

19



OFICINA ESPAÑOLA DE
PATENTES Y MARCAS

ESPAÑA



11 Número de publicación: **2 883 627**

51 Int. Cl.:

H04L 9/32 (2006.01)

H04L 29/06 (2006.01)

H04W 12/06 (2011.01)

G06F 21/32 (2013.01)

12

TRADUCCIÓN DE PATENTE EUROPEA

T3

86 Fecha de presentación y número de la solicitud internacional: **11.08.2017** **PCT/EP2017/070414**

87 Fecha y número de publicación internacional: **14.02.2019** **WO19029818**

96 Fecha de presentación y número de la solicitud europea: **11.08.2017** **E 17754139 (8)**

97 Fecha y número de publicación de la concesión europea: **21.07.2021** **EP 3665860**

54 Título: **Autenticación multifactor**

45 Fecha de publicación y mención en BOPI de la
traducción de la patente:
09.12.2021

73 Titular/es:

KOBIL GMBH (100.0%)
Pfortenring 11
67547 Worms, DE

72 Inventor/es:

KOYUN, ISMET y
WERNERT, FRANK

74 Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

ES 2 883 627 T3

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

DESCRIPCIÓN

Autenticación multifactor

5 **Campo**

La siguiente divulgación se refiere al campo de la autenticación y, en particular, a la autenticación de un usuario que solicita un servicio o, más particularmente, se refiere a sistemas, aparatos y métodos para la autenticación de un usuario.

10

Antecedentes

Hoy en día, existen diferentes enfoques para autenticar a un usuario que solicita un servicio. Como un ejemplo, el protocolo de SAML (SAML: Lenguaje de Marcas de Asertos de Seguridad) autentica a un usuario que solicita un servicio de un proveedor de servicios. De acuerdo con el protocolo de SAML, se ofrece la posibilidad de intercambiar información asociada a la seguridad entre dos entidades para proporcionar autenticación para la entidad que busca la autenticación.

15

De acuerdo con el protocolo de SAML, el servicio puede solicitarse, por ejemplo, por un terminal. Tras recibir la petición de servicio, un servidor del proveedor de servicios envía o desencadena el envío de una petición de autenticación a un servidor de autenticación, que autentica al usuario, por ejemplo, mediante credenciales de autenticación del usuario como un PIN a introducir por el usuario. En el caso en el que la autenticación fuera satisfactoria, el servidor de autenticación devuelve o desencadena una respuesta al servidor del proveedor de servicios. Por lo tanto, el usuario se autentica y el servicio solicitado puede proporcionarse al usuario.

20

25

Sin embargo, la protección de la identidad del usuario comprobada mediante el proceso de autenticación cada vez se está volviendo más importante. Por ejemplo, las credenciales de autenticación, que pueden usarse para identificar al usuario, pueden copiarse por una tercera persona no autorizada. La tercera persona no autorizada puede burlar al servidor de autenticación para que crea que la tercera persona no autorizada es el usuario apropiado. Para evitar un uso fraudulento, es deseable una protección adicional de la identidad. Tal protección adicional se divulga, por ejemplo, en los documentos US8635662 y US2015/242605.

30

Sumario

El inconveniente de los enfoques de la técnica anterior para autenticar a un usuario que solicita un servicio es que ya que la identidad de usuario se comprueba basándose en información estática del usuario, la identidad del usuario es bastante vulnerable y susceptible de uso fraudulento.

35

Por lo tanto, un objetivo de la presente invención es, entre otros, proporcionar una solución en la que puede proporcionarse una autenticación con seguridad mejorada.

40

De acuerdo con un primer aspecto ilustrativo de la presente invención, un método se divulga, comprendiendo el método:
las etapas de la reivindicación 1.

45

Este método puede, por ejemplo, realizarse y/o controlarse por un aparato, que se denominará, a continuación, como primer aparato. Este primer aparato puede ser, por ejemplo, un servidor. Como alternativa, este método puede realizarse y/o controlarse por más de un aparato, por ejemplo, un sistema que comprende varios aparatos, por ejemplo, una nube de servidores que comprende al menos dos servidores. Como alternativa, el primer aparato puede ser, por ejemplo, un aparato que es o comprende el dispositivo electrónico del usuario (por ejemplo, un terminal móvil). Por ejemplo, el método puede realizarse y/o controlarse usando al menos un procesador del primer aparato.

50

De acuerdo con un aspecto ilustrativo adicional de la invención, se divulga un programa informático, provocando el programa informático, cuando se ejecuta por un procesador, que un aparato, por ejemplo, un servidor o un dispositivo electrónico, realice y/o controle las acciones del método de acuerdo con el primer aspecto ilustrativo.

55

El programa informático puede almacenarse en un medio de almacenamiento legible por ordenador, en particular un medio tangible y/o no transitorio. El medio de almacenamiento legible por ordenador podría ser, por ejemplo, un disco o una memoria o similar. El programa informático podría almacenarse en el medio de almacenamiento legible por ordenador en forma de instrucciones que codifican el medio de almacenamiento legible por ordenador. El medio de almacenamiento legible por ordenador puede concebirse para tomar parte en la operación de un dispositivo, como una memoria interna o externa, por ejemplo, una Memoria de Sólo Lectura (ROM) o disco duro de un ordenador, o concebirse para la distribución del programa, como un disco óptico.

60

De acuerdo con un aspecto ilustrativo adicional de la invención, se divulga un aparato (y también se denomina como primer aparato a continuación), configurado para realizar y/o controlar o que comprende respectivos medios para

65

realizar y/o controlar el método de acuerdo con el primer aspecto ilustrativo. El aparato puede ser, por ejemplo, un servidor, o un dispositivo electrónico.

Los medios del aparato pueden implementarse en hardware y/o software. Pueden comprender, por ejemplo, al menos un procesador para ejecutar código de programa informático para realizar las funciones requeridas, al menos una memoria que almacena el código de programa, o ambos. Como alternativa, podrían comprender, por ejemplo, circuitería que se diseña para implementar las funciones requeridas, por ejemplo, implementadas en un conjunto de chips o un chip, como un circuito integrado. En general, los medios pueden comprender, por ejemplo, uno o más medios de procesamiento o procesadores.

De acuerdo con un aspecto ilustrativo adicional de la invención, se divulga un aparato (y también se denomina como primer aparato a continuación), que comprende al menos un procesador y al menos una memoria que incluye código de programa informático, la al menos una memoria y el código de programa informático configurados para, con el al menos un procesador, provocar que un aparato, por ejemplo, el aparato, al menos realice y/o controle el método de acuerdo con el primer aspecto ilustrativo.

El aparato anteriormente divulgado de acuerdo con cualquier aspecto de la invención puede ser un módulo o un componente para un dispositivo, por ejemplo, un chip. Como alternativa, el aparato divulgado de acuerdo con cualquier aspecto de la invención puede ser un dispositivo, por ejemplo, un servidor o nube de servidores, o un dispositivo electrónico. El aparato divulgado de acuerdo con cualquier aspecto de la invención puede comprender únicamente los componentes divulgados, por ejemplo, medios, procesador, memoria, o puede comprender adicionalmente uno o más componentes adicionales.

De acuerdo con un aspecto ilustrativo adicional de la invención, se divulga un sistema, que comprende: un aparato y al menos un (o más de un) aparato adicional, en donde el primer aparato está configurado para, con el al menos un (o más de un) aparato adicional, realizar y/o controlar un método de acuerdo con el primer aspecto de la presente invención.

A continuación, se describirán en detalle adicional características ilustrativas y realizaciones ilustrativas de todos los aspectos de la presente invención.

La una o más piezas de primera información de autenticación pueden derivarse, por ejemplo, del primer aparato (por ejemplo, un dispositivo electrónico como un terminal, teléfono inteligente, tableta, por nombrar solo algunos ejemplos no limitantes). Pueden recopilarse, por ejemplo, por el aparato, por ejemplo, mediante uno o más sensores del aparato. Como alternativa o adicionalmente, la una o más piezas de primera información de autenticación pueden recibirse, por ejemplo, por el aparato (por ejemplo, un servidor) desde otra entidad (por ejemplo, un dispositivo electrónico del usuario).

La una o más piezas de primera información de autenticación representan una información única asociada a un usuario y/o un dispositivo electrónico del usuario. Por ejemplo, la una o más piezas de primera información de autenticación (juntas) pueden ser indicativas de una clase de huella de cómo un usuario maneja el dispositivo electrónico.

Basándose, al menos en parte, en la una o más piezas (obtenidas) de primera información de autenticación, se determina el nivel de confianza (por ejemplo, de acuerdo con un algoritmo predefinido o conjunto de reglas). El nivel de confianza es indicativo de un nivel de confianza en la una o más piezas de primera información de autenticación. El nivel de confianza puede representar, por ejemplo, un valor. Por ejemplo, el nivel de confianza puede representar un valor entre un intervalo de valores predefinido, en donde el límite inferior del intervalo puede ser indicativo de una desconfianza total en la una o más piezas de primera información de autenticación. Adicionalmente, el límite superior del intervalo puede ser indicativo, por ejemplo, de un nivel máximo de confianza en la una o más piezas de primera información de autenticación. Un nivel de confianza (determinado) puede estar, por ejemplo, en cualquier sitio entre el intervalo predefinido. El nivel de confianza puede representar, por ejemplo, un valor abstracto de 0 a 100. Por ejemplo, en el caso anteriormente mencionado, un nivel de confianza de 100 indica una identificación perfecta de un usuario y, por lo tanto, una confianza total. En contraste, un nivel de confianza de 0 indica una desconfianza total. De acuerdo con el nivel de confianza determinado, por ejemplo, una aplicación realizada y/o controlada por un dispositivo electrónico, y/o un servidor, puede decidir, por ejemplo, si se efectúan o no tareas (por ejemplo, transacciones, en particular transacciones de dinero). Como alternativa o adicionalmente, de acuerdo con el nivel de confianza determinado, por ejemplo, una aplicación realizada y/o controlada por un dispositivo electrónico, y/o un servidor puede decidir, por ejemplo, qué cantidad de dinero está disponible para que se efectúe una transacción. Ejemplos de uno o más escenarios de nivel de confianza pueden ser uno o más de los siguientes: (i) nivel de confianza 0 a 30: no se permiten transacciones; (ii) nivel de confianza 31 a 60: únicamente se permiten transacciones no financieras (por ejemplo, conseguir un extracto bancario o similar); (iii) nivel de confianza 61 a 90: se permiten transacciones no financieras y transacciones financieras hasta una cantidad predefinida de dinero (por ejemplo, 1000 euros o dólares); (iv) nivel de confianza 91-100: se permiten transacciones ilimitadas; (v) o una combinación de los mismos.

Una aplicación realizada por el dispositivo electrónico del usuario puede obtener, por ejemplo, (por ejemplo, medir y/o determinar) la una o más piezas de primera información de autenticación. La una o más piezas obtenidas de primera

información de autenticación pueden proporcionarse, por ejemplo, a un servidor y, por lo tanto, obtenerse (por ejemplo, recibirse) por el servidor. El servidor puede, por ejemplo, determinar el nivel de confianza basándose, al menos en parte, en la una o más piezas de primera información de autenticación. Como alternativa, la aplicación realizada por el dispositivo electrónico puede obtener, por ejemplo, la una o más piezas de primera información de autenticación y determinar el nivel de confianza. El nivel de confianza determinado puede proporcionarse, por ejemplo, a un servidor. El servidor puede comprobar, por ejemplo, el nivel de confianza proporcionado. El método de acuerdo con el primer aspecto de la presente invención puede ser parte, por ejemplo, de una aplicación realizada por el dispositivo electrónico. Como alternativa, el método de acuerdo con el primer aspecto de la presente invención puede ser, por ejemplo, una aplicación construida expresamente para realizarse por el dispositivo electrónico. Como alternativa, el método de acuerdo con el primer aspecto de la presente invención puede ser, por ejemplo, parte de un paquete de desarrollo de software (SDK), por ejemplo, a usar con un dispositivo electrónico.

El nivel de confianza puede determinarse, por ejemplo, evaluando la una o más piezas de primera información de autenticación. Puede determinarse, por ejemplo, un respectivo nivel de confianza para cada de la una o más piezas de primera información de autenticación. En el caso en el que se determina más de un nivel de confianza, puede determinarse, por ejemplo, un nivel de confianza resumido, por ejemplo, se calcula un promedio aritmético o promedio medio basándose, al menos en parte, en los más de un nivel de confianza. El nivel de confianza resumido, por ejemplo, puede determinarse, por ejemplo, mediante una ponderación de las más de unas piezas de niveles de confianza. Por ejemplo, un nivel de confianza determinado puede no ser ni "verdadero" ni "falso". Un nivel de confianza determinado puede ser, por ejemplo, un valor entre un intervalo predefinido, por ejemplo, entre 0 y 100. De esta manera, la una o más piezas de primera información de autenticación pueden evaluarse, por ejemplo, determinando el nivel de confianza. El nivel de confianza puede determinarse, por ejemplo, basándose, al menos en parte, en una comparación de la una o más piezas (obtenidas) de primera información de autenticación con una o más piezas de información comparables. Por ejemplo, una o más piezas de información puede proporcionarse durante un proceso inicial para obtener una o más piezas de información de referencia. El proceso inicial puede representar, por ejemplo, un proceso de aprendizaje para obtener una o más piezas de información de referencia, que puede usarse para determinar el nivel de confianza. Adicionalmente o como alternativa, la una o más piezas de información de referencia pueden ser, por ejemplo, la una o más piezas de primera información de autenticación, que se proporcionaron en un momento anterior.

El primer aparato puede ser, por ejemplo, un dispositivo electrónico, en particular el dispositivo electrónico del usuario.

El dispositivo electrónico del usuario puede ser, por ejemplo, portátil (por ejemplo, con un peso menor de 5, 4, 3, 2 o 1 kg). El dispositivo electrónico puede instalarse, por ejemplo, al menos temporalmente (por ejemplo, de forma extraíble) o permanentemente en un vehículo. El dispositivo electrónico puede comprender, por ejemplo, o ser conectable a un visualizador para visualizar una interacción, por ejemplo, para la interacción con un usuario. El dispositivo electrónico puede comprender, por ejemplo, o ser conectable a medios para emitir sonido, por ejemplo, en forma de comandos o información hablados. El dispositivo electrónico puede comprender, por ejemplo, uno o más sensores. El uno o más sensores pueden ser, por ejemplo, para determinar la posición de dispositivos, tal como, por ejemplo, un receptor de Sistema Global de Navegación por Satélite (GNSS), por ejemplo, en forma de un receptor de Sistema de Posicionamiento Global (GPS). Como alternativa o adicionalmente, el uno o más sensores pueden ser, por ejemplo, para la determinación de gestos, deslizamiento, escritura, toque, retención, giro, transporte o una combinación de los mismos por nombrar solo algunos ejemplos no limitantes. Por ejemplo, el correspondiente uno o más sensores pueden ser acelerómetros, giroscopios, sensores táctiles, sensores de tiempo o una combinación de los mismos por nombrar solo algunos ejemplos no limitantes. Como alternativa o adicionalmente, el uno o más sensores pueden ser, por ejemplo, sensores de cámara para recopilar información de imagen. Por ejemplo, basándose en información (recopilada) de un sensor de imagen, puede obtenerse información fija o de vídeo. El dispositivo electrónico puede ser, por ejemplo, adecuado para o estar configurado para realizar y/o controlar una aplicación, por ejemplo, para proporcionar proceso de autenticación de un usuario.

El nivel de confianza determinado, por ejemplo, puede emitirse, por ejemplo, a un servidor, o - en el caso en el que el nivel de confianza se determina por un servidor - a un dispositivo electrónico (por ejemplo, el dispositivo electrónico del usuario) o a otro aparato que transfiere el nivel de confianza determinado al dispositivo electrónico. El nivel de confianza puede usarse, por ejemplo, en un proceso de autenticación, por ejemplo, una aplicación realizada y/o controlada por una aplicación, por ejemplo, realizada y/o controlada por un dispositivo electrónico (por ejemplo, el dispositivo electrónico del usuario).

Debería observarse que la etapa de obtención de la una o más piezas de primera información de autenticación y la etapa de determinación del nivel de confianza puede tener lugar al menos parcialmente en paralelo en el caso en el que al menos una de la una o más de más piezas de primera información de autenticación se obtiene antes de obtener las otras piezas de primera información de autenticación. Por lo tanto, un nivel de confianza puede determinarse, por ejemplo, para la al menos una de la una o más piezas de primera información de autenticación y adicionalmente una o más piezas de primera información de autenticación pueden obtenerse en paralelo. Como alternativa, la etapa de obtención de la una o más piezas de primera información de autenticación y la etapa de determinación del nivel de confianza pueden tener lugar secuencialmente.

Realizaciones de ejemplo de la presente invención, por lo tanto, hacen posible determinar un nivel de confianza que representa un nivel de confianza en información (la una o más piezas de primera información de autenticación) usada, por ejemplo, en un proceso de autenticación. Por lo tanto, esta información adicional (el nivel de confianza determinado) mejora la seguridad de autenticación del usuario y reduce el potencial de una autenticación fraudulenta.

De acuerdo con una realización ilustrativa de todos los aspectos de la presente invención, el nivel de confianza puede adoptar más de dos valores. Por ejemplo, el nivel de confianza puede representar un valor, o un estado. El valor puede ser, por ejemplo, un valor de un intervalo de valores predefinido que comprende al menos tres valores diferentes, por ejemplo, 0, 1, 2, o de 0 a 100, por nombrar solo algunos ejemplos no limitantes. El estado puede ser, por ejemplo, un estado indicativo de al menos tres estados diferentes, por ejemplo, -1, 0, 1 por nombrar solo un ejemplo no limitante. Como alternativa, el nivel de confianza puede adoptar, por ejemplo, dos valores, por ejemplo, un valor binario (por ejemplo, 0 y 1, o -1 y 1, por nombrar solo algunos ejemplos no limitantes).

