

DIRECCIÓN DE NUEVAS CREACIONES

SOLICITUD FASE NACIONAL - PCT

1 Titulo de la Invención(200 caracteres o espacios máximos)

MÉTODO Y SISTEMA PARA LA TRANSMISIÓN SEGURA DE MENSAJES DEL SERVICIO DE NOTIFICACIÓN A DISTANCIA A DISPOSITIVOS MÓVILES SIN ELEMENTOS DE SEGURIDAD

2 Datos del Solicitante

Nombre: MASTERCARD
INTERNATIONAL
INCORPORATED

**Dirección
Electrónica:** tmtamayo@gmail.com

Dirección: 2000 Purchase Street
Purchase, New York
10577

**Domicilio/País de
constitución:** ESTADOS UNIDOS DE
AMERICA - NEW YORK -
PURCHASE

Identificación:

☐ CEDULA DE
CIUDADANIA

☐ CEDULA DE
EXTRANJERIA

☒ EMPRESA
EXTRANJERA

☐ NIT

☐ PASAPORTE

Número: 1044316-

3 Solicitantes

Apellidos - Nombres o Razón Social

Tipo

Identificación

1. MASTERCARD INTERNATIONAL
INCORPORATED

EE

1044316

4 Datos del Inventor

Nombre:		Mehdi COLLINGE	Dirección Electrónica:	tmtamayo@gmail.com
Dirección:		8 Rue Cesar Franck, B-1420 Braine- L Alleud	Domicilio/País de constitución:	BELGICA - BRABANT WALLON - BRAINE- L´ALLEUD
Identificación: ☐ CEDULA DE CIUDADANIA ☐ EMPRESA EXTRANJERA ☐ PASAPORTE ☐ CEDULA DE EXTRANJERIA ☐ NIT ☒ No Aplica				
Número:		-		
5	Inventor(es)			
Apellidos - Nombres		Domicilio		
1.	COLLINGE Mehdi	BELGICA		
2.	WARD Michael Christopher	REINO UNIDO DE LA GRAN BRETAÑA		
3.	SMETS Patrik	BELGICA		
4.	CATELAND Axel Emile Jean Charles	ESTADOS UNIDOS DE AMERICA		
5.	RADU Cristian	BELGICA		
6	Datos Inventor(es)			
País de Residencia		Departamento/Estado	Ciudad	Dirección
1.	BELGICA	BRABANT WALLON	BRAINE-L´ALLEUD	8 Rue Cesar Franck, B-1420 Braine- L Alleud
2.	REINO UNIDO DE LA GRAN BRETAÑA	INGLATERRA	SOMERSET	Easterdown , Upton, Taunton, Somerset TA42JB
3.	BELGICA	ANTWERPEN	NIJLEN	Hooidonkstraat 59, B-2560 Nijlen

4.	ESTADOS UNIDOS DE AMERICA	NEW YORK	NEW YORK	15 Puritan Drive Scarsdale, New York 10583
5.	BELGICA	BRABANT WALLON	BEAUVECHAIN	Rue de Tourinnes 2, B-1320 Beauvechain
7	Datos del Representante Legal / Apoderado			
Nombre:		JOHAN SEBASTIAN GÓMEZ VILLA	Dirección Electrónica:	tmtamayo@gmail.com
Dirección:		CARRERA 13 A 28 38 OFC. 230 MZ 2. PARQUE BAVARIA	Domicilio/País de constitución:	COLOMBIA - CUNDINAMARCA - BOGOTA D.C.
Identificación: ☒ CEDULA DE CIUDADANIA ☐ CEDULA DE EXTRANJERIA ☐ EMPRESA EXTRANJERA ☐ NIT ☐ PASAPORTE				
Número:		9868640-		
Presentación de Poder				
Año de Radicación				
Número de Radicación				
8	Datos Solicitud: PCT / WO			
Número Solicitud:		PCT/US2014/068078	Fecha Solicitud:	02/12/2014
Número Publicacion:		WO/2015/084797	Fecha Publicacion:	11/06/2015
9	Declaraciones de prioridad		☒ SI ☐ NO	
	(33) País de origen	Codigo del país	(31) No. Solicitud	(32) Fecha
1.	ESTADOS UNIDOS DE AMERICA	US	61/910,819	02/12/2013
2.	ESTADOS UNIDOS DE AMERICA	US	61/951,842	12/03/2014
3.	ESTADOS UNIDOS DE AMERICA	US	61/955,716	19/03/2014

4.	ESTADOS UNIDOS DE AMERICA	US	61/979,113	14/04/2014
5.	ESTADOS UNIDOS DE AMERICA	US	61/979,132	14/04/2014
6.	ESTADOS UNIDOS DE AMERICA	US	61/979,122	14/04/2014
7.	ESTADOS UNIDOS DE AMERICA	US	61/980,784	17/04/2014
8.	ESTADOS UNIDOS DE AMERICA	US	61/996,665	14/05/2014

10	Reivindicaciones		
Número reivindicaciones:		28	Pago Reivindicaciones:
			Si

11	Reducción de tasas.
<i>Declaro que carezco de medios económicos para presentar la solicitud de patente.</i> ☐ SI ☒ NO Nota: En caso de ser persona natural y carecer de medios económicos, y por lo tanto, aplique la reducción de tasas a que se refiere la resolución vigente en tarifas, debe firmar la presente solicitud bajo la gravedad de juramento.	
☐ Micro, pequeñas y medianas empresas ☐ Universidades públicas o privadas ☐ Entidades sin ánimo de lucro Debe aportar los documentos que se indican en el numeral 17 de anexos	

12	Documentos Anexos
☒ Reivindicaciones ☒ Descripción ☒ Dibujos y/o Figuras ☒ Resumen ☐ Certificado Depósito Material Biológico ☐ Uso de Conocimiento tradicional ☐ Listado de secuencias ☐ Artes finales 12 x 12 cm ☐ Poderes, si fuere el caso ☐ Copia de la primera solicitud si se reivindica prioridad ☐ Traducción simple de la primera solicitud, si se reivindica prioridad ☒ Otros Anexos	

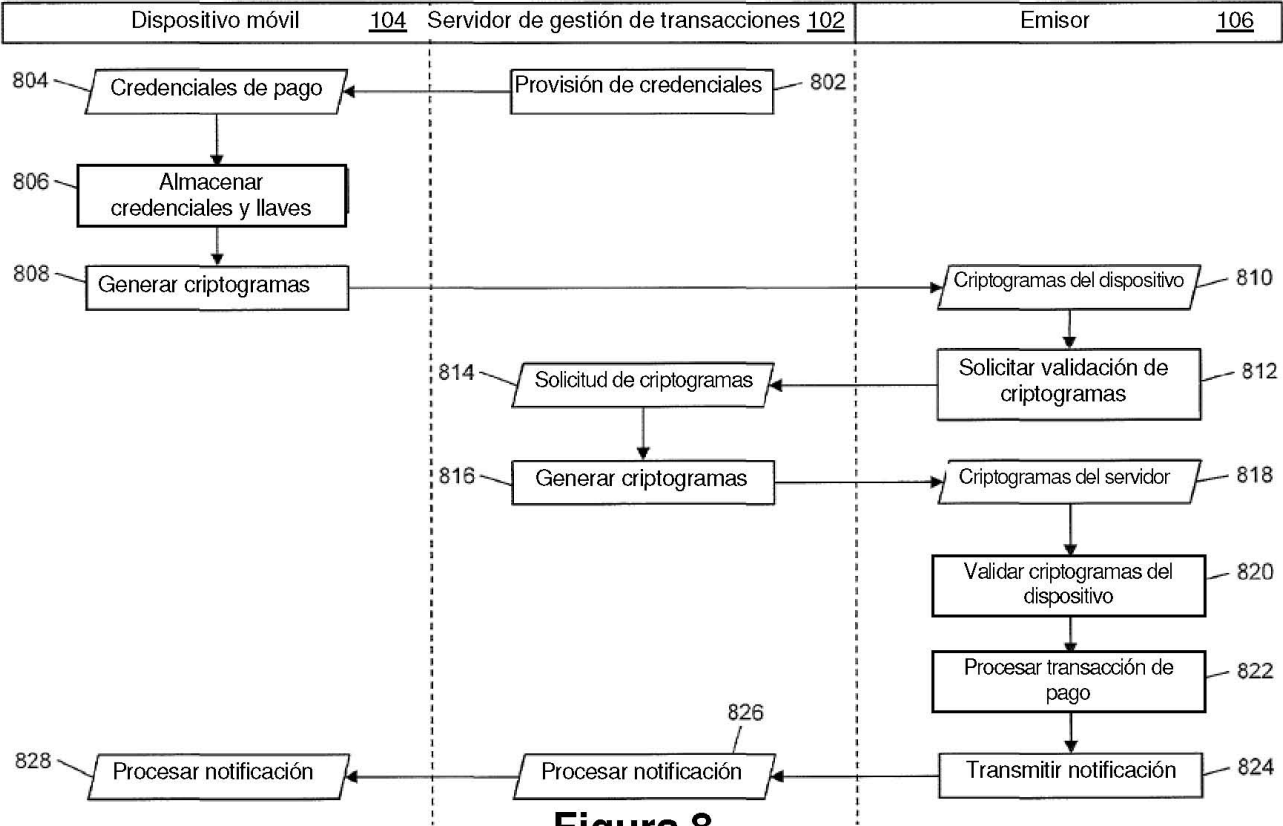
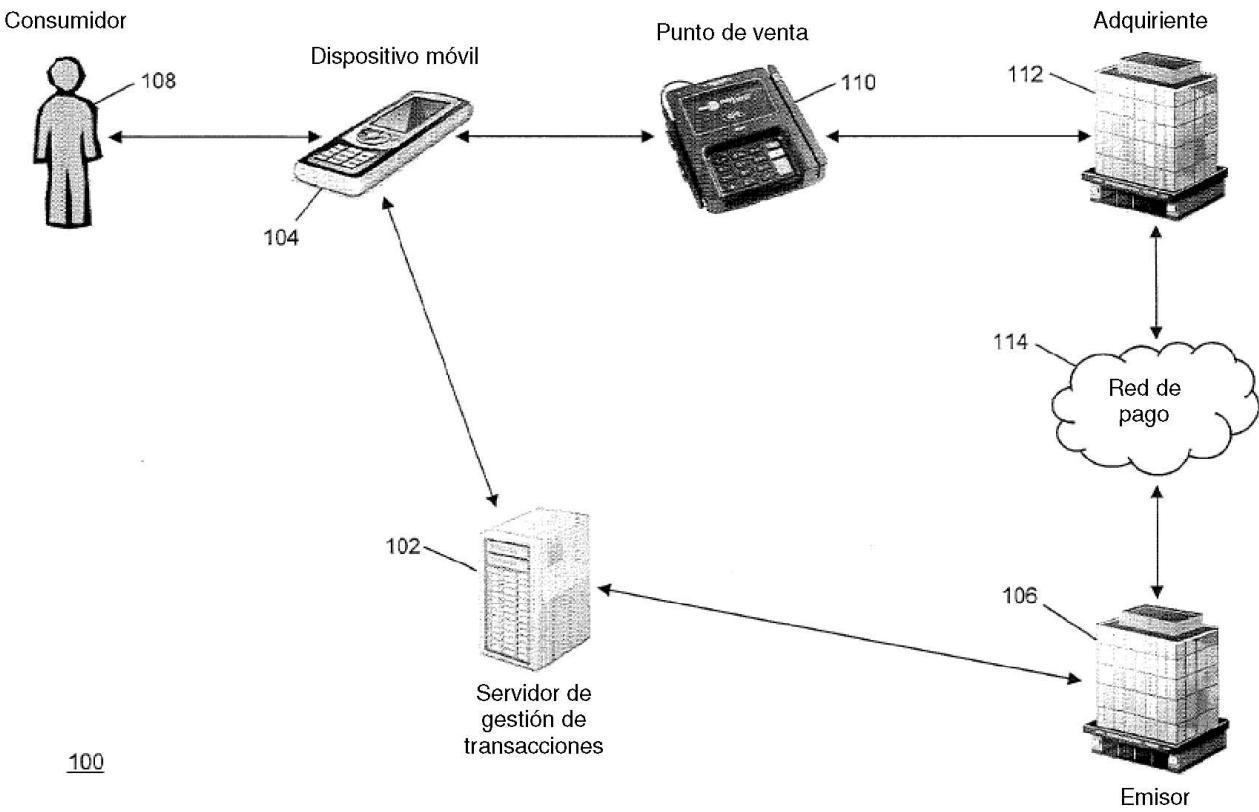


