(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 761 345**

(51) Int. CI.:

H04W 12/06 (2009.01)
H04W 12/04 (2009.01)
G06Q 20/32 (2012.01)
G06Q 20/38 (2012.01)
H04W 12/00 (2009.01)
G06Q 20/34 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **21.03.2013 PCT/US2013/033322**

(87) Fecha y número de publicación internacional: **10.10.2013 WO13151797**

(96) Fecha de presentación y número de la solicitud europea: **21.03.2013 E 13772978 (6)**

(97) Fecha y número de publicación de la concesión europea: **06.11.2019 EP 2835004**

(54) Título: **Sistemas y métodos para procesar pagos móviles proporcionando credenciales a dispositivos móviles sin elementos seguros**

(30) Prioridad:

02.04.2012 US 201261619095 P
18.04.2012 US 201261635248 P
10.12.2012 US 201261735383 P
07.02.2013 US 201361762098 P
14.03.2013 US 201313827042

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
19.05.2020

(73) Titular/es:

MASTERCARD INTERNATIONAL INCORPORATED (100.0%)
2000 Purchase Street
Purchase, NY 10577, US

(72) Inventor/es:

COLLINGE, MEHDI;
THOMPSON, SUSAN;
SMETS, PATRIK;
ROBERTS, DAVID ANTHONY y
WARD, MICHAEL CHRISTOPHER

(74) Agente/Representante:

ISERN JARA, Jorge

DESCRIPCIÓN

Sistemas y métodos para procesar pagos móviles proporcionando credenciales a dispositivos móviles sin elementos seguros

Solicitudes relacionadas

Esta solicitud reivindica el beneficio de prioridad de la Solicitud Provisional de Estados Unidos cedida comúnmente N.º 61/619.095, presentada el 2 de abril de 2012, titulada "Method and System for Processing Mobile Payments for Devices Without Secure Elements"; Solicitud Provisional de Estados Unidos N.º 61/639.248, presentada el 18 de abril de 2012, titulada "Method and System for Processing Mobile Payments by Provisioning Credentials to Mobile Devices Without Secure Elements"; Solicitud Provisional de Estados Unidos N.º 61/735.383, presentada el 10 de diciembre de 2012, titulada "Systems and Methods for Processing Mobile Payments by Provisioning Credentials to Mobile Devices Without Secure Elements", por Mehdi Collinge et al.; Solicitud Provisional de Estados Unidos N.º 61/762.098, presentada el 7 de febrero de 2013, titulada "Systems and Methods for Processing Mobile Payments by Provisioning Credentials to Mobile Devices Without Secure Elements", por Mehdi Collinge et al.; y Solicitud de Patente de Estados Unidos N.º 13/827.042, presentada el 14 de marzo de 2013, titulada "Systems and Methods for Processing Mobile Payments by Provisioning Credentials to Mobile Devices Without Secure Elements", por Mehdi Collinge et al.

Campo

La presente divulgación se refiere a la provisión de credenciales de pago a un dispositivo móvil que carece de un elemento seguro, específicamente la provisión y almacenamiento de credenciales de pago para su uso en la realización de una transacción financiera de campo cercano usando un dispositivo móvil que carece de un elemento seguro.

Antecedentes

Avances tanto en tecnologías móviles como de comunicación han creado grandes oportunidades, una de las cuales es proporcionar a usuario de los dispositivos informático móviles la capacidad de iniciar transacciones de pago usando su dispositivo móvil. Un enfoque de este tipo para habilitar que dispositivos móviles lleven a cabo transacciones de pago ha sido el uso de tecnología de comunicación de campo cercano (NFC) para transmitir de forma segura información de pago a un terminal punto de venta sin contacto cercano. Para conseguir esto, se usan teléfonos móviles con hardware de elemento seguro (por ejemplo, un chip de elemento seguro) para almacenar de forma segura credenciales de cuentas de pago, tal como credenciales de tarjeta de crédito.

Sin embargo, no todos dispositivos móviles tienen elementos seguros. Adicionalmente, algunos emisores pueden no tener acceso a un elemento seguro en un dispositivo móvil, incluso si el dispositivo móvil tiene uno disponible. Como resultado, un consumidor que tiene un dispositivo móvil con capacidad NFC puede no ser capaz de usar su dispositivo para llevar a cabo transacciones de pago si su dispositivo móvil carece de un elemento seguro, e incluso en algunos casos en los que su dispositivo móvil tiene un elemento seguro.

Por lo tanto, existe una necesidad de una solución técnica para habilitar que un dispositivo móvil que carece de un elemento seguro lleve a cabo transacciones de pago sin contacto.

El documento US2008040285 divulga un método y aparato para llevar a cabo una transacción segura que implica la generación de un código de autenticación dinámico en un dispositivo móvil, basándose en datos secretos que no identifican una cuenta. El código de autenticación e información de identificación de cuenta financiera se transmiten a una entidad de validación, que comparte información acerca de los datos secretos, para autorizar la transacción.

Sumario

La presente divulgación proporciona una descripción de sistemas y métodos para la provisión de credenciales de pago a dispositivos móviles que carecen de elementos seguros para su uso en transacciones de pago móviles.

De acuerdo con la reivindicación independiente 1, se proporciona un método para generar y proporcionar credenciales de pago a un dispositivo móvil que carece de un elemento seguro, que comprende: generar, por un dispositivo de procesamiento de un sistema remoto, un perfil de tarjeta asociado con una cuenta de pago, en el que el perfil de tarjeta incluye al menos credenciales de pago que corresponden a la cuenta de pago asociada y un identificador de perfil; proporcionar, por el sistema remoto, a un dispositivo móvil, el perfil de tarjeta generado; recibir, por el sistema remoto, desde el dispositivo móvil, una petición de clave, en el que la petición de clave incluye al menos un número de identificación personal, PIN, móvil y el identificador de perfil; en respuesta a recibir la petición de clave desde el dispositivo móvil, determinar, por un dispositivo de autenticación del sistema remoto, si el PIN móvil es auténtico; basándose en la determinación de autenticidad del PIN móvil generar, por el dispositivo de procesamiento del sistema remoto, una clave de un solo uso, en el que (i) la clave de un solo uso se configura para usarse una vez, por el dispositivo móvil, para generar un criptograma de pago válido para una única transacción financiera y (ii) la clave de

un solo uso incluye al menos el identificador de perfil, un contador de transacción de aplicación y una clave de generación; y transmitir, por un dispositivo de transmisión del sistema remoto, la clave de un solo uso generada al dispositivo móvil, en el que el dispositivo móvil carece de un elemento seguro.

De acuerdo con la reivindicación independiente 7, se proporciona un método para generar un criptograma de pago en un dispositivo móvil que carece de un elemento seguro, que comprende: recibir, por un dispositivo de recepción del dispositivo móvil, un perfil de tarjeta desde un sistema remoto, en el que el perfil de tarjeta incluye al menos credenciales de pago que corresponden a una cuenta de pago y un identificador de perfil; recibir, por un dispositivo de entrada del dispositivo móvil, un número de identificación personal, PIN, móvil introducido por un usuario del dispositivo móvil; transmitir, por un dispositivo de transmisión del dispositivo móvil, una petición de clave al sistema remoto, en el que la petición de clave incluye al menos el identificador de perfil y un número de identificación personal, PIN, móvil en el que dicha petición de clave provoca que dicho dispositivo remoto genere una clave de un solo uso; recibir, por el dispositivo de recepción del dispositivo móvil, la clave de un solo uso desde el sistema remoto, en el que la clave de un solo uso (i) se configura para usarse una vez, por el dispositivo móvil, para generar un criptograma de pago válido para una única transacción financiera y (ii) la clave de un solo uso incluye al menos un contador de transacción de aplicación, una clave de generación y el identificador de perfil; generar, por un dispositivo de procesamiento del dispositivo móvil, el criptograma de pago válido para la única transacción financiera basándose en al menos la clave de un solo uso recibida y el PIN móvil; y transmitir, por el dispositivo móvil, a través de comunicación de campo cercano, al menos las credenciales de pago y el criptograma de pago generado a un terminal punto de venta para su uso en una transacción financiera.

Otro método para generar y proporcionar credenciales de pago a un dispositivo móvil que carece de un elemento seguro incluye: almacenar, en una base de datos, al menos una clave de almacenamiento, una pluralidad de claves de código de validación de tarjeta dinámico y un contador de transacción de aplicación asociado con un programa de aplicación móvil; proporcionar, al dispositivo móvil, al menos la clave de almacenamiento, un componente de autenticación y credenciales de pago estáticas, en el que las credenciales de pago estáticas se asocian con una cuenta de pago; recibir, desde un dispositivo móvil, un testigo de programa de autenticación de chip (CAP); validar, por un dispositivo de validación, la autenticidad del testigo de CAP recibido; generar, por un dispositivo de procesamiento, un número impredecible de clave de sesión (KS_{UN}); generar, por el dispositivo de procesamiento, un número impredecible en la nube (UN_{NUBE}); identificar, por el dispositivo de procesamiento, una carga útil encriptada basándose en una clave de código de validación de tarjeta dinámico derivado (KD_{CVC3}), en el que la carga útil encriptada incluye al menos una clave de código de validación de tarjeta dinámico de la pluralidad de claves de código de validación de tarjeta dinámico, el KS_{UN} y el contador de transacción de aplicación; transmitir, por un dispositivo de transmisión, la carga útil encriptada al dispositivo móvil para su uso en la generación de un código de validación de tarjeta dinámico para su uso en una transacción financiera; y transmitir, por el dispositivo de transmisión, al menos el KSUN, UN_{NUBE} y contador de transacción de aplicación a un emisor asociado con la cuenta de pago para su uso en la validación del código de validación de tarjeta dinámico generado usado en la transacción financiera.

Un método para generar un código de validación de tarjeta dinámico en un dispositivo móvil que carece de un elemento seguro incluye: recibir, por un dispositivo de recepción, al menos una clave de almacenamiento, un componente de autenticación y credenciales de pago estáticas; recibir, por un dispositivo de entrada, al menos una credencial adicional; generar, por un dispositivo de procesamiento, un testigo de programa de autenticación de chip (CAP), en el que el testigo de CAP se basa en al menos el componente de autenticación y la al menos una credencial adicional; transmitir, por un dispositivo de transmisión, el testigo de CAP generado; recibir, por el dispositivo de recepción, una carga útil encriptada, en el que la carga útil encriptada incluye al menos un código de validación de tarjeta dinámico proporcionado, número impredecible de clave de sesión y contador de transacción de aplicación; desencriptar, por el dispositivo de procesamiento, la carga útil encriptada usando al menos la clave de almacenamiento recibida; recibir, a través de comunicación de campo cercano, un número impredecible de lector desde un terminal punto de venta; generar, por el dispositivo de procesamiento, un código de validación de tarjeta dinámico de pago basándose en al menos el código de validación de tarjeta dinámico proporcionado, el número impredecible de clave de sesión, el contador de transacción de aplicación y el número impredecible de lector; y transmitir, a través de comunicación de campo cercano, el código de validación de tarjeta dinámico de pago generado y el contador de transacción de aplicación al terminal punto de venta para incluir en una petición de autorización para una transacción financiera.

De acuerdo con la reivindicación independiente 14, se proporciona un sistema para generar y proporcionar credenciales de pago a un dispositivo móvil que carece de un elemento seguro, que comprende: un dispositivo de transmisión de un sistema remoto; un dispositivo de procesamiento, del sistema remoto configurado para generar un perfil de tarjeta asociado con una cuenta de pago, en el que el perfil de tarjeta incluye al menos credenciales de pago que corresponden a la cuenta de pago asociada y un identificador de perfil; un dispositivo de aprovisionamiento, del sistema remoto, configurado para proporcionar, a un dispositivo móvil que carece de un elemento seguro, el perfil de tarjeta generado; un dispositivo de recepción, del sistema remoto, configurado para recibir, desde el dispositivo móvil, una petición de clave, en el que la petición de clave incluye al menos un número de identificación personal, PIN, móvil y el identificador de perfil; y un dispositivo de autenticación, del sistema remoto, configurado para autenticar el PIN móvil en respuesta a recibir la petición de clave, en el que el dispositivo de procesamiento, del sistema remoto, se configura adicionalmente para generar una clave de un solo uso sobre una base de autenticidad de PIN móvil, en el que la clave de un solo uso (i) se configura para usarse una vez, por el dispositivo móvil, para generar un criptograma

de pago válido para una única transacción financiera e (ii) incluye al menos el identificador de perfil, un contador de transacción de aplicación y una clave de generación para su uso en la generación del criptograma de pago válido para la única transacción financiera, y el dispositivo de transmisión, del sistema remoto, se configura para transmitir la clave de un solo uso generada al dispositivo móvil.

De acuerdo con la reivindicación independiente 19, se proporciona un sistema para generar un criptograma de pago en un dispositivo móvil que carece de un elemento seguro, que comprende: un dispositivo de procesamiento, del dispositivo móvil; un dispositivo de recepción, del dispositivo móvil, configurado para recibir un perfil de tarjeta desde un sistema remoto, en el que el perfil de tarjeta incluye al menos credenciales de pago que corresponden a una cuenta de pago y un identificador de perfil; un dispositivo de entrada, del dispositivo móvil, configurado para recibir un número de identificación personal, PIN, móvil introducido por un usuario del dispositivo móvil; y un dispositivo de transmisión, del dispositivo móvil, configurado para transmitir una petición de clave al sistema remoto, en el que la petición de clave (i) incluye al menos el identificador de perfil y un número de identificación personal, PIN, móvil y (ii) provoca que dicho dispositivo remoto genere una clave de un solo uso, en el que el dispositivo de recepción, del dispositivo móvil, se configura adicionalmente para recibir la clave de un solo uso desde el sistema remoto, en el que la clave de un solo uso (i) se configura para usarse una vez, por el dispositivo móvil, para generar un criptograma de pago válido para una única transacción financiera y (ii) la clave de un solo uso incluye al menos un contador de transacción de aplicación, una clave de generación y el identificador de perfil, el dispositivo de procesamiento, del dispositivo móvil, se configura para generar el criptograma de pago válido para la única transacción financiera basándose en al menos la clave de un solo uso recibida y el PIN móvil, y el dispositivo de transmisión, del dispositivo móvil, se configura adicionalmente para transmitir, a través de comunicación de campo cercano, al menos las credenciales de pago y el criptograma de pago generado a un terminal punto de venta para su uso en una transacción financiera.

Otro sistema para generar y proporcionar credenciales de pago a un dispositivo móvil que carece de un elemento seguro incluye una base de datos, un dispositivo de aprovisionamiento, un dispositivo de recepción, un dispositivo de procesamiento y un dispositivo de transmisión. La base de datos se configura para almacenar al menos una clave de almacenamiento, una pluralidad de claves de código de validación de tarjeta dinámico y un contador de transacción de aplicación asociado con un programa de aplicación móvil. El dispositivo de aprovisionamiento se configura para proporcionar, al dispositivo móvil, al menos la clave de almacenamiento, un componente de autenticación y credenciales de pago estáticas, en el que las credenciales de pago estáticas se asocian con una cuenta de pago. El dispositivo de recepción se configura para recibir, desde un dispositivo móvil, un testigo de programa de autenticación de chip (CAP). El dispositivo de procesamiento se configura para: validar la autenticidad del testigo de CAP recibido; generar un número impredecible de clave de sesión (KS_{UN}); generar un número impredecible en la nube (UN_{NUBE}); e identificar una carga útil encriptada basándose en una clave de código de validación de tarjeta dinámico derivado (KD_{CVC3}), en el que la carga útil encriptada incluye al menos una clave de código de validación de tarjeta dinámico de la pluralidad de claves de código de validación de tarjeta dinámico, el KS_{UN} y el contador de transacción de aplicación. El dispositivo de transmisión se configura para: transmitir la carga útil encriptada al dispositivo móvil para su uso en la generación de un código de validación de tarjeta dinámico para su uso en una transacción financiera; y transmitir al menos el KSUN, UN_{NUBE} y contador de transacción de aplicación a un emisor asociado con la cuenta de pago para su uso en la validación del código de validación de tarjeta dinámico generado usado en la transacción financiera.

Un sistema para generar un código de validación de tarjeta dinámico en un dispositivo móvil que carece de un elemento seguro incluye un dispositivo de recepción, un dispositivo de entrada, un dispositivo de procesamiento y un dispositivo de transmisión. El dispositivo de recepción se configura para recibir al menos una clave de almacenamiento, un componente de autenticación y credenciales de pago estáticas. El dispositivo de entrada se configura para recibir al menos una credencial adicional. El dispositivo de procesamiento se configura para generar un testigo de programa de autenticación de chip (CAP), en el que el testigo de CAP se basa en al menos el componente de autenticación y la al menos una credencial adicional. El dispositivo de transmisión se configura para transmitir el testigo de CAP generado. El dispositivo de recepción se configura adicionalmente para recibir una carga útil encriptada, en el que la carga útil encriptada incluye al menos un código de validación de tarjeta dinámico proporcionado, número impredecible de clave de sesión y contador de transacción de aplicación. El dispositivo de procesamiento se configura adicionalmente para desencriptar la carga útil encriptada usando al menos la clave de almacenamiento recibida. El dispositivo de recepción se configura adicionalmente para recibir, a través de comunicación de campo cercano, un número impredecible de lector desde un terminal punto de venta. El dispositivo de procesamiento se configura adicionalmente para generar un código de validación de tarjeta dinámico de pago basándose en al menos el código de validación de tarjeta dinámico proporcionado, el número impredecible de clave de sesión, el contador de transacción de aplicación y el número impredecible de lector. El dispositivo de transmisión se configura adicionalmente para transmitir, a través de comunicación de campo cercano, el código de validación de tarjeta dinámico de pago generado y el contador de transacción de aplicación al terminal punto de venta para incluir en una petición de autorización para una transacción financiera.

Las realizaciones y/o ejemplos divulgados en la siguiente descripción que no están cubiertos por las reivindicaciones adjuntas se consideran que no son parte de la presente invención.

Breve descripción de las figuras de los dibujos

El alcance de la presente divulgación se entiende mejor a partir de la siguiente descripción detallada de realizaciones ilustrativas cuando se leen en conjunción con los dibujos adjuntos. En los dibujos se incluyen las siguientes figuras:

La Figura 1 en un diagrama de nivel alto que ilustra un sistema para generar y proporcionar credenciales de pago a un dispositivo móvil de acuerdo con realizaciones ilustrativas.
La Figura 2 es un diagrama de bloques que ilustra la carga útil de testigo de pago del sistema de la Figura 1 de acuerdo con realizaciones ilustrativas.
La Figura 3 en un diagrama de nivel alto que ilustra un sistema alternativo para proporcionar credenciales de pago a un dispositivo móvil de acuerdo con realizaciones ilustrativas.
La Figura 4 es un diagrama que ilustra un método para comunicación de canal dual para su uso en el sistema de la Figura 1 de acuerdo con realizaciones ilustrativas.
La Figura 5 es un diagrama de flujo que ilustra la experiencia de un usuario del dispositivo móvil del sistema de la Figura 1 de acuerdo con realizaciones ilustrativas.
La Figura 6 en un diagrama de nivel alto que ilustra métodos para proporcionar credenciales de pago a un dispositivo móvil y generar un criptograma de pago de acuerdo con realizaciones ilustrativas.
La Figura 7 en un diagrama de nivel alto que ilustra métodos para proporcionar credenciales de pago a un dispositivo móvil y generar un código de validación de tarjeta dinámico de acuerdo con realizaciones ilustrativas.
La Figura 8 es un diagrama de flujo que ilustra un método para el registro de un dispositivo móvil para su uso en el sistema de la Figura 1 de acuerdo con realizaciones ilustrativas.
La Figura 9 es un diagrama de flujo que ilustra un método para la inicialización de un programa de aplicación móvil en el dispositivo móvil del sistema de la Figura 1 de acuerdo con realizaciones ilustrativas.
La Figura 10 es un diagrama de flujo que ilustra un método para gestión remota del programa de aplicación móvil del dispositivo móvil de acuerdo con realizaciones ilustrativas.
La Figura 11 es un diagrama de flujo que ilustra un método para la distribución de un perfil de tarjeta al dispositivo móvil del sistema de la Figura 1 de acuerdo con realizaciones ilustrativas.
La Figura 12 es un diagrama de flujo que ilustra un método para la distribución de una clave de un solo uso al dispositivo móvil del sistema de la Figura 1 de acuerdo con realizaciones ilustrativas.
La Figura 13 es un diagrama de flujo que ilustra un método para gestionar el programa de aplicación móvil a continuación de la actualización de un número de identificación personal móvil del dispositivo móvil del sistema de la Figura 1 de acuerdo con realizaciones ilustrativas.
La Figura 14 es un diagrama de flujo que ilustra un método para llevar a cabo a transacción de pago usando el dispositivo móvil del sistema de la Figura 1 de acuerdo con realizaciones ilustrativas.
La Figura 15 es un diagrama de flujo que ilustra un método ilustrativo para generar y proporcionar credenciales de pago a un dispositivo móvil que carece de un elemento seguro de acuerdo con realizaciones ilustrativas.
La Figura 16 es un diagrama de flujo que ilustra un método ilustrativo para generar un criptograma de pago en un dispositivo móvil que carece de un elemento seguro de acuerdo con realizaciones ilustrativas.
La Figura 17 es un diagrama de flujo que ilustra un método alternativo para generar y proporcionar credenciales de pago a un dispositivo móvil que carece de un elemento seguro de acuerdo con realizaciones ilustrativas.
La Figura 18 es un diagrama de flujo que ilustra un método ilustrativo para generar un código de validación de tarjeta dinámico en un dispositivo móvil que carece de un elemento seguro de acuerdo con realizaciones ilustrativas.
La Figura 19 es un diagrama de bloques que ilustra un sistema informático arquitectura de acuerdo con realizaciones ilustrativas.

Adicionalmente áreas de aplicabilidad de la presente divulgación serán evidentes a partir de la descripción detallada proporcionada en lo sucesivo. Debería entenderse que la descripción detallada de realizaciones ilustrativas se concibe para propósitos de ilustración únicamente y no se concibe, por lo tanto, para limitar necesariamente el alcance de la divulgación.

Descripción detallada

Definición de términos

Red de pago - Un sistema o red usada para la transferencia de dinero a través del uso de sustitutos de dinero en efectivo. Redes de pago pueden usar una diversidad de diferentes protocolos y procedimientos para procesar la transferencia de dinero para diversos tipos de transacciones. Transacciones que pueden realizarse a través de una red de pago pueden incluir compras de productos o servicios, compras a crédito, transacciones de débito, transferencia de fondos, retiradas de cuenta, etc. Redes de pago pueden configurarse para realizar transacciones a través de sustitutos de dinero en efectivo, que pueden incluir tarjetas de pago, letras de crédito, cuentas financieras, etc. Ejemplos de redes o sistemas configurados para funcionar como redes de pago incluyen las operadas por MasterCard®, VISA®, Discover®, American Express®, etc.

Cuenta de pago - Una cuenta financiera que puede usarse para financiar una transacción, tal como una cuenta corriente, cuenta de ahorros, cuenta de crédito, cuenta de pago virtual, etc. Una cuenta de pago puede asociarse con una entidad, que puede incluir una persona, familia, empresa, corporación, entidad gubernamental, etc. En algunos casos, una cuenta de pago puede ser virtual, tal como las cuentas operadas por PayPal®, etc.

Tarjeta de crédito - Una tarjeta o datos asociados con una cuenta de pago que puede proporcionarse a un comerciante para financiar una transacción financiera a través de la cuenta de pago asociada. Tarjetas de pago pueden incluir tarjetas de crédito, tarjetas de débito, tarjetas de débito diferido, tarjetas de valor almacenado, tarjetas de prepago, tarjetas de flota, números de pago virtual, números de tarjeta virtual, números de pago controlado, etc. Una tarjeta de pago puede ser una tarjeta física que puede proporcionarse a un comerciante, o puede ser datos que representan la cuenta de pago asociada (por ejemplo, como se almacena en un dispositivo de comunicación, tal como un teléfono inteligente u ordenador). Por ejemplo, en algunos casos, datos que incluyen un número de cuenta de pago pueden considerarse una tarjeta de pago para el procesamiento de una transacción financiada por la cuenta de pago asociada. En algunos casos, un cheque puede considerarse una tarjeta de pago donde sea aplicable.

