(11) **MX 361793 B**

IMPI
INSTITUTO MEXICANO DE LA PROPIEDAD INDUSTRIAL

(12) **PATENTE**

(43) Fecha de publicación: **17/12/2018**

(22) Fecha de presentación: **02/06/2016**
(21) Número de solicitud: **2016007217**

(51) Int. Cl:
G06Q 20/40 *(2012.01)*
G06Q 20/32 *(2012.01)*
G06Q 20/38 *(2012.01)*
H04L 29/06 *(2006.01)*
H04W 12/06 *(2009.01)*
H04W 12/04 *(2009.01)*

(86) Número de solicitud PCT: **US 2014/067992**
(87) Número de publicación PCT: **WO 2015/084755 (11/06/2015)**

(30) Prioridad(es): **02/12/2013 US 61/910,819**
12/03/2014 US 61/951,842
19/03/2014 US 61/955,716
14/04/2014 US 61/979,132
17/04/2014 US 61/980,784

(71) Solicidante:
MASTERCARD INTERNATIONAL INCORPORATED
2000 Purchase Street 10577 Purchase New York US

(72) Inventor(es):
Mehdi COLLINGE
8, Rue Cesar Franck Braine-l ' Alleud B-1420 BE
Patrik SMETS
Axel Emile Jean Charles CATELAND

(74) Representante:
Sergio Luis OLIVARES LOBATO
Pedro Luis Ogazón 17 ALVARO OBREGON Ciudad de México 01000 MX

(54) Título: **MÉTODO Y SISTEMA PARA LA AUTENTIFICACIÓN SEGURA DEL USUARIO Y EL DISPOSITIVO MÓVIL SIN ELEMENTOS DE SEGURIDAD.**

(54) Title: **METHOD AND SYSTEM FOR SECURE AUTHENTICATION OF USER AND MOBILE DEVICE WITHOUT SECURE ELEMENTS.**

(57) Resumen

Un método para generar credenciales de pago en una transacción de pago incluye: almacenar, en una memoria, por lo menos una llave de un solo uso asociada con una cuenta de transacciones; recibir, mediante un dispositivo de recepción, un número de identificación personal; identificar, mediante un dispositivo de procesamiento, una primera llave de sesión; generar, mediante el dispositivo de procesamiento, una segunda llave de sesión basándose en por lo menos la llave de un solo uso almacenada y el número de identificación personal recibido; generar, mediante el dispositivo de procesamiento, un primer criptograma de la aplicación basándose en por lo menos la primera llave de sesión; generar, mediante el dispositivo de procesamiento, un segundo criptograma de la aplicación basándose en por lo menos la segunda llave de sesión; y transmitir, mediante un dispositivo de transmisión, por lo menos el primer criptograma de la aplicación y el segundo criptograma de la aplicación para utilizarse en una transacción de pago.

(57) Abstract

A method for generating payment credentials in a payment transaction includes: storing, in a memory, at least a single use key associated with a transaction account; receiving, by a receiving device, a personal identification number; identifying, by a processing device, a first session key; generating, by the processing device, a second session key based on at least the stored single use key and the received personal identification number; generating, by the processing device,

a first application cryptogram based on at least the first session key; generating, by the processing device, a second application cryptogram based on at least the second session key; and transmitting, by a transmitting device, at least the first application cryptogram and second application cryptogram for use in a payment transaction.

SE
SECRETARÍA DE ECONOMÍA

IMPI
INSTITUTO MEXICANO DE LA PROPIEDAD INDUSTRIAL

TÍTULO DE PATENTE No. 361793

Titular(es): MASTERCARD INTERNATIONAL INCORPORATED

Domicilio: 2000 Purchase Street, Purchase, New York, 10577, E.U.A.

Denominación: MÉTODO Y SISTEMA PARA LA AUTENTIFICACIÓN SEGURA DEL USUARIO Y EL DISPOSITIVO MÓVIL SIN ELEMENTOS DE SEGURIDAD.

Clasificación: **CIP:** G06Q20/40; G06Q20/32; G06Q20/38; H04L29/06; H04W12/04; H04W12/06
CPC: G06Q20/401; G06Q20/204; G06Q20/322; G06Q20/3829

Inventor(es): MEHDI COLLINGE; PATRIK SMETS; AXEL EMILE JEAN CHARLES CATELAND

SOLICITUD

Número: MX/a/2016/007217

Fecha de Presentación Internacional: 2 de Diciembre de 2014

PRIORIDAD

País:	Fecha:	Número:
US	2 de diciembre de 2013	61/910,819
US	12 de marzo de 2014	61/951,842
US	19 de marzo de 2014	61/955,716
US	14 de abril de 2014	61/979,132
US	17 de abril de 2014	61/980,784

Vigencia: Veinte años

Fecha de Vencimiento: 2 de diciembre de 2034

Fecha de Expedición: 17 de diciembre de 2018

La patente de referencia se otorga con fundamento en los artículos 1º, 2º fracción V, 6º fracción III, y 59 de la Ley de la Propiedad Industrial.

De conformidad con el artículo 23 de la Ley de la Propiedad Industrial, la presente patente tiene una vigencia de veinte años improrrogables, contada a partir de la fecha de presentación de la solicitud internacional y estará sujeta al pago de la tarifa para mantener vigentes los derechos.

Quien suscribe el presente título lo hace con fundamento en lo dispuesto por los artículos 6º fracciones III y 7º bis 2 de la Ley de la Propiedad Industrial (Diario Oficial de la Federación (D.O.F.) 27/06/1991, reformada el 02/08/1994, 25/10/1996, 26/12/1997, 17/05/1999, 26/01/2004, 16/06/2005, 25/01/2006, 06/05/2009, 06/01/2010, 18/06/2010, 28/06/2010, 27/01/2012, 09/04/2012, 01/06/2016 y 13/03/2018); artículos 1º, 3º fracción V inciso a), 4º y 12º fracciones I y III del Reglamento del Instituto Mexicano de la Propiedad Industrial (D.O.F. 14/12/1999, reformado el 01/07/2002, 15/07/2004, 28/07/2004 y 7/09/2007); artículos 1º, 3º, 4º, 5º fracción V inciso a), 16 fracciones I y III y 30 del Estatuto Orgánico del Instituto Mexicano de la Propiedad Industrial (D.O.F. 27/12/1999, reformado el 10/10/2002, 29/07/2004, 04/08/2004 y 13/09/2007); 1º, 3º y 5º inciso a) del Acuerdo que delega facultades en los Directores Generales Adjuntos, Coordinador, Directores Divisionales, Titulares de las Oficinas Regionales, Subdirectores Divisionales, Coordinadores Departamentales y otros subalternos del Instituto Mexicano de la Propiedad Industrial. (D.O.F. 15/12/1999, reformado el 04/02/2000, 29/07/2004, 04/08/2004 y 13/09/2007).

El presente oficio se signa con firma electrónica avanzada (FIEL), con fundamento en los artículos 7 BIS 2 de la Ley de la Propiedad Industrial; 3o de su Reglamento, y 1 fracción III, 2 fracción V, 26 BIS y 26 TER del Acuerdo por el que se establecen los lineamientos para el uso del Portal de Pagos y Servicios Electrónicos (PASE) del Instituto Mexicano de la Propiedad Industrial, en los trámites que se indican.

LA DIRECTORA DIVISIONAL DE PATENTES
NAHANNY CANAL REYES

Cadena Original:
NAHANNY MARISOL CANAL REYES|00001000000403252793|Servicio de Administración Tributaria|1695||MX/2019/13293|MX/a/2016/007217|Título de patente PCT|1027|RGZ|Pág(s) 1|VrXoNJw/GLR/fzdpw6pdWRGat74=

Sello Digital:
Z5YtloHEzvhIll5MFuWjNO0UTAtDHFfaSGF9u6OkBQveoWui2RVmSbwgbitXAfyQsJe7bpy3O0mzK3vqK0nPOhOtJ9
1SbmSudGRH5KVap0WdtdV+IXHfLEGDE8u3cZXkfv9mq+9eZdc4XoapThx7Hr/R9V+uIQival04IfU8qA1ZmL0Nxu64
uP0LwkD3OTdWv9tXnPDdprm3L/GljWdvr2MSbc1jqZ1Lv2/gwMQATy9Cthyt4JFKSveWi8wztXAc2cbCcUMLv1RgKl
gMRx1QR+Qj5jP32tO1KsMKgxc5oCTB7Wgrk1zNATpg+Y50hw/KxD+oZKc8mi0hxQNQ+Ps8bQ==

Arenal No. 550, Piso 1, Pueblo Santa María Tepepan, Xochimilco, 16020,
Ciudad de México.
(55)53340700 www.gob.mx/impi

MX/2019/13293

MÉTODO Y SISTEMA PARA LA AUTENTIFICACIÓN DEL USUARIO Y EL DISPOSITIVO MÓVIL SIN ELEMENTOS DE SEGURIDAD

SOLICITUDES RELACIONADAS

Esta solicitud reclama el beneficio de acuerdo con el Título 35 del Código de los Estados Unidos, Sección 119 (e), de las solicitudes provisionales de patente previamente presentadas números 61/979,122 presentada el 14 de abril de 2014; 61/996,665 presentada el 14 de mayo de 2014; 61/979,113 presentada el 14 de abril de 2014; y en particular las solicitudes provisionales de patente números 61/910,819 presentada el 2 de diciembre de 2013; 61/951,842 presentada el 12 de marzo de 2014; 61/955,716 presentada el 19 de marzo de 2014; 61/979,132 presentada el 14 de abril de 2014; y 61/980,784 presentada el 17 de abril de 2014; cada una incorporada a la presente como referencia en su totalidad.

CAMPO DE LA INVENCIÓN

La presente descripción se refiere a la autentificación de un usuario y un dispositivo móvil sin requerir de un elemento de seguridad en una transacción de pago, y más específicamente, a la generación de credenciales de pago en un dispositivo móvil utilizado en una transacción de pago sin el uso de elementos de seguridad.

ANTECEDENTES DE LA INVENCIÓN

Los avances en las tecnologías móviles y de comunicaciones han creado enormes oportunidades, una de las cuales está

proporcionando al usuario de un dispositivo informático la capacidad para iniciar y pagar transacciones de pago utilizando su dispositivo móvil. Uno de estos planteamientos para permitir este tipo de acciones en un dispositivo móvil ha sido el uso de la tecnología de comunicación de campo cercano (NFC) para transmitir de una forma segura los detalles del pago desde el dispositivo móvil hasta una terminal del punto de venta (POS) cercana sin contacto. Con el fin de lograr esto, los teléfonos móviles con hardware de elementos de seguridad, tal como un chip de elemento de seguridad (SE), se utilizan para almacenar de una forma segura las credenciales de pago. Un elemento de seguridad es un elemento especial que se puede incluir en algunos dispositivos habilitados con comunicación de campo cercano (NFC) que es una plataforma inviolable que puede albergar de una forma segura las aplicaciones y sus datos confidenciales.

Sin embargo, no todos los dispositivos móviles tienen elementos de seguridad. Además, algunas instituciones financieras pueden no tener acceso a los elementos de seguridad de los dispositivos móviles, incluso si el dispositivo móvil está equipado con un elemento de este tipo. Como resultado, muchos consumidores con dispositivos móviles que poseen el hardware requerido para conducir transacciones sin contacto u otros tipos de transacciones de pago a distancia pueden ser incapaces de utilizar realmente esta capacidad. Debido a estas dificultades, existe una necesidad de una solución técnica para hacer posible que los dispositivos informáticos móviles

inicien y conduzcan las transacciones de pago sin elementos de seguridad.

Algunos métodos y sistemas para la realización de transacciones de pago utilizando dispositivos móviles que carecen de elementos de seguridad, o sin el uso de elementos de seguridad en dispositivos móviles equipados con ellos, se pueden encontrar en la Solicitud de Patente de los Estados Unidos de Norteamérica Número 13/827,042 titulada como "Systems and Methods for Processing Mobile Payments by Provisioning Credentials to Mobile Devices Without Secure Elements", por Mehdi Collinge y colaboradores, presentada el 14 de marzo de 2013, la cual se incorpora a la presente como referencia en su totalidad. Si bien tales métodos y sistemas pueden ser adecuados para la realización de transacciones de pago por medio de un dispositivo móvil sin la necesidad de utilizar un elemento de seguridad, muchos consumidores, comerciantes e instituciones financieras pueden ser reacios a participar en dichas transacciones debido a un deseo de tener una seguridad todavía mayor.

Como resultado, existe una necesidad de soluciones técnicas para proporcionar aún más seguridad para la recepción y el almacenamiento de credenciales de pago en un dispositivo móvil que carezca de un elemento de seguridad, así como para proporcionar una mayor seguridad en la transmisión de credenciales de pago a un punto de venta desde el dispositivo móvil durante la realización de una transacción financiera. La mayor seguridad en estos procesos

puede dar como resultado una mayor tranquilidad de las entidades involucradas, lo cual puede dar como resultado un aumento en el uso de los dispositivos móviles para las transacciones de pago sin contacto o a distancia, lo cual puede proporcionar un gran número de beneficios a los consumidores sobre los métodos tradicionales de pago.

BREVE DESCRIPCIÓN DE LA INVENCIÓN

La presente descripción proporciona una descripción de los sistemas y métodos para generar credenciales de pago en las transacciones de pago.

Un método para generar credenciales de pago en una transacción de pago incluye: almacenar, en una memoria, por lo menos una llave de un solo uso asociada con una cuenta de transacciones; recibir, mediante un dispositivo de recepción, un número de identificación personal; identificar, mediante un dispositivo de procesamiento, una primera llave de sesión; generar, mediante el dispositivo de procesamiento, una segunda llave de sesión basándose en por lo menos la llave de un solo uso almacenada y el número de identificación personal recibido; generar, mediante el dispositivo de procesamiento, un primer criptograma de la aplicación basándose en por lo menos la primera llave de sesión; generar, mediante el dispositivo de procesamiento, un segundo criptograma de la aplicación basándose en por lo menos la segunda llave de sesión; y transmitir, mediante un dispositivo de transmisión, por lo menos el primer criptograma de la aplicación y el segundo

criptograma de la aplicación para utilizarse en una transacción de pago.

Otro método para generar credenciales de pago en una transacción de pago incluye: almacenar, en una memoria, por lo menos una llave maestra de la tarjeta asociada con una cuenta de transacciones; generar, mediante un dispositivo de procesamiento, una primera llave de sesión basándose en por lo menos la llave maestra de la tarjeta almacenada; generar, mediante el dispositivo de procesamiento, una segunda llave de sesión; generar, mediante el dispositivo de procesamiento, un primer criptograma de la aplicación basándose en por lo menos la primera llave de sesión; generar, mediante el dispositivo de procesamiento, un segundo criptograma de la aplicación basándose en por lo menos la segunda llave de sesión; y transmitir, mediante un dispositivo de transmisión, por lo menos el primer criptograma de la aplicación y el segundo criptograma de la aplicación para utilizarse en una transacción de pago.

Un sistema para generar credenciales de pago en una transacción de pago incluye una memoria, un dispositivo de recepción, un dispositivo de procesamiento, y un dispositivo de transmisión. La memoria está configurada para almacenar por lo menos una llave de un solo uso asociada con una cuenta de transacciones. El dispositivo de recepción está configurado para recibir un número de identificación personal. El dispositivo de procesamiento está configurado para: identificar una primera llave de

sesión; generar una segunda llave de sesión basándose en por lo menos la llave de un solo uso almacenada y el número de identificación personal recibido; generar un primer criptograma de la aplicación basándose en por lo menos la primera llave de sesión; y generar un segundo criptograma de la aplicación basándose en por lo menos la segunda llave de sesión. El dispositivo de transmisión está configurado para transmitir por lo menos el primer criptograma de la aplicación y el segundo criptograma de la aplicación para utilizarse en una transacción de pago.

Otro sistema para generar credenciales de pago en una transacción de pago incluye una memoria, un dispositivo de procesamiento, y un dispositivo de transmisión. La memoria está configurada para almacenar por lo menos una llave maestra de la tarjeta asociada con una cuenta de transacciones. El dispositivo de procesamiento configurado para generar una primera llave de sesión basándose en por lo menos la llave maestra de la tarjeta almacenada; generar una segunda llave de sesión; generar un primer criptograma de la aplicación basándose en por lo menos la primera llave de sesión; y generar un segundo criptograma de la aplicación basándose en por lo menos la segunda llave de sesión. El dispositivo de transmisión está configurado para transmitir por lo menos el primer criptograma de la aplicación y el segundo criptograma de la aplicación para utilizarse en una transacción de pago.

BREVE DESCRIPCIÓN DE LAS FIGURAS

El alcance de la presente descripción se entiende mejor a

partir de la siguiente descripción detallada de las ejemplo cuando se lee conjuntamente con los dibujos adjuntos. En los dibujos se incluyen las siguientes figuras:

La figura 1 es un diagrama de bloques que ilustra una arquitectura de sistema de alto nivel para el procesamiento de las transacciones de pago con una seguridad avanzada en el aprovisionamiento y almacenamiento de credenciales de pago de acuerdo con las modalidades de ejemplo.

La figura 2 es un diagrama de bloques que ilustra el dispositivo móvil de la figura 1 para el procesamiento de las transacciones de pago sin un elemento de seguridad, y la recepción y el almacenamiento seguros de las credenciales de pago de acuerdo con las modalidades de ejemplo.

La figura 3 es un diagrama de bloques que ilustra la base de datos de la tarjeta del dispositivo móvil de la figura 2 para el almacenamiento de las credenciales de pago de acuerdo con las modalidades de ejemplo.

La figura 4 es un diagrama de bloques que ilustra la memoria del dispositivo móvil de la figura 2 para el almacenamiento de datos utilizados en la generación de llaves de almacenamiento avanzadas y en la generación de criptogramas de aplicaciones de acuerdo con las modalidades de ejemplo.

La figura 5 es un diagrama de bloques que ilustra el servidor de gestión de transacciones de la figura 1, para el procesamiento de las transacciones de pago con un dispositivo móvil sin un elemento

de seguridad de acuerdo con las modalidades de ejemplo.

La figura 6 es un diagrama de bloques que ilustra la base de datos de cuentas del servidor de procesamiento de la figura 5, para el almacenamiento de las credenciales de pago y los detalles de las cuentas de acuerdo con las modalidades de ejemplo.

La figura 7 es un diagrama de flujo que ilustra un proceso para la transmisión y validación de los criptogramas de aplicaciones doble para el procesamiento de las transacciones de pago que involucran a un dispositivo móvil que carece de un elemento de seguridad de acuerdo con las modalidades de ejemplo.

La figura 8 es un diagrama de flujo que ilustra un proceso alternativo para la transmisión y validación de los criptogramas de aplicaciones doble para el procesamiento de las transacciones de pago que involucran a un dispositivo móvil que carece de un elemento de seguridad de acuerdo con las modalidades de ejemplo.

La figura 9 es un diagrama de flujo que ilustra un proceso para crear, transmitir y validar un servicio de notificación a distancia u otro mensaje de datos suministrado a un dispositivo móvil que carece de un elemento de seguridad de acuerdo con las modalidades de ejemplo.

Las figuras 10A y 10B son un diagrama de flujo que ilustra un proceso para la creación, transmisión y validación de un mensaje devuelto por un dispositivo móvil que carece de un elemento de seguridad de acuerdo con las modalidades de ejemplo.

La figura 11 es un diagrama de flujo que ilustra un proceso

para la validación de un mensaje del servicio de notificación a distancia utilizando el dispositivo móvil de la figura 2 de acuerdo con las modalidades de ejemplo.

La figura 12 es un diagrama que ilustra la generación de una llave de almacenamiento avanzada usando el dispositivo móvil de la figura 2 de acuerdo con las modalidades de ejemplo.

Las figuras 13 y 14 son diagramas de flujo que ilustran los métodos de ejemplo para las credenciales de pago generadas en una transacción de pago de acuerdo con las modalidades de ejemplo.

La figura 15 es un diagrama de flujo que ilustra un método de ejemplo para recibir y procesar un mensaje del servicio de notificación a distancia de acuerdo con las modalidades de ejemplo.

La figura 16 es un diagrama de flujo que ilustra un método de ejemplo para la construcción de una llave de almacenamiento avanzada, de acuerdo con las modalidades de ejemplo.

La figura 17 es un diagrama de bloques que ilustra una arquitectura del sistema de computación de acuerdo con las modalidades de ejemplo.

Otras áreas de aplicabilidad de la presente descripción se harán evidentes a partir de la descripción detallada proporcionada posteriormente en la presente. Se debe entender que la descripción detallada de las modalidades de ejemplo es solamente para propósitos de ilustración y, por consiguiente, no pretende limitar necesariamente el alcance de la divulgación.

DESCRIPCIÓN DETALLADA DE LA INVENCIÓN

Glosario de términos

Red de pago - Un sistema o red que se utiliza para la transferencia de dinero por medio del uso de sustitutos de efectivo. Las redes de pago pueden utilizar una variedad de diferentes protocolos y procedimientos con el fin de procesar la transferencia de dinero de diferentes tipos de transacciones. Las transacciones que se pueden llevar a cabo por medio de una red de pago pueden incluir compras de productos o servicios, compras a crédito, transacciones de débito, transferencias de fondos, retiros de cuenta, etc. Las redes de pago se pueden configurar para llevar a cabo transacciones por medio de sustitutos de efectivo, los cuales pueden incluir tarjetas de pago, cartas de crédito, cheques, cuentas de transacciones, etc. Los ejemplos de las redes o los sistemas configurados para funcionar como redes de pago incluyen aquéllos operados por MasterCard®, VISA®, Discover®, American Express®, PayPal®, etc. El uso del término "red de pago" en el presente documento puede referirse tanto a la red de pago como una entidad, como a la red de pago física, tal como el equipo, el hardware y el software que comprenden la red de pago.

Cuenta de transacciones - Una cuenta financiera que se puede utilizar para financiar una transacción, tal como una cuenta de cheques, cuenta de ahorros, cuenta de crédito, cuenta de pago virtual, etc. Una cuenta de transacciones puede estar asociada con un consumidor, que puede ser cualquier tipo adecuado de entidad

asociada a una cuenta de pago, que puede incluir una persona, familia, empresa, corporación, entidad gubernamental, etc. En algunos casos, una cuenta de transacciones puede ser virtual, tal como las cuentas gestionadas por PayPal®, etc.

Tarjeta de pago - Una tarjeta o los datos asociados con una cuenta de transacciones que se puedan proporcionar a un comerciante con el fin de financiar una transacción financiera por medio de la cuenta de transacciones asociada. Las tarjetas de pago pueden incluir tarjetas de crédito, tarjetas de débito, tarjetas de cargo, tarjetas de valor almacenado, tarjetas de prepago, tarjetas de flota, números de pagos virtuales, números de tarjetas virtuales, números de pagos controlados, etc. Una tarjeta de pago puede ser una tarjeta física que pueda ser proporcionada a un comerciante, o pueden ser los datos que representen la cuenta de transacciones asociada (por ejemplo, como se almacena en un dispositivo de comunicación, tal como un teléfono inteligente o una computadora). Por ejemplo, en algunos casos, los datos que incluyen un número de cuenta de pago pueden ser considerados como una tarjeta de pago para el procesamiento de una transacción financiada por la cuenta de transacciones asociada. En algunos casos, un cheque puede ser considerado como una tarjeta de pago cuando sea aplicable.

Transacción de pago - Una transacción entre dos entidades en la que se intercambia dinero u otro beneficio financiero de una entidad a la otra. La transacción de pago puede ser una transferencia de fondos, para la compra de bienes o servicios, para

el reembolso de una deuda, o para cualquier otro beneficio financiero, como será evidente para las personas que tengan experiencia en la técnica relevante. En algunos casos, las transacciones de pago pueden referirse a las transacciones financiadas por medio de una tarjeta de pago y/o cuenta de pago, tales como las transacciones con tarjeta de crédito. Estas transacciones de pago pueden ser procesadas por medio de un emisor, la red de pago, y el adquiriente. El proceso para tramitar una transacción de pago de este tipo puede incluir por lo menos uno de autorización, procesamiento por lotes, liberación, liquidación y financiamiento. La autorización puede incluir el suministro de los detalles del pago por parte del consumidor a un comerciante, la provisión de los detalles de la transacción (por ejemplo, incluyendo los detalles del pago) del comerciante a su adquiriente, y la verificación de los detalles del pago con el emisor de la cuenta de pago del consumidor utilizada para financiar la transacción. El procesamiento por lotes puede referirse al almacenamiento de una transacción autorizada en un lote con otras transacciones autorizadas para su distribución a un adquiriente. La liberación puede incluir el envío de las transacciones por lotes desde el adquiriente hasta una red de pago para su procesamiento. La liquidación puede incluir el débito del emisor por medio de la red de pago para las transacciones que involucran a los beneficiarios del emisor. En algunos casos, el emisor puede pagar al adquiriente por medio de la red de pago. En otros casos, el emisor puede pagar al

adquiriente directamente. El financiamiento puede comerciante por parte del adquiriente para las transacciones de pago que han sido liberadas y liquidadas. Será evidente para las personas que tengan experiencia en la técnica relevante que el orden y/o la categorización de los pasos discutidos anteriormente se realizan como parte del procesamiento de transacciones de pago.

Punto de venta - Un dispositivo informático o un sistema de computación configurado para recibir la interacción con un usuario (por ejemplo, un consumidor, empleado, etc.) para introducir los datos de la transacción, los datos de pago, y/u otros tipos adecuados de datos para la compra y/o el pago de bienes y/o servicios. El punto de venta puede ser un dispositivo físico (por ejemplo, una caja registradora, kiosco, computadora de escritorio, teléfono inteligente, computadora de tablet, etc.) en una ubicación física que un cliente visita como parte de la transacción, tal como en una tienda física tradicional, o puede ser virtual en los entornos del comercio electrónico, tales como los minoristas en línea que reciben las comunicaciones de los clientes por medio de una red tal como Internet. En los casos en donde el punto de venta puede ser virtual, el dispositivo informático operado por el usuario para iniciar la transacción, o el sistema de computación que recibe los datos como un resultado de la transacción, puede ser considerado como el punto de venta, como sea aplicable.

