(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 749 625**

(51) Int. CI.:

G06Q 20/18 (2012.01)
G06Q 20/32 (2012.01)
G06Q 20/36 (2012.01)
G06Q 20/38 (2012.01)
G06Q 20/40 (2012.01)
G07F 19/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **15.05.2014 PCT/IB2014/061471**

(87) Fecha y número de publicación internacional: **20.11.2014 WO14184771**

(96) Fecha de presentación y número de la solicitud europea: **15.05.2014 E 14797103 (0)**

(97) Fecha y número de publicación de la concesión europea: **28.08.2019 EP 2997531**

(54) Título: **Métodos y sistemas para proporcionar credenciales de pago**

(30) Prioridad:

15.05.2013 US 201361823840 P
22.05.2013 ZA 201303719
20.08.2013 ZA 201306249

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.03.2020

(73) Titular/es:

VISA INTERNATIONAL SERVICE ASSOCIATION (100.0%)
P.O. Box 8999
San Francisco, California 94128, US

(72) Inventor/es:

HUXHAM, HORATIO NELSON;
O'REGAN, ALAN JOSEPH;
MOSS, TARA ANNE;
VAN WYK, HOUGH ARIE y
SHEETS, JOHN FOXE

(74) Agente/Representante:

ROEB DÍAZ-ÁLVAREZ, María

DESCRIPCIÓN

Métodos y sistemas para proporcionar credenciales de pago

Campo de la invención

Esta solicitud se refiere al campo de provisión de credenciales de pago usables por un dispositivo móvil.

Antecedentes

A medida que más comerciantes están adoptando terminales punto de venta que son capaces de realizar transacciones con dispositivos móviles, es mucho más probable que consumidores sustituyan sus carteras físicas con aplicaciones de cartera digital que se ejecutan en sus dispositivos móviles (por ejemplo, teléfonos móviles). Transacciones con aplicaciones de cartera digital ejecutándose en un dispositivo móvil pueden ser sin contacto, por ejemplo, usando capacidades de comunicación de campo cercano (NFC) del dispositivo móvil.

Transacciones de pago sin contacto proporcionan una comodidad significativa a consumidores ya que permiten que los consumidores compren más rápida y cómodamente que en un entorno basado en contacto. En una transacción de pago sin contacto, un consumidor lleva un dispositivo de pago portátil de usuario con capacidad sin contacto (CPPD) tal como una tarjeta inteligente sin contacto o un teléfono móvil en proximidad cercana con un terminal de aceptación. Información tal como credenciales de pago se intercambia entre el CPPD sin contacto y el terminal de aceptación de una manera inalámbrica para efectuar la transacción de pago sin requerir contacto físico directo entre el CPPD sin contacto y el terminal de aceptación. En algunos casos, el CPPD sin contacto y el terminal de aceptación no están coubicados, sino que pueden estar en diferentes ubicaciones, por ejemplo, en diferentes ciudades o países. En un caso de este tipo la información se transmite entre el CPPD sin contacto y el terminal de aceptación a través de, por ejemplo, la Internet.

A menudo se requiere por diversas normas o autoridades de cumplimiento que un dispositivo móvil que se emplea como un CPPD sin contacto contenga un elemento seguro. Un elemento seguro de este tipo no es diferente a un circuito integrado seguro usado en CPPD convencionales, tal como tarjetas con circuito integrado seguro. Los elementos seguros que están en comunicación con los dispositivos móviles habitualmente proporcionan una memoria segura y procesador seguro que están separados de la memoria y procesador de dispositivo móvil y pueden accederse únicamente por aplicaciones confiables, a menudo únicamente después de que se ha introducido correctamente un número de identificación personal (PIN) especificado. Los dispositivos móviles en los que se disponen o embeben tales elementos seguros a menudo están equipados con interfaces de comunicaciones de proximidad tal como, por ejemplo, comunicaciones de campo cercano (NFC).

Es en esta memoria segura que puede almacenarse información, tal como credenciales de pago. En algunos casos, la provisión de tales credenciales de pago a la memoria segura del dispositivo móvil puede ser a través de los métodos de durante comunicaciones aéreas (OTA) que se originan desde un gestor de servicios confiable (TSM). Tales TSM se operan habitualmente desde centros de datos seguros de tal forma que el proceso cumple con las normas de seguridad impuestas por normas pertinentes o autoridades de cumplimiento.

La provisión de aplicaciones de cartera digital en dispositivos móviles puede ser una tarea complicada. Por ejemplo, para provisión un dispositivo móvil con las credenciales para realizar transacciones sin contacto tal como transacciones de pago sin contacto, puede requerirse a los usuarios que accedan a un proveedor de servicios de transacciones sin contactos desde su dispositivo móvil para efectuar un proceso de provisión de OTA. El proceso de OTA puede requerir que el usuario introduzca manualmente credenciales de usuario tal como números de cuenta. Ya que la mayoría de consumidores probablemente tienen muchos instrumentos de almacenamiento de credenciales tal como tarjetas de crédito/débito de diferentes bancos que el usuario querría incluir en la aplicación de cartera digital, introducir esta información para todos los instrumentos de almacenamiento de credenciales de un usuario puede ser un proceso que lleve mucho tiempo. Adicionalmente, el proceso de provisión de OTA puede generar cargos indeseados de uso de datos inalámbricos para el usuario.

Realizaciones de la invención tienen por objetivo abordar estos y otros problemas individual y colectivamente, al menos hasta cierto punto.

Breve sumario

De acuerdo con un primer aspecto de la presente invención se proporciona un método para proporcionar credenciales de pago usables por un dispositivo móvil en la realización de un pago como se define en la reivindicación 1.

El método puede incluir adicionalmente: cifrar las credenciales de pago recibidas, teniendo las credenciales de pago cifradas una clave de descifrado única. Las credenciales de pago pueden comunicarse en forma cifrada con la clave de descifrado única almacenándose en el sistema de provisión. En un ejemplo, comunicar una derivación de las

credenciales de pago comunica la clave de descifrado única y las credenciales de pago cifradas se almacenan en el sistema de provisión. En el caso en el que se comunica la clave de descifrado única, la clave de descifrado única puede purgarse desde el sistema de provisión.

En las realizaciones del método, el sistema de provisión es un servidor accesible de forma remota de una autoridad emisora, una pasarela de seguridad o gestor de servicios confiable, y en el que comunicar las credenciales de pago o una derivación de las credenciales de pago al dispositivo móvil identificado o el elemento seguro usa un canal seguro de comunicación.

En realizaciones alternativas del método, el sistema de provisión es un quiosco que tiene un procesador local al dispositivo de recepción, y en el que el método incluye: establecer un canal de comunicación entre el quiosco y el dispositivo móvil para comunicar las credenciales de pago o una derivación de las credenciales de pago. El quiosco puede actuar como un intermediario para un servidor accesible de forma remota y el método puede incluir el uso del identificador recibido para identificar y/o verificar un usuario o cuenta en un servidor accesible de forma remota.

El método puede incluir: solicitar autorización desde un gestor de servicios confiable para acceder a un elemento seguro; y recibir una clave de seguridad para acceder al elemento seguro.

El método puede incluir adicionalmente: comunicar credenciales adicionales al dispositivo móvil identificado o el elemento seguro a almacenar de forma segura en asociación con el dispositivo móvil, en el que las credenciales adicionales se requieren en uso además de las credenciales de pago o derivación de las credenciales de pago que efectúan una transacción. En una realización, las credenciales adicionales pueden ser valores de verificación de tarjeta. En otra realización, las credenciales adicionales pueden ser en forma de una aplicación o algoritmo de verificación dinámico para generar valores de verificación dinámicos. El método puede incluir obtener las credenciales adicionales de un servidor accesible de forma remota usando el identificador y reenviar las credenciales adicionales al dispositivo móvil.

El dispositivo de recepción puede ser uno del grupo de: un lector de tarjetas asociado con un quiosco, un dispositivo de punto de venta, un cajero automático, un terminal de punto de venta de comerciante o un dispositivo de entrada de PIN personal (PPED).

El dispositivo de pago portátil puede ser uno del grupo de: una tarjeta de débito o crédito con banda magnética, una tarjeta de débito o crédito con circuito integrado de seguridad, una tarjeta bancaria, una tarjeta bancaria sin contacto, una tarjeta de abono, una credencial de pago existente almacenada en un dispositivo móvil.

Las credenciales de pago recibidas pueden incluir recibir uno o más de datos de pista 1, datos de pista 2, datos de pista 3 y datos equivalentes de pista 2. Las credenciales de pago recibidas pueden incluir uno o más del grupo de: datos de pista, un número cuenta, nombre de titular de cuenta y/o fecha de nacimiento, un número de identificación bancaria (BIN), un número de cuenta primario (PAN), un código de servicio, una fecha de expiración, valores de verificación de tarjeta (CVV1 o CVV2), detalles personales de un titular de cuenta, un bloque o intervalo de PIN, un número de cuenta bancaria, un código de sucursal, un número de cuenta o identificador de fidelidad, información de número de tarjeta de crédito y/o débito, información de saldo de cuenta.

El identificador puede ser uno o más del grupo de: un número de directorio de abonados internacional de estación móvil (MSISDN), una dirección de correo electrónico, un identificador de red social, un nombre de consumidor predefinido, un número de cuenta de consumidor.

La etapa de recepción de credenciales de pago y la etapa de recepción de un identificador pueden incluir recibir un único mensaje de transacción segura que contiene las credenciales de pago y el identificador. El mensaje de transacción segura puede ser uno del grupo de: un mensaje de red de procesamiento de pago, un mensaje de transacción financiera, un mensaje de transacción financiera en forma de un mensaje ISO 8583, un mensaje de transacción financiera que contiene un código de encaminamiento de servidor. El código de encaminamiento de servidor puede usarse para encaminar el mensaje de transacción financiera al servidor accesible de forma remota mediante una red de procesamiento de pago.

Identificar un dispositivo móvil o un elemento seguro que corresponde al identificador puede incluir: determinar si un dispositivo móvil o elemento seguro que corresponde al identificador se ha registrado o no con un servidor accesible de forma remota y, si el dispositivo móvil o se ha registrado, identificar una correspondiente dirección de comunicación del dispositivo móvil y/o elemento seguro.

Características adicionales proporcionan la etapa de identificación de un dispositivo móvil que corresponde al identificador para incluir la etapa de uso del identificador para consultar una base de datos para obtener una dirección de comunicación del dispositivo asociado móvil con el identificador. Características adicionales proporcionan la etapa de comunicación de las credenciales de pago al dispositivo móvil para incluir comunicar las credenciales de pago al dispositivo móvil usando la dirección de comunicación.

Comunicar las credenciales de pago o una derivación de las credenciales de pago al dispositivo móvil identificado a almacenar de forma segura en asociación con el dispositivo móvil, puede incluir: comunicar las credenciales de pago o una derivación de las credenciales de pago al dispositivo móvil a almacenar en un elemento seguro, en el que el elemento seguro es uno del grupo de: un elemento seguro proporcionado en el dispositivo móvil, un elemento seguro embebido en una capa que se sitúa entre un componente de comunicación del dispositivo móvil y una interfaz de componente de comunicación del dispositivo móvil, un elemento seguro proporcionado en un componente de comunicación del dispositivo móvil, un elemento seguro basado en la nube asociado con el dispositivo móvil. En una realización, el elemento seguro puede embeberse en una etiqueta, tarjeta o placa y que se sitúa entre un componente de comunicación del dispositivo móvil y una interfaz de componente de comunicación del dispositivo móvil,

El método puede repetirse para múltiples credenciales de pago a almacenar de forma segura en asociación con un único dispositivo móvil.

El método puede usarse para transferir credenciales de pago a un segundo dispositivo móvil desde su almacenamiento seguro existente en un primer dispositivo móvil, en el que el dispositivo de pago portátil es una credencial de pago existente almacenada de forma segura en el primer dispositivo móvil.

De acuerdo con segundo aspecto de la presente invención se proporciona un método para proporcionar credenciales de pago usables por un dispositivo móvil en la realización de un pago, realizándose el método en un dispositivo de punto de venta y que comprende las etapas como se define en la reivindicación 10.

De acuerdo con un tercer aspecto de la presente invención se proporciona un sistema para proporcionar credenciales de pago usables por un dispositivo móvil en la realización de un pago, incluyendo un sistema de provisión como se define en la reivindicación 11.

El sistema de provisión puede incluir: un componente de cifrado para cifrar las credenciales de pago recibidas, teniendo las credenciales de pago cifradas una clave de descifrado única; y en el que comunicar una derivación de las credenciales de pago comunica la clave de descifrado única.

En ejemplos del sistema, el sistema de provisión es un servidor accesible de forma remota de una autoridad emisora, una pasarela de seguridad, o gestor de servicios confiable, y en el que el módulo de comunicación para comunicar las credenciales de pago o una derivación de las credenciales de pago al dispositivo móvil identificado o el elemento seguro usa un canal seguro de comunicación.

En realizaciones alternativas, el sistema de provisión es un quiosco que tiene un procesador local al dispositivo de recepción, y en el que el quiosco incluye el módulo de comunicación para establecer un canal de comunicación entre el quiosco y el dispositivo móvil para comunicar las credenciales de pago o una derivación de las credenciales de pago. El quiosco puede actuar como un intermediario para un servidor accesible de forma remota y el sistema incluye un servidor módulo de comunicación para usar el identificador recibido para identificar y/o verificar un usuario o cuenta en el servidor accesible de forma remota.

El sistema de provisión puede incluir adicionalmente: un componente de autorización para solicitar autorización desde un gestor de servicios confiable para acceder a un elemento seguro y recibir una clave de seguridad para acceder al elemento seguro.

El sistema de provisión puede incluir adicionalmente: un componente de credenciales adicionales para comunicar credenciales adicionales al dispositivo móvil identificado o el elemento seguro a almacenar de forma segura en asociación con el dispositivo móvil, en el que las credenciales adicionales se requieren en uso además de las credenciales de pago o derivación de las credenciales de pago que efectúan una transacción. En una realización, las credenciales adicionales pueden ser valores de verificación de tarjeta. En otra realización, las credenciales adicionales pueden ser en forma de una aplicación o algoritmo de verificación dinámico para generar valores de verificación dinámicos. El método puede incluir obtener las credenciales adicionales de un servidor accesible de forma remota usando el identificador y reenviar las credenciales adicionales al dispositivo móvil.

El componente de identificación para identificar un dispositivo móvil que corresponde al identificador puede incluir funcionalidad para determinar si un dispositivo móvil o un elemento seguro que corresponde al identificador se ha registrado o no con un servidor accesible de forma remota y, si el dispositivo móvil se ha registrado, identificar una correspondiente dirección de comunicación del dispositivo móvil o elemento seguro.

El módulo de comunicación para comunicar las credenciales de pago o una derivación de las credenciales de pago al dispositivo móvil identificado a almacenar de forma segura en asociación con el dispositivo móvil, incluye funcionalidad para comunicar las credenciales de pago o una derivación de las credenciales de pago al dispositivo móvil a almacenar en un elemento seguro, en el que el elemento seguro es uno del grupo de: un elemento seguro proporcionado en el dispositivo móvil, un elemento seguro embebido en una capa que se sitúa entre un componente de comunicación del dispositivo móvil y una interfaz de componente de comunicación del dispositivo móvil, un

elemento seguro proporcionado en un componente de comunicación del dispositivo móvil, un elemento seguro basado en la nube asociado con el dispositivo móvil.

En realizaciones adicionales, el sistema puede incluir: un dispositivo de punto de venta que comprende: un componente de obtención de credenciales de pago para obtener credenciales de pago desde un dispositivo de pago portátil presentado por un consumidor en el dispositivo de recepción; un receptor de identificador para recibir un identificador introducido por el consumidor en el dispositivo de punto de venta; un módulo de comunicación para comunicar las credenciales de pago e identificador a un servidor accesible de forma remota para comunicación adicional de las credenciales de pago o una derivación de las credenciales de pago a un dispositivo móvil a almacenar de forma segura en asociación con el dispositivo móvil.

En un aspecto adicional de la presente invención, se proporciona un quiosco para permitir que un usuario proporcione a un dispositivo móvil con credenciales desde los instrumentos de almacenamiento de credenciales del usuario también denominados como dispositivos de pago portátiles. El quiosco incluye un lector de instrumento de almacenamiento de credenciales para recuperar credenciales desde un instrumento de almacenamiento de credenciales. El quiosco también incluye una interfaz de dispositivo móvil para establecer un canal de comunicación con un dispositivo móvil, y para cargar credenciales desde el instrumento de almacenamiento de credenciales en el dispositivo móvil a través del canal de comunicación.

De acuerdo con un cuarto aspecto de la presente invención se proporciona un producto de programa informático para proporcionar credenciales de pago usables por un dispositivo móvil en la realización de un pago, comprendiendo el producto de programa informático un medio legible por ordenador que ha almacenado código de programa legible por ordenador para realizar las etapas del primer aspecto de la presente invención y una o más características definidas adicionalmente listadas anteriormente.

De acuerdo con un quinto aspecto de la presente invención se proporciona un producto de programa informático para proporcionar credenciales de pago usables por un dispositivo móvil en la realización de un pago, comprendiendo el producto de programa informático un medio legible por ordenador que ha almacenado código de programa legible por ordenador para realizar las etapas del segundo aspecto de la presente invención y una o más características definidas adicionalmente listadas anteriormente.

Características adicionales de la invención proporcionan que el medio legible por ordenador sea un medio legible por ordenador no transitorio y que el código de programa legible por ordenador sea ejecutable por un circuito de procesamiento.

Para que la invención se entienda más completamente, se describirán ahora implementaciones de la misma con referencia a los dibujos adjuntos.

