(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 812 541**

(51) Int. CI.:

G06F 21/35	(2013.01)
G06F 21/43	(2013.01)
G06F 21/32	(2013.01)
H04W 12/04	(2009.01)
H04W 4/80	(2008.01)
H04W 76/10	(2008.01)
H04W 12/06	(2009.01)
H04L 29/06	(2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **16.12.2014 PCT/US2014/070485**

(87) Fecha y número de publicación internacional: **09.07.2015 WO15102880**

(96) Fecha de presentación y número de la solicitud europea: **16.12.2014 E 14825533 (4)**

(97) Fecha y número de publicación de la concesión europea: **27.05.2020 EP 3090373**

(54) Título: **Aparato de autenticación con interfaz Bluetooth**

(30) Prioridad:

30.12.2013 US 201361921743 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
17.03.2021

(73) Titular/es:

ONESPAN INTERNATIONAL GMBH (100.0%)
World-Wide Business Center, Balz-Zimmermannstrasse 7
8152 Glattbrugg, CH

(72) Inventor/es:

GRANGE, BENOIT;
VERREPT, JOHAN y
CLAES, MATHIAS

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Aparato de autenticación con interfaz Bluetooth

Referencia cruzada a solicitud relacionada

Esta solicitud reivindica la prioridad de la Solicitud Provisoria de los Estados Unidos con Núm. de Serie 61/921.743 titulada "An Authentication Apparatus with a Bluetooth Interface", presentada el 30 de diciembre de 2013.

Campo de la invención

La invención se refiere al aseguramiento de acceso remoto a ordenadores y aplicaciones y transacciones remotas a través de redes de ordenadores. Más específicamente, la invención se refiere a procedimientos y aparatos para autenticación de usuarios a servidores de aplicaciones remotas usando una conexión Bluetooth entre un dispositivo de autenticación y un ordenador huésped.

Antecedentes de la invención

A medida que el acceso remoto a los sistemas y aplicaciones informáticas crece en popularidad, la cantidad y variedad de transacciones a las que se accede de forma remota a través de redes públicas tal como Internet ha aumentado drásticamente. Esta popularidad ha destacado la necesidad de seguridad; en particular: cómo asegurar que las personas que acceden de forma remota a una aplicación sean quienes dicen ser, cómo asegurar que las transacciones que se realizan de forma remota sean iniciadas por individuos legítimo y cómo asegurar que los datos de las transacciones no se hayan modificado antes de ser recibidos en un servidor de aplicaciones.

En el pasado, los proveedores de aplicaciones han confiado en contraseñas estáticas para proporcionar seguridad a las aplicaciones remotas. En los últimos años se ha hecho evidente que las contraseñas estáticas no son suficientes y que se requiere una tecnología de seguridad más avanzada.

Las alternativas al procedimiento de autenticación de contraseña estática bien conocido deben ser preferentemente rentables, confiables y convenientes para el usuario. El documento US 2011/099384 A1 se refiere a un aparato para generación de diferentes credenciales dinámicas para diferentes proveedores de aplicaciones. El usuario puede usar un token de autenticación fuerte para generar credenciales dinámicas para diferentes proveedores de aplicaciones sin la necesidad de compartir secretos mediante claves almacenadas combinadas criptográficas. El documento US 2013/268767 A1 se refiere a un procedimiento para autenticación de a un usuario usando un dispositivo de señal inalámbrico. Se usa para autenticación de un usuario en una sesión de computación particular alojada remotamente desde el dispositivo de computación, en base a los datos recibidos del dispositivo de token inalámbrico.

Descripción de la invención

La invención se define mediante las reivindicaciones independientes adjuntas. Un aspecto de la invención proporciona un dispositivo de autenticación con una interfaz Bluetooth para generación de una credencial dinámica.

En algunas realizaciones el dispositivo de autenticación (100) puede ser un aparato de mano portátil. En algunas realizaciones el dispositivo de autenticación puede comprender: un componente de almacenamiento (130) adaptado para almacenar de forma segura una clave secreta de generación de credenciales criptográficas; una interfaz de entrada de usuario (120) para recepción de entradas de un usuario del dispositivo de autenticación; una interfaz de salida de usuario (110) para presentación de salidas al usuario; un componente de procesamiento de datos (140) adaptado para generar dicha credencial dinámica mediante la combinación criptográfica de dicha clave secreta de generación de credenciales criptográficas con una variable dinámica; y una interfaz Bluetooth (150) para conexión del dispositivo de autenticación a un ordenador huésped usando una conexión Bluetooth entre el dispositivo de autenticación y dicho ordenador huésped; en el que dicho dispositivo de autenticación está adaptado para enviar dicha credencial dinámica generada a través de la conexión Bluetooth con dicho ordenador huésped.

En algunas realizaciones el dispositivo de autenticación puede ser cualquiera de los dispositivos de autenticación de las realizaciones anteriores que además comprenden: un reloj (160) para proporcionar un valor de tiempo; en el que el dispositivo de autenticación también está adaptado para determinar un valor de dicha variable dinámica en función de dicho valor de tiempo proporcionado por dicho reloj.

En algunas realizaciones el dispositivo de autenticación puede ser cualquiera de los dispositivos de autenticación de las realizaciones anteriores además adaptado para: almacenar en dicho componente de almacenamiento una segunda variable; determinar un valor de dicha variable dinámica en función de dicha segunda variable almacenada; y actualizar y almacenar en el componente de almacenamiento el valor de la segunda variable cuando el valor de la segunda variable se ha usado para generar dicha credencial dinámica. En algunas realizaciones dicha segunda variable puede comprender un contador y actualizar dicha segunda variable puede comprender al menos uno de aumentar monotónicamente (o incrementar) o reducir monotónicamente (o disminuir) el valor de dicho contador. Por ejemplo, en algunas realizaciones la variable dinámica puede ser un contador que el dispositivo de autenticación puede almacenar en su memoria y puede aumentar (o disminuir) en uno cada vez que el componente de procesamiento de

datos del dispositivo de autenticación genere una credencial dinámica.

En algunas realizaciones el dispositivo de autenticación puede ser cualquiera de los dispositivos de autenticación de las realizaciones anteriores además adaptado para recibir a través de dicha conexión Bluetooth una solicitud para dicha credencial dinámica, para generar dicha credencial dinámica (por ejemplo, mediante el componente de procesamiento de datos) en respuesta a dicha solicitud y retornar dicha credencial dinámica generada a través de dicha conexión Bluetooth. En algunas realizaciones el dispositivo de autenticación también puede estar adaptado para capturar, por ejemplo, después de recibir dicha solicitud, por medio de dicha interfaz de entrada de usuario una aprobación de dicho usuario para generar o retornar dicha credencial dinámica antes de generar o retornar dicha credencial dinámica. En algunas realizaciones, la generación y el retorno de dicha credencial dinámica mediante dicho dispositivo de autenticación pueden ser condicionales en dicha aprobación de usuario.

En algunas realizaciones el dispositivo de autenticación puede ser cualquiera de los dispositivos de autenticación de las realizaciones anteriores además adaptado para recibir a través de dicha conexión Bluetooth un desafío y usar dicho desafío recibido en dicha generación de dicha credencial dinámica. En algunas realizaciones, el desafío puede estar contenido en una solicitud para generar y retornar una credencial dinámica que recibe el dispositivo de autenticación a través de dicha conexión Bluetooth.

En algunas realizaciones el dispositivo de autenticación puede ser cualquiera de los dispositivos de autenticación de las realizaciones anteriores además adaptado para recibir a través de dicha de conexión Bluetooth datos relacionados con transacciones, para presentar dichos datos relacionados con transacciones recibidos al usuario por dicha interfaz de salida de usuario, para capturar por dicha interfaz de entrada de usuario una aprobación de dicho usuario de dichos datos relacionados con transacciones y para usar dichos datos relacionados con transacciones recibidos en dicha generación de dicha credencial dinámica. En algunas realizaciones la generación y el retorno de dicha credencial dinámica por dicho dispositivo de autenticación pueden ser condicionales a dicha aprobación de usuario de dichos datos relacionados con transacciones. En algunas realizaciones los datos relacionados con transacciones pueden incluir datos de transacción que representan una transacción que un usuario ha solicitado que realice una aplicación.

En algunas realizaciones el dispositivo de autenticación puede ser cualquiera de los dispositivos de autenticación de las realizaciones anteriores además adaptado para almacenar un elemento de datos de identificación del dispositivo y poner a disposición dicho elemento de datos de identificación del dispositivo a dicho ordenador huésped a través de dicha conexión Bluetooth.

En algunas realizaciones el dispositivo de autenticación puede ser cualquiera de los dispositivos de autenticación de las realizaciones anteriores además adaptado para almacenar un nombre de usuario y poner a disposición dicho nombre de usuario a dicho ordenador huésped a través de dicha conexión Bluetooth. En algunas realizaciones el dispositivo de autenticación también puede estar adaptado para recibir dicho nombre de usuario a través de dicha conexión Bluetooth and para almacenar dicho nombre de usuario para la posterior recuperación a través de dicha conexión Bluetooth.

En algunas realizaciones el dispositivo de autenticación puede ser cualquiera de los dispositivos de autenticación de las realizaciones anteriores además adaptado para poner a disposición un estado de aplicación a dicho ordenador huésped a través de dicha conexión Bluetooth.

En algunas realizaciones el dispositivo de autenticación puede ser cualquiera de los dispositivos de autenticación de las realizaciones anteriores además adaptado para enviar a través de dicha conexión Bluetooth a dicho ordenador huésped uno o más comandos para ser ejecutados por dicho ordenador huésped.

En algunas realizaciones el dispositivo de autenticación puede ser cualquiera de los dispositivos de autenticación de las realizaciones anteriores además adaptado para verificar un PIN y/o contraseña. En algunas realizaciones el dispositivo de autenticación también puede estar adaptado para capturar dicho PIN y/o contraseña que se proporcionan al dispositivo de autenticación a través de dicha interfaz de entrada de usuario. En algunas realizaciones el dispositivo de autenticación también puede estar adaptado para recibir dicho PIN y/o contraseña a través de dicha conexión Bluetooth. En algunas realizaciones el dispositivo de autenticación también puede estar adaptado para generar dicha credencial dinámica solo si fue exitosa dicha verificación de dicho PIN y/o contraseña.

En algunas realizaciones el dispositivo de autenticación puede ser cualquiera de los dispositivos de autenticación de las realizaciones anteriores además adaptado para almacenar datos de referencia biométricos y para verificar una medición biométrica de dicho usuario. En algunas realizaciones el dispositivo de autenticación también puede comprender un sensor biométrico y también puede estar adaptado para capturar ducha medición biométrica con dicho sensor biométrico. En algunas realizaciones el dispositivo de autenticación también puede estar adaptado para recibir dicha medición biométrica a través de dicha conexión Bluetooth. En algunas realizaciones el dispositivo de autenticación también puede estar adaptado para generar dicha credencial dinámica solo si fue exitosa dicha verificación de dicha medición biométrica.

En algunas realizaciones el dispositivo de autenticación puede ser cualquiera de los dispositivos de autenticación de las realizaciones anteriores en el que dicha interfaz de entrada de usuario consiste es un botón único y en el que dicho dispositivo de autenticación también está adaptado para capturar una aprobación de dicho usuario por dicho usuario

que presiona dicho botón. En otras realizaciones el dispositivo de autenticación puede ser cualquiera de los dispositivos de autenticación de las realizaciones anteriores en el que la interfaz de entrada de usuario consiste en dos botones en el que dicho dispositivo de autenticación también está adaptado para capturar una aprobación de dicho usuario por dicho usuario que presiona el primero de dichos dos botones y para capturar un rechazo o cancelación de dicho usuario por dicho usuario que presiona el segundo de dichos dos botones.

En algunas realizaciones el dispositivo de autenticación puede ser cualquiera de los dispositivos de autenticación de las realizaciones anteriores además adaptado para recibir o enviar a través de dichos mensajes de aplicación de conexión Bluetooth a través de dicha conexión Bluetooth que están asegurados por una técnica de mensajería segura para proteger la integridad, confidencialidad o autenticidad de dichos mensajes de aplicación, por lo que el dispositivo de autenticación también está adaptado para soportar dicha técnica de mensajería segura y para realizar operaciones de mensajería segura criptográfica que se usan en dicha técnica de mensajería segura por la cual dicha técnica de mensajería segura es independiente de cualquier mecanismo de mensajería seguro Bluetooth. En algunas realizaciones, el dispositivo de autenticación también puede estar adaptado para almacenar un secreto de mensajería segura y usar dicho secreto de mensajería segura para determinar el valor de una clave de mensajería segura criptográfica y usar dicha clave de mensajería segura criptográfica en dichas operaciones de mensajería segura criptográfica.

En algunas realizaciones el dispositivo de autenticación puede ser cualquiera de los dispositivos de autenticación de las realizaciones anteriores en el que dicha combinación criptográfica dicha clave secreta de generación de credenciales criptográficas con dicha variable dinámica comprende ejecutar un algoritmo criptográfico simétrico parametrizado con dicha clave secreta de generación de credenciales criptográficas. En algunas realizaciones dicho algoritmo criptográfico simétrico puede comprender un algoritmo de cifrado o descifrado simétrico. En algunas realizaciones dicho algoritmo criptográfico simétrico puede comprender un algoritmo de hash con clave.

En algunas realizaciones el dispositivo de autenticación puede ser cualquiera de los dispositivos de autenticación de las realizaciones anteriores en el que dicha interfaz Bluetooth soporta Bluetooth de baja energía.

Otro aspecto de la invención proporciona un sistema para asegurar una interacción entre una aplicación y un usuario. La aplicación puede incluir una parte de servidor y una parte de cliente.

En algunas realizaciones el sistema puede comprender: un servidor de aplicación (210) que aloja la parte de servidor de la aplicación; un ordenador huésped (230) que ejecuta una aplicación cliente que está en la parte de cliente de dicha aplicación y que permite al usuario (290) acceder remotamente a la aplicación a través de una red de ordenador (250), dicho ordenador huésped que comprende una interfaz de entrada de usuario para recepción de entradas del usuario y una interfaz de salida de usuario para proporcionar salidas al usuario; un dispositivo de autenticación (240) para generar una credencial dinámica, el dispositivo de autenticación que comprende un componente de almacenamiento (130) adaptado para almacenar de manera segura una clave secreta de generación de credenciales criptográficas, un componente de procesamiento de datos (140) para generar dicha credencial dinámica mediante la combinación criptográfica de dicha clave secreta de generación de credenciales criptográficas con una variable dinámica, y una interfaz Bluetooth (150) para conexión del dispositivo de autenticación a dicho ordenador huésped usando una conexión Bluetooth entre el dispositivo de autenticación y dicho ordenador huésped; y un servidor de verificación (220) para verificar la validez de dicha credencial dinámica; por lo cual dicho ordenador huésped está adaptado para montar una conexión Bluetooth con dicho dispositivo de autenticación; dicho dispositivo de autenticación está adaptado para generar dicha credencial dinámica y retornar dicha credencial dinámica por medio de la conexión Bluetooth a dicho ordenador huésped; dicha aplicación cliente en el ordenador huésped también está adaptado para recibir dicha credencial dinámica por medio de dicha conexión Bluetooth y enviar dicha credencial dinámica generada a dicho servidor de verificación para la verificación; y dicho servidor de verificación está adaptado para verificar la credencial dinámica generada y señalizar a dicho servidor de aplicación si se ha verificado que la credencial dinámica es válida.

En algunas realizaciones el sistema puede ser cualquiera de los sistemas de las realizaciones anteriores en el que dicho dispositivo de autenticación y dicho servidor de verificación comparten dicha clave secreta de generación de credenciales criptográficas y en el que dicha generación y dicha verificación de dicha credencial dinámica se realiza usando un algoritmo criptográfico simétrico usando una clave de autenticación secreta que es compartida entre dicho dispositivo de autenticación y dicho servidor de verificación.

En algunas realizaciones el sistema puede ser cualquiera de los sistemas de las realizaciones anteriores en el que dicho dispositivo de autenticación por una parte y dicho servidor de verificación o servidor de aplicación por otra parte comparten una o más claves de mensajería seguras; dicho servidor de aplicación o dicho servidor de verificación está adaptado para generar un mensaje de aplicación y asegurar dicho mensaje de aplicación con técnicas de mensajería seguras usando dicha una o más claves de mensajería seguras compartidas; dicha aplicación cliente está adaptada para recibir dicho mensaje de aplicación seguro y enviar dicho mensaje de aplicación seguro a dicho dispositivo de autenticación a través de dicha conexión Bluetooth; y dicho dispositivo de autenticación está adaptado para recibir a través de dicha conexión Bluetooth dicho mensaje de aplicación seguro y soportar dichas claves de mensajería seguras usando dichas una o más claves de mensajería seguras compartidas y actuar sobre dicho mensaje de aplicación seguro.