<u>Sistema para el procesamiento de transacciones de pago utilizando un dispositivo móvil sin elementos de seguridad</u>

La figura 1 ilustra un sistema 100 para el pro transacciones de pago utilizando un dispositivo móvil sin requerir del uso de elementos de seguridad, el cual puede incluir la provisión segura de credenciales de pago a un dispositivo móvil, el almacenamiento seguro de las mismas, y su uso en la generación de múltiples criptogramas de aplicaciones para usarse en la validación y el procesamiento de la transacción de pago.

El sistema 100 puede incluir un servidor de gestión de transacciones 102. El servidor de gestión de transacciones 102, descrito con mayor detalle más adelante, puede ser uno o más dispositivos informáticos programados específicamente para llevar a cabo las funciones descritas en la presente para proporcionar las credenciales de pago a un dispositivo móvil 104 utilizando el mensaje de notificación a distancia transmitido de una forma segura, y para la validación de las credenciales de pago producidas por el dispositivo móvil 104 como parte de una transacción de pago. Aunque se ilustra y se describe en el presente documento que el servidor de gestión de transacciones 102 realiza una variedad de funciones, será evidente para las personas que tengan experiencia en la técnica relevante, que el servidor de gestión de transacciones 102 puede estar comprendido de múltiples dispositivos informáticos, servidores, y/o redes de computación, configurados para llevar a cabo las funciones descritas en la presente. El dispositivo móvil 104, descrito con mayor detalle más adelante, puede ser cualquier tipo de dispositivo informático móvil adecuado para llevar a cabo las

funciones descritas en el presente documento, el dispositivo móvil 104 puede comprender un teléfono celular, teléfono inteligente, reloj inteligente, otro dispositivo informático portátil o incorporado, computadora de tablet, computadora laptop, etc. En algunas modalidades, el dispositivo móvil 104 puede carecer de un elemento de seguridad. En otras modalidades, el dispositivo móvil 104 puede incluir un elemento de seguridad, pero un elemento como ése puede no utilizarse en conjunto con los métodos y sistemas discutidos en el presente documento, o se puede utilizar en conjunto con los métodos y sistemas discutidos en el presente documento, tal como para proporcionar una seguridad adicional.

El dispositivo móvil 104 puede comunicarse con el servidor de gestión de transacciones 104 usando múltiples canales de comunicación, tal como usando la comunicación de doble canal. La comunicación de doble canal puede incluir el uso de dos canales de comunicación en la transmisión y recepción de datos, tal como para la verificación y autentificación, con el fin de garantizar una mayor seguridad en la transmisión de datos. El dispositivo móvil 104 puede incluir una aplicación de pagos móvil (MPA) configurada para ser ejecutada por el dispositivo móvil 104 con el fin de llevar a cabo las funciones del dispositivo móvil 104 discutidas en la presente. La aplicación de pagos móvil (MPA), discutida con mayor detalle más adelante, se puede instalar en el dispositivo móvil 104 y se puede activar utilizando un código de activación proporcionado por el servidor de gestión de transacciones 102 empleando los métodos y

sistemas que serán evidentes para las pers experiencia en la técnica relevante, de tal manera que el dispositivo móvil 104 y el servidor de gestión de transacciones 102 puedan transmitir y recibir las comunicaciones de una forma segura a través de uno o más canales de comunicación utilizando los datos compartidos.

El sistema 100 también puede incluir un emisor 106. El emisor 106 puede ser una institución financiera, como un banco emisor, que emite una tarjeta de pago o credenciales de pago a un consumidor 108 asociado con una cuenta de transacciones. El emisor 106 puede proporcionar los detalles del pago asociados con la cuenta de transacciones y/o la tarjeta de pago, al servidor de gestión de transacciones 102. Los detalles del pago pueden incluir, por ejemplo, un número de cuenta de transacciones, el nombre del titular de la cuenta, fecha de vencimiento, código de seguridad, etc. El servidor de gestión de transacciones 102 puede almacenar los datos en una base de datos de cuentas, lo cual se discute con mayor detalle más adelante. El servidor de gestión de transacciones 102 también puede proporcionar las credenciales de pago al dispositivo móvil 104. Tal como se usa en el presente documento, el término "credenciales de pago" puede referirse a cualesquiera datos utilizados por el dispositivo móvil 104 y/o el servidor de gestión de transacciones 102 en la transmisión y validación de la información de pago utilizada en una transacción de pago empleando los métodos y sistemas discutidos en el presente documento, incluyendo, pero no

limitándose a, los detalles del pago, las credenciales, llaves de un solo uso, las llaves de sesión, los criptogramas de aplicaciones, las llaves maestras de tarjetas, etc.

En algunas modalidades, las credenciales de pago se pueden proporcionar al dispositivo móvil 104 por medio de un mensaje del servicio de notificación a distancia. Como se discute con mayor detalle más adelante, el mensaje del servicio de notificación a distancia (RNS) puede ser un mensaje seguro que se transmita al dispositivo móvil 104, y posteriormente sea validado por el dispositivo móvil 104, de tal manera que los datos contenidos en el mismo puedan estar seguros de otros dispositivos y usuarios. La aplicación de pagos móvil (MPA) del dispositivo móvil 104 puede verificar la autenticidad del mensaje de recepción del servicio de notificación a distancia (RNS), y puede descifrarlo para obtener los datos incluidos en el mismo. El dispositivo móvil 104 puede entonces llevar a cabo las funciones necesarias, basándose en los datos (por ejemplo, tal como mediante la ejecución de las instrucciones incluidas en los datos), y, si es aplicable, puede generar un mensaje de regreso para ser enviado de vuelta al servidor de gestión de transacciones 102. En algunos casos, el mensaje de regreso puede ser validado por el servidor de gestión de transacciones 102.

En algunos casos, la validación de mensajes del servicio de notificación a distancia (RNS) en el dispositivo móvil 104, o la validación de mensajes de regreso en el servidor de gestión de transacciones 102, puede utilizar por lo menos contadores de

mensajes y el código de autentificación. El contadores como de los códigos de autentificación puede asegurar que solamente el dispositivo móvil 104 destinado sea capaz de validar y descifrar los datos incluidos en el mensaje del servicio de notificación a distancia (RNS). Además, si las reglas y/o los algoritmos utilizados en la generación del código de autentificación están incluidos en la aplicación de pagos móvil (MPA), entonces solamente un dispositivo móvil 104, que también incluya una instancia específica del programa de aplicación, puede ser capaz de validar el mensaje del servicio de notificación a distancia (RNS), dando como resultado, además, el aumento de la seguridad. En los casos en que el mensaje del servicio de notificación a distancia (RNS) pueda incluir las credenciales de pago, esto puede garantizar que las credenciales de pago solamente estén disponibles en el dispositivo móvil apropiado 104, y solamente si la aplicación de pagos móvil (MPA) utilizada para acceder a ellas es una aplicación adecuada y autorizada.

Las credenciales de pago proporcionadas al dispositivo móvil 104 pueden ser almacenadas con seguridad en el almacenamiento del dispositivo móvil 104, tal como una base de datos de la tarjeta, como se discute con mayor detalle más adelante. En algunas modalidades, el dispositivo móvil 104 puede estar configurado para generar una llave de almacenamiento avanzada para utilizarse en el almacenamiento de datos de una forma segura, tal como las credenciales de pago, en una base de datos o memoria del

dispositivo móvil 104. La generación de una llave de almacenamiento avanzada, como se discute con mayor detalle más adelante, puede utilizar la información única del dispositivo, la información única de la aplicación de pagos móvil (MPA), y la información generada al azar con el fin de identificar una llave de almacenamiento segura que se pueda utilizar para almacenar los datos de una forma segura en el dispositivo móvil 104. Como resultado, las credenciales de pago u otros datos confidenciales se pueden almacenar con seguridad en el dispositivo móvil 104 sin el uso de un elemento de seguridad, lo cual puede dar como resultado que el dispositivo móvil 104 sea capaz de iniciar y realizar la transacción de pago sin el uso de un elemento de seguridad, aumentando la disponibilidad para los emisores 106 y los consumidores 108, mientras que se mantiene un alto nivel de seguridad.

Una vez que el dispositivo móvil 104 tiene las credenciales de pago para una cuenta de transacciones recibida, validada, y almacenada de una forma segura en el mismo, un consumidor 108 puede llevar el dispositivo móvil 104 hasta un punto de venta 110 en un comercio, para llevar a cabo una transacción de pago. El consumidor 108 puede seleccionar los bienes o servicios para su compra, puede iniciar una transacción de pago para la compra de los mismos con un comerciante, y puede utilizar el dispositivo móvil 104 para transmitir las credenciales de pago para utilizarse en el financiamiento de la transacción de pago. La transmisión de las credenciales de pago al punto de venta 110 puede incluir la

transmisión de dos o más criptogramas de aplicaciones. El uso de dos o más criptogramas de aplicaciones puede dar como resultado un mayor nivel de seguridad para las transacciones procesadas empleando los métodos y sistemas discutidos en la presente, de lo que está disponible en las transacciones sin contacto y a distancia tradicionales, incluyendo las transacciones llevadas a cabo utilizando un dispositivo móvil 104 que tenga un elemento de seguridad.

Los criptogramas de aplicaciones pueden cada uno ser generados por el dispositivo móvil 104 usando llaves de sesión separadas y datos adicionales, los cuales se describen con mayor detalle más adelante. Los criptogramas de aplicaciones, generados utilizando los datos almacenados en el dispositivo móvil 104, tal como en el almacenamiento asegurado por medio de la llave de almacenamiento avanzada y asociado con la aplicación de pagos móvil (MPA), pueden asegurarse de que los criptogramas de aplicaciones autentifiquen el dispositivo móvil 104 y la instancia específica de la aplicación de pagos móvil (MPA). En algunos casos, uno de los criptogramas y/o llaves de sesión utilizadas para generar los criptogramas, puede utilizar la información proporcionada por el consumidor 108, tales como un número de identificación personal (PIN). El uso del número de identificación personal (PIN) u otra información de autentificación del consumidor, puede hacer posible que un criptograma autentifique tanto al consumidor 108 como al dispositivo móvil 104. En tal caso, los criptogramas generados por el dispositivo móvil 104 pueden incluir uno que autentifique al

dispositivo móvil 104, y un segundo que aut[illegible] dispositivo móvil 104 como al consumidor 108.

Los criptogramas pueden ser recibidos por el punto de venta 110 como parte de la realización de la transacción de pago, tal como por medio de la comunicación de campo cercano (NFC). Los criptogramas de aplicaciones pueden acompañar a la información de pago adicional, tal como pueda ser requerido en el contexto de cualquier tipo adecuado de transacción de pago, tal como una transacción sin contacto, una transacción a distancia, una transacción de pago a distancia segura, una transacción de banda magnética, y una transacción con M/Chip EMV, y se pueden transmitir al punto de venta 110 usando cualquier método adecuado de acuerdo con lo mismo, como será evidente para las personas que tengan experiencia en la técnica relevante. Los criptogramas pueden ser transmitidos a un adquiriente 112, que puede ser una institución financiera, como un banco adquiriente, asociado con el comerciante. El adquiriente 112, por ejemplo, puede emitir una cuenta de transacciones para el comerciante, que se utiliza para recibir el pago de los fondos del consumidor 108 para la transacción de pago. El adquiriente 112 puede presentar los criptogramas y los detalles adicionales de la transacción ante una red de pago 114 empleando los métodos y sistemas que serán evidentes para las personas que tengan experiencia en la técnica relevante. Por ejemplo, los detalles de la transacción y los criptogramas de la aplicación se pueden incluir en una solicitud de autorización presentada ante la red de

pago 114 en los carriles de pago.

En algunas modalidades, se pueden incluir los dos criptogramas de aplicaciones en un mensaje de transacción individual. Por ejemplo, el dispositivo móvil 104 y/o el punto de venta 110 pueden incluir ambos criptogramas de aplicaciones en los campos de datos heredados de un mensaje de transacción tradicional con el fin de transmitir ambos criptogramas de aplicaciones utilizando los sistemas de pago y el hardware existentes. En algunos casos, el servidor de gestión de transacciones 102 puede estar configurado para utilizar los datos de la Pista 2 para la validación de los criptogramas de aplicaciones, tal como en una transacción de banda magnética. En tales casos, si el mensaje de transacción incluye los datos de la Pista 1, el servidor de gestión de transacciones 102 puede estar configurado para convertir los datos de la Pista 1 en datos de la Pista 2, los cuales también pueden incluir la conversión de los datos de la Pista 1 o de la Pista 2 modificados en datos de la Pista 1 o de la Pista 2 no modificados (por ejemplo, originales, reconstruidos, etc.), respectivamente. Mediante la realización de estas funciones, y mediante la inclusión de los criptogramas de aplicaciones en los campos de datos heredados, el servidor de gestión de transacciones 102 puede estar configurado para procesar y validar las transacciones de pago a distancia y sin contacto utilizando un dispositivo móvil 104 con un mayor nivel de seguridad, sin que sea necesario el uso de un elemento de seguridad en el dispositivo móvil 104, y sin

modificaciones a los sistemas de pago tradicionales.

La red de pago 114 puede procesar la transacción de pago empleando los métodos y sistemas que serán evidentes para las personas que tengan experiencia en la técnica relevante. Como parte del procesamiento, la red de pago 114 puede transmitir los criptogramas de aplicaciones al emisor 106 para su verificación. En algunas modalidades, la verificación puede ser realizada por la red de pago 114. El emisor 106 o la red de pago 114 puede comunicarse con el servidor de gestión de transacciones 102. En algunas modalidades, los criptogramas de aplicaciones pueden ser transmitidos al servidor de gestión de transacciones 102, y pueden ser verificados por medio de la generación de la validación de los criptogramas de aplicaciones utilizando el servidor de gestión de transacciones 102, la cual puede ser generada utilizando las credenciales de pago almacenadas localmente. En otras modalidades, el emisor 106 o la red de pago 114 podrá solicitar los criptogramas de aplicaciones desde el servidor de gestión de transacciones 102, el cual puede generarlos y devolver los criptogramas al emisor 106 o a la red de pago 114 para la validación contra los criptogramas producidos por el dispositivo móvil 104.

Debido a que el servidor de gestión de transacciones 102 posee las credenciales de pago y otros datos utilizados por el dispositivo móvil 104 para generar los criptogramas de aplicaciones, la validación de las credenciales de pago producidas por el dispositivo móvil 104 para financiar la transacción de pago, se puede

realizar por medio de la comparación de los aplicaciones generados por el dispositivo móvil 104 y aquéllos generados por el servidor de gestión de transacciones 102. En algunas modalidades, el servidor de gestión de transacciones 102 pueden ser una parte de la red de pago 114 o el emisor 106. En los casos en que el servidor de gestión de transacciones 102 puede ser parte de la red de pago 114, la validación se puede realizar antes de hacer contacto con el emisor 106 como parte del procesamiento tradicional de la transacción de pago (por ejemplo, para la aprobación del financiamiento de la transacción utilizando la cuenta de transacciones 108 del consumidor con el emisor 106).

Mediante el uso de múltiples criptogramas de aplicaciones, se puede incrementar la seguridad de las transacciones de pago. Además, en los casos en que cada criptograma puede autentificar los datos separados, tales como los casos en los que un criptograma autentifica el dispositivo móvil 104 y el otro autentifica tanto el dispositivo móvil 104 como el consumidor 108 (por ejemplo, por medio del número de identificación personal (PIN) del consumidor), también se pueden proporcionar al emisor 106 datos y consideraciones adicionales para utilizarse en la decisión de aprobar o denegar una transacción. Por ejemplo, si los dos criptogramas son incorrectos (por ejemplo, los criptogramas generados por el dispositivo móvil 104 no corresponden a aquéllos generados por el servidor de gestión de transacciones 102), la transacción puede ser denegada. Si un criptograma es correcto y el otro es incorrecto, la

transacción puede ser denegada por razones de seguridad o ser aprobada, tal como basándose una decisión del emisor 106. Por ejemplo, el emisor 106 puede aprobar una transacción en donde falla la autentificación del consumidor, pero pasa la autentificación del dispositivo móvil, debido a que otros datos disponibles pueden indicar que un usuario autorizado, pero no el consumidor 108, está utilizando el dispositivo móvil 104 para la transacción.

Como resultado, el uso de ambos criptogramas puede proporcionar datos valiosos que puede ser utilizados por las por redes de pago 114 y los emisores 106 en el procesamiento de las transacciones de pago. Además, el uso de dos o más criptogramas puede proporcionar una mayor seguridad que en los métodos de pago sin contacto o a distancia tradicionales, lo cual puede dar como resultado menos fraude y una mayor aceptación de los consumidores 108, los emisores 106, y los comerciantes. En los casos en que el uso de dos o más criptogramas de aplicaciones se generan a partir las credenciales de pago que han sido proporcionadas de una forma segura empleando los métodos de mensajería del servicio de notificación a distancia (RNS) y los sistemas discutidos en la presente, y que han sido almacenadas de una forma segura por medio de llaves de almacenamiento avanzadas generadas empleando los métodos y sistemas discutidos en el presente documento, se puede aumentar enormemente la seguridad global del sistema 100 sobre los sistemas tradicionales para el procesamiento de transacciones y pagos sin contacto. Como resultado, el sistema

100 puede proporcionar una mayor seguridad en la transmisión, almacenamiento y procesamiento de datos, que la proporcionada para los sistemas de pago sin contacto tradicionales y para otros tipos de transacciones de pago a distancia y para las transacciones de pago en general que puedan utilizar los métodos y sistemas discutidos en la presente.

Dispositivo móvil

La figura 2 ilustra una modalidad del dispositivo móvil 104 del sistema 100. Será evidente para las personas que tengan experiencia en la técnica relevante, que la modalidad del dispositivo móvil 104 ilustrado en la figura 2 se proporciona solamente como ilustración y no es necesariamente exhaustiva para todas las posibles configuraciones del dispositivo móvil 104 adecuadas para llevar a cabo las funciones como se discuten en la presente. Por ejemplo, el sistema de computación 1700 ilustrado en la figura 17 y discutido con mayor detalle más adelante, puede ser una configuración adecuada del dispositivo móvil 104.

El dispositivo móvil 104 puede incluir una unidad de recepción 202. La unidad de recepción 202 puede estar configurada para recibir los datos a través de una o más redes por medio de uno o más protocolos de red. La unidad de recepción 202 puede recibir, por ejemplo, datos de programa para uno o más programas de aplicaciones para ser instalados en, y ejecutados por, el dispositivo móvil 104, tal como una aplicación de pagos móvil (MPA) discutida con mayor detalle más adelante. La unidad de recepción 202 también

puede recibir mensajes del servicio de notificación tales como los mensajes transmitidos por el servidor de gestión de transacciones 102, incluyendo los mensajes del servicio de notificación a distancia (RNS) que incluyan las credenciales de pago. La unidad de recepción 202 puede recibir también datos adicionales adecuados para la realización de las funciones tradicionales de un dispositivo móvil 104, tales como comunicaciones telefónicas, comunicaciones celulares, etc. En algunos casos, el dispositivo móvil 104 puede incluir una pluralidad de unidades de recepción 202, tales como unidades de recepción 202 separadas, cada una configurada para comunicarse con una o más redes separadas por medio de los protocolos adecuados. Por ejemplo, el dispositivo móvil 104 puede incluir una primera unidad de recepción 202 para recibir los datos para las transacciones de comunicación de campo cercano (NFC), y una segunda unidad de recepción 202 para recibir las comunicaciones a través de una red de comunicación móvil.

El dispositivo móvil 104 también puede incluir una unidad de entrada 214. La unidad de entrada 214 puede estar configurada para comunicarse con uno o más dispositivos de entrada que se conecten interna o externamente al dispositivo móvil 104 para recibir la entrada desde el consumidor 108, tales como un teclado, ratón, rueda de clic, rueda de desplazamiento, pantalla táctil, micrófono, cámara, receptor, etc. La unidad de entrada 214 puede recibir la entrada desde el consumidor 108, la cual puede ser procesada por una unidad de procesamiento 204.

La unidad de procesamiento 204 se puede llevar a cabo las funciones del dispositivo móvil 104 discutidas en la presente. La unidad de procesamiento 204 puede ejecutar el código del programa almacenado en el dispositivo móvil, tal como para la aplicación de pagos móvil (MPA), y se puede configurar para llevar a cabo una pluralidad de funciones asociadas a cada programa de aplicación, además de otras funciones del dispositivo móvil 104. La unidad de procesamiento 204 puede recibir la entrada por parte del consumidor 108 por medio de la unidad de entrada 214 y realizar las funciones de conformidad con lo mismo, tal como mediante la ejecución de programas de aplicaciones, la realización de funciones en los programas, la recepción de datos, la transmisión de datos, la visualización de datos, etc., como será evidente para las personas que tengan experiencia en la técnica relevante. Por ejemplo, la unidad de procesamiento 204 se puede configurar para validar los mensajes del servicio de notificación a distancia (RNS), generar las llaves de almacenamiento avanzadas, y generar los criptogramas de aplicaciones, como se discute con mayor detalle más adelante.

El dispositivo móvil 104 también puede incluir una unidad de visualización 210. La unidad de visualización 210 puede estar configurada para comunicarse con uno o más dispositivos de visualización que estén conectados interna o externamente al dispositivo móvil 104 para la visualización de los datos, tales como los datos transmitidos a la unidad de visualización 210 para la visualización mediante la unidad de procesamiento 204. Los

dispositivos de visualización pueden incluir pantallas de cristal líquido, pantallas de diodos emisores de luz, pantallas de transistores de película delgada, pantallas táctiles, etc.

El dispositivo móvil 104 también puede incluir una unidad de transmisión 206. La unidad de transmisión 206 puede estar configurada para transmitir los datos a través de una o más redes por medio de uno o más protocolos de red. La unidad de transmisión 206 puede transmitir mensajes de respuesta del servicio de notificación a distancia (RNS) al servidor de gestión de transacciones 102. La unidad de transmisión 206 también puede ser configurada para transmitir los criptogramas de aplicaciones y/o las credenciales de pago, tal como a un punto de venta 110, para utilizarse en una transacción de pago. La unidad de transmisión 206 puede estar configurada además para realizar funciones adicionales del dispositivo móvil 104, como será evidente para las personas que tengan experiencia en la técnica relevante, tales como las funciones tradicionales de un dispositivo de comunicación móvil para la transmisión de las comunicaciones celulares, etc. En algunos casos, el dispositivo móvil 104 puede incluir una pluralidad de unidades de transmisión 206, que se pueden configurar por separado para comunicarse con una o más redes separadas, tal como una unidad de transmisión 206 configurada para transmitir las credenciales de pago y los criptogramas de pago por medio de comunicación de campo cercano (NFC) y otra unidad de transmisión 206 configurada para transmitir los datos por medio de una red de comunicación

móvil.

El dispositivo móvil 104 también puede incluir una base de datos de la tarjeta 208. La base de datos de la tarjeta 208, descrita con mayor detalle más adelante, puede ser el almacenamiento de datos en el dispositivo móvil 104 que está configurado para almacenar los datos asociados con una o más cuentas de transacciones y/o tarjetas de pago. La base de datos de la tarjeta 208 puede almacenar las credenciales de pago asociadas con la cuenta de transacciones, tales como las suministradas al dispositivo móvil 104 por el servidor de gestión de transacciones 102 en un mensaje del servicio de notificación a distancia (RNS) seguro, y los datos adicionales que puedan ser utilizados en la generación de los criptogramas de aplicaciones, como se discute con mayor detalle más adelante. En algunos casos, la base de datos de la tarjeta 208 se puede almacenar como parte de la aplicación de pagos móvil.

El dispositivo móvil 104 puede incluir además una memoria 212. La memoria 212, la cual se describe con mayor detalle más adelante, puede estar configurada para almacenar los datos para el dispositivo móvil 104, adecuados para llevar a cabo las funciones del dispositivo móvil 104 discutidas en la presente. Por ejemplo, la memoria 212 puede almacenar los datos adecuados para la generación de llaves de almacenamiento avanzadas para el cifrado de datos adicionales en el dispositivo móvil 104, tal como la base de datos de la tarjeta 208, como se discute con mayor detalle más adelante. La memoria 212 también puede estar configurada para

almacenar el código del programa para los aplicaciones ejecutados por la unidad de procesamiento 204, tal como un sistema operativo, un código del programa para recibir datos por medio de la unidad de entrada 214 y para visualizar los datos por medio de la unidad de visualización 210, las reglas y/o los algoritmos para realizar las funciones discutidas en el presente documento, etc. La memoria 212 también puede almacenar los datos adecuados para la realización de las funciones tradicionales de un dispositivo móvil 104, tales como las reglas y/o los algoritmos para la transmisión y recepción de comunicaciones celulares por medio de una red móvil. Los datos adicionales almacenados en la memoria 212 serán evidentes para las personas que tengan experiencia en la técnica relevante.

Base de datos de la tarjeta del dispositivo móvil

La figura 3 ilustra una modalidad de la base de datos de la tarjeta 208 del dispositivo móvil 104 para almacenar las credenciales de pago y otros datos asociados con las cuentas de transacciones para utilizarse en el financiamiento de las transacciones de pago realizadas con el dispositivo móvil 108.

La base de datos de la tarjeta 208 puede incluir uno o más perfiles de pago 302, ilustrados en la figura 3 como los perfiles de pago 302a, 302b y 302c. Cada perfil de pago 302 puede estar asociado con una cuenta de transacciones que se puede utilizar para financiar una transacción de pago y puede incluir por lo menos las credenciales de pago 304, una o más llaves de un solo uso 306, una

primera llave de sesión 308, una segunda llave de sesión 310, y un contador de transacciones de la aplicación 312.

Las credenciales de pago 304 pueden incluir datos asociados con la cuenta de transacciones relacionada que se utiliza para la identificación y validación por parte de la red de pago 114 y/o el emisor 106 en el procesamiento de una transacción de pago utilizando la cuenta de transacciones relacionada. Las credenciales de pago 304 pueden incluir, por ejemplo, un número de cuenta de transacciones, código de seguridad, fecha de vencimiento, nombre del titular de la tarjeta, nombre del usuario autorizado, datos de seguimiento, datos de descripción del diseño de la tarjeta, cuenta de dígitos, mapas de bits, etc.