De acuerdo con una realización ilustrativa de todos los aspectos de la presente invención, el método comprende adicionalmente:

- comprobar el nivel de confianza, en donde el nivel de confianza se comprueba basándose, al menos en parte, en una comparación del nivel de confianza (determinado) con un umbral de comprobación (por ejemplo, predefinido).

El nivel de confianza puede comprobarse, por ejemplo, para determinar una información de autenticación. La información de autenticación puede ser indicativa, por ejemplo, de, al menos en parte, si la una o más piezas de primera información de autenticación, en función de la cuales se determina, al menos parcialmente, el nivel de confianza, son enteras o no. Adicionalmente o como alternativa, la información de autenticación puede ser indicativa, por ejemplo, de, al menos en parte, si una autenticación del usuario basándose en la una o más piezas de primera información de autenticación se considera satisfactoria o no. Adicionalmente o como alternativa, la información de autenticación puede comprender, por ejemplo, el nivel de confianza determinado.

En el caso en el que se determina una información de autenticación basándose, al menos en parte, en el nivel de confianza comprobado, la información de autenticación puede ser indicativa, por ejemplo, de, al menos en parte, una autenticación positiva en el caso en el que el nivel de confianza está por encima de (o es igual a) el umbral de comprobación (por ejemplo, predefinido), y/o la información de autenticación puede ser indicativa, por ejemplo, de, al menos en parte, una autenticación negativa en el caso en el que el nivel de confianza está por debajo de (o es igual a) el umbral de comprobación.

El umbral de comprobación puede predeterminarse, por ejemplo, o puede determinarse de acuerdo con una regla predefinida. El umbral de comprobación puede establecerse para depender de un tipo de servicio (por ejemplo, una transacción) en el que tiene que autenticarse el usuario. Servicios, que requieren un mayor nivel de seguridad, pueden ser, por ejemplo, transacciones de dinero, o transacciones de dinero que consideran la cantidad de dinero a transferir. En comparación, servicios, que requieren un nivel inferior de seguridad, pueden ser, por ejemplo, comprobar el saldo de la cuenta, o iniciar sesión en una cuenta bancaria por nombrar solo algunos ejemplos no limitantes.

En una realización ilustrativa de todos los aspectos de la presente invención, el nivel de confianza es una función dependiente del tiempo, en donde el nivel de confianza disminuye con el transcurso del tiempo. En esta realización, después de que se ha transmitido un nivel de confianza, el valor del nivel de confianza determinado disminuye con el transcurso del tiempo. El descenso del nivel de confianza con el transcurso del tiempo puede representar, por ejemplo, que la integridad de la una o más piezas obtenidas de primera información de autenticación se restringe en tiempo. De esta manera, se garantiza que la una o más piezas de primera información de autenticación usadas para determinar el nivel de confianza están actualizadas y se dificulta el uso fraudulento, ya que, por ejemplo, en el caso en el que un usuario fraudulento intenta copiar una o más piezas de primera información de autenticación, las posibilidades de que estas una o más piezas de primera información de autenticación copiadas estén obsoletas son altas, ya que la una o más piezas de primera información de autenticación copiadas ya se han usado para determinar el nivel de confianza, y el nivel de confianza ya había disminuido con el transcurso del tiempo. Por lo tanto, el nivel de confianza puede no aumentarse (de nuevo) por estas una o más piezas de primera información de autenticación copiadas.

En una realización ilustrativa de todos los aspectos de la presente invención, la función dependiente del tiempo define el descenso del nivel de confianza. Por ejemplo, la función dependiente del tiempo puede ser, por ejemplo, una función lineal. En este caso, el nivel de confianza disminuye con el transcurso del tiempo linealmente. Como alternativa, la función dependiente del tiempo puede ser, por ejemplo, una función exponencial. En este caso, el nivel de confianza también disminuye con el transcurso del tiempo. Primero, el nivel de confianza disminuye lentamente con el transcurso del tiempo. A medida que transcurre más el tiempo, el descenso del nivel de confianza se acelera. Como alternativa, la función dependiente del tiempo puede ser, por ejemplo, una combinación de una función lineal y una exponencial. Por ejemplo, primero el nivel de confianza puede disminuir linealmente. Después de que haya transcurrido una cantidad predefinida de tiempo, el descenso del nivel de confianza sigue una función exponencial. Después de que haya transcurrido otra cantidad predefinida de tiempo, el descenso puede seguir de nuevo, por ejemplo, una función lineal. De esta manera, pueden implementarse, por ejemplo, diferentes funciones dependientes del tiempo de acuerdo con requisitos de un caso de uso dado.

De acuerdo con una realización ilustrativa de todos los aspectos de la presente invención, las etapas de obtención de una o más piezas de primera información de autenticación y de determinación de un nivel de confianza se repiten (por ejemplo, una o varias veces) para obtener un nivel de confianza actualizado en el caso en el que el nivel de confianza haya caído por debajo de un umbral de autenticación predefinido.

El umbral de autenticación puede representar, por ejemplo, un umbral, en el que el usuario cumple un requisito de estar asociado a al menos una cantidad mínima de confianza a autenticar, de modo que la una o más piezas de primera información de autenticación, por ejemplo, proporcionadas por el usuario, pueden considerarse que son enteras. Esto puede ser, por ejemplo, en el caso en el que el nivel de confianza determinado es igual a o está por encima del umbral de autenticación. En el caso en el que el nivel de confianza determinado está por debajo del umbral de autenticación, o ha caído por debajo del umbral de autenticación, el usuario no cumple el requisito de estar asociado a al menos una cantidad mínima de confianza asociada a la una o más piezas de primera información de autenticación, por ejemplo, proporcionadas por el usuario. En este último caso mencionado, no es posible autenticar satisfactoriamente al usuario. Para autenticar al usuario satisfactoriamente (de nuevo), el nivel de confianza necesita (re)establecerse. Por lo tanto, en esta realización, necesitan obtenerse una o más piezas de primera información de autenticación, necesita determinarse un nivel de confianza, y el nivel de confianza puede comprobarse contra el umbral de autenticación (de nuevo).

El nivel de confianza actualizado se obtiene para aumentar el nivel de confianza, en particular para aumentar el nivel de confianza a establecer al menos igual al umbral de autenticación. Adicionalmente, el nivel de confianza actualizado se obtiene para aumentar el nivel de confianza a establecer al menos igual al umbral de comprobación, en el caso en el que el servicio en el que tiene que autenticarse el usuario requiere que el nivel de confianza sea igual que o esté por encima del umbral de comprobación.

El umbral de autenticación puede ser, por ejemplo, diferente del umbral de comprobación. El umbral de autenticación puede ser indicativo, por ejemplo, del nivel de confianza que el nivel de confianza determinado debe cumplir para una autenticación del usuario. El umbral de autenticación puede considerarse, por ejemplo, que sea un límite fijo. En contraste, el umbral de comprobación puede ser, por ejemplo, un límite variable. Como se ha mencionado anteriormente en esta memoria descriptiva, el umbral de comprobación puede depender, por ejemplo, del servicio (por ejemplo, una transacción o similar) al que un usuario solicita autenticarse. En algunos casos, el umbral de autenticación y el umbral de comprobación pueden establecerse, por ejemplo, al mismo valor. Debido a, por ejemplo, una comprobación del nivel de confianza contra el umbral de autenticación, en el caso en el que el nivel de confianza está por encima del umbral de autenticación, puede asegurarse un nivel mínimo de confianza. Por ejemplo, siempre que el nivel de confianza no haya caído por debajo del umbral de autenticación, la comprobación - en el contexto de una petición de transacción - del nivel de confianza contra un umbral de comprobación (por ejemplo, específico de la transacción) puede realizarse sin obtener una o más piezas "nuevas" de primera información de autenticación para autenticar el usuario para esta transacción. Por lo tanto, pueden usarse, por ejemplo, una o más piezas de primera información de autenticación obtenidas para una pluralidad (por ejemplo, varias) de peticiones de transacciones de un usuario siempre que el nivel de confianza determinado no haya caído por debajo del umbral de autenticación. Igualmente bien, el umbral de autenticación puede ser una función (por ejemplo, de un mínimo o máximo) de uno o más (por ejemplo, todos) respectivos umbrales de comprobación asociados a una pluralidad de servicios (por ejemplo, tipos de transacción) que el usuario puede solicitar y para los que requiere autenticación. Si la función es la función de mínimo, se garantiza que al menos la transacción con el menor umbral de comprobación asociado puede realizarse siempre sin que el usuario tenga que proporcionar una o más piezas de primera información de autenticación específicamente para esta transacción. Si la función es la función de máximo, se garantiza que todas transacciones pueden realizarse sin que el usuario tenga que proporcionar una o más piezas de primera información de autenticación específicamente para cualquiera de las transacciones.

De acuerdo con una realización ilustrativa de todos los aspectos de la presente invención, la una o más piezas de primera información de autenticación comprenden uno o más de los siguientes tipos i) a v) de parámetros:

- i) uno o más parámetros de reconocimiento de comportamiento;
- ii) uno o más parámetros de reconocimiento acústico;
- iii) uno o más parámetros de reconocimiento óptico, en particular uno o más parámetros de reconocimiento facial;
- iv) uno o más parámetros de restricciones temporales;
- v) uno o más parámetros de restricciones locales.

Cada uno del uno o más parámetros de la una o más piezas de primera información de autenticación puede obtenerse, por ejemplo, por uno o más sensores (por ejemplo, del dispositivo electrónico del usuario). En esta memoria descriptiva, los tipos de parámetros también pueden denominarse, por ejemplo, como "parámetros de autenticación inteligentes".

El uno o más parámetros de reconocimiento de comportamiento pueden ser indicativos, por ejemplo, de una forma única en la que un usuario maneja su dispositivo electrónico. El uno o más parámetros de reconocimiento de comportamiento pueden obtenerse, por ejemplo, recopilando información, por ejemplo, por uno o más sensores, del

dispositivo electrónico del usuario. Por ejemplo, el uno o más sensores pueden comprender, por ejemplo, al menos un acelerómetro, giroscopio, sensor táctil, sensor de tiempo o una combinación de los mismos por nombrar solo algunos ejemplos no limitantes. Una o más piezas de información recopiladas por estos uno o más sensores pueden formar, por ejemplo, una huella de comportamiento única. El uno o más parámetros de reconocimiento de comportamiento pueden representar, por ejemplo, una huella de comportamiento de este tipo. El uno o más parámetros de reconocimiento de comportamiento pueden obtenerse, por ejemplo, automáticamente mediante el uso del dispositivo electrónico. Por lo tanto, puede no requerirse, por ejemplo, ninguna acción explícita del usuario.

El uno o más parámetros de reconocimiento acústico pueden ser indicativos, por ejemplo, de una voz del usuario a autenticar. Por ejemplo, el uno o más parámetros de reconocimiento acústico pueden obtenerse, por ejemplo, por un sensor acústico, por ejemplo, un micrófono o similar de un dispositivo electrónico. El uno o más parámetro de reconocimiento acústico puede comprender, por ejemplo, una grabación de sonido del usuario, por ejemplo, obtenida por el sensor acústico. Además, el uno o más parámetros de reconocimiento acústico pueden analizarse, por ejemplo, para reconocer el usuario para determinar el nivel de confianza. Adicionalmente, puede conseguirse, por ejemplo, una protección contra falsificación en reconocimiento de usuario por un proceso de detección óptico basado en robot (por ejemplo, un proceso de detección de voz).

El uno o más parámetros de reconocimiento óptico pueden ser indicativos, por ejemplo, de una fotografía o vídeo de al menos una parte del usuario a autenticar. Por ejemplo, el uno o más parámetros de reconocimiento óptico pueden obtenerse, por ejemplo, por un sensor de cámara, por ejemplo, de un dispositivo electrónico. El uno o más parámetros de reconocimiento óptico pueden comprender, por ejemplo, una fotografía o un vídeo de al menos una parte del usuario, por ejemplo, obtenido por el sensor de cámara. Además, el uno o más parámetros de reconocimiento óptico pueden analizarse, por ejemplo, para reconocer el usuario para determinar el nivel de confianza. Adicionalmente, puede conseguirse, por ejemplo, una protección contra falsificación en reconocimiento de usuario por un proceso de detección óptico basado en robot (por ejemplo, un proceso de detección facial). Por ejemplo, un robot de detección facial puede proporcionar a un usuario instrucciones aleatorias, por ejemplo, decirle al usuario que cierre su ojo izquierdo u ojo derecho o que gire su cabeza a la izquierda o a la derecha. Si la instrucción o instrucciones dadas se efectúan correctamente, la cara en la fotografía o vídeo recopilado es genuina. Si la instrucción o instrucciones dadas no se efectúan correctamente, y está presente una fotografía o vídeo fraudulento del usuario (por ejemplo, obtenido (por ejemplo, tomado) antes por el usuario que pretende el fraude). Basándose, al menos en parte, en el resultado del proceso de detección óptica, puede determinarse el nivel de confianza.

El uno o más parámetros de restricciones temporales pueden ser indicativos, por ejemplo, de una cierta hora y/o fecha en la que el usuario quiere autenticarse. El uno o más parámetros de restricciones temporales pueden analizarse, por ejemplo, para determinar el nivel de confianza. Por ejemplo, pueden predefinirse una o más restricciones temporales. La una o más restricciones temporales pueden almacenarse, por ejemplo, en una base de datos. El uno o más parámetros de restricciones temporales de la una o más piezas de primera información de autenticación pueden verificarse, por ejemplo, contra la una o más restricciones temporales predefinidas. La una o más restricciones temporales predefinidas pueden ser indicativas, por ejemplo, de una cierta hora y/o fecha (o un intervalo de tiempo) en la que el usuario puede autenticarse. Ejemplos de una o más restricciones temporales pueden ser, por ejemplo, uno o más de los siguientes: (i) las transacciones pueden ser válidas únicamente durante horas laborales (por ejemplo, de 9 a 5); (ii) las transacciones pueden ser válidas únicamente si el usuario no está de vacaciones; (iii) las transacciones pueden ser válidas únicamente con una fecha de inicio y fin definida; (iv) o una combinación de los mismos.

El uno o más parámetros de restricciones locales pueden ser indicativos, por ejemplo, de una cierta posición (por ejemplo, horizontal), en la que está colocado un dispositivo electrónico (y, por lo tanto, el usuario del dispositivo electrónico a autenticar) (por ejemplo, en la actualidad, es decir, en un momento en el que se miden y/u obtienen la una o más piezas de primera información de autenticación). El uno o más parámetros de restricciones locales pueden ser, por ejemplo, una característica de detección de posición, por ejemplo, proporcionada por un dispositivo electrónico. Como alternativa o adicionalmente, el uno o más parámetros de restricciones locales pueden ser indicativos, por ejemplo, de una cierta red o componente de red al que está conectado en la actualidad el dispositivo electrónico del usuario, (por ejemplo, un punto de acceso WiFi o célula de sistema de radio celular), una cierta zona horaria en la que está ubicado y/o colocado el dispositivo electrónico del usuario en la actualidad, un cierto proveedor de servicios que usa el usuario del dispositivo electrónico del usuario en la actualidad, o una combinación de los mismos por nombrar solo algunos ejemplos no limitantes. Para proteger el uno o más parámetros de restricciones locales contra manipulación (por ejemplo, por terceras partes o usuarios fraudulentos), pueden usarse, por ejemplo, más de una característica de detección de posición y/o historial de ubicaciones. Por ejemplo, el uno o más parámetros de restricciones locales pueden combinarse y un algoritmo puede calcular un riesgo de manipulación, que puede usarse, por ejemplo, para determinar el nivel de confianza. La una o más restricciones locales pueden almacenarse, por ejemplo, en una base de datos. El uno o más parámetros de restricciones locales de la una o más piezas de primera información de autenticación pueden verificarse contra una o más restricciones locales predefinidas. Ejemplos de una o más restricciones locales pueden ser, por ejemplo, uno o más de los siguientes: (i) las transacciones pueden ser válidas únicamente dentro de una cierta área, y/o dentro de un cierto país, o fuera de un país particular; (ii) las transacciones pueden ser válidas únicamente en el domicilio del usuario; (iii) o una combinación de los mismos por nombrar solo algunos ejemplos no limitantes.