En algunas realizaciones el sistema puede ser cualquiera de los sistemas de las realizaciones anteriores en el que dicho dispositivo de autenticación está adaptado: para recibir a través de dicha conexión Bluetooth un mensaje de aplicación que contiene una solicitud para el dispositivo de autenticación para generar y retornar dicha credencial dinámica, y en respuesta a la recepción de dicho mensaje de aplicación, para generar dicha credencial dinámica y retornar dicha credencial dinámica a través de dicha conexión Bluetooth. En algunas realizaciones dicho mensaje de aplicación puede contener un desafío y dicha variable dinámica se puede basar en dicho desafío. En algunas realizaciones dicho desafío puede contener un valor impredecible que es generado por dicho servidor de aplicación o dicho servidor de verificación. En algunas realizaciones dicho mensaje de aplicación puede contener datos de transacción enviado por dicho usuario a dicha aplicación y dicha variable dinámica se puede basar en dichos datos de transacción.

En algunas realizaciones el sistema puede ser cualquiera de los sistemas de las realizaciones anteriores en el que dicho dispositivo de autenticación también está adaptada para mantener un estado de aplicación que cambia con el tiempo y para comunicar a través de dicha conexión Bluetooth información sobre su presente estado a dicho ordenador huésped; y en el que dicha aplicación cliente también está adaptada para recibir a través de dicha conexión Bluetooth dicha información de estado de dicho dispositivo de autenticación y para proporcionar pautas o instrucciones a dicho usuario sobre la forma en que tratar con dicho dispositivo de autenticación a través del cual dichas pautas o instrucciones son una función de dicha información de estado recibida.

En algunas realizaciones el sistema puede ser cualquiera de los sistemas de las realizaciones anteriores en el que dicho dispositivo de autenticación también está adaptado para generar comandos que serán ejecutados por dicho ordenador huésped y comunicar dichos comandos a dicho ordenador huésped a través de dicha conexión Bluetooth; y en el que dicha aplicación cliente también está adaptada para recibir dichos comandos a través de dicha conexión Bluetooth de dicho dispositivo de autenticación y ejecutar dichos comandos. En algunas realizaciones la realización de dichos comandos por dicho ordenador huésped puede comprender que dicho ordenador huésped interactúe con dicho usuario por dicha interfaz de salida de usuario o dicha interfaz de entrada de usuario. En algunas realizaciones la realización de los comandos mediante el ordenador huésped puede comprender que el ordenador huésped solicite al usuario que proporcione determinados datos o determinadas entradas, el ordenador huésped obtenga los datos o entradas del usuario (por ejemplo, mediante la interfaz de usuario del ordenador huésped), y el ordenador huésped que comunica los datos o entradas obtenidos al dispositivo de autenticación a través de dicha conexión Bluetooth.

En algunas realizaciones el sistema puede ser cualquiera de los sistemas de las realizaciones anteriores en el que dicha aplicación cliente también está adaptada para obtener mediante dicha interfaz de entrada de usuario de dicho ordenador huésped un valor de PIN y/o contraseña de dicho usuario y enviar a dicho valor de PIN y/o contraseña obtenido a través de dicha conexión Bluetooth a dicho dispositivo de autenticación; y en el que dicho dispositivo de autenticación también está adaptado para recibir a través de dicha conexión Bluetooth dicho valor de PIN y/o contraseña y verificar dicho.

En algunas realizaciones el sistema puede ser cualquiera de los sistemas de las realizaciones anteriores en el que dicho ordenador huésped además comprende un componente de medición biométrica adaptado para capturar una medición biométrica de dicho usuario; en el que dicha aplicación cliente también está adaptada para obtener por dicho componente de medición biométrica de dicho ordenador huésped una medición biométrica de dicho usuario y para enviar dicha medición biométrica obtenida a través de dicha conexión Bluetooth a dicho dispositivo de autenticación; y en el que dicho dispositivo de autenticación también está adaptado para recibir a través de dicha conexión Bluetooth dicha medición biométrica y para verificar dicha medición biométrica recibida.

En algunas realizaciones el sistema puede ser cualquiera de los sistemas de las realizaciones anteriores en el que dicha aplicación cliente también está adaptada para obtener, cuando dicho dispositivo de autenticación está conectada a dicho ordenador huésped con dicha conexión Bluetooth, una indicación de la distancia de dicho dispositivo de autenticación a dicho ordenador huésped; y en el que dicha aplicación está adaptada para tener en cuenta dicha indicación de distancia cuando se decide si conceder, mantener o revocar uno o más derechos de acceso para dicho usuario.

En un aspecto adicional, la invención proporciona un procedimiento para aseguramiento de la interacción de una aplicación basada en ordenador con un usuario mediante la cual el usuario opera o lleva un dispositivo de autenticación para generar una credencial dinámica, a través de la cual el dispositivo de autenticación puede comprender una interfaz Bluetooth para comunicarse con un dispositivo huésped Bluetooth. En algunas realizaciones el dispositivo de autenticación puede ser cualquiera de los dispositivos de autenticación previamente descritos. En algunas realizaciones el procedimiento se puede usar con cualquiera de los sistemas descritos anteriormente.

En algunas realizaciones el procedimiento puede comprender las etapas de: ejecutar en un ordenador huésped local una aplicación cliente que es una parte de cliente de la aplicación para permitir al usuario interactuar con la aplicación mediante el uso de una interfaz de entrada de usuario y una interfaz de salida de usuario del ordenador huésped local; montar en el ordenador huésped local una conexión Bluetooth con el dispositivo de autenticación; recibir a través de dicha conexión Bluetooth del dispositivo de autenticación la credencial dinámica que se ha generado en dicho dispositivo de autenticación mediante la combinación criptográfica de una variable dinámica con una primera clave de

autenticación criptográfica almacenada en dicho dispositivo de autenticación; y verificar dicha credencial dinámica usando un algoritmo criptográfico que está parametrizado con una segunda clave de autenticación criptográfica.

En algunas realizaciones el procedimiento puede ser cualquiera de los procedimientos de las realizaciones anteriores que también comprende las etapas de: generar un mensaje de aplicación; asegurar dicha aplicación mediante la aplicación de técnicas de mensajería seguras que se basan en un algoritmo criptográfico simétrico que se parametriza con al menos una clave de mensajería segura simétrica que es compartida con dicho dispositivo de autenticación; y en el ordenador huésped que envía dicho mensaje de aplicación a través de dicha conexión Bluetooth al dispositivo de autenticación.

En algunas realizaciones el procedimiento puede ser cualquiera de los procedimientos de las realizaciones anteriores que además comprende las etapas de: generar un mensaje de aplicación que comprende una solicitud para el dispositivo de autenticación para generar y retornar dicha credencial dinámica, y en el ordenador huésped enviar dicho mensaje de aplicación a través de dicha conexión Bluetooth al dispositivo de autenticación, a través del cual el dispositivo de autenticación puede generar y retornar dicha credencial dinámica a través de dicha conexión Bluetooth al ordenador huésped en respuesta al dispositivo de autenticación que recibe dicho mensaje de aplicación a través de dicha conexión Bluetooth. En algunas realizaciones el procedimiento también puede comprender las etapas de: generar un desafío e incluir dicho desafío en dicho mensaje de aplicación a través del cual dicha variable dinámica se basa en dicho desafío. En algunas realizaciones el procedimiento también puede comprender las etapas de: recibir de dicho usuario una solicitud para realizar una transacción; incluir en dicho mensaje de aplicación datos de transacción que representan dicha transacción; y realizar dicha solicitud de transacción si dicha verificación de dicha credencial dinámica es exitosa; a través de cual dicha variable dinámica se puede basar en dichos datos de transacción incluidos en dicho mensaje de aplicación.

En algunas realizaciones el procedimiento puede ser cualquiera de los procedimientos de las realizaciones anteriores que además comprende las etapas de: recibir en dicho ordenador huésped local a través de dicha conexión Bluetooth información del dispositivo de autenticación en el estado de aplicación del dispositivo de autenticación; proporcionar en el ordenador huésped local por dicha interfaz de salida de usuario pautas o instrucciones referentes a la operación de dicho dispositivo de autenticación al usuario; a través del cual dichas pautas o instrucciones pueden ser una función de dicha información recibida en el estado de aplicación del dispositivo de autenticación.

En algunas realizaciones el procedimiento puede ser cualquiera de los procedimientos de las realizaciones anteriores que además comprende las etapas de recibir en dicho ordenador huésped local a través de dicha conexión Bluetooth de dicho dispositivo de autenticación un comando para ser ejecutado y ejecutar dicho comando en dicho ordenador huésped local.

En algunas realizaciones el procedimiento puede ser cualquiera de los procedimientos de las realizaciones anteriores que además comprende las etapas de obtener en dicho ordenador huésped local un valor de PIN y/o contraseña de dicho usuario por dicha interfaz de entrada de usuario y enviar dicho valor obtenido de PIN y/o contraseña a través de dicha conexión Bluetooth a dicho dispositivo de autenticación para que dicho valor de PIN y/o contraseña sea verificado por dicho dispositivo de autenticación.

En algunas realizaciones el procedimiento puede ser cualquiera de los procedimientos de las realizaciones anteriores que además comprende las etapas de obtener en dicho ordenador huésped local una medición biométrica de dicho usuario mediante un sensor biométrico y enviar dicha medición biométrica obtenida a través de dicha conexión Bluetooth a dicho dispositivo de autenticación para que dicha medición biométrica se verifique por dicho dispositivo de autenticación.

En algunas realizaciones el procedimiento puede ser cualquiera de los procedimientos de las realizaciones anteriores que además comprende las etapas de obtener en el ordenador huésped local un valor indicador de la distancia que es indicativo de la distancia real entre el ordenador huésped local y el dispositivo de autenticación y usar dicho valor indicador de la distancia para determinar si conceder, mantener o revocar uno o más derechos de acceso al usuario

En algunas realizaciones el procedimiento puede ser cualquiera de los procedimientos de las realizaciones anteriores que además comprende al menos las etapas de: ejecutar en un ordenador huésped local una aplicación cliente que es una parte de cliente de la aplicación para permitir al usuario interactuar con la aplicación mediante el uso de una interfaz de entrada de usuario y una interfaz de salida de usuario del ordenador huésped local; montar en el ordenador huésped local una conexión Bluetooth con el dispositivo de autenticación; obtener en el ordenador huésped local un valor indicador de la distancia que es indicativo de la distancia real entre el ordenador huésped local y el dispositivo de autenticación; y usar dicho valor indicador de la distancia para determinar si conceder, mantener o revocar uno o más derechos de acceso al usuario. En algunas realizaciones el procedimiento también puede comprender las etapas de comparar dicho valor indicativo de distancia con un valor umbral predefinido y revocar al menos algunos de dichos uno o más derechos de acceso para el usuario si dicha comparación indica que el dispositivo de autenticación está más alejado del ordenador huésped que la distancia asociada con dicho valor umbral. En algunas realizaciones, el procedimiento también puede comprender las etapas de comparar dicho valor de indicación de distancia con un valor de umbral predefinido y conceder al menos algunos de dichos uno o más derechos de acceso al usuario si dicha comparación indica que el dispositivo de autenticación está más cerca del ordenador huésped que la distancia

asociada con dicho valor umbral.

En algunas realizaciones, el dispositivo de autenticación puede ser un dispositivo autónomo alimentado por batería. En algunas realizaciones, las baterías pueden ser recargables. En algunas realizaciones, las baterías pueden ser reemplazables. En algunas realizaciones, el dispositivo de autenticación puede ser un dispositivo de bolsillo, portátil y de mano.

En algunas realizaciones, el dispositivo de autenticación puede tener su propia interfaz de salida de usuario que, por ejemplo, puede comprender una pantalla. En algunas realizaciones, el dispositivo de autenticación puede tener su propia interfaz de entrada de usuario que, por ejemplo, puede comprender un teclado. En algunos casos, el teclado se puede reducir a un botón único, en otros casos el teclado puede consistir en dos botones, en otros casos, el teclado puede ser un teclado completo.

En algunas realizaciones, la interfaz de entrada de usuario y la interfaz de salida de usuario pueden ser no extraíbles y no reparables por el usuario, totalmente controladas por el dispositivo de autenticación e inmunes a la interferencia de software malicioso en un ordenador huésped. Por lo tanto, en tales realizaciones se puede considerar que el dispositivo de autenticación tiene una interfaz de usuario confiable en contraste con, por ejemplo, las PC en las que siempre existe la posibilidad de que un software malicioso tal como un virus o un troyano presente mensajes falsos al usuario, o capture lo que el usuario ingresa en el teclado, o lea en la memoria datos confidenciales asociados con una aplicación de seguridad o altere los datos antes de que se firmen.

En algunas realizaciones, el firmware del dispositivo de autenticación puede no ser alterable. En algunas realizaciones, el dispositivo de autenticación puede tener disposiciones de inviolabilidad. En algunas realizaciones, el dispositivo de autenticación puede ser un dispositivo de hardware seguro especializado dedicado a proporcionar funciones de firma de autenticación y/o transacción. En algunas realizaciones, el propósito principal del dispositivo de autenticación es generar credenciales dinámicas que en algunos casos se pueden denominar "Contraseñas de un solo uso" (OTP) o contraseñas dinámicas.

En algunas realizaciones el dispositivo de autenticación puede estar adaptado para generar estas credenciales dinámicas mediante la combinación criptográfica de un secreto con el valor de una variable dinámica.

En algunas realizaciones, este secreto puede ser una clave secreta criptográfica almacenada de forma segura en el dispositivo de autenticación. En algunas realizaciones, el dispositivo de autenticación puede usar el secreto para parametrizar un algoritmo criptográfico que usa la variable dinámica como entrada. En algunas realizaciones, el secreto puede comprender un valor secreto que se comparte entre el dispositivo de autenticación y un servidor de verificación o autenticación. En algunas realizaciones, el secreto puede comprender una clave secreta simétrica. En algunas realizaciones, el secreto puede comprender una clave privada de un par de claves pública-privada. En algunas realizaciones, el secreto de cada dispositivo de autenticación particular puede tener su propio valor individual o único.

En algunas realizaciones, la variable dinámica se puede derivar o basar en un valor de tiempo, un valor de contador o un desafío de servidor que se proporciona al dispositivo, o una combinación de estos. En algunas realizaciones, el dispositivo de autenticación también puede usar datos (tal como datos de transacción) que se han proporcionado al dispositivo como el valor dinámico o el dispositivo puede usar estos datos en combinación con cualquiera de los valores dinámicos mencionados anteriormente para generar una credencial dinámica. En los casos en que la variable dinámica se base en datos de transacciones, la credencial dinámica resultante puede indicar la aprobación de los datos por parte del usuario y la credencial dinámica se puede denominar firma electrónica o código de autenticación de mensaje (MAC). Por ejemplo, en algunas realizaciones, el dispositivo de autenticación puede combinar criptográficamente un secreto criptográfico con un valor de tiempo y datos de transacción para generar una credencial dinámica que comprende una firma electrónica sobre los datos de transacción.

En algunas realizaciones, el dispositivo de autenticación que combina criptográficamente el secreto con una variable dinámica puede comprender el dispositivo de autenticación que ejecuta un algoritmo criptográfico simétrico. En algunas realizaciones, este algoritmo criptográfico simétrico puede tomar la variable dinámica como entrada y se puede parametrizar con el secreto almacenado de forma segura en el dispositivo. En algunas realizaciones, el algoritmo criptográfico simétrico puede comprender un algoritmo de cifrado o descifrado simétrico (tal como, por ejemplo, DES, 3DES o AES) sobre datos relacionados con el valor dinámico y usando el secreto como clave de cifrado o descifrado simétrico. En algunos casos, el dispositivo de autenticación que combina criptográficamente el secreto con un valor dinámico puede comprender realizar una función hash criptográfica (tal como, por ejemplo, SHA-1) que está codificada con el secreto y usar los datos relacionados con el valor dinámico como datos de entrada a la función hash. En algunas realizaciones, el secreto que usa el dispositivo de autenticación para generar la credencial dinámica se puede compartir con la aplicación o un servidor de verificación que verifica la credencial dinámica en nombre de la aplicación, por lo que la aplicación o el servidor de verificación pueden usar el secreto compartido en la verificación de la credencial dinámica generada por el dispositivo de autenticación.

En algunas realizaciones, el secreto puede ser una variable dinámica. Por ejemplo, en algunas realizaciones, cuando el secreto se usa para generar una credencial dinámica, su valor puede ser reemplazado por un nuevo valor que es función del valor anterior (el nuevo valor del secreto, por ejemplo, se puede calcular como valor hash de una vía del

valor anterior). Debido a que en tales realizaciones el valor del secreto se puede determinar como una función del valor inicial del secreto y el número de veces que se ha cambiado el valor secreto, tales realizaciones son matemáticamente equivalentes al uso de un secreto estático en combinación con una variable dinámica que comprende un valor de contador.

En algunas realizaciones la variable dinámica que el dispositivo de autenticación puede usar para generar una credencial dinámica se puede basar en el valor de una variable externa (tal como un desafío o datos de transacción) que es proporcionada al dispositivo de autenticación por alguna entidad que es externa al dispositivo de autenticación. En algunas realizaciones, la variable dinámica que el dispositivo de autenticación puede usar para generar una credencial dinámica se puede basar en el valor de una variable interna proporcionada por el dispositivo de autenticación mismo, tal como por ejemplo el valor de tiempo de un reloj comprendido en el dispositivo de autenticación o el valor de un contador almacenado en una actualización por el dispositivo de autenticación. En algunas realizaciones, la variable dinámica se puede basar tanto en una variable externa como en una variable interna.