Figura 8



100

Figura 1

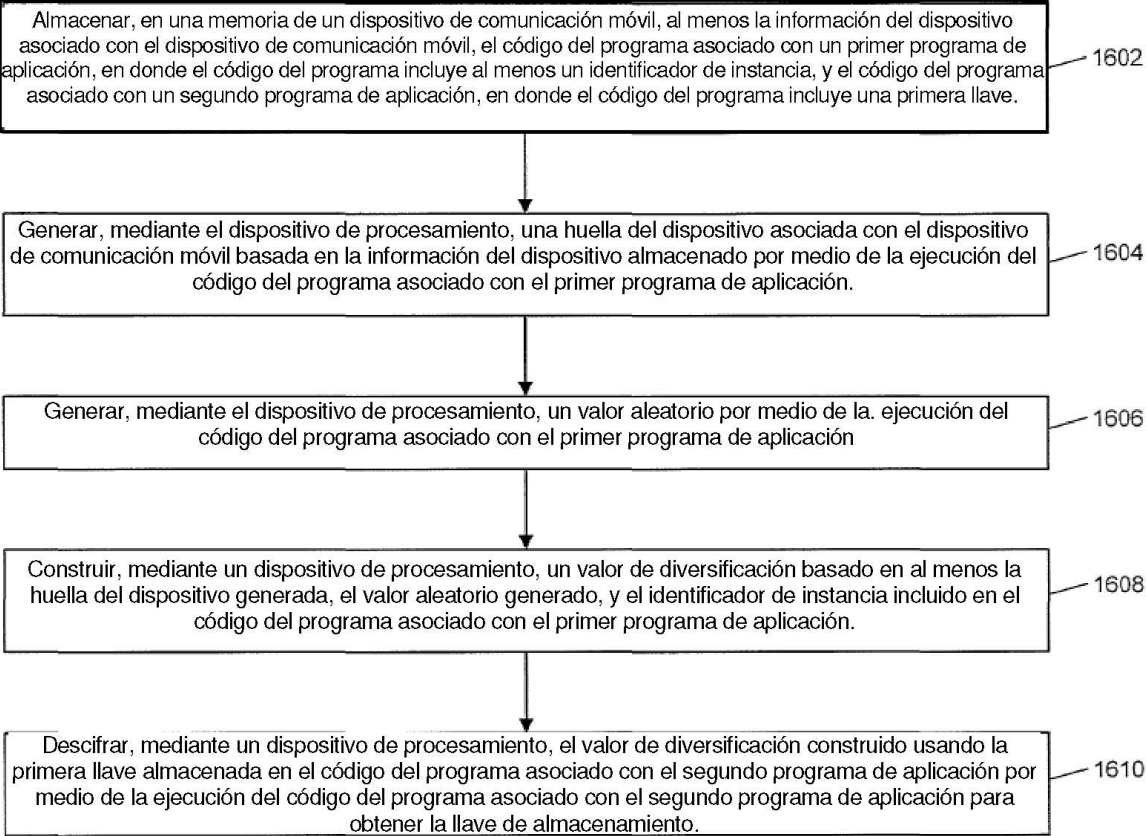


Figura 16

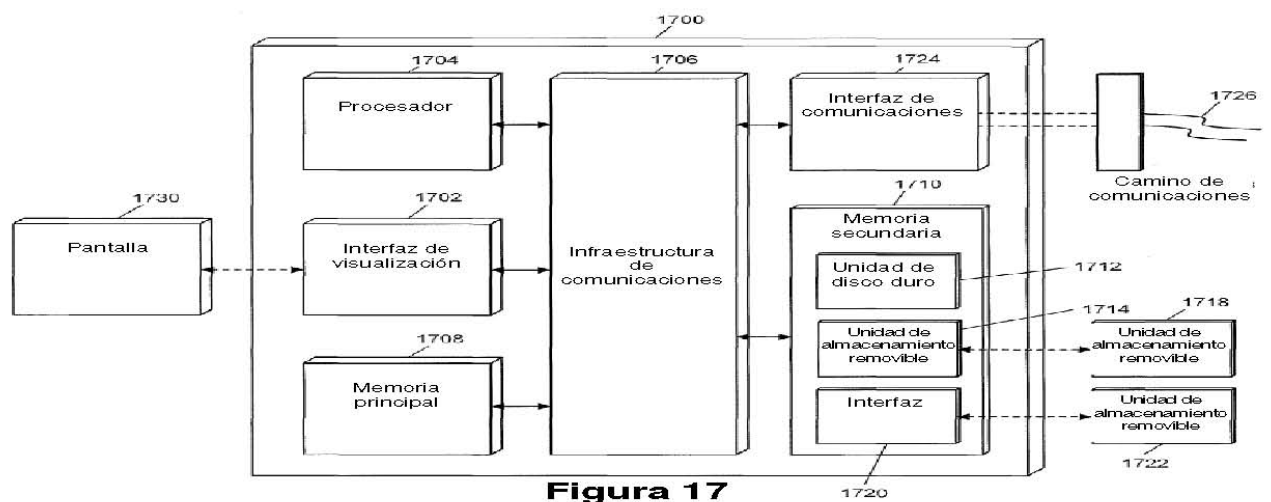


Figura 17

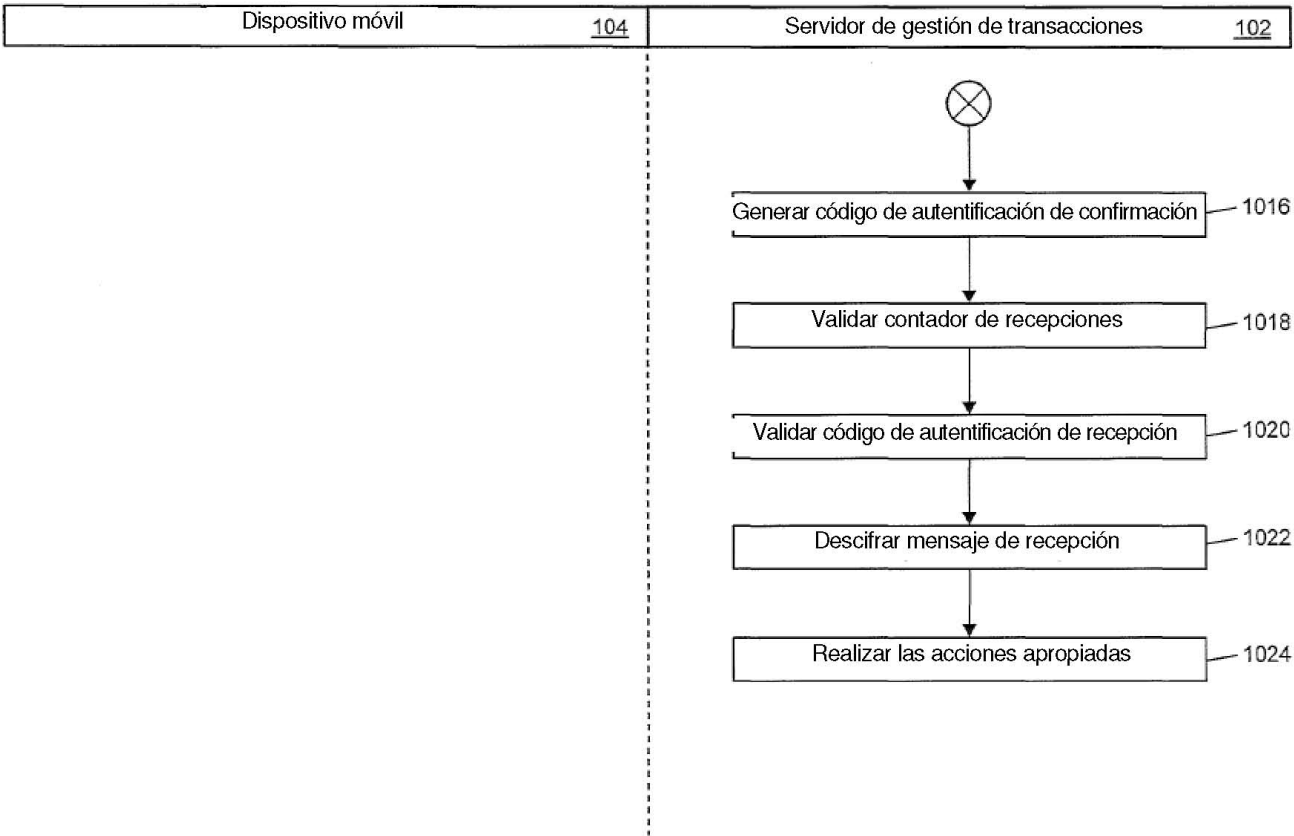


Figura 10B

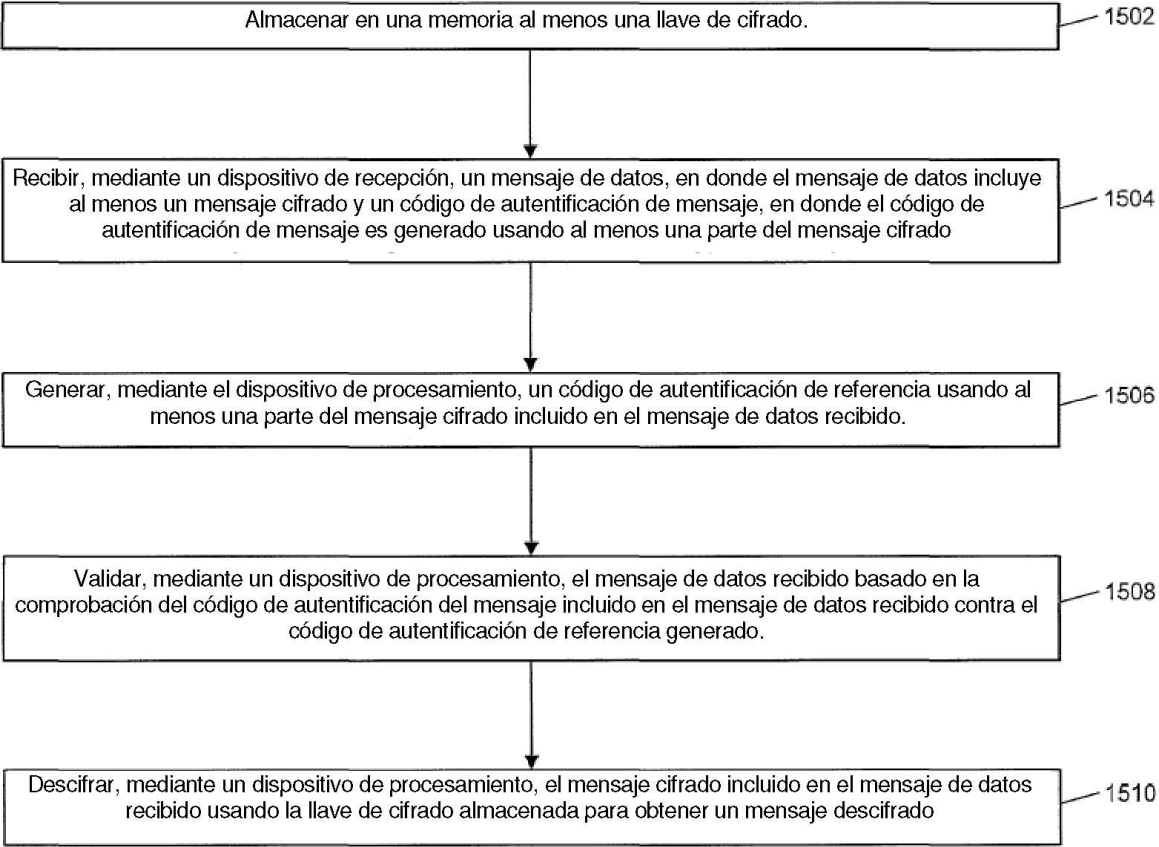


Figura 15

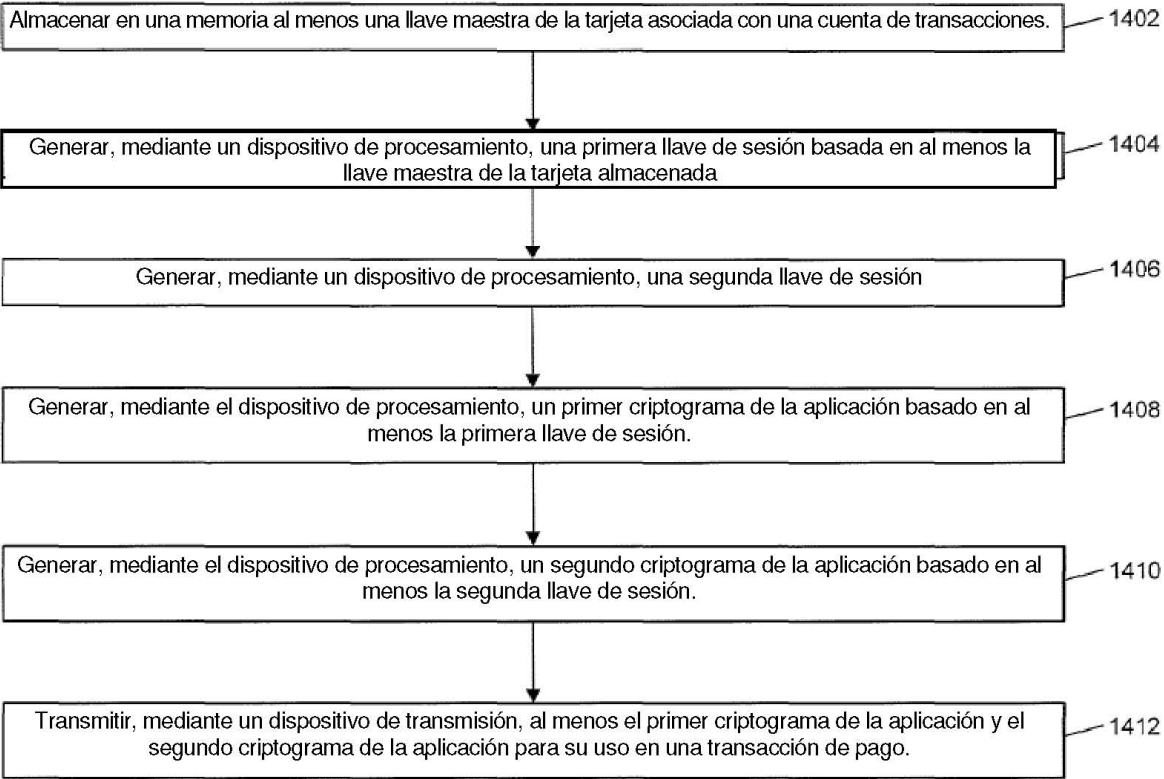


Figura 14

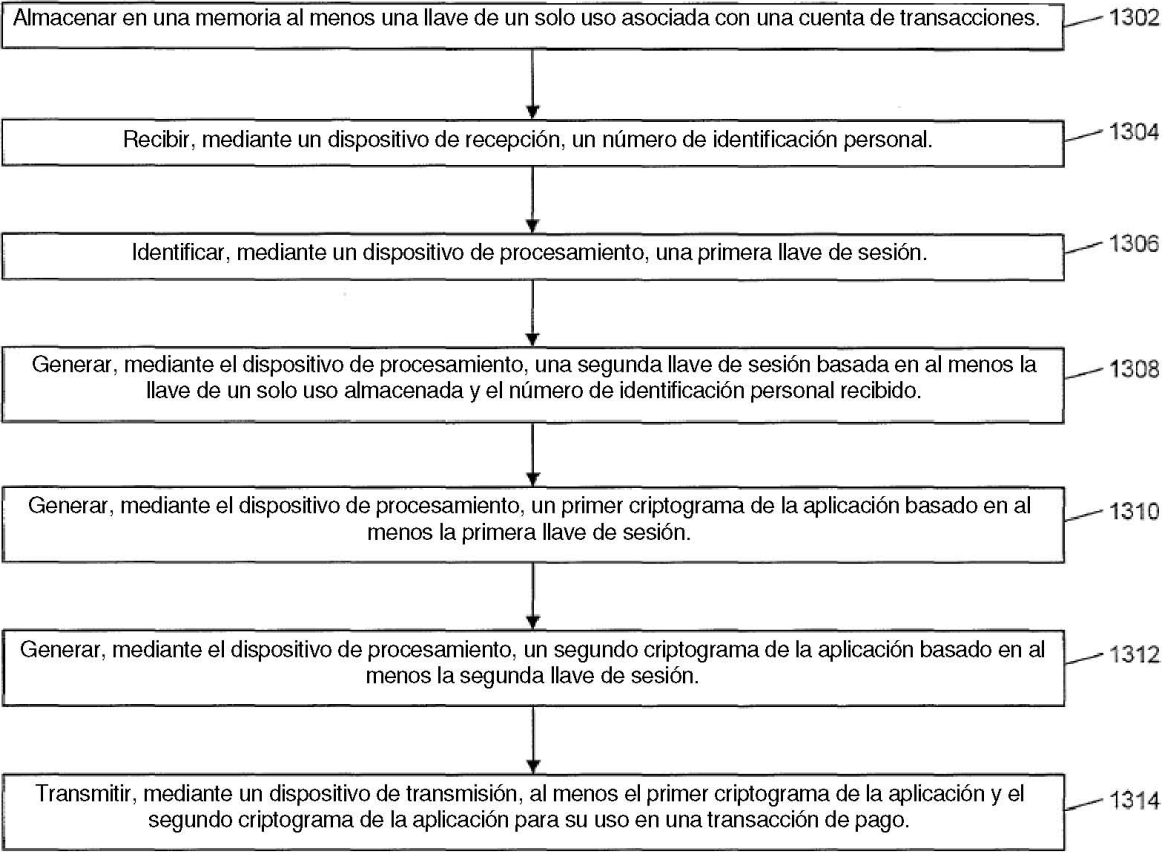


Figura 13

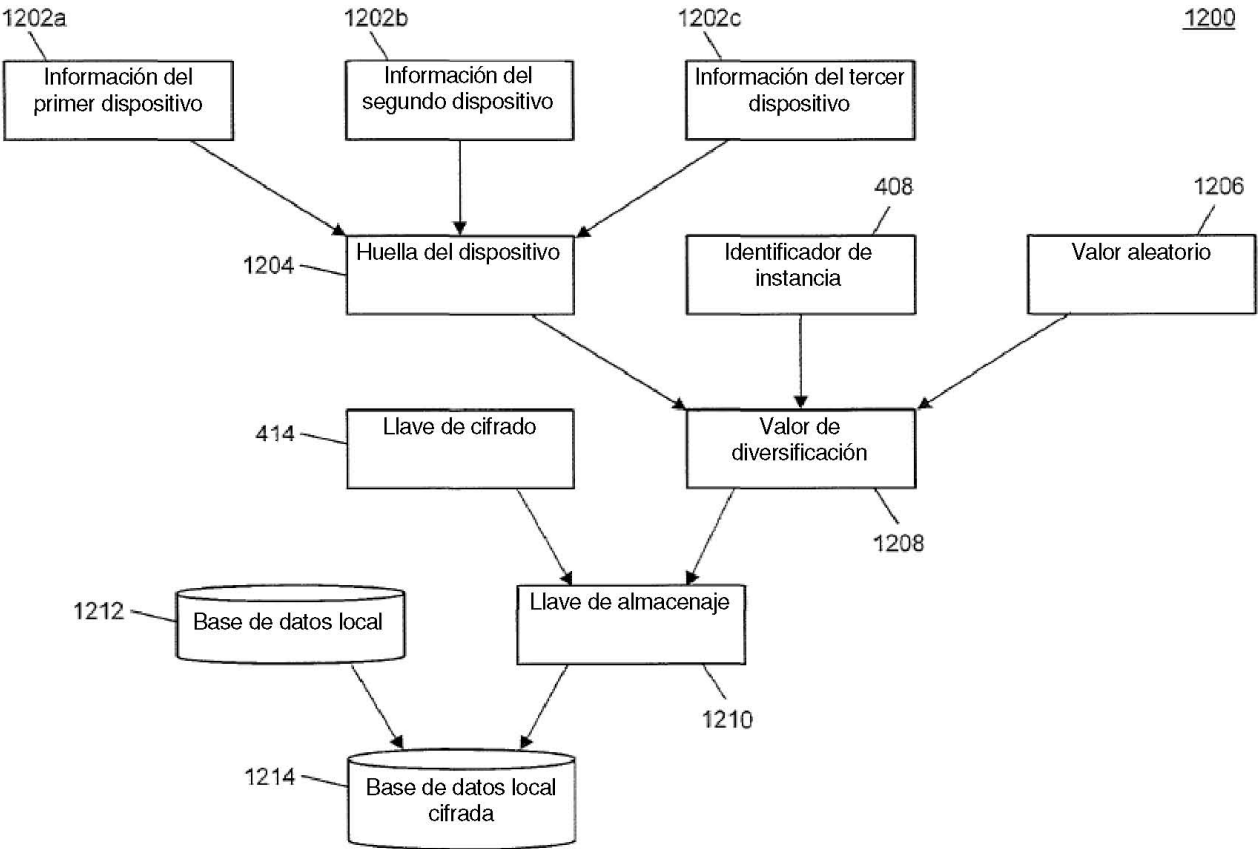


Figura 12

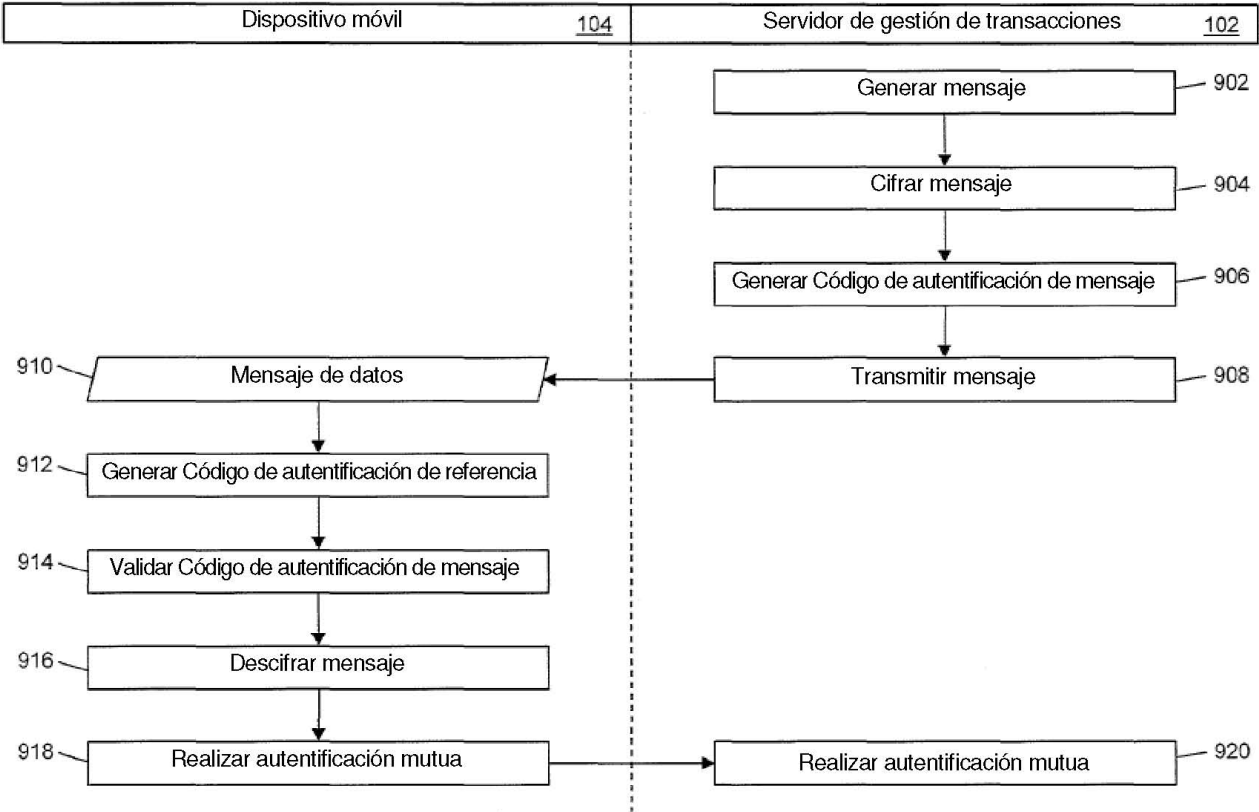


Figura 9

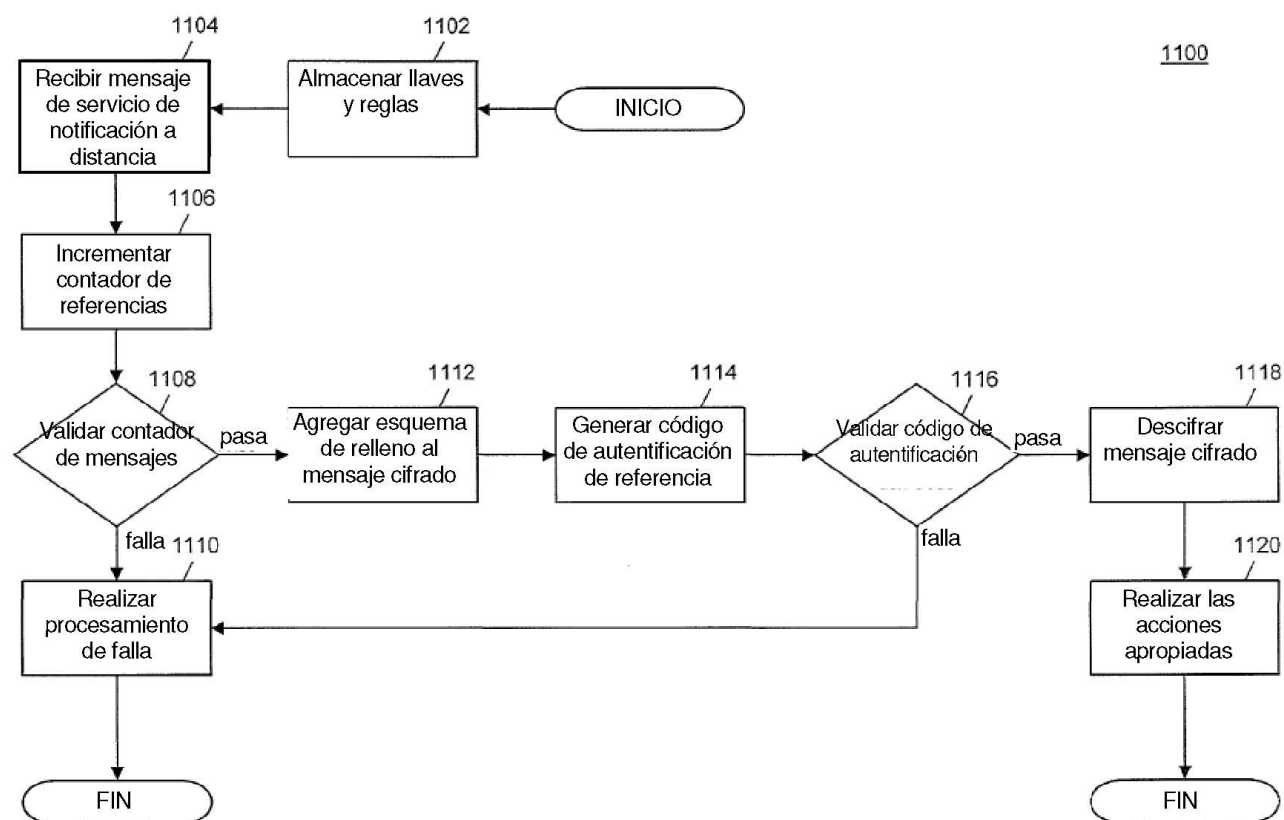


Figura 11

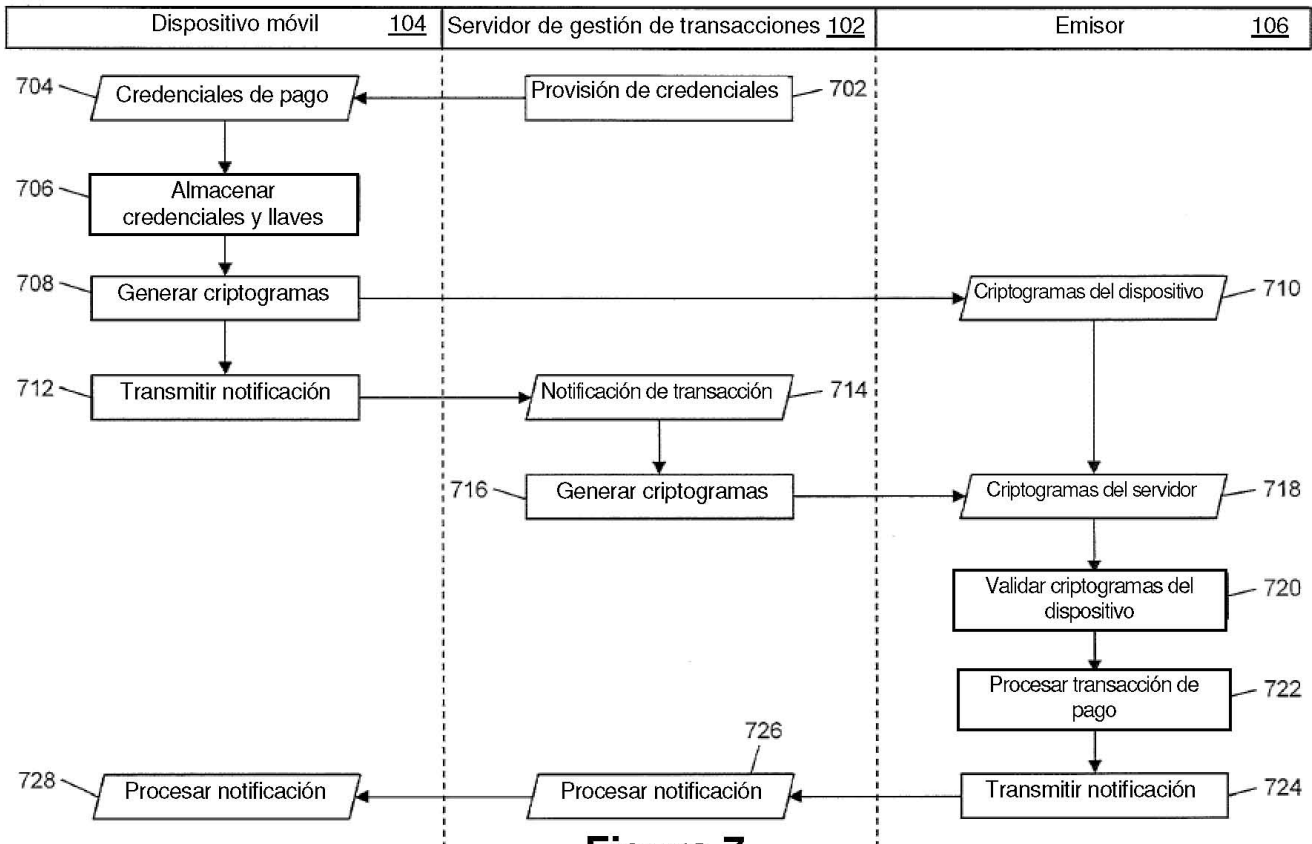


Figura 7

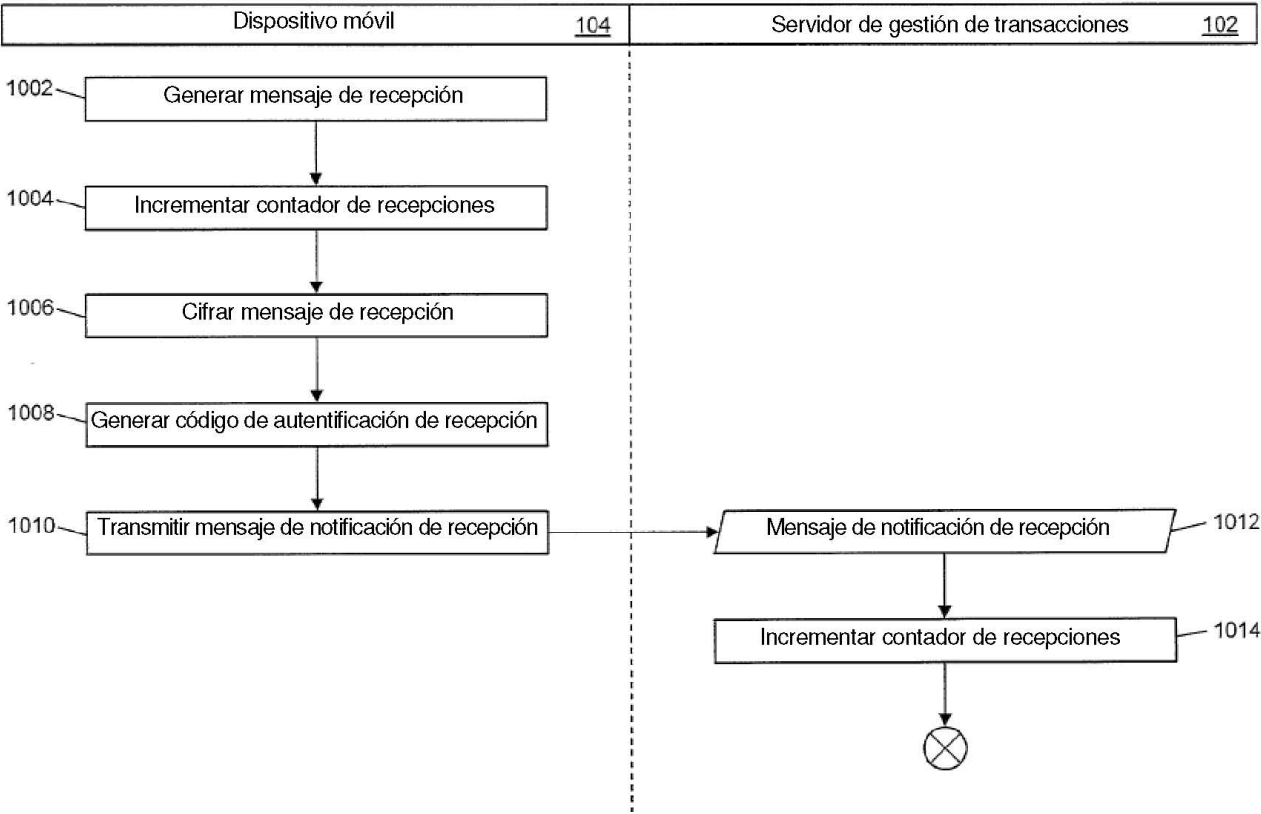


Figura 10A

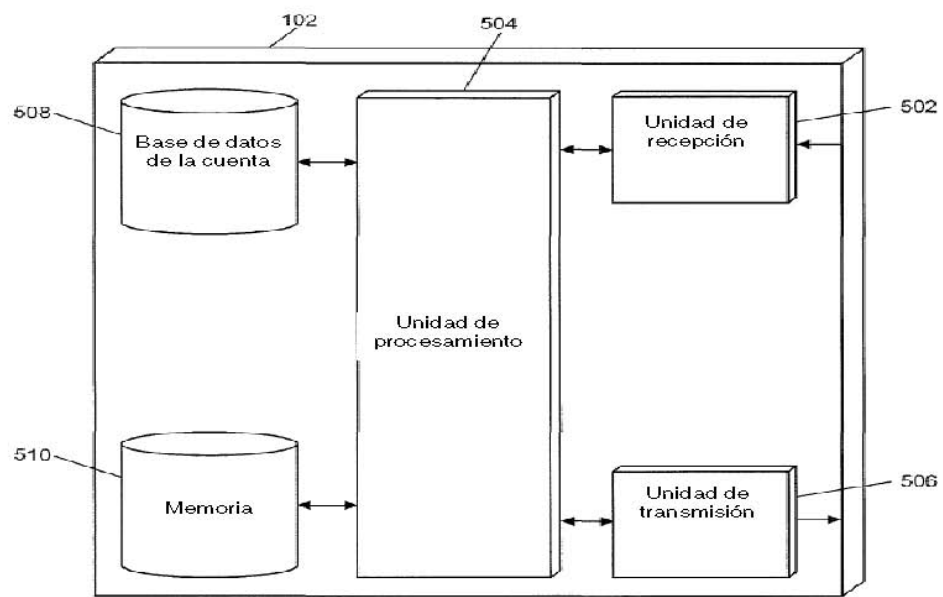


Figura 5

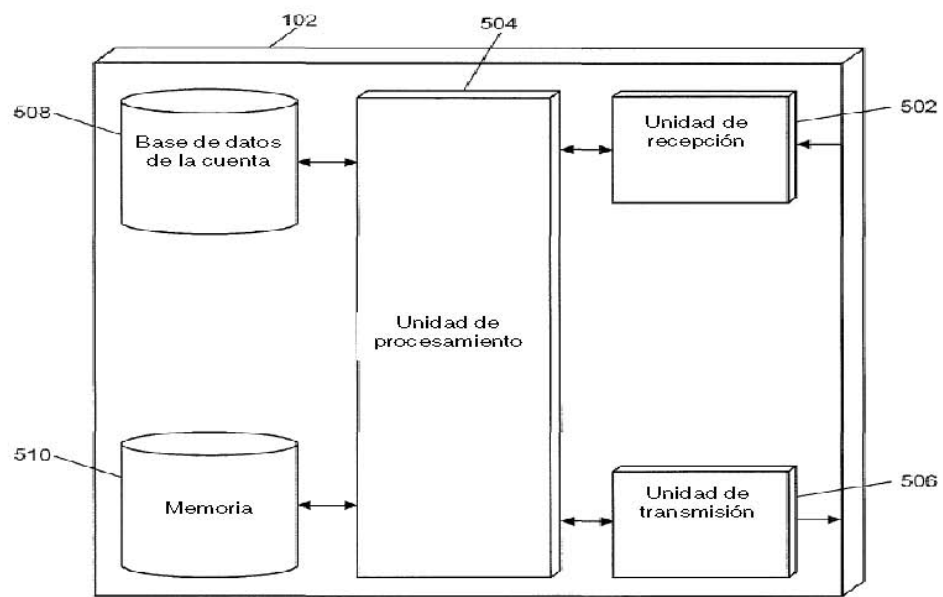


Figura 5

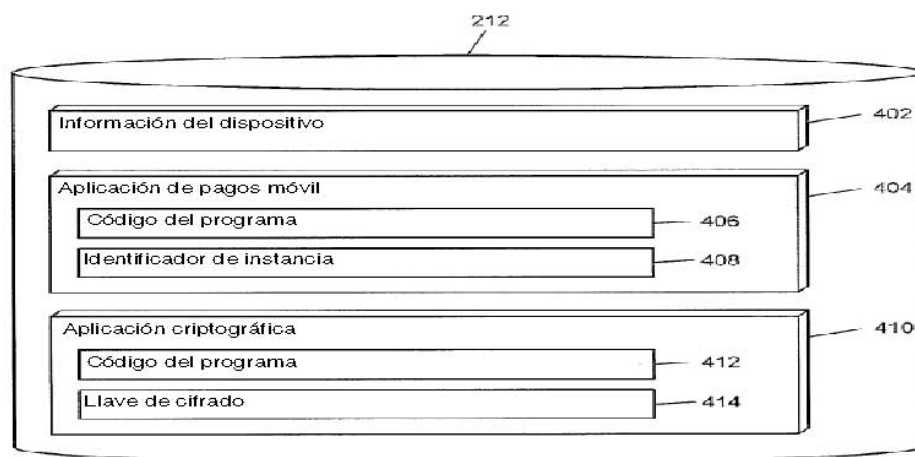


Figura 4

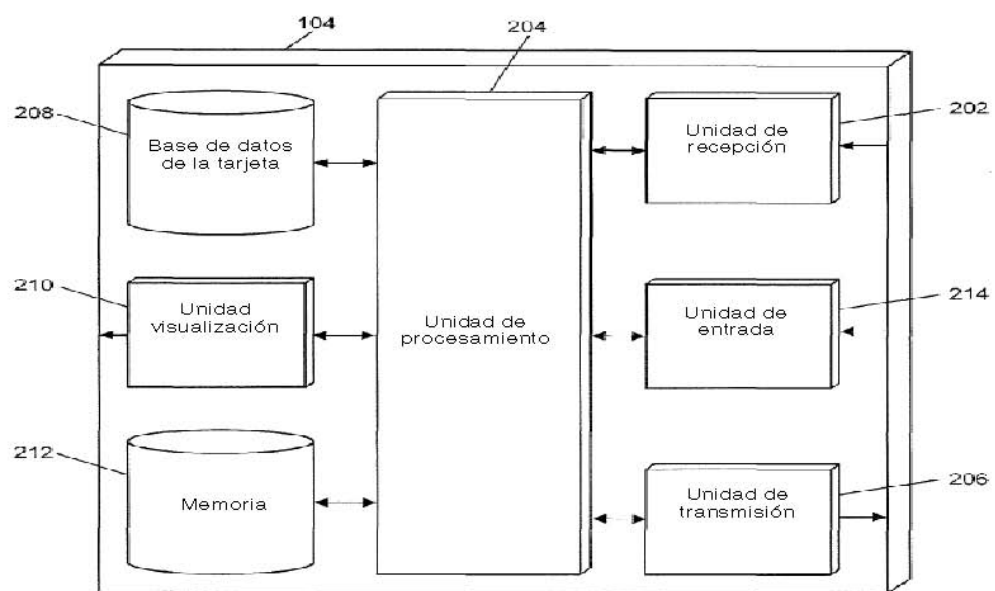


Figura 2

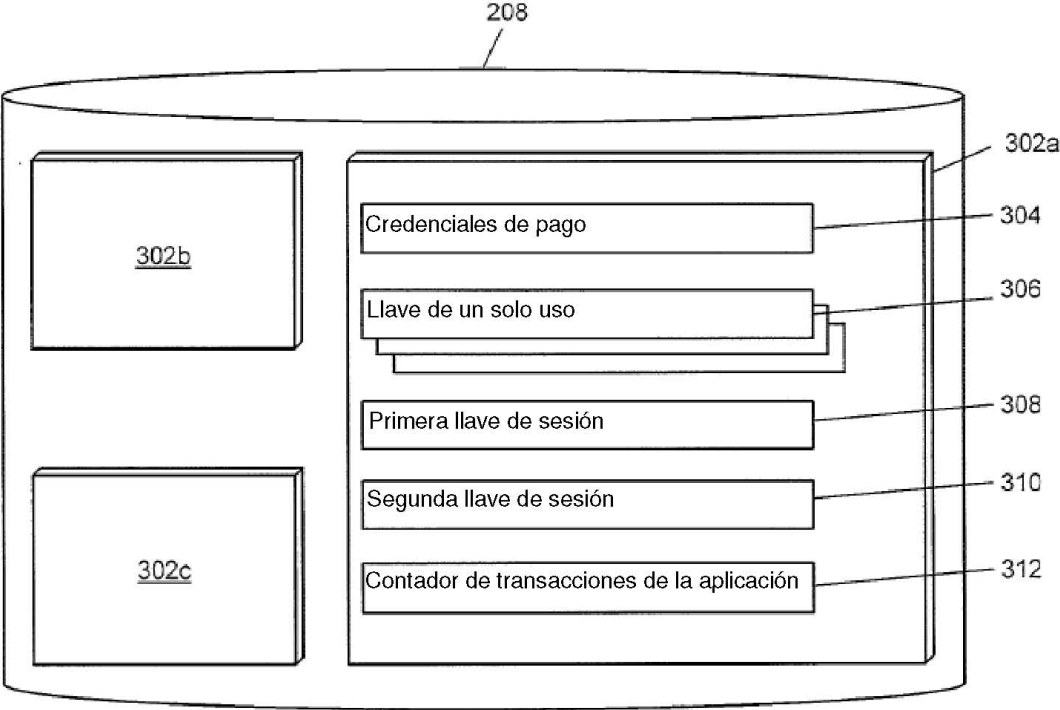


Figura 3

**MÉTODO Y SISTEMA PARA LA TRANSMISIÓN SEGURA DE
MENSAJES DEL SERVICIO DE NOTIFICACIÓN A DISTANCIA A
DISPOSITIVOS MÓVILES SIN ELEMENTOS DE SEGURIDAD**

5 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 61/979,113 presentada el 14 de abril de 2014; 61/910,819
10 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; y, en particular, de las solicitudes provisionales de patente números 61/979,122 presentada el 14 de
15 abril de 2014 y 61/996,665 presentada el 14 de mayo de 2014, cada una incorporada a la presente como referencia en su totalidad.

CAMPO DE LA INVENCION

La presente descripción se refiere a la transmisión de
20 mensajes del servicio de notificación a distancia a un dispositivo móvil sin requerir de un elemento de seguridad, y más específicamente, al uso de códigos de cifrado y autenticación para la transmisión, recepción y procesamiento seguros de mensajes del servicio de notificación a distancia sin el uso de elementos de
25 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 móvil, 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
5 inician y conduzcan las transacciones de pago sin el uso de 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
10 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,
15 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
20 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
25 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 para todas 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 divulgación proporciona una descripción de los sistemas y métodos para el procesamiento de mensajes de servicio de notificación a distancia.

Un método para recibir y procesar un mensaje de datos incluye: almacenar, en una memoria, por lo menos una llave de cifrado; recibir, mediante un dispositivo de recepción, un mensaje de datos, en donde el mensaje de datos incluye por lo menos un mensaje cifrado y un código de autenticación del mensaje, donde el código de autenticación del mensaje se genera usando por lo menos una parte del mensaje cifrado; generar, mediante un dispositivo de procesamiento, un código de autenticación de referencia utilizando por lo menos una parte del mensaje cifrado incluido en el mensaje de datos recibido; validar, mediante el

dispositivo de procesamiento, el mensaje de datos recibido basándose en una comprobación del código de autenticación del mensaje incluido en el mensaje de datos recibido contra el código de autenticación de referencia generado; y descifrar, mediante el
5 dispositivo de procesamiento, el mensaje cifrado incluido en el mensaje de datos utilizando la llave de cifrado almacenada para obtener un mensaje descifrado.

Un sistema para recibir y procesar un mensaje de datos incluye una memoria, un dispositivo de recepción, y un dispositivo de
10 procesamiento. La memoria está configurada para almacenar por lo menos una llave de cifrado. El dispositivo de recepción está configurado para recibir un mensaje de datos, en donde el mensaje de datos incluye por lo menos un mensaje cifrado y un código de autenticación del mensaje, donde el código de autenticación del
15 mensaje se genera usando por lo menos una parte del mensaje cifrado. El dispositivo de procesamiento está configurado para: generar un código de autenticación de referencia utilizando por lo menos una parte del mensaje cifrado incluido en el mensaje de datos recibido; validar el mensaje de datos recibido basándose en una
20 comprobación del código de autenticación del mensaje incluido en el mensaje de datos recibido contra el código de autenticación de referencia generado; y descifrar el mensaje cifrado incluido en el mensaje de datos recibido utilizando la llave de cifrado almacenada para obtener un mensaje descifrado.

BREVE DESCRIPCIÓN DE LAS FIGURAS

El alcance de la presente descripción se entiende mejor a partir de la siguiente descripción detallada de las modalidades de 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
5 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
10 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
15 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
20 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
25 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 INVENCION

Glosario de términos

Red de pago - Un sistema o red que se utiliza para la
5 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
10 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
15 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,
20 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
25 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 intercambio de 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 adquirente. 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 adquirente, 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 adquirente. La liberación puede incluir el envío de las transacciones por lotes desde el adquirente 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 adquirente por

medio de la red de pago. En otros casos, el emisor puede pagar al
adquiriente directamente. El financiamiento puede incluir el pago al
comerciante por parte del adquiriente para las transacciones de pago
que han sido liberadas y liquidadas. Será evidente para las personas
5 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
10 (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,
15 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
20 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.

25 Sistema para el procesamiento de transacciones de pago utilizando

un dispositivo móvil sin elementos de seguridad

La figura 1 ilustra un sistema 100 para el procesamiento de las transacciones de pago utilizando un dispositivo móvil sin requerir del uso de elementos de seguridad, el cual puede incluir la provisión
5 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
10 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
15 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
20 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,
25 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 cual puede incluir 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 autenticación, 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 personas que tengan experiencia en la técnica relevante, de tal manera que el dispositivo móvil 104 y el servidor de gestión de transacciones 102 puedan
5 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
10 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,
15 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
20 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
25 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 del pago, las llaves de un solo uso, las llaves de sesión, los criptogramas de aplicaciones, las llaves maestras de tarjetas, etc.

5 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
10 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
15 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
20 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
25 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 autenticación. El uso tanto de los contadores como de los códigos de autenticación puede asegurar que solamente el dispositivo móvil 104 destinado sea capaz de
5 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 autenticación están incluidos en la aplicación de pagos móvil (MPA), entonces solamente un dispositivo móvil 104, que también incluya una
10 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
15 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
20 104 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
25 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 autentiquen 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 autenticación del consumidor, puede hacer posible que un criptograma autentique tanto al consumidor 108 como al dispositivo móvil 104. En tal caso, los criptogramas generados por el

dispositivo móvil 104 pueden incluir uno que autentique al dispositivo móvil 104, y un segundo que autentique tanto al 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
5 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
10 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
15 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.
20 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
25 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
5 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
10 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
15 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
20 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,
25 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 criptogramas de 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 autenticar 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 puede ser aprobada, tal como basándose una decisión del emisor 106. Por ejemplo, el emisor 106 puede aprobar una transacción en donde falla la autenticación del consumidor, pero pasa la autenticación 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 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 varios aspectos de 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 a distancia (RNS), 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 configurar para llevar a cabo las funciones del dispositivo móvil 104 discutidas en la presente. La unidad de procesamiento 204 puede ejecutar el código
5 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
10 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
15 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.

20 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
25 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.

5 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
10 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
15 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,
20 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
25 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 programas de aplicaciones ejecutados por la unidad de procesamiento 204, tal como un sistema operativo, un código del programa para recibir
5 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
10 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.

15 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
20 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
25 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
5 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
10 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
15 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
20 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
25 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, o puede estar 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 autenticación 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 segunda llave de 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 autenticar 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 autenticar 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 por lo mismo 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 sistemas que serán evidentes para las personas que tengan experiencia en la técnica relevante.

5 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
10 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
15 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
20 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
25 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 almacenamiento 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 otra 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.

10 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 de confirmación, notificaciones de transacciones, etc., de la red de pago 114, del emisor 106, o de otra entidad adecuada. La unidad de recepción 502
5 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
10 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
15 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,
20 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
25 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 protocolos de red. La 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 el servidor de gestión de transacciones 102 en el desempeño de las funciones descritas en la presente. Por ejemplo, la memoria 510 puede
5 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
10 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
15 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.

20 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
25 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 tarjeta 614.

Cada perfil de cuenta 602 puede corresponder a un perfil de pago 302 proporcionado a un dispositivo móvil 104. Como tal, las
5 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
10 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.

15 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
20 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
25 (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 para generar una 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, de tal manera que 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 5 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 10 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 15 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 20 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 25 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 adecuados, tales como una o más de las llaves de sesión 308 y 310.

En el paso 708, la unidad de procesamiento 204 puede generar
5 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
10 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
15 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
20 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
25 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 pago 304
y los criptogramas de aplicaciones pueden ser recibidos por el
emisor 106 en el paso 710. En el paso 712, la unidad de transmisión
5 206 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
10 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
15 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
20 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
25 transacciones de la aplicación 610, o en cualquier otro tipo de datos

adecuado.

En el paso 718, la unidad de transmisión 506 del servidor de gestión de transacciones 102 puede transmitir los criptogramas de aplicaciones generados al emisor 106, el cual puede recibir los
5 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
10 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
15 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
20 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
25 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 indicación de la 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 criptogramas 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 procesamiento de transacciones de pago, como se discutió anteriormente, y otra información que se pueda usar en el establecimiento de una
5 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 autenticación mutua con el
10 dispositivo móvil 104, el mensaje puede incluir información adecuada para establecer la autenticación mutua, tal como un identificador de sesión. En otros casos, tales como cuando la autenticación 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
15 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,
20 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
25 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 puede ser cifrado 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 autenticación del mensaje. El código de autenticación 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 autenticación del mensaje se puede generar usando uno o más métodos de cifrado y ofuscación, como relleno. En algunas modalidades, el código de autenticación 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 autenticación 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 autenticación 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 la autenticación mutua, el mensaje de datos combinados también puede incluir un contador de mensajes.

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

20 En el paso 914, la unidad de procesamiento 204 puede validar el código de autenticación del mensaje incluido en el mensaje de datos combinados recibido al compararlo contra el código de autenticación de referencia generado. Si tanto el contador de mensajes y el código de autenticación del mensaje se validan,
25 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 casos en que el mensaje de datos combinados puede incluir un identificador de mensaje, la unidad de procesamiento 204 también puede validar el
5 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
10 204 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
15 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
20 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
25 realizar la autenticación 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 de procesamiento 204. En el paso 920, el servidor 102 de gestión de transacciones puede recibir al identificador de sesión y realizar cualquier acción
5 adicional necesaria para la autenticación mutua con el dispositivo móvil 104. En los casos en que la autenticación 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
10 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
15 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
20 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 autenticación mutua, el mensaje de regreso puede incluir al identificador de sesión utilizado para realizar la autenticación
25 mutua.

