(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 742 673**

(51) Int. CI.:

G06F 21/32 (2013.01)
G06F 21/33 (2013.01)
G06F 21/41 (2013.01)
G06F 21/45 (2013.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **01.07.2014 E 14175310 (3)**

(97) Fecha y número de publicación de la concesión europea: **22.05.2019 EP 2821931**

(54) Título: **Aplicación de verificación, método, dispositivo electrónico y programa informático**

(30) Prioridad:

02.07.2013 SE 1350821

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
17.02.2020

(73) Titular/es:

PRECISE BIOMETRICS AB (100.0%)
Mobilvägen 10
223 62 Lund, SE

(72) Inventor/es:

ÖSTERLUND, PETTER y
HJALMARSSON, HENRIK

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Aplicación de verificación, método, dispositivo electrónico y programa informático

Campo técnico

La presente invención se refiere, en general, a una aplicación de verificación dispuesta para interactuar con otras aplicaciones en un dispositivo electrónico, un dispositivo electrónico de este tipo, un método y un programa informático.

Antecedentes

Los dispositivos electrónicos con capacidad de procesamiento, donde las aplicaciones pueden descargarse y usarse, proporcionan una gran versatilidad del dispositivo a su usuario. Algunas de las aplicaciones necesitan o necesitarían alguna forma de autenticar al usuario, por ejemplo, para garantizar la integridad u otros valores. Algunas aplicaciones tienen tales disposiciones. Sin embargo, un usuario que tiene una multitud de aplicaciones descargadas en su dispositivo electrónico puede enfrentar una multitud correspondiente de soluciones de seguridad y todas sus diferentes formas de interactuar con el usuario.

Un sistema operativo del dispositivo electrónico puede proporcionar algunas soluciones de seguridad agregada.

Sin embargo, se ha demostrado que el diseño de soluciones de seguridad integradas en el sistema operativo que soporte la evolución del mercado de las aplicaciones es una tarea que rara vez mantiene el ritmo con el desarrollo de aplicaciones.

Se han sugerido otros enfoques. El documento WO 01/37067 A1 desvela un enfoque para un enlace seguro entre módulos de programa para que puedan autenticarse entre sí y proporcionar seguridad para el contenido digital al que acceden uno o más de los módulos. Al almacenar al menos una dirección de al menos una función de un primer módulo de programa en un archivo, llamando al segundo módulo de programa mediante el primer módulo de programa y pasando el archivo al segundo módulo de programa, verificando la integridad mediante el segundo módulo de programa del primer módulo de programa, y llamando mediante el segundo módulo de programa a una función seleccionada del primer módulo de programa usando una dirección obtenida a partir del archivo cuando se verifica la integridad del primer módulo de programa, puede proporcionarse un enlace seguro entre los módulos de programa primero y segundo. El enfoque se basa en una dirección de devolución de llamada dentro del módulo de programa a autenticar. Sin embargo, este enfoque puede no ser lo suficientemente versátil para el entorno en evolución indicado anteriormente, ya que se basa en un direccionamiento específico de la memoria.

Además, en el documento WO 2008/024454 A1 se desvela un método y aparato para la gestión de contraseñas y el acceso de inicio de sesión único (SSO) basado en la tecnología informática de confianza (TC). Además, en la presentación "Enabling SSO for native applications" de Paul Madsen, de la conferencia RSA 2013, se desvela un enfoque de SSO para aplicaciones nativas en un entorno móvil.

Por lo tanto, es un deseo de proporcionar una solución de seguridad mejorada para un entorno de aplicación.

Sumario

Un objeto de la invención es al menos aliviar el problema indicado anteriormente. La presente invención se basa en el entendimiento de que una aplicación que trabaja a nivel de pares con otras aplicaciones es adecuada para mantener el ritmo de la evolución de la aplicación. Los inventores se han dado cuenta de que la disposición de una aplicación para soluciones de seguridad que interactúe con otras aplicaciones a nivel de pares, es capaz de aliviar el problema mencionado anteriormente.

De acuerdo con un primer aspecto, se proporciona una aplicación de verificación dispuesta para interactuar con otras aplicaciones en un dispositivo electrónico, teniendo el dispositivo electrónico un procesador, una memoria y un sistema operativo que controlan la operación de la aplicación de verificación y las otras aplicaciones en el procesador usando localizaciones de memoria arbitrarias, donde las otras aplicaciones están habilitadas para llamar a la aplicación de verificación para determinar de manera segura la autenticidad de un usuario del dispositivo electrónico. La aplicación de verificación está dispuesta para recibir datos de verificación para la determinación segura de la autenticidad del usuario; y proporcionar, tras una llamada de cualquiera de las otras aplicaciones y una coincidencia entre los datos de verificación y una referencia de verificación, un testigo de confianza a la aplicación llamante.

La aplicación de verificación puede estar dispuesta para emparejarse con al menos una de las otras aplicaciones intercambiando recíprocamente al menos uno de entre la firma de aplicación, la clave o claves criptográficas, la contraseña, y un secreto compartido. La disposición del testigo de confianza solo puede proporcionarse cuando la aplicación de verificación y la una de las otras aplicaciones que proporcionan una llamada a la aplicación de

verificación están emparejadas correctamente.

El testigo de confianza puede comprender una información generada por un mecanismo criptográfico de la aplicación de verificación.

El testigo de confianza puede comprender cualquiera de entre una clave criptográfica, un secreto compartido, una identidad o datos asociados con un usuario, y una credencial de seguridad, almacenada por la aplicación de verificación.

Los parámetros para la generación del testigo de confianza pueden establecerse tras la instalación de la aplicación de verificación en el dispositivo electrónico y puede registrarse la referencia de verificación.

La llamada desde la una de las otras aplicaciones puede incluir un indicador en un grado de certeza necesaria en la coincidencia en la que la coincidencia entre los datos de verificación y la referencia de verificación puede considerarse presente si una tasa de aceptación falsa estimada por un mecanismo de coincidencia de la aplicación de verificación es menor que el grado de certeza necesaria en la coincidencia. El testigo de confianza puede incluir o acompañarse por un indicador de autenticidad, en el que el indicador de autenticidad puede basarse en la tasa de aceptación falsa estimada por el mecanismo de coincidencia.

La aplicación de verificación puede además estar dispuesta para proporcionar un indicador de confianza rota o no, si un grado de certeza necesaria en la autenticación para la coincidencia entre los datos de verificación recibidos y la referencia de verificación se restablece en un nivel de certeza más baja que antes del restablecimiento, la aplicación llamante no está emparejada correctamente con la aplicación de verificación, o una combinación de las mismas.

Recibir los datos de verificación puede comprender recibir una muestra biométrica, la referencia de verificación puede ser una referencia biométrica y la coincidencia entre los datos de verificación y la referencia de verificación puede realizarse por un mecanismo de coincidencia biométrica de la aplicación de verificación, en el que el mecanismo de coincidencia biométrica puede disponerse para hacer coincidir la muestra biométrica con la referencia biométrica.

De acuerdo con un segundo aspecto, se proporciona un método de una aplicación de verificación dispuesto para internet con otras aplicaciones en un dispositivo electrónico, teniendo el dispositivo electrónico un procesador, una memoria y un sistema operativo que controlan la operación de la aplicación de verificación y la otras aplicaciones en el procesador que usan localizaciones de memoria arbitrarias. El método comprende recibir una llamada a la aplicación de verificación desde una de las otras aplicaciones para determinar de manera segura la autenticidad de un usuario del dispositivo electrónico, recibir datos de verificación, autenticar los datos de verificación haciéndolos coincidir con una referencia de verificación almacenada por la aplicación de verificación, y proporcionar, tras una coincidencia entre los datos de verificación y la referencia de verificación, un testigo de confianza a la aplicación llamante.

El método puede comprender emparejar la aplicación de verificación con al menos una de las otras aplicaciones intercambiando recíprocamente al menos una de entre la firma de aplicación, la clave criptográfica, y una contraseña. La disposición del testigo de confianza solo puede realizarse cuando la aplicación de verificación y la una de las otras aplicaciones que proporciona una llamada a la aplicación de verificación están emparejadas correctamente.

La disposición del testigo de confianza puede comprender generar una información mediante un mecanismo criptográfico de la aplicación de verificación.

La disposición del testigo de confianza puede comprender cualquiera de entre una clave criptográfica, un secreto compartido, una identidad o datos asociados con un usuario, y una credencial de seguridad almacenada por la aplicación de verificación.

El método puede comprender proporcionar un indicador de confianza rota o no, si el grado de certeza necesaria en la autenticación para la coincidencia entre los datos de verificación recibidos y la referencia de verificación se restablece en un nivel de certeza inferior, la aplicación llamante no está correctamente emparejada con la aplicación de verificación, o una combinación de las mismas.

El método puede comprender, tras la instalación de la aplicación de verificación en el dispositivo electrónico, establecer los parámetros para la generación del testigo de confianza, y registrar la referencia de verificación.

