PKI. Normalmente, las entidades finales están configuradas con una o más "anclas de confianza" que se utilizan así como punto de partida para validar una ruta de certificación dada. Una vez queda establecida la confianza mediante la interfaz PKI, puede tener lugar el registro.

Las figs. 11A-I y 12A-B son pantallas de la interfaz de distintas realizaciones del cliente 320. Estas pantallas sirven para ilustrar la comodidad de la presente invención. Para un usuario, el procedimiento de registro se vuelve muy simple, aunque "entre bastidores" tienen lugar cálculos e interacciones complejas. Por ejemplo, el usuario no se da cuenta de que el dispositivo está sembrado para cada institución seleccionada y que la semilla es utilizada por un complejo algoritmo para generar un nuevo valor (OTP) para cada registro que se valida junto con otra información del usuario, de forma automática. La presente invención combina un nivel de seguridad muy alto con la automatización perfecta de la gestión de contraseñas. Esto puede incluir también una sola inscripción en ciertas realizaciones, en las que la información maestra del usuario se correlaciona automáticamente con todas las contraseñas y nombres de usuario individuales para las distintas instituciones. Existe una serie de procedimientos de identificación de usuario que pueden utilizarse con la presente invención, tales como la biometría, la contestación a preguntas, etc. En una realización, el sistema puede emplearse para proporcionar información de usuario para la

autenticación más de dos factores general y/o operaciones de gestión de contraseñas; de entre esta información, algunos datos pueden ser más sensibles que otros. El sistema puede diseñarse para separar esta información más sensible y pedir verificación al usuario, introducción adicional de un PIN o contraseña, u otra acción para asegurar que el usuario es consciente y autoriza que esta información sea proporcionada al sistema. Un ejemplo de ello podría ser la autorización o pago con tarjetas de crédito.

La fig. 11A muestra una pantalla de bienvenida, y la fig, 11B es una interfaz en la que el usuario puede rellenar su contraseña y nombre de usuario para acceder a una institución concreta. El usuario puede introducir una nueva institución o acceder a una institución que ha sido configurada previamente. En esta pantalla, el usuario puede introducir el ID del dispositivo o su MSD, aunque en las realizaciones preferidas el cliente recuperará esta información sin que el usuario tenga que introducirla. En la fig. 11C, una interfaz de usuario informa al usuario que el sistema está vinculando la MSD a su(s) cuenta(s). En este caso, la institución seleccionada es una institución financiera o un broker. Como se ve en la fig 11D, el usuario puede acceder a las múltiples cuentas que pueda tener en una institución concreta, y puede añadir, editar y eliminar cuentas. En la fig. 11E, se le pide al usuario que introduzca su contraseña maestra. Esta es una contraseña que el sistema más tarde correlaciona con todas las contraseñas restantes del usuario y su información de cuenta. Una vez el usuario ha sido vinculado, en una realización, solo tiene que introducir su contraseña maestra para acceder a su cuenta, y el procedimiento comenzará en la fig, 11D, en lugar de la 11A u 11B. En la fig. 11F, se le pide al usuario que espere mientras el sistema se conecta a su cuenta. Después, se informa al usuario de que ha sido conectado de forma segura a su cuenta, en la fig. 11G. En esta etapa, la página web u otra interfaz de la institución se abrirá en el dispositivo de acogida del usuario. Cuando el usuario finaliza el acceso a su(s) cuenta(s) puede hacer click en el botón de salida de la pantalla de la interfaz de usuario que se muestra en la fig. 11H. El usuario puede conectar entonces con cuentas adicionales, como se ve en la fig. 11I.

Las figs. 12A-B representan pantallas de la interfaz de usuario de otra realización del cliente 320. En la fig. 12A se muestran de manera simultánea en una pantalla de la interfaz de usuario los iconos que representan a una serie de distintas instituciones. El usuario puede añadir una institución, también referida como una "cuenta" y editar o eliminar una cuenta. El usuario puede añadir las instituciones manualmente o en otro caso, el usuario podría seleccionarla de una lista mantenida por el MSD. Esta lista podría actualizarse remotamente al MSD desde un servidor, bien bajo demanda del usuario o bien automáticamente, basándose en algún tipo de actualización programada. La lista también podría actualizarse en base a cualquier número de eventos, como también en base a la petición de inscripción del usuario. Haciendo click en los botones dentro de cada icono, el usuario también puede acceder o registrarse en la cuenta y cerrar la sesión de la cuenta o salir. Como se ve en la fig. 12B, cuando el usuario hace click en una cuenta concreta para abrirla, el cliente permitirá al usuario elegir entre sus cuentas en esta institución concreta, que también pueden ser referida como "subcuentas".

En una realización preferida, una vez que todas las cuentas mostradas se han configurado, el usuario solo tendría que introducir su contraseña maestra para el MSD y simplemente podría hacer click en el icono que corresponda a la institución en la que desea registrarse. En otras realizaciones, las contraseñas individuales y/o los ID de usuario tendrían que introducirse para aumentar la seguridad.

Las operaciones antes descritas en detalle respecto a la aplicación que facilita la inscripción, tendrían lugar de esa manera a la perfección y entre bastidores. Esto haría el manejo simultáneo del registro y la gestión de contraseñas muy cómodo al usuario, mientras que al mismo tiempo proporcionaría un alto nivel de seguridad que beneficiaría a los usuarios e instituciones por igual. Toda esta comodidad y seguridad se incorpora en un dispositivo que probablemente ya tiene un usuario. Esto se hace posible porque, al contrario que en los tokens especializados, se puede añadir el cliente a la memoria de almacenamiento masivo de un dispositivo de almacenamiento masivo de tamaño bolsillo. El dispositivo portátil de almacenamiento masivo posee una seguridad, tanto física como lógica, que es más sólida que en un entorno abierto como pueda ser un PC, y por tanto, el pirateo o "phishing" de la información es mucho más difícil. Además, al contrario que algunos dispositivos de almacenamiento masivo que *pueden* correlacionar diferentes contraseñas u otra información, la presente invención utiliza algoritmos y procedimientos que pueden generar valores de contraseña únicos que están en cambio constante pero se pueden verificar instantáneamente.

A pesar de las realizaciones de la invención descritas, debe entenderse que la presente invención no se limita a estas realizaciones ilustrativas sino que se define en las reivindicaciones anexas. Por ejemplo, para fines de almacenamiento masivo el MSD 100 puede utilizar un disco magnético mejor que una memoria de estado sólido de tipo flash, y se puede implementar cualquier forma de autenticación simétrica o asimétrica con fines de autenticación, para mejorar la seguridad tradicional de las contraseñas seleccionadas por el usuario.

REIVINDICACIONES

1. Procedimiento de acceso a cuentas de un usuario con un dispositivo de almacenamiento masivo (100); el procedimiento comprende:

detectar la conexión de un dispositivo de almacenamiento masivo (100) portátil con un dispositivo de acogida (110); proporcionar, el dispositivo portátil de almacenamiento masivo, almacenamiento masivo de datos que son independientes de la generación de contraseñas de un solo uso como las que se utilizan con reproductores musicales, cámaras digitales, PDA, ordenadores personales o similar; y tras esta detección:

lanzar una aplicación (320) que reside en el dispositivo portátil de almacenamiento masivo (100); dicha aplicación (320) hace que se establezca una conexión entre el dispositivo de acogida (100) y una primera entidad; en le que dicha aplicación, además: facilita la selección de una institución, haciendo que, una vez establecida la conexión, una semilla que se utiliza con un generador de contraseñas de un solo uso (330) implementado en el dispositivo portátil de almacenamiento masivo, se cargue en el dispositivo portátil de almacenamiento masivo (100) desde la entidad mientras está conectada con el dispositivo de acogida; haciendo que el generador de contraseñas de un solo uso genere una contraseña de un solo uso en del dispositivo portátil de almacenamiento masivo utilizando la semilla cargada, y obteniendo la contraseña de un solo uso del dispositivo portátil de almacenamiento masivo, y transmitiendo la contraseña de un solo uso a la institución seleccionada junto con la información de identificación del usuario, de modo que el usuario pueda acceder a su cuenta.

2. Procedimiento según la reivindicación 1, que también comprende el hacer que una serie de semillas adicionales que se van a utilizar con el generador de contraseñas de un solo uso (330) se carguen en el dispositivo de almacenamiento masivo (100) mientras está conectado, y que cada una de estas semillas adicionales se utilice con una cuenta o institución particular, y cada una de estas semillas se almacene en una partición oculta (308A) del dispositivo de almacenamiento masivo (100) que no es accesible mediante las órdenes estándar de lectura y escritura utilizadas por un sistema de archivos del dispositivo de acogida (110) para acceder a los datos dentro del volumen de almacenamiento del dispositivo (100).

3. Procedimiento según la reivindicación 2, en el cual, para que una entidad cargue una semilla debe establecerse que tiene permiso para cargar una semilla, para que cargue la semilla y acceda a la partición oculta (308A).

4. Procedimiento según las reivindicaciones 1, 2 ó 3, en el cual, la generación comprende calcular un valor con un algoritmo, y en el cual, la generación comprende el utilizar un algoritmo distinto para cada cuenta o institución a la que se quiere acceder.

5. Procedimiento según cualquiera de las reivindicaciones precedentes, que también comprende el vincular el dispositivo portátil de almacenamiento masivo (100) con una ranura (310A, 310B, 310X) del dispositivo portátil de almacenamiento masivo (100).

6. Procedimiento según cualquiera de las reivindicaciones precedentes, que también comprende el activar la ranura (310A, 310B, 310X).

7. Procedimiento según cualquiera de las reivindicaciones precedentes, que también comprende el hacer que el usuario y el dispositivo portátil de almacenamiento masivo (100) se autentifiquen.

8. Procedimiento según la reivindicación 5, en el que la vinculación comprende:

seleccionar una cuenta;
recibir un identificador de ranura;
recuperar un identificador de dispositivo en el dispositivo; y
crear un identificador único basándose en el identificador de la ranura y el identificador del dispositivo.

9. Procedimiento según la reivindicación 8, que también comprende el utilizar el identificador único para vincular el dispositivo de almacenamiento masivo (100) con un servidor de validación (124).

10. Procedimiento según la reivindicación 8, en el que el identificador de la ranura se recibe de un cliente (320D) almacenado en el dispositivo portátil de almacenamiento masivo (100) y ejecutado por el procesador del dispositivo de acogida (110).

