(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 718 540**

(51) Int. CI.:

H04L 9/32 (2006.01)
G06F 21/57 (2013.01)
G06Q 20/32 (2012.01)
H04W 4/00 (2008.01)
G06Q 20/38 (2012.01)
G06Q 20/40 (2012.01)
H04W 12/08 (2009.01)
H04W 4/80 (2008.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **16.10.2015 PCT/CN2015/092098**

(87) Fecha y número de publicación internacional: **27.10.2016 WO16169229**

(96) Fecha de presentación y número de la solicitud europea: **16.10.2015 E 15888732 (3)**

(97) Fecha y número de publicación de la concesión europea: **09.01.2019 EP 3121752**

(54) Título: **Dispositivo y método de pago móvil**

(30) Prioridad:

24.04.2015 CN 201510201343

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
02.07.2019

(73) Titular/es:

HUAWEI TECHNOLOGIES CO., LTD. (100.0%)
Huawei Administration Building, Bantian, Longgang District
Shenzhen, Guangdong 518129, CN

(72) Inventor/es:

PAN, SHILIN

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

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

Dispositivo y método de pago móvil.

Campo técnico

La presente invención se refiere al campo de la comunicación móvil y, en particular, a un aparato y un método de pago móvil.

Antecedentes

Pago móvil se refiere a una manera de servicio en la cual se permite a un usuario que use un terminal móvil como, por ejemplo, un teléfono móvil o una tableta del usuario, para realizar el pago de un producto básico o servicio consumido. Actualmente, existen tres maneras de implementar el pago móvil mediante el uso de un terminal móvil, las cuales son, respectivamente: una solución de tarjeta digital segura (SD, por sus siglas en inglés), una solución de módulo de identidad de abonado (SIM, por sus siglas en inglés) y una solución basada en terminal que combina la comunicación de campo cercano (NFC, por sus siglas en inglés) con un elemento seguro (SE, por sus siglas en inglés). Actualmente, la solución basada en el terminal que combina la comunicación de campo cercano con un elemento seguro se ha convertido gradualmente en una corriente principal para la implementación de una solución de pago móvil.

Una solución existente basada en terminal se muestra en la Figura 1: Un terminal móvil 10 se comunica con una máquina de punto de venta (POS, por sus siglas en inglés) 11 mediante el uso de una unidad de comunicación de campo cercano 101 en el terminal móvil 10, y un enlace de comunicación radioeléctrica de corta distancia 12 entre la unidad de comunicación de campo cercano 101 y la máquina POS 11 es un trayecto bidireccional, y puede implementarse mediante el uso de varios protocolos de comunicación radioeléctrica de corta distancia, para implementar una función de comunicación radioeléctrica básica en el pago móvil. Por ejemplo, el enlace de comunicación 12 puede usarse para transmitir datos de instrucción POS y similares de la máquina POS 11 a la unidad de comunicación de campo cercano 101 en el terminal móvil 10. Un elemento seguro 102 puede ser un componente acoplado a una unidad de procesamiento central (CPU, por sus siglas en inglés) independiente 103, y se configura para ejecutar varias funciones relacionadas con un servicio de pago financiero, y almacenar datos como, por ejemplo, una clave o un certificado que se relaciona con un servicio bancario. En una transacción, el elemento seguro 102 recibe los datos de instrucción POS de la unidad de comunicación de campo cercano 101, analiza los datos de instrucción y provee una respuesta correspondiente según un protocolo de transacción financiera. La respuesta se realimenta por la unidad de comunicación de campo cercano 101 a la máquina POS 11, para completar la transmisión de datos en el pago móvil, de modo que una función en la que el terminal móvil 10 se usa como una tarjeta de verificación de transacción se implementa. La unidad de procesamiento central 103 ejecuta el software del sistema operativo 1031, por ejemplo, software del sistema Android, y la unidad de procesamiento central 103 se configura para controlar la unidad de comunicación de campo cercano 101 y el elemento seguro 102, por ejemplo, controlar el encendido o apagado de la unidad de comunicación de campo cercano 101 y del elemento seguro 102. Además, el terminal móvil 10 puede incluir una unidad de entrada 104. La unidad de entrada 104 puede ser una pantalla táctil y se configura para intercambiar mensajes con un usuario mediante el uso de una interfaz de usuario (IU), de modo que el usuario puede ingresar una instrucción de operación en la unidad de entrada 104 mediante el uso de la IU, para ordenar al software del sistema operativo 1031 y al software de aplicación relacionado que lleven a cabo una operación relacionada, por ejemplo, confirmar una transacción o ingresar una contraseña de transacción personal. La máquina POS 11, como un dispositivo terminal para llevar a cabo una transacción, se conecta a un servidor en la nube 14 en un lado de red mediante el uso de Internet, de modo que un servicio de pago se calcula y completa mediante el uso del servidor 14. El servidor 14 en el lado de red se ejecuta, en general, por un banco.

La solución basada en el terminal puede incluir pago en línea y pago fuera de línea. En el pago fuera de línea, como se muestra en la Figura 1, la lectura de tarjeta sin contacto se lleva a cabo entre el terminal móvil 10 y la máquina POS 11, es decir, un teléfono móvil se lee, y la unidad de comunicación de campo cercano 101 y el elemento seguro 102 actúan juntos para completar una transacción de pago. El pago en línea puede implementarse sin usar la unidad de comunicación de campo cercano 10. En el presente caso, la unidad de procesamiento central 103 y el elemento seguro 102 pueden conectarse a Internet a través de una red de comunicación móvil, para implementar el pago en línea. En el presente caso, el elemento seguro 102 logra un propósito equivalente al de una clave USB bancaria, y se configura para almacenar y verificar un certificado bancario. Por lo tanto, la unidad de comunicación de campo cercano 101 en la Figura 1 es opcional. De manera específica, con referencia a la Figura 1, cuando el pago en línea se lleva a cabo, el terminal móvil 10 puede además incluir una unidad de comunicación móvil 105, configurada para funcionar en lugar de la unidad de comunicación de campo cercano 101 cuando el pago fuera de línea se lleva a cabo. La unidad de comunicación móvil 105 se conecta a una red de acceso radioeléctrico (RAN, por sus siglas en inglés) 15 y, de manera específica, a una estación base en la red de acceso radioeléctrico 15, y se conecta a Internet a través de la red de acceso radioeléctrico 15. Internet se conecta al servidor 14 ubicado en Internet, de modo que el servidor 14 recibe datos de instrucciones o transmite información al elemento seguro 102. El elemento seguro 102 analiza los datos de instrucciones y provee una respuesta correspondiente según el protocolo de transacción financiera, de modo que la unidad de comunicación móvil 105 transmite los datos al servidor 14 en un

lado de red a través de Internet móvil. En el presente caso, la unidad de comunicación móvil 105 puede ser una unidad que ejecuta un protocolo de comunicación radioeléctrica celular, y se configura para conectar el terminal móvil 10 a Internet mediante el uso de un enlace de comunicación radioeléctrica celular 13. La unidad de comunicación móvil 105 puede, de manera específica, ejecutar un protocolo de comunicación radioeléctrica celular como, por ejemplo, el Sistema Global para Comunicaciones Móviles (GSM, por sus siglas en inglés), el Sistema Universal de Telecomunicaciones Móviles (UMTS, por sus siglas en inglés), la Interoperabilidad Mundial para Acceso por Microondas (WiMAX, por sus siglas en inglés) o la Evolución a Largo Plazo (LTE, por sus siglas en inglés), para implementar una función de Internet móvil del terminal móvil 10.

Actualmente, en soluciones usadas por varios terminales móviles, el elemento seguro 102 se dispone fuera de un sistema primario. Como se muestra en la Figura 1, la unidad de procesamiento central 103 y la unidad de comunicación móvil 105 pueden ubicarse en un sustrato de circuito integrado, es decir, integrado a un chip central 106. El elemento seguro 102 es, de manera específica, un chip independiente del chip central 106. El elemento seguro 102 se comunica, de manera específica, con la unidad de procesamiento central 103 en el chip central 106 mediante el uso de una interfaz de periféricos serie (SPI, por sus siglas en inglés). Sin embargo, el elemento seguro 102 se dispone fuera del chip central 106, lo cual resulta en que el elemento seguro 102 y el chip central 106 ocupan un área grande en una placa principal del terminal móvil 10, y se requiere un coste más alto.

La Solicitud de Patente de Estados Unidos US2014/0020114 A1 describe un método, un aparato y un producto de programa de ordenador para la comunicación inalámbrica en conexión con la provisión de funcionalidad SE eficaz. La Solicitud de Patente de Estados Unidos US2014324698 A1 describe un dispositivo móvil con una CPU que ejecuta una aplicación de control de pago y un OS genérico y un elemento seguro que ejecutan una miniaplicación de pago y un sistema operativo de bajo nivel.

Compendio

Las realizaciones de la presente invención proveen un aparato y método de pago móvil, para reducir costes y un área para la implementación de hardware de pago móvil.

Según un primer aspecto, una realización de la presente invención provee un aparato de pago móvil, que incluye: una unidad de comunicación, configurada para intercambiar información de pago con un extremo par de comunicación mediante el uso de un enlace radioeléctrico; una memoria, configurada para almacenar software de pago móvil; un elemento seguro, que incluye un primer módulo de almacenamiento y un procesador; y al menos una unidad de procesamiento central, configurada para ejecutar software de sistema operativo general, y controlar al menos uno de la unidad de comunicación, la memoria, o el elemento seguro bajo la acción del software de sistema operativo general, donde el procesador se configura para cargar el software de pago móvil de la memoria al primer módulo de almacenamiento, ejecutar el software de pago móvil e intercambiar la información de pago con la unidad de comunicación bajo la acción del software de pago móvil; y el primer módulo de almacenamiento se configura para proveer espacio de memoria para ejecutar el software de pago móvil para el procesador, donde el elemento seguro y la al menos una unidad de procesamiento central se ubican en un primer chip semiconductor en el aparato de pago móvil. El elemento seguro y la al menos una unidad de procesamiento central se integran mediante el uso del mismo primer chip semiconductor; por lo tanto, los costes y un área para la implementación de hardware de pago móvil se reducen. De manera opcional, la unidad de comunicación puede incluir una unidad de banda base. La unidad de comunicación puede además incluir una unidad de frecuencia radioeléctrica.

Con referencia al primer aspecto, en una primera manera de implementación posible del primer aspecto, la memoria se ubica en un segundo chip semiconductor en el aparato de pago móvil. Dado que el primer chip semiconductor es independiente del segundo chip semiconductor, la unidad de almacenamiento que almacena el software de pago móvil no necesita integrarse al elemento seguro que ejecuta el software de pago móvil, lo cual reduce la dificultad y complejidad de la implementación de hardware. De manera especial, por motivos como, por ejemplo, un proceso y un área, es difícil integrar una memoria actual al primer chip que incluye una CPU. En la presente solución, solo el elemento seguro se integra a la CPU, y se usa una memoria fuera de chip, que es más apropiada para una solución de pago móvil.

Con referencia a la primera manera de implementación posible del primer aspecto, en una segunda manera de implementación posible del primer aspecto, la memoria incluye una región de almacenamiento seguro y una región de almacenamiento común que se encuentran aisladas entre sí, donde la región de almacenamiento seguro se usa para almacenar el software de pago móvil, y la región de almacenamiento común se usa para almacenar el software de sistema operativo general; y el procesador se configura, de manera específica, para cargar el software de pago móvil de la región de almacenamiento seguro en la memoria al primer módulo de almacenamiento; y la al menos una unidad de procesamiento central se configura, de manera específica, para leer el software de sistema operativo general de la región de almacenamiento común en la memoria y ejecutar el software de sistema operativo general. La manera de implementación es equivalente a aquella en la cual la memoria se reutiliza tanto para el software del sistema operativo general como para el software de pago móvil, de modo que el software del sistema operativo general y el software del pago móvil coexisten en una memoria y se encuentran aislados, de manera segura, entre sí, lo cual ahorra recursos de memoria sobre la premisa de garantizar la seguridad.

Con referencia a la primera manera de implementación posible del primer aspecto, en una tercera manera de implementación posible del primer aspecto, la memoria se dedica al almacenamiento del software de pago móvil; el aparato de pago móvil además incluye una unidad de almacenamiento común, donde la unidad de almacenamiento común se ubica en un tercer chip semiconductor en el aparato de pago móvil, y la unidad de almacenamiento común se configura para almacenar el software del sistema operativo general; y la al menos una unidad de procesamiento central se configura, de manera específica, para leer el software del sistema operativo general de la unidad de almacenamiento común y ejecutar el software del sistema operativo general. En la manera de implementación, la memoria dedicada que es específica para el almacenamiento del software de pago móvil puede estar físicamente aislada de la unidad de almacenamiento común, de modo que la seguridad operativa se mejora más.

Con referencia al primer aspecto o a cualquiera de la primera a la tercera maneras de implementación posibles del primer aspecto, en una cuarta manera de implementación posible del primer aspecto, el software de pago móvil incluye software del sistema operativo de pago móvil. El software del sistema operativo de pago móvil seguro y fiable se usa en el software de pago móvil, lo cual puede garantizar la seguridad operativa, y también ayudar a implementar más tipos de software de aplicación de pago móvil mediante el uso del software del sistema operativo de pago móvil como una plataforma, por ejemplo, para el soporte de servicios de diferentes bancos. De manera opcional, el software del sistema operativo de pago móvil es un espejo COS.

Con referencia a la cuarta manera de implementación posible del primer aspecto, en una quinta manera de implementación posible del primer aspecto, el software de pago móvil además incluye al menos un tipo de software de aplicación de pago móvil. Una cantidad mayor de software de aplicación de pago móvil ayuda a extender un servicio de pago móvil a más proveedores de servicio diferentes, por ejemplo, diferentes bancos u organizaciones comerciales.

Con referencia a la cuarta o quinta maneras de implementación posibles del primer aspecto, en una sexta manera de implementación posible del primer aspecto, el elemento seguro además incluye: un segundo módulo de almacenamiento, configurado para almacenar un programa de arranque para iniciar el procesador; y cuando el elemento seguro se enciende, el procesador se configura para leer el programa de arranque del segundo módulo de almacenamiento, cargar el software del sistema operativo de pago móvil de la memoria al primer módulo de almacenamiento bajo la acción del programa de arranque, y ejecutar el software del sistema operativo de pago móvil. Dado que un programa de arranque para iniciar el elemento seguro se ubica en un segundo módulo de almacenamiento independiente en el elemento seguro, la seguridad de arranque del elemento seguro puede garantizarse.

Con referencia a la quinta manera de implementación posible del primer aspecto, en una séptima manera de implementación posible del primer aspecto, el procesador se configura para cargar uno o más tipos de software de aplicación de pago móvil del al menos un tipo de software de aplicación de pago móvil de la memoria al primer módulo de almacenamiento después de activarse por la información de pago intercambiada entre el procesador y la unidad de comunicación, y ejecutar el único o más tipos de software de aplicación de pago móvil. Dado que la carga y ejecución del software de aplicación de pago móvil se activa por la información de pago intercambiada, cuando no hay servicio de pago, el software de aplicación de pago móvil relacionado puede no iniciarse, lo cual puede ahorrar espacio de memoria del primer módulo de almacenamiento. De manera especial, en un caso en el cual el elemento seguro se integra altamente, el espacio del primer módulo de almacenamiento es muy limitado, y la presente solución puede lograr un buen efecto de ahorro de costes.

Con referencia al primer aspecto o a cualquiera de la primera a la séptima maneras de implementación posibles del primer aspecto, en una octava manera de implementación posible del primer aspecto, la información de pago incluye: una instrucción de pago móvil que se transmite del extremo par de comunicación al procesador mediante la unidad de comunicación, y los datos de pago móvil transmitidos del procesador al extremo par de comunicación mediante la unidad de comunicación en respuesta a la instrucción de pago móvil. Por lo tanto, la información de pago implica un proceso de comunicación bidireccional en el pago móvil.

Con referencia a la octava manera de implementación posible del primer aspecto, en una novena manera de implementación posible del primer aspecto, los datos de pago móvil incluyen datos que resultan del procesamiento de seguridad, y el procesamiento de seguridad incluye al menos una de las siguientes: encriptación de datos o protección de integridad de datos. Dado que el procesamiento de seguridad se lleva a cabo en los datos de pago móvil, cuando el aparato de pago móvil se configura para llevar a cabo el pago móvil, la seguridad de los datos de pago móvil enviados al extremo par de comunicación es más segura.

Con referencia a la novena manera de implementación posible del primer aspecto, en una décima manera de implementación posible del primer aspecto, el procesador se configura además para generar los datos que resultan del procesamiento de seguridad. Dado que el procesador incluye un proceso de procesamiento de seguridad, el proceso de procesamiento de seguridad está más centralizado en el procesador, y no se necesita hardware de seguridad adicional, lo cual puede reducir el coste.

Con referencia a la novena manera de implementación posible del primer aspecto, en una undécima manera de implementación posible del primer aspecto, el procesador se configura además para generar datos originales; el

elemento seguro además incluye: un módulo de procesamiento de seguridad, configurado para llevar a cabo el procesamiento de seguridad en los datos originales para generar los datos que resultan del procesamiento de seguridad. El módulo de procesamiento de seguridad independiente del procesador se usa para llevar a cabo el procesamiento de seguridad y, de esta manera, implementar la aceleración del procesamiento de seguridad y además optimizar la implementación del procesamiento. De manera opcional, el módulo de procesamiento de seguridad puede ser un acelerador de hardware.