La llamada desde la una de las otras aplicaciones pueden incluir un indicador en un grado de certeza necesaria en la coincidencia en la que la coincidencia entre los datos de verificación y la referencia de verificación puede considerarse presente si una tasa de aceptación falsa estimada por la coincidencia es menor que el grado de certeza necesaria. El testigo de confianza puede incluir o acompañarse por un indicador de autenticidad, en el que el indicador de autenticidad puede basarse en la tasa de aceptación falsa estimada por la coincidencia.

La recepción de los datos de verificación puede comprender recibir una muestra biométrica, la referencia de verificación puede ser una referencia biométrica y la coincidencia entre los datos de verificación y la referencia de verificación puede realizarse comparando biométricamente la muestra biométrica con la referencia biométrica.

De acuerdo con un tercer aspecto, se proporciona un programa informático que comprende instrucciones ejecutables por ordenador que cuando son ejecutadas por un procesador de un dispositivo electrónico que tiene el procesador, una memoria y un sistema operativo controlan la operación de las aplicaciones en el procesador usando localizaciones de memoria arbitrarias, en el que la instrucción ejecutable por un ordenador provoca que el procesador realice el método del segundo aspecto.

De acuerdo con un cuarto aspecto, se proporciona un dispositivo electrónico que tiene un procesador, una memoria y un sistema operativo, que comprende una aplicación de verificación de acuerdo con el primer aspecto, al menos una otra aplicación habilitada para llamar a la aplicación de verificación para determinar de manera segura la autenticidad de un usuario del dispositivo electrónico, y una entrada de datos de verificación dispuesta para proporcionar datos de verificación a la aplicación de verificación, en el que el sistema operativo está dispuesto para controlar la operación de la aplicación de verificación y las otras aplicaciones en el procesador usando localizaciones de memoria arbitrarias.

La entrada de datos de verificación puede comprender un lector biométrico dispuesto para proporcionar muestras biométricas como los datos de verificación, y la aplicación de verificación está de acuerdo con los correspondientes del primer aspecto.

Otros objetivos, características y ventajas de la presente invención aparecerán a partir de la siguiente divulgación detallada de las reivindicaciones dependientes adjuntas así como a partir de los dibujos. En general, todos los términos usados en las reivindicaciones deben interpretarse de acuerdo con su significado ordinario en el campo técnico, a menos que se defina explícitamente lo contrario en el presente documento. Todas las referencias a "un/una/el/la [elemento, dispositivo, componente, medio, etapa, etc.]" deben interpretarse abiertamente como que hacen referencia a al menos una instancia de dicho elemento, dispositivo, componente, medio, etapa, etc. a menos que se indique explícitamente lo contrario. Las etapas de cualquier método desvelado en el presente documento no tienen que realizarse en el orden exacto desvelado, a menos que se indique explícitamente.

Breve descripción de los dibujos

Lo anterior, así como objetos, características y ventajas adicionales de la presente invención, se comprenderán mejor a través de la siguiente descripción detallada ilustrativa y no limitativa de las realizaciones preferidas de la presente invención, haciendo referencia a los dibujos adjuntos.

La figura 1 ilustra esquemáticamente un dispositivo electrónico de acuerdo con una realización.
La figura 2 es un esquema de señal que ilustra funciones de acuerdo con las realizaciones.
La figura 3 es un diagrama de flujo que ilustra métodos de acuerdo con las realizaciones.
La figura 4 es un esquema de señal que ilustra funciones de acuerdo con las realizaciones, en particular cuando una aplicación de verificación se reinstala sin emparejamiento.
La figura 5 es un esquema de señal que ilustra funciones de acuerdo con las realizaciones, en particular cuando una aplicación de verificación sirve a múltiples otras aplicaciones con diferentes demandas de certeza.
La figura 6 es un esquema de señal que ilustra funciones de acuerdo con las realizaciones, en particular cuando se agregan referencias de verificación sin la confianza adecuada.
La figura 7 es un esquema de señal que ilustra funciones de acuerdo con las realizaciones, en particular cuando el nivel de certeza ha cambiado.
La figura 8 es un esquema de señal que ilustra funciones de acuerdo con las realizaciones, en particular cuando otras aplicaciones correctamente emparejadas y no emparejadas operan con la aplicación de verificación.
La figura 9 ilustra esquemáticamente un medio legible por ordenador que contiene un programa informático para implementar la aplicación de verificación, y un procesador dispuesto para ejecutar la aplicación de verificación.

Descripción detallada

La figura 1 ilustra esquemáticamente un dispositivo electrónico 100 de acuerdo con una realización. El dispositivo electrónico comprende una entrada de datos de verificación 102, que por ejemplo puede ser un lector biométrico, una entrada para código de autenticación o contraseña, y/o un lector de tarjeta inteligente. El dispositivo electrónico 100 también comprende un procesador 104 y una memoria 106. El procesador 104 está dispuesto para ejecutar un sistema operativo 108 que a su vez es una recopilación de software que gestiona los recursos de hardware informático y proporciona servicios comunes para programas informáticos. Entre los programas informáticos, hay una aplicación de verificación 110 y una o más otras aplicaciones 112. En este contexto, las aplicaciones son mecanismos implementados por software que provocan que un dispositivo electrónico con un procesador realice tareas útiles más allá del funcionamiento del dispositivo o procesador electrónico en sí mismo, es decir, realiza tareas que benefician directamente a un usuario. La aplicación de verificación 110 se empareja con una o más de

las otras aplicaciones 112 para establecer una confianza entre la aplicación de verificación 110 y la otra aplicación respectiva 112. A continuación, una aplicación 112 puede llamar a la aplicación de verificación 110 para verificar si un usuario correcto está autenticado, y si la autenticación está en su lugar y se establece la confianza, la aplicación llamante 112 obtendrá un testigo de confianza de vuelta pudiendo la aplicación llamante continuar su tarea con cierta confianza de que el usuario correcto es el que maneja el dispositivo electrónico 100. La aplicación de verificación 110 está dispuesta a su vez para autenticar al usuario. Esto se realiza, por ejemplo, al requerir que el usuario presente un código de autenticación, contraseña, muestra biométrica y/o testigo de hardware a través de la entrada de datos de verificación 102. La aplicación de verificación 110 verifica la autenticidad del usuario haciendo coincidir los datos de entrada en la entrada de datos de verificación 102 con un conjunto de datos almacenados, por ejemplo, haciendo coincidir una muestra biométrica con una plantilla biométrica almacenada, verificado los datos de un testigo de hardware que se ha asimilado de acuerdo con un algoritmo criptográfico y/o comparando una contraseña de entrada con una contraseña almacenada o una contraseña de un solo uso sincronizada en el tiempo. El sistema operativo 108 puede tratar la aplicación de verificación 110 como cualquier aplicación, es decir, la aplicación de verificación puede usarse en localizaciones de memoria arbitrarias y no tiene que manejarse en ciertas áreas de memoria segura. El dispositivo electrónico 100 puede ser, por ejemplo, un ordenador o un aparato de comunicación, o cualquier combinación de los mismos, tal como un teléfono móvil, un teléfono inteligente, una tableta, un ordenador portátil, etc. El dispositivo electrónico 100 también puede ser, por supuesto, un ordenador y/o un aparato de comunicación que es parte de una máquina, tal como una herramienta o máquina de taller, vehículo, máquina expendedora o de entretenimiento, instrumento de monitorización o medición, etc. El dispositivo electrónico 100 por supuesto, también puede ser cualquiera de los ejemplos dados anteriores junto con accesorios adecuados, tales como accesorios para la entrada de datos de verificación 102, posiblemente con algunas partes funcionales del procesador 104, que pueden distribuirse entre entidades.

La figura 2 es un esquema de señales que ilustra las funciones de acuerdo con las realizaciones. Se cree que un eje de tiempo va hacia abajo en la figura. La señalización se demuestra entre las dos entidades, la aplicación de verificación y otra aplicación, y también la entrada de datos de un usuario a la aplicación de verificación.

La parte superior del esquema de señalización ilustra la inscripción de una referencia de verificación del usuario y el emparejamiento de la aplicación de verificación y la otra aplicación. La inscripción de la referencia de verificación comprende el usuario que presenta los datos de verificación que más tarde se destinan a la autenticación. Como se ha tratado anteriormente, este puede ser un código de autenticación, una contraseña, una muestra biométrica y/o un testigo de hardware que se presenta por el usuario a través de la entrada de datos de verificación. La inscripción también puede comprender sincronizar la aplicación de verificación para contraseñas de un solo uso sincronizadas en el tiempo, el intercambio de secretos o claves compartidos, o similares. El emparejamiento de la aplicación de verificación y la otra aplicación puede comprender intercambiar recíprocamente al menos una firma de aplicación, una clave o claves criptográficas, una contraseña y un secreto compartido. La complejidad del emparejamiento puede depender del nivel de seguridad exigido por la otra aplicación. Una aplicación que incluye transacciones financieras puede, por ejemplo, exigir un nivel de seguridad más alto que una aplicación que solo proporciona actividades de diversión para el usuario (pero aun así exige la autenticación del usuario, por ejemplo, para registrar correctamente puntuaciones altas). El emparejamiento puede incluir, por ejemplo, verificar recíprocamente los certificados de las aplicaciones de emparejamiento y/o recibir la autenticación de las aplicaciones de emparejamiento por parte de un usuario o administrador, es decir, se "dice" a las aplicaciones que confíen entre sí. En este caso, el administrador puede ser, por ejemplo, un proveedor, operador o autoridad que ayuda al usuario a instalar las aplicaciones de manera segura y confiable. Cuando la verificación de los certificados y/o la autenticación de las aplicaciones son exitosas, las aplicaciones se consideran correctamente emparejadas.

