(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 874 192**

(51) Int. CI.:

H04L 9/08 (2006.01)
H04L 9/32 (2006.01)
H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **20.03.2017 PCT/CN2017/077247**

(87) Fecha y número de publicación internacional: **28.09.2017 WO17162112**

(96) Fecha de presentación y número de la solicitud europea: **20.03.2017 E 17769389 (2)**

(97) Fecha y número de publicación de la concesión europea: **03.03.2021 EP 3435590**

(54) Título: **Método y dispositivo de registro de identidad**

(30) Prioridad:

25.03.2016 CN 201610180030

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
04.11.2021

(73) Titular/es:

ADVANCED NEW TECHNOLOGIES CO., LTD. (100.0%)
Cayman Corporate Centre, 27 Hospital Road George Town, Grand Cayman KY1-9008, KY

(72) Inventor/es:

MENG, FEI

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

DESCRIPCIÓN

Método y dispositivo de registro de identidad

La presente solicitud reivindica la prioridad de la Solicitud de Patente China No. 201610180030.4, presentada el 25 de marzo de 2016 y titulada "IDENTITY REGISTRATION METHOD AND DEVICE".

CAMPO TÉCNICO

La presente solicitud se refiere al campo de las tecnologías informáticas y, en particular, a un método y dispositivo de registro de identidad.

ANTECEDENTES

Con el desarrollo continuo de las tecnologías de red, el uso de servicios a través de la red se ha convertido en una parte integral de la vida de las personas, por ejemplo, las personas utilizan un servicio de previsión del tiempo a través de la red.

Actualmente, para mejorar la seguridad de la información cuando un usuario utiliza un servicio, el usuario necesita registrar una identidad de usuario de antemano para el servicio antes de utilizar el servicio. Posteriormente, al utilizar el servicio a través de la red, es necesario verificar la identidad de usuario. El usuario puede utilizar el servicio solo después de que la verificación tenga éxito. Por ejemplo, si se utiliza la información de huella dactilar para representar la identidad de usuario, la información de huella dactilar del usuario debe registrarse de antemano.

Debido a que el reconocimiento de información de huella dactilar en aplicaciones reales es cada vez más popular en dispositivos terminales, por ejemplo, la información de huella dactilar de un usuario se utiliza para desbloquear una interfaz de pantalla bloqueada. Para cualquier servicio, un proceso en el que un servidor del servicio registra una identidad de usuario utilizando la información de huella dactilar del usuario y luego verifica la identidad de usuario utilizando la información de huella dactilar del usuario, puede completarse utilizando un dispositivo terminal.

Además, con la mejora continua de las tecnologías informáticas, en un dispositivo terminal se puede almacenar al mismo tiempo una pluralidad de informaciones de huella dactilar de un usuario. Para cualquier servicio, cuando se registra una identidad de usuario utilizando la información de huella dactilar cargada por el usuario, el dispositivo terminal primero necesita verificar si la información de huella dactilar es una de la pluralidad de informaciones de huella dactilar almacenada en el dispositivo terminal. En caso afirmativo, el dispositivo terminal puede registrar la identidad de usuario con un servidor en base a la información de huella dactilar y, en caso negativo, el dispositivo terminal notifica directamente al usuario que el registro de identidad falla.

En la tecnología existente, en la FIG. 1 se muestra un proceso de registro de información de huella dactilar de un usuario.

S101. Un dispositivo terminal recibe una operación de registro de un usuario.

S102. Recopilar información de huella dactilar del usuario.

S103. Determinar si la información de huella dactilar se ha almacenado previamente en el dispositivo terminal y, en caso afirmativo, ejecutar S104 o, de lo contrario, ejecutar S105.

S104. Consultar un identificador correspondiente a la información de huella dactilar almacenada previamente en el dispositivo terminal, generar una clave privada y una clave pública correspondientes al identificador, almacenar una relación de correspondencia entre la clave privada y el identificador correspondientes a la información de huella dactilar en el dispositivo terminal y enviar una relación de correspondencia entre la clave pública y el identificador correspondientes a la información de huella dactilar a un servidor para su almacenamiento.

S105. Notificar al usuario que el registro falla.

Posteriormente, en la FIG. 2 se muestra un proceso de un usuario utilizando un servicio.

S201. Un dispositivo terminal recibe información de huella dactilar de un usuario.

S202. Comparar la información de característica biométrica estándar consistente con la información de huella dactilar.

S203. Buscar una clave privada correspondiente a un identificador en base al identificador correspondiente a la información de característica biométrica estándar.

S204. Cuando se identifica la clave privada correspondiente al identificador, firmar la información de servicio utilizando la clave privada y agregar la información de servicio firmada y el identificador correspondiente a la información de huella dactilar a una solicitud de procesamiento de servicio y enviar la solicitud a un servidor para que el servidor determine una clave pública correspondiente al identificador incluido en la solicitud de procesamiento de servicio recibida y realice el procesamiento de servicio en base a la clave pública y la información de servicio. Alternativamente, cuando no se identifica la clave privada correspondiente al identificador, notificar al usuario que el procesamiento de servicio falla.

El documento US 2015/0312041 A1 describe técnicas para la autenticación de usuarios en entornos ubicuos.

El documento US 2004/0059924 A1 describe proporcionar confianza y autenticación para las comunicaciones y transacciones de red utilizando una infraestructura de red que emplea claves privadas biométricas.

Sin embargo, en las aplicaciones reales, si un usuario olvida qué huella dactilar introdujo, el usuario necesita realizar la verificación de huella dactilar varias veces. Causa grandes inconvenientes al usuario para utilizar un servicio y reduce la tasa de éxito de utilizar el servicio. Además, si el dedo de un usuario utilizado para el registro se lesiona en la vida diaria, el usuario no puede autenticarse para utilizar el servicio.

RESUMEN

Las implementaciones de la presente solicitud proporcionan un método y un dispositivo de registro de identidad, para resolver problemas de la tecnología existente: un usuario olvida qué huella dactilar introdujo y, en consecuencia, causa inconvenientes al usuario para utilizar un servicio; y si el dedo de un usuario utilizado para el registro se lesiona en la vida diaria, el usuario no puede autenticarse para utilizar el servicio.

La presente invención está dirigida al método definido en la reivindicación 1 y al dispositivo definido en la reivindicación 10. Las reivindicaciones dependientes describen formas de realización ventajosas de la presente invención.