Con referencia al primer aspecto o a cualquiera de la primera a la undécima maneras de implementación posibles del primer aspecto, en una duodécima manera de implementación posible del primer aspecto, el control llevado a cabo por la al menos una unidad de procesamiento central en el al menos uno de la unidad de comunicación, la memoria, o el elemento seguro incluye: el control de encendido, apagado, entrada en o salida de un estado de potencia baja, o un estado de funcionamiento. De manera opcional, la al menos una unidad de procesamiento central puede ser un procesador de máquina de ordenador de conjunto de instrucciones reducidas avanzadas (Máquina RISC, por sus siglas en inglés, ARM, por sus siglas en inglés). La al menos una unidad de procesamiento central puede, de manera conveniente, controlar la ejecución de otra unidad en un sistema en general.

Con referencia al primer aspecto o a cualquiera de la primera a la duodécima maneras de implementación posibles del primer aspecto, en una decimotercera manera de implementación posible del primer aspecto, la unidad de comunicación es una unidad de comunicación de campo cercano, el extremo par de comunicación es un terminal de pago, y la unidad de comunicación de campo cercano se configura, de manera específica, para intercambiar la información de pago con el terminal de pago mediante la ejecución de un protocolo de comunicación radioeléctrica de corta distancia. En la presente solución, el pago móvil se lleva a cabo, de manera conveniente, mediante el uso de la unidad de comunicación de campo cercano y el terminal de pago, por ejemplo, una máquina POS. De manera opcional, la unidad de comunicación de campo cercano incluye una unidad de banda base de comunicación de campo cercano configurada para ejecutar el protocolo de comunicación radioeléctrica de corta distancia. Asimismo, la unidad de comunicación de campo cercano además incluye una unidad de frecuencia radioeléctrica de comunicación de campo cercano configurada para recibir o enviar una señal de frecuencia radioeléctrica, donde la señal de frecuencia radioeléctrica se convierte por la unidad de frecuencia radioeléctrica de comunicación de campo cercano en una señal de banda base que puede procesarse por la unidad de banda base de comunicación de campo cercano, y la señal de frecuencia radioeléctrica incluye la información de pago.

Con referencia a la decimotercera manera de implementación posible del primer aspecto, en una decimocuarta manera de implementación posible del primer aspecto, la unidad de comunicación de campo cercano se ubica en el primer chip semiconductor o se ubica en un cuarto chip semiconductor en el aparato de pago móvil. Cuando la unidad de comunicación de campo cercano se ubica en el primer chip semiconductor, la alta integración de la unidad de comunicación de campo cercano, el elemento seguro y la al menos una unidad de procesamiento central puede implementarse, y el coste de implementación puede reducirse. Cuando la unidad de comunicación de campo cercano se ubica en un cuarto chip semiconductor, la dificultad de diseño provocada por la necesidad de integrar la unidad de comunicación de campo cercano puede reducirse.

Con referencia al primer aspecto o a cualquiera de la primera a la duodécima maneras de implementación posibles del primer aspecto, en una decimoquinta manera de implementación posible del primer aspecto, la unidad de comunicación es una unidad de comunicación móvil, el extremo par de comunicación es una red de acceso radioeléctrico, y la unidad de comunicación móvil se configura para intercambiar la información de pago con la red de acceso radioeléctrico mediante la ejecución de un protocolo de comunicación radioeléctrica celular. La presente solución ayuda a implementar una función de pago seguro por medio de la comunicación móvil. De manera opcional, la unidad de comunicación móvil incluye una unidad de banda base de comunicación móvil usada en el protocolo de comunicación radioeléctrica celular. Asimismo, la unidad de comunicación móvil además incluye una unidad de frecuencia radioeléctrica de comunicación móvil configurada para recibir o enviar una señal de frecuencia radioeléctrica, donde la señal de frecuencia radioeléctrica se convierte por la unidad de frecuencia radioeléctrica de comunicación móvil en una señal de banda base que puede procesarse por la unidad de banda base de comunicación móvil, y la señal de frecuencia radioeléctrica incluye la información de pago.

Con referencia a la decimoquinta manera de implementación posible del primer aspecto, en una decimosexta manera de implementación posible del primer aspecto, la unidad de comunicación móvil se ubica en el primer chip semiconductor o se ubica en un quinto chip semiconductor en el aparato de pago móvil. Cuando la unidad de comunicación móvil se ubica en el primer chip semiconductor, la alta integración puede implementarse, y el coste de implementación puede reducirse. Cuando la unidad de comunicación móvil se ubica en un quinto chip semiconductor, la dificultad de diseño provocada por la integración puede reducirse.

Con referencia al primer aspecto o a cualquiera de la primera a la decimosexta maneras de implementación posibles del primer aspecto, en una decimoséptima manera de implementación posible del primer aspecto, el elemento seguro además incluye: un motor cifrado, configurado para llevar a cabo la verificación de seguridad en el software de pago móvil después de que el procesador carga el software de pago móvil de la memoria al primer módulo de almacenamiento, y ordenar al procesador que ejecute el software de pago móvil después de que la verificación de seguridad tiene éxito, donde la verificación de seguridad incluye al menos una de la desencriptación de seguridad o verificación de troceo. De manera opcional, el motor cifrado puede ser un acelerador de hardware. Dado que el

motor cifrado es independiente del procesador en el elemento seguro, y se dedica a la implementación de una función de verificación de seguridad, el software de pago móvil puede ejecutarse después de que la verificación tiene éxito, lo cual asegura que el software de pago móvil no se altera antes de la ejecución, y ayuda a mejorar el rendimiento del procesamiento cuando se lleva a cabo la verificación de seguridad.

Con referencia a la decimoséptima manera de implementación posible del primer aspecto, en una decimoctava manera de implementación posible del primer aspecto, el motor cifrado se configura además para llevar a cabo al menos un tipo de procesamiento en la encriptación de seguridad o primer procesamiento de operación de troceo en datos de actualización, para obtener datos de actualización procesados; y el procesador se configura además para escribir los datos de actualización procesados en la memoria, para actualizar el software de pago móvil. Cuando el software de pago móvil necesita actualizarse, el motor cifrado lleva a cabo el procesamiento, de modo que el software relacionado se verifica cuando el software de pago móvil actualizado se lee posteriormente otra vez, lo cual asegura que el software de pago móvil no se altera, y garantiza la seguridad del software que necesita actualizarse mejor.

Con referencia al primer aspecto o a cualquiera de la primera a la decimosexta maneras de implementación posibles del primer aspecto, en una decimonovena manera de implementación posible del primer aspecto, el procesador se configura además para llevar a cabo la verificación de seguridad en el software de pago móvil después de que el procesador carga el software de pago móvil de la memoria al primer módulo de almacenamiento, y ejecutar el software de pago móvil después de que la verificación de seguridad tiene éxito, donde la verificación de seguridad incluye al menos una de la desencriptación de seguridad o primera verificación de troceo. Dado que el procesador ya tiene la función de verificación de seguridad, el procesador no necesita una unidad adicional para implementar la función, lo cual reduce la dificultad de diseño.

Con referencia a la decimonovena manera de implementación posible del primer aspecto, en una vigésima manera de implementación posible del primer aspecto, el procesador se configura además para llevar a cabo al menos un tipo de procesamiento en la encriptación de seguridad o primer procesamiento de operación de troceo en datos de actualización, para obtener datos de actualización procesados, y escribir los datos de actualización procesados en la memoria, para actualizar el software de pago móvil. Cuando el software de pago móvil necesita actualizarse, el procesador puede además llevar a cabo el procesamiento de seguridad en el software que necesita actualizarse, de modo que el software relacionado se verifica cuando el software de pago móvil actualizado se lee posteriormente otra vez, lo cual implementa la integración de más funciones en el procesador.

Con referencia a la decimoctava o vigésima maneras de implementación posibles del primer aspecto, en una vigésimo primera manera de implementación posible del primer aspecto, el procesador se configura además para llevar a cabo el segundo procesamiento de operación de troceo en los datos de actualización procesados mediante el uso de una clave para obtener datos que se almacenarán cuando el procesador escribe los datos de actualización procesados en la memoria; y la memoria se configura además para llevar a cabo la segunda verificación de troceo en los datos que se almacenarán, obtener los datos de actualización procesados después de que la segunda verificación de troceo tiene éxito, y actualizar el software de pago móvil mediante el uso de los datos de actualización procesados. Dado que el procesador tiene la capacidad descrita más arriba, los datos escritos en la memoria necesitan, todos, verificarse por la memoria, lo cual garantiza la seguridad de los datos escritos en la memoria.

Con referencia a la decimoctava o vigésima maneras de implementación posibles del primer aspecto, en una vigésimo segunda manera de implementación posible del primer aspecto, el procesador se configura además para enviar los datos de actualización procesados a la al menos una unidad de procesamiento central cuando el procesador escribe los datos de actualización procesados en la memoria; la al menos una unidad de procesamiento central se configura además para llevar a cabo el segundo procesamiento de operación de troceo en los datos de actualización procesados en un entorno de ejecución fiable mediante el uso de una clave, para obtener datos que se almacenarán, y enviar los datos que se almacenarán a la memoria, donde el entorno de ejecución fiable se encuentra aislado, de manera segura, del software de sistema operativo general; y la memoria se configura además para llevar a cabo la segunda verificación de troceo en los datos que se almacenarán, obtener los datos de actualización procesados después de que la segunda verificación de troceo tiene éxito, y actualizar el software de pago móvil mediante el uso de los datos de actualización procesados. En la presente solución, cuando los datos de actualización se escriben del procesador a la memoria, los datos de actualización necesitan transferirse mediante el uso del entorno de ejecución fiable de la al menos una unidad de procesamiento central, y el procesamiento de troceo se lleva a cabo en los datos de actualización en el entorno de ejecución fiable, de modo que la memoria lleva a cabo la correspondiente verificación de troceo. Dado que el entorno de ejecución fiable es más fiable que el software del sistema operativo general, la seguridad de los datos escritos en la memoria puede mejorarse.

Con referencia a la vigésimo segunda manera de implementación posible del primer aspecto, en una vigésimo tercera manera de implementación posible del primer aspecto, el elemento seguro además incluye un tercer módulo de almacenamiento; el procesador se configura además para escribir los datos de actualización procesados en el tercer módulo de almacenamiento, y enviar una primera solicitud de interrupción a la al menos una unidad de procesamiento central; la al menos una unidad de procesamiento central se configura además para leer los datos de

actualización procesados del tercer módulo de almacenamiento en el entorno de ejecución fiable en respuesta a la primera solicitud de interrupción.

Con referencia al primer aspecto o a cualquiera de la primera a la vigésimo tercera maneras de implementación posibles del primer aspecto, en una vigésimo cuarta manera de implementación posible del primer aspecto, la al menos una unidad de procesamiento central se configura además para ejecutar el software de aplicación común a excepción del software de pago móvil. La al menos una unidad de procesamiento central es una unidad de procesamiento central general comúnmente usada en un terminal móvil, y ayuda a extender la solución en un terminal móvil común.

Con referencia al primer aspecto o a cualquiera de la primera a la vigésimo cuarta maneras de implementación posibles del primer aspecto, en una vigésimo quinta manera de implementación posible del primer aspecto, el software del sistema operativo general ejecutado por la al menos una unidad de procesamiento central se encuentra aislado, de manera segura, del elemento seguro. Dado que el aislamiento existe, el software del sistema operativo general no puede acceder, de manera aleatoria, al elemento seguro, lo cual puede mejorar la seguridad del pago móvil.

Con referencia al primer aspecto, o a cualquiera de la primera a la decimoséptima maneras de implementación posibles, la decimonovena manera de implementación posible, la vigésimo cuarta manera de implementación posible, y la vigésimo quinta manera de implementación posible del primer aspecto, en una vigésimo sexta manera de implementación posible del primer aspecto, el procesador se configura además para llevar a cabo un segundo procesamiento de operación de troceo en datos de actualización o una instrucción de borrado mediante el uso de una clave, para obtener un resultado de procesamiento; y la memoria se configura además para llevar a cabo una segunda verificación de troceo en el resultado de procesamiento, obtener los datos de actualización o la instrucción de borrado después de que la segunda verificación de troceo tiene éxito, y actualizar el software de pago móvil mediante el uso de los datos de actualización o datos de borrado que corresponden a la instrucción de borrado de la memoria según la instrucción de borrado. La presente solución mejora la seguridad de borrado de datos en el pago móvil.

Con referencia al primer aspecto o a cualquiera de la primera a la decimoséptima maneras de implementación posibles, la decimonovena manera de implementación posible, la vigésimo cuarta manera de implementación posible, y la vigésimo quinta manera de implementación posible del primer aspecto, en una vigésimo séptima manera de implementación posible del primer aspecto, el procesador se configura además para enviar datos de actualización o una instrucción de borrado a la al menos una unidad de procesamiento central; la al menos una unidad de procesamiento central se configura además para llevar a cabo un segundo procesamiento de operación de troceo en los datos de actualización o la instrucción de borrado en un entorno de ejecución fiable mediante el uso de una clave, para obtener un resultado de procesamiento, y enviar el resultado de procesamiento a la memoria, donde el entorno de ejecución fiable se encuentra aislado, de manera segura, del software del sistema operativo general; y la memoria se configura además para llevar a cabo la segunda verificación de troceo en el resultado de procesamiento, obtener los datos de actualización o la instrucción de borrado después de que la segunda verificación de troceo tiene éxito, y actualizar el software de pago móvil mediante el uso de los datos de actualización o datos de borrado que corresponden a la instrucción de borrado de la memoria según la instrucción de borrado. La presente solución mejora la seguridad de borrado de datos en el pago móvil, y la unidad de procesamiento central implementa el procesamiento de seguridad, lo cual simplifica el diseño del procesador.

Según un segundo aspecto, una realización de la presente invención provee un método para implementar el pago móvil mediante el uso de un aparato de pago móvil, que incluye: ejecutar software del sistema operativo general y controlar al menos uno de una unidad de comunicación o un elemento seguro bajo la acción del software del sistema operativo general, mediante el uso de al menos una unidad de procesamiento central; cargar software de pago móvil de una memoria al elemento seguro; ejecutar el software de pago móvil en el elemento seguro; e intercambiar, por el elemento seguro, información de pago con la unidad de comunicación bajo la acción del software de pago móvil, donde la unidad de comunicación intercambia la información de pago con un extremo par de comunicación mediante el uso de un enlace radioeléctrico, donde el elemento seguro y la al menos una unidad de procesamiento central se ubican en un primer chip semiconductor en el aparato de pago móvil. El elemento seguro y la al menos una unidad de procesamiento central se integran mediante el uso del mismo chip semiconductor; por lo tanto, los costes y un área para la implementación de hardware de pago móvil se reducen.

Según un tercer aspecto, una realización de la presente invención provee un chip semiconductor, usado en un aparato de pago móvil, donde el chip semiconductor incluye un elemento seguro y al menos una unidad de procesamiento central, donde el elemento seguro incluye un primer módulo de almacenamiento y un procesador, el primer módulo de almacenamiento configurado para proveer espacio de memoria para ejecutar el software de pago móvil para el procesador, y la al menos una unidad de procesamiento central configurada para ejecutar el software del sistema operativo general; el procesador se configura para cargar el software de pago móvil de una memoria en el aparato de pago móvil al primer módulo de almacenamiento, ejecutar el software de pago móvil, e intercambiar información de pago con una unidad de comunicación en el aparato de pago móvil bajo la acción del software de pago móvil; y la al menos una unidad de procesamiento central se configura además para controlar al menos uno de

la unidad de comunicación, la memoria o el elemento seguro bajo la acción del software del sistema operativo general.

Con referencia al tercer aspecto, en una primera manera de implementación posible del tercer aspecto, el software de pago móvil incluye software del sistema operativo de pago móvil.

Con referencia a la primera manera de implementación posible del tercer aspecto, en una segunda manera de implementación posible del tercer aspecto, el software de pago móvil además incluye al menos un tipo de software de aplicación de pago móvil.

Con referencia a la primera o a la segunda maneras de implementación posibles del tercer aspecto, en una tercera manera de implementación posible del tercer aspecto, el elemento seguro además incluye: un segundo módulo de almacenamiento, configurado para almacenar un programa de arranque para iniciar el procesador; y cuando el elemento seguro se enciende, el procesador se configura para leer el programa de arranque del segundo módulo de almacenamiento, cargar el software del sistema operativo de pago móvil de la memoria al primer módulo de almacenamiento bajo la acción del programa de arranque, y ejecutar el software del sistema operativo de pago móvil.

Con referencia a la segunda manera de implementación posible del tercer aspecto, en una cuarta manera de implementación posible del tercer aspecto, el procesador se configura para cargar uno o más tipos de software de aplicación de pago móvil del al menos un tipo de software de aplicación de pago móvil de la memoria al primer módulo de almacenamiento después de activarse por la información de pago intercambiada entre el procesador y la unidad de comunicación, y ejecutar el único o más tipos de software de aplicación de pago móvil.

Con referencia al tercer aspecto o a cualquiera de la primera a la cuarta maneras de implementación posibles del tercer aspecto, en una quinta manera de implementación posible del tercer aspecto, la información de pago incluye: una instrucción de pago móvil que se transmite del extremo par de comunicación al procesador mediante la unidad de comunicación, y datos de pago móvil transmitidos del procesador al extremo par de comunicación mediante la unidad de comunicación en respuesta a la instrucción de pago móvil.