La parte inferior del esquema de señalización ilustra la operación del aparato electrónico donde el usuario proporciona los datos de verificación para aplicar la verificación a través de la entrada de datos de verificación, como se ha tratado anteriormente, por ejemplo, cuando se inicia el manejo del dispositivo electrónico. La aplicación de verificación autentica al usuario, y en este ejemplo se supone que la autenticación es correcta. El usuario usa la otra aplicación, y la otra aplicación puede desear verificar en algún momento la autenticidad del usuario, por ejemplo, para realizar alguna transacción. A continuación, la otra aplicación llama a la aplicación de verificación, que sabe que la autenticidad del usuario es correcta. A continuación, la aplicación de verificación envía un testigo de confianza a la otra aplicación, que verifica el testigo de confianza y, por lo tanto, obtiene la afirmación de que el usuario correcto está manejando el dispositivo electrónico, o al menos en un cierto nivel de seguridad exigido. A continuación, la otra aplicación puede continuar con la tarea que ha requerido la verificación. Una ventaja es que el usuario solo necesita interactuar con una aplicación para la autenticación, lo que mejora tanto la usabilidad como la confianza desde una perspectiva de seguridad para el usuario. Otra ventaja es que la funcionalidad de autenticación y los problemas de la interfaz de usuario no tienen que implementarse en todas las aplicaciones.

La figura 3 es un diagrama de flujo que ilustra métodos de acuerdo con las realizaciones. Como se ha tratado anteriormente, los datos de verificación se reciben 310 por una aplicación de verificación de un usuario. Los datos de verificación se hacen coincidir 312 con la referencia de verificación respectiva cuando no coinciden, la acción puede ser para ignorar la entrada, solicitar un nuevo intento y/o elevar el nivel de seguridad, en función de la estrategia de autenticación, como es habitual en el campo. Tras recibir una llamada desde otra aplicación, la llamada se recibe 314, y se determina 316 si existe o no una confianza basándose en la coincidencia y se establece el emparejamiento

entre la aplicación llamante y la aplicación de verificación. Si se determina la confianza, se envía un testigo de confianza 318 a la aplicación llamante. Si hay algún problema con la confianza, puede enviarse 317 un mensaje al respecto a la aplicación llamante. Por ejemplo, si no hay un emparejamiento apropiado entre la aplicación de verificación y la aplicación llamante, el mensaje puede indicar que no hay confianza, o si se realiza el emparejamiento adecuado pero la coincidencia de los datos de verificación falla o muestra una certeza demasiado baja, el mensaje puede indicar una confianza rota. El mensaje sobre confianza/rota confianza/no confianza puede incluirse o agregarse 319 con un indicador de autenticidad que puede ser un indicador del nivel de confianza en la autenticidad. A continuación, el proceso puede volver a esperar otra llamada desde la aplicación llamante o desde otra aplicación.

Tras la iniciación de la aplicación de verificación, se registra 300 una referencia de verificación, como se ha tratado anteriormente. Tras la iniciación de la aplicación de verificación o al agregar una nueva aplicación para poder llamar a la aplicación de verificación, la aplicación de verificación se empareja 302 con la otra aplicación, es decir, las aplicaciones que son para llamar a la aplicación de verificación. Esto se realiza como se ha tratado anteriormente.

Una aplicación llamante puede incluir un indicador sobre la certeza solicitada de que el usuario correcto está manejando el aparato. A continuación, se extrae 315 el indicador y su valor se usa para determinar 316 la confianza. La aplicación de verificación puede guardar el indicador extraído para monitorizar si el nivel solicitado cambia repentinamente, por ejemplo, se reduce significativamente, lo que puede ser un signo de confianza rota y contar con la determinación 316 de la confianza. La certeza se estima preferentemente y la estimación puede basarse, por ejemplo, en cómo de bien coincide una muestra biométrica con una plantilla, y también la calidad de la plantilla y/o la complejidad de la coincidencia, pero también puede basarse en verificaciones agregadas, por ejemplo, una coincidencia biométrica agregada con una contraseña de un solo uso sincronizada en el tiempo o una contraseña convencional, o cualquier otra combinación de dos o más verificaciones como se ha tratado anteriormente. La certeza estimada puede expresarse como una tasa de aceptación falsa, FAR, es decir, la tasa de probabilidad de que un impostor logre ser aceptado, que puede expresarse, por ejemplo, como uno en un millón (1/1000000), lo que significa que el impostor puede ser aceptado una vez de un millón de intentos independientes. La función para la estimación agregada puede seleccionarse de diferentes maneras, por ejemplo, considerando cada verificación parcial como independiente entre sí y multiplicando simplemente las estimaciones o cálculos respectivos de las tasas de cada verificación parcial, por ejemplo, 1/1000 multiplicado por 1/10000 se convierte en 1/10000000, o usando algoritmos de agregación más complejos.

La figura 4 es un esquema de señales que ilustra las funciones de acuerdo con las realizaciones, en particular cuando una aplicación de verificación se vuelve a instalar sin emparejamiento. El mecanismo necesita estar a salvo de las puertas traseras en vista de la seguridad. Por lo tanto, si un usuario no autorizado intenta manipular el dispositivo desinstalando la aplicación de verificación y reinstalando una aplicación de verificación para poder acceder a algunas de las aplicaciones, por ejemplo, registrando una nueva referencia de verificación, la aplicación de verificación no podrá proporcionar una confianza adecuada para la aplicación llamante. La aplicación llamante se empareja con la aplicación de verificación instalada inicialmente y no aceptará un testigo de confianza procedente de la nueva aplicación de verificación, es decir, cualquier testigo de confianza de la nueva aplicación de verificación se interpretará como no confiable.

La figura 5 es un esquema de señales que ilustra las funciones de acuerdo con las realizaciones, en particular, cuando una aplicación de verificación sirve para múltiples otras aplicaciones con diferentes demandas de certeza. En esta figura, se supone que las aplicaciones y la aplicación de verificación están correctamente emparejadas. La aplicación de verificación recibe datos de verificación de un usuario. Los datos de verificación se hacen coincidir con la referencia de verificación, y la tasa de aceptación falsa, FAR, se estima en 1/1000, es decir, la probabilidad de que un usuario no autorizado haya logrado ser aceptado por el comparador es 1/1000. Véase también la exposición anterior sobre la estimación de FAR y la FAR agregada.

Una primera aplicación llama a la aplicación de verificación y la llamada incluye un indicador sobre el nivel necesario de certeza de 1/1000. Ya que se estima que se cumple ese nivel, se envía un testigo de confianza desde la aplicación de verificación a la primera aplicación. El testigo de confianza también puede incluir el valor FAR estimado. El valor FAR estimado puede expresar el FAR estimado directamente como, por ejemplo, 1/1000, o los diferentes niveles pueden codificarse de acuerdo con un esquema de nivel FAR con dos o más niveles. Preferentemente, los niveles son tres o más. Los niveles FAR pueden comunicarse como en la exposición siguiente sobre los niveles de certeza. Las aplicaciones emparejadas pueden, por ejemplo (por ejemplo, inherentemente) acordar un protocolo para las expresiones de las FAR y los niveles de certeza en su comunicación recíproca.

Una segunda aplicación llama a la aplicación de verificación y la llamada incluye un indicador sobre el nivel necesario de certeza de 1/10000. Ya que se estima que ese nivel no se cumple, se envía un mensaje de confianza rota desde la aplicación de verificación a la segunda aplicación. El mensaje de confianza rota también puede incluir el valor FAR estimado.

El usuario proporciona de nuevo datos de verificación, y esta vez, cuando los datos de verificación se comparan con la referencia de verificación, la FAR se estima en 1/100000. Tras recibir una nueva llamada de la segunda

aplicación, aún con un indicador en el nivel de certeza necesario de 1/10000, se envía un testigo de confianza desde la aplicación de verificación a la segunda aplicación, ya que se estima que se cumple ese nivel de certeza. En este caso, el indicador puede expresar el nivel de certeza directamente como, por ejemplo, 1/10000, o los diferentes niveles pueden codificarse de acuerdo con un esquema de nivel de certeza con dos o más niveles. Preferentemente, los niveles son tres o más. Por ejemplo, un nivel puede representar una certeza mejor que 1/1000000, otro nivel mejor que 1/10000, y otro nivel representa una certeza mejor que 1/100. La aplicación de verificación también puede proporcionar un nivel predeterminado en el caso de que falte el indicador en una llamada, por ejemplo 1/10000 para el ejemplo de tres niveles anterior y, por ejemplo, cuando la llamada se recibe desde una aplicación que no tiene mecanismo de llamada multinivel o un nivel de certeza asignado implementado. Los niveles pueden codificarse en la llamada de cualquier manera apropiada, y preferentemente siguen un protocolo asignado para la llamada. Debe observarse que los números dados en este caso son para una fácil comprensión de los principios, y pueden variar en función de las implementaciones y las demandas de los mismos.

