(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 804 198**

(51) Int. CI.:

H04L 9/32 (2006.01)
H04W 12/06 (2009.01)
H04L 29/06 (2006.01)
G06Q 20/32 (2012.01)
G06Q 20/38 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **05.09.2016 PCT/CN2016/097999**

(87) Fecha y número de publicación internacional: **23.03.2017 WO17045539**

(96) Fecha de presentación y número de la solicitud europea: **05.09.2016 E 16845653 (1)**

(97) Fecha y número de publicación de la concesión europea: **27.05.2020 EP 3352412**

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

(30) Prioridad:

14.09.2015 CN 201510583968

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
04.02.2021

(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:

SUN, YUANBO

(74) Agente/Representante:

VIDAL GONZÁLEZ, Maria Ester

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

DESCRIPCIÓN

Método y dispositivo de autenticación de identidad

Esta solicitud reivindica prioridad de la solicitud de patente china núm. 201510583968.6 presentada el 14 de septiembre de 2015 y titulada "METHOD AND DEVICE FOR IDENTITY AUTHENTICATION".

Campo técnico

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

Antecedentes de la técnica

Un dispositivo portátil es un dispositivo portátil que se usa directamente en el cuerpo de un usuario o integrado en la ropa o un accesorio del usuario. Actualmente, existen formas de productos convencionales que incluyen productos en una categoría de relojes que se usan en la muñeca (que incluye productos tales como relojes y correas de muñeca), una categoría de zapatos que se usan en los pies (que incluye zapatos, calcetines u otros productos futuros que se usan en las piernas), y una categoría de vidrio que se usa en la cabeza (que incluye anteojos, cascos, cintas para la cabeza y similares); y también hay varias formas de productos no convencionales, tales como ropa inteligente, mochilas escolares, muletas y accesorios.

Debido a que los dispositivos portátiles pueden ser portátiles cuando se usan en el cuerpo, se espera que los dispositivos portátiles estén más involucrados en la autenticación de identidad u operen un proceso de procesamiento correspondiente para una serie de servicios, a fin de lograr una interacción más estrecha con los usuarios y mejorar la seguridad.

Por lo tanto, cómo implementar la autenticación de pago o una operación de autenticación de identidad en otro proceso de operación con base en un dispositivo portátil se ha convertido en uno de los enfoques de investigación en el campo de las tecnologías informáticas.

La autenticación de pago, un tipo especial de autenticación de identidad, se refiere a un comportamiento operativo de juzgar la legitimidad de un comportamiento de pago relacionado con la transferencia de fondos que actualmente realiza un usuario. En relación con el fondo, dicha autenticación de identidad se ve particularmente cuestionada en términos de seguridad y conveniencia.

En la técnica anterior, un procedimiento convencional para implementar la autenticación de identidad, especialmente un proceso de operación de autenticación de pago, con base en un dispositivo portátil es sustancialmente el siguiente:
Después de que un terminal móvil vinculado al dispositivo portátil recibe una solicitud de autenticación de pago, el terminal móvil es responsable de autenticar la legitimidad de la solicitud de autenticación de pago. Después de que la autenticación se realiza correctamente y se completa la deducción de tarifa, el terminal móvil envía la información de éxito de la deducción de tarifa correspondiente al dispositivo portátil. De lo contrario, el terminal móvil envía la información de falla de deducción de tarifa correspondiente al dispositivo portátil, que muestra un resultado de deducción de tarifa.

En un proceso de implementación de la presente solicitud, el solicitante descubrió que el método convencional de autenticación de identidad basado en dispositivo portátil, especialmente el método de autenticación de pago, tiene al menos los siguientes problemas:
En la técnica anterior, la informática relacionada con la autenticación sobre la legitimidad de la solicitud de autenticación de pago se implementa en el terminal móvil, y el dispositivo portátil solo es responsable de mostrar el resultado de la deducción de tarifa.

Además, cuando la informática relacionada se implementa en el terminal móvil, un usuario tiene un sentido débil de participación en un proceso de pago, y el proceso de pago tiene baja seguridad, lo que afecta la tasa de éxito del pago.

Por lo tanto, los expertos en la técnica necesitan urgentemente encontrar un método que pueda mejorar el sentido de participación de un usuario en un proceso de autenticación de identidad, mejorar la seguridad del proceso de autenticación y aumentar la tasa de éxito de autenticación.

El documento US 2013/0054960 describe un dispositivo de usuario que incluye un procesador y una memoria configurados para almacenar una aplicación, un administrador de sesión, un identificador de aplicación y una biblioteca compartida. El administrador de sesión configura el procesador para comunicar el identificador de la aplicación y los datos del identificador de la aplicación a un servidor de autenticación y permitir la ejecución de la aplicación en respuesta a la autenticación de la aplicación por parte del servidor de autenticación.

El documento US 2005/0101295 describe un método para respaldar el pago sin efectivo. Una identidad de abonado móvil almacenada en el módulo de identificación de abonado del terminal móvil se envía a una unidad de interfuncionamiento de pagos. La unidad de interfuncionamiento de pagos transmite la identidad del abonado móvil a un servidor de autenticación de un sistema de comunicación móvil que responde un número de autenticación y una respuesta firmada. El número de autenticación se envía al terminal móvil que calcula una respuesta firmada y transmite la respuesta firmada al servidor de interfuncionamiento de pagos. Este servidor compara las respuestas firmadas recibidas del servidor de autenticación y del terminal móvil y envía un mensaje de confirmación a una unidad P0S o un sistema de facturación, si el resultado firmado recibido es correcto.

Resumen de la invención

Las modalidades de la presente solicitud proporcionan un método y un dispositivo para la autenticación de identidad, a fin de mejorar el sentido de participación del usuario en un proceso de autenticación de identidad, mejorar la seguridad del proceso de autenticación de identidad y aumentar la tasa de éxito de autenticación de identidad, especialmente para un proceso de autenticación de pago.

Para lograr los objetivos técnicos anteriores, la presente solicitud proporciona un método de autenticación de identidad, implementado en un dispositivo terminal que incluye una interfaz estándar preestablecida configurada para comunicarse con una aplicación de servicio de un tipo dedicado, y el método incluye específicamente:
recibir, por el dispositivo terminal a través de la interfaz estándar preestablecida, un mensaje de solicitud de autenticación de identidad enviado por un servidor correspondiente a la aplicación de servicio del tipo dedicado, en el que el mensaje de solicitud de autenticación de identidad es enviado por el servidor al dispositivo terminal después de que el servidor recibe una solicitud de servicio de la aplicación de servicio del tipo dedicado;
verificar, por el dispositivo terminal, una firma en el mensaje de solicitud de autenticación de identidad de acuerdo con una clave pública de la aplicación de servicio del tipo dedicado;
adquirir, por el dispositivo terminal si la verificación tiene éxito, información de autenticación de servicio de una cuenta correspondiente al mensaje de solicitud de autenticación de identidad a partir de información de autenticación de servicio previamente almacenada localmente; y
devolver, mediante el dispositivo terminal, un mensaje de respuesta de verificación que transporta la información de autenticación de servicio adquirida al servidor a través de la interfaz estándar preestablecida.

Además, las modalidades de la presente aplicación proporcionan además un método de autenticación de identidad, implementado en un servidor correspondiente a una aplicación de servicio de un tipo dedicado, en el que el servidor se comunica con un dispositivo terminal a través de una interfaz estándar preestablecida incluida en el dispositivo terminal, y el método incluye específicamente:
recibir, por el servidor, una solicitud de servicio de la aplicación de servicio del tipo dedicado;
enviar, por el servidor, un mensaje de solicitud de autenticación de identidad al dispositivo terminal a través de la interfaz estándar preestablecida incluida en el dispositivo terminal; recibir, por el servidor cuando una solicitud de autenticación de identidad tiene éxito, un mensaje de respuesta de verificación que es devuelto por el dispositivo terminal a través de la interfaz estándar preestablecida y transporta información de autenticación de servicio; y
procesar, por el servidor, la solicitud de servicio de acuerdo con el mensaje de autenticación del servicio.

Además, las modalidades de la presente solicitud proporcionan además un dispositivo terminal, que incluye específicamente:
una interfaz estándar preestablecida configurada para comunicarse con una aplicación de servicio de un tipo dedicado;
un módulo receptor configurado para recibir, a través de la interfaz estándar preestablecida, un mensaje de solicitud de autenticación de identidad enviado por un servidor correspondiente a la aplicación de servicio del tipo dedicado, en donde el servidor envía el mensaje de solicitud de autenticación de identidad al dispositivo terminal después de que el servidor recibe una solicitud de servicio de la aplicación de servicio del tipo dedicado;
un módulo de verificación configurado para verificar, de acuerdo con una clave pública de la aplicación de servicio del tipo dedicado, una firma en el mensaje de solicitud de autenticación de identidad recibido por el módulo receptor;
un módulo de adquisición configurado para adquirir, cuando la verificación por el módulo de verificación tiene éxito, la información de autenticación de servicio de una cuenta correspondiente al mensaje de solicitud de autenticación de identidad de la información de autenticación de servicio almacenada previamente en el dispositivo terminal; y
un módulo de retroalimentación configurado para devolver un mensaje de respuesta de verificación que transporta la información de autenticación del servicio adquirida por el módulo de adquisición al servidor a través de la interfaz estándar preestablecida.

Además, las modalidades de la presente solicitud proporcionan además un servidor, que corresponde a una aplicación de servicio de un tipo dedicado, y que incluye específicamente:
un módulo de envío configurado para enviar, cuando se recibe una solicitud de servicio de la aplicación de servicio del tipo dedicado, un mensaje de solicitud de autenticación de identidad a un dispositivo terminal a través de una interfaz estándar preestablecida incluida en el dispositivo terminal;

un módulo receptor configurado para recibir, cuando una solicitud de autenticación de identidad tiene éxito, un mensaje de respuesta de verificación que es devuelto por el dispositivo terminal a través de la interfaz estándar preestablecida y transporta información de autenticación de servicio; y
un módulo de procesamiento configurado para procesar la solicitud de servicio de acuerdo con el mensaje de autenticación de servicio recibido por el módulo receptor.

En comparación con la técnica anterior, las soluciones técnicas propuestas en las modalidades de la presente solicitud incluyen los siguientes efectos técnicos beneficiosos: las modalidades de la presente solicitud describen un método y un dispositivo para autenticación de identidad, implementado en un sistema compuesto por un servidor y un dispositivo terminal que incluye una interfaz estándar preestablecida configurada para comunicarse con una aplicación de servicio de un tipo dedicado. Mediante las soluciones técnicas propuestas en la presente descripción, cuando se requiere una operación de autenticación de identidad, el servidor puede solicitar información de autenticación de servicio de una cuenta de la aplicación de servicio del tipo dedicado desde el dispositivo terminal a través de la interfaz estándar preestablecida, y el dispositivo terminal puede realizar la verificación de seguridad en este proceso de acuerdo con una regla de verificación correspondiente, y enviar información de autenticación del servicio almacenada localmente de vuelta al servidor para su posterior procesamiento solo cuando la verificación tenga éxito. Como tal, la seguridad de un proceso de autenticación de identidad se puede garantizar por medio de la interfaz estándar preestablecida vinculada a la aplicación de servicio del tipo dedicado y la verificación de seguridad del dispositivo terminal, y el sentido de participación del operador del dispositivo terminal en este proceso puede mejorarse mediante el uso de la información de autenticación de identidad almacenada actualmente en el dispositivo terminal. Cuando el dispositivo terminal es específicamente un dispositivo portátil, puede mejorarse el sentido de participación del usuario en el proceso de autenticación de identidad, puede mejorarse la seguridad del proceso de autenticación de identidad y se puede aumentar la tasa de éxito de autenticación de identidad, especialmente para un proceso de autenticación de pago.