Breve descripción de los dibujos

La Figura 1 es un diagrama esquemático de una primera realización de un sistema de acuerdo con la presente invención;

La Figura 2 es un diagrama esquemático de que muestra variaciones de la primera realización la Figura 1;

La Figura 3 es un diagrama esquemático de que muestra variaciones de la primera realización la Figura 1;

La Figura 4A es un diagrama de flujo de un método efectuado en un sistema de provisión de acuerdo con la presente invención;

La Figura 4B es un diagrama de flujo de una realización del método de la Figura 4A;

La Figura 5 es un diagrama de flujo de un método efectuado en un dispositivo de punto de venta de acuerdo con la presente invención;

La Figura 6A es un diagrama de bloques de un aspecto de un sistema de acuerdo con la presente invención;

La Figura 6B es un diagrama de bloques de un aspecto de un sistema de acuerdo con la presente invención;

La Figura 7 es un diagrama en carriles de un ejemplo de un método de acuerdo con la presente invención;

La Figura 8 es un diagrama en carriles de otro ejemplo de un método de acuerdo con la presente invención;

La Figura 9A ilustra una segunda realización de un sistema de acuerdo con la presente invención;

La Figura 9B es un diagrama de bloques de un quiosco de la realización del sistema de la Figura 9A;

La Figura 9C es un diagrama esquemático de un sistema de la realización de la Figura 9A;

La Figura 9D es un diagrama de flujo de un método de la realización de la Figura 9A;

La Figura 10 es un diagrama en carriles de la realización de la Figura 9A;

La Figura 11 ilustra un diagrama de bloques de un dispositivo informático en el que pueden implementarse diversos aspectos de la invención; y

La Figura 12 ilustra un diagrama de bloques de un dispositivo de comunicación que puede usarse en diversas realizaciones de la invención.

Descripción detallada

En la siguiente descripción detallada, se exponen numerosos detalles específicos para proporcionar un completo entendimiento de la invención. Sin embargo, se entenderá por los expertos en la materia que la presente invención puede practicarse sin estos detalles específicos. En otros casos, métodos bien conocidos, procedimientos y componentes no se han descrito en detalle para no obstaculizar la presente invención.

Se describen métodos y sistemas para proporcionar credenciales de pago o derivaciones de credenciales de pago usables por un dispositivo móvil en la realización de un pago sin contacto.

Realizaciones de la invención incluyen un método efectuado en un servidor accesible de forma remota para proporcionar credenciales de pago o derivaciones de las mismas a un dispositivo móvil a través de un dispositivo de recepción en el que puede introducirse un dispositivo de pago portátil o instrumento de almacenamiento de credenciales tal como una tarjeta de pago. El dispositivo de recepción puede ser, por ejemplo, un dispositivo de punto de venta, un cajero automático u otro dispositivo intermediario.

Las credenciales de pago pueden proporcionarse de forma segura al dispositivo móvil desde el servidor accesible de forma remota a través de canales a un elemento seguro asociado con el dispositivo móvil.

Las credenciales de pago pueden proporcionarse al dispositivo móvil o, como alternativa, las credenciales de pago pueden almacenarse en el servidor accesible de forma remota en una forma cifrada y puede proporcionarse una clave de descifrado única al dispositivo móvil.

Otras realizaciones de la invención proporcionan un quiosco para permitir que un usuario proporcione un dispositivo móvil con credenciales desde los instrumentos de almacenamiento de credenciales del usuario. Proporcionando un quiosco como una interfaz entre el dispositivo móvil del usuario y los instrumentos de almacenamiento de credenciales del usuario, puede evitarse la introducción manual de las credenciales porque tales credenciales pueden leerse directamente desde los instrumentos de almacenamiento de credenciales del usuario. Adicionalmente, el quiosco puede actuar como un intermediario de comunicación entre el dispositivo móvil y entidades implicadas en el proceso de provisión tal como un emisor o un gestor de servicios confiable para evitar uso de datos inalámbricos en el dispositivo móvil durante el proceso de provisión. Por lo tanto, realizaciones de la presente invención proporcionan una forma cómoda y rentable para habilitar dispositivos móviles con aplicaciones de cartera digital para su uso en transacciones sin contacto.

Estas realizaciones y realizaciones adicionales se describen ahora en detalle.

La Figura 1 ilustra un diagrama de bloques de un sistema ilustrativo (100) de acuerdo con realizaciones de la invención. El sistema incluye un dispositivo móvil (112) y un dispositivo de pago portátil (114) de un consumidor (102). El sistema incluye adicionalmente un dispositivo de recepción para el dispositivo de pago portátil (114) y, en esta realización, el dispositivo de recepción es en forma de un dispositivo de punto de venta (120). El sistema incluye adicionalmente un servidor accesible de forma remota (140) que, en el sistema ilustrativo (100), está en comunicación con el dispositivo de punto de venta (120) a través de una red de procesamiento de pago (130). Mientras la figura únicamente muestra un consumidor (102), un dispositivo móvil (112), un dispositivo de pago portátil (114) y un dispositivo de punto de venta (120), se apreciará que esto es puramente para propósitos de ilustración y que la invención prevé uno o más de cada uno.

El dispositivo móvil (112) puede ser cualquier dispositivo móvil adecuado que tiene un elemento seguro (113). El elemento seguro (113) puede embeberse en el dispositivo móvil, disponerse dentro de un factor de forma de tarjeta digital segura (SD) mini o similar que se sitúa en una ranura de tarjeta SD mini del dispositivo móvil (112).

Como alternativa, el elemento seguro (113) puede disponerse dentro de un componente de comunicación del dispositivo móvil, tal como una tarjeta de circuito integrado universal (UICC). También se prevé que en algunas realizaciones el elemento seguro (113) puede disponerse en un dispositivo de expansión puede conectarse a un

dispositivo móvil o como alternativa disponerse dentro del mismo, por ejemplo una etiqueta, placa o tarjeta que se sitúa a continuación entre una UICC y una interfaz de UICC del dispositivo móvil de tal forma que el elemento seguro puede interceptar y procesar apropiadamente cualquier comunicación enviada entre la UICC y el dispositivo móvil y en consecuencia, entre el dispositivo móvil y una red de comunicación móvil.

Se prevé adicionalmente que el elemento seguro (113) puede ser un elemento seguro basado en la nube usando emulación de tarjeta del sistema (HCE) que habilita almacenamiento accesible por red externo al dispositivo móvil (112) con una aplicación en el dispositivo móvil (112) configurado para emular las funciones de tarjeta.

Dispositivos móviles ilustrativos incluyen teléfonos inteligentes, teléfonos básicos, ordenadores de tableta, asistentes digitales personales o similares. El dispositivo móvil (112) está en comunicación de datos con el servidor accesible de forma remota a través de, por ejemplo una red de datos móviles o de comunicación móvil, y se configura al menos para recibir de forma segura, almacenar, lanzar y transmitir credenciales de pago o derivaciones de credenciales de pago. Por ejemplo, el dispositivo móvil (112) puede ser cualquier dispositivo de este tipo que cumple con normas de esquemas de pago o financieros, tal como, por ejemplo, la Especificación de Tarjetas de Global Platform. Realizaciones de la invención proporcionan que una aplicación de software móvil apropiada esté residente en el dispositivo móvil (112) que permite que un usuario de la misma interactúe con el elemento seguro (113) se acople a la misma, o asocie con la misma en una arquitectura basada en la nube, y que también puede facilitar comunicaciones entre el dispositivo móvil (112) y el elemento seguro (113).

La aplicación de software puede proporcionar: una interfaz de usuario para facilitar la introducción de una clave de acceso en el dispositivo móvil (112) a comparar con un intervalo almacenado en el elemento seguro (113); una lista de la que usuarios pueden seleccionar credenciales de pago a usar; notificaciones de recepción o uso o credenciales de pago o similar. La interfaz de usuario puede incluir un menú desde el que pueden iniciarse al menos algunas de estas comunicaciones. Ejemplos de la invención proporcionan adicionalmente que una interfaz de este tipo se proporcione por una implementación de protocolo de conjunto de herramientas de aplicación SIM (comúnmente denominada como el protocolo STK) o similar.

El dispositivo de pago portátil (114) en la realización ilustrada es una tarjeta bancaria de circuito integrado de seguridad. Tales tarjetas también se conocen como tarjetas de 'chip y pin' o 'tarjetas inteligentes EMV'. El dispositivo de pago portátil (114) tiene credenciales de pago, que pueden ser información de pista 2 y/o equivalente de pista 2 (tal como datos de etiqueta 57 de EMV), almacenadas en el mismo. Información de pista 2 y/o equivalente de pista 2 puede incluir un número de identificación bancaria (BIN), un número de cuenta primario (PAN), una fecha de expiración, un código de servicio, datos discrecionales tal como valores de verificación de tarjeta (CVV) así como cualquier comprobación de espacio y redundancia. Además de esto, ejemplos de la invención proporcionan que el dispositivo de pago portátil (114) contenga credenciales de pago que pueden incluir uno cualquiera o más de un nombre de cliente y/o fecha de nacimiento, un BIN, un PAN, un código de servicio, una fecha de expiración, números CVV1 o CVV2, un bloque o intervalo de PIN, un número de cuenta bancaria, un código de sucursal, un número de cuenta o identificador de fidelidad, información de número de tarjeta de crédito y/o débito, información de saldo de cuenta y/u otra información de consumidor. En otros ejemplos de la invención, las credenciales de pago pueden incluir información de pista 1 y/o pista 3.

El dispositivo de punto de venta (120) puede ser cualquier dispositivo adecuado configurado para obtener credenciales de pago desde dispositivos de pago portátiles apropiados y para comunicar estas credenciales de pago a una red de procesamiento de pago o red de entidad financiera. El dispositivo de punto de venta (120) puede configurarse para obtener credenciales de pago desde dispositivos de pago portátiles a través de cualquier interfaz de comunicaciones apropiada con o sin contacto que puede ser, por ejemplo, normas ISO/IEC 7813, ISO/IEC 7816 o ISO/IEC 14443 donde corresponda.

El dispositivo de punto de venta (120) puede incluir uno o más de diversos medios para recuperar información desde un dispositivo de pago portátil que incluye que el usuario sitúe el dispositivo de pago portátil (114) en contacto físico con el dispositivo de punto de venta (120), por ejemplo, deslizando o insertando una tarjeta de banda magnética en un lector de banda magnética, o insertando una tarjeta con chip en una ranura de lector de tarjeta con chip, o el usuario situando el dispositivo de pago portátil (114) en proximidad cercana con el dispositivo de punto de venta (120), por ejemplo, situando una tarjeta sin contacto en proximidad cercana a un lector de tarjeta sin contacto, o situando un medio impreso, por ejemplo, con un código de barras o código de respuesta rápida (QR) frente a un escáner de infrarrojos.

En el sistema ilustrativo (100) ilustrado, el dispositivo de punto de venta (120) es un dispositivo de punto de venta de mano. Además de esto, el dispositivo de punto de venta (120) se configura para recibir un identificador introducido por un consumidor a través de, por ejemplo, un teclado numérico del dispositivo de punto de venta (120).

El dispositivo de punto de venta (120) se configura adicionalmente para formatear las credenciales de pago así como el identificador en un mensaje de transacción financiera y para comunicar este mensaje a la red de procesamiento de pago (130). El mensaje de transacción financiera puede ser, por ejemplo, un mensaje ISO 8583. Adicionalmente, el dispositivo de punto de venta (120) se configura para insertar un código de encaminamiento de

servidor en el mensaje de transacción financiera de tal forma que el mensaje de transacción financiera se encamina al servidor accesible de forma remota (140) mediante la red de procesamiento de pago (130) usando el código de encaminamiento de servidor. El código de encaminamiento de servidor puede situarse en el campo 'BIN' del mensaje de transacción financiera.

La red de procesamiento de pago (130) es una red de entidades financieras y entidades de procesamiento de pagos y se configura para encaminar mensajes de transacciones financieras entre, por ejemplo, comerciantes, adquirentes y emisores, entre otros. Un ejemplo de una red de procesamiento de pago de este tipo es VisaNet™ que tiene una pluralidad de entidades financieras adquirentes y emisoras que son una parte de la red.

El servidor accesible de forma remota (140) puede ser cualquier ordenador de servidor apropiado o sistema informático de servidor distribuido y tiene una base de datos (142) almacenada en una memoria digital en el mismo y también tiene una memoria segura que, en una realización preferida está dentro de un módulo de seguridad de hardware (144) del servidor accesible de forma remota. El servidor accesible de forma remota (140) se configura para recibir credenciales de pago desde un dispositivo de punto de venta (por ejemplo 120), en el que las credenciales de pago se han obtenido desde un dispositivo de pago portátil (por ejemplo 114) presentado por un consumidor (por ejemplo 102) en el dispositivo de punto de venta (120).

El servidor accesible de forma remota puede configurarse para cifrar las credenciales de pago, teniendo las credenciales de pago cifradas una clave de descifrado única. El cifrado puede realizarse en el módulo de seguridad de hardware (144). En un ejemplo, la clave para descifrar las credenciales de pago se mantiene por el servidor accesible de forma remota (140) y las credenciales de pago cifradas se envían al dispositivo móvil (112) para almacenamiento en el elemento seguro (114) asociado con el dispositivo móvil (112). En otro ejemplo, las credenciales de pago cifradas se almacenan en el módulo de seguridad de hardware (144) del servidor accesible de forma remota (140) y la clave de descifrado se envía al dispositivo móvil (112) para almacenamiento en el elemento seguro (113) asociado con el dispositivo móvil (112).

Además de esto, el servidor accesible de forma remota (140) se configura para recibir un identificador desde el dispositivo de punto de venta (120) que se introduce por el consumidor (102) en el dispositivo de punto de venta (120). El servidor accesible de forma remota (140) se configura para identificar a continuación un dispositivo móvil (por ejemplo 112), o un elemento seguro (113) asociado con un dispositivo móvil (112), que corresponde al identificador y para comunicar las credenciales de pago al dispositivo móvil (112) a almacenar en un elemento seguro (113) asociado con el dispositivo móvil (112).

Esto puede realizarse usando el identificador para consultar la base de datos (142) para obtener una dirección de comunicación del dispositivo móvil (112) asociado con el identificador. Las credenciales de pago pueden enviarse a continuación al dispositivo móvil (112) usando la dirección de comunicación. El identificador recibido por el servidor accesible de forma remota puede ser, por ejemplo, uno cualquiera o más de un número de directorio de abonados internacional de estación móvil (MSISDN), una dirección de correo electrónico, un identificador de red social, un nombre de consumidor predefinido, un número de cuenta de consumidor o similar. La dirección de comunicación del dispositivo móvil puede ser similarmente, por ejemplo, uno cualquiera o más de un MSISDN, una dirección de correo electrónico, un identificador de red social, un nombre de consumidor predefinido, un número de cuenta de consumidor o similar. El identificador y dirección de comunicación pueden ser el mismo.

Realizaciones de la invención proporcionan que el servidor accesible de forma remota se configure para asociar uno o más del grupo de: el identificador; clave de descifrado; credenciales de pago cifradas; y dirección de comunicación con un perfil de usuario en la base de datos.

En algunas realizaciones de la invención la función desempeñada por el servidor accesible de forma remota (140) puede ser similar a la de un gestor de servicios confiable (TSM) y por consiguiente puede cumplir con cualquier requisito de seguridad o identidad de datos impuesto por normas de esquemas de pago y financieros relevantes, tal como, por ejemplo, la especificación de tarjetas de Global Platform.

En uso, un consumidor (102) puede desear proporcionar sus credenciales de pago o una derivación de las mismas a un elemento seguro (113) en su dispositivo móvil (112) de tal forma que el dispositivo móvil (112) puede usarse para realizar pago sin contactos en comerciantes físicos o comerciantes en línea.

Para hacer esto, el consumidor, que ya ha registrado su dispositivo móvil (112) con el servidor accesible de forma remota (140) y asociado el mismo con un identificador y dirección de comunicación, visita, por ejemplo, un comerciante físico y presenta al comerciante su dispositivo de pago portátil (114). El dispositivo de pago portátil (114) se interconecta con un dispositivo de punto de venta (120) del comerciante y se selecciona, por ejemplo, una opción de menú de 'transferencia de credenciales' en el dispositivo de punto de venta (120). Puede avisarse al consumidor (102) que introduzca un PIN que él o ella introduce en el dispositivo de punto de venta (120), a continuación de lo cual, puede avisarse al consumidor (102) que introduzca su identificador. El consumidor (102) introduce su identificador predeterminado, que se ha registrado con el servidor accesible de forma remota (140), en el dispositivo de punto de venta (120).

Habiendo recibido el PIN del consumidor, el dispositivo de punto de venta (120) es capaz de extraer credenciales de pago del dispositivo de pago portátil (114). El dispositivo de punto de venta (120) formatea las credenciales de pago en un mensaje de transacción financiera. El dispositivo de punto de venta (120) también puede incluir el identificador en el mensaje de transacción financiera así como un código de encaminamiento de servidor. El código de encaminamiento de servidor puede ser similar a un BIN y asegura que el mensaje de transacción financiera se encamina al servidor accesible de forma remota (140) mediante la red de procesamiento de pago (130).

El mensaje de transacción financiera se recibe en el servidor accesible de forma remota (140). El servidor accesible de forma remota usa el identificador contenido en el mensaje de transacción financiera para identificar una dirección de comunicación de un dispositivo móvil (112) asociado. El servidor accesible de forma remota (140) usa la dirección de comunicación para comunicar las credenciales de pago o una derivación de las credenciales de pago al dispositivo móvil (112) para almacenamiento en el elemento seguro (113) asociado con el mismo.

Las credenciales de pago se reciben a continuación por el dispositivo móvil (112) y almacenan de forma segura en el elemento seguro (113) del dispositivo móvil (112). Puede avisarse al usuario para un PIN antes de que las credenciales de pago se almacenen en el elemento seguro. En algunos ejemplos las credenciales de pago se proporcionan al dispositivo móvil (112) desde el servidor accesible de forma remota (140) y almacenan en el elemento seguro (113) a través de provisión durante la comunicación (OTA). Esto por consiguiente puede habilitar que el usuario haga pago sin contactos usando su dispositivo móvil (112) como un dispositivo de pago portátil sin contacto, en el que las credenciales proporcionadas por el dispositivo móvil (112) al dispositivo de punto de venta apropiadamente configurado del comerciante son las del dispositivo de pago portátil (114) del usuario.