11. Procedimiento según la reivindicación 8, en el que el identificador de la ranura se recibe de un cliente (320D) almacenado en el dispositivo portátil de almacenamiento masivo (100) y ejecutado por un procesador (306) del dispositivo de almacenamiento masivo (100).

12. Procedimiento según la reivindicación 6, en el que la activación de la ranura (310A, 310B, 310X) comprende:

hacer que el usuario identifique la información que el usuario introduce;
hacer que el usuario seleccione una cuenta, correlacionando la cuenta y el usuario con la ranura (310A, 310B,

310X).

13. Procedimiento según cualquiera de las reivindicaciones precedentes, que también comprende el recibir la semilla de una primera entidad antes de cargar la semilla.

14. Procedimiento según la reivindicación 1, en el cual, una conexión del dispositivo portátil de almacenamiento masivo (100) comprende el insertar el dispositivo portátil de almacenamiento masivo (100) en una toma (104) del dispositivo de acogida (110), y dicha toma (104) tiene contactos electrónicos dispuestos para la inserción y retirada frecuente del dispositivo portátil de almacenamiento masivo (100) por parte del usuario del dispositivo (100); en el cual, la aplicación (320) permite la selección de una institución (118) de entre una pluralidad de instituciones hacia las cuales el usuario desea autenticarse; y en el cual, hacer que se establezca una conexión entre el dispositivo de acogida (110) y una primera entidad, comprende el conectar con una autoridad (126); y en el cual, hacer que una semilla se cargue en el dispositivo portátil de almacenamiento masivo (100) mientras está conectado con el dispositivo de acogida (110) incluye el recibir, en el dispositivo de acogida (110), una semilla procedente de la autoridad (126) y almacenar la semilla en el dispositivo de almacenamiento masivo (100); y en el cual, hacer que el usuario identifique la información que se transmite a la institución seleccionada (118) comprende el introducir la información identificativa del usuario y la información del secreto del usuario, y hacer que la información identificativa del usuario y la información del secreto del usuario se transmita a la institución seleccionada (118); y en el cual, el procedimiento también comprende: recibir, en el dispositivo de acogida (110), un identificador de dispositivo de la autoridad (126) y almacenar el identificador de dispositivo en los dispositivos de almacenamiento masivo (100); almacenar un identificador de institución en el dispositivo de almacenamiento masivo (100); y almacenar una cuenta para su utilización con la semilla.

15. Procedimiento según la reivindicación 14, en el cual el dispositivo de acogida (100) ejecuta la aplicación.

16. Procedimiento según las reivindicaciones 14 ó 15, que también comprende el presentar al usuario una lista de instituciones (118) en las cuales inscribirse.

17. Procedimiento según las reivindicaciones 14, 15 ó 16, en el cual, seleccionar una institución (118) comprende el introducir un identificador de institución.

18. Procedimiento según las reivindicaciones 14, 15 ó 16, en el cual, seleccionar una institución (118) comprende el seleccionar una institución de una lista.

19. Procedimiento según la reivindicación 17, en el cual, el identificador de la institución comprende un localizador universal de recursos.

20. Procedimiento según la reivindicación 17, en el cual, el identificador de la institución comprende el nombre o un alias de la institución (118).

21. Procedimiento según una de las reivindicaciones 14 a 20, en el cual, la semilla se almacena en un formato encriptado.

22. Procedimiento según las reivindicaciones 14 a 21, en el cual, la aplicación (320) almacena el identificador del dispositivo en el dispositivo de almacenamiento masivo (100) .

23. Procedimiento según cualquiera de las reivindicaciones 14 a 22, en el cual, la información de identificación del usuario comprende información biométrica.

24. Procedimiento según cualquiera de las reivindicaciones 14 a 23, en el cual, el introducir la información identificativa del usuario y la información del secreto del usuario se hace en un formulario de la aplicación.

25. Procedimiento según las reivindicaciones 14 a 24, que también comprende aprender a ubicar las credenciales de seguridad y la información identificativa.

26. Procedimiento según cualquiera de las reivindicaciones 14 a 25, que también comprende asociar la información de identificación del usuario y el secreto del usuario con el identificador de la institución.

27. Procedimiento según la reivindicación 20, que también comprende asociar la semilla con el identificador de la institución.

28. Procedimiento según una de las reivindicaciones 14 a 27, en el cual, el dispositivo portátil de almacenamiento masivo (100) tiene una interfaz de bus serie universal.

29. Procedimiento según una de las reivindicaciones 14 a 28, en el cual, el dispositivo portátil de almacenamiento masivo (100) tiene un factor de forma de una tarjeta de memoria.

30. Procedimiento según una de las reivindicaciones 14 a 29, en el cual, la semilla se almacena en el dispositivo de almacenamiento masivo (100) en un formato encriptado.

31. Procedimiento según una de las reivindicaciones 14 a 30, en el cual, la semilla se almacena en una zona segura de la memoria utilizada para el almacenamiento masivo en el dispositivo de almacenamiento masivo (100).

32. Procedimiento según la reivindicación 31, en el cual, la semilla solo puede almacenarse mientras el dispositivo de almacenamiento masivo (100) se encuentra en ciertos estados operativos.