Breve descripción de los dibujos

Para describir las soluciones técnicas de la presente solicitud más claramente, a continuación, se presentan brevemente los dibujos adjuntos para ilustrar las modalidades. Aparentemente, los dibujos en la siguiente descripción simplemente muestran algunas modalidades de la presente solicitud, y los expertos en la técnica pueden derivar otros dibujos con base en estos dibujos adjuntos sin esfuerzos creativos.

La Figura 1 es un diagrama de flujo esquemático de un método de autenticación de identidad de acuerdo con una modalidad de la presente solicitud;
La Figura 2 es un diagrama de flujo esquemático de un proceso de enlace en un método de autenticación de identidad de acuerdo con una modalidad de la presente solicitud;
La Figura 3 es un diagrama de flujo esquemático de un proceso de autenticación en un método de autenticación de identidad de acuerdo con una modalidad de la presente solicitud;
La Figura 4 es un diagrama estructural esquemático de un dispositivo terminal de acuerdo con una modalidad de la presente solicitud; y
La Figura 5 es un diagrama estructural esquemático de un servidor de acuerdo con una modalidad de la presente solicitud.

Descripción detallada

Como se indica en la técnica anterior de la presente solicitud, en la técnica anterior, la informática relacionada con la autenticación sobre la legitimidad de una solicitud de autenticación de identidad, especialmente una solicitud de autenticación de pago, se implementa en un terminal móvil, y un dispositivo portátil asociado solo es responsable para mostrar un resultado de procesamiento; como un resultado, en dicho proceso operativo, un usuario tiene un débil sentido de participación en un proceso de autenticación de identidad, especialmente en un proceso de pago, y el proceso tiene poca seguridad, lo que a su vez puede afectar la tasa de éxito del servicio.

Sin embargo, el inventor de la presente solicitud descubrió que, en comparación con un terminal móvil, un dispositivo portátil tiene las siguientes ventajas durante el procesamiento:

1. Es más conveniente operar, y también se mejora el sentido de participación del usuario correspondiente en un proceso de procesamiento correspondiente.

2. Es más seguro operar con el dispositivo portátil, por ejemplo, la operación es más privada y no se puede espiar fácilmente, y también se mejora la seguridad del proceso de pago correspondiente.

Con base en las dos ventajas anteriores, el procesamiento con un dispositivo portátil puede aumentar la tasa de éxito de un proceso de pago.

Con base en el análisis anterior, para resolver los problemas técnicos anteriores, las modalidades de la presente solicitud describen un método de autenticación de identidad que se implementa en un dispositivo portátil.

Ciertamente, este método también puede implementarse en un dispositivo terminal de otro tipo, y dicho cambio no afecta el alcance de protección de la presente solicitud.

Como se muestra en la Figura 1, que es un diagrama de flujo esquemático de un método de autenticación de identidad de acuerdo con una primera modalidad de la presente solicitud, el método se implementa en un dispositivo terminal que incluye una interfaz estándar preestablecida configurada para comunicarse con una aplicación de servicio de un tipo dedicado, y el método específicamente incluye:

Etapa S101. El dispositivo terminal recibe, a través de la interfaz estándar preestablecida, un mensaje de solicitud de autenticación de identidad enviado por un servidor correspondiente a la aplicación de servicio del tipo dedicado.

El servidor envía el mensaje de solicitud de autenticación de identidad al dispositivo terminal después de que el servidor recibe una solicitud de servicio de la aplicación de servicio del tipo dedicado.

En un escenario de aplicación específico, la aplicación de servicio del tipo dedicado como se describe en la presente descripción se refiere principalmente a una aplicación de servicio de un tipo que coincide con la interfaz estándar preestablecida y requiere una operación de autenticación de identidad durante la ejecución del servicio específico. Después de que un tipo coincide con una interfaz estándar preestablecida (que puede definirse sobre la interfaz o limitarse en un protocolo estándar), solo se transmite un mensaje activado por una aplicación de servicio que coincide con el tipo a través de la interfaz estándar preestablecida. Dicha limitación puede filtrar efectivamente un proceso de intercambio de información de una aplicación de servicio de otro tipo, evitando que otra información interfiera con un proceso de intercambio de información de la aplicación de servicio del tipo dedicado y mejorando la eficiencia del procesamiento de información correspondiente. Además, una limitación en el tipo dedicado también puede proteger eficazmente la entrada o el ataque de otros paquetes falsificados o la señalización a través de la interfaz estándar preestablecida, mejorando la seguridad de un proceso de autenticación de identidad.

Debe observarse que, en el procesamiento posterior, el intercambio de información entre el dispositivo terminal y la aplicación de servicio del tipo dedicado se implementa a través de la interfaz estándar preestablecida, y se describe correspondientemente en una etapa correspondiente posterior, y los detalles no se describen en la presente descripción.

Mediante la limitación de la interfaz estándar preestablecida, el dispositivo terminal no recibe un mensaje enviado por otra aplicación de servicio a través de la interfaz estándar preestablecida, y ciertamente la solución técnica propuesta en esta modalidad puede no activarse. Como tal, se puede implementar el filtrado de información en el proceso de autenticación de identidad, se puede evitar la interferencia de otro mensaje y puede mejorarse la seguridad del proceso de autenticación de identidad.

Etapa S102. El dispositivo terminal verifica una firma en el mensaje de solicitud de autenticación de identidad de acuerdo con una clave pública de la aplicación de servicio del tipo dedicado.

Si la verificación tiene éxito, se puede considerar que el mensaje de solicitud de autenticación de identidad es un mensaje legítimo enviado por la aplicación de servicio del tipo dedicado, y es seguro, y la etapa S103 puede realizarse más adelante.

Si la verificación falla, se puede considerar que el mensaje de solicitud de autenticación de identidad no es un mensaje legítimo enviado por la aplicación de servicio del tipo dedicado y, por lo tanto, el mensaje de solicitud de autenticación de identidad se descarta directamente.

Etapa S103. El dispositivo terminal adquiere información de autenticación de servicio de una cuenta correspondiente al mensaje de solicitud de autenticación de identidad a partir de información de autenticación de servicio previamente almacenada localmente.

Específicamente, en esta modalidad, antes de que se realice esta etapa, un proceso de operación de almacenamiento previo local de información de autenticación del servicio por parte del dispositivo terminal es específicamente como sigue:
Primero, el dispositivo terminal recibe, a través de la interfaz estándar preestablecida, un mensaje de solicitud de registro de vinculación para una cuenta que es enviada por la aplicación de servicio del tipo dedicado.

Luego, el dispositivo terminal verifica la legitimidad del mensaje de solicitud de registro de vinculación, es decir, verifica una firma en el mensaje de solicitud de registro de vinculación de acuerdo con la clave pública de la aplicación de servicio del tipo dedicado.

Si la verificación tiene éxito, el dispositivo terminal adquiere la información de autenticación del servicio que se incluye en el mensaje de solicitud de registro de vinculación y, de manera correspondiente, almacena la información de autenticación del servicio y la información de identificación de identidad de la cuenta localmente para una

operación de autenticación posterior, en donde la información de identificación de identidad se usa para indicar la cuenta a la que pertenece la información de autenticación del servicio.

Si la verificación falla, se puede considerar que el mensaje de solicitud de registro de vinculación no es un mensaje legítimo enviado por la aplicación de servicio del tipo dedicado y no es válido, por lo que el mensaje de solicitud de registro de vinculación se descarta directamente.

Finalmente, después de completar el almacenamiento de la información de autenticación del servicio y la información de identificación de identidad, el dispositivo terminal genera un mensaje de respuesta de registro de acuerdo con la información del identificador del dispositivo terminal, y devuelve el mensaje de respuesta de registro a la aplicación de servicio del tipo dedicado a través de la interfaz estándar preestablecida.

En un escenario de aplicación específico, un proceso de generación del mensaje de respuesta de registro es específicamente el siguiente:
adquirir, por el dispositivo terminal, información de identificador único e información del modelo de dispositivo del dispositivo terminal;
reunir, mediante el dispositivo terminal, la información del identificador único y la información del modelo del dispositivo de acuerdo con un formato de datos especificado por la aplicación de servicio del tipo dedicado; y
firmar, mediante el dispositivo terminal, la información reunida mediante el uso de una clave privada local y generar el mensaje de respuesta de registro.

Ciertamente, teniendo en cuenta que un usuario de la cuenta puede cambiar la información de autenticación del servicio (por ejemplo, una contraseña de pago, un gesto de pago o similar), la información almacenada actualmente puede actualizarse posteriormente mediante el siguiente procedimiento:

Etapa A. El dispositivo terminal recibe, a través de la interfaz estándar preestablecida, un mensaje de solicitud de actualización de información de autenticación de servicio para una cuenta que es enviada por la aplicación de servicio del tipo dedicado.

Etapa B. El dispositivo terminal verifica una firma en el mensaje de solicitud de actualización de información de autenticación de servicio de acuerdo con la clave pública de la aplicación de servicio del tipo dedicado.

Si la verificación falla, se puede considerar que el mensaje de solicitud de actualización de información de autenticación de servicio no es un mensaje legítimo enviado por la aplicación de servicio del tipo dedicado y no es válido, por lo que el mensaje de solicitud de actualización de información de autenticación de servicio se descarta directamente.

Si la verificación tiene éxito, se realiza la etapa C.

Etapa C. El dispositivo terminal juzga si la información de identificación de identidad correspondiente a la información de autenticación de servicio almacenada localmente es coherente con la información de identificación de identidad transportada en el mensaje de solicitud de actualización de información de autenticación de servicio.

Si son consistentes, se puede determinar que la información de autenticación de servicio de la misma cuenta se ha almacenado en el dispositivo terminal, que coincide con el mensaje de solicitud de actualización de información de autenticación de servicio, y se activa una operación posterior de la etapa D.

Por el contrario, si son inconsistentes, se puede determinar que la información de autenticación de servicio de la misma cuenta no se almacena en el dispositivo terminal, que no puede coincidir con el mensaje de solicitud de actualización de información de autenticación de servicio, no hay ningún objeto para actualizar, y posteriormente el procesamiento puede determinarse de acuerdo con una necesidad real.

Etapa D. El dispositivo terminal adquiere, la información de autenticación del servicio transportada en el mensaje de solicitud de actualización de información de autenticación del servicio.

Etapa E. El dispositivo terminal juzga si la información de versión de la información de autenticación de servicio adquirida es mayor que la información de versión de la información de autenticación de servicio correspondiente almacenada actualmente de manera local.

Mediante esta etapa, se puede determinar si la información de autenticación del servicio almacenada actualmente en el dispositivo terminal debe actualizarse.

Si el resultado del juicio es sí, puede indicar que la información de autenticación del servicio local no es de una versión más reciente y necesita actualizarse, y el dispositivo terminal reemplaza la información de autenticación del servicio correspondiente almacenada actualmente con la información de autenticación del servicio adquirida.

