(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 869 280**

(51) Int. CI.:

H04L 9/08	(2006.01)	***H04W 12/06***	(2011.01)
G06Q 20/20	(2012.01)		
G06Q 20/32	(2012.01)		
G06Q 20/38	(2012.01)		
H04W 12/08	(2011.01)		
H04L 29/06	(2006.01)		
G06Q 20/40	(2012.01)		
H04W 4/80	(2008.01)		
H04W 12/10	(2011.01)		
H04L 9/32	(2006.01)		

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **05.08.2016 PCT/US2016/045678**

(87) Fecha y número de publicación internacional: **09.02.2017 WO17024188**

(96) Fecha de presentación y número de la solicitud europea: **05.08.2016 E 16833906 (7)**

(97) Fecha y número de publicación de la concesión europea: **28.04.2021 EP 3332369**

(54) Título: **Método y aparato para autenticación de servicio**

(30) Prioridad:

05.08.2015 CN 201510475791
04.08.2016 US 201615228383

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
25.10.2021

(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:

ZHANG, YONGZHI;
SHEN, LINGNAN y
WANG, LEI

(74) Agente/Representante:

SÁEZ MAESO, Ana

DESCRIPCIÓN

Método y aparato para autenticación de servicio

Esta solicitud reivindica el beneficio de la prioridad de la solicitud de patente China No. 201510475791.8, presentada el 5 de agosto de 2015, titulada “Method and Apparatus for Service Verification", y la solicitud de patente US No. 15/228,383, presentada el 4 de agosto de 2016.

Antecedentes

Campo de la divulgación

La presente divulgación se refiere en general a la autenticación de servicios, y en particular se refiere a la autenticación de un servicio que utiliza un terminal de inicio de servicio y un terminal de autorización de servicio.

Descripción de la técnica relacionada

Con el desarrollo de dispositivos móviles y tecnologías NFC (comunicación de campo cercano), la tasa de popularización de la función NFC en dispositivos móviles es cada vez más alta. Las tecnologías NFC generalmente pueden servir como un canal de pago fuera de línea. Por lo tanto, la creciente popularización de la función NFC en dispositivos móviles indudablemente promueve el desarrollo de internet móvil.

En el proceso de pago fuera de línea, un usuario puede simular, en un dispositivo móvil, un medio de pago (por ejemplo, una tarjeta bancaria o un monedero electrónico, etc.) mediante un programa de aplicación específico, y luego interactuar con el terminal de un comerciante (por ejemplo, una máquina POS) mediante la función NFC para finalizar el proceso de pago. Sin embargo, en una implementación tradicional, el pago es un servicio con mayor seguridad. Por lo tanto, para protegerse de un riesgo potencial en el proceso de pago, generalmente se debe simular un entorno confiable para el terminal del usuario y el terminal del comerciante, lo que no beneficiará el avance y desarrollo progresivo del pago móvil. El documento US 2013/018214 analiza un sistema y método que proporciona a un comerciante asociado con un sistema de punto de venta y un consumidor asociado a un dispositivo informático portátil completar una transacción de compra sin transmitir ni presentar credenciales de pago confidenciales. El documento US 2009/0307139 describe un método para autenticar una transacción financiera en un punto de venta que incluye almacenar un programa de aplicación en un primer elemento seguro de un teléfono móvil.

Breve resumen

En las reivindicaciones adjuntas se exponen diversos aspectos y realizaciones de la invención.

Un aspecto de la divulgación se refiere a un método para la autenticación de un servicio que utiliza un terminal de inicio de servicio y un terminal de autorización de servicio. El método incluye enviar, por el terminal de inicio de servicio, información de servicio al terminal de autorización de servicio, recibir, por el terminal de inicio de servicio, un código de autorización de servicio correspondiente a la información de servicio enviada por el terminal de autorización de servicio, siendo el código de autorización de servicio calculado por el terminal de autorización del servicio con base en la información del servicio y la información del usuario, y generar, por el terminal de inicio del servicio, información de autenticación del servicio de acuerdo con la información del servicio y el código de autorización del servicio, y cargar la información de autenticación del servicio en un servidor para procesar el servicio después autenticar el código de autorización del servicio.

Un aspecto de la divulgación se refiere a un método para la autenticación de un servicio que usa un terminal de inicio de servicio y un terminal de autorización de servicio. El método incluye recibir, por el terminal de autorización de servicio, información de servicio enviada por el terminal de inicio de servicio, generar, por el terminal de autorización de servicio, un código de autorización de servicio correspondiente usando la información de servicio y la información de usuario de acuerdo con un algoritmo preestablecido, y enviar, por el terminal de autorización de servicio, el código de autorización de servicio al terminal de inicio del servicio. El código de autenticación del servicio permite que el terminal de inicio del servicio genere información de autenticación del servicio de acuerdo con la información del servicio y el código de autorización del servicio, y cargue la información de autenticación del servicio en un servidor para procesar el servicio después de autenticar el código de autorización del servicio.

Un aspecto de la divulgación se refiere a un aparato para la autenticación de un servicio que utiliza un terminal de autorización de servicios. El aparato incluye un procesador y una memoria no transitoria que almacena instrucciones ejecutables por ordenador. Cuando las ejecuta el procesador, las instrucciones hacen que el aparato envíe información de servicio generada al terminal de autorización de servicio, reciba un código de autorización de servicio correspondiente a la información de servicio enviada por el terminal de autorización de servicio, en donde el código de autorización de servicio es generado por el terminal de autorización de servicio mediante cálculo con base en la información del servicio y la información del usuario, y genera información de autenticación del servicio de acuerdo con la información del servicio y el código de autorización del servicio, y carga la información de autenticación del servicio en un servidor para procesar el servicio después de autenticar el código de autorización del servicio.

Un aspecto de la divulgación se refiere a un aparato para la autenticación de un servicio que utiliza un terminal de inicio de servicio. El aparato incluye un procesador y una memoria no transitoria que almacena instrucciones ejecutables por ordenador. Cuando las ejecuta el procesador, las instrucciones hacen que el aparato reciba información de servicio enviada por el terminal de inicio de servicio, genere un código de autorización de servicio correspondiente utilizando la información de servicio y la información de usuario de acuerdo con un algoritmo preestablecido, y envíe el código de autorización del servicio al terminal de inicio del servicio a través de un módulo de comunicación de campo cercano (NFC), el código de autorización del servicio permite que el terminal de inicio del servicio genere información de autenticación del servicio de acuerdo con la información del servicio y el código de autorización del servicio, y cargue la información de autenticación del servicio en un servidor para procesar el servicio después de autenticar el código de autorización del servicio.

En la presente divulgación, la información de servicio generada se envía al terminal de autorización de servicio por medio del terminal de inicio de servicio, el terminal de inicio de servicio recibe un código de autorización de servicio generado por el terminal de autorización de servicio mediante cálculo con base en la información de servicio y la información relevante del usuario. Luego, el terminal de inicio del servicio genera información de autenticación del servicio de acuerdo con la información del servicio y el código de autorización del servicio, y carga la información de autenticación del servicio a un lado del servidor para que el lado del servidor procese el servicio después de autenticar el código de autorización del servicio. En la presente divulgación, debido a que la autenticación de la información del servicio se lleva a cabo de manera uniforme por el lado del servidor, para algunos servicios con mayor seguridad, es posible que ya no sea necesario simular un entorno de servicio confiable en el terminal de autorización de servicio y el terminal de inicio del servicio beneficiando así la promoción del servicio.

Cuando la solución técnica de la presente divulgación se aplica a un servicio de pago fuera de línea, se puede implementar que, en el proceso de pago, ya no sea necesario simular un entorno de servicio confiable en el terminal de un comerciante y en el terminal de un usuario estableciendo un módulo de seguridad adicional. El terminal del comerciante y el terminal del usuario pueden finalizar el servicio de pago utilizando un terminal general, promoviendo así el servicio de pago fuera de línea.

Breve descripción de los dibujos

La figura 1 es un diagrama de flujo de un método de autenticación de servicios de acuerdo con algunas realizaciones de la presente divulgación.