Las llaves de un solo uso 306 pueden ser fichas de pago válidas para una sola transacción de pago, que pueden ser utilizadas por la unidad de procesamiento 204 del dispositivo móvil 104 para generar uno o más de los criptogramas de aplicaciones utilizados en la transacción de pago. En algunas modalidades, una llave de un solo uso 306 puede incluir uno o más de los otros elementos de datos incluidos en el perfil de pago 302. Por ejemplo, cada llave de un solo uso 306 puede incluir un contador de transacciones de la aplicación 312 distinto, que pueden no estar incluidas por separado en el perfil de pago 302. Las diferentes configuraciones de los datos almacenados en el perfil de pago 302 para utilizarse en la realización de las funciones descritas en la presente serán evidentes para las personas que tengan experiencia en la técnica relevante. En algunos

casos, la llave de un solo uso 306 puede incluir, comprendida de, una llave que se utiliza para generar los uno o más criptogramas de aplicaciones. En algunas modalidades, la primera llave de sesión 308 y la segunda llave de sesión 310 se pueden incluir en una llave de un solo uso 306 proporcionada al dispositivo móvil 104 y/o generada utilizando los datos incluidos en la llave de un solo uso 306.

La primera llave de sesión 308 y la segunda llave de sesión 310 pueden ser llaves adicionales que sean utilizadas por la unidad de procesamiento 204 en la generación de los criptogramas de aplicaciones transmitidos hasta el punto de venta 110 como parte de la realización de una transacción de pago utilizando el dispositivo móvil 104. En algunas modalidades, se puede utilizar la primera llave de sesión 308 en la generación de un primer criptograma de la aplicación por parte de la unidad de procesamiento 204, tal como utilizando el código del programa, las reglas o los algoritmos almacenados en la memoria 212 del dispositivo móvil 104. La segunda llave de sesión 310 se puede utilizar en la generación de un segundo criptograma de la aplicación.

En algunas modalidades, la segunda llave de sesión 310 puede ser generada por la unidad de procesamiento 204. En dicha modalidad, la segunda llave de sesión 310 puede ser generada utilizando una llave de un solo uso 306 y los datos de autentificación del usuario, tal como un número de identificación personal (PIN) proporcionado por el consumidor 108 (por ejemplo, por medio de la

unidad de entrada 214). En esta modalidad, la sesión 310 no se puede almacenar en el perfil de pago 302, y en su lugar puede ser generada, utilizada, y desechada como parte del proceso de transacción de pago. El segundo criptograma de la aplicación, por consiguiente, cuando se genera a partir de la segunda llave de sesión 310 que se genera utilizando la llave de un solo uso 306 y el número de identificación personal (PIN) del consumidor, sirve para autentificar tanto el dispositivo móvil 104 como el consumidor 108.

El número de identificación personal (PIN), puede ser un número suministrado por el consumidor 108 (por ejemplo, durante el registro de la aplicación de pagos móvil (MPA) en el dispositivo móvil 104 o durante el registro de la cuenta de transacciones con el emisor 106 y/o el servidor de gestión de transacciones 102) que puede utilizarse para autentificar al consumidor 108. Cuando se lleva a cabo una transacción de pago, el consumidor 108 u otro usuario del dispositivo móvil 104 puede suministrar un número de identificación personal (PIN) por medio de la unidad de entrada 214. En algunas modalidades, si el número de identificación personal (PIN) suministrado es incorrecto (por ejemplo, no coincide con el número de identificación personal (PIN) proporcionado por el consumidor 108 durante el registro), entonces la unidad de procesamiento 204 puede continuar generando la segunda llave de sesión 310 y posteriormente generar el segundo criptograma de la aplicación. Si el número de identificación personal (PIN) proporcionado es incorrecto, entonces

el segundo criptograma de la aplicación será incorrecto, lo que dará como resultado una validación fallida del segundo criptograma de la aplicación por parte del servidor de gestión de transacciones 102, el emisor 106, y/o la red de pago 114, lo cual puede proporcionar el emisor 106 una oportunidad para rechazar la transacción en consecuencia, o para todavía aprobar la transacción.

Memoria del dispositivo móvil

La figura 4 ilustra una modalidad de la memoria 212 del dispositivo móvil 104 para el almacenamiento de programas de aplicaciones y otros datos para ser utilizados en el almacenamiento seguro de los datos en el dispositivo móvil 104, y para la realización de transacciones de pago utilizando el dispositivo móvil 104. En una modalidad de ejemplo, la memoria 212 no puede ser un elemento de seguridad.

La memoria 212 puede incluir información del dispositivo 402. La información del dispositivo 402 puede incluir uno o más elementos de datos asociados con el dispositivo móvil 104 que, en algunos casos, pueden ser únicos para el dispositivo móvil 104. Por ejemplo, la información del dispositivo 402 puede incluir una dirección de control de acceso a los medios, un número de referencia, un número de serie, un número de identificación, etc. La información adicional que pueda ser considerada como información del dispositivo 402 de un dispositivo móvil 104 será evidente para las personas que tengan experiencia en la técnica relevante.

La memoria 212 también puede incluir una aplicación de pagos móvil (MPA) 404. La aplicación de pagos móvil (MPA) 404 puede ser un programa de la aplicación configurado para llevar a cabo las funciones del dispositivo móvil 104 descritas en la presente, tales como la recepción y el almacenamiento de las credenciales de pago, la validación de los mensajes del servicio de notificación a distancia (RNS), y la generación de criptogramas de aplicaciones para utilizarse en la realización de las transacciones de pago. Las características adicionales de la aplicación de pagos móvil (MPA) 404 pueden incluir características tradicionales de una cartera digital u otro programa de aplicación similar, como será evidente para las personas que tengan experiencia en la técnica relevante.

La aplicación de pagos móvil (MPA) 404 puede incluir el código del programa 406. El código del programa 406 puede ser un código, ejecutado por la unidad de procesamiento 204 del dispositivo móvil 104, que haga que la unidad de procesamiento 204 y otros componentes del dispositivo móvil 104 lleven a cabo las funciones de la aplicación de pagos móvil (MPA) 404, como se discute en la presente. Por ejemplo, el código del programa 406 puede incluir un código adecuado para generar criptogramas de aplicaciones, para validar los mensajes del servicio de notificación a distancia (RNS), etc. El código del programa 406 también puede incluir un código del programa adecuado para generar un valor aleatorio, el cual se puede utilizar en la generación de una llave de almacenamiento avanzada. El valor aleatorio puede ser un número aleatorio o pseudo-aleatorio,

el cual puede ser generado empleando los métodos y/o algoritmos serán evidentes para las personas que tengan experiencia en la técnica relevante.

La aplicación de pagos móvil (MPA) 404 también puede incluir un identificador de instancia 408. El identificador de instancia 408 puede ser un valor único para la aplicación de pagos móvil (MPA) específica 404, que se puede utilizar en la generación de la llave de almacenamiento avanzada que se utiliza para asegurar los datos en el dispositivo móvil 104, tal como la base de datos de la tarjeta 208. Al tener el identificador de instancia 408 único para la aplicación de pagos móvil (MPA) 404, se pueden instalar múltiples aplicaciones de pagos móviles (MPA) 404 en el dispositivo móvil 104, sin que ninguna aplicación de pagos móvil (MPA) 404 ser capaz de acceder a los datos que sean almacenados de una forma segura por cualquier otra aplicación de pagos móvil (MPA) 404, lo cual puede asegurar de esta manera que los perfiles de pago 302 para las cuentas de transacciones específicas no sean accesibles para otros programas. El identificador de instancia 408 puede ser un número, un valor alfanumérico, un valor hexadecimal, o cualquier valor adecuado que pueda ser único para una aplicación de pagos móvil (MPA) 404.

Como se discute con mayor detalle más adelante, la unidad de procesamiento 204 del dispositivo móvil 104 puede estar configurada para generar un valor de diversificación usando la información del dispositivo 402, el valor aleatorio generado utilizando el código del programa 406 de la aplicación de pagos móvil (MPA) 404, y el

identificador de instancia 408 almacenado en la aplicación de pagos móvil (MPA) 404. El valor de diversificación puede ser utilizado por una aplicación criptográfica 410 también almacenada en la memoria 212. La aplicación criptográfica 410 puede ser un programa de la aplicación configurado para realizar la criptografía white-box y/o cualquier otra función criptográfica adecuada que será evidente para las personas que tengan experiencia en la técnica relevante.

La aplicación criptográfica 410 puede incluir un código del programa 412. El código del programa 412 puede ser ejecutado por la unidad de procesamiento 204 del dispositivo móvil 104 para hacer posible que la unidad de procesamiento 204 y otros componentes del dispositivo móvil 104 lleven a cabo las funciones criptográficas de la aplicación criptográfica 410 que se discute en el presente documento. Las funciones pueden incluir la generación de una llave de almacenamiento avanzada. La llave de almacenamiento avanzada puede generarse utilizando el valor de diversificación generado por la aplicación de pagos móvil 404 y una llave de cifrado 414 incluida en la aplicación criptográfica 410. En algunas modalidades, la llave de diversificación puede ser descifrada utilizando la llave de cifrado de 414 para obtener la llave de almacenamiento avanzada.

La aplicación criptográfica 410 también se puede configurar para cifrar el almacenamiento en el dispositivo móvil 104 utilizando la llave de almacenamiento avanzada. En algunas modalidades, el cifrado se puede llevar a cabo utilizando una o más técnicas de criptografía white-box. El almacenamiento cifrado puede ser la base

de datos de la tarjeta 208 y/o cualquier otro adecuado en el dispositivo móvil 104, tal como los datos almacenados en la aplicación de pagos móvil (MPA) 404. En algunas modalidades, la aplicación criptográfica 410 se puede incluir como parte de la aplicación de pagos móvil (MPA) 404. La llave de almacenamiento avanzada se puede almacenar en la aplicación criptográfica 410 o en la aplicación de pagos móvil (MPA) 404, o, en algunos casos, puede ser regenerada por la aplicación de pagos móvil (MPA) 404 y la aplicación criptográfica 410 cuando sea necesario.

La memoria 212 también puede incluir datos adicionales almacenados en el dispositivo móvil 104 adecuados para llevar a cabo las funciones descritas en la presente, así como cualesquiera funciones adicionales de los dispositivos móviles. Por ejemplo, la memoria 212 puede incluir un código del programa para un sistema operativo, código, reglas o algoritmos para la recepción y transmisión de las comunicaciones móviles, tales como llamadas telefónicas, etc.

En algunas modalidades, el dispositivo móvil 104 también puede estar configurado para recibir los datos ya cifrados utilizando la llave de almacenamiento avanzada, los cuales se pueden almacenar en el almacenamiento local cifrado del dispositivo móvil 104, tal como en la memoria 212, la base de datos de la tarjeta 208, u otro almacenamiento adecuado. En esta modalidad, el dispositivo móvil 104 puede estar configurado para transmitir el valor aleatorio

generado al servidor de gestión de transacciones 102 o a una entidad de confianza, la cual puede generar la llave de almacenamiento avanzada empleando los mismos métodos y sistemas que utilizan el valor aleatorio generado, y se pueden cifrar los datos que se proporcionen al dispositivo móvil 104. El dispositivo móvil 104, por consiguiente, puede recibir los datos ya cifrados utilizando la llave de almacenamiento avanzada, para el almacenamiento local en el dispositivo móvil 104.

Servidor de gestión de transacciones

La figura 5 ilustra una modalidad del servidor de gestión de transacciones 102 del sistema 100. Será evidente para las personas que tengan experiencia en la técnica relevante, que la modalidad del servidor de gestión de transacciones 102 ilustrado en la figura 5 se proporciona solamente como ilustración y no es necesariamente exhaustiva para todas las posibles configuraciones del servidor de gestión de transacciones 102 adecuado para llevar a cabo las funciones como se discuten en la presente. Por ejemplo, el sistema de computación 1700 ilustrado en la figura 17 y discutido con mayor detalle más adelante, puede ser una configuración adecuada del servidor de gestión de transacciones 102.

El servidor de gestión de transacciones 102 puede incluir una unidad de recepción 502. La unidad de recepción 502 puede estar configurada para recibir los datos a través de una o más redes por medio de uno o más protocolos de red. La unidad de recepción 502 puede recibir los datos desde el dispositivo móvil 104, tales como

mensajes recepción o de regreso, mensajes notificaciones de transacciones, etc., de la red de pago 114, del emisor 106, o de otra entidad adecuada. La unidad de recepción 502 puede recibir las notificaciones de transacciones o solicitudes de criptogramas, tal como para iniciar la generación de los criptogramas de aplicaciones para utilizarse en la validación de las credenciales de pago en una transacción de pago. La unidad de recepción 502 puede recibir también los datos de la cuenta de transacciones, tal como desde el emisor 106, para utilizarse en la generación de las credenciales de pago para proporcionarse al dispositivo móvil 104.

El servidor de gestión de transacciones 102 también puede incluir una unidad de procesamiento 504. La unidad de procesamiento 504 se puede configurar para llevar a cabo las funciones del servidor de gestión de transacciones 102 discutido en la presente, como será evidente para las personas que tengan experiencia en la técnica relevante. La unidad de procesamiento 504 puede así ser configurado para generar y cifrar mensajes del servicio de notificación a distancia (RNS) y los datos incluidos en los mismos, validar los mensajes de regreso desde el dispositivo móvil 104, generar credenciales de pago, generar criptogramas de aplicaciones, validar criptogramas de aplicaciones, etc., como se discute con mayor detalle más adelante.

El servidor de gestión de transacciones 102 puede incluir además una unidad de transmisión 506. La unidad de transmisión 506 puede estar configurada para transmitir los datos a través de

una o más redes por medio de uno o más prot[illegible] unidad de transmisión 506 puede transmitir mensajes del servicio de notificación a distancia (RNS), credenciales de pago, criptogramas de aplicaciones, notificaciones de validación, y otros datos que serán evidentes para las personas que tengan experiencia en la técnica relevante. La unidad de transmisión 506 puede estar configurada para transmitir los datos al dispositivo móvil 104, tal como por medio de una red de comunicación móvil o la Internet, la red de pago 114, el emisor 106, y cualquier otra entidad adecuada.

El servidor de gestión de transacciones 102 también puede incluir una base de datos de cuentas 508. La base de datos de cuentas 508, la cual se describe con mayor detalle más adelante, puede estar configurada para almacenar la información de la cuenta para una pluralidad de cuentas de transacciones. La información de la cuenta puede incluir datos y llaves utilizadas para la generación de los criptogramas de aplicaciones utilizados en la validación de las credenciales de pago recibidas durante las transacciones de pago llevadas a cabo utilizando el dispositivo móvil 104. La base de datos de cuentas 508 también puede ser configurada para almacenar los datos de transacción para las transacciones de pago realizadas que involucren al dispositivo móvil 104 y otros datos, tales como los datos asociados con el consumidor 108 u otros usuarios autorizados de la cuenta de transacciones relacionada.

El servidor de gestión de transacciones 102 también puede incluir una memoria 510. La memoria 510 se puede configurar para

almacenar datos adicionales para se utilizados por la gestión de transacciones 102 en el desempeño de las funciones descritas en la presente. Por ejemplo, la memoria 510 puede almacenar reglas o algoritmos para la validación de los criptogramas de aplicaciones, reglas o algoritmos para la generación de las notificaciones de validación, los algoritmos para la generación de llaves de sesión y de criptogramas de aplicaciones, llaves de cifrado para el cifrado y descifrado de los datos y mensajes del servicio de notificación a distancia (RNS), etc. Los datos adicionales que se pueden almacenar en la memoria 510 serán evidentes para las personas que tengan experiencia en la técnica relevante.

Base de datos de cuentas del servidor de gestión de transacciones

La figura 6 ilustra una modalidad de la base de datos de cuentas 508 del servidor de gestión de transacciones 102 para almacenar los datos relacionados con las cuentas de transacciones para utilizarse en la validación de las credenciales de pago y otros datos de transacción proporcionados en la realización de las transacciones de pago, incluyendo el dispositivo móvil 104.

La base de datos de cuentas 508 puede incluir una pluralidad de perfiles de cuentas 602, ilustrados en la figura 6 como los perfiles de cuentas 602a, 602b, y 602c. Cada perfil de cuenta 602 puede incluir una o más llaves de un solo uso 604, una primera llave de sesión 606, una segunda llave de sesión 608, un contador de transacciones de la aplicación 610, y una llave maestra de la primera tarjeta 612. En algunas modalidades, un perfil de cuenta 602 puede

incluir además una llave maestra de la segunda tar

Cada perfil de cuenta 602 puede corresponder a un perfil de pago 302 proporcionado a un dispositivo móvil 104. Como tal, las llaves de un solo uso 604 almacenadas en un perfil de cuenta 602 pueden corresponder a las llaves de un solo uso 306 almacenadas en el perfil de pago correspondiente 302 en relación con la misma cuenta de transacciones. Los datos pueden ser similares, de tal manera que, cuando un criptograma de la aplicación es generado por el servidor de gestión de transacciones 102 o el dispositivo móvil 104, los criptogramas de aplicaciones deben coincidir si los datos son exactos y no han sido manipulados, lo cual puede hacer posible la validación de las credenciales de pago presentadas por el dispositivo móvil 104.

En algunas modalidades, un perfil de cuenta 602 puede incluir un número de identificación personal (PIN) que corresponda con el número de identificación personal (PIN) 314 almacenado en el perfil de pago 302 correspondiente. En esta modalidad, el número de identificación personal (PIN) 314 se puede proporcionar a la unidad de recepción 202 del servidor de gestión de transacciones 102 en un mensaje seguro, tal como un mensaje de recepción proporcionado por el dispositivo móvil 104, el cual se describe con mayor detalle más adelante. En otras modalidades, se puede utilizar una llave maestra de la tarjeta en lugar del número de identificación personal (PIN), tal como la llave maestra de la primera tarjeta 612. En esta modalidad, la unidad de procesamiento 504 del servidor de gestión

de transacciones 102 puede estar configurado segunda llave de sesión 608 basada en la llave maestra de la segunda tarjeta 614 que corresponde a la segunda llave de sesión 310 generada por el dispositivo móvil 104, utilizando la llave de un solo uso 306 y el número de identificación personal (PIN) 314. En algunos casos, la segunda llave de sesión 608 también puede basarse en la tecla de un solo uso 604 correspondiente. En estas modalidades, los algoritmos para la generación de llaves de sesión y/o criptogramas de aplicaciones pueden asegurarse de que los criptogramas generados por el dispositivo móvil 104 y el servidor de gestión de transacciones 102 sean correspondientes, basándose en los datos utilizados en los mismos.

La primera llave de sesión 606 puede ser utilizada por la unidad de procesamiento 504 del servidor de gestión de transacciones 102 para generar un primer criptograma de la aplicación, y la segunda llave de sesión 608 se puede usar para generar un segundo criptograma de la aplicación. En algunas modalidades, se puede utilizar el contador de transacciones de la aplicación 610 en la generación de una o más de las llaves de sesión y/o criptogramas de la aplicación. El contador de transacciones de la aplicación 610 puede ser un valor correspondiente a la transacción de pago que se va a realizar, el cual se incrementa o se modifica de otra manera durante cada transacción. El contador de transacciones de la aplicación 610 puede corresponder al contador de transacciones de la aplicación 312 almacenado en el perfil de pago

correspondiente 302 en el dispositivo móvil 104, su uso puede garantizar que solamente una aplicación de pagos móvil (MPA) 404 válida pueda poseer el contador de transacciones de la aplicación 312 correcto para generar llaves de sesión y/o criptogramas de aplicaciones válidos. Se pueden emplear técnicas adicionales para mejorar aún más la seguridad de la generación de la llave de sesión y/o del criptograma de la aplicación, tales como números impredecibles y otras técnicas que serán evidentes para las personas que tengan experiencia en la técnica relevante.

Procesamiento de transacciones de pago usando el dispositivo móvil

La figura 7 ilustra un proceso para el procesamiento de las transacciones de pago llevado a cabo utilizando el dispositivo móvil 104 sin un elemento de seguridad y utilizando la generación y validación de dos o más criptogramas de aplicaciones.

En el paso 702, el servidor de gestión de transacciones 102 puede proporcionar (por ejemplo, por medio de la unidad de transmisión 506) las credenciales de pago 304 y otros datos de la cuenta al dispositivo móvil 104, tal como por medio de un mensaje de servicio de notificación a distancia (RNS) se discute con mayor detalle más adelante. En el paso 704, la unidad de recepción 202 del dispositivo móvil 104 puede recibir las credenciales de pago 304 y otros datos de la cuenta. En el paso 706, la unidad de procesamiento 204 del dispositivo móvil 104 puede almacenar los datos en un perfil de pago 302 en la base de datos de la tarjeta 208. Los datos de la cuenta pueden incluir las credenciales de pago 304, una o más llaves

de un solo uso 308, y cualesquiera otros datos como una o más de las llaves de sesión 308 y 310.

En el paso 708, la unidad de procesamiento 204 puede generar dos criptogramas de aplicaciones para utilizarse en la realización de una transacción de pago. En algunas modalidades, el paso 708 puede ser iniciado por el consumidor 108, tal como mediante la indicación por medio de la unidad de entrada 214, colocando el dispositivo móvil 104 cerca del punto de venta 110 para iniciar la transacción por medio de la comunicación de campo cercano, u otro método adecuado. La generación de los criptogramas de aplicaciones puede incluir la generación de un primer criptograma de la aplicación utilizando la primera llave de sesión 308 almacenada en el perfil de pago 302. El segundo criptograma de la aplicación se puede generar usando una segunda llave de sesión 310, que puede ser generada usando una llave de un solo uso 306 y un número de identificación personal (PIN) 314. En algunos casos, el consumidor 108 puede introducir un código número de identificación personal (PIN) en el dispositivo móvil 104 (por ejemplo, por medio de la unidad de entrada 214) antes del paso 708 o durante la iniciación del paso 708. En algunas modalidades, uno o ambos de los criptogramas de aplicaciones también pueden ser generados utilizando el contador de transacciones de la aplicación 312.

Una vez que se han generado los criptogramas de aplicaciones, éstos, junto con las credenciales de pago 304, pueden ser transmitidos al emisor 106 por medio del punto de venta 110, el

adquiriente 112, y la red de pago 114. Las credenciales de aplicaciones y los criptogramas de aplicaciones pueden ser recibidos por el emisor 106 en el paso 710. En el paso 712, la unidad de transmisión 206 del dispositivo móvil 104 puede transmitir una notificación de transacción al servidor de gestión de transacciones 102. En el paso 714, la unidad de recepción 502 del servidor de gestión de transacciones 102 puede recibir la notificación de la transacción. La notificación de la transacción puede notificar al servidor de gestión de transacciones 102 de que el dispositivo móvil 104 ha iniciado una transacción de pago utilizando el perfil de pago 302. En algunos casos, la notificación de la transacción puede incluir la información de identificación.

En el paso 716, la unidad de procesamiento 504 del servidor de gestión de transacciones 102 puede identificar un perfil de cuenta 602 que corresponde al perfil de pago 302, y puede generar dos criptogramas de aplicaciones utilizando los datos contenidos en los mismos. El primer criptograma de la aplicación se puede generar utilizando la primera llave de sesión 606, la cual puede ser generada utilizando la llave maestra de la primera tarjeta 612. El segundo criptograma de la aplicación se puede generar utilizando la segunda llave de sesión 608. En algunas modalidades, uno o ambos de los criptogramas de aplicaciones y/o las llaves de sesión pueden basarse además en las llaves de un solo uso 604, en el contador de transacciones de la aplicación 610, o en cualquier otro tipo de datos adecuado.

En el paso 718, la unidad de transmisión 506 de gestión de transacciones 102 puede transmitir los criptogramas de aplicaciones generados al emisor 106, el cual puede recibir los criptogramas en el paso 718. En el paso 720, el emisor 106 puede validar los criptogramas de aplicaciones proporcionados por el dispositivo móvil 104 que acompaña a las credenciales de pago 304. La validación de los criptogramas de aplicaciones puede incluir la comparación de los criptogramas suministrados por el dispositivo móvil 104, con los criptogramas de aplicaciones generados y suministrados por el servidor de gestión de transacciones 102. Una vez que se lleva a cabo la validación, entonces, en el paso 722, el emisor 106 puede procesar la transacción en consecuencia. El procesamiento de transacciones puede incluir la aprobación de la transacción de pago, por ejemplo, si uno o ambos de los criptogramas son validados, o la denegación de la transacción de pago, por ejemplo, si se determina que uno o ambos de los criptogramas son inválidos.

En el paso 724, una notificación de transacción puede ser transmitida por el emisor 106, u otra entidad (por ejemplo, la red de pago 114, el adquiriente 112, etc.) como parte del procesamiento de la transacción de pago. La notificación de la transacción se puede transmitir al servidor de gestión de transacciones 102 y puede ser recibida por la unidad de recepción 502, en el paso 726. La notificación de la transacción también puede ser recibida por la unidad de recepción 202 del dispositivo móvil 104, en el paso 728.

La notificación de la transacción puede ser una aprobación o denegación de la transacción de pago. Las unidades de procesamiento 204 y 504 del dispositivo móvil 104 y del servidor de gestión de transacciones 102, respectivamente, pueden cada una realizar una o más funciones como resultado de la notificación de la transacción recibida. Por ejemplo, si la transacción fue aprobada y procesada con éxito, los contadores de transacciones de las aplicaciones 310 y 610 en los respectivos perfiles se pueden actualizar en consecuencia.

La figura 8 ilustra un proceso alternativo para el procesamiento de una transacción de pago utilizando el dispositivo móvil 104.