Si el resultado del juicio es no, es decir, la información de versión de la información de autenticación de servicio adquirida es igual o menor que la información de versión de la información de autenticación de servicio correspondiente almacenada actualmente de manera local, puede indicar que la información de autenticación de servicio local no necesita actualizarse y la operación de actualización actual finalizará.

Etapa S104. El dispositivo terminal transporta la información de autenticación de servicio adquirida en un mensaje de respuesta de verificación y devuelve el mensaje de respuesta de verificación al servidor a través de la interfaz estándar preestablecida.

En un escenario de aplicación específico, en aras de la seguridad, cuando se devuelve información de credenciales de pago en esta etapa, la información de autenticación del servicio puede cifrarse y guardarse como un paquete de datos de respuesta. Después de recibir el paquete de datos de respuesta, el servidor obtiene la información de autenticación del servicio por descifrado, para completar una operación de procesamiento de servicio posterior.

En un escenario de aplicación específico, después de completar esa etapa, se puede incluir un proceso de confirmación correspondiente, que se describe específicamente a continuación:
recibir, por el dispositivo terminal a través de la interfaz estándar preestablecida, una solicitud de confirmación que es enviada por el servidor correspondiente a la aplicación de servicio del tipo dedicado;
adquirir, por el dispositivo terminal, información de tipo modo de confirmación incluida en la solicitud de confirmación; y
completar, mediante el dispositivo terminal, una operación de confirmación correspondiente de acuerdo con la información de tipo modo de confirmación.

Específicamente, en esta modalidad, la información de tipo modo de confirmación incluida en la solicitud de confirmación puede incluir cualquiera o cualquier combinación de los siguientes modos de confirmación:
confirmación de texto, confirmación de sonido y confirmación de vibración.

De manera correspondiente, por ejemplo, la confirmación de texto puede mostrar directamente una línea de caracteres "su pago se realizó correctamente", "procesamiento de servicio exitoso" o similares en el dispositivo terminal, y ciertamente, una condición previa es que el dispositivo terminal tenga una pantalla de visualización. La confirmación de sonido puede estar emitiendo un "tono de llamada" preestablecido. La confirmación de vibración puede estar vibrando por un número de veces preestablecido o un período de tiempo continuo.

Esta operación de confirmación se realiza principalmente para permitir al usuario conocer con precisión el resultado del procesamiento de un servicio. Ciertamente, también puede establecerse que no se requiera ninguna operación adicional cuando el procesamiento del servicio tenga éxito. Dicha configuración puede ajustarse de acuerdo con una necesidad real y no afecta el alcance de protección de la presente solicitud.

El proceso de descripción anterior describe un proceso de implementación de solución en un lado del dispositivo terminal. En consecuencia, las modalidades de la presente descripción también proponen un procedimiento de implementación de solución en el lado del servidor. El método se implementa en un servidor correspondiente a una aplicación de servicio de un tipo dedicado, en donde el servidor se comunica con un dispositivo terminal a través de una interfaz estándar preestablecida incluida en el dispositivo terminal, y el método incluye específicamente las siguientes etapas:
Primero, el servidor recibe una solicitud de servicio de la aplicación de servicio del tipo dedicado.

Luego, el servidor envía un mensaje de solicitud de autenticación de identidad al dispositivo terminal a través de la interfaz estándar preestablecida incluida en el dispositivo terminal.

Cuando una solicitud de autenticación de identidad tiene éxito, el servidor recibe un mensaje de respuesta de verificación que es devuelto por el dispositivo terminal a través de la interfaz estándar preestablecida y transporta información de autenticación de servicio.

El servidor procesa la solicitud de servicio de acuerdo con el mensaje de autenticación del servicio.

En un escenario de aplicación específico, antes de que el servidor reciba la solicitud de servicio de la aplicación de servicio del tipo dedicado, se incluye además un proceso de almacenamiento previo de información de autenticación de servicio:
enviar, por el servidor, un mensaje de solicitud de registro de vinculación para una cuenta al dispositivo terminal a través de la interfaz estándar preestablecida incluida en el dispositivo terminal, en donde el mensaje de solicitud de registro de vinculación transporta información de autenticación de servicio de la cuenta; y
recibir, por el servidor cuando el enlace de registro tiene éxito, un mensaje de respuesta de registro que es devuelto por el dispositivo terminal a través de la interfaz estándar preestablecida, y el servidor confirma que el dispositivo terminal está vinculado exitosamente a la cuenta, en donde el mensaje de respuesta de registro transporta información de identificación del dispositivo terminal.

Este proceso de almacenamiento previo corresponde al proceso de operación de almacenamiento previo local de información de autenticación del servicio por parte del dispositivo terminal en la etapa S103, y los detalles no se describen nuevamente en la presente descripción.

Además, después de que el servidor confirme que el dispositivo terminal está vinculado exitosamente a la cuenta, el método comprende, además:
enviar, por el servidor cuando la información de autenticación de servicio de la cuenta necesita ser actualizada, un mensaje de solicitud de actualización de información de autenticación de servicio para la cuenta al dispositivo terminal a través de la interfaz estándar preestablecida incluida en el dispositivo terminal, en donde el mensaje de solicitud de actualización de información de autenticación de servicio transporta la información de autenticación del servicio que necesita ser actualizada de la cuenta.

Este proceso también corresponde al proceso de procesamiento de la etapa A a la etapa E en la etapa S103, y los detalles no se describen aquí nuevamente.

De acuerdo con otro aspecto, después de que el servidor procesa la solicitud de servicio de acuerdo con el mensaje de autenticación del servicio, se puede incluir un proceso de confirmación correspondiente, que se describe específicamente como sigue:
enviar, por el servidor después de que se complete el procesamiento de la solicitud de servicio, una solicitud de confirmación que transporte información de tipo modo de confirmación al dispositivo terminal a través de la interfaz estándar preestablecida incluida en el dispositivo terminal, de modo que el dispositivo terminal complete una operación de confirmación correspondiente de acuerdo con la información de tipo modo de confirmación.

Un proceso después del envío de la solicitud de confirmación corresponde a un proceso de confirmación posterior en la etapa S104, y los detalles no se describen aquí nuevamente.

Debe observarse aquí que, en las etapas anteriores, cada mensaje recibido por el dispositivo terminal a través de la interfaz estándar preestablecida incluye al menos información de tipo de operación e información de firma del mensaje.

La información de la firma debe coincidir con la aplicación de servicio del tipo dedicado correspondiente a la interfaz estándar preestablecida y, por lo tanto, se puede verificar de acuerdo con la clave pública de la aplicación de servicio del tipo dedicado. Si la verificación falla, ciertamente se puede determinar que el mensaje actual no coincide con el tipo dedicado. Como tal, se puede filtrar un mensaje no relacionado y puede mejorarse la seguridad.

En comparación con la técnica anterior, las soluciones técnicas propuestas en las modalidades de la presente solicitud incluyen los siguientes efectos técnicos beneficiosos: las modalidades de la presente solicitud describen un método y un dispositivo para autenticación de identidad, implementado en un sistema compuesto por un servidor y un dispositivo terminal que incluye una interfaz estándar preestablecida configurada para comunicarse con una aplicación de servicio de un tipo dedicado. Mediante las soluciones técnicas propuestas en la presente solicitud, cuando se requiere una operación de autenticación de identidad, el servidor puede solicitar información de autenticación de servicio de una cuenta de la aplicación de servicio del tipo dedicado desde el dispositivo terminal a través de la interfaz estándar preestablecida, y el dispositivo terminal puede realizar la verificación de seguridad en este proceso de acuerdo con una regla de verificación correspondiente, y enviar información de autenticación del servicio almacenada localmente de vuelta al servidor para su posterior procesamiento solo cuando la verificación tenga éxito. Como tal, la seguridad de un proceso de autenticación de identidad se puede garantizar por medio de la interfaz estándar preestablecida vinculada a la aplicación de servicio del tipo dedicado y la verificación de seguridad del dispositivo terminal, y el sentido de participación del operador del dispositivo terminal en este proceso puede ser mejorado mediante el uso de la información de autenticación de identidad almacenada actualmente en el dispositivo terminal. Cuando el dispositivo terminal es específicamente un dispositivo portátil, puede mejorarse el sentido de participación del usuario en el proceso de autenticación de identidad, puede mejorarse la seguridad del proceso de autenticación de identidad y puede aumentarse la tasa de éxito de autenticación de identidad, especialmente para un proceso de autenticación de pago.

Las soluciones técnicas en la presente solicitud se describen clara y completamente a continuación con referencia a los dibujos adjuntos en la presente solicitud. Aparentemente, las modalidades que se describirán son simplemente algunas en lugar de todas las modalidades de la presente solicitud. Todas las demás modalidades obtenidas por expertos de habilidad ordinaria en la técnica con base en las modalidades de la presente solicitud sin esfuerzos creativos estarán dentro del alcance de protección de la presente solicitud.

Teniendo en cuenta que un dispositivo portátil se transporta junto con un usuario y proporciona garantías de seguridad y que un servicio de tipo de pago tiene un alto estándar de seguridad, en una modalidad posterior de la presente solicitud, las soluciones técnicas se describen utilizando un ejemplo en el que el dispositivo portátil implementa un proceso de autenticación de pago. De manera correspondiente, el dispositivo terminal anterior es un dispositivo portátil posterior, la aplicación de servicio anterior del tipo dedicado es una aplicación de servicio de tipo de pago posterior, y el tipo dedicado correspondiente es el pago.

Cabe señalar que es simplemente una modalidad preferida, y las soluciones técnicas en la presente solicitud también pueden implementarse en un dispositivo terminal de otro tipo y un proceso de autenticación de identidad de un servicio de otro tipo, y dicho cambio no afecta el alcance de protección de la presente solicitud.

Primero, se presenta un escenario de aplicación de las soluciones técnicas propuestas en las modalidades de la presente solicitud de la siguiente manera:

(1) Dispositivo portátil: es un dispositivo portátil y también tiene una función de pago, por ejemplo, un reloj inteligente, una insignia inteligente o gafas inteligentes. El dispositivo tiene una función de pago propiamente dicha, o una aplicación que tiene una función de pago instalada, y por lo tanto, se puede realizar una operación de pago correspondiente para una cuenta asociada. El dispositivo se comunica, a través de una interfaz estándar preestablecida, con un servidor de una aplicación de tipo de pago y un terminal habilitado para pago en el que está instalada la aplicación de tipo de pago, en donde la interfaz estándar preestablecida puede ser una interfaz estándar conforme a un protocolo de pago.
(2) Terminal habilitado para pagos: es, por ejemplo, un teléfono inteligente, una tableta inteligente (Pad), y tiene una función de pago en sí misma, o una aplicación que tiene una función de pago instalada. El terminal está asociado con una misma cuenta de usuario que el dispositivo portátil. Según lo requiera o establezca un usuario, el terminal debe confirmar una operación de pago mediante el uso del dispositivo portátil. El dispositivo también se comunica con el dispositivo portátil y el servidor de pago a través de una interfaz estándar preestablecida. La interfaz estándar preestablecida puede ser una interfaz estándar conforme a un protocolo de pago.
(3) Servidor de pago: es un servidor que tiene capacidades de procesamiento y verificación de pagos, y finalmente realiza la operación de pago después de que la verificación tenga éxito.