- La una o más piezas de primera información de autenticación (por ejemplo, que comprende i) uno o más parámetros de reconocimiento de comportamiento; ii) uno o más parámetros de reconocimiento facial; iii) uno o más parámetros de restricciones temporales; iv) uno o más parámetros de restricciones locales; o una combinación de los mismos)
- 5 pueden almacenarse, por ejemplo, en una base de datos, por ejemplo. Una o más piezas de primera información de autenticación almacenadas pueden usarse, por ejemplo, para determinar un nivel de confianza, por ejemplo, verificando uno o más parámetros de autenticación inteligentes comprendidos por una o más piezas de primera información de autenticación contra los históricos almacenados (por ejemplo, almacenados en un momento anterior).
- 10 Una o más piezas de primera información de autenticación almacenadas pueden ser parte, por ejemplo, de una o más piezas de información histórica, que pueden usarse adicionalmente, por ejemplo, para determinar el nivel de confianza. Una o más piezas de primera información de autenticación almacenadas en la base de datos pueden actualizarse, por ejemplo, (por ejemplo, actualizarse de forma constante) mediante uno o más parámetros de autenticación inteligentes obtenidos, por ejemplo, comprendidos por una o más piezas de primera información de autenticación obtenidas.
- 15 En el caso en el que una de la una o más piezas de primera información de autenticación comprende más de un parámetro de autenticación inteligente, puede determinarse un respectivo nivel de confianza, por ejemplo, para cada uno de los parámetros comprendidos por la una o más piezas de primera información de autenticación.
- Además, el nivel de confianza puede determinarse, por ejemplo, basándose en una combinación aleatoria o pseudoaleatoria o variable con el tiempo de los parámetros de la una o más piezas de primera información de autenticación. De esta manera, puede mejorarse la seguridad de una autenticación ya que un usuario que pretende un uso fraudulento no sabe qué parámetro se usa para determinar el nivel de confianza.
- 20 De acuerdo con una realización ilustrativa de todos los aspectos de la presente invención, el nivel de confianza se determina basándose, al menos en parte, en al menos dos tipos diferentes de parámetros de tipos i) a v) comprendidos por la una o más piezas de primera información de autenticación. Por ejemplo, la una o más piezas de primera información de autenticación comprenden al menos dos parámetros diferentes en el caso en el que comprenden, por ejemplo, un parámetro de reconocimiento de comportamiento y, por ejemplo, un parámetro de restricciones temporales. Por el contrario, dentro del significado de la presente invención, la una o más piezas de primera información de autenticación comprenden al menos dos parámetros diferentes en el caso en el que comprenden, por ejemplo, dos parámetros de restricciones temporales.
- 25 En una realización ilustrativa de todos los aspectos de la presente invención, el uno o más parámetros de reconocimiento de comportamiento se obtienen durante un periodo de tiempo, que se preddefine o determina de acuerdo con una regla predefinida. El periodo de tiempo puede ser, por ejemplo, de una duración predeterminada, o la duración del periodo de tiempo puede determinarse (por ejemplo, adaptativamente), por ejemplo, de acuerdo con una regla predefinida. La duración del periodo de tiempo puede ser, por ejemplo, de uno o más minutos, horas, días o semanas por nombrar solo algunos ejemplos no limitantes.
- 30 De acuerdo con una realización ilustrativa de todos los aspectos de la presente invención, el uno o más parámetros de reconocimiento de comportamiento se obtienen más de una vez. Por ejemplo, el uno o más parámetros de reconocimiento de comportamiento pueden obtenerse, por ejemplo, al menos dos veces o una pluralidad de veces. El uno o más parámetros de reconocimiento de comportamiento pueden obtenerse, por ejemplo, más de una vez durante el periodo de tiempo. El uno o más parámetros de reconocimiento de comportamiento pueden obtenerse, por ejemplo, ininterrumpidamente, o discretamente, por ejemplo, después del transcurso de intervalos de tiempo predefinidos. Obteniendo el uno o más parámetros de reconocimiento de comportamiento más de una vez, la pluralidad de uno o más parámetros de reconocimiento de comportamiento como instancias pueden formar, por ejemplo, una huella de comportamiento. La huella de comportamiento puede representar, por ejemplo, al menos una parte de la al menos una pieza de información única asociada al usuario y/o el dispositivo electrónico del usuario.
- 35 De acuerdo con una realización ilustrativa de todos los aspectos de la presente invención, el uno o más parámetros de reconocimiento de comportamiento se obtienen basándose, al menos en parte, en (por ejemplo, una combinación con) uno o más parámetros de reconocimiento de comportamiento obtenidos en un momento anterior. Por ejemplo, la combinación puede representar un cambio desde el uno o más parámetros de reconocimiento de comportamiento obtenidos anteriormente al uno o más parámetros de reconocimiento de comportamiento. La combinación puede representar, por ejemplo, el historial de uno o más parámetros de reconocimiento de comportamiento obtenidos. Combinando el uno o más parámetros de reconocimiento de comportamiento con uno o más parámetros de reconocimiento de comportamiento obtenidos anteriormente, la combinación puede formar, por ejemplo, una huella de comportamiento. La huella de comportamiento puede representar, por ejemplo, al menos una parte de la al menos una pieza de información única asociada al usuario y/o el dispositivo electrónico del usuario.
- 40 De acuerdo con una realización ilustrativa de todos los aspectos de la presente invención, el uno o más parámetros de reconocimiento de comportamiento se obtienen basándose, al menos en parte, en (por ejemplo, una combinación con) uno o más parámetros de reconocimiento de comportamiento obtenidos en un momento anterior. Por ejemplo, la combinación puede representar un cambio desde el uno o más parámetros de reconocimiento de comportamiento obtenidos anteriormente al uno o más parámetros de reconocimiento de comportamiento. La combinación puede representar, por ejemplo, el historial de uno o más parámetros de reconocimiento de comportamiento obtenidos. Combinando el uno o más parámetros de reconocimiento de comportamiento con uno o más parámetros de reconocimiento de comportamiento obtenidos anteriormente, la combinación puede formar, por ejemplo, una huella de comportamiento. La huella de comportamiento puede representar, por ejemplo, al menos una parte de la al menos una pieza de información única asociada al usuario y/o el dispositivo electrónico del usuario.
- 45 De acuerdo con una realización ilustrativa de todos los aspectos de la presente invención, el uno o más parámetros de reconocimiento de comportamiento se obtienen basándose, al menos en parte, en (por ejemplo, una combinación con) uno o más parámetros de reconocimiento de comportamiento obtenidos en un momento anterior. Por ejemplo, la combinación puede representar un cambio desde el uno o más parámetros de reconocimiento de comportamiento obtenidos anteriormente al uno o más parámetros de reconocimiento de comportamiento. La combinación puede representar, por ejemplo, el historial de uno o más parámetros de reconocimiento de comportamiento obtenidos. Combinando el uno o más parámetros de reconocimiento de comportamiento con uno o más parámetros de reconocimiento de comportamiento obtenidos anteriormente, la combinación puede formar, por ejemplo, una huella de comportamiento. La huella de comportamiento puede representar, por ejemplo, al menos una parte de la al menos una pieza de información única asociada al usuario y/o el dispositivo electrónico del usuario.
- 50 De acuerdo con una realización ilustrativa de todos los aspectos de la presente invención, el uno o más parámetros de reconocimiento de comportamiento se obtienen basándose, al menos en parte, en (por ejemplo, una combinación con) uno o más parámetros de reconocimiento de comportamiento obtenidos en un momento anterior. Por ejemplo, la combinación puede representar un cambio desde el uno o más parámetros de reconocimiento de comportamiento obtenidos anteriormente al uno o más parámetros de reconocimiento de comportamiento. La combinación puede representar, por ejemplo, el historial de uno o más parámetros de reconocimiento de comportamiento obtenidos. Combinando el uno o más parámetros de reconocimiento de comportamiento con uno o más parámetros de reconocimiento de comportamiento obtenidos anteriormente, la combinación puede formar, por ejemplo, una huella de comportamiento. La huella de comportamiento puede representar, por ejemplo, al menos una parte de la al menos una pieza de información única asociada al usuario y/o el dispositivo electrónico del usuario.
- 55 De acuerdo con una realización ilustrativa de todos los aspectos de la presente invención, el uno o más parámetros de reconocimiento de comportamiento se obtienen basándose, al menos en parte, en (por ejemplo, una combinación con) uno o más parámetros de reconocimiento de comportamiento obtenidos en un momento anterior. Por ejemplo, la combinación puede representar un cambio desde el uno o más parámetros de reconocimiento de comportamiento obtenidos anteriormente al uno o más parámetros de reconocimiento de comportamiento. La combinación puede representar, por ejemplo, el historial de uno o más parámetros de reconocimiento de comportamiento obtenidos. Combinando el uno o más parámetros de reconocimiento de comportamiento con uno o más parámetros de reconocimiento de comportamiento obtenidos anteriormente, la combinación puede formar, por ejemplo, una huella de comportamiento. La huella de comportamiento puede representar, por ejemplo, al menos una parte de la al menos una pieza de información única asociada al usuario y/o el dispositivo electrónico del usuario.
- 60 De acuerdo con una realización ilustrativa de todos los aspectos de la presente invención, el uno o más parámetros de reconocimiento de comportamiento se obtienen basándose, al menos en parte, en (por ejemplo, una combinación con) uno o más parámetros de reconocimiento de comportamiento obtenidos en un momento anterior. Por ejemplo, la combinación puede representar un cambio desde el uno o más parámetros de reconocimiento de comportamiento obtenidos anteriormente al uno o más parámetros de reconocimiento de comportamiento. La combinación puede representar, por ejemplo, el historial de uno o más parámetros de reconocimiento de comportamiento obtenidos. Combinando el uno o más parámetros de reconocimiento de comportamiento con uno o más parámetros de reconocimiento de comportamiento obtenidos anteriormente, la combinación puede formar, por ejemplo, una huella de comportamiento. La huella de comportamiento puede representar, por ejemplo, al menos una parte de la al menos una pieza de información única asociada al usuario y/o el dispositivo electrónico del usuario.
- Adicionalmente o como alternativa, también pueden obtenerse, por ejemplo, uno o más de los otros tipos de parámetros diferentes del uno o más parámetros de reconocimiento de comportamiento durante el periodo de tiempo. Adicionalmente o como alternativa, uno o más de los otros tipos de parámetros también pueden obtenerse, por ejemplo, más de una vez. Adicionalmente o como alternativa, uno o más de los otros tipos de parámetros también pueden obtenerse, por ejemplo, basándose, al menos en parte, en una combinación con uno o más del mismo tipo de
- 65

parámetros obtenidos en un momento anterior.

La una o más piezas de segunda información de autenticación pueden derivarse, por ejemplo, de un aparato (por ejemplo, un dispositivo electrónico como un terminal, teléfono inteligente, tableta, por nombrar solo algunos ejemplos no limitantes), que puede ser, por ejemplo, el primer aparato de la presente invención (por ejemplo, el dispositivo electrónico del usuario) o puede ser otro aparato. Pueden recopilarse, por ejemplo, por el aparato, por ejemplo, por uno o más sensores del mismo. Como alternativa o adicionalmente, la una o más piezas de segunda información de autenticación pueden, por ejemplo, recibirse por el primer aparato, o por otra entidad. La una o más piezas de segunda información de autenticación pueden obtenerse, por ejemplo, automáticamente, por ejemplo, en intervalos de tiempo predefinidos. Como alternativa o adicionalmente, la una o más piezas de segunda información de autenticación pueden obtenerse, por ejemplo, a demanda, por ejemplo, en respuesta a una petición para obtener tales piezas de información. Una petición para obtener tales piezas de información puede derivarse, por ejemplo, de una aplicación de un dispositivo electrónico. Por ejemplo, la aplicación del dispositivo electrónico puede proporcionar, por ejemplo, uno o más servicios para un usuario del dispositivo electrónico. Por ejemplo, el uno o más servicios proporcionados por la aplicación pueden realizarse y/o controlarse (por ejemplo, satisfactoriamente o no satisfactoriamente), basándose en el uno o más servicios realizados y/o controlados (por ejemplo, satisfactoriamente o no satisfactoriamente), una o más piezas de segunda información de autenticación que comprenden uno o más parámetros de actualización de confianza que corresponden al uno o más servicios realizados y/o controlados (por ejemplo, satisfactoriamente o no satisfactoriamente) proporcionados por la aplicación del dispositivo electrónico.

Determinando el nivel de confianza basándose, al menos en parte, en la una o más segundas informaciones de autenticación, la seguridad de la identidad del usuario puede mejorarse incluso más debido a la consideración adicional de la una o más piezas de segunda información de autenticación cuando se determina el nivel de confianza. Para determinar el nivel de confianza basándose, al menos en parte, en la una o más piezas de primera información de autenticación y la una o más piezas de segunda información de autenticación, puede determinarse, por ejemplo, un nivel de confianza inicial basándose en la una o más piezas de primera información de autenticación. A continuación, el nivel de confianza determinado puede variarse, por ejemplo, correspondiendo a la una o más piezas de segunda información de autenticación. De esta manera, el nivel de confianza puede determinarse basándose, al menos en parte, en la una o más piezas de primera información de autenticación y en la una o más piezas de segunda información de autenticación.

De acuerdo con una realización ilustrativa de todos los aspectos de la presente invención, el nivel de confianza se determina adicionalmente basándose, al menos en parte, en la una o más piezas (obtenidas) de segunda información de autenticación.

El uno o más parámetros de actualización de confianza pueden representar, por ejemplo, un valor entre un intervalo de valores predefinido (por ejemplo, entre 0 y 100). En el caso en el que el nivel de confianza se determina basándose, al menos en parte, en la una o más piezas de segunda información de autenticación, el valor puede añadirse al nivel de confianza. El nivel de confianza puede aumentarse, por ejemplo, por el uno o más parámetros de actualización de confianza, por ejemplo, por el valor representado por la una o más piezas de segunda información de autenticación. El valor representado por el uno o más parámetros de actualización de confianza puede depender, por ejemplo, del tipo de parámetro usado para obtener el uno o más parámetros de actualización de confianza. Por ejemplo, en el caso en el que el uno o más parámetros de actualización de confianza se basan, al menos en parte, en información proporcionada por un sensor biométrico (por ejemplo, del dispositivo electrónico del usuario), el valor a añadir al nivel de confianza puede ser relativamente grande en comparación con un caso en el que el uno o más parámetros de actualización de confianza se basan, al menos en parte, en, por ejemplo, un PIN del usuario. El PIN del usuario puede falsificarse más fácilmente que, por ejemplo, una huella biométrica del usuario. Por lo tanto, una o más piezas de segunda información de autenticación que comprenden uno o más parámetros de actualización de confianza de un sensor biométrico pueden conducir, por ejemplo, a un mayor aumento del nivel de confianza que una o más piezas de segunda información de autenticación que comprenden uno o más parámetros de actualización de confianza de un PIN del usuario. Como alternativa o adicionalmente, un nivel de confianza disminuido, por ejemplo, puede actualizarse, por ejemplo, determinando un valor nuevo del nivel de confianza de acuerdo con reglas predefinidas, por ejemplo, por un algoritmo. Por ejemplo, un parámetro de actualización de confianza puede asociarse, por ejemplo, a uno o más ciertos eventos. Por ejemplo, un parámetro de actualización de confianza puede asociarse, por ejemplo, a una comprobación de un comportamiento del usuario. Basándose en el comportamiento del usuario, puede determinarse, por ejemplo, un valor nuevo del nivel de confianza de acuerdo con reglas predefinidas, por ejemplo, un algoritmo. El valor nuevo del nivel de confianza puede aumentarse o disminuirse, por ejemplo, basándose en el resultado de la comprobación del comportamiento del usuario. Por ejemplo, el valor de nivel de confianza puede disminuirse en el caso en el que el comportamiento del usuario contrasta con el comportamiento observado habitualmente del usuario. El valor de nivel de confianza puede aumentarse, por ejemplo, en el caso en el que el comportamiento del usuario coincide con el comportamiento habitualmente observado del usuario. El valor determinado del nivel de confianza, que puede ser, por ejemplo, un resultado del algoritmo, puede ser, por ejemplo, un valor en el intervalo de los valores 0 a 100. El valor determinado del nivel de confianza puede no estar fuera, por ejemplo, del intervalo de los valores 0 a 100.

El uno o más parámetros de actualización de confianza pueden determinarse, por ejemplo, basándose, al menos en

parte, en la una o más piezas de primera información de autenticación. Por ejemplo, el uno o más parámetros de actualización de confianza pueden aumentar o disminuir, por ejemplo, el nivel de confianza, por ejemplo, se establece una actualización de confianza aumentando el nivel de confianza. En contraste, el nivel de confianza puede disminuirse por una actualización de confianza, por ejemplo, en el caso en el que el usuario está bloqueado o el usuario se considera que no es entero de modo que los derechos de los usuarios se limitan. El bloqueo del usuario y/o la limitación de derechos del usuario pueden determinarse, por ejemplo, por un servidor, por ejemplo, un servidor del cierto proveedor de servicios que usa en la actualidad el usuario del dispositivo electrónico del usuario. Actualizar el nivel de confianza puede hacerse, por ejemplo, determinando el uno o más parámetros de actualización de confianza basándose, al menos en parte, en la una o más piezas de primera información de autenticación de dos formas.

La primera forma puede ser, por ejemplo, como se indica a continuación:

(i) explorando continuamente al usuario, por ejemplo, obteniendo uno o más parámetros de reconocimiento de comportamiento, uno o más parámetros de reconocimiento acústico, uno o más parámetros de reconocimiento óptico (por ejemplo, uno o más parámetros de reconocimiento facial), uno o más parámetros de restricciones locales, uno o más parámetros de restricciones de tiempo o una combinación de los mismos. Estos uno o más parámetros obtenidos pueden compararse, por ejemplo, con correspondientes uno o más parámetros almacenados en una base de datos. En el caso en el que el uno o más parámetros obtenidos coinciden con (por ejemplo, de una manera predefinida) o son iguales a los almacenados, el uno o más parámetros de actualización de confianza pueden considerarse, por ejemplo, para añadir un cierto valor al nivel de confianza.

La segunda forma para actualizar el nivel de confianza puede ser, por ejemplo, como se indica a continuación:

(ii) el nivel de confianza puede actualizarse, por ejemplo, a demanda, por ejemplo, por una petición del usuario. Por ejemplo, el nivel de confianza determinado puede caer por debajo de un umbral (por ejemplo, en el caso en el que el nivel de confianza es una función dependiente del tiempo, como se ha descrito anteriormente en esta memoria descriptiva) y debido a esto, se genera una petición para una actualización de confianza. La generación de una petición puede realizarse, por ejemplo, automáticamente en el caso en el que el nivel de confianza cae por debajo de un umbral (por ejemplo, predefinido, o determinado de acuerdo con un conjunto de reglas).