En el paso 802, las credenciales de pago 304 y otros datos de la cuenta se pueden transmitir al dispositivo móvil 104 por la unidad de transmisión 506 del servidor de gestión de transacciones 102. En el paso 804, la unidad de recepción 202 del dispositivo móvil 104 puede recibir las credenciales de pago 304 y otros datos de la cuenta, que se pueden almacenar en un perfil de pago 302 en el paso 806. En el paso 808, la unidad de procesamiento 204 del dispositivo móvil 104 pueden generar los dos criptogramas de las aplicaciones, como se discutió anteriormente, y puede transmitir los criptogramas, credenciales de pago 304, y otros datos adecuados para el emisor 106 (por ejemplo, por medio del punto de venta 110).

En el paso 810, el emisor 106 puede recibir los criptogramas de las aplicaciones y cualquier otro dato adecuado que pueda ser utilizado por el emisor 106 para validar los datos de transacciones

y/o proceso de aprobación o denegación de la transacción. En el paso 812, el emisor 106 puede presentar una solicitud de criptogramas de validación al servidor de gestión de transacciones 102. En algunas modalidades, la solicitud puede incluir las credenciales de pago 304 u otros datos adecuados para utilizarse por el servidor de gestión de la transacción 102 en la identificación del perfil de la cuenta 602 que se utilizará para generar los criptogramas de validación. En una modalidad, la petición puede incluir, además, los dos criptogramas de la aplicación generados mediante el dispositivo móvil 104 para su validación.

En el paso 814, la unidad de recepción 502 del servidor de gestión de transacciones 102 puede recibir la solicitud del criptograma. En el paso 816, la unidad de procesamiento 504 del servidor de gestión de transacciones 102 puede generar las dos aplicaciones de criptogramas que se utilizará para la validación, como se discutió anteriormente. En modalidades en las que la solicitud de criptograma también incluye las dos aplicaciones de criptogramas generadas mediante el dispositivo móvil 104, el paso 816 puede incluir también la validación de los dos criptogramas por la unidad de procesamiento 504 usando los dos criptogramas de las aplicaciones recién generadas. Los criptogramas de validación, o el resultado de la validación en modalidades aplicables, se pueden transmitir por la unidad de transmisión 506 al emisor 106. En el paso 818, el emisor 106 puede recibir los criptogramas de validación y/o el resultado de la validación.

En el paso 820, el emisor 106 puede validar los datos de aplicaciones proporcionados mediante el dispositivo móvil 104 utilizando los criptogramas de aplicaciones generados por el servidor de gestión de transacciones 102. En modalidades en las que el servidor de gestión de transacciones 102 proporciona un resultado de la validación al emisor 106, paso 820, se puede incluir la identificación del resultado de la validación de cada uno de los dos criptogramas de las aplicaciones. En el paso 822, el emisor 106 puede procesar la transacción de pago en consecuencia sobre la base del resultado de la validación. En el paso 824, las notificaciones de transacciones se pueden transmitir al servidor de gestión de transacciones 102 y al dispositivo móvil 104, recibidas por las respectivas unidades de recepción 502 y 202 en los pasos 826 y 828, respectivamente.

Servicio de notificación a distancia y mensajería de datos

La figura 9 ilustra un proceso para la transmisión y la validación de los mensajes de servicio de notificación a distancia (RNS) y otros mensajes de datos transmitidos desde el servidor de gestión de transacciones 102 al dispositivo móvil 104. Los mensajes del servicio de notificación a distancia (RNS) se pueden transmitir por medio de un servicio de notificación a distancia, tales como uno que utiliza una red de comunicación móvil asociada con el dispositivo móvil 104. Los mensajes del servicio de notificación a distancia (RNS) se puede utilizar para credenciales de disposición de pago 304 y otros datos de la cuenta al dispositivo móvil 104, como por

ejemplo los datos de cuenta utilizados en el transacciones de pago, como se discutió anteriormente, y otra información que se pueda usar en el establecimiento de una conexión segura entre el dispositivo móvil 104 y el servidor de gestión de transacciones 102.

En el paso 902, la unidad de procesamiento 504 del servidor de gestión de transacciones 102 puede generar un mensaje. En los casos en los que se ha establecido la autentificación mutua con el dispositivo móvil 104, el mensaje puede incluir información adecuada para establecer la autentificación mutua, tal como un identificador de sesión. En otros casos, tales como cuando la autentificación mutua se ha establecido entre el servidor de gestión de transacciones 102 y el dispositivo móvil 104 usando el proceso ilustrado en la figura 9 y discutido en el presente documento, el mensaje generado puede incluir las credenciales de pago 304 y los datos de la cuenta, pueden incluir uno o más comandos a ejecutar por la aplicación de pagos móvil (MPA) 404 del dispositivo móvil 104 (por ejemplo, la eliminación de llaves de un solo uso 306 o credenciales de pago 304, etc.), pueden ser notificaciones para presentarse al consumidor 108 (por ejemplo, saldos de cuentas, notificaciones de pago, etc.), o incluyen otros datos adecuados.

En el paso 904, la unidad de procesamiento 504 puede cifrar el mensaje generado. El mensaje puede ser cifrado usando una llave privada de una par de llaves privadas/públicas, en donde el dispositivo móvil 104 puede poseer una llave pública

correspondiente. En algunos casos, el mensaje usando una llave de cifrado asociada con el dispositivo móvil 104 o la aplicación de pagos móvil (MPA) 404, tal como el cifrado de llave 414. En el paso 906, la unidad de procesamiento 504 puede generar un código de autentificación del mensaje. El código de autentificación del mensaje se puede generar mediante el mensaje cifrado y puede ser una llave que se genera utilizando una o más reglas y/o algoritmos especialmente configurados. Por ejemplo, el código de autentificación del mensaje se puede generar usando uno o más métodos de cifrado y ofuscación, como relleno. En algunas modalidades, el código de autentificación del mensaje se puede generar usando la llave de cifrado.

En el paso 908, la unidad de transmisión 506 del servidor de gestión de transacciones 102 puede transmitir un mensaje de datos combinados al dispositivo móvil 104. En las modalidades en las que se puede estar efectuando la autentificación mutua, el mensaje de datos combinados puede ser un mensaje del servicio de notificación a distancia transmitida al dispositivo móvil 104 por medio del servicio de notificación a distancia. El mensaje de datos combinados puede ser recibido por la unidad de recepción 202 del dispositivo móvil 104 en el paso 910, y puede incluir el código de autentificación del mensaje y el mensaje cifrado. En algunos casos, el mensaje de datos combinados puede incluir también un identificador adicional, como uno generado empleando los métodos conocidos por la aplicación de pagos móvil (MPA) 404 para la verificación de los mismos. En

algunos casos, como cuando ya se ha realizado mutua, el mensaje de datos combinados también puede incluir un contador de mensajes.

En el paso 912, la unidad de procesamiento 204 puede generar un código de autentificación de referencia. El código de autentificación de referencia se puede generar utilizando el mensaje cifrado recibido y se puede generar utilizando las mismas reglas y algoritmos que el servidor de gestión de transacciones 102 utilizado para generar el código de autentificación del mensaje, de manera que el código de autentificación de referencia generado se correspondería con el código de autentificación del mensaje, si el código de autentificación del mensaje se genera por una fuente de confianza (por ejemplo, el servidor de gestión de transacciones 102). En las modalidades en las que el código de autentificación del mensaje se puede generar usando la llave de cifrado, la unidad de procesamiento 204 puede generar el código de autentificación de referencia utilizando el cifrado de llave 414 almacenada en la memoria 212 u otra llave de cifrado adecuada.

En el paso 914, la unidad de procesamiento 204 puede validar el código de autentificación del mensaje incluido en el mensaje de datos combinados recibido al compararlo contra el código de autentificación de referencia generado. Si tanto el contador de mensajes y el código de autentificación del mensaje se validan, entonces el mensaje de datos combinados se puede determinar como digno de confianza (por ejemplo, auténtico) como procedentes del

servidor de gestión de transacciones 102. En los mensaje de datos combinados puede incluir un identificador de mensaje, la unidad de procesamiento 204 también puede validar el identificador de mensaje mediante la generación de un identificador de mensaje usando un proceso conocido por la aplicación de pagos móvil (MPA) 404 para la generación y la comparación de los mismos. En las modalidades en las que el mensaje de datos combinados puede incluir un contador de mensajes, la unidad de procesamiento 204 puede validar el contador de mensajes incluido en el mensaje de datos combinada recibido con un contador de referencia almacenado en el dispositivo móvil 104, tal como en la aplicación de pagos móvil (MPA) 404 o en un pago el perfil 502.

En el paso 916, la unidad de procesamiento 204 puede descifrar el mensaje cifrado incluido en el mensaje de datos combinados recibido. El mensaje cifrado se puede descifrar utilizando una llave, tal como una almacenada en la memoria 212 (por ejemplo, en la aplicación criptográfica 410 o aplicación de pagos móvil 404) o almacenada en una base de datos cifrada local (por ejemplo, cifrada mediante una llave de almacenamiento avanzada), u otro método adecuado de descifrado. En el paso 918, la unidad de procesamiento 204 puede realizar una o más acciones apropiadas basándose en los datos descifrados del mensaje cifrado. En el ejemplo ilustrado en la figura 9, el dispositivo móvil 104 puede realizar la autentificación mutua con el servidor de gestión de transacciones 102, como el uso del identificador de sesión incluido

en el mensaje cifrado y descifrado por la unidad 204. En el paso 920, el servidor 102 de gestión de transacciones puede recibir al identificador de sesión y realizar cualquier acción adicional necesaria para la autentificación mutua con el dispositivo móvil 104. En los casos en que la autentificación mutua ya se ha realizado, el mensaje puede incluir otra información adecuada para llevar a cabo las funciones que se describen aquí, tales como las credenciales de pago 404, las llaves de un solo uso 406, las instrucciones de programa para la aplicación de pagos móvil (MPA) 404, etc.

En algunas modalidades, el dispositivo móvil 104 puede estar configurado (por ejemplo, por medio de la aplicación de pagos móvil (MPA) 404) para generar y enviar un mensaje de regreso al servidor de gestión de la transacción 102. En algunos casos, el mensaje de regreso puede incluir datos generados en respuesta a las acciones realizadas como se indica en el mensaje descifrado, como se discutió anteriormente. Por ejemplo, un mensaje de regreso puede indicar la recepción válida y el almacenamiento de credenciales de pago 304 o llaves de un solo uso 306. En otros casos, el mensaje de respuesta puede ser una notificación de recepción y validación del mensaje de datos combinados. En casos en los que primero se realiza la autentificación mutua, el mensaje de regreso puede incluir al identificador de sesión utilizado para realizar la autentificación mutua.

Las figuras 10A y 10B ilustran un proceso para la generación y

transmisión de un mensaje de respuesta mediante protocolo móvil 104 y la validación de los mismos por el servidor de gestión de transacciones 102.

En el paso 1002, la unidad de procesamiento 204 del dispositivo móvil 104 puede generar un mensaje de recepción. El mensaje de recepción se puede generar a partir del código del programa 406 almacenado en la aplicación de pagos móvil (MPA) 404, y se puede basar además en las acciones llevadas a cabo como se indica en un mensaje de datos combinados descifrado recibido del servidor de gestión de transacciones 102. Por ejemplo, el mensaje de recepción puede incluir una notificación de recepción y almacenamiento de credenciales de pago 304. En el paso 1004, la unidad de procesamiento 204 puede incrementar un contador de recepción. El contador de recepción puede ser un contador indicativo del número de mensajes de confirmación de transmisión al servidor de gestión de transacciones 102. El contador de recepción se puede almacenar en la memoria 212, como en la aplicación de pagos móvil (MPA) 404, o en una base de datos cifrada usando la llave de almacenamiento avanzada. Será evidente para las personas que tengan experiencia en la técnica relevante que el paso 1004 puede ser un paso opcional, y solamente se puede utilizar en casos en los que se utiliza un contador para la validación de un mensaje de datos.

En el paso 1006, la unidad de procesamiento 204 puede cifrar el mensaje de recepción. El mensaje de confirmación se puede cifrar utilizando la llave de cifrado 414 almacenada en la aplicación

criptográfica 410, o de lo contrario se puede aplicación de pagos móvil (MPA) 404 o en una base de datos cifrada localmente. La llave de cifrado utilizada para cifrar el mensaje de recepción puede ser una llave privada como parte de un par de llaves, con el servidor de gestión de transacciones 102 que posee una llave pública correspondiente. En el paso 1008, la unidad de procesamiento 204 puede generar un código de autentificación de recepción basado en el mensaje de confirmación de cifrado. En algunas modalidades, el código de autentificación de la recepción se puede generar utilizando las mismas reglas, algoritmos, y/o procesos, que se usan para generar el código de autentificación de referencia que se ilustra en el paso 912 de la figura 9, discutido anteriormente.

En el paso 1010, la unidad de transmisión 206 del dispositivo móvil 104 puede transmitir un mensaje de notificación de recepción al servidor de gestión de transacciones 102. El mensaje de notificación de recepción se puede recibir por la unidad de recepción 502 del servidor de gestión de transacciones 102 y puede incluir por lo menos el código de autentificación de recepción, el mensaje de confirmación de cifrado, y el contador de recepción. En algunas modalidades, el mensaje de notificación de recepción se puede transmitir al servidor de gestión de transacciones 102 usando una red de comunicación móvil, tal como una red celular, asociado con el dispositivo móvil 104.

En el paso 1014, la unidad de procesamiento 504 del servidor

de gestión de transacciones 102 puede incrementar el contador de confirmación. El contador de confirmación puede ser indicativo del número de mensajes recibidos desde el dispositivo móvil 104, que se utiliza para la validación de los mensajes recibidos desde el dispositivo móvil 104. El contador de confirmación se puede almacenar en la memoria 510 del servidor de gestión de transacciones 102 u otros almacenamientos de datos adecuados. Por ejemplo, en algunas modalidades, el contador de confirmación se puede almacenar en un perfil de cuenta 602 asociado con el dispositivo móvil 104. En un ejemplo, cada cuenta de perfil 602 puede incluir un contador de confirmación (por ejemplo, y/o un contador de mensajes) para ser utilizado para los mensajes transmitidos a/desde el servidor de gestión de transacciones 102 y el dispositivo móvil 104 en relación con la cuenta de transacciones correspondiente. Será evidente para los expertos en la materia que el paso 1014 puede ser un paso opcional y no se puede realizar en los casos en que no se puede utilizar un contador para la validación de los mensajes de regreso.

En el paso 1016, la unidad de procesamiento 504 puede generar un código de autentificación de confirmación. El código de autentificación de confirmación se puede generar sobre la base del mensaje de confirmación de cifrado incluido en el mensaje de notificación de recepción, y se puede generar utilizando las mismas reglas, algoritmos, y/o procesos utilizados para generar el código de autentificación del mensaje. En el paso 1018, la unidad de

procesamiento 504 puede validar el contador de en el mensaje de notificación de recepción por comparación con el contador de confirmación. En el paso 1020, la unidad de procesamiento 504 puede validar el código de autentificación de recepción comparándolo con el código de autentificación del mensaje, para asegurar que el mensaje se originó desde un dispositivo móvil autorizado 104.

Una vez que el contador (por ejemplo, si es aplicable) y el código de autentificación se han validado, entonces, en el paso 1022, la unidad de procesamiento 504 puede descifrar el mensaje cifrado incluido en el mensaje de notificación de recepción. El mensaje cifrado se puede descifrar utilizando una llave de cifrado almacenada u otro método adecuado de descifrado. El mensaje cifrado se puede descifrar para obtener el mensaje de recepción generado mediante el dispositivo móvil 104. En el paso 1024, la unidad de procesamiento 504 puede llevar a cabo todas las acciones apropiadas según sea necesario basándose en los datos incluidos en el mensaje de recepción. Por ejemplo, si el mensaje de recepción incluye una indicación de recepción y almacenamiento de las llaves de un solo uso 306 exitoso, la unidad de procesamiento 204 puede activar las llaves de un solo uso 604 correspondientes en un perfil de cuenta correspondiente 602.

Validación de Mensajes de Datos

La figura 11 ilustra un proceso 1100 para la validación de mensajes de datos recibidos mediante el dispositivo móvil 104 desde

el servidor de gestión de transacciones 102.

En el paso 1102, la unidad de procesamiento 204 del dispositivo móvil 104 pueden almacenar las llaves de cifrado, las llaves de generación de autentificación, y las reglas y/o algoritmos para el uso y aplicación del mismo en el almacenamiento local, tal como la memoria 212 o el almacenamiento cifrado de manera local cifrado usando una llave de almacenamiento avanzada. En el paso 1104, la unidad de recepción 202 del dispositivo móvil 104 puede recibir un mensaje de datos desde el servidor de gestión de transacciones 102. En algunas modalidades, el mensaje de datos se puede recibir desde el servidor de gestión de transacciones 102 siguiendo el establecimiento de la autentificación mutua entre los dos dispositivos, tal como usando el proceso ilustrado en la figura 9 y que se discutió anteriormente. El mensaje de datos puede incluir por lo menos un contador de mensajes, un código de autentificación del mensaje, y un mensaje cifrado.

En el paso 1106, la unidad de procesamiento 204 puede incrementar un contador de referencia. El contador de referencia se puede almacenar en la memoria 212 u otro almacenamiento local, y se puede utilizar para indicar el número de mensajes recibidos desde el servidor de gestión de transacciones 102. En algunos casos, el contador de referencia se puede incrementar mediante un algoritmo, de manera que el contador de referencia no se pueda incrementar usando números consecutivos, sino por medio de un algoritmo conocido para el dispositivo móvil 104 (por ejemplo, por medio de la

aplicación de pagos móvil (MPA) 404) y el servidor de gestión de transacciones 102.

En el paso 1108, la unidad de procesamiento 204 puede validar el contador de mensajes que se incluye en el mensaje de datos recibido. La validación del contador de mensajes puede incluir la comparación del contador de mensajes para el contador del valor de referencia después de haber sido incrementado. El error de validación puede indicar que la fuente del mensaje de datos no es el servidor de gestión de transacciones 102 o de otra manera, no es de confianza. Si la validación falla, entonces, en el paso 110, la unidad de procesamiento 204 puede llevar a cabo una o más acciones apropiadas asociadas con un mensaje de recepción y/o validación de datos que ha fallado. Por ejemplo, la unidad de procesamiento 204 puede descartar el mensaje de datos, podrá notificar al servidor de gestión de transacciones 102, puede bloquear el perfil asociado pago 302, u otra acción que será evidente para las personas que tengan experiencia en la técnica relevante.

Si la validación del contador de mensajes pasa, entonces el proceso 1100 puede proceder al paso 1112, en donde el mensaje cifrado puede ser rellenado. El relleno del mensaje cifrado puede incluir la adición de valores para el mensaje cifrado o datos asociados de los mismos. El esquema de relleno se puede utilizar para aumentar la seguridad del proceso de validación de mensajes, debido a que puede haber otra función que se deba realizar mediante el dispositivo móvil 104 y el servidor de gestión de transacciones 102

conocida por cada uno, que tendría que ser entidad no autorizada con el fin de transmitir o recibir un mensaje de datos con éxito sin autorización. Será evidente para las personas que tengan experiencia en la técnica relevante que el paso 1112 puede ser un paso opcional. En algunas modalidades, el paso 1112 se puede aplicar en algunos casos del proceso de 1110. Por ejemplo, el mensaje cifrado puede ser alineado en ciertos incrementos de contador de referencia.

En el paso 1114, la unidad de procesamiento 204 puede generar un código de autentificación de referencia. El código de autentificación de referencia se puede generar con base en el mensaje cifrado (por ejemplo, como relleno, si es aplicable) mediante una o más reglas o algoritmos, tales como almacenado en el paso 1102. En algunas modalidades, el código de autentificación de referencia puede ser una tecla o puede ser un valor generado por la aplicación de una llave para el mensaje cifrado. En el paso 1116, la unidad de procesamiento 204 puede validar el código de autentificación del mensaje de recepción en el mensaje del servicio de notificación a distancia (RNS). La validación del código de autentificación del mensaje puede incluir la comparación del código con el código de autentificación de referencia generado, como otro método de identificación si el mensaje de datos recibido se originó a partir de una fuente autorizada (por ejemplo, la transacción servidor de gestión 102).

Si la validación del código de autentificación del mensaje falla,

el proceso de 1100 puede proceder al paso 1110 en el procesamiento de falla. Si la validación del código de autentificación del mensaje pasa, más adelante, en el paso 1118, el mensaje cifrado incluido en el mensaje de datos recibido puede ser descifrado por la unidad de procesamiento 204. El mensaje puede ser descifrado utilizando una o más llaves de cifrado/descifrado, reglas y/o algoritmos, tal como se almacena en el dispositivo móvil 104 en el paso 1102. Por ejemplo, se puede usar el cifrado de llave 414 almacenadas en la aplicación criptográfica 410 de la memoria 212 para descifrar el mensaje cifrado. En el paso 1120, la unidad de procesamiento 204 puede realizar una o más acciones, según proceda en función del contenido del mensaje descifrado. Por ejemplo, si el mensaje descifrado incluye llaves de un solo uso 306, las llaves de un solo uso 306 se pueden almacenar en el perfil apropiado de pago 302 de la base de datos de la tarjeta 208, que por lo tanto se puede cifrar utilizando la llave de almacenamiento avanzada.

Teclas avanzadas de almacenamiento

La figura 12 ilustra la generación y el uso de la llave de almacenamiento avanzada mediante el dispositivo móvil 104 para el almacenamiento seguro de datos en el dispositivo móvil 104, tales como el pago de perfiles 302 y otros datos que se pueden almacenar de una forma segura y para acceder en el dispositivo móvil 104 sin el uso de elementos de seguridad.

La información del dispositivo 402 almacenada en la memoria

212 del dispositivo móvil 104 puede incluir tres piezas de información del dispositivo 1202, que se ilustra en la figura 12 como la información del dispositivo 1202a, 1202b, y 1202c. Cada pieza de información del dispositivo 1202 se puede asociar con el dispositivo móvil 104. En algunos casos, cada pieza de información del dispositivo 1202 puede ser única para el dispositivo móvil 104. En otros casos, una o más de las piezas de información del dispositivo 1202 puede no ser única para el dispositivo móvil 104 (por ejemplo, un número de modelo), pero las tres piezas de información del dispositivo 1202 cuando se toman juntas puede ser únicas para el dispositivo móvil 104 (por ejemplo, una combinación única). Las piezas de información del dispositivo 1202 pueden ser datos que no cambiarán durante la vida útil del dispositivo móvil 104.

La unidad de procesamiento 204 del dispositivo móvil 104 puede generar una huella digital del dispositivo móvil 1204 basándose en las tres piezas de información del dispositivo 1202a, 1202b, y 1202c. La huella digital del dispositivo móvil 1204 puede ser un valor único para el dispositivo móvil 104, y puede ser generada a partir de una o más reglas o algoritmos almacenados en la memoria 212, como se incluye en el código del programa 406 de la aplicación de pagos móvil (MPA) 404. El dispositivo móvil de huellas digitales 1204 puede ser, por ejemplo, un valor numérico, un valor hexadecimal, una cadena de caracteres, etc.

La unidad de procesamiento 204 también se puede configurar para generar un valor de diversificación 1208 utilizando la huella

digital del dispositivo móvil 1204. El valor de diversificación 1208 se puede generar mediante la combinación de la huella digital del dispositivo móvil 1204 con el identificador de la instancia 408 de la aplicación de pagos móvil (MPA) 404, así como una valor aleatorio 1206. El valor aleatorio 1206 puede ser un número aleatorio o pseudo-aleatorio generado por la unidad de procesamiento 204. En algunos casos, el valor aleatorio 1206 se puede generar de conformidad con una o más reglas o algoritmos almacenados en la memoria 212. La combinación de la huella digital del dispositivo móvil 1204, identificador de la instancia 408, y el valor aleatorio 1206 también se puede realizar usando una o más reglas o algoritmos, tal como la almacenada en el código del programa 406 de la aplicación de pagos móvil (MPA) 404. El uso del identificador de la instancia 408 para generar el valor diversificado puede dar lugar a la capacidad de almacenar de una forma segura los datos asociados con una instancia de la aplicación de pagos móvil (MPA) 404 de tal manera que varias instalaciones de la aplicación de pagos móvil (MPA) 404 pueden ser incapaces de acceder a los datos almacenados por otras instancias de la aplicación de pagos móvil (MPA) 404.

La unidad de procesamiento 204 entonces puede generar una llave de almacenamiento avanzada 1210 por medio de la aplicación del cifrado de llave 414 almacenada en la aplicación criptográfica 410 al valor de diversificación 1208. En algunos casos, se puede generar la llave avanzada de almacenamiento 1210 por el descifrado de la valor de diversificación 1208 usando la llave de cifrado 414. En

otros casos, la llave avanzada de almacenamiento 1210 es el valor resultante del cifrado del valor de diversificación 1208 utilizando el cifrado de llave 414. En algunas modalidades, la llave avanzada de almacenamiento 1210 se puede generar como el resultado de realizar la criptografía white-box usando la llave de encriptación 414 y el valor de diversificación 1208.

Una vez que se ha generado la llave avanzada de almacenamiento 1210, la unidad de procesamiento 204 puede utilizar la llave avanzada de almacenamiento 1210 para cifrar una base de datos local 1210. La base de datos local 1210 puede estar compuesta de, por ejemplo, la base de datos de la tarjeta 208, uno o más perfiles de pago 302, parte de la memoria 212, u otra fuente de datos adecuada. En algunos casos, la base de datos local 1210 puede ser una parte de otra base de datos en el dispositivo móvil 104, tal como la base de datos de la tarjeta 208. Por ejemplo, la base de datos de tarjetas 208 puede incluir una pluralidad de bases de datos locales 1212, tales como una base de datos local separada 1212 para cada instancia de la aplicación de pagos móvil (MPA) 404 para almacenar el pago de los mismos perfiles 302 asociados. La base cifrada de datos locales 1214 resultante de ese modo puede almacenar de una forma segura los datos que son inaccesibles por cualquier otro programa de la aplicación interna o externa del dispositivo móvil 104, excepto la instancia específica de la aplicación de pagos móvil (MPA) 404 que incluye el identificador de la instancia 408. En consecuencia, la base de datos local cifrada 1214 puede ser

ideal para almacenar las credenciales de pago 304, uso 306, y otros datos de la cuenta, y puede proporcionar almacenamiento seguro de información confidencial de las cuentas sin el uso de elementos de seguridad.