Las implementaciones de la presente solicitud describen un método y un dispositivo de registro de identidad. En el método, el dispositivo terminal recibe la información de característica biométrica del usuario que se va a verificar y compara la información de característica biométrica estándar consistente con la información de característica biométrica que se va a verificar. Una vez que la comparación tiene éxito, el dispositivo terminal busca la clave privada correspondiente al identificador en base al identificador correspondiente a la información de característica biométrica estándar y registra la identidad de usuario con el servidor en base a la información de característica biométrica a ser verificada cuando la clave privada correspondiente al identificador no está identificada. Como tal, el servidor almacena la clave pública correspondiente a la información de característica biométrica a ser verificada. De acuerdo con el método anterior, independientemente de la información de característica biométrica utilizada por el usuario para el registro, siempre que el dispositivo terminal pueda identificar información de característica biométrica estándar consistente con la información de característica biométrica a ser verificada, incluso si no se identifica una clave privada correspondiente a un identificador en el dispositivo terminal en base al identificador correspondiente a la información de característica biométrica estándar, el dispositivo terminal puede registrar directamente la identidad de usuario en base a la información de característica biométrica a ser verificada, para completar el procesamiento de servicio, proporcionar una gran comodidad para que el usuario utilice un servicio y también mejorar eficazmente la tasa de éxito del uso del servicio.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Los dibujos adjuntos descritos aquí están destinados a proporcionar una mayor comprensión de la presente solicitud y constituyen una parte de la presente solicitud. Las implementaciones ilustrativas de la presente solicitud y las descripciones de las implementaciones están destinadas a describir la presente solicitud y no constituyen limitaciones de la presente solicitud. En los dibujos adjuntos:

La FIG. 1 es un diagrama esquemático que ilustra un proceso de registro de información de huella dactilar de un usuario en la tecnología existente, de acuerdo con una implementación de la presente solicitud;
La FIG. 2 es un diagrama esquemático que ilustra un proceso de utilizar un servicio mediante un usuario en la tecnología existente, de acuerdo con una implementación de la presente solicitud;
La FIG. 3 es un diagrama esquemático que ilustra un proceso de registro de identidad, de acuerdo con una implementación de la presente solicitud; y
La FIG. 4 es un diagrama estructural esquemático que ilustra un dispositivo de registro de identidad, de acuerdo con una implementación de la presente solicitud.

DESCRIPCIÓN DE LAS REALIZACIONES

Para hacer más claros los objetivos, las soluciones técnicas y las ventajas de la presente solicitud, a continuación, se describen las soluciones técnicas de la presente solicitud con referencia a implementaciones específicas de la presente solicitud y los correspondientes dibujos adjuntos. Aparentemente, las implementaciones descritas son

simplemente algunas y no todas las implementaciones de la presente solicitud. Otras implementaciones obtenidas sin esfuerzos creativos por un experto en la técnica en base a las implementaciones de la presente solicitud caerán dentro del alcance de protección de la presente solicitud.

La FIG. 3 muestra un proceso de registro de identidad, de acuerdo con una implementación de la presente solicitud. El proceso incluye los siguientes pasos.

S301. Un dispositivo terminal recibe información de característica biométrica de un usuario que se va a verificar.

En aplicaciones reales, para mejorar la seguridad de información cuando un usuario utiliza un servicio, en un proceso utilizar el servicio, primero es necesario verificar una identidad del usuario actual para confirmar que la identidad de usuario actual es válida.

Por lo tanto, en la presente solicitud, primero se recibe la información de característica biométrica del usuario que se va a verificar. Debido a que el reconocimiento de información de característica biométrica es cada vez más popular en dispositivos terminales (por ejemplo, teléfonos móviles) en aplicaciones reales, la información de característica biométrica del usuario que se va a verificar puede recibirse por un dispositivo terminal. Después de recibir la información de característica biométrica, el dispositivo terminal realiza una respuesta correspondiente. La información de característica biométrica indica un indicador físico del usuario y puede ser el iris de un ojo o una huella dactilar de un dedo, y se utiliza principalmente para representar inequívocamente una identidad de usuario.

Además, en aplicaciones reales, para verificar la identidad del usuario actual, la verificación de información de huella dactilar es cada vez más popular y la tecnología es relativamente madura. Por lo tanto, que la información de característica biométrica es información de huella dactilar se utiliza como ejemplo para la descripción detallada a continuación.

Por ejemplo, suponiendo que un determinado foro proporciona un servicio de consulta de información solo para un usuario que ha registrado una cuenta, y el usuario puede iniciar sesión utilizando información de huella dactilar. Por tanto, cuando el usuario necesita consultar información en el foro, el usuario abre una aplicación correspondiente al foro en un teléfono móvil (es decir, el dispositivo terminal) y presiona con una huella dactilar. Posteriormente, el teléfono móvil (es decir, el dispositivo terminal) recibe la información de huella dactilar del usuario que se va a verificar y realiza el paso S302.

S302. Comparar la información de característica biométrica estándar consistente con la información de característica biométrica a ser verificada en la información de característica biométrica almacenada previamente.

Debido a que el reconocimiento de información de huella dactilar (es decir, información de característica biométrica) en aplicaciones reales es cada vez más popular en dispositivos terminales, por ejemplo, la información de huella dactilar de un usuario se utiliza para desbloquear una interfaz de pantalla bloqueada. Para cualquier servicio, un proceso, en el que un servidor del servicio registra una identidad de usuario utilizando la información de huella dactilar del usuario y luego verifica la identidad de usuario utilizando la información de huella dactilar del usuario, puede completarse utilizando la información de huella dactilar que se ha almacenado en un dispositivo terminal. En otras palabras, siempre que la información de huella dactilar se almacene en un dispositivo terminal, la información de huella dactilar se puede utilizar para completar todo el procesamiento de servicio en la presente solicitud.

Vale la pena señalar aquí que la información de huella dactilar almacenada en el dispositivo terminal puede introducirse por el usuario cuando el usuario utiliza otra función del dispositivo terminal, y no es la información de huella dactilar utilizada por el usuario para el registro de identidad para utilizar un servicio. Por ejemplo, cuando el usuario utiliza una función del dispositivo terminal para desbloquear una interfaz de pantalla bloqueada utilizando la información de huella dactilar, el dispositivo terminal puede almacenar localmente la información de huella dactilar.