Con base en la arquitectura de servicio anterior, la interfaz estándar preestablecida puede configurarse de acuerdo con un protocolo correspondiente. Para un ejemplo específico propuesto en las modalidades de la presente solicitud, la interfaz puede configurarse usando, por ejemplo, un protocolo de contenido:
Se adopta un estándar de protocolo de configuración de formato ATT y se usa UUID para identificar un atributo de tipo dedicado exclusivo.

Para un proceso de autenticación de identidad específico, se puede configurar un protocolo de la interfaz estándar predeterminada que incluya un servicio y cuatro características, específicamente:

Servicio UUID: 0x0001000 (para determinar un tipo dedicado de una aplicación de servicio correspondiente); y
Característica: Hay cuatro características, a saber, registro, verificación, actualización de clave y confirmación (vibración). Los UUID característicos correspondientes son: 0x00000011, 0x00000012, 0x00000013 y 0x00000014, de modo que se pueden identificar las diferencias de funciones entre interfaces específicas.

Ciertamente, dicha configuración es simplemente un ejemplo específico. Durante la aplicación actual, las diferencias de funciones anteriores pueden no distinguirse y, en su lugar, se desencadena un procesamiento diferente de acuerdo con un identificador de tipo de mensaje. Ciertamente, se pueden establecer más características de acuerdo con diferentes contenidos de servicio. Dichos cambios no afectan el alcance de protección de la presente solicitud.

Con base en el escenario del sistema anterior, y considerando además que el dispositivo portátil tiene capacidades limitadas de computación y almacenamiento y tiene un requisito de consumo de energía, el dispositivo portátil es responsable de procesar las operaciones lo menos posible.

En las soluciones técnicas propuestas en la presente solicitud, el dispositivo portátil almacena la información de verificación de clave (es decir, la información de autenticación del servicio), y retroalimenta la información de verificación al servidor de pago solo cuando se verifica que la identidad es legítima, para completar sin problemas la operación de pago.

Los procedimientos de operación en varias etapas se describen a continuación en orden cronológico.

1. Etapa de vinculación

En esta etapa, se debe establecer una relación de vinculación entre el dispositivo portátil y una cuenta específica, y la información de la credencial de pago (es decir, un caso especial de la información de autenticación del servicio, en donde hay una configuración similar en las descripciones posteriores, que no se establece uno por uno) de la cuenta vinculada se almacena sincrónicamente en el dispositivo portátil.

Específicamente, como se muestra en la Figura 2, que es un diagrama de flujo esquemático de un proceso de enlace en un método de autenticación de identidad de acuerdo con una modalidad de la presente solicitud, en esta modalidad, el dispositivo portátil almacena localmente información de autenticación de servicio de acuerdo con una política de registro preestablecida, para completar el enlace a una cuenta de una aplicación de servicio de un tipo dedicado correspondiente, y un procedimiento específico es el siguiente:

Etapa S201. El dispositivo portátil recibe una solicitud de registro a través de la interfaz estándar preestablecida.

En un escenario de aplicación específico, si se requiere la verificación de identidad de la cuenta con base en un lado de la red, el proceso de registro anterior puede activarse utilizando el servidor de pago; si se realiza la coincidencia de información de identificación local (por ejemplo, negociación de clave local), una aplicación de servicio de tipo de pago en el terminal habilitado para pago puede iniciar directamente el proceso de registro en el dispositivo portátil. Sin embargo, no importa qué forma de inicio se implemente, debido a que un tipo de servicio procesado es un servicio de tipo de pago, todas las operaciones deben completarse a través de la interfaz estándar preestablecida. Como tal, se puede proteger la interferencia de un mensaje de servicio de otro tipo, y puede mejorarse la seguridad de una operación de servicio del tipo actual.

Teniendo en cuenta que un objetivo final de este proceso de vinculación es almacenar sincrónicamente la información de verificación (es decir, la información de autenticación del servicio), si la aplicación de servicio de tipo de pago en el terminal habilitado para pago inicia directamente el proceso de registro en el dispositivo portátil, la aplicación de servicio de tipo de pago en el terminal con pago habilitado debe proporcionar directamente la información de verificación correspondiente.

No importa qué solución de procesamiento se implemente, teniendo en cuenta que la vinculación se basa en la vinculación de una misma cuenta de pago, en un proceso posterior se omite una diferencia entre formularios desencadenantes específicos y la aplicación de servicio de tipo de pago de la cuenta de pago se usa directamente como entidad desencadenante para realizar una operación de enlace correspondiente.

Etapa S202. El dispositivo portátil analiza la solicitud de registro de acuerdo con un estándar de formato de datos preestablecido, para adquirir la información que contiene.

La aplicación de servicio de tipo de pago inicia la solicitud de registro en la interfaz estándar preestablecida del dispositivo portátil (por ejemplo, para el proceso de enlace iniciado directamente por la aplicación de tipo de pago en el terminal habilitado para pago, la solicitud de registro puede transmitirse directamente por medio de Bluetooth; para el proceso de vinculación iniciado mediante el uso del servidor de pago, la solicitud de registro puede transmitirse a la interfaz estándar preestablecida del dispositivo portátil mediante el uso del servidor de pago). Después de recibir los datos, el dispositivo portátil realiza el procesamiento de deserialización (una operación de deserialización es una operación de análisis) de acuerdo con un formato de transmisión de datos preestablecido, para obtener la información de verificación que se incluye en la solicitud de registro.

Cabe señalar además que la solicitud de registro y otro mensaje que se envía a la interfaz estándar preestablecida en lo sucesivo se utilizan para completar una operación de verificación de legitimidad correspondiente, y necesitan transportar información de tipo de verificación e información de firma específica, que es información de verificación clave necesariamente transportada. Aquí se proporciona una descripción específica, y otros mensajes son similares, y no se describen repetidamente uno por uno.

A. Información del tipo de verificación:

Actualmente, hay dos soluciones de verificación disponibles para el dispositivo portátil. Una de ellas es una solución relativamente segura, en la que se adopta RSA para el cifrado y la verificación de firma, y la otra es una solución que no tiene un alto rendimiento de programación y tiene una seguridad relativamente baja, en la que se adopta el cifrado simétrico.

B. Información de firma: Es información de firma generada de acuerdo con un algoritmo de firma específico, y otros mensajes a continuación son similares a los mismos, para los cuales la información de firma se puede generar de acuerdo con un algoritmo de firma específico mediante el uso de información que debe transportarse por separado.

En un escenario de aplicación específico, los tipos de algoritmo de firma incluyen principalmente SHA 256 y rsawithsha256.

En un escenario de aplicación específico, además de la información de verificación clave anterior, la solicitud de registro puede incluir las siguientes partes de contenido, y ciertamente, con la condición previa de que se pueda implementar la operación de vinculación de registro, el tipo de información transportada en el registro la solicitud no afecta el alcance de protección de la presente solicitud:

(1) Información relacionada con el paquete: es información usada para identificar la solicitud de registro e incluye: una longitud de datos firmados y los datos firmados.
(2) Información relacionada con la identidad: se usa para verificar la legitimidad de la solicitud de registro e incluye: información de firma (es decir, la información de identificación de identidad) del servicio de pago, información de duración de la información de firma del servicio de pago, información de desafío e información de longitud de la información del desafío.

(3) Información relacionada con el algoritmo: se usa para analizar o generar una firma, e incluye: información del tipo de algoritmo de firma e información de longitud del algoritmo de firma.
Además, se debe tener en cuenta que, en esta modalidad, el algoritmo de firma puede ser un algoritmo de hash seguro SHA256 o un algoritmo de hash no simétrico RSA con SHA 256. En un entorno específico, el algoritmo de firma también puede ser otro algoritmo de firma, y los detalles no se describen aquí.
(4) Información relacionada con la credencial de pago: se usa para verificar una operación de pago en un proceso posterior e incluye: una clave compartida (es decir, la información de la credencial de pago) generada por el terminal habilitado para pagos y utilizada para admitir el servidor de pagos completar una operación de deducción de tarifa e información de longitud de la clave compartida.

Etapa S203. El dispositivo portátil verifica la legitimidad de la solicitud de registro.

En un escenario de aplicación específico, después de que la operación de deserialización de información tiene éxito, el dispositivo portátil realiza una operación de verificación de acuerdo con la información de verificación preestablecida. Específicamente, el dispositivo portátil puede realizar, de acuerdo con una clave pública incorporada para el servicio de pago, una operación de verificación de la información relacionada con la firma que se obtiene después de realizar la operación de deserialización en la etapa S202.

Si la verificación tiene éxito, se realiza la etapa S204. Si la verificación falla, el dispositivo portátil determina que la solicitud de registro es inválida o ilegítima y, por lo tanto, descarta directamente la solicitud de registro.

Etapa S204. El dispositivo portátil adquiere y almacena información de credenciales de pago e información de identificación de identidad.

El dispositivo portátil realiza, de acuerdo con una clave privada incorporada, una operación de descifrado de la información relacionada con la credencial de pago que se obtiene después de que se realiza la operación de deserialización en la etapa S202, para adquirir la información de credencial de pago.

El dispositivo portátil adquiere información relacionada con el identificador del dispositivo que se obtiene después de realizar la operación de deserialización en la etapa S202.

El dispositivo portátil almacena localmente la información de credenciales de pago adquirida y la información de identificación de identidad, por ejemplo, almacena la información en una memoria local de solo lectura (ROM).

Hasta ahora, el almacenamiento para la relación de vinculación se ha completado en el lado del dispositivo portátil, y en una operación posterior, un estado de vinculación debe retroalimentarse a la aplicación de servicio de tipo de pago en el terminal habilitado para el pago por pares. La operación de enlace se completa realmente solo después de que la relación de enlace se procesa con éxito en ambos lados.

Etapa S205. El dispositivo portátil retroalimenta información de identificación de identidad y otra información relacionada con el enlace de acuerdo con una regla de retroalimentación preestablecida.

El dispositivo portátil genera un mensaje de respuesta de registro correspondiente de acuerdo con una regla de ensamblaje de información de retroalimentación preestablecida mediante el uso de un ID único (la información de identificación de identidad), un modelo de dispositivo y otra información, y envía el mensaje de respuesta de registro a un remitente de solicitud de registro. Es decir, si el terminal habilitado para pagos inicia directamente la solicitud de registro, el mensaje de respuesta de registro se retroalimenta directamente al terminal habilitado para pagos; si la solicitud de registro se inicia utilizando el servidor de pago en el lado de la red, el mensaje de respuesta de registro se retroalimenta al servidor de pago, y luego el servidor de pago realiza una retroalimentación de confirmación de vinculación posterior.

Cabe señalar que la forma de cifrado/descifrado anterior es un trabajo de garantía en aras de la seguridad, y con la condición previa de que se pueda garantizar la seguridad, ni si se utiliza la forma de cifrado/descifrado, ni si se toma otra medida de protección de seguridad. alcance de protección de la presente solicitud.