Con referencia a la quinta manera de implementación posible del tercer aspecto, en una sexta manera de implementación posible del tercer aspecto, los datos de pago móvil incluyen datos que resultan del procesamiento de seguridad, y el procesamiento de seguridad incluye al menos una de las siguientes: encriptación de datos o protección de integridad de datos.

Con referencia a la sexta manera de implementación posible del tercer aspecto, en una séptima manera de implementación posible del tercer aspecto, el procesador se configura además para generar los datos que resultan del procesamiento de seguridad.

Con referencia a la sexta manera de implementación posible del tercer aspecto, en una octava manera de implementación posible del tercer aspecto, el procesador se configura además para generar datos originales; el elemento seguro además incluye: un módulo de procesamiento de seguridad, configurado para llevar a cabo el procesamiento de seguridad en los datos originales para generar los datos que resultan del procesamiento de seguridad.

Con referencia al tercer aspecto o a cualquiera de la primera a la octava maneras de implementación posibles del tercer aspecto, en una novena manera de implementación posible del tercer aspecto, el control llevado a cabo por la al menos una unidad de procesamiento central en el al menos uno de la unidad de comunicación, la memoria, o el elemento seguro incluye: control de encendido, apagado, entrada en o salida de un estado de potencia baja, o un estado de funcionamiento.

Con referencia al tercer aspecto o a cualquiera de la primera a la décima maneras de implementación posibles del tercer aspecto, en una undécima manera de implementación posible del tercer aspecto, el elemento seguro además incluye: un motor cifrado, configurado para llevar a cabo la verificación de seguridad en el software de pago móvil después de que el procesador carga el software de pago móvil de la memoria al primer módulo de almacenamiento, y ordenar al procesador que ejecute el software de pago móvil después de que la verificación de seguridad tiene éxito, donde la verificación de seguridad incluye al menos una de la desencriptación de seguridad o verificación de troceo.

Con referencia a la undécima manera de implementación posible del tercer aspecto, en una duodécima manera de implementación posible del tercer aspecto, el motor cifrado se configura además para llevar a cabo al menos un tipo de procesamiento en la encriptación de seguridad o primer procesamiento de operación de troceo en datos de actualización, para obtener datos de actualización procesados; y el procesador se configura además para escribir los datos de actualización procesados en la memoria, para actualizar el software de pago móvil.

Con referencia al tercer aspecto o a cualquiera de la primera a la décima maneras de implementación posibles del tercer aspecto, en una decimotercera manera de implementación posible del tercer aspecto, el procesador se configura además para llevar a cabo la verificación de seguridad en el software de pago móvil después de que el

procesador carga el software de pago móvil de la memoria al primer módulo de almacenamiento, y ejecutar el software de pago móvil después de que la verificación de seguridad tiene éxito, donde la verificación de seguridad incluye al menos una de la desencriptación de seguridad o primera verificación de troceo.

Con referencia a la decimotercera manera de implementación posible del tercer aspecto, en una decimocuarta manera de implementación posible del tercer aspecto, el procesador se configura además para llevar a cabo al menos un tipo de procesamiento en la encriptación de seguridad o primer procesamiento de operación de troceo en datos de actualización, para obtener datos de actualización procesados, y escribir los datos de actualización procesados en la memoria, para actualizar el software de pago móvil.

Con referencia a la duodécima o decimocuarta maneras de implementación posibles del tercer aspecto, en una decimoquinta manera de implementación posible del tercer aspecto, el procesador se configura además para llevar a cabo el segundo procesamiento de operación de troceo en los datos de actualización procesados mediante el uso de una clave para obtener datos que se almacenarán cuando el procesador escriba los datos de actualización procesados en la memoria; y la memoria se configura además para llevar a cabo la segunda verificación de troceo en los datos que se almacenarán, obtener los datos de actualización procesados después de que la segunda verificación de troceo tiene éxito, y actualizar el software de pago móvil mediante el uso de los datos de actualización procesados.

Con referencia a la duodécima o decimocuarta maneras de implementación posibles del tercer aspecto, en una decimosexta manera de implementación posible del tercer aspecto, el procesador se configura además para enviar los datos de actualización procesados a la al menos una unidad de procesamiento central cuando el procesador escribe los datos de actualización procesados en la memoria; la al menos una unidad de procesamiento central se configura además para llevar a cabo el segundo procesamiento de operación de troceo en los datos de actualización procesados en un entorno de ejecución fiable mediante el uso de una clave, para obtener datos que se almacenarán, y enviar los datos que se almacenarán a la memoria, donde el entorno de ejecución fiable se encuentra aislado, de manera segura, del software del sistema operativo general; y la memoria se configura además para llevar a cabo la segunda verificación de troceo en los datos que se almacenarán, obtener los datos de actualización procesados después de que la segunda verificación de troceo tiene éxito, y actualizar el software de pago móvil mediante el uso de los datos de actualización procesados.

Con referencia a la decimosexta manera de implementación posible del tercer aspecto, en una decimoséptima manera de implementación posible del tercer aspecto, el elemento seguro además incluye un tercer módulo de almacenamiento; el procesador se configura además para escribir los datos de actualización procesados en el tercer módulo de almacenamiento, y enviar una primera solicitud de interrupción a la al menos una unidad de procesamiento central; la al menos una unidad de procesamiento central se configura además para leer los datos de actualización procesados del tercer módulo de almacenamiento en el entorno de ejecución fiable en respuesta a la primera solicitud de interrupción.

Con referencia al tercer aspecto o a cualquiera de la primera a la decimoséptima maneras de implementación posibles del tercer aspecto, en una decimoctava manera de implementación posible del tercer aspecto, la al menos una unidad de procesamiento central se configura además para ejecutar el software de aplicación común a excepción del software de pago móvil.

Con referencia al tercer aspecto o a cualquiera de la primera a la decimoctava maneras de implementación posibles del tercer aspecto, en una decimonovena manera de implementación posible del tercer aspecto, el software del sistema operativo general ejecutado por la al menos una unidad de procesamiento central se encuentra aislado, de manera segura, del elemento seguro.

Con referencia al tercer aspecto, o a cualquiera de la primera a la undécima maneras de implementación posibles, la decimotercera manera de implementación posible, la decimoctava manera de implementación posible, y la decimonovena manera de implementación posible del tercer aspecto, en una vigésima manera de implementación posible del tercer aspecto, el procesador se configura además para llevar a cabo el segundo procesamiento de operación de troceo en datos de actualización o una instrucción de borrado mediante el uso de una clave, para obtener un resultado de procesamiento; y la memoria se configura además para llevar a cabo la segunda verificación de troceo en el resultado de procesamiento, obtener los datos de actualización o la instrucción de borrado después de que la segunda verificación de troceo tiene éxito, y actualizar el software de pago móvil mediante el uso de los datos de actualización o datos de borrado que corresponden a la instrucción de borrado de la memoria según la instrucción de borrado.

Con referencia al tercer aspecto o a cualquiera de la primera a la undécima maneras de implementación posibles, la decimotercera manera de implementación posible, la decimoctava manera de implementación posible, y la decimonovena manera de implementación posible del tercer aspecto, en una vigésimo primera manera de implementación posible del tercer aspecto, el procesador se configura además para enviar datos de actualización o una instrucción de borrado a la al menos una unidad de procesamiento central; la al menos una unidad de procesamiento central se configura además para llevar a cabo un segundo procesamiento de operación de troceo en los datos de actualización o la instrucción de borrado en un entorno de ejecución fiable mediante el uso de una

clave, para obtener un resultado de procesamiento, y enviar el resultado de procesamiento a la memoria, donde el entorno de ejecución fiable se encuentra aislado, de manera segura, del software del sistema operativo general; y la memoria se configura además para llevar a cabo la segunda verificación de troceo en el resultado de procesamiento, obtener los datos de actualización o la instrucción de borrado después de que la segunda verificación de troceo tiene éxito, y actualizar el software de pago móvil mediante el uso de los datos de actualización o datos de borrado que corresponden a la instrucción de borrado de la memoria según la instrucción de borrado.

En las soluciones técnicas provistas en las realizaciones de la presente invención, cuando la seguridad del pago móvil se garantiza, los costes y un área para la implementación de hardware pueden reducirse, un requisito de miniaturización de un terminal móvil en el pago móvil se satisface de mejor manera, y el pago móvil se populariza y expande de manera conveniente.

Breve descripción de los dibujos

Con el fin de describir las soluciones técnicas en las realizaciones de la presente invención o en la técnica anterior de forma más clara, a continuación se describen brevemente los dibujos anexos para describir las realizaciones o la técnica anterior. De manera aparente, los dibujos anexos en la siguiente descripción muestran simplemente algunas realizaciones de la presente invención o la técnica anterior, y una persona con experiencia ordinaria en la técnica puede incluso derivar otros dibujos a partir de dichos dibujos anexos sin esfuerzos creativos.

La Figura 1 es un diagrama esquemático simplificado de una estructura de un terminal móvil usado en el pago móvil según la técnica anterior;

la Figura 2 es un diagrama esquemático simplificado de una estructura de un aparato de pago móvil según una realización de la presente invención;

la Figura 3 es un diagrama esquemático simplificado de un procedimiento de pago móvil según una realización de la presente invención;

la Figura 4 es un diagrama esquemático simplificado para llevar a cabo una operación de acceso seguro en una región de almacenamiento seguro de una memoria por el software de pago móvil según una realización de la presente invención;

la Figura 5 es otro diagrama esquemático simplificado para llevar a cabo una operación de acceso seguro en una región de almacenamiento seguro de una memoria por el software de pago móvil según una realización de la presente invención;

la Figura 6 es un diagrama esquemático simplificado de una estructura de un sistema usado para el pago móvil en un aparato de pago móvil según una realización de la presente invención;

la Figura 7 es un diagrama estructural esquemático simplificado de una memoria usada para el pago móvil según una realización de la presente invención; y

la Figura 8 es un diagrama esquemático simplificado de una arquitectura de un sistema de software usado para el pago móvil según una realización de la presente invención.

Descripción de las realizaciones

A continuación, se describen de forma clara y completa las soluciones técnicas en las realizaciones de la presente invención con referencia a los dibujos anexos en las realizaciones de la presente invención. De manera aparente, las realizaciones descritas son, simplemente, una parte de, pero no todas, las realizaciones de la presente invención. Todas las demás realizaciones obtenidas por una persona con experiencia ordinaria en la técnica según las realizaciones de la presente invención sin esfuerzos creativos caerán dentro del alcance de protección de la presente invención.

La Figura 2 es un diagrama esquemático de un aparato de pago móvil 20 según una realización de la presente invención. El aparato de pago móvil 20 puede ubicarse en un terminal móvil 21. El terminal móvil 21 puede ser un equipo de usuario (EU), por ejemplo, varios tipos de dispositivos terminales portátiles como, por ejemplo, un teléfono móvil y una tableta. El aparato de pago móvil 20 puede ser, específicamente, un chip, un conjunto de chips, o una placa de circuito que lleva un chip o un conjunto de chips. El chip, el conjunto de chips, o la placa de circuito que lleva un chip o un conjunto de chips pueden funcionar cuando se accionan por el software necesario. El aparato de pago móvil 20 puede incluir: una unidad de comunicación de campo cercano 201, donde la unidad de comunicación de campo cercano 201 intercambia, mediante la ejecución de un protocolo de comunicación radioeléctrica de corta distancia, información de pago con un terminal de pago, por ejemplo, una máquina POS, que se ubica fuera del terminal móvil 21 y que se configura para conectarse a Internet para implementar una función de pago móvil, para implementar el pago fuera de línea; y una unidad de comunicación móvil 202, donde la unidad de comunicación móvil 202 intercambia información de pago con una red de acceso radioeléctrico, de manera específica, por ejemplo, una estación base en la red de acceso radioeléctrico, mediante la ejecución de un protocolo de comunicación

radioeléctrica celular, para conectarse a Internet a través de la red de acceso radioeléctrico que incluye la estación base, de modo que la unidad de comunicación móvil 202 finalmente intercambia información de pago con un servidor, que tiene una función de pago, en Internet, para implementar el pago en línea. Puede comprenderse que el aparato de pago móvil 20 puede incluir una unidad de comunicación de campo cercano 201 o la unidad de comunicación móvil 202, es decir, puede implementarse el pago fuera de línea o el pago en línea. Una tecnología de identificación por radiofrecuencia (RFID, por sus siglas en inglés) puede usarse en el protocolo de comunicación radioeléctrica de corta distancia ejecutado por la unidad de comunicación de campo cercano 201, puede soportar, de manera específica, varios tipos de protocolos RFID como, por ejemplo, un protocolo estándar de Asociación Europea de Fabricantes de Ordenadores (ECMA, por sus siglas en inglés). Además, la tecnología de identificación por radiofrecuencia puede también soportar otros tipos de protocolos de comunicación de corta distancia como, por ejemplo, un protocolo de comunicación Bluetooth, un protocolo de comunicaciones de infrarrojo y un protocolo de Fidelidad Inalámbrica (WiFi, por sus siglas en inglés). El protocolo de comunicación radioeléctrica celular ejecutado por la unidad de comunicación móvil 202 puede ser uno o más de los protocolos de comunicación radioeléctrica celular como, por ejemplo, GSM, UMTS, WiMAX o LTE, de modo que la comunicación con una red de acceso radioeléctrico en una red de comunicación móvil celular se implementa mediante el uso de la unidad de comunicación móvil 202. Puede comprenderse que la estación base en la red de acceso radioeléctrico es un elemento de red, que implementa la función de comunicación, en la red de acceso radioeléctrico, y la estación base puede tener múltiples formas como, por ejemplo, un NodoB o un eNodoB. La red de acceso radioeléctrico que incluye la estación base se conecta finalmente a un servidor en la red, es decir, un servidor en un lado de nube, de modo que el servidor intercambia información de pago con el aparato de pago móvil 20. La unidad de comunicación de campo cercano 201 o la unidad de comunicación móvil 202 pueden incluir una unidad de banda base que ejecuta un protocolo de comunicación. De manera opcional, la unidad de comunicación de campo cercano 201 o la unidad de comunicación móvil 202 pueden además incluir una unidad de frecuencia radioeléctrica. De manera similar a la técnica anterior, la unidad de frecuencia radioeléctrica puede configurarse para recibir una señal de radiofrecuencia y convertir la señal de radiofrecuencia en una señal de banda base para el procesamiento por la unidad de banda base. La información de pago se incluye en la señal de radiofrecuencia y, por lo tanto, se adquiere por la unidad de comunicación de campo cercano 201 o la unidad de comunicación móvil 202.

El aparato de pago móvil 20 en la Figura 2 además incluye una memoria 203 que puede configurarse para almacenar el software de pago móvil, un elemento seguro 204 y al menos una unidad de procesamiento central 205. La al menos una unidad de procesamiento central 205 se configura para ejecutar software del sistema operativo general como, por ejemplo, un sistema operativo general como un sistema operativo Android, un sistema operativo Windows o un sistema operativo iOS. Dichos sistemas operativos pueden usarse para soportar software de aplicación normal de pago no móvil. Una mayor cantidad de unidades de procesamiento central 205 indica una capacidad más fuerte para procesar datos. El software del sistema operativo general es una plataforma de software general en la cual el software de aplicación se ejecuta. La unidad de procesamiento central 205 puede implementarse según una arquitectura ARM, una arquitectura Intel X86, o una arquitectura de millones de instrucciones por segundo (MIPS, por sus siglas en inglés), lo cual no se encuentra limitado en la presente realización. La al menos una unidad de procesamiento central 205 controla la unidad de comunicación de campo cercano 201, la unidad de comunicación móvil 202, la memoria 203 y el elemento seguro 204 bajo la acción del software del sistema operativo general. Un proceso de control específico puede incluir: controlar el encendido, apagado, entrada en o salida de un estado de potencia baja. Por lo tanto, la unidad de procesamiento central 205 que ejecuta un sistema operativo general puede implementar el control uniforme en otras partes en el aparato de pago móvil 20, de modo que dichas partes se encienden o apagan normalmente, o entran en o salen de un estado de potencia baja, por ejemplo, entran en o salen de un estado de inactividad. El consumo de energía de cualquier componente, en un estado de potencia baja, en la unidad de comunicación, la memoria, o el elemento seguro es más bajo que el consumo de energía cuando el componente funciona. Además, el proceso de control de cualquier componente puede además incluir otra operación de control, por ejemplo, controlar un estado de funcionamiento. El control de un estado de funcionamiento puede ser ajustar una tensión de funcionamiento, un ritmo de reloj, una velocidad de procesamiento, o similares cuando el componente funciona, lo cual no se encuentra limitado en la presente realización. Para un proceso de control específico, puede hacerse referencia a una operación de control por una unidad de procesamiento central general en otro componente en la técnica anterior.