La figura 6 es un esquema de señales que ilustra las funciones de acuerdo con las realizaciones, en particular, cuando se añaden referencias de verificación sin una confianza apropiada. Similar a lo que se ha demostrado anteriormente, la referencia de verificación está registrada, la aplicación de verificación y la otra aplicación están emparejadas correctamente, y también hay una llamada desde la otra aplicación, que puede ser con o sin un nivel de certeza necesario, y que puede compararse con un nivel FAR estimado, que se responde con un testigo de confianza. Considérese a continuación que se registra una nueva referencia de verificación, que puede ser del usuario autorizado o de otra persona, y se introducen después de esto los datos de verificación correspondientes. El comparador puede proporcionar una estimación de la FAR que es solo 1/10000, ya que la correspondencia entre la nueva referencia de verificación y los datos de verificación de entrada es buena. Sin embargo, la aplicación de verificación aún puede, tras una llamada desde la otra aplicación, proporcionar un mensaje sobre la confianza rota ya que la referencia de verificación no pertenece al conjunto de datos que estaba presente tras emparejar la aplicación de verificación con la otra aplicación. Esto es para ilustrar la posibilidad de una configuración de seguridad donde no se aceptan nuevas referencias de verificación, al menos no sin un nuevo emparejamiento adecuado u otras medidas de seguridad, por ejemplo, como se ha tratado anteriormente haciendo referencia al emparejamiento.

La figura 7 es un esquema de señales que ilustra las funciones de acuerdo con las realizaciones, en particular, cuando el nivel de certeza ha cambiado. Similar a lo que se ha demostrado anteriormente, la referencia de verificación está registrada, la aplicación de verificación y la otra aplicación están emparejadas correctamente, y también hay una llamada desde la otra aplicación, que puede ser con o sin un nivel de certeza necesario, y que puede compararse con un nivel FAR estimado, que se responde con un testigo de confianza. Considérese a continuación que se registran nuevos datos de verificación, que pueden ser del usuario autorizado o de otra persona. El nivel FAR estimado es solo 1/100 ya que la correspondencia entre la referencia de verificación y los datos de verificación de entrada no es tan buena, incluso si son bastante similares, o si el método de verificación usado es en sí mismo bastante débil, por ejemplo, una contraseña corta y de baja complejidad. A continuación, la aplicación de verificación puede tener un registro en un nivel de certeza necesario anterior o en un nivel FAR que es la base para un testigo de confianza proporcionado anteriormente, que se desvía significativamente del nivel en cuestión. A continuación, la aplicación de verificación puede disponerse para proporcionar un mensaje sobre la confianza rota basándose en esta gran desviación. Esto es para ilustrar la posibilidad de una configuración de seguridad donde no se aceptan grandes desviaciones en comparación con los valores históricos, al menos no sin volver a registrar adecuadamente los datos de verificación u otras medidas de seguridad.

La figura 8 es un esquema de señales que ilustra las funciones de acuerdo con las realizaciones, en particular, cuando otras aplicaciones emparejadas adecuadamente y no emparejadas operan con la aplicación de verificación. Similar a lo que se ha demostrado anteriormente, la referencia de verificación está registrada, la aplicación de verificación y una primera aplicación están emparejadas correctamente, y también hay una llamada desde la primera aplicación, que puede ser con o sin un nivel de certeza necesario, y que puede compararse con un nivel FAR estimado, que se responde con un testigo de confianza. Considérese a continuación una segunda aplicación que llama a la aplicación de verificación que puede ser con o sin un nivel de certeza necesario, y que puede compararse con un nivel FAR estimado. Sin embargo, la segunda aplicación no está emparejada correctamente con la aplicación de verificación. Por lo tanto, aunque el usuario está autenticado, lo que se ilustra con más detalle en la primera aplicación que vuelve a llamar a la aplicación de verificación y se responde mediante un testigo de confianza, la segunda aplicación solo obtiene un mensaje que indica que no hay confianza. Preferentemente, no se proporciona más información a la segunda aplicación, tal como el nivel FAR estimado u otra información posiblemente sensible. Si la segunda aplicación está dispuesta correctamente, debería estar dispuesta para el emparejamiento, por ejemplo, tener certificados adecuados, etc., que a continuación pueden disponerse. Si la segunda aplicación se usa para tratar de extraer información indebidamente de la aplicación de verificación, esto se evita proporcionando solo un mensaje de no confianza.

Los métodos de acuerdo con la presente invención son adecuados para su implementación con ayuda de medios de procesamiento, tales como ordenadores y/o procesadores, especialmente para el caso en que el dispositivo electrónico comprende el procesador, como se ha demostrado anteriormente. Como también se ha tratado anteriormente, las aplicaciones son mecanismos implementados por software que hacen que un dispositivo electrónico con un procesador realice tareas útiles más allá de la ejecución del propio dispositivo electrónico o

procesador, y por lo tanto también la aplicación de verificación demostrada en diversas realizaciones anteriores. Por lo tanto, se proporcionan programas informáticos, que comprenden instrucciones dispuestas para hacer que el medio de procesamiento, el procesador o el ordenador realicen las etapas de cualquiera de los métodos de acuerdo con cualquiera de las realizaciones descritas haciendo referencia a la figura 3. Los programas informáticos comprenden preferentemente un código de programa que puede almacenarse en un medio legible por ordenador 900, como se ilustra en la figura 9, que puede cargarse y ejecutarse mediante un medio de procesamiento, procesador u ordenador 902 para hacer que realice los métodos, respectivamente, de acuerdo con las realizaciones de la presente invención, preferentemente como cualquiera de las realizaciones descritas haciendo referencia a la figura 9. El ordenador 902 y el producto de programa informático 900 pueden disponerse para ejecutar el código de programa secuencialmente donde las acciones de cualquiera de los métodos se realizan etapa a etapa. El medio de procesamiento, procesador u ordenador 902 es preferentemente lo que normalmente se denomina un sistema embebido. Por lo tanto, el medio legible por ordenador 900 y el ordenador 902 representados en la figura 9 deberían interpretarse solo como para fines ilustrativos para proporcionar una comprensión del principio, y no deben interpretarse como cualquier ilustración directa de los elementos.

La invención principalmente se ha descrito anteriormente haciendo referencia a unas pocas realizaciones. Sin embargo, como puede apreciar fácilmente un experto en la materia, otras realizaciones distintas de las desveladas anteriormente son igualmente posibles dentro del alcance de la invención, tal como se define en las reivindicaciones de patente adjuntas.

REIVINDICACIONES

1. Una aplicación de verificación (110) dispuesta para interactuar con otras aplicaciones (112) en un dispositivo electrónico (100), teniendo el dispositivo electrónico (100) un procesador (104), una memoria (106) y un sistema operativo (108) que controla la operación de la aplicación de verificación (110) y las otras aplicaciones (112) en el procesador (104) usando localizaciones de memoria arbitrarias, donde las otras aplicaciones (112) están habilitadas para llamar a la aplicación de verificación (110) para determinar de manera segura la autenticidad de un usuario del dispositivo electrónico (100),
la aplicación de verificación (110) está dispuesta además para
recibir datos de verificación para la determinación segura de la autenticidad del usuario; y
proporcionar, tras una llamada desde cualquiera de las otras aplicaciones (112) y una coincidencia entre los datos de verificación y una referencia de verificación, un testigo de confianza a la aplicación llamante, caracterizada por que los datos de verificación comprenden una muestra biométrica y la referencia de verificación comprende una referencia biométrica,
estando la aplicación de verificación (110) dispuesta para emparejarse con al menos una de las otras aplicaciones (112) intercambiando recíprocamente al menos una de
una firma de aplicación;
una clave o unas claves criptográficas;
una contraseña; y
un secreto compartido,
en la que la disposición del testigo de confianza solo se realiza cuando la aplicación de verificación (110) y la una de las otras aplicaciones (112) que proporcionan una llamada a la aplicación de verificación (110) están emparejadas correctamente.

2. La aplicación de verificación de la reivindicación 1, en la que tras la instalación de la aplicación de verificación (110) en el dispositivo electrónico (100) se establecen los parámetros para la generación del testigo de confianza, y se registra la referencia de verificación.

3. La aplicación de verificación de una cualquiera de las reivindicaciones 1 a 2, en la que la llamada desde la una de las otras aplicaciones (112) incluye un indicador sobre un grado de certeza necesaria en la coincidencia, en la que la coincidencia entre los datos de verificación y la referencia de verificación se considera presente si una tasa de aceptación falsa estimada por un mecanismo de coincidencia de la aplicación de verificación (110) es menor que el grado de certeza necesaria en la coincidencia.

