

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 986 209**

51 Int. Cl.:

G06F 21/36 (2013.01)

H04L 9/40 (2012.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

96 Fecha de presentación y número de la solicitud europea: **23.10.2019** **E 19204846 (0)**

97 Fecha y número de publicación de la concesión europea: **17.07.2024** **EP 3644578**

54 Título: **Autentificación de apuntar y pulsar**

30 Prioridad:

24.10.2018 FR 1859828

45 Fecha de publicación y mención en BOPI de la
traducción de la patente:
08.11.2024

73 Titular/es:

AMADEUS S.A.S. (100.0%)
485 route du Pin Montard, Sophia Antipolis
06410 Biot, FR

72 Inventor/es:

MAUPAY, FLORENT y
MAAROUFI, MOHAMED-AMINE

74 Agente/Representante:

ELZABURU, S.L.P

ES 2 986 209 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Autenticación de apuntar y pulsar

Campo técnico

5 La presente invención se refiere en general a autenticación multifactorial, aunque no se limita a la misma. Más específicamente, la presente invención se refiere a técnicas para autenticación multifactorial utilizando contraseñas gráficas.

Antecedentes

10 Las técnicas de autenticación existentes pueden utilizar contraseñas solas o en combinación con un identificador tal como un nombre de usuario para verificar identidades y/o limitar el acceso a recursos protegidos. En algunos casos, se puede utilizar la autenticación multifactorial en la que dos o más factores de distintas categorías de credenciales se evalúan durante la autenticación de tal manera que cada factor adicional añade una capa adicional de seguridad al proceso de autenticación.

15 Ejemplos de tales factores adicionales que se evalúan durante la autenticación incluyen: fichas basadas en hardware (por ejemplo, RSA SecurID proporcionado por RSA Security LLC. de Bedford, Massachusetts) para autenticación de desafío/respuesta; escáneres biométricos (por ejemplo, escáneres de huellas dactilares); contraseñas de un solo uso enviadas por mensajería de texto/voz o correo electrónico, y similares. Las capas adicionales de seguridad que proporcionan estos factores adicionales son eficaces en su mayor parte; sin embargo, estas técnicas existentes también suponen un aumento de los costes de implantación y mantenimiento.

20 Otras técnicas existentes de autenticación multifactorial utilizan contenido gráfico en el que se definen contraseñas (por ejemplo, contraseñas gráficas). Como un ejemplo, los puntos de pulsación indicados representan una técnica gráfica existente en la que una contraseña se basa en varias imágenes que se presentan en secuencia a un usuario. En particular, la posición en la que el usuario pulsa dentro de cada posición determina qué imagen posterior se presenta al usuario, y la trayectoria seguida por el usuario a través de la secuencia de imágenes representa la contraseña. Aunque son eficaces en la mayoría de los casos, estas técnicas basadas en gráficos pueden ser vulnerables a los ataques de grabación/repetición y phishing. Los puntos de pulsación indicados, por ejemplo, suelen presentar a los usuarios las mismas imágenes del mismo banco de imágenes para su autenticación. De este modo, la observación de un usuario introduciendo una contraseña podría comprometerla.

25 El documento US 2004/093527 A1 se refiere a autenticación basada en el reconocimiento. Por ejemplo, la autenticación de un usuario que opera un dispositivo de acceso no fiable incluye la visualización, en el dispositivo de acceso no fiable, de una pluralidad de fotografías para el usuario, siendo al menos una de las fotografías de la colección fotográfica personal del usuario y ya familiar para el usuario, siendo las fotografías restantes fotografías señuelo, aceptando una selección de entrada del usuario que identifique una de las fotografías visualizadas, y permitiendo el acceso cuando la selección del usuario identifique correctamente una secuencia de fotografías visualizadas de la colección fotográfica del usuario. No es necesario formar al usuario antes de utilizar el sistema de autenticación ni preseleccionar una contraseña o una fotografía.

30 El documento WO 2007/070014 A1 se refiere a un método y a un aparato para proporcionar seguridad mejorada. Por ejemplo, un método para el control de acceso comprende mostrar a un usuario, en una pantalla, un contenedor que contiene un conjunto de elementos de visualización interactivos. El conjunto de elementos de visualización comprende un primer subconjunto de elementos clave de visualización interactiva y se ha generado aleatoriamente una disposición en el contenedor de los elementos clave de visualización interactiva. Se solicita al usuario una selección de una pluralidad de elementos de visualización interactiva del conjunto y el método comprueba si la selección del usuario satisface un criterio de selección.

Otros ejemplos existentes de técnicas de autenticación de usuarios se presentan en los documentos US 6 209 104 B1 y US 2011/154482 A1.

Sumario

45 La presente invención se define en las reivindicaciones independientes. Las reivindicaciones dependientes definen realizaciones de las mismas.

50 Las realizaciones de la presente invención proporcionan sistemas, métodos y medios de almacenamiento legibles por ordenador para la autenticación multifactorial utilizando contraseñas gráficas. En una realización, un método incluye la recepción de una primera solicitud de acceso desde un dispositivo cliente. La primera solicitud de acceso identifica un recurso protegido e incluye un identificador. Se genera una primera interfaz que incluye una pluralidad de objetos gráficos para su presentación en ubicaciones aleatorias en una pantalla del dispositivo cliente según lo definido por un primer mapa de objetos. La pluralidad de objetos gráficos incluye un objeto nulo y un conjunto de objetos definidos por el usuario asociados al identificador que definen una contraseña gráfica. Los datos de entrada incluyen un evento de entrada para cada interacción con la primera interfaz que el dispositivo cliente detecta que se recibe. El evento de

entrada para cada interacción identifica una posición en la pantalla en la que se detectó una interacción correspondiente. Utilizando el primer mapa de objetos, se determina que los datos de entrada satisfacen la contraseña gráfica. El acceso al recurso protegido se concede en respuesta a la determinación de que los datos de entrada satisfacen la contraseña gráfica.

5 En otra realización, un sistema incluye un dispositivo electrónico con una pantalla, un procesador y un medio de almacenamiento legible por ordenador que incluye instrucciones. Al ser ejecutadas por el procesador, las instrucciones hacen que el sistema realice operaciones. Las operaciones incluyen el envío de una solicitud de acceso a un servicio de acceso de un servidor anfitrión. La solicitud de acceso identifica un recurso protegido e incluye un identificador. En respuesta, se recibe una interfaz del servicio de acceso que incluye una pluralidad de objetos gráficos para su presentación en la pantalla. Se registra un evento de entrada por cada interacción detectada con la interfaz mientras se presenta la interfaz en la pantalla. Cada evento de entrada identifica una posición en la pantalla en la que se ha detectado la interacción correspondiente. Los datos de entrada se envían al servicio de acceso que incluye cada evento de entrada registrado. El acceso al recurso protegido se recibe cuando el servicio de acceso determina que los datos de entrada satisfacen una contraseña gráfica mediante un mapa de objetos. La contraseña gráfica está definida por un conjunto de objetos definidos por el usuario incluidos entre la pluralidad de objetos gráficos. El mapa de objetos define posiciones asignadas aleatoriamente para presentar la pluralidad de objetos gráficos en la pantalla.

En otra realización, se proporciona un medio de almacenamiento legible por ordenador no transitorio que incluye instrucciones de programa. Al ser ejecutadas por un procesador de un dispositivo informático, las instrucciones de programa hacen que el dispositivo informático reciba, en un servicio de acceso asociado con un servidor anfitrión, una solicitud de acceso de un dispositivo cliente. La solicitud de acceso identifica un recurso protegido e incluye un identificador. Se genera una interfaz que incluye una pluralidad de objetos gráficos para su presentación en posiciones aleatorias en una pantalla del dispositivo cliente según lo definido por un mapa de objetos. La pluralidad de objetos gráficos incluye un objeto nulo y un conjunto de objetos definidos por el usuario asociados al identificador que definen una contraseña gráfica. Se reciben datos de entrada que incluyen un evento de entrada para cada interacción con la interfaz que detecta el dispositivo cliente. Cada evento de entrada identifica una posición en la pantalla en la que se ha detectado la interacción correspondiente. Mediante el mapa de objetos, se determina si los datos de entrada satisfacen la contraseña gráfica. El acceso se concede al recurso protegido de acuerdo con la determinación de que los datos de entrada satisfacen la contraseña gráfica.

Este sumario se proporciona para introducir una selección de conceptos en una forma simplificada que se describen adicionalmente a continuación en la descripción detallada. Este sumario no pretende identificar las características clave o esenciales de la materia reivindicada, ni está destinado a ser utilizado de manera aislada como una ayuda para determinar el alcance de la materia reivindicada.

Breve descripción de los dibujos

Los dibujos adjuntos ilustran diversas realizaciones de la presente invención y, junto con la descripción general de la invención dada anteriormente, y la descripción detallada de las realizaciones dada a continuación, sirven para explicar las realizaciones de la invención. En los dibujos, se utilizan números de referencia similares para indicar partes similares en las distintas vistas.

La Figura 1 es un diagrama de bloques de un entorno operativo de ejemplo que es adecuado para implementar aspectos de la presente invención.

La Figura 2 representa un ejemplo de un dispositivo cliente que envía una solicitud de acceso a un servicio de acceso.

La Figura 3 representa el servicio de acceso de la Figura 2, que envía una interfaz con una pluralidad de objetos gráficos al dispositivo cliente en respuesta a la solicitud de acceso.

La Figura 4 representa el dispositivo cliente de la Figura 2, que envía datos de entrada que incluyan un evento de entrada que identifique posiciones en una pantalla del dispositivo cliente para cada interacción con la interfaz de la Figura 3 al servicio de acceso y recibir una decisión de acceso del servicio de acceso basada en una comparación de los datos de entrada y un mapa de objetos.

Las Figuras 5A y 5B muestran ejemplos de mapas de objetos que definen posiciones asignadas aleatoriamente (o pseudoaleatoriamente) para presentar una pluralidad de objetos gráficos en la pantalla de un dispositivo cliente.

La Figura 6 representa un ejemplo de ataque de repetición en el servicio de acceso de la Figura 2 por parte de una entidad maliciosa que se hace pasar por el dispositivo cliente de la Figura 2.

La Figura 7 muestra un ejemplo de ataque de phishing al dispositivo cliente de la Figura 2 por parte de una entidad maliciosa que se hace pasar por el servicio de acceso de la Figura 2.

La Figura 8 es un diagrama de flujo que ilustra un proceso de ejemplo para la autenticación multifactorial utilizando contraseñas gráficas.

La Figura 9 es un diagrama de flujo que ilustra otro ejemplo de proceso para la autenticación multifactorial utilizando contraseñas gráficas.

La Figura 10 es un diagrama de bloques de un entorno informático de ejemplo adecuado para su uso en la implementación de realizaciones de la invención.

5 Descripción detallada

Las técnicas descritas en el presente documento se refieren a la autenticación multifactorial utilizando contraseñas gráficas. Haciendo referencia a la Figura 1, se ilustra un entorno operativo de ejemplo para implementar aspectos de la presente invención y se designa generalmente con 100. En general, el entorno operativo 100 representa los diversos componentes implicados en la provisión de autenticación multifactorial. El entorno operativo 100 incluye un dispositivo cliente 110, un servicio de acceso 120, un servidor 130 y una base de datos 140. A modo de ejemplo y no de limitación, el dispositivo cliente 110 puede ser un ordenador de sobremesa, un ordenador portátil, un dispositivo informático móvil, un teléfono inteligente, una tableta, un reloj inteligente, un dispositivo electrónico de consumo, una estación de trabajo y similares.