En algunas modalidades, la llave de almacenamiento también se puede utilizar por el servidor de gestión de transacciones 102 para proporcionar datos cifrados al dispositivo móvil 104 para su almacenamiento en la base de datos local cifrado 1214. Por ejemplo, la unidad de transmisión 206 del dispositivo móvil 104 puede transmitir el valor aleatorio generado 1206 al servidor de gestión de transacciones 102. En algunos casos, el identificador de la instancia 408 también se puede transmitir al servidor de gestión de transacciones 102, o puede ser poseído previamente por el servidor de gestión de transacciones 102, tal como durante el registro de la aplicación de pagos móvil (MPA) 404. El servidor de gestión de transacciones 102 puede entonces generar la llave de almacenamiento avanzada 1210 por sí mismo, cifrar los datos para que se doten al dispositivo móvil 104, tales como credenciales de pago 304, llaves de un solo uso 306, etc. utilizando el almacenamiento avanzado llave 1210, y luego transmitir los datos cifrados en el dispositivo móvil 104. El dispositivo móvil 104 puede entonces almacenar los datos ya codificados en la base de datos local cifrada 1214.

<u>Primer método de ejemplo para generar credenciales de pago en una transacción de pago</u>

La figura 13 ilustra un método 1300 para credenciales de pago en una transacción de pago, incluyendo el uso de dos criptogramas de aplicaciones para el uso seguro de las credenciales de pago en un dispositivo móvil 104 sin un elemento de seguridad.

En el paso 1302, por lo menos una llave de uso única (por ejemplo, de una llave de un solo uso 306) se puede almacenar en una memoria (por ejemplo, un perfil de pago 302) asociado con una cuenta de transacciones. En algunas modalidades, la memoria 302 puede ser una memoria de elemento no seguro de un dispositivo de comunicación móvil (por ejemplo, el dispositivo móvil 104). En el paso 1304, se puede recibir un número de identificación personal (PIN) mediante un dispositivo de recepción (por ejemplo, la unidad de recepción 202 y/o unidad de entrada 214).

En el paso 1306, se puede identificar una primera llave de sesión (por ejemplo, la primera llave de sesión 308) mediante un dispositivo de procesamiento (por ejemplo, la unidad de procesamiento 204). En el paso 1308, se puede generar una segunda llave de sesión (por ejemplo, la segunda llave de sesión 310) mediante el dispositivo de procesamiento 204 basándose en por lo menos el uso de la llave 306 individual almacenado y el número de identificación personal (PIN) recibido.

En el paso 1310, se puede generar un primer criptograma de la aplicación mediante el dispositivo de procesamiento 204 basado en por lo menos la primera llave de sesión 308. En el paso 1312, se

puede generar un segundo criptograma de la aplic dispositivo de procesamiento 204 basándose en por lo menos la segunda llave de sesión 310.

En el paso 1314, por lo menos el primer criptograma de la aplicación y el segundo criptograma de la aplicación se pueden transmitir mediante un dispositivo de transmisión (por ejemplo, la unidad de transmisión 206) para utilizarse en una transacción de pago. En algunas modalidades, el primer criptograma de la aplicación y el segundo criptograma de la aplicación se pueden transmitir a un dispositivo de punto de venta (por ejemplo, el punto de venta 110). En una modalidad, el método 1300 puede incluir, además del almacenamiento, en la memoria 302, una llave de la tarjeta principal asociada con la cuenta de transacciones, en donde la identificación de la primera llave de sesión 308 incluye la generación, mediante el dispositivo de procesamiento 204, la primera llave de sesión 308 con base en por lo menos la llave maestra de la tarjeta almacenada.

En algunas modalidades, el método 1300 puede incluir además del almacenamiento, en la memoria 302, un contador de transacciones de la aplicación (por ejemplo, el contador de transacciones de la aplicación 312), en donde la identificación de la primera llave de sesión 308 incluye la generación, mediante el dispositivo de procesamiento 204, la primera llave de sesión 308 con base en por lo menos el contador de aplicación de transacciones 312 de almacenamiento. En una modalidad, el método 1300 puede incluir

además la validación, mediante el dispositivo de procesamiento 204, el número de identificación personal (PIN) recibido antes de generar la segunda llave de sesión 310. En una modalidad adicional, el dispositivo de procesamiento 204 se puede configurar para generar una segunda llave de sesión no válido 310 si la validación del número de identificación personal (PIN) recibido falla.

Segundo método de ejemplo para generar credenciales de pago en una transacción de pago

La figura 14 ilustra un método 1400 para la generación de las credenciales de pago en una transacción de pago, incluyendo el uso de dos validaciones de criptogramas de la aplicación de las credenciales de pago generadas mediante un dispositivo móvil 104 sin el uso de un elemento de seguridad.

En el paso 1402, se pueden almacenar por lo menos una llave maestra de tarjeta (por ejemplo, llave maestra de la primera tarjeta 612) en una memoria (por ejemplo, la cuenta del perfil 602) asociada con una cuenta de transacciones. En el paso 1404, se puede generar una primera llave de sesión (por ejemplo, primera llave de sesión 606) mediante un dispositivo de procesamiento (por ejemplo, el dispositivo de procesamiento 504) con base en por lo menos la llave maestra de tarjeta 612 almacenada. En el paso 1406, se puede generar una segunda llave de sesión (por ejemplo, la segunda llave de sesión 608) mediante el dispositivo de procesamiento 504.

En el paso 1408, se puede generar un primer criptograma de la aplicación mediante el dispositivo de procesamiento 504 con base en

por lo menos la primera llave de sesión 606. En puede generar un segundo criptograma de la aplicación mediante el dispositivo de procesamiento 504 con base en por lo menos la segunda llave de sesión 608. En el paso 1412, por lo menos el primer criptograma de la aplicación y el segundo criptograma de la aplicación se pueden transmitir mediante un dispositivo de transmisión (por ejemplo, la unidad de transmisión 506) para el uso en una transacción de pago.

En una modalidad, el método 1400 puede incluir además el almacenamiento, en la memoria 602, un número de secuencia de la cuenta de transacciones asociado con la cuenta de transacciones, en donde la primera llave de sesión se basa además en el número de secuencia de cuenta de las transacciones almacenadas. En algunas modalidades, el método 1400 también puede incluir almacenar, en la memoria 602, una segunda llave maestra de tarjeta (por ejemplo, la segunda llave maestra de tarjeta 614) asociada con la cuenta de transacciones, en donde la segunda llave de sesión 608 se basa en por lo menos la segunda llave maestra de tarjeta 614 almacenada.

En una modalidad, el método 1400 puede incluir además: recibir, mediante un dispositivo de recepción (por ejemplo, la unidad de recepción 502), un primer criptograma de la aplicación correspondiente y un segundo criptograma de la aplicación correspondiente; validar, mediante el dispositivo de procesamiento, (i) el primer criptograma de la aplicación correspondiente recibida con base en el primer criptograma de la aplicación generado, y (ii) el

segundo criptograma de la aplicación correspond
base en el segundo criptograma de la aplicación generado; y transmitir, mediante el dispositivo de transmisión 506, un resultado de la validación para utilizarse en la transacción de pago. En una modalidad adicional, el primera criptograma de la aplicación correspondiente y el segundo criptograma de la aplicación correspondiente pueden ser recibidos desde un dispositivo del punto de venta (por ejemplo, el punto de venta 110). En otra modalidad adicional, el resultado de la validación se puede transmitir a una institución financiera (por ejemplo, el emisor 106) asociada con la cuenta de transacciones.

Método de ejemplo para procesar un mensaje de datos

La figura 15 ilustra un método 1500 para el procesamiento de un mensaje de datos, tal como un mensaje de notificación a distancia recibido por medio de un servicio de notificación a distancia, incluyendo la recepción y validación de los mismos mediante un dispositivo móvil 104 sin usar un elemento de seguridad.

En el paso 1502, se puede almacenar por lo menos una llave de cifrado en una memoria (por ejemplo, la memoria 212). En algunas modalidades, la memoria 212 puede ser un elemento de memoria no seguro de un dispositivo de comunicación móvil (por ejemplo, el dispositivo móvil 104). En el paso 1504, se puede recibir un mensaje de datos mediante un dispositivo de recepción (por ejemplo, la unidad de recepción 202), en donde el mensaje de datos puede incluir por lo menos un mensaje cifrado y un código de

autentificación del mensaje, en donde el código del mensaje se genera usando por lo menos una porción del mensaje cifrado. En algunas modalidades, el mensaje de datos puede ser un mensaje del servicio de notificación a distancia recibido por medio de un servicio de notificación a distancia.

En el paso 1506, se puede generar un código de autentificación de referencia mediante un dispositivo de procesamiento (por ejemplo, la unidad de procesamiento 204) usando por lo menos una parte del mensaje cifrado incluido en el mensaje de datos recibido. En una modalidad, la memoria 212 puede incluir además una o más reglas de generación de código de autentificación, y el código de autentificación de referencia se puede generar con base en la aplicación de las una o más reglas de generación de código de autentificación almacenadas a la parte del mensaje cifrado incluidas en el mensaje de datos recibido. En el paso 508, el mensaje de datos recibido puede ser validado mediante el dispositivo de procesamiento 204 basándose en una comprobación del código de autentificación del mensaje incluido en el mensaje de datos recibido contra el código de autentificación de referencia generado. En algunas modalidades, la memoria puede incluir además un contador de referencia, el mensaje de datos recibido puede incluir además un contador de mensaje, y el mensaje de datos recibido puede ser validado aún más mediante el dispositivo de procesamiento 204 basándose en una comprobación del contador de mensajes incluidos en el mensaje de datos recibido en el mostrador de referencia

almacenado.

En el paso 1510, el mensaje cifrado incluido en el mensaje de datos se puede descifrar mediante el dispositivo de procesamiento 204 usando la llave de cifrado almacenada para obtener un mensaje descifrado. En una modalidad, el mensaje descifrado puede incluir por lo menos uno de: un perfil de tarjeta digitalizada (por ejemplo, credenciales de pago 304) y una tecla de un solo uso (por ejemplo, la llave de un solo uso 306) para el uso en una transacción de pago. En algunas modalidades, el método 1500 también puede incluir la verificación, mediante el dispositivo de procesamiento 204, un formato de datos del mensaje descifrado con base en uno o más de los datos de las reglas de formato.

En una modalidad, el método 1500 puede incluir además la transmisión, mediante un dispositivo de transmisión (por ejemplo, la unidad de transmisión 206), una notificación de recepción en respuesta al mensaje de datos recibido. En una modalidad adicional, el proceso 1500 puede incluso incluir además: realizar, mediante el dispositivo de procesamiento 204, una o más acciones sobre la base del mensaje descifrado; generar, mediante el dispositivo de procesamiento 204, un mensaje de respuesta como resultado de o con base en las una o más acciones realizadas; cifrar, mediante el dispositivo de procesamiento 204, el mensaje de regreso generado utilizando la llave de cifrado almacenada para obtener un mensaje de respuesta encriptada; y generando, por medio del dispositivo de procesamiento 204, un código de autentificación de retorno

utilizando por lo menos una parte del mensaje de en donde la notificación de recepción de transmisión incluye el mensaje de regreso cifrado, y el código de autentificación de retorno. En una modalidad aún adicional, la memoria 212 puede incluir además un contador de retorno, y la notificación de recepción transmitida puede incluir, además, el contador de retorno.

En algunas modalidades, el método 1500 puede incluir también el relleno, mediante el dispositivo de procesamiento 204, el mensaje cifrado incluido en el mensaje de datos recibido utilizando una llave de relleno, en donde la parte del mensaje encriptado usado para generar el código de autentificación de referencia es el relleno del mensaje encriptado. En una modalidad adicional, la llave de relleno puede ser la llave de cifrado. En otra forma de modalidad adicional, la memoria 212 puede incluir además un algoritmo de código de autentificación de relleno, y el relleno del mensaje cifrado utilizando la llave de relleno puede incluir el relleno del mensaje cifrado con base en la aplicación de la llave de relleno para el algoritmo de relleno de código de autentificación.

Método de ejemplo para la construcción de una llave de almacenamiento avanzada

La figura 16 ilustra un método 600 para la construcción de una llave de almacenamiento avanzada para el cifrado seguro y almacenamiento de datos locales en un dispositivo móvil 104 sin usar un elemento de seguridad.

En el paso 1602, por lo menos la información del dispositivo

(por ejemplo, la información del dispositivo 402) dispositivo de comunicación móvil (por ejemplo, el dispositivo móvil 104), el código de programa (por ejemplo, el código de programa 406) asociado con un programa de primera aplicación (por ejemplo, la aplicación móvil de pago 404), y el código de programa (por ejemplo, el código de programa 412) asociado con un programa de segunda aplicación (por ejemplo, la aplicación criptografía 410) se pueden almacenar en una memoria (por ejemplo, la memoria 212) del dispositivo de comunicación móvil 104, en donde el código de programa 406 asociado con el primer programa de aplicación 404 incluye por lo menos un identificador de instancia (por ejemplo, el identificador de la instancia 408) y el código de programa 412 asociado con el segundo programa de la aplicación 410 incluye por lo menos una primera llave (por ejemplo, el cifrado de llave 414).

En algunas modalidades, la información del dispositivo 402 puede incluir uno o más identificadores únicos asociados con el dispositivo de comunicación móvil 104. En una modalidad, el identificador de la instancia 408 puede ser único para una instancia del primer programa de la aplicación 404. En algunas modalidades, el segundo programa de la aplicación 410 puede estar configurado para realizar la criptografía white-box usando la primera llave. En una modalidad, la primera llave puede ser una llave dinámica. En algunas modalidades, el código de programa 412 asociado con el segundo programa de la aplicación 410 se puede incluir en el código de programa 406 asociado con el primer programa de la aplicación

404. En modalidades adicionales, el segundo prog 410 puede ser una función ejecutable del programa de aplicación primero 404.

En el paso 1604, una huella digital del dispositivo (por ejemplo, huella digital del dispositivo móvil 1204) asociado con el dispositivo de comunicación móvil 104 se puede generar mediante un dispositivo de procesamiento (por ejemplo, la unidad de procesamiento 204) con base en la información del dispositivo almacenado 402 por medio de la ejecución del código del programa 406 asociado con el primer programa de la aplicación 404. En el paso 1606, un valor aleatorio (por ejemplo, el valor aleatorio 1206) se puede generar mediante el dispositivo de procesamiento 204 por medio de la ejecución del código del programa 406 asociado con el primera programa de la aplicación 404. En algunas modalidades, el valor aleatorio 1206 puede ser un número aleatorio o pseudo-aleatorio.

En el paso 1608, un valor de diversificación (por ejemplo, el valor de diversificación 1208) se puede construir mediante el dispositivo de procesamiento de 204 con base en por lo menos la huella digital generada mediante el dispositivo 204, el valor aleatorio generado 1206, y el identificador de instancia 408 incluidos en el programa de código 406 asociado con el primer programa de la aplicación 404. En el paso 1610, el valor de diversificación construido 1208 se puede descifrar mediante el dispositivo de procesamiento 204 usando la primera llave almacenada en el código de programa 412 asociada con el segundo programa de la aplicación

410 por medio de la ejecución del código de programa con el segundo programa de la aplicación 410 para obtener una llave de almacenamiento (por ejemplo, llave de almacenamiento avanzada 1210).

En algunas modalidades, el método 1600 puede incluir además: almacenar, en una base de datos local (por ejemplo, la base de datos local 1212) del dispositivo de comunicación móvil 104, los datos protegidos; y el cifrado, mediante el dispositivo de procesamiento 204, los datos protegidos almacenados en la base de datos local 1212 utilizando el almacenamiento de llaves 1210. En una modalidad, el método 1600 también puede incluir: almacenar, en la memoria 212, los datos del programa asociados con el primer programa de la aplicación 404; y almacenar, en los datos de programa asociados con el primer programa de la aplicación 404, el valor aleatorio generado 1206.

En una modalidad, el método 1600 también puede incluir: transmitir, mediante un dispositivo de transmisión (por ejemplo, la unidad de transmisión 206) por lo menos el valor aleatorio 1206; recibir, mediante un dispositivo de recepción (por ejemplo, la unidad de recepción 202), uno o más parámetros cifrados, en donde el uno o más parámetros cifrados están cifrados cada uno usando el almacenamiento de llaves 1210; y almacenar, en una base de datos local 1212 del dispositivo de comunicación móvil 104, los uno o más parámetros cifrados recibidos. En una modalidad adicional, la llave de almacenamiento 1210 puede transmitirse a un tercero (por

ejemplo, el servidor de gestión de transacciones 102 y parámetros cifrados se pueden recibir desde la tercera parte 102. En algunas modalidades adicionales, el identificador de instancia 408 también se puede transmitir mediante el dispositivo de transmisión 206.

Arquitectura del sistema de computación

La figura 17 ilustra un sistema de computación 1700 en donde las modalidades de la presente descripción, o porciones de las mismas, se pueden implementar como código legible por computadora. Por ejemplo, el dispositivo servidor de gestión de transacciones 102 y móvil 104 de la figura 1 se pueden implementar en el sistema de computación 1700 usando hardware, software, firmware, instrucciones de computadora que tiene medios legibles no transitorios 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 utilizados para implementar los métodos de las figuras 7, 8, 9A, 9B, 10A, 10B, 11, y 13 a 16.

Si se utiliza la lógica programable, tal lógica se puede ejecutar en una plataforma de procesamiento disponible comercialmente o un dispositivo de propósito especial. Una persona con experiencia ordinaria en la técnica puede apreciar que las modalidades de la materia descrita se pueden practicar con diversas configuraciones de sistema de computación, incluyendo sistemas de múltiples núcleos

multiprocesador, minicomputadoras, computadoras vinculados o agrupados con funciones distribuidas, así como penetrante o computadoras en miniatura que pueden ser incrustadas en prácticamente cualquier dispositivo. Por ejemplo, se pueden utilizar por lo menos un dispositivo procesador y una memoria para poner en práctica las modalidades descritas anteriormente.

Una unidad de procesador o dispositivo de memoria, como se discute en la presente, puede ser un procesador único, una pluralidad de procesadores, o combinaciones de los mismos. Los dispositivos procesadores pueden tener uno o más procesadores "núcleos". Los términos "medio de programa de computadora", "medio legible por computadora no transitoria", y "equipo medio utilizable" como se discute en el presente documento se utilizan para referirse en general a medios tangibles, tales como una unidad de almacenamiento extraíble 1718, una unidad de almacenamiento extraíble 1722, y una disco duro instalado en la unidad de disco duro 1712. Las diversas modalidades de la presente descripción se describen en términos de este ejemplo de sistema de computación 1700. Después de leer esta descripción, se hará evidente para un experto en la técnica relevante cómo implementar la presente descripción usando otros sistemas informáticos y/o arquitecturas informáticas. Aunque las transacciones se pueden describir como un proceso secuencial, algunas de las transacciones, en realidad, se pueden llevar a cabo en forma concurrente, y/o en un entorno

distribuido, y con código paralelo, programa alm[illegible] local o a distancia para el acceso de las máquinas individuales o múltiples procesadores. Además, en algunas modalidades el orden de las transacciones puede reordenarse sin apartarse del espíritu de la materia divulgada.

El dispositivo procesador 1704 puede ser un dispositivo procesador de propósito especial o de propósito general. El dispositivo procesador 1704 puede estar conectado a una infraestructura de comunicaciones 1706, tal como un bus, cola de mensajes, la red, el esquema de multi-núcleo de paso de mensajes, etc. La red puede ser cualquier red adecuada para llevar a cabo las funciones como se describen en el presente documento y pueden incluir una red de área local (LAN), una red de área amplia (WAN), una red inalámbrica (por ejemplo, WiFi), una red de comunicación móvil, una red de satélite, Internet, fibra óptica, cable coaxial, de infrarrojos, de frecuencia de radio (RF), o cualquier combinación de los mismos. Otros tipos y configuraciones de red adecuados serán evidentes para las personas que tienen experiencia en la técnica relevante. El sistema de computación 1700 también puede incluir una memoria principal 1708 (por ejemplo, memoria de acceso aleatorio, memoria de solamente lectura, etc.), y también puede incluir una memoria secundaria 1710. La memoria secundaria 1710 puede incluir la unidad de disco duro 1712 y una unidad extraíble de almacenamiento de 1714, como una unidad de disquete, una unidad de cinta magnética, una unidad de disco óptico, una memoria flash,

etc.

La unidad de almacenamiento extraíble 1714 puede leer y/o escribir en la unidad de almacenamiento extraíble 1718 de una manera bien conocida. La unidad de almacenamiento extraíble 1718 puede incluir un medio de almacenamiento extraíble que puede ser leído por y escrita en la unidad de almacenamiento extraíble 1714. Por ejemplo, si la unidad de almacenamiento extraíble 1714 es una unidad de disquete o puerto de bus serie universal, la unidad de almacenamiento extraíble 1718 puede ser un disquete o una unidad flash portátil, respectivamente. En una modalidad, la unidad de almacenamiento extraíble 1718 puede ser un medio de grabación legible por computadora no transitorio.

En algunas modalidades, la memoria secundaria 1710 puede incluir medios alternativos para permitir que los programas de computadora u otras instrucciones se carguen en el sistema de computación 1700, por ejemplo, la unidad de almacenamiento extraíble 1722 y una interfaz 1720. Los ejemplos de tales medios pueden incluir una interfaz de cartucho de programa y de cartucho (por ejemplo, como se encuentra en los sistemas de videojuegos), un chip de memoria extraíble (por ejemplo, EEPROM, PROM, etc.) y el sóquet asociado, y otras unidades de almacenamiento extraíbles 1722 e interfaces 1720, como será evidente a las personas expertos en la técnica relevante.

Los datos almacenados en el sistema de computación 1700 (por ejemplo, en la memoria principal 1708 y/o la memoria

secundaria 1710) se pueden almacenar en cualquier medio legibles por computadora adecuados, tales como el almacenamiento óptico (por ejemplo, un disco compacto, disco digital versátil, disco Blu-ray, etc.) o de almacenamiento en cinta magnética (por ejemplo, una unidad de disco duro). Los datos pueden estar configurados 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 estructurado (SQL), una base de datos distribuida, una base de datos de objeto, etc. Las configuraciones adecuadas y de los tipos de almacenamiento serán evidentes para las personas que tienen experiencia en la técnica relevante.

El sistema de computación 1700 también puede incluir una interfaz de comunicaciones 1724. La interfaz de comunicación 1724 puede estar configurada para permitir que el software y los datos sean transferidos entre el sistema de computación 1700 y los dispositivos externos. Los ejemplos de interfaces de comunicaciones 1724 pueden incluir un módem, una interfaz de red (por ejemplo, una tarjeta Ethernet), un puerto de comunicaciones, una ranura de PCMCIA y tarjeta, etc. El software y los datos transferidos por medio de la interfaz de comunicaciones 1724 puede estar en la forma de señales, que puede ser electrónicas, electromagnéticas, ópticas, u otras señales, como será evidente para las personas que tengan experiencia en la técnica relevante. Las señales pueden viajar por medio de un camino de comunicaciones 1726, que puede estar configurado para transportar las señales y se puede implementar

usando alambre, cable, fibra óptica, una línea tel[illegible] telefónico celular, un enlace de radiofrecuencia, etc.

El sistema de computación 1700 puede incluir, además, una interfaz de visualización 1702. La interfaz de pantalla 1702 se puede configurar para permitir que los datos sean transferidos entre el sistema de computación 1700 y la pantalla externa 1730. Las interfaces de pantalla a modo de ejemplo 1702 puede incluir la interfaz multimedia de alta definición (HDMI), interfaz visual digital (DVI), matriz de gráficos de vídeo (VGA), etc. La pantalla 1730 puede ser cualquier tipo adecuado de visualización para visualizar los datos transmitidos por medio de la interfaz de pantalla 1702 del sistema de computación 1700, que incluye un tubo de rayos catódicos (CRT), pantalla de cristal líquido (LCD), pantalla de diodos emisores de luz (LED), pantalla táctil capacitiva, transistor de película delgada (TFT), etc.

El medio de programa de computadora y medio utilizable por computadora puede referirse a memorias, tales como la memoria principal 1708 y la memoria secundaria 1710, que puede ser semiconductores de memoria (por ejemplo, DRAM, etc.). Estos productos de programa de computadora pueden ser medios para proporcionar software a los programas de computadora del sistema de computación 700. (por ejemplo, la lógica de control por computadora) se pueden almacenar en la memoria principal 1708 y/o la memoria 1710. Los programas de computadora secundarios pueden también ser recibidos por medio de la interfaz de

comunicaciones 1724. Tales programas de computadora cuando se ejecuta, pueden permitir que el sistema de computación 1700 ponga en práctica los métodos presentes como se discuten en la presente. En particular, los programas de computadora, cuando se ejecutan, pueden permitir que el dispositivo procesador 1704 implemente los métodos ilustrados por las figuras 7, 8, 9A, 9B, 10A, 10B, 11, y 13 a 16, como se discute en el presente documento. En consecuencia, tales programas de computadora pueden representar los controladores del sistema de computación 1700. Cuando la presente descripción se implementa usando software, el software se puede almacenar en un producto de programa de computadora y se carga en el sistema de computación 1700 usando la unidad de almacenamiento extraíble 1714, la interfaz 1720, y la unidad de disco duro 1712, o interfaz de comunicaciones 1724.

Las técnicas acordes con lo proporcionado en la presente divulgación, entre otras características, los sistemas y métodos para el procesamiento de las transacciones de pago utilizando un dispositivo móvil sin necesidad de utilizar un elemento de seguridad, incluyendo la transmisión y validación de mensajes del servicio de notificación a distancia y el almacenamiento seguro de datos mediante una llave de almacenamiento avanzada. Mientras que se han descrito anteriormente diferentes ejemplos de modalidad del sistema descrito y del método, se debe entender que se han presentado con fines de ejemplo solamente, no limitaciones. No es exhaustiva y no limita la divulgación a la forma precisa descrita. Las

modificaciones y variaciones son posibles a la luz de las enseñanzas anteriores o pueden adquirirse de la práctica de la divulgación, sin apartarse del alcance o ámbito de aplicación.