Además, en la presente solicitud, para distinguir entre la información de huella dactilar almacenada y la información de huella dactilar recibida por el dispositivo terminal cuando el usuario utiliza el servicio, la información de huella dactilar almacenada puede utilizarse como información de huella dactilar estándar (es decir, información de característica biométrica estándar), y se utiliza principalmente para verificar si el usuario puede autenticarse en un proceso de utilizar el servicio y para proporcionar el procesamiento de servicio para el usuario.

Por lo tanto, en la presente solicitud, después de recibir la información de huella dactilar (es decir, la información de característica biométrica) del usuario que se va a verificar, el dispositivo terminal compara directamente la información de huella dactilar estándar almacenada localmente (es decir, la información de característica biométrica estándar) consistente con la información de huella dactilar a ser verificada.

Continuando con el ejemplo descrito anteriormente, después de recibir la información de huella dactilar del usuario que se va a verificar, el teléfono móvil compara la información de huella dactilar estándar almacenada localmente consistente con la información de huella dactilar a ser verificada. Suponer que se identifica la información de huella dactilar estándar consistente con la información de huella dactilar a ser verificada.

S303. Buscar una clave privada correspondiente a un identificador en base al identificador correspondiente a la información de característica biométrica estándar después de que la comparación tenga éxito.

En la presente solicitud, para distinguir cada una de las piezas de información de huella dactilar (es decir, información de característica biométrica) que se ha almacenado en el dispositivo terminal, el dispositivo terminal puede asignar un identificador de información de huella dactilar (es decir, un identificador de información de característica biométrica) a cada una de las piezas de información de huella dactilar al almacenar la información de huella dactilar.

Además, para verificar una identidad de usuario mediante un servidor correspondiente a un servicio futuro, concretamente, el servidor correspondiente al servicio necesita conocer el usuario que utiliza el servicio. En la presente solicitud, es necesario generar una clave privada y una clave pública correspondientes a un identificador en base al identificador. El identificador corresponde a la información de huella dactilar utilizada para el registro. La clave privada y la clave pública representan una identidad de usuario. La clave privada generada se almacena en el dispositivo terminal. Al enviar una solicitud de procesamiento de servicio al servidor, el dispositivo terminal necesita utilizar la clave privada para firmar la solicitud de procesamiento de servicio y envía la solicitud de procesamiento de servicio firmada al servidor.

Por lo tanto, en la presente solicitud, después de identificar la información de huella dactilar estándar consistente con la información de huella dactilar a ser verificada, el dispositivo terminal necesita buscar la clave privada correspondiente al identificador en base al identificador correspondiente a la información de huella dactilar estándar.

Continuando con el ejemplo descrito anteriormente, después de identificar la información de huella dactilar estándar consistente con la información de huella dactilar a ser verificada, el teléfono móvil busca la clave privada correspondiente al identificador en base al identificador correspondiente a la información de huella dactilar estándar.

S304. Registrar una identidad de usuario con un servidor en base a la información de característica biométrica a ser verificada cuando no se identifica la clave privada correspondiente al identificador, de modo que el servidor almacena una clave pública correspondiente a la información de característica biométrica a ser verificada.

En la presente solicitud, si el dispositivo terminal identifica la información de huella dactilar estándar consistente con la información de huella dactilar a ser verificada en el paso S302, pero el dispositivo terminal no identifica la clave privada correspondiente al identificador en base al identificador correspondiente a la información de huella dactilar estándar, indica que la información de huella dactilar a ser verificada pertenece al usuario, pero no es la información de huella dactilar utilizada durante el registro. Para continuar proporcionando el servicio requerido para el usuario, la identidad de usuario se puede registrar directamente con el servidor en base a la información de huella dactilar (es decir, la información de característica biométrica) que se va a verificar.

Además, la presente solicitud proporciona a continuación un proceso específico para registrar una identidad de usuario:

La clave privada y la clave pública correspondientes al identificador se generan en base al identificador correspondiente a la información de característica biométrica estándar que coincide con la información de característica biométrica a ser verificada; una relación de correspondencia entre el identificador y la clave privada generada se almacena en el dispositivo terminal; y se envía una relación de correspondencia entre el identificador y la clave pública generada al servidor para su almacenamiento.

Vale la pena señalar aquí que la información de característica biométrica estándar corresponde exclusivamente a un identificador de información de característica biométrica estándar, y un identificador de información de característica biométrica estándar corresponde a una clave privada y una clave pública únicas. En otras palabras, la información de característica biométrica estándar y el identificador de información de característica biométrica estándar están en una relación de correspondencia uno a uno con una clave privada y una clave pública. En la presente solicitud, si la información de característica biométrica a ser verificada existe en el dispositivo terminal, en el paso S302, solo se puede identificar una pieza de información de característica biométrica estándar. En otras palabras, enviar la relación de correspondencia entre el identificador y la clave pública generada al servidor para su almacenamiento también puede ser almacenar, mediante el servidor, la clave pública correspondiente a la información de característica biométrica a ser verificada.

Aunque la clave privada correspondiente a la información de huella dactilar (es decir, la información de característica biométrica) no se encuentra localmente en el dispositivo terminal, la información de huella dactilar puede no ser información de huella dactilar del usuario. Para mejorar aún más la seguridad de información cuando el usuario utiliza el servicio, en la presente solicitud, antes de que la identidad de usuario se registre con el servidor en base a la información de característica biométrica a ser verificada, se le puede solicitar al usuario que introduzca una contraseña para el servicio. Cuando se recibe la contraseña introducida por el usuario, el dispositivo terminal verifica si la contraseña es correcta. Si la contraseña es correcta, la identidad de usuario se puede registrar con el servidor en base a la información de característica biométrica a ser verificada. Si la contraseña es incorrecta, la identidad de usuario no

se registra con el servidor en base a la información de característica biométrica a ser verificada y se notifica al usuario que el procesamiento de servicio falla.

Además, vale la pena señalar aquí que cuando el dispositivo terminal no identifica la clave privada correspondiente al identificador, el dispositivo terminal puede notificar directamente al usuario que el procesamiento de servicio falla. En tal caso, el usuario puede introducir una contraseña para el servicio para continuar utilizando el servicio. El dispositivo terminal puede recibir la contraseña introducida por el usuario y verificar si la contraseña es correcta y, en caso afirmativo, registra la identidad de usuario con el servidor en base a la información de característica biométrica a ser verificada.