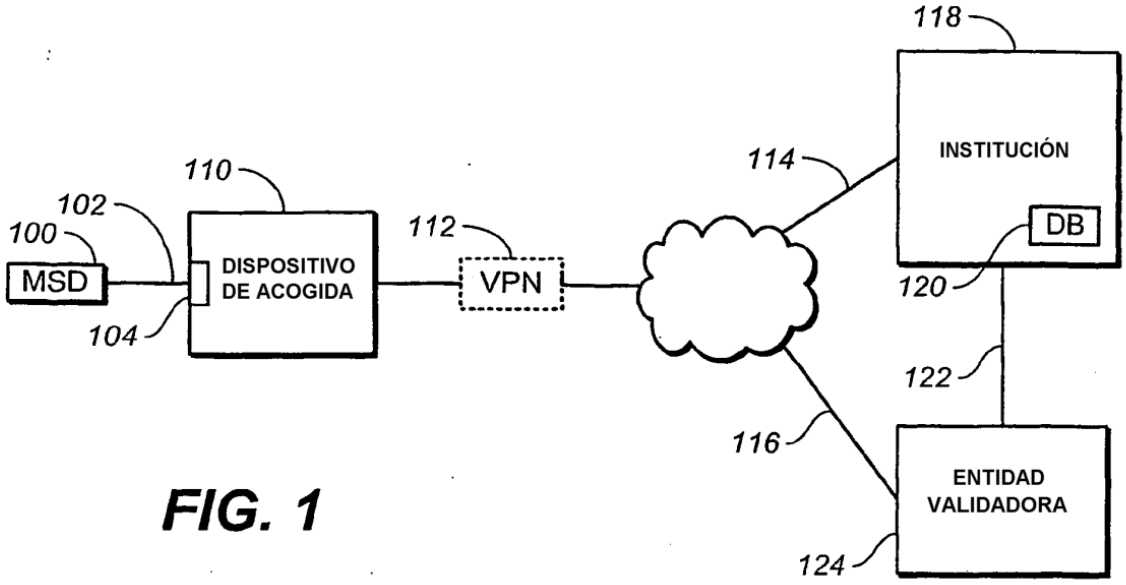

118
INSTITUCIÓN
DB
114
110
102
100
MSD
DISPOSITIVO
DE ACOGIDA
104
112
VPN
120
122
116
ENTIDAD
VALIDADORA
124

FIG. 1

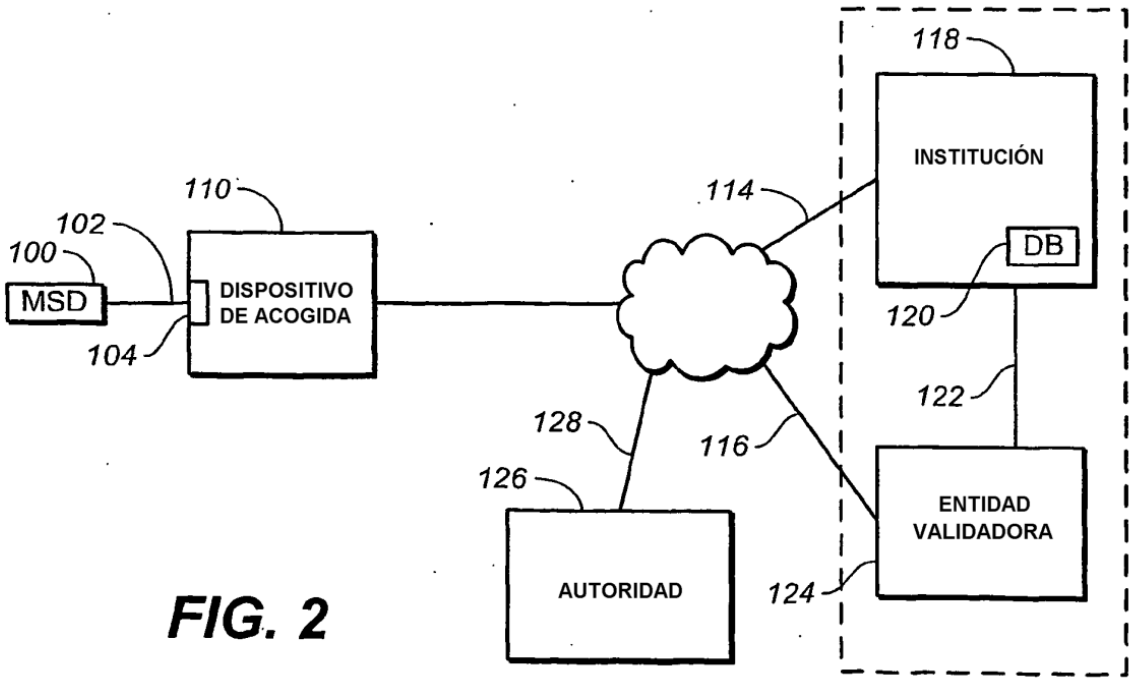

118
INSTITUCIÓN
DB
114
110
102
100
MSD
DISPOSITIVO
DE ACOGIDA
104
120
122
128
116
126
ENTIDAD
VALIDADORA
AUTORIDAD
124

FIG. 2

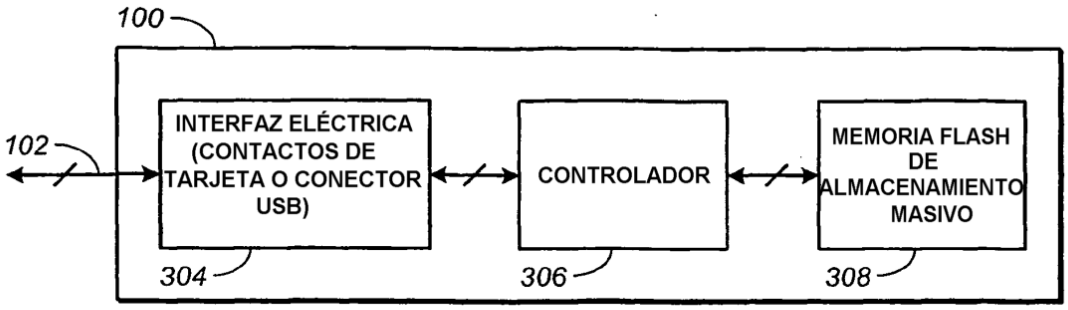


FIG. 3A

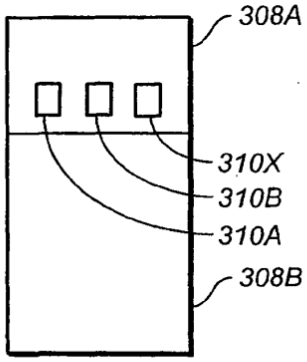


FIG. 3B

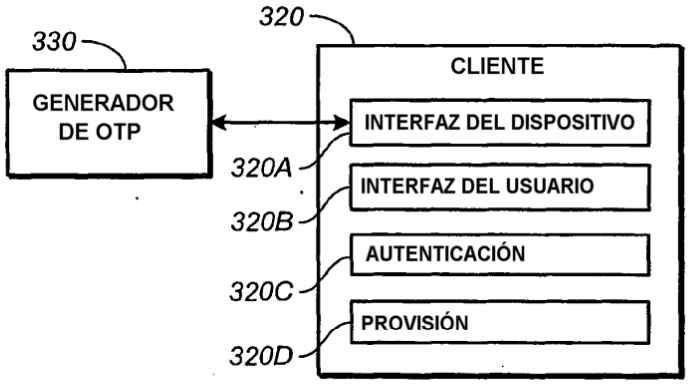


FIG. 3C

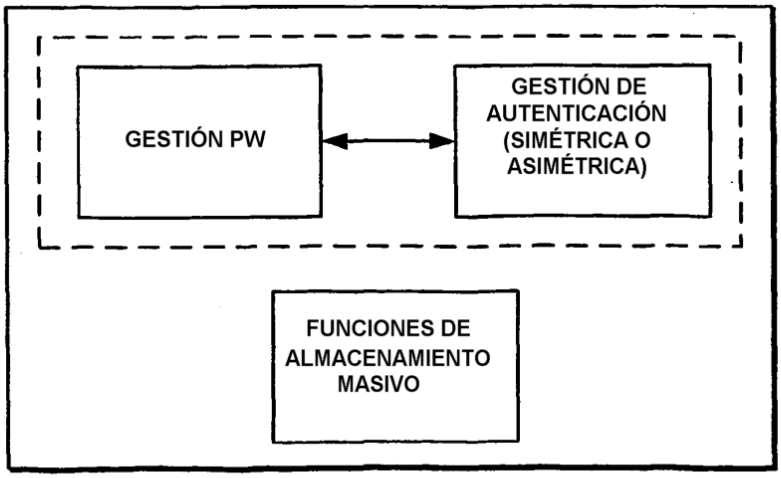
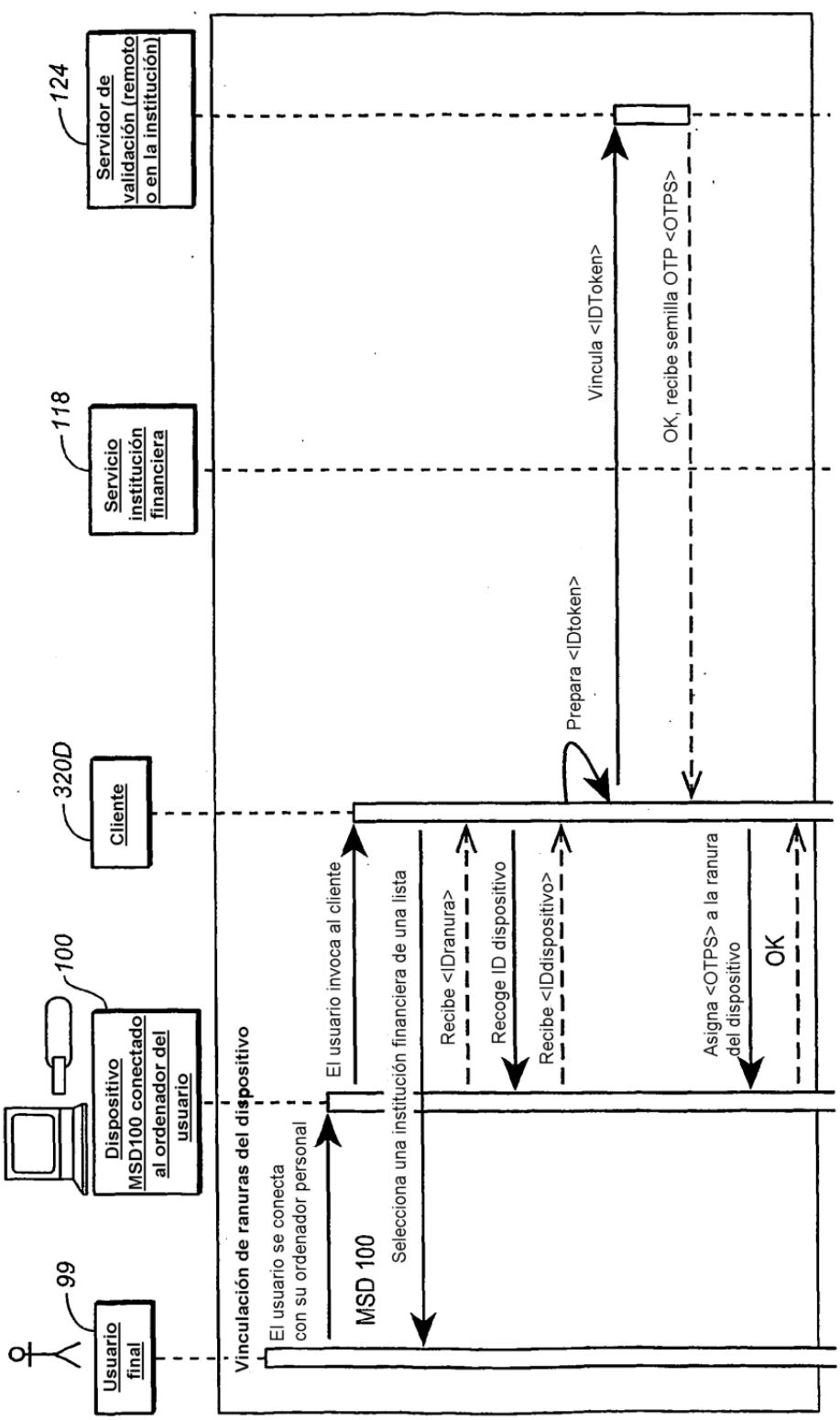