La una o más piezas de segunda información de autenticación pueden comprender, por ejemplo, uno o más parámetros de referencia de confianza. Por ejemplo, dependiendo de la autoridad de confianza (por ejemplo, externa), el uno o más parámetros de referencia de confianza pueden aumentar, por ejemplo, el nivel de confianza. El uno o más parámetros de referencia de confianza pueden representar, por ejemplo, un valor entre un intervalo de valores predefinido (por ejemplo, entre 0 y 100). En el caso en el que el nivel de confianza se determina basándose, al menos en parte, en la una o más piezas de segunda información de autenticación, el valor puede añadirse al nivel de confianza. El nivel de confianza puede aumentarse, por ejemplo, por el uno o más parámetros de referencia de confianza. Hacer referencia a autoridades de confianza (por ejemplo, externas) puede hacerse, por ejemplo, dinámicamente, periódicamente o a demanda. Ejemplos de uno o más parámetros de referencia de confianza pueden ser, por ejemplo, uno o más de los siguientes: (i) una o más activaciones de cartas (por ejemplo, un usuario contesta a una o más cartas de activación físicas enviadas a través de correo ordinario, las respuestas se almacenan); (ii) proveedores de identidad de terceros (por ejemplo, a través del protocolo de SAML) (por ejemplo, únicamente puede pasarse información no crítica a los proveedores de terceros); (iii) cualquier otra fuente de datos en un extremo final (por ejemplo, de una aplicación de extremo final para mejorar el nivel de confianza); (iv) o una combinación de los mismos.

El nivel de confianza puede aumentarse, por ejemplo, por una combinación del uno o más parámetros de actualización de confianza y del uno o más parámetros de referencia de confianza.

De acuerdo con una realización ilustrativa de todos los aspectos de la presente invención, el método comprende adicionalmente:

- determinar al menos una información de calibración basándose, al menos en parte, en la una o más piezas de primera información de autenticación y/o basándose, al menos en parte, en la una o más piezas de segunda información de autenticación, en donde la información de calibración usada para definir un umbral.

El umbral puede ser, por ejemplo, el umbral de autenticación o el umbral de comprobación. Como alternativa, la información de calibración puede usarse, por ejemplo, para definir el umbral de autenticación y el umbral de comprobación.

Como alternativa, el método puede comprender adicionalmente:

- determinar una o más piezas de información de calibración basándose, al menos en parte, en una o más piezas de primera información de autenticación obtenidas anteriormente, en donde la una o más piezas de información de calibración son indicativas de al menos un nivel de calibración calculado indicativo de una confianza en al menos una pieza de información única asociada al usuario y/o con el dispositivo electrónico del usuario.

La al menos una información de calibración puede obtenerse, por ejemplo, anteriormente, por ejemplo, en una etapa

inicial, por ejemplo, antes de realizar y/o controlar el método de acuerdo con todos los aspectos de la presente invención.

5 La al menos una información de calibración puede comprender, por ejemplo, una huella de comportamiento única determinada basándose, al menos en parte, en uno o más parámetros de reconocimiento de comportamiento. Durante una etapa inicial, la huella de comportamiento única se determina de modo que una o más primeras informaciones de autenticación obtenidas que comprenden uno o más parámetros de reconocimiento de comportamiento pueden verificarse, por ejemplo, contra la huella de comportamiento única.

10 Como alternativa o adicionalmente, la al menos una información de calibración puede comprender, por ejemplo, información de una cara (u otra parte) del usuario. Durante una etapa inicial, esta información puede obtenerse, por ejemplo, de modo que una o más primeras informaciones de autenticación obtenidas que comprenden uno o más parámetros de reconocimiento facial (u otra parte) pueden verificarse, por ejemplo, contra la información de una cara del usuario.

15 Como alternativa o adicionalmente, la al menos una información de calibración puede comprender, por ejemplo, una o más restricciones temporales y/o una o más restricciones locales (por ejemplo, obtenidas durante una etapa inicial). Una o más primeras informaciones de autenticación obtenidas que comprenden uno o más parámetros de restricciones temporales y/o uno o más parámetros de restricciones locales pueden verificarse, por ejemplo, contra la una o más restricciones temporales y/o la una o más restricciones locales. La una o más restricciones temporales y/o la una o más restricciones locales pueden introducirse, por ejemplo, por un usuario de acuerdo con sus preferencias, u obtenerse automáticamente.

20 El nivel de confianza umbral puede representar, por ejemplo, uno o más escenarios de nivel de confianza, como se ha descrito anteriormente.

25 El al menos un nivel de calibración calculado de al menos un parámetro de autenticación inteligente puede ser adaptable, por ejemplo. Por ejemplo, el al menos un nivel de calibración calculado de al menos un parámetro de autenticación inteligente puede calcularse en diferentes puntos de tiempo, o de forma continua en intervalos de tiempo predefinidos, o basándose en ciertos eventos (por ejemplo, se obtienen una o más piezas "nuevas" de primera y/o segunda información de autenticación), por nombrar solo algunos ejemplos no limitantes.

30 El cálculo del al menos un nivel de calibración de al menos un parámetro de autenticación inteligente puede basarse, por ejemplo, al menos en parte, en uno o más parámetros de autenticación inteligentes obtenidos en una etapa anterior. Por lo tanto, el cálculo del al menos un nivel de al menos un parámetro de autenticación inteligente puede basarse en información histórica.

35 En una realización ilustrativa de todos los aspectos de la presente invención, el umbral de autenticación y/o el umbral de comprobación se establece basándose, al menos en parte, en la al menos una información de calibración.

40 De acuerdo con una realización ilustrativa de todos los aspectos de la presente invención, la una o más piezas de primera información de autenticación y/o la una o más piezas de segunda información de autenticación se almacenan en una base de datos. La base de datos puede conectarse, por ejemplo, al primer aparato de acuerdo con el primer aspecto de la presente invención (por ejemplo, un servidor). La base de datos puede conectarse, por ejemplo, al servidor, por ejemplo, a través de la internet y que permite el acceso del aparato a información almacenada de la base de datos. Como alternativa, la base de datos puede incorporarse en el aparato, por ejemplo, el servidor.

45 En una realización ilustrativa de todos los aspectos de la presente invención, la una o más piezas de primera información de autenticación y/o la una o más piezas de segunda información de autenticación almacenadas en la base de datos son adaptables. Por ejemplo, la una o más piezas de primera información de autenticación y/o la una o más piezas de segunda información de autenticación pueden adaptarse, por ejemplo, de forma continua, en intervalos de tiempo predefinidos, en tiempo real o una combinación de los mismos, por nombrar solo algunos ejemplos no limitantes. Como alternativa, una o más instancias de la una o más piezas de primera información de autenticación y/o la una o más piezas de segunda información de autenticación se almacenan en la base de datos para adquirir información histórica. Para adquirir estas una o más instancias, cada vez que se obtiene una nueva instancia de una o más piezas de primera información de autenticación y/o de una o más piezas de segunda información de autenticación (por ejemplo, por el servidor), esta nueva instancia se almacena adicionalmente en la base de datos.

50 De acuerdo con una realización ilustrativa de todos los aspectos de la presente invención, la al menos una información de calibración se determina basándose, al menos en parte, en la una o más piezas de primera información de autenticación y/o la una o más piezas de segunda información de autenticación almacenadas en la base de datos.

55 Además, ya que el nivel de confianza es una función dependiente del tiempo, una actualización del nivel de confianza puede realizarse y/o controlarse, por ejemplo, en el caso en el que el valor del nivel de confianza cae por debajo del umbral predefinido. El umbral predefinido puede ser, por ejemplo, el umbral de autenticación o el umbral de comprobación. Además, puede determinarse, por ejemplo, un umbral predefinido adicional que es indicativo de un

nivel de confianza que es mayor que el valor del nivel de confianza del umbral predefinido. El umbral predefinido adicional puede usarse, por ejemplo, para emitir, por ejemplo, una alarma y/o aviso, que puede proporcionarse al usuario, por ejemplo, avisando al usuario que el nivel de confianza puede caer por debajo del umbral predefinido. En el caso en el que el valor del nivel de confianza cae por debajo del umbral predefinido, puede generarse, por ejemplo, una petición para actualizar el nivel de confianza. Basándose en la petición generada, por ejemplo, pueden obtenerse, por ejemplo, una o más piezas de segunda información de autenticación, por ejemplo, para realizar una actualización del nivel de confianza. En el caso en el que el nivel de confianza está aún por debajo del umbral predefinido después de que se realizó una actualización del nivel de confianza, puede bloquearse al usuario, por ejemplo, y/o puede bloquearse, por ejemplo, el uso de una aplicación del dispositivo electrónico y/o el uso de un servicio proporcionado al usuario.

En una realización ilustrativa de todos los aspectos de la presente invención, el método comprende adicionalmente:

- obtener una o más piezas de tercera información de autenticación, en donde la una o más piezas de tercera información de autenticación son indicativas, al menos en parte, de uno o más de los siguientes:

- (i) uno o más parámetros de propiedad;
- (ii) uno o más parámetros de conocimiento;
- (iii) uno o más parámetros biométricos;
- (iv) o una combinación de los mismos.

En contraste a la una o más piezas de primera información de autenticación, la una o más piezas de tercera información de autenticación se proporcionan solamente por el usuario. En contraste, la una o más piezas de primera información de autenticación comprenden alguna clase de proceso de determinación para generar, por ejemplo, una huella de comportamiento, un parámetro de reconocimiento acústico, un parámetro de reconocimiento óptico, restricciones de tiempo y/o fecha, por nombrar solo algunos ejemplos no limitantes realizados basándose en información única asociada al usuario y/o el dispositivo electrónico del usuario. La información única asociada al usuario y/o el dispositivo electrónico del usuario puede recopilarse, por ejemplo, por uno o más sensores del dispositivo electrónico.

La una o más piezas de tercera información de autenticación puede obtenerse, por ejemplo, recopilando la una o más piezas de tercera información de autenticación por uno o más sensores del dispositivo electrónico. La una o más piezas de tercera información de autenticación son indicativas, al menos en parte, de uno o más de los siguientes: (i) uno o más parámetros de propiedad; (ii) uno o más parámetros de conocimiento; (iii) uno o más parámetros biométricos; (iv) o una combinación de los mismos.

El uno o más parámetros de propiedad pueden representar, por ejemplo, una indicación de una propiedad de un dispositivo electrónico (por ejemplo, el dispositivo electrónico del usuario) por el usuario. Por ejemplo, el uno o más parámetros de propiedad pueden representar un identificador del dispositivo electrónico, que se usó, por ejemplo, durante un proceso de activación de una aplicación realizada y/o controlada por el dispositivo electrónico. Basándose en esto, la aplicación puede estar vinculada, por ejemplo, (por ejemplo, exclusivamente) al dispositivo electrónico usado durante el proceso de activación. Adicionalmente, otro identificador de la aplicación puede representarse, por ejemplo, por el uno o más parámetros de propiedad. Por lo tanto, el identificador para el dispositivo electrónico y el otro identificador de la aplicación pueden comprobarse, por ejemplo, para mejorar la probabilidad de que la autenticación del usuario no es fraudulenta.

El uno o más parámetros de conocimiento pueden representar, por ejemplo, un conocimiento único, que puede conocerse únicamente en parte del usuario. Por ejemplo, el uno o más parámetros de conocimiento pueden representar un PIN, por ejemplo, un PIN para desbloquear un dispositivo electrónico, y/u otro PIN para desbloquear una aplicación del dispositivo electrónico. La aplicación puede ser, por ejemplo, una aplicación del dispositivo electrónico usado durante un proceso de activación, y/o que solicita la autenticación del usuario. El uno o más parámetros biométricos pueden ser indicativos, por ejemplo, de un atributo (por ejemplo, físico) único del usuario. El uno o más parámetros biométricos pueden obtenerse, por ejemplo, (por ejemplo, recopilarse) por uno o más sensores de un dispositivo electrónico. Por ejemplo, el uno o más parámetros biométricos pueden representar, por ejemplo, una huella dactilar del usuario. La huella dactilar del usuario puede obtenerse, por ejemplo, por un sensor de huella dactilar de un dispositivo electrónico (por ejemplo, el dispositivo electrónico del usuario).

En una realización ilustrativa de todos los aspectos de la presente invención, el nivel de confianza se determina adicionalmente basándose, al menos en parte, en la una o más piezas de tercera información de autenticación. De esta manera, se mejora adicionalmente la seguridad.

De acuerdo con una realización ilustrativa de todos los aspectos de la presente invención, el método comprende adicionalmente:

- proporcionar el nivel de confianza determinado para su uso en un proceso de autenticación.

Debe apreciarse que la presentación de la invención en esta sección es solamente a modo de ejemplo y no limitación.

Otras características de la invención serán evidentes a partir de la siguiente descripción detallada considerada en conjunto con los dibujos adjuntos. Debe apreciarse, sin embargo, que los dibujos se diseñan solamente para propósitos de ilustración y no como una definición de los límites de la invención, para los que debería hacerse referencia a las reivindicaciones adjuntas. Debería entenderse adicionalmente que los dibujos no están dibujados a escala y que solamente pretenden ilustrar conceptualmente las estructuras y procedimientos descritos en este documento.

Breve descripción de los dibujos

En las figuras se muestran:

- Figura 1 un bloque esquemático y diagrama de interacción de un sistema de acuerdo con una realización ilustrativa de la presente invención;
- Figura 2a un diagrama de flujo que muestra una realización de ejemplo de un método adicional de acuerdo con el primer aspecto ilustrativo de la presente invención realizado, por ejemplo, por el dispositivo electrónico 130 de la Figura 1;
- Figura 2b un diagrama de flujo que muestra una realización de ejemplo de un método de acuerdo con el primer aspecto ilustrativo de la presente invención realizado, por ejemplo, por el dispositivo electrónico 130 de la Figura 1;
- Figura 3 un diagrama de bloques esquemático de un aparato de acuerdo con una realización ilustrativa de la presente invención;
- Figura 4 un diagrama de flujo que muestra una realización de ejemplo de un método adicional de acuerdo con el primer aspecto ilustrativo de la presente invención; y
- Figura 5 un diagrama representado de un nivel de confianza como una función dependiente del tiempo como se usa en una realización de ejemplo de un método de acuerdo con el primer aspecto ilustrativo de la presente invención.

Descripción detallada

La siguiente descripción sirve para profundizar en el entendimiento de la presente invención y se entenderá para complementar y leerse junto con la descripción según se proporciona en la sección de sumario anterior en esta memoria descriptiva.

La Figura 1 muestra un bloque esquemático y un diagrama de interacción de un sistema 100 de acuerdo con una realización ilustrativa de la presente invención.

El sistema 100 comprende un servidor 110, que puede incorporarse como alternativa como una nube de servidores (por ejemplo, una pluralidad de servidores conectados, por ejemplo, a través de la internet y que proporcionan servicios al menos parcialmente conjuntamente), una base de datos 120, que puede conectarse al servidor, por ejemplo, a través de la internet y que permite acceso desde el servidor 110 a datos de la base de datos 120. Como alternativa, la base de datos 120 puede incorporarse, por ejemplo, en el servidor 110. Además, el sistema 100 comprende un dispositivo electrónico 130, por ejemplo, un teléfono inteligente, una tableta, o un ordenador portátil por nombrar solo algunos ejemplos no limitantes, y una aplicación de extremo final 140, que puede configurarse para usarse y/o controlarse por otra aplicación 131 realizada por el dispositivo electrónico 130. Como alternativa, la aplicación de extremo final 140 puede realizarse también por el dispositivo electrónico 130. La aplicación de extremo final 140 puede instalarse, por ejemplo, en el dispositivo electrónico 130, o en el servidor 110, o en otro aparato.

De acuerdo con una realización de ejemplo, el dispositivo electrónico 130 puede proporcionar una o más piezas de primera información de autenticación (por ejemplo, obtenidas desde uno o más sensores 132 o elementos de interfaz de usuario del dispositivo electrónico 130). Adicionalmente, el dispositivo electrónico 130 puede proporcionar una o más piezas de segunda información de autenticación (por ejemplo, parámetros de referencia de confianza obtenidos desde una autoridad de confianza externa) y/o una o más piezas de tercera información de autenticación (por ejemplo, un PIN introducido por el usuario en el dispositivo electrónico 130). Adicionalmente, la base de datos 120 puede almacenar la una o más piezas proporcionadas de primera, segunda y/o tercera información de autenticación, por ejemplo, proporcionadas por el dispositivo electrónico 130, y/o proporcionadas por el servidor 110, y/o proporcionadas por la aplicación de extremo final 140, basándose en una o más piezas recibidas de primera, segunda y/o tercera información de autenticación. En una realización ilustrativa adicional, el servidor 110 puede proporcionar una información de autenticación al dispositivo electrónico 130. En una realización ilustrativa, el dispositivo electrónico 130 puede solicitar, por ejemplo, un servicio de un proveedor de servicios. El servidor del proveedor de servicios puede ser, por ejemplo, el servidor 110, pero también puede ser otro servidor (no mostrado en la Figura 1). Para autenticar al usuario del dispositivo electrónico que solicita el servicio, el servidor del proveedor de servicios

puede solicitar, por ejemplo, la autenticación del usuario del dispositivo electrónico 130 del servidor 110. La comunicación, por ejemplo, para la transmisión de la información, por ejemplo, entre el dispositivo electrónico 130 y el servidor 110, puede tener lugar, por ejemplo, al menos parcialmente en una función inalámbrica, por ejemplo, basándose en una comunicación de radio celular o en una comunicación basada en Red de Área Local Inalámbrica (WLAN), por nombrar solo algunos ejemplos no limitantes, o en su totalidad por cable.