Un usuario, en el entorno operativo 100, interactúa con el dispositivo cliente 110 para acceder a recursos protegidos dentro de un dominio anfitrión a través de la red 150. En el ejemplo ilustrado en la Figura 1, el dominio anfitrión está compuesto por una pluralidad de componentes que incluyen el servicio de acceso 120, el servidor 130 y la base de datos 140. Tal y como se utiliza en este documento, un "recurso protegido" se refiere generalmente a cualquier recurso informático que reside dentro de un dominio anfitrión cuyo acceso está limitado, controlado o restringido. Algunos ejemplos de recursos protegidos son: servicios, aplicaciones, documentos, archivos, información de cuentas, objetos, interfaces de programación de aplicaciones, páginas web, código ejecutable y similares.

En el entorno operativo 100, el usuario del dispositivo cliente 110 accede a un recurso protegido dentro del dominio anfitrión enviando una solicitud de acceso que identifica el recurso protegido. Por ejemplo, la solicitud de acceso puede identificar una aplicación que se ejecuta en un entorno de tiempo de ejecución del servidor 130 o datos que residen en la base de datos 140. En una realización, un recurso protegido se identifica mediante un Identificador Uniforme de Recursos ("URI"), como un Localizador Uniforme de Recursos ("URL"). El servicio de acceso 120 implementa un proceso de autenticación al recibir la solicitud de acceso, como se describe con más detalle a continuación. El servicio de acceso 120 concede o deniega el acceso al recurso protegido en función del resultado del proceso de autenticación.

La Figura 1 muestra los diversos componentes comunicándose entre sí a través de la red 150, que puede incluir una o más redes públicas y/o privadas. Ejemplos de redes que son adecuadas para implementar la red 150 incluyen: redes de área local (LAN), redes de área amplia (WAN), red celular, Internet, redes privadas virtuales (VPN), y similares. El dispositivo cliente 110 y los componentes del dominio anfitrión (por ejemplo, el servicio de acceso 120, el servidor 130 y la base de datos 140) intercambian datos de acuerdo con un protocolo de comunicación que rige la conexión, como el protocolo de transferencia de hipertexto ("HTTP"), el protocolo de transferencia de archivos ("FTP"), el protocolo WebSocket, el protocolo de datagramas de usuario ("UDP") y similares.

Cada uno de los sistemas mostrados en la Figura 1 puede implementarse a través de cualquier tipo de sistema informático, como el sistema informático 1000 descrito con más detalle a continuación con respecto a la Figura 10, por ejemplo. Cada sistema mostrado en la Figura 1 puede comprender un único dispositivo o múltiples dispositivos que cooperen en un entorno distribuido. Por ejemplo, el servicio de acceso 120, el servidor 130 y/o la base de datos 140 pueden proporcionarse a través de múltiples dispositivos dispuestos en un entorno distribuido que proporciona colectivamente la funcionalidad aquí descrita. Además, otros componentes no mostrados también pueden incluirse dentro del entorno distribuido.

De acuerdo con aspectos de la presente invención, autenticar usuarios que presentan solicitudes de acceso que identifican recursos protegidos de un dominio anfitrión implica que un servicio de acceso del dominio anfitrión genere una interfaz que incluye una pluralidad de objetos gráficos para su presentación en una pantalla de un dispositivo cliente a un usuario. Tal como se utiliza en el presente documento, un "objeto gráfico" se refiere generalmente a un elemento seleccionable por el usuario de una interfaz gráfica de usuario para su presentación en una pantalla de un dispositivo informático. Por ejemplo, un objeto gráfico puede implementarse como un icono, un pictograma, un ideograma, un emoji, un logotipo, una imagen, una foto y similares. La pluralidad de objetos gráficos incluye al menos un objeto nulo y un conjunto de objetos definidos por el usuario. El conjunto de objetos definidos por el usuario definen una contraseña gráfica, mientras que los objetos nulos representan señuelos.

La creación de una contraseña gráfica generalmente implica que un usuario seleccione un número de objetos gráficos que colectivamente forman el conjunto de objetos definidos por el usuario. Un dispositivo informático asociado a un dominio anfitrión (por ejemplo, el servicio de acceso 120 de la Figura 1 y el servicio de acceso 250) recibe esa selección y actualiza en consecuencia un perfil de usuario correspondiente del usuario. El conjunto de objetos definidos por el usuario es utilizado por un servicio de acceso del dominio anfitrión para autenticar cualquier solicitud de acceso posterior que incluya un identificador asociado a ese perfil de usuario, como se describe con más detalle a continuación.

En una realización, al menos un objeto definido por el usuario entre el conjunto de objetos definidos por el usuario es un objeto personalizado enviado por el usuario. Por ejemplo, el usuario puede cargar un icono creado por él mismo con un software de edición de gráficos o una imagen descargada de Internet para utilizarla como objeto definido por el usuario. En una realización, al menos un objeto definido por el usuario entre el conjunto de objetos definidos por el usuario incluye datos de imagen obtenidos utilizando un sensor de imagen de un dispositivo cliente. Por ejemplo, el usuario puede subir una foto suya o de un familiar para utilizarla como objeto definido por el usuario. En una realización, al menos un objeto definido por el usuario entre el conjunto de objetos definidos por el usuario es un objeto plantilla seleccionado de entre una pluralidad de objetos plantilla almacenados en un servidor anfitrión (por ejemplo, el servidor 130 y la base de datos 140 de la Figura 1) del dominio anfitrión. Por ejemplo, un servidor anfitrión puede almacenar una pluralidad de objetos de plantilla en una biblioteca de objetos gráficos de los que el usuario puede seleccionar para su uso como un objeto definido por el usuario. En una realización, cada objeto definido por el usuario entre el conjunto de objetos definidos por el usuario comparte un atributo visual común. Por ejemplo, al crear una contraseña gráfica, un usuario puede especificar que cada objeto definido por el usuario debe mostrarse en un color común (por ejemplo, rojo).

Las Figuras 2-4 representan un ejemplo de un dispositivo cliente 200 que interactúa con un servicio de acceso 250 de un dominio anfitrión para acceder a recursos protegidos dentro del dominio anfitrión, de acuerdo con aspectos de la presente invención. En una realización, el dispositivo cliente 200 y el servicio de acceso 250 pueden ser implementados por el dispositivo cliente 110 y el servicio de acceso 120 de la Figura 1, respectivamente. Para acceder a un recurso protegido dentro del dominio anfitrión, el dispositivo cliente 200 envía una solicitud de acceso identificando el recurso protegido al servicio de acceso 250. Como se ve en la Figura 2, la solicitud de acceso incluye un identificador que el dispositivo cliente 200 recibe de un usuario a través de la interfaz 210. En una realización, el identificador corresponde a un perfil de usuario (o cuenta) creado con el dominio anfitrión.

El servicio de acceso 250 está configurado para generar una interfaz que incluye una pluralidad de objetos gráficos, tal como la interfaz 310 de la Figura 3, en respuesta a la recepción de la solicitud de acceso del dispositivo cliente 200. En una realización, la interfaz 310 está asociada con una aplicación que se ejecuta en un servidor anfitrión (por ejemplo, el servidor 130 de la Figura 1) del dominio anfitrión. La pluralidad de objetos gráficos de la interfaz 310 incluye tanto objetos nulos (es decir, objetos gráficos 312A-312D) como un conjunto de objetos definidos por el usuario (es decir, objetos gráficos 314A-314D). Los objetos gráficos 314A-314D se seleccionan para su inclusión en la interfaz 310 como el conjunto de objetos definidos por el usuario utilizando datos que el servicio de acceso 250 obtiene de un perfil de usuario asociado con el identificador incluido en la solicitud de acceso. Los objetos gráficos 312A-312D se seleccionan para su inclusión en la interfaz 310 como objetos nulos utilizando datos que el servicio de acceso 250 obtiene de una biblioteca de objetos gráficos. En una realización, el servicio de acceso 250 está configurado para verificar que un objeto nulo es distinto de cualquier objeto gráfico incluido en un conjunto de objetos definidos por el usuario antes de seleccionar el objeto nulo para su inclusión en una interfaz.

Tras seleccionar los objetos gráficos 312A-312D como los objetos nulos y los objetos gráficos 314A-314D como el conjunto de objetos definidos por el usuario, el servicio de acceso 250 posiciona aleatoriamente (o pseudoaleatoriamente) cada objeto gráfico en una posición diferente sobre el contenido de imagen de fondo 316 para generar la interfaz 310. En una realización, el servicio de acceso 250 utiliza una salida de una función de aleatorización para definir una posición de cada objeto gráfico dentro de la interfaz 310. En una realización, la función de aleatorización reside en la memoria de sólo ejecución ("XOM") de un dispositivo informático que efectúa el servicio de acceso 250. Antes de enviar la interfaz 310 al dispositivo cliente 200, el servicio de acceso 250 almacena información de configuración para la interfaz 310 en un mapa de objetos (por ejemplo, los mapas de objetos 500 y 550 de las Figuras 5A y 5B, respectivamente). La información de configuración para la interfaz 310 almacenada en el mapa de objetos representa la única ubicación en la que una posición de visualización de un objeto gráfico particular dentro de la interfaz 310 está mapeada (o vinculada) a ese objeto gráfico.

Aunque se presenta la interfaz 310 en una pantalla del dispositivo cliente 200, un usuario del dispositivo cliente 200 interactuaba (o seleccionaba) los objetos gráficos 314A-314D, que se representan en la Figura 4 rodeando esos objetos gráficos. Un experto en la materia reconocerá que la selección de los objetos gráficos 314A-314D no requiere actualizar la interfaz 310 para proporcionar al usuario información visual que identifique los objetos gráficos seleccionados (por ejemplo, rodeando dichos objetos gráficos). En una realización, el dispositivo cliente 200 está configurado para actualizar la interfaz 310 en respuesta a la detección de una interacción con un objeto gráfico particular. Por ejemplo, el dispositivo cliente 200 puede modificar uno o más aspectos visuales del objeto gráfico en particular (por ejemplo, color, opacidad, y similares), superponer el objeto gráfico en particular con contenido visual (por ejemplo, una marca de verificación), o modificar uno o más aspectos visuales del contenido de la imagen de fondo 316 próxima al objeto gráfico en particular.

El dispositivo cliente 200 está configurado para registrar un evento de entrada para cada interacción detectada con la interfaz. Cada evento de entrada que el dispositivo cliente 200 registra identifica una posición en la pantalla en la que se detectó una interacción correspondiente. Los datos de entrada que incluyen cada evento de entrada registrado se envían al servicio de acceso 250 con fines de autenticación. Los datos de entrada enviados por el dispositivo cliente 200 al servicio de acceso 250 carecen de cualquier información que identifique objetos gráficos particulares de la interfaz 310. En su lugar, esos datos de entrada sólo incluyen información correspondiente a las interacciones detectadas, como posiciones de visualización, características de interacción y similares.

Puesto que el mapa de objetos para la interfaz 310 almacenado en el servicio de acceso 250 es la única ubicación en la que reside un mapeo de posición de objeto gráfico-pantalla y los datos de entrada enviados por el dispositivo cliente 200 solo incluyen información relacionada con la interacción, no se intercambia información que distinga entre objetos nulos y objetos seleccionados por el usuario entre el servicio de acceso 250 y el dispositivo cliente 200 durante la autenticación. Una de las ventajas de esta disposición es que ninguna información que identifique explícitamente el conjunto de objetos definidos por el usuario que definen la contraseña gráfica está disponible para ser interceptada por una entidad maliciosa. De este modo, la probabilidad de que la entidad maliciosa pueda efectuar con éxito un ataque de phishing (por ejemplo, el ataque de phishing descrito más adelante con respecto a la Figura 7 se reduce).