Sistema para generar y proporcionar credenciales de pago

La Figura 1 es un diagrama que ilustra un sistema 100 para la generación y provisión de credenciales de pago a un dispositivo móvil que carece de un elemento seguro.

El sistema 100 puede incluir un usuario 102. El usuario 102 puede poseer un dispositivo móvil 104. El dispositivo móvil 104 puede ser cualquier tipo de dispositivo informático móvil adecuado para realizar las funciones como se describen en este documento, tal como un teléfono celular, teléfono inteligente, ordenador de tableta, asistente digital personal, etc. En una realización ilustrativa, el dispositivo móvil 104 puede no incluir un elemento seguro.

El dispositivo móvil 104 puede incluir una aplicación de pago móvil 106, que puede ser un programa de aplicación almacenado en almacenamiento de datos del dispositivo móvil 104 y ejecutado por un procesador incluido en el dispositivo móvil 104. La aplicación de pago móvil 106 puede configurarse para recibir y almacenar credenciales de pago y llevar a cabo transacciones de pago a través de comunicación de campo cercano sin el uso de un elemento seguro, como se ha analizado en más detalle en este documento.

El usuario 102 puede tener una cuenta de pago con un emisor 108, tal como una cuenta de tarjeta de crédito. El usuario 102 puede desear usar su dispositivo móvil 104 para llevar a cabo transacciones de pago usando su cuenta de pago con el emisor 108 para la financiación de las transacciones. Credenciales de pago que corresponden a la cuenta de pago pueden almacenarse por un sistema de SE remoto (elemento seguro remoto) 110 para proporcionarse al dispositivo móvil 104. El sistema de SE remoto 110 puede incluir al menos un servicio de gestión de credenciales de pago 112 y un servidor de notificación remoto 114, cada uno de los cuales se analiza en más detalle a continuación.

El sistema de SE remoto 110 puede crear una carga útil de testigo de pago para proporcionar las credenciales de pago al dispositivo móvil 104 para su uso en una transacción de pago. La carga útil de testigo de pago (PTP) puede ser un contenedor usado para transportar credenciales de pago desde el sistema de SE remoto 100 a la aplicación de pago móvil 106 en el dispositivo móvil 104. La carga útil de testigo de pago puede incluir un perfil de tarjeta 116 y una clave de un solo uso 118, analizados en más detalle a continuación. El perfil de tarjeta 116 puede incluir las credenciales de pago, y la clave de un solo uso 118 puede ser una clave de un solo uso (por ejemplo, uso de una única vez) usada para generar un criptograma de pago válido para una única transacción de pago. En algunas realizaciones, el sistema de SE remoto 110 y el dispositivo móvil 104 pueden comunicarse usando comunicación de canal dual, analizada en más detalle a continuación.

El dispositivo móvil 104 puede configurarse adicionalmente para transmitir un criptograma de pago generado y credenciales de pago a un terminal punto de venta 120 en un comerciante. El terminal punto de venta 120 puede ser cualquier tipo de terminal punto de venta o dispositivo adecuado para recibir credenciales de pago a través de comunicación de campo cercano (NFC). Métodos y protocolos adecuados para la transmisión segura de información a través de NFC serán evidentes para expertos en la materia. El terminal punto de venta 120 puede transmitir las credenciales de pago recibidas y otra información de transacción (por ejemplo, cantidad de transacción, detalles de producto, etc.) a un adquirente 122, tal como un banco adquirente.

El adquirente 122 puede enviar una petición de autorización para la transacción de pago a una red de pago 124. La red de pago 124 puede configurarse para procesar la petición de autorización, tal como consultando al emisor 108 para aprobación de la transacción de pago (por ejemplo, basándose en fondos o créditos en la cuenta de pago). La red de pago 124 puede enviar a continuación una respuesta de autorización al adquirente 122 y/o al comerciante, que puede finalizar a continuación la transacción de pago con el usuario 102. Métodos y sistemas adecuados para el procesamiento de una transacción financiera serán evidentes para un experto en la materia.

El sistema 100 y el uso de la carga útil de testigo de pago pueden habilitar que el usuario 102 use el dispositivo móvil 104 para llevar a cabo transacciones de pago NFC sin el uso de un elemento seguro.

Carga útil de testigo de pago

La Figura 2 es un diagrama que ilustra la carga útil de testigo de pago proporcionado al dispositivo móvil 104 en detalle adicional.

Como se ha analizado anteriormente, la carga útil de testigo de pago puede incluir el perfil de tarjeta 116 y la clave de un solo uso 118. El perfil de tarjeta 116 puede incluir credenciales de pago proporcionadas a la aplicación de pago móvil 106 por el sistema de SE remoto para su uso en la realización de transacciones de pago. Las credenciales de pago incluidas en el perfil de tarjeta 116 pueden incluir credenciales de pago comunes 202, banda magnética (banda mag.) credenciales de pago 204 y credenciales de pago de m/chip 206.

Las credenciales de pago comunes 202 pueden incluir todos los elementos de datos comunes a cualquier tipo de transacciones de pago, tal como tanto transacciones de pago de banda mag. como de m/chip. Tales elementos de datos pueden incluir número de cuenta de pago, datos de seguimiento y datos de descripción de configuración de tarjeta. Las credenciales de pago de banda mag. 204 pueden incluir elementos de datos específicos para transacciones de banda mag., tal como el número de dígitos en un contador de transacción de aplicación y un mapa de bits para un número impredecible y el contador de transacción de aplicación. Las credenciales de pago de m/chip 206 pueden incluir elementos de datos específicos para transacciones de pago de o m/chip, tal como códigos de acción de emisor, datos de gestión de riesgo y listas de objetos de autenticación de datos fuera de línea. En algunas realizaciones, las credenciales de pago de banda mag. 204 pueden ser obligatorias en el perfil de tarjeta 116 y las credenciales de pago de m/chip 206 pueden ser opcionales.

La clave de un solo uso 118 puede ser un testigo de pago usado una vez para generar un criptograma de pago a usar en una transacción de pago. La clave de un solo uso puede incluir un contador de transacción de aplicación (ATC) y una clave de generación 208. El contador de transacción de aplicación puede ser un recuento de transacciones usado para gestión de fraude y autenticación como será evidente para expertos en la materia. La clave de generación 208 puede ser una clave usada para generar un criptograma de pago usado en una transacción financiera. En una realización, la clave de generación 208 puede generar un código de validación de tarjeta dinámico (CVC3) o un criptograma de aplicación (AC). En una realización adicional, el criptograma de aplicación puede ser opcional.

La clave de un solo uso 118 también puede incluir un identificador usado para identificar el perfil de tarjeta 116 al que corresponde. En algunas realizaciones, la clave de un solo uso 118 puede protegerse basándose en un valor de número de identificación personal (PIN) móvil. En una realización de este tipo, el usuario 102 puede proporcionar un PIN móvil para autenticación. Si el PIN móvil proporcionado es incorrecto, un valor incorrecto de la clave de un solo uso puede usarse por la aplicación de pago móvil 106. En un ejemplo de este tipo, el emisor 108 no autorizará la transacción de pago. Una realización de este tipo puede resultar en seguridad adicional para el usuario 102, el emisor 108 y el comerciante implicados en la transacción de pago.

Sistema alternativo para generar y proporcionar credenciales de pago

La Figura 3 ilustra un sistema alternativo 300 para generar y proporcionar credenciales de pago al dispositivo móvil 104 que carece de un elemento seguro.

En el sistema 300, el dispositivo móvil 104 puede incluir la aplicación de pago móvil 106. El dispositivo móvil 104 también puede incluir el almacenamiento 304, tal como una base de datos. El sistema de SE remoto 110 puede incluir un sistema en la nube 302. El sistema en la nube 302 puede almacenar claves, credenciales de pago y un contador de transacción de aplicación, que pueden proporcionarse desde el sistema en la nube 302 al dispositivo móvil 104 y almacenarse en el almacenamiento 304.

El dispositivo móvil 104 puede generar un testigo de programa de autenticación de chip (CAP). La generación y uso de testigos de CAP será evidente para un experto en la materia. El dispositivo móvil 104 puede transmitir el testigo de CAP generado al sistema en la nube 302. El sistema en la nube 302 puede autenticar a continuación (por ejemplo, validar) el testigo de CAP, tal como usando un sistema de validación de testigo de CAP como será evidente para expertos en la materia. El sistema en la nube 302 puede generar a continuación números impredecibles, y puede generar una carga útil encriptada que incluye una clave de código de validación de tarjeta dinámico derivado (KD_{CVC3}) y el número impredecible generado. El sistema en la nube 302 también puede transmitir al menos parte de la información al emisor 108. El emisor 108 puede almacenar la información recibida en un emisor base de datos 310.

La carga útil encriptada puede transmitirse al dispositivo móvil 104, que puede desencriptar la carga útil y generar a continuación un código de validación de tarjeta dinámico basándose en la información incluida en la carga útil encriptada y credenciales de pago almacenadas. El usuario 102 puede comprar en un comerciante 306, y, cuando se han seleccionado bienes o servicios para adquirir, puede transmitir las credenciales de pago y código de validación de tarjeta dinámico desde el dispositivo móvil 104 al terminal punto de venta 120. El terminal punto de venta 120 puede transmitir la información e información de transacción relevante al adquirente 122.

Un servidor de procesamiento de adquirente 312 puede recibir la información en el adquirente 122 y puede generar y enviar una petición de autorización para la transacción financiera que incluye las credenciales de pago y código de validación de tarjeta dinámico a la red de pago 124. La red de pago 124 puede reenviar información relevante al emisor 108 para autorización de la transacción para una cantidad de transacción específica. El emisor 108 puede incluir un servidor de procesamiento de emisor 308. El servidor de procesamiento de emisor 308 puede autenticar el código de

validación de tarjeta dinámico basándose en la información almacenada en la base de datos de emisor 310 y recibida desde el sistema en la nube 302. El emisor 108 puede, basándose en la autenticación, aprobar o denegar a continuación la transacción de pago.

El emisor 108 puede enviar una respuesta a la red de pago 124, que puede enviar a continuación una respuesta de autorización al adquirente 122. El adquirente puede informar al comerciante 306 de los resultados de la autorización, que puede finalizar a continuación la transacción con el titular de la tarjeta 102. Métodos para proporcionar credenciales de pago al dispositivo móvil 104 y para procesar a transacción de pago a través del dispositivo móvil 104 se analizan en más detalle a continuación.

Comunicación de canal dual

La Figura 4 ilustra un método para comunicación de canal dual para su uso en el sistema 100 de la Figura 1 para comunicación entre el dispositivo móvil 104 y el sistema de SE remoto 110. Comunicación de canal dual puede habilitar que el dispositivo móvil 104 y el sistema de SE remoto 110 se comuniquen usando múltiples protocolos, que puede permitir transmisiones más rápidas y/o más seguras entre los dos sistemas.

Comunicación de canal dual puede incluir usar notificación remota 402 como un primer canal y autenticación mutua 404 como un segundo canal. La notificación remota 402 puede realizarse entre el servicio de notificación remota 114 y el dispositivo móvil 104. En algunas realizaciones, el servicio de gestión de credenciales de pago 112 puede generar información, tal como la clave de un solo uso 118, a proporcionar a la aplicación de pago móvil 106. El servicio de gestión de credenciales de pago 112 puede generar un mensaje que incluye la clave de un solo uso encriptada con una clave aleatoria a proporcionarse y puede encriptar el mensaje usando la clave móvil.

El servicio de notificación remota 114 puede transmitir a continuación el mensaje al dispositivo móvil 104 usando notificación remota. El dispositivo móvil 104 puede proporcionar el mensaje a la aplicación de pago móvil 106, que puede desencriptar a continuación el mensaje usando la clave móvil compartida y, a continuación, puede desencriptar la clave de un solo uso encriptada con la clave aleatoria y, por lo tanto, usar la clave de un solo uso en una transacción de pago. Métodos para transmisión de mensaje usando notificación remota serán evidentes para un experto en la materia.

Puede usarse la autenticación mutua 404 en casos en los que puede desearse seguridad adicional, tal como en la formación de una conexión inicial entre el dispositivo móvil 104 y el sistema de SE remoto 110. La autenticación mutua 404 puede usar comunicación SSL/TLS para autenticar el sistema de SE remoto 110 al dispositivo móvil 104, y puede usar un código de autenticación, analizado en más detalle a continuación, para autenticar el dispositivo móvil 104 al sistema de SE remoto 110. En un ejemplo de este tipo, la autenticación de ambos sistemas entre sí proporciona la autenticación mutua y seguridad adicional.

Comunicación SSL/TLS es un método estándar de comunicación como será evidente para expertos en la materia. El código de autenticación puede ser un troceo calculado sobre un conjunto de datos conocido tanto por el sistema de SE remoto 110 como el dispositivo móvil 104. Por ejemplo, el código de autenticación puede calcularse sobre un identificador único definido por el sistema de SE remoto 110 para identificar inequívocamente al dispositivo móvil 104, que puede proporcionarse a la aplicación de pago móvil 106 durante inicialización, analizado en más detalle a continuación. En una realización ilustrativa, el código de autenticación puede basarse, en parte, en un identificador de sesión. El identificador de sesión puede transmitirse desde el sistema de SE remoto 110 al dispositivo móvil 104 usando la notificación remota 402. En una realización adicional, el identificador de sesión puede encriptarse (por ejemplo, usando la clave móvil). En una realización de este tipo, la clave móvil puede usarse para desencriptar el identificador de sesión a usar para crear el código de autenticación a usar para la autenticación mutua 404.

El dispositivo móvil 104 y el sistema de SE remoto 110 puede incluir tanto la clave móvil a usarse como una clave compartida para el encriptado y desencriptado de mensajes transmitidos a través de notificación remota. La aplicación de pago móvil 106 también puede incluir una clave de encriptación de almacenamiento local. La clave de encriptación de almacenamiento local puede generarse por la aplicación de pago móvil 106 y usarse para proporcionar el almacenamiento 304 como una base de datos local encriptada. El almacenamiento 304 puede almacenar a continuación la clave móvil compartida, credenciales de pago recibidas y cualquier información adicional en el dispositivo móvil 104 para evitar acceso no autorizado.

Inicialización y uso de la aplicación de pago móvil

La Figura 5 ilustra un método 500 para la inicialización y uso de la aplicación de pago móvil 106 en el dispositivo móvil 104.

En la etapa 502, el usuario 102 puede registrarse en el sistema de SE remoto 110 para usar el dispositivo móvil 104 para transacciones de pago sin contacto. El usuario 102 puede registrarse en el sistema de SE remoto 110 usando el dispositivo móvil 104 u otro dispositivo informático, tal como un ordenador de sobremesa. El registro puede realizarse a través de un explorador web, programa de aplicación, o cualquier otro método adecuado como será evidente para

expertos en la materia. Como parte del registro, el usuario 102 puede proporcionar información de cuenta para la cuenta de pago con la que el usuario 102 quiere usar para transacciones de pago usando el dispositivo móvil 104. El usuario 102 puede recibir un código de activación y también puede identificar y/o recibir un identificador único usado para identificar el usuario 102.

En la etapa 504, el usuario 102 puede instalar la aplicación de pago móvil 106 en el dispositivo móvil 104. Métodos para instalar programas de aplicación en un dispositivo móvil serán evidentes para un experto en la materia y pueden incluir usar un explorador web o programa de aplicación en el dispositivo móvil 104 para identificar y descargar la aplicación de pago móvil 106. También será evidente para expertos en la materia que la etapa 504 puede realizarse antes o simultáneamente con la etapa 502.

En la etapa 506, el usuario 102 puede inicializar/activar la aplicación de pago móvil 106. El usuario 102 puede introducir el código de activación recibido en la etapa 502 en la aplicación de pago móvil 106. La aplicación de pago móvil 106 puede comunicarse a continuación con el sistema de SE remoto 110 y puede recibir la clave móvil compartida. La aplicación de pago móvil 106 también puede generar la clave de encriptación de almacenamiento local y encriptar el almacenamiento 304 para crear la base de datos encriptada local.

En la etapa 508, el sistema de SE remoto 110 puede transmitir el perfil de tarjeta 116 al dispositivo móvil 104. En una realización, el dispositivo móvil 104 puede recibir un mensaje de notificación remota para notificar al usuario 102 que la aplicación de pago móvil 106 debe conectarse con el sistema de SE remoto 110 usando la autenticación mutua 404. Una vez conectado, el sistema de SE remoto 110 puede transmitir a continuación el perfil de tarjeta que incluye credenciales de pago para la cuenta especificada por el usuario 102 en la etapa 502, que puede a continuación almacenarse por la aplicación de pago móvil 106 en la base de datos encriptada local 304.

En la etapa 510, el sistema de SE remoto 110 puede transmitir una clave de un solo uso 118 a la aplicación de pago móvil 106. En algunas realizaciones, la transmisión puede realizarse usando autenticación mutua 404 en el mismo proceso realizado en la etapa 510. En algunas realizaciones, las etapas 508 y 510 pueden combinarse en una única etapa, de tal forma que el sistema de SE remoto puede transmitir tanto el perfil de tarjeta 116 como una clave de un solo uso 118 a la aplicación de pago móvil 106 en una única transacción o transacciones consecutivas.

En la etapa 512, el dispositivo móvil 104 puede llevar a cabo una transacción de pago sin contacto/NFC usando la aplicación de pago móvil 106 y la clave de un solo uso 118. La aplicación de pago móvil 106 puede generar un criptograma de pago, analizado en más detalle a continuación, y puede transmitir el criptograma generado y credenciales de pago a un terminal punto de venta 120. Métodos para transmitir credenciales de pago y un criptograma de pago a un terminal punto de venta 120 a través de NFC serán evidentes para un experto en la materia.

En la etapa 514, la aplicación de pago móvil 106 puede identificar si existe cualquier clave de un solo uso 118 disponible para su uso en posteriores transacciones de pago. Si existen claves adicionales 118 disponibles para su uso, a continuación el método 500 puede volver a la etapa 512 en la que pueden llevarse a cabo transacciones de pago adicionales con la clave o claves de un solo uso 118 restantes. Si no existen claves de un solo uso 118 restantes, a continuación, el método 500 puede volver a la etapa 510 en la que puede hacerse conexión con el sistema de SE remoto 110 y una nueva clave de un solo uso 118 proporcionada al dispositivo móvil 104.

Método para proporcionar credenciales de pago y generar un criptograma de pago

La Figura 6 ilustra una versión más detallada del sistema 100 e ilustra el proceso por el cual pueden generarse credenciales de pago y proporcionarse al dispositivo móvil 104 y el dispositivo móvil 104 usado para llevar a cabo una transacción de pago sin contacto sin el uso de un elemento seguro.

El usuario 102 puede registrarse en el sistema de SE remoto 110. El sistema de SE remoto 110 puede almacenar la información de registro de usuario (por ejemplo, información de cuenta de pago) en una base de datos 602 y puede devolver un código de activación al usuario 102. El usuario 102 puede instalar a continuación la aplicación de pago móvil 106 en el dispositivo móvil 104 y activar la aplicación de pago móvil 106 usando el código de activación. Como parte de la activación, el sistema de SE remoto 110 puede transmitir una clave móvil compartida 604 a la aplicación de pago móvil 106. La aplicación de pago móvil 106 también puede generar una clave de encriptación de almacenamiento local y puede encriptar el almacenamiento 304 en el dispositivo móvil 104. La clave móvil 604 puede almacenarse en la base de datos encriptada local 304.

El servicio de gestión de credenciales de pago 112 puede almacenar la clave móvil compartida 604 en la base de datos 602. El servicio de gestión de credenciales de pago 112 también puede identificar credenciales de pago que corresponden a la cuenta de pago indicada por el usuario, y crear el perfil de tarjeta 116 que incluye las credenciales de pago. El servicio de notificación remota 114 puede transmitir una notificación remota al dispositivo móvil 104 para indicar al usuario 102 que el perfil de tarjeta 116 está listo para descargarse a la aplicación de pago móvil 106. La aplicación de pago móvil 106 puede comunicarse a continuación con el servicio de gestión de credenciales de pago 112 usando autenticación mutua y recibir el perfil de tarjeta 116 desde el sistema de SE remoto. La aplicación de pago móvil 106 puede almacenar a continuación el perfil de tarjeta recibido 116 en la base de datos encriptada local 304.

El servicio de gestión de credenciales de pago 112 también puede generar una clave de un solo uso 118 que incluye una clave de generación. En algunas realizaciones, la clave de un solo uso 118 puede generarse en respuesta a la recepción de una petición de clave desde el dispositivo móvil 104. En una realización adicional, la petición de clave puede incluir un PIN móvil. El servicio de gestión de credenciales de pago 112 puede haber almacenado anteriormente el PIN móvil (por ejemplo, según se establece por el usuario 102) en la base de datos 602.

El servicio de gestión de credenciales de pago 112 puede transmitir a continuación la clave de un solo uso generada 118 al dispositivo móvil 104, que puede almacenar a continuación la clave de un solo uso 118 en la base de datos encriptada local 304. En algunos casos, la clave de un solo uso 118 puede ser incorrecta (por ejemplo, falsa, no auténtica, etc.) si la petición de clave incluye un PIN móvil para el que la autenticación no es satisfactoria. En algunas realizaciones la clave puede haberse combinado con el PIN de tal forma que cuando se usa es incorrecta sin ninguna etapa de autenticación explícita. En algunas realizaciones, el perfil de tarjeta 116 y/o la clave de un solo uso 118 puede encriptarse por el servicio de gestión de credenciales de pago 112 antes de transmisión al dispositivo móvil 104, tal como usando la clave móvil 604. La aplicación de pago móvil 106 puede desencriptar a continuación el mensaje recibido, también usando la clave móvil compartida 604 o, en algunas realizaciones, una clave aleatoria.

Una vez que la aplicación de pago móvil 106 incluye tanto el perfil de tarjeta 116 como la clave de un solo uso 118, el usuario 102 puede comprar en un comerciante 306 y seleccionar bienes o servicios para adquirir. El usuario 102 puede introducir a continuación a la aplicación de pago móvil 106 que tiene que llevarse a cabo una transacción de pago. La aplicación de pago móvil 106 puede generar a continuación un criptograma de pago usando la clave de generación incluida en la clave de un solo uso 118. El criptograma de pago puede ser, por ejemplo, un criptograma de aplicación o un código de validación de tarjeta dinámico (CVC3). La aplicación de pago móvil 106 puede transmitir el criptograma de pago al comerciante terminal punto de venta 120.

El comerciante terminal punto de venta 120 puede transmitir la información de pago recibida y cualquier información de transacción adicional (por ejemplo, cantidad de transacción, identificador de comerciante, etc.) al servidor de procesamiento de adquirente 312 del adquirente 122. El servidor de procesamiento de adquirente 312 puede generar y enviar a continuación una petición de autorización para la transacción financiera a la red de pago 124. La red de pago 124 puede transmitir datos de transacción relevantes, tal como la información de pago y cantidad de transacción, al servidor de procesamiento de emisor 308. El servidor de procesamiento de emisor 308 puede validar a continuación el criptograma de aplicación. Si la validación es satisfactoria, el emisor puede aprobar la transacción de pago para la cantidad de transacción (por ejemplo, basándose en una cantidad disponible, crédito, etc. para la cuenta de pago). Si la validación no es satisfactoria, el emisor puede denegar la transacción de pago. Métodos para validar un criptograma serán evidentes para un experto en la materia.

En algunas realizaciones, el sistema de SE remoto 110 puede transmitir información al emisor 108 para almacenamiento en la base de datos de emisor 310, tal como para gestión de fraude. Tal información será evidente para un experto en la materia y puede incluir, por ejemplo, contadores de transacción de aplicación. Métodos adecuados para realizar las funciones como se describen en este documento se analizan en más detalle a continuación con respecto a los diagramas de flujo ilustrados en las Figuras 8-14.

Método alternativo para proporcionar credenciales de pago y generar un criptograma de pago

La Figura 7 ilustra una versión más detallada del sistema alternativo 300 e ilustra el proceso por el cual pueden generarse y proporcionarse credenciales de pago al dispositivo móvil 104 y el dispositivo móvil 104 usado para llevar a cabo una transacción de pago sin contacto sin el uso de un elemento seguro.

El usuario 102 puede instalar el programa de aplicación móvil 106 en el dispositivo móvil 104. Antes del comienzo del proceso, en la etapa A, el programa de aplicación móvil 106 puede almacenar autenticación claves y credenciales en el almacenamiento 304 según se reciben desde el sistema de SE remoto 110. En la etapa B, también puede almacenarse una clave de almacenamiento ($K_{ALMACENAMIENTO}$) en el almacenamiento 304. En la etapa C, puede almacenarse información adicional, incluyendo credenciales de pago estáticas, en el almacenamiento 304.