En algunas realizaciones, el dispositivo de autenticación puede ser capaz de comunicarse con una tarjeta inteligente insertada, por lo que la generación de las credenciales dinámicas es realizada en parte por dispositivo de autenticación mismo y en parte por la tarjeta inteligente insertada.

En algunas realizaciones del dispositivo de autenticación, el dispositivo de autenticación puede estar adaptado para recibir datos (tales como un desafío de servidor o datos de transacción) que puede usar para generar credenciales dinámicas por parte del usuario que proporciona datos al dispositivo de autenticación mediante la interfaz de entrada de usuario del dispositivo de autenticación. Por ejemplo, en algunas realizaciones, el usuario puede ingresar los datos manualmente en el teclado del dispositivo de autenticación. Cuando la cantidad de datos que el usuario debe proporcionar al dispositivo de autenticación de esta manera excede unas pocas docenas de caracteres, los usuarios pueden percibir este proceso como demasiado engorroso.

En algunas realizaciones, el dispositivo de autenticación se puede adaptar para presentar una credencial dinámica generada al usuario por la interfaz de salida humana de modo que el usuario pueda proporcionar o reenviar la credencial dinámica presentada al sistema que necesita verificar esta credencial dinámica. Por ejemplo, en algunas realizaciones, el dispositivo de autenticación se puede adaptar para mostrar una OTP o MAC generada en su pantalla para que el usuario pueda copiar la OTP o MAC mostrada en su PC (u otro dispositivo de acceso a Internet) que pueda transmitir esta OTP o MAC al servidor de aplicación o autenticación donde se puede verificar la validez del OTP o MAC. Sin embargo, esto también requiere algunas acciones del usuario que se pueden percibir como inconvenientes.

En algunas realizaciones, el dispositivo de autenticación puede comprender una interfaz Bluetooth. En algunas realizaciones, la interfaz Bluetooth del dispositivo de autenticación se puede usar para conexión del dispositivo de autenticación a un ordenador huésped que soporte Bluetooth. El ordenador huésped puede ser un dispositivo de acceso que el usuario usa para interactuar (por ejemplo, a través de una red pública de telecomunicaciones tal como Internet) con una aplicación (que puede ser una aplicación accesible de forma remota). En algunas realizaciones, el dispositivo de autenticación puede estar adaptado para intercambiar datos con un ordenador huésped usando la interfaz Bluetooth del dispositivo de autenticación.

En algunas realizaciones, el dispositivo de autenticación puede estar adaptado para recibir datos a través de su interfaz Bluetooth. En algunas realizaciones, el dispositivo de autenticación puede estar adaptado para recibir datos a través de su interfaz Bluetooth que puede usar para generar una credencial dinámica. Por ejemplo, en algunas realizaciones, el dispositivo de autenticación puede recibir un desafío de servidor y/o datos de transacción de un ordenador huésped a través de su interfaz Bluetooth y el dispositivo de autenticación puede usar este desafío y/o datos de transacción para generar una credencial dinámica. En algunas realizaciones, el dispositivo de autenticación puede estar adaptado para devolver una credencial dinámica que generó a un ordenador huésped a través de su interfaz Bluetooth. En algunas realizaciones, la interfaz Bluetooth puede soportar Bluetooth de baja energía (BLE).

En algunas realizaciones el dispositivo de autenticación se puede usar para asegurar la interacción de un usuario con una aplicación de la siguiente manera.

En algunas realizaciones, el usuario puede usar el ordenador huésped como un dispositivo de acceso para interactuar con una aplicación basada en ordenador. En algunas realizaciones, el ordenador huésped puede comprender, por ejemplo, una PC (ordenador personal), una tableta o un teléfono inteligente. En algunas realizaciones, el ordenador huésped puede ejecutar un sistema operativo tal como, por ejemplo, Windows 8, Android o iOS.

Durante la interacción con la aplicación, la aplicación puede requerir que el usuario suministre una credencial dinámica. Por ejemplo, en algunas realizaciones, un usuario puede tener que proporcionar durante el procedimiento de inicio de sesión una credencial dinámica válida para aplicación para que la aplicación verifique y la aplicación puede conceder el acceso al usuario solo si esta verificación fue exitosa. Por ejemplo, en algunas realizaciones, el usuario puede enviar una transacción a la aplicación (por ejemplo, el usuario puede enviar una transacción de transferencia de dinero a una aplicación de banca por Internet) con lo cual la aplicación puede requerir que el usuario proporcione una credencial dinámica que comprenda una firma electrónica sobre la transacción datos.

En algunas realizaciones, la credencial dinámica puede ser generada por el dispositivo de autenticación del usuario.

En algunas realizaciones, el intercambio de datos entre la aplicación y el dispositivo de autenticación se puede realizar a través de la interfaz Bluetooth del dispositivo de autenticación. En algunas realizaciones, el sistema de autenticación (que puede ser parte de la aplicación o que pueda ser utilizada por la aplicación) puede comprender una aplicación de autenticación de cliente en el ordenador huésped para interactuar con el dispositivo de autenticación, por ejemplo, usando la interfaz Bluetooth del dispositivo de autenticación.

En algunas realizaciones, la aplicación se puede basar en ordenador. En algunas realizaciones, la aplicación puede comprender una aplicación cliente que comprende componentes de software de aplicación que se ejecutan en un ordenador con la que el usuario puede estar interactuando. La aplicación cliente puede estar adaptad para interactuar con el usuario a través de una interfaz de entrada de usuario (tal como un mouse y/o teclado y/o pantalla táctil) y/o una interfaz de salida de usuario (tal como altavoces y/o una pantalla) de un ordenador en la que se ejecuta la aplicación cliente. En algunas realizaciones, la aplicación puede comprender uno o más componentes basados en el servidor. En algunas realizaciones, la aplicación puede comprender partes del servidor que comprenden software que se ejecuta en ordenadores de servidor que se pueden conectar e interactuar con un ordenador que ejecuta una aplicación cliente. Los ordenadores del servidor y el ordenador que ejecuta la aplicación cliente se pueden conectar entre sí mediante una red informática, como por ejemplo Internet. Las acciones que se describen en esta descripción como realizadas por un ordenador huésped, al menos en algunas realizaciones, pueden ser realizadas por el ordenador huésped bajo impulso y control de la aplicación cliente que se ejecuta en ese ordenador huésped.

En algunas realizaciones, el dispositivo de autenticación puede intercambiar mensajes con un componente de la aplicación basado en el servidor. En algunas realizaciones, los mensajes que se intercambian entre un componente de la aplicación basado en el servidor y el dispositivo de autenticación se pueden proteger con técnicas de mensajería segura. En algunas realizaciones, la integridad de al menos algunos de los datos de al menos algunos mensajes intercambiados entre un componente de la aplicación basado en el servidor y el dispositivo de autenticación se puede proteger usando técnicas de mensajería seguras. En algunas realizaciones, la confidencialidad de al menos algunos de los datos de al menos algunos mensajes intercambiados entre un componente de la aplicación basado en el servidor y el dispositivo de autenticación se puede proteger usando técnicas de mensajería segura. En algunas realizaciones, la autenticidad de la entidad que envía al menos algunos mensajes intercambiados entre un componente de la aplicación basado en el servidor y el dispositivo de autenticación se puede proteger usando técnicas de mensajería segura.

En algunas realizaciones, al menos algunos de los datos de al menos algunos mensajes intercambiados entre un componente de la aplicación basado en el servidor y el dispositivo de autenticación pueden estar encriptados, por ejemplo, para proteger o garantizar la confidencialidad, integridad o autenticidad de los datos en los mensajes. En algunas realizaciones, este cifrado se puede realizar usando un algoritmo de cifrado simétrico, tal como, por ejemplo, AES (estándar de cifrado avanzado), que se puede parametrizar con una clave secreta simétrica que se puede compartir entre el dispositivo de autenticación y el componente de la aplicación basada en el servidor.

En algunas realizaciones, al menos algunos mensajes intercambiados entre un componente de la aplicación basado en el servidor y el dispositivo de autenticación pueden comprender un MAC (Código de autenticación de mensaje) sobre al menos algunos de los datos comprendidos en dicho mensaje, por ejemplo, para proteger o garantizar la integridad o autenticidad de los datos en los mensajes. En algunas realizaciones, tales MAC se pueden generar o verificar usando un algoritmo criptográfico simétrico, tal como un algoritmo de cifrado o descifrado simétrico, por ejemplo, AES (estándar de cifrado avanzado), o algún algoritmo de hash con clave tal como HMAC, que se puede parametrizar con una clave simétrica de secreto que se puede compartir entre el dispositivo de autenticación y el componente de la aplicación basada en el servidor.

En alguna realización, cada dispositivo de autenticación individual de una pluralidad de dispositivos de autenticación puede almacenar un conjunto diferente de uno o más secretos de mensajería segura que el dispositivo de autenticación puede usar para determinar los valores de una o más claves de mensajería segura que el dispositivo de autenticación se puede usar para parametrizar los algoritmos criptográficos de las técnicas de mensajería segura descritas anteriormente. En algunas realizaciones, un servidor puede almacenar uno o más secretos que pueden permitir que el servidor determine para un dispositivo de autenticación dado los secretos de mensajería seguros que se usarán con ese dispositivo de autenticación. En algunas realizaciones, el servidor puede almacenar una o más claves maestras de mensajería segura que el servidor puede usar, por ejemplo, con un elemento de datos que tiene un valor único para cada dispositivo de autenticación individual (por ejemplo, un número de serie del dispositivo de autenticación) para derivar los valores de las claves de mensajería segura para ese dispositivo de autenticación. En algunas realizaciones, el servidor puede almacenar en una base de datos para cada dispositivo de autenticación los secretos de mensajería seguros almacenados en ese dispositivo de autenticación asociado con un elemento de datos de identificación del dispositivo (por ejemplo, un número de serie) del dispositivo de autenticación.

En algunas realizaciones, la interfaz Bluetooth siempre está activa cuando el dispositivo de autenticación está activo. En algunas realizaciones, el usuario puede encender el dispositivo de autenticación (por ejemplo, al presionar un botón) y cuando el dispositivo de autenticación se enciende, también puede habilitar su interfaz Bluetooth. En algunas realizaciones, el usuario puede tener que indicar explícitamente al dispositivo de autenticación para habilitar la interfaz Bluetooth, por ejemplo, al presionar un botón.

En algunas realizaciones, la interfaz Bluetooth del dispositivo de autenticación puede notificar/anunciar su presencia (por ejemplo, mediante la transmisión de un mensaje) cuando se ha activado la interfaz Bluetooth del dispositivo de autenticación. En algunas realizaciones, el dispositivo de autenticación se puede configurar para anunciar su presencia a través de la interfaz Bluetooth solo durante un período de tiempo limitado (por ejemplo, durante un período de menos de 5 minutos). En algunas realizaciones, el dispositivo de autenticación es compatible con el modo detectable limitado Bluetooth. En algunas realizaciones, el dispositivo de autenticación soporta el modo de descubrimiento limitado de Bluetooth. En algunas realizaciones, el dispositivo de autenticación puede permanecer en algún modo de descubrimiento durante un período de tiempo limitado y, por lo tanto, puede apagarse por sí mismo.

En algunas realizaciones, cuando un componente del ordenador huésped (por ejemplo, la aplicación de autenticación del cliente) nota que está presente un dispositivo de autenticación con un Bluetooth activo, puede iniciar una conexión Bluetooth con el dispositivo de autenticación.

En algunas realizaciones, el dispositivo de autenticación está adaptado para soportar un mecanismo de apareamiento Bluetooth con el ordenador huésped. En algunas realizaciones, el dispositivo de autenticación está adaptado para soportar un mecanismo de apareamiento Bluetooth de baja energía. En algunas realizaciones, el dispositivo de autenticación está adaptado para soportar el apareamiento con clientes Bluetooth de baja energía con el procedimiento de apareamiento de entrada Passkey. En algunas realizaciones, el dispositivo de autenticación puede estar adaptado para recibir una solicitud de apareamiento de Bluetooth y después de recibir la solicitud de apareamiento, el dispositivo de autenticación puede generar un código de apareamiento y mostrar el código de apareamiento generado al usuario y el usuario puede proporcionar el código de apareamiento mostrado para el ordenador huésped (por ejemplo, para la aplicación de autenticación del cliente). En algunas realizaciones, el dispositivo de autenticación se puede configurar de modo que el número de dígitos o caracteres en el código de apareamiento pueda ser diferente del número de dígitos o caracteres en una credencial dinámica generada por el dispositivo de autenticación.

Una vez que se establece una conexión Bluetooth entre el ordenador huésped y el dispositivo de autenticación, un componente en el ordenador huésped (por ejemplo, la aplicación de autenticación del cliente) puede usar la conexión Bluetooth para enviar una solicitud al dispositivo de autenticación para obtener una credencial dinámica. En algunas realizaciones, el dispositivo de autenticación puede estar adaptado para recibir por la interfaz Bluetooth del dispositivo de autenticación tal solicitud para generar una credencial dinámica. En algunas realizaciones, después de recibir la solicitud para generar una credencial dinámica, el dispositivo de autenticación puede solicitar al usuario que confirme que continúe con la generación de la credencial dinámica solicitada (por ejemplo, presionando un botón).

En algunas realizaciones, el dispositivo de autenticación puede no necesitar ningún otro dato externo para la generación de la credencial dinámica y ahora puede proceder con la generación de la credencial dinámica. Por ejemplo, el dispositivo de autenticación puede generar la credencial dinámica usando el secreto y una variable dinámica que se puede basar en un valor de tiempo generado por un reloj en el dispositivo de autenticación o que se puede basar en un valor de contador que el dispositivo de autenticación puede almacenar en su memoria y que el dispositivo de autenticación incrementa cada vez que genera una credencial dinámica.

En algunas realizaciones, el dispositivo de autenticación puede generar la credencial dinámica usando una variable dinámica que se basa en un desafío generado por la aplicación. En algunas realizaciones, el desafío se puede generar por una parte de servidor de la aplicación y se puede comunicar a la aplicación cliente y la aplicación cliente puede enviar el desafío al dispositivo de autenticación a través de la conexión Bluetooth. En algunas realizaciones, la aplicación cliente puede generar el desafío, puede enviar el desafío al dispositivo de autenticación a través de la conexión Bluetooth y puede comunicar el desafío a la parte de servidor de la aplicación (por ejemplo, junto con la respuesta del dispositivo de autenticación al desafío). En algunas realizaciones, el dispositivo de autenticación puede recibir este desafío a través de la conexión Bluetooth. En algunas realizaciones, el dispositivo de autenticación puede recibir el desafío como parte de la solicitud para generar una credencial dinámica. En otras realizaciones, el dispositivo de autenticación puede recibir el desafío como parte de otro mensaje.

En algunas realizaciones, el dispositivo de autenticación puede generar la credencial dinámica usando una variable dinámica que se basa en datos de transacción. En algunas realizaciones, el dispositivo de autenticación puede recibir estos datos de transacción a través de la conexión Bluetooth. En algunas realizaciones, el dispositivo de autenticación puede recibir estos datos de transacción como parte de la solicitud para generar una credencial dinámica. En otras realizaciones, el dispositivo de autenticación puede recibir estos datos de transacción como parte de otro mensaje (o como parte de otros mensajes múltiples). En algunas realizaciones, el dispositivo de autenticación puede presentar los datos de transacción recibidos al usuario y puede solicitar al usuario que apruebe estos datos en el dispositivo de autenticación antes de generar la credencial dinámica. En algunas realizaciones, los datos de la transacción se pueden dividir en partes (por ejemplo, en campos de datos) y el usuario puede presentar y aprobar cada parte por separado. En algunas realizaciones, el dispositivo de autenticación puede tener una interfaz de entrada de usuario que está adaptada para capturar una aprobación del usuario de los datos de la transacción. En algunas realizaciones, el dispositivo de autenticación puede tener un botón que el usuario puede presionar para aprobar los datos de la transacción. En algunas realizaciones, si el usuario aprobó todas las partes de los datos de la transacción, el dispositivo de autenticación puede generar una credencial dinámica mediante la combinación criptográfica del secreto con una variable dinámica basada en estos datos de transacción aprobados. En algunas realizaciones, la variable dinámica también se puede basar, por ejemplo, en un valor de tiempo que puede proporcionar un reloj comprendido en el

dispositivo de autenticación. En algunas realizaciones, no todos los datos de la transacción se pueden presentar al usuario y aprobados por el usuario en el dispositivo de autenticación y la variable dinámica se puede basar en los datos de la transacción que también han sido presentados y aprobados por el usuario en el dispositivo de autenticación así como los datos que no han sido presentados y aprobados por el usuario en el dispositivo de autenticación.

En algunas realizaciones, el dispositivo de autenticación también puede generar una credencial dinámica en respuesta a otro evento que no sea recibir un mensaje del ordenador huésped a través de la conexión Bluetooth con ese ordenador huésped. Por ejemplo, en algunas realizaciones, el dispositivo de autenticación puede generar una credencial dinámica en respuesta a una acción del usuario capturada por el dispositivo de autenticación, tal como, por ejemplo, que el usuario presione un botón de la interfaz de entrada de usuario del dispositivo de autenticación. En algunas realizaciones, el dispositivo de autenticación puede usar su interfaz de salida de usuario para presentar la credencial dinámica generada al usuario. En algunas realizaciones, el dispositivo de autenticación puede impulsar la credencial dinámica generada al ordenador huésped usando la conexión Bluetooth entre el ordenador huésped y el dispositivo de autenticación.