La figura 2 es un diagrama de interacción esquemático de un terminal de comerciante y un terminal de comprador de acuerdo con algunas realizaciones de la presente divulgación.

La figura 3 es un diagrama de bloques lógicos de un aparato de autenticación de servicios de acuerdo con algunas realizaciones de la presente divulgación.

La figura 4 es un diagrama de estructura de hardware de un terminal para llevar el aparato de autenticación de servicios de acuerdo con algunas realizaciones de la presente divulgación.

La figura 5 es un diagrama de bloques lógico de otro aparato de autenticación de servicios de acuerdo con algunas realizaciones de la presente divulgación.

La figura 6 es un diagrama de estructura de hardware de un terminal para llevar otro aparato de autenticación de servicios de acuerdo con algunas realizaciones de la presente divulgación.

Descripción de las realizaciones

En algunas realizaciones, la presente divulgación proporciona un método de autenticación de servicio, donde el método incluye enviar información de servicio generada a un terminal de autorización de servicio y recibir un código de autorización de servicio correspondiente a la información de servicio enviada por el terminal de autorización de servicio, en donde el código de autorización de servicio es generado por el terminal de autorización de servicio mediante cálculo con base en la información de servicio y la información de usuario relevante. El método también incluye generar información de autenticación de servicio de acuerdo con la información de servicio y el código de autorización de servicio, y cargar la información de autenticación de servicio a un lado del servidor para que el lado del servidor procese el servicio después de autenticar el código de autorización de servicio.

En algunas realizaciones, enviar información de servicio generada a un terminal de autorización de servicio incluye enviar la información de servicio generada al terminal de autorización de servicio con base en un módulo NFC preestablecido.

En algunas realizaciones, el método incluye además firmar digitalmente la información de autenticación del servicio antes de cargar la información de autenticación del servicio en un lado del servidor para que el lado del servidor continúe autenticando la información de autenticación del servicio después de autenticar la firma.

En algunas realizaciones, el método incluye además recibir un mensaje de notificación enviado por el lado del servidor después de terminar de procesar el servicio, en donde el mensaje de notificación está configurado para notificar que el servicio ha sido procesado por el lado del servidor.

En algunas realizaciones, el servicio incluye un servicio de pago fuera de línea, la información del servicio incluye información de pedido correspondiente al servicio de pago fuera de línea y la información de autenticación del servicio incluye información de transacción correspondiente al servicio de pago fuera de línea.

En algunas realizaciones, la presente divulgación proporciona además un método de autenticación de servicio, donde el método incluye recibir información de servicio enviada por un terminal de inicio de servicio, generar un código de autorización de servicio correspondiente calculando la información de servicio y la información de usuario relevante de acuerdo con un algoritmo preestablecido, y enviar el código de autorización del servicio al terminal de inicio del servicio para que el terminal de inicio del servicio genere información de autenticación del servicio de acuerdo con la información del servicio y el código de autorización del servicio, y cargue la información de autenticación del servicio a un lado del servidor para que el lado del servidor procese el servicio después de autenticar el código de autorización del servicio.

En algunas realizaciones, recibir información de servicio enviada por un terminal de inicio de servicio incluye recibir, con base en un módulo NFC preestablecido, la información de servicio enviada por el terminal de inicio de servicio.

En algunas realizaciones, el método incluye además, antes de generar un código de autorización de servicio correspondiente calculando la información de servicio y la información de usuario relevante de acuerdo con un algoritmo preestablecido, realizar una autorización de servicio sobre la información de servicio. La realización de una autorización de servicio sobre la información de servicio incluye adquirir información de autorización de servicio introducida por un usuario, en donde la información de autorización de servicio incluye una contraseña o huella digital configurada para realizar una autorización de servicio, haciendo coincidir la información de autorización de servicio adquirida con la información de autorización de servicio almacenada localmente, y determinar la autorización de la información de servicio a completar cuando la información de autorización de servicio adquirida coincide con la información de autorización de servicio almacenada localmente.

En algunas realizaciones, el método incluye además recibir un mensaje de notificación enviado por el lado del servidor después de terminar de procesar el servicio, en donde el mensaje de notificación está configurado para notificar que el servicio ha sido procesado por el lado del servidor.

En algunas realizaciones, el código de autorización de servicio es válido dentro de un período de tiempo preestablecido.

En algunas realizaciones, el servicio incluye un servicio de pago fuera de línea, la información del servicio incluye información de pedido correspondiente al servicio de pago fuera de línea y la información de autenticación del servicio incluye información de transacción correspondiente al servicio de pago fuera de línea.

En algunas realizaciones, la presente divulgación proporciona además un aparato de autenticación de servicio, donde el aparato incluye un primer módulo de envío configurado para enviar información de servicio generada a un terminal de autorización de servicio, y un primer módulo de recepción configurado para recibir un código de autorización de servicio correspondiente a la información de servicio enviada por el terminal de autorización de servicio, en donde el código de autorización de servicio es generado por el terminal de autorización de servicio mediante cálculo con base en la información de servicio y la información de usuario relevante. El aparato también incluye un primer módulo de generación configurado para generar información de autenticación de servicio de acuerdo con la información de servicio y el código de autorización de servicio, y cargar la información de autenticación de servicio a un lado del servidor para que el lado del servidor procese el servicio después de autenticar el código de autorización del servicio.

En algunas realizaciones, el primer módulo de envío está configurado específicamente para enviar la información de servicio generada al terminal de autorización de servicio con base en un módulo NFC preestablecido.

En algunas realizaciones, el aparato incluye además un módulo de firma configurado para firmar digitalmente, antes de cargar la información de autenticación del servicio en un lado del servidor, la información de autenticación del servicio para que el lado del servidor continúe autenticando la información de autenticación del servicio después de autenticar la firma.

En algunas realizaciones, el primer módulo de recepción está configurado además para recibir un mensaje de notificación enviado por el lado del servidor después de terminar de procesar el servicio, en donde el mensaje de notificación está configurado para notificar que el servicio ha sido procesado por el lado del servidor.

En algunas realizaciones, el servicio incluye un servicio de pago fuera de línea, la información del servicio incluye información de pedido correspondiente al servicio de pago fuera de línea y la información de autenticación del servicio incluye información de transacción correspondiente al servicio de pago fuera de línea.

En algunas realizaciones, la presente divulgación proporciona además un aparato de autenticación de servicio, donde el aparato incluye un segundo módulo de recepción configurado para recibir información de servicio enviada por un terminal de inicio de servicio, un segundo módulo de generación configurado para generar un código de autorización de servicio correspondiente calculando la información del servicio y la información de usuario relevante de acuerdo con un algoritmo preestablecido, y un segundo módulo de envío configurado para enviar el código de autorización del servicio al terminal de inicio del servicio por medio de un módulo NFC para que el terminal de inicio del servicio genere información de autenticación del servicio de acuerdo con la información del servicio y el código de autorización del servicio, y cargue la información de autenticación del servicio en el lado del servidor para que el lado del servidor procese el servicio después de autenticar el código de autorización del servicio.

En algunas realizaciones, el segundo módulo de recepción está configurado específicamente para recibir, con base en un módulo NFC preestablecido, la información de servicio enviada por el terminal de inicio de servicio.

En algunas realizaciones, el aparato incluye además un módulo de autorización configurado para realizar, antes de generar un código de autorización de servicio correspondiente calculando la información de servicio y la información de usuario relevante de acuerdo con un algoritmo preestablecido, una autorización de servicio sobre la información de servicio. El módulo de autorización está configurado específicamente para adquirir información de autorización de servicio ingresada por un usuario, en donde la información de autorización de servicio incluye una contraseña o huella digital configurada para realizar una autorización de servicio, hacer coincidir la información de autorización de servicio adquirida con información de autorización de servicio almacenada localmente, y determinar la autorización de la información de servicio para finalizar cuando la información de autorización de servicio adquirida coincida con la información de autorización de servicio almacenada localmente.

En algunas realizaciones, el segundo módulo de recepción está configurado específicamente para recibir un mensaje de notificación enviado por el lado del servidor después de terminar de procesar el servicio, en donde el mensaje de notificación está configurado para notificar que el servicio ha sido procesado por el lado del servidor.