La una o más piezas de primera, segunda y/o tercera información de autenticación pueden proporcionarse por el dispositivo electrónico 130 al servidor 110, por ejemplo, a través de la aplicación de extremo final 140. La provisión de la una o más piezas de primera información de autenticación al servidor 110 puede desencadenarse, por ejemplo, por el servidor del proveedor de servicios, en donde el usuario del dispositivo electrónico 130 ha solicitado la provisión de un servicio. El servidor 110, a continuación, puede determinar, por ejemplo, un nivel de confianza basándose en la una o más piezas de primera información de autenticación o basándose en la una o más piezas de primera información de autenticación y en la una o más piezas de segunda información de autenticación. Adicionalmente, el servidor 110 puede comprobar, por ejemplo, el nivel de confianza determinado basándose, al menos en parte, en una comparación con un umbral de comprobación predefinido. Basándose en el resultado de la comparación, el servidor 110 puede generar, por ejemplo, una información de autenticación indicativa de si el usuario está o no autenticado satisfactoriamente. El dispositivo electrónico 130 puede configurarse para recibir la información de autenticación proporcionada por el servidor 110. La información de autenticación recibida puede proporcionarse, a continuación, al servidor del proveedor de servicios. La provisión de la autenticación desde el dispositivo electrónico 130 al servidor del proveedor de servicios puede indicar, por ejemplo, al servidor del proveedor de servicios que el usuario se autenticó o no satisfactoriamente. Como alternativa, la información de autenticación puede proporcionarse al servidor del proveedor de servicios, por ejemplo, directamente o a través de una operación redirigida que implica al dispositivo electrónico 130.

La una o más piezas de primera, segunda y/o tercera información de autenticación, la información de autenticación, y/o comunicación adicional transmitida entre la aplicación 131 del dispositivo electrónico 130 y el servidor 110 puede usar, por ejemplo, un canal de comunicación seguro que se establece entre la aplicación 131 del dispositivo electrónico 130 y el servidor 110. En la Figura 1, se muestran dos realizaciones ilustrativas de un canal seguro de este tipo: el canal seguro I establecido directamente entre la aplicación 131 del dispositivo electrónico 130 y el servidor 110; y el canal seguro II establecido indirectamente entre la aplicación 131 del dispositivo electrónico 130 y el servidor 110. El canal seguro II se divide en dos partes: canal seguro II.a y canal seguro II.b. El canal seguro II.a y el canal seguro II.b indican que el canal seguro II se establece indirectamente entre la aplicación 131 del dispositivo electrónico 130 y el servidor 110, en donde el canal seguro II.a de primera parte del canal seguro II puede establecerse, por ejemplo, entre el servidor 110 y la aplicación de extremo final 140, y el canal seguro II.b de segunda parte del canal seguro II puede establecerse, por ejemplo, entre la aplicación de extremo final 140 y la aplicación 131 del dispositivo electrónico 130. El establecimiento del canal de comunicación seguro (por ejemplo, canal seguro I o canal seguro II) puede tener lugar, por ejemplo, antes de la provisión de la una o más piezas de primera, segunda y/o tercera información de autenticación por el dispositivo electrónico 130 al servidor 110. El establecimiento del canal de comunicación seguro (por ejemplo, canal seguro I o canal seguro II) puede realizarse, por ejemplo, basándose en una petición para un servicio desde un servidor de un proveedor de servicios que se origina desde el dispositivo electrónico 130, en particular la aplicación 131 del dispositivo electrónico 130, que puede ejecutarse, por ejemplo, por un usuario a proporcionar con el servicio del proveedor de servicios.

De esta manera, por ejemplo, una autenticación basándose en múltiples parámetros (por ejemplo, como factores) inteligentes o inteligentes y dinámicos comprendidos por la una o más piezas de primera información de autenticación o comprendidos por la una o más piezas de primera información de autenticación y la una o más piezas de segunda información de autenticación y/o la una o más piezas de tercera información de autenticación pueden proporcionarse como un servicio a dispositivo o dispositivos electrónicos de usuario o usuarios.

La Figura 2a muestra un diagrama de flujo 200a que muestra una realización de ejemplo de un método de acuerdo con el primer aspecto ilustrativo de la presente invención. Este diagrama de flujo 200a puede realizarse, por ejemplo, por el servidor 110 de la Figura 1, y/o por el dispositivo electrónico 130 y/o por la aplicación de extremo final 140.

En la etapa 201a, se obtienen una o más piezas de primera información de autenticación. La una o más piezas de primera información de autenticación representan al menos una pieza de información única asociada a un usuario y/o un dispositivo electrónico (por ejemplo, el dispositivo electrónico 130 de la Figura 1) del usuario. Por ejemplo, la una o más piezas de primera información de autenticación pueden comprender uno o más de los siguientes tipos i) a v) de parámetros: i) uno o más parámetros de reconocimiento de comportamiento; ii) uno o más parámetros de reconocimiento acústico; iii) uno o más parámetros de reconocimiento óptico; iv) uno o más parámetros de restricciones temporales; v) uno o más parámetros de restricciones locales. La una o más piezas de primera información de autenticación pueden recibirse, por ejemplo, desde, por ejemplo, un dispositivo electrónico (por ejemplo, el dispositivo electrónico 130 de la Figura 1). Como alternativa, la una o más piezas de primera información de autenticación, por ejemplo, pueden recopilarse, por ejemplo, por uno o más sensores 132. El uno o más sensores 132 pueden estar, por ejemplo, comprendidos por el dispositivo electrónico. La una o más piezas de primera información de autenticación pueden representar, por ejemplo, información recopilada por el uno o más sensores 132, por ejemplo, del dispositivo electrónico (por ejemplo, el dispositivo electrónico 130 de la Figura 1). El uno o más

sensores pueden ser, por ejemplo, sensores conectables al dispositivo electrónico (por ejemplo, el dispositivo electrónico 130 de la Figura 1). Basándose en estas piezas de información, por ejemplo, puede determinarse, por ejemplo, un parámetro de reconocimiento de comportamiento indicativo de comportamiento específico de usuario.

- 5 En la etapa 202a, se determina un nivel de confianza, por ejemplo, por un servidor (por ejemplo, el servidor 110 de la Figura 1). El nivel de confianza se determina basándose, al menos en parte, en la una o más piezas de primera información de autenticación. El nivel de confianza es indicativo de un nivel de confianza en la una o más piezas de primera información de autenticación. Por ejemplo, el nivel de confianza puede representar un valor (por ejemplo, entre un intervalo predeterminado, en donde el intervalo especifica un límite de intervalo inferior sin ningún nivel de confianza
- 10 en la una o más piezas de primera información de autenticación asociadas, y un límite de intervalo mayor con nivel de confianza máximo en una o más piezas de primera información de autenticación asociadas).

- En una etapa opcional 203a, se comprueba el nivel de confianza. Por ejemplo, el nivel de confianza determinado de etapa 202a se compara con un umbral predeterminado (por ejemplo, un umbral de comprobación). Por nombrar un ejemplo no limitante: basándose en el resultado de la comparación (por ejemplo, el nivel de confianza es menor, mayor o igual que el umbral predeterminado), puede permitirse, por ejemplo, únicamente que se efectúe una tarea (por ejemplo, un servicio solicitado por un usuario que requiere una autenticación) en el caso en el que el nivel de confianza determinado está por encima o es igual que el umbral predeterminado. En el caso en el que el nivel de confianza determinado es menor que el umbral predeterminado, puede no permitirse, por ejemplo, que se efectúe la tarea. Puede ser posible, por ejemplo, una especificación adicional: pueden definirse, por ejemplo, uno o más intervalos adicionales dentro del intervalo predeterminado. Uno del uno o más intervalos adicionales puede ser indicativo, por ejemplo, de una cantidad de dinero, que se permite transferir, en el caso en el que la tarea solicitada por el usuario como un servicio es, por ejemplo, una transferencia bancaria. Por ejemplo, en el caso en el que el nivel de confianza determinado es mayor que el umbral predeterminado, y dentro del intervalo brevemente adyacente al umbral predeterminado, la cantidad de dinero que se permite que transfiera el usuario puede limitarse, por ejemplo. Adicionalmente, en el caso en el que el nivel de confianza determinado es mayor que el umbral predeterminado, y dentro del intervalo orientado hacia el extremo mayor del intervalo que especifica un límite de intervalo inferior sin nivel de confianza y un extremo mayor con nivel de confianza máximo, la cantidad de dinero que se permite que el usuario transfiera puede no limitarse, o limitarse a la máxima cantidad posible.
- 15
- 20
- 25
- 30

En la etapa opcional 204a, se genera una información de autenticación que comprende, por ejemplo, el nivel de confianza determinado. Adicionalmente, la información de autenticación generada puede emitirse, por ejemplo, a un servidor de un proveedor de servicios, para su uso en un proceso de autenticación.

- 35 De esta manera, puede mejorarse la seguridad de una autenticación del usuario usando una o más piezas de primera información de autenticación. Además, la seguridad de la autenticación del usuario puede mejorarse, por ejemplo, adicionalmente usando una o más piezas de segunda información de autenticación o una o más piezas de segunda información de autenticación y una o más piezas de tercera información de autenticación adicionalmente.

- 40 La Figura 2b muestra un diagrama de flujo 200b que muestra una realización de ejemplo de un método adicional de acuerdo con el primer aspecto ilustrativo de la presente invención. Este diagrama de flujo 200b puede realizarse, por ejemplo, por el servidor 110 de la Figura 1, y/o por el dispositivo electrónico 130 y/o por la aplicación de extremo final 140.

- 45 Como en la Figura 2a, en la etapa 201b se obtienen una o más piezas de primera información de autenticación. Adicionalmente, pueden obtenerse, por ejemplo, una o más piezas de segunda información de autenticación. La una o más piezas de segunda información de autenticación pueden comprender, por ejemplo, uno o más de los siguientes tipos a) y b) de parámetros: a) uno o más parámetros de actualización de confianza; b) uno o más parámetros de referencia de confianza.

- 50 En la etapa 202b se determina un nivel de confianza, basándose, al menos en parte, en la una o más piezas obtenidas de primera información de autenticación, o basándose, al menos en parte, en la una o más piezas obtenidas de primera información de autenticación y en la una o más piezas obtenidas de segunda información de autenticación. Para determinar el nivel de confianza basándose, al menos en parte, en la una o más piezas de primera información de autenticación y la una o más piezas de segunda información de autenticación, puede determinarse, por ejemplo, un nivel de confianza inicial basándose en la una o más piezas de primera información de autenticación. A continuación, el nivel de confianza determinado puede variarse, por ejemplo, correspondiendo a la una o más piezas de segunda información de autenticación. De esta manera, el nivel de confianza puede determinarse basándose, al menos en parte, en la una o más piezas de primera información de autenticación y en la una o más piezas de segunda información de autenticación.
- 55
- 60

En esta realización de la presente invención, el nivel de confianza determinado es una función dependiente del tiempo, en donde el nivel de confianza disminuye con el transcurso del tiempo.

- 65 En la etapa 203b, se comprueba si el nivel de confianza determinado se ha degradado - debido al descenso del nivel de confianza con el transcurso del tiempo - por debajo de un umbral de autenticación. El umbral de autenticación

puede representar, por ejemplo, un umbral, en el que el usuario cumple un requisito de estar asociado a al menos una cantidad mínima de confianza a autenticar.

En el caso en el que el nivel de confianza está por encima del umbral de autenticación, puede asegurarse un nivel mínimo de confianza. Por ejemplo, siempre que el nivel de confianza no haya caído por debajo del umbral de autenticación, la comprobación del nivel de confianza contra un umbral de comprobación (por ejemplo, específico de la transacción) puede realizarse sin obtener una o más piezas "nuevas" o adicionales de primera información de autenticación. Por lo tanto, pueden usarse, por ejemplo, una o más piezas de primera información de autenticación obtenidas para una pluralidad (por ejemplo, varias) de peticiones de transacciones de un usuario siempre que el nivel de confianza determinado no haya caído por debajo del umbral de autenticación. En la etapa 204b, se comprueba si el usuario desea realizar una transacción, por ejemplo, se recibe una petición de transacción del usuario, por ejemplo, por el servidor del proveedor de servicios. Una petición de transacción del usuario puede comprender, por ejemplo, una petición para la comprobación de un saldo de cuenta, o de transferencia de dinero a otra persona, por nombrar solo algunos ejemplos no limitantes.

En el caso en el que el nivel de confianza haya caído por debajo del umbral de autenticación, no pueden cumplirse las peticiones de transacciones del usuario, por ejemplo, realizadas por un proveedor de servicios que ofrece un servicio al usuario. Por lo tanto, puede continuarse con la etapa 201b.

En la etapa 205b, el nivel de confianza se comprueba contra un umbral de comprobación específico de la transacción. El umbral de comprobación puede ser, por ejemplo, mayor para transacciones solicitadas por el usuario de mayores requisitos de seguridad. Por ejemplo, una simple petición del usuario para comprobar un saldo de cuenta puede tener un menor umbral de comprobación que una petición para transferir dinero a otro usuario. En el caso en el que el nivel de confianza es igual a o está por encima del umbral de comprobación específico de la transacción, se realiza la transacción solicitada por el usuario. En el caso en el que el nivel de confianza no está por encima del umbral de comprobación específico de la transacción, se deniega la petición del usuario para realizar la transacción.

En la etapa opcional 206b, puede generarse una información de autenticación basándose, al menos en parte, en el resultado de la comprobación de la etapa 205b. La información de autenticación generada puede ser indicativa, por ejemplo, de si se permite que la transacción solicitada por el usuario se realice o no. Además, la información de autenticación generada puede emitirse, por ejemplo, para su uso en un proceso de autenticación del usuario, por ejemplo, un proceso de autenticación de un servicio de un proveedor de servicios para realizar una transacción solicitada por el usuario. La Figura 3 es un diagrama de bloques esquemático de un aparato 300 de acuerdo con un aspecto ilustrativo de la presente invención, que puede representar, por ejemplo, el dispositivo electrónico 130, 140 y/o 150 de la Figura 1. Como alternativa, el diagrama de bloques esquemático del aparato 300 de acuerdo con un aspecto ilustrativo de la presente invención puede representar, por ejemplo, el servidor 110 de la Figura 1. El aparato 300 puede representar, por ejemplo, el primer aparato.

El aparato 300 comprende un procesador 310, una memoria de trabajo 330, una memoria de programa 320, una memoria de datos opcional 340, una interfaz o interfaces de comunicación 350, una interfaz de usuario opcional 360 y un sensor o sensores opcionales 370.

El aparato 300 puede estar configurado, por ejemplo, para realizar y/o controlar o comprender respectivos medios (al menos uno de 310 a 370) para realizar y/o controlar el método de acuerdo con el primer aspecto ilustrativo de la presente invención. El aparato 300 también puede constituir un aparato que comprende al menos un procesador (310) y al menos una memoria (320) que incluye código de programa informático, la al menos una memoria y el código de programa informático configurados para, con el al menos un procesador, provocar que un aparato, por ejemplo, el aparato 300 al menos realice y/o controle el método de acuerdo con aspectos ilustrativos de la invención.

El procesador 310 puede comprender, por ejemplo, un determinador de nivel de confianza 311 como una unidad funcional y/o estructural. El determinador de nivel de confianza 311 puede estar configurado, por ejemplo, para determinar un nivel de confianza (véase la etapa 202 de la Figura 2). El procesador 310 puede controlar adicionalmente, por ejemplo, las memorias 320 a 340, la interfaz o interfaces de comunicación 350, la interfaz de usuario opcional 360 y el sensor o sensores opcionales 370.

El procesador 310 puede ejecutar, por ejemplo, código de programa informático almacenado en la memoria de programa 320, que puede representar, por ejemplo, un medio de almacenamiento legible por ordenador que comprende código de programa que, cuando se ejecuta por el procesador 310, provoca que el procesador 310 realice el método de acuerdo con el primer aspecto ilustrativo.

El procesador 310 (y también cualquier otro procesador mencionado en esta memoria descriptiva) puede ser un procesador de cualquier tipo adecuado. El procesador 310 puede comprender pero sin limitación uno o más microprocesador o microprocesadores, uno o más procesador o procesadores con uno o más procesador o procesadores de señales digitales adjuntos, uno o más chips de ordenador de fin especial, una o más matriz o matrices de puertas programables en campo (FPGA), uno o más controlador o controladores, uno o más circuito o circuitos integrados

específicos de aplicación (ASIC), o uno o más ordenador u ordenadores. La estructura/hardware pertinente se ha programado de tal forma para efectuar la función descrita. El procesador 310 puede ser, por ejemplo, un procesador de aplicación que ejecuta un sistema operativo.

- 5 La memoria de programa 320 también puede incluirse en el procesador 310. Esta memoria puede conectarse de forma fija, por ejemplo, al procesador 310, o ser al menos parcialmente extraíble del procesador 310, por ejemplo, en forma de una tarjeta de memoria o memoria USB. La memoria de programa 320 puede ser, por ejemplo, una memoria no volátil. Puede ser, por ejemplo, una memoria flash (o una parte de la misma), cualquiera de una memoria ROM, PROM, EPROM y EEPROM (o una parte de la misma) o un disco duro (o una parte del mismo), por nombrar solo algunos ejemplos no limitantes. La memoria de programa 320 también puede comprender un sistema operativo para el procesador 310. La memoria de programa 320 también puede comprender un firmware para el aparato 300.

- 10 El aparato 300 comprende una memoria de funcionamiento 330, por ejemplo, en forma de una memoria volátil. Puede ser, por ejemplo, una memoria de acceso aleatorio (RAM) o RAM Dinámica (DRAM), por proporcionar solo algunos ejemplos no limitantes. Puede usarse, por ejemplo, por el procesador 310 cuando se ejecuta un sistema operativo y/o programa informático.

- La memoria de datos opcional 340 puede ser, por ejemplo, una memoria no volátil. Puede ser, por ejemplo, una memoria flash (o una parte de la misma), cualquiera de una memoria ROM, PROM, EPROM y EEPROM (o una parte de la misma) o un disco duro (o una parte del mismo), por nombrar solo algunos ejemplos no limitantes. La memoria de datos 340 puede almacenar, por ejemplo, una o más piezas de primera información de autenticación. Una o más piezas de primera información de autenticación pueden recopilarse, por ejemplo, por el sensor o sensores opcionales 370.