REIVINDICACIONES

1. Un método para autentificación segura por medio de la generación de credenciales de pago en una transacción de pago, el cual comprende:

almacenar, en una memoria, por lo menos una llave de un solo uso asociada con una cuenta de transacciones;

recibir, mediante un dispositivo de recepción, un número de identificación personal;

identificar, mediante un dispositivo de procesamiento, una primera llave de sesión;

generar, mediante el dispositivo de procesamiento, una llave segunda sesión basándose en por lo menos la llave de un solo uso almacenada y el número de identificación personal recibido;

generar, mediante el dispositivo de procesamiento, un primer criptograma de la aplicación basándose en por lo menos la primera llave de sesión;

generar, mediante el dispositivo de procesamiento, un segundo criptograma de la aplicación basándose en por lo menos la segunda llave de sesión; y

transmitir, mediante un dispositivo de transmisión, por lo menos el primer criptograma de la aplicación y el segundo criptograma de la aplicación para utilizarse en una transacción de pago.

2. El método de acuerdo con la reivindicación 1, el cual

comprende además:

almacenar, en la memoria, una llave maestra de la tarjeta asociada con la cuenta de transacciones, en donde:

la identificación de la primera llave de sesión incluye la generación, mediante el dispositivo de procesamiento, de la primera llave de sesión basándose en por lo menos la llave maestra de la tarjeta almacenada.

3. El método de acuerdo con la reivindicación 1, el cual comprende además:

almacenar, en la memoria, un contador de transacciones de la aplicación, en donde:

la identificación de la primera llave de sesión incluye la generación, mediante el dispositivo de procesamiento, de la primera llave de sesión basándose en por lo menos el contador de transacciones de la aplicación almacenado.

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

validar, mediante el dispositivo de procesamiento, el número de identificación personal recibido antes de generar la segunda llave de sesión.

5. El método de acuerdo con la reivindicación 4, en donde el dispositivo de procesamiento está configurado para generar una segunda llave de sesión inválida si falla la validación del número de identificación personal recibido.

6. El método de acuerdo con la reivindicación 1, en donde el

primer criptograma de la aplicación y el segundo criptograma de la aplicación se transmiten hasta un dispositivo de punto de venta.

7. El método de acuerdo con la reivindicación 1, en donde la memoria es una memoria de elemento no seguro de un dispositivo de comunicación móvil.

8. Un método para autentificación segura por medio de la generación de credenciales de pago en una transacción de pago, el cual comprende:

almacenar, en una memoria, por lo menos una llave maestra de la tarjeta asociada con una cuenta de transacciones;

generar, mediante un dispositivo de procesamiento, una primera llave de sesión basándose en por lo menos la llave maestra de la tarjeta almacenada;

generar, mediante el dispositivo de procesamiento, una segunda llave de sesión;

generar, mediante el dispositivo de procesamiento, un primer criptograma de la aplicación basándose en por lo menos la primera llave de sesión;

generar, mediante el dispositivo de procesamiento, un segundo criptograma de la aplicación basándose en por lo menos la segunda llave de sesión; y

transmitir, mediante un dispositivo de transmisión, por lo menos el primer criptograma de la aplicación y el segundo criptograma de la aplicación para utilizarse en una transacción de pago.

9. El método de acuerdo con la reivindicación 8, el cual comprende además:

almacenar, en la memoria, un número de secuencia de la cuenta de transacciones asociado con la cuenta de transacciones, en donde:

la primera llave de sesión se basa además en el número de secuencia de la cuenta transacciones almacenada.

10. El método de acuerdo con la reivindicación 8, el cual comprende además:

almacenar, en la memoria, una llave maestra de la segunda tarjeta asociada con la cuenta de transacciones, en donde:

la segunda llave de sesión se basa en por lo menos la llave maestra de la segunda tarjeta almacenada.

11. El método de acuerdo con la reivindicación 8, el cual comprende además:

recibir, mediante un dispositivo de recepción, un primer criptograma de la aplicación correspondiente y un segundo criptograma de la aplicación correspondiente;

validar, mediante el dispositivo de procesamiento, (i) el primer criptograma de la aplicación correspondiente recibido, basado en el primer criptograma de la aplicación generado, y (ii) el segundo criptograma de la aplicación correspondiente recibido, basado en el segundo criptograma de la aplicación generado; y

transmitir, mediante el dispositivo de transmisión, un resultado de la validación para utilizarse en la transacción de pago.

12. El método de acuerdo con la reivindicación 11, en donde el primer criptograma de la aplicación correspondiente y el segundo criptograma de la aplicación correspondiente se reciben desde un dispositivo de punto de venta.

13. El método de acuerdo con la reivindicación 11, en donde el resultado de la validación se transmite a una institución financiera asociada con la cuenta de transacciones.

14. Un sistema para autentificación segura por medio de la generación de credenciales de pago en una transacción de pago, el cual comprende:

una memoria configurada para almacenar por lo menos una llave de un solo uso asociada con una cuenta de transacciones;

un dispositivo de recepción configurado para recibir un número de identificación personal;

un dispositivo de procesamiento configurado para:

identificar una primera llave de sesión,

generar una segunda llave de sesión basándose, por lo menos, en la llave de un solo uso almacenada y el número de identificación personal recibido,

generar un primer criptograma de la aplicación basándose en por lo menos la primera llave de sesión, y

generar un segundo criptograma de la aplicación basándose en por lo menos la segunda llave de sesión; y

un dispositivo de transmisión configurado para transmitir por lo menos el primer criptograma de la aplicación y el segundo

criptograma de la aplicación para utilizarse en una transacción de pago.

15. El sistema de acuerdo con la reivindicación 14, en donde:

la memoria está configurada además para almacenar una llave maestra de la tarjeta asociada con la cuenta de transacciones, y

la identificación de la primera llave de sesión incluye la generación, mediante el dispositivo de procesamiento, de la primera llave de sesión basándose en por lo menos la llave maestra de la tarjeta almacenada.

16. El sistema de acuerdo con la reivindicación 14, en donde:

la memoria está configurada además para almacenar un contador de transacciones de la aplicación, y

la identificación de la primera llave de sesión incluye la generación, mediante el dispositivo de procesamiento, de la primera llave de sesión, basándose en por lo menos el contador de transacciones de la aplicación almacenado.

17. El sistema de acuerdo con la reivindicación 14, en donde el dispositivo de procesamiento está configurado además para validar el número de identificación personal recibido antes de generar la segunda llave de sesión.

18. El sistema de acuerdo con la reivindicación 17, en donde el dispositivo de procesamiento está configurado para generar una segunda llave de sesión inválida si falla la validación del número de identificación personal recibido.

19. El sistema de acuerdo con la reivindicación 14, en donde el primer criptograma de la aplicación y el segundo criptograma de la aplicación se transmiten hasta un dispositivo de punto de venta.

20. El sistema de acuerdo con la reivindicación 14, en donde la memoria es una memoria de elemento no seguro de un dispositivo de comunicación móvil.

21. Un sistema para autentificación segura por medio de la generación de credenciales de pago en una transacción de pago, el cual comprende:

una memoria configurada para almacenar por lo menos una llave maestra de la tarjeta asociada con una cuenta de transacciones;

un dispositivo de procesamiento configurado para:

generar una primera llave de sesión basándose en por lo menos la llave maestra de la tarjeta almacenada,

generar una segunda llave de sesión,

generar un primer criptograma de la aplicación basándose en por lo menos la primera llave de sesión, y

generar un segundo criptograma de la aplicación basándose en por lo menos la segunda llave de sesión; y

un dispositivo de transmisión configurado para transmitir por lo menos el primer criptograma de la aplicación y un segundo criptograma de la aplicación para utilizarse en una transacción de pago.

22. El sistema de acuerdo con la reivindicación 21, en donde:

la memoria está configurada además para almacenar un número de secuencia de cuenta de transacciones asociado con la cuenta de transacciones, y

la primera llave de sesión se basa además en el número de secuencia de la cuenta de transacciones almacenado.

23. El sistema de acuerdo con la reivindicación 21, en donde:

la memoria está además configurada para almacenar una llave maestra de la segunda tarjeta asociada con la cuenta de transacciones, y

la segunda llave de sesión se basa por lo menos en la llave maestra de la segunda tarjeta almacenada.

24. El sistema de acuerdo con la reivindicación 21, el cual comprende además:

un dispositivo de recepción configurado para recibir un primer criptograma de la aplicación correspondiente y un segundo criptograma de la aplicación correspondiente, en donde:

el dispositivo de procesamiento está configurado además para validar (i) el primer criptograma de la aplicación correspondiente recibido basado en el primer criptograma de la aplicación generado, y (ii) el segundo criptograma de la aplicación correspondiente recibido basado en el segundo criptograma de la aplicación generado, y

el dispositivo de transmisión está configurado además para transmitir un resultado de la validación para utilizarse en la transacción de pago.

25. El sistema de acuerdo con la reivindicación 24, en donde el primer criptograma de la aplicación correspondiente y el segundo criptograma de la aplicación correspondiente son recibidos desde un dispositivo de punto de venta.

26. El sistema de acuerdo con la reivindicación 24, en donde el resultado de la validación se transmite a una institución financiera asociada con la cuenta de transacciones.

RESUMEN

Un método para generar credenciales de pago en una transacción de pago incluye: almacenar, en una memoria, por lo menos una llave de un solo uso asociada con una cuenta de transacciones; recibir, mediante un dispositivo de recepción, un número de identificación personal; identificar, mediante un dispositivo de procesamiento, una primera llave de sesión; generar, mediante el dispositivo de procesamiento, una segunda llave de sesión basándose en por lo menos la llave de un solo uso almacenada y el número de identificación personal recibido; generar, mediante el dispositivo de procesamiento, un primer criptograma de la aplicación basándose en por lo menos la primera llave de sesión; generar, mediante el dispositivo de procesamiento, un segundo criptograma de la aplicación basándose en por lo menos la segunda llave de sesión; y transmitir, mediante un dispositivo de transmisión, por lo menos el primer criptograma de la aplicación y el segundo criptograma de la aplicación para utilizarse en una transacción de pago.