En algunas realizaciones, el código de autorización de servicio es válido dentro de un período de tiempo preestablecido.

En algunas realizaciones, el servicio incluye un servicio de pago fuera de línea, la información del servicio incluye información de pedido correspondiente al servicio de pago fuera de línea y la información de autenticación del servicio incluye información de transacción correspondiente al servicio de pago fuera de línea.

En la presente divulgación, la información de servicio generada se envía al terminal de autorización de servicio por medio del terminal de inicio de servicio, recibe un código de autorización de servicio generado por el terminal de autorización de servicio mediante cálculo con base en la información del servicio y la información relevante del usuario. El terminal de inicio del servicio genera información de autenticación del servicio de acuerdo con la información del servicio y el código de autorización del servicio, y carga la información de autenticación del servicio en un lado del servidor para que el lado del servidor procese el servicio después de autenticar el código de autorización del servicio. En la presente divulgación, debido a que la autenticación de la información del servicio se lleva a cabo de manera uniforme por el lado del servidor, para algunos servicios con mayor seguridad, es posible que ya no sea necesario simular un entorno de servicio confiable en el terminal de autorización del servicio y el terminal de inicio del servicio, beneficiando así la promoción del servicio.

Cuando la solución técnica de la presente divulgación se aplica a un servicio de pago fuera de línea, se puede implementar que, en el proceso de pago, ya no sea necesario simular un entorno de servicio confiable en el terminal de un comerciante y el terminal de usuario estableciendo un módulo de seguridad adicional. El terminal del comerciante y el terminal del usuario pueden finalizar el servicio de pago utilizando un terminal general, beneficiando así la promoción del servicio de pago.

A continuación se describe la presente divulgación con referencia a realizaciones y escenarios de aplicación específicos.

Haciendo referencia a la figura 1, que muestra un método de autenticación de servicio de acuerdo con algunas realizaciones de la presente divulgación, un anfitrión para ejecutar el método puede ser un terminal y un lado del servidor, en donde el terminal puede incluir un terminal de inicio de servicio y un terminal de autorización de servicio. El terminal y el lado del servidor cooperan entre sí para realizar los siguientes pasos.

En el paso 101, el terminal de inicio de servicio envía la información de servicio generada al terminal de autorización de servicio.

En el paso 102, el terminal de autorización de servicio genera un código de autorización de servicio correspondiente calculando la información de servicio y la información de usuario relevante de acuerdo con un algoritmo preestablecido.

En el paso 103, el terminal de autorización de servicio envía el código de autorización de servicio al terminal de inicio de servicio.

En el paso 104, el terminal de inicio del servicio genera información de autenticación del servicio de acuerdo con la información del servicio y el código de autorización del servicio, y carga la información de autenticación del servicio en un lado del servidor para que el lado del servidor procese el servicio después de autenticar el código de autorización del servicio.

Mediante los pasos anteriores, como iniciador del servicio, un primer usuario puede iniciar un servicio por medio del terminal de iniciación del servicio. Como un autorizador de servicios, un segundo usuario puede autorizar el servicio iniciado por el primer usuario por medio del terminal de autorización de servicios. Por ejemplo, en un escenario de aplicación de pago fuera de línea, el primer usuario puede ser un comerciante que inicia una orden de pago por medio del terminal de un comerciante (por ejemplo, una máquina POS), y el segundo usuario puede ser un comprador que paga por medio de un terminal de comprador (por ejemplo, un terminal de teléfono móvil), de acuerdo con la orden de pago iniciada por el comerciante.

Cuando el primer usuario inicia un servicio por medio del terminal de inicio de servicio, el terminal de inicio de servicio puede generar la información de servicio correspondiente de acuerdo con la información ingresada por el primer usuario, y luego enviar la información de servicio generada al terminal de autorización de servicio.

Cuando el primer usuario envía la información de servicio al terminal de autorización de servicio, esto puede realizarse mediante un módulo NFC dispuesto en el terminal de antemano. Por ejemplo, después de que el primer usuario inicia un servicio por medio del terminal de inicio del servicio, el segundo usuario puede acercar el terminal de autorización del servicio al terminal de inicio del servicio. Cuando la distancia entre ambos alcanza una distancia de reconocimiento (por ejemplo, 10 cm) del módulo NFC, el terminal de inicio del servicio puede activarse para transmitir la información del servicio del servicio al terminal de autorización del servicio a través de un canal inalámbrico del módulo NFC.

En algunas realizaciones, cuando el terminal de autorización de servicio recibe la información de servicio enviada por el terminal de inicio de servicio, el segundo usuario puede realizar primero una autorización de servicio sobre la información de servicio recibida por medio del terminal de autorización de servicio. Cuando el terminal de autorización de servicio realiza una autorización de servicio sobre la información de servicio recibida, esto puede implementarse autenticando localmente la información de autorización de servicio adquirida introducida por el segundo usuario. Por ejemplo, en la implementación, la información de autorización de servicio puede incluir una contraseña o huella digital introducida por el segundo usuario para realizar una autorización de servicio.

Cuando el terminal de autorización de servicio realiza una autorización de servicio sobre la información de servicio recibida, el terminal de autorización de servicio puede adquirir la contraseña o huella digital introducida por el segundo usuario para realizar la autorización, y luego autentica localmente la contraseña o huella digital haciendo coincidir la contraseña o huella digital adquirida con una contraseña o huella digital almacenada localmente. Cuando la contraseña o huella digital adquirida coincide con la contraseña o huella digital almacenada localmente, la contraseña o huella digital adquirida se autentica y el terminal de autorización de servicio puede determinar la autorización de la información de servicio a completar. De este modo, se puede evitar que otros usuarios, en lugar del segundo usuario, procesen un servicio iniciado por el terminal iniciador del servicio, mejorando así la seguridad del servicio.

Después de que se completa la autorización de la información de servicio, el terminal de autorización de servicio puede generar un código de autorización de servicio correspondiente calculando la información de servicio y la información de usuario relevante de acuerdo con un algoritmo preestablecido, y luego enviar el código de autorización del servicio al terminal de inicio del servicio por medio del módulo NFC. Cuando el terminal de autorización de servicio calcula el código de autorización de servicio, la información de usuario relevante adoptada puede incluir información de terminal del terminal de autorización de servicio e información de usuario del segundo usuario, o similar, y el algoritmo preestablecido adoptado puede incluir una firma preestablecida o un algoritmo de cifrado, etc. El tipo de algoritmo no está particularmente limitado en la presente divulgación y puede seleccionarse de acuerdo con la demanda real.

Además, para mejorar la seguridad, cuando el terminal de autorización de servicio calcula el código de autorización de servicio de acuerdo con el algoritmo configurado, se puede establecer una hora válida para el código de autorización de servicio calculado, y el código de autorización de servicio puede ser normalmente autenticado dentro del tiempo válido. Por ejemplo, cuando el terminal de autorización de servicio calcula el código de autorización de servicio, se puede introducir una marca de tiempo en el código de autorización de servicio calculado. Se establece un tiempo válido para el código de autorización del servicio, y luego el tiempo válido establecido por el terminal de autorización del servicio se carga en el lado del servidor por el terminal de inicio del servicio. Cuando el código de autorización del servicio se carga en el lado del servidor para la autenticación, el lado del servidor puede verificar la marca de tiempo en el código de autorización del servicio para confirmar si el código de autorización del servicio es válido o no. Si el tiempo actual está más allá de una duración válida, esto indica que el código de autorización del servicio no es válido y el lado del servidor puede descartar directamente el código de autorización del servicio sin autenticación. De esta forma, se puede evitar eficazmente el riesgo de divulgación del código de autorización de servicio.