- 20 La interfaz o interfaces de comunicación 350 habilitan que el aparato 300 se comunique con otras entidades, por ejemplo, con el servidor 110 de la Figura 1. La interfaz o interfaces de comunicación 350 pueden comprender, por ejemplo, una interfaz inalámbrica, por ejemplo, una interfaz de comunicación de radio celular y/o una interfaz de WLAN) y/o interfaz por cable, por ejemplo, una interfaz basada en IP, por ejemplo, para comunicarse con entidades a través de la Internet. La interfaz o interfaces de comunicación pueden habilitar que el aparato 300 se comunique con otras entidades, por ejemplo, con el servidor 110 de la Figura 1.

- La interfaz de usuario 360 es opcional y puede comprender un visualizador para visualizar información a un usuario y/o un dispositivo de entrada (por ejemplo, un teclado, teclado numérico, panel táctil, ratón, etc.) para recibir información desde un usuario.

- 35 El sensor o sensores 370 son opcionales y pueden comprender, por ejemplo, un sensor de entrada (por ejemplo, para recopilar información de entrada de gesto, deslizamiento, escritura, toque y/o retención), acelerómetro y/o sensor de giroscopio (por ejemplo, para recopilar información de retención, giro y/o transporte), un sensor de cámara, un sensor de localización (por ejemplo, un sensor de GPS para recopilar, por ejemplo, una posición horizontal del dispositivo electrónico), o una combinación de los mismos por nombrar solo algunos ejemplos no limitantes. La información recopilada puede usarse, por ejemplo, como parámetros de autenticación inteligentes.

- Algunos o todos los componentes del aparato 300 pueden conectarse, por ejemplo, a través de un bus. Algunos o todos los componentes del aparato 300 pueden combinarse, por ejemplo, en uno o más módulos.

- 45 La Figura 4 muestra un diagrama de flujo que muestra una realización de ejemplo de un método adicional de acuerdo con el primer aspecto ilustrativo de la presente invención.

- La etapa 401 representa un estado inicial, en donde una aplicación (por ejemplo, la aplicación 131 de la Figura 1), por ejemplo, configurada para realizar y/o controlar el método de acuerdo con el primer aspecto ilustrativo de la presente invención, no está instalada en un dispositivo electrónico, por ejemplo, el dispositivo electrónico 130 de la Figura 1.

- En la etapa 402, la aplicación no instalada en el dispositivo electrónico (etapa 401) está ahora instalada en el dispositivo electrónico. La aplicación instalada no está activada, de modo que, por ejemplo, una petición para un servicio que requiere la autenticación del usuario no es posible en el estado presentado por la etapa 402. Por lo tanto, necesita activarse la aplicación. Esto puede hacerse, por ejemplo, enviando una carta impresa a una dirección conocida del usuario. La carta puede contener, por ejemplo, un código o similar, que el usuario puede introducir en el dispositivo electrónico como una correspondiente petición para introducir el código solicitado por la aplicación (por ejemplo, la aplicación 131 de la Figura 1) del dispositivo electrónico (por ejemplo, el dispositivo electrónico 130 de la Figura 1). Por lo tanto, puede efectuarse un proceso de activación de la aplicación. Pueden ser posibles procesos de activación adicionales de la aplicación, por ejemplo, un proceso de activación digital, por ejemplo, realizado durante o en la primera ejecución de la aplicación. El código contenido puede introducirse, por ejemplo, y la aplicación del dispositivo electrónico (por ejemplo, el dispositivo electrónico 130 de la Figura 1) puede transmitir, por ejemplo, la información a un servidor (por ejemplo, el servidor 110 de la Figura 1). El proceso de activación puede realizarse, por lo tanto, entre el dispositivo electrónico (por ejemplo, el dispositivo electrónico 130 de la Figura 1) y el servidor (por ejemplo, el servidor 110 de la Figura 1).

Después del proceso de activación, la aplicación está en un estado activado instalada en el dispositivo electrónico (etapa 403).

- 5 En la etapa 404, aún no se ha calibrado un nivel de confianza. Por lo tanto, puede determinarse, por ejemplo, al menos una información de calibración (por ejemplo, por el servidor 110 de la Figura 1) basándose, al menos en parte, en una o más piezas de primera información de autenticación. En el caso en el que la al menos una información de calibración puede no determinarse respectivamente determinable, la etapa 404 puede repetirse hasta que se determina la al menos una información de calibración, como se indica por la flecha trazada apuntando desde la etapa 404 a la etapa 404. Además, en el caso en el que la al menos una información de calibración no puede determinarse, por ejemplo, después de una pluralidad (por ejemplo, tres) de intentos no satisfactorios para determinar la al menos una información de calibración, puede continuarse con la etapa 402, como se indica por la flecha trazada apuntando desde la etapa 404 a 402. Adicionalmente, la al menos una información de calibración puede determinarse basándose en una o más piezas de segunda información de autenticación y/o una o más piezas de tercera información de autenticación. La al menos una información de calibración puede usarse, por ejemplo, para definir un umbral. Además, el umbral puede usarse, por ejemplo, como una base para un umbral de autenticación predefinido para la comprobación de un nivel de confianza determinado (etapas 408a o 408b).

- 20 La etapa 405 representa que el nivel de confianza está calibrado, por ejemplo, mediante el proceso de calibración anteriormente mencionado.

- La etapa 406 representa que la aplicación del dispositivo electrónico está en uso. Ya que el nivel de confianza puede ser, por ejemplo, como en esta realización descrita, una función dependiente del tiempo, un nivel de confianza determinado inicialmente disminuye con la expiración de tiempo. Esto representa una integridad restringida en tiempo de, por ejemplo, una o más piezas de primera información de autenticación, en función de las cuales se determina, al menos en parte, el nivel de confianza. Puede actualizarse, por ejemplo, un nivel de confianza disminuido (por ejemplo, por el servidor 110 de la Figura 1), por ejemplo, añadiendo un cierto valor al valor actual del nivel de confianza. Por ejemplo, un parámetro de actualización de confianza puede representar, por ejemplo, un cierto valor (por ejemplo, entre un intervalo de 0 a 100) a añadir al nivel de confianza. Además, un parámetro de actualización de confianza puede asociarse, por ejemplo, a uno o más ciertos eventos. Por ejemplo, un parámetro de actualización de confianza puede asociarse, por ejemplo, a una comprobación de un comportamiento del usuario. Pueden obtenerse, por ejemplo, uno o más parámetros de reconocimiento de comportamiento, por ejemplo, recopilados por uno o más sensores (por ejemplo, los sensores 132 de la Figura 1) del dispositivo electrónico (por ejemplo, el dispositivo electrónico 130 de la Figura 1) y pueden proporcionarse, por ejemplo, a un servidor (por ejemplo, el servidor 110 de la Figura 1). El uno o más parámetros de reconocimiento de comportamiento obtenidos, por ejemplo, pueden comprobarse (por ejemplo, por el servidor 110 de la Figura 1), por ejemplo, comparando los mismos con uno o más parámetros de reconocimiento de comportamiento ya obtenidos (por ejemplo, almacenados en una base de datos (por ejemplo, la base de datos 120 de la Figura 1)). En el caso en el que se reconozca una cierta similitud o identidad entre el uno o más parámetros obtenidos de comportamiento y los almacenados, puede añadirse, por ejemplo, una cierta cantidad de valor de nivel de confianza al nivel de confianza. Como alternativa o adicionalmente, un nivel de confianza disminuido, por ejemplo, puede actualizarse (por ejemplo, por el servidor 110 de la Figura 1), por ejemplo, determinando un valor nuevo del nivel de confianza de acuerdo con reglas predefinidas, por ejemplo, por un algoritmo. Por ejemplo, un parámetro de actualización de confianza puede asociarse, por ejemplo, a uno o más ciertos eventos. Por ejemplo, un parámetro de actualización de confianza puede asociarse, por ejemplo, a una comprobación de un comportamiento del usuario. Basándose en el comportamiento del usuario, puede determinarse, por ejemplo, un valor nuevo del nivel de confianza de acuerdo con reglas predefinidas, por ejemplo, un algoritmo. El valor nuevo del nivel de confianza puede aumentarse o disminuirse, por ejemplo, basándose en el resultado de la comprobación del comportamiento del usuario. Por ejemplo, el valor de nivel de confianza puede disminuirse en el caso en el que el comportamiento del usuario contrasta con el comportamiento observado habitualmente del usuario. El valor de nivel de confianza puede aumentarse, por ejemplo, en el caso en el que el comportamiento del usuario coincide con el comportamiento habitualmente observado del usuario. En contraste a la determinación del nivel de confianza, que se basa, al menos en parte, en la una o más piezas de primera información de autenticación (por ejemplo, que comprende uno o más parámetros de comportamiento), la comprobación de comportamiento se reduce a comprobar parámetros específicos de los parámetros de autenticación inteligentes. De esta manera, puede mejorarse, por ejemplo, la eficiencia (por ejemplo, consumo de energía, tráfico de volumen de datos por nombrar solo algunos ejemplos no limitantes). Como alternativa o adicionalmente, la actualización anteriormente mencionada del nivel de confianza puede realizarse, por ejemplo, (por ejemplo, por el servidor 110 de la Figura 1) usando en particular otros parámetros de autenticación inteligentes que comprenden uno o más de los siguientes: (i) uno o más parámetros de reconocimiento de comportamiento; (ii) uno o más parámetros de reconocimiento facial; (iii) uno o más parámetros de restricciones temporales; (iv) uno o más parámetros de restricciones locales; (v) o una combinación de los mismos.

- 65 La actualización del nivel de confianza puede realizarse, por ejemplo, de forma continua (por ejemplo, en intervalos de tiempo predefinidos, o basándose en ciertos eventos, por nombrar solo algunos ejemplos no limitantes) y/o a demanda (por ejemplo, basándose en una petición por el usuario, por ejemplo, la petición introducida en el dispositivo electrónico por el usuario).

En la etapa 407, un usuario ha solicitado un servicio (por ejemplo, desde un servidor de un proveedor de servicios) que requiere una autenticación (por ejemplo, una transacción para transferir dinero). Pueden obtenerse, por ejemplo, una o más nuevas piezas de primera información de autenticación (por ejemplo, recopiladas por el dispositivo electrónico 130 de la Figura 1, o adicionalmente o como alternativa obtenidas, por ejemplo, por el servidor 110 de la Figura 1), en el caso en el que el nivel de confianza determinado haya caído por debajo del umbral de autenticación. Adicionalmente, se determina un nivel de confianza (por ejemplo, por el servidor 110 de la Figura 1) basándose, al menos en parte, en la una o más piezas de primera información de autenticación.

En las etapas 408a y 408b, se comprueba el nivel de confianza (por ejemplo, por el servidor 110 de la Figura 1). Se comprueba si el nivel de confianza está por encima (etapa 408a) de un umbral predefinido (por ejemplo, determinado por el proceso de calibración como se ha descrito anteriormente) o no. En el caso en el que el nivel de confianza está por encima del umbral predefinido, se realiza la interacción de usuario solicitada (por ejemplo, la transacción). Por ejemplo, puede generarse, por ejemplo, ((por ejemplo, por el servidor 110 de la Figura 1) una información de autenticación indicativa de que el usuario se autentica satisfactoriamente o no. La información de autenticación generada puede proporcionarse, por ejemplo, desde, por ejemplo, el servidor 110 de la Figura 1 al dispositivo electrónico del usuario (por ejemplo, el dispositivo electrónico 130 de la Figura 1), que puede transmitir, por ejemplo, la información de autenticación al servidor del proveedor de servicios. Como alternativa, el servidor que generó la información de autenticación (por ejemplo, el servidor 110 de la Figura 1) puede proporcionar la información de autenticación al servidor del proveedor de servicios.

En el caso en el que el nivel de confianza está por debajo (etapa 408b) del umbral predefinido, puede realizarse una demanda para actualizar el nivel de confianza, por ejemplo, (por ejemplo, por el servidor 110 de la Figura 1) indicada por la etapa 409. Por ejemplo, puede realizarse una comprobación de comportamiento o comprobación de posición (como se ha descrito anteriormente). En el caso en el que la actualización del nivel de confianza es satisfactoria (por ejemplo, añadiendo un cierto valor al nivel de confianza de modo que la comparación del nivel de confianza con el umbral predefinido resulta en el nivel de confianza está por encima del umbral predefinido), se realiza la interacción de usuario solicitada (por ejemplo, la transacción). En el caso en el que, por ejemplo, falla la comprobación de comportamiento o comprobación de posición para actualizar los niveles de confianza (por ejemplo, el uno o más parámetros de reconocimiento de comportamiento obtenidos no coinciden con o no son similares a uno o más parámetros de reconocimiento de comportamiento prealmacenados indicativos del comportamiento individual del usuario), no se realiza la interacción de usuario solicitada (por ejemplo, la transacción). Además, la aplicación activada del dispositivo electrónico puede establecerse, por ejemplo, de vuelta a un estado no activado, por ejemplo, para evitar un uso fraudulento de la aplicación.

En la etapa 410, se finaliza la petición del usuario y la aplicación del dispositivo electrónico puede usarse, por ejemplo, para interacciones de usuario adicionales representadas por la flecha que apunta a la etapa 406.

La Figura 5 muestra un diagrama representado 500 de un nivel de confianza como una función dependiente del tiempo como se usa en una realización de ejemplo de un método de acuerdo con el primer aspecto ilustrativo de la presente invención. El eje x representa el tiempo, y el eje y representa el nivel de confianza.

El nivel de confianza representado en el diagrama 500 varía, por ejemplo, entre un intervalo de valores de 0 y 100. Por lo tanto, un valor de 0 puede representar que no hay ningún nivel de confianza asociado a la una o más primeras informaciones de autenticación. Un valor de 100 puede representar el nivel de confianza máximo asociado a la una o más primeras informaciones de autenticación.

El valor de la confianza se determina basándose, al menos en parte, en una o más piezas de primera información de autenticación. El valor del nivel de confianza puede determinarse, por ejemplo, durante varios puntos de tiempo. Adicionalmente o como alternativa, el valor del nivel de confianza puede determinarse, por ejemplo, de forma continua, por ejemplo, que la representación del nivel de confianza es constante.

El valor indicado con la etiqueta 'no activada' representa una aplicación no activada (por ejemplo, la aplicación 131 de la Figura 1) de un dispositivo electrónico (por ejemplo, el dispositivo electrónico 130 de la Figura 1) (véase la etapa 402 de la Figura 4). El valor de nivel de confianza puede ser, por ejemplo, 0. Después de que se activa la aplicación del dispositivo electrónico (por ejemplo, a través de un proceso de activación por una carta impresa; véase la etapa 403 de la Figura 4), se establece un nivel de confianza inicial. En el caso actual, el valor de nivel de confianza después del proceso de activación puede ser, por ejemplo, 100.

Ya que el nivel de confianza es una función dependiente del tiempo, el nivel de confianza determinado inicialmente disminuye con la expiración de tiempo, indicado con la etiqueta 'descenso de nivel de confianza'. Después del proceso de activación, el nivel de confianza disminuye, en el caso actual hasta que está por debajo de un umbral predefinido 510. Una tarea (por ejemplo, un servicio solicitado por un usuario que requiere una autenticación) puede efectuarse únicamente, por ejemplo, en el caso en el que el nivel de confianza determinado está por encima o es igual que el umbral predeterminado 510. En el caso en el que el nivel de confianza determinado es menor que el umbral predeterminado 510, la tarea puede no efectuarse, por ejemplo.

En el caso en el que la expiración de tiempo ha disminuido el nivel de confianza por debajo del umbral predefinido 510, puede ser necesario actualizar el nivel de confianza de modo que es posible que se efectúe una tarea solicitada por el usuario. Por ejemplo, la actualización del nivel de confianza puede realizarse por una comprobación de comportamiento, indicada por la etiqueta 'comprobación de comportamiento de actualización de confianza', y/o por una comprobación de posición (por ejemplo, comparando la ubicación horizontal actual obtenida, por ejemplo, por un sensor de GPS del dispositivo electrónico con una ubicación o área de ubicación almacenada en una base de datos (por ejemplo, la base de datos 120 de la Figura 1)), indicada por la etiqueta 'comprobación de posición de actualización de confianza'.

De esta manera, la autenticación es más segura ya que un nivel de confianza determinado puede, por ejemplo, no volverse más entero.

Las siguientes realizaciones de la presente invención también se considerarán divulgadas:

En realizaciones de la invención, la tecnología básica "Identidad de Plataforma Inteligente" es la base de todos los casos de uso. Una vez que las identidades del usuario se aseguran, protegen y prueban, todos los demás casos de uso pueden confiar en esta identidad segura. Se ofrecen diversos niveles de protección de identidad:

- Autenticación Multifactor Estándar.
- Autenticación Multifactor Inteligente.
- Autenticación Multifactor Dinámica.

Hoy la identidad de un usuario está protegida por diferentes factores para conseguir una Autenticación Multifactor Estándar:

- Tengo:
El usuario tiene el teléfono inteligente. La aplicación está vinculada a este teléfono inteligente especial a través de la activación de aplicación. La activación de aplicación se hace de acuerdo con la activación de AST estándar. Tanto el teléfono inteligente como la aplicación están protegidos contra amenazas.
- Sé:
El usuario tiene un pin para desbloquear el teléfono inteligente (mecanismo de desbloqueo estándar) y tiene un pin para usar la aplicación después de que se ha activado la aplicación. Se comprueba la aplicación contra el servidor de SSMS a través del canal de comunicación seguro.
- Soy:
Pueden usarse las huellas dactilares del usuario para identificar al usuario del teléfono inteligente. Las huellas dactilares pueden obtenerse, por ejemplo, por un sensor biométrico del teléfono inteligente. Este es un mecanismo de desbloqueo estándar de los teléfonos inteligentes del estado de la técnica.