En algunos ejemplos, el servidor accesible de forma remota (140) puede cifrar las credenciales de pago y una clave de descifrado única puede asociarse con las credenciales de pago. Una de las credenciales de pago cifradas o la clave de descifrado puede almacenarse a continuación en memoria segura, tal como un módulo de seguridad de hardware (144) del servidor accesible de forma remota. La otra de las credenciales de pago cifradas o la clave de descifrado puede enviarse al elemento seguro (113) asociado con el dispositivo móvil (112). Las credenciales de pago pueden cifrarse usando cualquier algoritmo de encriptación apropiado de tal forma que, una vez cifradas, las credenciales de pago pueden desencriptarse únicamente usando la clave de descifrado única. Si la clave de descifrado se envía al dispositivo móvil (112) para almacenamiento en el elemento seguro (113), esta clave de descifrado no se almacena en el servidor accesible de forma remota ni en su módulo de seguridad de hardware.

Las credenciales de pago cifradas o clave de descifrado recibidas por el dispositivo móvil (112) se almacenan de forma segura en el elemento seguro (113) del dispositivo móvil (112). Puede avisarse al usuario para un PIN antes de que las credenciales de pago cifradas o claves de descifrado se almacenen en el elemento seguro. En algunos ejemplos claves de descifrado se proporcionan al dispositivo móvil (112) desde el servidor accesible de forma remota (140) y almacenan en el elemento seguro (113) a través de provisión durante la comunicación aérea (OTA).

En el escenario de la derivación de las credenciales de pago en forma de a clave de descifrado se almacena en el elemento seguro (113) asociado con el dispositivo móvil (112), un usuario puede presentar el identificador a un comerciante como un método de pago en la realización de una transacción. El comerciante puede solicitar credenciales de pago del servidor accesible de forma remota (140) y, en conjunción, comunicar el identificador al servidor accesible de forma remota (140). El servidor accesible de forma remota (140) puede usar el identificador recibido para identificar un dispositivo móvil (112) y solicitar una clave de descifrado del dispositivo móvil identificado (112). El dispositivo móvil (112), tras recibir esta solicitud, puede avisar a continuación al usuario para un PIN, clave de acceso o contraseña antes de comunicar una clave de descifrado relevante al servidor accesible de forma remota (140) de modo que correspondientes credenciales de pago cifradas pueden desencriptarse y comunicarse al comerciante y/o el adquirente del comerciante y/o la red de procesamiento de pago de modo que la transacción puede completarse.

La Figura 2 ilustra un sistema ilustrativo (200) de acuerdo con una segunda realización de la invención. El sistema es similar al que se ilustra en la Figura 1 y números de referencia similares se refieren a sistemas, entidades o dispositivos similares. El sistema (200) de la Figura 2 difiere del de la Figura 1 en que el dispositivo de punto de venta en esta realización es una máquina de cajero automático (ATM) (222). La ATM (222) puede ser cualquier ATM adecuada y se configura para obtener credenciales de pago desde un dispositivo de pago portátil (214) de un consumidor (202) y para comunicar estas credenciales de pago a una red de procesamiento de pago (230) o red de entidad financiera. La ATM (222) puede configurarse para obtener credenciales de pago desde el dispositivo de pago portátil (214) a través de cualquier interfaz de comunicaciones apropiada con o sin contacto, por ejemplo un lector de tarjetas o interfaz de comunicación de campo cercano (NFC).

La ATM (222) en la realización ilustrada se configura para recibir un identificador introducido por un consumidor (202) a través de, por ejemplo, un teclado numérico de la ATM (222). La ATM (222) se configura adicionalmente para formatear las credenciales de pago así como el identificador en un mensaje de transacción financiera y para comunicar este mensaje a la red de procesamiento de pago (230). El mensaje de transacción financiera puede, por ejemplo, ser un mensaje ISO 8583. Adicionalmente, la ATM (222) se configura para insertar un código de

encaminamiento de servidor en el mensaje de transacción financiera de tal forma que el mensaje de transacción financiera se encamina al servidor accesible de forma remota (240) mediante la red de procesamiento de pago (230) usando el código de encaminamiento de servidor. El código de encaminamiento de servidor puede situarse en el campo 'BIN' del mensaje de transacción financiera.

Una vez que las credenciales de pago se reciben en el servidor accesible de forma remota, pueden comunicarse o puede comunicarse una derivación de las credenciales de pago al dispositivo móvil para almacenamiento en un elemento seguro del mismo como se ha descrito en la descripción anterior.

El sistema (200) puede ponerse en uso por un usuario (202) de manera similar al sistema de la Figura 1. El usuario (202) presenta su dispositivo de pago portátil (214) a una interfaz de dispositivo de pago portátil de la ATM (222). Puede avisarse al usuario para un PIN, en respuesta a una introducción correcta del cual, el usuario (202) selecciona una opción de 'transferencia de credenciales' de un menú visualizado en una pantalla de la ATM (222). También se avisará al usuario (202) para un identificador, que él o ella introduce en la ATM (222) a través de teclado numérico de la ATM (222). La ATM (222) obtiene credenciales de pago desde el dispositivo de pago portátil (214) y formatea las credenciales de pago, identificador, así como el código de encaminamiento de servidor en un mensaje de transacción financiera que se envía a continuación a la red de procesamiento de pago (230) y encamina desde allí al servidor accesible de forma remota (240). Similar al escenario en uso de la Figura 1, las credenciales de pago se comunican a continuación al dispositivo móvil del usuario (926) a almacenar en un elemento seguro del mismo.

La Figura 3 ilustra aún otro sistema ilustrativo (300) de acuerdo con un tercer ejemplo de la invención. El sistema (300) es similar al que se ilustra en las Figuras 1 y 2, y números de referencia similares se refieren a sistemas, entidades o dispositivos similares. El sistema (300) de la Figura 3 difiere del de las Figuras 1 y 2 en que el dispositivo móvil (316) no tiene un elemento seguro embebido. En su lugar, el dispositivo móvil (316) tiene una etiqueta de expansión criptográfica (318) en la que se dispone un elemento seguro. La etiqueta de expansión criptográfica (318) tiene contactos eléctricos dispuestos en un lado superior y un lado inferior de la misma que interactúa con un componente de comunicación (317) y una interfaz de componente de comunicación del dispositivo móvil (316) respectivamente. La etiqueta de expansión criptográfica (318) puede fijarse a continuación al componente de comunicación (317) que se inserta en un puerto de comunicación del dispositivo móvil (316) de tal forma que el elemento seguro puede interceptar y procesar apropiadamente cualquier comunicación enviada entre el componente de comunicación (317) y el dispositivo móvil (316) y, en consecuencia, entre el dispositivo móvil (316) y una red de comunicación móvil. En el ejemplo ilustrado, el componente de comunicación es una tarjeta de circuito integrado universal (UICC).

La Figura 4A ilustra un diagrama de flujo de un método de acuerdo con una realización de un aspecto de la invención. El método se realiza en un sistema de provisión que puede ser un servidor accesible de forma remota, similar a los descritos en la descripción anterior con referencia a las Figuras 1 a 3, o un quiosco especializado como se describe adicionalmente a continuación en relación con las Figuras 9A a 9D.

El método incluye una serie de etapas, una primera (402) de las cuales es la etapa de recepción de credenciales de pago desde un dispositivo de recepción que puede ser un dispositivo de punto de venta, incorporado en o usado en asociación con un dispositivo de punto de venta, como se describe con referencia a las Figuras 1 a 3, o un lector de instrumento de almacenamiento de credenciales de un quiosco con referencia a las Figuras 9A a 9D, u otra forma de dispositivo de recepción para recibir credenciales de pago. El dispositivo de punto de venta puede ser, por ejemplo, una máquina de cajero automático, un terminal punto de venta de comerciante o un dispositivo de entrada de PIN personal (PPED).

Las credenciales de pago recibidas desde el dispositivo de punto de venta se obtienen desde un dispositivo de pago portátil (también referido a continuación en relación con la realización de las Figuras 9A a 9D como un instrumento de almacenamiento de credenciales) que se presenta por un consumidor en el dispositivo de recepción. El dispositivo de pago portátil puede ser una tarjeta de crédito o débito que puede ser una cualquiera de una tarjeta bancaria de banda magnética, una tarjeta bancaria de circuito integrado de seguridad o una tarjeta bancaria sin contacto. Las credenciales de pago pueden ser datos de pista 1, datos de pista 2, datos de pista 3 o datos equivalentes de pista 2 (tal como datos de etiqueta 57 de EMV). Adicionalmente, las credenciales de pago pueden incluir un nombre de titular de cuenta y/o fecha de nacimiento, un número de identificación bancaria (BIN), un número de cuenta primario (PAN), un código de servicio, una fecha de expiración, valores de verificación de tarjeta (CVV1 o CVV2), un bloque o intervalo de PIN, un número de cuenta bancaria, un código de sucursal, un número de cuenta o identificador de fidelidad, información de número de tarjeta de crédito y/o débito, información de saldo de cuenta y/o información de consumidor tal como nombre, fecha de nacimiento. Las credenciales de pago pueden recibirse por el servidor accesible de forma remota a través de una red de procesamiento de pago.

El método incluye una etapa (404) de recepción de un identificador desde el dispositivo de recepción, por ejemplo, el dispositivo de punto de venta, o interfaz de entrada de usuario de quiosco. El identificador puede ser uno cualquiera o más de un número de directorio de abonados internacional de estación móvil (MSISDN), una dirección de correo electrónico, un identificador de red social, un nombre de consumidor predefinido o un número de cuenta de consumidor. En una realización preferida de la invención, las credenciales de pago e identificador se reciben en el

servidor accesible de forma remota en un mensaje de transacción financiera, que puede ser, por ejemplo, un mensaje ISO 8583. Adicionalmente, el mensaje de transacción financiera puede comunicarse desde el dispositivo de punto de venta al servidor accesible de forma remota a través de una red de procesamiento de pago. El mensaje de transacción financiera puede por consiguiente incluir un código de encaminamiento de servidor de tal forma que la red de procesamiento de pago es capaz de encaminar el mensaje de transacción financiera al servidor accesible de forma remota.

El método incluye una siguiente etapa (406) de identificación de un dispositivo móvil y/o un elemento seguro de un dispositivo móvil que corresponde al identificador. Esta etapa puede incluir la etapa de determinación de si un dispositivo móvil y/o elemento seguro que corresponde al identificador se ha registrado o no con el servidor accesible de forma remota y, si un dispositivo móvil y/o elemento seguro se ha registrado, identificar una correspondiente dirección de comunicación del dispositivo móvil y/o elemento seguro. Esto puede realizarse usando el identificador para consultar una base de datos del servidor accesible de forma remota para obtener la dirección de comunicación del dispositivo móvil y/o elemento seguro asociado con el identificador.

Como una etapa adicional opcional (408), puede enviarse un registro o petición de activación a un servicio de gestión confiable (TSM) que gestiona claves de seguridad o testigos que se usan para acceder a un elemento seguro. La petición puede incluir el identificador. El TSM puede autorizar el desbloqueo de un elemento seguro asociado con el dispositivo móvil. El TSM puede proporcionarse en el servidor accesible de forma remota o mediante un servicio remoto proporcionado en un servidor accesible de forma remota separado.

El método incluye una etapa (410) de comunicación de las credenciales de pago al dispositivo móvil a almacenar en un elemento seguro asociado con el dispositivo móvil. Esto puede incluir comunicar las credenciales de pago al dispositivo móvil usando la dirección de comunicación. Esto también puede incluir comunicar las credenciales de pago al elemento seguro asociado con el dispositivo móvil usando un código de identificación de un elemento seguro para configurar un canal seguro de comunicación con el elemento seguro que puede ser a través del dispositivo móvil. En algunos ejemplos como se describen adicionalmente en relación con la Figura 4B, una derivación de las credenciales de pago se comunica al dispositivo móvil o elemento seguro, por ejemplo, la derivación de las credenciales de pago puede ser una clave de descifrado que corresponde a credenciales de pago cifradas almacenadas de forma remota.

Como una etapa adicional opcional (412) adicional, pueden solicitarse credenciales adicionales por o suministrarse por el servidor accesible de forma remota. Las credenciales adicionales pueden ser credenciales que no pueden leerse automáticamente desde un dispositivo de pago portátil tal como un valor de verificación de tarjeta impreso (por ejemplo el número CVV2) que es legible por el ser humano desde el dispositivo de pago portátil. En este caso, las credenciales adicionales pueden solicitarse por el servidor accesible de forma remota y obtenerse del consumidor a través del dispositivo de punto de venta.

Las credenciales adicionales también pueden incluir software de valor de verificación de tarjeta dinámico (dCVV) que se usa para generar un dCVV para transacciones individuales. Tales credenciales adicionales pueden identificarse usando el identificador y suministrarse por el servidor accesible de forma remota o por un servidor accesible de forma remota separado durante el proceso de provisión. Las credenciales adicionales pueden comunicarse al elemento seguro asociado con el dispositivo móvil. Estas pueden comunicarse separadamente a las credenciales de pago o derivación de las credenciales de pago.

El elemento seguro del dispositivo móvil puede, de acuerdo con algunos ejemplos de la invención, embeberse en una etiqueta, tarjeta o placa como se describe anteriormente en la descripción siguiente. Antes de comunicar las credenciales de pago al dispositivo móvil, el servidor accesible de forma remota puede cifrar las credenciales de pago usando uno cualquiera de un número de algoritmos de encriptación. Algoritmos de encriptación ilustrativos incluyen Norma de Encriptación Avanzada (AES), Norma de Encriptación de Datos (DES), Norma/Algoritmo de Encriptación de Datos Triple (TDES/TDEA), Capa de Conexión Segura (SSL), Blowfish, Serpent, Twofish, Algoritmo de Encriptación de Datos Internacional (IDEA), Rivest, Shamir y Adleman (RSA), Algoritmo de Firma Digital (DSA), Algoritmo Diminuto de Encriptación (TEA), TEA extendido (XTEA), y/u otros algoritmos o protocolos de encriptación. En algunos ejemplos, la clave de descifrado, también denominada como la clave privada, se almacena en una memoria segura del servidor accesible de forma remota en asociación con el identificador, de tal forma que únicamente el servidor accesible de forma remota, o un módulo de seguridad de hardware del mismo, puede descifrar las credenciales de pago antes de la presentación a, por ejemplo, un comerciante. En este ejemplo, las credenciales de pago se almacenan en su forma cifrada en el elemento seguro del dispositivo móvil.

La Figura 4B ilustra un diagrama de flujo de un método de acuerdo con otra realización de un aspecto de la invención. El método se realiza en servidor accesible de forma remota, tal como el de las Figuras 1 a 3. El método incluye una serie de etapas, una primera (422) de las cuales es la recepción de credenciales de pago desde un dispositivo de recepción tal como dispositivo de punto de venta similar al de la etapa (402) de la Figura 4A.

El método incluye una siguiente etapa (424) de recepción de un identificador desde el dispositivo de recepción tal como un dispositivo de punto de venta similar al de la etapa (404) de la Figura 4A.

El método incluye una siguiente etapa (426) de cifrado de las credenciales de pago. Las credenciales de pago pueden cifrarse con cualquier algoritmo apropiado y una vez cifrado, tener una clave de descifrado única. Algoritmos de encriptación ilustrativos incluyen, pero sin limitación, Norma de Encriptación Avanzada (AES), Norma de Encriptación de Datos (DES), Norma/Algoritmo de Encriptación de Datos Triple (TDES/TDEA), Capa de Conexión Segura (SSL), Blowfish, Serpent, Twofish, Algoritmo de Encriptación de Datos Internacional (IDEA), Rivest, Shamir y Adleman (RSA), Algoritmo de Firma Digital (DSA), Algoritmo Diminuto de Encriptación (TEA), TEA extendido (XTEA) y/u otros algoritmos o protocolos de encriptación.

Como la clave de descifrado es única para esas credenciales de pago, únicamente esa clave de descifrado puede usarse para desencriptar esas credenciales de pago. La clave de descifrado única, que en algunas realizaciones puede ser una clave privada, no se almacena en la misma ubicación que las credenciales de pago cifradas.

El método incluye una siguiente etapa (428) de almacenamiento de una de las credenciales de pago cifradas o la clave de descifrado en una memoria segura del servidor accesible de forma remota, que en una realización preferida, es un módulo de seguridad de hardware. Las credenciales de pago cifradas o la clave de descifrado única, dirección de comunicación e identificador pueden asociarse con un perfil de usuario almacenado en una base de datos del servidor accesible de forma remota. Tras recibir, por ejemplo, una clave de descifrado única, pueden identificarse las correspondientes credenciales de pago, almacenadas en el módulo de seguridad de hardware.

El método incluye una siguiente etapa (430) de identificación de un dispositivo móvil y/o un elemento seguro que corresponde al identificador. Esta etapa es similar a la etapa (406) de la Figura 4A.

El método incluye una etapa final (432) de comunicación de la otra de las credenciales de pago cifradas y la clave de descifrado única al dispositivo móvil a almacenar en un elemento seguro asociado con el dispositivo móvil. Esto puede incluir comunicar al dispositivo móvil usando la dirección de comunicación. El elemento seguro del dispositivo móvil puede, de acuerdo con algunos ejemplos de la invención, embeberse en una etiqueta, tarjeta o placa como se describe anteriormente en la descripción anterior.

Como únicamente una de las credenciales de pago cifradas y la clave de descifrado se almacena únicamente en el elemento seguro del dispositivo móvil, las credenciales de pago cifradas no pueden descifrarse y, en consecuencia, no pueden usarse.

En el escenario en el que las credenciales de pago cifradas se almacenan en el servidor accesible de forma remota y la clave de descifrado única se transmite al elemento seguro del dispositivo móvil, la clave de descifrado única se purga y no se almacena en el módulo de seguridad de hardware del servidor accesible de forma remota.