Después de recibir el código de autorización de servicio enviado por el terminal de autorización de servicio, el terminal de inicio de servicio puede generar información de autenticación de servicio de acuerdo con la información de servicio y el código de autorización de servicio, y cargar la información de autenticación de servicio en el lado del servidor para

que el lado del servidor autentique el código de autorización del servicio. Para garantizar la seguridad en el proceso de transmisión de la información de autorización del servicio, antes de cargar la información de autenticación del servicio en el lado del servidor, el terminal de autorización del servicio también puede realizar una firma en la información de autenticación del servicio y luego cargar la información de autenticación del servicio firmada en el lado del servidor. Debe entenderse que cuando el terminal de autorización de servicio envía el código de autorización de servicio al terminal de inicio de servicio, también puede enviar información de cuenta de usuario, etc. Por tanto, el terminal de inicio del servicio envía la información de autorización junto con la información de la cuenta del usuario al lado del servidor, de modo que el lado del servidor puede determinar la información de la cuenta del usuario para realizar el procesamiento del servicio correspondiente.

Por ejemplo, el terminal de inicio del servicio puede ensamblar directamente la información del servicio y el código de autorización del servicio, tomar la información ensamblada como la información de autenticación del servicio, luego realizar un procesamiento de firma en la información de autenticación del servicio de acuerdo con un algoritmo de firma preestablecido, y luego cargar la información de autenticación del servicio firmada en el lado del servidor. A continuación, el lado del servidor autentica respectivamente la firma y la información de autenticación del servicio.

En algunas realizaciones, cuando el lado del servidor autentica la información de autenticación del servicio recibida, el lado del servidor puede primero autenticar la firma de la información de autenticación del servicio. Por ejemplo, el lado del servidor puede usar el mismo algoritmo de firma para analizar la firma y luego autenticar la validez de la firma de acuerdo con el resultado del análisis.

Después de que se autentica la firma, el lado del servidor puede autenticar además el código de autorización del servicio en la información de autenticación del servicio. Por ejemplo, el lado del servidor puede verificar una marca de tiempo válida en el código de autorización del servicio para determinar si el código de autorización del servicio es inválido o no. Cuando el código de autorización del servicio es válido, el lado del servidor puede utilizar el mismo algoritmo que utiliza el terminal de autorización del servicio para calcular el código de autorización del servicio para calcular la información del servicio y la información del usuario relevante, y luego juzgar si el código de autorización del servicio calculado es consistente con un código de autenticación de servicio en la información de autenticación de servicio. La información de autenticación del servicio se utiliza para autenticar el código de autenticación del servicio en la información de autorización del servicio. Para garantizar la coherencia del algoritmo utilizado por el lado del servidor y el terminal de autorización del servicio para calcular el código de autorización del servicio, el algoritmo puede ser emitido uniformemente por el lado del servidor y actualizado en tiempo real, o el algoritmo puede configurarse por separado en el terminal de autorización de servicio y el lado del servidor de antemano.

Después de que se autentiquen tanto la firma en la información de autenticación del servicio como la información de autenticación del servicio, el lado del servidor puede procesar directamente el servicio localmente porque el servicio ha sido autorizado por el terminal de autorización del servicio. Puede enviar por separado, después de que el servicio se haya procesado con éxito, un mensaje de notificación al terminal de inicio del servicio y al terminal de autorización del servicio para informar a ambos que el servicio ha finalizado el procesamiento. Por supuesto, si la firma en la información de autenticación del servicio o el código de autenticación del servicio falla en la autenticación, el lado del servidor puede enviar por separado un mensaje de notificación al terminal de inicio del servicio y al terminal de autorización del servicio para informar a ambos que el servicio falla en el procesamiento.

En la aplicación práctica, las soluciones técnicas de las realizaciones anteriores se pueden aplicar a escenarios de servicio de pago fuera de línea. A continuación se hace una descripción tomando un ejemplo en el que las soluciones técnicas de las realizaciones anteriores se aplican a escenarios de servicio de pago fuera de línea.

En la aplicación del pago tradicional fuera de línea, un usuario puede simular, en el terminal de un comprador, un medio de pago (por ejemplo, una tarjeta bancaria o un monedero electrónico, etc.) mediante un programa de aplicación específico, y luego interactuar con el terminal de un comerciante (por ejemplo, una máquina POS) por medio de un módulo NFC en el terminal del comprador para finalizar el proceso de pago.

Debido a que el pago es un servicio con mayor seguridad, para proteger un riesgo potencial en el proceso de pago, generalmente los terminales de ambos lados necesitan proporcionar un entorno de ejecución confiable en el proceso de pago fuera de línea.

Por parte del comerciante, el terminal del comerciante generalmente es un dispositivo dedicado que tiene una mayor seguridad, tal como una máquina POS o similar. Por parte del comprador, cuando el medio de pago se simula en el terminal del comprador mediante el programa de aplicación específico, generalmente es necesario montar un SE (elemento de seguridad) en el terminal del comprador. Mediante un algoritmo de seguridad proporcionado por la SE, se simula un entorno de ejecución confiable (TEE) en el terminal del comprador.

Por ejemplo, se toma un ejemplo en el que el medio de pago es una tarjeta bancaria, luego de que el terminal del comerciante genera un pedido, el comprador puede finalizar la acción de "deslizar la tarjeta" al traer el terminal del comprador, en el cual el módulo NFC está dispuesto, cerca del terminal del comerciante, de modo que el terminal del comerciante se activa para enviar una instrucción de consumo al terminal del comprador. Después de recibir la instrucción de consumo, el terminal del comprador procesa la instrucción de consumo y genera un MAC 1 configurado

para autenticar la validez de la tarjeta bancaria simulada. Después de autenticar el MAC 1 en el TEE, el terminal del comerciante procesa el pedido y genera un MAC2 configurado para autenticar la validez del comerciante. Bajo la protección de seguridad proporcionada por el SE, el terminal del comprador autentica el MAC2, si se pasa la autenticación, la transacción se realiza correctamente y luego informa al lado del servidor para que realice la transferencia.

Como puede verse, en la implementación tradicional, para garantizar la seguridad del pago, existen ciertos requisitos de hardware tanto para el terminal del comprador como para el terminal del comerciante, y no se puede utilizar un terminal general que tenga un módulo NFC. Por ejemplo, el comerciante debe usar una máquina POS que tenga mayor seguridad, y el comprador debe usar un terminal SE provisto con un SE, por lo que no es beneficioso para la promoción del servicio de pago móvil.

Para resolver el problema anterior, mediante el cambio del proceso de pago tradicional fuera de línea y la protección de un paso sensible en el proceso de pago fuera de línea, la autenticación del pago en el proceso de pago fuera de línea es ejecutada uniformemente por el lado del servidor, ni por el terminal del comerciante. ni el terminal del comprador necesita autenticar respectivamente la validez de cada uno a nivel local. De esta manera, ni el terminal del comerciante ni el terminal del comprador deben contar con un SE adicional para brindar protección para el proceso de pago porque el paso sensible en el proceso de pago ha sido protegido. Por lo tanto, el terminal del comerciante y el terminal del comprador pueden utilizar un terminal general que tenga un módulo NFC, beneficiando así la promoción del servicio de pago móvil.

Cuando las soluciones técnicas de las realizaciones anteriores se aplican a escenarios de servicio de pago, el servicio puede ser un servicio de pago fuera de línea, el primer usuario puede ser el comerciante y el segundo usuario puede ser el comprador, la información del servicio puede ser información del pedido correspondiente al servicio de pago fuera de línea, la información de autenticación del servicio puede ser información de transacción correspondiente al servicio de pago fuera de línea, y el terminal de autorización del servicio y el terminal de inicio del servicio pueden ser dispositivos terminales generales que tienen un módulo NFC, por ejemplo, un teléfono móvil inteligente. El lado del servidor puede ser un servidor para proporcionar un servicio de pago para el comprador y el comerciante, un grupo de servidores o una plataforma en la nube construida con base en el grupo de servidores. Por ejemplo, el lado del servidor puede ser una plataforma Alipay o un servidor bancario que coopera con la plataforma Alipay.

Se hace una descripción a continuación tomando un ejemplo en el que tanto el terminal de autorización de servicio como el terminal de inicio del servicio son teléfonos móviles inteligentes. Por supuesto, la descripción en la que tanto el terminal de autorización de servicio como el terminal de inicio del servicio son teléfonos móviles inteligentes es solo a modo de ejemplo, y la divulgación no se limita a este ejemplo. En la implementación, el terminal de autorización del servicio y el terminal de inicio del servicio también pueden usar otros tipos de terminales móviles generales que tienen un módulo NFC.