4. La aplicación de verificación de la reivindicación 3, en la que el testigo de confianza incluye o está acompañado por un indicador de autenticidad, en la que el indicador de autenticidad se basa en la tasa de aceptación falsa estimada por el mecanismo de coincidencia.

5. La aplicación de verificación de una cualquiera de las reivindicaciones 1 a 4, dispuesta además para proporcionar un indicador de confianza rota o no si
un grado de certeza necesaria en la autenticación para la coincidencia entre los datos de verificación recibidos y la referencia de verificación se restablece en un nivel de certeza menor que antes del restablecimiento;
la aplicación llamante no está correctamente emparejada con la aplicación de verificación; o
una combinación de los mismos.

6. La aplicación de verificación de una cualquiera de las reivindicaciones 1 a 5, en la que recibir los datos de verificación comprende recibir una muestra biométrica, la referencia de verificación es una referencia biométrica y la coincidencia entre los datos de verificación y la referencia de verificación se realiza mediante un mecanismo de coincidencia biométrica de la aplicación de verificación (110), en la que el mecanismo de coincidencia biométrica está dispuesto para hacer coincidir la muestra biométrica con la referencia biométrica.

7. Un método de una aplicación de verificación dispuesta para interactuar con otras aplicaciones en un dispositivo electrónico, teniendo el dispositivo electrónico un procesador, una memoria y un sistema operativo que controlan la operación de la aplicación de verificación y las otras aplicaciones en el procesador usando localizaciones de memoria arbitrarias, comprendiendo el método recibir (314) una llamada, para la aplicación de verificación desde una de las otras aplicaciones, para determinar de manera segura la autenticidad de un usuario del dispositivo electrónico;
recibir (312) los datos de verificación;
autenticar los datos de verificación haciéndolos coincidir (312) con una referencia de verificación almacenada por la aplicación de verificación; y
proporcionar (318), tras una coincidencia entre los datos de verificación y la referencia de verificación, un testigo de confianza a la aplicación llamante, caracterizado por que los datos de verificación comprenden una muestra biométrica y la referencia de verificación comprende una referencia biométrica,
comprendiendo el método además
emparejar (302) la aplicación de verificación con al menos una de las otras aplicaciones intercambiando recíprocamente al menos una de

una firma de aplicación;
una clave criptográfica; una contraseña; y un secreto compartido, en el que la disposición (318) del testigo de confianza solo se realiza cuando la aplicación de verificación y la una de las otras aplicaciones que proporcionan una llamada a la aplicación de verificación están emparejadas correctamente (302).

8. El método de la reivindicación 7, que comprende además proporcionar (317) un indicador de confianza rota o no si
el grado de certeza necesaria en la autenticación para la coincidencia entre los datos de verificación recibidos y la referencia de verificación se restablece en un nivel de certeza más bajo;
la aplicación llamante no está correctamente emparejada con la aplicación de verificación; o
una combinación de los mismos.

9. El método de una cualquiera de las reivindicaciones 7 u 8, que comprende además, tras la instalación de la aplicación de verificación en el dispositivo electrónico,
establecer unos parámetros para la generación del testigo de confianza; y
registrar (300) la referencia de verificación.

10. El método de una cualquiera de las reivindicaciones 7 a 9, en el que la llamada desde la una de las otras aplicaciones incluye un indicador sobre un grado de certeza necesaria en la coincidencia, en el que la coincidencia entre los datos de verificación y la referencia de verificación se considera presente si una tasa de aceptación falsa estimada por la coincidencia (312) es menor que el grado de certeza necesaria.

11. El método de la reivindicación 10, en el que el testigo de confianza incluye o está acompañado por un indicador de autenticidad, en el que el indicador de autenticidad se basa en la tasa de aceptación falsa estimada por la coincidencia.

12. El método de una cualquiera de las reivindicaciones 7 a 11, en el que la recepción (310) de los datos de verificación comprende recibir una muestra biométrica, la referencia de verificación es una referencia biométrica y la coincidencia (312) entre los datos de verificación y la referencia de verificación se realiza mediante la coincidencia biométrica de la muestra biométrica con la referencia biométrica.

13. Un programa informático que comprende instrucciones ejecutables por ordenador que cuando se ejecutan por un procesador (104, 900) de un dispositivo electrónico (100) que tiene el procesador (104, 900), una memoria (106) y un sistema operativo (108) controlan la operación de las aplicaciones (110, 112) en el procesador usando localizaciones de memoria arbitrarias, en el que la instrucción ejecutable por ordenador provoca que el procesador (104, 900) realice el método de una cualquiera de las reivindicaciones 7 a 12.

14. Un dispositivo electrónico (100) que tiene un procesador (104), una memoria (106) y un sistema operativo (108), que comprende una aplicación de verificación (110) de acuerdo con una cualquiera de las reivindicaciones 1 a 5, al menos otra aplicación (112) habilitada para llamar a la aplicación de verificación (110) para determinar de manera segura la autenticidad de un usuario del dispositivo electrónico (100), y una entrada de datos de verificación (102) dispuesta para proporcionar datos de verificación a la aplicación de verificación (110), en el que el sistema operativo (108) está dispuesto para controlar la operación de la aplicación de verificación (108) y las otras aplicaciones (112) en el procesador (104) usando localizaciones de memoria arbitrarias.

15. El dispositivo electrónico de la reivindicación 14, en el que la entrada de datos de verificación (102) comprende un lector biométrico dispuesto para proporcionar muestras biométricas como datos de verificación, y la aplicación de verificación (110) está de acuerdo con la reivindicación 6.

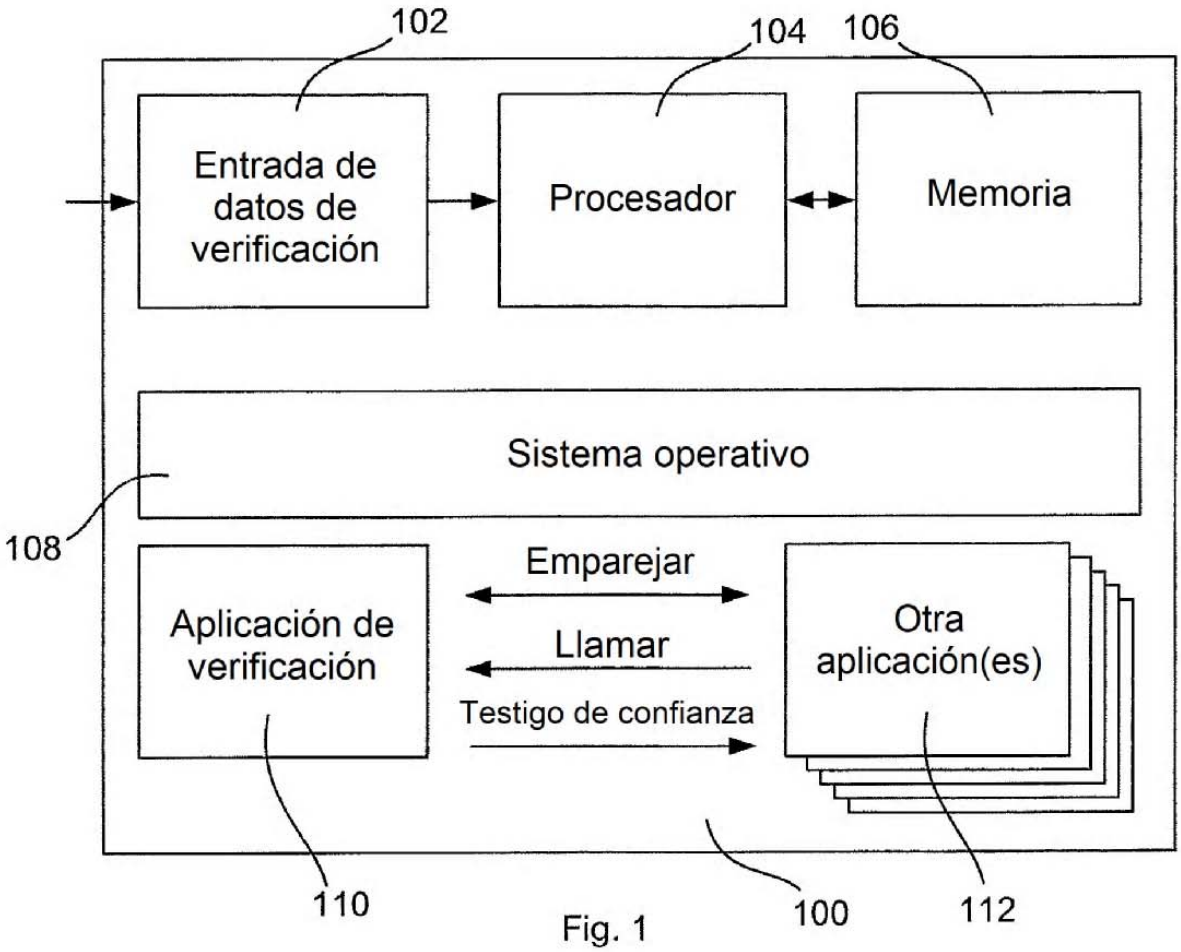
102
104
106
Entrada de datos de verificación
Procesador
Memoria
Sistema operativo
108
Emparejar
Aplicación de verificación
Llamar
Otra aplicación(es)
Testigo de confianza
110
100
112