En realizaciones de la presente invención, se proporciona autenticación multifactor estándar (así como todos los niveles de autenticación adicionales) en un dispositivo.

Ya que la protección de identidad se está volviendo cada vez más importante en el futuro, se necesitan mecanismos de protección adicionales. Existirán nuevos mecanismos para mejorar incluso más la autenticación multifactor básica. Por lo tanto, en realizaciones de la presente invención, la autenticación multifactor estándar se eleva a Autenticación Multifactor Inteligente que proporciona características adicionales para asegurar la identidad de un usuario.

La Autenticación Multifactor Inteligente es una forma estática de mejorar la seguridad de identidad. Los mecanismos "inteligentes" son:

- Reconocimiento de comportamiento:
Cada usuario tiene su propia forma de manejar su teléfono inteligente. Gestos, deslizamiento, escritura, toque, retención, giro y transporte del teléfono inteligente forman una huella "de comportamiento" única. Los componentes de esta huella de comportamiento se recopilan automáticamente mediante el uso los sensores internos del teléfono inteligente como sensores giroscópicos, sensores de pantalla táctil o por otros sensores de detección de movimiento. Todos los resultados de sensores se combinan para formar una huella digital única que representa la huella de comportamiento. Esta huella de comportamiento se almacena en un servidor (por ejemplo, un servidor de autenticación), que se actualiza y calibra constantemente. En producción, la huella de comportamiento actual (por ejemplo, obtenida) se verifica contra la huella almacenada.
- Reconocimiento acústico/sonido/voz:
El teléfono inteligente usa el micrófono interno del teléfono inteligente para grabar un sonido o una voz del usuario. Este sonido o voz se analiza para "reconocer" al usuario. Únicamente si se reconoce correctamente al usuario, se concede acceso a la aplicación y la funcionalidad estará disponible. Esta característica está protegida contra sonidos o voces falsos. La protección contra sonidos o voces falsos puede conseguirse, por ejemplo, mediante procesos de detección falsa basada en robot.
- Reconocimiento óptico/facial:
El teléfono inteligente usa la cámara interna del teléfono inteligente para hacer una fotografía o un vídeo del usuario. Esta fotografía o vídeo se analiza para "reconocer" al usuario. Únicamente si se reconoce correctamente al usuario,

se concede acceso a la aplicación y la funcionalidad estará disponible. Esta característica está protegida contra caras falsas en fotografías o vídeos. La protección contra caras falsas puede conseguirse, por ejemplo, mediante procesos de detección falsa basada en robot. Un robot de detección facial proporciona instrucciones aleatorias, por ejemplo, le dice al usuario que cierre el ojo izquierdo o derecho o que gire su cabeza a la izquierda o derecha. Si las instrucciones se efectúan correctamente, la cara es genuina y no un vídeo o una fotografía de una cara. Además de este reconocimiento facial lógico basado el robot, también existe una instancia de seguridad que es capaz de asegurar el tomar fotografías o vídeos. Esta característica se denomina "Fotografía segura".

- Restricciones temporales:

Basándose en la fecha y hora, un servidor (por ejemplo, el servidor de autenticación) decide si una identidad de un usuario es válida o no. Las reglas de estas restricciones se definen en el servidor.

Ejemplos

- las transacciones son válidas únicamente durante horas laborales de 9 - 5;
- las transacciones son válidas únicamente si el usuario no está de vacaciones;
- las transacciones son válidas únicamente con una fecha de inicio y fin definida.

- Restricciones locales:

La aplicación usa las características de detección de posición del teléfono inteligente como gps, wlan, zona horaria, proveedor, etc. para detectar la ubicación actual del teléfono inteligente. Para proteger la ubicación establecida contra manipulación por piratas informáticos, se combinan todas las características de detección de posición disponibles (y el respectivo historial de ubicaciones) y un algoritmo calcula el riesgo de una manipulación. De acuerdo con este riesgo, la aplicación y un servidor (por ejemplo, el servidor de autenticación) pueden decidir si una ubicación del teléfono inteligente es válida o no. Esto se denomina "Ubicación segura".

Ejemplos:

- las transacciones son válidas únicamente dentro/fuera de un país particular;
- las transacciones son válidas únicamente en el domicilio del usuario.

En realizaciones de la invención, todos los mecanismos pueden tener que calibrarse antes de que puedan usarse para identificar al usuario. Después de haber instalado la aplicación en el dispositivo (por ejemplo, el teléfono inteligente), el usuario tiene que activar la aplicación. La activación de la aplicación (por ejemplo, mediante una carta de activación a través de un correo registrado) conduce a un nivel de confianza inicial. Después de iniciar sesión en la aplicación, los mecanismos de Autenticación Multifactor Inteligente tienen que calibrarse. Los datos de calibración se almacenan en un servidor (por ejemplo, el servidor de autenticación). Cada vez que se solicita un mecanismo de Autenticación Multifactor Inteligente, la aplicación tiene que proporcionar los respectivos datos (gestos/escritura, fotografía, información de ubicación, zonas horarias). El servidor verifica los datos actuales con los datos calibrados y calcula la coincidencia: este valor es un valor entre 0 y 100 y se denomina nivel de confianza.

Definición de nivel de confianza:

El nivel de confianza es un valor abstracto de 0 a 100 que indica el nivel de confianza. Un nivel de confianza de 100 indica una identificación perfecta de un usuario y, por lo tanto, una confianza total. Un nivel de 0 indica una desconfianza total. De acuerdo con el nivel de confianza, la aplicación y el servidor pueden decidir si se efectúan o no las tareas o qué cantidad de dinero está disponible para transacciones. Los niveles de confianza pueden adaptarse (también dinámicamente) de acuerdo con los casos de uso y riesgos esperados.

Ejemplo para un escenario financiero:

- nivel de confianza 0 - 30: no se permiten transacciones;
- nivel de confianza 31- 60: únicamente se permiten transacciones no financieras (por ejemplo, conseguir saldos de cuentas bancarias);
- nivel de confianza 61- 90: se permiten transacciones no financieras y transacciones financieras hasta 1000 €;
- nivel de confianza 91- 100: se permiten transacciones ilimitadas.

"Reconocimiento facial" de ejemplo:

Un reconocimiento facial no es ni "verdadero" ni "falso". El resultado de un reconocimiento facial es un valor entre 0 y 100. El valor 0 indica que definitivamente no se reconoce la cara, el valor 100 declara que se reconoce la cara sin ninguna duda. Las mismas métricas se aplican a todas las demás características. Las características que implican una cierta cantidad de calibración y aprendizaje (como reconocimiento facial y de comportamiento) estarán disponibles únicamente después de que se haga la curva de aprendizaje.

Por supuesto, pueden combinarse todas las características de Autenticación Multifactor Inteligente. Por ejemplo, las

transacciones son válidas únicamente si se desencadenan dentro de una ubicación geográfica particular y dentro de un periodo dado y los datos de comportamiento deberían haberse actualizado dentro de un cierto tiempo.

Las piezas de datos para la Autenticación Multifactor Inteligente se adquieren o bien por una aplicación de adquisición especial o por una aplicación de usuario final.

La Autenticación Multifactor Dinámica es un enfoque dinámico para mejorar la seguridad de identidad aún más. Esto se hace mediante los siguientes mecanismos:

- Actualización de confianza dinámica:

En un escenario dinámico, el nivel de confianza es una función de tiempo. Esto significa que los niveles de confianza disminuyen a medida que pasa el tiempo. Cuanto más tiempo no se verifique un mecanismo, menor será el valor que tiene para identificar al usuario. Una actualización de confianza aumenta el nivel de confianza de nuevo, de acuerdo con el nivel de seguridad de la respectiva actualización.

La actualización del nivel de confianza puede, por ejemplo, hacerse de dos formas:

- Explorando constantemente al usuario, por ejemplo, comportamiento del usuario, la ubicación actual, la hora del dispositivo o una combinación de los mismos; y/o
- A demanda, que significa que el nivel de confianza cae por debajo de un umbral de nivel de confianza mínimo y la aplicación solicita una actualización de confianza.

- Referencias de confianza dinámicas:

El nivel de confianza de cada usuario puede definirse mediante mecanismos de confianza internos (véase lo anterior) o mediante autoridades de confianza externas. Las autoridades de confianza externas proporcionan un nivel de confianza para cada identidad que también puede usarse internamente. La referencia a autoridades de confianza externas puede hacerse dinámicamente, o bien periódicamente o bien a demanda.

Referencias de confianza de ejemplo son:

- activaciones de cartas (los usuarios responden a cartas de activación físicas enviadas a través de correo ordinario, las respuestas se almacenan en un sistema de CRM (Gestión de Relaciones con Clientes) interno).
- proveedores de identidad de terceros (por ejemplo, a través de SAML). Únicamente se pasa información no crítica a los proveedores de terceros.
- Cualquier otra fuente de datos en el extremo final.

En la presente memoria descriptiva, cualquier conexión presentada en las realizaciones descritas se entenderá en una forma que los componentes implicados se acoplan operacionalmente. Por lo tanto, las conexiones pueden ser directas o indirectas con cualquier número o combinación de elementos intervinientes, y puede haber solamente una relación funcional entre los componentes.

Además, cualquiera de los métodos, procesos y acciones descritos o ilustrados en este documento puede implementarse usando instrucciones ejecutables en un procesador de fin general o fin especial y almacenadas en un medio de almacenamiento legible por ordenador (por ejemplo, disco, memoria o similar) a ejecutar por un procesador de este tipo. Referencias a un 'medio de almacenamiento legible por ordenador' debería entenderse para abarcar circuitos especializados tales como FPGA, ASIC, dispositivos de procesamiento de señales y otros dispositivos.

La expresión "A y/o B" se considera que comprende uno cualquiera de los siguientes tres escenarios: (i) A, (ii) B, (iii) A y B. Adicionalmente, el artículo "un" o "una" no debe entenderse como "uno" o "una", es decir, el uso de la expresión "un elemento" no excluye que también estén presentes elementos adicionales. La expresión "que comprende" debe entenderse en un sentido abierto, es decir, de una forma que un objeto que "comprende un elemento A" también puede comprender elementos adicionales además del elemento A.

Se entenderá que todas las realizaciones presentadas son únicamente ilustrativas, y que cualquier característica presentada para una realización de ejemplo particular puede usarse con cualquier aspecto de la invención por sí misma o en combinación con cualquier característica presentada para la misma u otra realización de ejemplo particular y/o en combinación con cualquier otra característica no mencionada. En particular, las realizaciones de ejemplo presentadas en esta memoria descriptiva también se entenderán que se divulgan en todas las posibles combinaciones entre sí, en la medida en que sea técnicamente razonable y las realizaciones de ejemplo no son alternativas entre sí. Se entenderá adicionalmente que cualquier característica presentada para una realización de ejemplo en una categoría particular (método/aparato/programa informático/sistema) también puede usarse de una manera correspondiente en una realización de ejemplo de cualquier otra categoría. También debería entenderse que la presencia de una característica en las realizaciones de ejemplo presentadas no significará necesariamente que esta

característica forma una característica esencial de la invención y no puede omitirse o sustituirse.

La indicación de que una característica comprende al menos una de las características enumeradas posteriormente no es obligatoria en el sentido en que la característica comprende todas las características enumeradas posteriormente, o al menos una característica de la pluralidad de las características enumeradas posteriormente. También, es posible una selección de las características enumeradas en cualquier combinación o una selección de únicamente una de las características enumeradas. También puede considerarse la combinación específica de todas las características enumeradas posteriormente. También, puede ser posible una pluralidad de únicamente una de las características enumeradas.

La secuencia de todas las etapas de método presentadas anteriormente no es obligatoria, también pueden ser posibles secuencias alternativas. Sin embargo, la secuencia específica de etapas de método mostradas ilustrativamente en las figuras se considerará como una secuencia posible de etapas de método para la respectiva realización descrita por la respectiva figura.

La invención se ha descrito anteriormente por medio de realizaciones de ejemplo. Debería observarse que existen formas alternativas y variaciones que son obvias para un experto en la materia y pueden implementarse sin desviarse del alcance de las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un método, que comprende:

- 5 - obtener una o más piezas de primera información de autenticación, en donde la una o más piezas de primera información de autenticación representan al menos una pieza de información única asociada a un usuario y/o un dispositivo electrónico del usuario;
 - obtener una o más piezas de segunda información de autenticación, en donde la una o más piezas de segunda información de autenticación comprenden:
10 uno o más parámetros de actualización de confianza, en donde el uno o más parámetros de actualización de confianza son indicativos de un valor de nivel de confianza, en donde el uno o más parámetros de actualización de confianza se determinan basándose, al menos en parte, en la una o más piezas de primera información de autenticación,
15 en donde el parámetro de actualización de confianza se asocia a una comprobación de un comportamiento de un usuario; y/o
 uno o más parámetros de referencia de confianza, en donde el uno o más parámetros de referencia de confianza son indicativos de un valor de nivel de confianza asociado a una autoridad de confianza externa; y
20 - determinar un nivel de confianza basándose, al menos en parte, en la una o más piezas de primera información de autenticación, en donde el valor de nivel de confianza es indicativo de un nivel de confianza en la una o más piezas de primera información de autenticación,
 en donde el nivel de confianza se determina adicionalmente basándose, al menos en parte, en la una o más piezas de segunda información de autenticación.
25 2. El método de acuerdo con la reivindicación 1, en donde el nivel de confianza puede adoptar más de dos valores.
 3. El método de acuerdo con la reivindicación 1 o la reivindicación 2, que comprende adicionalmente:
30 - comprobar el nivel de confianza, en donde el nivel de confianza se comprueba basándose, al menos en parte, en una comparación del nivel de confianza con un umbral de comprobación predefinido.
 4. El método de acuerdo con cualquiera de las reivindicaciones anteriores, en donde el nivel de confianza se varía basándose al menos parcialmente en una función dependiente del tiempo, en donde el nivel de confianza disminuye con el transcurso del tiempo.
35 5. El método de acuerdo con la reivindicación 4, en donde la función dependiente del tiempo define el descenso del nivel de confianza.
40 6. El método de acuerdo con la reivindicación 4 o la reivindicación 5, en donde las etapas de obtención de una o más piezas de primera información de autenticación y de determinación de un nivel de confianza se repiten para obtener un nivel de confianza actualizado en el caso en el que el nivel de confianza haya caído por debajo de un umbral de autenticación predefinido.
45 7. El método de acuerdo con cualquiera de las reivindicaciones anteriores, en donde la una o más piezas de primera información de autenticación comprenden uno o más de los siguientes tipos i) a v) de parámetros:
50 i) uno o más parámetros de reconocimiento de comportamiento;
 ii) uno o más parámetros de reconocimiento acústico;
 iii) uno o más parámetros de reconocimiento óptico;
 iv) uno o más parámetros de restricciones temporales;
 v) uno o más parámetros de restricciones locales.
55 8. El método de acuerdo con la reivindicación 7, en donde el nivel de confianza se determina basándose, al menos en parte, en al menos dos tipos diferentes de los tipos i) a v) de parámetros comprendidos por la una o más piezas de primera información de autenticación.
60 9. El método de acuerdo con la reivindicación 7 o la reivindicación 8, en donde el uno o más parámetros de reconocimiento de comportamiento se obtienen durante un periodo de tiempo, que se predefine o determina de acuerdo con una regla predefinida.
 10. El método de acuerdo con cualquiera de las reivindicaciones 7 a 9, en donde el uno o más parámetros de reconocimiento de comportamiento se obtienen más de una vez.
65 11. El método de cualquiera de las reivindicaciones 7 a 10, en donde el uno o más parámetros de comportamiento se

obtienen basándose, al menos en parte, en una combinación con uno o más parámetros de reconocimiento de comportamiento obtenidos en un momento anterior.

12. El método de acuerdo con cualquiera de las reivindicaciones anteriores, que comprende adicionalmente:

- obtener una o más piezas de tercera información de autenticación, en donde la una o más piezas de tercera información de autenticación son indicativas, al menos en parte, de uno o más de los siguientes:

- (i) uno o más parámetros de propiedad;
- (ii) uno o más parámetros de conocimiento;
- (iii) uno o más parámetros biométricos;

en donde el nivel de confianza se determina, al menos en parte, en la una o más piezas de tercera información de autenticación.

13. El método de acuerdo con cualquiera de las reivindicaciones anteriores, que comprende adicionalmente:

- determinar al menos una información de calibración basándose, al menos en parte, en la una o más piezas de primera información de autenticación y/o basándose, al menos en parte, en la una o más piezas de segunda información de autenticación, en donde la al menos una información de calibración se usa para definir un umbral.

14. El método de acuerdo con la reivindicación 13, en donde el umbral de autenticación y/o el umbral de comprobación se establece basándose, al menos en parte, en la al menos una información de calibración.

15. Un aparato o un sistema que comprenden varios aparatos configurados para realizar y/o controlar o que comprenden respectivos medios para realizar y/o controlar el método de cualquiera de las reivindicaciones 1 a 14.