Continuando con el ejemplo descrito anteriormente, suponer que el teléfono móvil no ha identificado la clave privada correspondiente al identificador. El teléfono móvil solicita al usuario que utilice una contraseña para el servicio de consulta de información. Suponer que el usuario ingresa la contraseña xxxx. Después de recibir la contraseña xxxx que introduce el usuario, si el dispositivo terminal verifica que la contraseña es correcta, el dispositivo terminal genera la clave privada y la clave pública correspondientes al identificador, donde el identificador corresponde a la información de huella dactilar estándar que coincide con la información de huella dactilar a ser verificada en base al identificador, almacena una relación de correspondencia entre el identificador y la clave privada generada en el teléfono móvil y envía una relación de correspondencia entre el identificador y la clave pública generada al servidor para su almacenamiento.

De acuerdo con el método anterior, independientemente de la información de característica biométrica utilizada por el usuario para el registro, siempre que el dispositivo terminal pueda identificar información de característica biométrica estándar consistente con la información de característica biométrica a ser verificada, incluso si no se identifica una clave privada correspondiente a un identificador en el dispositivo terminal en base al identificador correspondiente a la información de característica biométrica estándar, el dispositivo terminal puede registrar directamente la identidad de usuario en base a la información de característica biométrica a ser verificada, para completar el procesamiento de servicio, proporcionar una gran comodidad para que el usuario utilice un servicio y también mejorar eficazmente la tasa de éxito del uso del servicio.

Además, en aplicaciones reales, se puede enviar una solicitud de procesamiento de servicio al servidor en base a la información de característica biométrica a ser verificada después de que la identidad de usuario se registre con el servidor. Como tal, el servidor realiza el procesamiento de servicio en base a la clave pública correspondiente a la información de característica biométrica a ser verificada.

En el paso S304, la clave privada y la clave pública correspondientes al identificador de la información de huella dactilar (es decir, la información de característica biométrica) se han vuelto a generar en base a la información de huella dactilar a ser verificada, y la clave pública se envía al servidor para su almacenamiento. Por lo tanto, en un proceso de enviar una solicitud de procesamiento de servicio al servidor en base a la información de huella dactilar a ser verificada, la presente solicitud puede incluir lo siguiente: firmar la información de servicio en base a la clave privada generada y enviar la solicitud de procesamiento de servicio que incluye la información de servicio y el identificador al servidor, por lo que el servidor determina la clave pública correspondiente al identificador incluido en la solicitud de procesamiento de servicio en base al identificador, verifica la firma de la información de servicio incluida en la solicitud de procesamiento de servicio en base a la clave pública determinada para verificar la identidad de usuario y realiza el procesamiento de servicio en la información de servicio.

Continuando con el ejemplo descrito anteriormente, el teléfono móvil firma la información de inicio de sesión en base a la clave privada generada del identificador y envía una solicitud de procesamiento de inicio de sesión que incluye la información de inicio de sesión firmada y el identificador al servidor. El servidor identifica una clave pública correspondiente al identificador en base al identificador incluido en la solicitud de procesamiento de inicio de sesión, verifica la firma de la información de inicio de sesión incluida en la solicitud de procesamiento de inicio de sesión utilizando la clave pública y completa el inicio de sesión del usuario.

En las aplicaciones reales, el pago de mercancía comprada utilizando una aplicación de pago se ha vuelto cada vez más popular. En la presente solicitud, a continuación, se describe la presente divulgación en detalle utilizando un ejemplo en el que una solicitud de procesamiento de servicios es una solicitud de pago.

Por ejemplo, suponer que el usuario A ha registrado información de huella dactilar (es decir, información de identidad) en una aplicación de pago. Cuando el usuario A paga la mercancía comprada utilizando la aplicación de pago, el usuario A abre la aplicación de pago en el teléfono móvil (es decir, el dispositivo terminal) y presiona con una huella dactilar. Después de recibir la información de huella dactilar del usuario que se va a verificar, el teléfono móvil compara localmente la información de huella dactilar estándar consistente con la información de huella dactilar a ser verificada. Suponer que se identifica la información de huella dactilar estándar consistente con la información de huella dactilar a ser verificada. El teléfono móvil busca una clave privada correspondiente a un identificador en base al identificador correspondiente a la información de huella dactilar estándar. Si el teléfono móvil no identifica la clave privada correspondiente al identificador, el teléfono móvil solicita directamente al usuario que introduzca una contraseña de pago. El teléfono móvil recibe la contraseña cccc de pago introducida por el usuario y verifica si la contraseña es

correcta. En caso afirmativo, el teléfono móvil genera la clave privada y una clave pública correspondiente a un identificador, donde el identificador corresponde a la información de huella dactilar estándar que coincide con la información de huella dactilar a verificar en base al identificador, almacena una relación de correspondencia entre el identificador y la clave privada generada en el teléfono móvil y envía una relación de correspondencia entre el identificador y la clave pública generada al servidor para su almacenamiento.

En un proceso posterior de procesamiento de un servicio de pago, el teléfono móvil firma la información de pago en base a la clave privada generada correspondiente al identificador y envía una solicitud de procesamiento de pago que incluye la información de pago firmada y el identificador al servidor. El servidor identifica la clave pública correspondiente al identificador en base al identificador incluido en la solicitud de procesamiento de pago, verifica la firma de la información de pago utilizando la clave pública y completa el pago con éxito.

Lo que se describe anteriormente es el método de registro de identidad proporcionado en la implementación de la presente solicitud. Como se muestra en la FIG. 4, en base a la misma idea, la presente solicitud proporciona además un dispositivo de registro de identidad correspondiente.

La FIG. 4 es un diagrama estructural esquemático que ilustra un dispositivo de registro de identidad, de acuerdo con una implementación de la presente solicitud. El dispositivo incluye lo siguiente: un módulo 401 de recepción, configurado para recibir información de característica biométrica de un usuario que se va a verificar; un módulo 402 de coincidencia, configurado para comparar información de característica biométrica estándar consistente con la información de característica biométrica a ser verificada en la información de característica biométrica almacenada previamente; un módulo 403 de búsqueda, configurado para buscar una clave privada correspondiente a un identificador en base al identificador correspondiente a la información de característica biométrica estándar después de que la comparación tenga éxito; y un módulo 404 de registro, configurado para registrar una identidad de usuario con un servidor en base a la información de característica biométrica a ser verificada cuando el módulo 403 de búsqueda no identifica la clave privada correspondiente al identificador, por lo que el servidor almacena una clave pública correspondiente a la información de característica biométrica a ser verificada.