En una realización, la posición en la pantalla ("posición de pantalla") se define por un par de valores de coordenadas de posición de pantalla (por ejemplo, valores "x" e "y"). En una realización, la posición de visualización se define mediante valores de coordenadas de píxeles. En una realización, cada evento de entrada registrado puede incluir información que caracteriza la interacción correspondiente. Por ejemplo, si la pantalla es táctil, la información que caracteriza la interacción correspondiente puede incluir la duración del tiempo durante el cual un objeto permanece en contacto con la pantalla táctil, la orientación del objeto cuando entra en contacto con la pantalla táctil, el área de la pantalla táctil en la que se produce el contacto entre el objeto y la pantalla táctil, cualquier información de movimiento o aceleración asociada con el objeto cuando permanece en contacto con la pantalla táctil, y similares.

En respuesta a la recepción de los datos de entrada desde el dispositivo cliente 200, el servicio de acceso 250 determina si los datos de entrada satisfacen la contraseña gráfica utilizando el mapa de objetos que almacena la información de configuración para la interfaz 310. Esa determinación generalmente implica que el servicio de acceso 250 evalúe la posición de visualización asociada con cada evento de entrada con el mapa de objetos para identificar un objeto gráfico particular que fue seleccionado en una interacción dada. En el ejemplo de la Figura 4, el servicio de acceso 250 identificaría los objetos gráficos 314A-314D como seleccionados en función de la información de posición de visualización incluida en los datos de entrada. Dado que el conjunto de objetos definidos por el usuario que definen la contraseña gráfica de este ejemplo consiste en los objetos gráficos 314A-314D, el servicio de acceso 250 determinaría que los datos de entrada satisfacen la contraseña gráfica.

En algunas realizaciones, un orden en el que se seleccionan los objetos gráficos del conjunto de objetos definidos por el usuario es relevante para determinar si los datos de entrada satisfacen la contraseña gráfica. Por ejemplo, el servicio de acceso 250 puede evaluar las marcas de tiempo asociadas con cada evento de entrada registrado y determinar que el orden en el que se seleccionó el conjunto de objetos definidos por el usuario fue: objeto gráfico 314C, objeto gráfico 314A, objeto gráfico 314B y objeto gráfico 314D. Sin embargo, los datos del perfil de usuario pueden indicar que un orden prescrito para la contraseña gráfica es: objeto gráfico 314B, objeto gráfico 314D, objeto gráfico 314C y objeto gráfico 314A. Como tal, la contraseña gráfica se define además por un criterio basado en la secuencia. En este ejemplo, el servicio de acceso 250 determinaría que, aunque se han seleccionado todos los objetos gráficos incluidos en el conjunto de objetos definidos por el usuario, los datos de entrada no satisfacen la contraseña gráfica porque el conjunto de objetos definidos por el usuario no se ha seleccionado en el orden prescrito.

En algunas realizaciones, los datos del perfil de usuario pueden especificar otro criterio para definir aún más la contraseña gráfica. En una realización, los datos del perfil de usuario pueden especificar que cada objeto definido por el usuario que define la contraseña gráfica debe seleccionarse sin seleccionar un objeto nulo. En una realización, los datos del perfil de usuario pueden incluir múltiples criterios. Por ejemplo, los datos del perfil de usuario pueden especificar que cada objeto definido por el usuario que define la contraseña gráfica debe seleccionarse en un orden especificado sin seleccionar un objeto nulo. En una realización, los datos del perfil de usuario pueden especificar una característica de una interacción para seleccionar al menos un objeto definido por el usuario entre el conjunto de objetos definidos por el usuario. En esta realización, la contraseña gráfica se define además por un criterio basado en el comportamiento. Un criterio basado en el comportamiento puede especificar que un determinado objeto definido por el usuario debe seleccionarse haciendo doble clic sobre el mismo. Otro criterio basado en el comportamiento puede especificar que, cuando la pantalla es táctil, cada objeto definido por el usuario debe seleccionarse sin romper el contacto con la pantalla táctil.

Como otro ejemplo de criterio basado en el comportamiento, los datos del perfil de usuario pueden indicar que una interacción con el objeto gráfico 314C debe durar al menos 2 segundos. Si la pantalla es táctil, el servicio de acceso 250 puede identificar un evento de interacción en los datos de entrada que corresponda al objeto gráfico 314C. A continuación, el servicio de acceso 250 puede extraer información que caracterice una interacción correspondiente de dicha interacción. Si una evaluación de la información indica que un objeto permaneció en contacto con la pantalla táctil en la posición de visualización asociada con el objeto gráfico 314C durante al menos dos segundos, el servicio de acceso 250 puede determinar que los datos de entrada satisfacen la contraseña gráfica. De lo contrario, si una evaluación de la información indica que un objeto permaneció en contacto con la pantalla táctil en la posición de visualización asociada con el objeto gráfico 314C durante sólo un segundo, el servicio de acceso 250 puede determinar que los datos de entrada no satisfacen la contraseña gráfica.

Tras determinar si los datos de entrada satisfacen la contraseña gráfica, el servicio de acceso 250 proporciona al dispositivo cliente 200 una decisión de acceso basada en dicha determinación. Si el servicio de acceso 250 determina que los datos de entrada satisfacen la contraseña gráfica mediante el mapa de objetos, el servicio de acceso 250 concede al dispositivo cliente 200 acceso al recurso protegido. Alternativamente, si el servicio de acceso 250 determina

que los datos de entrada no satisfacen la contraseña gráfica utilizando el mapa de objetos, el servicio de acceso 250 deniega al dispositivo cliente 200 el acceso al recurso protegido. En una realización en la que el servicio de acceso 250 deniega el acceso al recurso protegido, el servicio de acceso 250 proporciona al dispositivo cliente 200 una indicación de que el acceso ha sido denegado. En una realización en la que el servicio de acceso 250 deniega el acceso al recurso protegido, el servicio de acceso 250 registra información relativa al dispositivo cliente 200 y a la solicitud de acceso. En una realización en la que el servicio de acceso 250 deniega el acceso al recurso protegido, el servicio de acceso 250 finaliza una conexión entre el servicio de acceso 250 y el dispositivo cliente 200.

En una realización, en la que el servicio de acceso 250 proporciona autenticación basada en fichas, la concesión de acceso al recurso protegido incluye el envío de una ficha de acceso al dispositivo cliente 200. En esta realización, el dispositivo cliente 200 almacena la ficha de acceso (por ejemplo, una ficha web de notación de objeto de JavaScript) en la memoria local para su inclusión en posteriores solicitudes de acceso. El dispositivo cliente 200 incluiría la ficha de acceso en posteriores solicitudes de acceso que identifiquen recursos protegidos en el dominio anfitrión. En una realización, en la que el servicio de acceso 250 proporciona autenticación basada en sesión, la concesión de acceso al recurso protegido incluye la generación de una sesión en un espacio de memoria de un servidor anfitrión que permite al dispositivo cliente 200 acceder al recurso protegido. Por ejemplo, el servicio de acceso 250 puede instruir al servidor anfitrión (por ejemplo, el servidor 130 de la Figura 1) iniciar una sesión remota de escritorio o de aplicación (sesión remota) efectuada en un espacio de memoria del servidor anfitrión. En este ejemplo, el servicio de acceso 250 puede proporcionar al dispositivo cliente 200 un identificador de sesión correspondiente a la sesión remota iniciada por el servidor anfitrión.

En una realización, la interfaz 310 incluye opcionalmente el campo de entrada de contraseña 318. En una realización, el campo de entrada de contraseña 318 está en un estado inactivo antes de que el servicio de acceso determine si los datos de entrada satisfacen una contraseña gráfica. En una realización, en respuesta a la determinación de que los datos de entrada satisfacen la contraseña gráfica, el servicio de acceso 250 está configurado para activar el campo de entrada de contraseña 318 antes de conceder al dispositivo cliente 200 acceso al recurso protegido. En una realización, el servicio de acceso 250 activa el campo de entrada de contraseña 318 comunicando datos al dispositivo cliente 200 que hacen que el campo de entrada de contraseña 318 pase del estado inactivo a un estado activo.

En una realización, la interfaz 210 de la Figura 2 incluye un campo de entrada de contraseña que es similar al campo de entrada de contraseña 318 con la excepción de que el campo de entrada de contraseña está en un estado activo antes de enviar una solicitud de acceso. En una realización, el dispositivo cliente 200 envía al servicio de acceso 250 una solicitud de acceso que incluye una contraseña asociada a un identificador. En una realización, el servicio de acceso 250 valida la contraseña antes de enviar la interfaz 310.

Las Figuras 5A-5B muestran ejemplos de mapas de objetos que definen posiciones asignadas aleatoriamente (o pseudoaleatoriamente) para presentar una pluralidad de objetos gráficos en la pantalla de un dispositivo cliente. En particular, la Figura 5A representa un mapa de objetos 500 correspondiente a una primera solicitud de acceso que incluye un identificador y la Figura 5B representa un mapa de objetos 550 correspondiente a una segunda solicitud de acceso que incluye el mismo identificador de la primera solicitud de acceso. A modo de ejemplo, la primera solicitud de acceso puede ser recibida por un servicio de acceso (por ejemplo, el servicio de acceso 120 de la Figura 1 y el servicio de acceso 250 de la Figura 2) durante una primera sesión, mientras que la segunda solicitud de acceso puede ser recibida por el servicio de acceso durante una segunda sesión posterior a la primera sesión.

Una comparación entre las Figuras 5A y 5B pretende ilustrar que un servicio de acceso implementado de acuerdo con la presente invención enviará diferentes interfaces a través de sesiones de autenticación incluso cuando múltiples peticiones de acceso incluyan el mismo identificador. En los ejemplos ilustrados por las Figuras 5A y 5B, los mapas de objetos 500 y 550 incluyen generalmente cada uno información relativa a: (i) una sesión asociada a una interfaz correspondiente; (ii) objetos gráficos incluidos en la interfaz correspondiente; y (iii) posiciones de visualización de cada objeto gráfico dentro de la interfaz correspondiente.

En los ejemplos de las Figuras 5A y 5B, los mapas de objetos 500 y 550 se representan y describen como si solo incluyeran información gráfica relacionada con objetos pertenecientes a objetos definidos por el usuario. Sin embargo, un experto en la materia apreciará que son posibles otras variaciones. Por ejemplo, en algunas realizaciones, un mapa de objetos también incluirá información gráfica relativa a objetos nulos.

Como se ha indicado anteriormente, los mapas de objetos 500 y 550 corresponden a una primera y segunda solicitudes de acceso, respectivamente, que incluyen cada una el mismo identificador. En este ejemplo, un conjunto de objetos definidos por el usuario consistirá en los objetos gráficos 1.1, 1.2 y 1.3. Por consiguiente, tanto la interfaz definida por el mapa de objetos 500 (la "primera interfaz") como la interfaz definida por el mapa de objetos 550 (la "segunda interfaz") incluyen el mismo conjunto de objetos definidos por el usuario. Sin embargo, a través de la colocación aleatoria o pseudoaleatoria, los objetos gráficos individuales que comprenden ese mismo conjunto de objetos definidos por el usuario se encuentran en diferentes posiciones de visualización dentro de la primera y segunda interfaces.