En un escenario de aplicación específico, además de la información clave de verificación, el mensaje de respuesta de registro puede incluir las siguientes partes del contenido, y ciertamente, con la condición previa de que se pueda implementar la operación de vinculación de registro, el tipo de información que se transporta en el mensaje de respuesta de registro no afecta el alcance de protección de la presente solicitud:

(1) Información relacionada con el paquete: es información usada para identificar la solicitud de registro e incluye: una longitud de datos firmados y los datos firmados.
(2) Información relacionada con la identidad: se usa para verificar la legitimidad de la solicitud de registro e incluye: información de firma (es decir, la información de identificación de identidad) del servicio de pago, información de duración de la información de firma del servicio de pago, información de desafío e información de longitud de la información del desafío.

(3) Información relacionada con el algoritmo: se usa para analizar o generar una firma, e incluye: información del tipo de algoritmo de firma e información de longitud del algoritmo de firma.
Además, debe tenerse en cuenta que, en esta modalidad, el algoritmo de firma puede ser SHA256 o RSA con SHA 256. En un entorno específico, el algoritmo de firma también puede ser otro algoritmo de firma, y los detalles no se describen aquí.
(4) Información relacionada con el dispositivo portátil: es información usada para permitir que el iniciador de registro adquiera un dispositivo portátil registrado con éxito, e incluye: información de identificación única del dispositivo portátil, información de longitud de la información de identificación única, información del modelo del dispositivo e información de longitud de la información del modelo del dispositivo.

Mediante el procesamiento anterior, el dispositivo portátil almacena con éxito la información de autenticación de pago y la información de identificación de identidad de una cuenta de la aplicación de servicio de tipo de pago que está vinculada al dispositivo portátil. Sin embargo, teniendo en cuenta que un usuario puede cambiar la información de la credencial de pago (por ejemplo, una contraseña de pago, un gesto de pago o similar), la información almacenada actualmente puede actualizarse posteriormente mediante el siguiente procedimiento. Para una operación de actualización específica, se puede hacer referencia al proceso de registro anterior, y la única diferencia es que, antes de que se determine actualizar la información de autenticación de pago, es necesario realizar adicionalmente un proceso de comparación de información de identificación de identidad (para determinar que es una operación de actualización del mismo usuario), así como también un proceso de comparación de versiones de información de autenticación de pago (solo se almacena la información de autenticación de pago de una versión superior). Los detalles no se describen aquí nuevamente.

2. Etapa de autenticación

En esta etapa, el dispositivo portátil realiza el procesamiento central de las soluciones técnicas propuestas en la presente solicitud, es decir, el dispositivo portátil realiza una operación de autenticación en un proceso de solicitud de pago, y el proceso puede continuar solo después de que se realiza una operación de autenticación exitosa.

Específicamente, como se muestra en la Figura 3, que es un diagrama de flujo esquemático de un proceso de autenticación en un método de autenticación de identidad de acuerdo con una modalidad de la presente solicitud, en esta modalidad, el dispositivo portátil realiza, de acuerdo con una política de autenticación preestablecida, operación de autenticación de legitimidad en una solicitud de autenticación de pago enviada por el terminal habilitado para pagos, y un procedimiento específico es el siguiente:
Etapa S301. El dispositivo portátil recibe, a través de la interfaz estándar preestablecida, una solicitud de autenticación de pago enviada por el servidor de pago.

En un escenario de aplicación específico, una operación de pago generalmente es iniciada por el terminal habilitado para pagos, en donde el terminal habilitado para pagos envía una solicitud de pago al servidor de pagos, para solicitar la operación de pago, y después de recibir la solicitud de pago, el servidor de pagos desencadena un proceso de autenticación de pago y envía la solicitud de autenticación de pago al dispositivo portátil.

La solicitud de autenticación de pago se puede recibir a través de la interfaz estándar preestablecida del dispositivo portátil.

Etapa S302. El dispositivo portátil analiza la solicitud de autenticación de pago de acuerdo con un estándar de formato de datos preestablecido, para adquirir la información que contiene.

Cuando la aplicación de servicio de tipo de pago recibe un proceso de pago iniciado por un usuario, la aplicación de servicio de tipo de pago inicia la solicitud de autenticación de pago a la interfaz estándar preestablecida del dispositivo portátil. Después de recibir los datos, el dispositivo portátil realiza el procesamiento de deserialización (una operación de deserialización es una operación de análisis) de acuerdo con un formato de transmisión de datos preestablecido, para obtener la información de verificación que se incluye en la solicitud de autenticación de pago.

En un escenario de aplicación específico, además de la información de verificación clave, la solicitud de autenticación de pago puede incluir las siguientes partes del contenido, y ciertamente, con la condición previa de que se pueda implementar la operación de autenticación de pago, el tipo de información transportada en la solicitud de autenticación de pago no afecta el alcance de protección de la presente solicitud:

(1) Información relacionada con el paquete: Es información usada para identificar la solicitud de autenticación de pago e incluye: una longitud de datos firmados y los datos firmados.
(2) Información relacionada con la identidad: Se usa para verificar la correspondencia entre la solicitud de autenticación de pago y la cuenta vinculada al dispositivo portátil, e incluye: información de firma (es decir, la información de identificación de identidad) del servicio de pago, información de duración de la información de firma del servicio de pago, información del desafío e información de duración de la información del desafío.
(3) Información relacionada con el algoritmo: Se usa para analizar o generar una firma, e incluye: información del tipo de algoritmo de firma e información de longitud del algoritmo de firma.

Además, debe tenerse en cuenta que, en esta modalidad, el algoritmo de firma puede ser SHA256 o RSAwithSHA256. En un entorno específico, el algoritmo de firma también puede ser otro algoritmo de firma, y los detalles no se describen aquí.

Etapa S303. El dispositivo portátil verifica una relación de vinculación entre una cuenta correspondiente a la solicitud de autenticación de pago y una cuenta correspondiente a la información de credenciales de pago almacenada localmente.

En un escenario de aplicación específico, el dispositivo portátil necesita comparar la información obtenida por deserialización con la información local, para juzgar si una cuenta de una aplicación de servicio de tipo de pago correspondiente a la solicitud de autenticación de pago es una cuenta de la aplicación de servicio de tipo de pago vinculada al dispositivo portátil.

En un escenario de aplicación específico, se puede verificar si la información de identificación de identidad contenida en el mensaje coincide con la información de identificación de identidad correspondiente a la información de credencial de pago almacenada localmente.

Si la verificación tiene éxito, se realiza la etapa S304. Si la verificación falla, se puede considerar que la solicitud de autenticación de pago corresponde a otra cuenta que no está relacionada con el dispositivo portátil y, por lo tanto, la solicitud de autenticación de pago se descarta directamente.

Etapa S304. El dispositivo portátil genera una clave de identidad de acuerdo con la información de credencial de pago almacenada del terminal habilitado para pago.

La clave de identidad se genera utilizando la información de credenciales de pago almacenada en la ROM en el proceso de enlace anterior.

En un escenario de aplicación específico, la clave de identidad puede cifrarse utilizando una clave pública de la aplicación de servicio de tipo de pago, y los datos se serializan de acuerdo con un parámetro de salida de autenticación, para generar datos de retroalimentación (es decir, el paquete de datos de respuesta) que puede ser retroalimentado.

En un escenario de aplicación específico, además de la información de verificación clave, los datos de retroalimentación pueden incluir las siguientes partes del contenido, y ciertamente, con la condición previa de que se pueda implementar la operación de retroalimentación de la clave de identidad, el tipo de información transportada en los datos de retroalimentación no afecta el alcance de protección de la presente solicitud:

(1) Información relacionada con el paquete: Es información usada para identificar los datos de retroalimentación e incluye: una longitud de datos firmados y los datos firmados.
(2) Información relacionada con la identidad: Se usa para verificar la legitimidad de los datos de retroalimentación e incluye: información de firma (es decir, la información de identificación de identidad) del servicio de pago, información de duración de la información de firma del servicio de pago, información de desafío e información de longitud de la información del desafío.
(3) Información relacionada con el algoritmo: Se usa para analizar o generar una firma, e incluye: información del tipo de algoritmo de firma e información de longitud del algoritmo de firma.
Además, debe tenerse en cuenta que, en esta modalidad, el algoritmo de firma puede ser SHA256 o RSA con SHA 256. En un entorno específico, el algoritmo de firma también puede ser otro algoritmo de firma, y los detalles no se describen aquí.
(4) Información relacionada con la credencial de pago: Se usa para permitir que el iniciador de verificación adquiera la información de la credencial de pago e incluye: una longitud de una cadena de identidad obtenida cifrando la información de la credencial de pago que se almacena permanentemente en la ROM local durante el enlace, y datos de cadena de identidad.

Etapa S205. El dispositivo portátil envía datos de retroalimentación de acuerdo con una regla de retroalimentación preestablecida, de modo que el servidor de pago complete una operación de deducción de tarifa.

Después de recibir los datos de retroalimentación, el servidor de pago obtiene la información de la credencial de pago mediante descifrado, para completar una operación de deducción de tarifa posterior.

Cabe señalar que la forma de cifrado/descifrado anterior es un trabajo de garantía en aras de la seguridad, y con la condición previa de que se pueda garantizar la seguridad, ni si se usa el modo de cifrado/descifrado, ni si se toma otra medida de protección de seguridad. alcance de protección de la presente solicitud.

3. Etapa de confirmación

En esta etapa, el dispositivo portátil devuelve una respuesta de confirmación al usuario de acuerdo con el resultado de la operación del proceso de pago que el servidor de pago retroalimenta.

El dispositivo portátil recibe, a través de la interfaz estándar preestablecida, una solicitud de confirmación enviada desde el servidor de pago.
El dispositivo portátil adquiere información de tipo modo de confirmación incluida en la solicitud de confirmación.

El dispositivo portátil completa una operación de confirmación correspondiente de acuerdo con la información de tipo modo de confirmación.

Específicamente, en esta modalidad, la información de tipo modo de confirmación incluida en la solicitud de confirmación puede incluir cualquiera o cualquier combinación de los siguientes modos de confirmación:
confirmación de texto, confirmación de sonido y confirmación de vibración.

En consecuencia, por ejemplo, la confirmación de texto puede mostrar directamente una línea de caracteres "su pago se realizó correctamente" en el dispositivo portátil, y ciertamente, una condición previa es que el dispositivo portátil tenga una pantalla de visualización. La confirmación de sonido puede estar emitiendo un "tono de llamada" preestablecido. La confirmación de vibración puede estar vibrando por un número predeterminado de veces o un período de tiempo continuo.

Esta operación de confirmación se realiza principalmente para permitir al usuario conocer con precisión el resultado de un pago. Ciertamente, también se puede establecer que no se requiere ninguna operación adicional cuando el pago se realiza correctamente. Dicha configuración puede ajustarse de acuerdo con una necesidad real y no afecta el alcance de protección de la presente solicitud.