FIG. 4

FIG. 5A

FIG. 5A-1

FIG. 5A-2



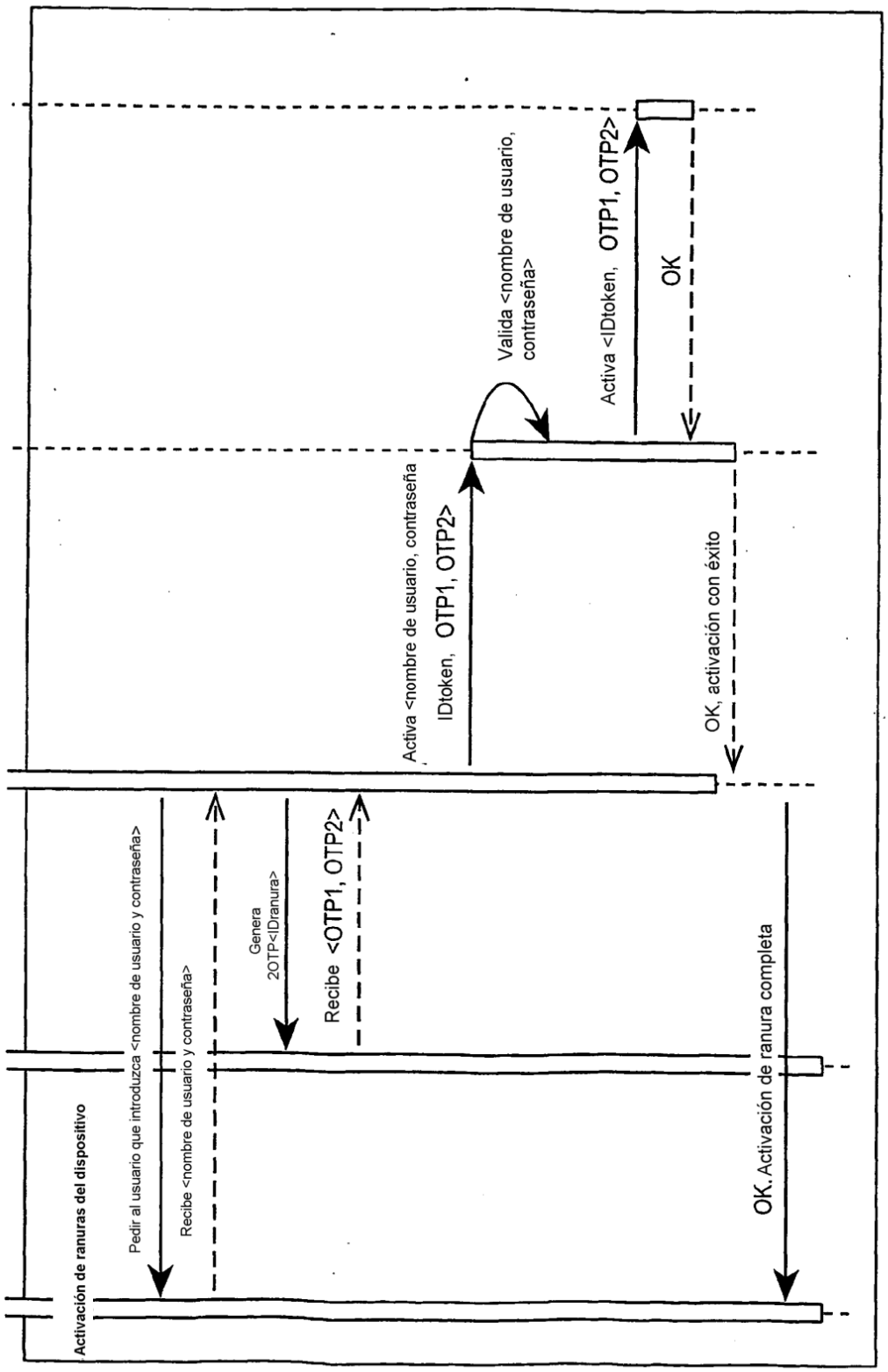
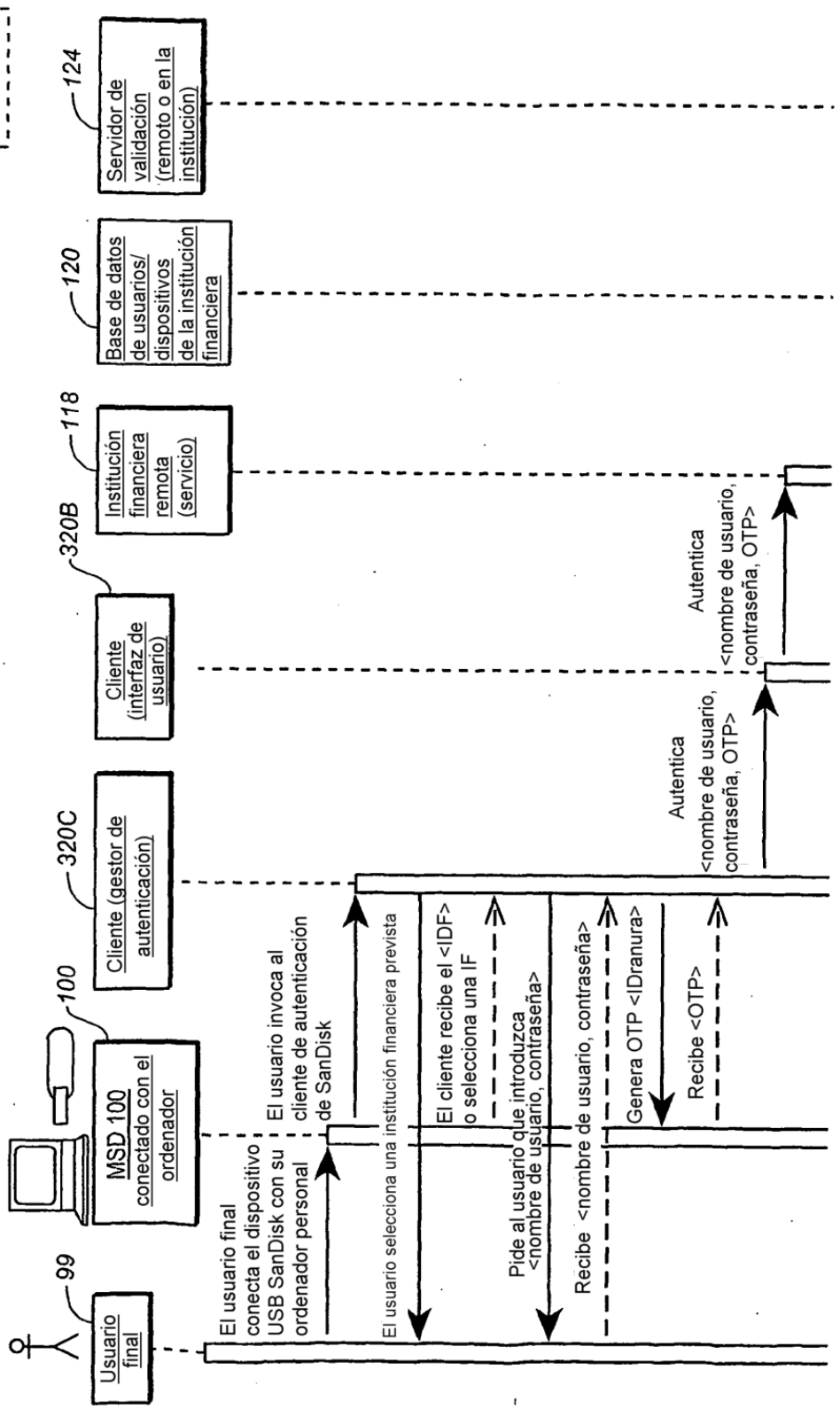

Activación de ranuras del dispositivo
Pedir al usuario que introduzca <nombre de usuario y contraseña>
Recibe <nombre de usuario y contraseña>
Genera 2OTP<IDranura>
Recibe <OTP1, OTP2>
Activa <nombre de usuario, contraseña IDtoken, OTP1, OTP2>
OK, activación con éxito
Valida <nombre de usuario, contraseña>
Activa <IDtoken, OTP1, OTP2>
OK
OK. Activación de ranura completa

FIG. 5A-2

FIG. 5B

FIG. 5B-1

FIG. 5B-2



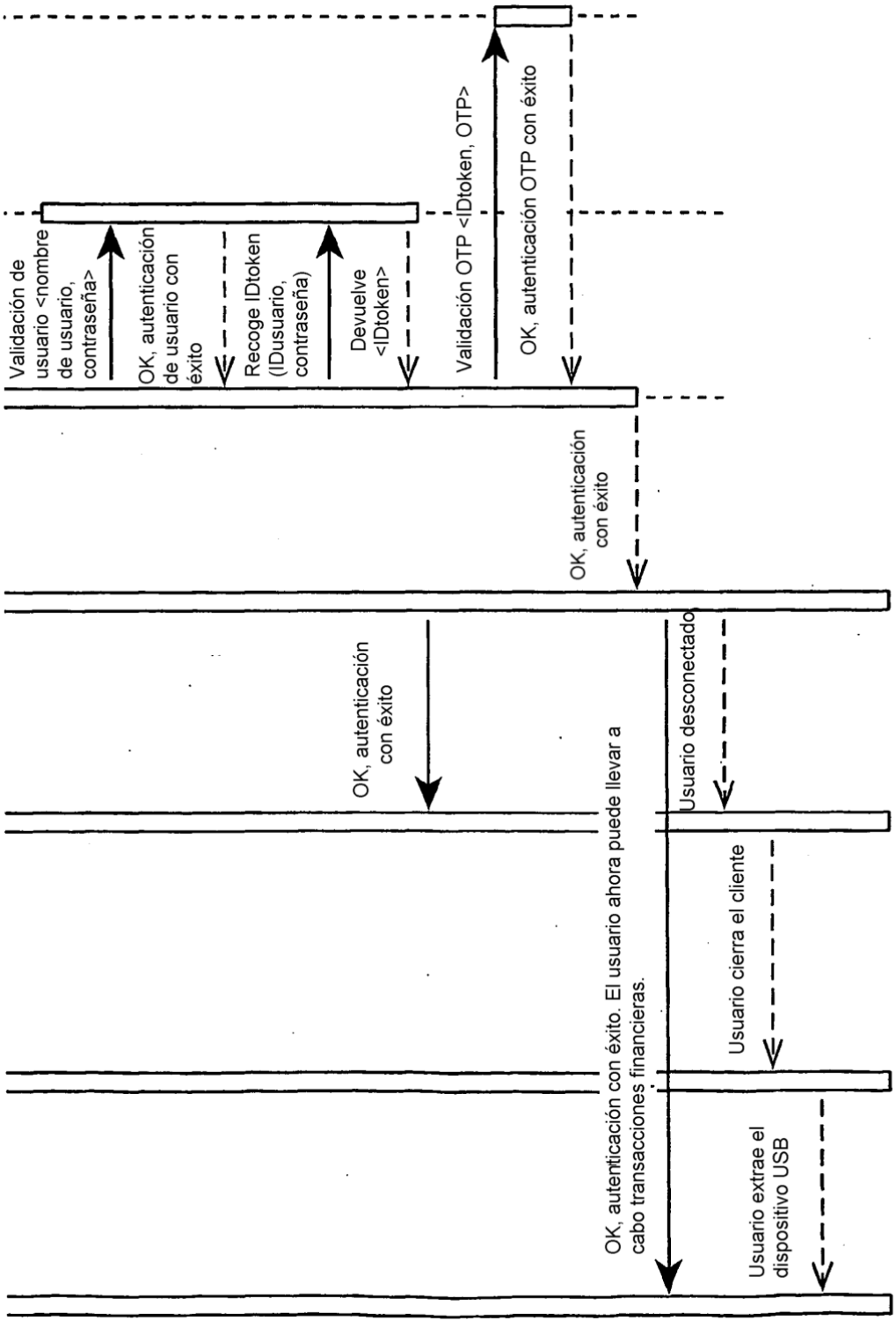

Validación de usuario <nombre de usuario, contraseña>
OK, autenticación de usuario con éxito
Recoge IDtoken (IDusuario, contraseña)
Devuelve <IDtoken>
Validación OTP <IDtoken, OTP>
OK, autenticación OTP con éxito
OK, autenticación con éxito
OK, autenticación con éxito
Usuario desconectado
Usuario cierra el cliente
OK, autenticación con éxito. El usuario ahora puede llevar a cabo transacciones financieras.
Usuario extrae el dispositivo USB