Por ejemplo, una posición de visualización del objeto gráfico 1.2 en la primera interfaz está próxima al par de coordenadas (x_2, y_2) mientras que dicha posición de visualización está próxima al par de coordenadas (x_4, y_7) en la segunda interfaz. Como otro ejemplo, el par de coordenadas (x_1, y_1) está próximo a una posición de visualización del

objeto gráfico 1.1 en la primera interfaz, mientras que ese par de coordenadas está próximo al objeto gráfico 1.3 en la segunda interfaz. Una de las ventajas de esta variación entre sesiones de las posiciones de visualización de objetos gráficos dentro de las interfaces es que la utilidad de la información obtenida por una entidad maliciosa a partir de la grabación (u observación) de una interfaz presentada en una sesión de autenticación se reduce con respecto a las sesiones de autenticación posteriores. Como tal, la probabilidad de que la entidad maliciosa pueda efectuar con éxito un ataque de repetición (por ejemplo, el ataque de repetición descrito más adelante con respecto a la Figura 6) se reduce.

La Figura 6 representa un ejemplo de ataque de repetición en el servicio de acceso de la Figura 2 por una entidad maliciosa 600 que se hace pasar por el dispositivo cliente de la Figura 2. En este ejemplo, la entidad maliciosa 600 está intentando obtener acceso a recursos protegidos del dominio anfitrión enviando una solicitud de acceso al servicio de acceso 250 que incluye el identificador del usuario del dispositivo cliente 200. De forma similar a los ejemplos representados por las Figuras 2-4, el servicio de acceso 250 utiliza los datos obtenidos del perfil de usuario asociado al identificador incluido en la solicitud de acceso para seleccionar los objetos gráficos adecuados que definen la contraseña gráfica establecida para el perfil de usuario. Dado que la entidad maliciosa 600 envía una solicitud de acceso con el mismo identificador que se incluyó en la solicitud de acceso enviada por el dispositivo cliente 200 en la Figura 2, los objetos gráficos 314A-314D se seleccionan de nuevo para su inclusión en la interfaz 610 como conjunto de objetos definidos por el usuario.

Sin embargo, debido a la variación de sesión a sesión de las posiciones de visualización de objetos gráficos dentro de las interfaces discutidas anteriormente, una comparación entre las Figuras 3 y 6 muestra que las posiciones de visualización de los objetos gráficos 314A-314D dentro de la interfaz 610 son distintas de sus correspondientes posiciones de visualización dentro de la interfaz 310. Como resultado, un mapa de objetos que define las posiciones de visualización de los objetos gráficos dentro de la interfaz 610 será distinto de un mapa de objetos que define las posiciones de visualización de los objetos gráficos dentro de la interfaz 310. Así, cuando la entidad maliciosa 600 envía los mismos datos de entrada al servicio de acceso 250 que fueron enviados por el dispositivo cliente 200 en la Figura 4 con fines de autenticación, el servicio de acceso 250 determinará en este caso que los mismos datos de entrada no satisfacen la contraseña gráfica utilizando el mapa de objetos correspondiente a la interfaz 610. En consecuencia, el servicio de acceso 250 denegará a la entidad maliciosa 600 el acceso al recurso protegido.

La Figura 7 representa un ejemplo de ataque de phishing al dispositivo cliente por parte de una entidad maliciosa 750 que se hace pasar por el servicio de acceso de la Figura 2. En este ejemplo, la entidad maliciosa 750 intenta engañar a un usuario del dispositivo cliente 200 para que introduzca en la interfaz maliciosa 710 información indicativa de la contraseña gráfica establecida para su perfil de usuario. A modo de ejemplo, la entidad maliciosa 750 puede representar a la entidad maliciosa 600 después de su infructuoso ataque de repetición representado en la Figura 6.

Como se discute anteriormente con respecto a la Figura 4, el mapa de objetos para la interfaz 310 almacenado en el servicio de acceso 250 es la única ubicación en la que reside un mapeo de posición de objeto gráfico-pantalla. Además, los datos de entrada enviados por el dispositivo cliente 200 cuando la interfaz 310 se presenta en una pantalla del dispositivo cliente 200 solo incluyen información relacionada con la interacción. Por lo tanto, no se intercambió información que distinguiera entre objetos nulos y objetos seleccionados por el usuario entre el servicio de acceso 250 y el dispositivo cliente 200 durante el proceso de autenticación de ejemplo ilustrado en las Figuras 2-4. De este modo, ninguna información que identificara explícitamente el conjunto de objetos definidos por el usuario que definen la contraseña gráfica establecida para el perfil de usuario asociado al dispositivo cliente 200 estaba disponible para ser interceptada por una entidad maliciosa, tal como la entidad maliciosa 750.

La Figura 7 ilustra un ejemplo de cómo la implementación de la presente invención reduce la probabilidad de que una entidad maliciosa pueda efectuar con éxito un ataque de phishing. Una comparación entre la Figura 7 y la Figura 3 o la Figura 6 ilustra que la interfaz 710 en muchos aspectos parece similar a las interfaces 310 y 610 que fueron generadas cada una por el servicio de acceso 250. Una diferencia notable entre la interfaz 710 y la interfaz 310 o la interfaz 610 es que ninguno de los objetos gráficos incluidos en la interfaz 310 o la interfaz 610 está incluido en la interfaz 710. En particular, ninguno de los objetos gráficos del conjunto de objetos definidos por el usuario que definen la contraseña gráfica establecida para el dispositivo cliente 200 asociado al perfil de usuario está presente en la interfaz 710. El usuario del dispositivo cliente 200 observó la ausencia del objeto definido por el usuario en la interfaz 710, por lo que el dispositivo cliente 200 no registró ningún evento de interacción. Sin ningún evento de interacción registrado, el dispositivo cliente 200 no tiene datos de entrada para enviar a la entidad maliciosa 750. En consecuencia, se frustra el ataque de phishing de la entidad maliciosa 750.

Con referencia a la Figura 8, se ilustra un ejemplo de proceso 800 de autenticación multifactorial utilizando contraseñas gráficas. En una realización, el proceso 800 es efectuado por el servicio de autenticación 122 de la Figura 1. En el bloque 801, se recibe desde un dispositivo cliente una solicitud de acceso que identifica un recurso protegido. La solicitud de acceso que se envía en el bloque 801 incluye un identificador. En el bloque 803, se genera una interfaz que incluye una pluralidad de objetos gráficos para su presentación en ubicaciones aleatorias (o pseudoaleatorias) en una pantalla del dispositivo cliente según lo definido por un primer mapa de objetos. La pluralidad de objetos gráficos de la interfaz generada en el bloque 803 incluye un objeto nulo y un conjunto de objetos definidos por el usuario asociados al identificador que definen una contraseña gráfica. En una realización, la interfaz está asociada con una aplicación que se ejecuta en un servidor anfitrión (por ejemplo, el servidor 130 de la Figura 1) de un

dominio anfitrión.

En el bloque 805, se reciben datos de entrada desde el dispositivo cliente. Los datos de entrada que se reciben desde el dispositivo cliente en el bloque 805 incluyen un evento de entrada para cada interacción con la interfaz que detecta el dispositivo cliente. El evento de entrada para cada interacción identifica una posición en la pantalla en la que se detectó una interacción correspondiente. En el bloque 807, se determina que los datos de entrada satisfacen la contraseña gráfica utilizando el mapa de objetos. En el bloque 809, se concede acceso al recurso protegido en respuesta a la determinación de que los datos de entrada satisfacen la contraseña gráfica.

Con referencia a la Figura 9, se ilustra otro ejemplo de proceso 900 de autenticación multifactorial utilizando contraseñas gráficas. En una realización, el proceso 900 es efectuado por el dispositivo cliente 110 de la Figura 1 y/o el dispositivo cliente 200 de las Figuras 2-4. En el bloque 901, se envía una solicitud de acceso que identifica un recurso protegido a un servicio de acceso de un servidor anfitrión. La solicitud de acceso que se envía en el bloque 901 incluye un identificador. En una realización, la solicitud de acceso incluye además una contraseña asociada al identificador. En respuesta, se recibe una interfaz del servicio de acceso que incluye una pluralidad de objetos gráficos para su presentación en la pantalla en el bloque 903. En una realización en la que la solicitud de acceso incluye además una contraseña asociada al identificador, el servicio de acceso valida la contraseña antes de enviar la interfaz. En una realización, la interfaz está asociada a una aplicación que se ejecuta en el servidor anfitrión.

En el bloque 905, se registra un evento de entrada para cada interacción detectada con la interfaz mientras se presenta la interfaz en la pantalla. Cada evento de entrada registrado en el bloque 905 identifica una posición en la pantalla en la que se detectó la interacción correspondiente. En el bloque 907, los datos de entrada se envían al servicio de acceso que incluye cada entrada registrada. En el bloque 909, se recibe acceso al recurso protegido cuando el servicio de acceso determina que los datos de entrada satisfacen una contraseña gráfica mediante un mapa de objetos. El mapa de objetos define posiciones asignadas aleatoriamente (o pseudoaleatoriamente) para presentar cada uno de la pluralidad de objetos gráficos en la pantalla. La contraseña gráfica está definida por un conjunto de objetos definidos por el usuario que se incluyen entre la pluralidad de objetos gráficos de la interfaz recibida en el bloque 903.

En una realización, cada objeto definido por el usuario entre un conjunto de objetos definidos por el usuario que definen una contraseña gráfica comparten un atributo visual común. En una realización, al menos un objeto definido por el usuario entre un conjunto de objetos definidos por el usuario es un objeto personalizado enviado por un usuario de un dispositivo cliente. En una realización, al menos un objeto definido por el usuario entre un conjunto de objetos definidos por el usuario es un objeto de plantilla seleccionado de entre una pluralidad de objetos de plantilla almacenados en un servidor anfitrión.

En una realización, la contraseña gráfica se define además por un criterio basado en secuencia que especifica un orden para seleccionar cada objeto definido por el usuario entre el conjunto de objetos definidos por el usuario. En una realización, la contraseña gráfica se define además por un criterio basado en el comportamiento que especifica una característica de una interacción para seleccionar al menos un objeto definido por el usuario entre el conjunto de objetos definidos por el usuario.

En una realización, la recepción de acceso al recurso protegido incluye la recepción de una ficha de acceso desde el servicio de acceso para su inclusión en solicitudes posteriores enviadas al servidor anfitrión. En una realización, recibir acceso al recurso protegido incluye recibir un identificador de sesión del servicio de acceso correspondiente a una sesión en un espacio de memoria del servidor anfitrión que permite el acceso al recurso protegido.

En una realización, el proceso 800 y/o el proceso 900 se realizan mediante lógica de procesamiento, incluyendo hardware, firmware, software, o una combinación de los mismos. En una realización, el proceso 800 y/o el proceso 900 se llevan a cabo mediante un procesador que ejecuta un código almacenado en un medio no transitorio legible por ordenador (por ejemplo, una memoria).

Habiendo descrito diversas realizaciones de la invención, se describe ahora un entorno informático ejemplar adecuado para implementar realizaciones de la invención. Con referencia a la Figura 10, el dispositivo cliente 110, el servicio de acceso 120, el servidor 130, la base de datos 140, el dispositivo cliente 200, el servicio de acceso 250, la entidad maliciosa 600 y la entidad maliciosa 750 pueden implementarse en uno o más dispositivos o sistemas informáticos, como el sistema informático 1000 de ejemplo. El sistema informático 1000 puede incluir un procesador 1026, una memoria 1028, un dispositivo de memoria de almacenamiento masivo 1030, una interfaz de entrada/salida (E/S) 1032 y una interfaz hombre-máquina (HMI) 1034. El sistema informático 1000 también puede estar acoplado operativamente a uno o más recursos externos 1036 a través de la red 1023 o la interfaz de E/S 1032. Los recursos externos pueden incluir, entre otros, servidores, bases de datos, dispositivos de almacenamiento masivo, dispositivos periféricos, servicios de red basados en la nube o cualquier otro recurso informático adecuado que pueda utilizar el sistema informático 1000.