Este escenario, que puede considerarse un inverso de uno en el que las credenciales de pago se almacenan en el elemento seguro del dispositivo móvil, es ventajoso en que si el elemento seguro del dispositivo móvil se pone en peligro, únicamente pueden obtenerse la claves de descifrado de credenciales de pago cifradas. Adicionalmente, en el caso de que el elemento seguro se pone en peligro, la claves de descifrado almacenadas en el mismo pueden revocarse simplemente, sin tener que emitir de nuevo credenciales de pago.

La Figura 5 ilustra un diagrama de flujo de un método de acuerdo con otro aspecto de la invención. El método se realiza en un dispositivo de punto de venta modificado adecuado, tal como cualquiera de los descritos en la descripción anterior con referencia a las Figuras 1 a 3.

El método incluye una primera etapa (502) de obtención de credenciales de pago desde un dispositivo de pago portátil presentado por un consumidor en el dispositivo de punto de venta. Esto puede realizarse de una manera similar a operaciones de acceso a credenciales de pago convencionales, tal como por ejemplo a través de un protocolo de comunicación de ISO 7816 o ISO/IEC 14443 o similar. Las credenciales de pago obtenidas podrían considerarse como credenciales de pago 'presentes en tarjeta' en que proporcionan suficiente información para una transacción posterior usando las credenciales de pago a considerarse una transacción presente en tarjeta. Las credenciales de pago pueden entonces, por ejemplo, ser datos de pista 1, datos de pista 2, datos de pista 3 o datos equivalentes de pista 2 (tal como datos de etiqueta 57 de EMV). Adicionalmente, las credenciales de pago pueden incluir un nombre de titular de cuenta y/o fecha de nacimiento, un número de identificación bancaria (BIN), un número de cuenta primario (PAN), un código de servicio, una fecha de expiración, valores de verificación de tarjeta (CVV1 o CVV2), un bloque o intervalo de PIN, un número de cuenta bancaria, un código de sucursal, un número de cuenta o identificador de fidelidad, información de número de tarjeta de crédito y/o débito, información de saldo de cuenta o información de consumidor tal como nombre, fecha de nacimiento.

El método incluye una siguiente etapa (504) de recepción de un identificador introducido por el consumidor en el dispositivo de punto de venta. El identificador puede ser uno cualquiera o más de uno o más de un número de directorio de abonados internacional de estación móvil (MSISDN), una dirección de correo electrónico, un identificador de red social, un nombre de consumidor predefinido o un número de cuenta de consumidor.

El método incluye adicionalmente una siguiente etapa (506) de comunicación de las credenciales de pago e identificador a un servidor accesible de forma remota para comunicación adicional a un elemento seguro asociado con un dispositivo móvil del consumidor. Esta etapa puede incluir formatear las credenciales de pago e identificador en un mensaje de transacción financiera. El mensaje de transacción financiera puede, por ejemplo, ser un mensaje de transacción financiera de ISO 8583. El dispositivo de punto de venta puede adicionalmente configurarse para insertar un código de encaminamiento de servidor en el mensaje de transacción financiera de tal forma que el mensaje de transacción financiera se encamina al servidor accesible de forma remota mediante una red de procesamiento de pago y no, por ejemplo, un banco emisor como se indica por el BIN incluido originalmente en las credenciales de pago.

Si se solicita, el consumidor puede introducir credenciales adicionales en el dispositivo de punto de venta y pueden comunicarse al servidor accesible de forma remota, por ejemplo, valores de verificación de tarjeta no legibles por máquina (por ejemplo, datos CVV2).

En la Figura 6A se ilustra un servidor accesible de forma remota para proporcionar de credenciales de pago, tal como el de las Figuras 1, 2 y 3. El servidor accesible de forma remota (140) tiene un receptor de credenciales de pago (602) para recibir credenciales de pago. Las credenciales de pago pueden recibirse desde un dispositivo de punto de venta en el que las credenciales de pago pueden haberse obtenido desde un dispositivo de pago portátil presentado por un consumidor. El servidor accesible de forma remota (140) tiene un receptor de identificador (604) para recibir, desde el dispositivo de punto de venta, un identificador introducido por el consumidor. En algunos ejemplos el receptor de credenciales de pago (602) y el receptor de identificador (604) pueden proporcionarse en un único receptor que puede configurarse para recibir credenciales de pago y un identificador en un mensaje de transacción financiera. En algunos ejemplos, el mensaje de transacción financiera puede ser un mensaje ISO 8583.

El servidor accesible de forma remota (140) puede incluir un componente de cifrado (606) para cifrar las credenciales de pago recibidas, teniendo las credenciales de pago cifradas una clave de descifrado única. El servidor accesible de forma remota (140) puede tener una memoria segura (608) incorporada en el mismo o asociada con el servidor accesible de forma remota (140) para almacenar una de las credenciales de pago cifradas o la clave de descifrado única. En la realización ilustrada, la memoria segura (608) y el componente de cifrado (606) están dentro de un módulo de seguridad de hardware (644) del servidor accesible de forma remota (140).

El servidor accesible de forma remota (140) puede incluir un componente de identificación (610) para identificar un dispositivo móvil y/o elemento seguro que corresponde al identificador. En la realización ilustrada, el componente de identificación (610) forma parte de una base de datos (642) del servidor accesible de forma remota (140) en la que uno o más del grupo de: un identificador; clave de descifrado; credenciales de pago cifradas; y dirección de comunicación pueden asociarse con un perfil de usuario.

El servidor accesible de forma remota (140) incluye adicionalmente un módulo de comunicación (612) para comunicar al dispositivo móvil identificado o el elemento seguro asociado con el dispositivo móvil. El módulo de comunicación puede comunicarse con el dispositivo móvil a través de cualquier red de datos móviles o de comunicación móvil apropiada. El módulo de comunicación (612) puede configurar un canal de comunicación seguro con el elemento seguro a través del dispositivo móvil para comunicación de una de las credenciales de pago cifradas o la clave de descifrado única.

El servidor accesible de forma remota (140) puede incluir opcionalmente un componente de autorización (646) para enviar un registro o petición de activación a un servicio de gestión confiable (TSM) que gestiona claves de seguridad o testigos que se usan para acceder a un elemento seguro.

El servidor accesible de forma remota (140) puede incluir opcionalmente un componente de credenciales adicionales (648) para solicitar o suministrar credenciales adicionales para comunicar al dispositivo móvil o el elemento seguro. El componente de credenciales adicionales (648) puede solicitar credenciales adicionales desde un consumidor a través de un dispositivo de punto de venta, por ejemplo, valores de verificación de tarjeta legibles por el ser humano, que se reenvían para almacenamiento en el elemento seguro asociado con el dispositivo móvil. Como alternativa o adicionalmente, el componente de credenciales adicional (648) puede suministrar credenciales adicionales almacenados en el servidor accesible de forma remota o un servidor remoto relacionado, por ejemplo, en forma de software de valor de verificación de tarjeta dinámico (dCVV) usado para generar un dCVV para transacciones individuales. Las credenciales adicionales suministradas pueden reenviarse para almacenamiento en el elemento seguro asociado con el dispositivo móvil.

En la Figura 6B se ilustra un dispositivo de punto de venta para proporcionar de credenciales de pago, tal el que de las Figuras 1, 2 y 3.

El dispositivo de punto de venta (120) puede incluir un componente de obtención de credenciales de pago (652) que puede ser en forma de un lector de tarjetas o escáner como se ha descrito anteriormente. El dispositivo de punto de venta (120) también puede incluir un receptor de identificador (654) para recibir un identificador como entrada por un consumidor.

El dispositivo de punto de venta (120) puede incluir un módulo de comunicación (656) para comunicación con un servidor accesible de forma remota. El módulo de comunicación (656) puede comunicarse con el servidor accesible de forma remota de forma segura usando mensajes de transacciones financieras.

En algunos ejemplos, el dispositivo de punto de venta (120) puede incluir un componente de autorización (658) para enviar un registro o petición de activación a un servicio de gestión confiable (TSM) que gestiona claves de seguridad o testigos que se usan para acceder a un elemento seguro.

En ejemplos adicionales, el dispositivo de punto de venta (120) puede incluir un receptor de credenciales adicionales (659) para recibir credenciales adicionales desde un cliente, por ejemplo, en forma de un valor de verificación de tarjeta impreso que no es obtenible por el componente de obtención de credenciales de pago (652).

La Figura 7 muestra un diagrama de flujo en carriles que ilustra el flujo entre un dispositivo móvil (112), un dispositivo de punto de venta (120) y un servidor accesible de forma remota (140) de acuerdo con ejemplos. El servidor accesible de forma remota (140) puede proporcionarse por una institución financiera o proveedor de servicios. En un ejemplo, el servidor accesible de forma remota (140) es parte de una red de procesamiento de pago.

Un consumidor puede presentar (701) su dispositivo de pago portátil (por ejemplo, una tarjeta de pago) en el dispositivo de punto de venta que puede extraer credenciales de pago desde el dispositivo de pago portátil. El consumidor también puede proporcionar (702) un identificador. Por ejemplo, el consumidor puede presentar a un comerciante su tarjeta de pago que puede insertarse en un dispositivo de punto de venta y puede solicitarse una transacción de “transferencia de credenciales”. Puede avisarse al consumidor para su PIN de tarjeta de pago que puede introducirse en el dispositivo de punto de venta a través de un teclado numérico. El dispositivo de punto de venta también puede avisar al consumidor para un “alias” que se usa como un identificador para el consumidor y su dispositivo móvil.

El dispositivo de punto de venta puede formatear (703) las credenciales de pago y el identificador extraídos en un mensaje de transacción, por ejemplo, un mensaje ISO 8583. Este mensaje es similar a un mensaje de transacción de punto de venta normal con la adición del identificador proporcionado. El campo del BIN puede rellenarse con un BIN de red de procesamiento de pago de modo que el mensaje se encamina a una pasarela de procesamiento de pago en lugar de un emisor. El BIN del consumidor permanece proporcionado en el mensaje.

El servidor accesible de forma remota recibe (704) el mensaje de transacción y extrae las credenciales de pago y el identificador. El identificador se usa para identificar (705) uno o más de: un consumidor que tiene un dispositivo móvil y/o elemento seguro registrados; una cuenta que tiene un dispositivo móvil y/o elemento seguro registrados; o propio el dispositivo móvil y/o elemento seguro.

El servidor accesible de forma remota puede cifrar (706) las credenciales de pago y puede generarse una clave de descifrado única específica para las credenciales de pago. Una de las credenciales de pago cifradas y la clave de descifrado única puede comunicarse de forma segura (707) al elemento seguro asociado con el dispositivo móvil, mientras que la otra de las credenciales de pago cifradas y la clave de descifrado única puede almacenarse (708) en el servidor accesible de forma remota.

El elemento seguro asociado con el dispositivo móvil puede recibir (709) o bien las credenciales de pago cifradas o bien la clave de descifrado única y puede avisar al usuario para un PIN (710), el intervalo del cual se almacena en asociación con las credenciales de pago o la clave de descifrado de tal forma que las credenciales de pago se liberarán únicamente por el elemento seguro en el caso de que se introduzca el PIN correcto.

La Figura 8 es un diagrama en carriles que ilustra el flujo entre un dispositivo móvil (112), un dispositivo de punto de venta (120) y un servidor accesible de forma remota (140) de acuerdo con una realización del método descrito en el que la clave de descifrado para las credenciales de pago se proporciona al elemento seguro asociado con el dispositivo móvil.

Un consumidor puede presentar (801) un identificador a un comerciante como un método de pago en la realización de una transacción. El comerciante puede solicitar (802) credenciales de pago desde el servidor accesible de forma remota enviando el identificador con la petición.

El servidor accesible de forma remota puede usar el identificador recibido para identificar (803) un dispositivo móvil asociado con un elemento seguro en el que se almacena una clave de descifrado. El servidor accesible de forma remota puede solicitar (804) la clave de descifrado a través de una comunicación segura con el elemento seguro que puede ser a través del dispositivo móvil.

El dispositivo móvil tras recibir la petición puede avisar (805) al consumidor para un PIN antes de comunicar (806) la clave de descifrado al servidor accesible de forma remota.

El servidor accesible de forma remota puede recuperar (807) las credenciales de pago cifradas desde su almacenamiento y descifrar (808) las credenciales de pago usando la clave de descifrado. A continuación pueden transmitirse (809) y recibirse (810) las credenciales de pago en un dispositivo de punto de venta u otro intermediario usando un canal seguro para completar la transacción.

Una ventaja de almacenar credenciales de pago, cifradas, en un servidor accesible de forma remota en lugar de en un elemento seguro de un dispositivo móvil, de acuerdo con ejemplos de la presente invención, es que si el elemento seguro del dispositivo móvil se pone en peligro por una tercera parte maliciosa y esa tercera parte obtiene información almacenada en el mismo, la información obtenida por la tercera parte no incluirá credenciales de pago. Esto es en contraste a escenarios en los que credenciales de pago se almacenan en el elemento seguro y en los que la tercera parte puede obtener y hacer uso de forma fraudulenta de estas credenciales de pago.

Además de esto, en el caso de que el elemento seguro se ponga en peligro o pierda, la claves de descifrado almacenadas en el mismo pueden simplemente revocarse, sin tener que emitir de nuevo credenciales.

Una ventaja adicional de almacenar las credenciales de pago, cifradas, en el servidor accesible de forma remota en lugar de en un elemento seguro de un dispositivo móvil es que el dispositivo móvil no necesita cumplir con normas de seguridad impuestas por normas pertinentes o autoridades de cumplimiento. Por ejemplo, el elemento seguro no necesita cumplir con EMV o puede no tener que cumplir con requisitos PCI DSS.

De forma similar ya que la clave de descifrado única se almacena únicamente en el elemento seguro del dispositivo móvil del consumidor, las correspondientes credenciales de pago cifradas no pueden descifrarse y, en consecuencia, no pueden usarse, sin que la clave de descifrado se libere desde el elemento seguro en el que se almacena de forma segura. Por lo tanto el consumidor tiene control definitivo sobre cuándo pueden usarse sus credenciales de pago. Adicionalmente, si el servidor accesible de forma remota se pone en peligro por una tercera parte maliciosa, credenciales de pago cifradas almacenadas en el mismo no serán de utilidad a esa tercera parta sin una correspondiente clave de descifrado única.

Las Figuras 9A a 9D se describen ahora ilustrando una realización alternativa de la invención en la que el sistema de provisión se proporciona por un quiosco (901).

La Figura 9A ilustra un quiosco (901) que puede configurarse en tiendas minoristas, centros comerciales, aeropuertos y otros sitios públicos. Por ejemplo, el quiosco (901) puede configurarse convenientemente en un minorista de dispositivo móvil o una tienda de operador de red móvil para permitir que usuarios provisionen su recientemente comprado dispositivo móvil con capacidades de cartera digital, en algunos ejemplos, el quiosco (901) puede atornillarse al suelo o a una pared con hardware a prueba de manipulación. El quiosco (901) también puede implementarse para ser lo suficientemente pequeño, ligero y compacto para ser portátil de tal forma que el quiosco (901) puede moverse fácilmente de ubicación a ubicación. Por ejemplo, en algunos ejemplos, el quiosco (901) puede implementarse en un factor de forma similar a un ordenador de tableta o un portátil.

El quiosco (901) incluye un visualizador (902), un interfaz de dispositivo móvil (910) y un lector de instrumento de almacenamiento de credenciales (920). El visualizador (902) puede rodearse por un alojamiento. El visualizador (902) puede situarse a una altura adecuada (por ejemplo, en un mostrador) para permitir que un usuario lea o vea fácilmente información o imágenes proporcionadas en el visualizador (902). El visualizador (902) puede usarse para proporcionar instrucciones al usuario durante el proceso de provisión de cartera digital. El visualizador (902) también puede usarse para mostrar anuncios, videos y/u otras imágenes cuando el quiosco (901) no se está usando. El visualizador (902) también puede actuar como una interfaz de entrada de usuario tal como pantalla táctil para aceptar entradas de usuario.

La interfaz de dispositivo móvil (910) se usa para establecer un canal de comunicación o enlace entre el quiosco (901) y un dispositivo móvil. Un dispositivo móvil puede ser un teléfono móvil, un asistente digital personal, un dispositivo informático de tableta, dispositivo reproductor de medios portátil u otro dispositivo informático portátil adecuado que puede almacenar y ejecutar una aplicación de cartera digital. La interfaz de dispositivo móvil (910) puede ser un conector físico como se muestra que puede enchufarse en un puerto de comunicación físico de un dispositivo móvil. Por ejemplo, el conector físico puede ser un conector USB que puede enchufarse en un puerto USB (por ejemplo, mini-USB) de un dispositivo móvil. El conector físico también puede ser un conector propietario que es compatible con un puerto de comunicación propietario de algunos fabricantes de dispositivos móviles. El conector físico puede proporcionarse como una clavija, como parte de un cable (por ejemplo, un cable retráctil, un cable externo, etc.) que puede extenderse desde el alojamiento del quiosco (901), o como parte de una estación de acoplamiento o una plataforma incorporada en el alojamiento del quiosco (901). En algunas realizaciones, el quiosco (901) puede incluir múltiples tipos de conectores de tal forma que quiosco (901) puede ser compatible con un número de fabricantes de dispositivos móviles. En algunas realizaciones, la interfaz de dispositivo móvil (910) puede ser una interfaz inalámbrica (por ejemplo, transceptor inalámbrico) que se usa para establecer un canal de comunicación ad hoc con un dispositivo móvil usando NFC, RF, Bluetooth, Wi-Fi u otros protocolos de comunicación inalámbrica durante el proceso de provisión de cartera digital. El quiosco (901) también puede incluir uno o más

conectores físicos en combinación con uno o más interfaces inalámbricas que pueden usarse para establecer un canal de comunicación con un dispositivo móvil.