En la etapa 1, el usuario 102 puede lanzar la aplicación de pago móvil 106 usando el dispositivo móvil 104. En la etapa 2a, la aplicación de pago móvil 106 puede conectarse con el sistema de SE remoto 110 a través del sistema en la nube 302, tal como usando autenticación SSL o cualquier otro método adecuado para transmisión autenticada. El sistema en la nube 302 puede transmitir credenciales de pago a la aplicación de pago móvil 106, que pueden almacenarse a continuación en el almacenamiento 304. En la etapa 2b, la aplicación de pago móvil 106 puede generar un testigo de CAP usado para autenticación. En algunas realizaciones, el usuario 102 puede proporcionar credenciales de autenticación adicionales, tal como un gesto, una contraseña o un identificador biométrico.

En la etapa 3, la aplicación de pago móvil 106 puede transmitir el testigo de CAP generado al sistema de SE remoto 100. En la etapa 4, el testigo de CAP puede reenviarse a un servicio de validación de testigo de CAP (CTVS) 702. En la etapa 5, el CTVS 702 puede validar el testigo de CAP usando métodos evidentes para expertos en la materia. En la etapa 6, los resultados de la validación pueden enviarse al sistema de gestión de credenciales de pago 704. En

algunas realizaciones, el sistema de gestión de credenciales de pago 704 puede operarse por o en nombre del emisor 108.

En la etapa 7, el sistema de gestión de credenciales de pago 704 puede generar una carga útil encriptada. Como parte de la carga útil encriptada, el sistema de gestión de credenciales de pago 704 puede generar un número impredecible de clave de sesión (KS_{UN}), un número impredecible en la nube (UN_{NUBE}), y puede identificar y/o almacenar una pluralidad de claves de código de validación de tarjeta dinámico (CVC3) y la $K_{ALMACENAMIENTO}$. Métodos y sistemas para la generación de números impredecibles serán evidentes para expertos en la materia. La carga útil encriptada puede incluir al menos una clave CVC3, el KSUN y el contador de transacción de aplicación y puede generarse usando una clave CVC3 derivada (KD_{CVC3}). En una realización, la KD_{CVC3} usada puede ser falsa si la validación de testigo de CAP no es satisfactoria. La carga útil puede encriptarse usando la $K_{ALMACENAMIENTO}$.

En la etapa 8a, el sistema de gestión de credenciales de pago 704 puede realizar un proceso de sincronización con el emisor 108. El proceso de sincronización puede incluir definir reglas para la validez de los valores generados por la aplicación de pago móvil 106 para llevar a cabo a transacción de pago. En una realización, el proceso puede incluir transmitir al menos el KS_{UN}, contador de transacción de aplicación y UN_{NUBE} al emisor 108 para almacenamiento en la base de datos de emisor 310.

En la etapa 8b, la carga útil encriptada puede transmitirse al sistema en la nube 302 para transmitir a la aplicación de pago móvil 106 en la etapa 9. En la etapa 10, la carga útil encriptada puede desencriptarse usando la $K_{ALMACENAMIENTO}$ y almacenarse en el almacenamiento 304. En la etapa 11, el usuario 102 puede comprar en el comerciante 306 y seleccionar bienes o servicios para adquirir. Como parte de la adquisición, en la etapa 12, la aplicación de pago móvil 106 puede generar un valor CVC3 de pago. En una realización, el dispositivo móvil 104 puede comunicarse con el terminal punto de venta 120. El terminal punto de venta 120 puede generar un número impredecible de lector (UN_{LECTOR}) y transmitir el UN_{LECTOR} a la aplicación de pago móvil 106, que puede generar a continuación el valor CVC3 de pago usando la información en la carga útil encriptada y el UN_{LECTOR}. El valor CVC3 de pago generado y el contador de transacción de aplicación pueden transmitirse al terminal punto de venta 120 a través de NFC.

En algunas realizaciones, puede requerirse que el usuario 102 introduzca un PIN en el terminal punto de venta 120 para autenticación adicional en la etapa 13. En la etapa 14, el terminal punto de venta 120 puede ejecutar procesos de transacciones de pago NFC estándar como será evidente para expertos en la materia. En la etapa 15, el terminal punto de venta 120 puede generar una petición de autorización para la transacción de pago, que puede incluir el UN_{LECTOR}, el valor CVC3 generado, el contador de transacción de aplicación y, si es aplicable, el valor de PIN introducido por el usuario 102. En la etapa 16, el servidor de procesamiento de adquirente 312 puede traducir el PIN incluido en la petición de autorización usando métodos evidentes para expertos en la materia. Será adicionalmente evidente que la etapa 16 puede ser opcional.

En la etapa 17, la petición de autorización puede reenviarse a la red de pago 124, que puede reenviar la petición de autorización y/o información incluida en la petición de autorización al emisor 108. En la etapa opcional 18, el emisor puede verificar el PIN traducido. En la etapa 19a, el emisor 108 puede identificar si es necesario un procesamiento adicional y puede, si fuera necesario, recuperar los valores almacenados en la base de datos de emisor 310. En la etapa 19b, el servidor de procesamiento de emisor 308 puede validar el valor CVC3 de pago usando al menos el UN_{LECTOR}, UN_{NUBE} y contador de transacción de aplicación. Métodos para validar un CVC3 serán evidentes para un experto en la materia. En la etapa 20, el emisor 108 puede enviar una respuesta basándose en la validación, y el método puede proceder en consecuencia como en transacciones de pago tradicionales.

Método para el registro de un usuario para transacciones de pago remotas

La Figura 8 es un diagrama de flujo que ilustra un método para que el usuario 102 se registre con el sistema de SE remoto 110 para habilitar una cuenta de pago para transacciones de pago remotas usando un dispositivo móvil 104 que carece de un elemento seguro.

En la etapa 806, el usuario 102 puede acceder al sistema de registro del sistema de SE remoto 110. El usuario 102 puede acceder al sistema a través de un explorador web 804, que puede ejecutarse en un dispositivo informático. En una realización, el dispositivo informático puede ser el dispositivo móvil 104. El usuario 102 puede navegar a una página web alojada por o en nombre del sistema de SE remoto 110. En la etapa 808, el usuario 102 puede registrarse en el servicio de gestión de credenciales de pago 112 a través del navegador 804. Como parte del registro, el usuario 102 puede proporcionar detalles de cuenta para una cuenta de pago, y el servicio de gestión de credenciales de pago 112 puede garantizar la cuenta de pago es apta para transacciones de pago remotas.

En la etapa 810, el servicio de gestión de credenciales de pago 112 puede crear un perfil de usuario para el usuario 102 en el sistema de SE remoto 110. En algunas realizaciones, también puede crearse un perfil de usuario en el sistema de emisor 108. Como parte de la creación del perfil de usuario, el servicio de gestión de credenciales de pago 112 puede generar y/o identificar un código de activación. En la etapa 812, puede completarse el registro de usuario y el código de activación transmitirse de vuelta al 102 a través del navegador 804. En la etapa 814, el servicio de gestión de credenciales de pago 112 puede sincronizar información (por ejemplo, el perfil de usuario, estado de código

de activación, etc.) con el emisor 108 para gestión de fraude. Será evidente para expertos en la materia que la etapa 814 puede ser opcional.

En la etapa 816, el usuario 102 puede recibir el código de activación a través del explorador web 804. En la etapa 818, el usuario 102 puede descargar la aplicación de pago móvil 106 al dispositivo móvil 104. En una realización, el usuario 102 puede utilizar una tienda de aplicaciones 802, tal como la tienda de aplicaciones de Apple®, para descargar la aplicación de pago móvil 106. La aplicación de pago móvil 106 puede validarse e instalarse en el dispositivo móvil en la etapa 820 usando métodos y sistemas evidentes para expertos en la materia. En la etapa 822, la aplicación de pago móvil 106 puede instalarse satisfactoriamente en el dispositivo móvil 104 y puede esperar la inicialización.

Método para inicialización de la aplicación de pago móvil

La Figura 9 es un diagrama de flujo que ilustra un método para inicialización de la aplicación de pago móvil 106 en el dispositivo móvil 104 para su uso en transacciones de pago sin contacto.

En la etapa 902, el usuario puede iniciar (por ejemplo, ejecutar) la aplicación de pago móvil en el dispositivo móvil 104. En la etapa 904, la aplicación de pago móvil 106 puede realizar una comprobación de integridad. Como parte de la comprobación de integridad, la aplicación de pago móvil 106 puede autenticar al usuario 102 y solicitar el código de activación proporcionado al usuario 102 durante el registro proceso (por ejemplo, en la etapa 812 en la Figura 8). En la etapa 906, la aplicación de pago móvil 106 puede generar un identificador único y valores y claves adicionales, tal como una clave de almacenamiento de base de datos local (por ejemplo, clave de almacenamiento móvil).

En la etapa 908, la aplicación de pago móvil 106 puede conectarse al servicio de gestión de credenciales de pago 112 usando autenticación mutua. La aplicación de pago móvil 106 puede transmitir el código de activación y cualquier otra información de autenticación de usuario adicional (por ejemplo, un identificador de usuario, una contraseña, etc.) como un método de autenticación. La aplicación de pago móvil 106 también puede transmitir el identificador único generado. En algunas realizaciones, el usuario 102 también puede proporcionan un PIN móvil a transmitir al servicio de gestión de credenciales de pago 112 como parte de la etapa 908.

En la etapa 910, el servicio de gestión de credenciales de pago 112 puede validar la aplicación de pago móvil 106 usando la información de autenticación proporcionada y puede, si se valida, actualizar el perfil de usuario para incluir el identificador único. En la etapa 912, el servicio de gestión de credenciales de pago 112 también puede registrar el dispositivo móvil 104 con el servicio de notificación remota 114 usando el identificador único. En la etapa 914, el servicio de gestión de credenciales de pago 112 puede generar la clave móvil compartida 604 y puede almacenar la clave móvil compartida 604 en el perfil de usuario. En la etapa opcional 916, el servicio de gestión de credenciales de pago 112 puede sincronizar con el emisor 108 para gestión de fraude.

En la etapa 918, la aplicación de pago móvil 106 puede recibir la clave móvil compartida 604 desde el servicio de gestión de credenciales de pago 112 y puede almacenar la clave móvil 604 en el almacenamiento local encriptado 304. En la etapa 920, la aplicación de pago móvil 106 puede borrar la clave de almacenamiento móvil, de tal forma que puede no accederse al almacenamiento local encriptado 304 sin autorización. La aplicación de pago móvil 106 puede almacenar datos con los que se genera la clave de almacenamiento móvil separados del almacenamiento local encriptado 304 para su uso en regenerar la clave de almacenamiento móvil para acceder al almacenamiento local encriptado 304. En la etapa 922, la aplicación de pago móvil 106 puede estar lista para gestión remota por el servicio de gestión de credenciales de pago 112. En algunas realizaciones, la aplicación de pago móvil 106 puede notificar al usuario 102 cuando se completa la inicialización.

Método para gestión remota de la aplicación de pago móvil

La Figura 10 es un diagrama de flujo que ilustra un método para gestión remota de la aplicación de pago móvil 106 del dispositivo móvil 104 a través del servicio de gestión de credenciales de pago 112.

En la etapa 1002, el servicio de gestión de credenciales de pago 112 puede recibir un desencadenante para iniciar la gestión remota de la aplicación de pago móvil 106. En algunas realizaciones, el desencadenante puede recibirse desde el propio servicio de gestión de credenciales de pago 112 basándose en reglas predefinidas. En otra realización, el desencadenante puede recibirse desde el emisor 108. En la etapa 1004, el servicio de gestión de credenciales de pago 112 puede prepare datos para notificación remota. La preparación de datos puede incluir la creación de una notificación basándose en una función a realizar, tal como la provisión del perfil de tarjeta 116, provisión de una clave de un solo uso 118, cambio del PIN móvil, etc. Un método ilustrativo para la provisión del perfil de tarjeta 116 al dispositivo móvil 104 se analiza en más detalle a continuación con referencia a la Figura 11.

El servicio de gestión de credenciales de pago 112 puede crear un mensaje que incluye la notificación y un identificador de sesión y, a continuación, puede encriptar el mensaje usando la clave móvil 604. El servicio de gestión de credenciales de pago 112 también puede identificar el dispositivo móvil 104 para recepción usando el identificador único en el perfil de usuario. En realizaciones en las que etapa 1004 puede incluir la provisión de la clave de un solo uso 118, la clave de un solo uso 118 puede encriptarse usando una clave aleatoria (por ejemplo, o clave adecuada

distinta de la clave móvil 604), y a continuación la clave de un solo uso encriptada puede encriptarse usando el móvil 604 y proporcionarse a la aplicación de pago móvil 106 similar a la encriptación y transmisión del mensaje como se describen en este documento.

En la etapa 1006, el servicio de gestión de credenciales de pago 112 puede transmitir el mensaje encriptado a la aplicación de pago móvil 106 usando notificación remota 402. Como se ha analizado anteriormente, la notificación remota 402 puede incluir el reenvío del mensaje encriptado al servicio de notificación remota 114, que puede transmitir el mensaje encriptado al dispositivo móvil 104 usando notificación remota, que puede a continuación hacer el mensaje encriptado disponible para la aplicación de pago móvil 106. En la etapa 1008, la aplicación de pago móvil 106 puede recibir el mensaje encriptado.

En la etapa 1010, el usuario 102 puede iniciar la aplicación de pago móvil 106. Será evidente para expertos en la materia que la etapa 1010 puede ser opcional (por ejemplo, la aplicación de pago móvil 106 puede iniciarse tras la recepción del mensaje encriptado, la aplicación de pago móvil 106 puede ejecutarse siempre en segundo plano, etc.). En la etapa 1012, la aplicación de pago móvil 106 puede iniciar, que puede incluir regenerar la clave de almacenamiento móvil, recuperar la clave móvil 406 del almacenamiento encriptado local 304 y desencriptar el mensaje usando la clave móvil recuperada 406.

En la etapa 1014, la aplicación de pago móvil 106 puede conectarse al servicio de gestión de credenciales de pago 112 usando autenticación mutua 404 como se ha analizado anteriormente, tal como generando, transmitiendo y, a continuación, borrando un código de autenticación que incluye el identificador de sesión. En la etapa 1016, el servicio de gestión de credenciales de pago 112 puede validar las credenciales de autenticación transmitidas por la aplicación de pago móvil 106. Si se validan, el servicio de gestión de credenciales de pago 112 puede a continuación tener una conexión segura con la aplicación de pago móvil 106 y puede proceder con la función indicada en la notificación.

Método para proporcionar de un perfil de tarjeta a la aplicación de pago móvil

La Figura 11 es un diagrama de flujo que ilustra un método para proporcionar el perfil de tarjeta 116 a la aplicación de pago móvil 106 del dispositivo móvil 104 por el servicio de gestión de credenciales de pago 112.

Utilizar la conexión hecha tras el desencadenamiento de gestión remota ilustrada en la Figura 10, en la etapa 1102 el servicio de gestión de credenciales de pago 112 puede crear la carga útil de testigo de pago perfil de tarjeta 116. El perfil de tarjeta 116 puede incluir credenciales de pago para la cuenta de pago indicada por el usuario 102 durante registro, que puede haberse almacenado en el perfil de usuario. El servicio de gestión de credenciales de pago 112 puede crear el perfil de tarjeta generando un mensaje que incluye las credenciales de pago, generando una clave de sesión móvil y encriptando el mensaje usando la clave de sesión móvil. El servicio de gestión de credenciales de pago 112 puede almacenar el perfil de tarjeta 116 en el perfil de usuario y, en la etapa 1104, puede transmitir el mensaje que incluye el perfil de tarjeta 116 a la aplicación de pago móvil 106.

En la etapa 1106, la aplicación de pago móvil 106 puede recibir el mensaje y puede generar la clave de sesión móvil usada para desencriptar el mensaje. En la etapa 1108, la aplicación de pago móvil 106 puede desencriptar el mensaje usando la clave de sesión móvil generada y puede validar el mensaje. Una vez validado, en la etapa 1110 la aplicación de pago móvil 106 puede crear un mensaje de recepción que indica recepción y validación satisfactorias del perfil de tarjeta 116, y puede usarse como un mensaje de activación y/o usarse para transportar información desde la aplicación de pago móvil 106 al sistema de SE remoto 110. El mensaje de recepción puede encriptarse usando la clave de sesión móvil. La aplicación de pago móvil 106 también puede actualizar un estado para indicar que el perfil de tarjeta 116 se recibe y almacena satisfactoriamente.

En la etapa 1112, el mensaje de recepción puede recibirse por el servicio de gestión de credenciales de pago 112 y puede desencriptarse usando la clave de sesión móvil y validarse. Tras validación satisfactoria, en la etapa 1114 el servicio de gestión de credenciales de pago 112 puede activar el perfil de tarjeta 116 y puede actualizar el perfil de usuario en consecuencia. En la etapa 1116, el servicio de gestión de credenciales de pago 112 puede transmitir una notificación a la aplicación de pago móvil 106 que el perfil de tarjeta 116 se ha activado y puede borrar la clave de sesión móvil. En la etapa 1118, el servicio de gestión de credenciales de pago 112 puede sincronizar el perfil de usuario que indica activación del perfil de tarjeta 116 con el emisor 108 para gestión de fraude.

En la etapa 1120, la aplicación de pago móvil 106 puede analizar el código de devolución que indica activación del perfil de tarjeta 116. En la etapa 1122, la aplicación de pago móvil 106 puede borrar la clave de sesión móvil, y en la etapa 1124 puede estar lista para recibir claves de un solo uso 118 para su uso en la realización de transacciones de pago. En algunas realizaciones, la aplicación de pago móvil 106 puede visualizar una notificación al usuario 102 a través de una interfaz de usuario para indicar que pueden recibirse claves de un solo uso 118.

Método para proporcionar claves de un solo uso a la aplicación de pago móvil

La Figura 12 es un diagrama de flujo que ilustra un método para la provisión de claves de un solo uso 118 a la aplicación de pago móvil 106 en el dispositivo móvil 104 por el servicio de gestión de credenciales de pago 112 para

su uso en transacciones de pago.

En una realización ilustrativa, mientras se realiza la conexión con el servicio de gestión de credenciales de pago 112 hecha tras el desencadenamiento de gestión remota ilustrada en la Figura 10, la clave de un solo uso encriptada 118, puede transmitirse anteriormente a la aplicación de pago móvil 106 en un mensaje encriptado por la clave móvil 604. En la etapa 1202, el servicio de gestión de credenciales de pago 112 puede crear un mensaje con una acción para activar (por ejemplo, desencriptar) la clave de un solo uso 118 anteriormente proporcionada, incluyendo el mensaje la clave aleatoria usada para encriptar la clave de un solo uso 118. El servicio de gestión de credenciales de pago 112 puede generar a continuación una clave de sesión móvil y a continuación puede encriptar el mensaje que incluye la clave aleatoria usando la clave de sesión móvil. El servicio de gestión de credenciales de pago 112 puede transmitir a continuación, en la etapa 1204, el mensaje que incluye la clave aleatoria a la aplicación de pago móvil 106.

En la etapa 1206, la aplicación de pago móvil 106 puede recibir el mensaje y puede generar la clave de sesión móvil usada para desencriptar el mensaje. En la etapa 1208, la aplicación de pago móvil 106 puede desencriptar el mensaje usando la clave de sesión móvil generada y puede validar el mensaje. La aplicación de pago móvil 106 también puede desencriptar la clave de un solo uso 118 usando la clave aleatoria incluida en el mensaje desencriptado, y puede validar la clave de un solo uso 118 desencriptada. Una vez validada, en la etapa 1210 la aplicación de pago móvil 106 puede crear un mensaje de recepción que indica recepción y validación satisfactorias de la clave de un solo uso 118. El mensaje de recepción puede encriptarse usando la clave de sesión móvil. La aplicación de pago móvil 106 también puede actualizar un estado para indicar que la clave de un solo uso 118 se recibe y almacena satisfactoriamente y que la aplicación de pago móvil 106 está lista para llevar a cabo a transacción de pago.

En la etapa 1212, el mensaje de recepción puede recibirse por el servicio de gestión de credenciales de pago 112 y puede desencriptarse usando la clave de sesión móvil y validarse. Tras validación satisfactoria, en la etapa 1214 el servicio de gestión de credenciales de pago 112 puede activar la clave de un solo uso 118 y puede actualizar el perfil de usuario en consecuencia. En la etapa 1216, el servicio de gestión de credenciales de pago 112 puede transmitir una notificación a la aplicación de pago móvil 106 que la clave de un solo uso 118 se ha activado y puede borrar la clave de sesión móvil. En la etapa 1218, el servicio de gestión de credenciales de pago 112 puede sincronizar el perfil de usuario que indica activación de la clave de un solo uso 118 con el emisor 108 para gestión de fraude.

En la etapa 1220, la aplicación de pago móvil 106 puede analizar el código de devolución que indica activación de la clave de un solo uso 118. En la etapa 1222, la aplicación de pago móvil 106 puede borrar la clave de sesión móvil, y en la etapa 1224 puede estar lista para llevar a cabo una transacción de pago sin contacto. En algunas realizaciones, la aplicación de pago móvil 106 puede visualizar una notificación al usuario 102 a través de una interfaz de usuario para indicar que la aplicación de pago móvil 106 está lista para llevar a cabo una transacción de pago sin contacto.

Método para modificación de PIN móvil en la aplicación de pago móvil

La Figura 13 es un diagrama de flujo que ilustra un método para la gestión de un cambio en el PIN móvil del usuario 102 en la aplicación de pago móvil 106 por el servicio de gestión de credenciales de pago 112.

Utilizando la conexión hecha tras el desencadenamiento de gestión remota ilustrada en la Figura 10, en la etapa 1302 el servicio de gestión de credenciales de pago 112 puede crear una acción de gestión remota que indica un cambio en el PIN móvil y eliminación de todas las claves de un solo uso 118 almacenadas. El servicio de gestión de credenciales de pago 112 puede crear un mensaje que incluye la acción de gestión remota, generar una clave de sesión móvil y encriptar el mensaje usando la clave de sesión móvil. El servicio de gestión de credenciales de pago 112 puede transmitir, en la etapa 1304, el mensaje que incluye acción de gestión remota a la aplicación de pago móvil 106.

En la etapa 1306, la aplicación de pago móvil 106 puede recibir el mensaje y puede generar la clave de sesión móvil usada para desencriptar el mensaje. En la etapa 1308, la aplicación de pago móvil 106 puede desencriptar el mensaje usando la clave de sesión móvil generada y puede validar el mensaje. Una vez que el mensaje se ha validado, la aplicación de pago móvil puede actualizar el perfil de tarjeta 116 en consecuencia y puede eliminar cualquier clave de un solo uso 118 disponible del almacenamiento local encriptado 304. A continuación, en la etapa 1310, la aplicación de pago móvil 106 puede crear un mensaje de recepción que indica recepción y ejecución satisfactorias de la acción de gestión remota. El mensaje de recepción puede encriptarse usando la clave de sesión móvil.

En la etapa 1312, el mensaje de recepción puede recibirse por el servicio de gestión de credenciales de pago 112 y puede desencriptarse usando la clave de sesión móvil y validarse. Tras validación satisfactoria, en la etapa 1314 el servicio de gestión de credenciales de pago 112 puede actualizar el perfil de usuario en consecuencia. En la etapa 1316, el servicio de gestión de credenciales de pago 112 puede transmitir una notificación a la aplicación de pago móvil 106 que el perfil de usuario se ha actualizado y no se ha emitido ninguna clave de un solo uso 118, y puede borrar la clave de sesión móvil. En la etapa 1318, el servicio de gestión de credenciales de pago 112 puede sincronizar el perfil de usuario que indica el cambio en el PIN móvil y borrado de claves de un solo uso 118 con el emisor 108 para gestión de fraude.

En la etapa 1320, la aplicación de pago móvil 106 puede analizar el código de devolución. En la etapa 1322, la aplicación de pago móvil 106 puede borrar la clave de sesión móvil, y en la etapa 1324 puede estar lista para recibir claves de un solo uso 118 para su uso en la realización de transacciones de pago. En algunas realizaciones, la aplicación de pago móvil 106 puede visualizar una notificación al usuario 102 a través de una interfaz de usuario para indicar que pueden recibirse claves de un solo uso 118.