En algunas realizaciones, cuando el dispositivo de autenticación ha generado la credencial dinámica, que puede ser en respuesta a la recepción de un mensaje Bluetooth o en respuesta a otro evento, puede usar la conexión Bluetooth para enviar la credencial dinámica generada al ordenador huésped. En algunas realizaciones, el dispositivo de autenticación puede mostrar la credencial dinámica generada al usuario antes de enviar la credencial dinámica generada al ordenador huésped. En algunas realizaciones, el dispositivo de autenticación puede solicitar al usuario que confirme el envío de la credencial dinámica generada al ordenador huésped. En algunas realizaciones, el usuario puede confirmar que envía la credencial dinámica generada al ordenador huésped al presionar un botón del dispositivo de autenticación.

En algunas realizaciones, la interfaz de entrada del usuario del dispositivo de autenticación tiene un botón único para el accionamiento por un usuario humano. En algunas realizaciones, el usuario puede presionar este botón único, por ejemplo, para encender el dispositivo de autenticación y/o activar la interfaz Bluetooth y/o aprobar los datos de la transacción y/o confirmar que se debe generar y/o enviar una credencial dinámica al ordenador huésped. En algunas realizaciones para permitir al usuario cancelar una operación o desaprobar los datos presentados al usuario o apagar el dispositivo, el dispositivo de autenticación puede establecer un período de tiempo de espera y si el usuario no ha presionado el botón único antes del período de tiempo de espera expira, el dispositivo de autenticación puede interpretar esto como una cancelación, desaprobación o apagado.

En algunas realizaciones, la interfaz de entrada del usuario del dispositivo de autenticación puede tener exactamente dos botones para el accionamiento de un ser humano. En algunas realizaciones, el usuario puede usar un primer botón de la interfaz de entrada del usuario para encender el dispositivo de autenticación y/o activar la interfaz Bluetooth y/o aprobar los datos de transacción y/o confirmar que se debe generar y/o enviar una credencia dinámica al ordenador huésped, y se puede usar un segundo botón para apagar el dispositivo de autenticación y/o desactivar la interfaz Bluetooth y/o rechazar los datos de la transacción y/o rechazar que se debe generar y/o enviar una credencial dinámica al ordenador huésped.

En algunas realizaciones, el dispositivo de autenticación puede estar adaptado para proporcionar también un elemento de datos de identificación del dispositivo al ordenador huésped a través de la conexión Bluetooth. Cada dispositivo de autenticación particular puede tener un valor único diferente para este elemento de datos de identificación del dispositivo, de modo que el valor de este elemento de datos de identificación del dispositivo se puede usar para identificar el dispositivo de autenticación particular que, por ejemplo, generó la credencial dinámica. En algunas realizaciones, el dispositivo de autenticación puede devolver su elemento de datos de identificación del dispositivo en respuesta a una solicitud específica del ordenador huésped. En algunas realizaciones, el dispositivo de autenticación puede devolver su elemento de datos de identificación del dispositivo junto con una credencial dinámica generada (en el mismo o en otro mensaje). En algunas realizaciones, el elemento de datos de identificación del dispositivo se puede proporcionar al ordenador huésped durante la configuración de la conexión, por ejemplo, como (parte de) un nombre Bluetooth amigable o un nombre de dispositivo o una dirección de Bluetooth. En algunas realizaciones, el dispositivo de autenticación puede proporcionar un elemento de datos de identificación del dispositivo como parte de un mensaje de anuncio de Bluetooth. En algunas realizaciones, esto se puede usar por un ordenador huésped de la siguiente manera. Si un ordenador huésped detecta la presencia de múltiples dispositivos de autenticación que anuncian su presencia, el ordenador huésped puede usar los elementos de datos de identificación del dispositivo en los mensajes de anuncio para seleccionar el dispositivo de autenticación con el que desea establecer una conexión Bluetooth. Por ejemplo, el ordenador huésped puede seleccionar el dispositivo de autenticación con un elemento de datos de identificación del dispositivo que corresponde al elemento de datos de identificación del dispositivo de un dispositivo de autenticación que ya se ha utilizado previamente con ese ordenador huésped. En el caso de que se hayan usado previamente múltiples dispositivos de autenticación con ese ordenador huésped, el ordenador huésped, por ejemplo, puede elegir el dispositivo de autenticación que se ha usado más recientemente o, alternativamente, el dispositivo de autenticación que se ha usado con más frecuencia en el pasado.

En algunas realizaciones, la aplicación cliente en el ordenador huésped puede obtener un identificador de usuario, tal como un nombre de usuario, del usuario que usa el dispositivo de autenticación y puede usar ese identificador de usuario para determinar una lista de uno o más dispositivos de autenticación asociados con ese usuario. Por ejemplo,

la aplicación cliente puede enviar el identificador de usuario a una parte de servidor de la aplicación y puede recibir a cambio de la parte de servidor una lista de uno o más identificadores del dispositivo de autenticación. La aplicación cliente después puede verificar cuál de los múltiples dispositivos de autenticación que anuncian su presencia está en esa lista y seleccionar un dispositivo de autenticación que esté en esa lista.

En algunas realizaciones cuando un componente en el ordenador huésped (por ejemplo, la aplicación de autenticación de cliente) ha recibido del dispositivo de autenticación el elemento de datos de identificación del dispositivo de este dispositivo de autenticación, el ordenador huésped puede enviar el elemento de datos de identificación recibidos del dispositivo al servidor de aplicación. En algunas realizaciones el valor de elemento de datos de identificación del dispositivo del dispositivo de autenticación de un usuario particular se puede asociar al lado del servidor con este usuario particular. Por ejemplo, la identificación de usuario y/o el nombre de usuario de cada usuario pueden estar asociados en una base de datos del servidor con el valor del elemento de datos de identificación del dispositivo de autenticación asignado a ese usuario. En algunas realizaciones, después de recibir el valor del elemento de datos de identificación del dispositivo de un dispositivo de autenticación particular, el servidor puede buscar el ID de usuario y/o el nombre de usuario asociados. En algunas realizaciones, esto puede evitar la necesidad de que el usuario deba proporcionar activamente un nombre de usuario para identificar cuando, por ejemplo, inicie sesión.

En algunas realizaciones, el dispositivo de autenticación puede soportar una lista blanca de ordenadores anfitriones (por ejemplo, en forma de una lista de direcciones Bluetooth de ordenadores anfitriones). En algunas realizaciones, dicha lista blanca puede contener los ordenadores anfitriones que les permite configurar una conexión Bluetooth con el dispositivo de autenticación. Si un ordenador huésped intenta establecer una conexión Bluetooth con el dispositivo de autenticación, el dispositivo de autenticación puede verificar si ese ordenador huésped está incluido en esa lista blanca y si el ordenador huésped está realmente incluido en esa lista blanca, el dispositivo de autenticación puede aceptar el intento de conexión. En algunas realizaciones, el dispositivo de autenticación puede rechazar el intento de conexión de un ordenador huésped que no está en la lista blanca del dispositivo de autenticación. En algunas realizaciones, el dispositivo de autenticación puede soportar un mecanismo para añadir o eliminar ordenadores anfitriones a o desde la lista blanca del dispositivo de autenticación. En algunas realizaciones, un dispositivo de autenticación puede soportar comandos que pueden ser emitidos por una aplicación para añadir o eliminar ordenadores anfitriones a o de la lista blanca del dispositivo de autenticación. En algunas realizaciones, tales comandos se pueden asegurar mediante un mecanismo de mensajería seguro como se explica en otra parte de esta descripción con más detalle, por ejemplo para asegurar la autenticidad y/o integridad de los comandos. En algunas realizaciones, cuando un ordenador huésped intenta configurar una conexión Bluetooth con el dispositivo de autenticación y el ordenador huésped no está en la lista blanca del dispositivo de autenticación, el dispositivo de autenticación puede solicitar al usuario que confirme si acepta o no la conexión y/o si se debe incluir el ordenador huésped en la lista blanca.

En algunas realizaciones, un dispositivo de autenticación se puede fabricar con una lista blanca inicial incorporada de ordenadores anfitriones aceptables. En algunas realizaciones, dicha lista blanca inicial incorporada puede comprender los ordenadores anfitriones que en una etapa posterior se pueden usar para cargar datos de personalización y configuración en el dispositivo de autenticación. En algunas realizaciones, la lista blanca inicial se puede eliminar, reemplazar por otra lista blanca y/o actualizar durante una etapa posterior, tal como una etapa de personalización y/o configuración.

En algunas realizaciones, también se le puede solicitar al usuario que proporcione una contraseña estática extra a la aplicación por encima de la credencial dinámica generada por el dispositivo de autenticación. Esto proporciona la autenticación de dos factores: algo que usted conoce (la contraseña estática) y algo que tiene (el dispositivo de autenticación particular asociado con el usuario, cuya posesión se demuestra por la capacidad del usuario para proporcionar una credencial dinámica correcta a la aplicación).

En algunas realizaciones, el dispositivo de autenticación puede tener una interfaz de entrada de usuario que está adaptada para capturar un valor de PIN y/o contraseña proporcionado por el usuario. En algunas realizaciones, el dispositivo de autenticación puede estar adaptado para recibir un PIN (número de identificación personal) y/o valor de contraseña a través de la conexión Bluetooth desde el ordenador huésped. En algunas realizaciones, la aplicación cliente que se ejecuta en el ordenador huésped puede solicitar al usuario que ingrese un valor de PIN y/o contraseña en la interfaz de entrada del usuario del ordenador huésped y puede reenviar ese valor de PIN y/o contraseña al dispositivo de autenticación a través de la conexión Bluetooth que se ha configurado entre el ordenador huésped y el dispositivo de autenticación. En algunas realizaciones, el dispositivo de autenticación puede estar adaptado para verificar un valor de PIN y/o contraseña que ha recibido a través de la conexión Bluetooth o que ha recibido del usuario a través del dispositivo de entrada de usuario del dispositivo de autenticación. En algunas realizaciones, el dispositivo de autenticación puede estar adaptado para almacenar un valor de referencia de PIN y/o contraseña y puede verificar el valor de PIN y/o contraseña recibido mediante la comparación del valor recibido con el valor de referencia almacenado. En algunas realizaciones, una verificación exitosa de PIN y/o contraseña puede ser una condición para que el dispositivo de autenticación genere una credencial dinámica. Es decir, en algunas realizaciones, el dispositivo de autenticación puede generar una credencial dinámica solo si se ha proporcionado primero un PIN y/o contraseña al dispositivo de autenticación y se ha verificado con éxito por el dispositivo de autenticación.

En algunas realizaciones, el dispositivo de autenticación puede tener un sensor biométrico para capturar una medición

de alguna biometría del usuario. Por ejemplo, en algunas realizaciones, el dispositivo de autenticación puede tener un sensor de huellas digitales. En algunas realizaciones, el dispositivo de autenticación puede estar adaptado para recibir a través de una conexión Bluetooth con un ordenador huésped una medición de alguna biometría del usuario que se puede haber obtenido por el ordenador huésped. En algunas realizaciones, el dispositivo de autenticación puede almacenar datos de referencia biométricos para un usuario. En algunas realizaciones, el dispositivo de autenticación puede estar adaptado para comparar una medición de una biometría del usuario (que el dispositivo de autenticación puede haber capturado usando un sensor biométrico del dispositivo de autenticación o que el dispositivo de autenticación puede haber recibido del ordenador huésped) con datos de referencia biométricos almacenados en el dispositivo de autenticación. En algunas realizaciones, el éxito de dicha comparación puede ser una condición para que el dispositivo de autenticación genere una credencial dinámica. Es decir, en algunas realizaciones, el dispositivo de autenticación puede generar una credencial dinámica solo si una medición de una biométrica del usuario se ha proporcionado primero al dispositivo de autenticación y el dispositivo de autenticación ha comparado con éxito los datos de referencia biométricos almacenados en el dispositivo.

En algunas realizaciones, cuando un componente del ordenador huésped (por ejemplo, la aplicación de autenticación de cliente) ha recibido del dispositivo de autenticación la credencial dinámica generada por el dispositivo de autenticación, el ordenador huésped puede reenviar la credencial dinámica recibida al servidor de aplicación o algún servidor de verificación de credenciales dinámicas. Después de recibir la credencial dinámica reenviada, el servidor de aplicación del servidor de verificación puede verificar la credencial dinámica recibida. Después de la verificación exitosa de la credencial dinámica, el servidor de aplicación puede tomar la acción apropiada, como iniciar sesión en el usuario o dar acceso al usuario a un determinado recurso o determinada información o aceptar una transacción presentada por el usuario.

En algunas realizaciones, la conexión Bluetooth también se puede usar para proporcionar datos personalizados al dispositivo de autenticación, tal como, por ejemplo, datos asociados con el usuario con los que está asociado el dispositivo de autenticación (por ejemplo, un nombre de usuario) o datos secretos extra tales como las claves criptográficas.

En algunas realizaciones, el dispositivo de autenticación puede estar adaptado para almacenar uno o más nombres de usuario del usuario que está asociado con el dispositivo de autenticación. En algunas realizaciones, una aplicación cliente en un ordenador huésped que está conectado por una conexión Bluetooth con el dispositivo de autenticación puede leer uno de los nombres de usuario almacenados en el dispositivo de autenticación usando la conexión Bluetooth. En algunas realizaciones, una aplicación cliente también puede escribir un nombre de usuario en el dispositivo de autenticación usando la conexión Bluetooth.

En algunas realizaciones, la capacidad de un dispositivo de autenticación para almacenar un nombre de usuario puede ser usada por la aplicación de la siguiente manera. Cuando el usuario intenta iniciar sesión en una aplicación, la aplicación puede requerir un nombre de usuario y credenciales de usuario. La aplicación cliente en el ordenador huésped que el usuario está usando para acceder a la aplicación puede configurar una conexión Bluetooth con el dispositivo de autenticación del usuario. Esto puede implicar que la aplicación cliente indique o solicite al usuario que encienda el dispositivo de autenticación. Alternativamente, el usuario puede encender el dispositivo de autenticación sobre el cual el dispositivo de autenticación puede usar su interfaz Bluetooth para anunciar su presencia al ordenador huésped y se puede establecer una conexión Bluetooth entre el ordenador huésped y el dispositivo de autenticación y la aplicación cliente puede reconocer el dispositivo de autenticación como un dispositivo de autenticación y asumir automáticamente que el usuario desea iniciar sesión. La aplicación cliente después puede usar la conexión Bluetooth para verificar si el dispositivo de autenticación tiene un nombre de usuario almacenado y obtener ese nombre de usuario si efectivamente el dispositivo de autenticación almacena un nombre de usuario. Si la aplicación cliente no pudo obtener el nombre de usuario del dispositivo de autenticación, puede solicitar o indicar al usuario que proporcione manualmente el nombre de usuario apropiado a través de la interfaz de entrada de usuario del ordenador huésped. La aplicación cliente puede usar la conexión Bluetooth para obtener también una credencial de usuario, tal como una contraseña de un solo uso o una respuesta a un desafío, del dispositivo de autenticación. La aplicación cliente puede reenviar el nombre de usuario y la credencial de usuario a la aplicación para su verificación. Si la verificación fue exitosa, la aplicación cliente puede almacenar el nombre de usuario que se utilizó con éxito en el dispositivo de autenticación mediante la conexión Bluetooth.

En algunas realizaciones, el dispositivo de autenticación puede estar adaptado para generar comandos y comunicar estos comandos a través de la conexión Bluetooth al ordenador huésped conectado, con lo cual la aplicación cliente puede ejecutar estos comandos en el ordenador huésped. Por ejemplo, en algunas realizaciones, el dispositivo de autenticación puede usar la conexión Bluetooth para enviar un comando al ordenador huésped que contiene un mensaje para presentar al usuario, y la aplicación cliente puede recibir dicho comando y presentar el mensaje contenido en el comando al usuario en la interfaz de salida de usuario del ordenador huésped. En algunas realizaciones, el mensaje contenido en el comando puede tener la forma de una cadena de caracteres (por ejemplo, una cadena de caracteres ASCII o Unicode). En algunas realizaciones, el mensaje puede estar contenido en el comando en forma de un indicador de mensaje o referencia que la aplicación del cliente puede usar para determinar el mensaje real para presentar al usuario.