En comparación con la técnica anterior, las soluciones técnicas propuestas en las modalidades de la presente solicitud incluyen los siguientes efectos técnicos beneficiosos: las modalidades de la presente descripción reciben un método y un dispositivo para autenticación de identidad, implementado en un sistema compuesto por un servidor y un dispositivo terminal que incluye una interfaz estándar preestablecida configurada para comunicarse con una aplicación de servicio de un tipo dedicado. Mediante las soluciones técnicas propuestas en la presente solicitud, cuando se requiere una operación de autenticación de identidad, el servidor puede solicitar información de autenticación de servicio de una cuenta de la aplicación de servicio del tipo dedicado desde el dispositivo terminal a través de la interfaz estándar preestablecida, y el dispositivo terminal puede realizar la verificación de seguridad en este proceso de acuerdo con una regla de verificación correspondiente, y enviar información de autenticación del servicio almacenada localmente de vuelta al servidor para su posterior procesamiento solo cuando la verificación tenga éxito. Como tal, la seguridad de un proceso de autenticación de identidad se puede garantizar por medio de la interfaz estándar preestablecida vinculada a la aplicación de servicio del tipo dedicado y la verificación de seguridad del dispositivo terminal, y el sentido de participación del operador del dispositivo terminal en este proceso puede ser mejorado mediante el uso de la información de autenticación de identidad almacenada actualmente en el dispositivo terminal. Cuando el dispositivo terminal es específicamente un dispositivo portátil, puede mejorarse el sentido de participación del usuario en el proceso de autenticación de identidad, puede mejorarse la seguridad del proceso de autenticación de identidad y se puede aumentar la tasa de éxito de autenticación de identidad, especialmente para una autenticación de pago proceso.

Para describir las soluciones proporcionadas en las modalidades anteriores de la presente solicitud más claramente, con base en la misma idea de invención que el método anterior, las modalidades de la presente aplicación proponen además un dispositivo terminal, cuyo diagrama estructural esquemático se muestra en la Figura 4, e incluye específicamente:
una interfaz estándar preestablecida 41 configurada para comunicarse con una aplicación de servicio de un tipo dedicado; un módulo receptor 42 configurado para recibir, a través de la interfaz estándar preestablecida 41, un mensaje de solicitud de autenticación de identidad enviado por un servidor correspondiente a la aplicación de servicio del tipo dedicado, en donde el servidor envía el mensaje de solicitud de autenticación de identidad al dispositivo terminal después el servidor recibe una solicitud de servicio de la aplicación de servicio del tipo dedicado;
un módulo de verificación 43 configurado para verificar, de acuerdo con una clave pública de la aplicación de servicio del tipo dedicado, una firma en el mensaje de solicitud de autenticación de identidad recibido por el módulo receptor 42;
un módulo de adquisición 44 configurado para adquirir, cuando la verificación por el módulo de verificación 43 tiene éxito, la información de autenticación de servicio de una cuenta correspondiente al mensaje de solicitud de autenticación de identidad de la información de autenticación de servicio almacenada previamente en el dispositivo terminal; y
un módulo de retroalimentación 45 configurado para devolver un mensaje de respuesta de verificación que transporta la información de autenticación de servicio adquirida por el módulo de adquisición 44 al servidor a través de la interfaz estándar preestablecida 41.

En un escenario de aplicación específico, el módulo de recepción 42 se configura además para recibir, a través de la interfaz estándar preestablecida 41, un mensaje de solicitud de registro de vinculación para una cuenta que es enviada por la aplicación de servicio del tipo dedicado;
el módulo de verificación 43 se configura además para verificar, de acuerdo con la clave pública de la aplicación de servicio del tipo dedicado, una firma en el mensaje de solicitud de registro de vinculación recibido por el módulo receptor 42; el módulo de adquisición 44 se configura además para adquirir, cuando la verificación por el módulo de verificación 43 tiene éxito, la información de autenticación de servicio transportada en el mensaje de solicitud de registro de vinculación, y correspondientemente almacenar la información de autenticación de servicio y la información de identificación de identidad de la cuenta en el dispositivo terminal; y
el módulo de retroalimentación 45 se configura además para generar un mensaje de respuesta de registro de acuerdo con la información del identificador del dispositivo terminal, y devolver el mensaje de respuesta de registro a la aplicación de servicio del tipo dedicado a través de la interfaz estándar preestablecida 41.

Además, el dispositivo terminal incluye además un módulo de actualización 46, donde el módulo de recepción 42 se configura además para recibir, a través de la interfaz estándar preestablecida 41, un mensaje de solicitud de actualización de información de autenticación de servicio para una cuenta que es enviada por la aplicación de servicio del tipo dedicado;
el módulo de verificación 43 se configura además para verificar, de acuerdo con la clave pública de la aplicación de servicio del tipo dedicado, una firma en el mensaje de solicitud de actualización de información de autenticación de servicio recibida por el módulo receptor 42, y juzgar, cuando la verificación tiene éxito, si la información de identificación de identidad correspondiente a la información de autenticación de servicio almacenada en el dispositivo terminal es coherente con la información de identificación de identidad transportada en el mensaje de solicitud de actualización de información de autenticación de servicio;
el módulo de adquisición 44 se configura además para adquirir, cuando el resultado del juicio del módulo de verificación 43 es sí, la información de autenticación de servicio transportada en el mensaje de solicitud de actualización de información de autenticación de servicio; y
el módulo de actualización 46 se configura para juzgar si la información de versión de la información de autenticación de servicio adquirida por el módulo de adquisición 44 es mayor que la información de versión de la información de autenticación de servicio correspondiente almacenada actualmente de manera local en el dispositivo terminal, y reemplazar, si el resultado del juicio es sí, la información de autenticación de servicio correspondiente almacenada actualmente en el dispositivo terminal con la información de autenticación de servicio adquirida por el módulo de adquisición 44.

En un escenario de aplicación específico, el módulo receptor 42 se configura además para recibir, a través de la interfaz estándar preestablecida 41, una solicitud de confirmación que es enviada por el servidor correspondiente a la aplicación de servicio del tipo dedicado; y
el módulo de adquisición 44 se configura además para adquirir información de tipo modo de confirmación incluida en la solicitud de confirmación, de modo que el dispositivo terminal completa una operación de confirmación correspondiente de acuerdo con la información de tipo modo de confirmación.

De acuerdo con otro aspecto, las modalidades de la presente solicitud proponen además un servidor, cuyo diagrama estructural esquemático se muestra en la Figura 5, en donde el servidor proporciona un servicio para una aplicación de servicio de un tipo dedicado, e incluye específicamente:
un módulo de envío 51 configurado para enviar, cuando se recibe una solicitud de servicio de la aplicación de servicio del tipo dedicado, un mensaje de solicitud de autenticación de identidad a un dispositivo terminal a través de una interfaz estándar preestablecida incluida en el dispositivo terminal;
un módulo receptor 52 configurado para recibir, cuando una solicitud de autenticación de identidad tiene éxito, un mensaje de respuesta de verificación que es devuelto por el dispositivo terminal a través de la interfaz estándar preestablecida y transporta información de autenticación de servicio; y
un módulo de procesamiento 53 configurado para procesar la solicitud de servicio de acuerdo con el mensaje de autenticación de servicio recibido por el módulo receptor 52.

En un escenario de aplicación específico, el módulo de envío 51 se configura además para enviar un mensaje de solicitud de registro de vinculación para una cuenta al dispositivo terminal a través de la interfaz estándar preestablecida incluida en el dispositivo terminal, en donde el mensaje de solicitud de registro de vinculación transporta información de autenticación de servicio de la cuenta; y
el módulo de recepción 52 se configura además para recibir, cuando el vínculo de registro tiene éxito, un mensaje de respuesta de registro que es devuelto por el dispositivo terminal a través de la interfaz estándar preestablecida, y confirma que el dispositivo terminal está vinculado exitosamente a la cuenta, en donde el mensaje de respuesta de registro transporta información de identificación del dispositivo terminal.

Específicamente, el módulo de envío 51 se configura además para:
enviar, cuando la información de autenticación de servicio de la cuenta necesita ser actualizada, un mensaje de solicitud de actualización de información de autenticación de servicio para la cuenta al dispositivo terminal a través de la interfaz estándar preestablecida incluida en el dispositivo terminal, en donde el mensaje de solicitud de

actualización de información de autenticación de servicio transporta la información de autenticación de servicio que necesita ser actualizada de la cuenta;
y/o enviar, después de que el módulo de procesamiento 53 completa el procesamiento de la solicitud de servicio, una solicitud de confirmación que transporta información de tipo modo de confirmación al dispositivo terminal a través de la interfaz estándar preestablecida incluida en el dispositivo terminal, de modo que el dispositivo terminal complete una operación de confirmación correspondiente de acuerdo con la información de tipo modo de confirmación.

En comparación con la técnica anterior, las soluciones técnicas propuestas en las modalidades de la presente solicitud tienen al menos los siguientes efectos técnicos beneficiosos:
Las modalidades de la presente aplicación describen un método y un dispositivo para autenticación de identidad, implementado en un sistema compuesto por un servidor y un dispositivo terminal que incluye una interfaz estándar preestablecida configurada para comunicarse con una aplicación de servicio de un tipo dedicado. Mediante las soluciones técnicas propuestas en la presente solicitud, cuando se requiere una operación de autenticación de identidad, el servidor puede solicitar información de autenticación de servicio de una cuenta de la aplicación de servicio del tipo dedicado desde el dispositivo terminal a través de la interfaz estándar preestablecida, y el dispositivo terminal puede realizar la verificación de seguridad en este proceso de acuerdo con una regla de verificación correspondiente, y enviar información de autenticación del servicio almacenada localmente de vuelta al servidor para su posterior procesamiento solo cuando la verificación tenga éxito. Como tal, la seguridad de un proceso de autenticación de identidad se puede garantizar por medio de la interfaz estándar preestablecida vinculada a la aplicación de servicio del tipo dedicado y la verificación de seguridad del dispositivo terminal, y el sentido de participación del operador del dispositivo terminal en este proceso puede mejorarse mediante el uso de la información de autenticación de identidad almacenada actualmente en el dispositivo terminal. Cuando el dispositivo terminal es específicamente un dispositivo portátil, puede mejorarse el sentido de participación del usuario en el proceso de autenticación de identidad, puede mejorarse la seguridad del proceso de autenticación de identidad y se puede aumentar la tasa de éxito de autenticación de identidad, especialmente para un proceso de autenticación de pago.

A partir de la descripción de los modos de implementación anteriores, los expertos en la técnica pueden entender claramente que las modalidades de la presente invención pueden implementarse mediante soporte físico, o pueden implementarse mediante programa informático más una plataforma de soporte físico universal necesaria. Con base en tal comprensión, las soluciones técnicas en las modalidades de la presente invención pueden implementarse en forma de un producto de programa informático. El producto de programa informático puede almacenarse en un medio de almacenamiento no volátil (que puede ser un CD-ROM, un disco flash USB, un disco duro extraíble o similares) e incluye varias instrucciones para instruir a un dispositivo informático (que puede ser un ordenador personal, un servidor, un dispositivo del lado de la red o similar) para realizar todos o algunos de las etapas de los métodos descritos en varios escenarios de implementación de las modalidades de la presente invención.

Los expertos en la técnica pueden entender que un dibujo adjunto es simplemente un diagrama esquemático de un escenario de implementación preferido, y un módulo o procedimiento en los dibujos adjuntos no es necesariamente obligatorio para implementar las modalidades de la presente invención.

Los expertos en la técnica pueden entender que los módulos en un aparato en un escenario de implementación pueden distribuirse en el aparato en el escenario de implementación de acuerdo con una descripción del escenario de implementación, y también pueden cambiarse y ubicarse correspondientemente en uno o más aparatos diferentes de aquellos en el escenario de implementación. Los módulos en el escenario de implementación se pueden combinar en un módulo y también se pueden dividir en una pluralidad de submódulos.