* * * * *

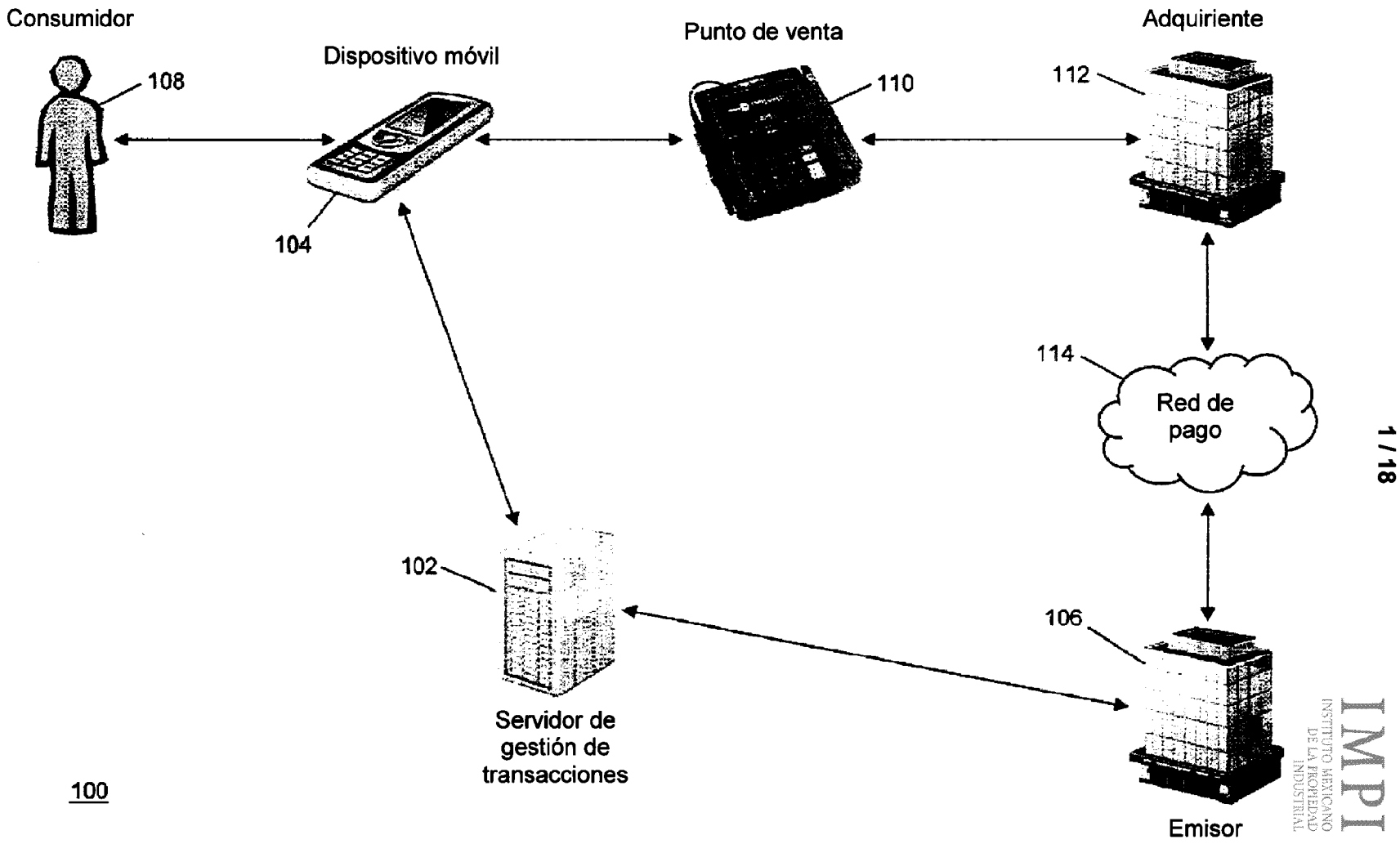

Figura 1

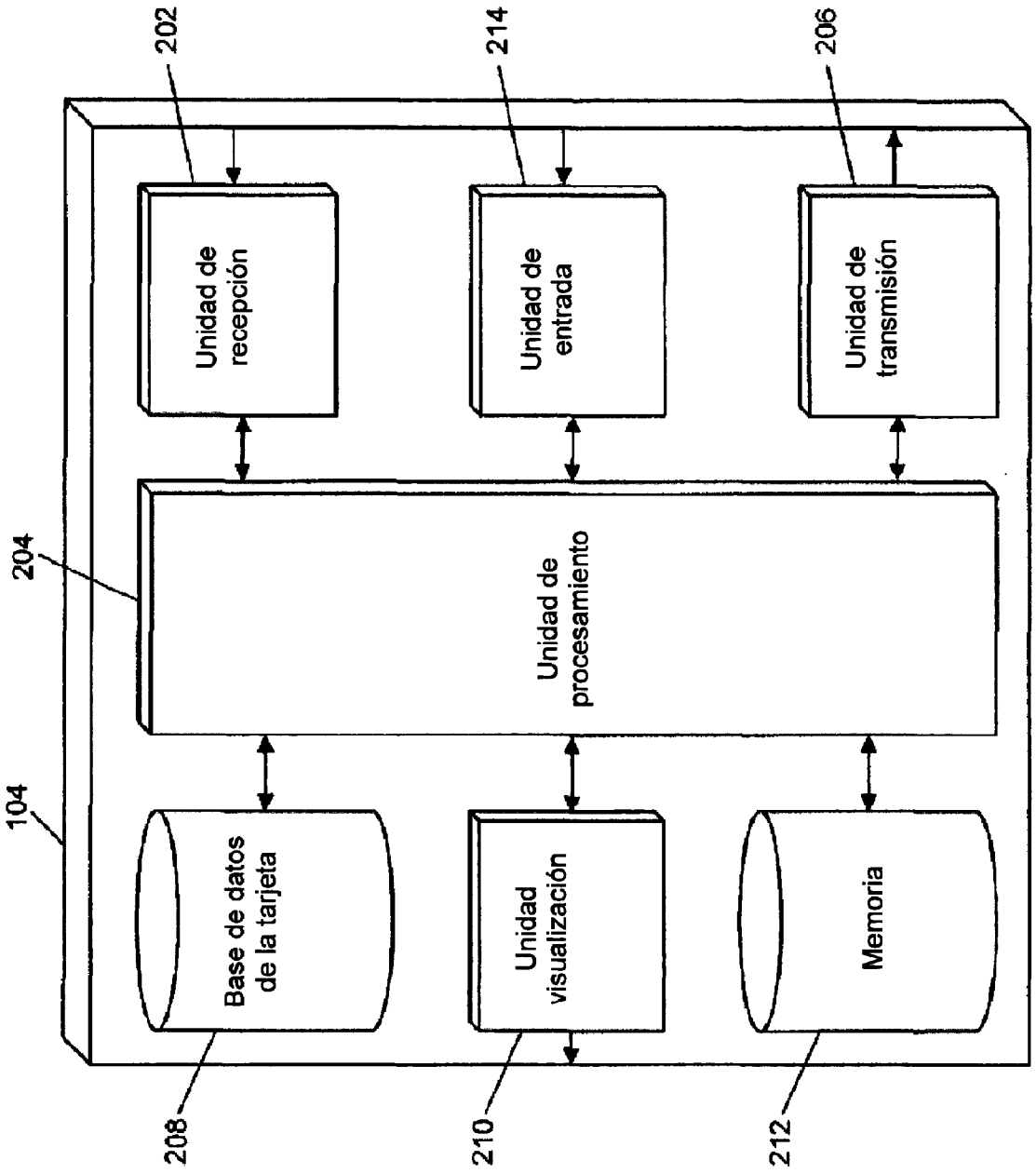

Figura 2

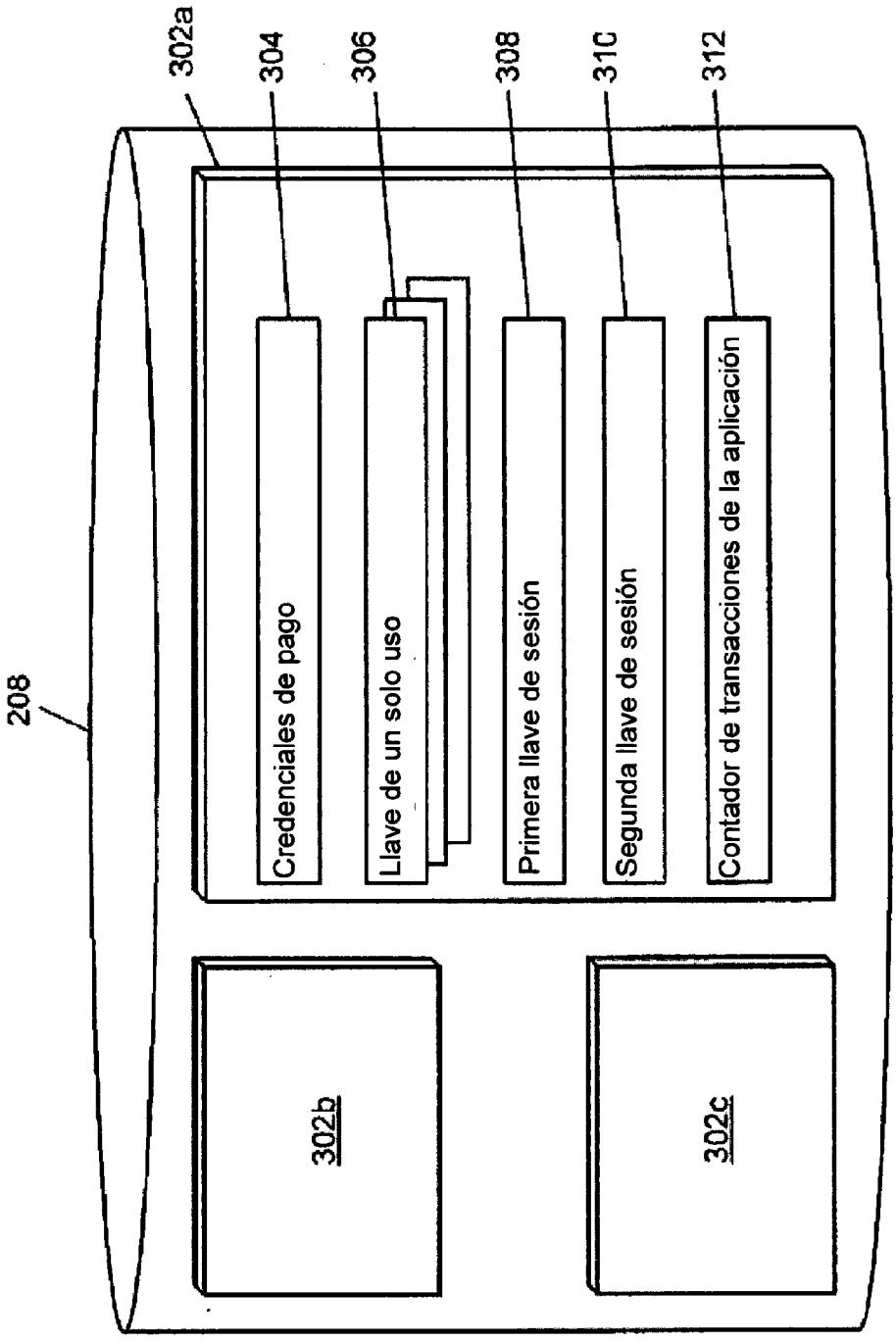

Figura 3

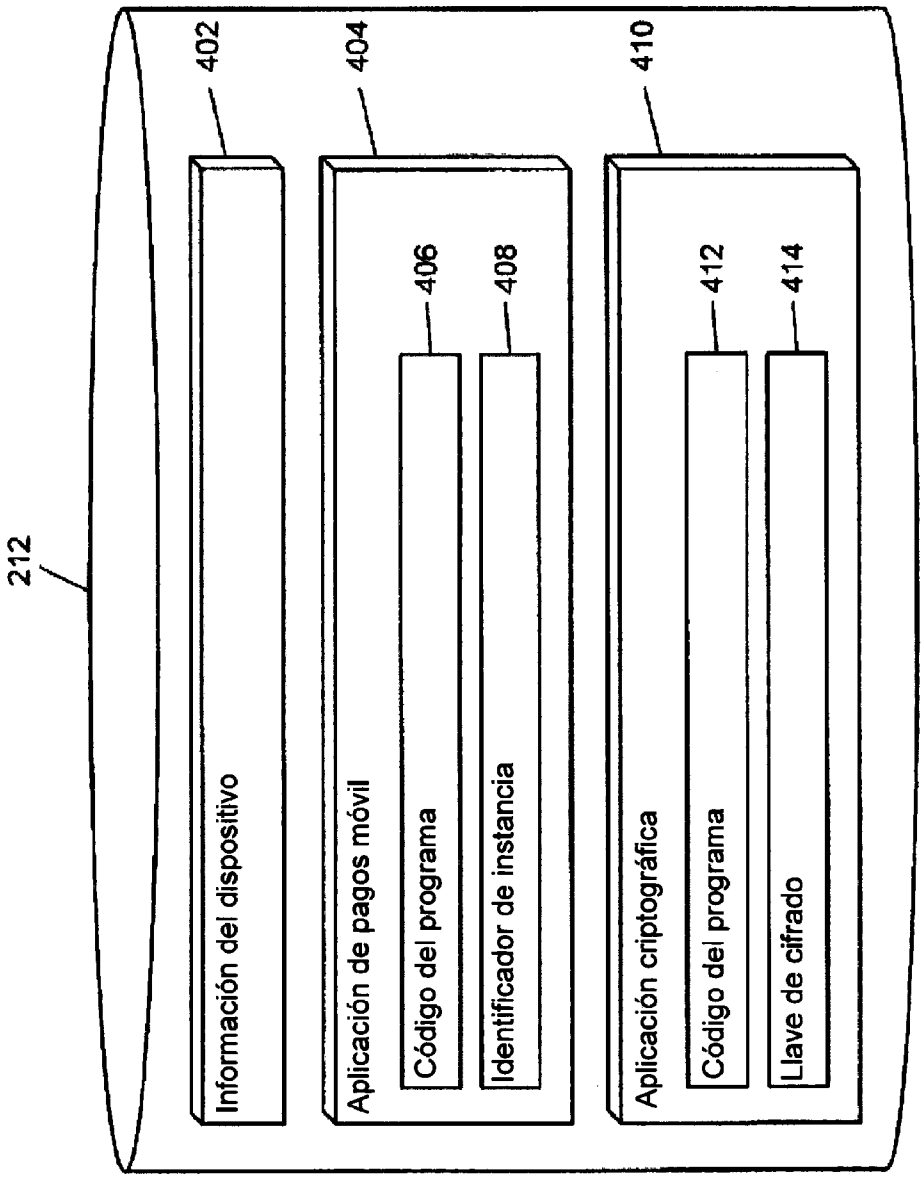

Figura 4

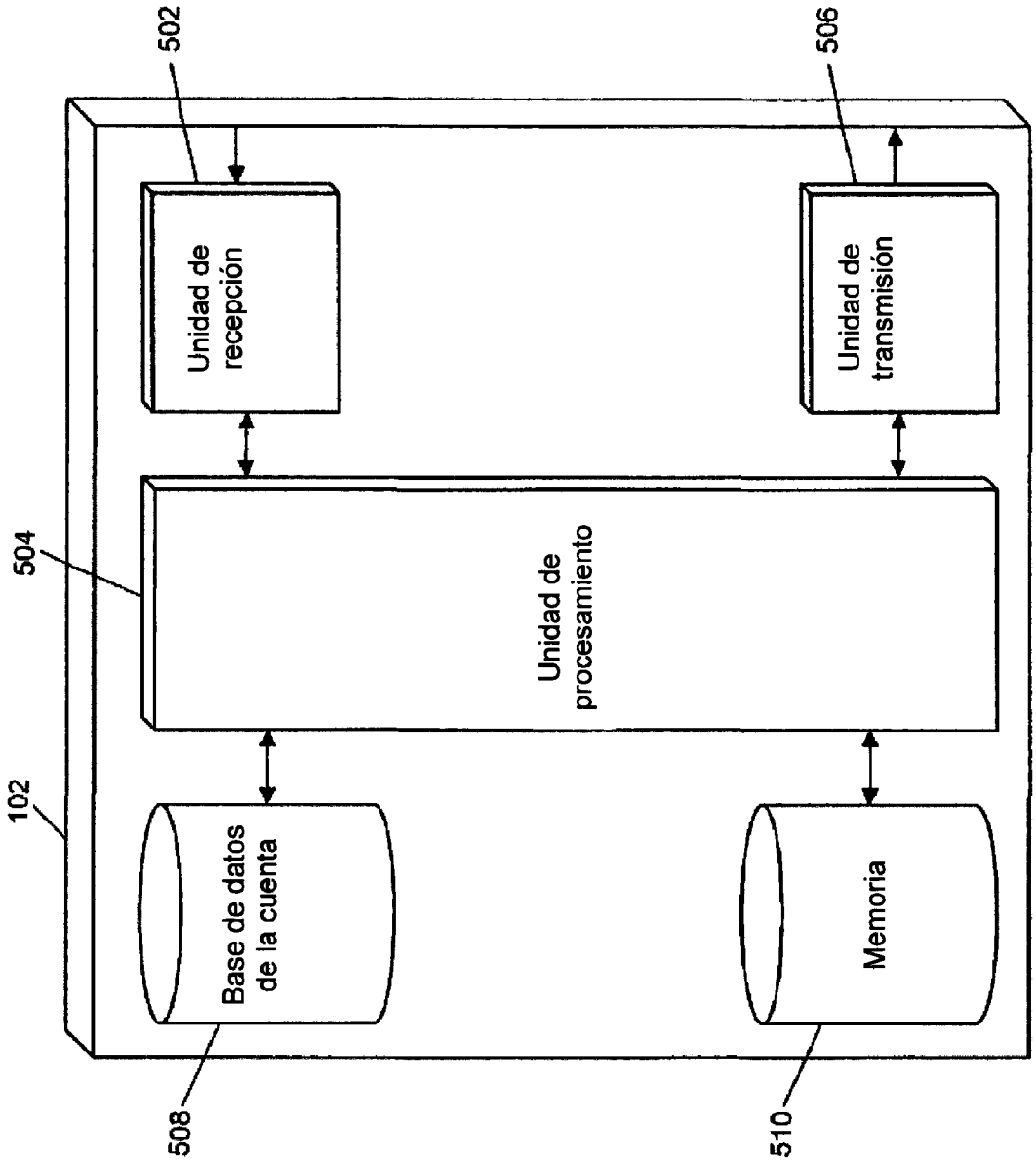

Figura 5

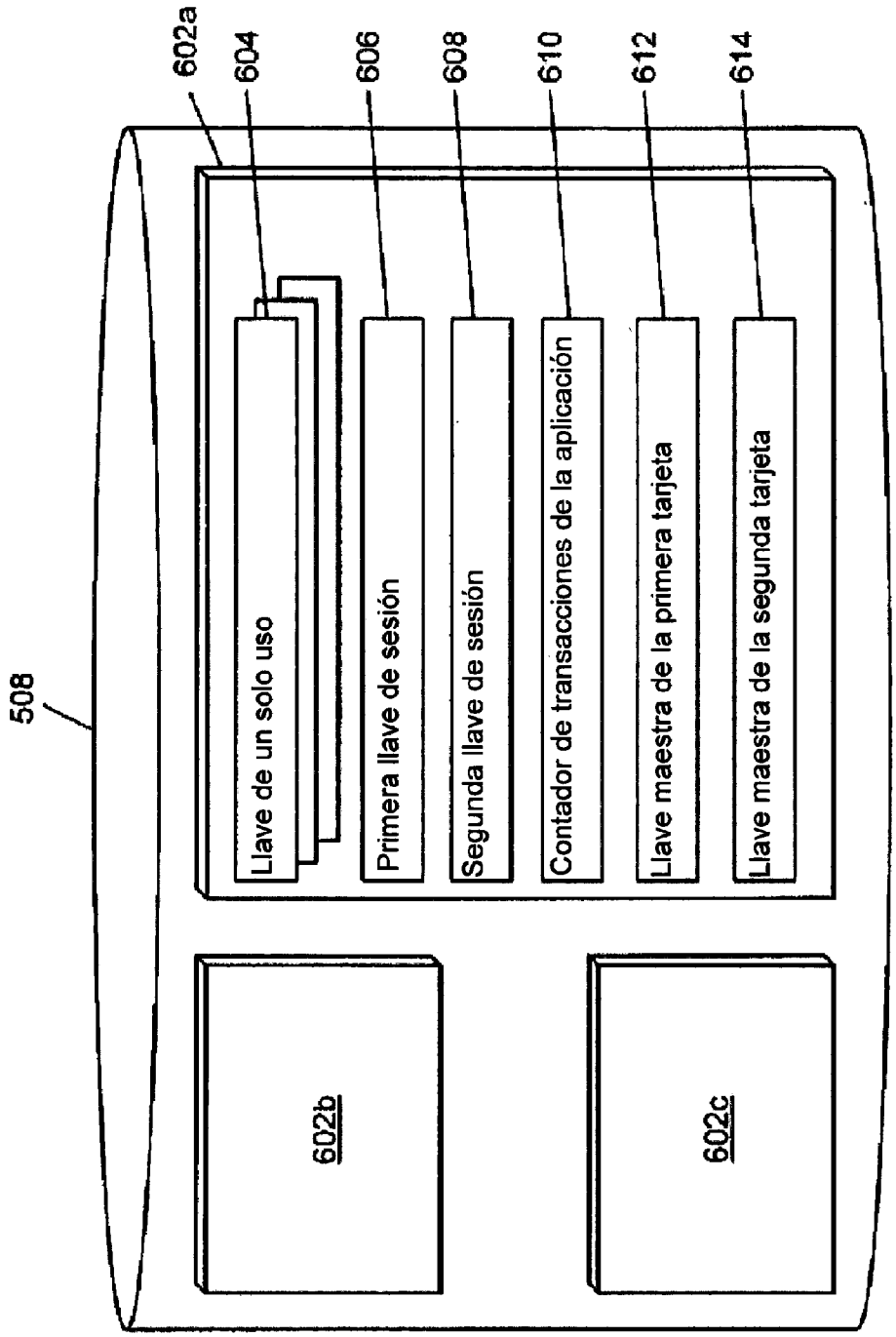

Figura 6

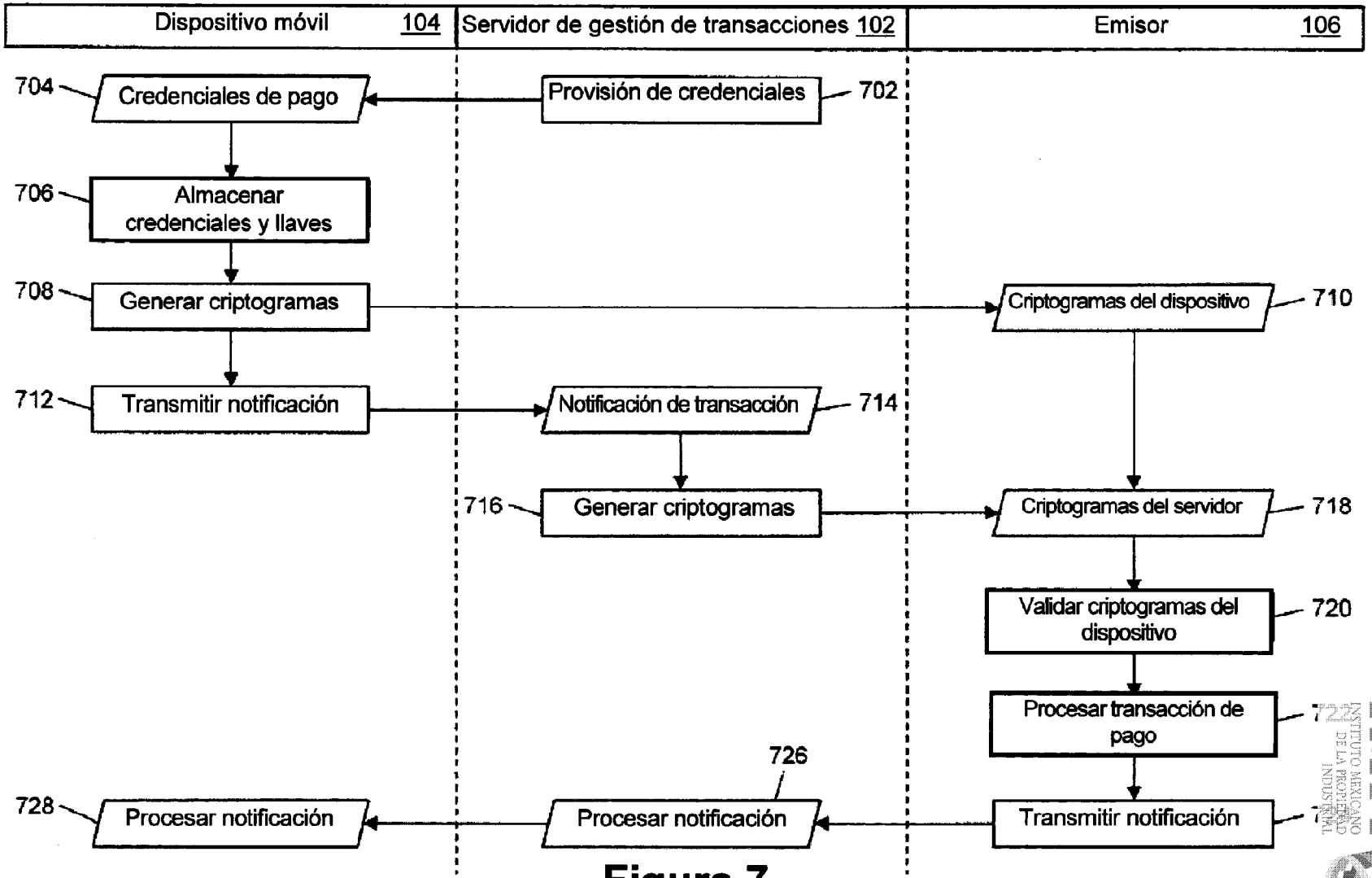

Figura 7

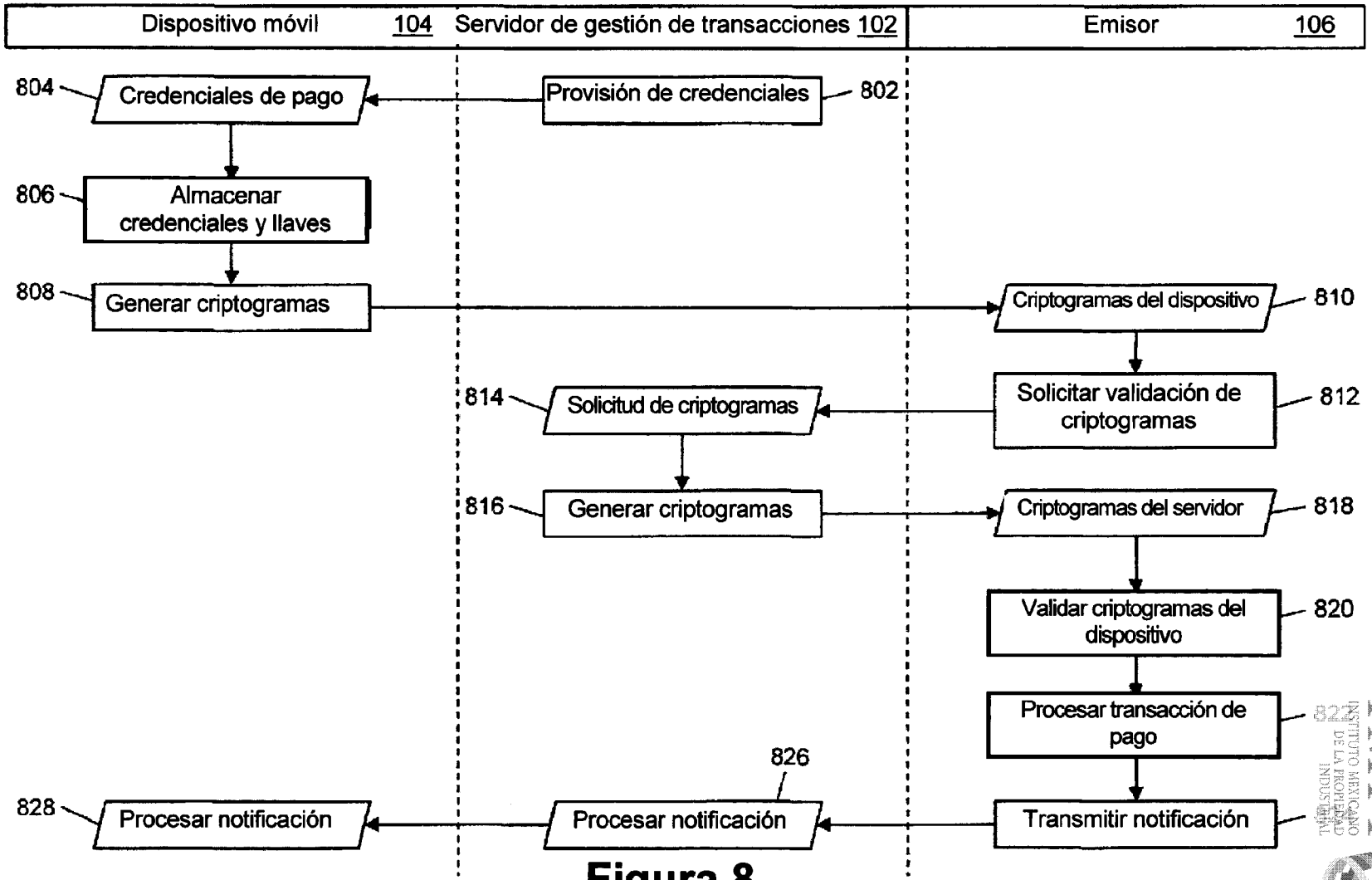

Figura 8

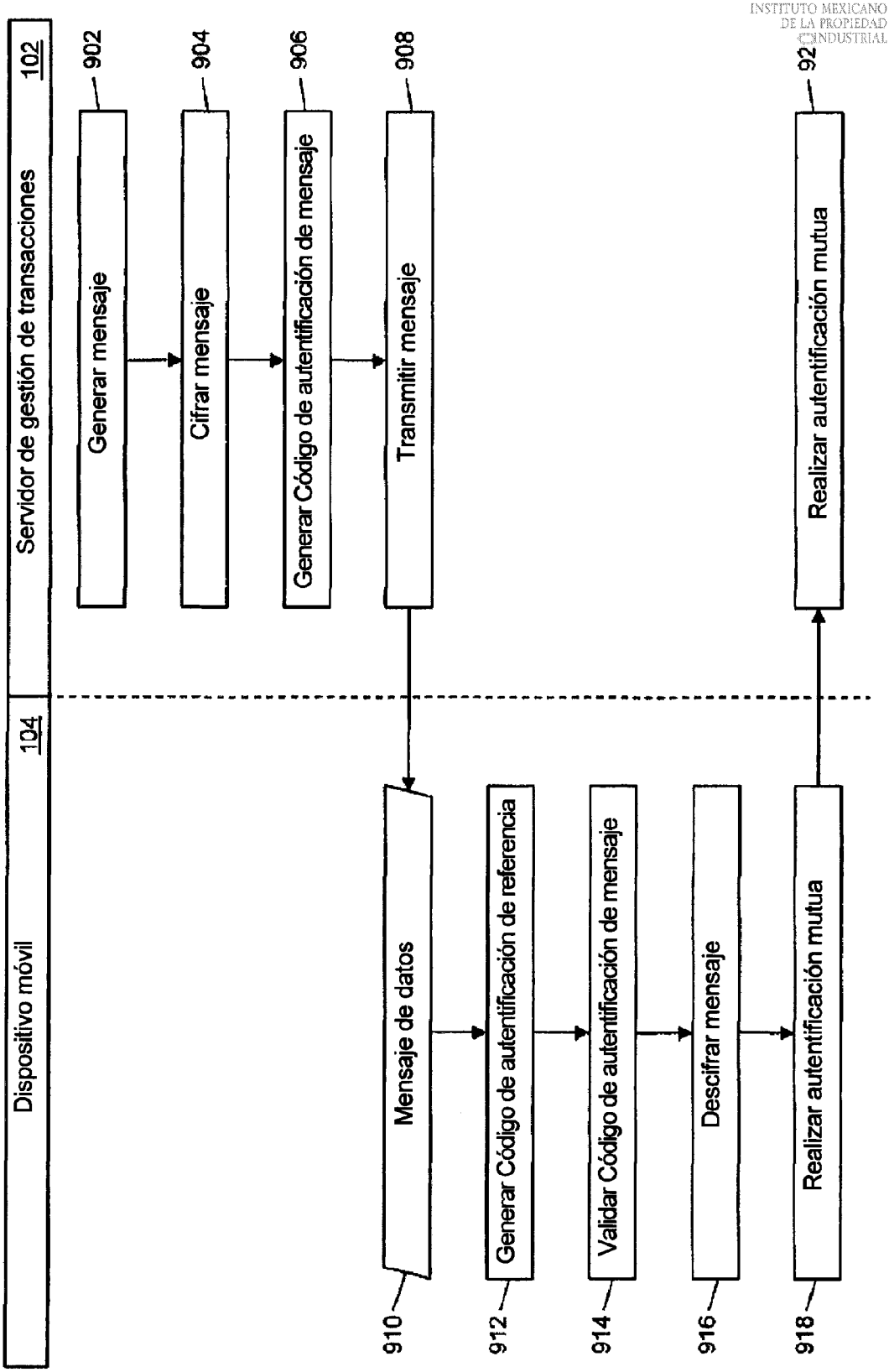

Figura 9