En algunas realizaciones, el dispositivo de autenticación puede usar la conexión Bluetooth para enviar un comando al

ordenador huésped solicitando que devuelva un PIN o contraseña al dispositivo de autenticación. La aplicación cliente en el ordenador huésped puede recibir este mensaje y en respuesta puede usar la interfaz de salida del usuario del ordenador huésped para solicitar al usuario que proporcione un PIN y/o contraseña y la aplicación cliente puede capturar el PIN y/o la contraseña provistos por el usuario usando la interfaz de entrada de usuario del ordenador huésped y usar la conexión Bluetooth para enviar el PIN y/o contraseña capturados. En algunas realizaciones, el dispositivo de autenticación puede usar la conexión Bluetooth para enviar un comando al ordenador huésped que solicita devolver la medición biométrica del usuario al dispositivo de autenticación. La aplicación cliente en el ordenador huésped puede recibir este mensaje y, en respuesta, puede usar la interfaz de salida del usuario del ordenador huésped para solicitar al usuario que proporcione una información biométrica y la aplicación cliente puede usar, por ejemplo, un sensor biométrico (tal como un sensor de huellas digitales) del ordenador huésped para medir la biometría presentada por el usuario y usar la conexión Bluetooth para enviar esa medición biométrica al dispositivo de autenticación.

En algunas realizaciones, una aplicación también puede tener en cuenta la mera presencia de un dispositivo de autenticación habilitado con Bluetooth para autenticar a un usuario. Por ejemplo, en algunas realizaciones, un usuario puede autenticar sobre la base de únicamente en la detección de Bluetooth por un ordenador huésped del dispositivo de autenticación. En algunas realizaciones, una aplicación puede autorizar a un usuario a realizar algunas acciones tan pronto como se ha detectado la presencia del dispositivo de autenticación del usuario y puede autorizar al usuario a realizar otras acciones (adicionales) una vez que una credencial dinámica generada por el dispositivo de autenticación se ha recibido y verificado con éxito.

En algunas realizaciones, la aplicación puede monitorear la presencia continua del dispositivo de autenticación. En algunas realizaciones, la aplicación puede tener en cuenta la presencia o ausencia del dispositivo de autenticación de un usuario cuando se concede o revoca autorizaciones a ese usuario. Por ejemplo, en algunas realizaciones después de que un usuario se haya autenticado con éxito, la autorización que el usuario puede haber recibido en respuesta a esa autenticación exitosa (por ejemplo, para realizar ciertas acciones o tener acceso a ciertos recursos) se puede retirar cuando la aplicación detecta que el dispositivo de autenticación ya no está presente en el ordenador huésped. En algunas realizaciones, la aplicación puede considerar que el dispositivo está presente a condición de que se mantenga la conexión Bluetooth. En algunas realizaciones, la aplicación puede considerar que el dispositivo de autenticación está presente siempre que el dispositivo de autenticación permanezca dentro de una determinada distancia del ordenador huésped (por lo que la intensidad de la señal Bluetooth del dispositivo de autenticación se puede usar como un proxy para la distancia como se explica con más detalle a continuación). En algunas realizaciones, la aplicación puede considerar que el dispositivo está ausente cuando se rompe la conexión Bluetooth. En algunas realizaciones, la aplicación puede considerar que el dispositivo de autenticación está ausente cuando el dispositivo de autenticación ya no está dentro de una determinada distancia mínima del ordenador huésped (por lo que la intensidad de la señal Bluetooth del dispositivo de autenticación se puede usar como un proxy para la distancia como se explica con más detalle a continuación).

En algunas realizaciones, la aplicación puede tener en cuenta la distancia del dispositivo de autenticación desde el ordenador huésped. Por ejemplo, en algunas realizaciones, la aplicación solo puede aceptar un usuario o solicitudes del usuario si la distancia del dispositivo de autenticación del usuario desde el ordenador huésped es menor que cierto umbral. En algunas realizaciones, la aplicación puede cerrar una sesión que el usuario ha configurado usando el dispositivo de autenticación, cuando la aplicación detecta que la distancia entre el dispositivo de autenticación y el ordenador huésped ha excedido un cierto valor umbral. En algunas realizaciones, la aplicación puede usar la intensidad de la señal Bluetooth emitida por el dispositivo de autenticación como un proxy de la distancia entre el dispositivo de autenticación y el ordenador huésped. En algunas realizaciones, el dispositivo de autenticación puede tener la intensidad de la señal recibida desde el ordenador huésped, por ejemplo, cuando decida aceptar un intento de conexión o cuando decida aceptar o rechazar un mensaje o comando de aplicación entrante. En algunas realizaciones, el RSSI (Indicador de intensidad de señal recibida) de la conexión Bluetooth se puede usar como una medida de la intensidad de la señal.

En algunas realizaciones, la aplicación puede configurar automáticamente una conexión Bluetooth con un dispositivo de autenticación que esté cerca de un ordenador huésped. En algunas realizaciones, la aplicación puede configurar una conexión Bluetooth con el dispositivo de autenticación cuando la intensidad de la señal Bluetooth del dispositivo de autenticación es mejor que un cierto nivel mínimo. En algunas realizaciones, el Bluetooth o apareamiento Bluetooth de baja energía se usa automáticamente para la conexión Bluetooth que se configura. En algunas realizaciones, diferentes dispositivos de autenticación individuales pueden tener diferentes claves de apareamiento. En algunas realizaciones, la aplicación puede recuperar la clave de apareamiento que se utilizará para un dispositivo de autenticación específico usando un elemento de datos de identificación del dispositivo (tales como por ejemplo, una dirección Bluetooth) del dispositivo de autenticación. En algunas realizaciones, la aplicación puede derivar la clave de apareamiento del dispositivo de autenticación del elemento de datos de identificación del dispositivo del dispositivo de autenticación y alguna clave maestra que sea la misma para una pluralidad de dispositivos de autenticación. En algunas realizaciones, el usuario puede proporcionar la clave de apareamiento a la aplicación (por ejemplo, en el primer uso del dispositivo de autenticación) y la aplicación puede almacenar (por ejemplo, en una base de datos) una relación entre la clave de apareamiento proporcionada por el usuario y un elemento de datos de identificación del dispositivo de autenticación. En algunas realizaciones, después de que se ha configurado la conexión Bluetooth, la aplicación puede identificar automáticamente al usuario del dispositivo de autenticación (por ejemplo, usando un

elemento de datos de identificación del dispositivo o un identificador de usuario suministrado por el dispositivo de autenticación a través de la conexión Bluetooth). En algunas realizaciones, la aplicación puede autenticar al usuario. En algunas realizaciones (por ejemplo, si el apareamiento se usa con una clave de apareamiento única para cada dispositivo de autenticación diferente), se puede considerar implícitamente que el usuario se autentica con éxito una vez que la conexión Bluetooth se ha configurado con éxito usando el apareamiento. En algunas realizaciones, la aplicación puede solicitar al dispositivo de autenticación que genere y devuelva (a través de la conexión Bluetooth) una credencial dinámica que después se puede verificar mediante la aplicación. En algunas realizaciones, se puede requerir que el usuario tome alguna acción durante el proceso de autenticación. Por ejemplo, en algunas realizaciones, el usuario debe indicar su aprobación al dispositivo de autenticación (por ejemplo, presionando un determinado botón en el dispositivo de autenticación). En algunas realizaciones, se puede requerir que el usuario durante el proceso de autenticación proporcione un PIN o contraseña estática que después puede ser verificada por la aplicación. En algunas realizaciones, la aplicación puede, tras una autenticación exitosa del usuario, conceder algunas autorizaciones al usuario (tales como concesión de acceso a algunos recursos o aceptar solicitudes de la aplicación de usuario, tales como solicitudes para realizar ciertas acciones o transacciones). Entonces la aplicación puede monitorear si el dispositivo de autenticación permanece presente. En algunas realizaciones, la aplicación puede revocar una o más de las autorizaciones concedidas cuando la aplicación advierte que el dispositivo de autenticación ya no está presente. En algunas realizaciones, si después que la aplicación detecta que el dispositivo de autenticación está presente nuevamente (en el mismo o en otro ordenador huésped), la aplicación puede volver a conceder una o más de las autorizaciones revocadas. En algunas realizaciones, si la aplicación detecta que el dispositivo de autenticación está presente nuevamente, la aplicación puede volver a autenticar al usuario. En algunas realizaciones, la autenticación de nuevo del usuario se puede hacer usando un procedimiento de autenticación que puede ser más simple que un procedimiento de autenticación usado para una autenticación anterior. Por ejemplo, en algunas realizaciones, el procedimiento de autenticación más simple puede no requerir acciones explícitas del usuario, tal como indicar la aprobación del suministro de un PIN o contraseña estática, mientras que el procedimiento de autenticación original o estándar puede requerir tales acciones explícitas del usuario. En algunas realizaciones, la aplicación puede decidir qué tipo de reautenticación usar (y/o si la reautenticación debe ocurrir) sobre la base del tiempo transcurrido entre el momento de la reautorización y algún evento de referencia tal como una autenticación previa o cuando la aplicación notó que el dispositivo de autenticación ya no estaba presente.

Por ejemplo, en algunas realizaciones, un usuario puede recibir ciertas autorizaciones en algún ordenador huésped tan pronto como la aplicación detecta la presencia del dispositivo de autenticación del usuario en el ordenador huésped y estas autorizaciones se pueden revocar cuando la aplicación detecta que el dispositivo de autenticación del usuario ya no está presente. Este mecanismo se puede usar, por ejemplo, para asegurar el acceso del personal médico a los archivos médicos de los pacientes en los ordenadores de un hospital o para asegurar el acceso físico a ubicaciones físicas mediante el desbloqueo y rebloqueo de puertas que dependen de la presente de los dispositivos de autenticación de los usuarios en las puertas.

Breve descripción de los dibujos

Las características y ventajas anteriores y otras de la invención serán evidentes a partir de la siguiente descripción más particular de las realizaciones de la invención, como se ilustra en los dibujos adjuntos.

La **Figura** 1 ilustra esquemáticamente un ejemplo de un aparato de acuerdo con un aspecto de la invención.

La **Figura** 2 ilustra esquemáticamente un ejemplo de un sistema de acuerdo con un aspecto de la invención.

Las **Figuras** 3A y 3B ilustran esquemáticamente un ejemplo de un procedimiento de acuerdo con un aspecto de la invención.

Descripción detallada

Algunas implementaciones de la presente invención se analizan a continuación. Si bien se analizan implementaciones específicas, se debe entender que esto se hace solo con fines ilustrativos. Una persona experta en la técnica relevante reconocerá que se pueden usar otros componentes y configuraciones sin separarse del alcance de la invención.

La **Figura** 1 ilustra esquemáticamente un ejemplo de aparato de la invención de acuerdo con un aspecto de la invención.

En algunas realizaciones el aparato comprende un dispositivo de autenticación (100) para generación de una credencial dinámica que puede comprender: un componente de almacenamiento (130) adaptado para almacenar de manera segura un secreto criptográfico; una interfaz de entrada de usuario (120) para recepción de entradas de un usuario del dispositivo de autenticación; una interfaz de salida de usuario (110) para presentación de salidas al usuario; un componente de procesamiento de datos (140) adaptado para generar dicha credencial dinámica mediante la combinación criptográfica de dicha clave de secreto criptográfico con una variable dinámica; y una interfaz Bluetooth (150) para conexión del dispositivo de autenticación a un ordenador huésped; en el que dicho dispositivo de autenticación está adaptado para enviar dicha credencial dinámica generada a dicho ordenador huésped. En algunas realizaciones el dispositivo de autenticación también puede comprender un reloj (160). En algunas realizaciones el dispositivo de autenticación también puede comprender un sensor biométrico (170).

En algunas realizaciones la interfaz de salida del usuario (110) puede comprender una pantalla tal como una pantalla de cristal líquido (LCD). En algunas realizaciones, la interfaz de salida de usuario puede comprender un altavoz. En algunas realizaciones, la interfaz de salida de usuario puede comprender un componente de síntesis de voz. En algunas realizaciones, la interfaz de salida del usuario (110) se puede adaptar para presentar a los datos del usuario, tal como por ejemplo los datos de transacción que se aprobarán para el usuario. En algunas realizaciones, la interfaz de salida del usuario se puede adaptar para presentar al usuario una credencial dinámica generada. En algunas realizaciones, la credencial dinámica generada puede ser presentada por el dispositivo de autenticación al usuario como una cadena de dígitos o caracteres. En algunas realizaciones, la cadena de dígitos puede consistir en una cadena de dígitos numéricos. En algunas realizaciones, la cadena de caracteres puede consistir en una cadena de caracteres alfanuméricos. En algunas realizaciones, la interfaz de salida del usuario puede consistir en una pantalla que está limitada a mostrar una línea única de caracteres al usuario. En algunas realizaciones, la interfaz de salida del usuario puede consistir en una pantalla que se limita a mostrar dos líneas de caracteres al usuario. Un dispositivo de autenticación con una pantalla que se limita a mostrar solo una o dos líneas al usuario puede tener un factor de forma muy compacto.

En alguna realización, la interfaz de entrada de usuario (120) puede comprender un teclado. En algunas realizaciones, la interfaz de entrada de usuario puede consistir en un botón único. En algunas realizaciones, la interfaz de entrada de usuario puede consistir exactamente de dos botones: un botón se puede usar, por ejemplo, para indicar la aprobación del usuario mientras que el otro botón puede usarse, por ejemplo, por el usuario para rechazar datos o cancelar una operación. En algunas realizaciones, el usuario puede encender el dispositivo presionando los dos botones simultáneamente o uno rápidamente después del otro (por ejemplo, con un intervalo de tiempo entre las dos presiones de menos de 2 segundos). En algunas realizaciones, la interfaz de entrada del usuario se puede adaptar para capturar una aprobación del usuario. En algunas realizaciones, la interfaz de entrada del usuario se puede adaptar para capturar un rechazo del usuario. En algunas realizaciones, la interfaz de entrada del usuario se puede adaptar para capturar el valor de un PIN o contraseña proporcionada por el usuario al dispositivo de autenticación.

En algunas realizaciones el componente de almacenamiento (130) por ejemplo, puede comprender memoria ROM, EEPROM, Flash o RAM. En algunas realizaciones el componente de almacenamiento puede estar adaptado para almacenar de manera segura secretos criptográficos y/o claves criptográficas que el dispositivo de autenticación puede usar por ejemplo, en la generación de una credencial dinámica o soportar técnicas de mensajería seguras cuando se recibe o generan mensajes de aplicación que están protegidos por mensajería segura. En algunas realizaciones el componente de almacenamiento se puede adaptar para almacenar datos de referencia de PIN y/o contraseña. En algunas realizaciones, el componente de almacenamiento se puede adaptar para almacenar datos de referencia biométricos. En algunas realizaciones, el componente de almacenamiento se puede adaptar para almacenar datos de referencia biométricos. En algunas realizaciones, el componente de almacenamiento se puede adaptar para almacenar una variable dinámica cuyo valor puede ser actualizado por el dispositivo de autenticación, por ejemplo, cada vez que el dispositivo de autenticación utiliza la variable dinámica almacenada para generar una credencial dinámica.

En algunas realizaciones, el componente de procesamiento de datos (140) por ejemplo, puede comprender uno o más microprocesadores, controladores (por ejemplo, para manejar las interfaces de entrada y salida), FPGA (matrices de puertas programables en campo) y/o ASIC (circuitos integrados específicos de la aplicación) En algunas realizaciones el componente de procesamiento de datos se puede adaptar para realizar algoritmos criptográficos. En algunas realizaciones el componente de procesamiento de datos puede estar adaptado para generar credenciales dinámicas. En algunas realizaciones el componente de procesamiento de datos puede estar adaptado para generar una credencial dinámica mediante la combinación criptográfica de un secreto (que se puede almacenar, por ejemplo en el componente de almacenamiento (130)) con una variable dinámica. En algunas realizaciones, la variable dinámica se puede basar en el valor de una variable interna tal como un valor de tiempo provisto por un reloj del dispositivo de autenticación, o tal como un valor relacionado con el contador que se puede almacenar en el componente de almacenamiento (130). En algunas realizaciones, la variable dinámica se puede basar en un valor generado externamente, tal como por ejemplo un desafío o datos de transacción, que se pueden proporcionar al dispositivo de autenticación, por ejemplo, a través de una conexión Bluetooth. En algunas realizaciones, el componente de procesamiento de datos se puede adaptar para verificar un valor de PIN y/o contraseña, por ejemplo, mediante su comparación con datos de referencia de PIN y/o contraseña que se pueden almacenar en el componente de almacenamiento (130). En algunas realizaciones, el componente de procesamiento de datos se puede adaptar para verificar una medición de un biometría del usuario, por ejemplo, mediante su comparación con los datos de referencia biométricos que se pueden almacenare en el componente de almacenamiento (130).

En algunas realizaciones, la interfaz Bluetooth (150) puede ser del tipo Bluetooth baja energía o Bluetooth LE. En algunas realizaciones, la interfaz de Bluetooth puede ser compatible con la especificación del núcleo de Bluetooth Versión 4.0. En algunas realizaciones, la interfaz Bluetooth puede soportar la operación de la función de periférico (esclavo). En algunas realizaciones, el dispositivo de autenticación puede funcionar como un Periférico de Perfil de acceso genérico (GAP) de Bluetooth y puede ser un esclavo de Bluetooth LE y/o un servidor de Perfil de atributo genérico (GATT).