Las figuras 10A y 10B ilustran un proceso para la generación y transmisión de un mensaje de respuesta mediante el dispositivo móvil 104 y la validación de los mismos por el servidor de gestión de transacciones 102.

5 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
10 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
15 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
20 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
25 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 almacenar en la 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 autenticación de recepción basado en el mensaje de confirmación de cifrado. En algunas modalidades, el código de autenticación de la recepción se puede generar utilizando las mismas reglas, algoritmos, y/o procesos, que se usan para generar el código de autenticación 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 autenticación 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 un contador de confirmación. El contador de confirmación puede ser indicativo del número de mensajes recibidos desde el dispositivo móvil 104, que se
5 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
10 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
15 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.

20 En el paso 1016, la unidad de procesamiento 504 puede generar un código de autenticación de confirmación. El código de autenticación 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
25 reglas, algoritmos, y/o procesos utilizados para generar el código de

autenticación del mensaje. En el paso 1018, la unidad de procesamiento 504 puede validar el contador de recepción incluido 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 autenticación de recepción comparándolo con el código de autenticación 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 autenticación 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 autenticación, 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 autenticación 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 autenticación 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
5 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
10 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
15 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
20 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,
25 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 replicada por una entidad no autorizada con el fin de transmitir o recibir un mensaje de datos con éxito sin autorización. Será evidente para las personas
5 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.

10 En el paso 1114, la unidad de procesamiento 204 puede generar un código de autenticación de referencia. El código de autenticación 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
15 1102. En algunas modalidades, el código de autenticación 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 autenticación del mensaje de recepción en el mensaje del servicio
20 de notificación a distancia (RNS). La validación del código de autenticación del mensaje puede incluir la comparación del código con el código de autenticación 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
25 de gestión 102).

Si la validación del código de autenticación del mensaje falla, el proceso de 1100 puede proceder al paso 1110 en donde se realiza el procesamiento de falla. Si la validación del código de autenticación 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 o más 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 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 un 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 puede ser un valor resultante del cifrado del valor de diversificación 1208 utilizando el cifrado de llave 414. En algunas modalidades, la llave
5 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
10 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
15 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
20 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
25 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, llaves de un solo 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.

Primer método de ejemplo para generar credenciales de pago en una

transacción de pago

La figura 13 ilustra un método 1300 para la generación de 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 aplicación mediante el dispositivo de procesamiento 204 basándose en por lo menos la segunda llave de sesión 310.

5 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
10 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
15 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
20 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
25 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
5 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

10 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.

15 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
20 606) 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.

25 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 el paso 1410, se puede generar un segundo criptograma de la aplicación mediante el dispositivo de procesamiento 504 con base en por lo menos la
5 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.

10 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
15 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.

20 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,
25 (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 correspondiente recibido con 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 modalid 5 ad 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 modalid 10 ad 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. 15

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 20 25

puede incluir por lo menos un mensaje cifrado y un código de autenticación del mensaje, en donde el código de autenticación 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 autenticación 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 autenticación, y el código de autenticación de referencia se puede generar con base en la aplicación de las una o más reglas de generación de código de autenticación 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 autenticación del mensaje incluido en el mensaje de datos recibido contra el código de autenticación 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 autenticación de retorno utilizando por lo menos una parte del mensaje de respuesta cifrado, en donde la notificación de recepción de transmisión incluye el mensaje de regreso cifrado, y el código de autenticación de retorno.

5 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
10 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 autenticación 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,
15 la memoria 212 puede incluir además un algoritmo de código de autenticación 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 autenticación.

20 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
25 usar un elemento de seguridad.

En el paso 1602, por lo menos la información del dispositivo (por ejemplo, la información del dispositivo 402) asociada con un 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 programa de aplicación 410 puede ser una función ejecutable del programa de aplicación primero 404.

5 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
10 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
15 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
20 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
25 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 412 asociado con el segundo programa de la aplicación 410 para obtener una llave de almacenamiento (por ejemplo, llave de almacenamiento avanzada 5 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 10 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 15 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; 20 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 25 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 el uno o más parámetros cifrados se pueden recibir desde la tercera parte 102. En algunas modalidades adicionales, el identificador de instancia 408
5 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
10 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
15 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
20 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
25 materia descrita se pueden practicar con diversas configuraciones de

sistema de computación, incluyendo sistemas de múltiples núcleos multiprocesador, minicomputadoras, computadoras centrales, computadoras vinculados o agrupados con funciones distribuidas, así como penetrante o computadoras en miniatura que pueden ser
5 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
10 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
15 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
20 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
25 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 almacenado de forma 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
5 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
10 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
15 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
20 (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.

25 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 tipo de medios 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 telefónica, un enlace telefónico celular, un enlace de radiofrecuencia, etc.

El sistema de computación 1700 puede incluir, además, una
5 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
10 (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
15 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
20 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
25 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.

5 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.

5

10

15

20

25

REIVINDICACIONES

1. Un método para recibir y procesar un mensaje de datos, el cual comprende:

5 almacenar, en una memoria, por lo menos una llave de cifrado;

recibir, mediante un dispositivo de recepción, un mensaje de datos, en donde el mensaje de datos incluye por lo menos un mensaje cifrado y un código de autenticación del mensaje, en
10 donde el código de autenticación del mensaje se genera usando por lo menos una parte del mensaje cifrado;

generar, mediante un dispositivo de procesamiento, un código de autenticación de referencia, utilizando por lo menos una parte del mensaje cifrado incluido en el mensaje de datos recibido;

15 validar, mediante el dispositivo de procesamiento, el mensaje de datos recibido basándose en una comprobación del código de autenticación del mensaje incluido en el mensaje de datos recibido contra el código de autenticación de referencia generado; y

20 descifrar, mediante el dispositivo de procesamiento, el mensaje cifrado incluido en el mensaje de datos recibido, utilizando la llave de cifrado almacenada, para obtener un mensaje descifrado.

2. El método de acuerdo con la reivindicación 1, en donde el mensaje de datos es un mensaje del servicio de notificación a
25 distancia recibido por medio de un servicio de notificación a

distancia.

3. El método de acuerdo con la reivindicación 1, en donde:

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

5 la validación del mensaje de datos recibido incluye además comprobar el contador de mensajes incluido en el mensaje de datos recibido contra el contador de referencia almacenado.

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

10 transmitir, mediante un dispositivo de transmisión, una notificación de recepción en respuesta al mensaje de datos recibido.

5. El método de acuerdo con la reivindicación 4, en donde:

el método comprende además:

15 realizar, mediante el dispositivo de procesamiento, una o más acciones basándose en el mensaje descifrado;

generar, mediante el dispositivo de procesamiento, un mensaje de regreso como resultado de, o basándose en, las una o más acciones realizadas;

20 cifrar, mediante el dispositivo de procesamiento, el mensaje de regreso generado, utilizando la llave de cifrado almacenada, para obtener un mensaje de regreso cifrado; y

generar, mediante el dispositivo de procesamiento, un código de autenticación de regreso, utilizando por lo menos una parte del mensaje de regreso cifrado, en donde:

25 la notificación de recepción transmitida incluye el

mensaje de regreso cifrado y el código de autenticación de regreso.

6. El método de acuerdo con la reivindicación 5, en donde:
la memoria incluye además un contador de regreso, y
la notificación de recepción transmitida incluye, además,
5 el contador de regreso.

7. El método de acuerdo con la reivindicación 1, en donde:
la memoria incluye, además, una o más reglas de
generación de códigos de autenticación, y
el código de autenticación de referencia se genera
10 basándose en la aplicación de las una o más reglas de generación
de código de autenticación almacenadas, para la parte del mensaje
cifrado incluida en el mensaje de datos recibido.

8. El método de acuerdo con la reivindicación 1, el cual
comprende además:
15 agregar un esquema de relleno, mediante el dispositivo
de procesamiento, al mensaje cifrado incluido en el mensaje del
servicio de notificación a distancia recibido utilizando una llave del
esquema de relleno, en donde:

la parte del mensaje cifrado utilizada para generar el
20 código de autenticación de referencia es el mensaje cifrado con
esquema de relleno.

9. El método de acuerdo con la reivindicación 8, en donde la
llave de relleno es la llave de cifrado.

10. El método de acuerdo con la reivindicación 8, en donde:
25 la memoria incluye además un algoritmo de esquema de

relleno del código de autenticación, y

la adición del esquema de relleno al mensaje cifrado utilizando la llave del esquema de relleno incluye agregar el esquema de relleno al mensaje cifrado basándose en la aplicación de la llave del esquema de relleno al algoritmo del esquema de relleno del código de autenticación.

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

comprobar, mediante el dispositivo de procesamiento, un formato de datos del mensaje descifrado basándose en una o más reglas de formateo de datos.

12. El método de acuerdo con la reivindicación 1, en donde el mensaje descifrado incluye por lo menos uno de: un perfil de tarjeta digitalizada y una llave de un solo uso para utilizarse en una transacción de pago.

13. El método de acuerdo con la reivindicación 1, en donde el código de autenticación de referencia se genera adicionalmente utilizando la llave de cifrado almacenada.

14. 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.

15. Un sistema para recibir y procesar un mensaje de datos, el cual comprende:

una memoria configurada para almacenar por lo menos una llave de cifrado;

un dispositivo de recepción configurado para recibir un mensaje de datos, en donde el mensaje de datos incluye un mensaje cifrado y un código de autenticación del mensaje, en donde el código de autenticación del mensaje se genera utilizando por lo menos una parte del mensaje cifrado; y

un dispositivo de procesamiento configurado para:
generar un código de autenticación de referencia utilizando por lo menos una parte del mensaje cifrado incluido en el mensaje de datos recibido,

validar los datos recibidos basándose en una comprobación del código de autenticación del mensaje incluido en el mensaje de datos recibido contra el código de autenticación de referencia generado, y

descifrar el mensaje cifrado incluido en el mensaje de datos recibido utilizando la llave de cifrado almacenada para obtener un mensaje descifrado.

16. El sistema de acuerdo con la reivindicación 15, en donde el mensaje de datos es un mensaje del servicio de notificación a distancia recibido por medio de un servicio de notificación a distancia.

17. El sistema de acuerdo con la reivindicación 5, en donde:
la memoria está además configurada para almacenar un contador de referencia, y

la validación del mensaje de datos recibido incluye además comprobar el contador de mensajes incluido en el mensaje

de datos recibido contra el contador de referencia almacenado.

18. El sistema de acuerdo con la reivindicación 15, el cual comprende además:

un dispositivo de transmisión configurado para transmitir
5 una notificación de recepción en respuesta al mensaje del servicio de notificación a distancia recibido.

19. El sistema de acuerdo con la reivindicación 18, en donde:
el dispositivo de procesamiento está configurado además para:

10 realizar una o más acciones basándose en el mensaje descifrado,

generar un mensaje de regreso como resultado de,
o basándose en, las una o más acciones realizadas,

cifrar el mensaje de regreso generado utilizando la
15 llave de cifrado almacenada para obtener un mensaje de regreso cifrado, y

generar un código de autenticación de regreso
utilizando por lo menos una parte del mensaje de regreso cifrado, y

la notificación de recepción transmitida incluye el
20 mensaje de regreso cifrado, el contador de regreso, y el código de autenticación de regreso.

20. El sistema de acuerdo con la reivindicación 19, en donde:
la memoria incluye además un contador de regreso, y
la notificación de recepción transmitida incluye, además,
25 el contador de regreso.

21. El sistema de acuerdo con la reivindicación 15, en donde:
la memoria incluye, además, una o más reglas de
generación de códigos de autenticación, y
el código de autenticación de referencia se genera
5 basándose en la aplicación de las una o más reglas de generación
de código de autenticación almacenadas, a la parte del mensaje
cifrado incluida en el mensaje del servicio de notificación a distancia
recibido.
22. El sistema de acuerdo con la reivindicación 15, en donde:
10 el dispositivo de procesamiento está configurado,
además, para agregar un esquema de relleno al mensaje cifrado
incluido en el mensaje del servicio de notificación a distancia
recibido, utilizando una llave de esquema de relleno, y
la parte del mensaje cifrado usada para generar el código
15 de autenticación de referencia es el mensaje cifrado con el
esquema de relleno.
23. El sistema de acuerdo con la reivindicación 22, en donde
la llave del esquema de relleno es la llave de cifrado.
24. El sistema de acuerdo con la reivindicación 22, en donde:
20 la memoria incluye además un algoritmo de esquema de
relleno del código de autenticación, y
la adición del esquema de relleno al mensaje cifrado
utilizando la llave del esquema de relleno incluye agregar el
esquema de relleno al mensaje cifrado, basándose en la aplicación
25 de la llave del esquema de relleno al algoritmo del esquema de

relleno del código de autenticación.

25. El sistema de acuerdo con la reivindicación 15, en donde el dispositivo de procesamiento está configurado, además, para comprobar un formato de datos del mensaje descifrado basándose en una o más reglas de formateo de datos.

26. El sistema de acuerdo con la reivindicación 15, en donde el mensaje descifrado incluye por lo menos uno de: un perfil de tarjeta digitalizada y una llave de un solo uso para utilizarse en una transacción de pago.

27. El sistema de acuerdo con la reivindicación 15, en donde el código de autenticación de referencia se genera adicionalmente utilizando la llave de cifrado almacenada.

28. El sistema de acuerdo con la reivindicación 15, en donde la memoria es una memoria de elemento no seguro de un dispositivo de comunicación móvil.

20

25

TRATADO DE COOPERACION DE PATENTES

De la AUTORIDAD DE BUSQUEDA INTERNACIONAL

A: WIELAND III, CHARLES F. BUCHANAN INGERSOLL & ROONEY PC P.O. BOX 1404 ALEXANDRIA VA 22313-1404 USA	PCT NOTIFICACION DE TRANSMISION DEL INFORME DE BUSQUEDA INTERNACIONAL Y LA OPINION ESCRITA DE LA AUTORIDAD DE BUSQUEDA INTERNACIONAL O LA DECLARACION (PCT Regla 44.1) Fecha de envío (día/mes/año) 24 de febrero de 2015 (24.02.2015)
Referencia de archivo del solicitante o agente 0076412-0400	PARA ACCION ADICIONAL Ver párrafos 1 y 4 a continuación
Solicitud internacional No. PCT/US2014/068078	Fecha de presentación internacional (día/mes/año) 02 de diciembre de 2014 (02.12.2014)
Solicitante MASTERCARD INTERNATIONAL INCORPORATED	
1. ☒ El solicitante es notificado aquí que el informe de búsqueda internacional y la opinión escrita de la Autoridad de Búsqueda Internacional han sido establecidos y son transmitidos con la presente. Presentación de enmiendas y declaración bajo el artículo 19: El solicitante tiene derecho, si así lo desea, a enmendar las reivindicaciones de la solicitud internacional (ver Regla 46): ¿Cuándo? El tiempo límite para presentar tales enmiendas es normalmente dos meses a partir de la fecha de transmisión del informe de búsqueda internacional. ¿Cómo? Directamente a la Oficina Internacional de WIPO de preferencia a través de ePCT o en papel a 34 chemin des Colombettes 1211 Geneva 20, Suiza, Facsímil No.: +41 22 338 82 70 Para instrucciones más detalladas, ver <i>PCT Applicant's Guide</i>, Fase internacional, párrafos 9.004, 9-011. 2. ☐ El solicitante es notificado aquí que no se establecerá informe de búsqueda internacional y que la declaración bajo el artículo 17(2)(a) para ese efecto y la opinión escrita de la Autoridad de Búsqueda Internacional se transmiten con la presente. 3. ☐ Con respecto a cualquier protesta contra pago de derechos adicionales bajo la Regla 40.2, el solicitante es notificado que: ☐ la protesta junto con la decisión sobre la misma ha sido transmitida a la Oficina Internacional junto con cualquier petición para adelantar los textos tanto de la protesta como la decisión sobre la misma para las Oficinas designadas. ☐ no se ha tomado decisión alguna sobre la protesta; el solicitante será notificado tan pronto se tome una decisión. 4. Recordatorios El solicitante puede presentar comentarios sobre una base informal sobre la opinión escrita de la Autoridad de Búsqueda Internacional a la Oficina Internacional. La Oficina Internacional enviará una copia de tales comentarios a las Oficinas designadas a menos que se haya establecido o vaya a establecerse un informe de examen preliminar internacional. Después de la expiración de 30 meses a partir de la fecha de prioridad, estos comentarios también se harán disponibles al público. Poco después de la expiración de los 18 meses a partir de la fecha de prioridad, la solicitud internacional será publicada por la Oficina Internacional. Si el solicitante desea evitar o posponer la publicación, una notificación de abandono de la solicitud internacional o de la reclamación de prioridad, debe llegar a la Oficina Internacional antes de la terminación de las preparaciones técnicas para la publicación internacional (Reglas 90bis.1 y 90bis.3). Dentro de 19 meses a partir de la fecha de prioridad, ero solo con respecto a algunas Oficinas designadas, una demanda para el examen preliminar internacional debe ser presentado si el solicitante desea posponer la entrada a la fase nacional hasta 30 meses a partir de la fecha de prioridad (en algunas Oficinas incluso después); de otra manera, el solicitante debe, dentro de 20 meses a partir de la fecha de prioridad, realizar los actos prescritos para la entrada a la fase nacional ante esas Oficinas designadas. Con respecto a otras Oficinas designadas, el tiempo límite de 30 meses (o posterior) aplicará incluso no son se presenta demanda dentro de 19 meses. Para detalles sobre los tiempos límites aplicables, Oficina por Oficina, ver www.wipo.int/pct/en/texts/tiem_limits.html y la <i>PCT Applicant's Guide</i>, capítulos nacionales. Dentro de 19 meses a partir de la fecha de prioridad, el solicitante puede solicitar que una búsqueda internacional complementaria sea realizada por una Autoridad de Búsqueda Internacional, que ofrezca este servicio (Regla 45bis.1). El procedimiento para solicitar la búsqueda internacional complementaria se describe en la <i>PCT Applicant's Guide</i>, Fase internacional, párrafos 8,006-8,032.	
Nombre y dirección postal de ISA/KR Internacional Application Division Korean Intellectual Property Office 189 Cheongsu-ro, Seo-gu, Duejeon Metropolitan City, 302-701, República de Corea Facsímil No. +82 42 472 3473	Funcionario autorizado COMISIONADO Teléfono núm. 82-42-481-8751

Forma PCT/ISA/220 (Julio 2014)

***Atención**

Copias de los documentos citados en el informe de búsqueda internacional pueden buscarse en el siguiente sitio web en inglés de la Oficina de Propiedad Intelectual de Corea durante seis meses (fecha de expiración: **2015.08.24**) a partir de la fecha de envío del informe de búsqueda internacional.

<http://www.kipo.go.kr/en/>=> PCT Services => PCT Services

ID: número de solicitud internacional de PCT
PW: Q4MB22R7

Consultas relacionadas con el Informe de Búsqueda Internacional de PCT u Opinión Escrita preparadas por KIPO como una Autoridad de Búsqueda Internacional pueden ser respondidas no solo por KIPO sino también a través de IPKC (Centro de Propiedad Intelectual de Corea), ubicado en Vienna, VA, el cual funciona como una oficina de ayuda de PCT para los solicitantes de PCT.

Página principal: <http://www.ipkcenter.com>

Correo electrónico: ipkc@ipkcenter.com

TRATADO DE COOPERACION DE PATENTES

PCT

INFORME DE BUSQUEDA INTERNACIONAL

(Artículo de PCT 18 y Reglas 43 y 44)

Referencia de archivo del solicitante o agente 0076412-0400	PARA ACCION ADICIONAL	Ver forma PCT/ISA/220 así como, donde se aplicable, punto 5 a continuación
Solicitud internacional No. PCT/US2014/068078	Fecha de presentación internacional (día/mes/año) 02 de diciembre de 2014 (02.12.2014)	Fecha de prioridad (primera) (día/mes/año) 02 de diciembre de 2013 (02.12.2013)
Solicitante MASTERCARD INTERNATIONAL INCORPORATED		
Este informe de búsqueda internacional ha sido preparado por esta Autoridad de Búsqueda Internacional y se transmite al solicitante de acuerdo con el Artículo 18. Una copia está siendo transmitida a la Oficina Internacional.		
Este informe de búsqueda internacional consiste de un total de <u>3</u> hojas ___ También está acompañado por una copia de cada documento de la técnica anterior citado en este informe.		
1. Base del informe a. Con respecto al idioma, la búsqueda internacional se realizó basándose en: <u>X</u> la solicitud internacional en el idioma en el cual se presentó ___ una traducción de la solicitud internacional a _____, el cual es el idioma de una traducción provista para los fines de búsqueda internacional (Reglas 12.3(a) y 23.1(b)) b. ___ Este informe de búsqueda internacional ha sido establecido considerando la rectificación de un error obvio autorizado por o notificado por esta Autoridad bajo la Regla 91 (Regla 43.6bis(a)) c. ___ Con respecto a cualquier secuencia de nucleótidos y/o aminoácidos descrita en la solicitud internacional, ver Casilla núm. 1. 2. ___ Ciertas reivindicaciones fueron encontradas inescrutables (Ver Casilla núm. II) 3. ___ Falta la unidad de invención (Ver Casilla núm. III) 4. Con respecto al título, <u>X</u> el texto es aprobado como se presentó por el solicitante. ___ el texto ha sido establecido por esta autoridad para leerse como sigue: 5. Con respecto al resumen, <u>X</u> el texto es aprobado como se presentó por el solicitante. ___ el texto ha sido establecido, de acuerdo con la Regla 38.2, por esta autoridad como aparece en la Casilla núm. IV. El solicitante puede, dentro de un mes a partir de la fecha de envío de este Informe de Búsqueda Internacional, presentar comentarios a esta Autoridad. 6. Con respecto a los dibujos, a. la figura de los dibujos a ser publicada con el resumen son las figuras núm. _____ <u>X</u> como es sugerido por el solicitante. ___ como es seleccionado por esta Autoridad, debido a que el solicitante falló en sugerir una figura. ___ como es seleccionado por esta Autoridad, debido a que esta figura caracteriza mejor la invención. b. ___ ninguna de las figuras se va a publicar con el resumen.		

Forma PCT/ISA/210 (primera hoja) (Enero 2015)

INFORME DE BÚSQUEDA INTERNACIONAL

N° de solicitud internacional
PCT/US2014/068078

A. CLASIFICACIÓN DEL OBJETO DE LA SOLICITUD

H04 12/08 (2009.01) I, H04W 12/06 (2009.01) i

De acuerdo con la Clasificación Internacional de Patentes (CIP) o según la clasificación nacional y la CIP

B. SECTORES COMPRENDIDOS POR LA BÚSQUEDA

Documentación mínima consultada (sistema de clasificación, seguido de los símbolos de la clasificación)

H04W 12/08; H04L 9/08; H04W 28/06; H04L 9/28; H04L 9/32; 1104W 12/06

Otra documentación consultada, además de la documentación mínima, en la medida en que tales documentos formen parte de los sectores comprendidos por la búsqueda

Modelos de utilidad coreanos y solicitudes para modelos de utilidad

Modelos de utilidad japoneses y solicitudes para modelos de utilidad

Bases de datos electrónicas consultadas durante la búsqueda internacional (nombre de la base de datos y, si es posible, términos de búsqueda utilizados)

eKOPASS(KIPO interna) y palabras clave: clave, autenticación, código, encriptado* y desencriptado*

C. DOCUMENTOS CONSIDERADOS RELEVANTES

Categoría *	DOCUMENTOS CITADOS, CON INDICACIÓN, SI PROCEDE, DE LAS PARTES RELEVANTES	Relevante para las reivindicaciones N°
Y	US 2011-0002459 A1 (DAE YOUR KIM) 06 de enero de 2011	1-2, 7, 11-16, 21, 25-28
A	Ver resumen. Figuras 7, 9. Párrafos [0146]-[0149]. [0161]-[0164]	3-6, 8-10, 14-20, 23-24
Y	KR 10-1256114 B1 (KOREA UNIVERSITY RESERCH AND BUSINESS FOUNDATION) 23 de abril de 2013	1-2, 7, 11-16, 21, 25-28
A	Ver figura 3 y párrafos [0065]-[0066]	3-6, 8-10, 17-20, 22-24
A	US 77029 B2 (CHRISTIAN GEHRMANN) 20 de abril de 2010	1-28
A	Ver resumen, figura 7 y reivindicaciones 1-9	
A	WO 2013-095074 A1 (SAMSUNG ELECTRONICS CO., LTD) 27 de junio de 2013	1-28
A	Ver figuras 2-3, 6-9 y la descripción detallada correspondiente	

[] En la continuación del recuadro C se relacionan otros documentos.

[X] Los documentos de familia de patentes se indican en el anexo.

* Categorías especiales de los documentos citados:

"A" documento que define el estado general de la técnica no considerado como particularmente relevante

"E" solicitud de patente o patente anterior pero publicada en la fecha de presentación internacional o en fecha posterior

"L" documento que puede plantear dudas sobre una reivindicación de prioridad o que se cita para determinar la fecha de publicación de otra cita o por una razón especial (como la indicada)

"O" documento que se refiere a una divulgación oral, a una utilización, a una exposición o a cualquier otro medio

"P" documento publicado antes de la fecha de presentación internacional pero con posterioridad a la fecha de prioridad reivindicada

"T" documento ulterior publicado con posterioridad a la fecha de presentación internacional o de prioridad que no pertenece al estado de la técnica pertinente pero que se cita por permitir la comprensión del principio o teoría que constituye la base de la invención

"X" documento particularmente relevante; la invención reivindicada no puede considerarse nueva o que implique una actividad inventiva por referencia al documento aisladamente considerado

"Y" documento particularmente relevante; la invención reivindicada no puede considerarse que implique una actividad inventiva cuando el documento se asocia a otros documentos de la misma naturaleza, cuya combinación resulta evidente para un experto en la materia.

"&" documento que forma parte de la misma familia de patentes

Fecha en que se ha concluido efectivamente la búsqueda internacional

13 de febrero de 2015 (13.02.2015)

Fecha de expedición del informe de búsqueda internacional

24 de febrero de 2015 (24.02.2015)

Nombre y dirección postal de la ISA/KR

International Application Division

Oficina Coreana de Propiedad Intelectual (KIPO)

189, Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701

Republic of Korea

República de Corea

Fax. ++82 42 472 3473

Funcionario autorizado

YOO, Sun Jung

Tel. +82-42-481-5775

INFORME DE BÚSQUEDA INTERNACIONAL

Información relativa a miembros de familia de patentes

No. de solicitud internacional

PCT/US2014/068078

Documento de patente citado en el informe de búsqueda	Fecha de publicación	Miembro(s) de la familia de patentes	Fecha de publicación
US 2011-0002459 A1	06/01/2011	KR 10-2010-0131678 A US 8464070 B2	16/12/2010 11/06/2013
KR 10-1256114 B1	23/04/2013	None	
US 7702910 B2	20/04/2010	AU 2003-268933 A1 AU 2003-276090 A1 CN 1729645 A CN 1729646 A CN 1729646 B DE 60310439 D1 EP 1554834 A1 EP 1554834 B1 EP 1554835 A1 EP 1554835 B1 JP 04-550736B2 JP 04-664206B2 JP 2006-504361A JP 2006-504362A KR 10-1092696 B1 KR 10-1095239 B1 KR 10-1255357 B1 KR 10-2005-0083819A KR 10-2010-0114947A KR 10-2011-0053391 A US 2004-0083368 A1 US 2005-0262418 A1 US 2007-0288753 A1 US 7284127 B2 US 7502930 B2 WO 2004-038998 A1 WO 2004-038999 A1	13/05/2004 13/05/2004 01/02/2006 01/02/2006 29/09/2010 25/01/2007 20/07/2005 13/12/2006 20/07/2005 13/12/2006 22/09/2010 06/04/2011 02/02/2006 02/02/2006 09/12/2011 20/12/2011 17/04/2013 26/08/2005 26/10/2010 20/05/2011 29/04/2004 24/11/2005 13/12/2007 16/10/2007 10/03/2009 06/05/2004 06/05/2004
WO 2013-095074 A1	27/06/2013	CN 104012134 A KR 10-2014-0116144 A US 2014-372758 A1	27/08/2014 01/10/2014 18/12/2014

TRATADO DE COOPERACION DE PATENTES

De la AUTORIDAD DE BUSQUEDA INTERNACIONAL

A: WIELAND III, CHARLES F. BUCHANAN INGERSOLL & ROONEY PC P.O. BOX 1404 ALEXANDRIA VA 22313-1404 USA		PCT OPINION ESCRITA DE LA AUTORIDAD DE BUSQUEDA INTERNACIONAL (PCT Regla 43bis.1)	
		Fecha de envío (día/mes/año) 24 de febrero de 2015 (24.02.2015)	
Referencia de archivo del solicitante o agente 0076412-0400		PARA ACCION ADICIONAL Ver párrafo 2 a continuación	
Solicitud internacional No. PCT/US2014/068078	Fecha de presentación internacional (día/mes/año) 02 de diciembre de 2014 (02.12.2014)	Fecha de prioridad (día/mes/año) 02 de diciembre de 2013 (02.12.2013)	
Clasificación de patente internacional (IPC) o tanto clasificación nacional como IPC <i>H04W 12/08(2009.01)I, H04W 12/06(2009.01)i</i>			
Solicitante MASTERCARD INTERNATIONAL INCORPORATED			
1. Esta opinión contiene indicaciones se refieren a los siguientes artículos: ☒ Casilla núm. I Base de la opinión ☐ Casilla núm. II Prioridad ☐ Casilla núm. III Sin establecimiento de opinión con respecto a novedad, etapa inventiva y aplicabilidad industrial ☐ Casilla núm. IV Falta de unidad de invención ☒ Casilla núm. V Declaración razonada bajo Regla 43bis.1(a)(i) con respecto a novedad, etapa inventiva y aplicabilidad industrial; citas y explicaciones que soportan tal declaración ☐ Casilla núm. VI Ciertos documentos citados ☐ Casilla núm. VII Ciertos defectos en la solicitud internacional ☐ Casilla núm. VIII Ciertas observaciones sobre la solicitud internacional 2. ACCION ADICIONAL Si se hace una demanda para examen preliminar internacional, esta opinión será considerada como una opinión escrita de la Autoridad Examinadora Preliminar Internacional ("IPEA") excepto que no aplica donde el solicitante elige una Autoridad diferente de ésta para ser la IPEA y la IPEA elegida ha notificado a la Oficina Internacional bajo la Regla 66.1bis(b) que las opiniones escritas de esta Autoridad de Búsqueda Internacional no será considerada así. Si esta opinión es considerada, como se proporcionó antes, una opinión escrita de la IPEA, se invita al solicitante a presentar a la IPEA una réplica escrita junto con, donde sea apropiado, con enmiendas, antes de la expiración de 3 meses a partir de la fecha de envío de la Forma PCT/ISA/220 o antes de la expiración de 22 meses a partir de la fecha de prioridad, la que expire al último. Para opiniones adicionales, ver la Forma PCT/ISA/220.			
Nombre y dirección postal de ISA/KR Internacional Application Division Korean Intellectual Property Office 189 Cheongsu-ro, Seo-gu, Daejeon Metropolitan City, 302-701, República de Corea Facsímil No. +82 42 472 3473		Fecha de terminación de esta opinión 13 de febrero de 2015 (13.02.2015)	Funcionario autorizado YOO, Sun Jung Teléfono núm. 82-42-481-5775

Forma PCT/ISA/237 (portada) (Enero 2015)

**OPINION ESCRITA DE LA AUTORIDAD DE
BÚSQUEDA INTERNACIONAL**

Solicitud internacional No.
PCT/US2014/068078

Casilla No. I Base de esta opinión

1. Con respecto al idioma, esta opinión ha sido establecida basándose en:
 ☒ la solicitud internacional en el idioma en el cual se presentó
 ___ una traducción de la solicitud internacional en ___ el cual es el idioma de una traducción provista para los fines de búsqueda internacional (Reglas 12.3(a) y 23.1(b))
2. ___ Esta opinión ha sido establecida considerando la rectificación de un error obvio autorizado por o notificado a esta Autoridad bajo la Regla 91 (Regla 43bis1(a))
3. ___ Con respecto a cualquier secuencia de nucleótidos y/o aminoácidos descritos en la solicitud internacional, esta opinión ha sido establecida con base a un listado de secuencias:
 - a. ___ que forma parte de la solicitud internacional como se presenta:
 ___ en la forma de un archivo de texto anexo C/ST.25.
 ___ en papel o en la forma de un archivo de imagen.
 - b. ___ provista junto con la solicitud internacional bajo la Regla de PCT 13ter.1(a) para los fines de búsqueda internacional solamente en la forma de un archivo de texto anexo C/ST.25.
 - c. ___ provista subsecuente a la fecha de presentación internacional para los fines de búsqueda internacional solamente:
 ___ en la forma de un archivo de texto anexo C/ST.25 (Regla 13ter.1(a))
 ___ en papel o en la forma de un archivo de imagen (Regla 13ter.1(b) e Instrucciones administrativas, sección 713).
4. ___ Además, en el caso de que más de una versión o copia de un listado de secuencias se ha presentado o provisto, se proporcionaron las declaraciones requeridas de que la información en las copias subsecuentes o adicionales es idéntica a la que forma parte de la solicitud como se presenta o no va más allá de la solicitud como se presentó, según sea apropiado.
5. Comentarios adicionales:

**OPINION ESCRITA DE LA AUTORIDAD DE
BÚSQUEDA INTERNACIONAL**

Solicitud internacional No.