Se hace ahora referencia a la figura 2, que es un diagrama de interacción esquemático del terminal del comerciante y el terminal del comprador mostrados de acuerdo con algunas realizaciones de la presente divulgación.

Como se muestra en la figura 2, en el proceso de pago fuera de línea realizado por el terminal del comprador al terminal del comerciante, el comerciante puede generar un pedido en el teléfono móvil cliente del comerciante de acuerdo con las demandas de compra del comprador, y luego el teléfono móvil cliente del comerciante puede enviar una instrucción de consumo correspondiente al cliente de telefono móvil del comprador, en donde la instrucción de consumo puede incluir información del pedido correspondiente al pedido, por ejemplo, información relativa al tipo, importe y cantidad de mercancías compradas por el comprador.

Una vez que el teléfono móvil cliente del comprador recibe la instrucción de consumo enviada por el teléfono móvil cliente del comerciante, el comprador puede ver la información del pedido en el teléfono móvil cliente del comprador y confirmar la información del pedido. Después de confirmar la información del pedido, el comprador puede autorizar el pedido ingresando una contraseña de pago preestablecida o una huella digital en el teléfono móvil cliente del comprador. Después de adquirir la contraseña de pago o la huella digital introducida por el comprador, el teléfono móvil cliente del comprador puede autenticar la contraseña de pago o huella digital recibida localmente, generar un código de autorización de pago único, cuando se pasa la autenticación, de acuerdo con la información del pedido, la información del comprador y la información del teléfono móvil del comprador, y establecer el tiempo válido para el código de autorización de pago, que es válido dentro del tiempo válido.

Después de generar el código de autorización de pago, el teléfono móvil cliente del comprador puede enviar el código de autorización de pago al cliente de teléfono móvil del comerciante mediante el módulo NFC. Después de recibir el código de autorización de pago, el teléfono móvil cliente del comerciante puede ensamblar la información del pedido y el código de autorización de pago en la información de la transacción correspondiente, luego firmar la información de la transacción de acuerdo con el algoritmo de firma preestablecido y luego cargar la información de la transacción firmada en el servidor.

Después de recibir la información de la transacción enviada por el teléfono móvil cliente del comerciante, el lado del servidor primero autentica la firma de la información de la transacción. Si la autenticación de la firma falla, el lado del

servidor notifica directamente al cliente de teléfono móvil del comprador y al cliente de teléfono móvil del comerciante sobre la transacción fallida. Si la autenticación de la firma falla, el lado del servidor puede autenticar aún más el código de autorización de pago en la información de la transacción y notificar directamente al cliente de teléfono móvil del comprador y al cliente de teléfono móvil del comerciante sobre la transacción fallida si falla la autenticación del código de autorización de pago. Si la autenticación del código de autorización de pago tiene éxito, el lado del servidor puede autenticar además si el pedido correspondiente al código de autorización de pago es consistente con el pedido iniciado por el comerciante. La autorización del pedido tiene éxito si los dos pedidos son consistentes, y el lado del servidor puede completar directamente el pago localmente y transferir la suma de dinero de la cuenta del comprador a la cuenta del comerciante. Una vez que se completa el pago, el lado del servidor realiza un procesamiento comercial en el pedido y, respectivamente, envía un mensaje de notificación que indica el pago exitoso al cliente de teléfono móvil del comprador y al cliente de teléfono móvil del comerciante. Una vez que el teléfono móvil cliente del comprador y el teléfono móvil cliente del comerciante reciben el mensaje de notificación, se completa el pago de este pedido.

Como puede verse en las realizaciones anteriores de la presente divulgación, la información de servicio generada se envía al terminal de autorización de servicio por medio del terminal de inicio de servicio, recibe un código de autorización de servicio generado por el terminal de autorización de servicio por medio de cálculo con base en la información del servicio y la información relevante del usuario. El terminal de inicio del servicio genera información de autenticación del servicio de acuerdo con la información del servicio y el código de autorización del servicio, y carga la información de autenticación del servicio en un lado del servidor para que el lado del servidor procese el servicio después de autenticar el código de autorización del servicio. En la presente divulgación, debido a que la autenticación de la información del servicio se lleva a cabo de manera uniforme por el lado del servidor, para algunos servicios con mayor seguridad, es posible que ya no sea necesario simular un entorno de servicio confiable en el terminal de autorización de servicio y el terminal de inicio del servicio beneficiando así la promoción del servicio.

Cuando la solución técnica de la presente divulgación se aplica a un servicio de pago fuera de línea, se puede implementar que, en el proceso de pago, ya no sea necesario simular un entorno de servicio confiable en el terminal de un comerciante y en el terminal de un usuario estableciendo un módulo de seguridad adicional. El terminal del comerciante y el terminal del usuario pueden finalizar el servicio de pago utilizando un terminal general, beneficiando así la promoción del servicio de pago.

En correspondencia con las realizaciones del método anterior, la presente divulgación proporciona además realizaciones del aparato.

Haciendo referencia a la figura 3, la presente divulgación proporciona un aparato 30 de autenticación de servicio aplicable a un terminal, que puede ser un terminal de inicio de servicio. Refiriéndose a la figura 4 como un ejemplo de una realización del aparato 30 de autenticación de servicios, una arquitectura de hardware involucrada con el soporte del terminal del aparato 30 de autenticación de servicios generalmente incluye una CPU, una memoria, una memoria no volátil, una interfaz de red y un bus interno, y similares. Tomando la implementación de software como un ejemplo, el aparato 30 de autenticación de servicios generalmente puede interpretarse como un dispositivo lógico formado por un programa de ordenador cargado en la memoria que combina hardware y software después de la ejecución de la CPU, y el aparato 30 incluye los siguientes módulos 301 a 303 (figura 3).

Un primer módulo 301 de envío está configurado para enviar información de servicio generada a un terminal de autorización de servicio.

Un primer módulo 302 receptor está configurado para recibir un código de autorización de servicio correspondiente a la información de servicio enviada por el terminal de autorización de servicio, en donde el código de autorización de servicio es generado por el terminal de autorización de servicio mediante cálculo con base en la información de servicio y la información relevante del usuario.

Un primer módulo 303 de generación está configurado para generar información de autenticación del servicio de acuerdo con la información del servicio y el código de autorización del servicio, y cargar la información de autenticación del servicio a un lado del servidor para que el lado del servidor procese el servicio después de autenticar el código de autorización del servicio.

En algunas realizaciones, el primer módulo 301 de envío está configurado específicamente para enviar la información de servicio generada al terminal de autorización de servicio con base en un módulo NFC preestablecido.

En algunas realizaciones, el aparato incluye además un módulo 304 de firma configurado para firmar digitalmente la información de autenticación del servicio antes de cargar la información de autenticación del servicio a un lado del servidor para que el lado del servidor continúe autenticando la información de autenticación del servicio después de autenticar la firma.

En algunas realizaciones, el primer módulo 302 receptor está configurado además para recibir un mensaje de notificación enviado por el lado del servidor después de terminar de procesar el servicio, en donde el mensaje de notificación está configurado para notificar que el servicio ha sido procesado por el lado del servidor.

En algunas realizaciones, el servicio incluye un servicio de pago fuera de línea, la información del servicio incluye información de pedido correspondiente al servicio de pago fuera de línea y la información de autenticación del servicio incluye información de transacción correspondiente al servicio de pago fuera de línea.

Haciendo referencia a la figura 5, la presente divulgación proporciona un aparato 50 de autenticación de servicios aplicable a un terminal, que puede ser un terminal de autorización de servicios. Refiriéndose a la figura 6 como un ejemplo de una realización del aparato 50 autenticación de servicios, una arquitectura de hardware involucrada con el soporte del terminal del aparato 50 de autenticación de servicios generalmente incluye una CPU, una memoria, una memoria no volátil, una interfaz de red y un bus interno, o similar. Tomando la implementación de software como un ejemplo, el aparato 50 de autenticación de servicio generalmente puede interpretarse como un dispositivo lógico formado por un programa de ordenador cargado en la memoria que combina hardware y software después de la ejecución de la CPU, y el aparato 50 incluye los siguientes módulos 501 a 503 (figura 5).