FIG. 5B-2

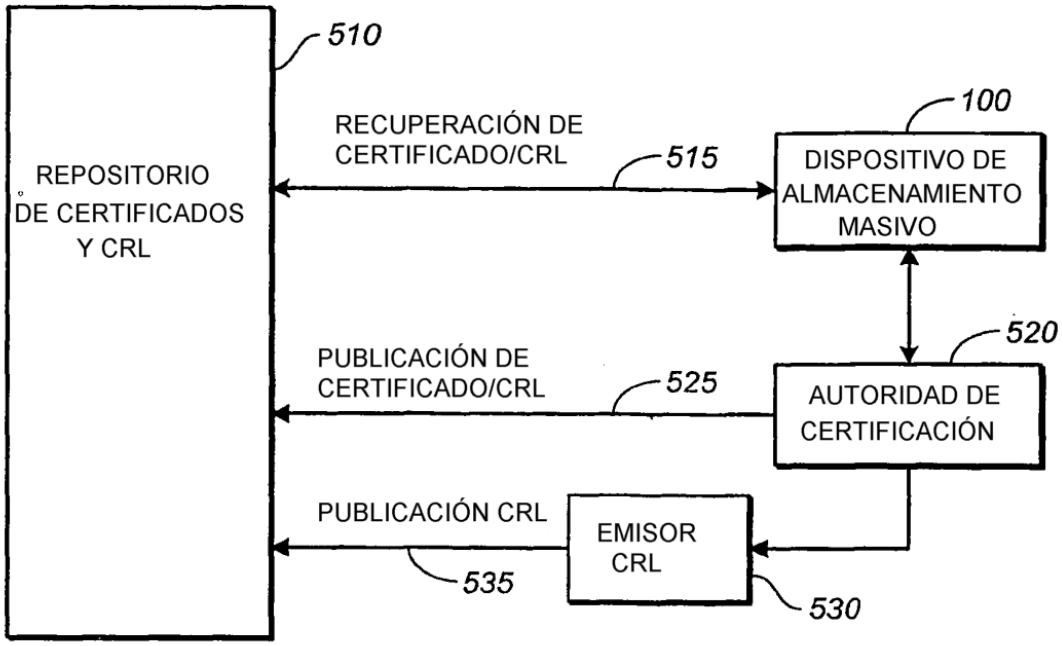

510
REPOSITORIO DE CERTIFICADOS Y CRL
RECUPERACIÓN DE CERTIFICADO/CRL
515
100
DISPOSITIVO DE ALMACENAMIENTO MASIVO
520
PUBLICACIÓN DE CERTIFICADO/CRL
525
AUTORIDAD DE CERTIFICACIÓN
PUBLICACIÓN CRL
EMISOR CRL
535
530

FIG. 5C

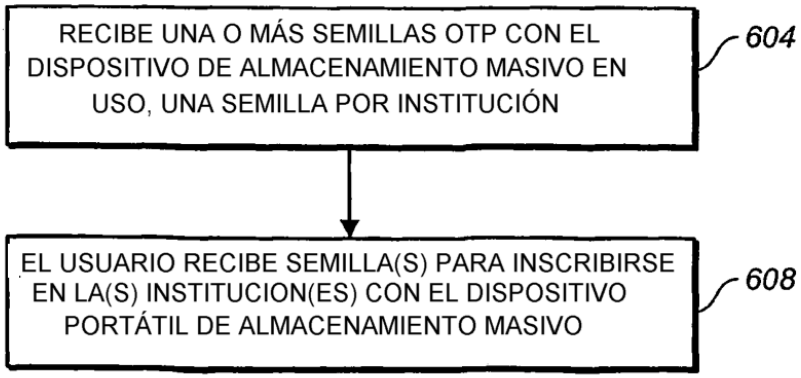

RECIBE UNA O MÁS SEMILLAS OTP CON EL DISPOSITIVO DE ALMACENAMIENTO MASIVO EN USO, UNA SEMILLA POR INSTITUCIÓN
604
EL USUARIO RECIBE SEMILLA(S) PARA INSCRIBIRSE EN LA(S) INSTITUCION(ES) CON EL DISPOSITIVO PORTÁTIL DE ALMACENAMIENTO MASIVO
608

FIG. 6

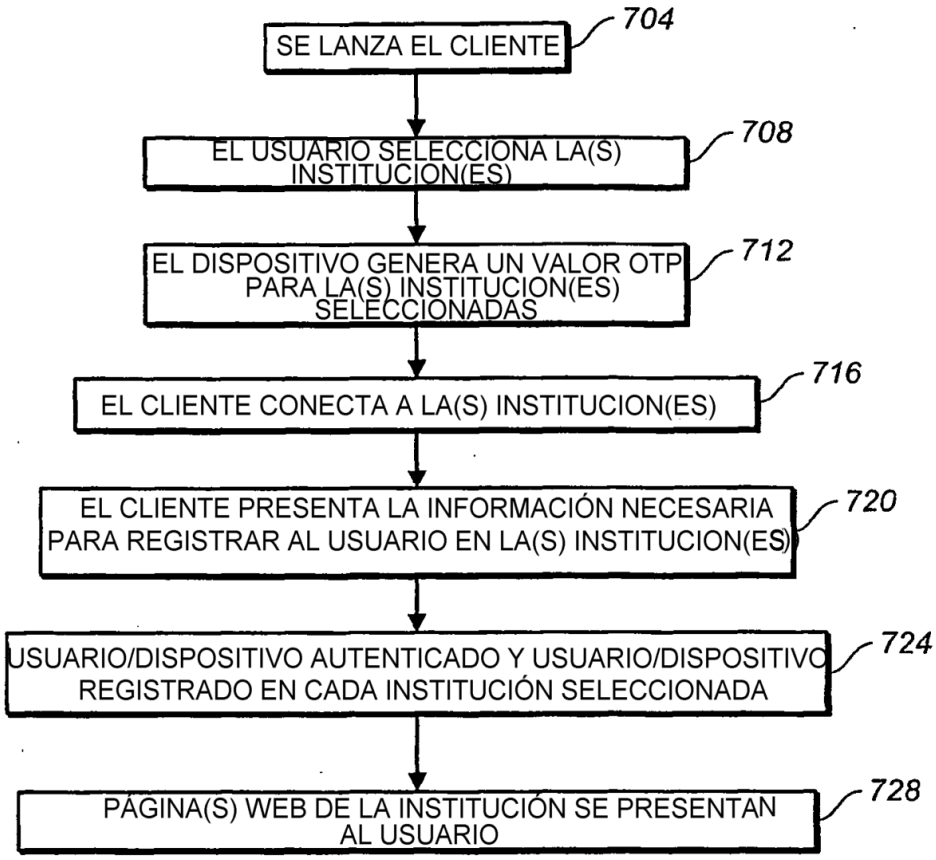

SE LANZA EL CLIENTE
704
EL USUARIO SELECCIONA LA(S) INSTITUCION(ES)
708
EL DISPOSITIVO GENERA UN VALOR OTP PARA LA(S) INSTITUCION(ES) SELECCIONADAS
712
EL CLIENTE CONECTA A LA(S) INSTITUCION(ES)
716
EL CLIENTE PRESENTA LA INFORMACIÓN NECESARIA PARA REGISTRAR AL USUARIO EN LA(S) INSTITUCION(ES)
720
USUARIO/DISPOSITIVO AUTENTICADO Y USUARIO/DISPOSITIVO REGISTRADO EN CADA INSTITUCIÓN SELECCIONADA
724
PÁGINA(S) WEB DE LA INSTITUCIÓN SE PRESENTAN AL USUARIO
728

FIG. 7

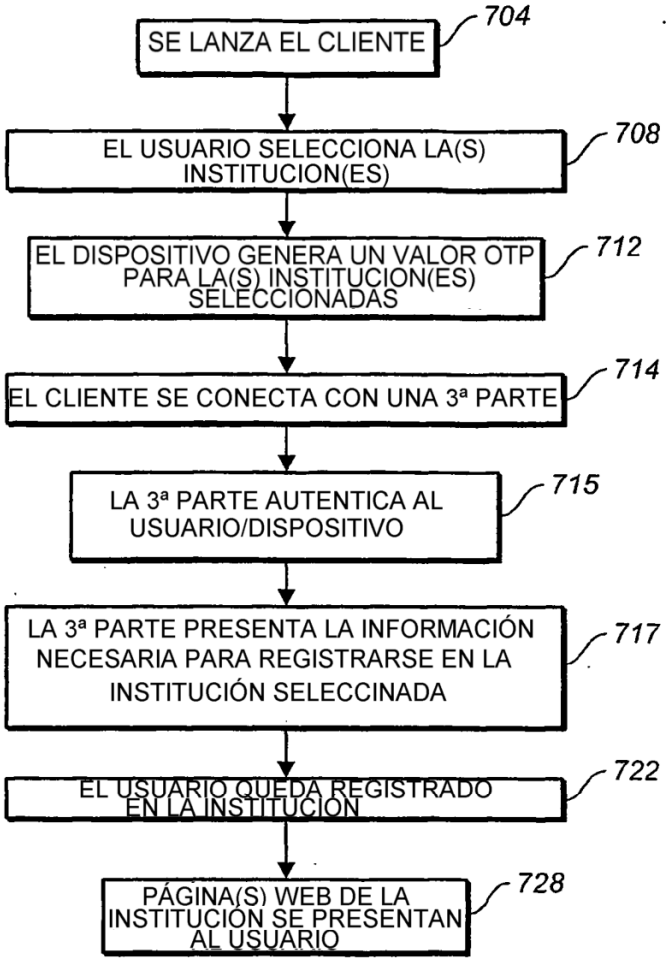

SE LANZA EL CLIENTE
704
EL USUARIO SELECCIONA LA(S) INSTITUCION(ES)
708
EL DISPOSITIVO GENERA UN VALOR OTP PARA LA(S) INSTITUCION(ES) SELECCIONADAS
712
EL CLIENTE SE CONECTA CON UNA 3ª PARTE
714
LA 3ª PARTE AUTENTICA AL USUARIO/DISPOSITIVO
715
LA 3ª PARTE PRESENTA LA INFORMACIÓN NECESARIA PARA REGISTRARSE EN LA INSTITUCIÓN SELECCINADA
717
EL USUARIO QUEDA REGISTRADO EN LA INSTITUCION
722
PÁGINA(S) WEB DE LA INSTITUCION SE PRESENTAN AL USUARIO
728

FIG. 8

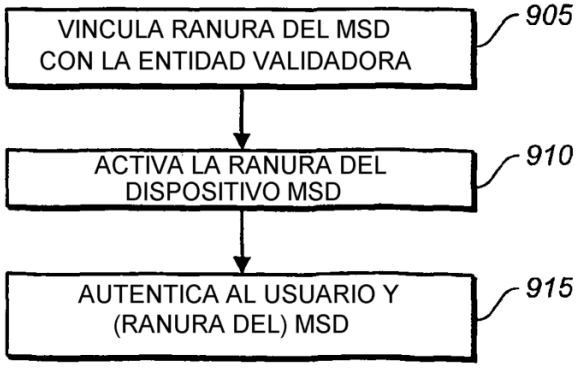

VINCULA RANURA DEL MSD CON LA ENTIDAD VALIDADORA
905
ACTIVA LA RANURA DEL DISPOSITIVO MSD
910
AUTENTICA AL USUARIO Y (RANURA DEL) MSD
915