Con referencia a una estructura de sistema en la Figura 6, la estructura de sistema además describe algunos componentes en detalle según la Figura 2. El elemento seguro 204 puede incluir un primer módulo de almacenamiento 2041 y un procesador 2042. Para el contenido específico incluido en la memoria 203 en la Figura 6, puede hacerse referencia a la Figura 7, y software de pago móvil 2030 puede almacenarse en la memoria 203. Con referencia a la Figura 6 y Figura 7, el procesador 2042 se configura para cargar el software de pago móvil 2030 de la memoria 203 al primer módulo de almacenamiento 2041, ejecutar el software de pago móvil 2030 e intercambiar la información de pago con al menos una de la unidad de comunicación de campo cercano 201 o la unidad de comunicación móvil 202 bajo la acción del software de pago móvil 2030. El primer módulo de almacenamiento 2041 provee espacio de memoria para ejecutar el software de pago móvil 2030 para el procesador 2042. El primer módulo de almacenamiento 2041 puede ser una memoria de acceso aleatorio (RAM, por sus siglas en inglés). La memoria 203 puede ser una memoria de solo lectura (ROM, por sus siglas en inglés). De manera específica, como se muestra en la Figura 7, el software de pago móvil 2030 almacenado en la memoria 203 puede incluir software del sistema operativo de pago móvil 2031, donde el software del sistema operativo de pago móvil 2031 es diferente del

software del sistema operativo común, y solo es una plataforma del sistema operativo usada para ejecutar el software de aplicación de pago móvil 2032. Por lo tanto, el pago móvil es más fiable.

En una manera de implementación opcional, el software del sistema operativo de pago móvil 2031 puede ser un sistema operativo de chip (COS, por sus siglas en inglés). También se hace referencia al COS como un espejo COS, y puede ser equivalente al software del sistema operativo en una tarjeta inteligente residente o una tarjeta financiera de circuito integrado (CI). En el presente caso, el elemento seguro 204 tiene, de manera equivalente, una función de la tarjeta inteligente residente o la tarjeta financiera, y se configura para proveer una máquina POS externa, un lector de tarjeta, o un servidor financiero en un lado de nube con datos requeridos por un servicio de pago móvil como, por ejemplo, lectura de tarjeta, donde los datos son, por ejemplo, datos relacionados con un servicio financiero bancario o datos de una cuenta personal de un usuario como, por ejemplo, un número de cuenta personal, una contraseña e información de verificación para verificar una cuenta personal por un servidor bancario. Además, el espejo COS también es una plataforma de operación que recibe y procesa información de pago externa, por ejemplo, información de pago enviada por un servidor financiero, un lector de tarjeta, o una máquina POS al elemento seguro 204. El espejo COS puede configurarse para ejecutar varias instrucciones que provienen del exterior, donde las instrucciones son, por ejemplo, una operación como una operación de autenticación, gestionar espacio del primer módulo de almacenamiento 2041 en el elemento seguro 204, devolver información de respuesta al exterior, y similares. El elemento seguro 204, en general, usa un COS que se basa en el lenguaje de programación de ordenadores JAVA como un sistema de seguridad. No solo el COS puede preestablecerse en el elemento seguro 204, sino que también el aparato de pago móvil 20 puede además descargar, de forma dinámica, e instalar software de aplicación de pago móvil 2032 como, por ejemplo, software de aplicación financiera según el COS. Un diseño específico del COS es contenido que pertenece a la técnica anterior, y no se encuentra en el alcance de descripción de la presente solicitud.

En la Figura 7, además del software del sistema operativo de pago móvil 2031, el software de pago móvil 2030 además incluye múltiples tipos de software de aplicación de pago móvil 2032. Un tipo de software de aplicación de pago móvil 2032 se usa para una categoría de funciones de pago móvil. Por ejemplo, cada tipo de software de aplicación de pago móvil 2032 puede ser software de aplicación relacionado con un banco, y se usa para implementar una función de software relacionada con el banco, donde la función de software incluye, por ejemplo, una cuenta, una contraseña, e información relacionada con la autenticación y verificación que se relacionan con el banco, y una función relacionada con un servicio especial del banco. Ciertamente, una aplicación de pago móvil no se encuentra limitada a solamente un servicio bancario, y también incluye, pero sin limitación a ello, un servicio de tarjeta de débito, un servicio de tarjeta de crédito, u otro tipo de pago móvil, por ejemplo, un servicio de pago de una tarjeta de la seguridad social, una tarjeta de transporte, o una tarjeta CI interna de una unidad, lo cual no se encuentra limitado en la presente realización.

En la Figura 2 o Figura 6, el elemento seguro 204 y la al menos una unidad de procesamiento central 205 se ubican en un primer chip semiconductor IC1 en el aparato de pago móvil 20 y también se hace referencia al IC1 como un chip central del aparato de pago móvil 20. El elemento seguro 204 y la al menos una unidad de procesamiento central 205 se integran mediante el uso del mismo chip central semiconductor IC1, lo cual reduce los costes y un área para la implementación de hardware de pago móvil. A diferencia de la técnica anterior en la cual una unidad de función de hardware relacionada con el pago seguro y el chip central se transforma, respectivamente, en dos chips independientes, el chip central IC1 que tiene una capacidad de integración más alta puede disponerse en una placa principal del aparato de pago móvil 20 de manera más simple. De manera opcional, como se muestra en la Figura 2 o Figura 6, la unidad de comunicación de campo cercano 201 puede ubicarse en un cuarto chip semiconductor IC4 en el aparato de pago móvil 20. Puede comprenderse que, además de implementar la unidad de comunicación de campo cercano 201 mediante el uso del cuarto chip semiconductor IC4 que se muestra en la Figura 2 o Figura 6, la unidad de comunicación de campo cercano 201 también puede ubicarse en el primer chip semiconductor IC1 (no se muestra en la figura), para además implementar la integración del chip central IC1 y reducir los costes de implementación. De manera similar, como se muestra en la Figura 6, la unidad de comunicación móvil 202 puede ubicarse en el primer chip semiconductor IC1 o, como se muestra en la Figura 2, la unidad de comunicación móvil 202 se ubica, de manera independiente, en un quinto chip semiconductor IC5 en el aparato de pago móvil 20. Si la unidad de comunicación de campo cercano 201 o la unidad de comunicación móvil 202 se integran al chip central IC1 depende de un diseño específico por una persona con experiencia en la técnica.

En las varias realizaciones de la presente invención, también se hace referencia brevemente a un chip semiconductor como un chip, y puede ser un conjunto de circuitos integrados que se realizan en un sustrato de circuito integrado (que, en general, es un material semiconductor como, por ejemplo, silicio) mediante el uso de una tecnología de circuito integrado. Una capa externa del chip semiconductor se empaqueta, en general, mediante el uso de un material de empaquetado semiconductor. El circuito integrado puede incluir un transistor de metal-óxido-semiconductor (MOS, por sus siglas en inglés), un transistor bipolar, un diodo, o similares. El chip semiconductor puede, de manera independiente, funcionar o puede funcionar bajo la acción del software de controlador necesario, para implementar funciones como, por ejemplo, comunicación, cálculo o almacenamiento.

Para la distribución de partes en el aparato de pago móvil 20 en diferentes chips, aún es preciso remitirse a la Figura 2. Además de que la unidad de comunicación de campo cercano 201 y la unidad de comunicación móvil 202 se disponen en otro chip diferente del chip central IC1, la memoria 203 puede ubicarse, de manera específica, en un

segundo chip semiconductor IC2 en el aparato de pago móvil 20. De manera alternativa, la memoria 203 puede integrarse al chip central IC1 (no se muestra en la figura) junto con la unidad de comunicación de campo cercano 201 o la unidad de comunicación móvil 202. En el presente caso, la memoria 203 y el elemento seguro 204 pueden considerarse un sistema que implementa el pago seguro. Sin embargo, en general, de manera similar a la solución en la Figura 2 o Figura 6, el segundo chip semiconductor IC2 independiente del chip central IC1 se usa con mayor frecuencia en la técnica para implementar la memoria 203, dado que la memoria 203, en general, existe en forma de memoria flash si la memoria 203 se integra al chip central IC1, pero una memoria flash tiene, en general, espacio de memoria muy limitado, y si un espacio de memoria grande necesita implementarse, ello resultará en un gran aumento de coste e implementación compleja. Si la memoria flash 203 se implementa mediante el uso del segundo chip semiconductor IC2 independiente, el coste de implementación se reducirá en cierta medida con un diseño más simple, y un requisito de una gran capacidad de almacenamiento puede satisfacerse de mejor manera. De manera especial, por motivos como, por ejemplo, la técnica y el área de procesamiento, es difícil integrar una memoria actual al chip central IC1. Por lo tanto, solo el elemento seguro 204 se integra a la al menos una unidad de procesamiento central 205, y se usa una memoria 203 independiente del chip central, que es más apropiada para una solución de pago móvil existente.

Cuando se usa una memoria similar a la memoria 203 fuera de chip en la Figura 2 o Figura 6, la memoria 203 puede además usarse tanto para el software de pago móvil 2030 como para otro software. En la presente manera de implementación, la memoria 203 incluye una región de almacenamiento seguro 203A y una región de almacenamiento común 203B que se encuentran aisladas entre sí. Para detalles, es preciso remitirse a la Figura 7. La región de almacenamiento seguro 203A se usa para almacenar el software de pago móvil 2030 y la región de almacenamiento común 203B se usa para almacenar el software del sistema operativo general que se menciona más arriba. La al menos una unidad de procesamiento central 205 se configura, de manera específica, para leer el software del sistema operativo general de la región de almacenamiento común 203B en la memoria 203 y ejecutar el software del sistema operativo general, y el procesador 2042 se configura, de manera específica, para cargar el software de pago móvil 2030 de la región de almacenamiento seguro 203A al primer módulo de almacenamiento 2041. El aislamiento indica que el software del sistema operativo general y el software de pago móvil 2030 no se mezclan, pero coexisten en la misma memoria 203, y se accede a ellos por sus respectivas entidades de ejecución, lo cual ahorra recursos de memoria bajo la premisa de garantizar la seguridad. En el presente caso, la memoria 203 puede ser una tarjeta multimedia integrada (eMMC, por sus siglas en inglés), y la región de almacenamiento seguro 203A puede ser un bloque de memoria protegido contra la reproducción (RPMB, por sus siglas en inglés) de la memoria eMMC 203. De hecho, la memoria 203 también puede ser otro dispositivo de almacenamiento, lo cual no se encuentra limitado en la presente realización.

En otra manera de implementación opcional, la memoria 203 puede dedicarse al almacenamiento del software de pago móvil 2030. Es decir, en el presente caso, la memoria 203 no almacena otro software que no esté relacionado con el pago móvil, incluido el software del sistema operativo general. En el presente caso, el aparato de pago móvil 20 además incluye una unidad de almacenamiento común 206. Como se muestra en la Figura 2, la unidad de almacenamiento común 206 se ubica en un tercer chip semiconductor IC3 en el aparato de pago móvil 20 y la unidad de almacenamiento común 206 se configura para almacenar el software del sistema operativo general. La al menos una unidad de procesamiento central 205 se configura, de manera específica, para leer el software del sistema operativo general de la unidad de almacenamiento común 206 y ejecutar el software del sistema operativo general. En el presente caso, la memoria dedicada 203 se encuentra físicamente aislada de la unidad de almacenamiento común 206, de modo que la seguridad operativa se mejora aún más. La unidad de almacenamiento común 206 puede ser la eMMC descrita más arriba. La memoria dedicada 203 puede ser una memoria Flash independiente del chip central IC1. Sin embargo, los tipos de almacenamiento específicos de la unidad de almacenamiento común 206 y la memoria dedicada 203 no se encuentran limitados en la presente realización.

De manera específica, con referencia a la Figura 6, en una manera de implementación opcional, el elemento seguro 204 además incluye un segundo módulo de almacenamiento 2043, configurado para almacenar un programa de arranque para iniciar el procesador 2042, por ejemplo, código de arranque para el arranque; y cuando el elemento seguro 204 se enciende, el procesador se configura para leer el programa de arranque del segundo módulo de almacenamiento 2043, cargar el software del sistema operativo de pago móvil 2031, por ejemplo, un espejo COS, de la memoria 203 al primer módulo de almacenamiento 2041 bajo la acción del programa de arranque, y ejecutar el software del sistema operativo de pago móvil 2031. Dado que un programa de arranque para iniciar el elemento seguro 204 se ubica en el segundo módulo de almacenamiento 2043 en el elemento seguro 204, el segundo módulo de almacenamiento 2043 se dedica al arranque del elemento seguro 204, y no se accede libremente a aquel por cualquier programa de ejecución de software o cualquier hardware a excepción del elemento seguro 204, lo cual garantiza la seguridad.

En una manera de implementación opcional, cuando el procesador 2042 intercambia la información de pago con la unidad de comunicación de campo cercano 201 o la unidad de comunicación móvil 202, el procesador 2042 puede activarse por la información de pago para cargar uno o más tipos de software de aplicación de pago móvil 2032 del al menos un tipo de software de aplicación de pago móvil 2032 de la memoria 203 al primer módulo de almacenamiento 2041, y ejecutar el único o más tipos de software de aplicación de pago móvil 2032. Dado que la carga y ejecución del software de aplicación de pago móvil 2032 se activan por la información de pago

intercambiada, cuando no hay servicio de pago, el software de aplicación de pago móvil 2032 relacionado puede no iniciarse, lo cual puede ahorrar espacio de memoria del primer módulo de almacenamiento 2041. Es decir, el software de aplicación de pago móvil 2032 se carga en una manera de carga dinámica, es decir, solo el software de aplicación seleccionado se carga de la memoria externa 203 al primer módulo de almacenamiento 2041 correspondiente, es decir, una RAM. Otro tipo de software de aplicación que no necesita usarse no se carga a la RAM y, de esta manera, se garantiza que el espacio ocupado en la RAM se usa para alojar solamente el espejo COS y archivos de programa de uno a dos tipos de software de aplicación, lo cual hace que la RAM no esté sobreocupada.

La solución en la cual el procesador 2042 intercambia la información de pago con el extremo par de comunicación (como, por ejemplo, un terminal de pago o una red de acceso radioeléctrico) mediante el uso de la unidad de comunicación (como, por ejemplo, la unidad de comunicación de campo cercano 201 o la unidad de comunicación móvil 202) es contenido que pertenece a un protocolo de pago móvil. Ya existen múltiples soluciones para esto en la técnica anterior, y un procedimiento de la solución puede ser similar a un proceso de lectura de tarjeta de crédito. Cada proveedor de servicios diferente como, por ejemplo, un banco o una autoridad de transporte público, puede tener su propio protocolo de comunicación de intercambio de pago móvil, que se usa para implementar un intercambio de pago, por ejemplo, transferencia de información confidencial personal y envío de datos de seguridad, entre el procesador 2042 en el elemento seguro 204 y el extremo par de comunicación mediante la unidad de comunicación.

En aras de la descripción, la presente realización provee un diagrama de flujo de pago móvil que se muestra en la Figura 3. En un procedimiento relacionado, la información que se relaciona con el pago móvil y que se transfiere entre el aparato de pago móvil 20 y un terminal de pago mediante el uso de un enlace radioeléctrico (incluido un enlace de comunicación radioeléctrica celular o un enlace de comunicación radioeléctrica de corta distancia) puede considerarse como la información de pago. Etapas simplificadas del procedimiento de pago pueden incluir: E31: La unidad de procesamiento central 205 ejecuta el software del sistema operativo general, y controla la unidad de comunicación y el elemento seguro 204 bajo la acción del software del sistema operativo general, donde el control puede ser controlar el encendido, apagado, entrada en o salida de un estado de potencia baja. E32: El elemento seguro 204 carga el software de pago móvil 2030 de la memoria 203 y ejecuta el software de pago móvil 2030. E33: La unidad de comunicación recibe una instrucción de pago móvil del extremo par de comunicación mediante un enlace de comunicación radioeléctrica, donde la instrucción puede ser un mensaje de solicitud para solicitar al aparato de pago móvil 20 que lleve a cabo el pago móvil, y el mensaje puede incluirse en la señalización de interfaz aérea. Para la implementación específica y una estructura de señalización de la señalización de interfaz aérea, puede hacerse referencia al contenido de un protocolo de comunicación radioeléctrica existente. Además de usarse para iniciar un servicio de pago, la instrucción de pago móvil puede además incluir una solicitud de verificación y autenticación necesaria. Para el contenido específico de la instrucción de pago móvil, puede hacerse referencia a la técnica anterior en el campo del pago móvil, y el contenido específico de la instrucción de pago móvil no se describe en la presente solicitud. E34: La unidad de comunicación analiza la señalización de interfaz aérea mediante la ejecución de software de protocolo de comunicación radioeléctrica para obtener la instrucción de pago móvil, y transmite la instrucción de pago móvil al procesador 2042 en el elemento seguro 204. E35: Cuando se acciona por el software de pago móvil 2030, el procesador 2042 envía datos de pago móvil a la unidad de comunicación en respuesta a la instrucción de pago móvil. De manera específica, los datos de pago móvil pueden incluir datos para proveer una identidad de un usuario, y los datos son, por ejemplo, un número de tarjeta bancaria, un número de cuenta, información confidencial personal, o textos cifrados que se necesitan en varias transacciones bancarias, y son similares a la información de tarjeta de crédito para el pago de tarjeta de crédito y se usan para la lectura por el extremo par de comunicación. E36: La unidad de comunicación ejecuta el protocolo de comunicación radioeléctrica para encapsular los datos de pago móvil en la señalización de interfaz aérea, y transmite la señalización de interfaz aérea al extremo par de comunicación. E37: El extremo par de comunicación transmite los datos de pago móvil a un servidor, y el servidor procesa los datos de pago móvil para completar un servicio de pago.