El dispositivo incluye además lo siguiente: un módulo 405 de verificación de contraseña, configurado para recibir una contraseña introducida por el usuario y verificar que la contraseña sea correcta antes de que el módulo 404 de registro registre la identidad de usuario con el servidor en base a la información de característica biométrica a ser verificada.

El módulo 404 de registro está configurado para generar la clave privada y la clave pública correspondientes al identificador en base al identificador correspondiente a la información de característica biométrica estándar que coincide con la información de característica biométrica a ser verificada; almacenar una relación de correspondencia entre el identificador y la clave privada generada en un dispositivo terminal; y enviar una relación de correspondencia entre el identificador y la clave pública generada al servidor para su almacenamiento.

El dispositivo incluye además lo siguiente: un módulo 406 de procesamiento, configurado para enviar una solicitud de procesamiento de servicio al servidor en base a la información de característica biométrica a ser verificada después de que el módulo 404 de registro registre la identidad de usuario con el servidor, por lo que el servidor realiza el procesamiento de servicio. en base a la clave pública correspondiente a la información de característica biométrica a ser verificada.

El módulo 406 de procesamiento está configurado para firmar información de servicio en base a la clave privada generada y enviar la solicitud de procesamiento de servicio que incluye la información de servicio firmada y el identificador al servidor, por lo que el servidor determina la clave pública correspondiente al identificador incluido en la solicitud de procesamiento de servicio recibida y realiza el procesamiento de servicio en base a la clave pública determinada y la información de servicio firmada.

La solicitud de procesamiento de servicio incluye una solicitud de pago.

En una configuración típica, un dispositivo informático incluye uno o más procesadores (CPU), una interfaz de entrada/salida, una interfaz de red y una memoria.

La memoria puede incluir una memoria no persistente, una memoria de acceso aleatorio (RAM) y/o una memoria no volátil, etc. en un medio legible por computadora, tal como una memoria de solo lectura (ROM) o una memoria flash (flash RAM). La memoria es un ejemplo del medio legible por computadora.

El medio legible por ordenador incluye medios persistentes, no persistentes, móviles e inmovibles que pueden almacenar información utilizando cualquier método o tecnología. La información puede ser una instrucción legible por ordenador, una estructura de datos, un módulo de programa u otros datos. Los ejemplos de un medio de almacenamiento informático incluyen, pero no se limitan a una memoria de acceso aleatorio de cambio de fase (PRAM), una RAM estática (SRAM), una RAM dinámica (DRAM), una RAM de otro tipo, una memoria de solo lectura (ROM), una memoria de solo lectura programable y borrable eléctricamente (EEPROM), una memoria flash u otra tecnología de memoria, una memoria de disco compacto de solo lectura (CD-ROM), un disco versátil digital (DVD) u otro

almacenamiento óptico, una cinta magnética, un almacenamiento en disco magnético, otro dispositivo de almacenamiento magnético o cualquier otro medio que no sea de transmisión. El medio de almacenamiento informático se puede utilizar para almacenar información a la que se puede acceder mediante un dispositivo informático. Como se describe en la presente memoria descriptiva, el medio legible por computadora no incluye medios transitorios, por ejemplo, una señal de datos modulada y un portador.

Vale la pena señalar además que, el término "incluye", "contiene" o cualquier otra variante pretende cubrir la inclusión no exclusiva de modo que un proceso, un método, un producto o un dispositivo que incluya una serie de elementos no solo incluye estos elementos, sino que también incluye otros elementos que no se enumeran expresamente, o incluye además elementos inherentes a dicho proceso, método, producto o dispositivo. Un elemento precedido por "incluye un..." no excluye, sin más restricciones, la existencia de elementos idénticos adicionales en el proceso, método, producto o dispositivo que incluye el elemento.

Un experto en la técnica debe comprender que las implementaciones de la presente solicitud pueden proporcionarse como un método, un sistema o un producto de programa informático. Por lo tanto, la presente solicitud puede utilizar una forma de implementaciones de solo hardware, implementaciones de solo software o implementaciones con una combinación de software y hardware. Además, la presente solicitud puede utilizar una forma de un producto de programa informático implementado en uno o más medios de almacenamiento utilizables por computadora (que incluyen, pero no se limitan a una memoria de disco magnético, un CD-ROM y una memoria óptica) que incluyen código de programa utilizable por computadora.

Las descripciones anteriores son implementaciones de la presente solicitud y no pretenden limitar la presente solicitud. Un experto en la técnica puede realizar diversas modificaciones y cambios en la presente solicitud. Cualesquiera modificaciones, reemplazos equivalentes, mejoras, etc. caerán dentro del alcance de protección de las reivindicaciones de la presente solicitud.

REIVINDICACIONES

1. Un método para registrar una identidad de usuario, el método que comprende:
recibir (S301), mediante un dispositivo terminal, información de característica biométrica de un usuario que se va a verificar, en donde el usuario tiene una cuenta registrada con un servicio proporcionado por un servidor;
comparar (S302), mediante el dispositivo terminal, una pieza de información de característica biométrica estándar almacenada localmente que es consistente con la información de característica biométrica recibida del usuario que se va a verificar, en donde a cada una de las piezas de información de característica biométrica estándar almacenada localmente se le asigna un respectivo identificador de característica biométrica y se utiliza para determinar si un usuario respectivo se puede verificar cuando utiliza el servicio;
determinar, mediante el dispositivo terminal, si una clave privada correspondiente a un identificador de característica biométrica de la pieza de información de característica biométrica estándar almacenada localmente está almacenada en el dispositivo terminal, que comprende buscar (S303), mediante el dispositivo terminal y después de que la comparación tenga éxito, una clave privada correspondiente a un identificador de característica biométrica de la pieza de información de característica biométrica estándar almacenada localmente; y
en respuesta a determinar que una clave privada correspondiente a un identificador de característica biométrica de la pieza de información de característica biométrica estándar almacenada localmente no está almacenada en el dispositivo terminal, determinar que la información de característica biométrica recibida del usuario que se va a verificar pertenece al usuario, pero no es información de característica biométrica proporcionada por el usuario durante el registro inicial con el servidor y registrar (S304) directamente una identidad de usuario con el servidor en base a la información de característica biométrica recibida del usuario que se va a verificar y la clave privada y clave pública regeneradas correspondientes, en donde el servidor almacena la clave pública generada correspondiente a la información de característica biométrica recibida del usuario que se va a verificar (S304) y la relación de correspondencia entre el respectivo identificador de característica biométrica y la clave pública generada.