Fig. 1

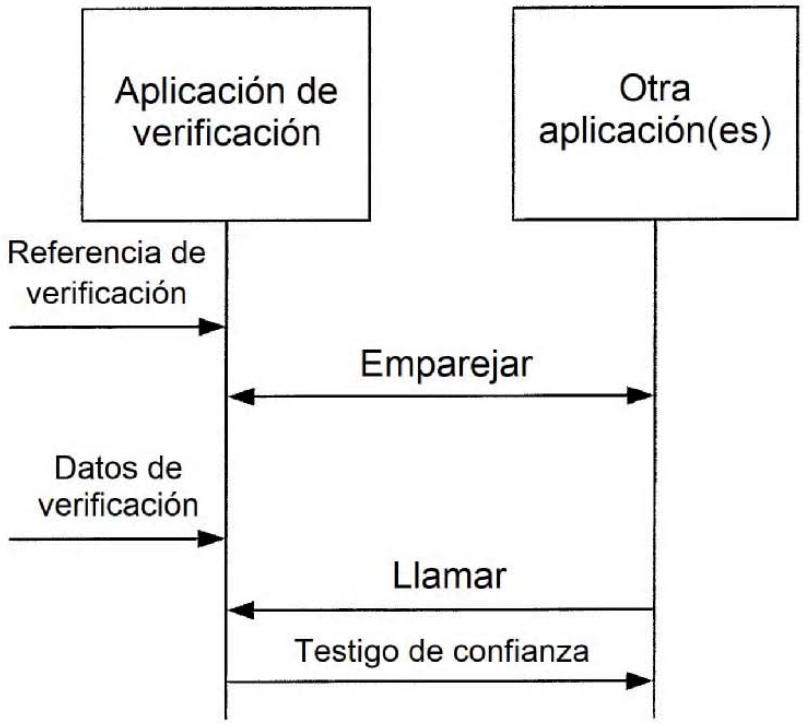
Aplicación de verificación
Otra aplicación(es)
Referencia de verificación
Emparejar
Datos de verificación
Llamar
Testigo de confianza

Fig. 2

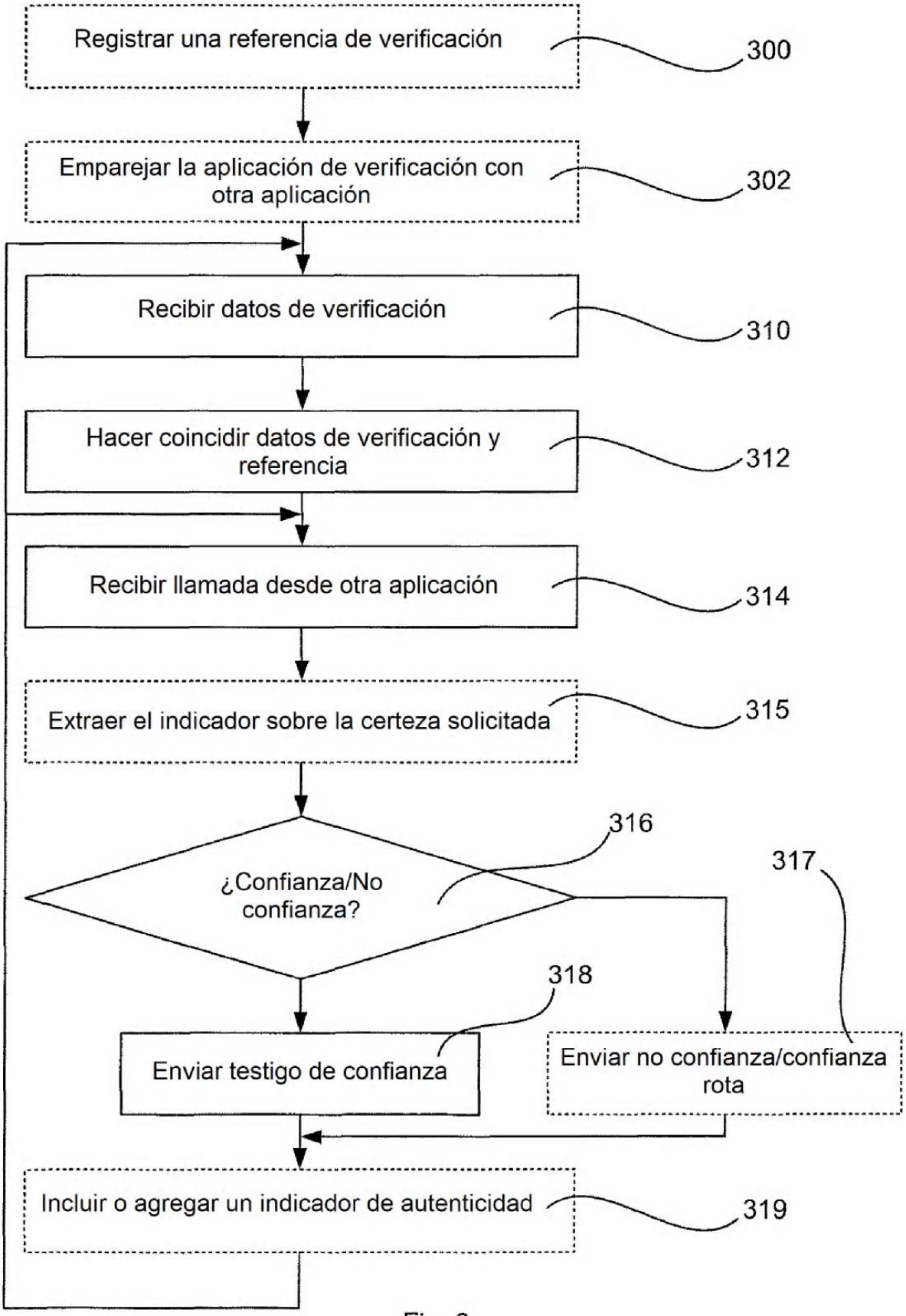
Registrar una referencia de verificación
300
Emparejar la aplicación de verificación con otra aplicación
302
Recibir datos de verificación
310
Hacer coincidir datos de verificación y referencia
312
Recibir llamada desde otra aplicación
314
Extraer el indicador sobre la certeza solicitada
315
316
¿Confianza/No confianza?
317
318
Enviar testigo de confianza
Enviar no confianza/confianza rota
Incluir o agregar un indicador de autenticidad
319

Fig. 3

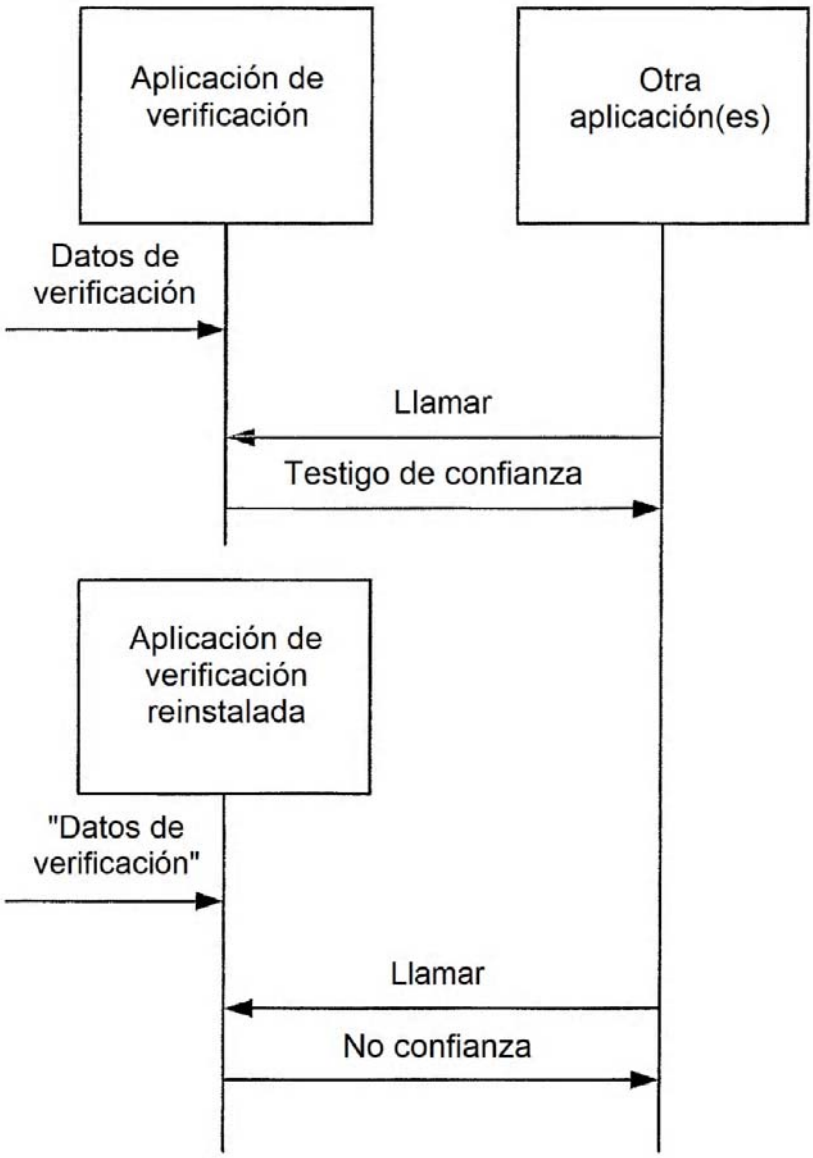
Aplicación de verificación
Otra aplicación(es)
Datos de verificación
Llamar
Testigo de confianza
Aplicación de verificación reinstalada
"Datos de verificación"
Llamar
No confianza