De manera opcional, cuando se lleva a cabo el pago fuera de línea, el extremo par de comunicación es un terminal de pago, por ejemplo, una máquina POS, y el terminal de pago transmite los datos de pago móvil a un servidor en un lado de nube a través de Internet. De manera alternativa, cuando se lleva a cabo el pago en línea, la unidad de comunicación móvil 202 se usa como una unidad de comunicación para transferir los datos de pago móvil al servidor a través de la red de acceso radioeléctrico. Para una operación específica del servidor, puede hacerse referencia a una solución de pago existente, por ejemplo, un servicio de pago bancario en línea existente. La operación específica del servidor no se describe en la presente aplicación. Después de completar una transacción, el servidor puede devolver información de éxito de transacción a una máquina POS con la cual el pago fuera de línea se lleva a cabo y la información de éxito de transacción se muestra en la máquina POS; o cuando se lleva a cabo el pago en línea, el servidor directamente devuelve información de éxito de transacción a la unidad de comunicación móvil 202 del aparato de pago móvil 20, de modo que la información puede mostrarse en el aparato de pago móvil 20. De manera opcional, cuando la transacción falla, el servidor puede devolver información de fallo de pago en lugar de la información de éxito de transacción, lo cual no se encuentra limitado en la presente realización. La información de pago incluye un proceso de comunicación bidireccional, y se usa para implementar la comunicación de intercambio de pago móvil entre un servidor en la nube en un lado de red y el aparato de pago móvil 20. Un proceso de intercambio de comunicación bidireccional de la información de pago varía con diferentes proveedores de servicio y

diferente software de aplicación de pago móvil 2032 ejecutado por el procesador 2042 y, en general, depende de diferentes proveedores de servicio.

Como se muestra en la Figura 6, para el pago fuera de línea, cuando el procesador 2042 intercambia la información de pago con la unidad de comunicación de campo cercano 201, el procesador 2042 puede intercambiar la información de pago con la unidad de comunicación de campo cercano 201 (ubicada en el IC4) fuera del chip central IC1 mediante el uso de una interfaz de comunicación 2044 incluida en el elemento seguro 204. De manera específica, la interfaz de comunicación 2044 puede cumplir con un Protocolo de Cable Único (SWP, por sus siglas en inglés). Ciertamente, la interfaz de comunicación 2044 puede también implementar la transmisión de datos o información mediante el uso de otro protocolo de interfaz. Si la unidad de comunicación de campo cercano 201 también se integra al chip central IC1, el procesador 2042 puede intercambiar información con la unidad de comunicación de campo cercano 201 mediante el uso de un cable de conexión en chip, por ejemplo, un bus en chip 207 en la Figura 6. Dado que la interfaz de comunicación 2044 es una interfaz SWP estándar, la interfaz de comunicación 2044 puede implementarse mediante el uso del protocolo SWP estándar. Cómo la unidad de comunicación de campo cercano 201 transmite, según el protocolo SWP, datos que se adquieren de la máquina POS, al elemento seguro 204 es una solución madura existente, y no se describe en la presente solicitud. Además, la unidad de comunicación de campo cercano 201 y la al menos una unidad de procesamiento central 205 pueden conectarse mediante el uso de una interfaz de circuito inter-integrado (I2C), para transferir otros datos. Ciertamente, otra interfaz puede también implementar un propósito similar y no debe excluirse de la solución de implementación. La unidad de comunicación de campo cercano 201 puede, internamente, almacenar una tabla de encaminamiento, y la unidad de comunicación de campo cercano 201 puede identificar a qué tipo pertenece la comunicación iniciada por el extremo par de comunicación. Si el servicio iniciado es un servicio de pago, la unidad de comunicación de campo cercano 201 reenvía datos relacionados del servicio de pago relacionado al elemento seguro 204 mediante el uso de la interfaz SWP mediante consulta de la tabla de encaminamiento, de modo que el procesador 2042 en el elemento seguro 204 lleva a cabo el procesamiento. Si el servicio iniciado es un servicio de no pago, la unidad de comunicación de campo cercano 201 reenvía datos del servicio de no pago relacionado a al menos una unidad de procesamiento central 205 mediante el uso de la interfaz I2C mediante consulta de la tabla de encaminamiento. Por ejemplo, si el servicio iniciado es para contar horas de trabajo mediante contacto de una tarjeta del personal con un lector de tarjetas en una empresa, la unidad de comunicación de campo cercano 201 puede enviar datos a la al menos una unidad de procesamiento central 205 mediante el uso de la interfaz I2C, y los datos se usan para llevar a cabo la aplicación analógica de lectura de tarjeta en un sistema operativo general, por ejemplo, un entorno Android.

Para el pago en línea, suponiendo que se usa la manera de implementación en la cual la unidad de comunicación móvil 202 se integra al chip central IC1, con referencia a la Figura 6, el procesador 2042 puede también intercambiar la información de pago con la unidad de comunicación móvil 202 mediante el uso de un bus en chip 207. El bus en chip 207 puede además conectarse a la unidad de procesamiento central 205 y a una interfaz de almacenamiento 208. La interfaz de almacenamiento 208 se usa por el chip central IC1 para intercambiar datos con la memoria 203 en el segundo chip IC2.

En una manera de implementación opcional, los datos de pago móvil provistos por el procesador 2042 al extremo par de comunicación pueden ser un resultado de procesamiento de seguridad, y el procesamiento de seguridad puede incluir al menos una de las siguientes: encriptación de datos o protección de integridad de datos. De manera específica, el procesador 2042 puede además generar los datos que resultan del procesamiento de seguridad cuando se acciona por el software de pago móvil 2030, es decir, el procesador puede accionarse por software para llevar a cabo el procesamiento de seguridad, para asegurar que los datos de pago móvil procesados se transmitan al servidor. El servidor puede, por consiguiente, llevar a cabo la desencriptación y la protección de integridad de cálculo en los datos de pago móvil, para verificar si los datos de pago móvil se alteran. Si los datos de pago móvil se alteran, el servidor puede devolver la información de fallo de pago mencionada más arriba, para garantizar la seguridad del procedimiento de pago móvil. De manera alternativa, el procesador 2042 puede generar solamente datos originales, donde los datos originales son datos de pago móvil que no han atravesado el procesamiento de seguridad. Un módulo de procesamiento de seguridad independiente 2045 en el elemento seguro 204 lleva a cabo el procesamiento de seguridad en los datos originales para generar los datos que resultan del procesamiento de seguridad. El módulo de procesamiento de seguridad 2045 puede ser independiente del procesador 2042 en forma de hardware, y puede ser, de manera específica, un acelerador de hardware que incluye una estructura de circuito, donde el acelerador de hardware se configura para acelerar el procesamiento de seguridad, de modo que la implementación del procesamiento se optimiza más.

Además de que los datos intercambiados con el extremo par de comunicación necesitan atravesar el procesamiento de seguridad, el procesador 2042 además necesita leer el software de pago móvil 2030 de la memoria 203, y la protección de seguridad puede también proveerse para la lectura y escritura del software de pago móvil 2030, para implementar una mejor seguridad. Por ejemplo, el elemento seguro 204 además incluye: un motor cifrado 2046, configurado para llevar a cabo la verificación de seguridad en el software de pago móvil 2030 después de que el procesador 2042 carga el software de pago móvil 2030 de la memoria 203 al primer módulo de almacenamiento 2041, y ordenar al procesador 2042 que ejecute el software de pago móvil 2030 después de que la verificación de seguridad tiene éxito, donde la verificación de seguridad incluye al menos una de la desencriptación de seguridad o primera verificación de troceo. De manera opcional, el motor cifrado puede ser un acelerador de hardware que

incluye una estructura de circuito. Dado que el motor cifrado 2046 en forma de hardware es independiente del procesador 2042, y se dedica a la implementación de una función de verificación de seguridad, puede asegurarse que el software de pago móvil 2030 se ejecuta solamente después de que la verificación tiene éxito, lo cual evita que el software del sistema operativo de pago móvil 2031 o el software de aplicación de pago móvil 2032 en el software de pago móvil 2030 se alteren, y ayuda a mejorar el rendimiento de procesamiento cuando la verificación de seguridad se lleva a cabo.

Además de la lectura del software de pago móvil 2030 para verificar el software de pago móvil 2030, el motor cifrado 2046 puede asimismo configurarse para llevar a cabo al menos un tipo de procesamiento en la encriptación de seguridad o primer procesamiento de operación de troceo en datos de actualización. El procesador 2042 se configura además para escribir los datos de actualización procesados en la memoria 203, para actualizar el software de pago móvil 2030. Por ejemplo, la actualización de datos puede ser una actualización de un espejo COS o una actualización de cualquier tipo de software de aplicación de pago móvil 2032. El contenido de los datos de actualización puede incluir un archivo para actualizar el espejo COS o el software de aplicación de pago móvil 2032, y puede incluir actualización de información usada para llevar a cabo la encriptación de datos o protección de integridad de datos en los datos de pago móvil, por ejemplo, actualización de una clave, o puede incluir un archivo de registro de pago móvil como, por ejemplo, modificación de información personal y un registro de transacciones. El contenido de los datos de actualización no se encuentra limitado en la presente realización.

De manera alternativa, las funciones del motor cifrado 2046 pueden también reemplazarse por el procesador 2042. En el presente caso, un motor cifrado 2046 de hardware independiente no necesita llevar a cabo el procesamiento de seguridad en el software de pago móvil 2030 que se lee desde la memoria 203 o que se escribe en la memoria 203, y el procesador 2042 integra las funciones de seguridad. Asimismo, cuando se escriben los datos de actualización procesados en la memoria, el procesador 2042 puede además llevar a cabo el segundo procesamiento de operación de troceo en los datos de actualización procesados mediante el uso de una clave Krpmb, para obtener datos que se almacenarán. El segundo procesamiento de operación de troceo puede ser similar a un proceso del primer procesamiento de operación de troceo mencionado más arriba, y las claves específicamente usadas cuando los dos tipos de procesamiento de troceo se llevan a cabo son, en general, diferentes. Por ejemplo, los datos de actualización pueden encriptarse en el segundo procesamiento de operación de troceo mediante el uso de la clave Krpmb para obtener un valor *digest*, el valor *digest* y los datos de actualización se combinan para generar los datos que se almacenarán, y el valor *digest* puede también ser una firma de código de autenticación de mensaje (MAC, por sus siglas en inglés). La memoria 203 se configura además para llevar a cabo la segunda verificación de troceo en los datos que se almacenarán, donde la segunda verificación de troceo es un proceso correspondiente al segundo procesamiento de operación de troceo, y se usa para verificar si los datos que se almacenarán que han atravesado el segundo procesamiento de operación de troceo se alteran. Para detalles, puede hacerse referencia a la técnica anterior para verificar la firma MAC. Después de que la segunda verificación de troceo tiene éxito, la memoria 203 obtiene los datos de actualización procesados, y actualiza el software de pago móvil 2030 mediante el uso de los datos de actualización procesados.

Se usa un ejemplo en el cual la memoria 203 es una eMMC. Con referencia a la Figura 7, la región de almacenamiento seguro 203A de la memoria 203 se usa para almacenar el software de pago móvil 2030. Cuando el procesador 2042 lleva a cabo una operación de escritura, una operación de borrado, o similares en la región de almacenamiento seguro 203A, se necesita una firma de un comando de verificación, donde el comando de verificación es una clave Krpmb. La memoria 203 eMMC verifica, según una clave Krpmb preestablecida, si un paquete de datos de comandos de escritura enviado por el procesador 2042 es correcto, y cada paquete de datos de comando de escritura puede incluir algunos paquetes de datos de todos los datos de actualización. De manera específica, el algoritmo de procesamiento de verificación de troceo llevado a cabo mediante el uso de la clave Krpmb puede ser un algoritmo de algoritmo de troceo seguro de código de autenticación de mensaje basado en troceo (HMAC SHA, por sus siglas en inglés) 256. En una manera de implementación opcional, cuando la memoria 203 eMMC se produce, una clave Krpmb única de cada memoria 203 eMMC se programa en la memoria 203 eMMC, la clave Krpmb puede también programarse en el elemento seguro 204 o registrarse en el elemento seguro 204. De manera específica, la clave Krpmb puede programarse en el procesador 2042 del elemento seguro 204 mediante el uso de una tecnología de fusible electrónico (eFuse) o puede programarse en otro circuito de hardware en lugar del procesador 2042, y el elemento seguro 204 gestiona y usa la clave Krpmb.

Además de la gestión y uso de la clave Krpmb por el elemento seguro 204, en otra manera de implementación opcional, la gestión y el uso de la clave Krpmb en una zona fiable (TZ, por sus siglas en inglés) de la unidad de procesamiento central 205 es una manera de implementación más común. La TZ es un entorno de ejecución fiable (TEE, por sus siglas en inglés). De manera específica, un entorno formado mediante la ejecución de un tipo de software, es decir, un sistema de software, puede intercambiar datos con otro sistema de hardware o software externo. Como se muestra en la Figura 8, el entorno de ejecución fiable ejecutado por la unidad de procesamiento central 205 se encuentra aislado, de manera segura, del software del sistema operativo general (por ejemplo, un entorno de sistema Android) que también se ejecuta por la unidad de procesamiento central 205. El entorno de ejecución fiable y el software del sistema operativo general son, respectivamente, dos sistemas de software independientes. Aunque el entorno de ejecución fiable y el software del sistema operativo general se ejecutan por la misma unidad de procesamiento central 205, el aislamiento de seguridad entre el entorno de ejecución fiable y el

software del sistema operativo general es muy deseable, y el software del sistema operativo general y un programa de ejecución de software de aplicación general que se basa en el sistema operativo no pueden acceder al entorno de ejecución fiable libremente. El entorno de ejecución fiable puede transmitir datos con un entorno, es decir, el elemento seguro 204, formado mediante la ejecución del software de pago móvil 2030 por el procesador 2042. Por lo tanto, el software del sistema operativo general se encuentra aislado, de manera segura, tanto del entorno de ejecución fiable como del elemento seguro 204, de modo que el software del sistema operativo general o el programa de ejecución del software de aplicación común que se basa en el software no acceden libremente al entorno de ejecución fiable y al elemento seguro 204. Incluso si el acceso necesita llevarse a cabo mediante el uso de una interfaz de seguridad de software o hardware específico, hay menos aislamiento de seguridad entre el entorno de ejecución fiable y el elemento seguro 204, y las operaciones son relativamente convenientes. El software de aplicación común puede incluir software relacionado con pago no seguro, por ejemplo, software de mensajería instantánea, juegos, software de oficina, software de libro electrónico, o jugadores de audio y vídeo de flujo continuo.

En una manera de implementación opcional, la gestión de la clave Krpmb puede implementarse en un entorno de ejecución fiable. De manera específica, la clave Krpmb puede programarse en un circuito de hardware relacionado de la unidad de procesamiento central 205. De esta manera, el software de no seguridad del software del sistema operativo general (por ejemplo, un sistema Android) de la unidad de procesamiento central 205 no conoce la Krpmb. Por lo tanto, una operación de escritura no puede llevarse a cabo en la región de almacenamiento seguro 203A de la memoria 203 eMMC. Para otra región de almacenamiento común 203B en la memoria 203 eMMC, puede accederse al software del sistema operativo general de la unidad de procesamiento central 205 y a programas de ejecución de software de aplicación común. Dado que el software del sistema operativo general se encuentra aislado, de manera segura, del elemento seguro 204, el software del sistema operativo general no puede acceder libremente al elemento seguro, lo cual puede mejorar la seguridad de pago móvil.

De manera opcional, el entorno de ejecución fiable puede proveer una interfaz de usuario (IU) visual de pago bancario u otro servicio financiero, de modo que un usuario ingresa una instrucción mediante el uso de la IU, y la instrucción se transmite al elemento seguro 204 mediante el uso del entorno de ejecución fiable, que implementa que el usuario complete el intercambio de información con el elemento seguro 204 mediante el uso de la IU. La IU es una IU fiable, y diferente de una IU común provista por el software del sistema operativo general, la IU puede permitir que una contraseña de pago móvil ingresada por el usuario se transmita al elemento seguro 204 mediante el uso de un entorno de ejecución fiable relativamente seguro, y entonces la información que incluye la contraseña de pago móvil se somete a la encriptación de datos y se transmite a un servidor en un lado de red mediante el uso de la unidad de comunicación de campo cercano 201 o la unidad de comunicación móvil 202.

En una manera de implementación específica, se usa un ejemplo en el cual la memoria 203 es, en tipo, una eMMC. La Figura 4 es un diagrama esquemático de una arquitectura de software para llevar a cabo una operación de acceso en la región de almacenamiento seguro 203A de la memoria 203 eMMC según una realización de la presente invención. El acceso puede incluir leer datos de la región de almacenamiento seguro 203A o escribir datos en la región de almacenamiento seguro 203A (actualización o reclasificación de datos de seguridad), donde una unidad de la lectura o escritura puede ser una unidad de longitud fija. La arquitectura de software incluye el software de pago móvil 2030 y se ejecuta por el elemento seguro 204. El software de pago móvil 2030 provee una función similar relacionada con una operación de lectura de tarjeta de una tarjeta inteligente residente o una tarjeta CI, y puede incluir el software del sistema operativo de pago móvil 2031 y el software de aplicación de pago móvil 2032 que se mencionan más arriba.