En algunas realizaciones, la interfaz Bluetooth soporta el apareamiento Bluetooth. En algunas realizaciones, el dispositivo de autenticación puede soportar el apareamiento con múltiples ordenadores anfitriones y puede almacenar

información de apareamiento para múltiples ordenadores anfitriones. En algunas realizaciones, el dispositivo de autenticación puede soportar el apareamiento con como máximo un ordenador huésped único y puede almacenar información de apareamiento para un ordenador huésped único. En algunas realizaciones, si el dispositivo de autenticación se ha apareado, el dispositivo de autenticación sólo puede permitir un nuevo apareamiento si primero se elimina explícitamente un apareamiento existente. En algunas realizaciones, el dispositivo de autenticación se puede adaptar para permitir que el usuario indique que se debe eliminar un apareamiento existente.

En algunas realizaciones, cuando la interfaz Bluetooth del dispositivo de autenticación está en el estado de anuncios, solo envía eventos de anuncios no dirigidos conectables. En algunas realizaciones, la interfaz Bluetooth del dispositivo de autenticación soporta el modo de descubrimiento descubrible limitado. En algunas realizaciones, el dispositivo de autenticación está adaptado para iniciar el modo de descubrimiento descubrible limitado tras un evento iniciado por un usuario específico, tal como por ejemplo, cuando el usuario presiona un botón. En algunas realizaciones, el dispositivo de autenticación permanece descubrible durante no más de 60 segundos.

En algunas realizaciones, el dispositivo de autenticación soporta varios servicios GATT. En algunas realizaciones, el dispositivo de autenticación soporta uno o más servicios, que pueden ser servicios GATT, para intercambiar mensajes de autenticación con el ordenador huésped. En algunas realizaciones, el dispositivo de autenticación soporta uno o más servicios, que pueden ser servicios GATT, para informar al ordenador huésped sobre el estado del dispositivo de autenticación y más en particular sobre el estado de la aplicación de autenticación en el dispositivo de autenticación. En algunas realizaciones, el dispositivo de autenticación puede dedicar ciertas Características de Servicio para recibir ciertos datos (por ejemplo, valores de desafío o datos de transacción para ser usados por el dispositivo de autenticación para generar una credencial dinámica) desde el ordenador huésped conectado al dispositivo de autenticación. En algunas realizaciones, el dispositivo de autenticación puede dedicar ciertas Características de Servicio para enviar ciertos datos (por ejemplo, credenciales dinámicas generadas por el dispositivo de autenticación o información de estado) al ordenador huésped conectado al dispositivo de autenticación.

Por ejemplo, en algunas realizaciones, el dispositivo de autenticación puede soportar un servicio GATT de mensajería de aplicación de autenticación para intercambiar mensajes de aplicación de autenticación entre el dispositivo de autenticación, por un lado, y el ordenador huésped o el servidor de aplicaciones (a través del ordenador huésped) por otro lado. Este servicio GATT de mensajería de aplicación puede comprender una Característica para transmitir mensajes de aplicación de autenticación desde el ordenador huésped al dispositivo de autenticación y otra Característica para transmitir mensajes de aplicación de autenticación desde el dispositivo de autenticación al ordenador huésped.

El dispositivo de autenticación también puede soportar otro servicio GATT de información de estado de la aplicación que comprende al menos una característica para enviar actualizaciones sobre el estado de la aplicación del dispositivo de autenticación al ordenador huésped.

En algunas realizaciones, la aplicación puede recibir ciertos datos o información del dispositivo de autenticación mediante el sondeo regular del dispositivo de autenticación, mediante la lectura regular de una o más características.

En algunas realizaciones, el dispositivo de autenticación puede enviar ciertos datos al ordenador huésped conectado al dispositivo de autenticación usando el mecanismo de notificación Bluetooth GATT. En algunas realizaciones, el dispositivo de autenticación puede enviar ciertos datos al ordenador huésped conectado al dispositivo de autenticación usando el mecanismo de indicación GATT de Bluetooth. En realizaciones en las que el dispositivo de autenticación usa el mecanismo de indicación para enviar ciertos datos al ordenador huésped, el dispositivo de autenticación puede así obtener la confirmación después de que el ordenador huésped ha recibido efectivamente los datos que el dispositivo de autenticación pretendía enviar al ordenador huésped, lo que a su vez, puede permitir que el dispositivo de autenticación asegure que el ordenador huésped permanece sincronizado con el dispositivo de autenticación. Por ejemplo, en algunas realizaciones, un dispositivo de autenticación se puede adaptar para cambiar el estado de la aplicación solo cuando el ordenador huésped haya confirmado que ha recibido la información última del estado de la aplicación. En algunas realizaciones, el dispositivo de autenticación puede enviar algunos mensajes de aplicación de autenticación en múltiples paquetes uno tras otro (por ejemplo, usando la misma característica) y puede estar adaptado para enviar un paquete siguiente solo después de que el ordenador huésped haya confirmado que ha recibido el paquete anterior.

En algunas realizaciones, el dispositivo de autenticación puede estar adaptado para recibir a través de los mensajes de aplicación entrantes de la interfaz Bluetooth que se pueden haber generado por una aplicación. En algunas realizaciones, el dispositivo de autenticación puede estar adaptado para generar mensajes de aplicación salientes que el dispositivo de autenticación puede comunicar a la aplicación a través de la interfaz Bluetooth. En algunas realizaciones, al menos algunos de estos mensajes de aplicación entrantes y/o salientes pueden haber sido asegurados por técnicas de mensajería segura y el dispositivo de autenticación puede estar adaptado para soportar estas técnicas de mensajería seguras. El componente de procesamiento de datos del dispositivo de autenticación puede estar adaptado para ejecutar algoritmos criptográficos usados para asegurar estos mensajes de aplicación. Por ejemplo, el componente de procesamiento de datos puede estar adaptado para cifrado y/o descifrado de datos transportados en mensajes de aplicación, y/o puede estar adaptado para generar o verificar MAC que se pueden incluir en mensajes de aplicación para asegurar la integridad y/o autenticidad de estos mensajes.

En algunas realizaciones el dispositivo de autenticación también puede comprender un reloj (160) para proporcionar un valor de tiempo que se puede usar con el dispositivo de autenticación para determinar el valor de la variable dinámica.

En algunas realizaciones el dispositivo de autenticación también puede comprender un sensor biométrico (170). En algunas realizaciones el sensor biométrico, por ejemplo, puede comprender un sensor de huellas digitales. En algunas realizaciones, el sensor de huellas digitales por ejemplo, puede comprender un sensor de deslizamiento del dedo.

En algunas realizaciones, el dispositivo de autenticación puede ser un dispositivo de bolsillo, portátil y de mano. En algunas realizaciones, el dispositivo de autenticación puede tener una longitud de menos de 7 cm, un ancho de menos de 3 cm y un espesor de menos de 1 cm. En algunas realizaciones, el dispositivo puede tener un peso total (baterías incluidas) de menos de 20 gramos. En algunas realizaciones, el dispositivo de autenticación puede tener una longitud de menos de 10 cm, un ancho de menos de 6 cm y un espesor de menos de 1,5 cm y el dispositivo de autenticación puede tener un peso total (baterías incluidas) de menos de 100 gramos.

La **Figura 2** ilustra esquemáticamente un ejemplo de un sistema de acuerdo con un aspecto de la invención.

En algunas realizaciones, un sistema para asegurar una interacción entre una aplicación y un usuario, tal como el sistema (200) ilustrado en la figura 2, puede comprender: un servidor de aplicación (210) para alojar partes de servidor de la aplicación; un ordenador huésped (230) para permitir al usuario (290) acceder de forma remota a la aplicación a través de una red pública de telecomunicaciones (250); un dispositivo de autenticación (240) para generar una credencial dinámica, tal como cualquiera de los dispositivos de autenticación descritos en los párrafos anteriores; y un servidor de verificación (220) para verificar la validez de la credencial dinámica; por lo que el ordenador huésped puede estar adaptado para establecer una conexión Bluetooth con el dispositivo de autenticación y puede estar adaptado para ejecutar una parte del cliente de la aplicación, el dispositivo de autenticación puede estar adaptado para generar la credencial dinámica y devolver la credencial dinámica a dicho ordenador huésped, el ordenador huésped también puede estar adaptado para enviar la credencial dinámica generada al servidor de verificación para su verificación; el servidor de verificación puede estar adaptado para verificar la credencial dinámica generada y para señalar al servidor de aplicación si se ha verificado que la credencial dinámica es válida.

En algunas realizaciones, el servidor de aplicaciones y el servidor de verificación pueden ser el mismo servidor. En algunas realizaciones, el servidor de aplicación y el servidor de verificación pueden comprender uno o más ordenadores servidor. En algunas realizaciones, la red de telecomunicaciones puede comprender Internet y/o una red de telecomunicaciones inalámbrica. En algunas realizaciones, el ordenador huésped puede tener una interfaz de usuario para interactuar localmente con el usuario. Por ejemplo, en algunas realizaciones, el ordenador huésped puede tener una interfaz de entrada de usuario, tal como un teclado, un ratón o una pantalla táctil para recibir la entrada de usuario. En algunas realizaciones, el ordenador huésped puede tener una interfaz de salida de usuario, tal como una pantalla o un altavoz, para presentar la salida, que puede comprender señales visuales o auditivas, a un usuario. En algunas realizaciones, el ordenador huésped puede comprender una PC (ordenador personal), tableta o teléfono inteligente.

En algunas realizaciones, la aplicación (tal como una aplicación de banca por Internet) puede comprender una parte de servidor que se ejecuta en un servidor de aplicación remoto y una parte de cliente que se ejecuta en el ordenador huésped local del usuario y con la que el usuario interactúa para acceder a la parte de servidor de la aplicación, por ejemplo, a través de Internet. En algunas realizaciones, la aplicación puede comprender una aplicación basada en web y el servidor de aplicaciones puede comprender un servidor web. En algunas realizaciones, el usuario puede acceder al servidor de aplicaciones usando un navegador web en el ordenador huésped del usuario. En algunas realizaciones, la parte de cliente de la aplicación puede comprender un subprograma (tal como un subprograma de Java) o un guión que se ejecuta en un navegador web en el ordenador huésped del usuario. En algunas realizaciones, el navegador web puede usar un complemento de cliente de autenticación o una extensión de cliente de autenticación para interactuar con el dispositivo de autenticación que está conectado al ordenador huésped a través de una conexión Bluetooth. En algunas realizaciones, el usuario puede acceder a la parte de servidor de una aplicación con un teléfono inteligente. El teléfono inteligente entonces puede funcionar como el ordenador huésped (230) y la aplicación cliente que se ejecuta en el teléfono inteligente puede comprender una aplicación (tal como una aplicación de banca por Internet) en el teléfono inteligente mediante la cual la aplicación puede interactuar con el usuario a través de la interfaz de usuario del teléfono inteligente, con el servidor de aplicación por ejemplo, a través de Internet y con el dispositivo de autenticación a través de una conexión Bluetooth entre el teléfono inteligente y el dispositivo de autenticación. En algunas realizaciones, la parte de cliente de la aplicación que se ejecuta en el ordenador huésped se puede adaptar para proporcionar al usuario pautas sobre cómo interactuar con el dispositivo de autenticación. En algunas realizaciones, las pautas que la parte del cliente de la aplicación puede proporcionar al usuario sobre cómo interactuar con el dispositivo de autenticación se pueden referir al estado real de la aplicación del dispositivo de autenticación. En algunas realizaciones, la parte de cliente de la aplicación está adaptada para realizar un seguimiento del estado real de la aplicación del dispositivo de autenticación. En algunas realizaciones, el dispositivo de autenticación puede estar adaptado para enviar información del estado de la aplicación, que puede reflejar el estado de la aplicación real del dispositivo de autenticación, al ordenador huésped, y la parte de cliente de la aplicación que se ejecuta en el ordenador huésped puede estar adaptada para recibir esa información sobre el estado de la aplicación y usar esa información sobre el estado de la aplicación del dispositivo de autenticación para proporcionar pautas o instrucciones adecuadas

al usuario sobre cómo interactuar con el dispositivo de autenticación..

Por ejemplo, en algunas realizaciones, si bien el ordenador huésped aún no ha detectado la presencia de un dispositivo de autenticación, la aplicación cliente en el ordenador huésped puede indicar al usuario que encienda un dispositivo de autenticación. Cuando el ordenador huésped haya establecido una conexión Bluetooth con el dispositivo de autenticación del usuario, el ordenador huésped puede enviar un mensaje al dispositivo de autenticación solicitando una credencial dinámica, tal como una contraseña de un solo uso. En algunas realizaciones, el dispositivo de autenticación puede, al recibir tal mensaje de solicitud, entrar en un estado en el que espera que el usuario apruebe la generación de la credencial dinámica solicitada y puede indicar este estado al ordenador huésped. El ordenador huésped después puede solicitar al usuario que indique al dispositivo de autenticación (por ejemplo, presionando un botón específico de la interfaz de entrada de usuario del dispositivo de autenticación) que el usuario aprueba efectivamente la generación de la credencial dinámica solicitada. Si el usuario rechaza la solicitud (por ejemplo, presionando un botón específico para indicar el rechazo) o si se produce el tiempo de espera, el dispositivo de autenticación puede ir al estado correspondiente y comunicar ese estado al ordenador huésped, después de lo cual el ordenador huésped puede tomar la acción apropiada.

En algunas realizaciones, la aplicación puede solicitar al dispositivo de autenticación que firme numerosos campos de datos. Por ejemplo, en algunas realizaciones, la aplicación cliente en el ordenador huésped puede usar la conexión Bluetooth para enviar o reenviar una solicitud de aplicación al dispositivo de autenticación para firmar varios numerosos campos de datos. En algunas realizaciones, la aplicación cliente puede haber recibido esta solicitud desde una parte de servidor de la aplicación y puede reenviar la solicitud al dispositivo de autenticación usando la conexión Bluetooth. En algunas realizaciones, el dispositivo de autenticación puede presentar los campos de datos para firmar (usando una interfaz de salida de usuario del dispositivo de autenticación) uno por uno para que el usuario los revise y apruebe en el dispositivo de autenticación (por lo que el dispositivo de autenticación puede capturar la aprobación del usuario usando la interfaz de entrada de usuario del dispositivo de autenticación). En algunas realizaciones, cada vez que el dispositivo de autenticación presenta un campo de datos al usuario para su aprobación, puede entrar en un estado en el que espera la aprobación del usuario del campo de datos en el dispositivo de autenticación y puede informar al ordenador huésped que se encuentra en ese estado esperando que el usuario apruebe el campo de datos. La aplicación cliente en el ordenador huésped entonces puede solicitar al usuario que revise en el dispositivo de autenticación el campo de datos presentado por el dispositivo de autenticación y aprobar en el dispositivo de autenticación el campo de datos si parece ser correcto. Cuando el usuario haya aprobado el campo de datos, el dispositivo de autenticación puede pasar a un estado siguiente en el que presenta el campo de datos siguiente y espera la aprobación de ese campo de datos siguiente y puede informar al ordenador huésped que se ha movido al estado siguiente. La aplicación cliente en el ordenador huésped puede usar esa nueva información de estado para deducir que el usuario ha aprobado el campo de datos anterior en el dispositivo de autenticación y que el dispositivo de autenticación está esperando la aprobación del siguiente campo de datos y la aplicación cliente en el ordenador huésped ahora puede solicitar al usuario que revise y apruebe el siguiente campo de datos en el dispositivo de autenticación. Si el usuario rechaza un campo de datos o el tiempo de espera del dispositivo de autenticación se agota mientras espera la aprobación del usuario de un campo de datos, el dispositivo de autenticación se puede mover a un estado correspondiente e informar al ordenador huésped de ese estado. Si ese estado le indica al ordenador huésped que el usuario rechazó los datos, la aplicación puede cancelar la transacción a la que corresponden los datos. Si ese estado le indica al ordenador huésped que el dispositivo de autenticación agotó el tiempo de espera mientras esperaba la aprobación del usuario, la aplicación cliente en el ordenador huésped puede preguntarle al usuario si la transacción se debe cancelar o si el proceso de firma se debe reiniciar.

Las **Figuras 3A y 3B** ilustran esquemáticamente un ejemplo de un procedimiento (300) de acuerdo con un aspecto de la invención.

En algunas realizaciones, un sistema de autenticación y/o un dispositivo de autenticación como se describe en cualquiera de los párrafos anteriores se puede usar como sigue en un procedimiento para aseguramiento de la interacción de un usuario con una aplicación basada en ordenador. En algunas realizaciones, un usuario puede usar una aplicación cliente en un ordenador huésped local para interactuar con una aplicación mediante la cual el ordenador huésped local puede estar conectado a través de una red informática tal como, por ejemplo, Internet a un servidor de aplicaciones remoto que esté ejecutando una parte de servidor de la aplicación.

En algunas realizaciones, la aplicación cliente puede estar escaneando (305) la presencia de un dispositivo de autenticación habilitado para Bluetooth (posiblemente) adecuado. Si la aplicación cliente no puede detectar la presencia de un dispositivo de autenticación habilitado para Bluetooth activo (posiblemente) adecuado, la aplicación cliente puede solicitar o sugerir (306) al usuario (por ejemplo, mediante la muestra de un mensaje apropiado en la interfaz de salida del usuario del ordenador huésped) para encender un dispositivo de autenticación habilitado para Bluetooth o para activar la interfaz de Bluetooth de un dispositivo de autenticación.