Lector de instrumento de almacenamiento de credenciales (920) del quiosco (901) se usa para leer o acceder a un instrumento de almacenamiento de credenciales (905) (también denominado en este documento como un dispositivo de pago portátil) para obtener credenciales y/u otra información de usuario o cuenta almacenada en el instrumento de almacenamiento de credenciales (905). El lector de instrumento de almacenamiento de credenciales (920) puede ser un lector de banda magnética o un lector de tarjeta con chip para leer credenciales desde el instrumento de almacenamiento de credenciales (905) a través de contacto físico con el instrumento de almacenamiento de credenciales (905). El lector de instrumento de almacenamiento de credenciales (920) puede ser un escáner de infrarrojos tal como escáner de un código de barras o código QR para leer credenciales que se codifican como una imagen, o puede ser un lector de tarjeta sin contacto capaz de comunicarse con el instrumento de almacenamiento de credenciales (905) a través de NFC, RF, Bluetooth, Wi-Fi u otros protocolos de comunicación inalámbrica para leer credenciales desde el instrumento de almacenamiento de credenciales (905) de una manera inalámbrica cuando el instrumento de almacenamiento de credenciales (905) está en proximidad cercana al quiosco (901). En algunas realizaciones, el quiosco (901) puede incluir uno o más tipos de lector de instrumento de almacenamiento de credenciales descritos anteriormente.

El instrumento de almacenamiento de credenciales (905) puede ser en forma de una tarjeta (por ejemplo, de crédito/débito y otra tarjeta de pago, tarjeta de identificación, tarjeta de carnet de conducir, tarjeta de tránsito, tarjeta de acceso, tarjeta de seguro, tarjeta de fidelización de minorista, tarjeta regalo, etc.) u otra estructura adecuada. El instrumento de almacenamiento de credenciales (905) puede incluir una banda magnética y/o un chip de memoria para almacenar las credenciales del usuario. El instrumento de almacenamiento de credenciales (905) también puede ser un medio impreso que incluye una imagen que codifica las credenciales del usuario tal como un código de barras o un código QR. En algunas realizaciones, el instrumento de almacenamiento de credenciales (905) también puede ser el dispositivo móvil existente de un usuario que tiene las credenciales del usuario almacenadas en el mismo.

Credenciales pueden incluir información almacenada en un instrumento de almacenamiento de credenciales que puede usarse para realizar una transacción con el instrumento de almacenamiento de credenciales. Por ejemplo, credenciales pueden ser información que se usa para identificar y/o verificar el usuario, o para identificar o acceder a una cuenta asociada con el instrumento de almacenamiento de credenciales. Credenciales pueden incluir información financiera, información de identificación, información de cuenta, información de tránsito (por ejemplo, como en un billete de metro o tren), información de acceso (por ejemplo, como placas de acceso), etc. Algunos ejemplos de credenciales incluyen información de cuenta bancaria, número de cuenta primario (PAN), número de identificación bancaria (BIN), número de tarjeta de crédito o débito, fecha de expiración, nombre, nombre de usuario, fecha de nacimiento, número de carnet de conducir, dirección, número de la seguridad social, número de pasaporte, número de póliza del seguro tal como número de cuenta del seguro médico o del automóvil, número de cuenta de programa de fidelización de viajes o del minorista, número de tarjeta regalo, número de cuenta de tarifa de tránsito, número de identificación de empleado o similares. Credenciales también pueden incluir información adicional que se usa para facilitar una transacción. Por ejemplo, credenciales pueden incluir un valor de verificación de tarjeta (CVV) y/o un código de servicio usado para facilitar el procesamiento de una transacción.

En algunos ejemplos, credenciales también pueden incluir información adicional que se usa para facilitar una transacción, pero no se almacena en el instrumento de almacenamiento de credenciales (905) o no puede recuperarse por lector de instrumento de almacenamiento de credenciales (920) del quiosco (901). Por ejemplo, credenciales pueden incluir un valor de verificación de tarjeta 2 (CVV2) que se imprime en la cara de una tarjeta de crédito, pero puede no recuperarse leyendo la banda magnética de la tarjeta. Credenciales también pueden incluir software de código de verificación de tarjeta dinámico (dCVV) que se usa para generar un dCVV para transacciones individuales. Para tales credenciales que no se almacenan en el instrumento de almacenamiento de credenciales (905) o no pueden recuperarse por el lector de instrumento de almacenamiento de credenciales (920), el quiosco (901) puede obtener tales credenciales del emisor de instrumento de almacenamiento de credenciales (905) durante el proceso de provisión de tal forma que estas credenciales pueden cargarse en el dispositivo móvil.

Credenciales pueden almacenarse en un chip de memoria del instrumento de almacenamiento de credenciales (905) o pueden codificarse como una imagen impresa en el instrumento de almacenamiento de credenciales (905). Credenciales almacenadas en el instrumento de almacenamiento de credenciales (905) también pueden almacenarse en forma de pistas de datos magnéticas tal como las asociadas tradicionalmente con tarjetas de crédito. Tales pistas pueden incluir Pista 1 y Pista 2. Pista 1 (“Asociación Internacional de Transporte Aéreo”) almacena más información que la Pista 2, y contiene el nombre del titular de la tarjeta así como número de cuenta y otros datos discrecionales. Esta pista se usa en ocasiones por las compañías aéreas cuando aseguran reservas con una tarjeta de crédito. Pista 2 (“Asociación Americana de Banca”) es la más usada comúnmente en la actualidad. Esta es la pista que se leer por ATM y verificadores de tarjetas de crédito. La ABA (Asociación Americana de Banca) diseñó las especificaciones de esta pista y todos los bancos del mundo se atienen a la misma. Contiene la cuenta del titular de la tarjeta, PIN cifrado, más otros datos discrecionales.

La Figura 9B ilustra un diagrama de bloques de un quiosco (901) de acuerdo con diversas realizaciones. El quiosco (901) incluye uno o más procesadores (921) acoplados a un medio de almacenamiento (204). El medio de almacenamiento (204) almacena código legible por máquina que puede ejecutarse por el procesador (921) para proporcionar capacidades de dispositivo móvil con cartera digital. El quiosco (901) incluye una o más interfaces de dispositivo móvil (910) y uno o más lectores de instrumento de almacenamiento de credenciales (920). El quiosco (901) incluye adicionalmente el visualizador (925) y sistema de sonido (924) que pueden usarse para proporcionar a un usuario con instrucciones visuales y de audio durante el proceso de provisión de la cartera digital. Cuando quiosco (901) no se está usando para proporcionar un dispositivo móvil, el visualizador (925) y el sistema de sonido 208 pueden usarse para presentar otros medios tal como anuncios o videos y sonidos informativos. El quiosco (901) también incluye interfaz de entrada de usuario (926) para recibir entradas de usuario. La interfaz de entrada de usuario (926) puede implementarse con uno o más de una pantalla táctil, un teclado numérico, un teclado, un panel táctil, un ratón, una almohadilla táctil, un micrófono u otros componentes de interfaz de entrada de usuario adecuados.

En algunos ejemplos, el quiosco (901) puede incluir una la interfaz de red (923) para permitir que el quiosco (901) se comunique, si fuera necesario, con entidades que pueden implicarse con el proceso de provisión de la cartera digital. Por ejemplo, la interfaz de red (923) puede usarse por el quiosco (901) para comunicar con un emisor del instrumento de almacenamiento de credenciales (por ejemplo, un banco que emitió una tarjeta de crédito, una agencia de tránsito que emitió una tarjeta de acceso de tránsito, una agencia del gobierno que emitió una tarjeta de identificación, un minorista que emitió una tarjeta de programa de fidelización, etc.). La interfaz de red (923) también puede usarse por el quiosco (901) para comunicar con un gestor de servicios confiable para adquirir claves de seguridad o testigos que se usan para proporcionar capacidades de dispositivo móvil con cartera digital. El quiosco (901) también puede comunicarse con un operador de red móvil a través de la interfaz de red (923) para verificar o acceder a información asociada a un dispositivo móvil. La interfaz de red (923) puede implementarse como una interfaz inalámbrica tal como un puerto de Ethernet o como una interfaz inalámbrica tal como un transceptor inalámbrico que puede acceder a una red inalámbricamente (por ejemplo, usando Wi-Fi u otro protocolo de comunicación inalámbrica).

La Figura 9C ilustra un sistema (930) para proporcionar un dispositivo móvil (931) con capacidades de cartera digital usando el quiosco (901). El dispositivo móvil (931) puede ser un dispositivo móvil recientemente comprado o puede ser un dispositivo móvil existente que un usuario ya posee. En algunas realizaciones, el dispositivo móvil (931) puede precargarse con una aplicación de cartera digital, y el quiosco (901) se usa para cargar credenciales en la aplicación de cartera digital del dispositivo móvil (931). En otras realizaciones, el quiosco (901) puede usarse para cargar una aplicación de cartera digital junto con credenciales personalizadas en el dispositivo móvil (931) si el dispositivo móvil (931) no incluye una aplicación de cartera digital precargada.

De acuerdo con algunos ejemplos, el quiosco (901) se acopla comunicativamente a un gestor de servicios confiable (TSM) (933), por ejemplo, a través de una red (932). El TSM (933) ofrece servicios para soportar servicios de transacción sin contacto que se realizan con dispositivos móviles. Las funcionalidades básicas que pueden proporcionarse por el TSM (933) incluyen la capacidad de gestionar claves de seguridad o testigos que se usan para acceder al chip de elemento seguro (SE) de un dispositivo móvil (por ejemplo, un chip de memoria segura o una partición asegurada de una memoria) en el que pueden almacenarse credenciales de una aplicación de cartera digital. El SE se usa por el dispositivo móvil (931) para alojar y almacenar datos y aplicaciones que requieren un alto grado de seguridad. El SE puede proporcionarse al dispositivo móvil (931), por ejemplo, mediante una entidad de la red de procesamiento de pago tal como un emisor de una tarjeta de crédito, mediante un proveedor de servicios de transacciones sin contacto, mediante un operador de red móvil (MNO), mediante un fabricante de dispositivos móviles o mediante otras entidades adecuadas. Puede conseguirse acceso al SE del dispositivo móvil (931) obteniendo la clave de seguridad o testigo apropiado del proveedor de SE.

Aunque el TSM (933) se muestra como una entidad separada, en algunas realizaciones, el TSM (933) puede integrarse con sistema de emisor (935) para activar y personalizar una aplicación de cartera digital con credenciales de un usuario, o integrarse con el quiosco (901). Bajo solicitud, el TSM (933) puede obtener la clave de seguridad o testigo apropiado de un proveedor de SE para bloquear o desbloquear el SE en el dispositivo móvil (931), por ejemplo, para permitir que el quiosco (901) cargue credenciales de usuario en el SE del dispositivo móvil (931).

La provisión del dispositivo móvil (931) para capacidades de cartera digital puede iniciarse cuando un usuario interactúa con el quiosco (901) proporcionando entrada de usuario a una interfaz de entrada de usuario del quiosco (901), por ejemplo, tocando una pantalla táctil del quiosco (901) o presionando una tecla en un teclado del quiosco (901), etc. Tras la interactuación del usuario, el quiosco (901) puede proporcionar instrucciones visuales y/o de audio para que el usuario complete el proceso de provisión. Por ejemplo, el quiosco (901) puede visualizar un mensaje que ordena al usuario que conecte comunicativamente el dispositivo móvil del usuario (931) al quiosco (901).

Para conectar comunicativamente el dispositivo móvil del usuario (931) al quiosco (901), un usuario puede conectar físicamente el dispositivo móvil (931) a la interfaz de dispositivo móvil (por ejemplo, un conector o cable) del quiosco (901) para un canal de comunicación por cable, o situando el dispositivo móvil (931) en proximidad cercana al interfaz de dispositivo móvil (por ejemplo, transceptor inalámbrico) del quiosco (901) para permitir que se establezca

un canal de comunicación inalámbrica ad hoc entre el dispositivo móvil (931) y el quiosco (901). El canal de comunicación inalámbrica ad hoc puede establecerse a través de NFC, RF, Bluetooth, Wi-Fi u otros protocolos de comunicación inalámbrica adecuados. En algunas realizaciones, cuando el quiosco (901) detecta que un dispositivo móvil (931) está en proximidad cercana, el quiosco (901) puede visualizar un mensaje preguntado si el usuario concede permiso para que el quiosco (901) establezca un canal de comunicación inalámbrica con el dispositivo móvil (931).

Una vez que se establece un canal de comunicación (por cable o inalámbrico) entre el dispositivo móvil (931) y quiosco (901), el quiosco (901) puede proporcionar adicionalmente instrucciones visuales y/o de audio al usuario para presentar un instrumento de almacenamiento de credenciales (905) para continuar con el proceso de provisión de la cartera digital. Por ejemplo, el quiosco (901) puede ordenar al usuario que sitúe instrumento de almacenamiento de credenciales (905) en contacto físico con el lector de instrumento de almacenamiento de credenciales del quiosco (901) (por ejemplo, deslizando o insertando una tarjeta de banda magnética en un lector de banda magnética, o insertando una tarjeta con chip en una ranura de lector de tarjeta con chip), o sitúe instrumento de almacenamiento de credenciales (905) en proximidad cercana con el lector de instrumento de almacenamiento de credenciales del quiosco (901) (por ejemplo, situando una tarjeta sin contacto en proximidad cercana a un lector de tarjeta sin contacto, o situando un medio impreso con un código de barras o Código QR frente a un escáner de infrarrojos). Tras presentar el instrumento de almacenamiento de credenciales (905) al lector de instrumento de almacenamiento de credenciales del quiosco (901), el quiosco (901) accede al instrumento de almacenamiento de credenciales (905) para leer credenciales de usuario del instrumento de almacenamiento de credenciales (905).

Se ha de observar que aunque en el proceso anterior se establece primero un canal de comunicación entre el dispositivo móvil (931) y quiosco (901) antes de que se presente un instrumento de almacenamiento de credenciales al quiosco (901), en algunas realizaciones, puede presentarse al quiosco (901) un instrumento de almacenamiento de credenciales antes de conectar comunicativamente el dispositivo móvil (931) al quiosco (901). Adicionalmente, además de proporcionar entrada de usuario en la interfaz de entrada de usuario del quiosco (901) para iniciar el proceso, el proceso de provisión de la cartera digital puede iniciarse como alternativa simplemente conectando comunicativamente el dispositivo móvil (931) al quiosco (901) o presentando un instrumento de almacenamiento de credenciales al quiosco (901).

Una vez que quiosco (901) ha recuperado credenciales de usuario del instrumento de almacenamiento de credenciales (905), el quiosco (901) puede efectuar un proceso de verificación para confirmar que el usuario está autorizado para proporcionar al dispositivo móvil (931) con credenciales del instrumento de almacenamiento de credenciales (905). En algunos ejemplos, el proceso de verificación puede efectuarse por el quiosco (901) sin requerir ninguna entrada de usuario adicional. Por ejemplo, el quiosco (901) puede recuperar un número de teléfono móvil y/o un identificador de dispositivo móvil del dispositivo móvil (931) que puede usarse para consultar el nombre de abonado de servicio móvil asociado con el dispositivo móvil (931) del operador de red móvil (936). El quiosco (901) también puede recuperar el nombre en el instrumento de almacenamiento de credenciales (905), o consultar el nombre asociado con el instrumento de almacenamiento de credenciales (905) usando credenciales recuperadas del instrumento de almacenamiento de credenciales (905) contactando el sistema de emisor (935). Si el nombre de abonado de servicio móvil coincide con el nombre de usuario del instrumento de almacenamiento de credenciales (905), puede asumirse que el usuario es el propietario apropiado tanto del dispositivo móvil (931) como del instrumento de almacenamiento de credenciales (905), y que el usuario está autorizado para proporcionar el dispositivo móvil (931) con credenciales del instrumento de almacenamiento de credenciales (905).

Se ha de observar que realizaciones de la presente invención proporcionan un método más seguro de provisión del dispositivo móvil (931) en comparación con algunos procesos de provisión durante la comunicación aérea (OTA), porque el instrumento de almacenamiento de credenciales (905) está en posesión física del usuario durante el proceso de provisión de quiosco. Esto puede evitar, por ejemplo, que un usuario fraudulento proporcione a un dispositivo móvil con credenciales robadas cuando el usuario fraudulento no tiene posesión física del instrumento de almacenamiento de credenciales.

En algunos ejemplos, para seguridad adicional, antes de proceder adicionalmente con el proceso de provisión, el quiosco (901) puede solicitar que el usuario introduzca un número PIN asociado con el instrumento de almacenamiento de credenciales (905) para autenticar al usuario. El quiosco (901) puede solicitar como alternativa o adicionalmente que el usuario se registre en una cuenta en línea proporcionada por un emisor del instrumento de almacenamiento de credenciales (905) a través de un navegador con capacidad web, y/o solicitar que el usuario se registre en una cuenta en línea proporcionada por el operador de red móvil del dispositivo móvil (931).

Después de que el quiosco (901) determina que el usuario está autorizado para proporcionar al dispositivo móvil (931) con credenciales del instrumento de almacenamiento de credenciales (905), el quiosco (901) puede enviar un registro o petición de activación al TSM (933). En algunos ejemplos, el registro o petición de activación se envía con los datos de personalización adecuados (por ejemplo, credenciales recuperadas del instrumento de almacenamiento de credenciales (905)). El TSM (933) puede procesar el registro o petición de activación personalizando una aplicación de cartera digital con los datos de personalización apropiados, desbloquear el SE del dispositivo móvil (931) y proporcionar la aplicación de cartera digital personalizada al quiosco (901) para descargar al dispositivo

móvil (931). En algunos ejemplos, por ejemplo, en los que el dispositivo móvil (931) incluye una aplicación de cartera digital precargada, el TSM (933) puede procesar la petición desbloqueando el SE del dispositivo móvil (931) para permitir que el quiosco (901) transfiera credenciales recuperadas del instrumento de almacenamiento de credenciales (905) en el SE del dispositivo móvil (931). De acuerdo con algunos ejemplos, alguna o toda de la funcionalidad realizada por el TSM (9) puede integrarse en el quiosco (901).