Fig. 4

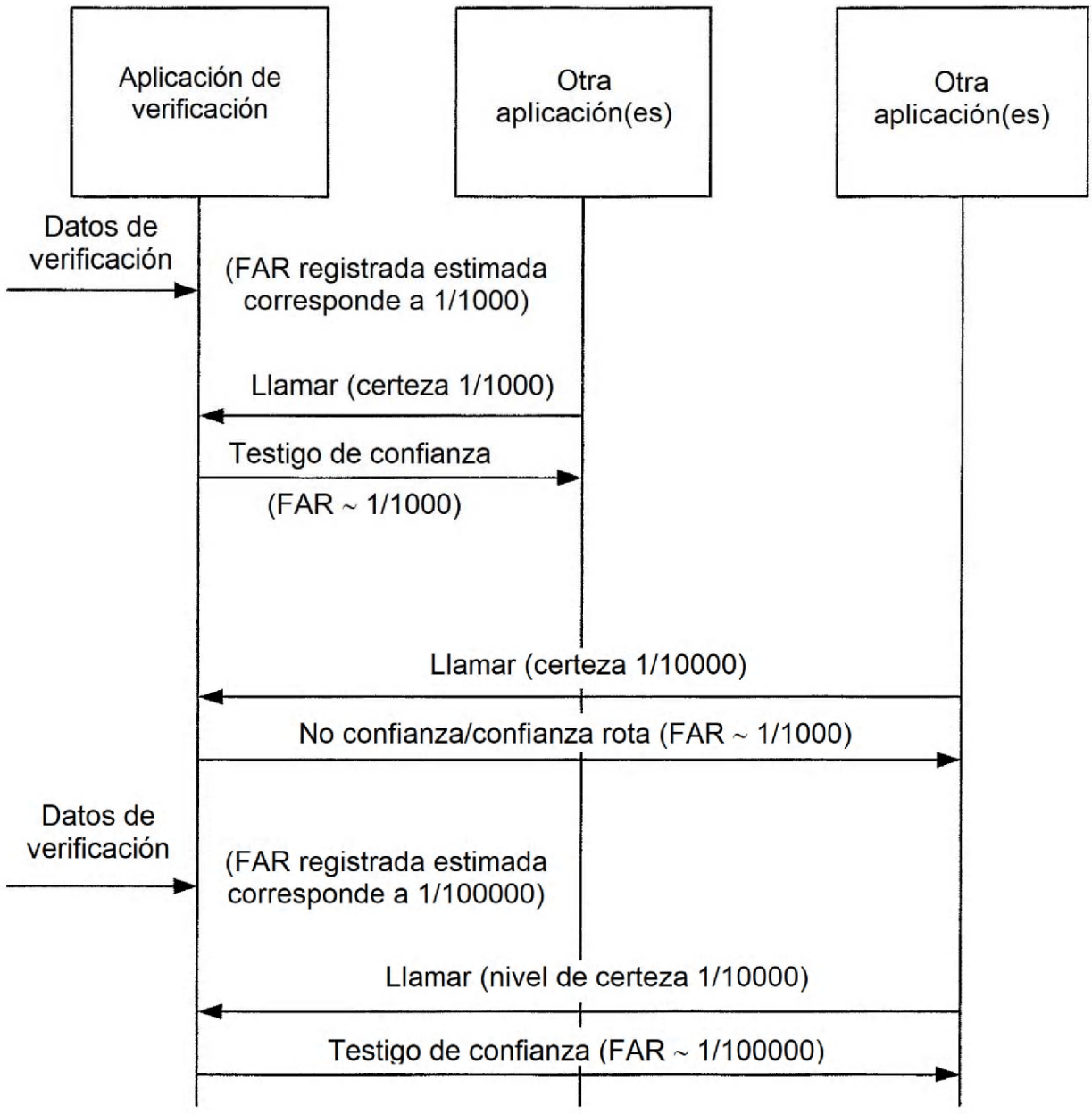
Aplicación de verificación
Otra aplicación(es)
Otra aplicación(es)
Datos de verificación
(FAR registrada estimada corresponde a 1/1000)
Llamar (certeza 1/1000)
Testigo de confianza
(FAR ~ 1/1000)
Llamar (certeza 1/10000)
No confianza/confianza rota (FAR ~ 1/1000)
Datos de verificación
(FAR registrada estimada corresponde a 1/100000)
Llamar (nivel de certeza 1/10000)
Testigo de confianza (FAR ~ 1/100000)

Fig. 5

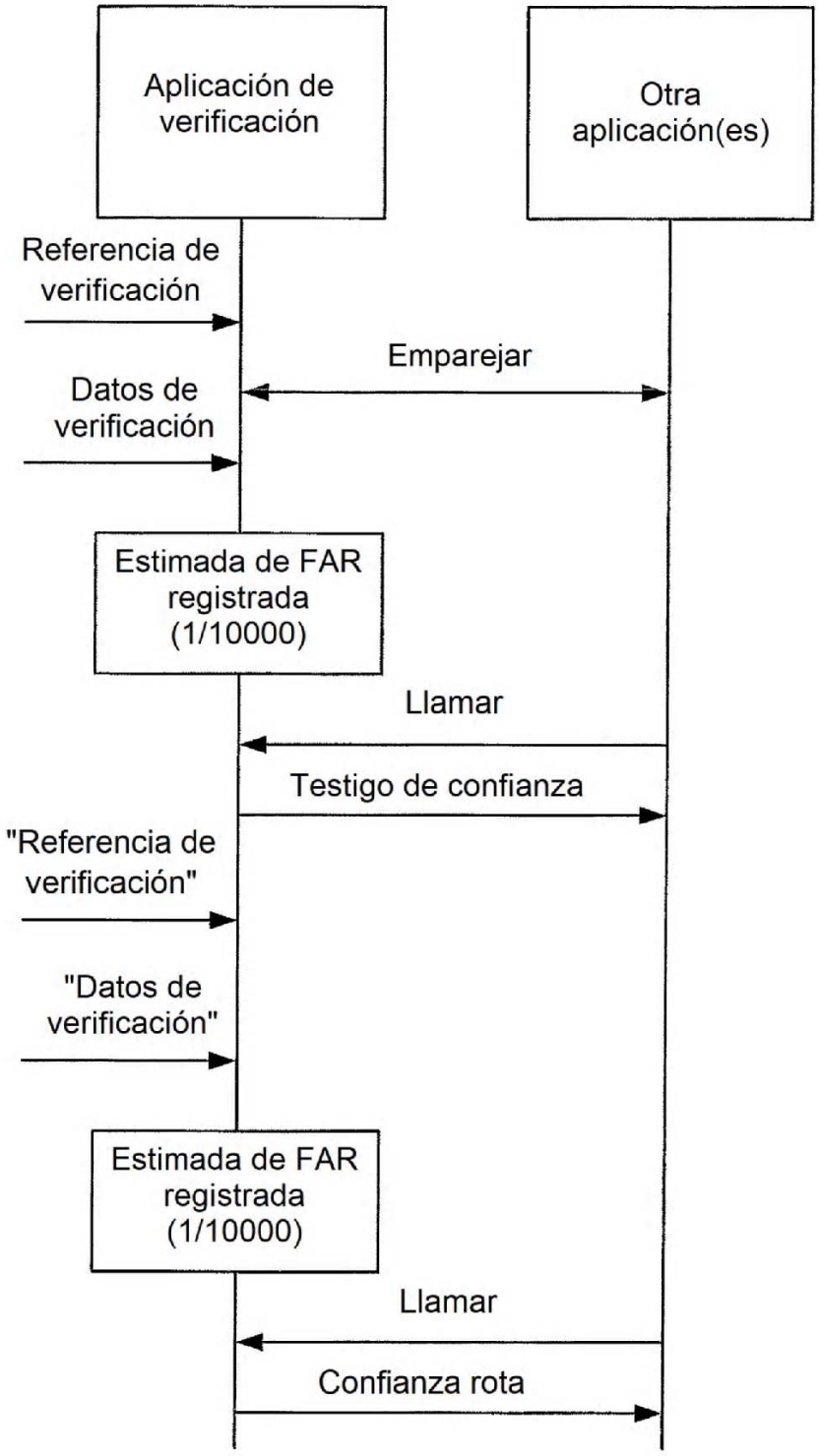
Aplicación de verificación
Otra aplicación(es)
Referencia de verificación
Emparejar
Datos de verificación
Estimada de FAR registrada (1/10000)
Llamar
Testigo de confianza
"Referencia de verificación"
"Datos de verificación"
Estimada de FAR registrada (1/10000)
Llamar
Confianza rota