Si la aplicación cliente detecta la presencia de múltiples dispositivos de autenticación habilitados para Bluetooth (posiblemente) adecuados, la aplicación cliente puede seleccionar (307) uno de los dispositivos de autenticación. Por ejemplo, en algunas realizaciones, la aplicación cliente puede recuperar un elemento de datos de identificación de dispositivo de cada uno de los dispositivos de autenticación detectados y usarlo para seleccionar el dispositivo de autenticación con el que interactuar. Por ejemplo, la aplicación cliente puede comparar los valores recuperados del

elemento de datos de identificación del dispositivo de los dispositivos de autenticación detectados con los elementos de datos de identificación del dispositivo de uno o más dispositivos de autenticación que pueden haber sido ya usados en el pasado con este ordenador huésped. En algunas realizaciones, la aplicación cliente puede presentar al usuario una lista de dispositivos de autenticación detectados y solicitar al usuario que seleccione uno.

Si la aplicación cliente ha detectado un dispositivo de autenticación habilitado para Bluetooth único o ha seleccionado uno de una pluralidad de dispositivos de autenticación habilitados para Bluetooth detectados, la aplicación cliente puede establecer una conexión Bluetooth (310) con el dispositivo de autenticación detectado o seleccionado.

En algunas realizaciones, la aplicación cliente puede recuperar (315) del dispositivo de autenticación un elemento de datos de identificación del dispositivo, tal como un número de serie, y reenviar ese elemento de datos de identificación del dispositivo a un componente de servidor de la aplicación. En respuesta, la aplicación cliente puede recibir del componente servidor de la aplicación un nombre de usuario. En algunas realizaciones, la aplicación cliente puede usar la conexión Bluetooth para recuperar (317) del dispositivo de autenticación un nombre de usuario. La aplicación cliente puede utilizar el nombre de usuario obtenido en interacciones posteriores con el componente de servidor de la aplicación y/o el usuario, tal como por ejemplo durante un intento de inicio de sesión. En algunas realizaciones, el componente de servidor de la aplicación puede usar el elemento de datos de identificación del dispositivo recibido para determinar el valor de uno o más valores secretos o claves criptográficas asociadas con el dispositivo de autenticación, tal como por ejemplo un conjunto de claves de mensajería seguras para asegurar mensajes para enviar al dispositivo de autenticación o uno o más secretos para verificar las credenciales dinámicas generadas por el dispositivo de autenticación.

En algunas realizaciones, la aplicación cliente puede usar la conexión Bluetooth para solicitar (320) al dispositivo de autenticación conectado que genere y devuelva una credencial dinámica. En algunas realizaciones, la aplicación cliente puede haber generado la solicitud. En algunas realizaciones, esta solicitud se puede haber generado por una parte de servidor de la aplicación y la aplicación cliente puede haber recibido la solicitud de la parte de servidor de la aplicación y puede reenviar la solicitud al dispositivo de autenticación. En algunas realizaciones, la aplicación cliente puede enviar (321) a través de la conexión Bluetooth un desafío al dispositivo de autenticación para ser usado por el dispositivo de autenticación en la generación de la credencial dinámica. En algunas realizaciones, la aplicación cliente puede haber recibido el desafío de un componente de servidor de la aplicación. En algunas realizaciones, la aplicación cliente puede haber interactuado con el usuario para permitirle al usuario definir una transacción para realizar por la aplicación y la aplicación cliente puede enviar (322) al dispositivo de autenticación a través de conexión Bluetooth los datos relacionados con esa transacción que deben ser firmados por el dispositivo de autenticación. En algunas realizaciones, la aplicación cliente puede comunicar los datos de la transacción al dispositivo de autenticación en un mensaje de aplicación que puede haber sido generado por una parte de servidor de la aplicación.

En algunas realizaciones, el dispositivo de autenticación puede capturar (325) una aprobación por parte del usuario para generar y/o devolver una credencial dinámica al ordenador huésped que ejecuta la aplicación cliente. En algunas realizaciones, el dispositivo de autenticación puede presentar (326) datos al usuario y puede capturar (327) una aprobación (o rechazo) de los datos presentados, en el que los datos presentados y aprobados pueden ser usados por el dispositivo de autenticación en la generación de una credencial dinámica.

En algunas realizaciones, el dispositivo de autenticación puede capturar (330) un valor de PIN y/o contraseña proporcionado por el usuario al dispositivo de autenticación o el dispositivo de autenticación puede recibir (331) a través de la conexión Bluetooth un valor de PIN y/o contraseña de la aplicación cliente que el usuario ha proporcionado a la aplicación cliente. En algunas realizaciones, el dispositivo de autenticación puede verificar (332) el PIN y/o la contraseña capturados o recibidos como se explica con más detalle en otra parte de esta descripción.

En algunas realizaciones, el dispositivo de autenticación puede capturar (335) una medición de una biometría del usuario que ha sido tomada por un sensor biométrico en el dispositivo de autenticación o el dispositivo de autenticación puede recibir (336) a través de la conexión Bluetooth una medición biométrica del usuario desde la aplicación cliente que ha sido tomada por el ordenador huésped. En algunas realizaciones, el dispositivo de autenticación puede verificar (337) la medición biométrica capturada o recibida como se explica con más detalle en otra parte de esta descripción.

En algunas realizaciones, la interfaz de salida de usuario del dispositivo de autenticación puede tener capacidades relativamente limitadas, de modo que el dispositivo de autenticación puede no ser capaz de dar al usuario una guía clara usando esta interfaz de salida de usuario sobre en qué estado se encuentra la aplicación de autenticación en el dispositivo de autenticación y qué puede hacer el usuario y cuál sería el efecto de las acciones del usuario. En algunas realizaciones, la aplicación cliente puede asistir (340) al usuario a interactuar con el dispositivo de autenticación, por ejemplo, proporcionando una guía sobre qué acciones (por ejemplo, presionar varios botones, esperar un tiempo de espera, etc.) puede y/o debería hacer el usuario para obtener ciertos efectos (por ejemplo, aprobación o rechazo de datos de transacciones). En algunas realizaciones, el dispositivo de autenticación (341) puede informar a la aplicación cliente del estado de la aplicación en el que se encuentra. En algunas realizaciones, la aplicación cliente puede realizar un seguimiento (342) del estado de la aplicación en el que se encuentra el dispositivo de autenticación y puede usar este conocimiento para realizar para ajustar su guía al usuario sobre cómo interactuar con el dispositivo de autenticación de modo que la guía que proporciona sea pertinente al estado real de la aplicación en el que se encuentra el dispositivo de autenticación, como se explica con más detalle en otra parte de esta descripción.

En algunas realizaciones, el dispositivo de autenticación puede usar la conexión Bluetooth para enviar (345) comandos al ordenador huésped con la que está conectado y la aplicación cliente en la ordenador huésped puede recibir y ejecutar (346) estos comandos, como se explica con más detalle en otra parte de esta descripción. En algunas realizaciones, la ejecución de estos comandos requiere que la aplicación cliente en el ordenador huésped interactúe (347) con el usuario, por ejemplo, proporcionando salida al usuario mediante, por ejemplo, la interfaz de salida de usuario de la ordenador huésped y/u obtener información del usuario mediante, por ejemplo, la interfaz de entrada de usuario del ordenador huésped.

En algunas realizaciones, el dispositivo de autenticación puede generar (350) una credencial dinámica como se explica con más detalle en otra parte de esta descripción. En algunas realizaciones, la autenticación puede generar la credencial dinámica solo si se han cumplido ciertas condiciones tales como, por ejemplo, que un PIN o una contraseña o una medición biométrica se han verificado con éxito, o que el usuario ha indicado una aprobación explícita para generar la credencial dinámica.

En algunas realizaciones, después de que se ha generado la credencial dinámica, el dispositivo de autenticación puede enviar (351) la credencial dinámica generada al ordenador huésped a través de la conexión Bluetooth.

En algunas realizaciones, la aplicación cliente puede recibir (352) la credencial dinámica generada a través de la conexión Bluetooth desde el dispositivo de autenticación conectado y puede reenviar (353) la credencial dinámica recibida a una parte de servidor de la aplicación.

En algunas realizaciones, la parte de servidor de la aplicación puede recibir (354) la credencial dinámica de la aplicación cliente y puede verificar la corrección de la credencial dinámica recibida. En algunas realizaciones, la parte de servidor de la aplicación puede verificar (360) la corrección de la credencial dinámica recibida mediante la aplicación de un algoritmo de verificación de credenciales criptográficas que puede ser parametrizado por un secreto criptográfico que está asociado con el dispositivo de autenticación. En algunas realizaciones, la parte de servidor de la aplicación puede usar en la verificación de la credencial dinámica recibida un algoritmo criptográfico simétrico que se parametriza con una clave criptográfica secreta que se comparte entre el dispositivo de autenticación y la parte de servidor de verificación de la aplicación. En algunas realizaciones, la parte de servidor de la aplicación puede usar un elemento de datos de identificación del dispositivo (tal como un número de serie) del dispositivo de autenticación para obtener un secreto que puede usar en la verificación de la credencial dinámica. Por ejemplo, en algunas realizaciones, la parte de servidor de la aplicación puede almacenar en una base de datos para cada dispositivo de autenticación individual uno o más secretos relacionados con ese dispositivo de autenticación y puede recuperar estos secretos de la base de datos usando el elemento de datos de identificación del dispositivo, por ejemplo, en una consulta de base de datos. En algunas realizaciones, la parte de servidor de la aplicación puede determinar el valor de un secreto para usar en la verificación de una credencial dinámica mediante la derivación de ese valor de un secreto maestro y el elemento de datos de identificación del dispositivo del dispositivo de autenticación que supuestamente ha generado la credencial dinámica.

En algunas realizaciones, la parte de servidor de la aplicación puede usar (370) el resultado de la verificación de la credencial dinámica recibida para decidir si realizar o no una determinada acción (tal como iniciar sesión en el usuario o concederle acceso a recursos de aplicación tales como cierta información, o la realización de una transacción solicitada por el usuario mediante la cual los datos relacionados con esta transacción se pueden haber firmado por la credencial dinámica). Por ejemplo, en algunas realizaciones, la parte de servidor de la aplicación puede decidir realizar la acción si la verificación de la credencial dinámica fue exitosa. En algunas realizaciones, la parte de servidor de la aplicación puede decidir no realizar la acción si la verificación de la credencial dinámica no tuvo éxito. En algunas realizaciones, la parte de servidor también puede tener en cuenta otros elementos para decidir si realizar o no la acción, tal como por ejemplo el resultado de la verificación de un PIN o contraseña estático que la aplicación cliente puede haber recibido del usuario y que la parte de servidor de la aplicación puede haber recibido de la aplicación cliente

Se han descrito varias implementaciones. No obstante, se entenderá que se pueden realizar varias modificaciones. Por ejemplo, los elementos de una o más implementaciones se pueden combinar, eliminar, modificar o complementar para formar implementaciones adicionales. Por consiguiente, otras implementaciones están dentro del alcance de las reivindicaciones adjuntas. Además, aunque una característica particular de la presente invención se puede haber descrito con respecto a solo una de varias implementaciones, dicha característica se puede combinar con una o más características de las otras implementaciones según se desee y sea ventajoso para cualquier aplicación dada o particular. Si bien se han descrito anteriormente varias realizaciones de la presente invención, se debe entender que se han presentado solo a modo de ejemplo y no de limitación. En particular, obviamente, no es posible describir cada combinación concebible de componentes o metodologías con el propósito de describir el tema reivindicado, pero un experto en la técnica puede reconocer que muchas combinaciones y permutaciones adicionales de la presente invención son posibles. En particular con respecto a los procedimientos que se han descrito, se pueden omitir algunas etapas de los procedimientos presentados, se pueden añadir otras etapas y el orden en el que se realizan las diversas etapas puede ser diferentes al orden en el que se descrito estas etapas. Por tanto, la amplitud y el alcance de la presente invención no deberían estar limitados por ninguno de los ejemplos de realizaciones descritos anteriormente, sino que se deberían definir únicamente de acuerdo con las siguientes reivindicaciones.

REIVINDICACIONES

1. Un dispositivo de autenticación de mano portátil (100) para generación de una credencial dinámica que comprende:

un componente de almacenamiento (130) adaptado para almacenar de forma segura una clave secreta de generación de credenciales criptográficas;

una interfaz de entrada de usuario (120) para recepción de entradas de un usuario del dispositivo de autenticación;

una interfaz de salida de usuario (110) para presentación de salidas al usuario;

un componente de procesamiento de datos (140) adaptado para generar dicha credencial dinámica mediante la combinación criptográfica de dicha clave secreta de generación de credenciales criptográficas con una variable dinámica; y

una interfaz Bluetooth (150) para conexión del dispositivo de autenticación a un ordenador huésped con una conexión Bluetooth entre el dispositivo de autenticación y dicho ordenador huésped;

en el que dicho dispositivo de autenticación está adaptado para enviar dicha credencial dinámica generada a través de la conexión Bluetooth con dicho ordenador huésped;

caracterizado por que:

en uso, dicho dispositivo de autenticación mantiene un estado de aplicación que cambia con el tiempo, a través del cual diferentes estados de aplicación requieren diferentes acciones de dicho usuario; y dicho dispositivo de autenticación también se adapta para volver disponible un estado de aplicación presente a dicho ordenador huésped a través de dicha conexión Bluetooth, a través del cual dicho ordenador huésped tiene la función de proporcionar al menos una de las pautas o instrucciones a dicho usuario sobre la forma en que tratar con dicho dispositivo de autenticación a través del cual al menos una de dichas pautas o instrucciones son una función de dicha información de estado de aplicación presente.

2. El dispositivo de autenticación de la reivindicación 1 además adaptado para recibir a través de dicha conexión Bluetooth una solicitud para dicha credencial dinámica, para generar dicha credencial dinámica con dicho componente de procesamiento de datos en respuesta a dicha solicitud y retornar dicha credencial dinámica generada a través de dicha conexión Bluetooth.

3. El dispositivo de autenticación de la reivindicación 2 además adaptado para capturar por dicha interfaz de entrada de usuario al menos una de una aprobación de dicho usuario para generar dicha credencial dinámica antes de generar dicha credencial dinámica o una aprobación de dicho usuario para retornar dicha credencial dinámica antes de retornar dicha credencial dinámica.

4. El dispositivo de autenticación de la reivindicación 2 además adaptado para recibir a través de dicha de conexión Bluetooth datos relacionados con transacciones, para presentar dichos datos relacionados con transacciones recibidos al usuario por dicha interfaz de salida de usuario, para capturar mediante dicha interfaz de entrada de usuario una aprobación de dicho usuario de dichos datos relacionados con transacciones, y usar dichos datos relacionados con transacciones recibidos para generar dicha credencial dinámica por dicho componente de procesamiento de datos.

5. El dispositivo de autenticación de cualquiera de las reivindicaciones 1 a 4 además adaptado para almacenar un nombre de usuario en dicho componente de almacenamiento y volver dicho nombre de usuario disponible para dicho ordenador huésped a través de dicha conexión Bluetooth.

6. El dispositivo de autenticación de la reivindicación 5 además adaptado para recibir dicho nombre de usuario a través de dicha conexión Bluetooth y para almacenar dicho nombre de usuario en dicho componente de almacenamiento para posterior recuperación a través de dicha conexión Bluetooth.

7. El dispositivo de autenticación de cualquiera de las reivindicaciones 1 a 6 en el que dicha interfaz Bluetooth soporta Bluetooth de baja energía.

8. Un sistema de aseguramiento de una interacción entre una aplicación y un usuario, incluyendo dicha aplicación una parte de servidor y parte de cliente, comprendiendo el sistema:

un servidor de aplicación (210) que aloja dicha parte de servidor de la aplicación;

un ordenador huésped (230) que ejecuta una aplicación cliente que es dicha parte de cliente de dicha aplicación y que permite al usuario (290) acceder remotamente a la parte de servidor de la aplicación a través de una red de ordenador (250), comprendiendo dicho ordenador huésped una interfaz de entrada de usuario para recibir entradas de usuario y una interfaz de salida de usuario para proporcionar salidas al usuario;

un dispositivo de autenticación (240) para generación de una credencial dinámica, comprendiendo el dispositivo de

autenticación

un componente de almacenamiento (130) adaptado para almacenar de manera segura una clave secreta de generación de credenciales criptográficas,

un componente de procesamiento de datos (140) adaptado para generar dicha credencial dinámica mediante la combinación criptográfica de dicha clave secreta de generación de credenciales criptográficas con una variable dinámica, y

una interfaz Bluetooth (150) para conexión del dispositivo de autenticación a dicho ordenador huésped con una conexión Bluetooth entre el dispositivo de autenticación y dicho ordenador huésped; y

un servidor de verificación (220) para verificación de la validez de dicha credencial dinámica; a través del cual

dicho ordenador huésped está adaptado para configurar la conexión Bluetooth con dicho dispositivo de autenticación;

dicho dispositivo de autenticación está adaptado para retornar dicha credencial dinámica por medio de la conexión Bluetooth a dicho ordenador huésped;

dicha aplicación cliente en el ordenador huésped está además adaptada para recibir dicha credencial dinámica por medio de dicha conexión Bluetooth y reenviar dicha credencial dinámica generada a dicho servidor de verificación para verificación;

dicho servidor de verificación está adaptado para verificar la credencial dinámica generada y señalizar a dicho servidor de aplicación si la credencial dinámica se ha verificado como válida;

caracterizado por que:

dicho dispositivo de autenticación está además adaptado para mantener un estado de aplicación que cambia con el tiempo, a través del cual diferentes estados de aplicación requieren diferentes acciones de dicho usuario, y para comunicar a través de dicha conexión Bluetooth información sobre un estado de aplicación presente de dicho dispositivo de autenticación a dicho ordenador huésped; y

dicha aplicación cliente además está adaptada para recibir a través de dicha conexión Bluetooth dicha información de estado de aplicación presente de dicho dispositivo de autenticación y proporcionar al menos una de las pautas o instrucciones a dicho usuario sobre la forma en que tratar con dicho dispositivo de autenticación a través del cual la al menos una de dichas pautas o instrucciones son una función de dicha información de estado de aplicación presente recibida.