Dependiendo del tipo de instrumento de almacenamiento de credenciales (905) que se use, pueden necesitarse credenciales adicionales que no se almacenan en el instrumento de almacenamiento de credenciales (905), o credenciales adicionales que no pueden leerse por el lector de instrumento de almacenamiento de credenciales del quiosco (901) para habilitar que el dispositivo móvil (931) realice transacciones sin contacto. Por ejemplo, si el instrumento de almacenamiento de credenciales (905) es una tarjeta de crédito, puede requerirse un valor de verificación de tarjeta dinámico (dCVV) para realizar transacciones de pago sin contacto efectuadas por el dispositivo móvil (931). En tales ejemplos, durante el proceso de provisión de la cartera digital, el quiosco (901) puede enviar un registro o petición de activación al sistema de emisor (935) para obtener credenciales adicionales tal como un software de dCVV que puede usarse por el dispositivo móvil (931) para generar un dCVV cuando realiza transacciones de pago sin contacto. Las credenciales adicionales (por ejemplo, software de dCVV) obtenidas del sistema de emisor (935) pueden almacenarse en el SE del dispositivo móvil (931) junto con credenciales recuperadas del instrumento de almacenamiento de credenciales (905) durante el proceso de provisión de la cartera digital. En algunos ejemplos, las credenciales recuperas del instrumento de almacenamiento de credenciales (905) también pueden modificarse o aumentarse por el sistema de emisor (935) antes de almacenarse en el dispositivo móvil (931). Credenciales cargadas en el SE del dispositivo móvil (931) por el quiosco (901) también pueden usar normas de cifrado de datos tal como, por ejemplo, RSA con una clave de al menos 1024 bits, norma de encriptación de datos triple (DES), norma de encriptación avanzada de 128 bits (AES), un algoritmo de encriptación de flujo de RC4 que usa una longitud de clave mínima de 128 bits, etc.

Una vez que credenciales del instrumento de almacenamiento de credenciales (905) se han cargado en una aplicación de cartera digital del dispositivo móvil (931), el quiosco (901) puede proporcionar instrucciones visuales y/o de audio preguntando al usuario si el usuario desea cargar credenciales de instrumentos de almacenamiento de credenciales adicionales en el dispositivo móvil (931). Si es así, el proceso descrito anteriormente puede repetirse para cada instrumento de almacenamiento de credenciales. En algunos ejemplos, los instrumentos de almacenamiento de credenciales pueden procesarse en un modo por lotes. Por ejemplo, el quiosco (901) puede permitir que un usuario deslice primero múltiples instrumentos de almacenamiento de credenciales antes de que el quiosco (901) comience a cargar las respectivas credenciales en el dispositivo móvil (931). Credenciales de los múltiples instrumentos de almacenamiento de credenciales pueden almacenarse temporalmente en el quiosco (901), y una vez que el usuario ha presentado el número deseado de instrumentos de almacenamiento de credenciales al quiosco (901), el quiosco (901) a continuación comienza el proceso de provisión de carga las credenciales en el dispositivo móvil (931).

De acuerdo con algunos ejemplos, el quiosco (901) también puede usarse para transferir credenciales desde una aplicación de cartera digital a otra. Por ejemplo, cuando un usuario compra un nuevo dispositivo móvil, el usuario puede tener ya una aplicación de cartera digital personalizada en el antiguo dispositivo móvil del usuario. El usuario puede querer transferir las credenciales almacenadas en el antiguo dispositivo móvil al nuevo. En lugar de presentar para lectura instrumentos de almacenamiento de credenciales para quiosco (901) individuales, el usuario puede situar el antiguo dispositivo móvil del usuario en proximidad cercana al lector de instrumento de almacenamiento de credenciales del quiosco (901). El quiosco (901) puede a continuación acceder a la aplicación de cartera digital almacenada en el antiguo dispositivo móvil para recuperar las credenciales almacenadas en el mismo. Después de recuperar las credenciales del antiguo dispositivo móvil, el quiosco (901) puede proporcionar al nuevo dispositivo móvil con las credenciales recuperadas usando el proceso descrito anteriormente.

Además de o como una alternativa a la provisión del dispositivo móvil (931), el quiosco (901) también puede cargar credenciales en una cartera digital basada en la nube (934). La cartera digital basada en la nube (934) permite que credenciales a almacenar en almacenamiento accesible por red que es externo al dispositivo móvil (931). Usar la cartera digital basada en la nube (934) tiene la ventaja de que una vez que las credenciales se han cargado a la cartera digital basada en la nube (934), el usuario puede evitar tener que transferir las credenciales a un nuevo dispositivo móvil cada vez que el usuario cambia de dispositivos móviles. Por lo tanto, en algunos ejemplos, un usuario puede usar el quiosco (901) para cargar credenciales desde instrumentos de almacenamiento de credenciales en la cartera digital basada en la nube (934) sin la presencia de un dispositivo móvil.

En algunos ejemplos, el quiosco (901) puede realizar funciones de gestión de cartera digital adicionales. Por ejemplo, una vez que se ha proporcionado y personalizado la aplicación de cartera digital en el dispositivo móvil (931), el quiosco (901) puede permitir que un usuario compre medios digitales para el dispositivo móvil (931) usando credenciales cargadas en la aplicación de cartera digital. El quiosco (901) también puede permitir que un usuario deposite o añada valor en cuentas asociadas con las credenciales almacenadas en la aplicación de cartera digital. Por ejemplo, el quiosco (901) puede permitir que el usuario añada valor a una cuenta de tarifa de tránsito almacenada en la aplicación de cartera digital. Sin embargo, debería observarse que estas funciones adicionales son diferentes del proceso de provisión de la cartera digital en que estas funciones adicionales requieren que la

aplicación de cartera digital tenga las credenciales necesarias antes de que estas funciones puedan realizarse. En contraste, el proceso de provisión descrito en este documento se usa para proporcionar al dispositivo móvil con credenciales que la aplicación de cartera digital carecía antes de proporcionarse por el quiosco (901). Quioscos de acuerdo con realizaciones de la invención pueden o no proporcionar las funciones adicionales anteriormente mencionadas.

La Figura 9D ilustra un diagrama de flujo de un método (950) realizado por un quiosco u otros dispositivos informáticos adecuados para proporcionar a una aplicación de cartera digital de un dispositivo móvil de acuerdo con algunas realizaciones. En el bloque (951), se establece un canal de comunicación entre el dispositivo móvil de un usuario. El canal de comunicación puede ser una conexión por cable o una conexión inalámbrica como se describe anteriormente. En el bloque (952), se accede a un instrumento de almacenamiento de credenciales tal como una tarjeta de banda magnética, una tarjeta con chip u otros instrumentos de almacenamiento de credenciales descritos anteriormente para recuperar credenciales almacenadas en el instrumento de almacenamiento de credenciales. En el bloque (953), se determina si el usuario está autorizado para proporcionar a una aplicación de cartera digital para el dispositivo móvil con las credenciales recuperadas. Esta determinación puede hacerse de acuerdo con cualquiera de los procesos descritos anteriormente. Si se determina que el usuario no está autorizado, en el bloque (956), el proceso se termina sin la provisión del dispositivo móvil. Si se determina que el usuario está autorizado, a continuación en el bloque (954), se hace una petición para desbloquear el elemento seguro (SE) del dispositivo móvil. El SE puede desbloquearse con una clave de seguridad o testigo proporcionado por un TSM o por un quiosco con funcionalidad de TSM integrada. Una vez que el SE del dispositivo móvil se desbloquea, se proporciona una aplicación de cartera digital para el dispositivo móvil descargando las credenciales de usuario recuperadas desde el instrumento de almacenamiento de credenciales en el SE. En algunas realizaciones, las credenciales de usuario pueden modificarse, aumentarse (por ejemplo, con un CVV2), y/o cifrarse antes de almacenarse en el SE del dispositivo móvil. El método (950) puede repetirse para múltiples instrumentos de almacenamiento de credenciales. Posterior al proceso de provisión, el SE de dispositivo móvil se bloquea para evitar acceso no autorizado.

Debería entenderse que el método (950) para proporcionar a una aplicación de cartera digital de un dispositivo móvil puede incluir operaciones adicionales que no se representan en la Figura 9D, o puede incluir menos operaciones en otros ejemplos. Adicionalmente, algunas de las operaciones pueden realizarse en un orden diferente al que se representa.

La Figura 10 muestra un diagrama de flujo en carriles que ilustra el flujo entre un dispositivo móvil (931), un quiosco (901), y un servidor accesible de forma remota tal como un emisor de credenciales de pago (935) o un TSM (933) de acuerdo con realizaciones.

Un consumidor puede presentar (1001) su dispositivo de pago portátil o instrumento de almacenamiento de credenciales (por ejemplo, una tarjeta de pago) en el quiosco que puede extraer credenciales de pago del dispositivo de pago portátil. Por ejemplo, el consumidor puede insertar su tarjeta de pago en un quiosco y puede solicitarse una transacción de “transferencia de credenciales”. Puede avisarse al consumidor para su PIN de tarjeta de pago que puede introducirse en el quiosco a través de un teclado numérico. El consumidor también puede proporcionar (1002) un identificador, por ejemplo, el quiosco también puede avisar al consumidor para un “alias” que se usa como un identificador para el consumidor y su dispositivo móvil.

El quiosco puede conectarse (1003) al dispositivo móvil del consumidor como se ha descrito anteriormente para establecer (1004) una conexión. El quiosco puede usar el identificador proporcionado del consumidor para identificar el dispositivo móvil para conexión, por ejemplo, si esta es de una manera inalámbrica.

El quiosco puede enviar (1005) una petición de activación a un servidor accesible de forma remota proporcionado por un TSM para obtener autorización para almacenar las credenciales de pago en el elemento seguro asociado con el dispositivo móvil y también para desbloquear el elemento seguro. La petición de activación puede usar el identificador proporcionado por el consumidor que puede registrarse para el dispositivo móvil del consumidor y/o elemento seguro y el identificador puede usarse para identificar (1006) el dispositivo móvil y su elemento seguro. El TSM puede desbloquear (1007/1008) el elemento seguro asociado con el dispositivo móvil.

Las credenciales de pago pueden proporcionarse (1009/1010) al elemento seguro del dispositivo móvil usando la conexión al quiosco. Estos pueden proporcionarse de forma segura al elemento seguro.

Credenciales adicionales que no se almacenan en el dispositivo de pago portátil pueden necesitarse también que se almacenen en el elemento seguro para habilitar que el dispositivo móvil realice transacciones sin contacto. Por ejemplo, un valor de verificación de tarjeta dinámico (dCVV) puede requerirse para realizar transacciones de pago sin contacto efectuadas por el dispositivo móvil. En tales realizaciones, el quiosco puede enviar una solicitud de registro (1011) a un servidor accesible de forma remota de un sistema de emisor para obtener credenciales adicionales. El identificador puede incluirse en la petición y usarse por el servidor accesible de forma remota para identificar (1012) las credenciales adicionales correctas. Las credenciales adicionales pueden ser, en un ejemplo, software de dCVV que puede usarse por el dispositivo móvil para generar un dCVV cuando realiza transacciones de pago sin contacto. La solicitud de registro puede incluir el identificador proporcionado por el consumidor para obtener

las credenciales adicionales correctas para el dispositivo de pago portátil del consumidor.

Las credenciales adicionales (por ejemplo, software de dCVV) obtenido del sistema de emisor puede transmitirse (1013/1014) a y almacenarse en el elemento seguro asociado con el dispositivo móvil junto con credenciales de pago recuperado del quiosco durante el proceso de provisión de la cartera digital. Como alternativa, las credenciales adicionales pueden comunicarse directamente al elemento seguro del dispositivo móvil.

La Figura 11 ilustra un ejemplo de un dispositivo informático (1100) en el que pueden implementarse diversos aspectos de la divulgación. El dispositivo informático (1100) puede ser adecuado para almacenar y ejecutar código de programa informático. Los diversos participantes y elementos en los diagramas de sistema anteriormente descritos pueden usar cualquier número adecuado de subsistemas o componentes del dispositivo informático (1100) para facilitar las funciones descritas en este documento.

El dispositivo informático (1100) puede incluir subsistemas o componentes interconectados a través de una infraestructura de comunicación (1105) (por ejemplo, un bus de comunicaciones, un dispositivo de barra cruzada o una red). El dispositivo informático (1100) puede incluir al menos un procesador central (1110) y al menos un componente de memoria en la forma de medio legible por ordenador.

Los componentes de memoria pueden incluir la memoria de sistema (1115), que puede incluir memoria de sólo lectura (ROM) y memoria de acceso aleatorio (RAM). Un sistema básico de entrada/salida (BIOS) puede almacenarse en ROM. Software de sistema puede almacenarse en la memoria de sistema (1115) incluyendo software de sistema operativo.

Los componentes de memoria también pueden incluir la memoria secundaria (1120). La memoria secundaria (1120) puede incluir un disco fijo (1121), tal como una unidad de disco duro y, opcionalmente, una o más interfaces de almacenamiento extraíble (1122) para componentes de almacenamiento extraíble (1123).

Las interfaces de almacenamiento extraíble (1122) pueden ser en forma de unidades de almacenamiento extraíbles (por ejemplo, unidades de cinta magnética, unidades de disco óptico, unidades de disco flexible, etc.) para correspondientes componentes de almacenamiento extraíble (por ejemplo, una cinta magnética, un disco óptico, un disco flexible, etc.), que puede escribirse o leerse por la unidad de almacenamiento extraíble.

Las interfaces de almacenamiento extraíble (1122) también puede ser en forma de puertos o conexiones para interactuar con otras formas de componentes de almacenamiento extraíble (1123) tal como una unidad de memoria flash, disco duro externo o chip de memoria extraíble, etc.

El dispositivo informático (1100) puede incluir una interfaz de comunicaciones externa (1130) para operación del dispositivo informático (1100) en un entorno en red habilitando transferencia de datos entre múltiples dispositivos informáticos (1100). Datos transferidos a través de la interfaz de comunicaciones externa (1130) puede ser en forma de señales, que pueden ser electrónicas, electromagnéticas, ópticas, radio u otros tipos de señal.

La interfaz de comunicaciones externa (1130) puede habilitar comunicación de datos entre el dispositivo informático (1100) y otros dispositivos informáticos incluyendo servidores e instalaciones almacenamiento externas. Servicios web pueden ser accesibles por el dispositivo informático (1100) a través de la interfaz de comunicaciones (1130).

La interfaz de comunicaciones externa (1130) también puede habilitar otras formas de comunicación a y desde el dispositivo informático (1100) incluyendo comunicación por voz, comunicación de campo cercano, Bluetooth, etc.

El medio legible por ordenador en forma de los diversos componentes de memoria puede proporcionar almacenamiento de instrucciones ejecutables por ordenador, estructuras de datos, módulos de programa y otros datos. Puede proporcionarse un producto de programa informático por un medio legible por ordenador que ha almacenado código de programa legible por ordenador ejecutable por el procesador central (1110).

Puede proporcionarse un producto de programa informático por un medio legible por ordenador no transitorio, o puede proporcionarse a través de una señal u otro medio transitorio a través de la interfaz de comunicaciones (1130).

Interconexión a través de la infraestructura de comunicación (1105) permite que un procesador central (1110) se comunique con cada subsistema o componente y controle la ejecución de instrucciones desde los componentes de memoria, así como el intercambio de información entre subsistemas o componentes.

Periféricos (tal como impresoras, escáneres, cámaras, o similar) y dispositivos de entrada/salida (I/O) (tal como un ratón, panel táctil, teclado, micrófono, palanca de mando o similar) pueden acoplarse al dispositivo informático (1100) o bien directamente o bien a través de un controlador de I/O (1135). Estos componentes pueden conectarse al dispositivo informático (1100) mediante cualquier número de medios conocidos en la técnica, tal como un puerto en serie.

Pueden acoplarse uno o más monitores (1145) a través de un adaptador de visualización o video (1140) al dispositivo informático (1100).

La Figura 12 muestra un diagrama de bloques de un dispositivo de comunicación (1200) que puede usarse en las realizaciones de la divulgación. El dispositivo de comunicación (1200) puede ser un teléfono celular, un teléfono básico, un teléfono inteligente, un teléfono por satélite o un dispositivo informático que tiene capacidad telefónica.

El dispositivo de comunicación (1200) puede incluir un procesador (1205) (por ejemplo, un microprocesador) para procesar las funciones del dispositivo de comunicación (1200) y un visualizador (1220) para permitir que un usuario vea los números de teléfono y otra información y mensajes. El dispositivo de comunicación (1200) puede incluir adicionalmente un elemento de entrada (1225) para permitir que un usuario introduzca información en el dispositivo (por ejemplo, botones entrada, pantalla táctil, etc.), un altavoz (1230) para permitir que el usuario escuche comunicación por voz, música, etc., y un micrófono (1235) para permitir que el usuario transmita su voz a través del dispositivo de comunicación (1200).

El procesador (1210) del dispositivo de comunicación (1200) puede conectarse a una memoria (1215). La memoria (1215) puede ser en forma de un medio legible por ordenador que almacena datos y, opcionalmente, instrucciones ejecutables por ordenador. La memoria (1215).

El dispositivo de comunicación (1200) también puede incluir un elemento de comunicación (1240) para conexión a canales de comunicación (por ejemplo, una red de teléfono celular, red de transmisión de datos, red Wi-Fi, red de teléfono por satélite, red de Internet, red de Internet por satélite, etc.). El elemento de comunicación (1240) puede incluir un elemento de transferencia inalámbrica asociado, tal como una antena.

El elemento de comunicación (1240) puede incluir un módulo de identidad de abonado (SIM) en forma de un circuito integrado que almacena una identidad de abonado de servicio móvil internacional y la clave relacionada usada para identificar y autenticar a un abonado que usa el dispositivo de comunicación (1200). Uno o más módulos de identidad de abonado pueden ser extraíbles del dispositivo de comunicación (1200) o embeberse en el dispositivo de comunicación (1200).