Método para llevar a cabo una transacción de pago usando la aplicación de pago móvil

La Figura 14 es un diagrama de flujo que ilustra un método para llevar a cabo una transacción de pago sin contacto usando la aplicación de pago móvil 106 en el dispositivo móvil 104 usando el perfil de tarjeta 116 y clave de un solo uso 118 proporcionada por el servicio de gestión de credenciales de pago 112.

En la etapa 1402, el usuario 102 puede iniciar la aplicación de pago móvil 106 en el dispositivo móvil 104. En la etapa 1404, la aplicación de pago móvil 106 puede prepararse para el pago. Para prepararse para el pago, la aplicación de pago móvil 106 puede regenerar la clave de almacenamiento móvil y puede recuperar las credenciales de pago y clave de generación desde el perfil de tarjeta 116 y la clave de un solo uso 118 en el almacenamiento local encriptado 304. La clave de generación puede usarse por la aplicación de pago móvil 106 para generar un criptograma de pago para su uso en la transacción de pago. La aplicación de pago móvil 106 también puede indicar al usuario 102 que la aplicación está lista para el pago.

En la etapa 1406, puede ejecutarse un método de pago NFC entre el usuario 102, el dispositivo móvil 104, la aplicación de pago móvil 106 y el terminal punto de venta 120. Métodos para ejecutar transmisión de credenciales de pago desde un dispositivo móvil a un terminal punto de venta serán evidentes para un experto en la materia.

En la etapa 1408, el terminal punto de venta 120 en el comerciante 306 puede proporcionar datos de transacción al adquirente 122 que incluye las credenciales de pago y criptograma de pago. En la etapa 1410, el adquirente 122 puede enviar una petición de autorización que incluye la transacción datos a la red de pago 124. En la etapa 1412, la red de pago 124 puede buscar autorización desde el emisor 108 para la transacción de pago y puede reenviar información relevante al emisor 108. En la etapa 1414, el emisor 108 puede validar el criptograma de pago usando métodos que serán evidentes para un experto en la materia. El emisor 108 puede, una vez que se valida el criptograma de pago, aprobar o denegar la transacción de pago (por ejemplo, basándose en una cantidad de transacción y crédito disponible en la cuenta de pago para el usuario 102) y notificar la red de pago 124. En la etapa 1416, la red de pago 124 puede enviar una respuesta de autorización al adquirente 122, que puede a continuación reenviar la respuesta al comerciante 306 y/o terminal punto de venta 120 en la etapa 1418. En la etapa 1420, el comerciante puede finalizar la transacción de pago, tal como proporcionando bienes o servicios transaccionados al usuario 102 o proporcionando un recibo al usuario 102.

Una vez que se ha completado la transacción de pago, la aplicación de pago móvil 106 puede actualizar, en la etapa 1422, la carga útil de testigo de pago almacenada en el almacenamiento local encriptado 304 basándose en el resultado de la transacción de pago. En la etapa 1424, la aplicación de pago móvil 106 puede borrar la clave de almacenamiento móvil, y en la etapa 1426, puede indicar (por ejemplo, al usuario 102) que la aplicación de pago móvil 106 está lista para otra transacción de pago sin contacto (por ejemplo, si hay disponibles claves adicionales de un solo uso 118) o para recibir claves de un solo uso 118.

En algunas realizaciones, la transacción de pago puede llevarse a cabo a través del uso de autenticación de datos local (LDA). En algunos casos, el almacenamiento de credenciales de pago recibidas por el dispositivo móvil 104 en el almacenamiento local encriptado 304 (por ejemplo, y no en un elemento seguro) puede ser de tal forma que CDA (autenticación de datos dinámicos combinados/generación de criptograma de aplicación) puede no estar disponible para soportar métodos de verificación de tarjeta tradicionales para verificar las credenciales de pago usadas en la transacción financiera. Como resultado, el terminal punto de venta 120 puede configurarse de tal forma que puede requerir autenticación por el usuario 102 tanto en el dispositivo móvil 104 (por ejemplo, introduciendo del PIN móvil) y el terminal punto de venta 120 (por ejemplo, introduciendo de un PIN en línea o firma).

LDA puede usarse para proporcionar soporte de autenticación de tarjeta de tal forma que una transacción financiera puede soportarse por el terminal punto de venta 120 utilizando un único punto de autenticación (por ejemplo, el PIN móvil). Para realizar LDA, el perfil de tarjeta 116 puede incluir adicionalmente un par de claves RSA y certificado. La realización de la LDA puede incluir el intercambio del significado de fecha efectiva y fecha de vencimiento en las credenciales de pago incluidas en el perfil de tarjeta 116, y el establecimiento de al menos un código de acción de emisor para forzar que la transacción de pago sea una transacción en línea. En una realización adicional, la fecha de vencimiento puede establecerse como una fecha anterior a la fecha de emisión, o la fecha efectiva puede establecerse como una fecha más allá de la fecha de caducidad, o ambas pueden establecerse como se definen. Esto puede resultar en el terminal punto de venta 120 declinando la transacción debido a las fechas de vencimiento y/o efectivas, pero transmitiendo la transacción para autorización en línea, que puede resultar en el procesamiento de la transacción usando el único punto de autenticación por el usuario 102. En una realización adicional, la fecha de vencimiento puede establecerse como una fecha anterior, o la fecha efectiva puede establecerse como una fecha futura, o ambas pueden establecerse como se definen. En algunas realizaciones, realizar LDA puede incluir adicionalmente establecer un

código de acción de emisor configurado para declinar transacciones fuera de línea (por ejemplo, de tal forma que si el terminal punto de venta 120 es un terminal de solo fuera de línea, este puede declinar todas tales transacciones).

Se observa que, aunque el método ilustrado en la Figura 14 y descrito anteriormente es un método para llevar a cabo una transacción de pago sin contacto, un método de este tipo también puede usarse para llevar a cabo una transacción de pago remota, para la transmisión segura de credenciales de pago, para su uso como parte de una solución de autenticación (si parte de una transacción o de otra manera), o en otras aplicaciones como será evidente para expertos en la materia y no limitado a las ilustradas en este documento.

Método ilustrativo para generar y proporcionar credenciales de pago

La Figura 15 es un diagrama de flujo que ilustra un método 1500 para generar y proporcionar credenciales de pago a un dispositivo móvil que carece de un elemento seguro.

En la etapa 1502, puede generarse un perfil de tarjeta (por ejemplo, el perfil de tarjeta 116) asociado con una cuenta de pago por un dispositivo de procesamiento (por ejemplo, del servicio de gestión de credenciales de pago 112), en el que el perfil de tarjeta 116 incluye al menos credenciales de pago que corresponden a la cuenta de pago asociada y un identificador de perfil. En la etapa 1504, el perfil de tarjeta generado 116 puede proporcionarse a un dispositivo móvil (por ejemplo, el dispositivo móvil 104) que carece de un elemento seguro. En una realización, proporcionar el perfil de tarjeta 116 puede incluir crear un mensaje que incluye el perfil de tarjeta generado 116, generar una clave de encriptación, encriptar el mensaje usando la clave de encriptación generada y proporcionar el mensaje encriptado al dispositivo móvil 104.

En la etapa 1506, una petición de clave puede recibirse desde el dispositivo móvil 104, en el que la petición de clave incluye al menos un número de identificación personal (PIN) móvil y el identificador de perfil. En la etapa 1508, un dispositivo de autenticación (por ejemplo, del servicio de gestión de credenciales de pago 112) puede usar el PIN móvil. En una realización, el dispositivo de autenticación puede usar el PIN móvil usando un método XOR. En la etapa 1510, una clave de un solo uso (por ejemplo, la clave de un solo uso 118) puede generarse por el dispositivo de procesamiento, en el que la clave de un solo uso 118 incluye al menos el identificador de perfil, un contador de transacción de aplicación y una clave de generación para su uso en la generación de un criptograma de pago válido para una única transacción financiera. En algunas realizaciones, la clave de un solo uso 118 puede ser auténtica si el PIN móvil se autentica satisfactoriamente en la etapa 1508, y falsa si el PIN móvil no se autentica satisfactoriamente. En una realización, el método 1500 puede incluir adicionalmente transmitir la clave de un solo uso generada 118 a un emisor asociado con la cuenta de pago. En algunas realizaciones, la clave de un solo uso generada 118 puede estar inactiva.

En la etapa 1512, la clave de un solo uso generada 118 puede transmitirse, por un dispositivo de transmisión, al dispositivo móvil 104. En una realización, transmitir la clave de un solo uso generada 118 puede incluir crear un mensaje que incluye la clave de un solo uso generada 118, generar una clave de encriptación, encriptar el mensaje usando la clave de encriptación generada y proporcionar el mensaje encriptado al dispositivo móvil 104.

En realizaciones en las que la clave de un solo uso generada 118 puede estar inactiva, el método 1500 puede incluir adicionalmente recibir, desde el dispositivo móvil 104, una indicación de uso de la clave de un solo uso 118 y activar, por el dispositivo de procesamiento, la clave de un solo uso generada 118. En una realización adicional, el método 1500 también puede incluir transmitir, por el dispositivo de transmisión, una indicación de activación de la clave de un solo uso 118 a un emisor (por ejemplo, el emisor 108) asociado con la cuenta de pago.

Método para generar un criptograma de pago

La Figura 16 es un diagrama de flujo que ilustra un método 1600 para generar un criptograma de pago en un dispositivo móvil (por ejemplo, el dispositivo móvil 104) que carece de un elemento seguro.

En la etapa 1602, un perfil de tarjeta (por ejemplo, el perfil de tarjeta 116) puede recibirse por un dispositivo de recepción (por ejemplo, en el dispositivo móvil 104), en el que el perfil de tarjeta 116 incluye al menos credenciales de pago que corresponden a una cuenta de pago y un identificador de perfil. En una realización, recibir el perfil de tarjeta 116 puede incluir recibir un mensaje encriptado que incluye el perfil de tarjeta 116, generar una clave de sesión móvil y desencriptar el mensaje usando la clave de sesión móvil generada para obtener el perfil de tarjeta 116 incluido. En algunas realizaciones, el perfil de tarjeta 116 puede configurarse para utilizar autenticación de datos local, en las que la autenticación de datos local incluye intercambiar, en las credenciales de pago, el significado de una fecha de vencimiento y una fecha efectiva, y establecer un código de acción de emisor configurado para forzar que la transacción financiera sea una transacción en línea. En una realización adicional, la fecha de vencimiento puede establecerse como una fecha anterior a la fecha de emisión, o la fecha efectiva puede establecerse como una fecha más allá de la fecha de caducidad, o ambas pueden establecerse como se definen. En una realización adicional, el perfil de tarjeta 116 puede incluir adicionalmente un par de claves RSA y certificado.

En la etapa 1604, un dispositivo de entrada (por ejemplo, del dispositivo móvil 104, tal como una pantalla táctil) puede

recibir un número de identificación personal (PIN) móvil introducido por un usuario (por ejemplo, el usuario 102) del dispositivo móvil 104. En la etapa 1606, un dispositivo de transmisión puede transmitir una petición de clave, en el que la petición de clave incluye al menos el identificador de perfil.

En la etapa 1608, puede recibirse una clave de un solo uso (por ejemplo, la clave de un solo uso 118), por el dispositivo de recepción, en el que la clave de un solo uso 118 incluye al menos un contador de transacción de aplicación y una clave de generación. En una realización, recibir la clave de un solo uso 118 puede incluir recibir un mensaje encriptado que incluye la clave de un solo uso 118, generar una clave de sesión móvil, y desencriptar el mensaje usando la clave de sesión móvil generada para obtener la clave de un solo uso 118 incluida.

En la etapa 1610, un criptograma de pago válido para una única transacción de pago puede generarse, por un dispositivo de procesamiento, basándose en al menos la clave de un solo uso recibida 108 y el PIN móvil. En algunas realizaciones, el criptograma de pago puede ser un criptograma de aplicación o un código de validación de tarjeta dinámico. En la etapa 1612, pueden transmitirse al menos las credenciales de pago y el criptograma de pago generado, a través de comunicación de campo cercano, a un terminal punto de venta (por ejemplo, el terminal punto de venta 120) para su uso en una transacción financiera.

En algunas realizaciones, el método 1600 puede incluir adicionalmente recibir, por el dispositivo de entrada, una indicación de uso de la clave de un solo uso recibida 118, transmitir, por el dispositivo de transmisión, una petición de activación que incluye al menos el identificador de perfil, y recibir, por el dispositivo de recepción, una indicación de activación de la clave de un solo uso 118. En una realización adicional, las credenciales de pago y criptograma de pago generado pueden transmitirse al terminal punto de venta 120 en respuesta a recibir la indicación de activación de la clave de un solo uso 118. En una realización alternativa adicional, el criptograma de pago puede generarse en respuesta a recibir la indicación de activación de la clave de un solo uso 118.

Método alternativo para generar y proporcionar detalles de pago

La Figura 17 es un diagrama de flujo que ilustra un método alternativo 1700 para generar y proporcionar detalles de pago a un dispositivo móvil (por ejemplo, el dispositivo móvil 104) que carece de un elemento seguro.

En la etapa 1702, al menos una clave de almacenamiento, una pluralidad de claves de código de validación de tarjeta dinámico (CVC3), y un contador de transacción de aplicación asociado con un programa de aplicación móvil (por ejemplo, la aplicación de pago móvil 106) puede almacenarse en una base de datos (por ejemplo, el almacenamiento 304). En la etapa 1704, pueden proporcionarse al menos la clave de almacenamiento, un componente de autenticación y credenciales de pago estáticas al dispositivo móvil 104, en el que las credenciales de pago estáticas se asocian con una cuenta de pago.

En la etapa 1706, puede recibirse un testigo de programa de autenticación de chip (CAP) desde el dispositivo móvil 104. En la etapa 1708, la autenticidad del testigo de CAP recibido puede validarse por un servicio de validación (por ejemplo, el CTVS 702). En una realización, el testigo de CAP puede validarse basándose en al menos el componente de autenticación proporcionado y una credencial adicional recibida desde el dispositivo móvil 104. En una realización adicional, la credencial adicional puede ser al menos uno de: un gesto, una contraseña, un código de acceso y un identificador biométrico. En otra realización, validar la autenticidad del testigo de CAP puede incluir validar la autenticidad del testigo de CAP basándose en al menos el contador de transacción de aplicación.

En la etapa 1710, puede generarse un número impredecible de clave de sesión (KS_{UN}) por un dispositivo de procesamiento (por ejemplo, el sistema en la nube 302). En la etapa 1712, puede generarse un número impredecible en la nube (UN_{NUBE}) por el dispositivo de procesamiento 302. En la etapa 1714, el dispositivo de procesamiento 302 puede identificar una carga útil encriptada basándose en una clave CVC3 derivada (KD_{CVC3}), en el que la carga útil encriptada incluye al menos una clave CVC3 de la pluralidad de CVC3 claves, el KS_{UN} y el contador de transacción de aplicación. En una realización, la KD_{CVC3} puede ser auténtica si el testigo de CAP recibido se valida satisfactoriamente, y puede ser falsa si el testigo de CAP recibido no se valida satisfactoriamente. En alguna realización, la carga útil puede encriptarse usando al menos la clave de almacenamiento.

En la etapa 1716, un dispositivo de transmisión puede transmitir la carga útil encriptada al dispositivo móvil 104 para su uso en la generación de un valor de CVC3 para su uso en una transacción financiera. En la etapa 1718, el dispositivo de transmisión puede transmitir al menos el KS_{UN}, UN_{NUBE} y contador de transacción de aplicación a un emisor (por ejemplo, el emisor 108) asociado con la cuenta de pago para su uso en la validación del valor CVC3 generado usado en la transacción financiera.

Método para generar un código de validación de tarjeta dinámico

La Figura 18 es un diagrama de flujo que ilustra un método 1800 para generar un valor de código de validación de tarjeta dinámico (CVC3) en un dispositivo móvil (por ejemplo, el dispositivo móvil 104) que carece de un elemento seguro.

En la etapa 1802, pueden recibirse al menos una clave de almacenamiento, un componente de autenticación y credenciales de pago estáticas por un dispositivo de recepción. En la etapa 1804, puede recibirse al menos una credencial adicional por un dispositivo de entrada (por ejemplo, del dispositivo móvil 104). En algunas realizaciones, la al menos una credencial adicional puede incluir al menos uno de: un gesto, una contraseña, un código de acceso y un identificador biométrico. En la etapa 1806, puede generarse un testigo de programa de autenticación de chip (CAP) por un dispositivo de procesamiento, en el que el testigo de CAP se basa en al menos el componente de autenticación y la al menos una credencial adicional.

En la etapa 1808 el testigo de CAP generado puede transmitirse por un dispositivo de transmisión. En la etapa 1810, puede recibirse una carga útil encriptada por el dispositivo de recepción, en el que la carga útil encriptada incluye al menos un valor de CVC3 proporcionado, número impredecible de clave de sesión y un contador de transacción de aplicación. En la etapa 1812, el dispositivo de procesamiento puede desencriptar la carga útil encriptada usando al menos la clave de almacenamiento recibida.

En la etapa 1814, puede recibirse un número impredecible de lector, a través de comunicación de campo cercano, desde un terminal punto de venta (por ejemplo, el terminal punto de venta 120). En la etapa 1816, el dispositivo de procesamiento puede generar un valor de CVC3 de pago basándose en al menos el valor de CVC3 proporcionado, el número impredecible de clave de sesión, el contador de transacción de aplicación y el número impredecible de lector. En la etapa 1818, el valor CVC3 de pago generado y el contador de transacción de aplicación pueden transmitirse, a través de comunicación de campo cercano, al terminal punto de venta 120 para incluir en una petición de autorización en una transacción financiera.

Arquitectura de sistema informático

La Figura 19 ilustra un sistema informático 1900 en el que pueden implementarse realizaciones de la presente divulgación, o porciones de la misma, como código legible por ordenador. Por ejemplo, la gestión de credenciales de pago 112, el servicio de notificación remota 114, el dispositivo móvil 104, el servidor de procesamiento de adquirente 312 y el servidor de procesamiento de emisor 308 pueden implementarse en el sistema informático 1900 usando hardware, software, firmware, medio legible por ordenador no transitorio que tiene instrucciones almacenadas en el mismo, o una combinación de los mismos y pueden implementarse en uno o más sistemas informáticos u otros sistemas de procesamiento. Hardware, software o cualquier combinación de los mismos puede incorporar módulos y componentes usados para implementar los métodos de las Figuras 6-18.

Si se usa lógica programable, tal lógica puede ejecutarse en una plataforma de procesamiento comercialmente disponible o un dispositivo de fin especial. Un experto en la materia puede apreciar que realizaciones de la materia objeto divulgada pueden practicarse con diversas configuraciones de sistema informático, incluyendo sistemas multiprocesador, miniordenadores, ordenadores centrales, ordenadores enlazados o agrupados con funciones distribuidas, así como ordenadores ubicuos o en miniatura que pueden embeberse en prácticamente cualquier dispositivo. Por ejemplo, pueden usarse al menos un dispositivo de procesador y una memoria para implementar las realizaciones anteriormente descritas.

Un dispositivo de procesador como se analiza en este documento puede ser un único procesador, una pluralidad de procesadores o combinaciones de los mismos. Dispositivos de procesador pueden tener uno o más "núcleos" de procesador. Los términos "medio de programa informático", "medio legible por ordenador no transitorio" y "medio usable por ordenador" como se analizan en este documento se usan para referirse generalmente a medios tangibles tal como una unidad de almacenamiento extraíble 1918, una unidad de almacenamiento extraíble 1922 y un disco duro instalado en unidad de disco duro 1912.

Diversas realizaciones de la presente divulgación se describen en términos de este sistema informático 1900 de ejemplo. Después de leer esta descripción, será evidente para un experto en la materia cómo implementar la presente divulgación usando otros sistemas informáticos y/o arquitecturas informáticas. Aunque operaciones pueden describirse como un proceso secuencial, algunas de las operaciones pueden de hecho realizarse en paralelo, simultáneamente y/o en un entorno distribuido, y con código de programa almacenado local o remotamente para acceso por máquina de un único o múltiples procesadores.

El dispositivo de procesador 1904 puede ser un dispositivo de fin especial o dispositivo de procesador de fin general. El dispositivo de procesador 1904 puede conectarse a una infraestructura de comunicación 1906, tal como un bus, cola de mensajes, red, esquema de traspaso de mensajes de múltiples núcleos, etc. La red puede ser cualquier red adecuada para realizar las funciones como se describen en este documento y puede incluir una red de área local (LAN), una red de área extensa (WAN), una red inalámbrica (por ejemplo, WiFi), una red de comunicación móvil, una red por satélite, la Internet, fibra óptica, cable coaxial, infrarrojos, frecuencia de radio (RF) o cualquier combinación de las mismas. Otros tipos y configuraciones de red adecuados serán evidentes para un experto en la materia. El sistema informático 1900 también puede incluir una memoria principal 1908 (por ejemplo, memoria de acceso aleatorio, memoria de solo lectura, etc.), y también puede incluir una memoria secundaria 1910. La memoria secundaria 1910 puede incluir la unidad de disco duro 1912 y una unidad de disco de almacenamiento extraíble 1914, tal como una unidad de disco flexible, una unidad de cinta magnética, una unidad de disco óptico, una memoria flash, etc.

La unidad de disco de almacenamiento extraíble 1914 puede leer de y/o escribir en la unidad de almacenamiento extraíble 1918 de una manera bien conocida. La unidad de almacenamiento extraíble 1918 puede incluir un medio de almacenamiento extraíble que puede leerse por y escribirse por la unidad de disco de almacenamiento extraíble 1914. Por ejemplo, si la unidad de disco de almacenamiento extraíble 1914 es una unidad de disco flexible, la unidad de almacenamiento extraíble 1918 puede ser un disco flexible. En una realización, la unidad de almacenamiento extraíble 1918 puede ser medio de grabación legible por ordenador no transitorio.

En algunas realizaciones, la memoria secundaria 1910 puede incluir medios alternativos para permitir que programas informáticos u otras instrucciones se carguen en el sistema informático 1900, por ejemplo, la unidad de almacenamiento extraíble 1922 y una interfaz 1920. Ejemplos de tales medios pueden incluir un cartucho de programa e interfaz de cartucho (por ejemplo, como se encuentran en sistemas de video juegos), un chip de memoria extraíble (por ejemplo, EEPROM, PROM, etc.) y conexión asociada, y otras unidades de almacenamiento extraíbles 1922 e interfaces 1920 como será evidente para expertos en la materia.

Datos almacenados en el sistema informático 1900 (por ejemplo, en la memoria principal 1908 y/o la memoria secundaria 1910) pueden almacenarse en cualquier tipo de medio legible por ordenador adecuado, tal como almacenamiento óptico (por ejemplo, un disco compacto, disco versátil digital, Disco Blu-ray, etc.) o almacenamiento de cinta magnética (por ejemplo, una unidad de disco duro). Los datos pueden configurarse en cualquier tipo de configuración de base de datos adecuada, tal como una base de datos relacional, una base de datos de lenguaje de consulta estructurada (SQL), una base de datos distribuida, una base de datos de objetos, etc. Configuraciones y tipos de almacenamiento adecuados serán evidentes para un experto en la materia.

El sistema informático 1900 también puede incluir una interfaz de comunicaciones 1924. La interfaz de comunicaciones 1924 puede configurarse para permitir que software y datos se transfieran entre el sistema informático 1900 y dispositivos externos. Interfaces de comunicaciones 1924 ilustrativas pueden incluir un módem, una interfaz de red (por ejemplo, una tarjeta de Ethernet), un puerto de comunicaciones, una ranura y tarjeta PCMCIA, etc. Software y datos transferidos a través de la interfaz de comunicaciones 1924 pueden ser en forma de señales, que pueden ser electrónicas, electromagnéticas, ópticas u otras señales como será evidente para expertos en la materia. Las señales pueden viajar a través de una trayectoria de comunicación 1926, que puede configurarse para transportar las señales y pueden implementarse usando alambre, cable, fibra óptica, una línea telefónica, un enlace de teléfono celular, un enlace de frecuencia de radio, etc.