En la Figura 4, para un proceso de escritura de la memoria 203 eMMC, en un entorno seguro provisto mediante la ejecución del software de pago móvil 2030 por el procesador 2042, los datos 410 son datos que se actualizarán o reclasificarán, el procesamiento de cálculo de troceo se lleva a cabo en los datos 410, para obtener datos procesados 411, y los datos 411 incluyen los datos 410 que se usan como datos de texto en lenguaje claro y un valor de troceo 410A (al que también puede hacerse referencia como un *digest* de los datos 410) de los datos en lenguaje claro 410. Entonces, la encriptación de seguridad se lleva a cabo en los datos 411 en el entorno seguro. De manera específica, una clave Kse puede usarse para encriptar los datos 411, para obtener datos de texto cifrado 412. La clave Kse puede ser uno o más grupos de claves, y un algoritmo de encriptación para la encriptación de seguridad puede ser cualquier algoritmo de encriptación simétrico o algoritmo de encriptación asimétrico. Por ejemplo, un algoritmo de encriptación disponible puede ser un algoritmo de encriptación avanzada (AES, por sus siglas en inglés), lo cual no se encuentra limitado en la presente realización. Entonces, el elemento seguro 204 puede transmitir los datos de texto cifrado 412 y una dirección de escritura a la unidad de procesamiento central 205 mediante el uso de un bus de sistema 207 que se muestra en la Figura 6, es decir, los datos de texto cifrado 412 y la dirección de escritura de los datos de texto cifrado 412 se transfieren de un entorno del software de pago móvil 2030 al entorno de ejecución fiable 2051 generado por la unidad de procesamiento central 205. Llevar a cabo, por la unidad de procesamiento central 205, el segundo procesamiento de operación de troceo en los datos de texto cifrado 412 y la dirección de escritura de los datos de texto cifrado 412 en el entorno de ejecución fiable generado 2051 puede ser, de manera específica, encriptar los datos de texto cifrado 412 o una parte de los datos de texto cifrado 412 mediante el uso de la clave Krpmb, para obtener un valor *digest* que resulta del procesamiento de troceo, es decir, una firma MAC. El algoritmo de encriptación puede ser un algoritmo de troceo, por ejemplo, un algoritmo HMAC SHA 256, descrito en la realización anterior. El segundo procesamiento de operación de troceo

puede también ser otro algoritmo de procesamiento que satisface un requisito de seguridad de datos de la región de almacenamiento seguro 203A de la memoria 203 eMMC. De manera específica, en el entorno de ejecución fiable 2051, los datos de texto cifrado 412 y la dirección de escritura, como datos, pueden dividirse en múltiples partes, y todas las partes se procesan en paralelo. Como se muestra en la Figura 4, el entorno de ejecución fiable 2051 incluye múltiples colas L1, ..., y LN, donde para cada cola, por ejemplo, una cola L1 incluye algunos paquetes L11 y una parte de verificación L12, y la parte de verificación L12 es un valor *digest* que resulta del segundo procesamiento de operación de troceo en el paquete L11 mediante el uso de la clave Krpmb. Entonces, cada cola se transfiere del entorno de ejecución fiable 2051 al software del sistema operativo general 2052 y, en general, se transfiere, de manera específica, a un núcleo del software del sistema operativo general 2052. El proceso de transferencia es una transmisión, en general, transparente, es decir, el software del sistema operativo general 2052 no modifica contenido de datos. En un entorno de software del sistema operativo general 2052, cada una de las colas L1, ..., y LN se convierte en datos RPMB D que pueden leerse por la memoria 203 eMMC, y D puede también dividirse en múltiples segmentos o colas, por ejemplo, D1, ..., y DN, y se transmite a la memoria 203 eMMC mediante el uso de la interfaz de almacenamiento 208 que se muestra en la Figura 2 o Figura 6. De manera específica, en el entorno de software del sistema operativo general 2052, el procesamiento de comando de protocolo eMMC se lleva a cabo en la cola L1 para obtener los datos D1, ..., y DN en cumplimiento de un estándar de la interfaz de almacenamiento 208, pero el contenido de datos originales no se procesa o reconstruye. Según se describe más arriba, la memoria 203 eMMC tiene la clave Krpmb, obtiene la cola L1 según los datos D1, y lleva a cabo la verificación de firma MAC en la parte de verificación L12 en la cola L1 mediante el uso de la clave Krpmb. De manera específica, la clave Krpmb se usa para encriptar el paquete L11 en la cola L1 para obtener un valor *digest*, y el valor *digest* se compara con la parte de verificación L12, para obtener un resultado de verificación. Si la verificación tiene éxito, los datos de texto cifrado 412 o una parte de ellos y una dirección de escritura correspondiente se obtienen según los múltiples paquetes L11, y los datos de texto cifrado 412 o la parte de ellos se escriben en la región de almacenamiento seguro 203A, por ejemplo, un RPMB, de la memoria 203 eMMC según la dirección de escritura.

Con referencia a la Figura 4, el proceso de lectura de la memoria 203 eMMC es un procedimiento inverso al proceso de escritura previo, y no se describe en detalle en la presente realización. La cola de datos que se envía por la memoria 203 eMMC al software del sistema operativo general 2052 y que se transfiere por el software del sistema operativo general 2052 al entorno de ejecución fiable 2051 se encripta mediante el uso de la clave Krpmb, y la cola de datos incluye el paquete L11 de contenido de datos y la parte de verificación L12 generada por medio de la encriptación. En el entorno de ejecución fiable 2051, la unidad de procesamiento central 205 encripta, mediante el uso de la clave Krpmb, el paquete L11 en la cola L1 almacenada temporalmente para obtener el valor *digest*, y el valor *digest* se compara con la parte de verificación L12 para verificar si los datos se alteran. El elemento seguro 204 puede ser, de manera específica, el motor cifrado 2046 o el procesador 2042 descritos más arriba, y en el entorno provisto por el software de pago móvil 2030, los datos de texto cifrado 412 se obtienen mediante el uso del bus de sistema 207 u otra interfaz, y la desencriptación de seguridad se lleva a cabo mediante el uso de la clave Kse para obtener los datos 410 y el valor de troceo 410A de los datos 410. El elemento de seguridad 204 además lleva a cabo la verificación de troceo en el valor de troceo 410A y después de que la verificación tiene éxito, confirma que los datos relacionados no se alteran, de modo que la lectura se lleva a cabo de manera exitosa. Si cualquiera de la verificación de troceo o desencriptación de seguridad no tiene éxito, puede concluirse que los datos relacionados se alteran, y los datos buscados esta vez no son fiables. Por lo tanto, el procesador 2042 en el elemento seguro 204 puede determinar descartar los datos. De manera opcional, cuando los datos no son fiables, el procesador 2042 puede informar un error o proveer una alarma a la unidad de procesamiento central 205, lo cual no se encuentra limitado en la presente realización. Para la operación de la memoria 203 eMMC, el proceso de lectura y el proceso de escritura del software del sistema operativo de pago móvil 2031 como, por ejemplo, un espejo COS, y del software de aplicación de pago móvil 2032 pueden ser similares a aquellos en la Figura 4.

En la realización correspondiente a la Figura 4, se usa un ejemplo en el cual los datos se escriben en la memoria 203. En realidad, cuando el procesador 2042 necesita borrar datos en la memoria 203, el procesador 2042 puede también generar una instrucción de borrado, donde la instrucción lleva una dirección de datos que necesitan borrarse. La instrucción se transmite por el procesador 2042 a la unidad de procesamiento central 205, es decir, se transmite por el software de pago móvil 2030 al entorno de ejecución fiable 2051. La encriptación (procesamiento de troceo) puede llevarse a cabo en la instrucción por la unidad de procesamiento central 205 en el entorno de ejecución fiable 2051 mediante el uso de la clave Krpmb, para obtener un valor *digest*, y el valor *digest* y la instrucción se transfieren, ambos, por el software del sistema operativo general 2052 a la memoria 203. En el presente caso, la memoria 203 usa un método de verificación similar al de más arriba, es decir, la encriptación (procesamiento de troceo) se lleva a cabo en la instrucción mediante el uso de la misma Krpmb, y el resultado obtenido se compara con el valor *digest*, para determinar si la verificación llevada a cabo en la instrucción tiene éxito. Cuando la verificación tiene éxito, la memoria 203 puede borrar datos correspondientes según una dirección en la instrucción. De manera alternativa, en la operación de borrado, la encriptación de clave Krpmb (procesamiento de troceo) puede también procesarse por el procesador 2042 en el elemento seguro 204, y no llevarse a cabo por la unidad de procesamiento central 205 en el entorno de ejecución fiable 2051. Dado que el procesamiento de troceo necesita llevarse a cabo en el proceso de la operación de borrado, y otro software de no seguridad basado en el software del sistema operativo general 2052 no puede conocer la clave Krpmb, los datos en la memoria 203 no pueden borrarse libremente, lo cual mejora la seguridad. Los datos borrados pueden ser algunos datos del software

de pago móvil 2030 almacenados en la memoria 203. Por ejemplo, la memoria 203 puede borrar algunos datos del software del sistema operativo de pago móvil o todos o algunos de los datos del software de aplicación de pago móvil 2032 en respuesta a la instrucción según la dirección en la instrucción.

Debe notarse que la solución anterior puede usarse en un caso en el cual la memoria 203 eMMC se usa tanto para el software de pago móvil 2030 como para el software del sistema operativo general 2052. Puede verse que es muy difícil para el software de no seguridad acceder a la región de almacenamiento seguro 203A de la memoria 203 eMMC a menos que las claves Krpmb y Kse estén, ambas, desencriptadas, de modo que la privacidad e integridad de los datos puedan garantizarse mejor. La clave Kse es el medio más importante para generar un texto cifrado en el elemento seguro 204 y evitar la intrusión. La seguridad del intercambio de datos entre el elemento seguro 204, la unidad de procesamiento central 205 y la interfaz de almacenamiento 208 mediante el uso de un bus en chip 207 es más alta que otra tecnología de transmisión de interfaz, por ejemplo, transmisión SPI, en la técnica anterior, de modo que la seguridad del intercambio de datos entre el elemento seguro 204 y la memoria 203 eMMC se mejora. Por lo tanto, en comparación con una solución en la cual los datos se intercambian entre una CPU en un chip central y un elemento seguro fuera del chip central mediante el uso de una SPI, en la presente realización de la presente invención, el elemento seguro 204 puede integrarse al chip central IC1, y la transferencia de datos se implementa entre el elemento seguro 204 y el entorno de ejecución fiable 2051 de la unidad de procesamiento central 205 mediante el uso del bus 207, de modo que la seguridad es mejor.

Además, como se muestra en la Figura 6, el elemento seguro 204 puede incluir un tercer módulo de almacenamiento 2047. Cuando los datos se envían del entorno de software de pago móvil 2030 al entorno de ejecución fiable 2051 mediante el uso del procedimiento de procesamiento en la Figura 4, el procesador 2042 puede primero escribir los datos en el tercer módulo de almacenamiento 2047, y envía una solicitud de interrupción a la unidad de procesamiento central 205 en el bus 207, para solicitar a la unidad de procesamiento central 205 que lea datos en el tercer módulo de almacenamiento 2047. De manera específica, la solicitud de interrupción puede incluir una dirección de los datos de lectura en el tercer módulo de almacenamiento 2047. De esta manera, la unidad de procesamiento central 205 puede leer datos correspondientes del tercer módulo de almacenamiento 2047 en respuesta a la solicitud de interrupción. Cuando se envían datos al elemento seguro 204, la unidad de procesamiento central 205 puede también escribir datos en el tercer módulo de almacenamiento 2047, y solicita, mediante el envío de la solicitud de interrupción, al procesador 2042 en el elemento seguro 204 u otro componente que lea los datos. La solicitud de interrupción en la presente realización es un mensaje de indicación usado para solicitar la lectura de datos. El tercer módulo de almacenamiento 2047 puede ser una RAM, por ejemplo, una RAM de comunicación entre procesos (IPC, por sus siglas en inglés). De manera alternativa, el tercer módulo de almacenamiento 2047 puede también ser otro tipo de memoria, por ejemplo, una caché. En comparación con una manera de llevar a cabo la comunicación mediante el uso de una SPI fuera de chip, mediante el uso del tercer módulo de almacenamiento 2047, la comunicación y el intercambio de datos entre el elemento seguro 204 y la unidad de procesamiento central 205 se llevan a cabo, ambos, mediante el uso de la memoria 2047 en el chip central IC1 y el bus 207, y la seguridad se mejora.

En otra manera de implementación opcional, una memoria que almacena el software de pago móvil 2030 y una memoria que almacena el software del sistema operativo general 2052 pueden estar físicamente aisladas. En el presente caso, un procedimiento básico de escritura o lectura de datos se simplifica. Como se muestra en la Figura 5, en el presente caso, la memoria 203 se ubica en un segundo chip semiconductor IC2, que puede ser, de manera específica, una memoria no Flash. En un entorno seguro provisto por el software de pago móvil 2030, los datos 410 son datos que se actualizarán o reclasificarán, el procesamiento de cálculo de troceo se lleva a cabo en los datos 410, para obtener datos procesados 411, y los datos 411 incluyen los datos 410 que se usan como datos de texto en lenguaje claro y un valor de troceo 410A de los datos 410. Entonces, la encriptación de seguridad se lleva a cabo en los datos 411 en el entorno seguro. De manera específica, una clave Kse puede usarse para encriptar los datos 411, para obtener datos de texto cifrado 412. Entonces, los datos de texto cifrado 412 se escriben directamente en la memoria 203. El proceso de lectura de datos es inverso al proceso de escritura de datos, y no se describe en la presente realización. En la presente solución de implementación, la memoria 203 es un aparato de almacenamiento dedicado al pago móvil. En el presente caso, el elemento seguro 204 puede escribir directamente varios datos en la memoria 203 o leer varios datos de la memoria 203 sin reenviar el entorno de ejecución fiable 2051, donde los datos incluyen un espejo COS o datos de software de aplicación. Cuando una operación de borrado se lleva a cabo, el procesador 2042 en el elemento seguro 204 puede enviar una instrucción de borrado a la memoria 203, donde la instrucción lleva una dirección de datos que necesita borrarse. Después de recibir la instrucción, la memoria 203 puede directamente borrar los datos en la dirección relacionada, para mejorar la seguridad.

Según las soluciones técnicas, las realizaciones de la presente invención pueden implementar pago móvil seguro, y reducir costes y dificultad de diseño de pago móvil. Debe notarse que el pago móvil es una definición extensiva, y no solo incluye servicios de pago móvil comerciales y financieros, sino que también incluye otros tipos de servicios de pago como, por ejemplo, transporte público, una tarjeta de identidad y una tarjeta de la seguridad social. Es decir, por medio del pago móvil, un terminal móvil puede conectarse a un extremo par de comunicación, para intercambiar finalmente información de pago con un servidor, y para implementar una transacción de datos, rescate de datos, o acuerdo de datos asociados a una o más cuentas en el terminal móvil. Además de la moneda, otra unidad de una transacción de datos, rescate o acuerdo de datos pueden aplicarse también, por ejemplo, moneda virtual, varios

tipos de puntos de bonificación o una línea de crédito, que pueden usarse para implementar el pago, rescate o acuerdo de transacciones, lo cual no se encuentra limitado en la presente realización. La cuenta incluye, pero sin limitación a ello, una cuenta personal, una cuenta de grupo, o una cuenta de organización. En comparación con un comportamiento de pago implementado en solamente un terminal fijo, el pago móvil se implementa de manera más flexible, y una entidad para implementar el pago móvil es un terminal móvil, que pueden satisfacer mejor un requisito para llevar a cabo el pago en cualquier momento y en cualquier lugar.

Debe notarse que, en las realizaciones de la presente invención, puede haber múltiples unidades de procesamiento central 205. Que las múltiples unidades de procesamiento central 205 intercambian datos con otro componente, por ejemplo, el elemento seguro 204, en el aparato de pago móvil 20 puede ser que una o más de las múltiples unidades de procesamiento central 205 intercambian datos con el otro componente. Cuando el aparato de pago móvil 20 se encuentra en un estado de funcionamiento, todas o algunas de las múltiples unidades de procesamiento central 205 pueden iniciarse, e implementan el entorno de ejecución fiable 2051, el software de sistema operativo general 2052, y otro software de aplicación por medio de la división de trabajo y coordinación entre sí.

Además, el aparato de pago móvil 20 puede además incluir una unidad de procesamiento de gráficos (GPU, por sus siglas en inglés), una unidad de procesamiento de audio, una unidad de gestión de potencia (PMU, por sus siglas en inglés) o un sistema de posicionamiento global (GPS, por sus siglas en inglés). Además, el terminal móvil 21 puede asimismo incluir, además del aparato de pago móvil 20 que incluye principalmente varios circuitos, una pantalla táctil usada para llevar a cabo la entrada, una visualización, y otro sensor necesario como, por ejemplo, un acelerómetro de gravedad, un giroscopio o un sensor óptico.

Las anteriores son meramente realizaciones a modo de ejemplo de la presente invención. Una persona con experiencia en la técnica puede realizar varias modificaciones y variaciones en la presente invención sin apartarse del alcance de la presente invención. Por ejemplo, las formas o estructuras específicas de los componentes en los dibujos anexos en las realizaciones de la presente invención pueden ajustarse según un escenario de aplicación real.