PCT/US2014/068078

Casilla No. V Declaración razonada bajo la Regla 43bis1(a)(i) con respecto a novedad, etapa inventiva o aplicabilidad industrial; citas y explicaciones que portan dicha declaración

1. Declaración

Novedad (N)	Reivindicaciones <u>1-28</u>	SI
	Reivindicaciones <u>NINGUNA</u>	NO
Paso inventivo (IS)	Reivindicaciones <u>3-6,8-10,17-20,22-24</u>	SI
	Reivindicaciones <u>1-2,7,11-17,21,25-28</u>	NO
Aplicabilidad industrial (IA)	Reivindicaciones <u>1-28</u>	SI
	Reivindicaciones <u>NINGUNA</u>	NO

2. Citas y explicaciones:

Se hace referencia a los siguientes documentos:

D1: US 2011-0002459 A1 (DAE YOUB KIM) 06 de enero de 2011

D2: KR 10-1256114 B1 (KOREA UNIVERSITY RESEARCH AND BUSINESS FOUNDATION) 23 de abril de 2013

D3: US 7702910 B2 (CHRISTIAN GEHRMANN) 20 de abril de 2010

D4: WO 2013-095074 A1 (SAMSUNG ELECTRONICS CO., LTD.) 27 de junio de 2013

1. Novedad y etapa inventiva

1.1 Reivindicación independiente 1

D1, el cual es considerado como la técnica anterior más cercana a la materia en cuestión de la reivindicación 1, describe un método para recibir datos, el método comprende:

- recibir un primer paquete de datos que incluye un mensaje iésimo, un primer criptograma y un segundo criptograma: (ver figura 7 y párrafos [0146]-[0147] en D1)
- almacenar el mensaje iésimo, el primer criptograma y el segundo criptograma; (ver la figura 7 y párrafo [0148] en D1)
- recibir un segundo paquete de datos que incluye una clave de encriptado asignada a un mensaje (i-k)ésimo: (ver figura 7 y párrafo [0149] en D1)
- generar si el código de autenticación de mensaje generado es idéntico al primer criptograma almacenado: (ver figura 9 y párrafo [0161] en D1)
- determinar si el código de autenticación de mensaje generado es idéntico al primer criptograma almacenado: (ver figura 9 y párrafo [0162] en D1)
- autenticar el mensaje (i-k)ésimo como un mensaje (i-k)ésimo válido, cuando el código de autenticación de mensaje generado es idéntico al primer criptograma almacenado: (ver figura 9 y párrafos [0163]-[0164] en D1)

Continúa en la siguiente página

**OPINION ESCRITA DE LA AUTORIDAD DE
BÚSQUEDA INTERNACIONAL**

Solicitud internacional núm.

PCT/US2014/068078

Casilla complementaria

En el caso de que el espacio en cualquiera de las casillas precedentes no sea suficiente.

Continuación de: Casilla núm. V

La materia en cuestión de la reivindicación 1 difiere de la de D1 porque genera un código de autenticación de referencia y valida el mensaje de datos recibido con base en una verificación del código de autenticación de mensaje incluido en el mensaje de datos recibido contra el código de autenticación de referencia generado. Sin embargo, entra dentro del alcance de la práctica acostumbrada seguida por una persona experta en la técnica y puede predecirse fácilmente a partir de “determinar si el código de autenticación de mensaje generado es idéntico al primer criptograma almacenado (ver figura 9 y párrafo [00162] en D1), “generar un código de autenticación de mensaje de referencia (ver figura 3 y párrafo [0065] en D2)” y “verificar el código de autenticación de mensaje de referencia al comparar con el código de autenticación de mensaje de referencia (ver figura 3 y párrafo [0066] en D2)”. En consecuencia, la reivindicación 1 habría sido obvia sobre D1 en vista de D2. Por lo tanto, la materia en cuestión de la reivindicación 1 cumple los requerimientos del artículo de PCT 33(2) con respecto a novedad pero carece de una etapa inventiva bajo el artículo de PCT (33(3).

1.2 Reivindicación dependiente 2

Las características adicionales de la reivindicación 2 pueden ser derivadas fácilmente a partir de “transmitir y recibir datos “ver resumen en D1)” de documento D1. Por lo tanto, la materia en cuestión de la reivindicación 2 cumple los requerimientos del artículo de PC 33(2) con respecto a novedad pero carece de una etapa inventiva bajo el artículo de PCT 33(3).

1.3 Reivindicaciones dependientes 3-6 y 8-10

Las características contenidas en las reivindicaciones dependientes 3-6 y 8-10 no son conocidas ni obvias a partir de la técnica anterior disponible. Por lo tanto, la materia en cuestión de las reivindicaciones 3-6 y 8-10 cumple los requerimientos del artículo de PCT 33(2) y 33(3) con respecto a novedad y etapa inventiva.

1.4 Reivindicaciones dependientes 7 y 13

Las características adicionales de las reivindicaciones 7 y 13 pueden ser derivadas fácilmente a partir de “generar un código de autenticación de mensaje de referencia (ver figura 3 y párrafo [0065] en D2)” del documento D2. Por lo tanto, la materia en cuestión de las reivindicaciones 7 y 13 cumple los requerimientos del artículo de PCT 33(2) con respecto a novedad pero carece de una etapa inventiva bajo el artículo de PCT 33(3).

Continúa en la siguiente página

**OPINION ESCRITA DE LA AUTORIDAD DE
BÚSQUEDA INTERNACIONAL**

Solicitud internacional núm.

PCT/US2014/068078

Casilla complementaria

En el caso de que el espacio en cualquiera de las casillas precedentes no sea suficiente.

Continuación de: Página previa

1.5 Reivindicaciones dependientes 8, 11-12 y 14

Las características adicionales de las reivindicaciones 8, 11-12 y 14 no son descritas explícitamente en D1 y D2, pero entran dentro del alcance de la práctica acostumbrada seguido por una persona experta en la técnica. Por lo tanto, la materia en cuestión de las reivindicaciones 8, 11-12 y 14 es novedosa bajo el artículo de PCT 33(2) pero carece de una etapa inventiva bajo el artículo de PCT 33(3).

1.6 Reivindicación independiente 15 y reivindicaciones dependientes 16, 21, 25-28

Las características de las reivindicaciones del aparato 15-15, 21, 25-28 corresponden esencialmente a aquéllas de las reivindicaciones de método 1-2, 7, 11-14, respectivamente. Por lo tanto, la materia en cuestión de las reivindicaciones 15-16, 21, 25-28 cumple los requerimientos del artículo de PCT 33(2) y 33(3) por las razones dadas en los puntos 1.1-1.2, 1.4-1.5.

1.7 Reivindicaciones dependientes 17-20 y 22-24

Las características de las reivindicaciones de aparato 17-20 y 22-24 corresponden esencialmente a aquéllas de reivindicaciones de método 3-6 y 22-24, respectivamente. Por lo tanto, la materia en cuestión de las reivindicaciones 17-20 y 22-24 cumple los requerimientos del artículo de PCT 33(2) y 33(3) por las razones dadas en el punto 1.3

2. Aplicabilidad industrial

La materia en cuestión de las reivindicaciones 1-18 es industrialmente aplicable bajo el artículo de PCT 33(4).

Forma PCT/ISA/237 (Casilla complementaria) (Enero 2015)

(12) SOLICITUD INTERNACIONAL PUBLICADA DE ACUERDO CON EL TRATADO DE COOPERACIÓN EN MATERIA DE PATENTES (TCP)

(19) Organización Mundial de la Propiedad Intelectual
Oficina Internacional

(43) Fecha de Publicación Internacional
11 de junio de 2015 (11.06.2015)

OMPI (10) Número de Publicación Internacional
PCT WO 2015/084797 A1

(51) Clasificación Internacional de Patente:
H04W 12/08 (2009.01) **H04W 12/06** (2009.01)

(21) Número de Solicitud Internacional:
PCT/US2014/068078

(22) Fecha de Presentación Internacional:
2 de diciembre de 2014 (02.12.2014)

(25) Idioma de Presentación: Inglés

(26) Idioma de Publicación: Inglés

(30) Información de Prioridad

61/910,819	2-diciembre-2013 (02.12.2013)	US
61/951,842	12-marzo-2014 (12.03.2014)	US
61/955,716	19-marzo-2014 (19.03.2014)	US
61/979,113	14-abril-2014 (14.04.2014)	US
61/979,132	14-abril-2014 (14.04.2014)	US
61/979,122	14-abril-2014 (14.04.2014)	US
61/980,784	17-abril-2014 (17.04.2014)	US
61/996,665	14-mayo-2014 (14.05.2014)	US

(71) Solicitante: MASTERCARD INTERNATIONAL INCORPORATED [US/US]; 2000 Purchase Street, Purchase, Nueva York 10577 (US).

(72) Inventores: COLLINGE, Mehdi; 8, Rue Cesar Franck, B-1420 Braine-l'Alleud (BE). **WARD, Michael Christopher**; Easterdown, Upton, Taunton Somerset TA4 2JB (GB). **SMETS, Patrik**; Hooidonkstraat 59, B-2560 Nijlen (BE). **CATELAND, Axel Emile Jean Charles**; 15 Puritan Drive, Scarsdale, Nueva York 10583 (US). **RADU, Cristian**; Rue de Tourinnes 2, B-1320 Beauvechain (BE).

(74) Agente(s): WIELAND III, Charles F.; Buchanan Ingersoll & Rooney PC, P.O. Box 1404, Alexandria, Virginia 22313-1404 (US).

(81) Estados (Países) Designados (a menos que se indique de otra manera, para cada tipo de protección nacional disponible): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Estados (Países) Designados (a menos que se indique de otra manera, para cada tipo de protección regional disponible): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasiáticos (AM, AZ, BY, KG, KZ, RU, TJ, TM), Europeos (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Declaraciones de acuerdo con la Regla 4.17:

- con respecto al derecho de la solicitante de solicitar y que le sea otorgada una patente (Regla 4.17(ii))
- con respecto al derecho de la solicitante de reclamar la prioridad de la solicitud anterior (Regla 4.17(iii))

Publicada:

- con reporte de búsqueda internacional (Art. 21(3))

(54) Título : MÉTODO Y SISTEMA PARA LA TRANSMISIÓN SEGURA DE MENSAJES DEL SERVICIO DE NOTIFICACIÓN A DISTANCIA A DISPOSITIVOS MÓVILES SIN ELEMENTOS DE SEGURIDAD

(57) Resumen: Un método para recibir y procesar un mensaje de datos incluye: almacenar por lo menos una llave de cifrado; recibir un mensaje de datos, incluyendo el mensaje de datos un mensaje cifrado y un código de autenticación del mensaje, siendo el código de autenticación del mensaje generado utilizando por lo menos una parte del mensaje cifrado; generar un código de autenticación de referencia utilizando por lo menos una parte del mensaje cifrado incluida en el mensaje de datos recibido; validar el mensaje de datos recibido basándose en una comprobación del código de autenticación del mensaje incluido en el mensaje de datos recibido, contra el código de autenticación de referencia generado; y descifrar el mensaje cifrado incluido en el mensaje de datos recibido utilizando la llave de cifrado almacenada para obtener un mensaje descifrado.

WO 2015/084797 A1

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property

Organization

International Bureau

(43) International Publication Date

11 June 2015 (11.06.2015)



WIPO | PCT



(10) International Publication Number

WO 2015/084797 A1

(51) International Patent Classification:

H04W 12/08 (2009.01) H04W 12/06 (2009.01)

(21) International Application Number:

PCT/US2014/068078

(22) International Filing Date:

2 December 2014 (02.12.2014)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

61/910,819	2 December 2013 (02.12.2013)	US
61/951,842	12 March 2014 (12.03.2014)	US
61/955,716	19 March 2014 (19.03.2014)	US
61/979,113	14 April 2014 (14.04.2014)	US
61/979,132	14 April 2014 (14.04.2014)	US
61/979,122	14 April 2014 (14.04.2014)	US
61/980,784	17 April 2014 (17.04.2014)	US
61/996,665	14 May 2014 (14.05.2014)	US

(81) Designated States (unless otherwise indicated, for every

kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every

kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

(71) Applicant: MASTERCARD INTERNATIONAL INCORPORATED [US/US]; 2000 Purchase Street, Purchase, New York 10577 (US).

(72) Inventors: COLLINGE, Mehdi; 8, Rue Cesar Franck, B-1420 Braine-l'Alleud (BE). WARD, Michael Christopher; Easterdown, Upton, Taunton Somerset TA4 2JB (GB). SMETS, Patrik; Hooionkstraat 59, B-2560 Nijlen (BE). CATELAND, Axel Emile Jean Charles; 15 Puritan Drive, Scarsdale, New York 10583 (US). RADU, Cristian; Rue de Tourinnes 2, B-1320 Beauvechain (BE).

(74) Agent: WIELAND III, Charles F.; Buchanan Ingersoll & Rooney PC, P.O. Box 1404, Alexandria, Virginia 22313-1404 (US).

Declarations under Rule 4.17:

- as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))
- as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))

Published:

- with international search report (Art. 21(3))

(54) Title: METHOD AND SYSTEM FOR SECURE TRANSMISSION OF REMOTE NOTIFICATION SERVICE MESSAGES TO MOBILE DEVICES WITHOUT SECURE ELEMENTS

(57) Abstract: A method for receiving and processing a data message includes: storing at least an encryption key; receiving a data message, the data message including at an encrypted message and a message authentication code, the message authentication code generated using at least a portion of the encrypted message; generating a reference authentication code using at least a portion of the encrypted message included in the received data message; validating the received data message based on a check of the message authentication code included in the received data message against the generated reference authentication code; and decrypting the encrypted message included in the received data message using the stored encryption key to obtain a decrypted message.

WO 2015/084797 A1

**METHOD AND SYSTEM FOR SECURE TRANSMISSION OF REMOTE
NOTIFICATION SERVICE MESSAGES TO MOBILE DEVICES WITHOUT
SECURE ELEMENTS**

RELATED APPLICATIONS

[0001] This application claims the benefit, under 35 U.S.C. 119(e), of prior-filed Provisional Patent Application Nos. 61/979,113 filed April 14, 2014; 61/910,819 filed December 2, 2013; 61/951,842 filed March 12, 2014; 61/955,716 filed March 19, 2014; 61/979,132 filed April 14, 2014; and 61/980,784 filed April 17, 2014; and, in particular, Provisional Patent Application Nos. 61/979,122 filed April 14, 2014 and 61/996,665 filed May 14, 2014, each herein incorporated by reference in their entirety.

FIELD

[0002] The present disclosure relates to the transmission of remote notification service messages to a mobile device without requiring a secure element, and more specifically the use of encryption and authentication codes for the secure transmission, receipt, and processing of remote notification service messages without the use of secure elements.

BACKGROUND

[0003] Advances in mobile and communication technologies have created tremendous opportunities, one of which is providing the user of a mobile computing device with the ability to initiate and pay for payment transactions using their mobile device. One such approach to enable such actions on a mobile device has been the use of near field communication (NFC) technology to securely transmit payment details from the mobile device to a nearby contactless point of sale (POS) terminal. In order to achieve this, mobile phones with secure element hardware, such as a secure element (SE) chip, are used to securely store the payment credentials. A secure element is a special that may be included in some NFC-enabled devices that

is a temper-resistant platform that may securely host applications and their confidential data.

[0004] However, not all mobile devices have secure elements. In addition, some financial institutions may not have access to secure elements on mobile devices, even if the mobile device is equipped with such an element. As a result, many consumers with mobile devices that possess the required hardware for conducting contactless or other types of remote payment transactions may be unable to actually utilize this capability. Because of such difficulties, there is a need for a technical solution to enable mobile computing devices to initiate and conduct payment transactions without the use of secure elements.

[0005] Some methods and systems for conducting payment transactions using mobile devices lacking secure elements, or without the use of secure elements in mobile devices equipped with them, can be found in U.S. Patent Application No. 13/827,042, entitled "Systems and Methods for Processing Mobile Payments by Provisioning Credentials to Mobile Devices Without Secure Elements," by Mehdi Collinge et al., filed on March 14, 2013, which is herein incorporated by reference in its entirety. While such methods and systems can be suitable for conducting payment transactions via a mobile device without using a secure element, many consumers, merchants, and financial institutions may be wary of participating in such transactions due to a desire for even greater security.

[0006] As a result, there is a need for technical solutions to provide even more security for the receipt and storage of payment credentials in a mobile device lacking a secure element, as well as providing increased security for in the transmission of payment credentials to a point of sale from the mobile device during conducting of a financial transaction. Increased security in these processes can result in increased peace of mind for all entities involved, which can result in an increase in the use of mobile devices for contactless or remote payment transactions, which can provide a vast number of benefits to consumers over traditional payment methods.

SUMMARY

[0007] The present disclosure provides a description of systems and methods for processing remote notification service messages.

[0008] A method for receiving and processing a data message includes: storing, in a memory, at least an encryption key; receiving, by a receiving device, a data message, wherein the data message includes at least an encrypted message and a message authentication code, where the message authentication code is generated using at least a portion of the encrypted message; generating, by a processing device, a reference authentication code using at least a portion of the encrypted message included in the received data message; validating, by the processing device, the received data message based on a check of the message authentication code included in the received data message against the generated reference authentication code; and decrypting, by the processing device, the encrypted message included in the data message using the stored encryption key to obtain a decrypted message.

[0009] A system for receiving and processing a data message includes a memory, a receiving device, and a processing device. The memory is configured to store at least an encryption key. The receiving device is configured to receive a data message, wherein the data message includes at least an encrypted message and a message authentication code, where the message authentication code is generated using at least a portion of the encrypted message. The processing device is configured to: generate a reference authentication code using at least a portion of the encrypted message included in the received data message; validate the received data message based on a check of the message authentication code included in the received data message against the generated reference authentication code; and decrypt the encrypted message included in the received data message using the stored encryption key to obtain a decrypted message.

BRIEF DESCRIPTION OF THE DRAWING FIGURES

[0010] The scope of the present disclosure is best understood from the following detailed description of exemplary embodiments when read in conjunction with the accompanying drawings. Included in the drawings are the following figures:

[0011] FIG. 1 is a block diagram illustrating a high level system architecture for processing payment transactions with advanced security in the provisioning and storage of payment credentials in accordance with exemplary embodiments.

[0012] FIG. 2 is a block diagram illustrating the mobile device of FIG. 1 for the processing payment transactions without a secure element and the secure receipt and storage of payment credentials in accordance with exemplary embodiments.

[0013] FIG. 3 is a block diagram illustrating the card database of the mobile device of FIG. 2 for storing payment credentials in accordance with exemplary embodiments.

[0014] FIG. 4 is a block diagram illustrating the memory of the mobile device of FIG. 2 for storing data used in the generation of advanced storage keys and generating of application cryptograms in accordance with exemplary embodiments.

[0015] FIG. 5 is a block diagram illustrating the transaction management server of FIG. 1 for the processing of payment transactions with a mobile device without a secure element in accordance with exemplary embodiments.

[0016] FIG. 6 is a block diagram illustrating the account database of the processing server of FIG. 5 for the storage of payment credentials and account details in accordance with exemplary embodiments.

[0017] FIG. 7 is a flow diagram illustrating a process for the transmitting and validation of dual application cryptograms for the processing of payment transactions involving a mobile device lacking a secure element in accordance with exemplary embodiments.

[0018] FIG. 8 is a flow diagram illustrating an alternative process for the transmitting and validation of dual application cryptograms for the processing of payment transactions involving a mobile device lacking a secure element in accordance with exemplary embodiments

[0019] FIG. 9 is a flow diagram illustrating a process for creating, transmitting, and validating a remote notification service or other data message provisioned to a mobile device lacking a secure element in accordance with exemplary embodiments.

[0020] FIGS. 10A and 10B are a flow diagram illustrating a process for the creation, transmission, and validation of a message returned by a mobile device lacking a secure element in accordance with exemplary embodiments.

[0021] FIG. 11 is a flow diagram illustrating a process for validating a remote notification service message using the mobile device of FIG. 2 in accordance with exemplary embodiments.

[0022] FIG. 12 is a diagram illustrating the generation of an advanced storage key using the mobile device of FIG. 2 in accordance with exemplary embodiments.

[0023] FIGS. 13 and 14 are flow charts illustrating exemplary methods for generated payment credentials in a payment transaction in accordance with exemplary embodiments.

[0024] FIG. 15 is a flow chart illustrating an exemplary method for receiving and processing a remote notification service message in accordance with exemplary embodiments.

[0025] FIG. 16 is a flow chart illustrating an exemplary method for building an advanced storage key in accordance with exemplary embodiments.

[0026] FIG. 17 is a block diagram illustrating a computer system architecture in accordance with exemplary embodiments.

[0027] Further areas of applicability of the present disclosure will become apparent from the detailed description provided hereinafter. It should be understood that the detailed description of exemplary embodiments are intended for illustration purposes only and are, therefore, not intended to necessarily limit the scope of the disclosure.

DETAILED DESCRIPTION

Glossary of Terms

[0028] Payment Network – A system or network used for the transfer of money via the use of cash-substitutes. Payment networks may use a variety of different protocols and procedures in order to process the transfer of money for various types of transactions. Transactions that may be performed via a payment network may include product or service purchases, credit purchases, debit transactions, fund transfers, account withdrawals, etc. Payment networks may be configured to perform transactions via cash-substitutes, which may include payment cards, letters of credit, checks, transaction accounts, etc. Examples of networks or systems configured to perform as payment networks include those operated by MasterCard[®],

VISA[®], Discover[®], American Express[®], PayPal[®], etc. Use of the term “payment network” herein may refer to both the payment network as an entity, and the physical payment network, such as the equipment, hardware, and software comprising the payment network.

[0029] Transaction Account – A financial account that may be used to fund a transaction, such as a checking account, savings account, credit account, virtual payment account, etc. A transaction account may be associated with a consumer, which may be any suitable type of entity associated with a payment account, which may include a person, family, company, corporation, governmental entity, etc. In some instances, a transaction account may be virtual, such as those accounts operated by PayPal[®], etc.

[0030] Payment Card – A card or data associated with a transaction account that may be provided to a merchant in order to fund a financial transaction via the associated transaction account. Payment cards may include credit cards, debit cards, charge cards, stored-value cards, prepaid cards, fleet cards, virtual payment numbers, virtual card numbers, controlled payment numbers, etc. A payment card may be a physical card that may be provided to a merchant, or may be data representing the associated transaction account (e.g., as stored in a communication device, such as a smart phone or computer). For example, in some instances, data including a payment account number may be considered a payment card for the processing of a transaction funded by the associated transaction account. In some instances, a check may be considered a payment card where applicable.

[0031] Payment Transaction – A transaction between two entities in which money or other financial benefit is exchanged from one entity to the other. The payment transaction may be a transfer of funds, for the purchase of goods or services, for the repayment of debt, or for any other exchange of financial benefit as will be apparent to persons having skill in the relevant art. In some instances, payment transaction may refer to transactions funded via a payment card and/or payment account, such as credit card transactions. Such payment transactions may be processed via an issuer, payment network, and acquirer. The process for processing such a payment transaction may include at least one of authorization, batching, clearing, settlement, and funding. Authorization may include the furnishing of payment details by the consumer to a merchant, the submitting of transaction details (e.g., including the

payment details) from the merchant to their acquirer, and the verification of payment details with the issuer of the consumer's payment account used to fund the transaction. Batching may refer to the storing of an authorized transaction in a batch with other authorized transactions for distribution to an acquirer. Clearing may include the sending of batched transactions from the acquirer to a payment network for processing. Settlement may include the debiting of the issuer by the payment network for transactions involving beneficiaries of the issuer. In some instances, the issuer may pay the acquirer via the payment network. In other instances, the issuer may pay the acquirer directly. Funding may include payment to the merchant from the acquirer for the payment transactions that have been cleared and settled. It will be apparent to persons having skill in the relevant art that the order and/or categorization of the steps discussed above performed as part of payment transaction processing.

[0032] Point of Sale - A computing device or computing system configured to receive interaction with a user (e.g., a consumer, employee, etc.) for entering in transaction data, payment data, and/or other suitable types of data for the purchase of and/or payment for goods and/or services. The point of sale may be a physical device (e.g., a cash register, kiosk, desktop computer, smart phone, tablet computer, etc.) in a physical location that a customer visits as part of the transaction, such as in a "brick and mortar" store, or may be virtual in e-commerce environments, such as online retailers receiving communications from customers over a network such as the Internet. In instances where the point of sale may be virtual, the computing device operated by the user to initiate the transaction or the computing system that receives data as a result of the transaction may be considered the point of sale, as applicable.

System for Processing Payment Transactions Using a Mobile Device Without Secure Elements

[0033] FIG. 1 illustrates a system 100 for the processing of payment transactions using a mobile device without requiring the use of secure elements, which can include the secure provisioning of payment credentials to a mobile device, secured storage thereof, and use in generating multiple application cryptograms for use in validating and processing the payment transaction.

[0034] The system 100 may include a transaction management server 102. The transaction management server 102, discussed in more detail below, may be one or more computing devices specifically programmed to perform the functions discussed herein for provisioning payment credentials to a mobile device 104 using securely transmitted remote notification message, and for validating payment credentials produced by the mobile device 104 as part of a payment transaction. While it is illustrated and discussed herein that the transaction management server 102 performs a variety of functions, it will be apparent to persons having skill in the relevant art that the transaction management server 102 may be comprised of multiple computing devices, servers, and/or computing networks configured to perform the functions discussed herein. The mobile device 104, discussed in more detail below, may be any type of mobile computing device suitable for performing the functions discussed herein, which may include a cellular phone, smart phone, smart watch, other wearable or embedded computing device, tablet computer, laptop computer etc. In some embodiments, the mobile device 104 may lack a secure element. In other embodiments, the mobile device 104 may include a secure element, but such an element may not be used in conjunction with the methods and systems discussed herein, or may be used in conjunction with the methods and systems discussed herein, such as to provide additional security.

[0035] The mobile device 104 may communicate with the transaction management server 104 using multiple communication channels, such as utilizing dual channel communication. Dual channel communication may include using two channels of communication in the transmitting and receiving of data, such as for verification and authentication, to ensure greater security in the transmission of data. The mobile device 104 may include a mobile payment application (MPA) configured to be executed by the mobile device 104 for performing the functions of the mobile device 104 discussed herein. The MPA, discussed in more detail below, may be installed on the mobile device 104 and may be activated using an activation code provided by the transaction management server 102 using methods and systems that will be apparent to persons having skill in the relevant art, such that the mobile device 104 and transaction management server 102 may securely transmit and receiving communications across one or more communication channels using shared data.

[0036] The system 100 may also include an issuer 106. The issuer 106 may be a financial institution, such as an issuing bank, that issues a payment card or payment credentials to a consumer 108 associated with a transaction account. The issuer 106 may provide payment details associated with the transaction account and/or payment card to the transaction management server 102. The payment details may include, for example, a transaction account number, account holder name, expiration date, security code, etc. The transaction management server 102 may store the data in an account database, discussed in more detail below. The transaction management server 102 may also provision the payment credentials to the mobile device 104. As used herein, the term "payment credentials" may refer to any data used by the mobile device 104 and/or transaction management server 102 in the transmission and validation of payment information used in a payment transaction using the methods and systems discussed herein, including, but not limited to, payment details, payment credentials, single use keys, session keys, application cryptograms, card master keys, etc.

[0037] In some embodiments, the payment credentials may be provisioned to the mobile device 104 via a remote notification service message. As discussed in more detail below, the remote notification service (RNS) message may be a secure message that is transmitted to the mobile device 104 and subsequently validated by the mobile device 104 such that the data contained therein may be secure from other devices and users. The MPA of the mobile device 104 may verify the authenticity of the received RNS message and may decrypt it to obtain the data included therein. The mobile device 104 may then perform any necessary functions, based on the data (e.g., such as by executing instructions included in the data), and, if applicable, may generate a return message to be sent back to the transaction management server 102. In some instances, the return message may be validated by the transaction management server 102.

[0038] In some instances, the validation of RNS messages in the mobile device 104, or the validation of return messages at the transaction management server 102, may utilize at least message counters and authentication code. The use of both counters and authentication codes may ensure that only the mobile device 104 that is intended may be able to validate and decrypt the data included in the RNS message. In addition, if the rules and/or algorithms used in the generation of the

authentication code are included in the MPA, then only a mobile device 104 that also includes a specific instance of the application program may be able to validate the RNS message, resulting in additionally increased security. In instances where the RNS message may include payment credentials, this may ensure that the payment credentials are available only on the appropriate mobile device 104, and only if the MPA used to access them is a proper and authorized application.

[0039] Payment credentials provisioned to the mobile device 104 may be securely stored in storage in the mobile device 104, such as a card database, discussed in more detail below. In some embodiments, the mobile device 104 may be configured to generate an advanced storage key for use in securely storing data, such as the payment credentials, in a database or memory in the mobile device 104. The generating of an advanced storage key, as discussed in more detail below, may utilize unique device information, unique MPA information, and randomly generated information in order to identify a secure storage key that can be used to securely store data in the mobile device 104. As a result, the payment credentials or other sensitive data may be securely stored in the mobile device 104 without the use of a secure element, which can result in the mobile device 104 being capable of initiating and conducting payment transaction's without the use of a secure element, increasing availability to issuers 106 and consumers 108, while maintaining a high level of security.

[0040] Once the mobile device 104 has payment credentials for a transaction account received, validated, and stored securely therein, a consumer 108 may take the mobile device 104 to a point of sale 110 at a merchant to conduct a payment transaction. The consumer 108 may select goods or services for purchase, may initiate a payment transaction for the purchase thereof with a merchant, and may use the mobile device 104 to convey the payment credentials for use in funding the payment transaction. The conveyance of payment credentials to the point of sale 110 may include the transmission of two or more application cryptograms. The use of two or more application cryptograms may result in a higher level of security for transactions processed using the methods and systems discussed herein than is available in traditional contactless and remote transactions, including transactions conducted using a mobile device 104 having a secure element.

[0041] The application cryptograms may each be generated by the mobile device 104 using separate session keys and additional data, discussed in more detail below. The application cryptograms, generated using data stored in the mobile device 104, such as in storage secured via the advanced storage key and associated with the MPA, may ensure that the application cryptograms authenticate the mobile device 104 and the specific instance of the MPA. In some instances, one of the cryptograms and/or session keys used to generate the cryptograms may use information provided by the consumer 108, such as a personal identification number (PIN). Use of the PIN or other consumer authentication information may enable for a cryptogram to authenticate both the consumer 108 and the mobile device 104. In such an instance, the cryptograms generated by the mobile device 104 may include one that authenticates the mobile device 104, and a second that authenticates both the mobile device 104 and the consumer 108.

[0042] The cryptograms may be received by the point of sale 110 as part of the conducting of the payment transaction, such as via near field communication. The application cryptograms may accompany additional payment information, such as may be required in the context of any suitable type of payment transaction, such as a contactless transaction, a remote transaction, a secure remote payment transaction, a magnetic stripe transaction, and an M/Chip EMV transaction, and may be transmitted to the point of sale 110 using any suitable method in accordance therein as will be apparent to persons having skill in the relevant art. The cryptograms may be transmitted to an acquirer 112, which may be a financial institution, such as an acquiring bank, associated with the merchant. The acquirer 112 may, for instance, issue a transaction account to the merchant that is used to receive payment of funds from the consumer 108 for the payment transaction. The acquirer 112 may submit the cryptograms and additional transaction details to a payment network 114 using methods and systems that will be apparent to persons having skill in the relevant art. For instance, the transaction details and application cryptograms may be included in an authorization request submitted to the payment network 114 on the payment rails.

[0043] In some embodiments, both application cryptograms may be included in a single transaction message. For example, the mobile device 104 and/or point of sale 110 may include both application cryptograms in legacy data fields of a traditional transaction message in order to transmit both application cryptograms using existing

payment systems and hardware. In some instances, the transaction management server 102 may be configured to use Track 2 data for validation of the application cryptograms, such as in a magnetic stripe transaction. In such instances, if the transaction message include Track 1 data, the transaction management server 102 may be configured to convert Track 1 data into Track 2 data, which may also include converting modified Track 1 or Track 2 data into unmodified (e.g., original, reconstructed, etc.) Track 1 or Track 2 data, respectively. By performing these functions, and by including the application cryptograms in legacy data fields, the transaction management server 102 may be configured to process and validate remote and contactless payment transactions using a mobile device 104 with a higher level of security, without requiring the use of a secure element on the mobile device 104, and without modification to legacy payment systems.