Los números de secuencia de las modalidades anteriores de la presente invención son meramente descriptivos y no implican la preferencia entre los escenarios de implementación.

Más arriba se describen simplemente varios escenarios de implementación específicos de las modalidades de la presente invención. Sin embargo, las modalidades de la presente invención no están limitadas a las mismas. Cualquier cambio que puedan concebir los expertos en la técnica estará dentro del alcance de limitación de servicio de las modalidades de la presente invención.

REIVINDICACIONES

1. Un método de autenticación de identidad, implementado por un dispositivo portátil que comprende una interfaz del protocolo de pago configurada para comunicarse con una aplicación de servicio de un tipo de pago, la aplicación de servicio que requiere una operación de autenticación de identidad para el dispositivo portátil durante la ejecución específica del servicio, el método que comprende específicamente:
configurar el dispositivo portátil para incluir la interfaz del protocolo de pago para la comunicación entre el dispositivo portátil y la aplicación de servicio del tipo de pago, en donde la interfaz del protocolo de pago está dedicada al tipo de pago de la aplicación de servicio, en donde la interfaz del protocolo de pago se configura para identificar un identificador de tipo de pago único correspondiente a la aplicación de servicio del tipo de pago en un mensaje a partir de mensajes de solicitud de autenticación de identidad recibidos de diferentes aplicaciones de servicio que incluyen la aplicación de servicio y para proceder con la autenticación de identidad con el mensaje;
recibir, mediante el dispositivo portátil a través de la interfaz del protocolo de pago, un mensaje de solicitud de autenticación de identidad enviado por un servidor correspondiente a la aplicación de servicio del tipo de pago (S101), en donde el mensaje de solicitud de autenticación de identidad se envía mediante el servidor al dispositivo portátil después de que el servidor recibe una solicitud de servicio de la aplicación de servicio del tipo de pago, y en donde la interfaz del protocolo de pago procesa el mensaje de solicitud de autenticación de identidad solo si la solicitud de autenticación de identidad incluye el identificador único de la aplicación de servicio del tipo de pago;
verificar (102), mediante el dispositivo portátil, una firma en el mensaje de solicitud de autenticación de identidad de acuerdo con una clave pública de la aplicación de servicio del tipo de pago;
adquirir (103), mediante el dispositivo portátil, si la verificación tiene éxito, información de autenticación de servicio de una cuenta correspondiente al mensaje de solicitud de autenticación de identidad de información de autenticación de servicio almacenada previamente de manera local; y
devolver (104), mediante el dispositivo portátil, un mensaje de respuesta de verificación que comprende la información de autenticación de servicio adquirida al servidor a través de la interfaz del protocolo de pago.

2. El método de acuerdo con la reivindicación 1, en donde el dispositivo portátil almacena previamente de manera local información de autenticación de servicio mediante el uso del siguiente proceso:
recibir, mediante el dispositivo portátil a través de la interfaz del protocolo de pago, un mensaje de solicitud de registro de vinculación para una cuenta que es enviada por la aplicación de servicio del tipo de pago;
verificar, mediante el dispositivo portátil, una firma en el mensaje de solicitud de registro de vinculación de acuerdo con la clave pública de la aplicación de servicio del tipo de pago;
adquirir, mediante el dispositivo portátil, si la verificación tiene éxito, la información de autenticación del servicio transportada en el mensaje de solicitud de registro de vinculación, y correspondientemente almacenar de manera local, mediante el dispositivo portátil, la información de autenticación del servicio y la información de identificación de identidad de la cuenta; y
generar, mediante el dispositivo portátil, un mensaje de respuesta de registro de acuerdo con la información de identificación del dispositivo portátil, y devolver, mediante el dispositivo portátil, el mensaje de respuesta de registro a la aplicación de servicio del tipo de pago a través de la interfaz del protocolo de pago.

3. El método de acuerdo con la reivindicación 2, en donde la generación, mediante el dispositivo portátil, del mensaje de respuesta de registro de acuerdo con la información de identificación del dispositivo portátil comprende específicamente:
adquirir, mediante el dispositivo portátil información del identificador único e información del modelo del dispositivo del dispositivo portátil;
reunir, mediante el dispositivo portátil, la información del identificador único y la información del modelo del dispositivo de acuerdo con un formato de datos especificado por la aplicación de servicio del tipo de pago; y
firmar, mediante el dispositivo portátil, la información reunida mediante el uso de una clave privada local y generar el mensaje de respuesta de registro.

4. El método de acuerdo con la reivindicación 2, en donde después de adquirir mediante el dispositivo portátil la información de autenticación del servicio transportada en el mensaje de solicitud de registro de vinculación, y correspondientemente almacenar de manera local mediante el dispositivo portátil la información de autenticación del servicio y la información de identificación de identidad de la cuenta localmente, el método comprende, además:
recibir, mediante el dispositivo portátil a través de la interfaz del protocolo de pago, un mensaje de solicitud de actualización de información de autenticación de servicio para una cuenta que es enviado por la aplicación de servicio del tipo de pago;
verificar, mediante el dispositivo portátil, una firma en el mensaje de solicitud de actualización de información de autenticación de servicio de acuerdo con la clave pública de la aplicación de servicio del tipo de pago;
determinar, mediante el dispositivo portátil, si la verificación tiene éxito, si la información de identificación de identidad correspondiente a la información de autenticación de servicio almacenada localmente es coherente con la información de identificación de identidad transportada en el mensaje de solicitud de actualización de información de autenticación de servicio;

adquirir, mediante el dispositivo portátil, si el resultado de la determinación es sí, la información de autenticación del servicio transportada en el mensaje de solicitud de actualización de información de autenticación del servicio;
determinar, mediante el dispositivo portátil, si la información de versión de la información de autenticación de servicio adquirida es mayor que la información de versión de la información de autenticación de servicio correspondiente almacenada actualmente de manera local, que comprende determinar si la información de autenticación de servicio almacenada actualmente en el dispositivo portátil necesita ser actualizada; y
reemplazar, mediante el dispositivo portátil, si el resultado de la determinación es sí, la información de autenticación de servicio correspondiente almacenada actualmente con la información de autenticación de servicio adquirida.

5. El método de acuerdo con la reivindicación 1, en donde después de devolver, mediante el dispositivo portátil, un mensaje de respuesta de verificación que transporta la información de autenticación de servicio adquirida al servidor a través de la interfaz del protocolo de pago, el método comprende, además:
recibir, mediante el dispositivo portátil a través de la interfaz del protocolo de pago, una solicitud de confirmación enviada por el servidor correspondiente a la aplicación de servicio del tipo de pago;
adquirir, mediante el dispositivo portátil, información de tipo modo de confirmación comprendida en la solicitud de confirmación; y
completar, mediante el dispositivo portátil, una operación de confirmación correspondiente de acuerdo con la información de tipo modo de confirmación.

6. El método de acuerdo con la reivindicación 1, en donde los mensajes enviados por otras aplicaciones de servicio no son recibidos por el dispositivo portátil a través de la interfaz del protocolo de pago.

7. El método de acuerdo con la reivindicación 1, en donde devolver, por el dispositivo portátil, un mensaje de respuesta de verificación que transporta la información de autenticación de servicio adquirida al servidor a través de la interfaz del protocolo de pago comprende:
cifrar la información de autenticación del servicio;
guardar la información de autenticación del servicio cifrada como un paquete de datos de respuesta; y
devolver el paquete de datos de respuesta al servidor para descifrarlo.

8. Un dispositivo portátil, que comprende específicamente:
una interfaz del protocolo de pago configurada para comunicarse con una aplicación de servicio de un tipo de pago;
múltiples módulos configurados para realizar el método de acuerdo con cualquiera de las reivindicaciones de la 1 a la 7.

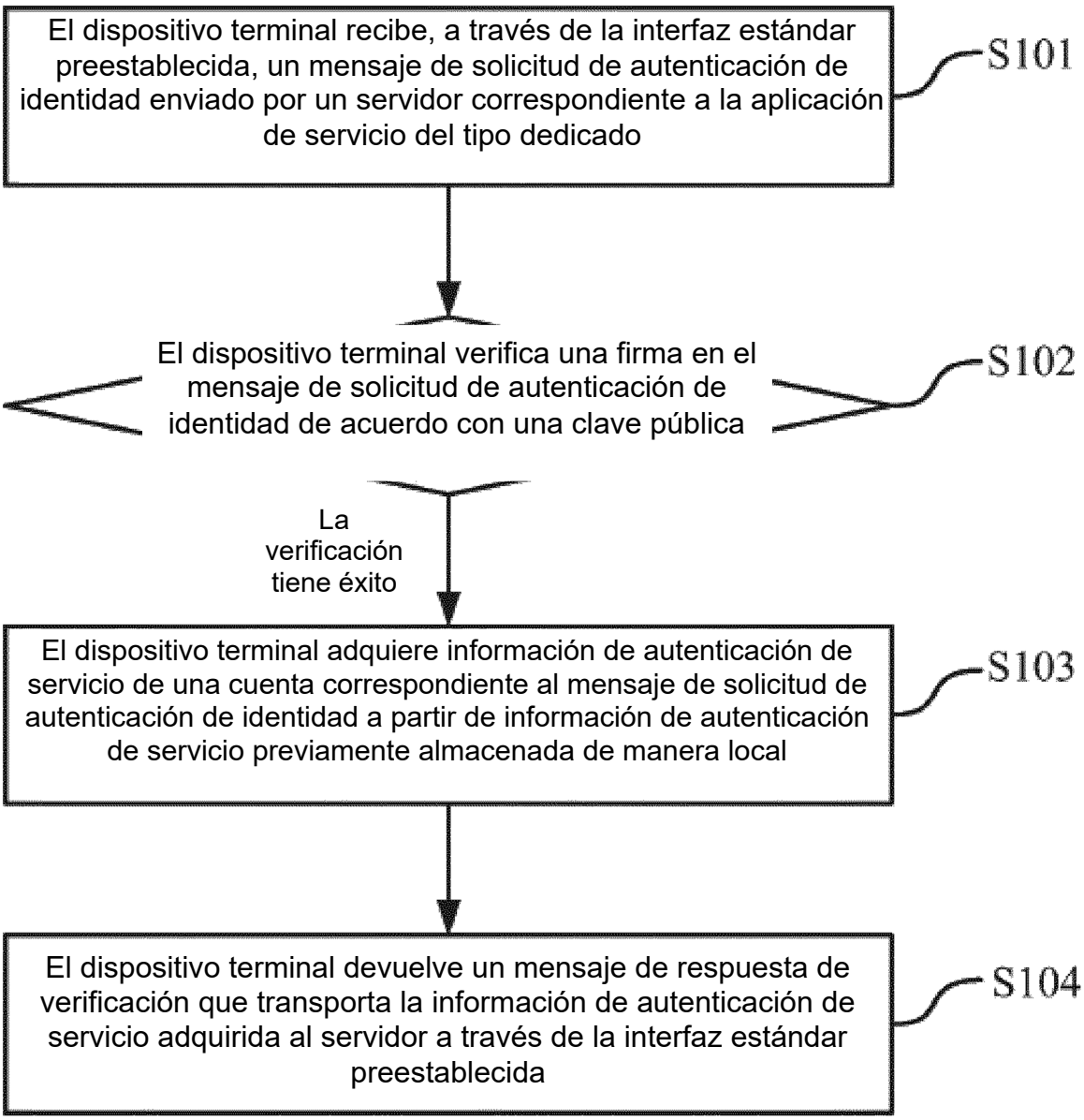
El dispositivo terminal recibe, a través de la interfaz estándar preestablecida, un mensaje de solicitud de autenticación de identidad enviado por un servidor correspondiente a la aplicación de servicio del tipo dedicado
S101
El dispositivo terminal verifica una firma en el mensaje de solicitud de autenticación de identidad de acuerdo con una clave pública
S102
La verificación tiene éxito
El dispositivo terminal adquiere información de autenticación de servicio de una cuenta correspondiente al mensaje de solicitud de autenticación de identidad a partir de información de autenticación de servicio previamente almacenada de manera local
S103
El dispositivo terminal devuelve un mensaje de respuesta de verificación que transporta la información de autenticación de servicio adquirida al servidor a través de la interfaz estándar preestablecida
S104