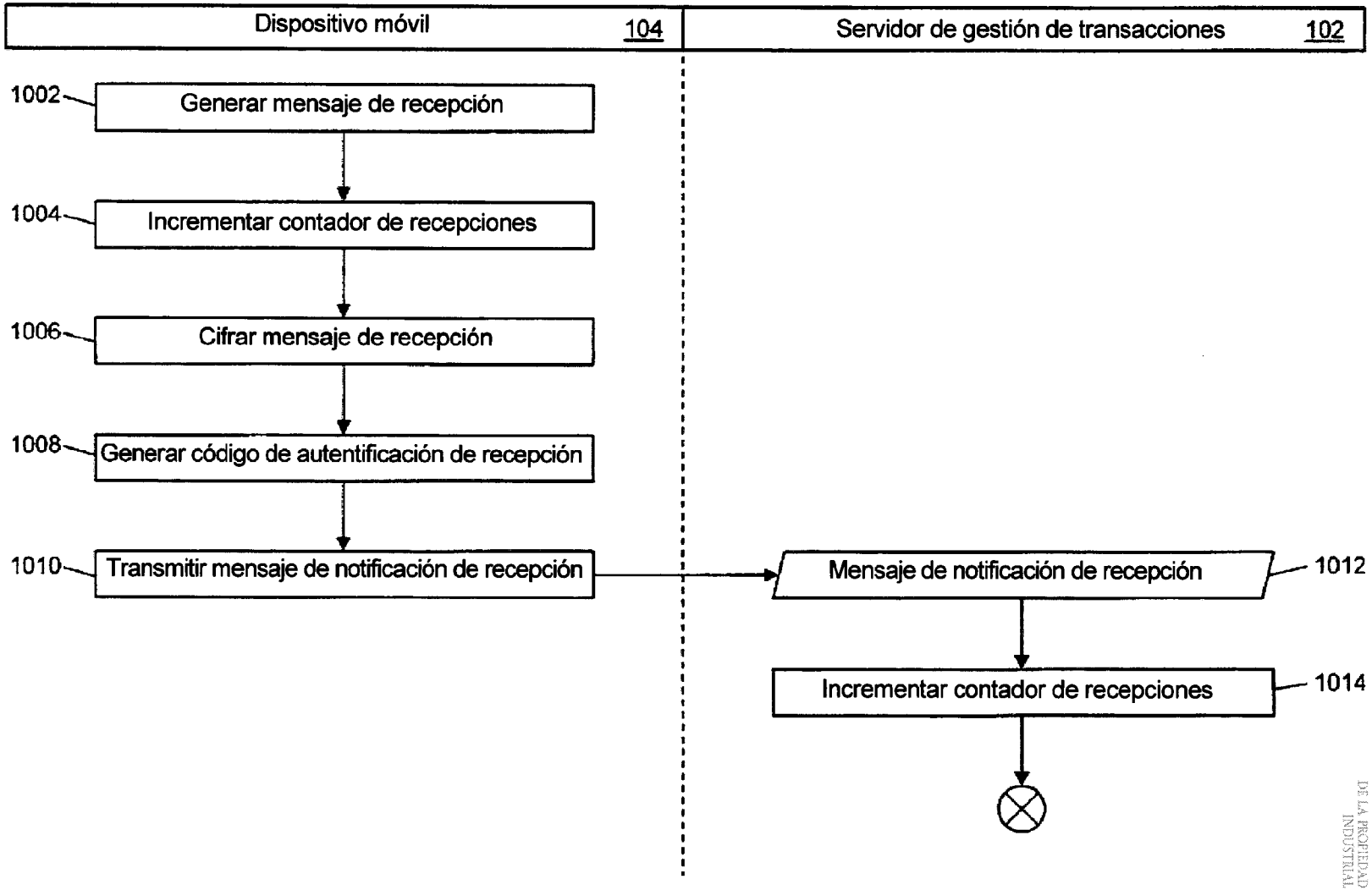

Figura 10A

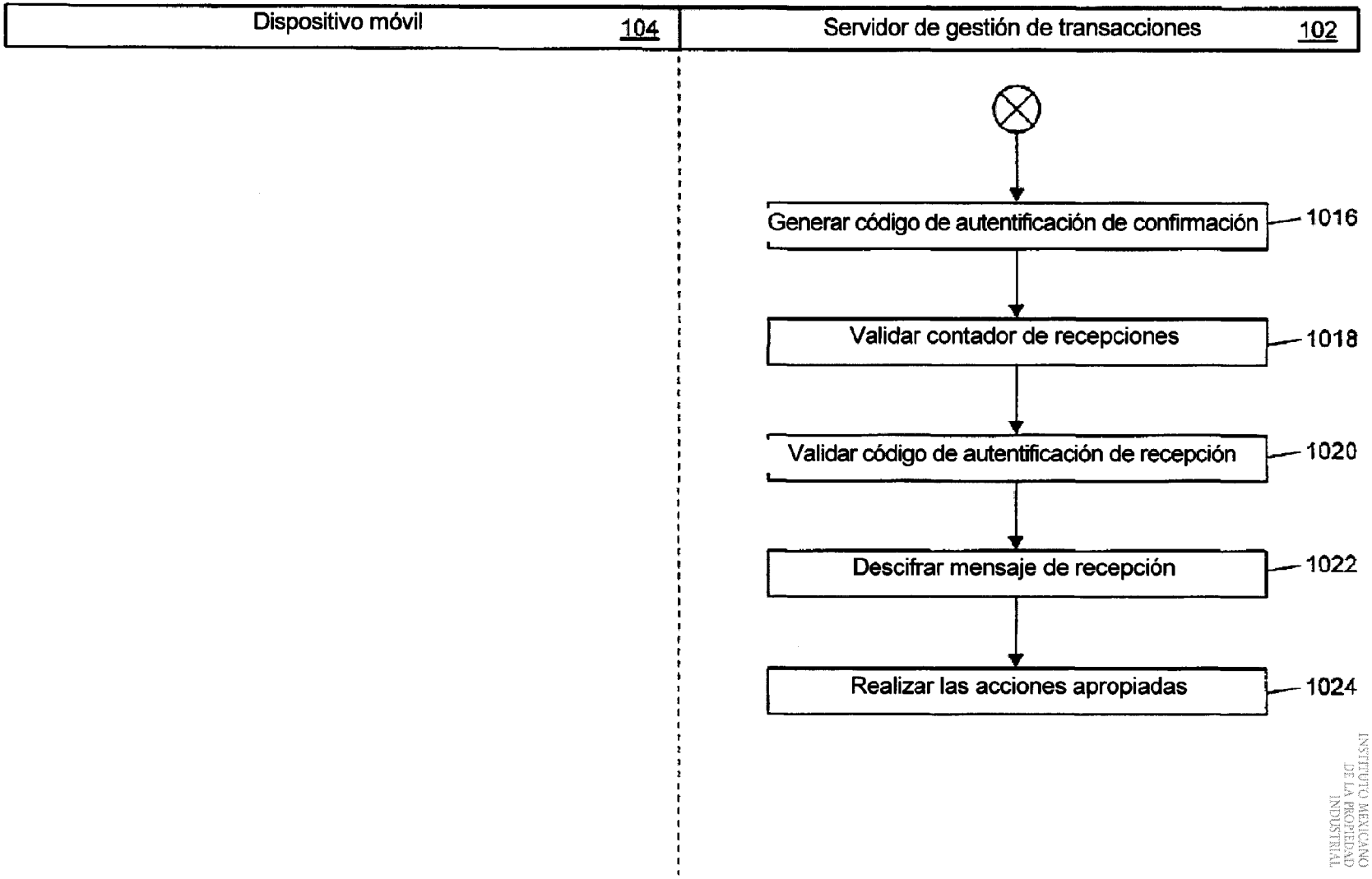

Figura 10B

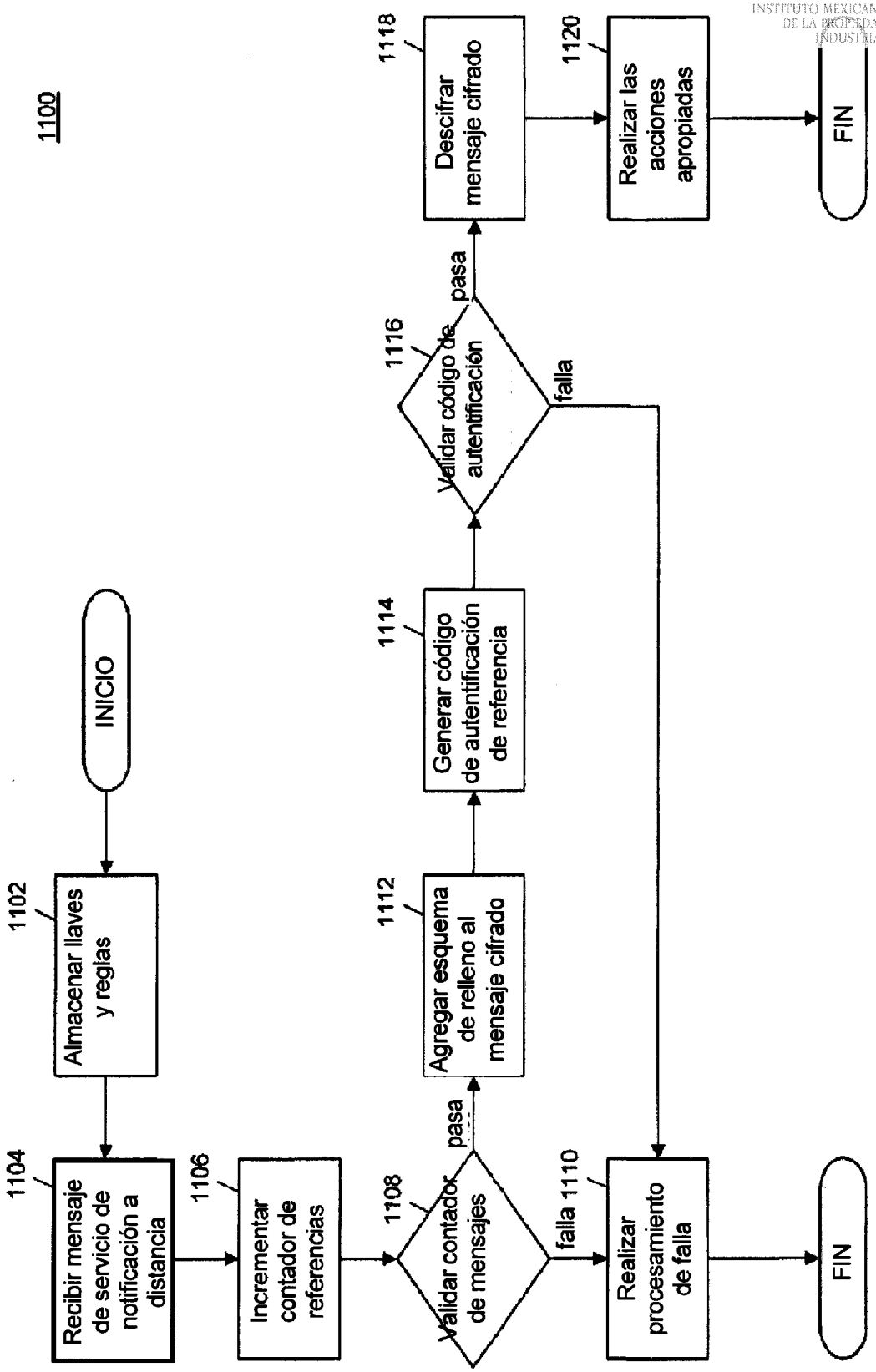

Figura 11

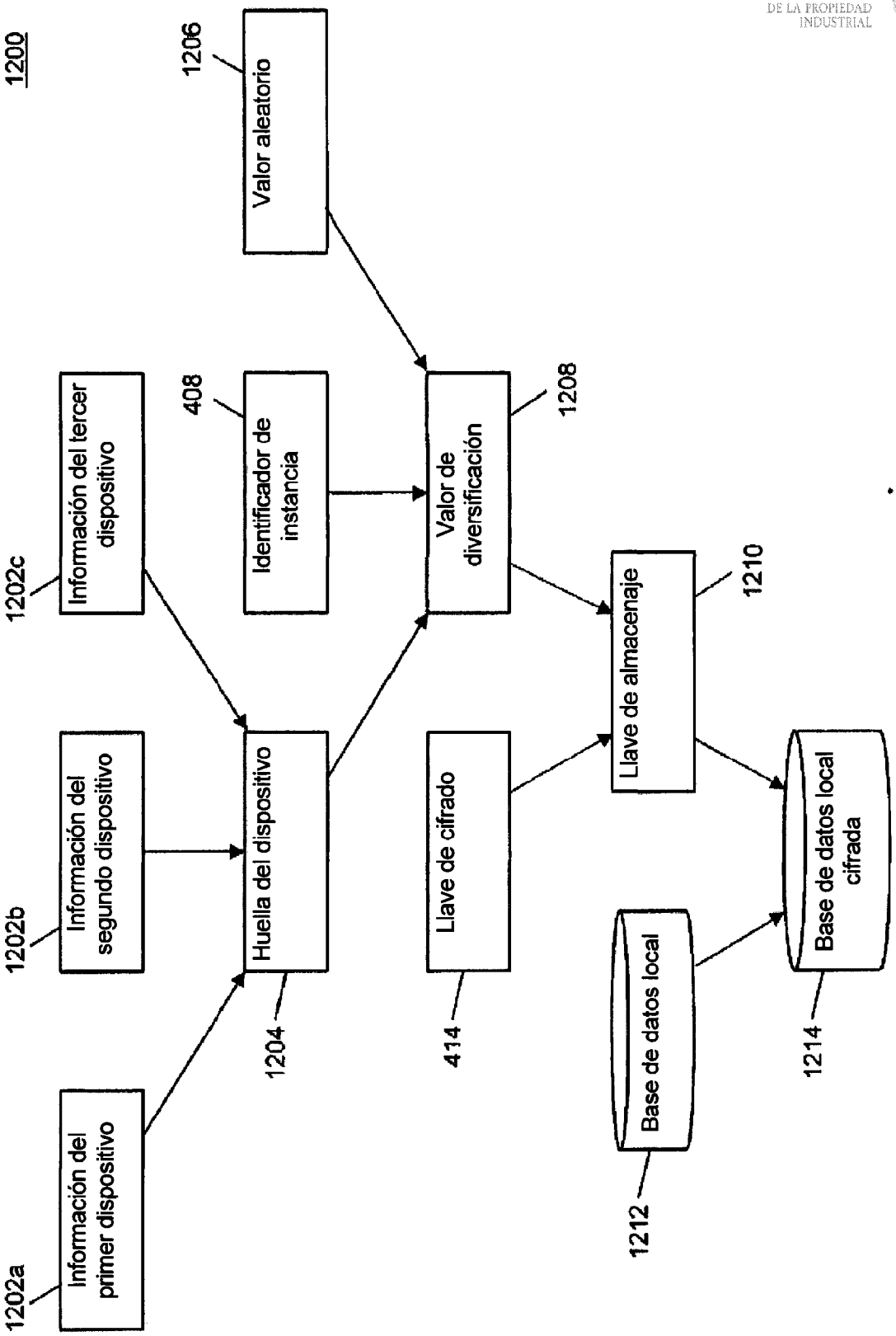

Figura 12

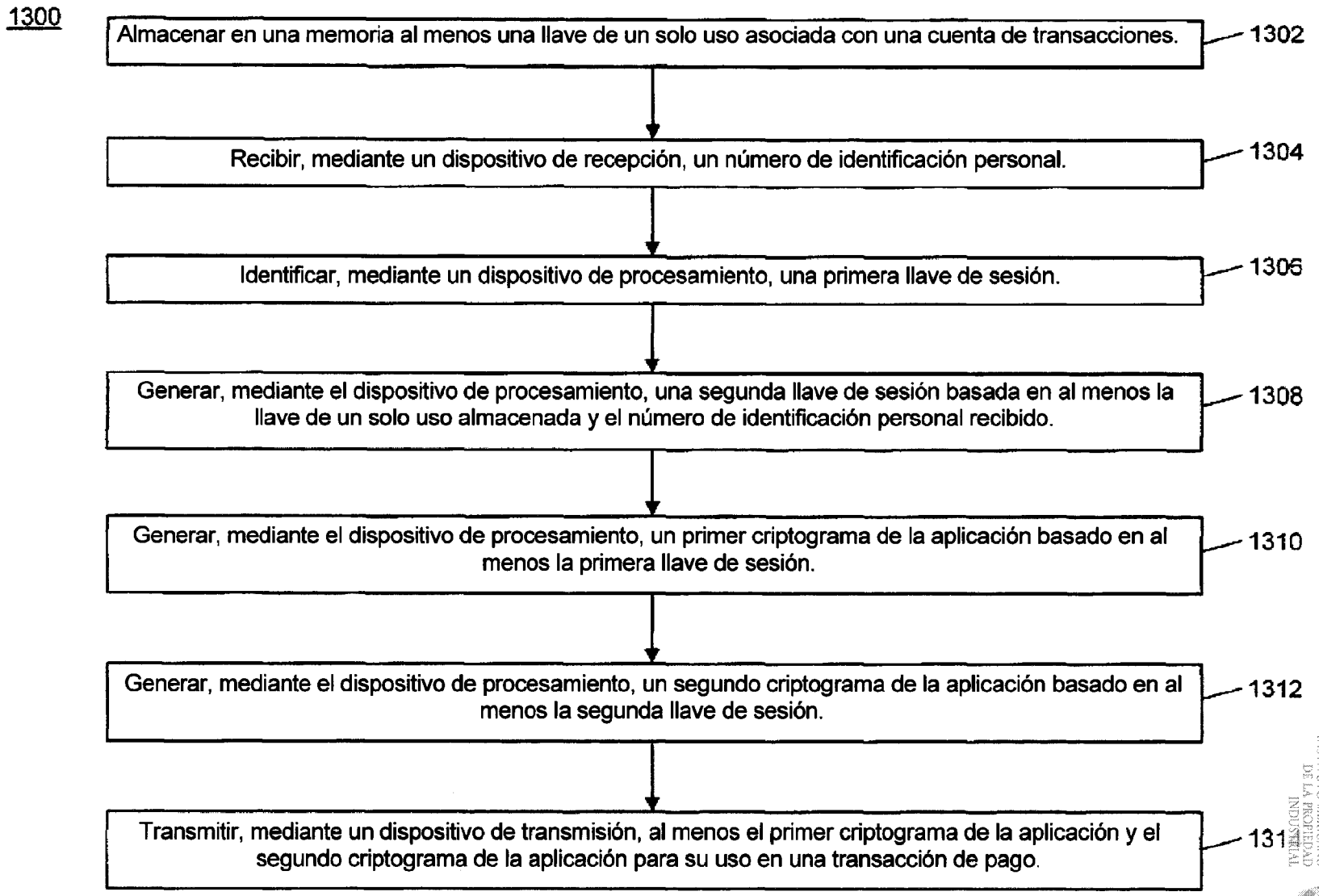

Figura 13

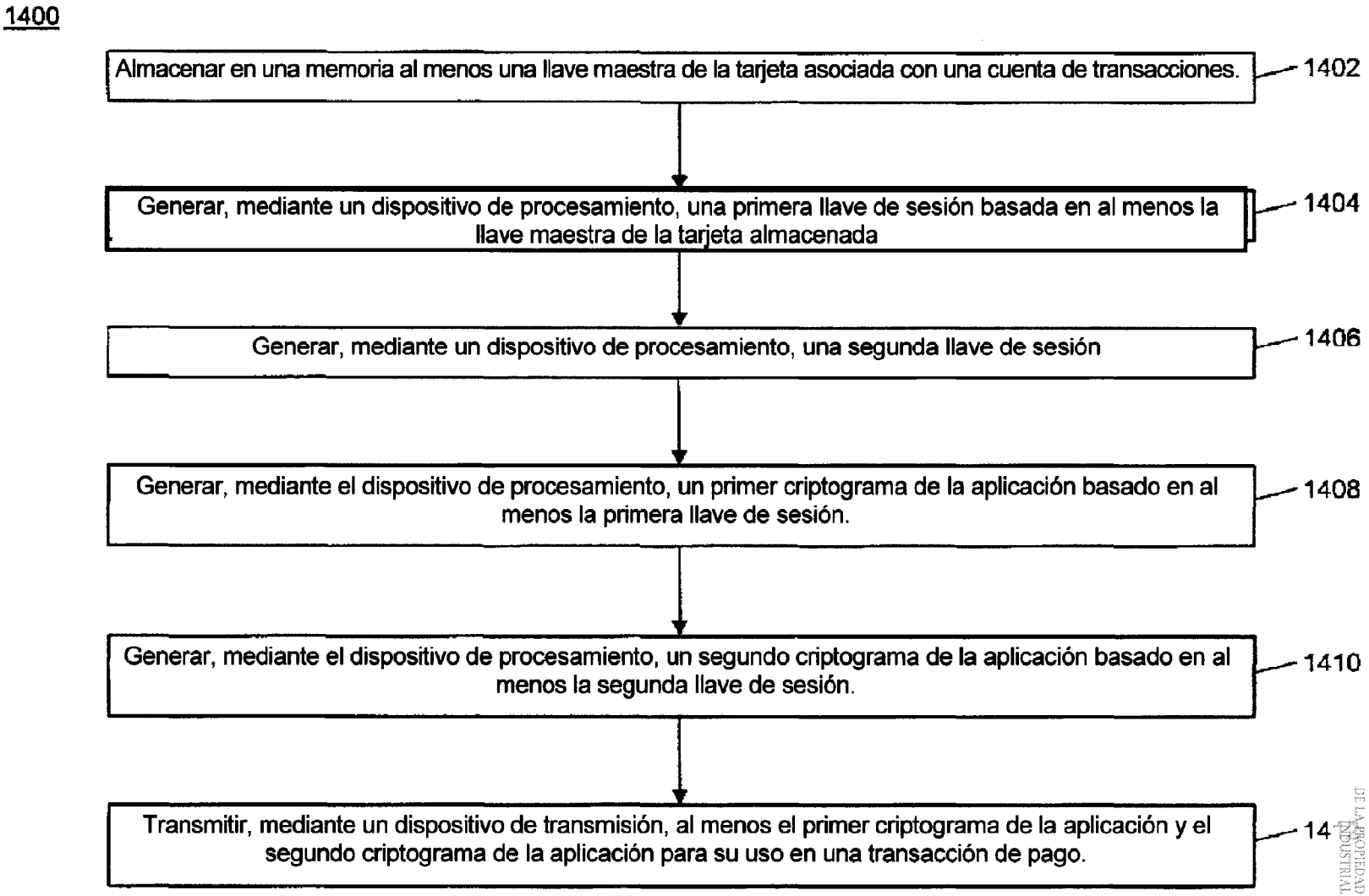

Figura 14

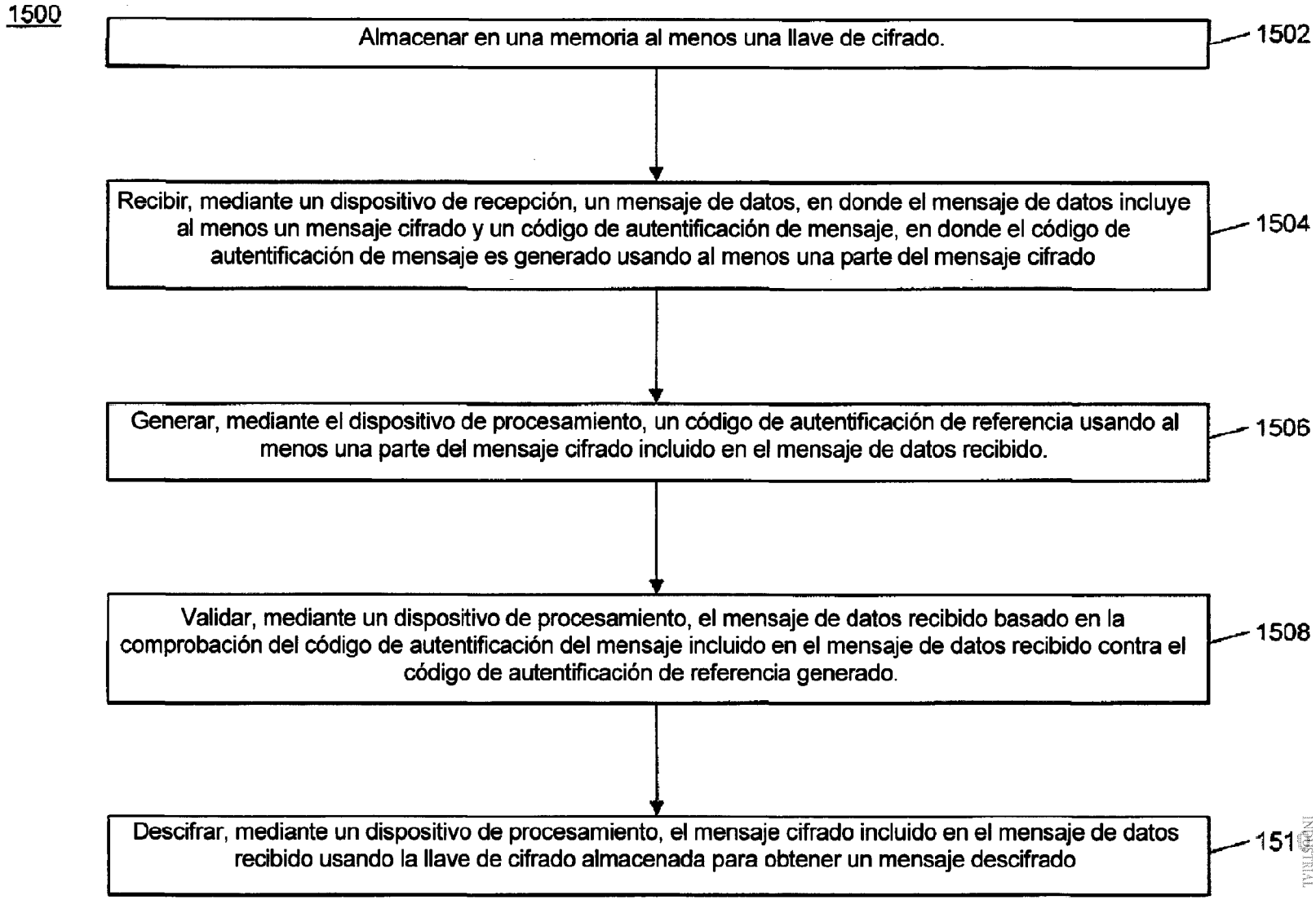

Figura 15

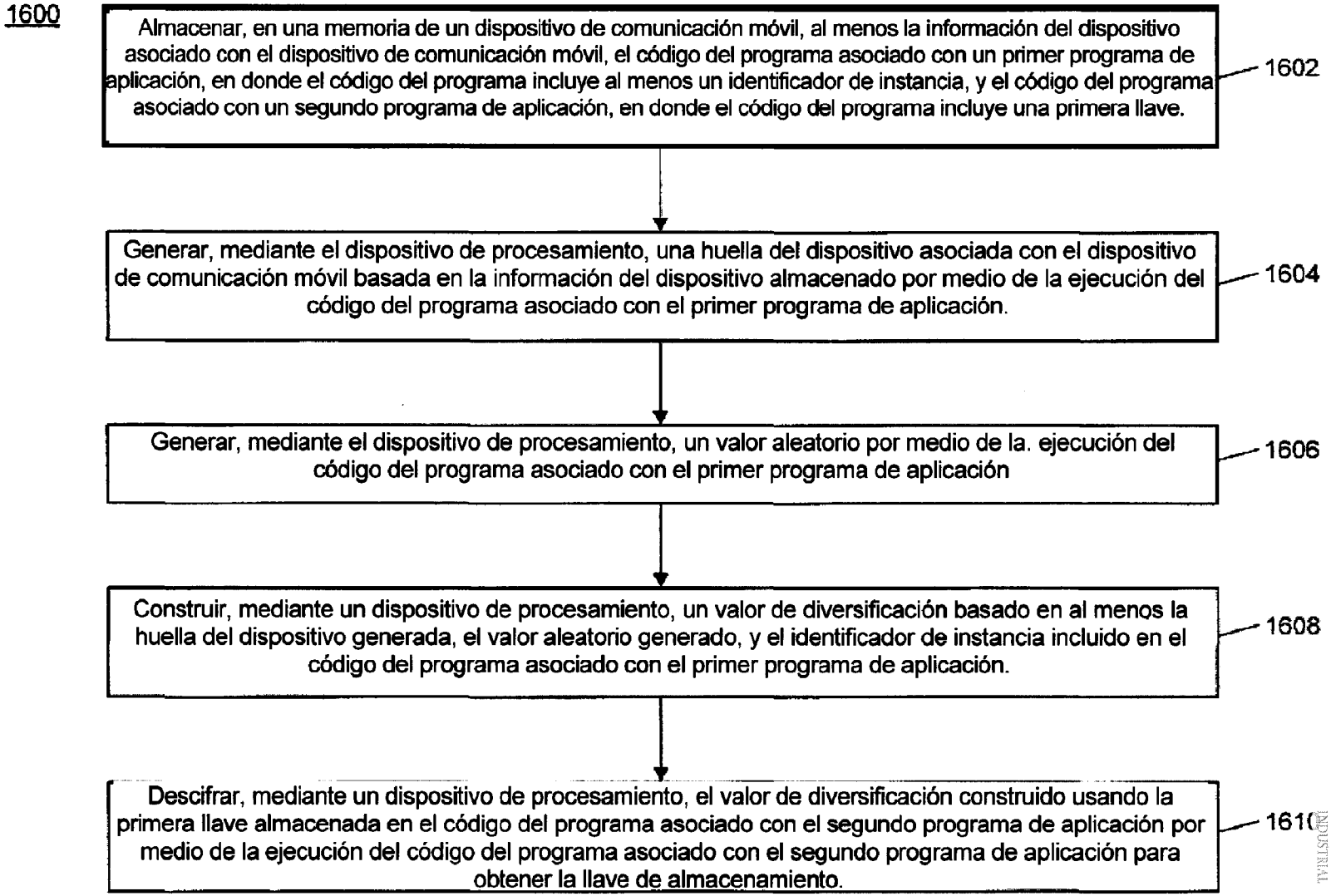

Figura 16

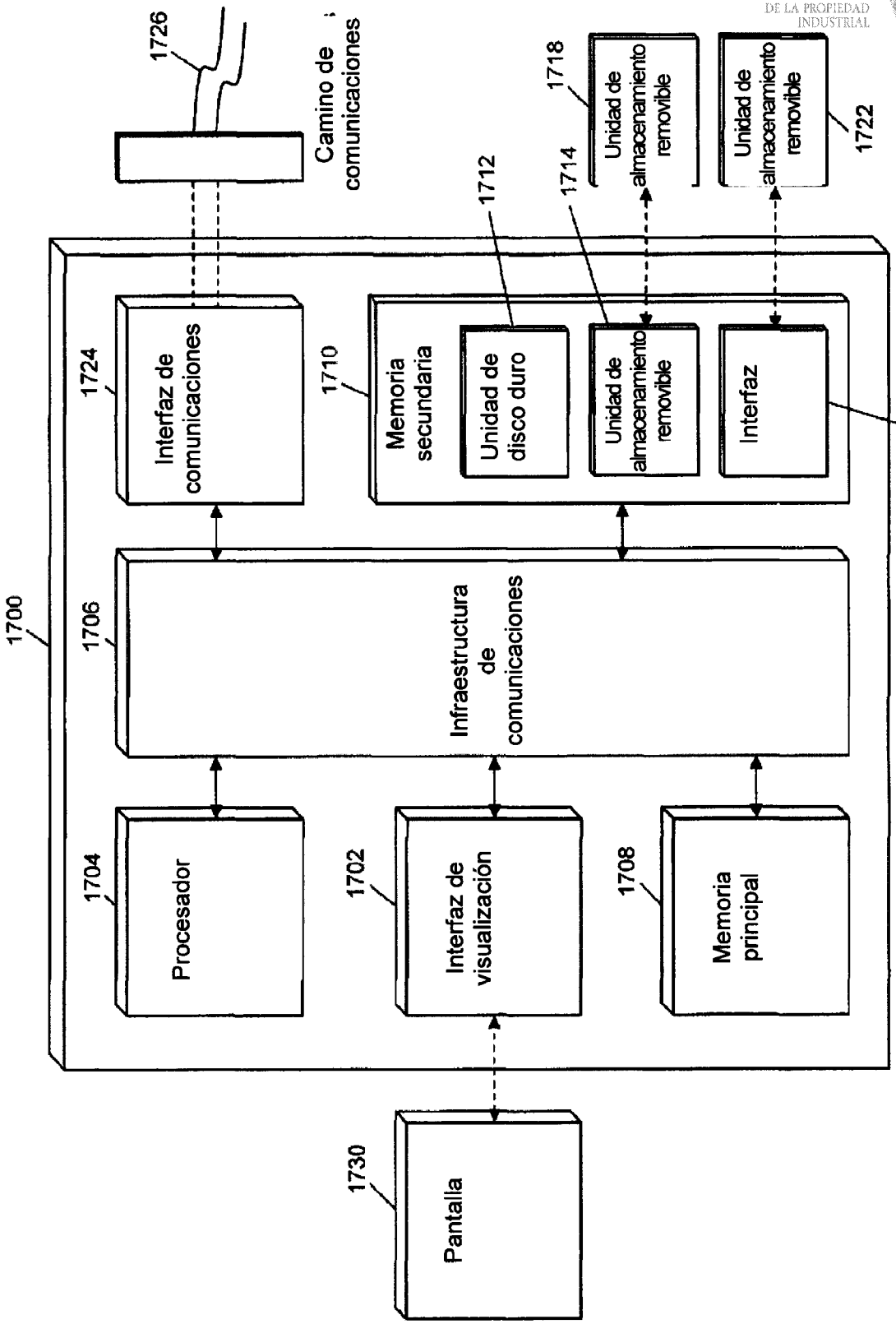

Figura 17