REIVINDICACIONES

1. Un aparato de pago móvil (20), que comprende:

una unidad de comunicación, configurada para intercambiar información de pago con un extremo par de comunicación mediante el uso de un enlace radioeléctrico;

una memoria (203), configurada para almacenar software de pago móvil (2030) que comprende software del sistema operativo de pago móvil (2031);

un elemento seguro (204), que comprende un primer módulo de almacenamiento (2041) y un procesador (2042); y

al menos una unidad de procesamiento central (205), configurada para ejecutar software del sistema operativo general (2052), y controlar al menos uno de la unidad de comunicación, la memoria (203), o el elemento seguro (204) bajo la acción del software del sistema operativo general (2052); en donde

el procesador (2042) se configura para cargar el software de pago móvil (2030) de la memoria (203) al primer módulo de almacenamiento (2041), ejecutar el software de pago móvil (2030) e intercambiar la información de pago con la unidad de comunicación bajo la acción del software de pago móvil (2030);

el primer módulo de almacenamiento (2041) se configura para proveer espacio de memoria para ejecutar el software de pago móvil (2030) para el procesador (2042); y

el elemento seguro (204) y la al menos una unidad de procesamiento central (205) se ubican en un primer chip semiconductor (IC1) en el aparato de pago móvil (20).

2. El aparato de pago móvil (20) según la reivindicación 1, en donde la memoria (203) se ubica en un segundo chip semiconductor (IC2) en el aparato de pago móvil (20).

3. El aparato de pago móvil (20) según la reivindicación 2, en donde la memoria (203) comprende una región de almacenamiento seguro (203A) y una región de almacenamiento común (203B) que se encuentran aisladas entre sí, en donde

la región de almacenamiento seguro (203A) se usa para almacenar el software de pago móvil (2030); y

la región de almacenamiento común (203B) se usa para almacenar el software del sistema operativo general (2052);

el procesador (2042) se configura, de manera específica, para cargar el software de pago móvil (2030) de la región de almacenamiento seguro (203A) en la memoria (203) al primer módulo de almacenamiento (2041); y

la al menos una unidad de procesamiento central (205) se configura, de manera específica, para leer el software del sistema operativo general (2052) de la región de almacenamiento común (203B) en la memoria (203) y ejecutar el software del sistema operativo general (2052).

4. El aparato de pago móvil (20) según la reivindicación 2, en donde la memoria (203) se dedica al almacenamiento del software de pago móvil (2030);

el aparato de pago móvil (20) además comprende una unidad de almacenamiento común, en donde la unidad de almacenamiento común (206) se ubica en un tercer chip semiconductor (IC3) en el aparato de pago móvil (20), y la unidad de almacenamiento común (206) se configura para almacenar el software del sistema operativo general (2052); y

la al menos una unidad de procesamiento central (205) se configura, de manera específica, para leer el software del sistema operativo general (2052) de la unidad de almacenamiento común (206) y ejecutar el software del sistema operativo general (2052).

5. El aparato de pago móvil (20) según la reivindicación 1, en donde el software de pago móvil (2030) además comprende al menos un tipo de software de aplicación de pago móvil (2032).

6. El aparato de pago móvil (20) según la reivindicación 1 o 2, en donde el elemento seguro (204) además comprende un segundo módulo de almacenamiento (2043), configurado para almacenar un programa de arranque para iniciar el procesador (2042); y

cuando el elemento seguro (204) se enciende, el procesador (2042) se configura para leer el programa de arranque del segundo módulo de almacenamiento (2043), cargar el software del sistema operativo de pago móvil (2031) de la memoria (203) al primer módulo de almacenamiento (2041) bajo la acción del programa de arranque, y ejecutar el software del sistema operativo de pago móvil (2031).

7. El aparato de pago móvil (20) según la reivindicación 5, en donde el procesador (2042) se configura para cargar uno o más tipos de software de aplicación de pago móvil (2032) del al menos un tipo de software de aplicación de

pago móvil (2032) de la memoria (203) al primer módulo de almacenamiento (2041) después de activarse por la información de pago intercambiada entre el procesador (2042) y la unidad de comunicación, y ejecutar el único o más tipos de software de aplicación de pago móvil (2032).

8. El aparato de pago móvil (20) según cualquiera de las reivindicaciones 1 a 7, en donde el elemento seguro (204) además comprende: un motor cifrado (2046), configurado para llevar a cabo la verificación de seguridad en el software de pago móvil (2030) después de que el procesador (2042) carga el software de pago móvil (2030) de la memoria (203) al primer módulo de almacenamiento (2041), y ordenar al procesador (2042) que ejecute el software de pago móvil (2030) después de que la verificación de seguridad tiene éxito, en donde la verificación de seguridad comprende al menos una de la desencriptación de seguridad o primera verificación de troceo.

9. El aparato de pago móvil (20) según cualquiera de las reivindicaciones 1 a 7, en donde el procesador (2042) se configura además para llevar a cabo la verificación de seguridad en el software de pago móvil (2030) después de cargar el software de pago móvil (2030) de la memoria (203) al primer módulo de almacenamiento (2041), y ejecutar el software de pago móvil (2030) después de que la verificación de seguridad tiene éxito, en donde la verificación de seguridad comprende al menos una de la desencriptación de seguridad o primera verificación de troceo.

10. El aparato de pago móvil (20) según cualquiera de las reivindicaciones 1 a 9, en donde la al menos una unidad de procesamiento central (205) se configura además para ejecutar software de aplicación común a excepción del software de pago móvil (2030).

11. El aparato de pago móvil (20) según cualquiera de las reivindicaciones 1 a 10, en donde el software del sistema operativo general (2052) ejecutado por la al menos una unidad de procesamiento central (205) se encuentra aislado, de manera segura, del elemento seguro (204).

12. El aparato de pago móvil (20) según cualquiera de las reivindicaciones 1 a 10, en donde el procesador (2042) se configura además para llevar a cabo el segundo procesamiento de operación de troceo en datos de actualización o una instrucción de borrado mediante el uso de una clave, para obtener un resultado de procesamiento; y

la memoria (203) se configura además para llevar a cabo la segunda verificación de troceo en el resultado de procesamiento, obtener los datos de actualización o la instrucción de borrado después de que la segunda verificación de troceo tiene éxito, y actualizar el software de pago móvil (2030) mediante el uso de los datos de actualización o datos de borrado que corresponden a la instrucción de borrado de la memoria (203) según la instrucción de borrado.

13. El aparato de pago móvil (20) según cualquiera de las reivindicaciones 1 a 10, en donde el procesador (2042) se configura además para enviar datos de actualización o una instrucción de borrado a la al menos una unidad de procesamiento central (205);

la al menos una unidad de procesamiento central (205) se configura además para llevar a cabo un segundo procesamiento de operación de troceo en los datos de actualización o la instrucción de borrado en un entorno de ejecución fiable (2051) mediante el uso de una clave, para obtener un resultado de procesamiento, y enviar el resultado de procesamiento a la memoria (203), en donde el entorno de ejecución fiable (2051) se encuentra aislado, de manera segura, del software del sistema operativo general (2052); y

la memoria (203) se configura además para llevar a cabo la segunda verificación de troceo en el resultado de procesamiento, obtener los datos de actualización o la instrucción de borrado después de que la segunda verificación de troceo tiene éxito, y actualizar el software de pago móvil (2030) mediante el uso de los datos de actualización o datos de borrado que corresponden a la instrucción de borrado de la memoria (203) según la instrucción de borrado.

14. Un método para implementar el pago móvil mediante el uso de un aparato de pago móvil (20), que comprende:

ejecutar (E31) software del sistema operativo general (2052) y controlar al menos uno de una unidad de comunicación, una memoria (203), o un elemento seguro (204) bajo la acción del software del sistema operativo general (2052), mediante el uso de al menos una unidad de procesamiento central (205);

cargar (E32) software de pago móvil (2030) que comprende software del sistema operativo de pago móvil (2031) de la memoria (203) al elemento seguro (204);

ejecutar (E32) el software de pago móvil (2030) en el elemento seguro (204); e

intercambiar (E33, E34, E35, E36), por el elemento seguro (204), información de pago con la unidad de comunicación bajo la acción del software de pago móvil (2030), en donde la unidad de comunicación intercambia la información de pago con un extremo par de comunicación mediante el uso de un enlace radioeléctrico; en donde

el elemento seguro (204) y la al menos una unidad de procesamiento central (205) se ubican en un primer chip semiconductor (IC1) en el aparato de pago móvil (20).

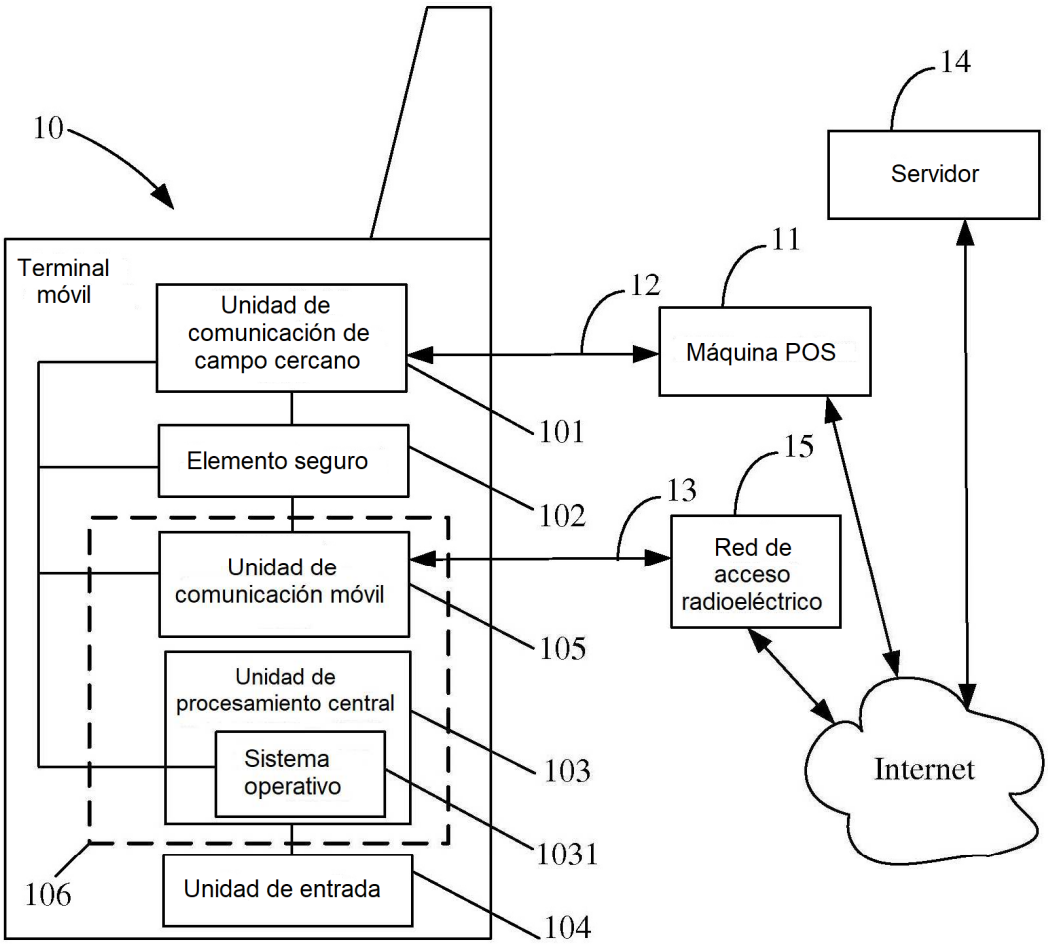
10
Terminal móvil
Unidad de comunicación de campo cercano
Elemento seguro
Unidad de comunicación móvil
Unidad de procesamiento central
Sistema operativo
Unidad de entrada
106
101
102
105
103
1031
104
12
11
Máquina POS
14
Servidor
13
15
Red de acceso radioeléctrico
Internet

FIG. 1

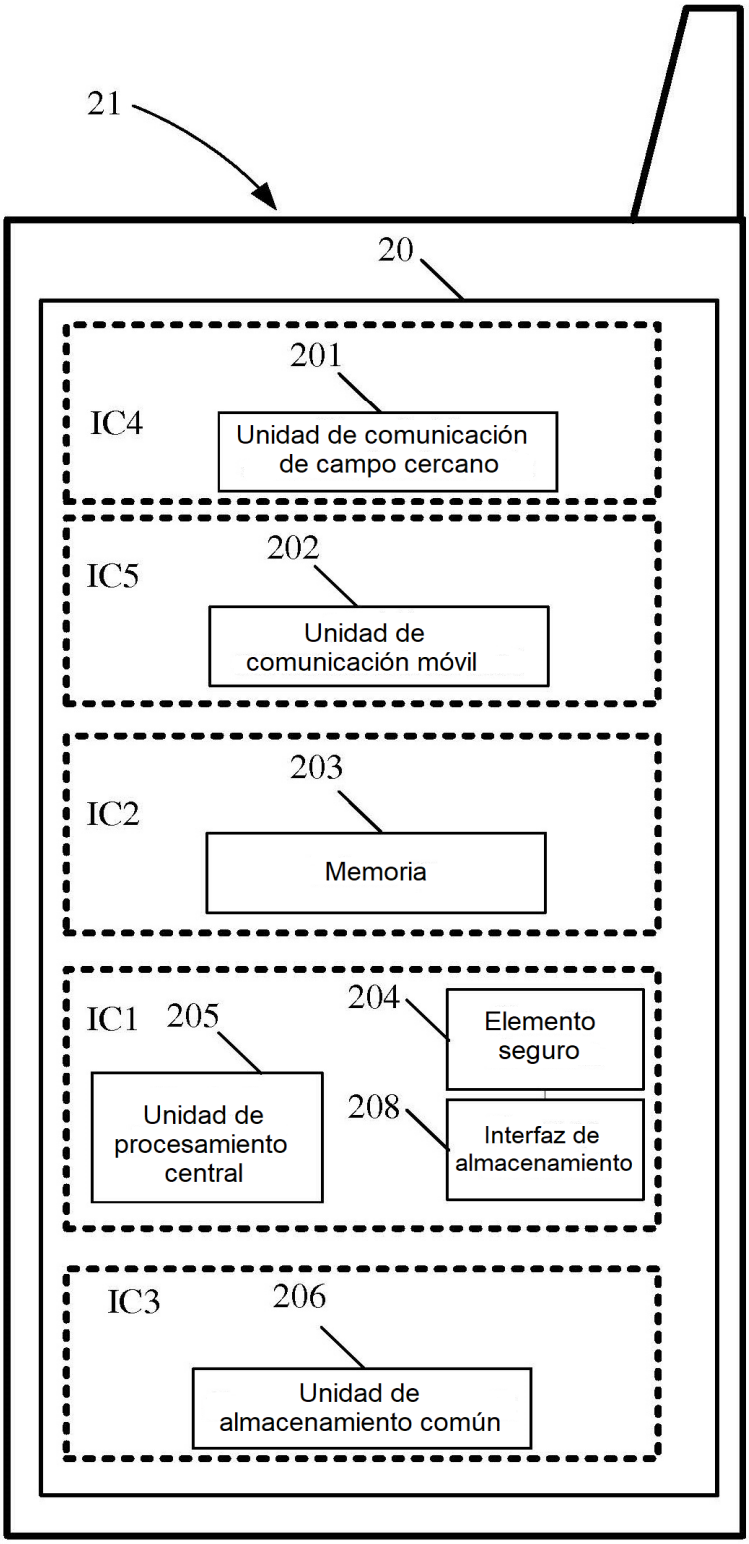
21
20
201
IC4
Unidad de comunicación de campo cercano
202
IC5
Unidad de comunicación móvil
203
IC2
Memoria
IC1
205
Unidad de procesamiento central
204
Elemento seguro
208
Interfaz de almacenamiento
IC3
206
Unidad de almacenamiento común