[0044] The payment network 114 may process the payment transaction using methods and systems that will be apparent to persons having skill in the relevant art. As part of the processing, the payment network 114 may transmit the application cryptograms to the issuer 106 for verification. In some embodiments, the verification may be performed by the payment network 114. The issuer 106 or payment network 114 may communicate with the transaction management server 102. In some embodiments, the application cryptograms may be transmitted to the transaction management server 102, and may be verified via the generation of validating application cryptograms using the transaction management server 102, which may be generated using the locally stored payment credentials. In other embodiments, the issuer 106 or payment network 114 may request application cryptograms from the transaction management server 102, which may generate them and return the cryptograms to the issuer 106 or payment network 114 for validation against the cryptograms produced by the mobile device 104.

[0045] Because the transaction management server 102 possesses the payment credentials and other data used by the mobile device 104 to generate the application cryptograms, validation of the payment credentials produced by the mobile device 104 to fund the payment transaction may be performed via comparison of the application cryptograms generated by the mobile device 104 and those generated by the transaction management server 102. In some embodiments, the transaction management server 102 may be a part of the payment network 114 or issuer 106. In

instances where the transaction management server 102 may be part of the payment network 114, the validation may be performed prior to contacting the issuer 106 as part of the traditional processing of the payment transaction (e.g., for approval of funding the transaction using the consumer's 108 transaction account with the issuer 106).

[0046] By using multiple application cryptograms, the security of the payment transactions can be increased. In addition, in instances where each cryptogram may authenticate separate data, such as instances where one cryptogram authenticates the mobile device 104 and the other authenticates both the mobile device 104 and the consumer 108 (e.g., via the consumer's PIN), it may also provide the issuer 106 with additional data and considerations for use in deciding to approve or deny a transaction. For example, if both cryptograms are incorrect (e.g., the cryptograms generated by the mobile device 104 do not match those generated by the transaction management server 102), the transaction may be denied. If one cryptogram is correct and the other incorrect, the transaction may be denied for security reasons, or may be approved, such as based on a decision of the issuer 106. For example, the issuer 106 may approve a transaction where consumer authentication fails but mobile device authentication passes, as other available data may indicate that an authorized user, but not the consumer 108, is using the mobile device 104 for the transaction.

[0047] As a result, the use of both cryptograms may provide for valuable data that can be used by payment networks 114 and issuers 106 in the processing of payment transactions. In addition, the use of two or more cryptograms may provide for increased security than in traditional contactless or remote payment methods, which may result in less fraud and more acceptance for consumers 108, issuers 106, and merchants. In instances where the use of two or more application cryptograms are generated from payment credentials that have been provisioned securely using RNS messaging methods and systems discussed herein, and stored securely via advanced storage keys generated using methods and systems discussed herein, the overall security of the system 100 can be vastly increased over traditional systems for contactless payments and transaction processing. As a result, the system 100 may provide for increased security in several aspects of data transmission, storage, and processing than provided for in traditional contactless payment systems and for

other types of remote payment transactions and payment transactions in general that may use the methods and systems discussed herein.

Mobile Device

[0048] FIG. 2 illustrates an embodiment of the mobile device 104 of the system 100. It will be apparent to persons having skill in the relevant art that the embodiment of the mobile device 104 illustrated in FIG. 2 is provided as illustration only and may not be exhaustive to all possible configurations of the mobile device 104 suitable for performing the functions as discussed herein. For example, the computer system 1700 illustrated in FIG. 17 and discussed in more detail below may be a suitable configuration of the mobile device 104.

[0049] The mobile device 104 may include a receiving unit 202. The receiving unit 202 may be configured to receive data over one or more networks via one or more network protocols. The receiving unit 202 may receive, for instance, program data for one or more application programs to be installed on and executed by the mobile device 104, such as a mobile payment application (MPA) discussed in more detail below. The receiving unit 202 may also receive remote notification service (RNS) messages, such as messages transmitted by the transaction management server 102 including RNS messages that include payment credentials. The receiving unit 202 may also receive additional data suitable for performing the traditional functions of a mobile device 104, such as telephone communications, cellular communications, etc. In some instances, the mobile device 104 may include a plurality of receiving units 202, such as separate receiving units 202 each configured to communicate with one or more separate networks via suitable protocols. For example, the mobile device 104 may include a first receiving unit 202 for receiving data for NFC transactions, and a second receiving unit 202 for receiving communications over a mobile communication network.

[0050] The mobile device 104 may also include an input unit 214. The input unit 214 may be configured to communicate with one or more input devices that are internally or externally connected to the mobile device 104 for receiving input from the consumer 108, such as a keyboard, mouse, click wheel, scroll wheel, touch screen, microphone, camera, receiver, etc. The input unit 214 may receive input from the consumer 108, which may be processed by a processing unit 204.

[0051] The processing unit 204 may be configured to perform the functions of the mobile device 104 discussed herein. The processing unit 204 may execute program code stored in the mobile device, such as for the MPA, and may be configured to perform a plurality of functions associated with each application program, in addition to other functions of the mobile device 104. The processing unit 204 may receive input from the consumer 108 via the input unit 214 and perform functions accordingly, such as by executing application programs, performing functions in programs, receiving data, transmitting data, displaying data, etc., as will be apparent to persons having skill in the relevant art. For example, the processing unit 204 may be configured to validate RNS messages, generate advanced storage keys, and generate application cryptograms, as discussed in more detail below.

[0052] The mobile device 104 may also include a display unit 210. The display unit 210 may be configured to communicate with one or more display devices that are internally or externally connected to the mobile device 104 for displaying data, such as data transmitted to the display unit 210 for display by the processing unit 204. Display devices may include liquid crystal displays, light-emitting diode displays, thin film transistor displays, touch screen displays, etc.

[0053] The mobile device 104 may also include a transmitting unit 206. The transmitting unit 206 may be configured to transmit data over one or more networks via one or more network protocols. The transmitting unit 206 may transmit RNS response messages to the transaction management server 102. The transmitting unit 206 may also be configured to transmit application cryptograms and/or payment credentials, such as to a point of sale 110, for use in a payment transaction. The transmitting unit 206 may be further configured to perform additional functions of the mobile device 104 as will be apparent to persons having skill in the relevant art, such as the traditional functions of a mobile communication device for transmitting cellular communications, etc. In some instances, the mobile device 104 may include a plurality of transmitting units 206, which may be separately configured to communicate with one or more separate networks, such as a transmitting unit 206 configured to transmit payment credentials and payment cryptograms via NFC and another transmitting unit 206 configured to transmit data over a mobile communication network.

[0054] The mobile device 104 may also include a card database 208. The card database 208, discussed in more detail below, may be data storage on the mobile device 104 that is configured to store data associated with one or more transaction accounts and/or payment cards. The card database 208 may store payment credentials associated with the transaction account, such as provisioned to the mobile device 104 by the transaction management server 102 in a secure RNS message, and additional data that may be used in the generation of application cryptograms, as discussed in more detail below. In some instances, the card database 208 may be stored as part of the mobile payment application.

[0055] The mobile device 104 may further include a memory 212. The memory 212, discussed in more detail below, may be configured to store data for the mobile device 104 suitable for performing the functions of the mobile device 104 discussed herein. For example, the memory 212 may store data suitable for the generation of advanced storage keys for the encrypting of additional data in the mobile device 104, such as the card database 208, as discussed in more detail below. The memory 212 may also be configured to store program code for application programs executed by the processing unit 204, such as an operating system, program code for receiving data via the input unit 214 and displaying data via the display unit 210, rules and/or algorithms for performing functions discussed herein, etc. The memory 212 may also store data suitable for performing the traditional functions of a mobile device 104, such as rules and/or algorithms for transmitting and receiving cellular communications via a mobile network. Additional data stored in the memory 212 will be apparent to persons having skill in the relevant art.

Mobile Device Card Database

[0056] FIG. 3 illustrates an embodiment of the card database 208 of the mobile device 104 for storing payment credentials and other data associated with transaction accounts for use in funding payment transactions conducted with the mobile device 108.

[0057] The card database 208 may include one or more payment profiles 302, illustrated in FIG. 3 as payment profiles 302a, 302b, and 302c. Each payment profile 302 may be associated with a transaction account that may be used to fund a payment transaction and may include at least payment credentials 304, one or more

single use keys 306, a first session key 308, a second session key 310, and an application transaction counter 312.

[0058] The payment credentials 304 may include data associated with the related transaction account that is used for identification and validation by the payment network 114 and/or issuer 106 in the processing of a payment transaction using the related transaction account. The payment credentials 304 may include, for example, a transaction account number, security code, expiration date, cardholder name, authorized user name, tracking data, card layout description data, digit counts, bitmaps, etc.

[0059] Single use keys 306 may be payment tokens valid for a single payment transaction that may be used by the processing unit 204 of the mobile device 104 to generate one or more of the application cryptograms used in the payment transaction. In some embodiments, a single use key 306 may include one or more of the other data elements included in the payment profile 302. For example, each single use key 306 may include a distinct application transaction counter 312, which may not be included separately in the payment profile 302. Different configurations of the data stored in the payment profile 302 for use in performing the functions disclosed herein will be apparent to persons having skill in the relevant art. In some instances, the single use key 306 may include, or may be comprised of, a key used to generate the one or more application cryptograms. In some embodiments, the first session key 308 and second session key 310 may be included in a single use key 306 provisioned to the mobile device 104 and/or generated using data included in the single use key 306.

[0060] The first session key 308 and second session key 310 may be additional keys that are used by the processing unit 204 in the generation of the application cryptograms transmitted to the point of sale 110 as part of the conducting of a payment transaction using the mobile device 104. In some embodiments, the first session key 308 may be used in the generation of a first application cryptogram by the processing unit 204, such as using program code, rules, or algorithms stored in the memory 212 of the mobile device 104. The second session key 310 may be used in the generation of a second application cryptogram.

[0061] In some embodiments, the second session key 310 may be generated by the processing unit 204. In such an embodiment, the second session key 310 may

be generated using a single use key 306 and user authentication data, such as a PIN provided by the consumer 108 (e.g., via the input unit 214). In such an embodiment, the second session key 310 may not be stored in the payment profile 302, and may instead be generated, used, and discarded as part of the payment transaction process. The second application cryptogram may therefore, when generated from the second session key 310 that is generated using the single use key 306 and the consumer PIN, serve to authenticate both the mobile device 104 and the consumer 108.

[0062] The personal identification number (PIN), may be a number supplied by the consumer 108 (e.g., during registration of the MPA on the mobile device 104 or registration of the transaction account with the issuer 106 and/or transaction management server 102) that may be used to authenticate the consumer 108. When conducting a payment transaction, the consumer 108 or other user of the mobile device 104 may supply a PIN via the input unit 214. In some embodiments, if the supplied PIN is incorrect (e.g., does not match the PIN supplied by the consumer 108 during registration), then the processing unit 204 may continue to generate the second session key 310 and subsequently generate the second application cryptogram. If the supplied PIN is incorrect, then the second application cryptogram will thereby be incorrect, which will result in a failed validation of the second application cryptogram by the transaction management server 102, issuer 106, and/or payment network 114, which may provide the issuer 106 with an opportunity to decline the transaction accordingly, or still approve the transaction.

Mobile Device Memory

[0063] FIG. 4 illustrates an embodiment of the memory 212 of the mobile device 104 for storing application programs and other data to be used in the secured storage of data on the mobile device 104 and for the conducting of payment transactions using the mobile device 104. In an exemplary embodiment, the memory 212 may not be a secure element.

[0064] The memory 212 may include device information 402. The device information 402 may include one or more pieces of data associated with the mobile device 104 that may, in some instances, be unique to the mobile device 104. For example, the device information 402 may include a media access control address, a reference number, a serial number, an identification number, etc. Additional

information that may be considered device information 402 of a mobile device 104 will be apparent to persons having skill in the relevant art.

[0065] The memory 212 may also include a mobile payment application (MPA) 404. The MPA 404 may be an application program configured to perform the functions of the mobile device 104 discussed herein, such as the receipt and storage of payment credentials, validation of RNS messages, and generation of application cryptograms for use in conducting payment transactions. Additional features of the MPA 404 may include traditional features of a digital wallet or other similar application program, as will be apparent to persons having skill in the relevant art.

[0066] The MPA 404 may include program code 406. The program code 406 may be code, executed by the processing unit 204 of the mobile device 104, that causes the processing unit 204 and other components of the mobile device 104 to perform the functions of the MPA 404 as discussed herein. For example, the program code 406 may include code suitable for generating application cryptograms, validating RNS messages, etc. The program code 406 may also include program code suitable for generating a random value, which may be used in the generation of an advanced storage key. The random value may be a random or pseudo-random number, which may be generated using methods and systems that will be apparent to persons having skill in the relevant art.

[0067] The MPA 404 may also include an instance identifier 408. The instance identifier 408 may be a value unique to the specific MPA 404, which may be used in the generation of the advanced storage key used to secure data in the mobile device 104, such as the card database 208. By having the instance identifier 408 unique to the MPA 404, multiple MPAs 404 may be installed on the mobile device 104, without any one MPA 404 being able to access data that is securely stored by any other MPA 404, which can thereby ensure that payment profiles 302 for specific transaction accounts are not accessible by other programs. The instance identifier 408 may be a number, alphanumeric value, hexadecimal value, or any suitable value that may be unique to an MPA 404.

[0068] As discussed in more detail below, the processing unit 204 of the mobile device 104 may be configured to generate a diversifier value using the device information 402, the random value generated using the program code 406 of the MPA 404, and the instance identifier 408 stored in the MPA 404. The diversifier

value may be used by a cryptography application 410 also stored in the memory 212. The cryptography application 410 may be an application program configured to perform white box cryptography and/or any other suitable cryptographic function that will be apparent to persons having skill in the relevant art.

[0069] The cryptography application 410 may include program code 412. The program code 412 may be executed by the processing unit 204 of the mobile device 104 to enable the processing unit 204 and other components of the mobile device 104 to perform the cryptographic functions of the cryptography application 410 discussed herein. The functions may include the generation of an advanced storage key. The advanced storage key may be generated using the diversifier value generated by the mobile payment application 404 and an encryption key 414 included in the cryptography application 410. In some embodiments, the diversifier key may be decrypted using the encryption key 414 to obtain the advanced storage key.

[0070] The cryptography application 410 may also be configured to encrypt storage in the mobile device 104 using the advanced storage key. In some embodiments, the encryption may be performed using one or more white box cryptography techniques. The encrypted storage may be the card database 208 and/or any other suitable storage in the mobile device 104, such as data stored in the MPA 404. In some embodiments, the cryptography application 410 may be included as part of the MPA 404. The advanced storage key may be stored in the cryptography application 410 or MPA 404, or, in some instances, may be re-generated by the MPA 404 and cryptography application 410 when needed.

[0071] The memory 212 may also include any additional data stored in the mobile device 104 suitable for performing the functions discussed herein, as well as any additional functions of mobile devices. For instance, the memory 212 may include program code for an operating system, code, rules, or algorithms for receiving and transmitting mobile communications, such as telephone calls, etc.

[0072] In some embodiments, the mobile device 104 may also be configured to receive data already encrypted using the advanced storage key, which may be stored in encrypted local storage in the mobile device 104, such as in the memory 212, the card database 208, or other suitable storage. In such an embodiment, the mobile device 104 may be configured to transmit the generated random value to the

transaction management server 102 or other trusted entity, which may generate the advanced storage key using the same methods and systems using the generated random value, and may encrypt data that is provisioned to the mobile device 104. The mobile device 104 may thus receive data already encrypted using the advanced storage key, for local storage in the mobile device 104.

Transaction Management Server

[0073] FIG. 5 illustrates an embodiment of the transaction management server 102 of the system 100. It will be apparent to persons having skill in the relevant art that the embodiment of the transaction management server 102 illustrated in FIG. 5 is provided as illustration only and may not be exhaustive to all possible configurations of the transaction management server 102 suitable for performing the functions as discussed herein. For example, the computer system 1700 illustrated in FIG. 17 and discussed in more detail below may be a suitable configuration of the transaction management server 102.

[0074] The transaction management server 102 may include a receiving unit 502. The receiving unit 502 may be configured to receive data over one or more networks via one or more network protocols. The receiving unit 502 may receive data from the mobile device 104, such as receipt or return messages, confirmation messages, transaction notifications, etc., payment network 114, issuer 106, or other suitable entity. The receiving unit 502 may receive transaction notifications or cryptogram requests, such as to initiate the generation of application cryptograms for use in validation of payment credentials in a payment transaction. The receiving unit 502 may also receive transaction account data, such as from the issuer 106, for use in generating payment credentials for provisioning to the mobile device 104.

[0075] The transaction management server 102 may also include a processing unit 504. The processing unit 504 may be configured to perform the functions of the transaction management server 102 discussed herein, as will be apparent to persons having skill in the relevant art. The processing unit 504 may thus be configured to generate and encrypt RNS messages and data included therein, validate return messages from the mobile device 104, generate payment credentials, generate application cryptograms, validate application cryptograms, etc., as discussed in more detail below.

[0076] The transaction management server 102 may further include a transmitting unit 506. The transmitting unit 506 may be configured to transmit data over one or more networks via one or more network protocols. The transmitting unit 506 may transmit RNS messages, payment credentials, application cryptograms, validation notifications, and other data that will be apparent to persons having skill in the relevant art. The transmitting unit 506 may be configured to transmit data to the mobile device 104, such as via a mobile communication network or the Internet, the payment network 114, the issuer 106, and any other suitable entity.

[0077] The transaction management server 102 may also include an account database 508. The account database 508, discussed in more detail below, may be configured to store account information for a plurality of transaction accounts. The account information may include data and keys used for the generation of application cryptograms used in validation of payment credentials received during payment transactions conducted using the mobile device 104. The account database 508 may also be configured to store transaction data for payment transactions conducted involving the mobile device 104 and other data, such as data associated with the consumer 108 or other authorized users of the related transaction account.

[0078] The transaction management server 102 may also include a memory 510. The memory 510 may be configured to store additional data for use by the transaction management server 102 in performing the functions disclosed herein. For example, the memory 510 may store rules or algorithms for the validation of application cryptograms, rules or algorithms for the generation of validation notifications, algorithms for the generation of session keys and application cryptograms, encryption keys for the encryption and decryption of data and RNS messages, etc. Additional data that may be stored in the memory 510 will be apparent to persons having skill in the relevant art.

Transaction Management Server Account Database

[0079] FIG. 6 illustrates an embodiment of the account database 508 of the transaction management server 102 for storing data related to transaction accounts for use in validating payment credentials and other transaction data provided in the conducting of payment transactions including the mobile device 104.

[0080] The account database 508 may include a plurality of account profiles 602, illustrated in FIG. 6 as account profiles 602a, 602b, and 602c. Each account profile

602 may include one or more single use keys 604, a first session key 606, a second session key 608, an application transaction counter 610, and a first card master key 612. In some embodiments, an account profile 602 may further include a second card master key 612.

[0081] Each account profile 602 may correspond to a payment profile 302 provisioned to a mobile device 104. As such, the single use keys 604 stored in an account profile 602 may correspond to the single use keys 306 stored in the corresponding payment profile 302 related to the same transaction account. The data may be similar such that, when an application cryptogram is generated by the transaction management server 102 or the mobile device 104, the application cryptograms should match if the data is accurate and has not been tampered with, which may enable validation of payment credentials presented by the mobile device 104.

[0082] In some embodiments, an account profile 602 may include a personal identification number (PIN) that corresponds to the PIN 314 stored in the corresponding payment profile 302. In such an embodiment, the PIN 314 may be provided to the receiving unit 202 transaction management server 102 in a secure message, such as a receipt message provided by the mobile device 104 discussed in more detail below. In other embodiments, a card master key may be used in place of the PIN, such as the first card master key 612. In such an embodiment, the processing unit 504 of the transaction management server 102 may be configured to generate a second session key 608 based on the second card master key 614 that corresponds to the second session key 310 generated by the mobile device 104 using the single use key 306 and the PIN 314. In some instances, the second session key 608 may also be based on the corresponding single use key 604. In such embodiments, algorithms for the generation of session keys and/or application cryptograms may ensure that the cryptograms generated by the mobile device 104 and the transaction management server 102 correspond based on data used therein.

[0083] The first session key 606 may be used by the processing unit 504 of the transaction management server 102 to generate a first application cryptogram, and the second session key 608 may be used to generate a second application cryptogram. In some embodiments, the application transaction counter 610 may be used in the generation of one or more of the session keys and/or application

cryptograms. The application transaction counter 610 may be a value corresponding to the payment transaction to be conducted that is incremented or otherwise modified during each transaction. The application transaction counter 610 may correspond to the application transaction counter 312 stored in the corresponding payment profile 302 in the mobile device 104, such that its use may ensure that only a valid MPA 404 may possess the correct application transaction counter 312 to generate valid session keys and/or application cryptograms. Additional techniques to further enhance the security of the session key and/or application cryptogram generation may be used, such as unpredictable numbers and other techniques that will be apparent to persons having skill in the relevant art.

Processing of Payment Transactions Using the Mobile Device

[0084] FIG. 7 illustrates a process for the processing of payment transactions conducted using the mobile device 104 without a secure element and using the generation and validation of two or more application cryptograms.

[0085] In step 702, the transaction management server 102 may provision (e.g., via the transmitting unit 506) payment credentials 304 and other account data to the mobile device 104, such as via an RNS message discussed in more detail below. In step 704, the receiving unit 202 of the mobile device 104 may receive the payment credentials 304 and other account data. In step 706, the processing unit 204 of the mobile device 104 may store the data in a payment profile 302 in the card database 208. The account data may include the payment credentials 304, one or more single use keys 308, and any other suitable data, such as one or more of the session keys 308 and 310.

[0086] In step 708, the processing unit 204 may generate two application cryptograms for use in conducting a payment transaction. In some embodiments, step 708 may be initiated by the consumer 108, such as by indicating via the input unit 214, by placing the mobile device 104 near the point of sale 110 to initiate the transaction via near field communication, or other suitable method. Generation of the application cryptograms may include generating a first application cryptogram using the first session key 308 stored in the payment profile 302. The second application cryptogram may be generated using a second session key 310, which may be generated using a single use key 306 and a PIN 314. In some instances, the consumer 108 may enter a PIN into the mobile device 104 (e.g., via the input unit

214) prior to step 708 or during the initiation of step 708. In some embodiments, one or both of the application cryptograms may also be generated using the application transaction counter 312.

[0087] Once the application cryptograms have been generated, they, along with the payment credentials 304, may be transmitted to the issuer 106 via the point of sale 110, acquirer 112, and payment network 114. The payment credentials 304 and application cryptograms may be received by the issuer 106 in step 710. In step 712, the transmitting unit 206 of the mobile device 104 may transmit a transaction notification to the transaction management server 102. In step 714, the receiving unit 502 of the transaction management server 102 may receive the transaction notification. The transaction notification may notify the transaction management server 102 that the mobile device 104 has initiated a payment transaction using the payment profile 302. In some instances, the transaction notification may include identification information.

[0088] In step 716, the processing unit 504 of the transaction management server 102 may identify an account profile 602 corresponding to the payment profile 302 and may generate two application cryptograms using the data contained therein. The first application cryptogram may be generated using the first session key 606, which may be generated using the first card master key 612. The second application cryptogram may be generated using the second session key 608. In some embodiments, one or both of the application cryptograms and/or session keys may be further based on the single use keys 604, application transaction counter 610, or any other suitable data.

[0089] In step 718, the transmitting unit 506 of the transaction management server 102 may transmit the generated application cryptograms to the issuer 106, which may receive the cryptograms in step 718. In step 720, the issuer 106 may validate the application cryptograms provided by the mobile device 104 accompanying the payment credentials 304. Validation of the application cryptograms may include comparing the mobile device 104 supplied cryptograms with the application cryptograms generated and supplied by the transaction management server 102. Once validation is performed, then, in step 722, the issuer 106 may process the transaction accordingly. Transaction processing may include approval of the payment transaction, such as if one or both of the cryptograms are validated, or

denial of the payment transaction, such as if one or both of the cryptograms are determined to be invalid.

[0090] In step 724, a transaction notification may be transmitted by the issuer 106, or other entity (e.g., the payment network 114, acquirer 112, etc.) as part of the processing of the payment transaction. The transaction notification may be transmitted to the transaction management server 102 and received by the receiving unit 502, in step 726. The transaction notification may also be received by the receiving unit 202 of the mobile device 104, in step 728. The transaction notification may be an indication of approval or denial of the payment transaction. The processing units 204 and 504 of the mobile device 104 and transaction management server 102, respectively, may each perform one or more functions as a result of the received transaction notification. For instance, if the transaction was approved and processed successfully, the application transaction counters 310 and 610 in the respective profiles may be updated accordingly.

[0091] FIG. 8 illustrates an alternative process for processing a payment transaction using the mobile device 104.

[0092] In step 802, the payment credentials 304 and other account data may be transmitted to the mobile device 104 by the transmitting unit 506 of the transaction management server 102. In step 804, the receiving unit 202 of the mobile device 104 may receive the payment credentials 304 and other account data, which may be stored in a payment profile 302 in step 806. In step 808, the processing unit 204 of the mobile device 104 may generate the two application cryptograms, as discussed above, and may transmit the cryptograms, payment credentials 304, and other suitable data to the issuer 106 (e.g., via the point of sale 110).

[0093] In step 810, the issuer 106 may receive the application cryptograms and any other suitable data that may be used by the issuer 106 to validate the transaction data and/or process approval or denial of the transaction. In step 812, the issuer 106 may submit a request for validation cryptograms to the transaction management server 102. In some embodiments, the request may include the payment credentials 304 or other data suitable for use by the transaction management server 102 in identifying the account profile 602 to be used to generate the validation cryptograms. In one embodiment, the request may further include the two application cryptograms generated by the mobile device 104 for validation.

[0094] In step 814, the receiving unit 502 of the transaction management server 102 may receive the cryptogram request. In step 816, the processing unit 504 of the transaction management server 102 may generate the two application cryptograms to be used for validation, as discussed above. In embodiments where the cryptogram request also includes the two application cryptograms generated by the mobile device 104, step 816 may also include the validation of the two cryptograms by the processing unit 504 using the two newly generated application cryptograms. The validation cryptograms, or the validation result in applicable embodiments, may be transmitted by the transmitting unit 506 to the issuer 106. In step 818, the issuer 106 may receive the validation cryptograms and/or the validation result.

[0095] In step 820, the issuer 106 may validate the application cryptograms provided by the mobile device 104 using the application cryptograms generated by the transaction management server 102. In embodiments where the transaction management server 102 provides a validation result to the issuer 106, step 820 may include identifying the result of the validation of each of the two application cryptograms. In step 822, the issuer 106 may process the payment transaction accordingly based on the result of the validation. In step 824, transaction notifications may be transmitted to the transaction management server 102 and the mobile device 104, received by the respective receiving units 502 and 202 in steps 826 and 828, respectively.

Remote Notification Service and Data Messaging

[0096] FIG. 9 illustrates a process for the transmission and validation of remote notification service (RNS) messages and other data messages transmitted from the transaction management server 102 to the mobile device 104. RNS messages may be transmitted via a remote notification service, such as one that utilizes a mobile communication network associated with the mobile device 104. RNS messages may be used to provision payment credentials 304 and other account data to the mobile device 104, such as the account data used in the processing of payment transactions, as discussed above, and other information that may be used in the establishing of a secure connection between the mobile device 104 and the transaction management server 102.

[0097] In step 902, the processing unit 504 of the transaction management server 102 may generate a message. In instances where mutual authentication is being

established with the mobile device 104, the message may include information suitable for establishing the mutual authentication, such as a session identifier. In other instances, such as when mutual authentication has been established between the transaction management server 102 and mobile device 104 using the process illustrated in FIG. 9 and discussed herein, the generated message may include payment credentials 304 and account data, may include one or more commands to be executed by the MPA 404 of the mobile device 104 (e.g., the removal of single use keys 306 or payment credentials 304, etc.), may be notifications to be presented to the consumer 108 (e.g., account balances, payment notifications, etc.), or include other suitable data.

[0098] In step 904, the processing unit 504 may encrypt the generated message. The message may be encrypted using a private key of a private/public key pair, where the mobile device 104 may possess a corresponding public key. In some instances, the message may be encrypted using an encryption key associated with the mobile device 104 or the MPA 404, such as the encryption key 414. In step 906, the processing unit 504 may generate a message authentication code. The message authentication code may be generated using the encrypted message and may be a key that is generated using one or more specially configured rules and/or algorithms. For instance, the message authentication code may be generated using one or more encryption and obfuscation methods, such as padding. In some embodiments, the message authentication code may be generated using the encryption key.

[0099] In step 908, the transmitting unit 506 of the transaction management server 102 may transmit a combined data message to the mobile device 104. In embodiments where the mutual authentication may be being performed, the combined data message may be a remote notification service message transmitted to the mobile device 104 via the remote notification service. The combined data message may be received by the receiving unit 202 of the mobile device 104 in step 910, and may include the message authentication code and the encrypted message. In some instances, the combined data message may also include an additional identifier, such as one generated using methods known to the MPA 404 for verification thereof. In some cases, such as when mutual authentication has already been performed, the combined data message may also include a message counter.

[0100] In step 912, the processing unit 204 may generate a reference authentication code. The reference authentication code may be generated using the received encrypted message and may be generated using the same rules and algorithms as the transaction management server 102 used to generate the message authentication code, such that the generated reference authentication code would correspond to the message authentication code, if the message authentication code is generated by a trustworthy source (e.g., the transaction management server 102). In embodiments where the message authentication code may be generated using the encryption key, the processing unit 204 may generate the reference authentication code using the encryption key 414 stored in the memory 212 or other suitable encryption key.

[0101] In step 914, the processing unit 204 may validate the message authentication code included in the received combined data message by comparing it against the generated reference authentication code. If both the message counter and message authentication code are validated, then the combined data message may be determined to be trustworthy (e.g., genuine) as coming from the transaction management server 102. In instances where the combined data message may include a message identifier, the processing unit 204 may also validate the message identifier by generating a message identifier using a process known by the MPA 404 for generation and comparison thereof. In embodiments where the combined data message may include a message counter, the processing unit 204 may validate the message counter included in the received combined data message with a reference counter stored in the mobile device 104, such as in the MPA 404 or in a payment profile 502.

[0102] In step 916, the processing unit 204 may decrypt the encrypted message included in the received combined data message. The encrypted message may be decrypted using a key, such as one stored in the memory 212 (e.g., in the cryptography application 410 or MPA 404) or stored in a local encrypted database (e.g., encrypted using an advanced storage key), or other suitable method of decryption. In step 918, the processing unit 204 may perform one or more appropriate actions based on the data decrypted from the encrypted message. In the example illustrated in FIG. 9, the mobile device 104 may perform mutual authentication with the transaction management server 102, such as using the

session identifier included in the encrypted message and decrypted by the processing unit 204. In step 920, the transaction management server 102 may receive the session identifier and perform any additional actions necessary for mutual authentication with the mobile device 104. In instances where mutual authentication has already been performed, the message may include other information suitable for performing the functions disclosed herein, such as payment credentials 404, single use keys 406, program instructions for the MPA 404, etc.

[0103] In some embodiments, the mobile device 104 may be configured (e.g., via the MPA 404) to generate and submit a return message to the transaction management server 102. In some instances, the return message may include data generated in response to the actions performed as instructed in the decrypted message, as discussed above. For example, a return message may indicate valid receipt and storage of payment credentials 304 or single use keys 306. In other instances, the return message may be a notification of receipt and validation of the combined data message. In instances where mutual authentication is first being performed, the return message may include the session identifier used to perform the mutual authentication.

[0104] FIGS. 10A and 10B illustrate a process for the generation and transmission of a return message by the mobile device 104 and validation thereof by the transaction management server 102.

[0105] In step 1002, the processing unit 204 of the mobile device 104 may generate a receipt message. The receipt message may be generated based on program code 406 stored in the MPA 404, and may be further based on actions performed as indicated in a decrypted combined data message received from the transaction management server 102. For instance, the receipt message may include a notification of successful receipt and storage of payment credentials 304. In step 1004, the processing unit 204 may increment a receipt counter. The receipt counter may be a counter indicative of the number of receipt messages transmitted to the transaction management server 102. The receipt counter may be stored in the memory 212, such as in the MPA 404, or in a database encrypted using the advanced storage key. It will be apparent to persons having skill in the relevant art

that step 1004 may be an optional step, and may only be used in instances where a counter is used for validation of a data message.