FIGURA 1

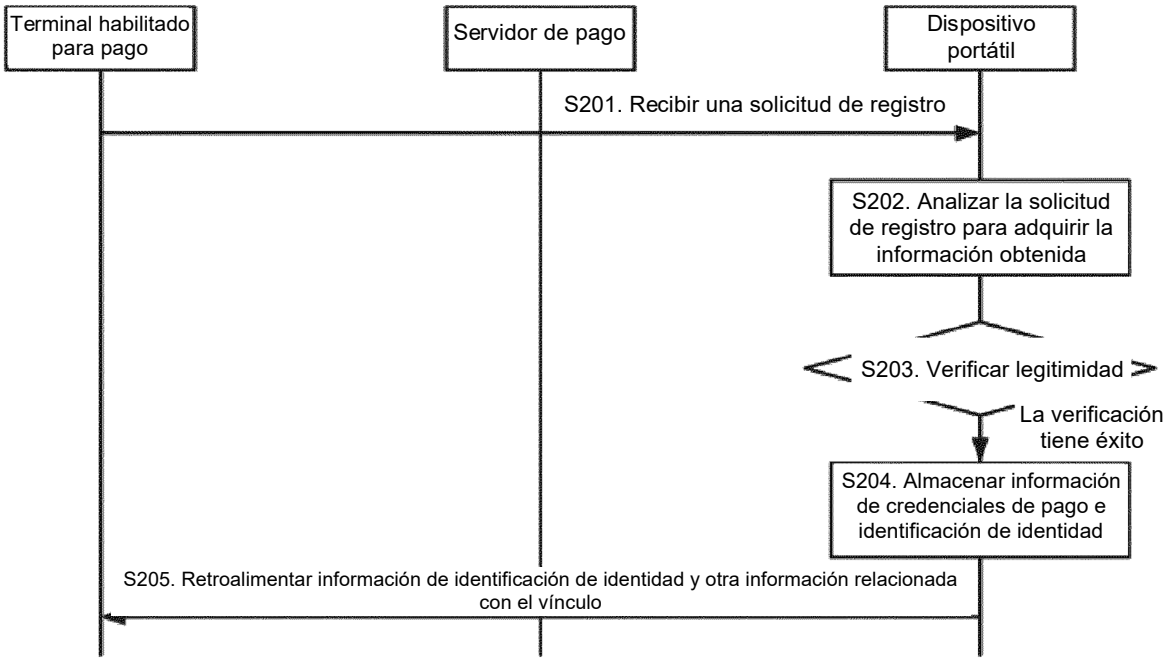

FIGURA 2

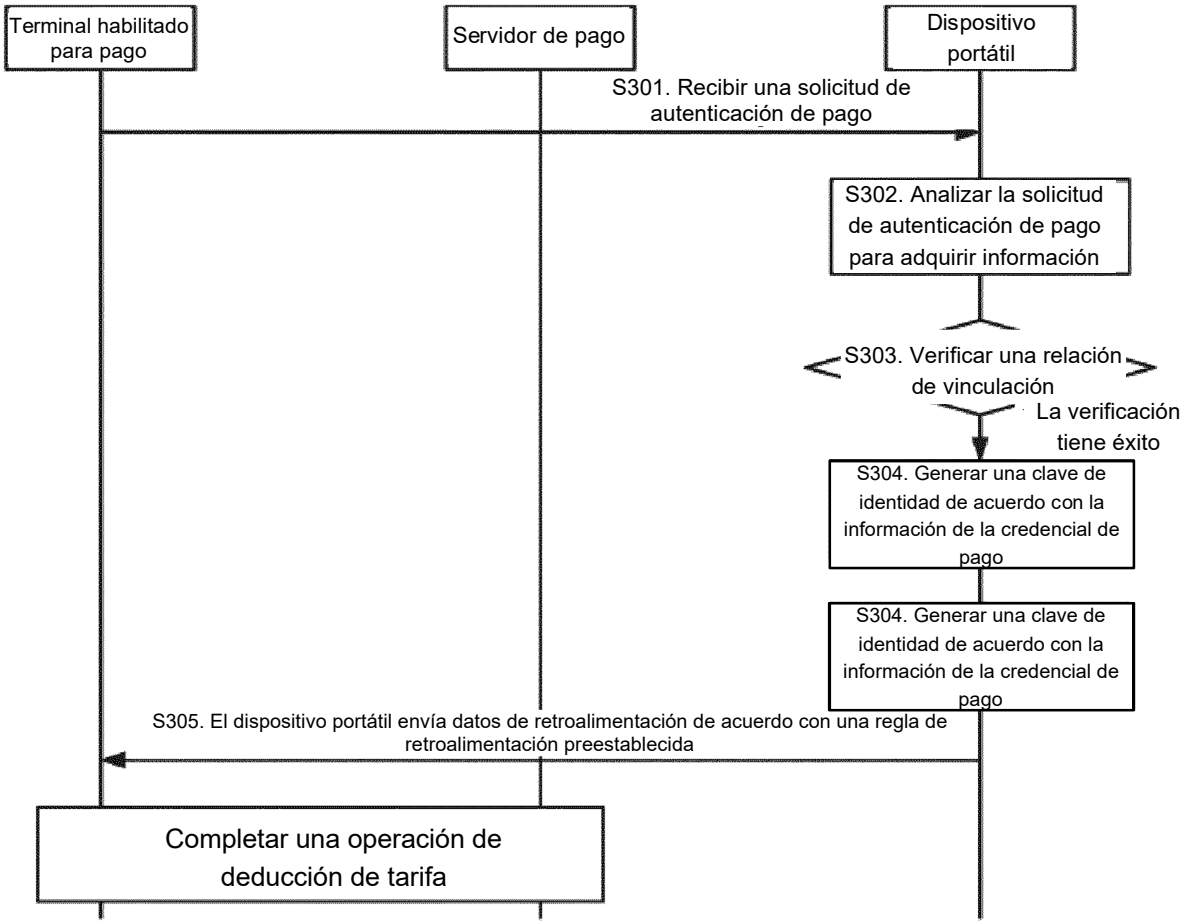

FIGURA 3

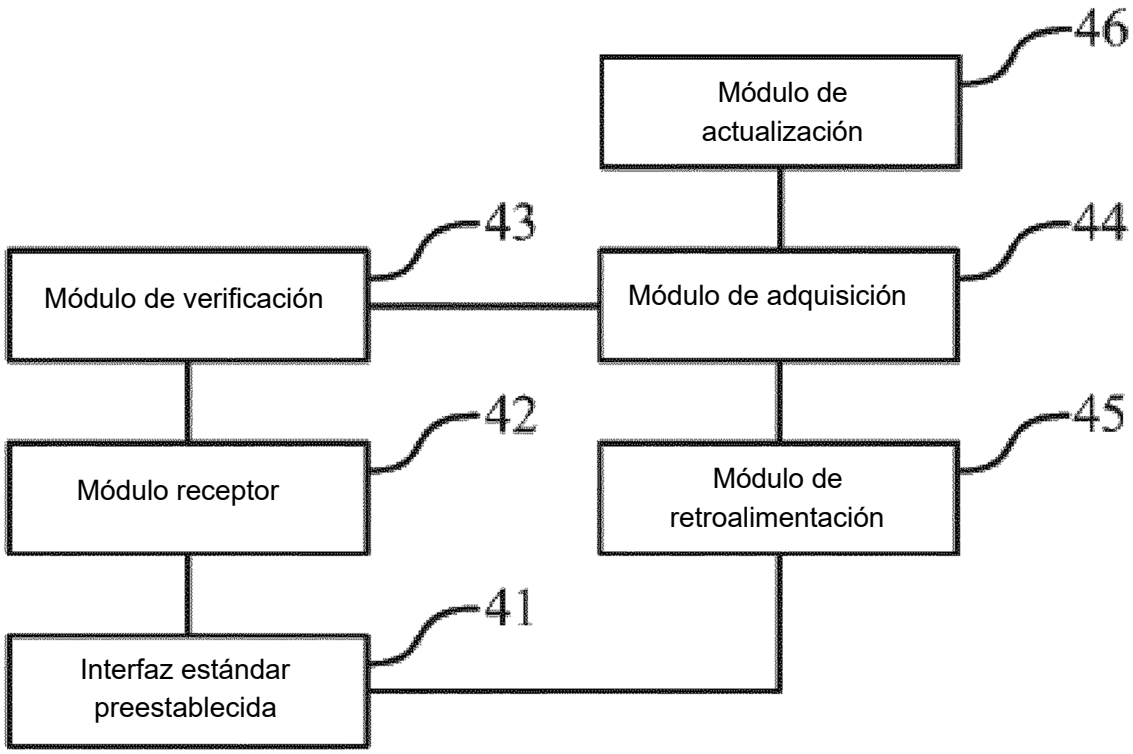

FIGURA 4

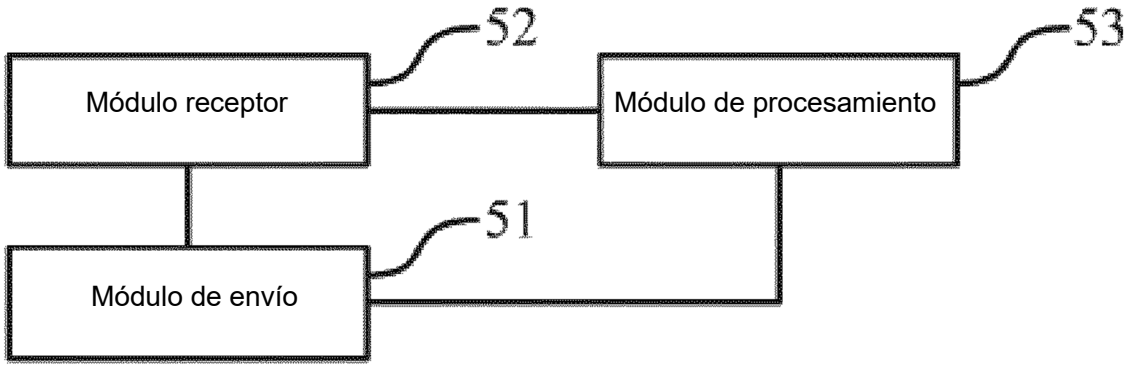

FIGURA 5