FIG. 2

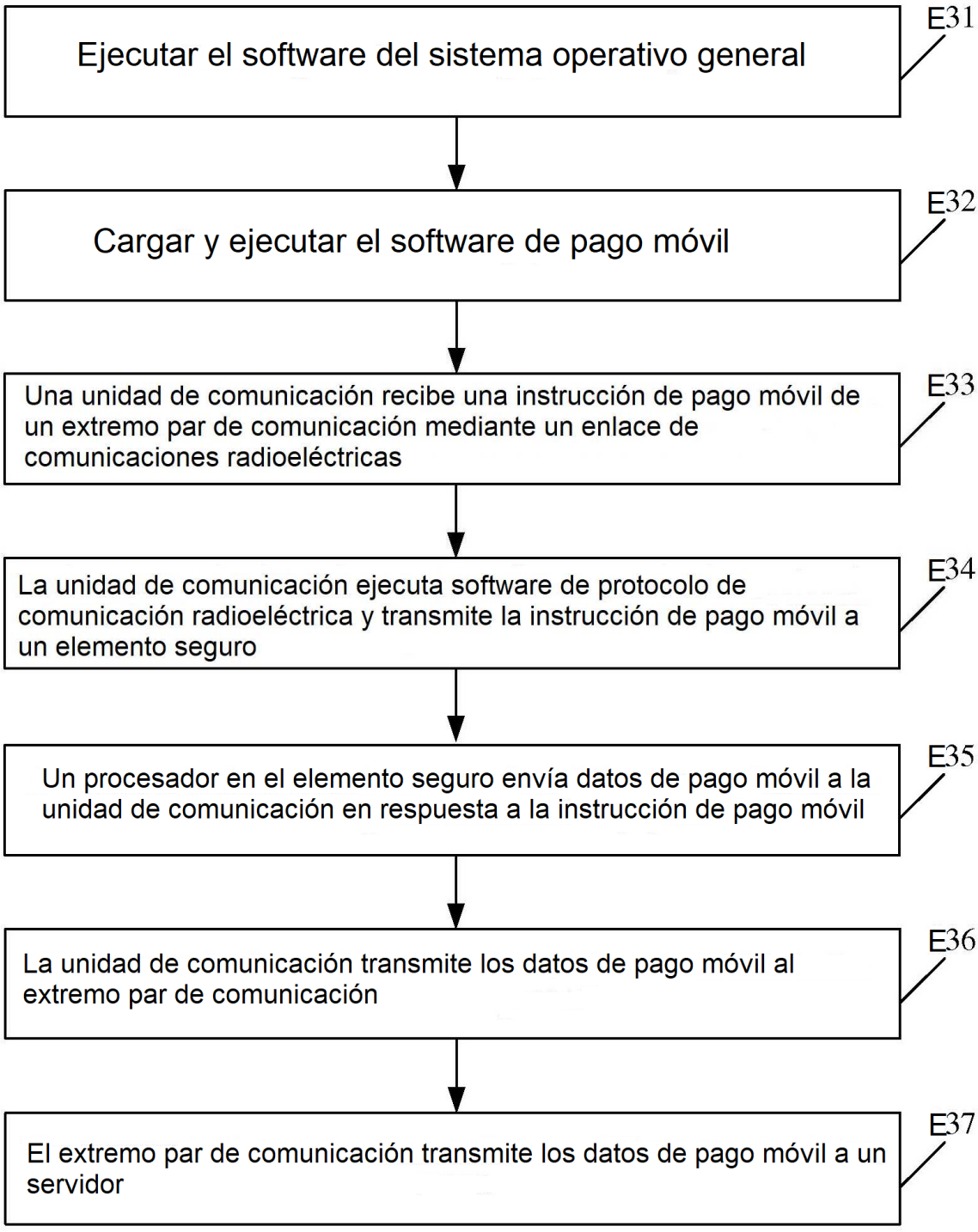
Ejecutar el software del sistema operativo general
E31
Cargar y ejecutar el software de pago móvil
E32
Una unidad de comunicación recibe una instrucción de pago móvil de un extremo par de comunicación mediante un enlace de comunicaciones radioeléctricas
E33
La unidad de comunicación ejecuta software de protocolo de comunicación radioeléctrica y transmite la instrucción de pago móvil a un elemento seguro
E34
Un procesador en el elemento seguro envía datos de pago móvil a la unidad de comunicación en respuesta a la instrucción de pago móvil
E35
La unidad de comunicación transmite los datos de pago móvil al extremo par de comunicación
E36
El extremo par de comunicación transmite los datos de pago móvil a un servidor
E37

FIG. 3

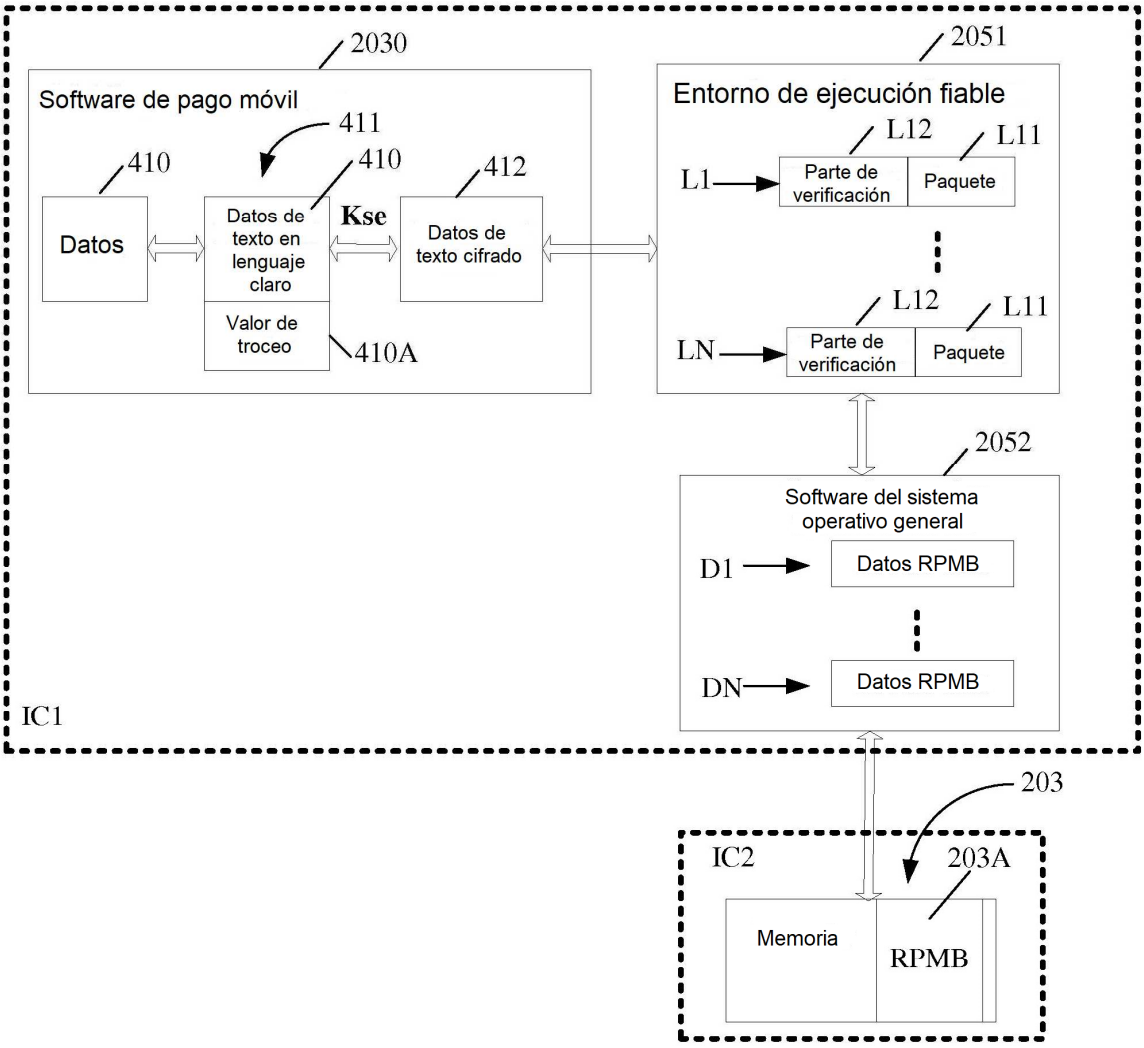
2030
Software de pago móvil
411
410
410
412
Datos
Datos de texto en lenguaje claro
Kse
Datos de texto cifrado
Valor de troceo
410A
2051
Entorno de ejecución fiable
L12
L11
L1
Parte de verificación
Paquete
L12
L11
LN
Parte de verificación
Paquete
2052
Software del sistema operativo general
D1
Datos RPMB
DN
Datos RPMB
IC1
203
IC2
203A
Memoria
RPMB

FIG. 4

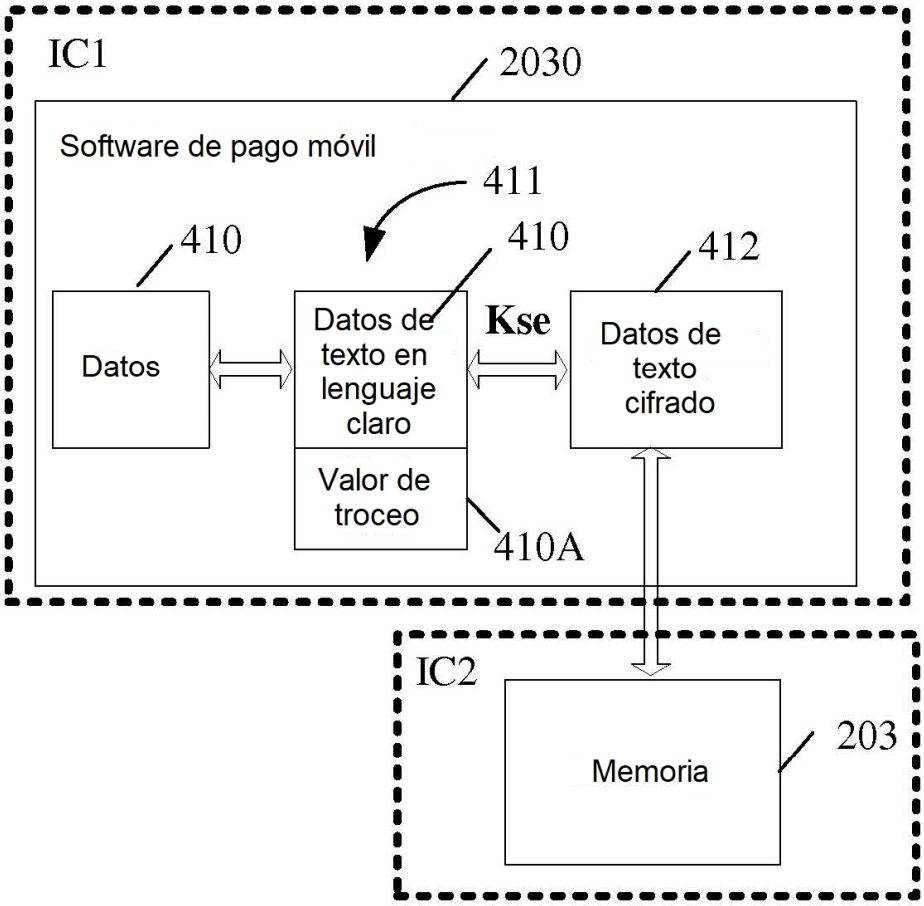
IC1
2030
Software de pago móvil
411
410
410
412
Datos
Datos de texto en lenguaje claro
Kse
Datos de texto cifrado
Valor de troceo
410A
IC2
Memoria
203

FIG. 5

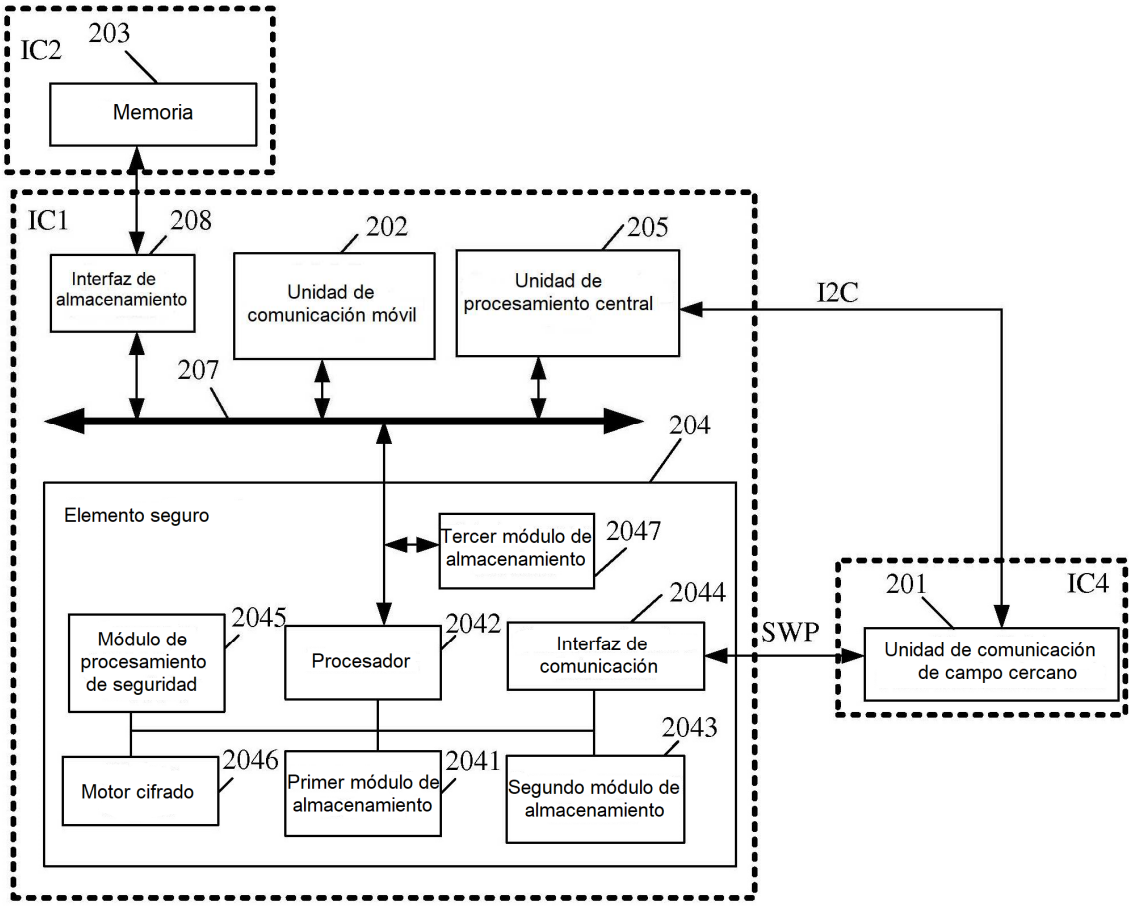
IC2
203
Memoria
IC1
208
202
205
Interfaz de almacenamiento
Unidad de comunicación móvil
Unidad de procesamiento central
I2C
207
204
Elemento seguro
Tercer módulo de almacenamiento
2047
2044
201
IC4
2045
2042
Módulo de procesamiento de seguridad
Procesador
Interfaz de comunicación
SWP
Unidad de comunicación de campo cercano
2043
2046
2041
Motor cifrado
Primer módulo de almacenamiento
Segundo módulo de almacenamiento

FIG. 6

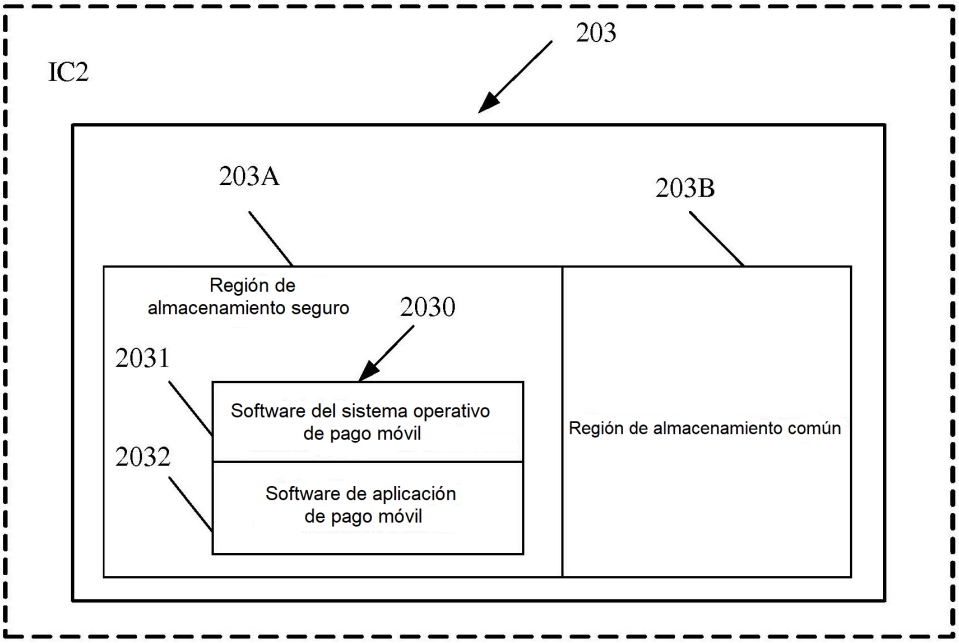
IC2
203
203A
203B
Región de almacenamiento seguro
2030
2031
Software del sistema operativo de pago móvil
2032
Software de aplicación de pago móvil
Región de almacenamiento común

FIG. 7

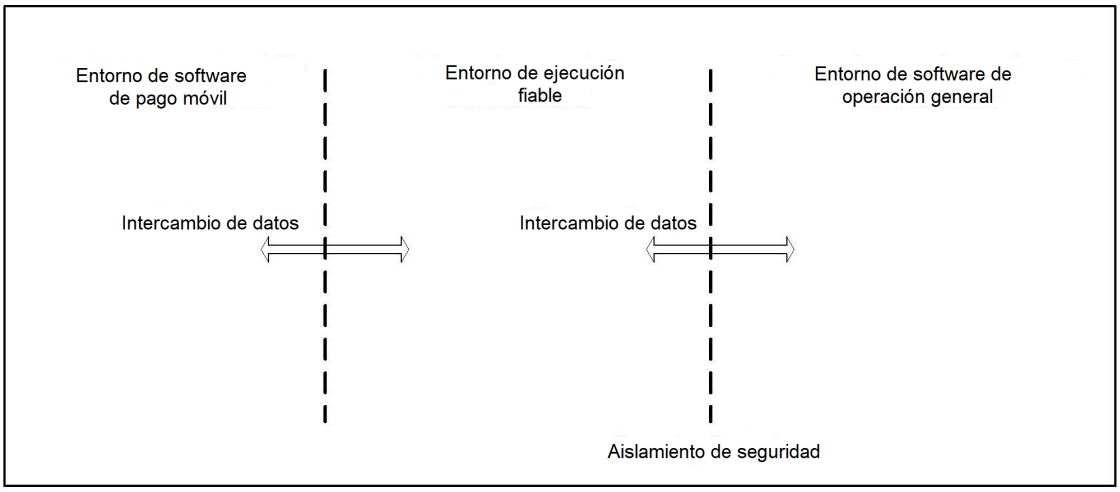
Entorno de software de pago móvil
Entorno de ejecución fiable
Entorno de software de operación general
Intercambio de datos
Intercambio de datos
Aislamiento de seguridad

FIG. 8