El dispositivo de comunicación (1200) puede incluir adicionalmente un elemento sin contacto (1250), que se implementa habitualmente en forma de un chip semiconductor (u otros elementos de almacenamiento de datos) con un elemento de transferencia inalámbrica asociado, tal como una antena. El elemento sin contacto (1250) puede asociarse con (por ejemplo, embeberse dentro de) el dispositivo de comunicación (1200) y datos o instrucciones de control transmitidas a través de una red celular pueden aplicarse al elemento sin contacto (1250) por medio de una interfaz de elemento sin contacto (no mostrado). La interfaz de elemento sin contacto puede funcionar para permitir el intercambio de datos y/o instrucciones de control entre dispositivo móvil circuitería (y, por lo tanto, la red celular) y el elemento sin contacto (1250).

El elemento sin contacto (1250) puede ser capaz de transferir y recibir datos usando una capacidad de comunicación de campo cercano (NFC) (o medio de comunicación de campo cercano) habitualmente de acuerdo con un protocolo normalizado o mecanismo de transferencia de datos (por ejemplo, ISO 14443/NFC). Capacidad de comunicación de campo cercano es una capacidad de comunicación de corto alcance, tal como identificación por frecuencia de radio (RFID), Bluetooth, infrarrojos u otra capacidad de transferencia de datos que puede usarse para intercambiar datos entre el dispositivo de comunicación (1200) y un dispositivo de interrogación. Por lo tanto, el dispositivo de comunicación (1200) puede ser capaz de comunicar y transferir datos y/o instrucciones de control a través tanto de una red celular como capacidad de comunicación de campo cercano.

Dispositivos de comunicación (1200) que soportan pago sin contactos móvil habitualmente soportan transacciones sin contacto usando el protocolo de comunicación sin contacto de EMV (EMV-CCP), que se basa en ISO 14443, para interactuar con dispositivos de acceso de comerciante. Esta capacidad se cumple habitualmente implementando NFC. La capacidad de NFC en el dispositivo de comunicación (1200) podría habilitarse por un chip NFC embebido o mediante la adición de una tarjeta o accesorio de memoria externa que contiene el chip NFC. Adicionalmente, el dispositivo de comunicación (1200) habitualmente incluye un elemento seguro (SE) (1260) o bien embebido en el microteléfono o bien en la tarjeta de módulo de identidad de abonado (SIM). El SE (1260) también puede incluirse en un dispositivo de adición tal como una micro tarjeta Segura Digital (SD), o un componente de expansión para añadir a un componente de comunicación del dispositivo de comunicación (1200).

Los datos almacenados en la memoria (1215) pueden incluir: operación de datos relacionados con la operación del dispositivo de comunicación (1200), datos personales (por ejemplo, nombre, fecha de nacimiento, número de identificación, etc.), datos financieros (por ejemplo, información de cuenta bancaria, un número de identificación bancaria (BIN), información de número de tarjeta de crédito o débito, información de saldo de cuenta, fecha de expiración, números de cuenta de proveedores de fidelización, etc.), información de tránsito (por ejemplo, como en un billete de metro o tren), información de acceso (por ejemplo, en placas de acceso), etc. Un usuario puede transmitir estos datos desde el dispositivo de comunicación (1200) a receptores seleccionados.

El dispositivo de comunicación (1200) puede ser, entre otras cosas, un dispositivo de notificación que puede recibir mensajes de alerta e informes de acceso, un dispositivo de comerciante portátil que puede usarse para transmitir datos de control que identifican un descuento a aplicar, así como un dispositivo de consumidor portátil que puede usarse para hacer pagos.

La descripción anterior de las realizaciones de la invención se ha presentado para el propósito de ilustración; no pretende ser exhaustiva o limitar la invención a las formas precisas divulgadas. Expertos en la materia pueden apreciar que son posibles muchas modificaciones y variaciones a la vista de la anterior divulgación.

Algunas porciones de esta descripción describen las realizaciones de la invención en términos de algoritmos y representaciones simbólicas de operaciones sobre información. Estas descripciones algorítmicas y representaciones se usan comúnmente por los expertos en las técnicas de procesamiento para transmitir la sustancia de su trabajo de forma efectiva a otros expertos en la materia. Estas operaciones, mientras se describen funcional, computacional o lógicamente, se entienden para implementarse mediante programas informáticos o circuitos eléctricos equivalentes, microcódigo o similar. Las operaciones descritas pueden incorporarse en software, firmware, hardware o cualquier combinación de los mismos.

Los componentes de software o funciones descritas en esta aplicación pueden implementarse como código de software a ejecutarse por uno o más procesadores usando cualquier lenguaje informático adecuado tal como, por ejemplo, Java, C++ o Perl usando, por ejemplo, técnicas convencionales u orientadas a objeto. El código de software puede almacenarse como una serie de instrucciones, u órdenes en un medio legible por ordenador no transitorio, tal como una memoria de acceso aleatorio (RAM), una memoria de sólo lectura (ROM), un medio magnético tal como un disco duro o un disco flexible, o un medio óptico tal como un CD-ROM. Cualquier medio legible por ordenador de este tipo también puede residir en o dentro de un único aparato de cálculo, y puede estar presente en o dentro de diferentes aparatos de cálculo dentro de un sistema o red.

Cualquiera de las etapas, operaciones o procesos descritos en este documento puede realizarse o implementarse con uno o más módulos de hardware o software, solo o en combinación con otros dispositivos. En una realización, un módulo de software se implementa con un producto de programa informático que comprende un medio legible por ordenador no transitorio que contiene código de programa informático, que puede ejecutarse por un procesador informático para realizar cualquiera o todas las etapas, operaciones o procesos descritos.

REIVINDICACIONES

1. Un método para proporcionar a una aplicación de cartera digital en un dispositivo móvil (112, 212, 316, 931) con credenciales de pago que la aplicación de cartera digital carecía antes de la provisión, siendo las credenciales de pago usables por el dispositivo móvil (112, 212, 316, 931) en la realización de un pago sin contacto, realizándose el método en un sistema de provisión (140, 240, 340, 901) y comprendiendo las etapas de:

recepción (402, 422, 704) de credenciales de pago desde un punto de venta o dispositivo de ATM (120, 222, 320, 920) en un mensaje de transacción financiera, habiéndose obtenido las credenciales de pago por el punto de venta o dispositivo de ATM (120, 222, 320, 920) desde un dispositivo de pago portátil (114, 214, 314, 905) a través de una interfaz de comunicaciones con o sin contacto del punto de venta o dispositivo de ATM (120, 222, 320, 920) presentándose el dispositivo de pago portátil (114, 214, 314, 905) por un consumidor en el punto de venta o dispositivo de ATM (120, 222, 320, 920);
recepción (404, 424, 704), desde el punto de venta o dispositivo de ATM (120, 222, 320, 920), de un identificador introducido por el consumidor en el mensaje de transacción financiera;
identificación (406, 430, 705) de un dispositivo móvil (112, 212, 316, 931) o un elemento seguro (113) en el dispositivo móvil (112, 212, 316, 931) que corresponde al identificador; y
comunicación (410, 432, 707) de las credenciales de pago al dispositivo móvil identificado (112, 212, 316, 931) o el elemento seguro (113) en el dispositivo móvil (112, 212, 316, 931), provocando que las credenciales de pago se almacenen de forma segura en el elemento seguro (113) del dispositivo móvil (112, 212, 316, 931), siendo el elemento seguro (113) uno del grupo de: un elemento seguro (113) proporcionado en el dispositivo móvil (112, 212, 316, 931), un elemento seguro (113) embebido en una capa (318) que se sitúa entre un componente de comunicación (317) del dispositivo móvil (112, 212, 316, 931) y una interfaz de componente de comunicación del dispositivo móvil (112, 212, 316, 931), y un elemento seguro (113) proporcionado en un componente de comunicación (317) del dispositivo móvil (112, 212, 316, 931).

2. El método de acuerdo con la reivindicación 1, que incluye:

solicitar (408) autorización desde un gestor de servicios confiable para acceder al elemento seguro (113); y
recibir una clave de seguridad para acceder al elemento seguro (113).

3. El método según se reivindica en una cualquiera de las reivindicaciones anteriores, que incluye:

comunicar (412) credenciales adicionales al dispositivo móvil identificado (112, 212, 316, 931) o el elemento seguro (113) a almacenar de forma segura en asociación con el dispositivo móvil (112, 212, 316, 931), en el que las credenciales adicionales se requieren en uso además de las credenciales de pago que efectúan una transacción.

4. El método de acuerdo con la reivindicación 3, que incluye:

obtener las credenciales adicionales de un servidor accesible de forma remota (140, 240, 340,) usando el identificador y reenviar las credenciales adicionales al dispositivo móvil (112, 212, 316, 931).

5. El método de acuerdo con la reivindicación 3 o la reivindicación 4, en el que las credenciales adicionales son en forma de un algoritmo de verificación dinámico para generar valores de verificación dinámicos.

6. El método según se reivindica en una cualquiera de las reivindicaciones anteriores, en el que el método se repite para múltiples credenciales de pago a almacenar de forma segura en asociación con un único dispositivo móvil.

7. El método según se reivindica en una cualquiera de las reivindicaciones anteriores, en el que el método se usa para transferir credenciales de pago a un segundo dispositivo móvil desde su almacenamiento seguro existente en un primer dispositivo móvil, en el que el dispositivo de pago portátil es el primer dispositivo móvil.

8. Un método para proporcionar a una aplicación de cartera digital en un dispositivo móvil (112, 212, 316, 931) con credenciales de pago que la aplicación de cartera digital carecía antes de la provisión, siendo las credenciales de pago usables por el dispositivo móvil (112, 212, 316, 931) en la realización de un pago sin contacto, realizándose el método en un punto de venta o dispositivo de ATM (120, 222, 320, 920) y comprendiendo las etapas de:

obtención (502), por el punto de venta o dispositivo de ATM (120, 222, 320, 920), de credenciales de pago desde un dispositivo de pago portátil (114, 214, 314, 905) a través de una interfaz de comunicaciones con o sin contacto del punto de venta o dispositivo de ATM (120, 222, 320, 920) presentándose el dispositivo de pago portátil (114, 214, 314, 905) por un consumidor en el punto de venta o dispositivo de ATM (120, 222, 320, 920);
recepción (504), por el punto de venta o dispositivo de ATM (120, 222, 320, 920), de un identificador introducido por el consumidor en el punto de venta o dispositivo de ATM (120, 222, 320, 920); y
comunicación (506), por el punto de venta o dispositivo de ATM (120, 222, 320, 920), de las credenciales de pago e identificador en un mensaje de transacción financiera a un sistema de provisión (140, 240, 340, 901) para

comunicación adicional de las credenciales de pago al dispositivo móvil (112, 212, 316, 931) o un elemento seguro (113) del dispositivo móvil, provocando que las credenciales de pago se almacenen de forma segura en el elemento seguro (113), siendo el elemento seguro (113) uno del grupo de: un elemento seguro (113) proporcionado en el dispositivo móvil (112, 212, 316, 931), un elemento seguro (113) embebido en una capa (318) que se sitúa entre un componente de comunicación (317) del dispositivo móvil (112, 212, 316, 931) y una interfaz de componente de comunicación del dispositivo móvil (112, 212, 316, 931), y un elemento seguro (113) proporcionado en un componente de comunicación (317) del dispositivo móvil (112, 212, 316, 931).

9. Un método para proporcionar a una aplicación de cartera digital en un dispositivo móvil (112, 212, 316, 931) con credenciales de pago que la aplicación de cartera digital carecía antes de la provisión, siendo las credenciales de pago usables por el dispositivo móvil (112, 212, 316, 931) en la realización de un pago sin contacto, realizándose el método en un punto de venta o dispositivo de ATM (120, 222, 320, 920) y comprendiendo las etapas de:

obtención, por el punto de venta o dispositivo de ATM (120, 222, 320, 920), de credenciales de pago desde un dispositivo de pago portátil (114, 214, 314, 905) a través de interfaz de comunicaciones con o sin contacto del punto de venta o dispositivo de ATM (120, 222, 320, 920) presentándose (1001) el dispositivo de pago portátil (114, 214, 314, 905) por un consumidor en el punto de venta o dispositivo de ATM (120, 222, 320, 920);
recepción, por el punto de venta o dispositivo de ATM (120, 222, 320, 920), de un identificador introducido (1002) por el consumidor en el punto de venta o dispositivo de ATM (120, 222, 320, 920); y
comunicación (1005), por el punto de venta o dispositivo de ATM (120, 222, 320, 920), del identificador con una petición de activación a un gestor de servicios confiable (933, 935) para desbloquear (1008) un elemento seguro (113) en el dispositivo móvil (112, 212, 316) identificado por el identificador,
comunicación (1009, 1010), por el punto de venta o dispositivo de ATM (120, 222, 320, 920) de las credenciales de pago al dispositivo móvil (112, 212, 316, 931) o el elemento seguro desbloqueado (113) del dispositivo móvil, provocando que las credenciales de pago se almacenen de forma segura en el elemento seguro desbloqueado (113), siendo el elemento seguro (113) uno del grupo de: un elemento seguro (113) proporcionado en el dispositivo móvil (112, 212, 316, 931), un elemento seguro (113) embebido en una capa (318) que se sitúa entre un componente de comunicación (317) del dispositivo móvil (112, 212, 316, 931) y una interfaz de componente de comunicación del dispositivo móvil (112, 212, 316, 931), y un elemento seguro (113) proporcionado en un componente de comunicación (317) del dispositivo móvil (112, 212, 316, 931).

10. Un sistema (100, 200, 300) para proporcionar a una aplicación de cartera digital en un dispositivo móvil (112, 212, 316, 931) con credenciales de pago que la aplicación de cartera digital carecía antes de la provisión, siendo las credenciales de pago usables por el dispositivo móvil (112, 212, 316, 931) en la realización de un pago sin contacto, incluyendo un sistema de provisión (140, 240, 340, 901) que comprende:

un receptor de credenciales de pago (602) para recibir credenciales de pago desde un punto de venta o dispositivo de ATM (120, 222, 320, 920) en un mensaje de transacción financiera, habiéndose obtenido las credenciales de pago por el punto de venta o dispositivo de ATM (120, 222, 320, 920) desde un dispositivo de pago portátil (114, 214, 314, 905) a través de una interfaz de comunicaciones con o sin contacto del punto de venta o dispositivo de ATM (120, 222, 320, 920) presentándose el dispositivo de pago portátil (114, 214, 314, 905) por un consumidor en el punto de venta o dispositivo de ATM (120, 222, 320, 920);
un receptor de identificador (604) para recibir, desde el punto de venta o dispositivo de ATM (120, 222, 320, 920), un identificador introducido por el consumidor en el mensaje de transacción financiera;
un componente de identificación (610) para identificar un dispositivo móvil (112, 212, 316, 931) o un elemento seguro (113) en el dispositivo móvil (112, 212, 316, 931) que corresponde al identificador; y
un módulo de comunicación (612) para comunicar las credenciales de pago al dispositivo móvil identificado (112, 212, 316, 931) o el elemento seguro (113) en el dispositivo móvil (112, 212, 316, 931) a almacenar de forma segura en el elemento seguro (113) del dispositivo móvil (112, 212, 316, 931), siendo el elemento seguro (113) uno del grupo de: un elemento seguro (113) proporcionado en el dispositivo móvil (112, 212, 316, 931), un elemento seguro (113) embebido en una capa (318) que se sitúa entre un componente de comunicación (317) del dispositivo móvil (112, 212, 316, 931) y una interfaz de componente de comunicación del dispositivo móvil (112, 212, 316, 931), y elemento seguro (113) proporcionado en un componente de comunicación (317) del dispositivo móvil (112, 212, 316, 931).

11. El sistema de acuerdo con la reivindicación 10, en el que el sistema incluye:

el punto de venta o dispositivo de ATM (120, 222, 320, 920) que comprende:
un componente de obtención de credenciales de pago (652) para obtener credenciales de pago desde el dispositivo de pago portátil (114, 214, 314, 905) a través de una interfaz de comunicaciones con o sin contacto presentándose el dispositivo de pago portátil (114, 214, 314, 905) por el consumidor en el punto de venta o dispositivo de ATM;
un receptor de identificador (654) para recibir el identificador introducido por el consumidor en el punto de venta o dispositivo de ATM;
un módulo de comunicación (656) para comunicar las credenciales de pago e identificador al sistema de provisión (140, 240, 340, 901) para comunicación adicional de las credenciales de pago al dispositivo móvil (112,

212, 316, 931) a almacenar de forma segura en el elemento seguro (113) del dispositivo móvil (112, 212, 316, 931).

12. Un producto de programa informático para proporcionar a una aplicación de cartera digital en un dispositivo móvil (112, 212, 316, 931) con credenciales de pago que la aplicación de cartera digital carecía antes de la provisión, siendo las credenciales de pago usables por el dispositivo móvil (112, 212, 316, 931) en la realización de un pago sin contacto, comprendiendo el producto de programa informático un medio legible por ordenador que ha almacenado código de programa legible por ordenador para realizar las etapas de:

recepción (402, 422, 704) de credenciales de pago desde un punto de venta o dispositivo de ATM (120, 222, 320, 920) en un mensaje de transacción financiera, habiéndose obtenido las credenciales de pago por el punto de venta o dispositivo de ATM (120, 222, 320, 920) desde un dispositivo de pago portátil (114, 214, 314, 905) a través de una interfaz de comunicaciones con o sin contacto del punto de venta o dispositivo de ATM (120, 222, 320, 920) presentándose el dispositivo de pago portátil (114, 214, 314, 905) por un consumidor en el punto de venta o dispositivo de ATM (120, 222, 320, 920);
recepción (404, 424, 704), desde el punto de venta o dispositivo de ATM (120, 222, 320, 920) en el mensaje de transacción financiera, de un identificador introducido por el consumidor;
identificación (406, 430, 705) de un dispositivo móvil (112, 212, 316, 931) o un elemento seguro (113) en el dispositivo móvil (112, 212, 316, 931) que corresponde al identificador; y
comunicar (410, 432, 707) las credenciales de pago al dispositivo móvil identificado (112, 212, 316, 931) o el elemento seguro (113) en el dispositivo móvil (112, 212, 316, 931), provocando que las credenciales de pago se almacenen de forma segura en el elemento seguro (113) del dispositivo móvil (112, 212, 316, 931), siendo el elemento seguro (113) uno del grupo de: un elemento seguro (113) proporcionado en el dispositivo móvil (112, 212, 316, 931), un elemento seguro (113) embebido en una capa (318) que se sitúa entre un componente de comunicación (317) del dispositivo móvil (112, 212, 316, 931) y una interfaz de componente de comunicación del dispositivo móvil (112, 212, 316, 931), y un elemento seguro (113) proporcionado en un componente de comunicación (317) del dispositivo móvil (112, 212, 316, 931).