2. El método de acuerdo con la reivindicación 1, en donde antes de registrar la identidad de usuario con el servidor en base a la información de característica biométrica recibida del usuario que se va a verificar, el método comprende, además:
recibir una contraseña introducida por el usuario; y
verificar que la contraseña es correcta.

3. El método de acuerdo con la reivindicación 1, en donde registrar la identidad de usuario con el servidor en base a la información de característica biométrica recibida del usuario que se va a verificar comprende:
generar la clave privada y la clave pública correspondientes al identificador de característica biométrica de la información de característica biométrica estándar almacenada localmente en base al identificador de característica biométrica de la información de característica biométrica estándar almacenada localmente que coincide con la información de característica biométrica recibida del usuario que se va a verificar;
almacenar una relación de correspondencia entre el identificador de característica biométrica de la pieza de información de característica biométrica estándar almacenada localmente y la clave privada generada en el dispositivo terminal; y
enviar una relación de correspondencia entre el identificador de la pieza de información de característica biométrica estándar almacenada localmente y la clave pública generada al servidor para su almacenamiento.

4. El método de acuerdo con la reivindicación 1, en donde después de registrar la identidad de usuario en el servidor, el método comprende además:
enviar una solicitud de procesamiento de servicio al servidor en base a la información de característica biométrica recibida del usuario que se va a verificar, en donde el servidor realiza el procesamiento de servicio en base a la clave pública correspondiente a la información de característica biométrica recibida del usuario que se va a verificar.

5. El método de acuerdo con la reivindicación 4, en donde enviar la solicitud de procesamiento de servicio al servidor en base a la información de característica biométrica recibida del usuario que se va a verificar comprende:
firmar información de servicio en base a la clave privada generada y enviar la solicitud de procesamiento de servicio que comprende la información de servicio firmada y el identificador de la pieza de información biométrica estándar almacenada localmente al servidor, en donde el servidor recupera la clave pública correspondiente al identificador comprendido en la solicitud de procesamiento de servicio recibida y realiza el procesamiento de servicio en base a la clave pública determinada y la información de servicio firmada.

6. El método de acuerdo con la reivindicación 4 o 5, en donde la solicitud de procesamiento de servicio comprende una solicitud de pago.

7. El método de acuerdo con la reivindicación 4 o 5, que además comprende:
generar una solicitud para una entrada de usuario que comprende una contraseña para el servicio de consulta de información.

8. El método de acuerdo con una cualquiera de las reivindicaciones 1 a 6, en donde la información de característica biométrica representa una identidad de usuario e indica una característica física del usuario.

9. El método de acuerdo con la reivindicación 8, en donde la característica física del usuario comprende un iris de un ojo o una huella dactilar de un dedo.

10. Un dispositivo para el registro de identidad, el dispositivo que comprende una pluralidad de módulos configurados para realizar el método de una cualquiera de las reivindicaciones 1 a 9.

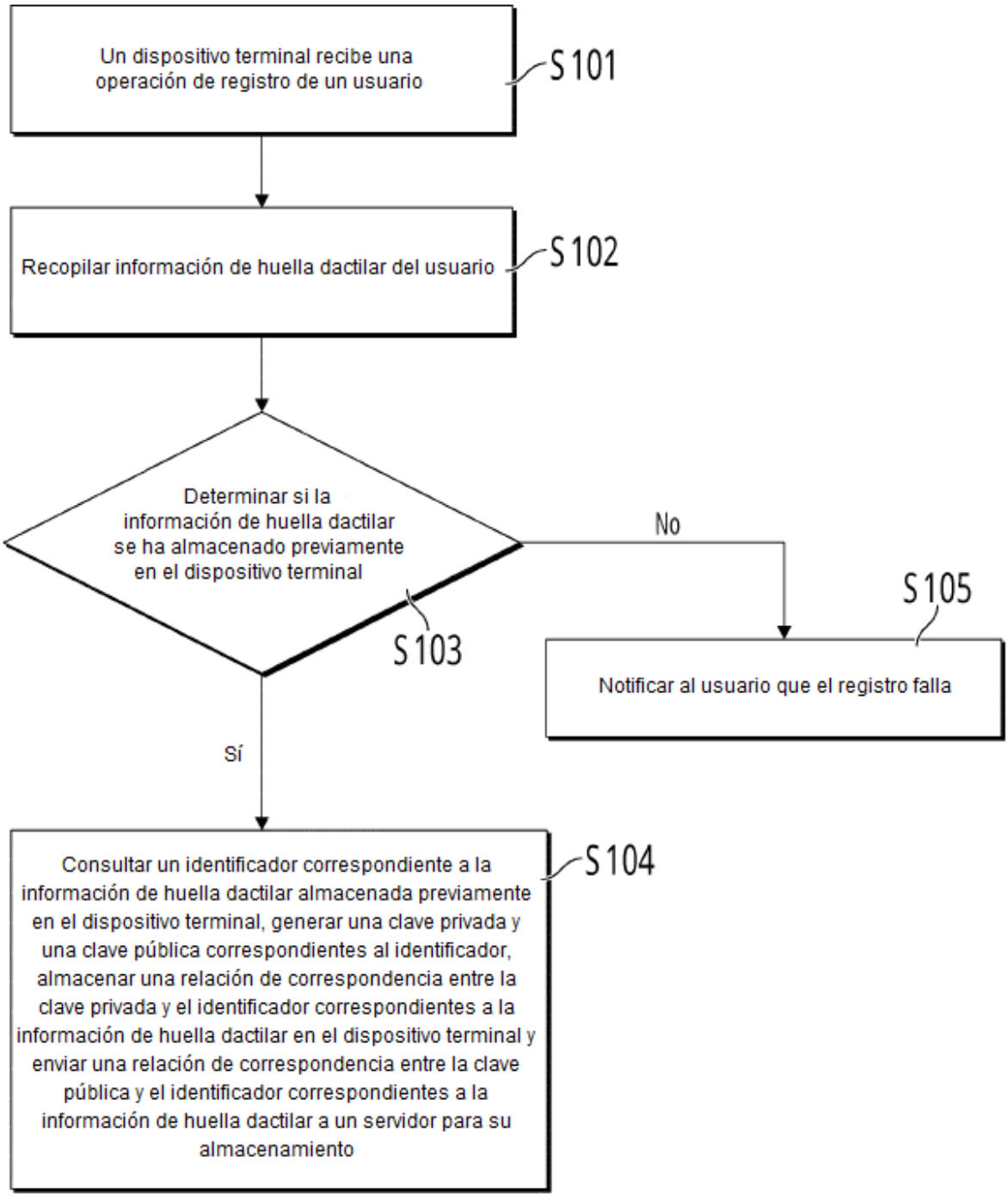
Un dispositivo terminal recibe una operación de registro de un usuario
S101
Recopilar información de huella dactilar del usuario
S102
Determinar si la información de huella dactilar se ha almacenado previamente en el dispositivo terminal
S103
No
S105
Notificar al usuario que el registro falla
Sí
Consultar un identificador correspondiente a la información de huella dactilar almacenada previamente en el dispositivo terminal, generar una clave privada y una clave pública correspondientes al identificador, almacenar una relación de correspondencia entre la clave privada y el identificador correspondientes a la información de huella dactilar en el dispositivo terminal y enviar una relación de correspondencia entre la clave pública y el identificador correspondientes a la información de huella dactilar a un servidor para su almacenamiento
S104