[0106] In step 1006, the processing unit 204 may encrypt the receipt message. The receipt message may be encrypted using the encryption key 414 stored in the cryptography application 410, or may be otherwise stored in the MPA 404 or a locally encrypted database. The encryption key used to encrypt the receipt message may be a private key as part of a key pair, with the transaction management server 102 possessing a corresponding public key. In step 1008, the processing unit 204 may generate a receipt authentication code based on the encrypted receipt message. In some embodiments, the receipt authentication code may be generated using the same rules, algorithms, and/or processes as used to generate the reference authentication code illustrated in step 912 of FIG. 9, discussed above.

[0107] In step 1010, the transmitting unit 206 of the mobile device 104 may transmit a receipt notification message to the transaction management server 102. The receipt notification message may be received by the receiving unit 502 of the transaction management server 102 and may include at least the receipt authentication code, the encrypted receipt message, and the receipt counter. In some embodiments, the receipt notification message may be transmitted to the transaction management server 102 using a mobile communication network, such as a cellular network, associated with the mobile device 104.

[0108] In step 1014, the processing unit 504 of the transaction management server 102 may increment a confirmation counter. The confirmation counter may be indicative of the number of messages received from the mobile device 104, used for validation of messages received from the mobile device 104. The confirmation counter may be stored in the memory 510 of the transaction management server 102 or other suitable data storage. For instance, in some embodiments, the confirmation counter may be stored in an account profile 602 associated with the mobile device 104. In one example, each account profile 602 may include a confirmation counter (e.g., and/or a message counter) to be used for messages transmitted to/from the transaction management server 102 and mobile device 104 related to the corresponding transaction account. It will be apparent to persons having skill in the

relevant art that step 1014 may be an optional step and may not be performed in instances where a counter may not be used for validation of return messages.

[0109] In step 1016, the processing unit 504 may generate a confirmation authentication code. The confirmation authentication code may be generated based on the encrypted receipt message included in the receipt notification message, and may be generated using the same rules, algorithms, and/or processes used to generate the message authentication code. In step 1018, the processing unit 504 may validate the receipt counter included in the receipt notification message by comparing it to the confirmation counter. In step 1020, the processing unit 504 may validate the receipt authentication code by comparing it to the message authentication code, to ensure that the message originated from an authorized mobile device 104.

[0110] Once the counter (e.g., if applicable) and authentication code have been validated, then, in step 1022, the processing unit 504 may decrypt the encrypted message included in the received receipt notification message. The encrypted message may be decrypted using a stored encryption key or other suitable method of decryption. The encrypted message may be decrypted to obtain the receipt message generated by the mobile device 104. In step 1024, the processing unit 504 may perform any appropriate actions as necessary based on the data included in the receipt message. For example, if the receipt message includes an indication of successful receipt and storage of single use keys 306, the processing unit 204 may activate corresponding single use keys 604 in a corresponding account profile 602.

Validation of Data Messages

[0111] FIG. 11 illustrates a process 1100 for the validation of data messages received by the mobile device 104 from the transaction management server 102.

[0112] In step 1102, the processing unit 204 of the mobile device 104 may store encryption keys, authentication generation keys, and rules and/or algorithms for the use and application thereof in local storage, such as the memory 212 or locally encrypted storage encrypted using an advanced storage key. In step 1104, the receiving unit 202 of the mobile device 104 may receive a data message from the transaction management server 102. In some embodiments, the data message may be received from the transaction management server 102 following the establishing

of mutual authentication between the two devices, such as using the process illustrated in FIG. 9 and discussed above. The data message may include at least a message counter, a message authentication code, and an encrypted message.

[0113] In step 1106, the processing unit 204 may increment a reference counter. The reference counter may be stored in the memory 212 or other local storage, and may be used to indicate the number of messages received from the transaction management server 102. In some instances, the reference counter may be incremented using an algorithm, such that the reference counter may not be incremented using consecutive numbers, but via an algorithm known to the mobile device 104 (e.g., via the MPA 404) and the transaction management server 102.

[0114] In step 1108, the processing unit 204 may validate the message counter included in the received data message. Validation of the message counter may include comparison of the message counter to the value of reference counter after being incremented. Failed validation may indicate that the source of the data message is not the transaction management server 102 or is otherwise not trustworthy. If the validation fails, then, in step 1110, the processing unit 204 may perform one or more appropriate actions associated with a failed data message receipt and/or validation. For example, the processing unit 204 may discard the data message, may notify the transaction management server 102, may lock the associated payment profile 302, or other action that will be apparent to persons having skill in the relevant art.

[0115] If the validation of the message counter passes, then the process 1100 may proceed to step 1112, where the encrypted message may be padded. Padding of the encrypted message may include the addition of values to the encrypted message or data associated thereof. Padding may be used to heighten the security of the message validation process, as it may be another function that must be performed by the mobile device 104 and transaction management server 102 known to each other that would need to be replicated by an unauthorized entity in order to transmit or receive a data message successfully without authorization. It will be apparent to persons having skill in the relevant art that step 1112 may be an optional step. In some embodiments, step 1112 may be applied in some instances of the process

1110. For example, the encrypted message may be padded at certain increments of the reference counter.

[0116] In step 1114, the processing unit 204 may generate a reference authentication code. The reference authentication code may be generated based on the encrypted message (e.g., as padded, if applicable) using one or more rules or algorithms, such as stored in step 1102. In some embodiments, the reference authentication code may be a key or may be a value generated by application of a key to the encrypted message. In step 1116, the processing unit 204 may validate the message authentication code received in the RNS message. Validation of the message authentication code may include comparison of the code to the generated reference authentication code, as another method of identification if the received data message originated from an authorized source (e.g., the transaction management server 102).

[0117] If the validation of the message authentication code fails, the process 1100 may proceed to step 1110 where the failure processing is performed. If the validation of the message authentication code passes, then, in step 1118, the encrypted message included in the received data message may be decrypted by the processing unit 204. The message may be decrypted using one or more encryption/decryption keys, rules, and/or algorithms, such as stored in the mobile device 104 in step 1102. For example, the encryption key 414 stored in the cryptography application 410 of the memory 212 may be used to decrypt the encrypted message. In step 1120, the processing unit 204 may perform one or more actions as appropriate based on the content of the decrypted message. For example, if the decrypted message includes single use keys 306, the single use keys 306 may be stored in the appropriate payment profile 302 of the card database 208, which may thereby be encrypted using the advanced storage key.

Advanced Storage Key

[0118] FIG. 12 illustrates the generation and use of the advanced storage key by the mobile device 104 for the secure storage of data in the mobile device 104, such as payment profiles 302 and other data that may be securely stored and accessed in the mobile device 104 without the use of secure elements.

[0119] The device information 402 stored in the memory 212 of the mobile device 104 may include three or more pieces of device information 1202, illustrated in FIG. 12 as device information 1202a, 1202b, and 1202c. Each piece of device information 1202 may be associated with the mobile device 104. In some instances, each piece of device information 1202 may be unique to the mobile device 104. In other instances, one or more of the pieces of device information 1202 may not be unique to the mobile device 104 (e.g., a model number), but the three pieces of device information 1202 when taken together may be unique to the mobile device 104 (e.g., a unique combination). The pieces of device information 1202 may be data that will not change during the lifespan of the mobile device 104.

[0120] The processing unit 204 of the mobile device 104 may generate a mobile device fingerprint 1204 based on the three pieces of device information 1202a, 1202b, and 1202c. The mobile device fingerprint 1204 may be a value unique to the mobile device 104, and may be generated using one or more rules or algorithms stored in the memory 212, such as included in the program code 406 of the MPA 404. The mobile device fingerprint 1204 may be, for example, a numerical value, a hexadecimal value, a character string, etc.

[0121] The processing unit 204 may also be configured to generate a diversifier value 1208 using the mobile device fingerprint 1204. The diversifier value may be generated by combining the mobile device fingerprint 1204 with the instance identifier 408 of the MPA 404 as well as a random value 1206. The random value 1206 may be a random or pseudo-random number generated by the processing unit 204. In some instances, the random value 1206 may be generated pursuant to one or more rules or algorithms stored in the memory 212. The combination of the mobile device fingerprint 1204, instance identifier 408, and random value 1206 may also be performed using one or more rules or algorithms, such as stored in the program code 406 of the MPA 404. Use of the instance identifier 408 to generate the diversifier value may result in the ability to securely store data associated with an instance of the MPA 404 such that multiple installations of the MPA 404 may be unable to access data stored by other instances of the MPA 404.

[0122] The processing unit 204 may then generate an advanced storage key 1210 via application of the encryption key 414 stored in the cryptography application 410

to the diversifier value 1208. In some instances, the advanced storage key 1210 may be generated by decryption of the diversifier value 1208 using the encryption key 414. In other instances, the advanced storage key 1210 may be a value resultant from the encryption of the diversifier value 1208 using the encryption key 414. In some embodiments, the advanced storage key 1210 may be generated as the result of performing white box cryptography using the encryption key 414 and the diversifier value 1208.

[0123] Once the advanced storage key 1210 has been generated, the processing unit 204 may use the advanced storage key 1210 to encrypt a local database 1210. The local database 1210 may be comprised of, for example, the card database 208, one or more payment profiles 302, part of the memory 212, or other suitable data source. In some instances, the local database 1210 may be a part of another database in the mobile device 104, such as the card database 208. For example, the card database 208 may include a plurality of local databases 1212, such as a separate local database 1212 for each instance of the MPA 404 for storing payment profiles 302 associated thereof. The resulting encrypted local database 1214 may thereby securely store data that is inaccessible by any other application program internal or external the mobile device 104 except the specific instance of the MPA 404 that includes the instance identifier 408. Accordingly, the encrypted local database 1214 may be ideal to store payment credentials 304, single use keys 306, and other account data, and may provide for secure storage of sensitive account information without the use of secure elements.

[0124] In some embodiments, the storage key may also be used by the transaction management server 102 to provide encrypted data to the mobile device 104 for storage in the encrypted local database 1214. For example, the transmitting unit 206 of the mobile device 104 may transmit the generated random value 1206 to the transaction management server 102. In some instances, the instance identifier 408 may also be transmitted to the transaction management server 102, or it may be previously possessed by the transaction management server 102, such as during registration of the MPA 404. The transaction management server 102 may then generate the advanced storage key 1210 itself, encrypt data to be provisioned to the mobile device 104, such as payment credentials 304, single use keys 306, etc. using

the advanced storage key 1210, and then transmit the encrypted data to the mobile device 104. The mobile device 104 may then store the already encrypted data in the encrypted local database 1214.

First Exemplary Method for Generating Payment Credentials in a Payment Transaction

[0125] FIG. 13 illustrates a method 1300 for the generating of payment credentials in a payment transaction, including the use of two application cryptograms for the secure use of payment credentials in a mobile device 104 without a secure element.

[0126] In step 1302, at least a single use key (e.g., single use key 306) may be stored in a memory (e.g., a payment profile 302) associated with a transaction account. In some embodiments, the memory 302 may be a non-Secure Element memory in a mobile communication device (e.g., the mobile device 104). In step 1304, a personal identification number (PIN) may be received by a receiving device (e.g., the receiving unit 202 and/or input unit 214).

[0127] In step 1306, a first session key (e.g., first session key 308) may be identified by a processing device (e.g., the processing unit 204). In step 1308, a second session key (e.g., second session key 310) may be generated by the processing device 204 based on at least the stored single use key 306 and the received PIN.

[0128] In step 1310, a first application cryptogram may be generated by the processing device 204 based on at least the first session key 308. In step 1312, a second application cryptogram may be generated by the processing device 204 based on at least the second session key 310.

[0129] In step 1314, at least the first application cryptogram and the second application cryptogram may be transmitted by a transmitting device (e.g., the transmitting unit 206) for use in a payment transaction. In some embodiments, the first application cryptogram and the second application cryptogram may be transmitted to a point of sale device (e.g., the point of sale 110). In one embodiment, the method 1300 may further include storing, in the memory 302, a card master key associated with the transaction account, wherein identifying the first session key 308

includes generating, by the processing device 204, the first session key 308 based on at least the stored card master key.

[0130] In some embodiments, the method 1300 may also include storing, in the memory 302, an application transaction counter (e.g., the application transaction counter 312), wherein identifying the first session key 308 includes generating, by the processing device 204, the first session key 308 based on at least the stored application transaction counter 312. In one embodiment, the method 1300 may further include validating, by the processing device 204, the received PIN prior to generating the second session key 310. In a further embodiment, the processing device 204 may be configured to generate an invalid second session key 310 if validation of the received PIN fails.

Second Exemplary Method for Generating Payment Credentials in a Payment Transaction

[0131] FIG. 14 illustrates a method 1400 for the generating of payment credentials in a payment transaction, including the use of two application cryptograms validation of payment credentials generated by a mobile device 104 without the use of a secure element.

[0132] In step 1402, at least a card master key (e.g., first card master key 612) may be stored in a memory (e.g., account profile 602) associated with a transaction account. In step 1404, a first session key (e.g., first session key 606) may be generated by a processing device (e.g., the processing device 504) based on at least the stored card master key 612. In step 1406, a second session key (e.g., second session key 608) may be generated by the processing device 504.

[0133] In step 1408, a first application cryptogram may be generated by the processing device 504 based on at least the first session key 606. In step 1410, a second application cryptogram may be generated by the processing device 504 based on at least the second session key 608. In step 1412, at least the first application cryptogram and the second application cryptogram may be transmitted by a transmitting device (e.g., the transmitting unit 506) for use in a payment transaction.

[0134] In one embodiment, the method 1400 may further include storing, in the memory 602, a transaction account sequence number associated with the transaction account, wherein the first session key is further based on the stored transaction account sequence number. In some embodiments, the method 1400 may also include storing, in the memory 602, a second card master key (e.g., the second card master key 614) associated with the transaction account, wherein the second session key 608 is based on at least the stored second card master key 614.

[0135] In one embodiment, the method 1400 may further include: receiving, by a receiving device (e.g., the receiving unit 502), a first corresponding application cryptogram and a second corresponding application cryptogram; validating, by the processing device, (i) the received first corresponding application cryptogram based on the generated first application cryptogram, and (ii) the received second corresponding application cryptogram based on the generated second application cryptogram; and transmitting, by the transmitting device 506, a result of the validation for use in the payment transaction. In a further embodiment, the first corresponding application cryptogram and the second corresponding application cryptogram may be received from a point of sale device (e.g., the point of sale 110). In another further embodiment, the result of the validation may be transmitted to a financial institution (e.g., the issuer 106) associated with the transaction account.

Exemplary Method for Processing a Data Message

[0136] FIG. 15 illustrates a method 1500 for processing a data message, such as a remote notification message received via a remote notification service, including the receipt and validation thereof by a mobile device 104 without using a secure element.

[0137] In step 1502, at least an encryption key may be stored in a memory (e.g., the memory 212). In some embodiments, the memory 212 may be non-Secure Element memory in a mobile communication device (e.g., the mobile device 104). In step 1504, a data message may be received by a receiving device (e.g., the receiving unit 202), wherein the data message may include at least an encrypted message and a message authentication code, where the message authentication code is generated using at least a portion of the encrypted message. In some

embodiments, the data message may be an remote notification service message received via a remote notification service.

[0138] In step 1506, a reference authentication code may be generated by a processing device (e.g., the processing unit 204) using at least a portion of the encrypted message included in the received data message. In one embodiment, the memory 212 may further include one or more authentication code generation rules, and the reference authentication code may be generated based on application of the stored one or more authentication code generation rules to the portion of the encryption message included in the received data message. In step 1508, the received data message may be validated by the processing device 204 based on a check of the message authentication code included in the received data message against the generated reference authentication code. In some embodiments, the memory may further include a reference counter, the received data message may further include a message counter, and the received data message may be further validated by the processing device 204 based on a check of the message counter included in the received data message against the stored reference counter.

[0139] In step 1510, the encrypted message included in the data message may be decrypted by the processing device 204 using the stored encryption key to obtain a decrypted message. In one embodiment, the decrypted message may include at least one of: a digitized card profile (e.g., payment credentials 304) and a single use key (e.g., the single use key 306) for use in a payment transaction. In some embodiments, the method 1500 may also include checking, by the processing device 204, a data format of the decrypted message based on one or more data formatting rules.

[0140] In one embodiment, the method 1500 may further include transmitting, by a transmitting device (e.g., the transmitting unit 206), a receipt notification in response to the received data message. In a further embodiment, the method 1500 may even further include: performing, by the processing device 204, one or more actions based on the decrypted message; generating, by the processing device 204, a return message as a result of or based on the performed one or more actions; encrypting, by the processing device 204, the generated return message using the stored encryption key to obtain an encrypted return message; and generating, by the

processing device 204, a return authentication code using at least a portion of the encrypted return message, wherein the transmitted receipt notification includes the encrypted return message, and the return authentication code. In an even further embodiment, the memory 212 may further include a return counter, and the transmitted receipt notification may further include the return counter.

[0141] In some embodiments, the method 1500 may also include padding, by the processing device 204, the encrypted message included in the received data message using a padding key, wherein the portion of the encrypted message used to generate the reference authentication code is the padded encrypted message. In a further embodiment, the padding key may be the encryption key. In another further embodiment, the memory 212 may further include an authentication code padding algorithm, and padding the encrypted message using the padding key may include padding the encrypted message based on application of the padding key to the authentication code padding algorithm.

Exemplary Method for Building an Advanced Storage Key

[0142] FIG. 16 illustrates a method 600 for building an advanced storage key for the secure encryption and storage of local data in a mobile device 104 without using a secure element.

[0143] In step 1602, at least device information (e.g., device information 402) associated with a mobile communication device (e.g., the mobile device 104), program code (e.g., program code 406) associated with a first application program (e.g., the mobile payment application 404), and program code (e.g., program code 412) associated with a second application program (e.g., the cryptography application 410) may be stored in a memory (e.g., the memory 212) of the mobile communication device 104, wherein the program code 406 associated with the first application program 404 includes at least an instance identifier (e.g., instance identifier 408) and the program code 412 associated with the second application program 410 includes at least a first key (e.g., the encryption key 414).

[0144] In some embodiments, the device information 402 may include one or more unique identifier associated with the mobile communication device 104. In one embodiment, the instance identifier 408 may be unique to an instance of the first application program 404. In some embodiments, the second application program

410 may be configured to perform white box cryptography using the first key. In one embodiment, the first key may be a dynamic key. In some embodiments, the program code 412 associated with the second application program 410 may be included in the program code 406 associated with the first application program 404. In further embodiments, the second application program 410 may be an executable function of the first application program 404.

[0145] In step 1604, a device fingerprint (e.g., mobile device fingerprint 1204) associated with the mobile communication device 104 may be generated by a processing device (e.g., the processing unit 204) based on the stored device information 402 via execution of the program code 406 associated with the first application program 404. In step 1606, a random value (e.g., random value 1206) may be generated by the processing device 204 via execution of the program code 406 associated with the first application program 404. In some embodiments, the random value 1206 may be a random or pseudo-random number.

[0146] In step 1608, a diversifier value (e.g., diversifier value 1208) may be built by the processing device 204 based on at least the generated device fingerprint 1204, the generated random value 1206, and the instance identifier 408 included in the program code 406 associated with the first application program 404. In step 1610, the built diversifier value 1208 may be decrypted by the processing device 204 using the first key stored in the program code 412 associated with the second application program 410 via execution of the program code 412 associated with the second application program 410 to obtain a storage key (e.g., advanced storage key 1210).

[0147] In some embodiments, the method 1600 may further include: storing, in a local database (e.g., the local database 1212) of the mobile communication device 104, protected data; and encrypting, by the processing device 204, the protected data stored in the local database 1212 using the storage key 1210. In one embodiment, the method 1600 may also include: storing, in the memory 212, program data associated with the first application program 404; and storing, in the program data associated with the first application program 404, the generated random value 1206.

[0148] In one embodiment, the method 1600 may also include: transmitting, by a transmitting device (e.g., the transmitting unit 206) at least the random value 1206;

receiving, by a receiving device (e.g., the receiving unit 202), one or more encrypted parameters, wherein the one or more encrypted parameters are each encrypted using the storage key 1210; and storing, in a local database 1212 of the mobile communication device 104, the received one or more encrypted parameters. In a further embodiment, the storage key 1210 may be transmitted to a third party (e.g., the transaction management server 102) and the one or more encrypted parameters may be received from the third party 102. In some further embodiments, the instance identifier 408 may also be transmitted by the transmitting device 206.

Computer System Architecture

[0149] FIG. 17 illustrates a computer system 1700 in which embodiments of the present disclosure, or portions thereof, may be implemented as computer-readable code. For example, the transaction management server 102 and mobile device 104 of FIG. 1 may be implemented in the computer system 1700 using hardware, software, firmware, non-transitory computer readable media having instructions stored thereon, or a combination thereof and may be implemented in one or more computer systems or other processing systems. Hardware, software, or any combination thereof may embody modules and components used to implement the methods of FIGS. 7, 8, 9A, 9B, 10A, 10B, 11, and 13-16.

[0150] If programmable logic is used, such logic may execute on a commercially available processing platform or a special purpose device. A person having ordinary skill in the art may appreciate that embodiments of the disclosed subject matter can be practiced with various computer system configurations, including multi-core multiprocessor systems, minicomputers, mainframe computers, computers linked or clustered with distributed functions, as well as pervasive or miniature computers that may be embedded into virtually any device. For instance, at least one processor device and a memory may be used to implement the above described embodiments.

[0151] A processor unit or device as discussed herein may be a single processor, a plurality of processors, or combinations thereof. Processor devices may have one or more processor "cores." The terms "computer program medium," "non-transitory computer readable medium," and "computer usable medium" as discussed herein are used to generally refer to tangible media such as a removable storage unit 1718, a removable storage unit 1722, and a hard disk installed in hard disk drive 1712.

[0152] Various embodiments of the present disclosure are described in terms of this example computer system 1700. After reading this description, it will become apparent to a person skilled in the relevant art how to implement the present disclosure using other computer systems and/or computer architectures. Although operations may be described as a sequential process, some of the operations may in fact be performed in parallel, concurrently, and/or in a distributed environment, and with program code stored locally or remotely for access by single or multi-processor machines. In addition, in some embodiments the order of operations may be rearranged without departing from the spirit of the disclosed subject matter.

[0153] Processor device 1704 may be a special purpose or a general purpose processor device. The processor device 1704 may be connected to a communications infrastructure 1706, such as a bus, message queue, network, multi-core message-passing scheme, etc. The network may be any network suitable for performing the functions as disclosed herein and may include a local area network (LAN), a wide area network (WAN), a wireless network (e.g., WiFi), a mobile communication network, a satellite network, the Internet, fiber optic, coaxial cable, infrared, radio frequency (RF), or any combination thereof. Other suitable network types and configurations will be apparent to persons having skill in the relevant art. The computer system 1700 may also include a main memory 1708 (e.g., random access memory, read-only memory, etc.), and may also include a secondary memory 1710. The secondary memory 1710 may include the hard disk drive 1712 and a removable storage drive 1714, such as a floppy disk drive, a magnetic tape drive, an optical disk drive, a flash memory, etc.

[0154] The removable storage drive 1714 may read from and/or write to the removable storage unit 1718 in a well-known manner. The removable storage unit 1718 may include a removable storage media that may be read by and written to by the removable storage drive 1714. For example, if the removable storage drive 1714 is a floppy disk drive or universal serial bus port, the removable storage unit 1718 may be a floppy disk or portable flash drive, respectively. In one embodiment, the removable storage unit 1718 may be non-transitory computer readable recording media.

[0155] In some embodiments, the secondary memory 1710 may include alternative means for allowing computer programs or other instructions to be loaded into the computer system 1700, for example, the removable storage unit 1722 and an interface 1720. Examples of such means may include a program cartridge and cartridge interface (e.g., as found in video game systems), a removable memory chip (e.g., EEPROM, PROM, etc.) and associated socket, and other removable storage units 1722 and interfaces 1720 as will be apparent to persons having skill in the relevant art.

[0156] Data stored in the computer system 1700 (e.g., in the main memory 1708 and/or the secondary memory 1710) may be stored on any type of suitable computer readable media, such as optical storage (e.g., a compact disc, digital versatile disc, Blu-ray disc, etc.) or magnetic tape storage (e.g., a hard disk drive). The data may be configured in any type of suitable database configuration, such as a relational database, a structured query language (SQL) database, a distributed database, an object database, etc. Suitable configurations and storage types will be apparent to persons having skill in the relevant art.

[0157] The computer system 1700 may also include a communications interface 1724. The communications interface 1724 may be configured to allow software and data to be transferred between the computer system 1700 and external devices. Exemplary communications interfaces 1724 may include a modem, a network interface (e.g., an Ethernet card), a communications port, a PCMCIA slot and card, etc. Software and data transferred via the communications interface 1724 may be in the form of signals, which may be electronic, electromagnetic, optical, or other signals as will be apparent to persons having skill in the relevant art. The signals may travel via a communications path 1726, which may be configured to carry the signals and may be implemented using wire, cable, fiber optics, a phone line, a cellular phone link, a radio frequency link, etc.

[0158] The computer system 1700 may further include a display interface 1702. The display interface 1702 may be configured to allow data to be transferred between the computer system 1700 and external display 1730. Exemplary display interfaces 1702 may include high-definition multimedia interface (HDMI), digital visual interface (DVI), video graphics array (VGA), etc. The display 1730 may be

any suitable type of display for displaying data transmitted via the display interface 1702 of the computer system 1700, including a cathode ray tube (CRT) display, liquid crystal display (LCD), light-emitting diode (LED) display, capacitive touch display, thin-film transistor (TFT) display, etc.

[0159] Computer program medium and computer usable medium may refer to memories, such as the main memory 1708 and secondary memory 1710, which may be memory semiconductors (e.g., DRAMs, etc.). These computer program products may be means for providing software to the computer system 1700. Computer programs (e.g., computer control logic) may be stored in the main memory 1708 and/or the secondary memory 1710. Computer programs may also be received via the communications interface 1724. Such computer programs, when executed, may enable computer system 1700 to implement the present methods as discussed herein. In particular, the computer programs, when executed, may enable processor device 1704 to implement the methods illustrated by FIGS. 7, 8, 9A, 9B, 10A, 10B, 11, and 13-16, as discussed herein. Accordingly, such computer programs may represent controllers of the computer system 1700. Where the present disclosure is implemented using software, the software may be stored in a computer program product and loaded into the computer system 1700 using the removable storage drive 1714, interface 1720, and hard disk drive 1712, or communications interface 1724.

[0160] Techniques consistent with the present disclosure provide, among other features, systems and methods for processing payment transactions using a mobile device without using a secure element, including the transmission and validation of remote notification service messages and secure storage of data using an advanced storage key. While various exemplary embodiments of the disclosed system and method have been described above it should be understood that they have been presented for purposes of example only, not limitations. It is not exhaustive and does not limit the disclosure to the precise form disclosed. Modifications and variations are possible in light of the above teachings or may be acquired from practicing of the disclosure, without departing from the breadth or scope.

WHAT IS CLAIMED IS:

1. A method for receiving and processing a data message, comprising:
 - storing, in a memory, at least an encryption key;
 - receiving, by a receiving device, a data message, wherein the data message includes at least an encrypted message and a message authentication code, where the message authentication code is generated using at least a portion of the encrypted message;
 - generating, by a processing device, a reference authentication code using at least a portion of the encrypted message included in the received data message;
 - validating, by the processing device, the received data message based on a check of the message authentication code included in the received data message against the generated reference authentication code; and
 - decrypting, by the processing device, the encrypted message included in the received data message using the stored encryption key to obtain a decrypted message.
2. The method of claim 1, wherein the data message is a remote notification service message received via a remote notification service.
3. The method of claim 1, wherein
 - the memory is further configured to store a reference counter, and
 - validating the received data message further includes checking the message counter included in the received data message against the stored reference counter.
4. The method of claim 1, further comprising:
 - transmitting, by a transmitting device, a receipt notification in response to the received data message.
5. The method of claim 4, wherein
 - the method further comprises:

- 48 -

performing, by the processing device, one or more actions based on the decrypted message;

generating, by the processing device, a return message as a result of or based on the performed one or more actions;

encrypting, by the processing device, the generated return message using the stored encryption key to obtain an encrypted return message; and

generating, by the processing device, a return authentication code using at least a portion of the encrypted return message, wherein

the transmitted receipt notification includes the encrypted return message and the return authentication code.

6. The method of claim 5, wherein

the memory further includes a return counter, and

the transmitted receipt notification further includes the return counter.

7. The method of claim 1, wherein

the memory further includes one or more authentication code generation rules, and

the reference authentication code is generated based on application of the stored one or more authentication code generation rules to the portion of the encrypted message included in the received data message.

8. The method of claim 1, further comprising:

padding, by the processing device, the encrypted message included in the received remote notification service message using a padding key, wherein

the portion of the encrypted message used to generate the reference authentication code is the padded encrypted message.

9. The method of claim 8, wherein the padding key is the encryption key.
10. The method of claim 8, wherein
the memory further includes an authentication code padding algorithm, and
padding the encrypted message using the padding key includes padding the
encrypted message based on application of the padding key to the authentication
code padding algorithm.
11. The method of claim 1, further comprising:
checking, by the processing device, a data format of the decrypted message
based on one or more data formatting rules.
12. The method of claim 1, wherein the decrypted message includes at
least one of: a digitized card profile and a single use key for use in a payment
transaction.
13. The method of claim 1, wherein the reference authentication code is
further generated using the stored encryption key.
14. The method of claim 1, wherein the memory is non-Secure Element
memory in a mobile communication device.
15. A system for receiving and processing a data message, comprising:
a memory configured to store at least an encryption key;
a receiving device configured to receive a data message, wherein the data
message includes at an encrypted message and a message authentication code,
where the message authentication code is generated using at least a portion of the
encrypted message; and

- 50 -

a processing device configured to

- generate a reference authentication code using at least a portion of the encrypted message included in the received data message,
- validate the received data based on a check of the message authentication code included in the received data message against the generated reference authentication code, and
- decrypt the encrypted message included in the received data message using the stored encryption key to obtain a decrypted message.

16. The system of claim 15, wherein the data message is a remote notification service message received via a remote notification service.

17. The system of claim 15, wherein

- the memory is further configured to store a reference counter, and
- validating the received data message further includes checking the message counter included in the received data message against the stored reference counter.

18. The system of claim 15, further comprising:

- a transmitting device configured to transmit a receipt notification in response to the received remote notification service message.

19. The system of claim 18, wherein

- the processing device is further configured to
 - perform one or more actions based on the decrypted message,
 - generate a return message as a result of or based on the performed one or more actions,
 - encrypt the generated return message using the stored encryption key to obtain an encrypted return message, and

generate a return authentication code using at least a portion of the encrypted return message, and

the transmitted receipt notification includes the encrypted return message, the return counter, and the return authentication code.

20. The system of claim 19, wherein

the memory further includes a return counter, and

the transmitted receipt notification further includes the return counter.

21. The system of claim 15, wherein

the memory further includes one or more authentication code generation rules, and

the reference authentication code is generated based on application of the stored one or more authentication code generation rules to the portion of the encrypted message included in the received remote notification service message.

22. The system of claim 15, wherein

the processing device is further configured to pad the encrypted message included in the received remote notification service message using a padding key, and

the portion of the encrypted message used to generate the reference authentication code is the padded encrypted message.

23. The system of claim 22, wherein the padding key is the encryption key.

24. The system of claim 22, wherein

the memory further includes an authentication code padding algorithm, and

padding the encrypted message using the padding key includes padding the encrypted message based on application of the padding key to the authentication code padding algorithm.

25. The system of claim 15, wherein the processing device is further configured to check a data format of the decrypted message based on one or more data formatting rules.

26. The system of claim 15, wherein the decrypted message includes at least one of: a digitized card profile and a single use key for use in a payment transaction.

27. The system of claim 15, wherein the reference authentication code is further generated using the stored encryption key.