Un segundo módulo 501 de recepción está configurado para recibir información de servicio enviada por un terminal de inicio de servicio.

Un segundo módulo 502 de generación está configurado para generar un código de autorización de servicio correspondiente calculando la información de servicio y la información de usuario relevante de acuerdo con un algoritmo preestablecido.

Un segundo módulo 503 de envío está configurado para enviar el código de autorización de servicio al terminal de inicio de servicio por medio de un módulo NFC para que el terminal de inicio de servicio genere información de autenticación de servicio de acuerdo con la información de servicio y el código de autorización de servicio, y cargue la información de autenticación del servicio a un lado del servidor para que el lado del servidor procese el servicio después de autenticar el código de autorización del servicio.

En algunas realizaciones, el segundo módulo 501 de recepción está configurado específicamente para recibir, con base en un módulo NFC preestablecido, la información de servicio enviada por el terminal de inicio del servicio.

En algunas realizaciones, el aparato incluye además un módulo 504 de autorización configurado para realizar, antes de generar un código de autorización de servicio correspondiente calculando la información de servicio y la información de usuario relevante de acuerdo con un algoritmo preestablecido, una autorización de servicio sobre la información de servicio. El módulo 504 de autorización está configurado específicamente para adquirir información de autorización de servicio ingresada por un usuario, en donde la información de autorización de servicio incluye una contraseña o huella digital configurada para realizar una autorización de servicio, hacer coincidir la información de autorización de servicio adquirida con información de autorización de servicio almacenada localmente y determinar la autorización de la información de servicio para finalizar cuando la información de autorización de servicio adquirida coincida con la información de autorización de servicio almacenada localmente.

En algunas realizaciones, el segundo módulo 501 de recepción está configurado específicamente para recibir un mensaje de notificación enviado por el lado del servidor después de terminar de procesar el servicio, en donde el mensaje de notificación está configurado para notificar que el servicio ha sido procesado por el lado del servidor.

En algunas realizaciones, el código de autorización de servicio es válido dentro de un período de tiempo preestablecido.

En algunas realizaciones, el servicio incluye un servicio de pago fuera de línea, la información del servicio incluye información de pedido correspondiente al servicio de pago fuera de línea y la información de autenticación del servicio incluye información de transacción correspondiente al servicio de pago fuera de línea.

Otras realizaciones de la presente divulgación resultarán evidentes para los expertos en la técnica a partir de la consideración de la especificación y la práctica de la invención descrita en el presente documento. Esta divulgación está destinada a cubrir cualquier variación, uso o adaptación de la presente divulgación siguiendo los principios generales de la misma e incluyendo las desviaciones de la presente divulgación que se encuentran dentro de la práctica conocida o habitual en la técnica. Se pretende que la memoria descriptiva y los ejemplos se consideren únicamente a modo de ejemplo, indicándose el verdadero alcance de la presente divulgación mediante las siguientes reivindicaciones.

Se apreciará que la presente divulgación no se limita a la construcción exacta que se ha descrito anteriormente e ilustrada en los dibujos adjuntos, y que se pueden realizar diversas modificaciones y cambios sin apartarse del alcance de la misma. Se pretende que el alcance de la presente divulgación solo esté limitado por las reivindicaciones adjuntas.

Las realizaciones expuestas anteriormente solo se ilustran como realizaciones preferidas de la presente divulgación y no pretenden limitar la presente divulgación. Todas las modificaciones y principios de la presente divulgación estarán dentro del alcance de protección de la presente divulgación.

REIVINDICACIONES

1. Un método para la autenticación de un servicio de pago que utiliza un terminal de inicio de servicio y un terminal de autorización de servicio, el método que comprende:

enviar (101), por el terminal de inicio de servicio, información de servicio al terminal de autorización de servicio;
recibir, por el terminal de autorización de servicio, información de servicio enviada por el terminal de inicio del servicio;
generar (102), mediante el terminal de autorización de servicio, un código de autorización de servicio correspondiente a la información de servicio recibida, en donde el código de autorización de servicio es válido dentro de un período de tiempo preestablecido;
enviar, por el terminal de autorización de servicio, el código de autorización de servicio al terminal de inicio del servicio,
recibir (103), por el terminal de inicio del servicio, el código de autorización del servicio enviado por el terminal de autorización del servicio;
generar (104), mediante el terminal de inicio del servicio, información de autenticación del servicio que incluye la información del servicio y el código de autorización del servicio, y cargar la información de autenticación del servicio a un servidor para la autenticación del código de autorización del servicio y el procesamiento posterior del servicio después de dicha autenticación; y
recibir (106), en el terminal de autorización del servicio, un mensaje de notificación de que el servicio ha sido procesado por el servidor, siendo enviado el mensaje por el servidor después de terminar de procesar el servicio.

2. El método de acuerdo con la reivindicación 1, en donde el código de autorización de servicio es calculado por el terminal de autorización de servicio con base en información seleccionada del grupo que consiste en información de usuario y la información de servicio.

3. El método de acuerdo con la reivindicación 1, en donde el envío de la información de servicio al terminal de autorización de servicio es a través de un módulo de comunicación de campo cercano (NFC).

4. El método de acuerdo con la reivindicación 1, que comprende además:

firmar digitalmente, por el terminal de inicio del servicio, la información de autenticación del servicio antes de cargar la información de autenticación del servicio en el servidor, donde el servidor autentica la información de autenticación del servicio después de autenticar la firma.

5. El método de acuerdo con la reivindicación 1,

en donde el servicio incluye un servicio de pago fuera de línea,
en donde la información del servicio incluye información de pedido correspondiente al servicio de pago fuera de línea, y
en donde la información de autenticación del servicio incluye información de transacción correspondiente al servicio de pago fuera de línea.

6. El método de acuerdo con la reivindicación 1, en donde la recepción de la información de servicio enviada por el terminal de inicio del servicio se comprende a través de un módulo de comunicación de campo cercano (NFC).

7. El método de acuerdo con la reivindicación 1, que comprende además:

realizar, mediante el terminal de autorización de servicio, una autorización de servicio sobre la información de servicio antes de generar un código de autorización de servicio correspondiente utilizando la información de servicio y la información de usuario de acuerdo con un algoritmo preestablecido, incluyendo la realización de la autorización de servicio la adquisición de una contraseña o huella digital;
comparar, mediante el terminal de autorización de servicio, la información de autorización de servicio adquirida con la información de autorización de servicio almacenada localmente; y
determinar, mediante el terminal de autorización de servicio, la autorización de la información de servicio que se completará cuando la información de autorización de servicio adquirida coincida con la información de autorización de servicio almacenada localmente.

8. Un medio legible por ordenador que tiene almacenadas en él una pluralidad de instrucciones, la pluralidad de instrucciones que incluyen instrucciones que, cuando son ejecutadas por al menos dos procesadores, hacen que los procesadores realicen los pasos del método de acuerdo con una cualquiera de las reivindicaciones anteriores.