FIG. 1

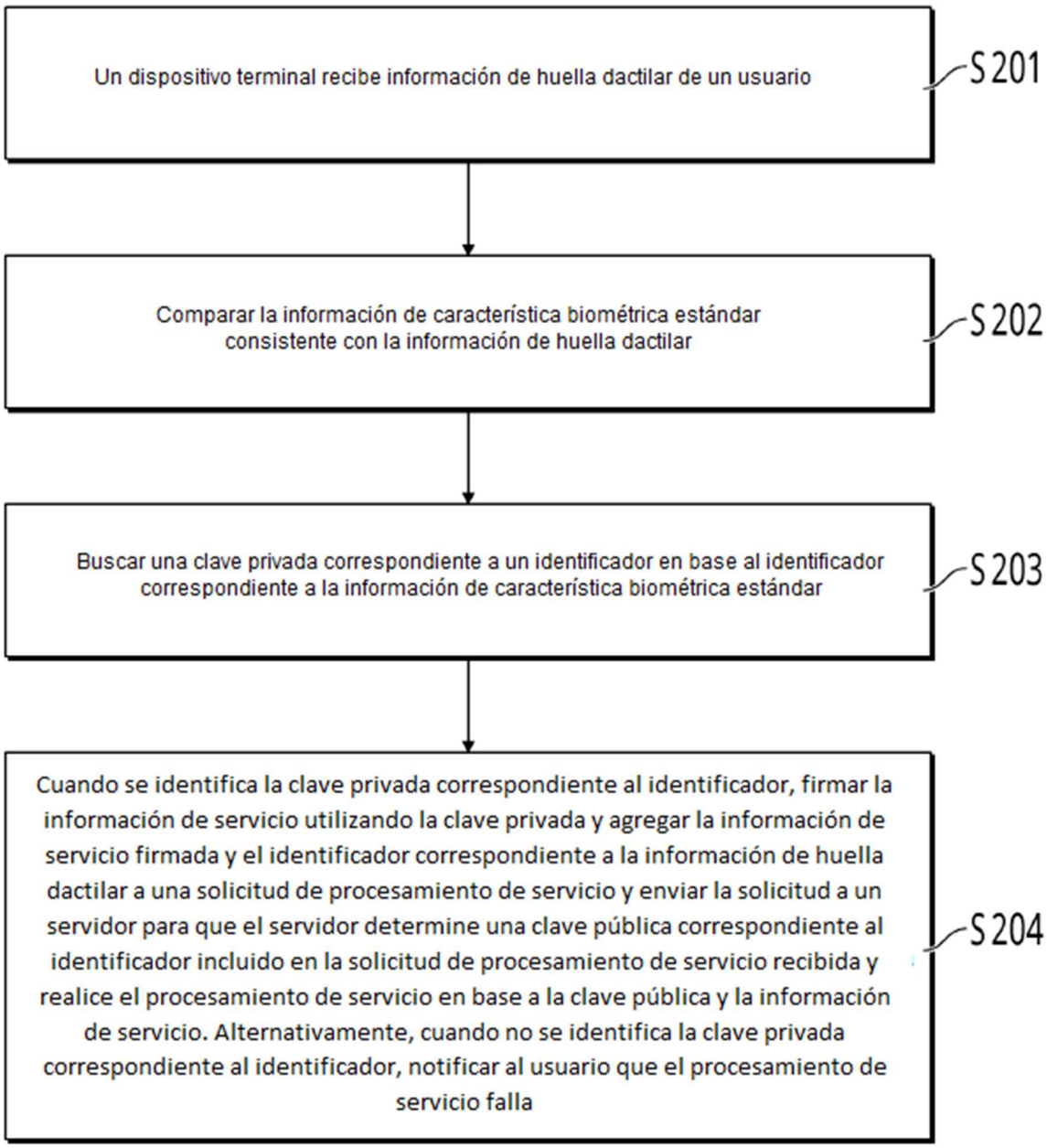
Un dispositivo terminal recibe información de huella dactilar de un usuario
S201
Comparar la información de característica biométrica estándar consistente con la información de huella dactilar
S202
Buscar una clave privada correspondiente a un identificador en base al identificador correspondiente a la información de característica biométrica estándar
S203
Cuando se identifica la clave privada correspondiente al identificador, firmar la información de servicio utilizando la clave privada y agregar la información de servicio firmada y el identificador correspondiente a la información de huella dactilar a una solicitud de procesamiento de servicio y enviar la solicitud a un servidor para que el servidor determine una clave pública correspondiente al identificador incluido en la solicitud de procesamiento de servicio recibida y realice el procesamiento de servicio en base a la clave pública y la información de servicio. Alternativamente, cuando no se identifica la clave privada correspondiente al identificador, notificar al usuario que el procesamiento de servicio falla
S204