FIG. 9

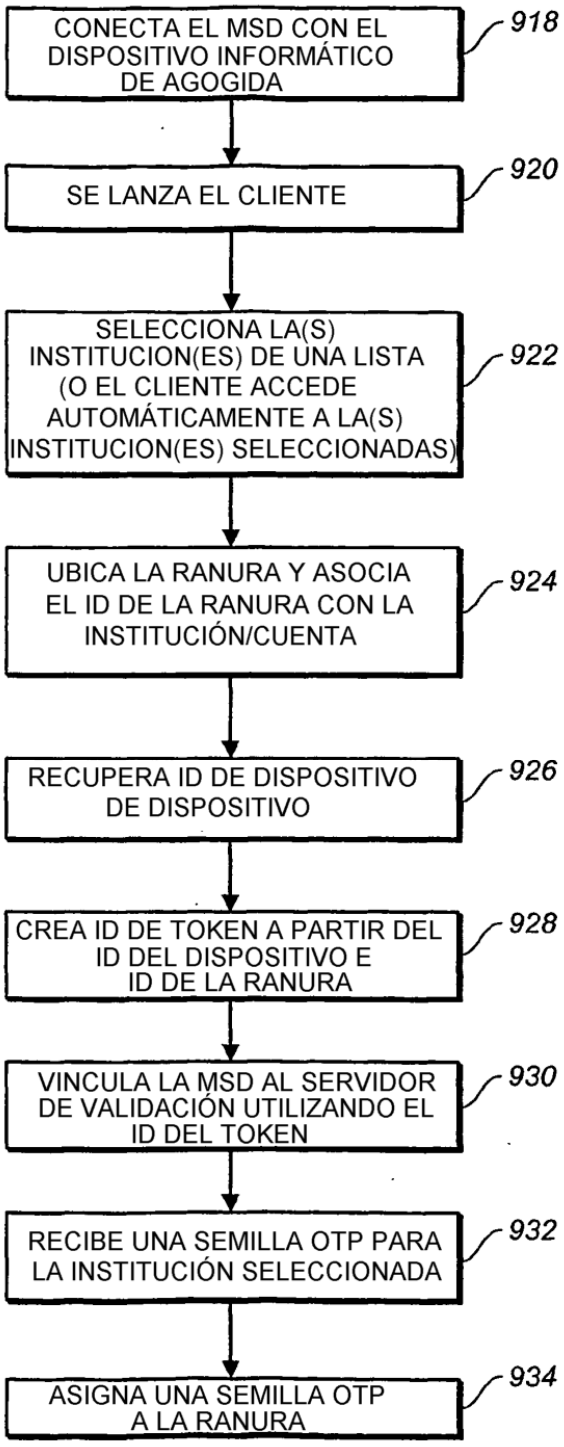


FIG. 10A

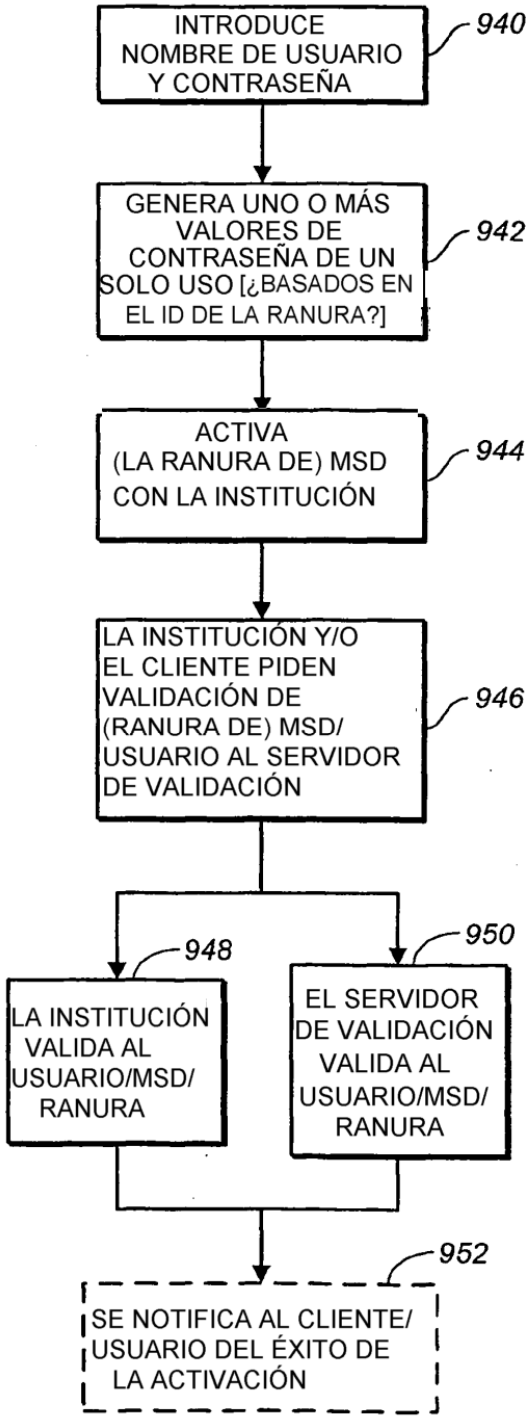


FIG. 10B

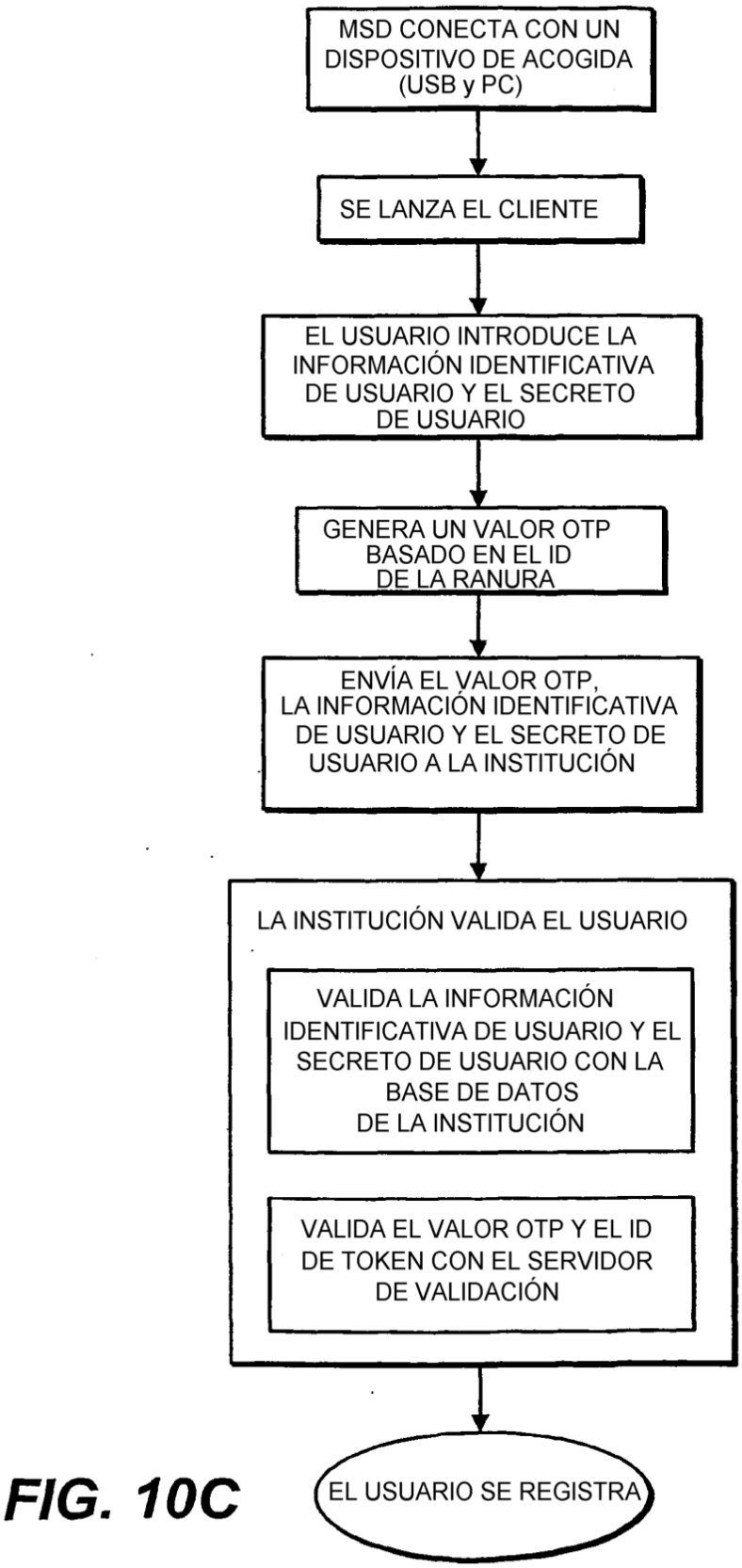

MSD CONECTA CON UN DISPOSITIVO DE ACOGIDA (USB y PC)
SE LANZA EL CLIENTE
EL USUARIO INTRODUCE LA INFORMACIÓN IDENTIFICATIVA DE USUARIO Y EL SECRETO DE USUARIO
GENERA UN VALOR OTP BASADO EN EL ID DE LA RANURA
ENVÍA EL VALOR OTP, LA INFORMACIÓN IDENTIFICATIVA DE USUARIO Y EL SECRETO DE USUARIO A LA INSTITUCIÓN
LA INSTITUCIÓN VALIDA EL USUARIO
VALIDA LA INFORMACIÓN IDENTIFICATIVA DE USUARIO Y EL SECRETO DE USUARIO CON LA BASE DE DATOS DE LA INSTITUCIÓN
VALIDA EL VALOR OTP Y EL ID DE TOKEN CON EL SERVIDOR DE VALIDACIÓN
EL USUARIO SE REGISTRA