Medio de programa informático y medio usable por ordenador pueden referirse a memorias, tal como la memoria principal 1908 y memoria secundaria 1910, que pueden ser semiconductores de memoria (por ejemplo, DRAM, etc.). Estos productos de programa informático pueden ser medios para proporcionar software al sistema informático 1900. Programas informáticos (por ejemplo, lógica de control de ordenador) puede almacenarse en la memoria principal 1908 y/o la memoria secundaria 1910. También pueden recibirse programas informáticos a través de la interfaz de comunicaciones 1924. Tales programas informáticos, cuando se ejecutan, pueden habilitar que el sistema informático 1900 implemente los presentes métodos como se analizan en este documento. En particular, los programas informáticos, cuando se ejecutan, pueden habilitar que el dispositivo de procesador 1904 implemente los métodos ilustrados por las Figuras 6-18, como se analiza en este documento. En consecuencia, tales programas informáticos pueden representar controladores del sistema informático 1900. Donde la presente divulgación se implementa usando software, el software puede almacenarse en un producto de programa informático y cargarse en el sistema informático 1900 usando la unidad de disco de almacenamiento extraíble 1914, interfaz 1920 y unidad de disco duro 1912 o interfaz de comunicaciones 1924.

Técnicas consistentes con la presente divulgación proporcionan, entre otras características, sistemas y métodos para la provisión de credenciales de pago a dispositivos móviles que carecen de un elemento seguro y la generación de criptogramas de pago basados en las mismas. Mientras se han descrito anteriormente diversas realizaciones ilustrativas del sistema y método divulgados debería entenderse que se han presentado para propósitos de ejemplo únicamente, no limitaciones. No es exhaustivo y no limita la divulgación a la forma precisa divulgada.

REIVINDICACIONES

1. Un método para generar y proporcionar credenciales de pago a un dispositivo móvil (104) que carece de un elemento seguro, que comprende:

generar, por un dispositivo de procesamiento de un sistema remoto (110), un perfil de tarjeta asociado con una cuenta de pago, en el que el perfil de tarjeta incluye al menos credenciales de pago que corresponden a la cuenta de pago asociada y un identificador de perfil;
proporcionar, por el sistema remoto, a un dispositivo móvil, el perfil de tarjeta generado;
recibir, por el sistema remoto, desde el dispositivo móvil, una petición de clave, en el que la petición de clave incluye al menos un número de identificación personal, PIN, móvil y el identificador de perfil;
en respuesta a recibir la petición de clave desde el dispositivo móvil, determinar, por un dispositivo de autenticación del sistema remoto, si el PIN móvil es auténtico;
basándose en la determinación de autenticidad del PIN móvil generar, por el dispositivo de procesamiento del sistema remoto, una clave de un solo uso, en el que la clave de un solo uso se configura para usarse una vez, por el dispositivo móvil, para generar un criptograma de pago válido para una única transacción financiera y la clave de un solo uso incluye al menos el identificador de perfil, un contador de transacción de aplicación y una clave de generación; y
transmitir, por un dispositivo de transmisión del sistema remoto, la clave de un solo uso generada al dispositivo móvil, en el que el dispositivo móvil carece de un elemento seguro.

2. El método de la reivindicación 1, comprendiendo además:
transmitir, por el dispositivo de transmisión del sistema remoto, la clave de un solo uso generada a un emisor asociado con la cuenta de pago.

3. El método de la reivindicación 1, en el que proporcionar, por el sistema remoto, el perfil de tarjeta generado al dispositivo móvil incluye crear un mensaje que incluye el perfil de tarjeta generado, generar una clave de encriptación, encriptar el mensaje usando la clave de encriptación generada y proporcionar el mensaje encriptado al dispositivo móvil.

4. El método de la reivindicación 1, en el que transmitir la clave de un solo uso generada al dispositivo móvil incluye crear un mensaje, por el sistema remoto, incluyendo la clave de un solo uso generada, generar una clave de encriptación, encriptar el mensaje usando la clave de encriptación generada y proporcionar el mensaje encriptado al dispositivo móvil.

5. El método de la reivindicación 1, en el que la clave de un solo uso generada está inactiva, comprendiendo dicho método además:

recibir, por el sistema remoto, desde el dispositivo móvil, una indicación de uso de la clave de un solo uso;
activar, por el dispositivo de procesamiento del sistema remoto, la clave de un solo uso generada; y
transmitir, por el dispositivo de transmisión del sistema remoto, una indicación de activación de la clave de un solo uso a un emisor asociado con la cuenta de pago.

6. El método de la reivindicación 1, en el que el criptograma de pago es un criptograma de aplicación o un código de validación de tarjeta dinámico.

7. Un método para generar un criptograma de pago en un dispositivo móvil (104) que carece de un elemento seguro, que comprende:

recibir, por un dispositivo de recepción del dispositivo móvil, un perfil de tarjeta desde un sistema remoto (110), en el que el perfil de tarjeta incluye al menos credenciales de pago que corresponden a una cuenta de pago y un identificador de perfil;
recibir, por un dispositivo de entrada del dispositivo móvil, un número de identificación personal, PIN, móvil introducido por un usuario del dispositivo móvil;
transmitir, por un dispositivo de transmisión del dispositivo móvil, una petición de clave al sistema remoto, en el que la petición de clave incluye al menos el identificador de perfil y un número de identificación personal, PIN, móvil en el que dicha petición de clave provoca que dicho dispositivo remoto genere una clave de un solo uso;
recibir, por el dispositivo de recepción del dispositivo móvil, la clave de un solo uso desde el sistema remoto, en el que la clave de un solo uso se configura para usarse una vez, por el dispositivo móvil, para generar un criptograma de pago válido para una única transacción financiera y la clave de un solo uso incluye al menos un contador de transacción de aplicación, una clave de generación y el identificador de perfil;
generar, por un dispositivo de procesamiento del dispositivo móvil, el criptograma de pago válido para la única transacción financiera basándose en al menos la clave de un solo uso recibida y el PIN móvil; y transmitir, por el dispositivo móvil, a través de comunicación de campo cercano, al menos las credenciales de pago y el criptograma de pago generado a un terminal punto de venta para su uso en una transacción financiera.

8. El método de la reivindicación 7, en el que el criptograma de pago es un criptograma de aplicación o un código de validación de tarjeta dinámico.

9. El método de la reivindicación 7, en el que recibir, por el dispositivo móvil, el perfil de tarjeta incluye recibir un mensaje encriptado que incluye el perfil de tarjeta, generar una clave de sesión móvil y desencriptar el mensaje usando la clave de sesión móvil generada para obtener el perfil de tarjeta incluido.

10. El método de la reivindicación 7, en el que recibir, por el dispositivo móvil, la clave de un solo uso incluye recibir un mensaje encriptado que incluye la clave de un solo uso, generar una clave de sesión móvil y desencriptar el mensaje usando la clave de sesión móvil generada para obtener la clave de un solo uso incluida.

11. El método de la reivindicación 7, comprendiendo además:

recibir, por el dispositivo de entrada del dispositivo móvil, una indicación de uso de la clave de un solo uso recibida;
transmitir, por el dispositivo de transmisión del dispositivo móvil, una petición de activación, en el que la petición de activación incluye al menos el identificador de perfil; y
recibir, por el dispositivo de recepción del dispositivo móvil, una indicación de activación de la clave de un solo uso, en el que las credenciales de pago y criptograma de pago generado se transmiten, por el dispositivo móvil, al terminal punto de venta en respuesta a recibir la indicación de activación de la clave de un solo uso.

12. El método de la reivindicación 11, en el que el criptograma de pago se genera, por el dispositivo móvil, en respuesta a recibir la indicación de activación de la clave de un solo uso.

13. El método de la reivindicación 7, en el que
el perfil de tarjeta se configura para utilizar autenticación de datos local, y
autenticación de datos local incluye uno de (1) intercambiar, en las credenciales de pago, el significado de una fecha de vencimiento y una fecha efectiva, (2) establecer la fecha de vencimiento como una fecha anterior a la fecha de emisión, o (3) establecer la fecha efectiva como una fecha más allá de la fecha de caducidad, o ambas pueden establecerse como la fecha de vencimiento y fecha efectiva según se definen, y establecer un código de acción de emisor configurado para forzar que la transacción financiera sea una transacción en línea.

14. Un sistema (100) para generar y proporcionar credenciales de pago a un dispositivo móvil (104) que carece de un elemento seguro, que comprende:

un dispositivo de transmisión de un sistema remoto (110);
un dispositivo de procesamiento, del sistema remoto configurado para generar un perfil de tarjeta asociado con una cuenta de pago, en el que el perfil de tarjeta incluye al menos credenciales de pago que corresponden a la cuenta de pago asociada y un identificador de perfil;
un dispositivo de aprovisionamiento, del sistema remoto, configurado para proporcionar, a un dispositivo móvil que carece de un elemento seguro, el perfil de tarjeta generado;
un dispositivo de recepción, del sistema remoto, configurado para recibir, desde el dispositivo móvil, una petición de clave, en el que la petición de clave incluye al menos un número de identificación personal, PIN, móvil y el identificador de perfil; y
un dispositivo de autenticación, del sistema remoto, configurado para autenticar el PIN móvil en respuesta a recibir la petición de clave, en el que
el dispositivo de procesamiento, del sistema remoto, se configura adicionalmente para generar una clave de un solo uso sobre una base de autenticidad de PIN móvil, en el que la clave de un solo uso se configura para usarse una vez, por el dispositivo móvil, para generar un criptograma de pago válido para una única transacción financiera y la clave de un solo uso incluye al menos el identificador de perfil, un contador de transacción de aplicación y una clave de generación para su uso en la generación del criptograma de pago válido para la única transacción financiera, y
el dispositivo de transmisión, del sistema remoto, se configura para transmitir la clave de un solo uso generada al dispositivo móvil.

15. El sistema de la reivindicación 14, en el que el dispositivo de transmisión, del sistema remoto, se configura adicionalmente para transmitir la clave de un solo uso generada a un emisor asociado con la cuenta de pago.

16. El sistema de la reivindicación 14, en el que el dispositivo de aprovisionamiento, del sistema remoto, proporciona el perfil de tarjeta generado al dispositivo móvil dentro de un mensaje encriptado por una clave de encriptación.

17. El sistema de la reivindicación 14, en el que el dispositivo de transmisión, del sistema remoto, transmite la clave de un solo uso generada al dispositivo móvil dentro de un mensaje encriptado por una clave de encriptación.

18. El sistema de la reivindicación 14, en el que
la clave de un solo uso generada está inactiva,
el dispositivo de recepción, del sistema remoto, se configura adicionalmente para recibir desde el dispositivo móvil,

una indicación de uso de la clave de un solo uso,
el dispositivo de procesamiento, del sistema remoto, se configura adicionalmente para activar la clave de un solo uso generada, y
el dispositivo de transmisión, del sistema remoto, se configura adicionalmente para transmitir una indicación de activación de la clave de un solo uso a un emisor asociado con la cuenta de pago.

19. Un sistema (100) para generar un criptograma de pago en un dispositivo móvil (104) que carece de un elemento seguro, que comprende:

un dispositivo de procesamiento, del dispositivo móvil;
un dispositivo de recepción, del dispositivo móvil, configurado para recibir un perfil de tarjeta desde un sistema remoto (110), en el que el perfil de tarjeta incluye al menos credenciales de pago que corresponden a una cuenta de pago y un identificador de perfil;
un dispositivo de entrada, del dispositivo móvil, configurado para recibir un número de identificación personal, PIN, móvil introducido por un usuario del dispositivo móvil; y
un dispositivo de transmisión, del dispositivo móvil, configurado para transmitir una petición de clave al sistema remoto, en el que la petición de clave incluye al menos el identificador de perfil y un número de identificación personal, PIN, móvil y provoca que dicho dispositivo remoto genere una clave de un solo uso, en el que

el dispositivo de recepción, del dispositivo móvil, se configura adicionalmente para recibir la clave de un solo uso desde el sistema remoto, en el que la clave de un solo uso se configura para usarse una vez, por el dispositivo móvil, para generar un criptograma de pago válido para una única transacción financiera y la clave de un solo uso incluye al menos un contador de transacción de aplicación, una clave de generación y el identificador de perfil,
el dispositivo de procesamiento, del dispositivo móvil, se configura para generar el criptograma de pago válido para la única transacción financiera basándose en al menos la clave de un solo uso recibida y el PIN móvil, y
el dispositivo de transmisión, del dispositivo móvil, se configura adicionalmente para transmitir, a través de comunicación de campo cercano, al menos las credenciales de pago y el criptograma de pago generado a un terminal punto de venta para su uso en una transacción financiera.

20. El sistema de la reivindicación 19, en el que
el dispositivo de entrada, del dispositivo móvil, se configura adicionalmente para recibir indicación de uso de la clave de un solo uso recibida,
el dispositivo de transmisión, del dispositivo móvil, se configura adicionalmente para transmitir una petición de activación, en el que la petición de activación incluye al menos el identificador de perfil,
el dispositivo de recepción, del dispositivo móvil, se configura adicionalmente para recibir una indicación de activación de la clave de un solo uso, y
el dispositivo de transmisión, del dispositivo móvil, se configura adicionalmente para transmitir las credenciales de pago y el criptograma de pago generado en respuesta una recepción de la indicación de activación de la clave de un solo uso.

21. El sistema de la reivindicación 20, en el que el dispositivo de procesamiento, del dispositivo móvil, se configura para generar el criptograma de pago en respuesta a la recepción de la indicación de activación de la clave de un solo uso.

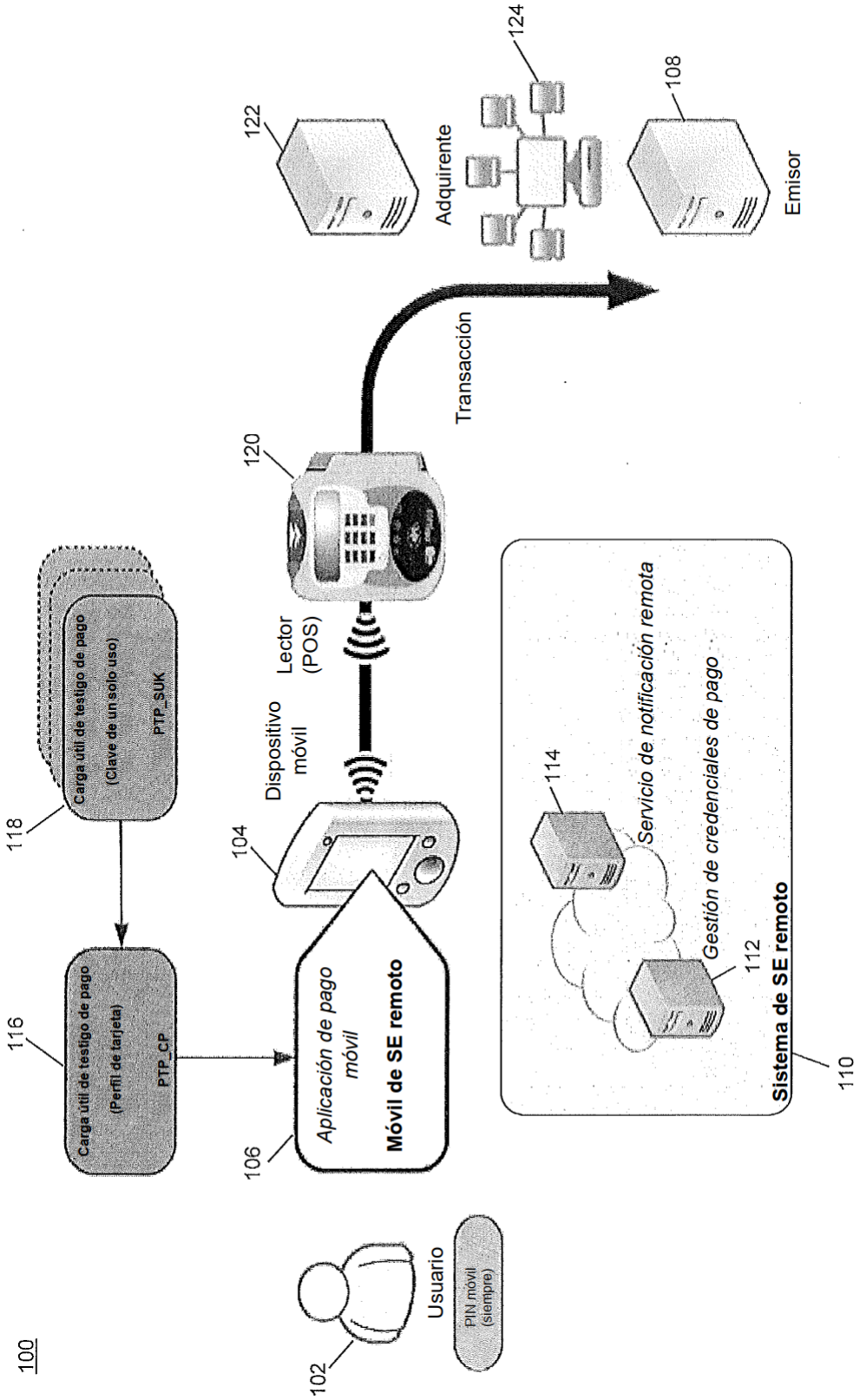
100
102
Usuario
PIN móvil (siempre)
104
Dispositivo móvil
Aplicación de pago móvil
Móvil de SE remoto
106
116
Carga útil de testigo de pago (Perfil de tarjeta)
PTP_CP
118
Carga útil de testigo de pago (Clave de un solo uso)
PTP_SUK
120
Lector (POS)
122
124
Adquirente
108
Emisor
Transacción
110
Sistema de SE remoto
112
Gestión de credenciales de pago
114
Servicio de notificación remota

FIG. 1

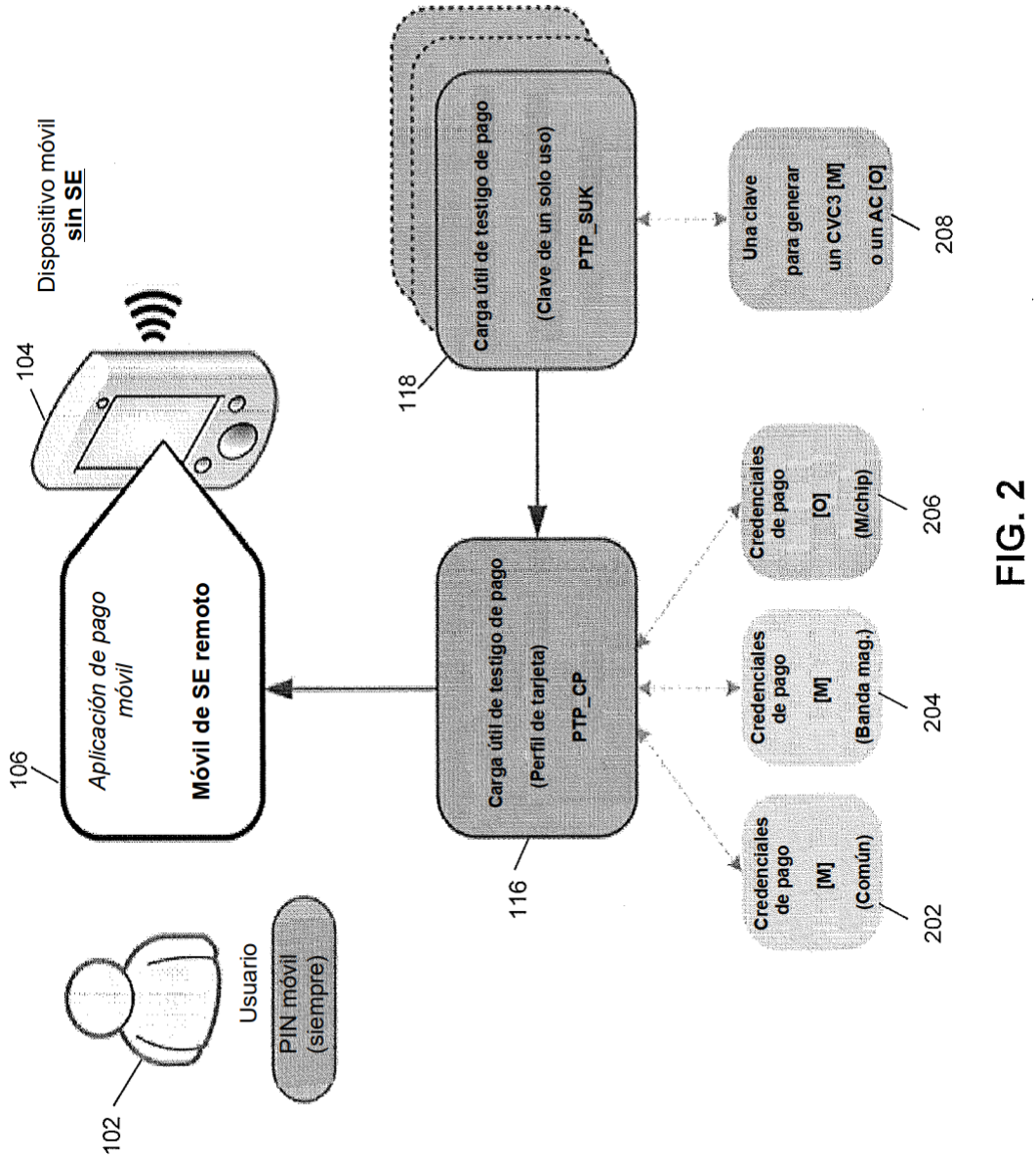
Dispositivo móvil
sin SE
104
Aplicación de pago
móvil
Móvil de SE remoto
106
Usuario
PIN móvil
(siempre)
102
Carga útil de testigo de pago
(Perfil de tarjeta)
PTP_CP
116
Carga útil de testigo de pago
(Clave de un solo uso)
PTP_SUK
118
Credenciales
de pago
[M]
(Común)
202
Credenciales
de pago
[M]
(Banda mag.)
204
Credenciales
de pago
[O]
(M/chip)
206
Una clave
para generar
un CVC3 [M]
o un AC [O]
208

FIG. 2

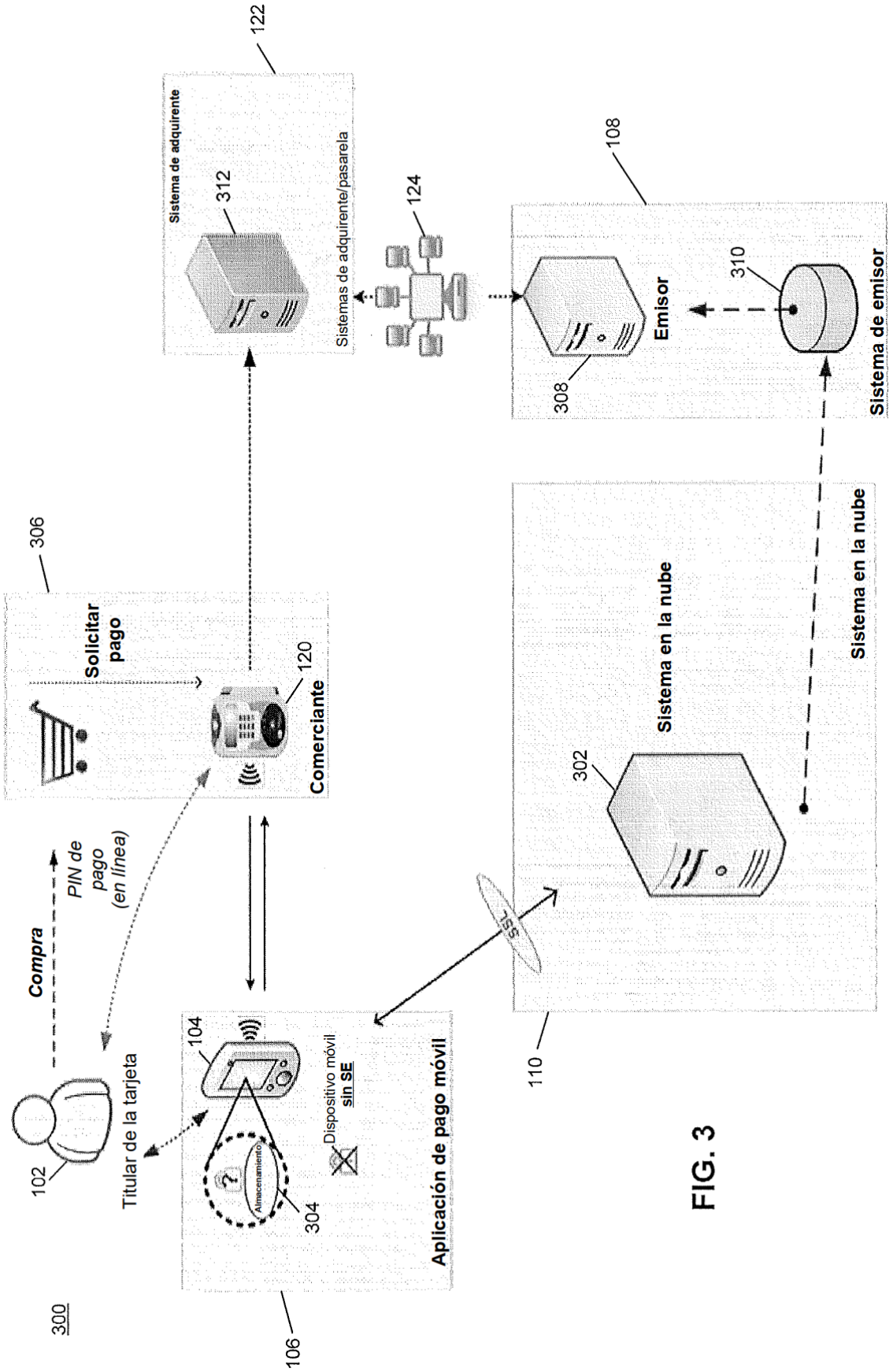
300
102
Titular de la tarjeta
Compra
PIN de pago (en línea)
306
Solicitar pago
120
Comerciante
104
Dispositivo móvil sin SE
Almacenamiento
304
Aplicación de pago móvil
106
SSE
110
Sistema en la nube
302
Sistema en la nube
122
Sistema de adquirente
312
Sistemas de adquirente/pasarela
124
108
Emisor
308
310
Sistema de emisor