28. The system of claim 15, wherein the memory is non-Secure Element memory in a mobile communication device.

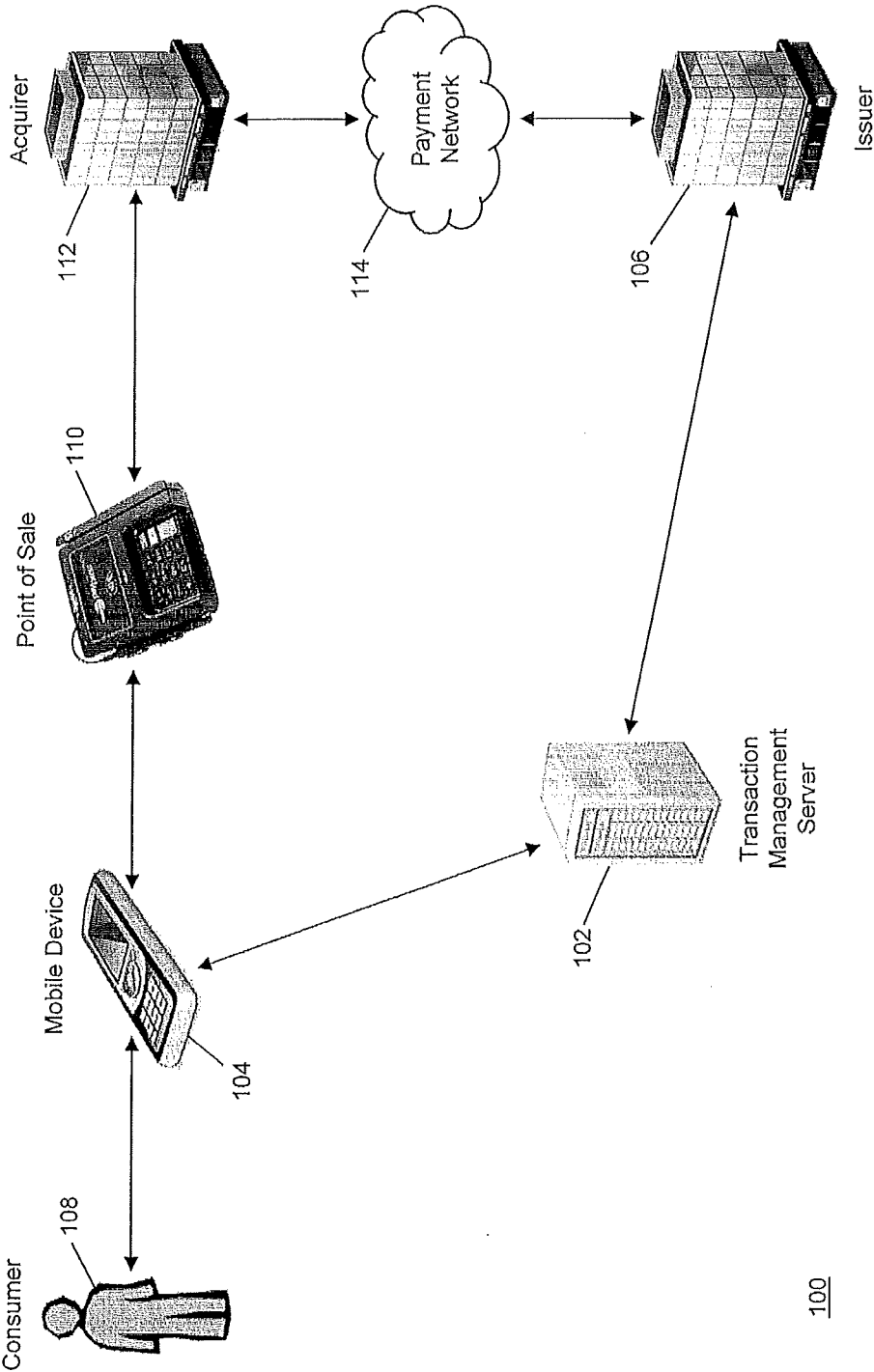


FIG. 1

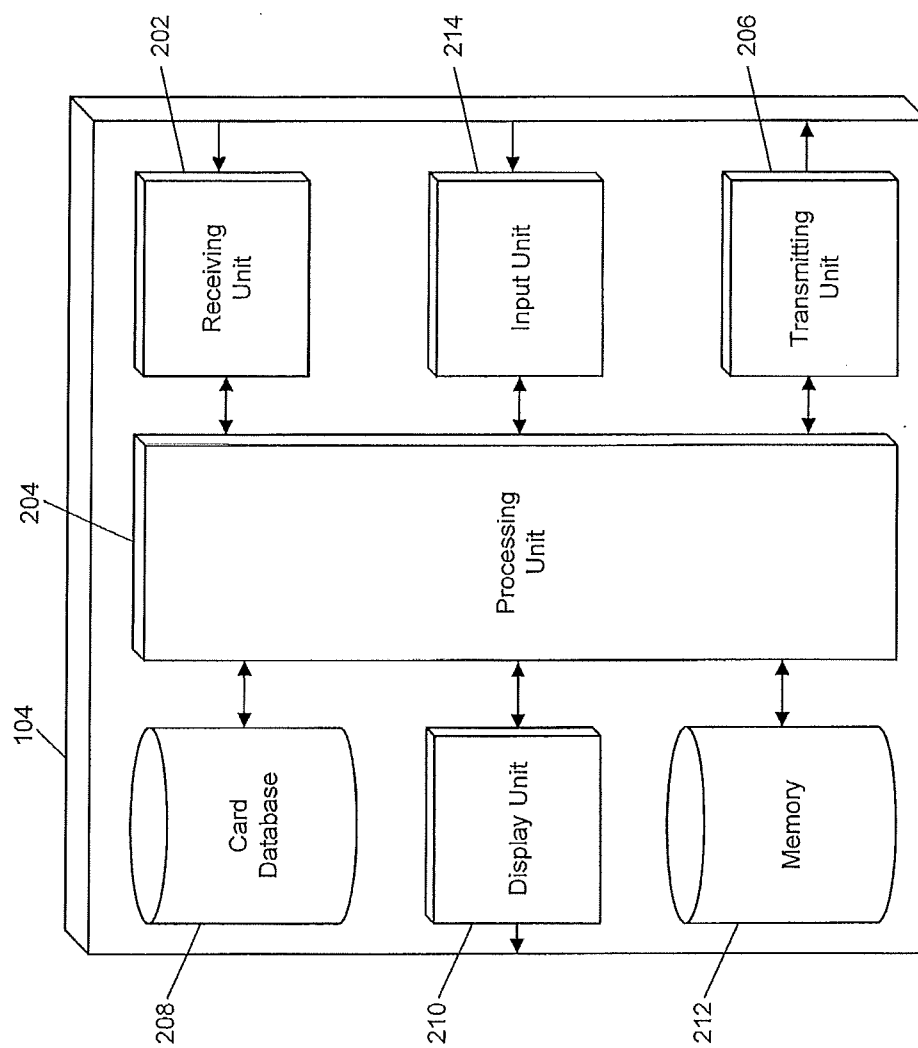


FIG. 2

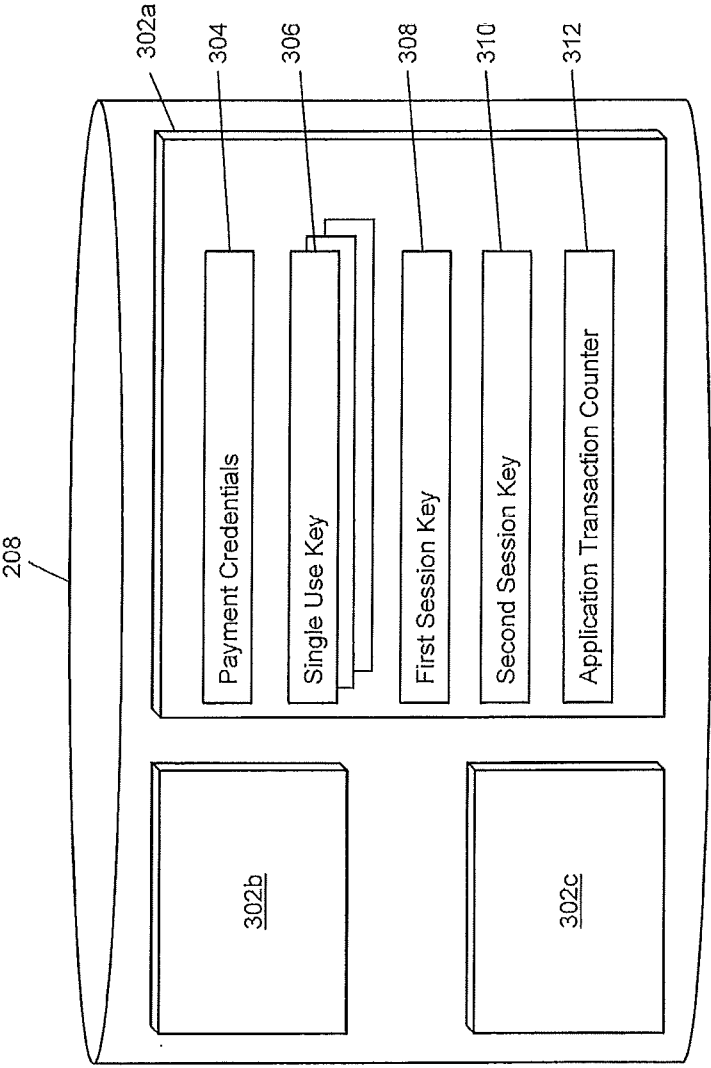


FIG. 3

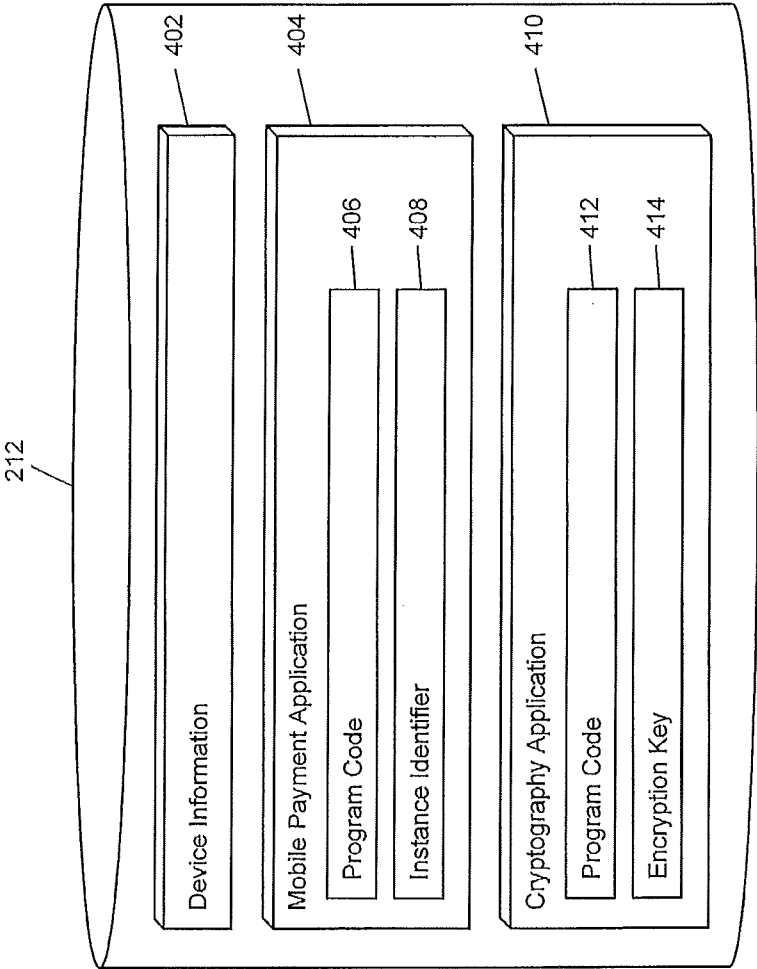


FIG. 4

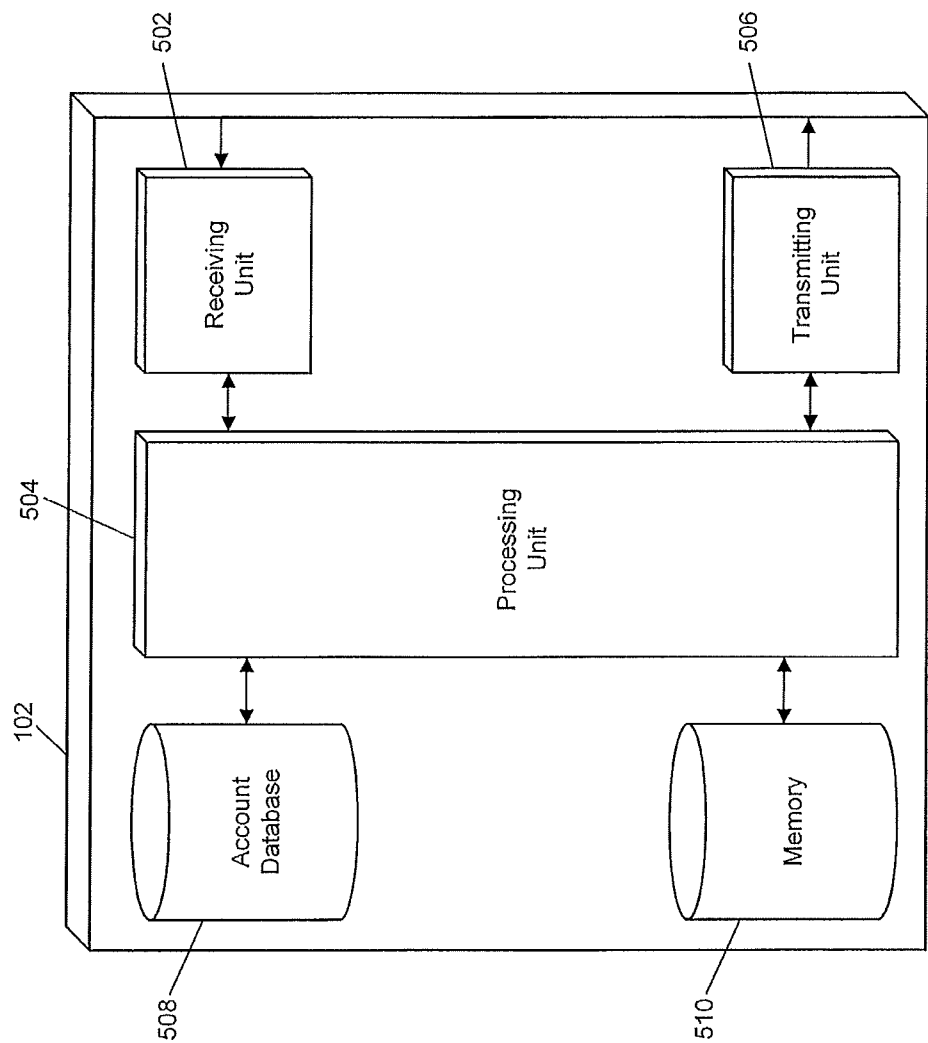


FIG. 5

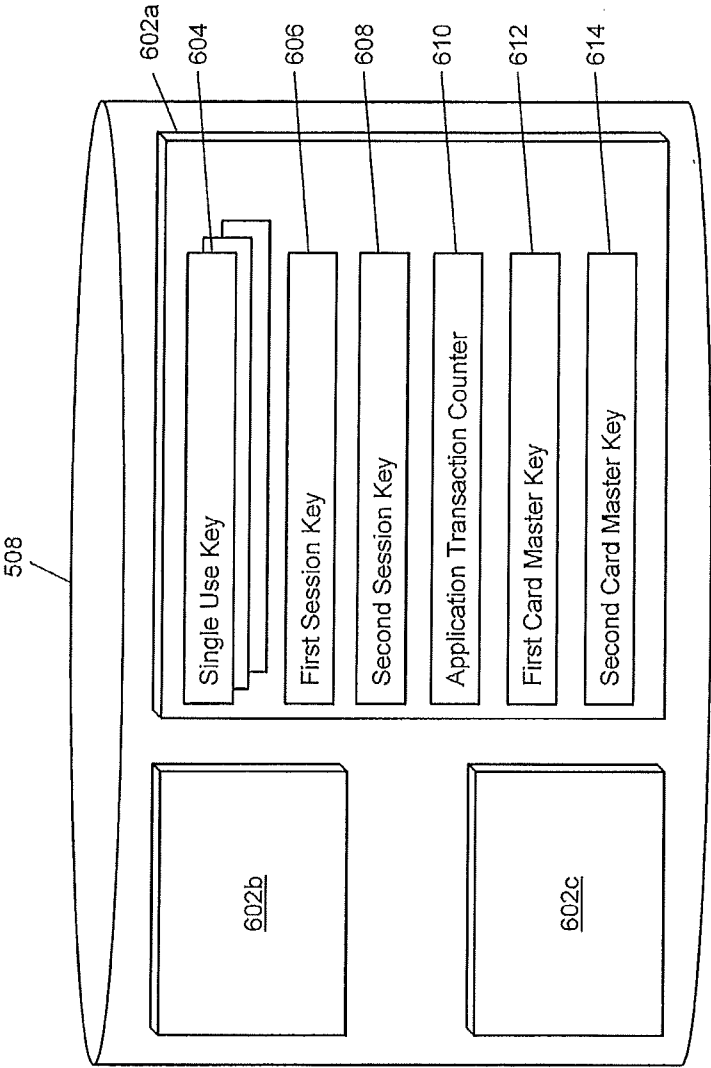


FIG. 6

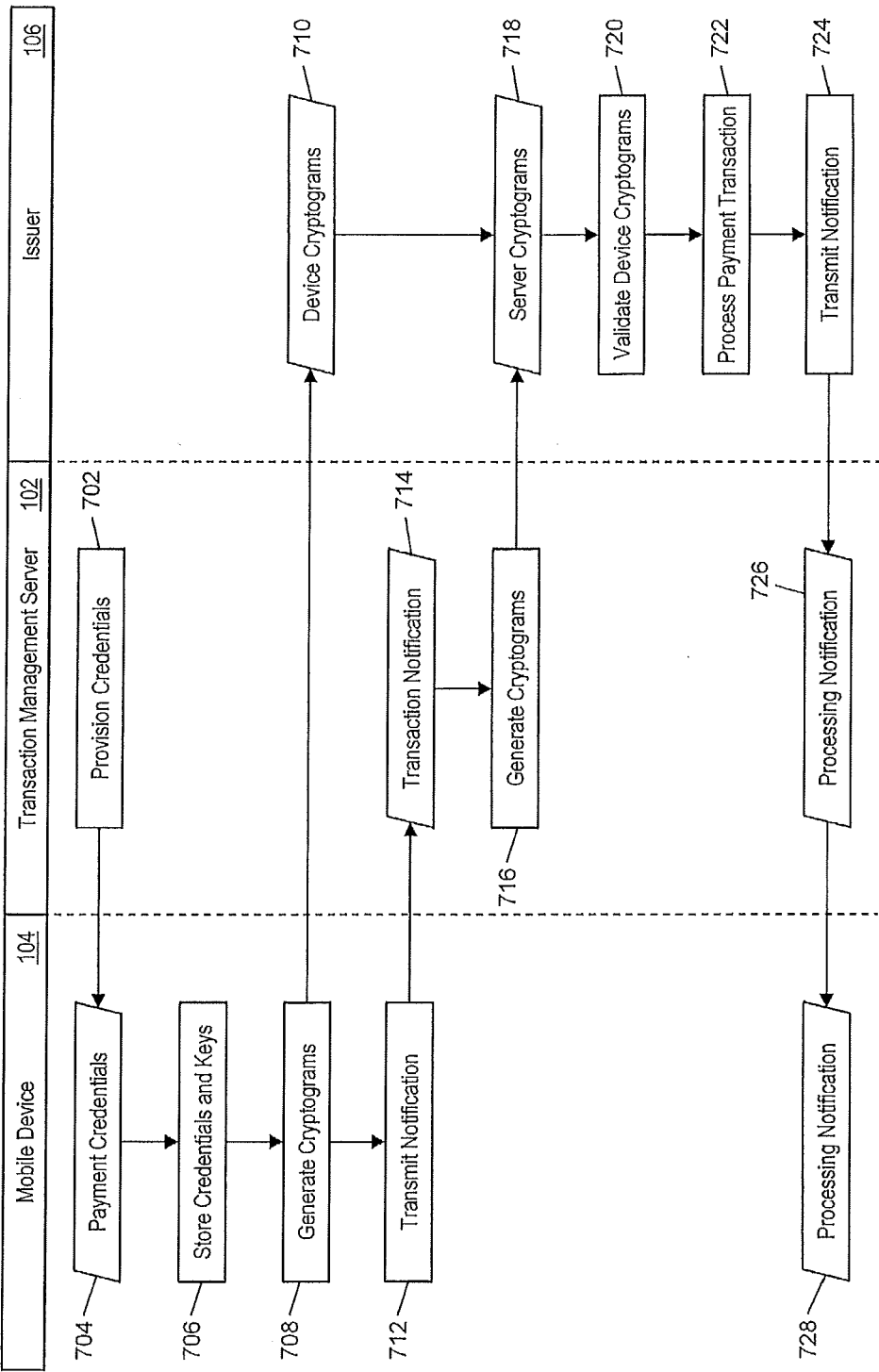


FIG. 7

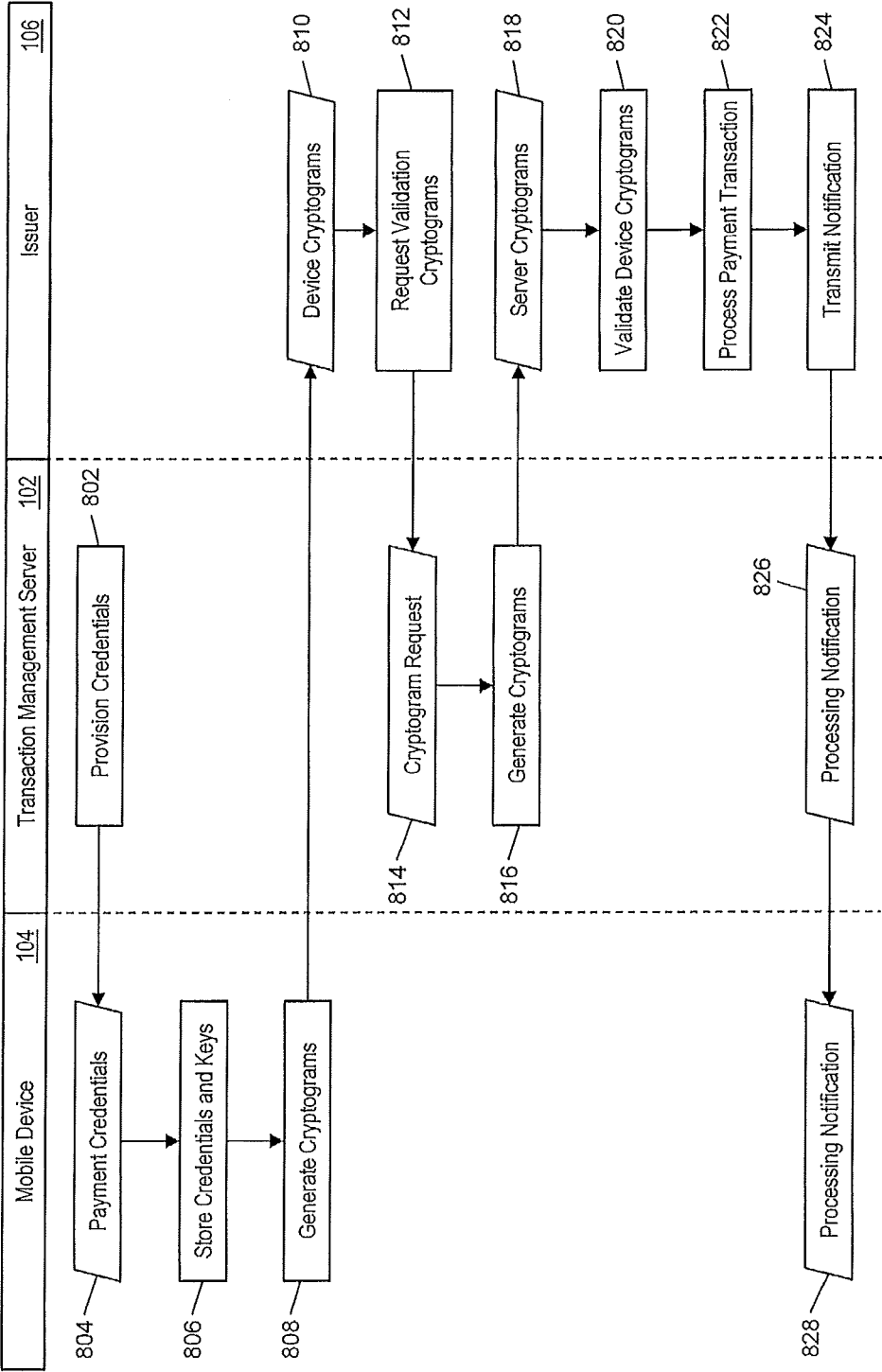


FIG. 8

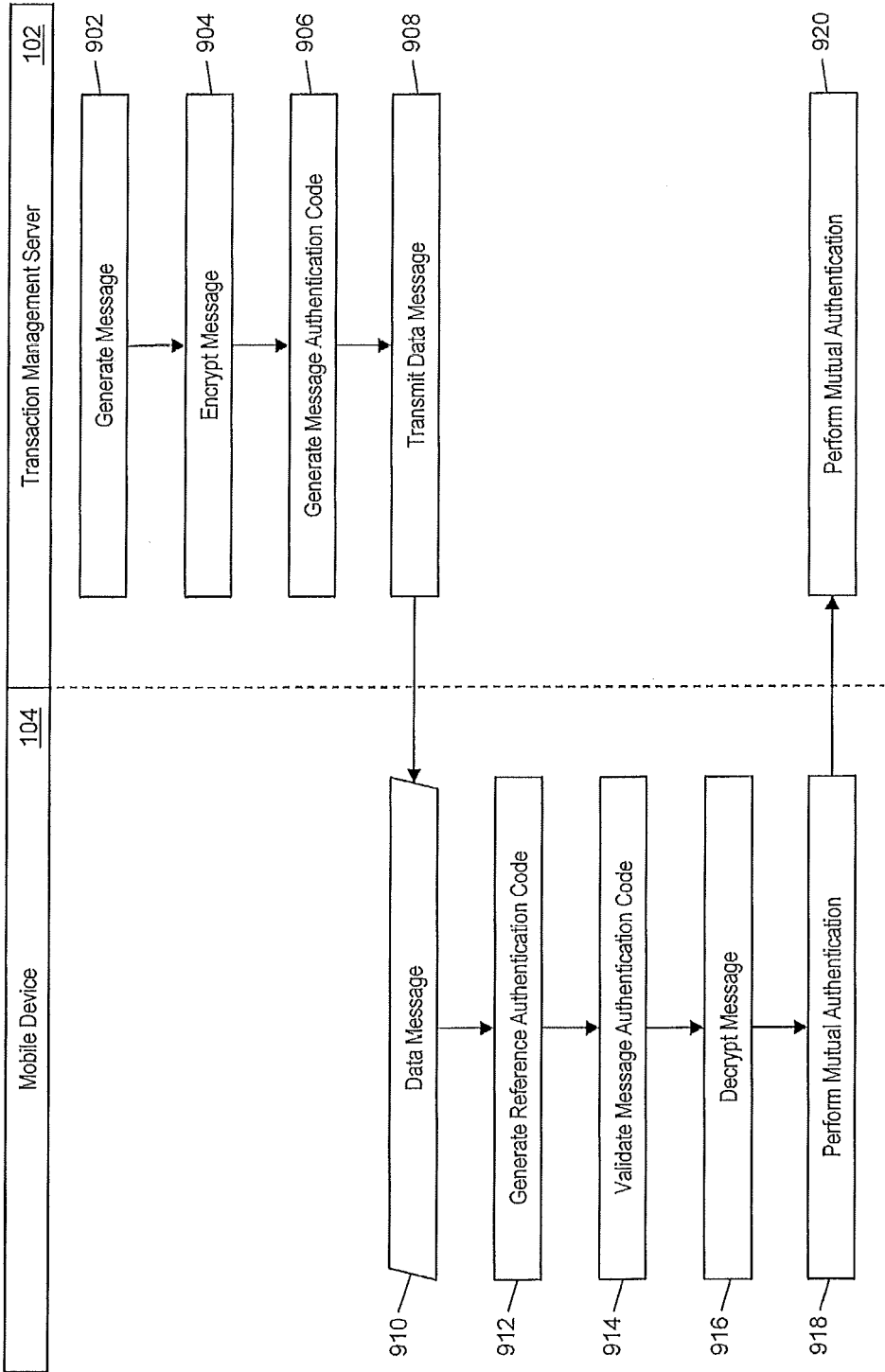


FIG. 9

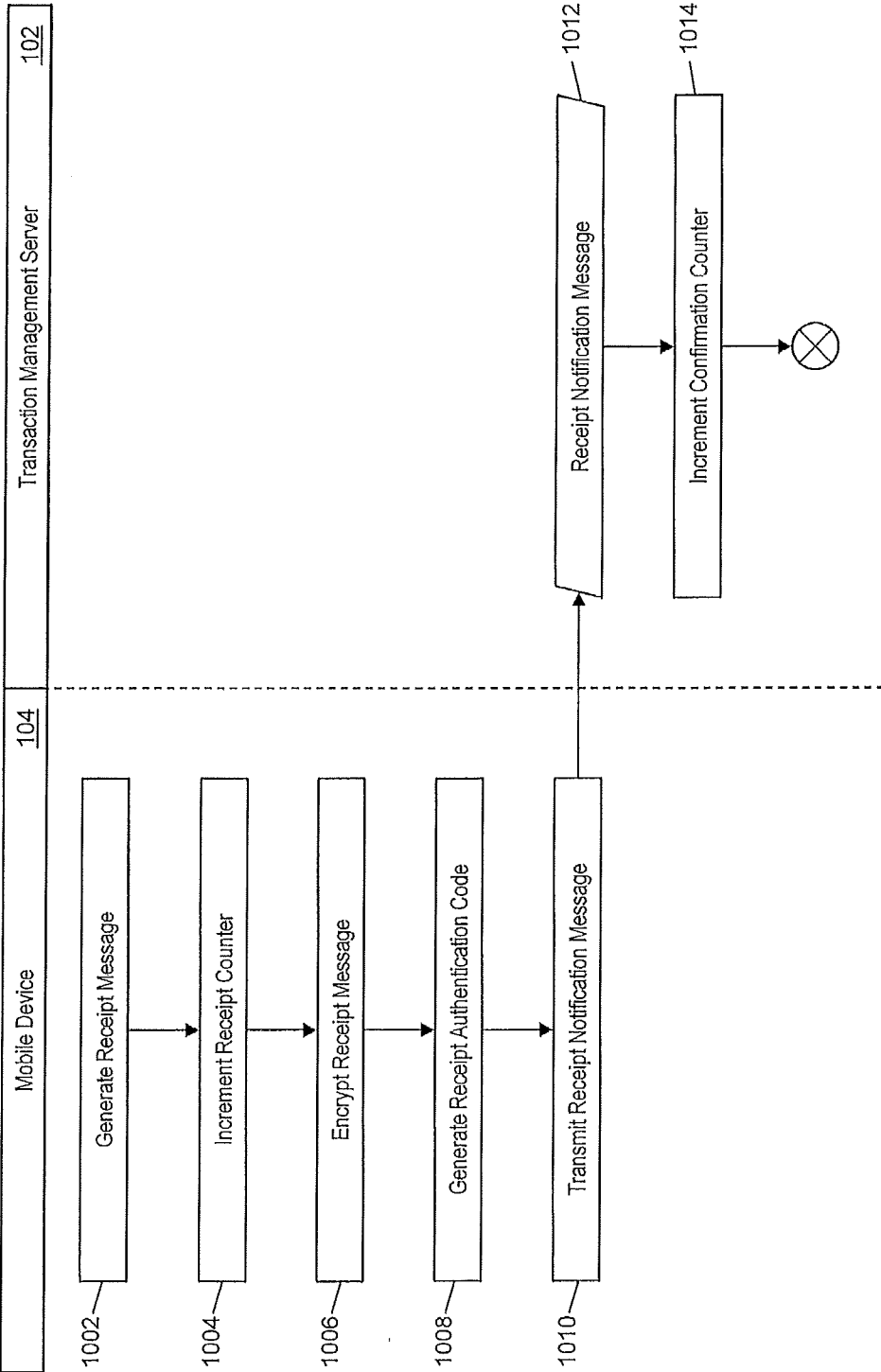


FIG. 10A

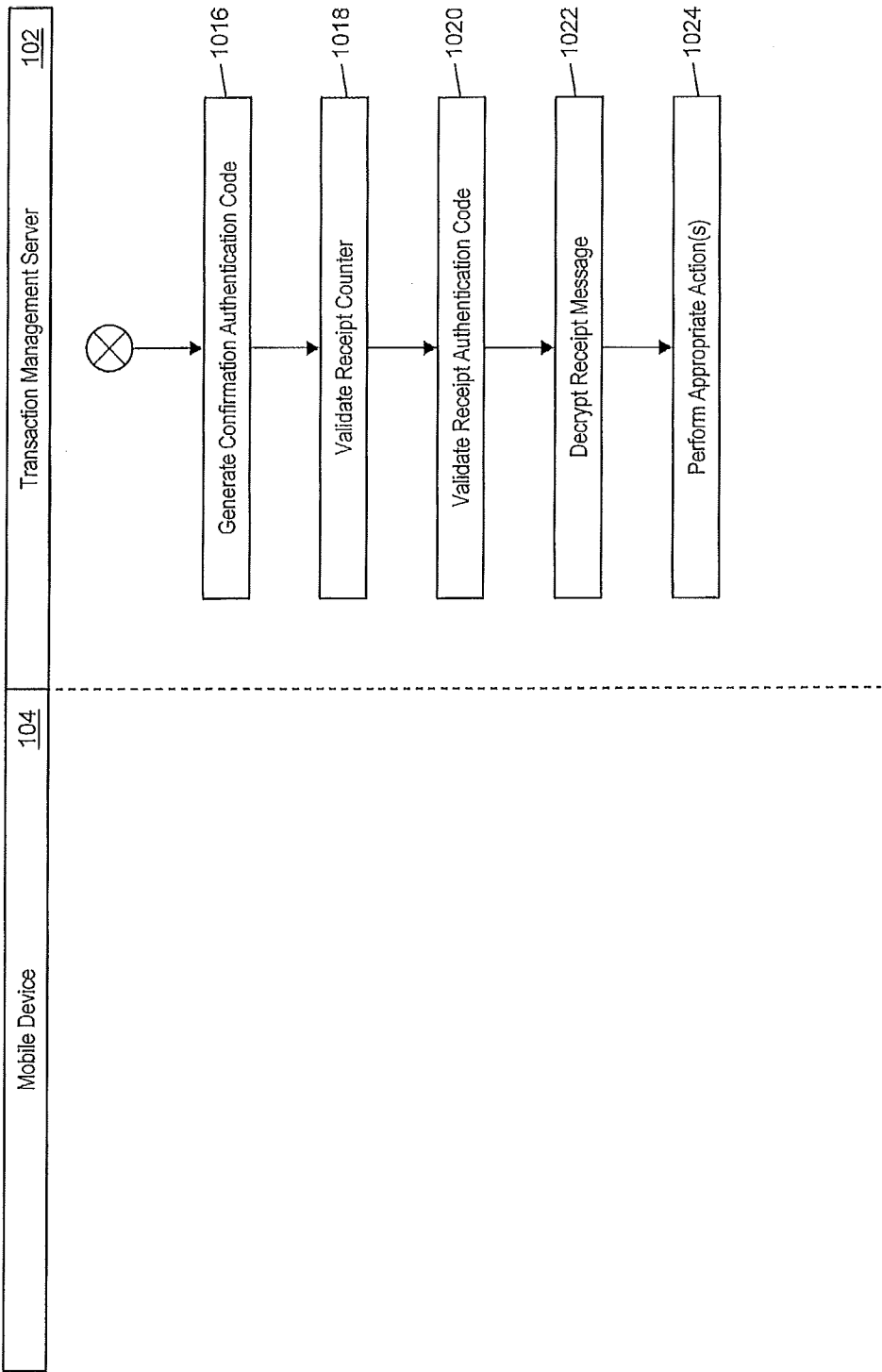


FIG. 10B

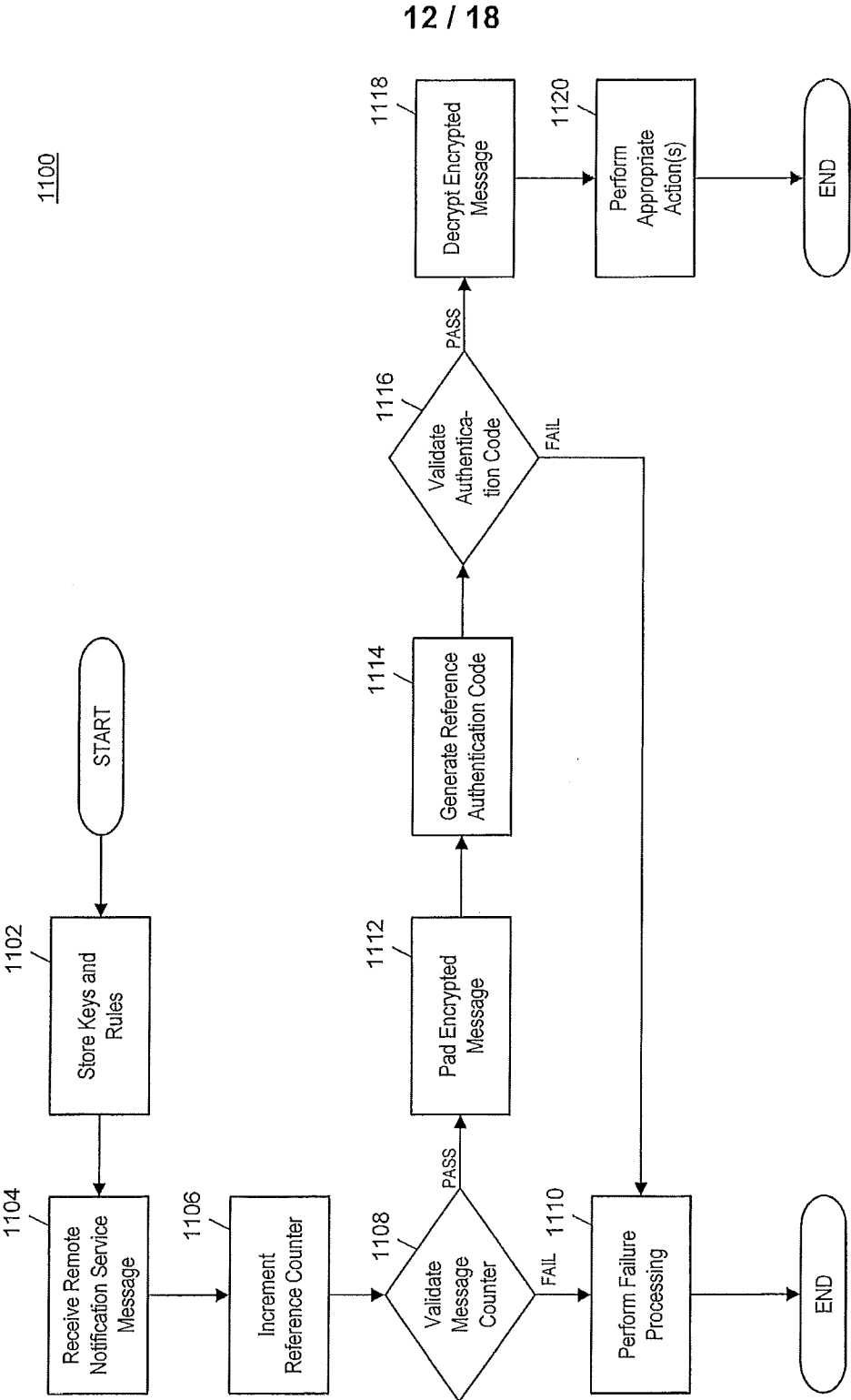


FIG. 11

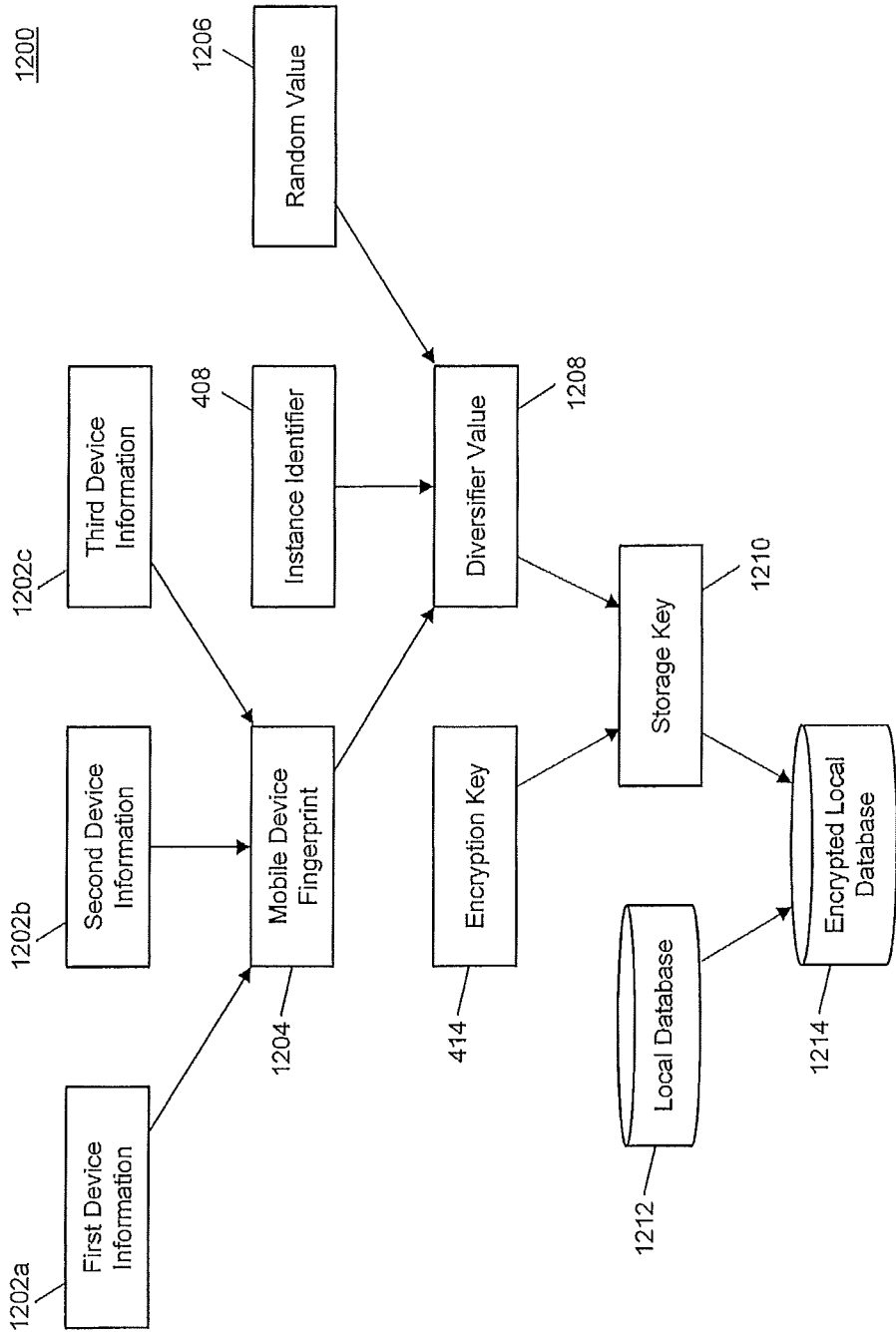


FIG. 12

14 / 18

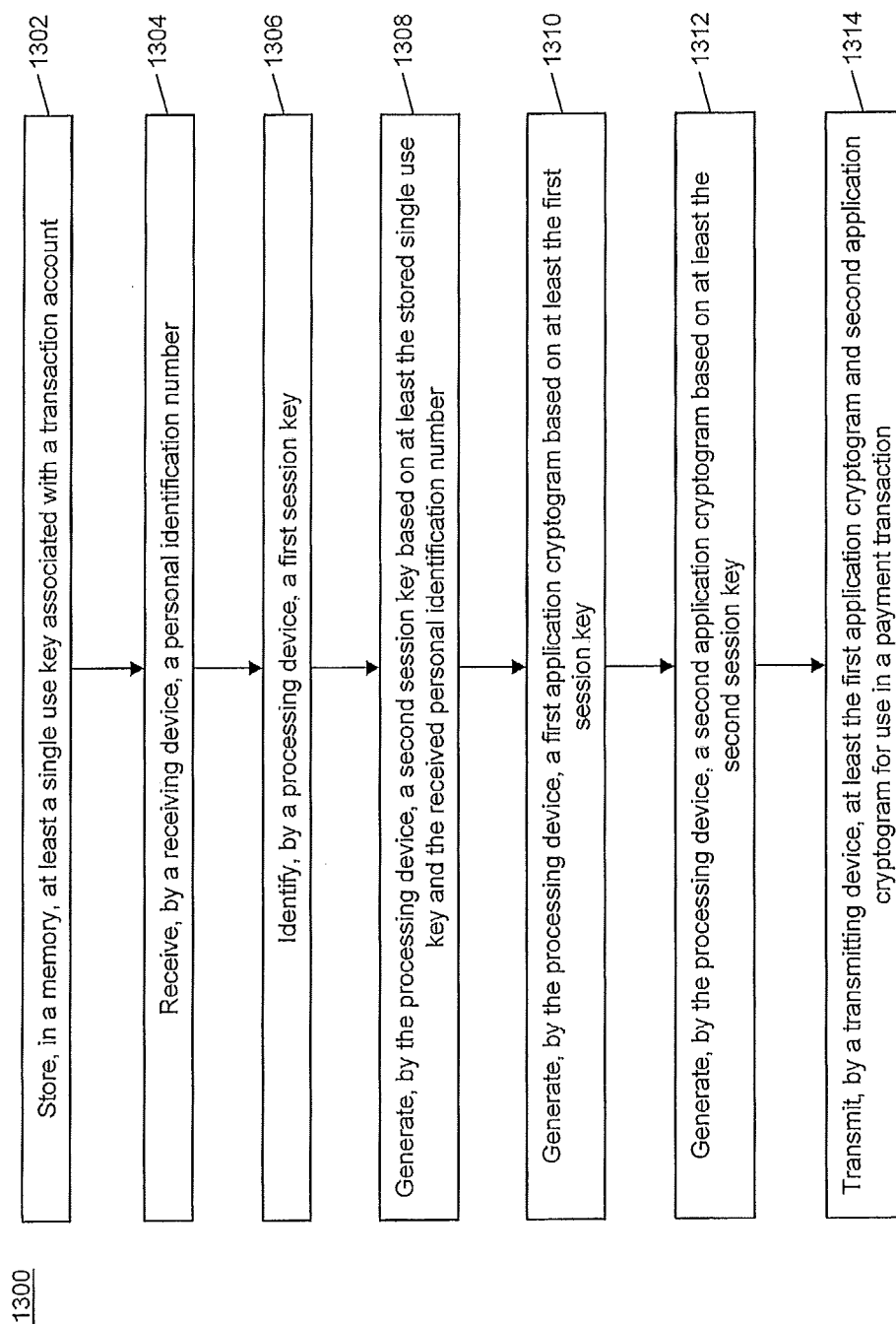


FIG. 13

1400

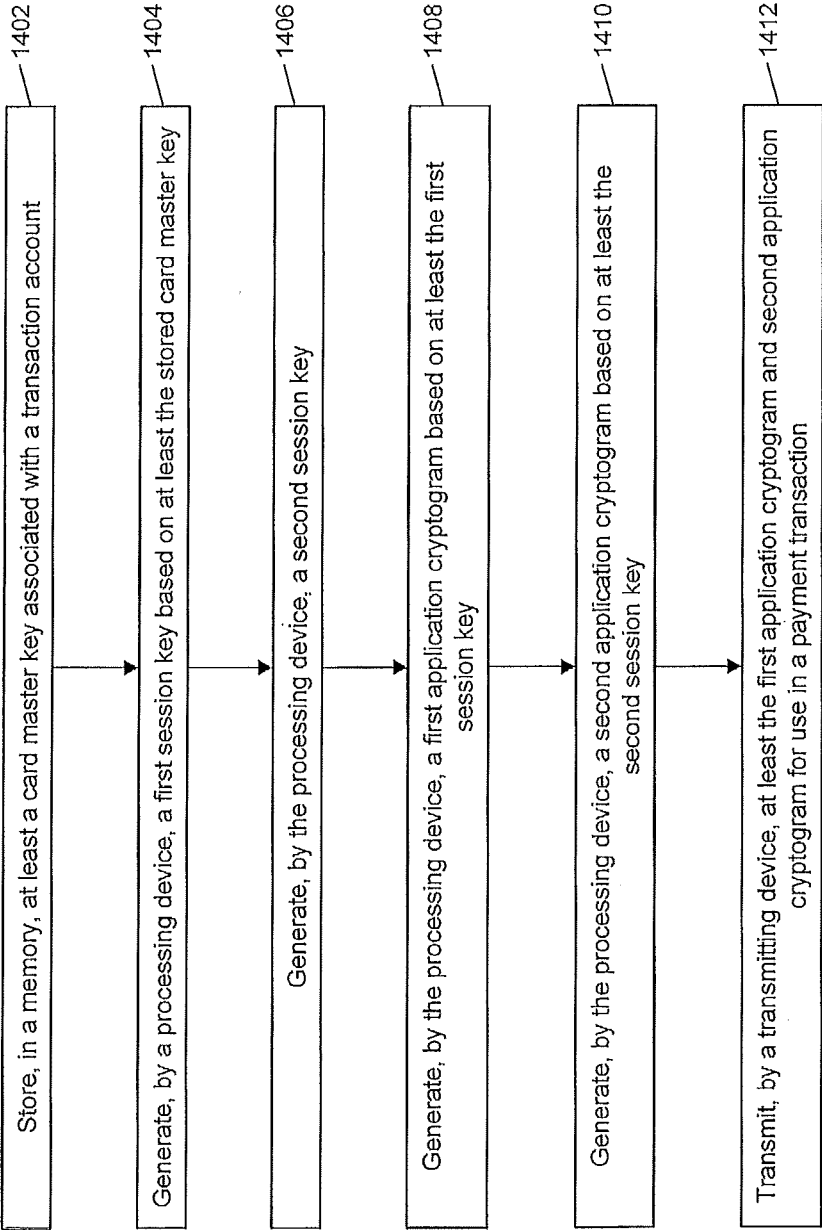


FIG. 14

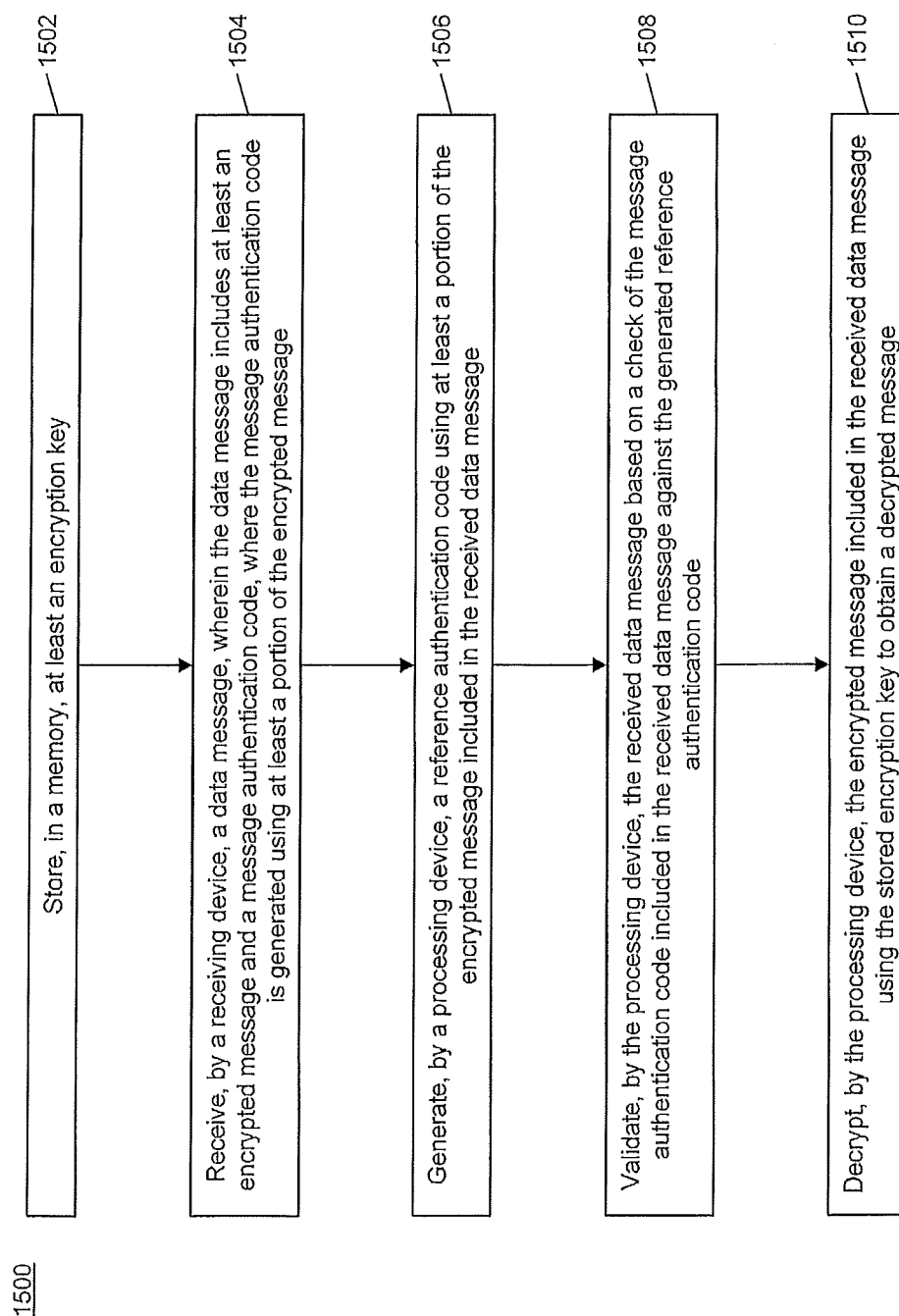


FIG. 15

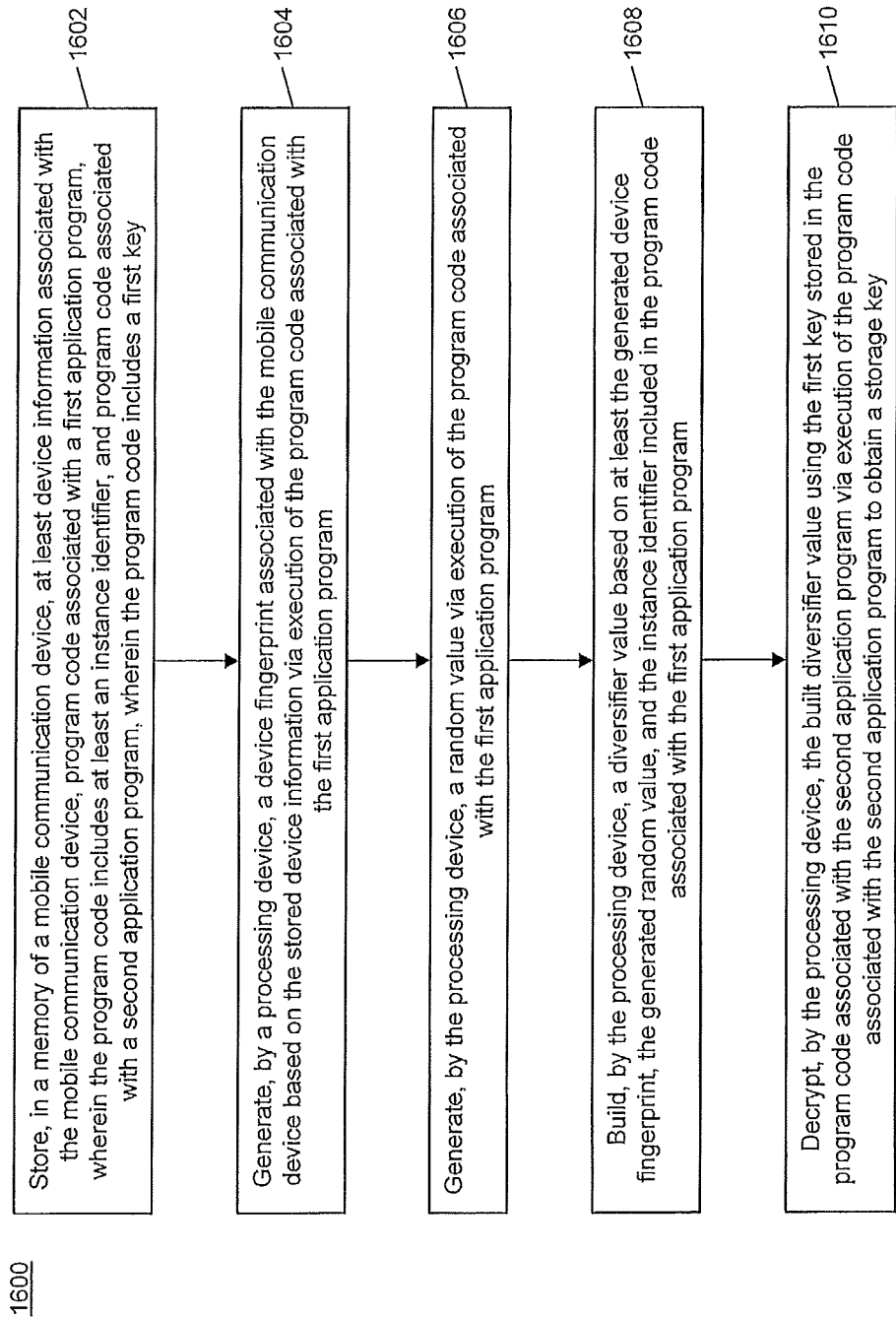


FIG. 16

18 / 18

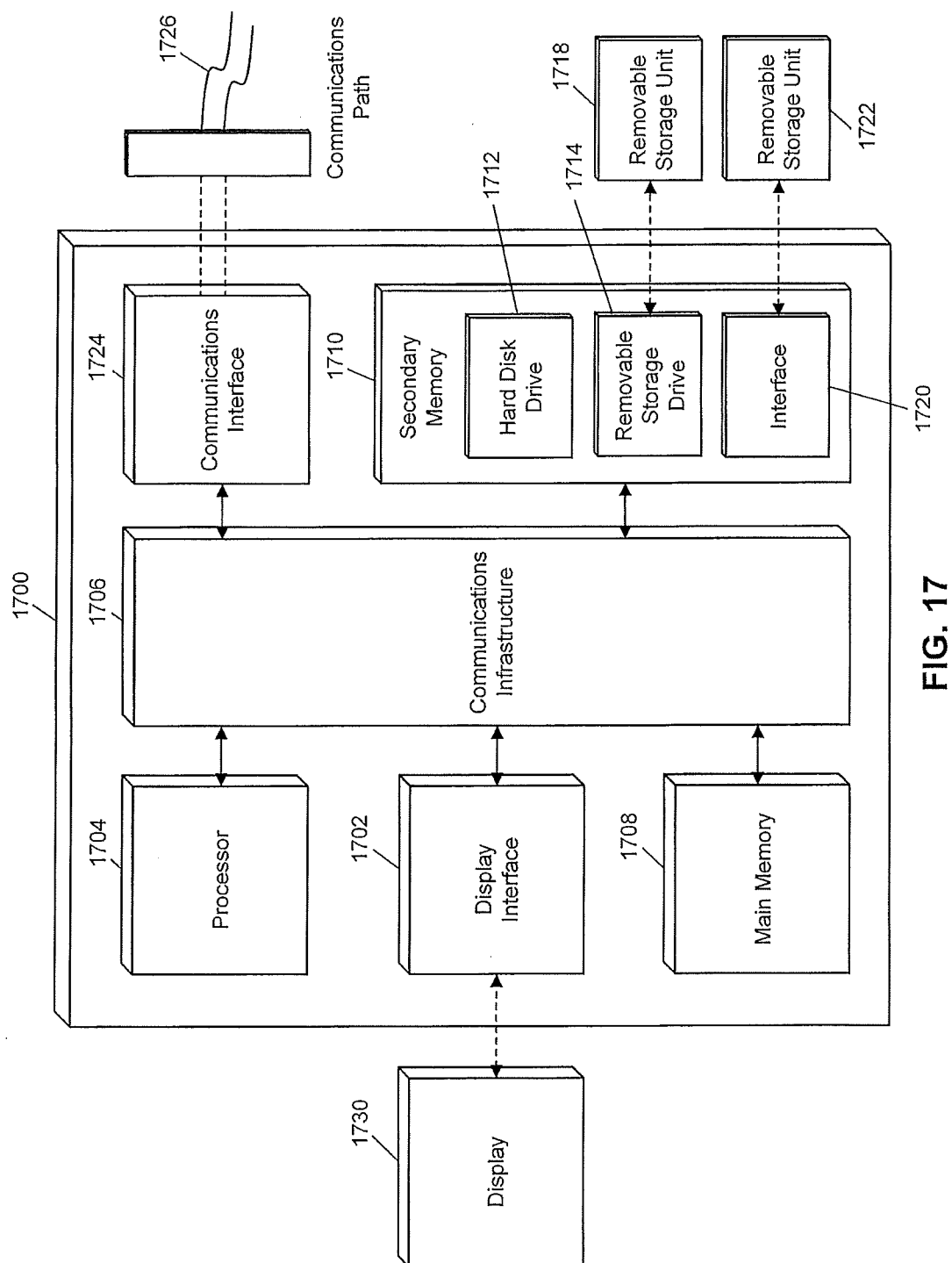


FIG. 17

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2014/068078**A. CLASSIFICATION OF SUBJECT MATTER****H04W 12/08(2009.01)i, H04W 12/06(2009.01)i**

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHEDMinimum documentation searched (classification system followed by classification symbols)
H04W 12/08; H04L 9/08; H04W 28/06; H04L 9/28; H04L 9/32; H04W 12/06Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Korean utility models and applications for utility models
Japanese utility models and applications for utility modelsElectronic data base consulted during the international search (name of data base and, where practicable, search terms used)
eKOMPASS(KIPO internal) & Keywords: key, authentication, code, encrypt*, decrypt***C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	US 2011-0002459 A1 (DAE YOUB KIM) 06 January 2011 See abstract, figures 7,9, paragraphs [0146]-[0149],[0161]-[0164].	1-2, 7, 11-16, 21 ,25-28 3-6, 8-10, 17-20 ,22-24
Y A	KR 10-1256114 B1 (KOREA UNIVERSITY RESEARCH AND BUSINESS FOUNDATION) 23 April 2013 See figure 3 and paragraphs [0065]-[0066].	1-2, 7, 11-16, 21 ,25-28 3-6, 8-10, 17-20 ,22-24
A	US 7702910 B2 (CHRISTIAN GEHRMANN) 20 April 2010 See abstract, figure 7 and claims 1-9.	1-28
A	WO 2013-095074 A1 (SAMSUNG ELECTRONICS CO., LTD.) 27 June 2013 See figures 2-3,6-9 and corresponding detailed description.	1-28