Fig. 6

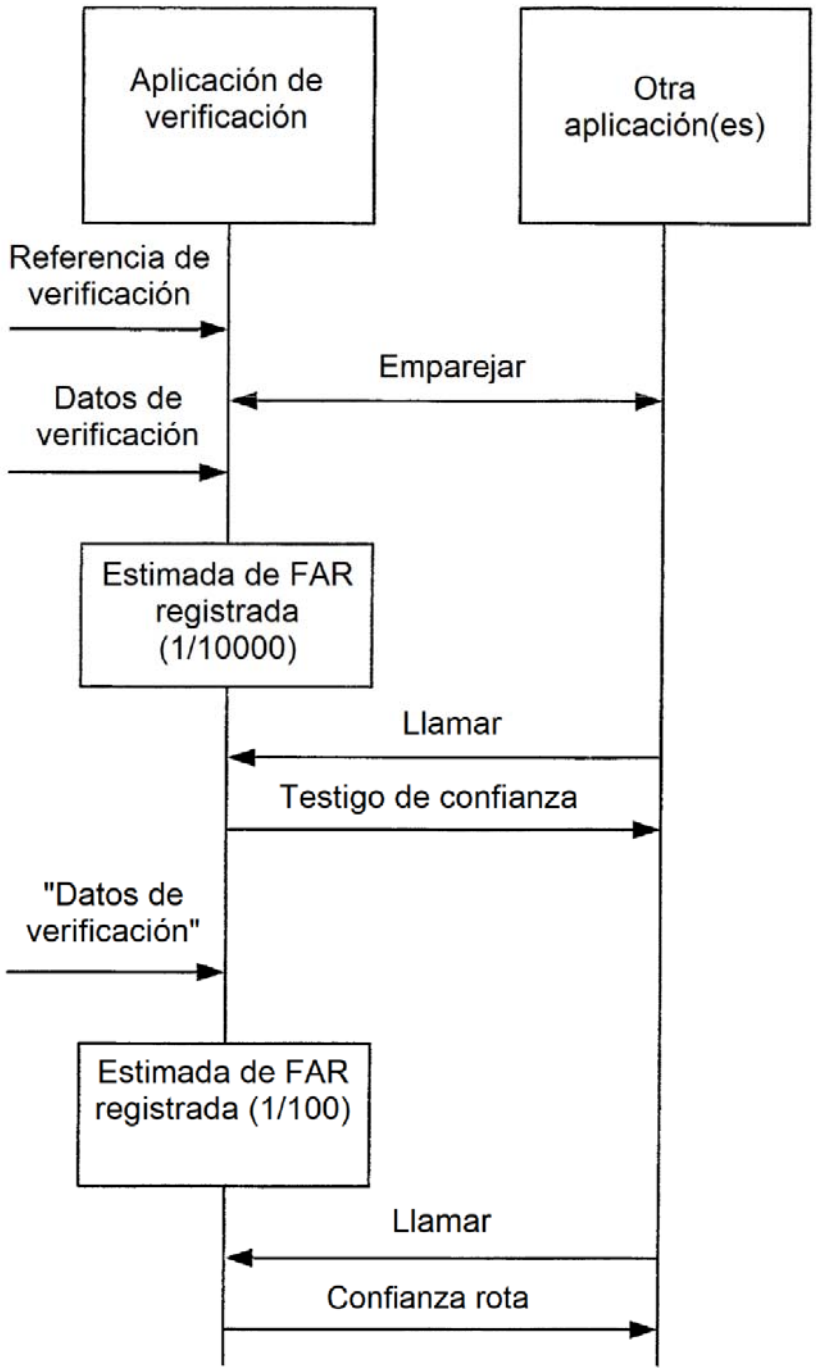
Aplicación de verificación
Otra aplicación(es)
Referencia de verificación
Emparejar
Datos de verificación
Estimada de FAR registrada (1/10000)
Llamar
Testigo de confianza
"Datos de verificación"
Estimada de FAR registrada (1/100)
Llamar
Confianza rota

Fig. 7

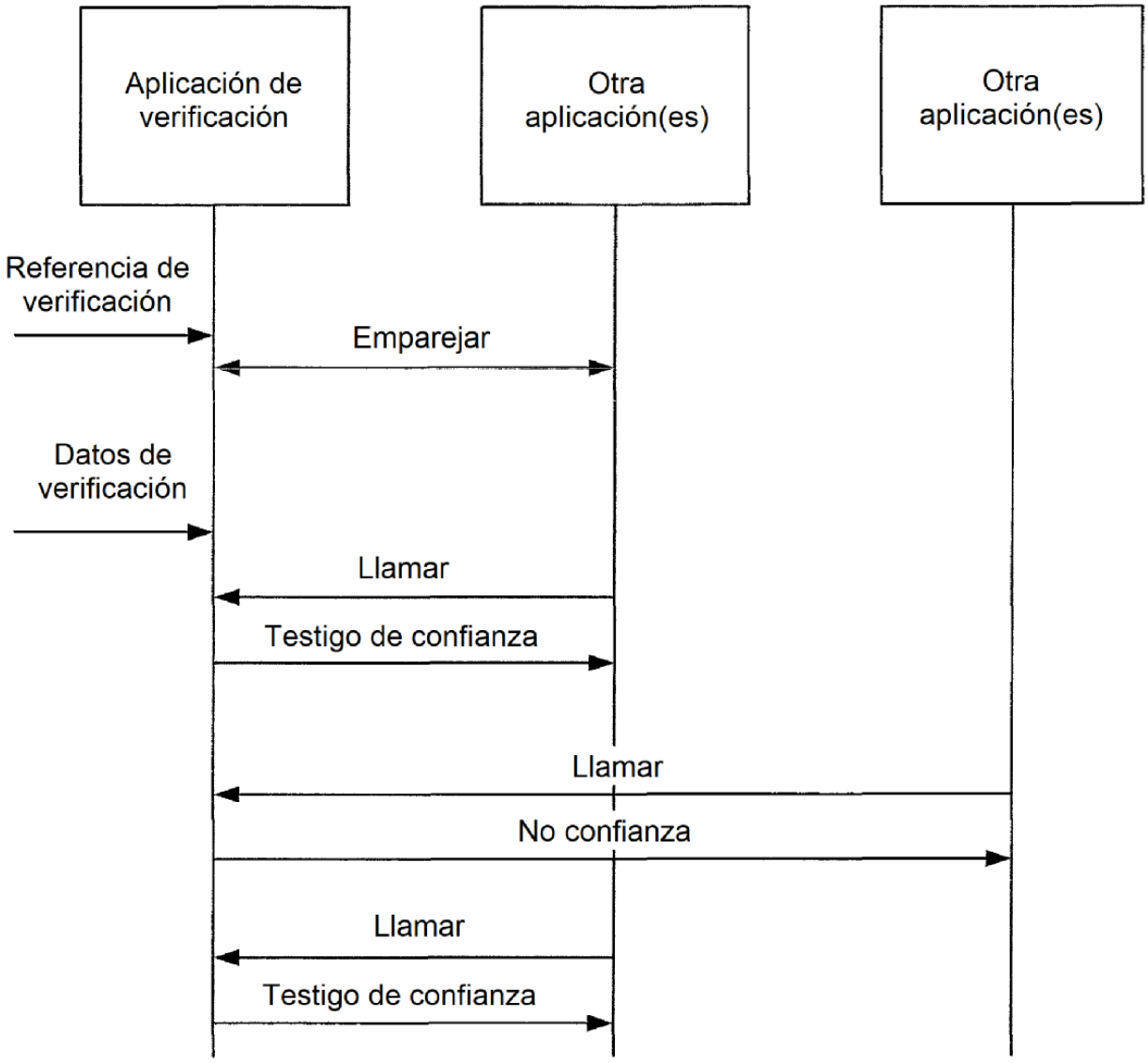
Aplicación de verificación
Otra aplicación(es)
Otra aplicación(es)
Referencia de verificación
Emparejar
Datos de verificación
Llamar
Testigo de confianza
Llamar
No confianza
Llamar
Testigo de confianza

Fig. 8

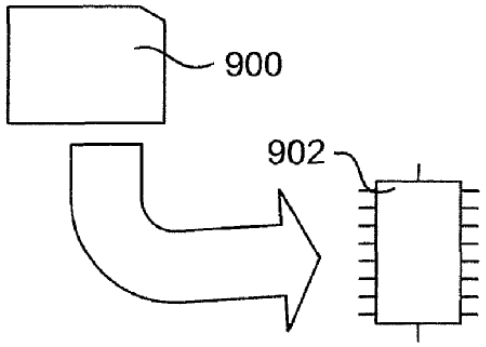
900
902

Fig. 9