FIG. 3

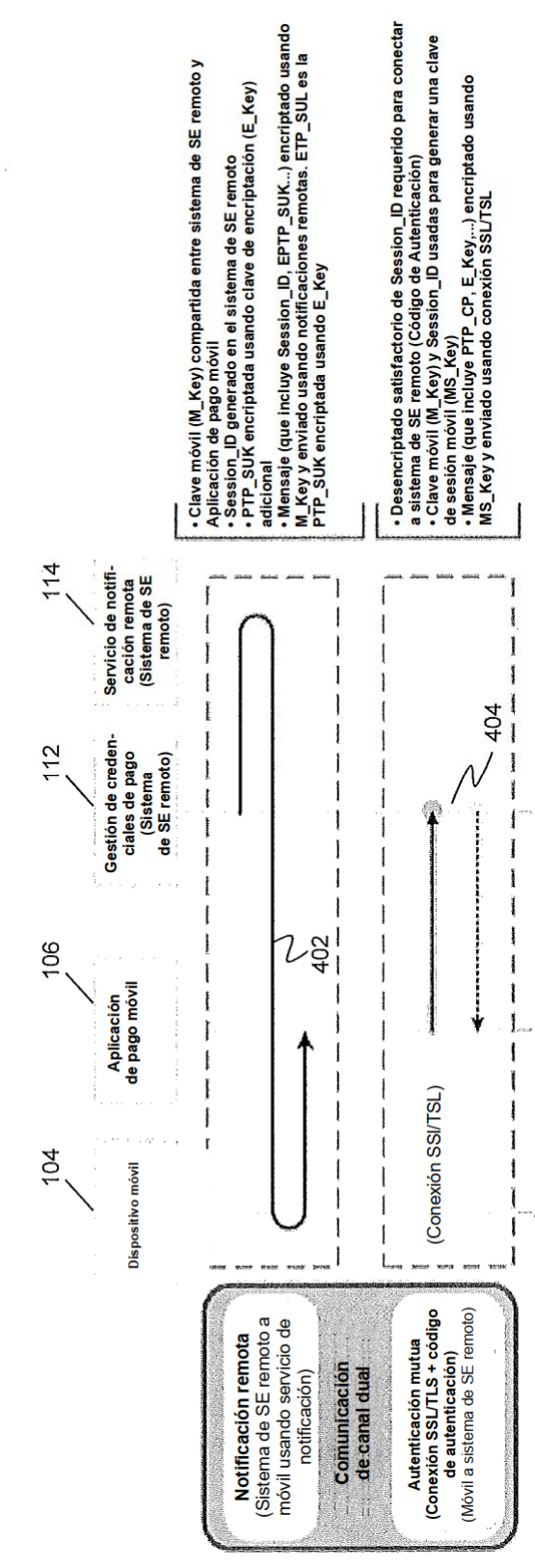
104
106
112
114
Dispositivo móvil
Aplicación de pago móvil
Gestión de credenciales de pago (Sistema de SE remoto)
Servicio de notificación remota (Sistema de SE remoto)
• Clave móvil (M_Key) compartida entre sistema de SE remoto y Aplicación de pago móvil
• Session_ID generado en el sistema de SE remoto
• PTP_SUK encriptada usando clave de encriptación (E_Key) adicional
• Mensaje (que incluye Session_ID, EPTP_SUK...) encriptado usando M_Key y enviado usando notificaciones remotas. ETP_SUL es la PTP_SUK encriptada usando E_Key
• Desencriptado satisfactorio de Session_ID requerido para conectar a sistema de SE remoto (Código de Autenticación)
• Clave móvil (M_Key) y Session_ID usadas para generar una clave de sesión móvil (MS_Key)
• Mensaje (que incluye PTP_CP, E_Key,...) encriptado usando MS_Key y enviado usando conexión SSL/TSL
402
404
(Conexión SSl/TSL)
Notificación remota (Sistema de SE remoto a móvil usando servicio de notificación)
Comunicación de canal dual
Autenticación mutua (Conexión SSL/TLS + código de autenticación) (Móvil a sistema de SE remoto)
Base de datos local encriptada en datos de aplicación de pago móvil (software)
• Clave de encriptación local (definida por aplicación de pago móvil)
• Usada para almacenar:
• Clave móvil (M_Key)
•Información de carga útil de testigo de pago (PTP_CP y PTP_SUK)
PTP_CP
PTP_SUK
304
116
118

FIG. 4

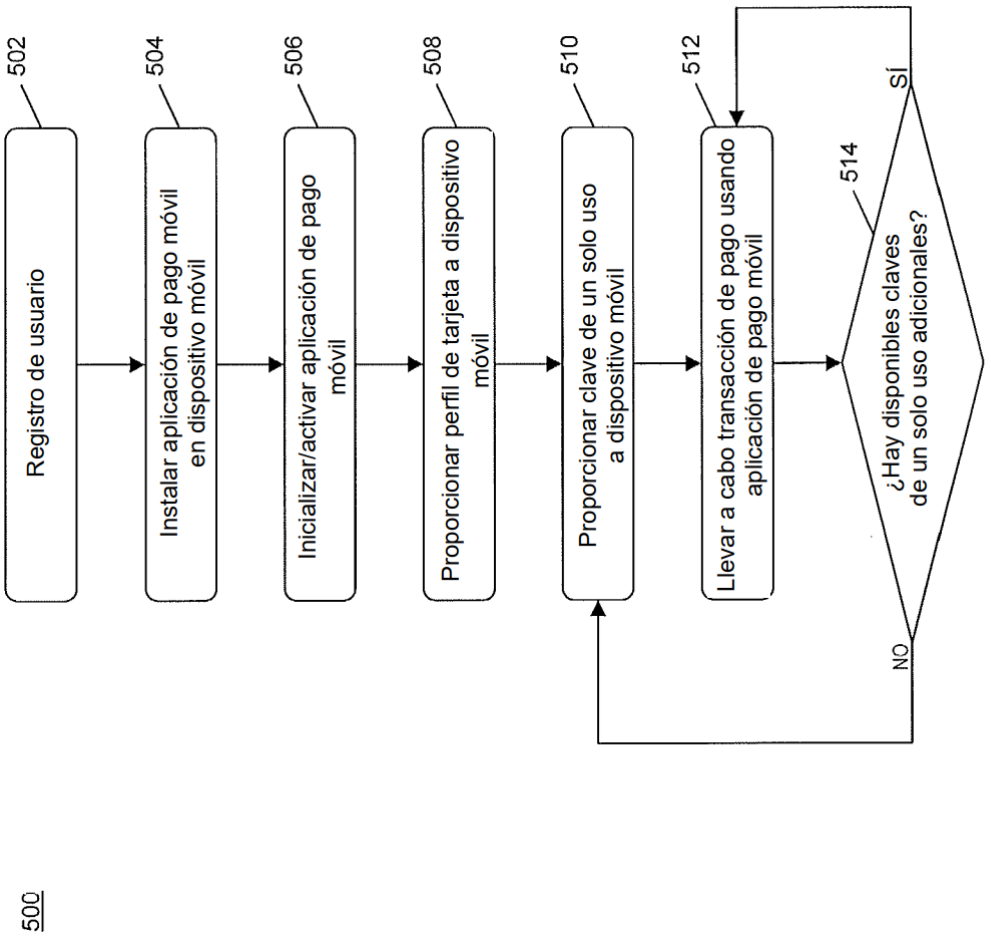
500
502
Registro de usuario
504
Instalar aplicación de pago móvil en dispositivo móvil
506
Inicializar/activar aplicación de pago móvil
508
Proporcionar perfil de tarjeta a dispositivo móvil
510
Proporcionar clave de un solo uso a dispositivo móvil
512
Llevar a cabo transacción de pago usando aplicación de pago móvil
514
¿Hay disponibles claves de un solo uso adicionales?
SÍ
NO

FIG. 5

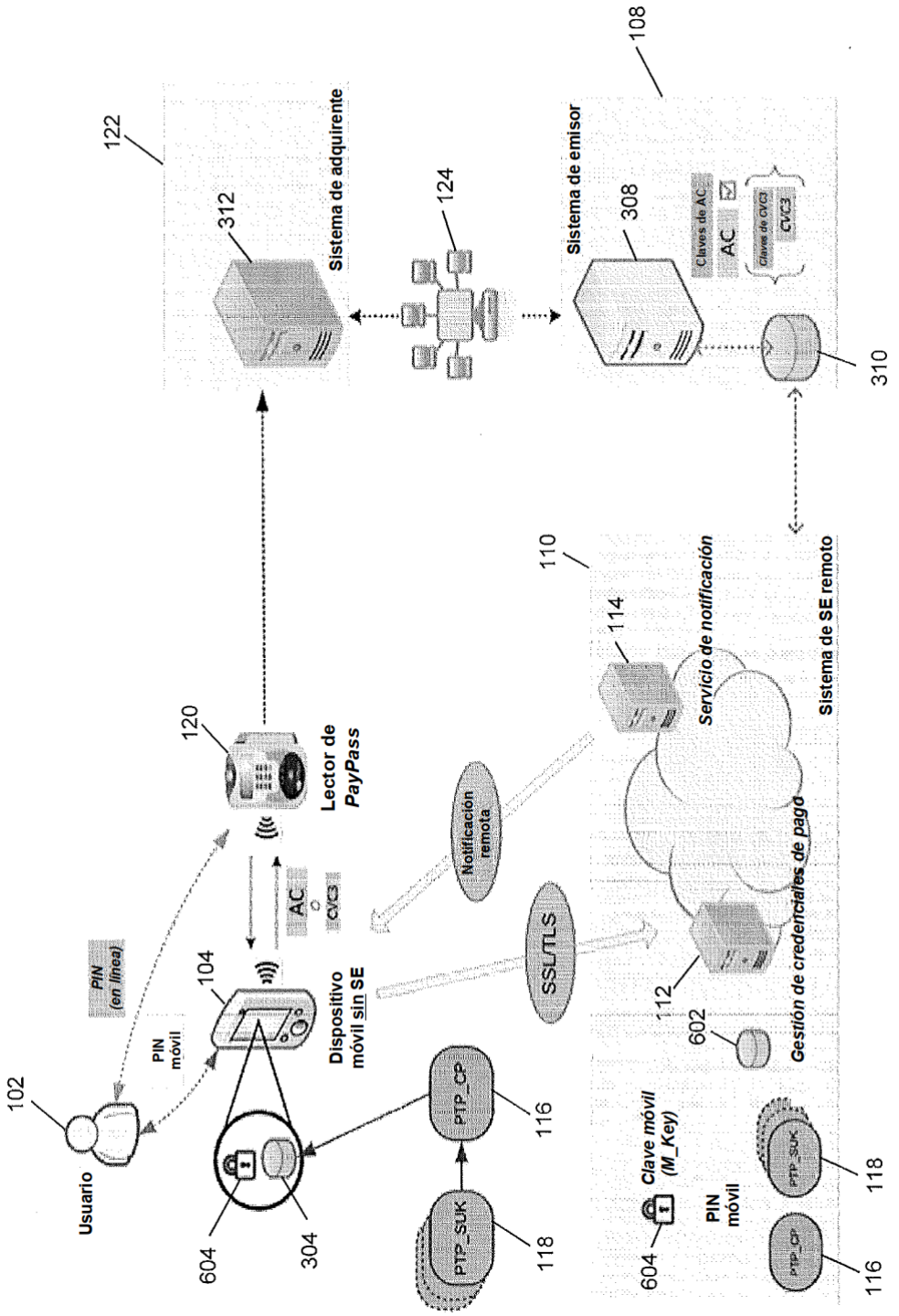
122
Sistema de adquirente
312
124
108
Sistema de emisor
308
Claves de AC
AC
Claves de CVC3
CVC3
310
110
Sistema de SE remoto
114
Servicio de notificación
Gestión de credenciales de pago
112
602
Clave móvil (M_Key)
604
PIN móvil
PTP_SUK
118
PTP_CP
116
120
Lector de PayPass
AC
o
CVC3
Notificación remota
SSL/TLS
104
Dispositivo móvil sin SE
PIN (en línea)
PIN móvil
102
Usuario
604
304
PTP_SUK
118
PTP_CP
116

FIG. 6

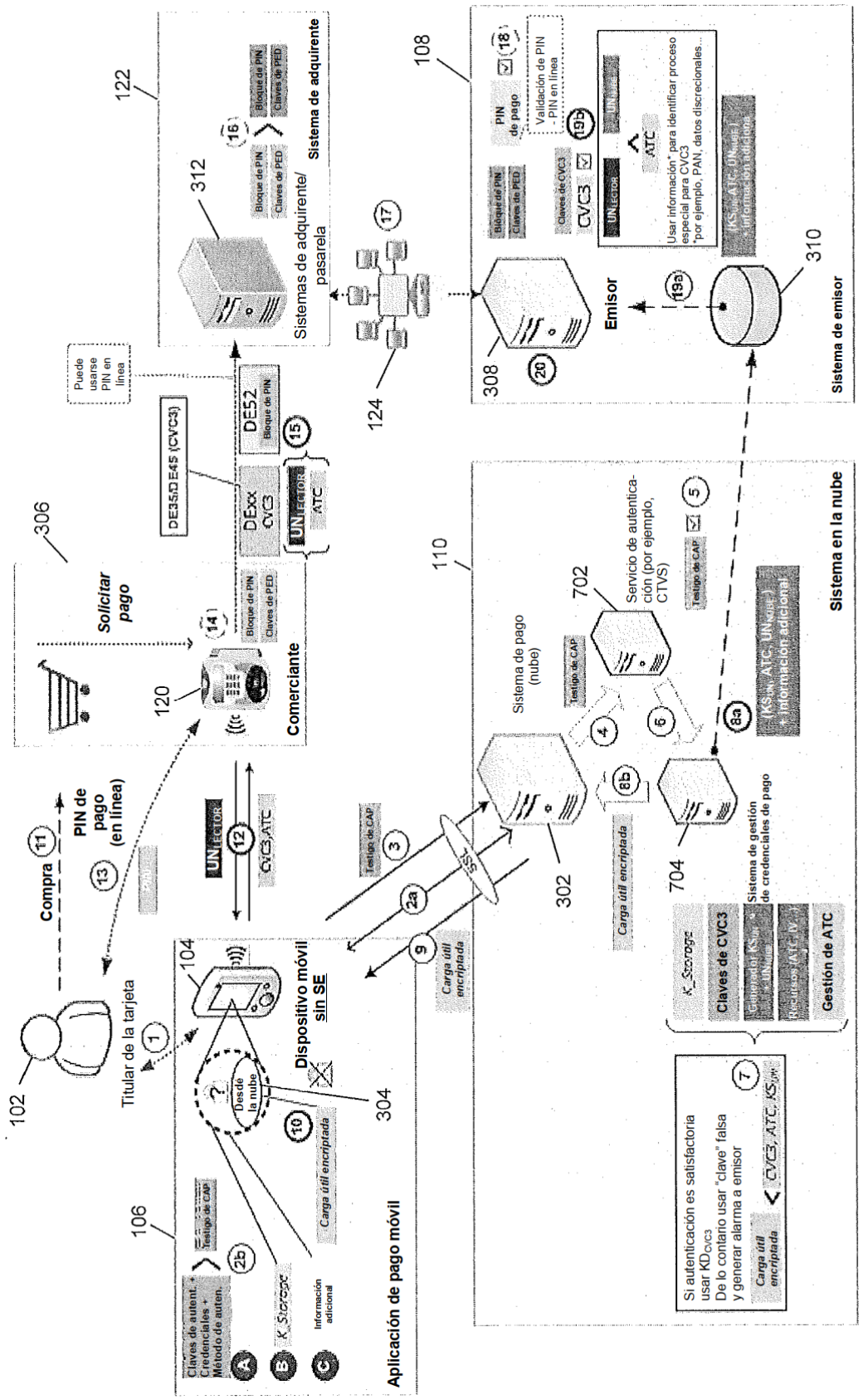
Sistema en la nube
Sistema de emisor
Aplicación de pago móvil
Dispositivo móvil sin SE
Comerciante
Sistemas de adquirente/ pasarela
Sistema de adquirente
Emisor
Sistema de pago (nube)
Servicio de autenticación (por ejemplo, CTVS)
Sistema de gestión de credenciales de pago
Claves de CVC3
Gestión de ATC
Titular de la tarjeta
Compra
PIN de pago (en línea)
Solicitar pago
Puede usarse PIN en línea
Validación de PIN - PIN en línea
Usar información* para identificar proceso especial para CVC3 *por ejemplo, PAN, datos discrecionales...
Si autenticación es satisfactoria usar KDCVC3 De lo contario usar "clave" falsa y generar alarma a emisor
Carga útil encriptada
Testigo de CAP
Desde la nube
Bloque de PIN
Claves de PED
Claves de CVC3
ATC
102
104
106
108
110
120
122
124
302
304
306
308
310
312
702
704

FIG. 7

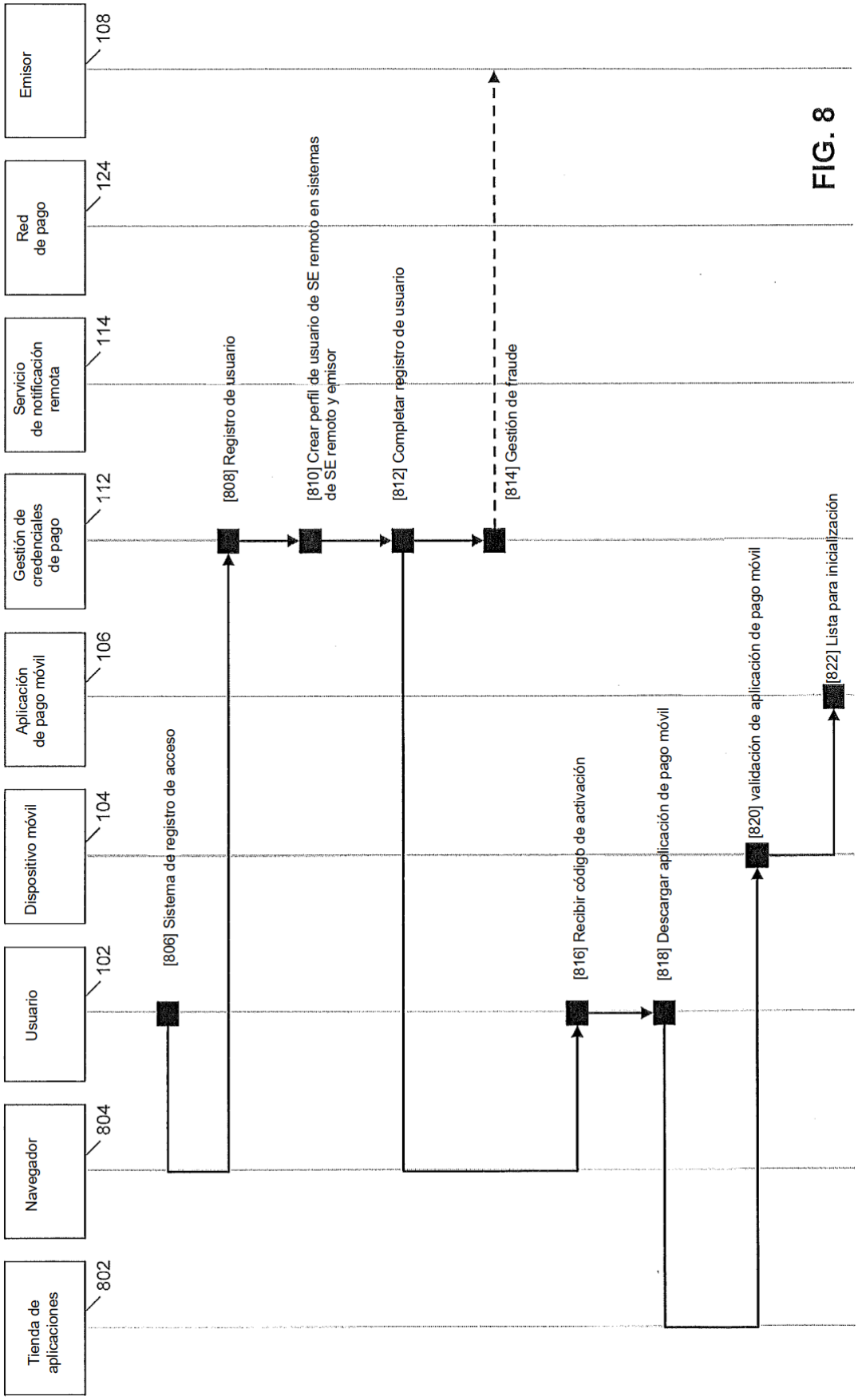
Tienda de aplicaciones
802
Navegador
804
Usuario
102
Dispositivo móvil
104
Aplicación de pago móvil
106
Gestión de credenciales de pago
112
Servicio de notificación remota
114
Red de pago
124
Emisor
108
[806] Sistema de registro de acceso
[808] Registro de usuario
[810] Crear perfil de usuario de SE remoto en sistemas de SE remoto y emisor
[812] Completar registro de usuario
[814] Gestión de fraude
[816] Recibir código de activación
[818] Descargar aplicación de pago móvil
[820] validación de aplicación de pago móvil
[822] Lista para inicialización