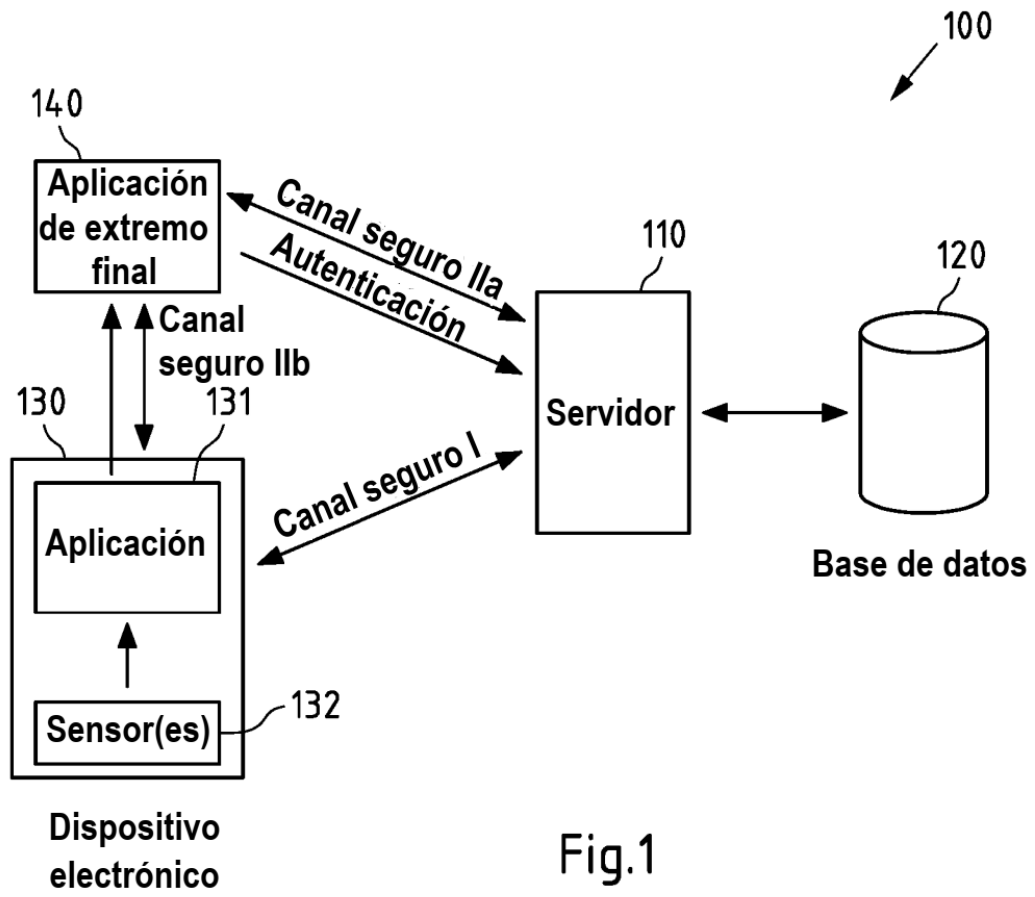
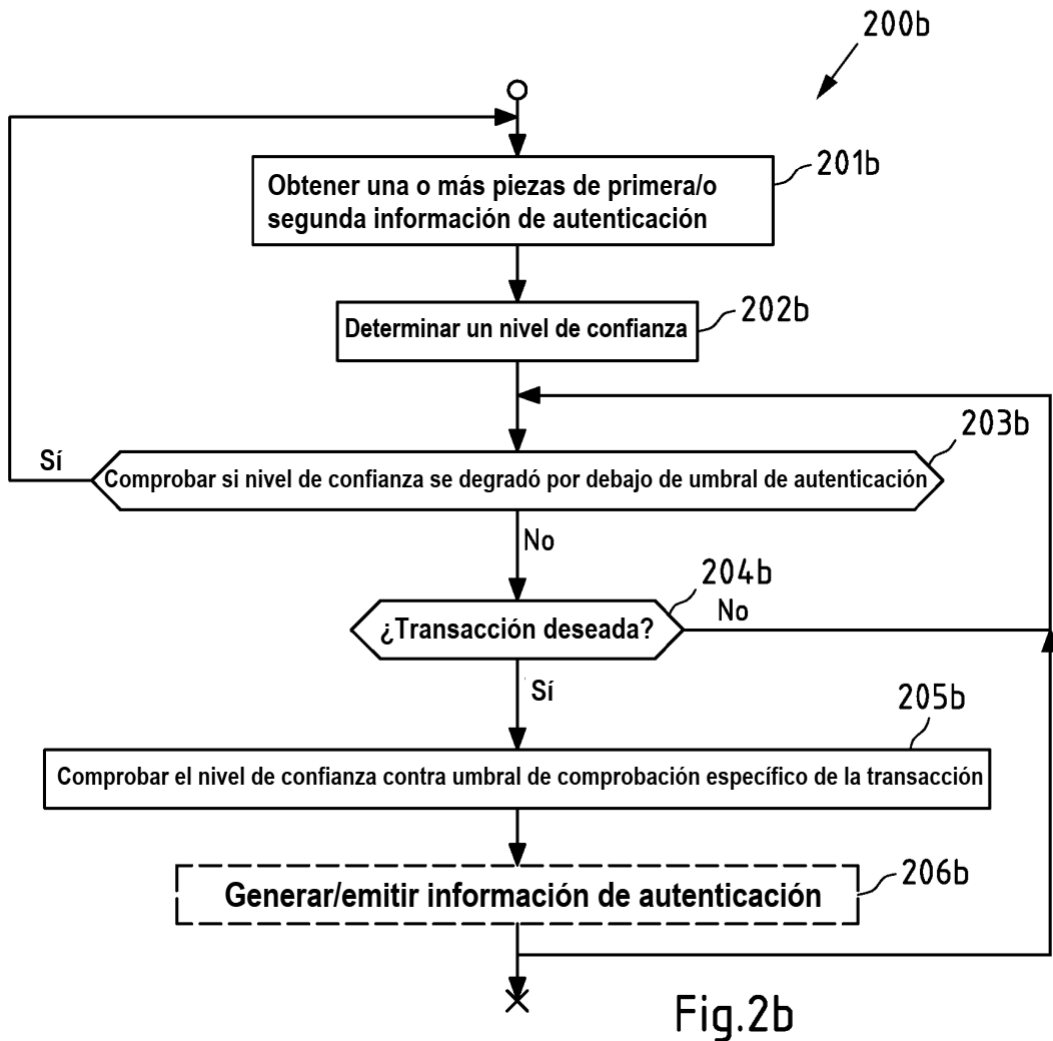
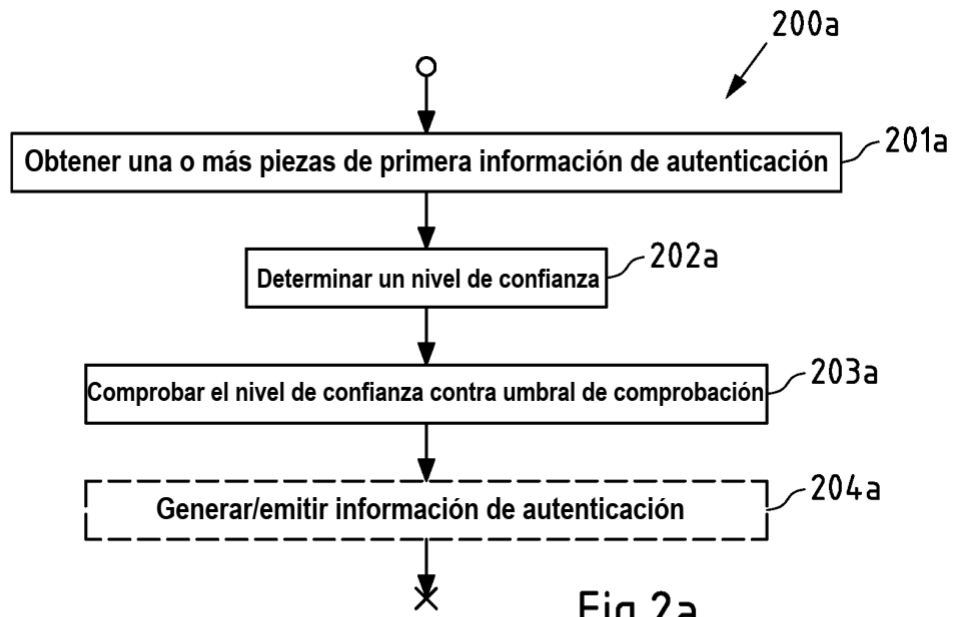


Fig.1



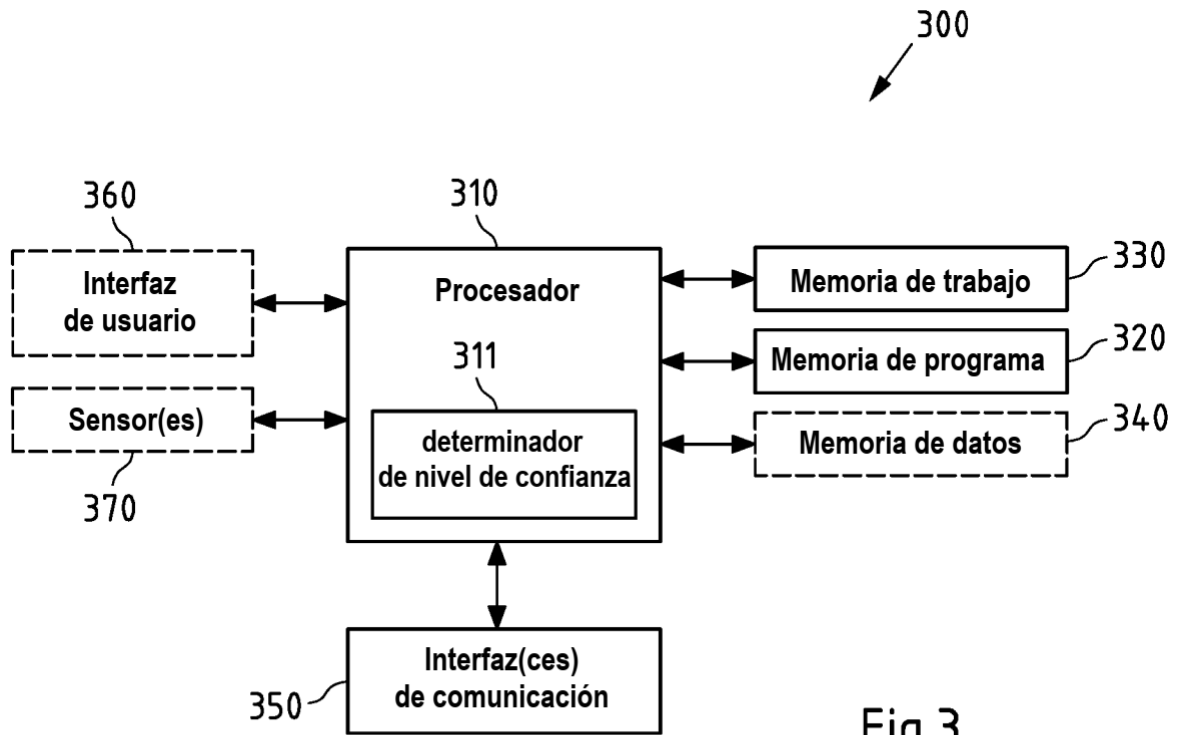
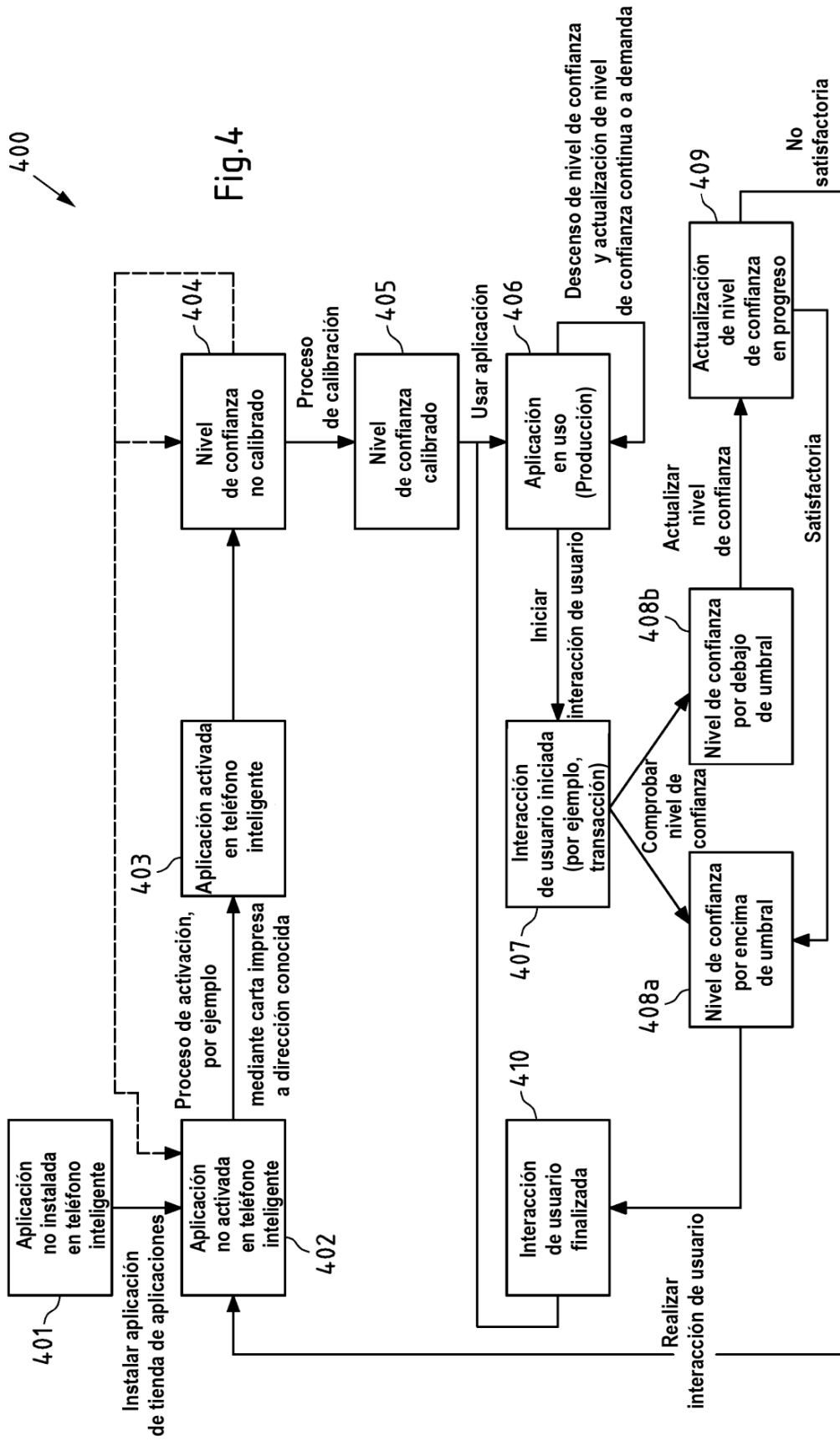


Fig.3



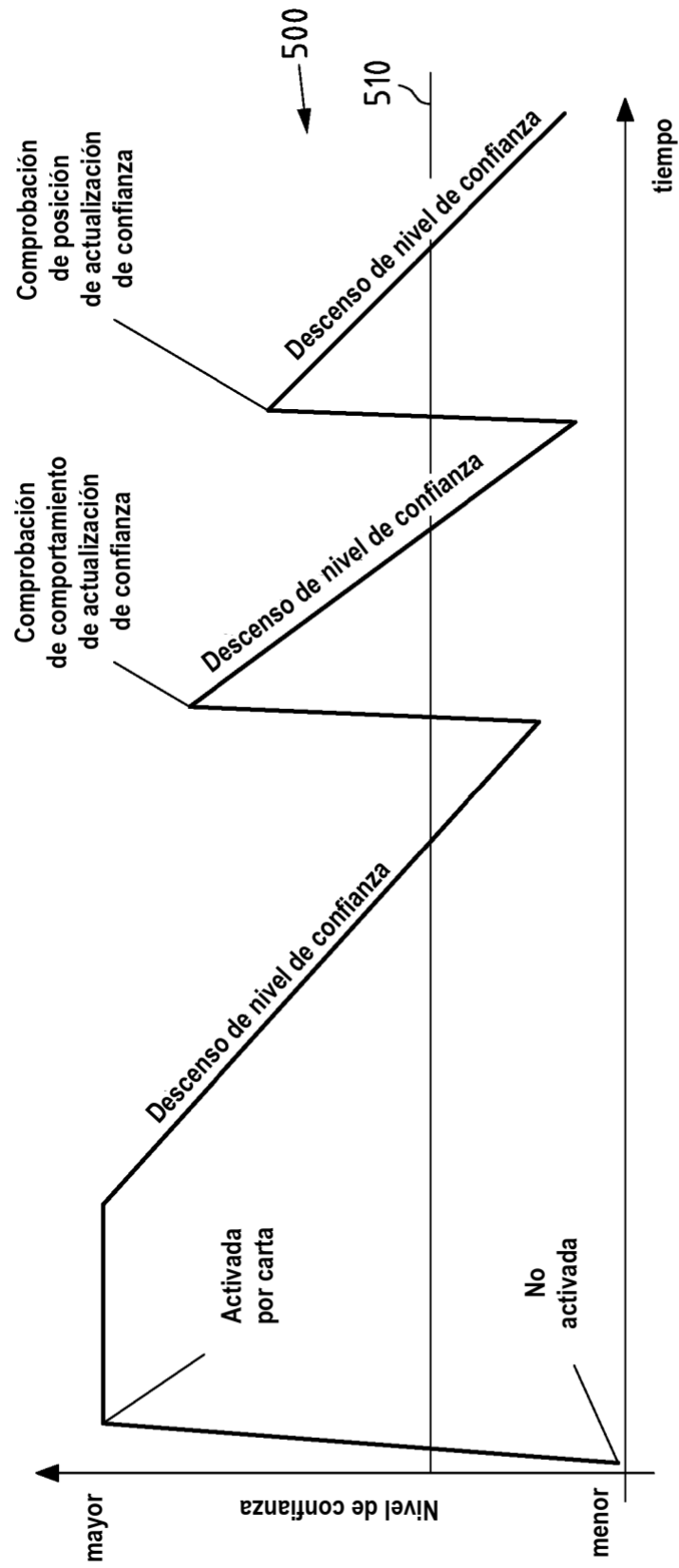


Fig.5