9. Un sistema adaptado para realizar el método de acuerdo con una cualquiera de las reivindicaciones 1 a 7.

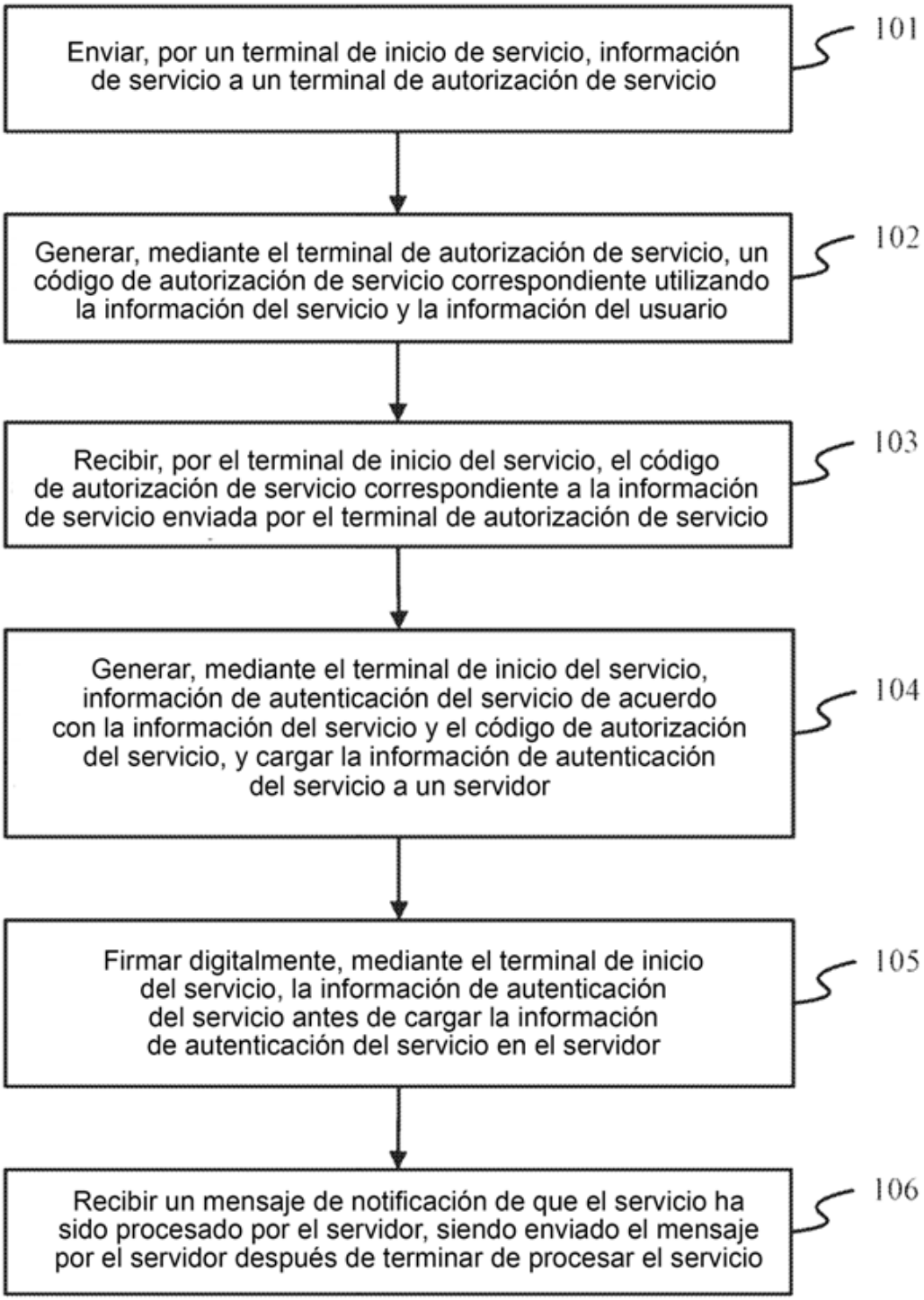
Enviar, por un terminal de inicio de servicio, información de servicio a un terminal de autorización de servicio
101
Generar, mediante el terminal de autorización de servicio, un código de autorización de servicio correspondiente utilizando la información del servicio y la información del usuario
102
Recibir, por el terminal de inicio del servicio, el código de autorización de servicio correspondiente a la información de servicio enviada por el terminal de autorización de servicio
103
Generar, mediante el terminal de inicio del servicio, información de autenticación del servicio de acuerdo con la información del servicio y el código de autorización del servicio, y cargar la información de autenticación del servicio a un servidor
104
Firmar digitalmente, mediante el terminal de inicio del servicio, la información de autenticación del servicio antes de cargar la información de autenticación del servicio en el servidor
105
Recibir un mensaje de notificación de que el servicio ha sido procesado por el servidor, siendo enviado el mensaje por el servidor después de terminar de procesar el servicio
106

FIG. 1

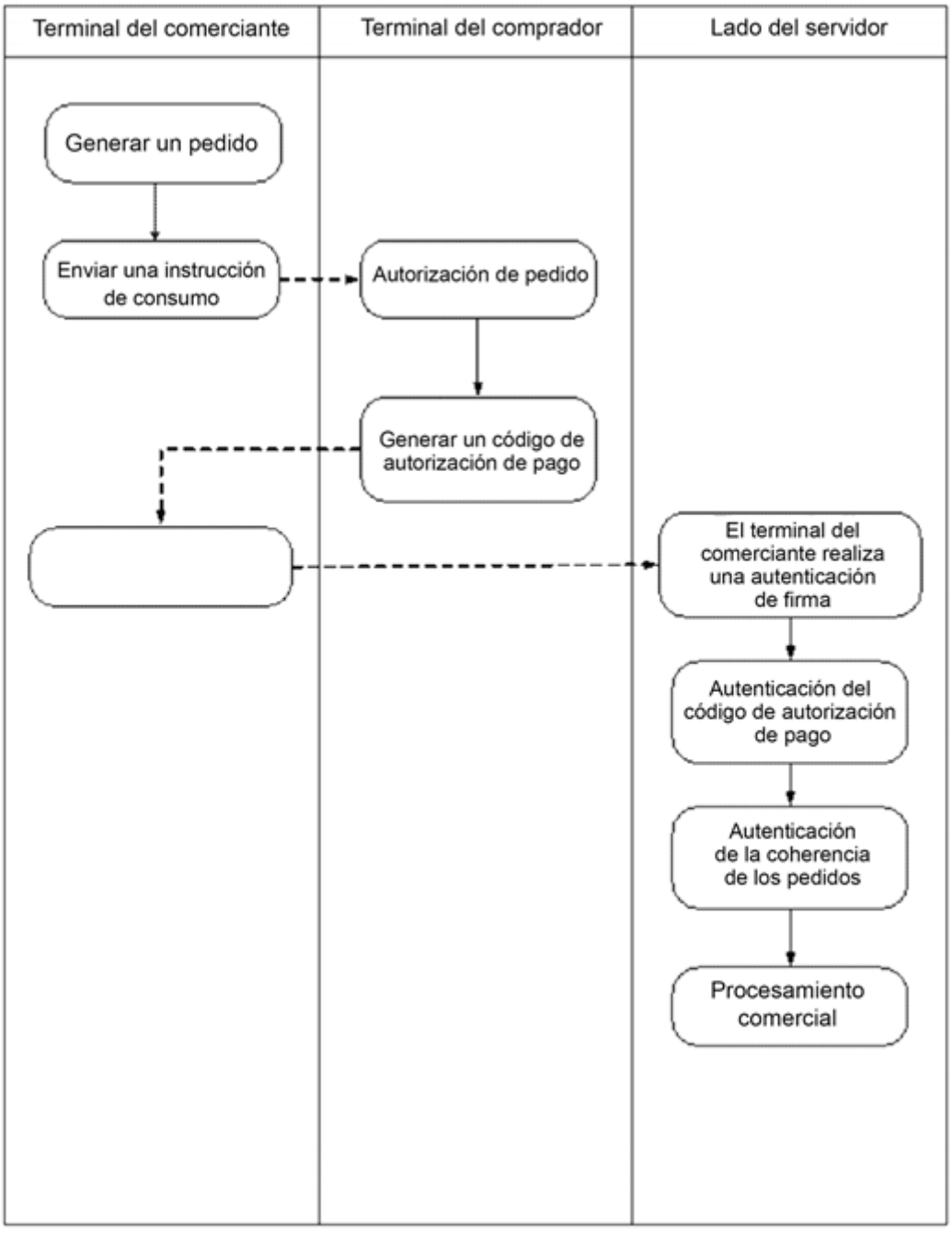
Terminal del comerciante
Terminal del comprador
Lado del servidor
Generar un pedido
Enviar una instrucción de consumo
Autorización de pedido
Generar un código de autorización de pago
El terminal del comerciante realiza una autenticación de firma
Autenticación del código de autorización de pago
Autenticación de la coherencia de los pedidos
Procesamiento comercial