El procesador 1026 puede incluir uno o más dispositivos seleccionados entre microprocesadores, microcontroladores, procesadores de señales digitales, microordenadores, unidades centrales de procesamiento, matrices de puertas programables en campo, dispositivos lógicos programables, máquinas de estado, circuitos lógicos, circuitos analógicos, circuitos digitales, o cualquier otro dispositivo que manipule señales (analógicas o digitales) basándose en

instrucciones operativas que se almacenan en la memoria 1028. La memoria 1028 puede incluir un único dispositivo de memoria o una pluralidad de dispositivos de memoria incluyendo, pero sin limitarse a, memoria de solo lectura (ROM), memoria de acceso aleatorio (RAM), memoria volátil, memoria no volátil, memoria estática de acceso aleatorio (SRAM), memoria dinámica de acceso aleatorio (DRAM), memoria flash, memoria caché, o cualquier otro dispositivo capaz de almacenar información. El dispositivo de memoria de almacenamiento masivo 1030 puede incluir dispositivos de almacenamiento de datos como un disco duro, una unidad óptica, una unidad de cinta, un dispositivo de estado sólido no volátil o cualquier otro dispositivo capaz de almacenar información.

El procesador 1026 puede operar bajo el control de un sistema operativo 1038 que reside en la memoria 1028. El sistema operativo 1038 puede gestionar recursos informáticos para que el código de programa informático incorporado como una o más aplicaciones de software informático, como una aplicación 1040 que reside en la memoria 1028, pueda tener instrucciones ejecutadas por el procesador 1026. En una realización alternativa, el procesador 1026 puede ejecutar la aplicación 1040 directamente, en cuyo caso el sistema operativo 1038 puede omitirse. Una o más estructuras de datos 1042 también pueden residir en la memoria 1028, y pueden ser utilizadas por el procesador 1026, el sistema operativo 1038, o la aplicación 1040 para almacenar o manipular datos.

La interfaz de E/S 1032 puede proporcionar una interfaz de máquina que acopla operativamente el procesador 1026 a otros dispositivos y sistemas, tales como la red 1023 o el uno o más recursos externos 1036. La aplicación 1040 puede así trabajar en cooperación con la red 1023 o los recursos externos 1036 comunicándose a través de la interfaz de E/S 1032 para proporcionar las diversas características, funciones, aplicaciones, procesos o módulos que comprenden las realizaciones de la invención. La aplicación 1040 también puede tener código de programa que es ejecutado por uno o más recursos externos 1036, o de otro modo depender de funciones o señales proporcionadas por otros componentes del sistema o de la red externos al sistema informático 1000. De hecho, dadas las casi infinitas configuraciones de hardware y software posibles, las personas con conocimientos ordinarios en la materia entenderán que las realizaciones de la invención pueden incluir aplicaciones que se encuentran fuera del sistema informático 1000, distribuidas entre múltiples ordenadores u otros recursos externos 1036, o proporcionadas por recursos informáticos (hardware y software) que se proporcionan como un servicio a través de la red 1023, como un servicio de computación en la nube.

La HMI 1034 puede estar acoplada operativamente al procesador 1026 del sistema informático 1000 de una manera conocida para permitir a un usuario interactuar directamente con el sistema informático 1000. La HMI 1034 puede incluir pantallas de vídeo o alfanuméricas, una pantalla táctil, un altavoz y cualquier otro indicador sonoro y visual adecuado capaz de proporcionar datos al usuario. La HMI 1034 también puede incluir dispositivos de entrada y controles como un teclado alfanumérico, un dispositivo señalador, teclados, pulsadores, mandos de control, micrófonos, etc., capaces de aceptar comandos o entradas del usuario y transmitir la entrada introducida al procesador 1026.

Una base de datos 1044 puede residir en el dispositivo de memoria de almacenamiento masivo 1030, y puede utilizarse para recopilar y organizar datos utilizados por los diversos sistemas y módulos descritos en el presente documento. La base de datos 140, el mapa de objetos 500 y el mapa de objetos 550 pueden implementarse utilizando una o más bases de datos, tal como la base de datos 1044. La base de datos 1044 puede incluir datos y estructuras de datos de apoyo que almacenan y organizan los datos. En particular, la base de datos 1044 puede disponerse con cualquier organización o estructura de base de datos incluyendo, pero sin limitarse a, una base de datos relacional, una base de datos jerárquica, una base de datos de red, o combinaciones de las mismas. Un sistema de gestión de base de datos en la forma de una aplicación de software de ordenador que se ejecuta como instrucciones en el procesador 1026 puede ser utilizado para acceder a la información o datos almacenados en registros de la base de datos 1044 en respuesta a una consulta, donde una consulta puede ser determinada dinámicamente y ejecutada por el sistema operativo 1038, otras aplicaciones 1040, o uno o más módulos.

En general, las rutinas ejecutadas para implementar las realizaciones de la invención, ya sean implementadas como parte de un sistema operativo o una aplicación específica, componente, programa, objeto, módulo o secuencia de instrucciones, o incluso un subconjunto de las mismas, pueden ser referidas aquí como "código de programa de ordenador, o simplemente "código de programa". El código de programa comprende típicamente instrucciones legibles por ordenador que residen en diversos momentos en diversas memorias y dispositivos de almacenamiento de un ordenador y que, cuando son leídas y ejecutadas por uno o más procesadores de un ordenador, hacen que dicho ordenador realice las operaciones necesarias para ejecutar operaciones y/o elementos que encarnan los diversos aspectos de las realizaciones de la invención. Las instrucciones de programa legibles por ordenador para llevar a cabo las operaciones de las realizaciones de la invención pueden ser, por ejemplo, lenguaje ensamblador o código fuente o código objeto escrito en cualquier combinación de uno o más lenguajes de programación.

El código de programa incorporado en cualquiera de las aplicaciones/módulos descritos en el presente documento puede distribuirse individual o colectivamente como un producto de programa en una variedad de formas diferentes. En particular, el código de programa puede distribuirse usando un medio de almacenamiento legible por ordenador que tiene instrucciones de programa legibles por ordenador para hacer que un procesador lleve a cabo aspectos de las realizaciones de la invención.

Los medios de almacenamiento legibles por ordenador, que no son transitorios de manera inherente, pueden incluir medios tangibles volátiles y no volátiles, amovibles y no amovibles implementados en cualquier método o tecnología para el almacenamiento de información, tal como instrucciones legibles por ordenador, estructuras de datos, módulos de programas u otros datos. Los medios de almacenamiento legibles por ordenador pueden incluir además memoria de acceso aleatorio (RAM), memoria de solo lectura (ROM), memoria de solo lectura programable y borrable (EPROM), memoria de solo lectura programable y borrable eléctricamente (EEPROM), memoria flash u otra tecnología de memoria de estado sólido, disco compacto portátil de memoria de solo lectura (CD-ROM), u otro almacenamiento óptico, casetes magnéticos, cinta magnética, almacenamiento en disco magnético u otros dispositivos de almacenamiento magnético, o cualquier otro medio que pueda usarse para almacenar la información deseada y que puede ser leído por un ordenador. Un medio de almacenamiento legible por ordenador no debe interpretarse como señales transitorias por sí mismas (por ejemplo, ondas de radio u otras ondas electromagnéticas que se propagan, ondas electromagnéticas que se propagan a través de un medio de transmisión como una guía de ondas, o señales eléctricas transmitidas a través de un cable). Las instrucciones de programa legibles por ordenador pueden descargarse a un ordenador, otro tipo de aparato de procesamiento de datos programable u otro dispositivo desde un medio de almacenamiento legible por ordenador o a un ordenador externo o dispositivo de almacenamiento externo a través de una red.

Las instrucciones de programas legibles por ordenador almacenadas en un medio legible por ordenador pueden usarse para dirigir un ordenador, otros tipos de aparatos de procesamiento de datos programables u otros dispositivos para que funcionen de una manera particular, de modo que las instrucciones almacenadas en el medio legible por ordenador produzcan un artículo de fabricación, incluyendo instrucciones que implementan las funciones/actos especificadas en los diagramas de flujo, diagramas de secuencia y/o diagramas de bloques. Las instrucciones del programa informático pueden proporcionarse a uno o más procesadores de un ordenador de propósito general, un ordenador de propósito especial u otro aparato programable de procesamiento de datos para producir una máquina, de tal manera que las instrucciones, que se ejecutan a través de uno o más procesadores, causan una serie de cálculos a realizar para implementar las funciones y/o actos especificadas en los diagramas de flujo, diagramas de secuencia y/o diagramas de bloques.

En ciertas realizaciones alternativas, las funciones y/o actos especificados en los diagramas de flujo, diagramas de secuencia, y/o diagramas de bloques pueden ser reordenados, procesados en serie, y/o procesados concurrentemente sin apartarse del alcance de las realizaciones de la invención. Además, cualquiera de los diagramas de flujo, diagramas de secuencia y/o diagramas de bloques puede incluir más o menos bloques que los ilustrados de acuerdo con las realizaciones de la invención.

La terminología usada en el presente documento tiene la finalidad de describir realizaciones particulares solamente y no se pretende que sea limitante de las realizaciones de la invención. Se entenderá además que los términos "comprende", "que comprende", "incluye" y/o "incluyendo", cuando se usan en este documento, especifican la presencia de características, enteros, artículos, etapas, operaciones, elementos y/o componentes indicados, pero no excluye la presencia o adición de una o más características, artículos, enteros, etapas, operaciones, elementos, componentes y/o grupos de los mismos. Además, en la medida en que los términos "incluye", "teniendo", "tiene", "con", "compuesto de", o variantes de los mismos se utilizan en la descripción detallada o en las reivindicaciones, dichos términos pretenden ser inclusivos de manera similar al término "que comprende".

Aunque toda la invención ha sido ilustrada mediante la descripción de diversas realizaciones y aunque estas realizaciones han sido descritas con todo detalle, no es intención del solicitante restringir o limitar de ninguna manera el alcance a tales detalles. Ventajas y modificaciones adicionales aparecerán fácilmente a los expertos en la técnica. Por lo tanto, la invención en sus aspectos más amplios no se limita a los detalles específicos, aparatos y método representativos, y a los ejemplos ilustrativos mostrados y descritos.