9. El sistema de la reivindicación 8 en el que

dicho dispositivo de autenticación y dicho servidor de verificación comparten dicha clave secreta de generación de credenciales criptográficas;

dicha generación y dicha verificación de dicha credencial dinámica se realizan con un algoritmo criptográfico simétrico usando una clave de autenticación secreta compartida entre dicho dispositivo de autenticación y dicho servidor de verificación.

10. El sistema de la reivindicación 8 o 9 en el que

dicho dispositivo de autenticación comparte una o más claves de mensajería seguras con al menos uno de dicho servidor de verificación o dicho servidor de aplicación;

al menos uno de dicho servidor de aplicación o dicho servidor de verificación está adaptado para generar un mensaje de aplicación y asegurar dicho mensaje de aplicación con técnicas de mensajería seguras usando dichas una o más claves de mensajería seguras compartidas;

dicha aplicación cliente está adaptada para recibir dicho mensaje de aplicación seguro y para reenviar dicho mensaje de aplicación seguro a dicho dispositivo de autenticación a través de dicha conexión Bluetooth; y

dicho dispositivo de autenticación está adaptado para recibir a través de dicha conexión Bluetooth dicho mensaje de aplicación seguro y soportar dichas claves de mensajería seguras usando dichas una o más técnicas de mensajería seguras compartidas y actuar sobre dicho mensaje de aplicación seguro.

11. El sistema de cualquiera de las reivindicaciones 8 a 10 en el que dicho dispositivo de autenticación está adaptado:

para recibir a través de dicha conexión Bluetooth un mensaje de aplicación que contiene una solicitud para el dispositivo de autenticación para generar y retornar dicha credencial dinámica; y

para, en respuesta a la recepción de dicho mensaje de aplicación, generar dicha credencial dinámica y retornar dicha

credencial dinámica a través de dicha conexión Bluetooth; y

en el que dicho mensaje de aplicación contiene datos de transacción enviados por dicho usuario a dicha aplicación y en el que dicha variable dinámica se basa en dichos datos de transacción.

12. El sistema de cualquiera de las reivindicaciones 8 a 11 en el que

dicha aplicación cliente también está adaptada para obtener mediante dicha interfaz de entrada de usuario de dicho ordenador huésped al menos uno de un valor de PIN o un valor de contraseña de dicho usuario y enviar el al menos uno de dicho valor de PIN obtenido o dicho valor de contraseña obtenidos a través de dicha conexión Bluetooth a dicho dispositivo de autenticación; y

dicho dispositivo de autenticación también está adaptado para recibir a través de dicha conexión Bluetooth el al menos uno de dicho valor de PIN o dicho valor de contraseña y verificar el al menos uno de dicho valor de PIN recibido o dicho valor de contraseña recibido;

o en el que

dicho ordenador huésped además comprende un componente de medición biométrica adaptado para capturar una medición biométrica de dicho usuario;

dicha aplicación cliente también está adaptada para obtener mediante dicho componente de medición biométrica de dicho ordenador huésped una medición biométrica de dicho usuario y enviar dicha medición biométrica obtenida a través de dicha conexión Bluetooth a dicho dispositivo de autenticación; y

dicho dispositivo de autenticación también está adaptado para recibir a través de dicha conexión Bluetooth dicha medición biométrica y verificar dicha medición biométrica recibida.

13. El sistema de cualquiera de las reivindicaciones 8 a 12 en el que

dicho dispositivo de autenticación también está adaptado para generar comandos para ser ejecutados por dicho ordenador huésped y comunicar dichos comandos a dicho ordenador huésped a través de dicha conexión Bluetooth; y

dicha aplicación cliente también está adaptada para recibir dichos comandos a través de dicha conexión Bluetooth de dicho dispositivo de autenticación y ejecutar dichos comandos.

14. El sistema de la reivindicación 13 en el que la realización de dichos comandos por parte dicho ordenador huésped comprende que dicho ordenador huésped que interactúe con dicho usuario usando al menos una de dicha interfaz de salida de usuario o dicha interfaz de entrada de usuario.

15. Un procedimiento para aseguramiento de la interacción de una aplicación basada en ordenador con un usuario, en el que la aplicación basada en ordenador incluye una parte de cliente, a través de la que el usuario opera un dispositivo de autenticación para generar una credencial dinámica, comprendiendo el dispositivo de autenticación una interfaz Bluetooth para comunicarse con un dispositivo huésped Bluetooth,

comprendiendo el procedimiento las etapas de:

ejecutar en un ordenador huésped local una aplicación cliente que es dicha parte de cliente de la aplicación basada en ordenador para permitir al usuario interactuar con la aplicación basada en ordenador mediante el uso de una interfaz de entrada de usuario y una interfaz de salida de usuario del ordenador huésped local;

configurar en el ordenador huésped local una conexión Bluetooth con el dispositivo de autenticación;

recibir a través de dicha conexión Bluetooth del dispositivo de autenticación la credencial dinámica, la credencial dinámica generada por dicho dispositivo de autenticación mediante la combinación criptográfica de una variable dinámica con una primera clave de autenticación criptográfica almacenada en dicho dispositivo de autenticación

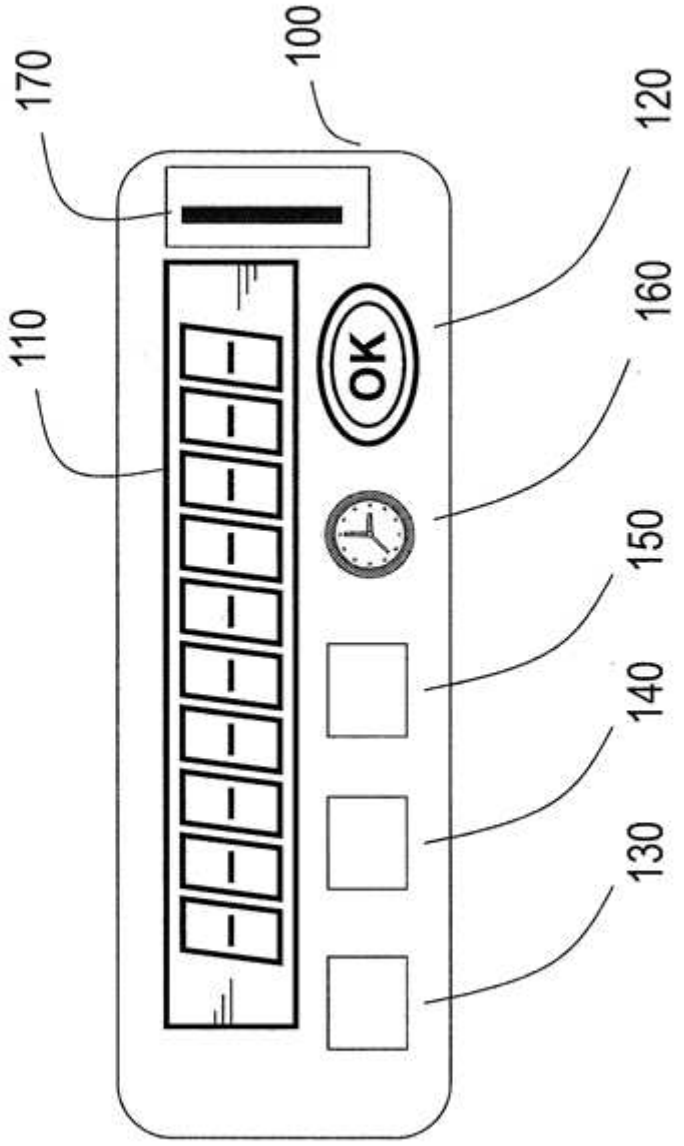
caracterizado por que el procedimiento además comprende las etapas de:

recibir en dicho ordenador huésped local a través de dicha conexión Bluetooth de dicho dispositivo de autenticación información sobre el estado de aplicación del dispositivo de autenticación, en el que dicho dispositivo de autenticación mantiene un estado de aplicación que cambia con el tiempo, a través del cual diferentes estados de aplicación requieren diferentes acciones de dicho usuario; y

proporcionar en el ordenador huésped local mediante dicha interfaz de salida de usuario al menos una de las pautas o instrucciones referentes a la operación de dicho dispositivo de autenticación al usuario, a través de la que al menos una de dichas pautas o dichas instrucciones son una función de dicha información recibida en el estado de aplicación del dispositivo de autenticación.

16. El procedimiento de la reivindicación 15 que además comprende las etapas de obtener en el ordenador huésped local un valor indicador de la distancia que es indicativo de la distancia real entre el ordenador huésped local y el dispositivo de autenticación y usar dicho valor indicador de la distancia para determinar si conceder, mantener o revocar uno o más derechos de acceso al usuario.

FIGURA 1



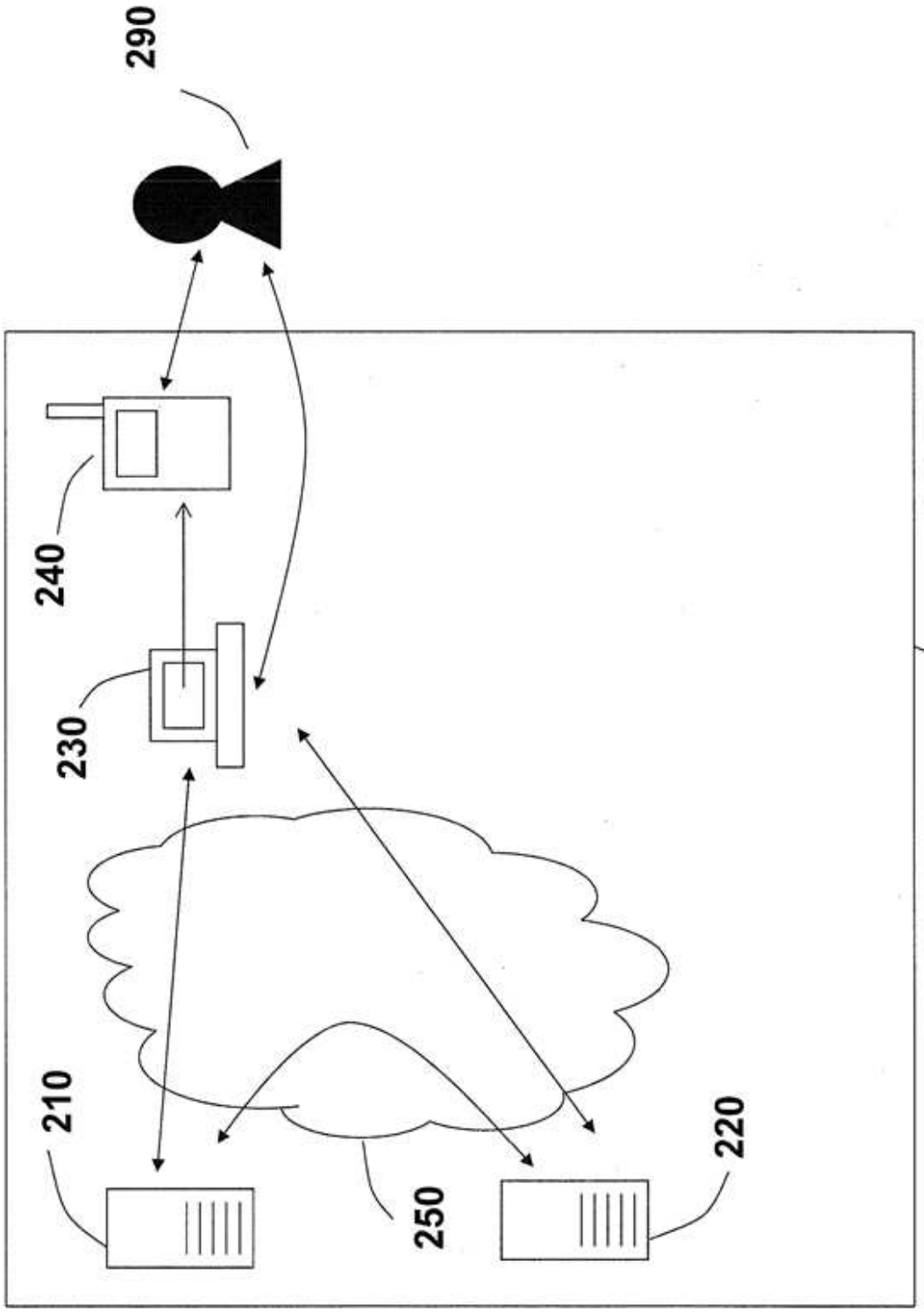
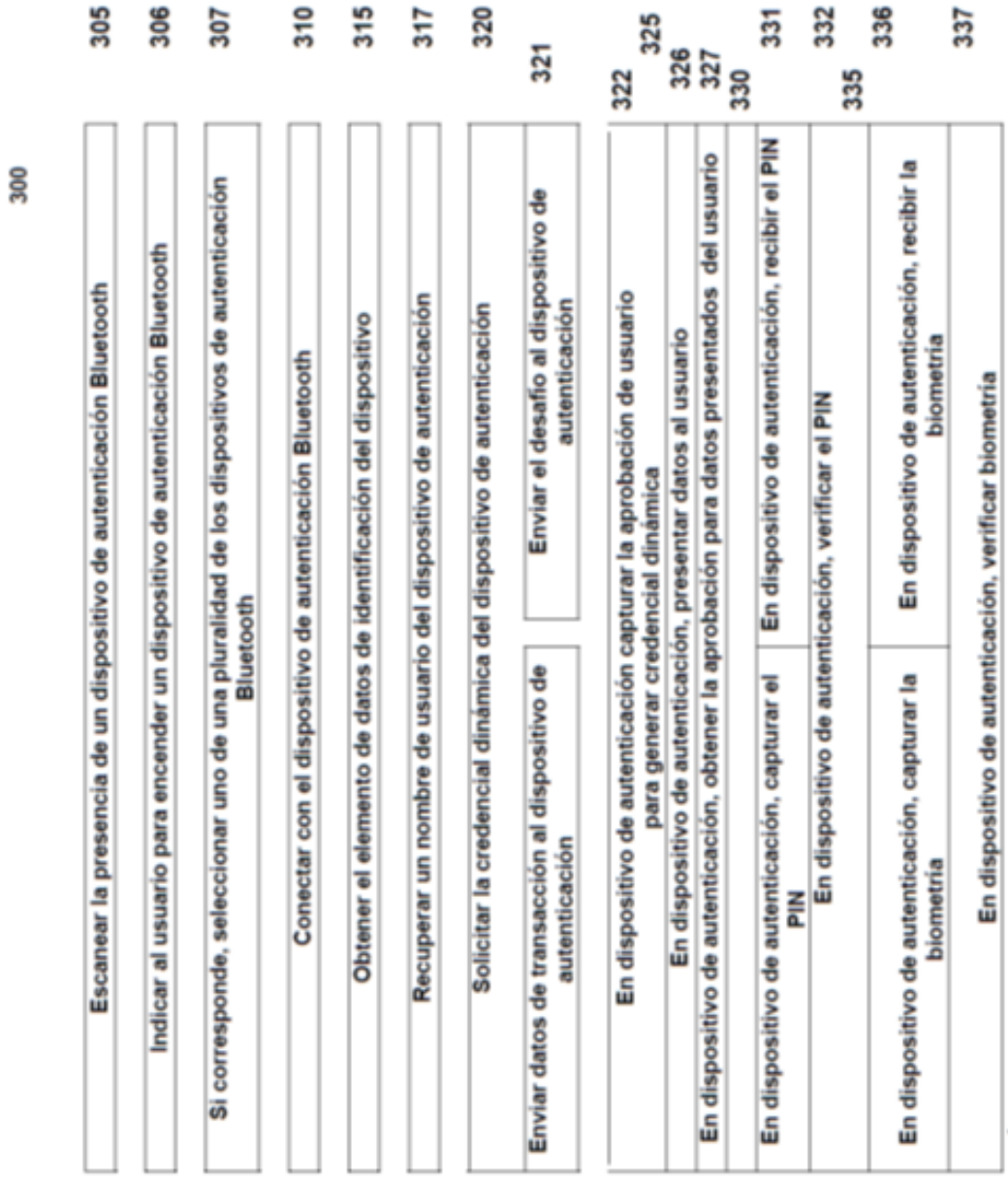


Figura 2



Continúa en la Fig. 3B

FIG. 3A

FIG. 3B

Continúa de la Fig. 3A