FIG. 8

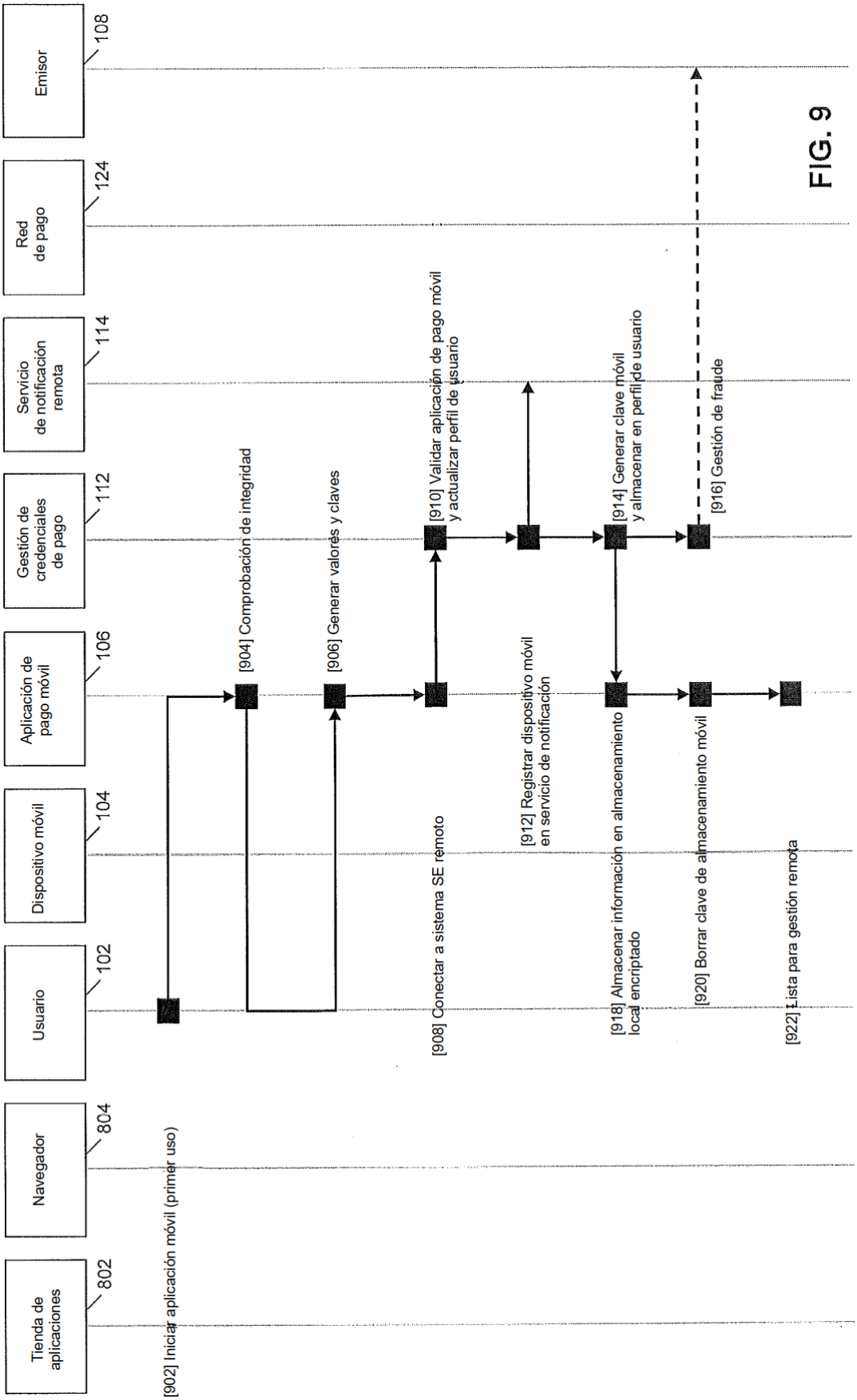
Tienda de aplicaciones
802
Navegador
804
Usuario
102
Dispositivo móvil
104
Aplicación de pago móvil
106
Gestión de credenciales de pago
112
Servicio de notificación remota
114
Red de pago
124
Emisor
108
[902] Iniciar aplicación móvil (primer uso)
[904] Comprobación de integridad
[906] Generar valores y claves
[908] Conectar a sistema SE remoto
[910] Validar aplicación de pago móvil y actualizar perfil de usuario
[912] Registrar dispositivo móvil en servicio de notificación
[914] Generar clave móvil y almacenar en perfil de usuario
[916] Gestión de fraude
[918] Almacenar información en almacenamiento local encriptado
[920] Borrar clave de almacenamiento móvil
[922] Lista para gestión remota

FIG. 9

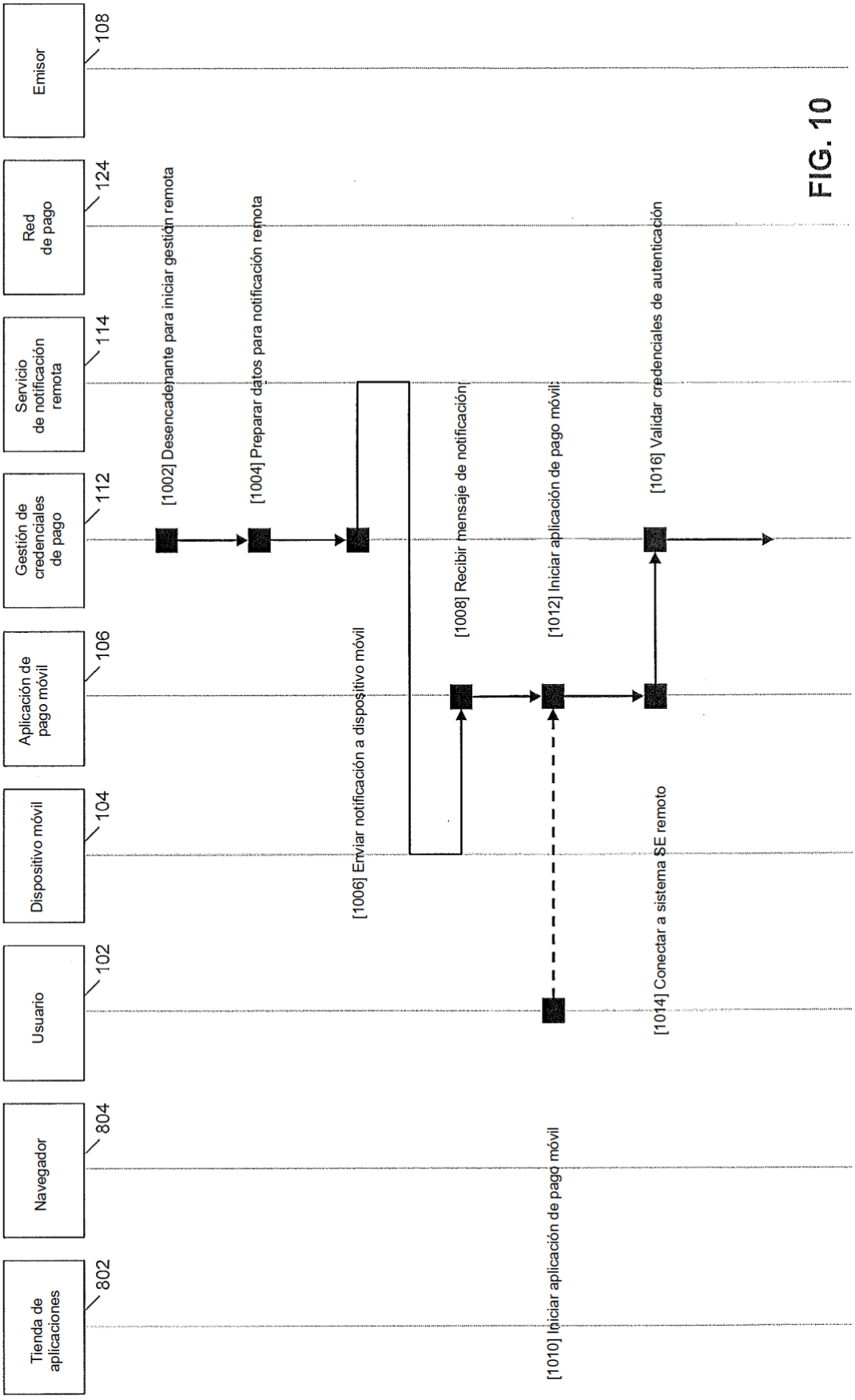
Tienda de aplicaciones
802
Navegador
804
Usuario
102
Dispositivo móvil
104
Aplicación de pago móvil
106
Gestión de credenciales de pago
112
Servicio de notificación remota
114
Red de pago
124
Emisor
108
[1002] Desencadenante para iniciar gestión remota
[1004] Preparar datos para notificación remota
[1006] Enviar notificación a dispositivo móvil
[1008] Recibir mensaje de notificación
[1010] Iniciar aplicación de pago móvil
[1012] Iniciar aplicación de pago móvil
[1014] Conectar a sistema SE remoto
[1016] Validar credenciales de autenticación

FIG. 10

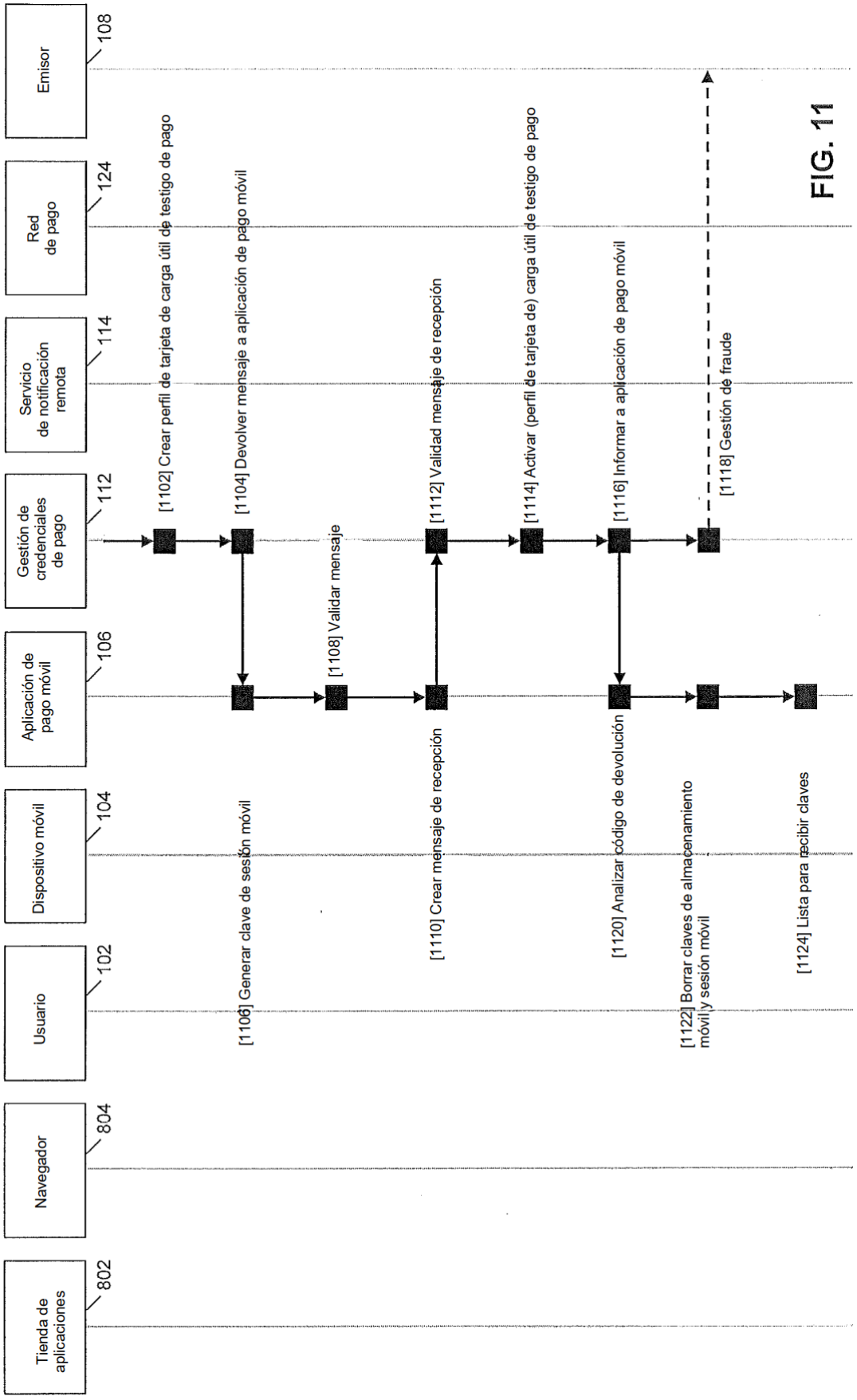
Tienda de aplicaciones
802
Navegador
804
Usuario
102
Dispositivo móvil
104
Aplicación de pago móvil
106
Gestión de credenciales de pago
112
Servicio de notificación remota
114
Red de pago
124
Emisor
108
[1102] Crear perfil de tarjeta de carga útil de testigo de pago
[1104] Devolver mensaje a aplicación de pago móvil
[1106] Generar clave de sesión móvil
[1108] Validar mensaje
[1110] Crear mensaje de recepción
[1112] Validad mensaje de recepción
[1114] Activar (perfil de tarjeta de) carga útil de testigo de pago
[1116] Informar a aplicación de pago móvil
[1118] Gestión de fraude
[1120] Analizar código de devolución
[1122] Borrar claves de almacenamiento móvil y sesión móvil
[1124] Lista para recibir claves

FIG. 11

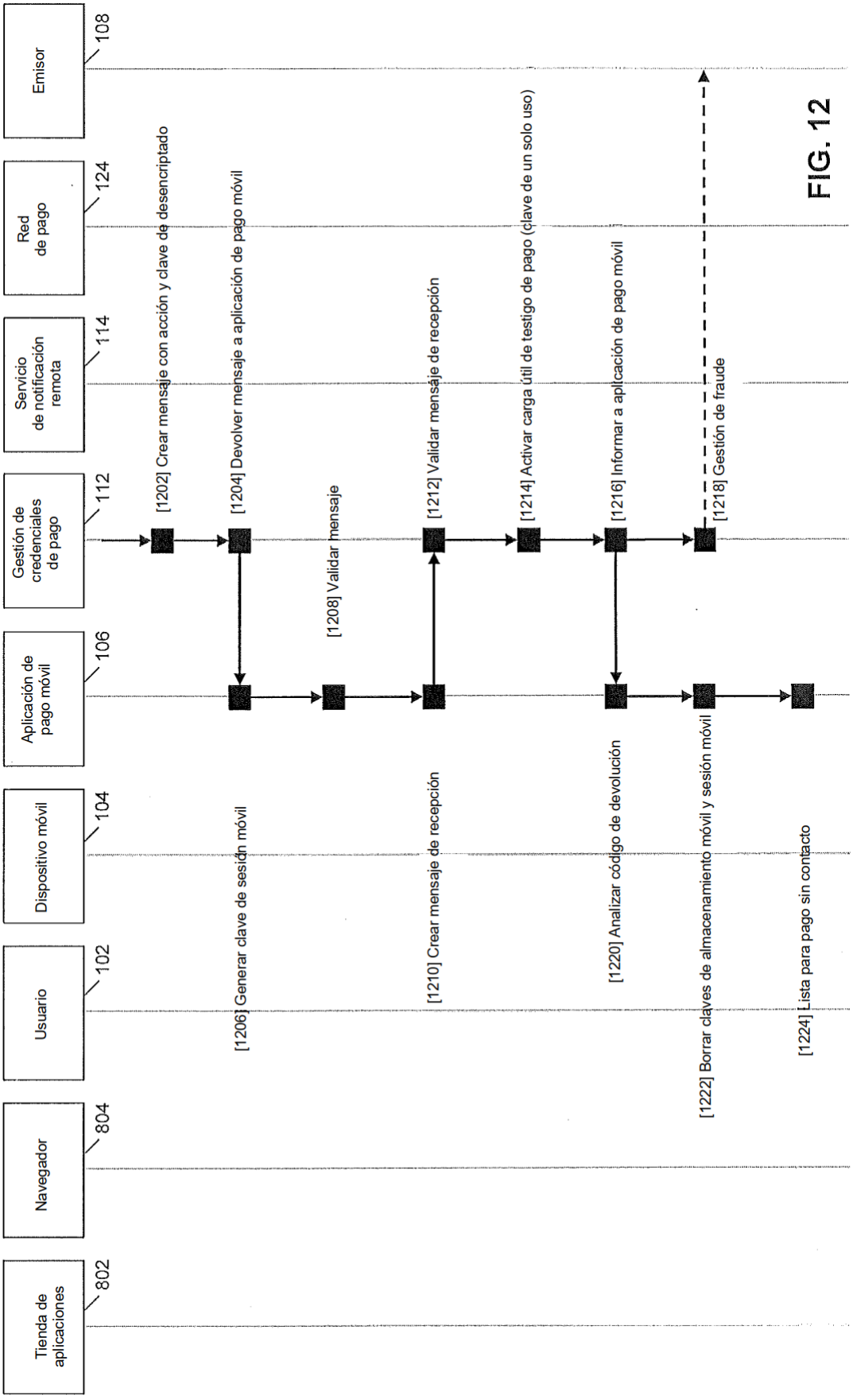
Tienda de aplicaciones
802
Navegador
804
Usuario
102
Dispositivo móvil
104
Aplicación de pago móvil
106
Gestión de credenciales de pago
112
Servicio de notificación remota
114
Red de pago
124
Emisor
108
[1202] Crear mensaje con acción y clave de desencriptado
[1204] Devolver mensaje a aplicación de pago móvil
[1206] Generar clave de sesión móvil
[1208] Validar mensaje
[1210] Crear mensaje de recepción
[1212] Validar mensaje de recepción
[1214] Activar carga útil de testigo de pago (clave de un solo uso)
[1216] Informar a aplicación de pago móvil
[1218] Gestión de fraude
[1220] Analizar código de devolución
[1222] Borrar claves de almacenamiento móvil y sesión móvil
[1224] Lista para pago sin contacto

FIG. 12

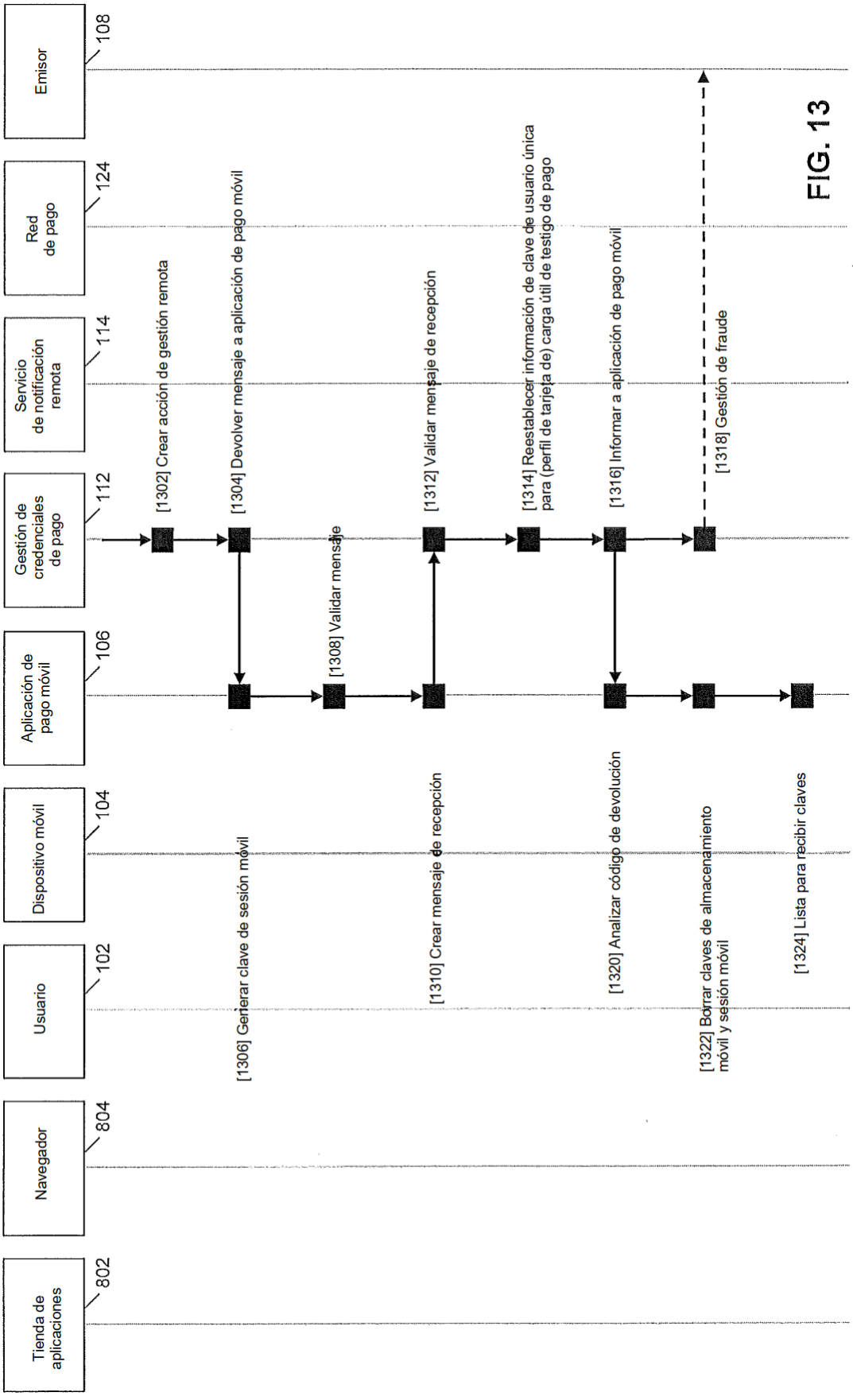
Tienda de aplicaciones
802
Navegador
804
Usuario
102
Dispositivo móvil
104
Aplicación de pago móvil
106
Gestión de credenciales de pago
112
Servicio de notificación remota
114
Red de pago
124
Emisor
108
[1302] Crear acción de gestión remota
[1304] Devolver mensaje a aplicación de pago móvil
[1306] Generar clave de sesión móvil
[1308] Validar mensaje
[1310] Crear mensaje de recepción
[1312] Validar mensaje de recepción
[1314] Reestablecer información de clave de usuario única para (perfil de tarjeta de) carga útil de testigo de pago
[1316] Informar a aplicación de pago móvil
[1318] Gestión de fraude
[1320] Analizar código de devolución
[1322] Borrar claves de almacenamiento móvil y sesión móvil
[1324] Lista para recibir claves

FIG. 13

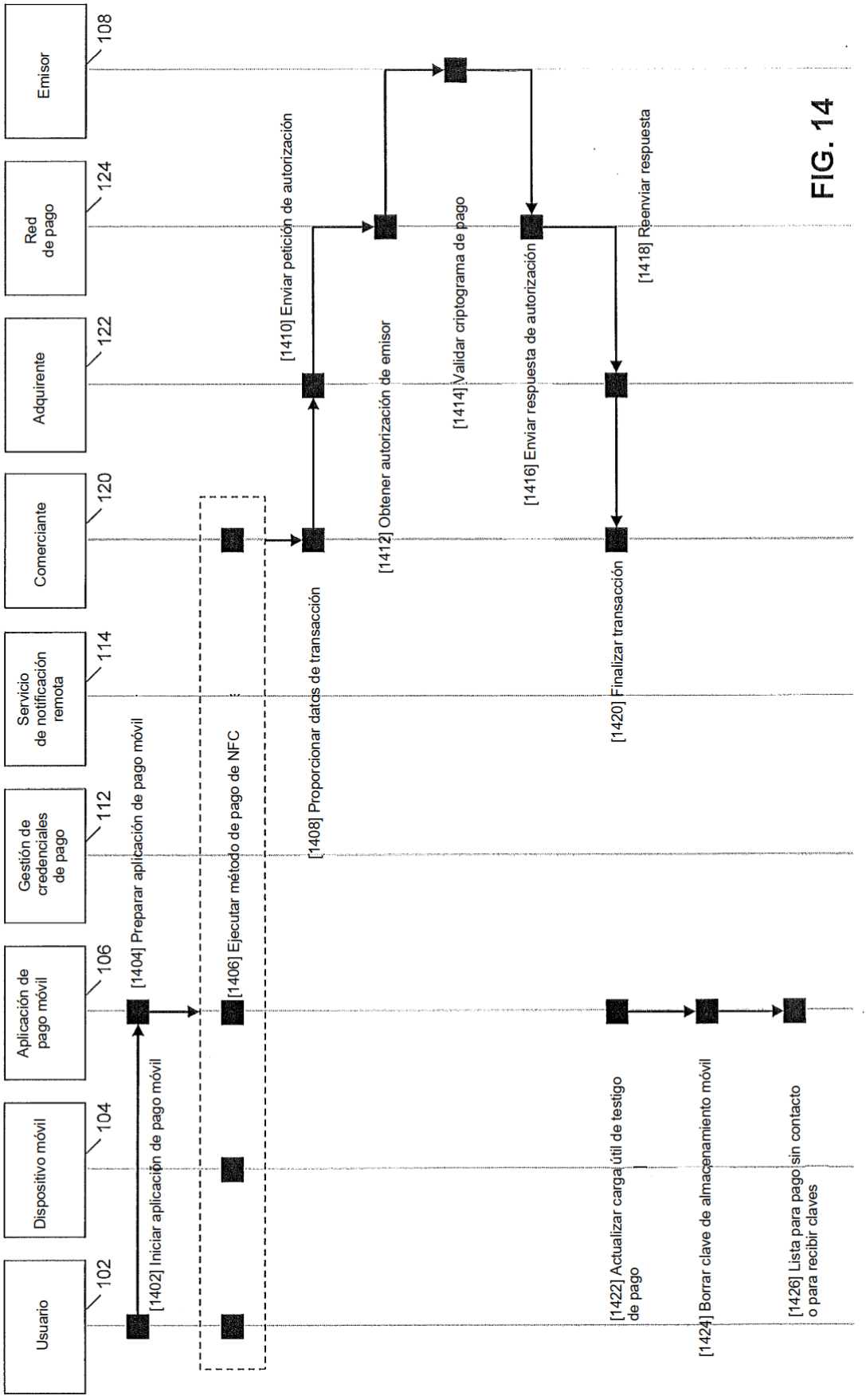
Usuario
102
Dispositivo móvil
104
Aplicación de pago móvil
106
Gestión de credenciales de pago
112
Servicio de notificación remota
114
Comerciante
120
Adquirente
122
Red de pago
124
Emisor
108
[1402] Iniciar aplicación de pago móvil
[1404] Preparar aplicación de pago móvil
[1406] Ejecutar método de pago de NFC
[1408] Proporcionar datos de transacción
[1410] Enviar petición de autorización
[1412] Obtener autorización de emisor
[1414] Validar criptograma de pago
[1416] Enviar respuesta de autorización
[1418] Reenviar respuesta
[1420] Finalizar transacción
[1422] Actualizar carga útil de testigo de pago
[1424] Borrar clave de almacenamiento móvil
[1426] Lista para pago sin contacto o para recibir claves