REIVINDICACIONES

1. Un método mediante un dispositivo de servicio de acceso (120) configurado para autenticar un dispositivo cliente (800), comprendiendo el método:
 - 5 recibir una primera solicitud de acceso que identifique un recurso protegido desde el dispositivo cliente (801), incluyendo la primera solicitud de acceso un identificador;
 - 10 generar una primera interfaz que incluya una pluralidad de objetos gráficos para su presentación en ubicaciones aleatorias en una pantalla del dispositivo cliente según lo definido por un primer mapa de objetos (803), incluyendo la pluralidad de objetos gráficos un objeto señuelo y un conjunto de objetos definidos por el usuario asociados con el identificador que definen una contraseña gráfica, estando la contraseña gráfica definida además por un orden específico en el que el conjunto de objetos definidos por el usuario deben ser seleccionados;
 - recibir datos de entrada que incluyan un evento de entrada para cada interacción con la primera interfaz que el dispositivo cliente detecte (805), identificando el evento de entrada para cada interacción una posición en la pantalla en la que se detectó una interacción correspondiente, e identificando los datos de entrada que no incluyan información los objetos gráficos de la primera interfaz;
 - 15 determinar que los datos de entrada satisfacen la contraseña gráfica utilizando el primer mapa de objetos (807) evaluando la posición identificada por el evento de entrada para cada interacción con el primer mapa de objetos para identificar un objeto gráfico concreto que se seleccionó en una interacción dada; y
 - en respuesta a la determinación de que los datos de entrada satisfacen la contraseña gráfica, conceder acceso al recurso protegido (809),
 - 20 en el que determinar que los datos de entrada satisfacen la contraseña gráfica utilizando el primer mapa de objetos (807) comprende:
 - evaluar la posición en la pantalla de cada evento de entrada utilizando el primer mapa de objetos y las marcas de tiempo asociadas a cada evento de entrada; y
 - 25 determinar, basándose en la posición evaluada en la pantalla de cada evento de entrada y en las marcas de tiempo evaluadas asociadas a cada evento de entrada, que cada objeto definido por el usuario que define la contraseña gráfica fue seleccionado en el orden especificado sin seleccionar el objeto señuelo.
2. El método (800) de la reivindicación 1, que comprende además:
 - recibir una segunda solicitud de acceso que incluya el identificador; y
 - 30 en respuesta, generar una segunda interfaz que incluya el conjunto de objetos definidos por el usuario para su presentación en posiciones aleatorias en la pantalla del dispositivo cliente según lo definido por un segundo mapa de objetos,
 - en el que el primer mapa de objetos y el segundo mapa de objetos definen diferentes posiciones en la pantalla para al menos un objeto definido por el usuario entre el conjunto de objetos definidos por el usuario.
3. El método (800) de la reivindicación 1 o 2, que comprende además:
 - 35 antes de conceder acceso al recurso protegido, activar un campo de entrada de contraseña de la interfaz en respuesta a la determinación de que los datos de entrada satisfacen la contraseña gráfica.
4. El método (800) de una cualquiera de las reivindicaciones 1 a 3, en el que cada objeto definido por el usuario entre el conjunto de objetos definidos por el usuario comparte un atributo visual común.
5. El método (800) de una cualquiera de las reivindicaciones 1 a 4, en el que al menos un objeto definido por el usuario entre el conjunto de objetos definidos por el usuario es un objeto personalizado enviado por un usuario del dispositivo cliente.
- 40 6. El método (800) de una cualquiera de las reivindicaciones 1 a 5, en el que al menos un objeto definido por el usuario entre el conjunto de objetos definidos por el usuario incluye datos de imagen obtenidos mediante un sensor de imagen del dispositivo cliente.
7. El método (800) de una cualquiera de las reivindicaciones 1 a 6, en el que al menos un objeto definido por el usuario entre el conjunto de objetos definidos por el usuario es un objeto plantilla seleccionado de entre una pluralidad de objetos plantilla almacenados en un servidor anfitrión.

8. El método (800) de una cualquiera de las reivindicaciones 1 a 7, en el que la concesión de acceso al recurso protegido (809) incluye:

enviar una ficha de acceso al dispositivo cliente que el dispositivo cliente envía a un servidor anfitrión que almacena el recurso protegido.

5 9. El método (800) de una cualquiera de las reivindicaciones 1 a 8, en el que la concesión de acceso al recurso protegido (809) incluye:

generar una sesión en un espacio de memoria de un servidor anfitrión que permita al dispositivo cliente acceder al recurso protegido.

10. Un dispositivo de servicio de acceso (120) configurado para autenticar un dispositivo cliente, que comprende:

10 un procesador; y

un medio de almacenamiento legible por ordenador que comprende instrucciones que al ser ejecutadas por el procesador hacen que el dispositivo de servicio de acceso (120) realice operaciones, comprendiendo las operaciones:

recibir una primera solicitud de acceso que identifique un recurso protegido desde el dispositivo cliente, incluyendo la primera solicitud de acceso un identificador;

15 generar una primera interfaz que incluya una pluralidad de objetos gráficos para su presentación en ubicaciones aleatorias en una pantalla del dispositivo cliente según lo definido por un primer mapa de objetos, incluyendo la pluralidad de objetos gráficos un objeto señuelo y un conjunto de objetos definidos por el usuario asociados con el identificador que definen una contraseña gráfica, estando la contraseña gráfica definida además por un orden específico en el que el conjunto de objetos definidos por el usuario deben ser seleccionados;

20 recibir datos de entrada que incluyan un evento de entrada para cada interacción con la primera interfaz que el dispositivo cliente detecte, identificando el evento de entrada para cada interacción una posición en la pantalla en la que se detectó una interacción correspondiente, e identificando los datos de entrada que no incluyan información los objetos gráficos de la primera interfaz;

25 determinar que los datos de entrada satisfacen la contraseña gráfica utilizando el primer mapa de objetos evaluando la posición identificada por el evento de entrada para cada interacción con el primer mapa de objetos para identificar un objeto gráfico concreto que se seleccionó en una interacción dada; y

en respuesta a la determinación de que los datos de entrada satisfacen la contraseña gráfica, conceder acceso al recurso protegido,

30 en el que determinar que los datos de entrada satisfacen la contraseña gráfica utilizando el primer mapa de objetos comprende:

evaluar la posición en la pantalla de cada evento de entrada utilizando el primer mapa de objetos y las marcas de tiempo asociadas a cada evento de entrada; y

35 determinar, basándose en la posición evaluada en la pantalla de cada evento de entrada y en las marcas de tiempo evaluadas asociadas a cada evento de entrada, que cada objeto definido por el usuario que define la contraseña gráfica fue seleccionado en el orden especificado sin seleccionar el objeto señuelo.

11. El dispositivo de servicio de acceso (120) de la reivindicación 10, en el que el medio de almacenamiento legible por ordenador comprende además instrucciones que al ser ejecutadas por el procesador hacen que el dispositivo de servicio de acceso (120) realice operaciones según el método de una cualquiera de las reivindicaciones 2 a 9.

40 12. Un producto de programa de ordenador que comprende instrucciones de código de programa almacenadas en un medio legible por ordenador para ejecutar las etapas del método según una cualquiera de las reivindicaciones 1 a 9 cuando dicho programa se ejecuta en un dispositivo de servicio de acceso (120).

Fig. 1

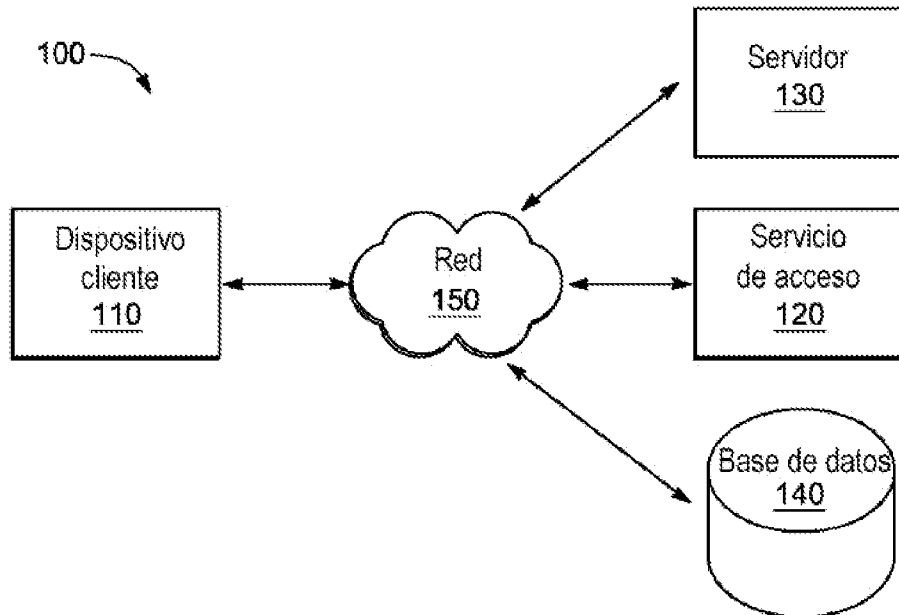
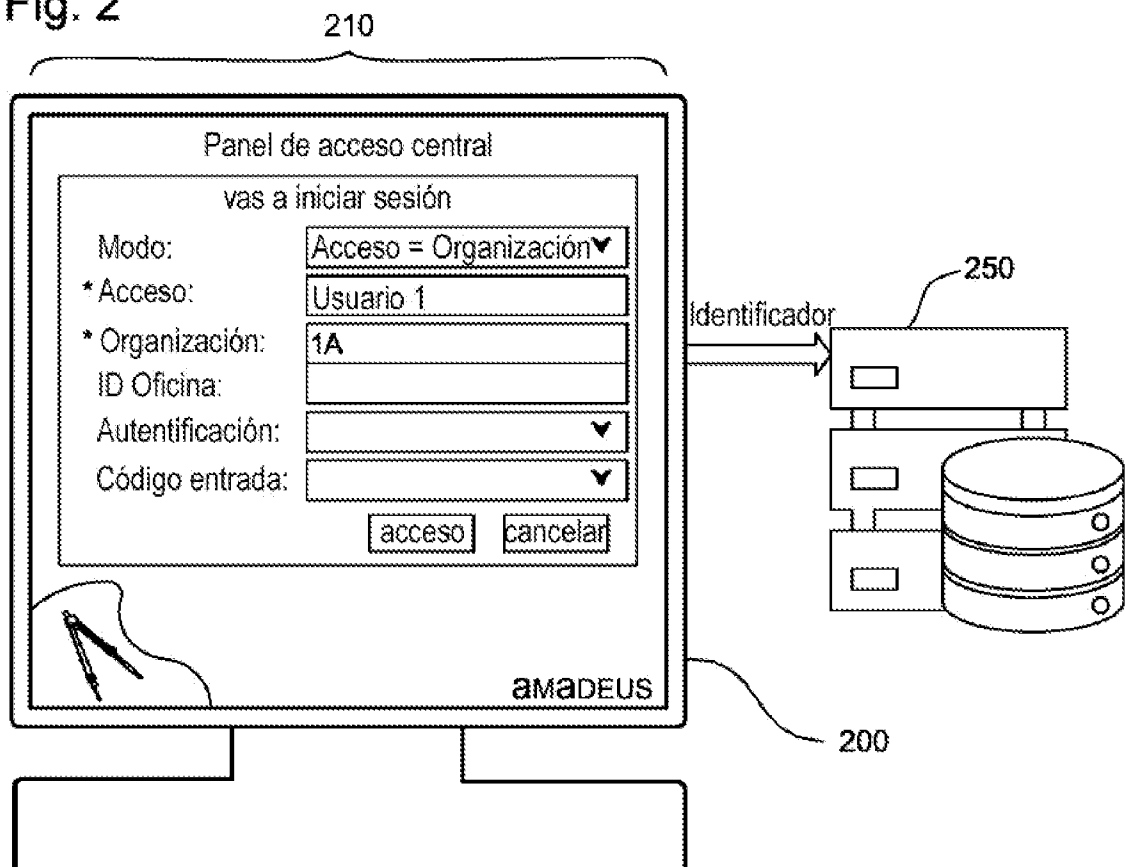