FIG. 2

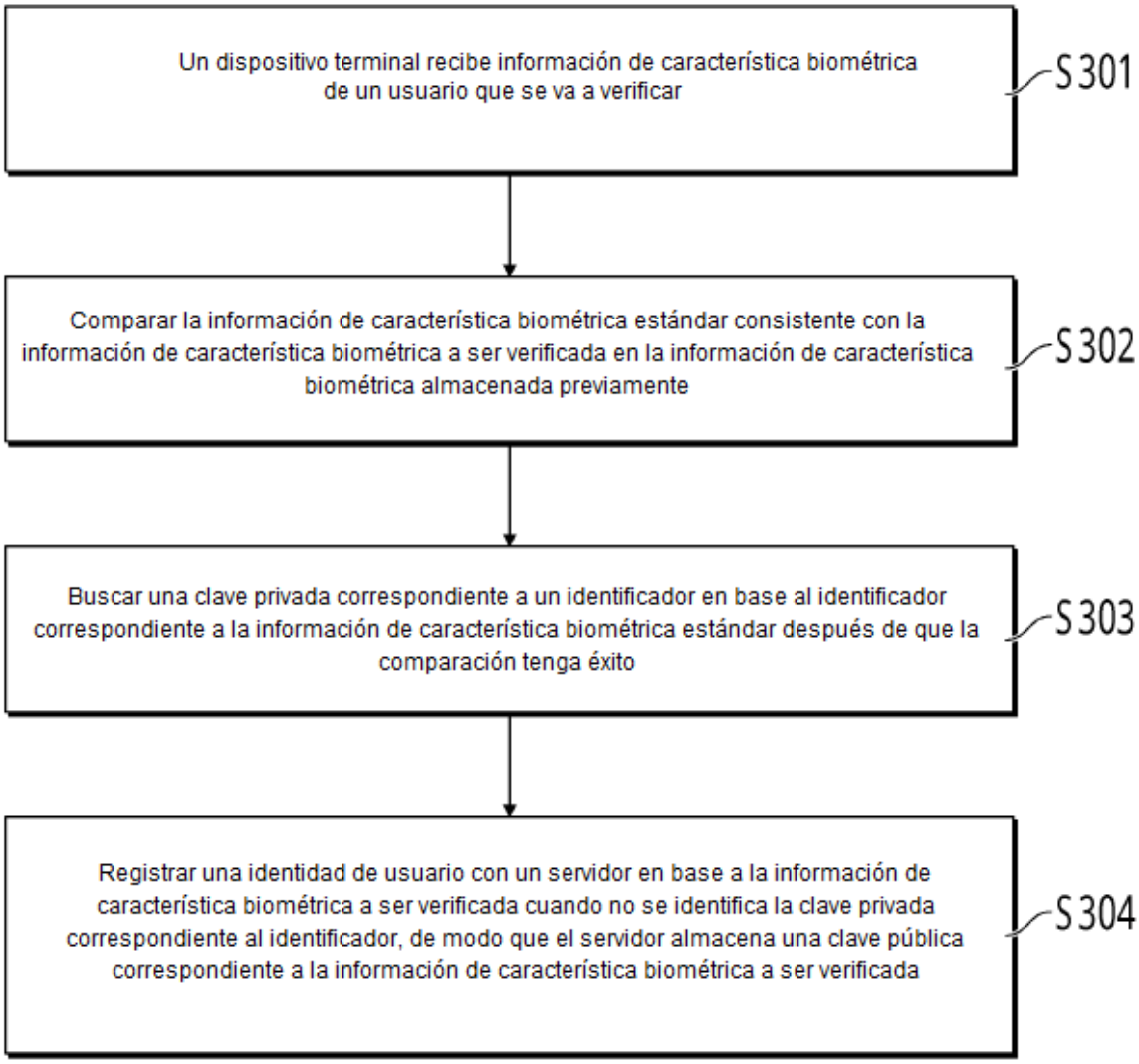
Un dispositivo terminal recibe información de característica biométrica de un usuario que se va a verificar
S301
Comparar la información de característica biométrica estándar consistente con la información de característica biométrica a ser verificada en la información de característica biométrica almacenada previamente
S302
Buscar una clave privada correspondiente a un identificador en base al identificador correspondiente a la información de característica biométrica estándar después de que la comparación tenga éxito
S303
Registrar una identidad de usuario con un servidor en base a la información de característica biométrica a ser verificada cuando no se identifica la clave privada correspondiente al identificador, de modo que el servidor almacena una clave pública correspondiente a la información de característica biométrica a ser verificada
S304

FIG. 3

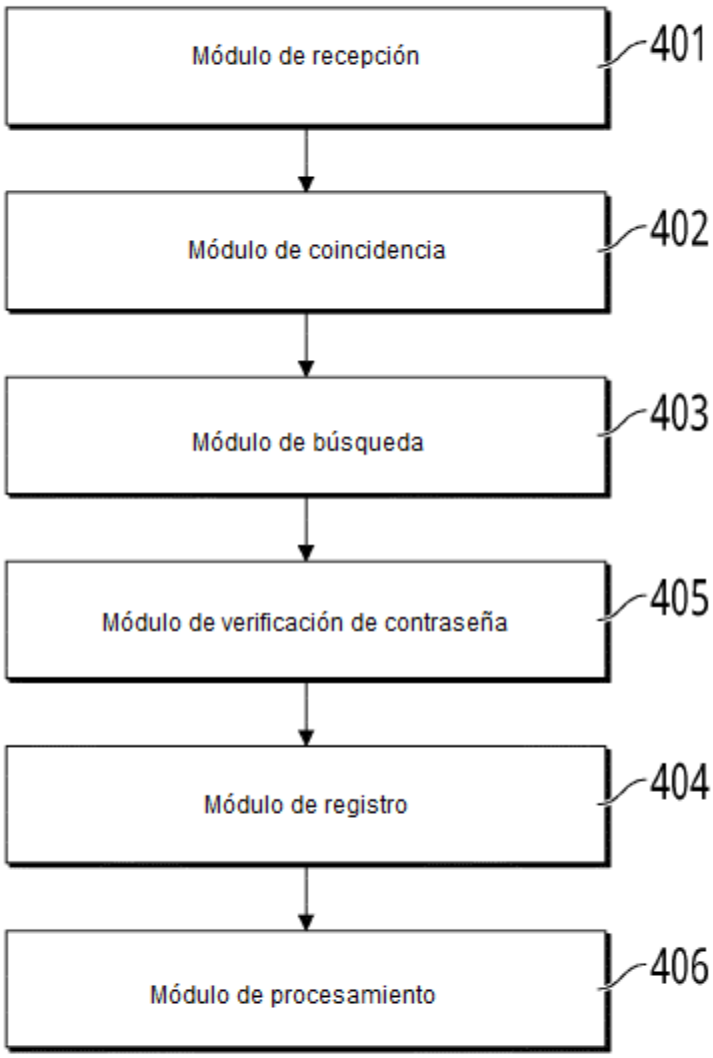
Módulo de recepción
401
Módulo de coincidencia
402
Módulo de búsqueda
403
Módulo de verificación de contraseña
405
Módulo de registro
404
Módulo de procesamiento
406

FIG. 4