FIG. 10C

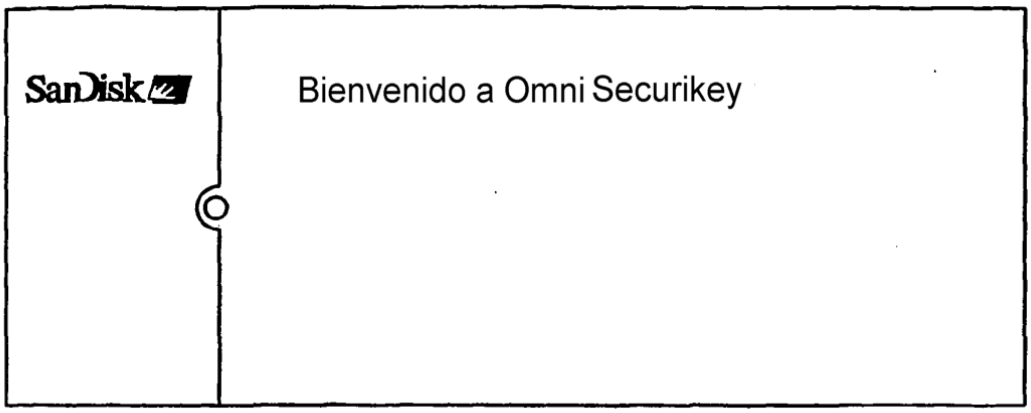


FIG. 11A

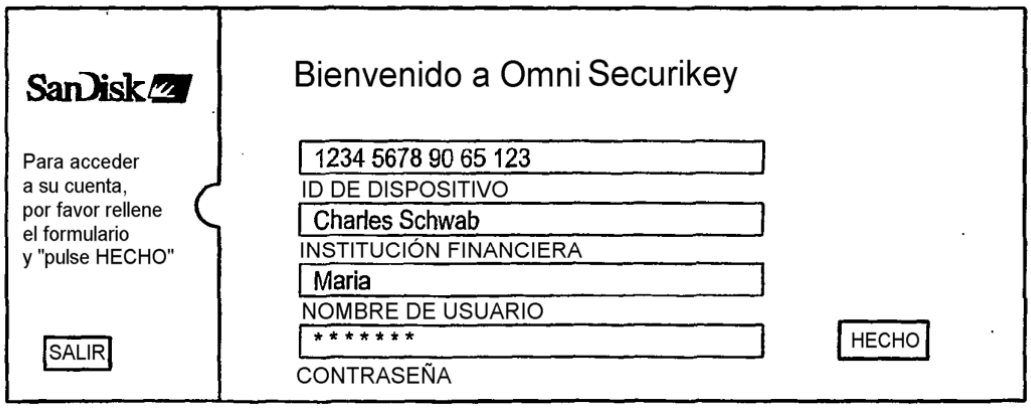


FIG. 11B

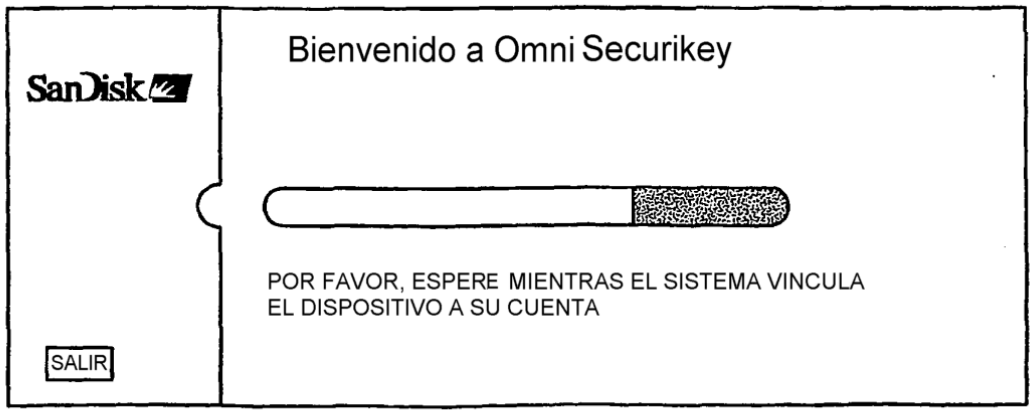


FIG. 11C

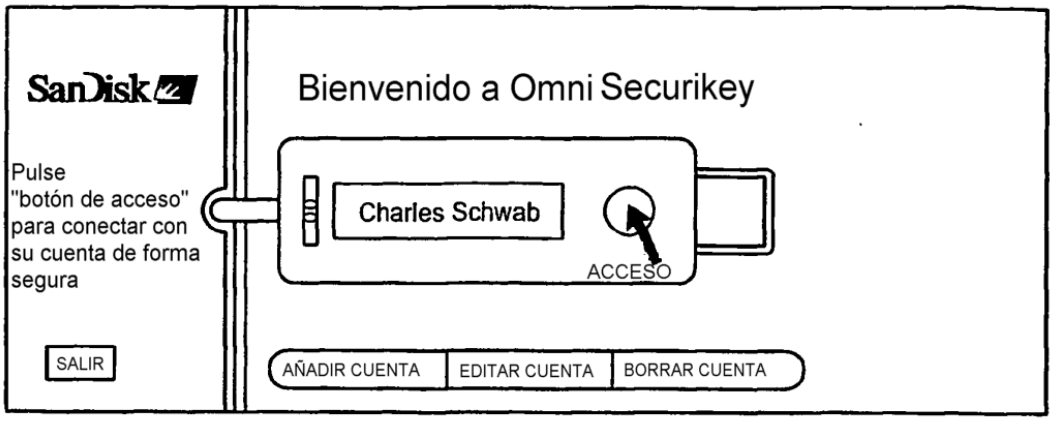


FIG. 11D

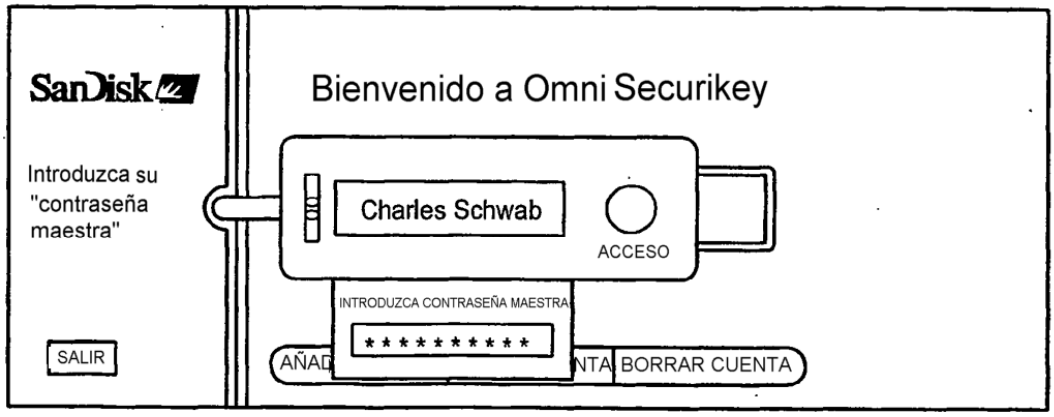


FIG. 11E

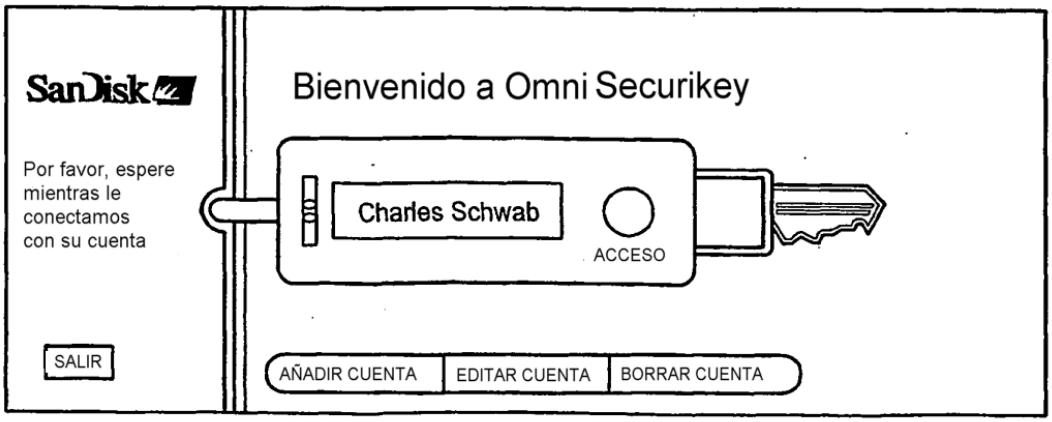


FIG. 11F

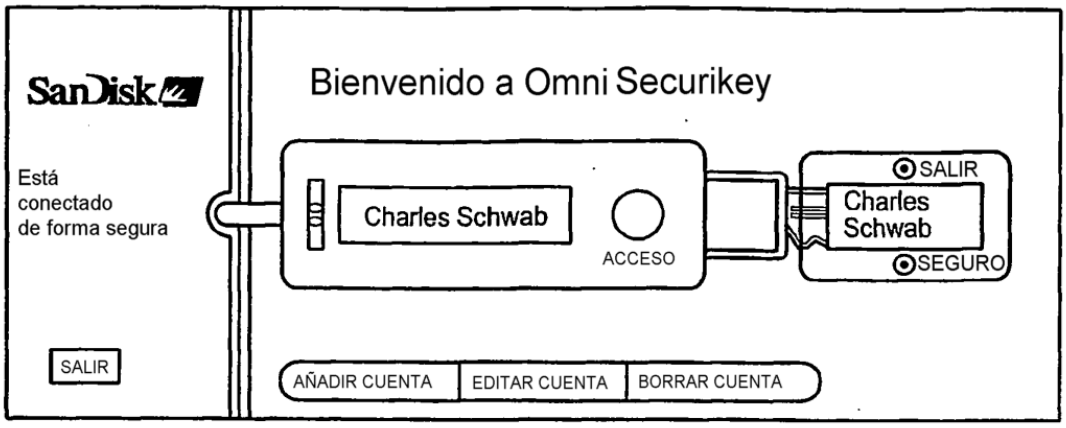


FIG. 11G

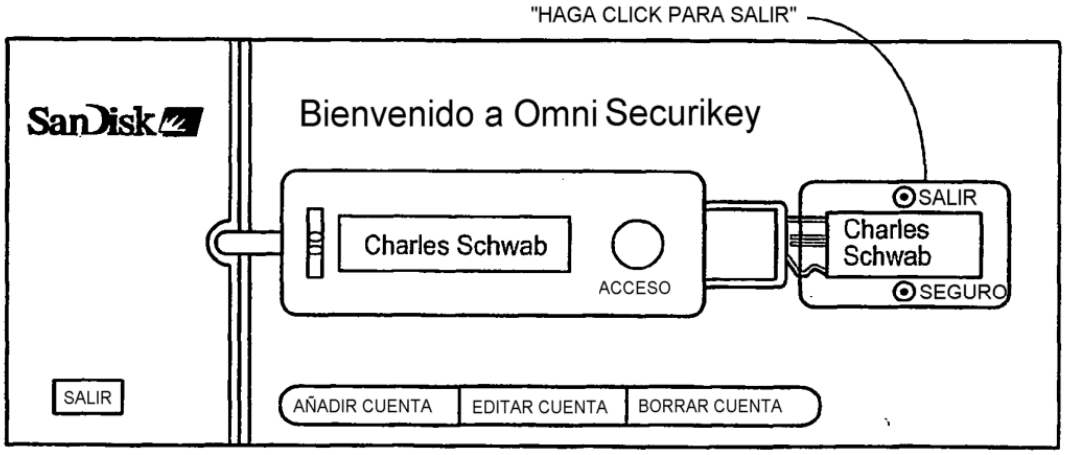


FIG. 11H