FIG. 2

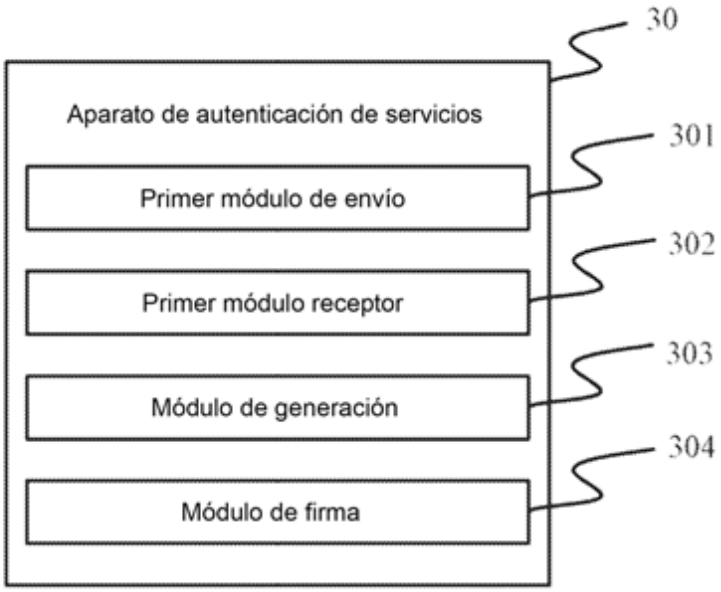
30
Aparato de autenticación de servicios
301
Primer módulo de envío
302
Primer módulo receptor
303
Módulo de generación
304
Módulo de firma

FIG. 3

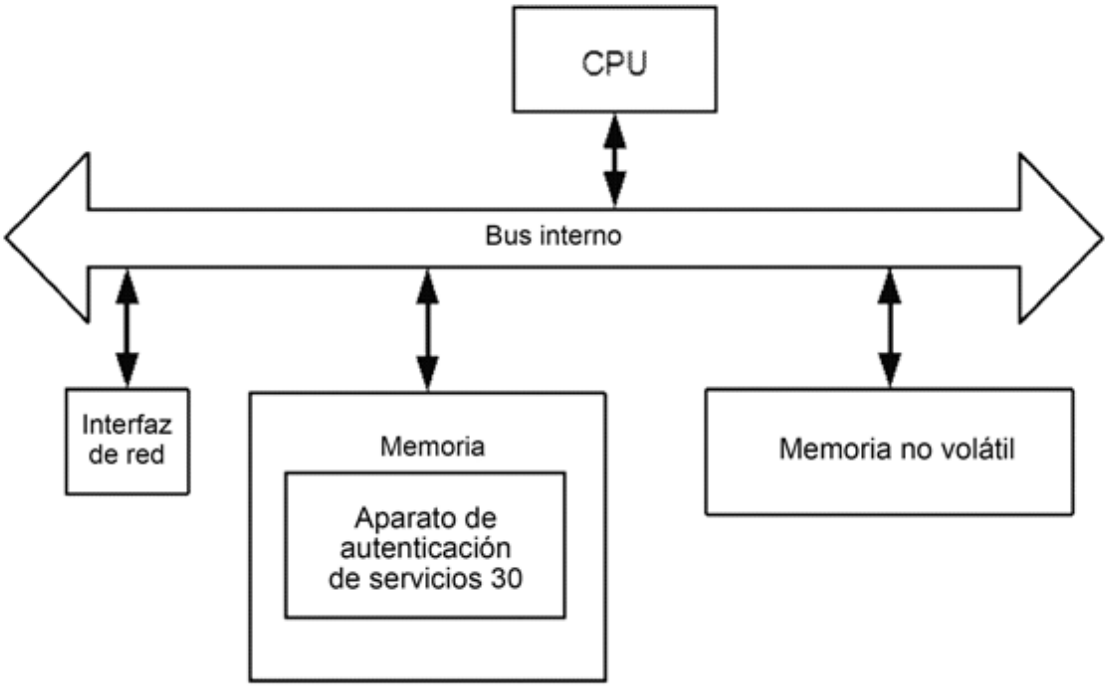
CPU
Bus interno
Interfaz de red
Memoria
Aparato de autenticación de servicios 30
Memoria no volátil

FIG. 4

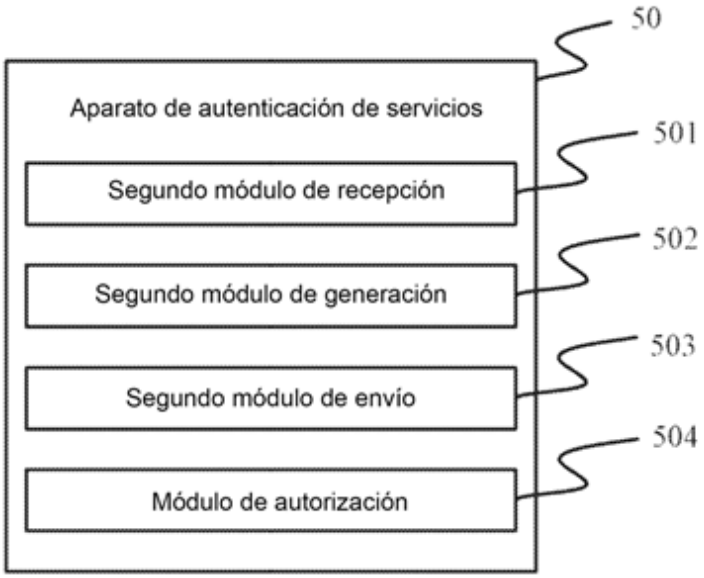
50
Aparato de autenticación de servicios
501
Segundo módulo de recepción
502
Segundo módulo de generación
503
Segundo módulo de envío
504
Módulo de autorización

FIG. 5

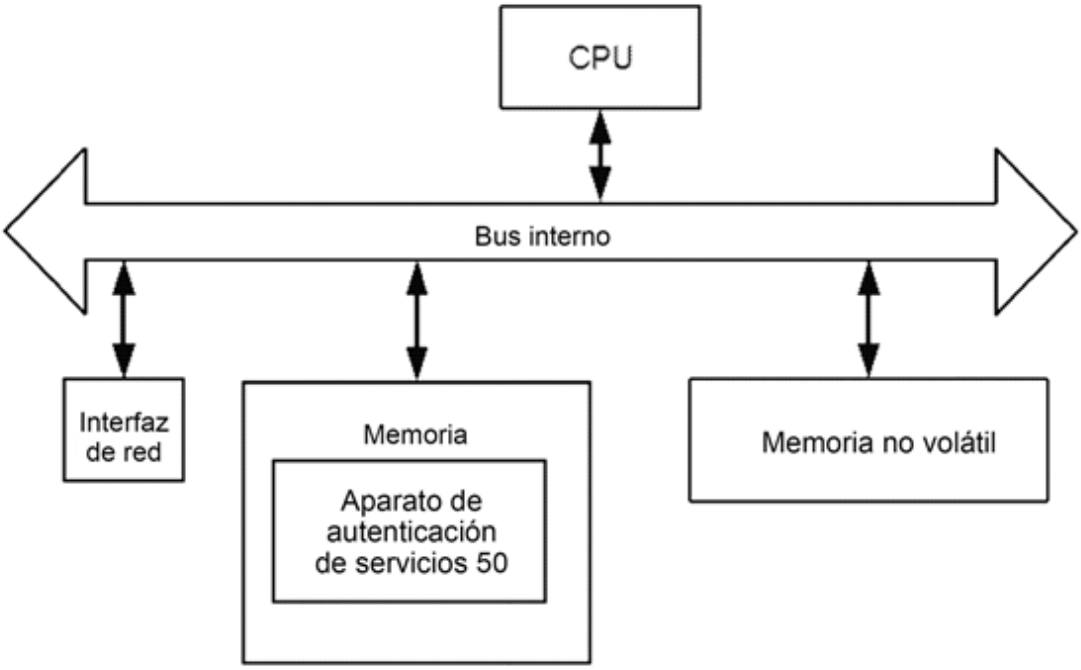
CPU
Bus interno
Interfaz de red
Memoria
Aparato de autenticación de servicios 50
Memoria no volátil

FIG. 6