☐ Further documents are listed in the continuation of Box C.☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

13 February 2015 (13.02.2015)

Date of mailing of the international search report

24 February 2015 (24.02.2015)

Name and mailing address of the ISA/KR

International Application Division
Korean Intellectual Property Office
189 Cheongsa-ro, Seo-gu, Daejeon Metropolitan City, 302-701,
Republic of Korea

Facsimile No. ++82 42 472 3473

Authorized officer

YOO, Sun Jung

Telephone No. +82-42-481-5775



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2014/068078

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2011-0002459 A1	06/01/2011	KR 10-2010-0131678 A US 8464070 B2	16/12/2010 11/06/2013
KR 10-1256114 B1	23/04/2013	None	
US 7702910 B2	20/04/2010	AU 2003-268933 A1 AU 2003-276090 A1 CN 1729645 A CN 1729646 A CN 1729646 B DE 60310439 D1 EP 1554834 A1 EP 1554834 B1 EP 1554835 A1 EP 1554835 B1 JP 04-550736B2 JP 04-664206B2 JP 2006-504361A JP 2006-504362A KR 10-1092696 B1 KR 10-1095239 B1 KR 10-1255357 B1 KR 10-2005-0083819A KR 10-2010-0114947A KR 10-2011-0053391 A US 2004-0083368 A1 US 2005-0262418 A1 US 2007-0288753 A1 US 7284127 B2 US 7502930 B2 WO 2004-038998 A1 WO 2004-038999 A1	13/05/2004 13/05/2004 01/02/2006 01/02/2006 29/09/2010 25/01/2007 20/07/2005 13/12/2006 20/07/2005 13/12/2006 22/09/2010 06/04/2011 02/02/2006 02/02/2006 09/12/2011 20/12/2011 17/04/2013 26/08/2005 26/10/2010 20/05/2011 29/04/2004 24/11/2005 13/12/2007 16/10/2007 10/03/2009 06/05/2004 06/05/2004
WO 2013-095074 A1	27/06/2013	CN 104012134 A KR 10-2014-0116144 A US 2014-372758 A1	27/08/2014 01/10/2014 18/12/2014

RESUMEN

Un método para recibir y procesar un mensaje de datos incluye: almacenar por lo menos una llave de cifrado; recibir un
5 mensaje de datos, incluyendo el mensaje de datos un mensaje cifrado y un código de autenticación del mensaje, siendo el código de autenticación del mensaje generado utilizando por lo menos una parte del mensaje cifrado; generar un código de autenticación de referencia utilizando por lo menos una parte del mensaje cifrado
10 incluida en el mensaje de datos recibido; validar el mensaje de datos recibido basándose en una comprobación del código de autenticación del mensaje incluido en el mensaje de datos recibido, contra el código de autenticación de referencia generado; y descifrar el mensaje cifrado incluido en el mensaje de datos recibido
15 utilizando la llave de cifrado almacenada para obtener un mensaje descifrado.

* * * * *

20

25