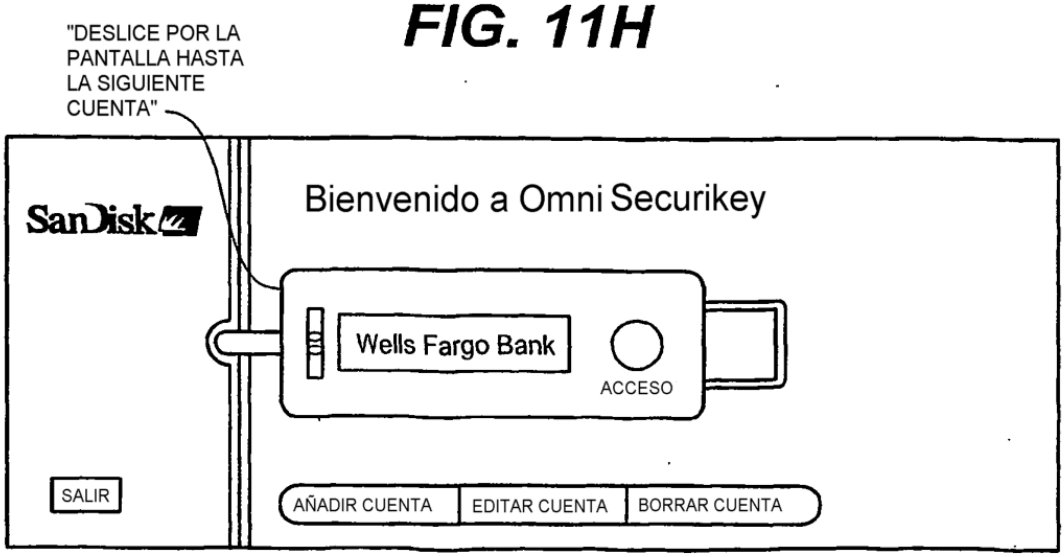


FIG. 11I

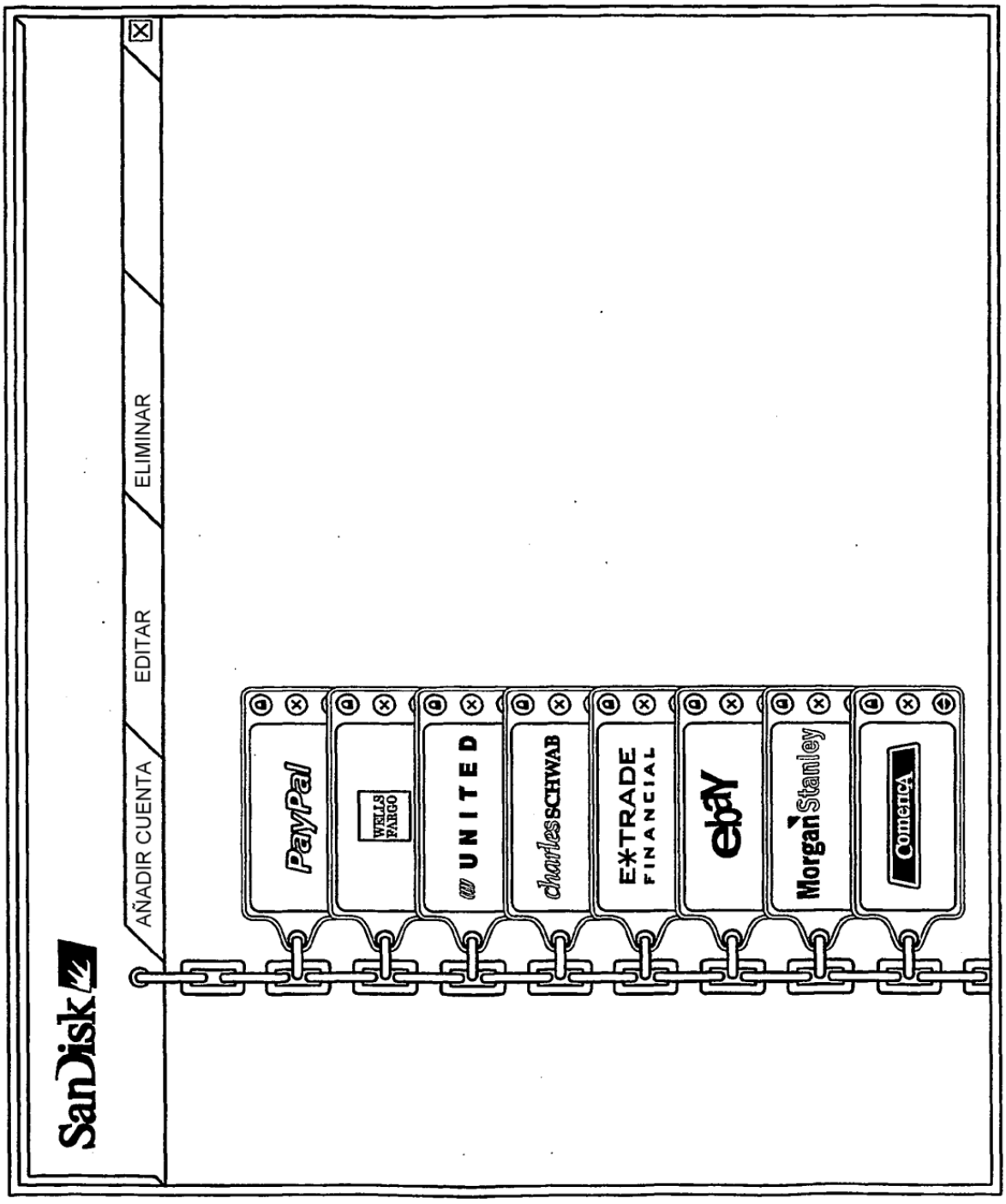

SanDisk
AÑADIR CUENTA
EDITAR
ELIMINAR
PayPal
WELLS FARGO
UNITED
charlesSCHWAB
E*TRADE FINANCIAL
eBaY
MorganStanley
ComericA

FIG. 12A

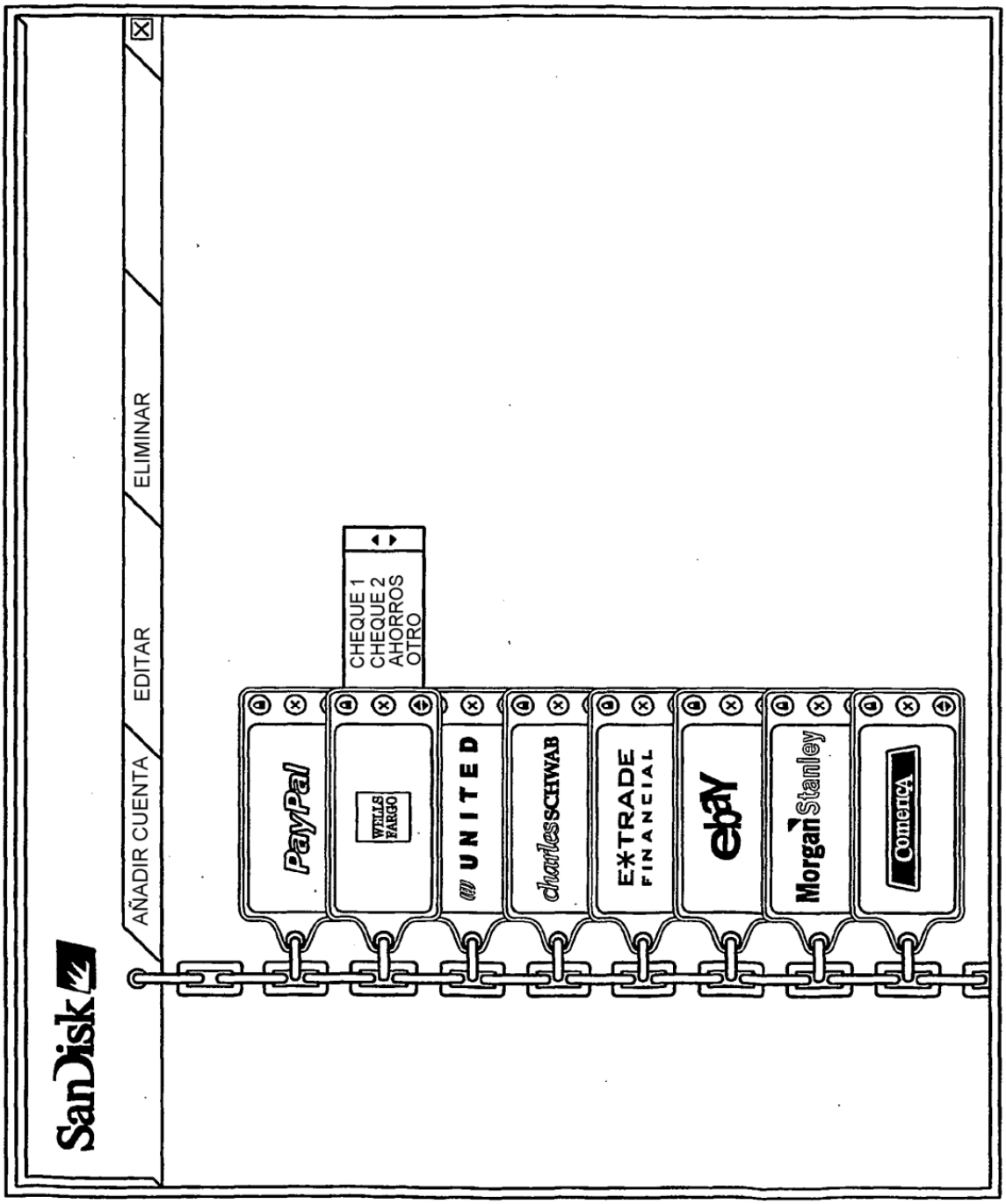

SanDisk
AÑADIR CUENTA
EDITAR
ELIMINAR
CHEQUE 1
CHEQUE 2
AHORROS
OTRO
PayPal
WELLS FARGO
UNITED
charlesSCHWAB
E*TRADE FINANCIAL
eBay
Morgan Stanley
Comerica

FIG. 12B