Fig. 2



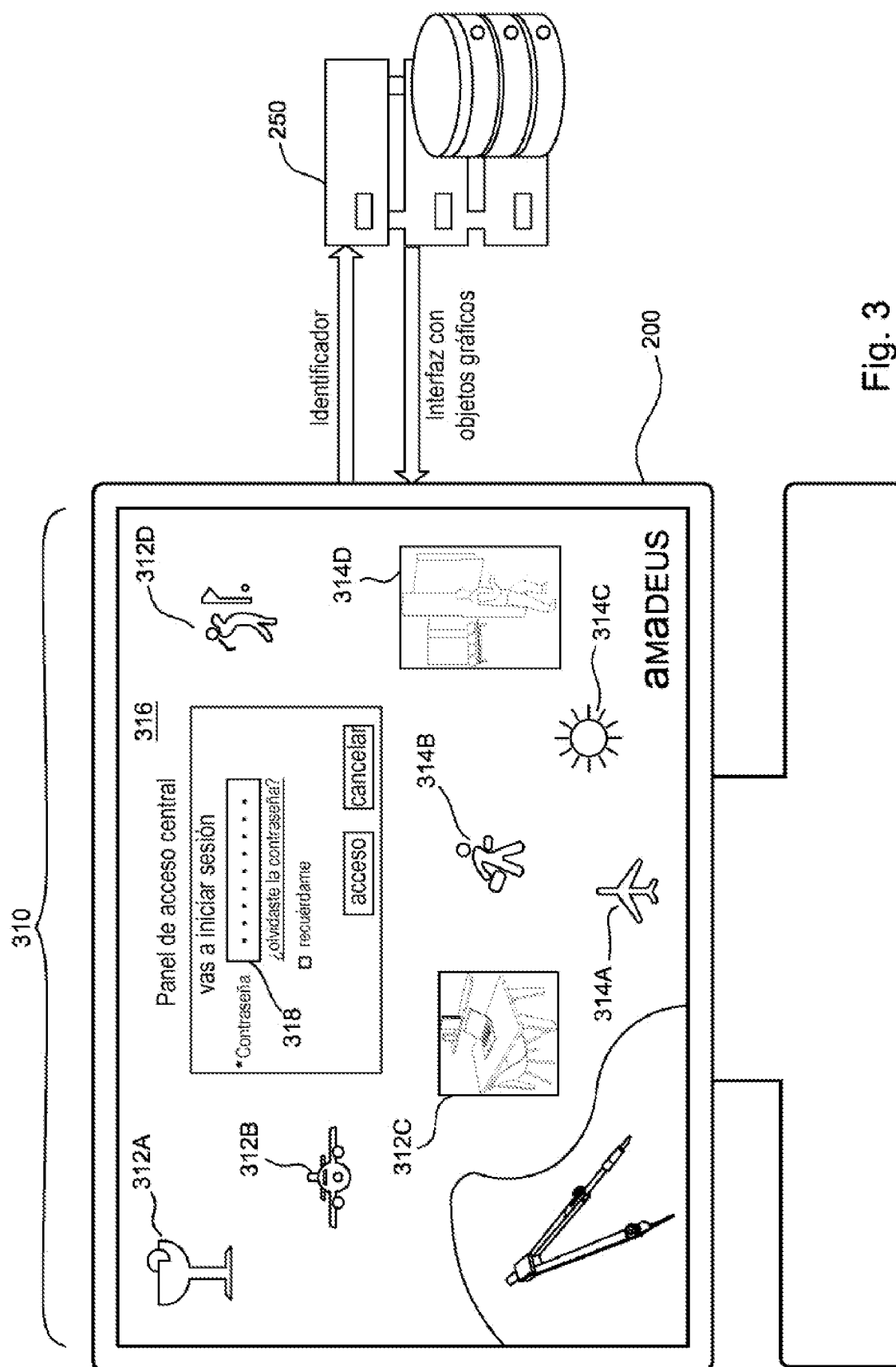


Fig. 3

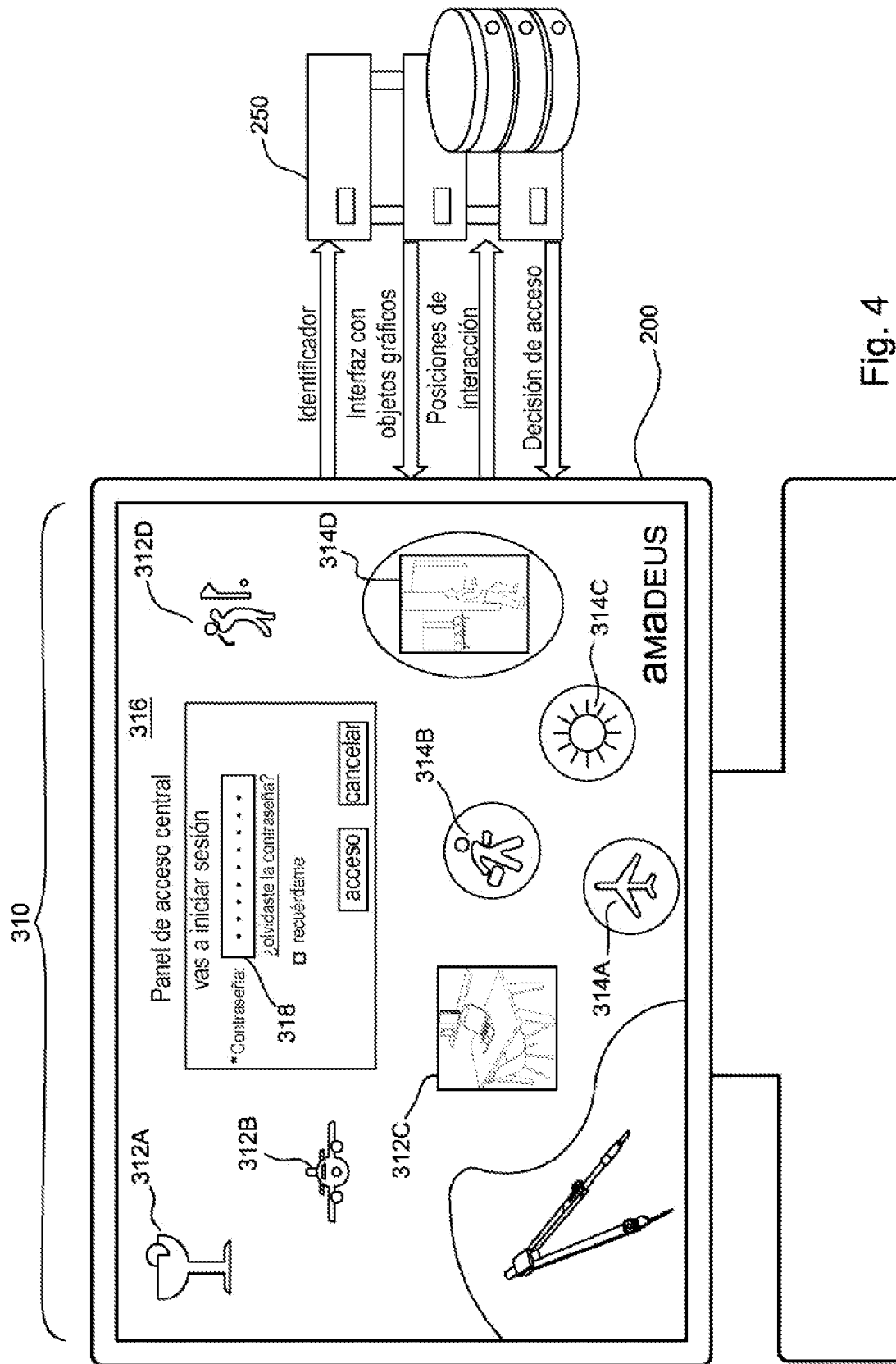


Fig. 4

Fig. 5A

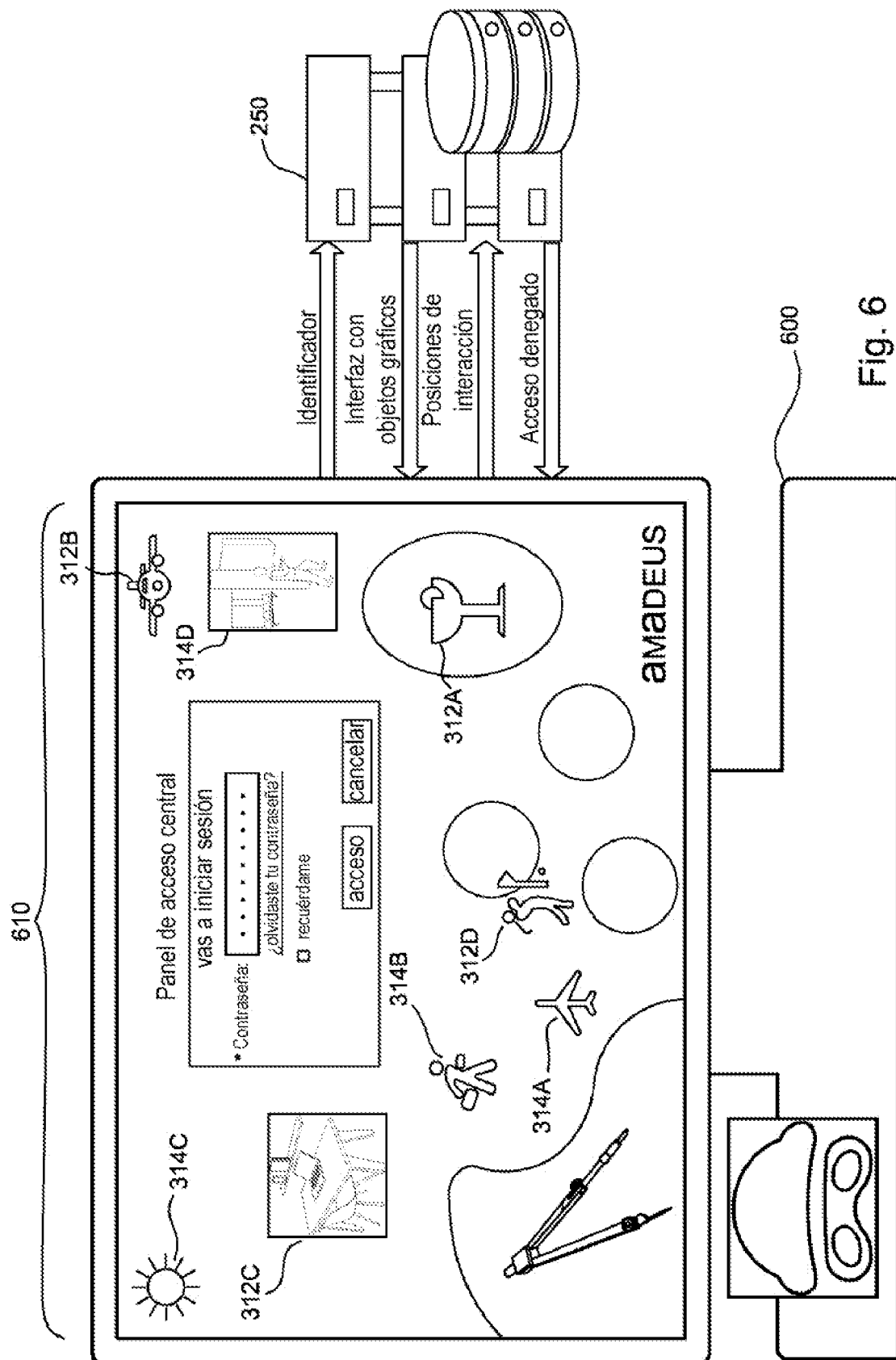
500 

Sesión	Objeto	Posición pantalla
Sesión 1	Obj1.1	Coordenada(x_1, y_1)
Sesión 1	Obj1.2	Coordenada(x_2, y_2)
Sesión 1	Obj1.3	Coordenada(x_3, y_3)
...	...	...

Fig. 5B

550 

Sesión	Objeto	Posición pantalla
Sesión 2	Obj1.1	Coordenada(x_3, y_2)
Sesión 2	Obj1.2	Coordenada(x_4, y_7)
Sesión 2	Obj1.3	Coordenada(x_1, y_1)
...	...	...