FIG. 14

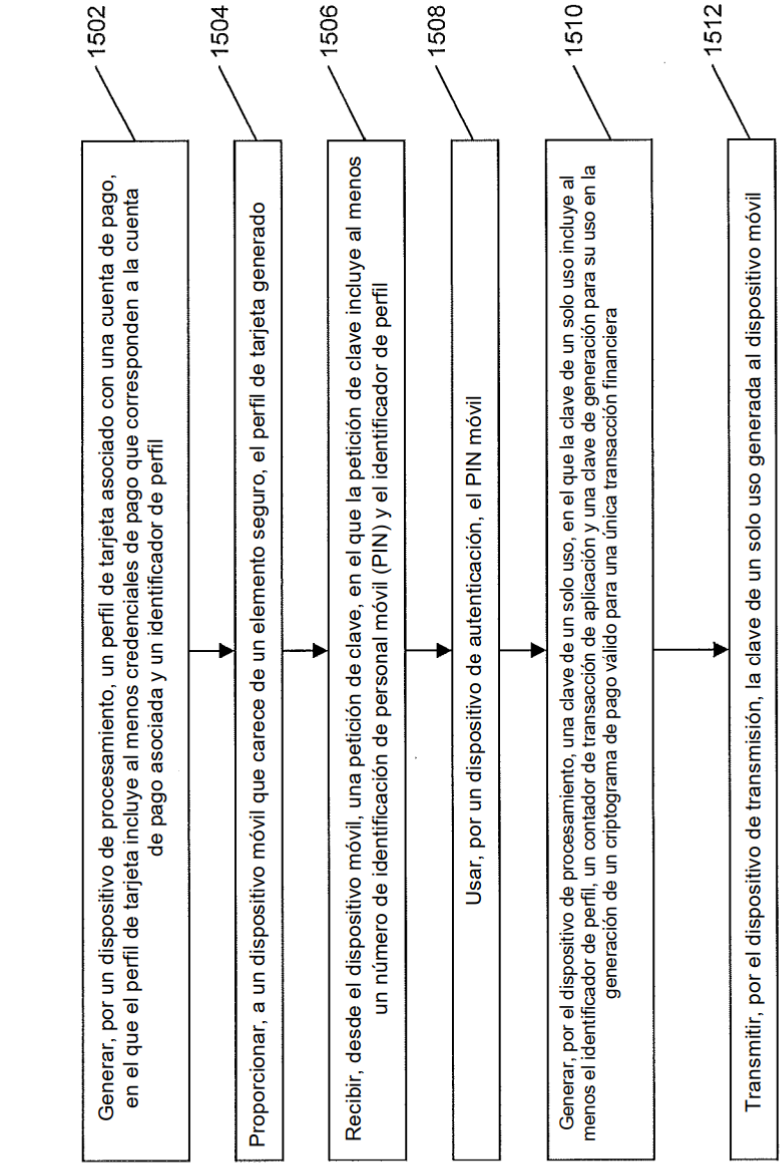
1500
1502
Generar, por un dispositivo de procesamiento, un perfil de tarjeta asociado con una cuenta de pago, en el que el perfil de tarjeta incluye al menos credenciales de pago que corresponden a la cuenta de pago asociada y un identificador de perfil
1504
Proporcionar, a un dispositivo móvil que carece de un elemento seguro, el perfil de tarjeta generado
1506
Recibir, desde el dispositivo móvil, una petición de clave, en el que la petición de clave incluye al menos un número de identificación de personal móvil (PIN) y el identificador de perfil
1508
Usar, por un dispositivo de autenticación, el PIN móvil
1510
Generar, por el dispositivo de procesamiento, una clave de un solo uso, en el que la clave de un solo uso incluye al menos el identificador de perfil, un contador de transacción de aplicación y una clave de generación para su uso en la generación de un criptograma de pago válido para una única transacción financiera
1512
Transmitir, por el dispositivo de transmisión, la clave de un solo uso generada al dispositivo móvil

FIG. 15

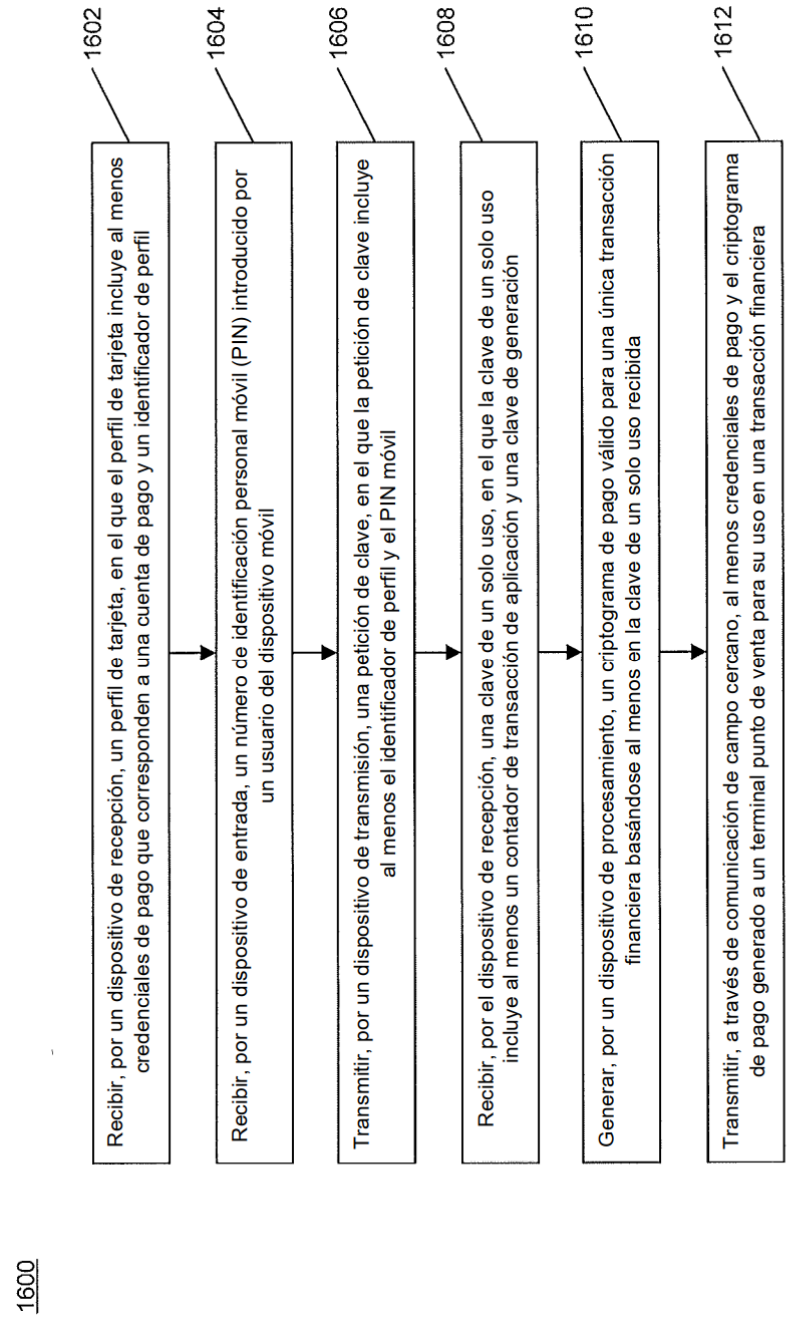
1600
1602
Recibir, por un dispositivo de recepción, un perfil de tarjeta, en el que el perfil de tarjeta incluye al menos credenciales de pago que corresponden a una cuenta de pago y un identificador de perfil
1604
Recibir, por un dispositivo de entrada, un número de identificación personal móvil (PIN) introducido por un usuario del dispositivo móvil
1606
Transmitir, por un dispositivo de transmisión, una petición de clave, en el que la petición de clave incluye al menos el identificador de perfil y el PIN móvil
1608
Recibir, por el dispositivo de recepción, una clave de un solo uso, en el que la clave de un solo uso incluye al menos un contador de transacción de aplicación y una clave de generación
1610
Generar, por un dispositivo de procesamiento, un criptograma de pago válido para una única transacción financiera basándose al menos en la clave de un solo uso recibida
1612
Transmitir, a través de comunicación de campo cercano, al menos credenciales de pago y el criptograma de pago generado a un terminal punto de venta para su uso en una transacción financiera

FIG. 16

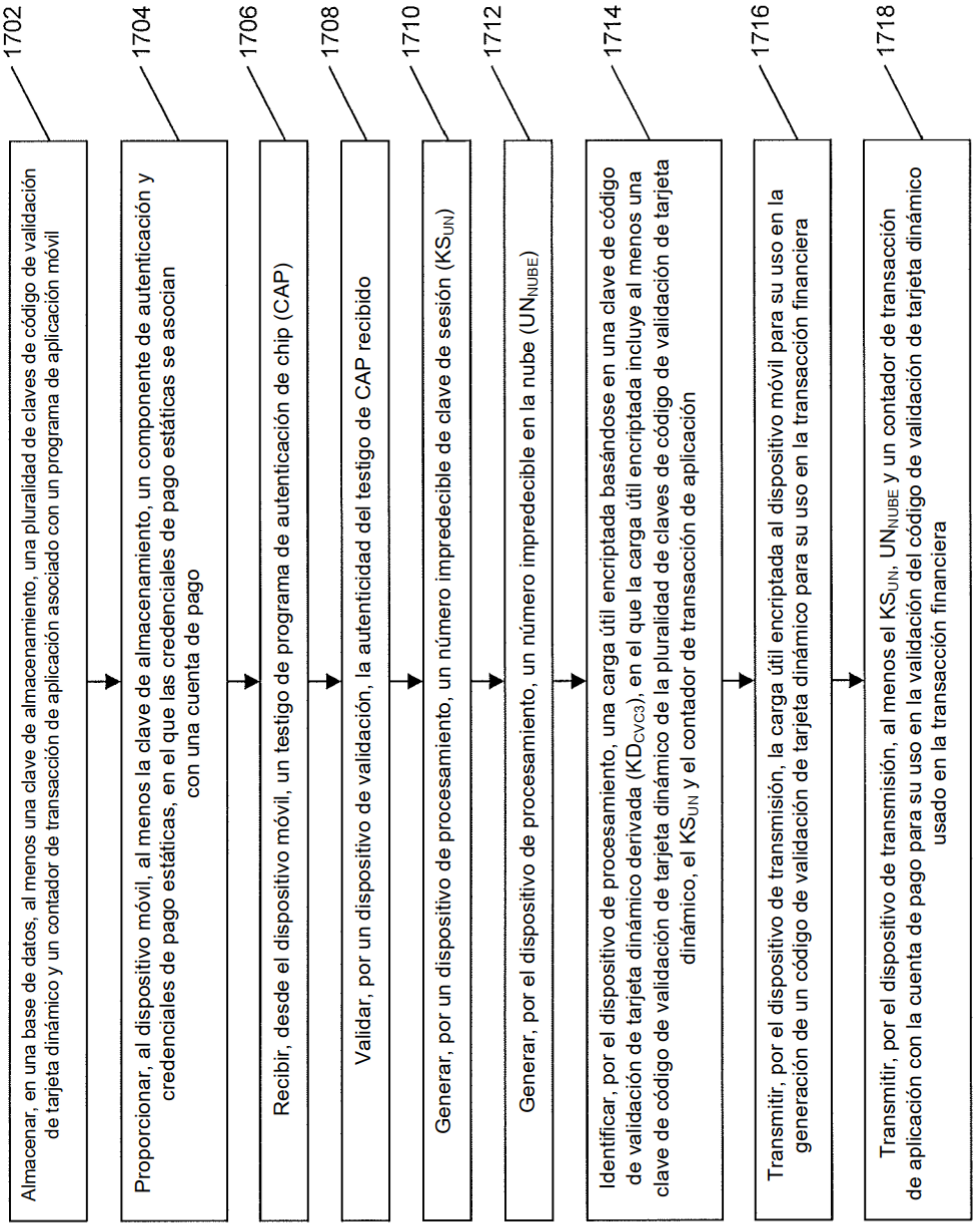
1700
1702
Almacenar, en una base de datos, al menos una clave de almacenamiento, una pluralidad de claves de código de validación de tarjeta dinámico y un contador de transacción de aplicación asociado con un programa de aplicación móvil
1704
Proporcionar, al dispositivo móvil, al menos la clave de almacenamiento, un componente de autenticación y credenciales de pago estáticas, en el que las credenciales de pago estáticas se asocian con una cuenta de pago
1706
Recibir, desde el dispositivo móvil, un testigo de programa de autenticación de chip (CAP)
1708
Validar, por un dispositivo de validación, la autenticidad del testigo de CAP recibido
1710
Generar, por un dispositivo de procesamiento, un número impredecible de clave de sesión (KS_{UN})
1712
Generar, por el dispositivo de procesamiento, un número impredecible en la nube (UN_{NUBE})
1714
Identificar, por el dispositivo de procesamiento, una carga útil encriptada basándose en una clave de código de validación de tarjeta dinámico derivada (KD_{CVC3}), en el que la carga útil encriptada incluye al menos una clave de código de validación de tarjeta dinámico de la pluralidad de claves de código de validación de tarjeta dinámico, el KS_{UN} y el contador de transacción de aplicación
1716
Transmitir, por el dispositivo de transmisión, la carga útil encriptada al dispositivo móvil para su uso en la generación de un código de validación de tarjeta dinámico para su uso en la transacción financiera
1718
Transmitir, por el dispositivo de transmisión, al menos el KS_{UN}, UN_{NUBE} y un contador de transacción de aplicación con la cuenta de pago para su uso en la validación del código de validación de tarjeta dinámico usado en la transacción financiera

FIG. 17

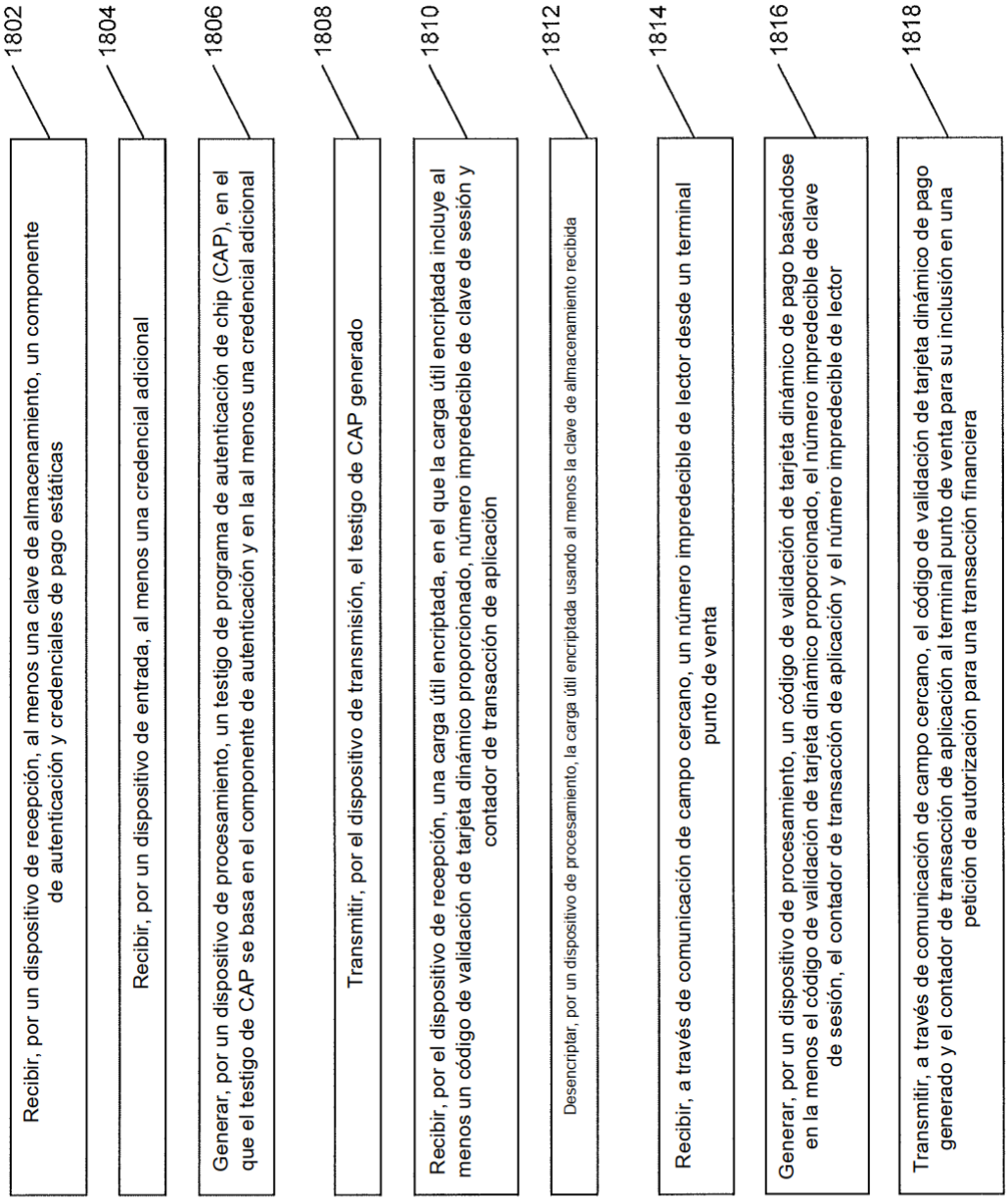
1800
1802
Recibir, por un dispositivo de recepción, al menos una clave de almacenamiento, un componente de autenticación y credenciales de pago estáticas
1804
Recibir, por un dispositivo de entrada, al menos una credencial adicional
1806
Generar, por un dispositivo de procesamiento, un testigo de programa de autenticación de chip (CAP), en el que el testigo de CAP se basa en el componente de autenticación y en la al menos una credencial adicional
1808
Transmitir, por el dispositivo de transmisión, el testigo de CAP generado
1810
Recibir, por el dispositivo de recepción, una carga útil encriptada, en el que la carga útil encriptada incluye al menos un código de validación de tarjeta dinámico proporcionado, número impredecible de clave de sesión y contador de transacción de aplicación
1812
Desencriptar, por un dispositivo de procesamiento, la carga útil encriptada usando al menos la clave de almacenamiento recibida
1814
Recibir, a través de comunicación de campo cercano, un número impredecible de lector desde un terminal punto de venta
1816
Generar, por un dispositivo de procesamiento, un código de validación de tarjeta dinámico de pago basándose en la menos el código de validación de tarjeta dinámico proporcionado, el número impredecible de clave de sesión, el contador de transacción de aplicación y el número impredecible de lector
1818
Transmitir, a través de comunicación de campo cercano, el código de validación de tarjeta dinámico de pago generado y el contador de transacción de aplicación al terminal punto de venta para su inclusión en una petición de autorización para una transacción financiera

FIG. 18

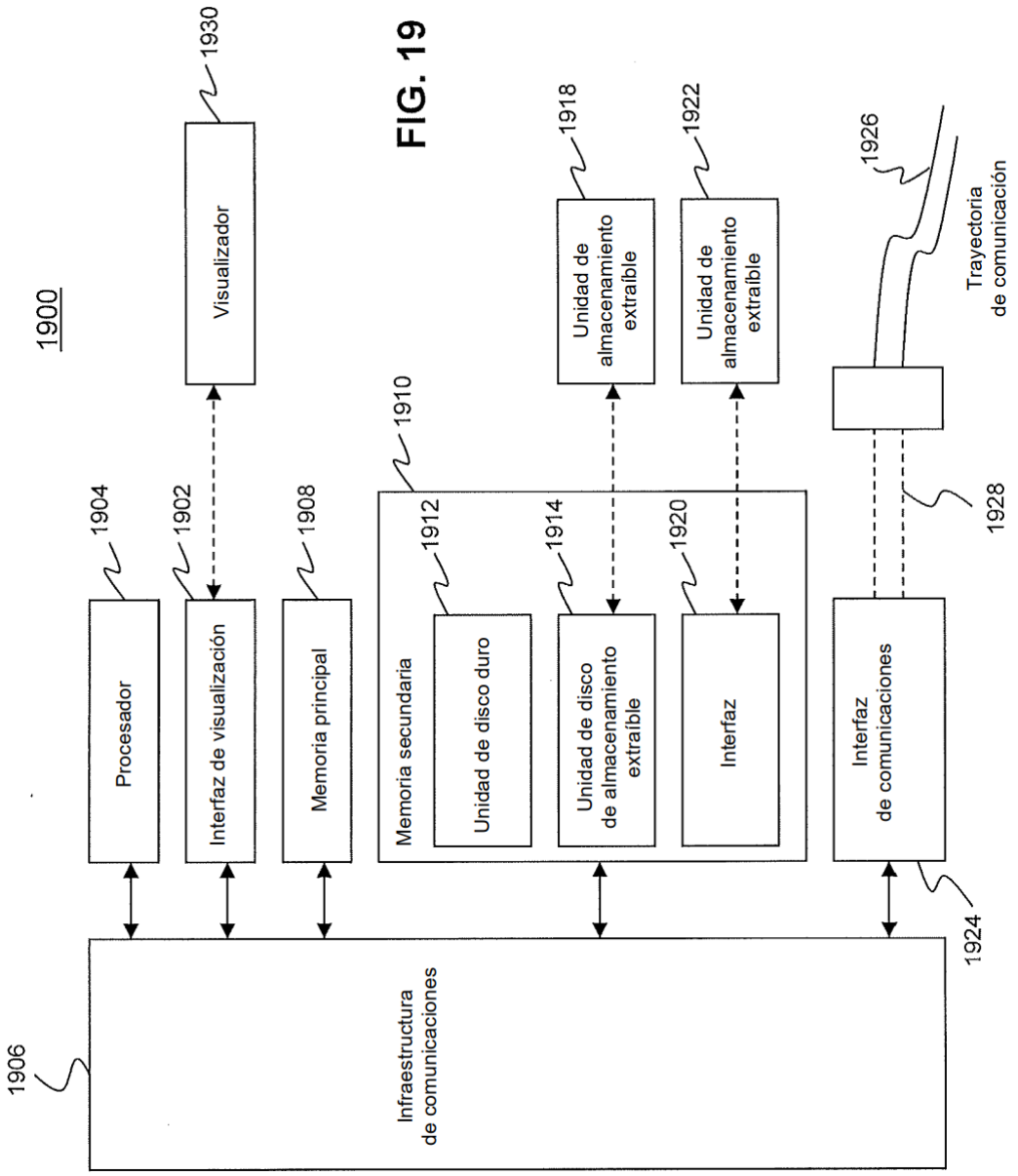
1900
1930
Visualizador
1904
1902
1908
1910
1912
1914
1920
1918
1922
1926
Trayectoria
de comunicación
Procesador
Interfaz de visualización
Memoria principal
Memoria secundaria
Unidad de disco duro
Unidad de disco
de almacenamiento
extraíble
Interfaz
Unidad de
almacenamiento
extraíble
Unidad de
almacenamiento
extraíble
1928
Interfaz
de comunicaciones
1924
1906
Infraestructura
de comunicaciones

FIG. 19