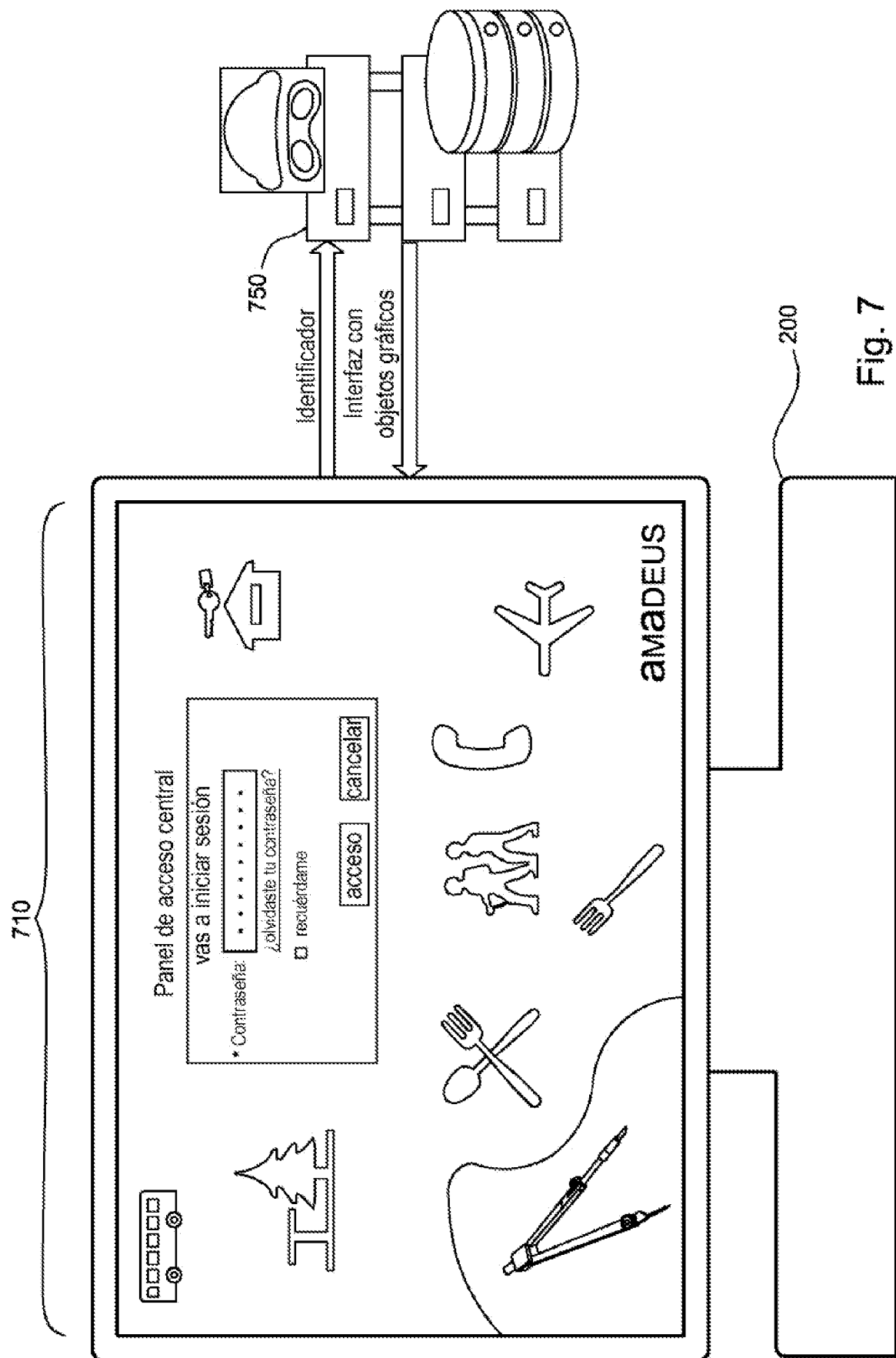


Fig. 7

Fig. 8

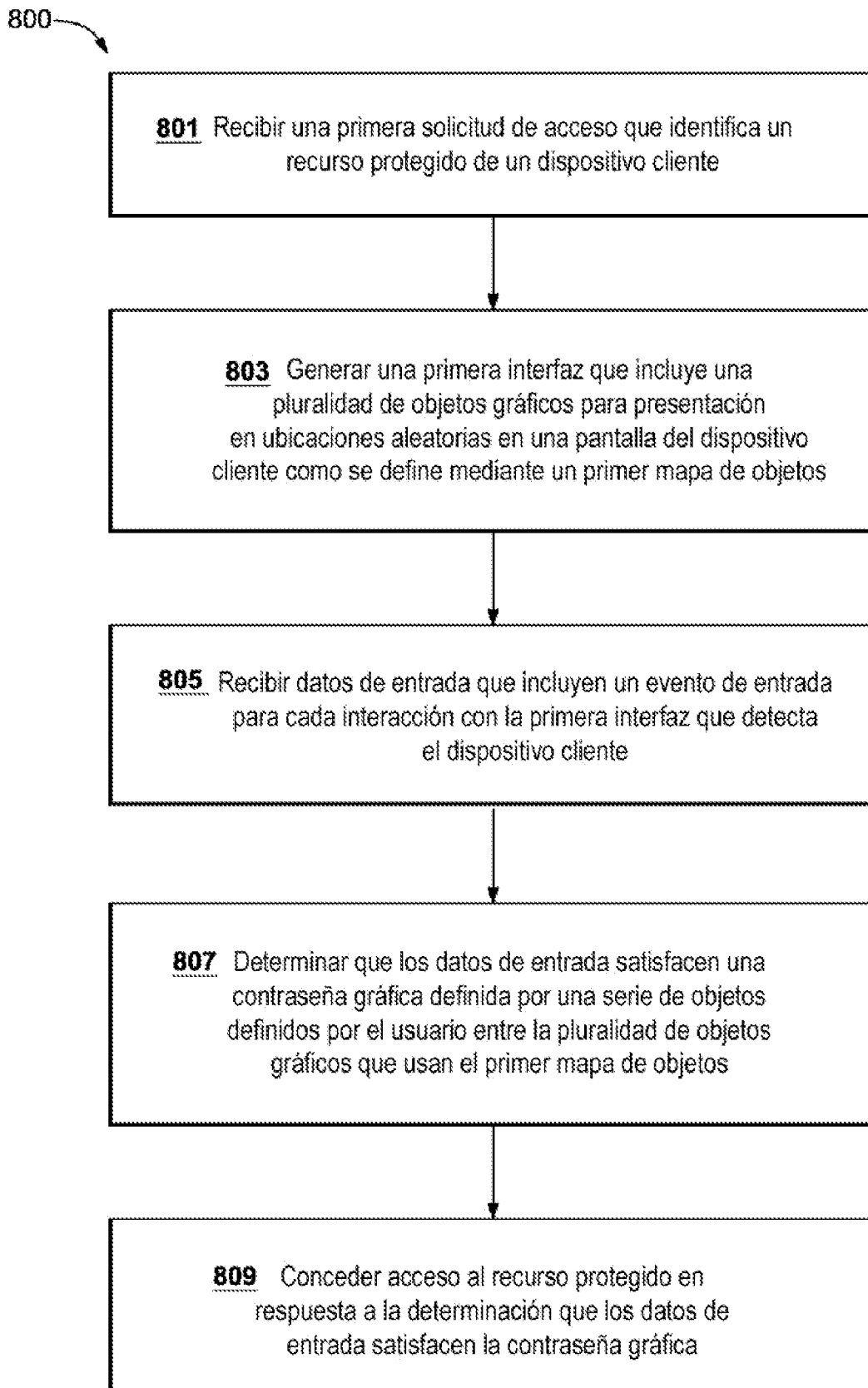


Fig. 9

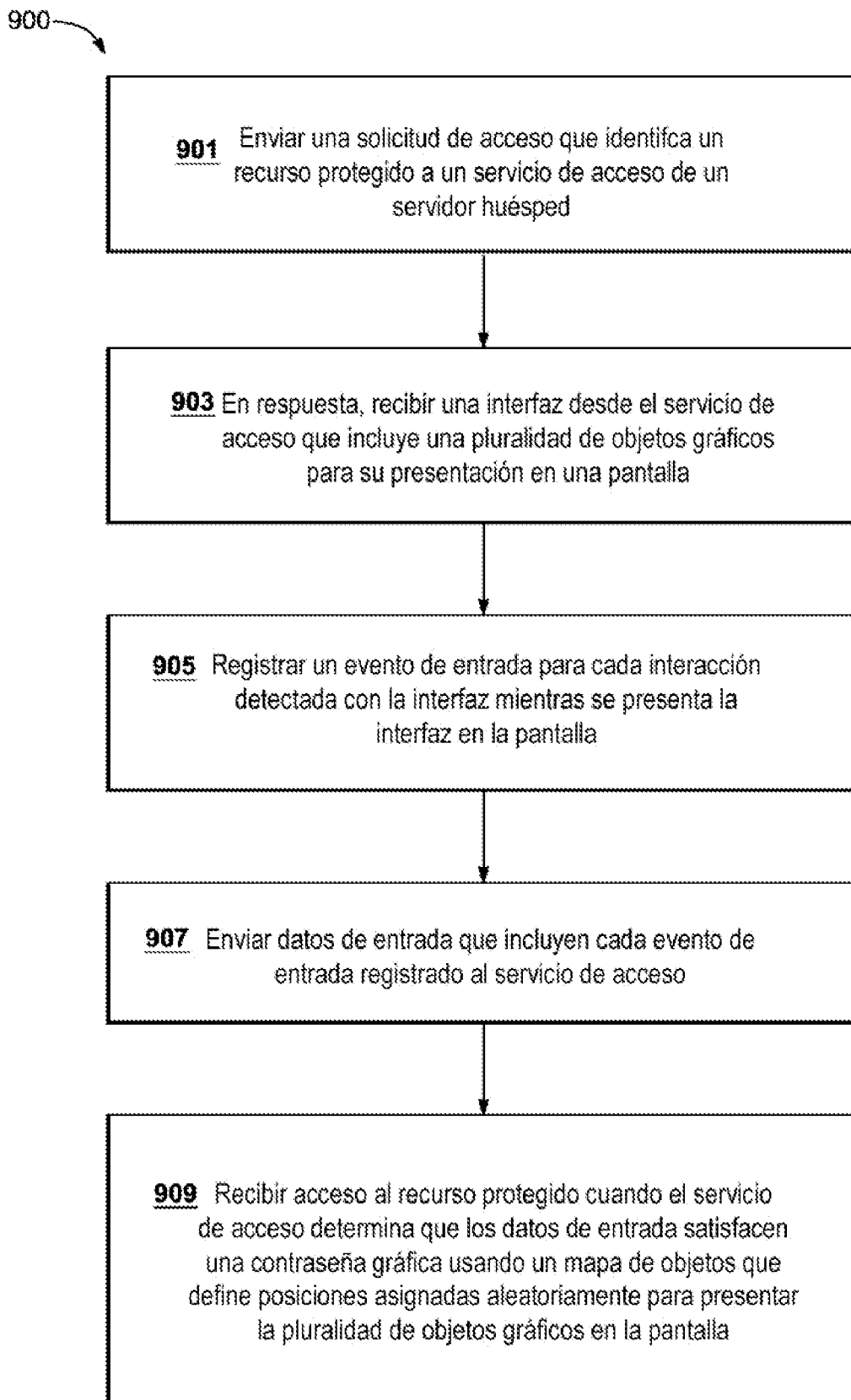


Fig. 10