13. Un producto de programa informático para proporcionar a una aplicación de cartera digital en un dispositivo móvil (112, 212, 316, 931) con credenciales de pago que la aplicación de cartera digital carecía antes de la provisión, siendo las credenciales de pago usables por el dispositivo móvil (112, 212, 316, 931) en la realización de un pago sin contacto, comprendiendo el producto de programa informático un medio legible por ordenador que ha almacenado código de programa legible por ordenador para realizar las etapas de:

obtención, por un punto de venta o dispositivo de ATM (120, 222, 320, 920), credenciales de pago desde un dispositivo de pago portátil (114, 214, 314, 905) a través de interfaz de comunicaciones con o sin contacto del punto de venta o dispositivo de ATM (120, 222, 320, 920) presentándose (1001) el dispositivo de pago portátil (114, 214, 314, 905) por un consumidor en el punto de venta o dispositivo de ATM (120, 222, 320, 920);
recepción, por el punto de venta o dispositivo de ATM (120, 222, 320, 920), de un identificador introducido (1002) por el consumidor en el punto de venta o dispositivo de ATM (120, 222, 320, 920); y
comunicación (1005), por el punto de venta o dispositivo de ATM (120, 222, 320, 920), del identificador con una petición de activación a un gestor de servicios confiable (933, 935) para desbloquear (1008) un elemento seguro (113) en el dispositivo móvil (112, 212, 316) identificado por el identificador,
comunicación (1009, 1010), por el punto de venta o dispositivo de ATM (120, 222, 320, 920) de las credenciales de pago al dispositivo móvil (112, 212, 316, 931) o el elemento seguro desbloqueado (113), provocando que las credenciales de pago se almacenen de forma segura en el elemento seguro desbloqueado (113) del dispositivo móvil, siendo el elemento seguro (113) uno del grupo de: un elemento seguro (113) proporcionado en el dispositivo móvil (112, 212, 316, 931), un elemento seguro (113) embebido en una capa (318) que se sitúa entre un componente de comunicación (317) del dispositivo móvil (112, 212, 316, 931) y una interfaz de componente de comunicación del dispositivo móvil (112, 212, 316, 931), y un elemento seguro (113) proporcionado en un componente de comunicación (317) del dispositivo móvil (112, 212, 316, 931).

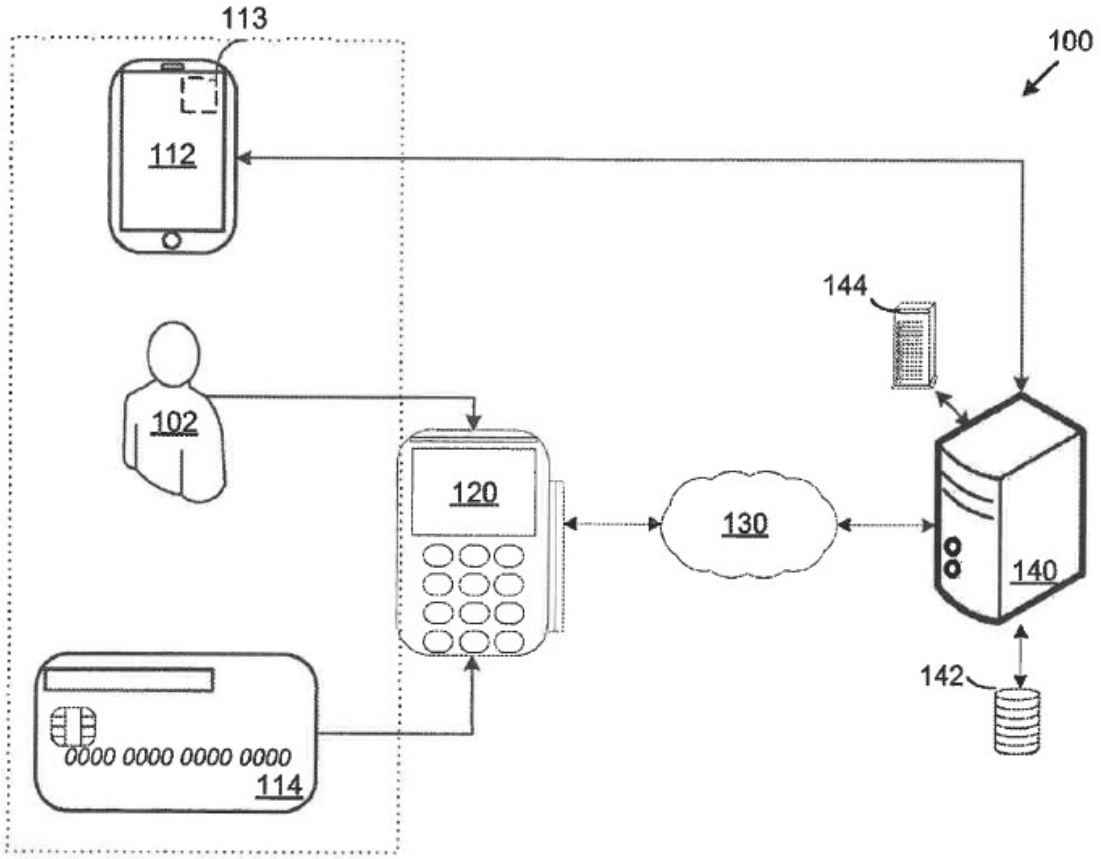

FIG. 1

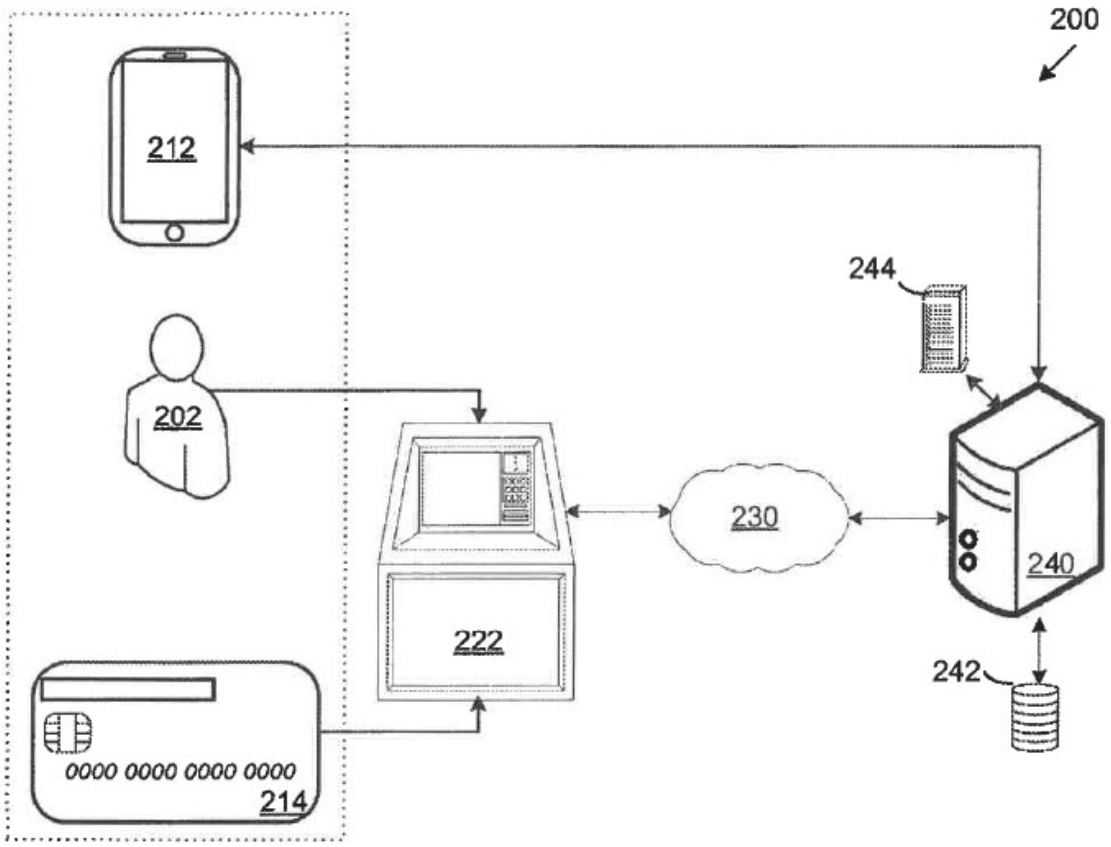

FIG. 2

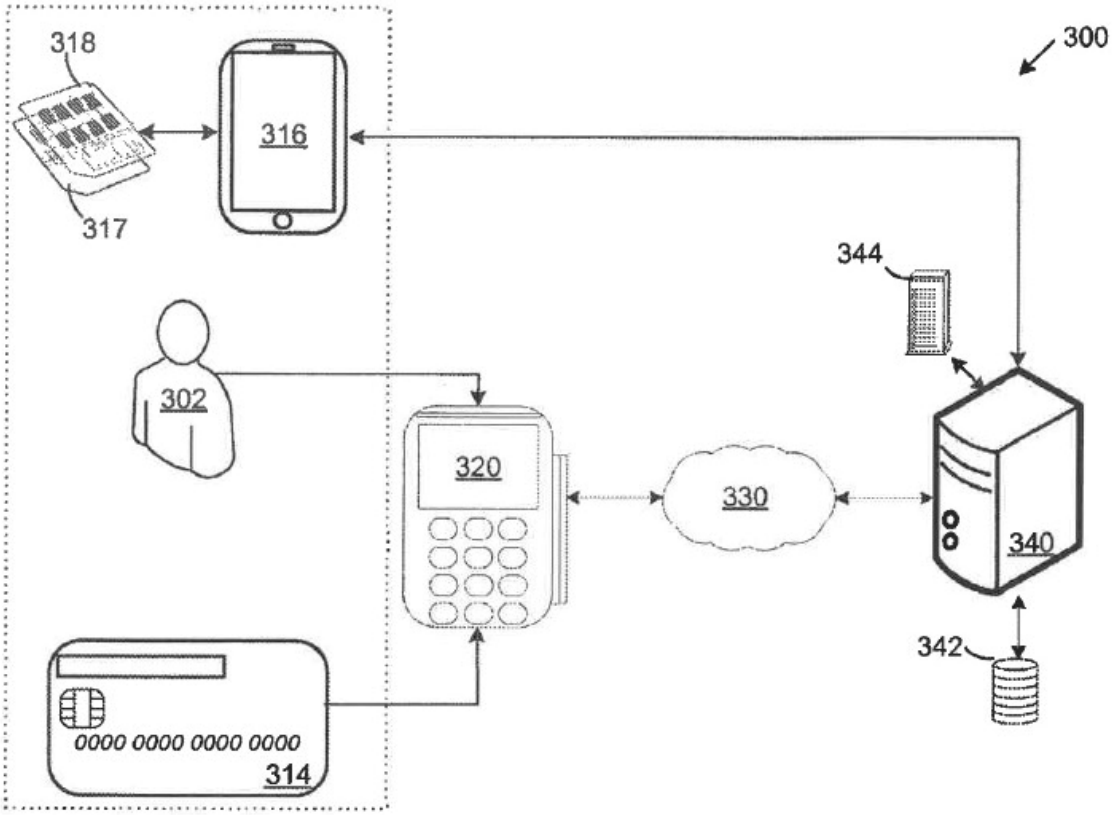

FIG. 3


Inicio
Recibir credenciales de pago desde dispositivo de recepción 402
Recibir un identificador desde dispositivo de recepción 404
Identificar un dispositivo móvil y/o elemento seguro que corresponde al identificador 406
Solicitar autorización/acceso a elemento seguro desde TSM 408
Comunicar las credenciales de pago o una derivación de las mismas, al dispositivo móvil identificado para almacenamiento en un elemento seguro del dispositivo móvil 410
Solicitar o suministrar credenciales adicionales y comunicar las credenciales adicionales al dispositivo móvil identificado 412

FIG. 4A

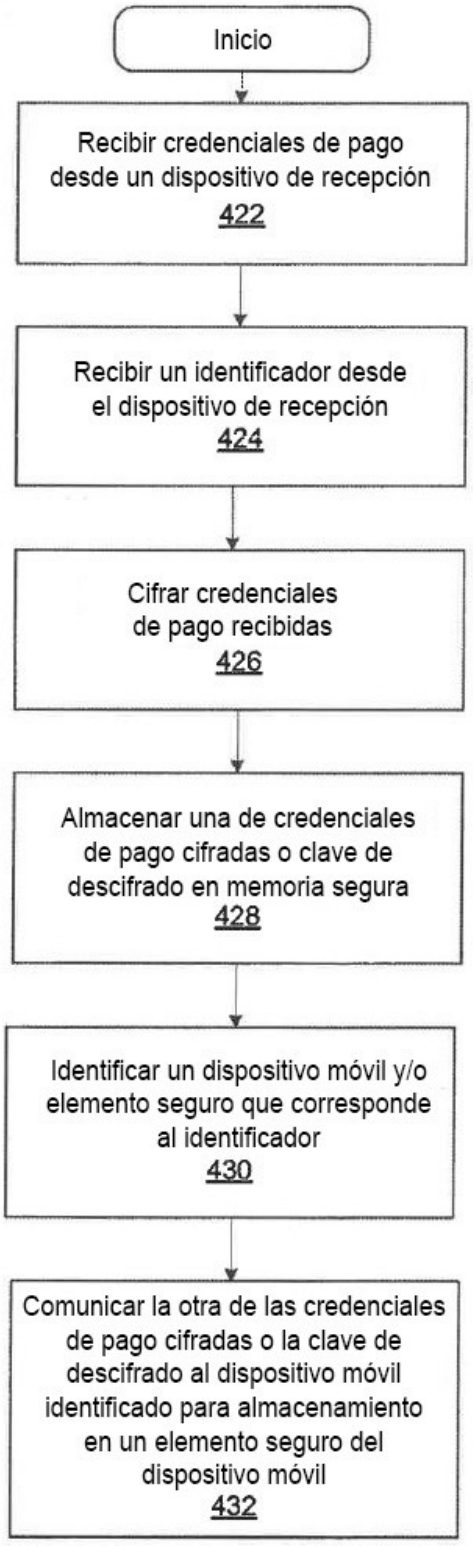
Inicio
Recibir credenciales de pago desde un dispositivo de recepción 422
Recibir un identificador desde el dispositivo de recepción 424
Cifrar credenciales de pago recibidas 426
Almacenar una de credenciales de pago cifradas o clave de descifrado en memoria segura 428
Identificar un dispositivo móvil y/o elemento seguro que corresponde al identificador 430
Comunicar la otra de las credenciales de pago cifradas o la clave de descifrado al dispositivo móvil identificado para almacenamiento en un elemento seguro del dispositivo móvil 432

FIG. 4B

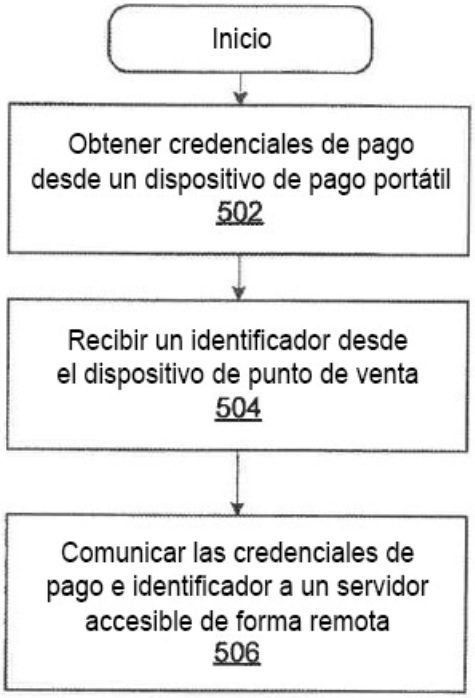

FIG. 5

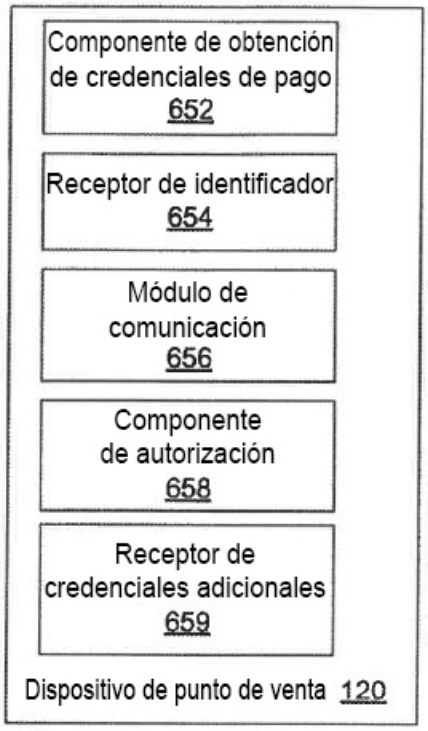

FIG. 6B

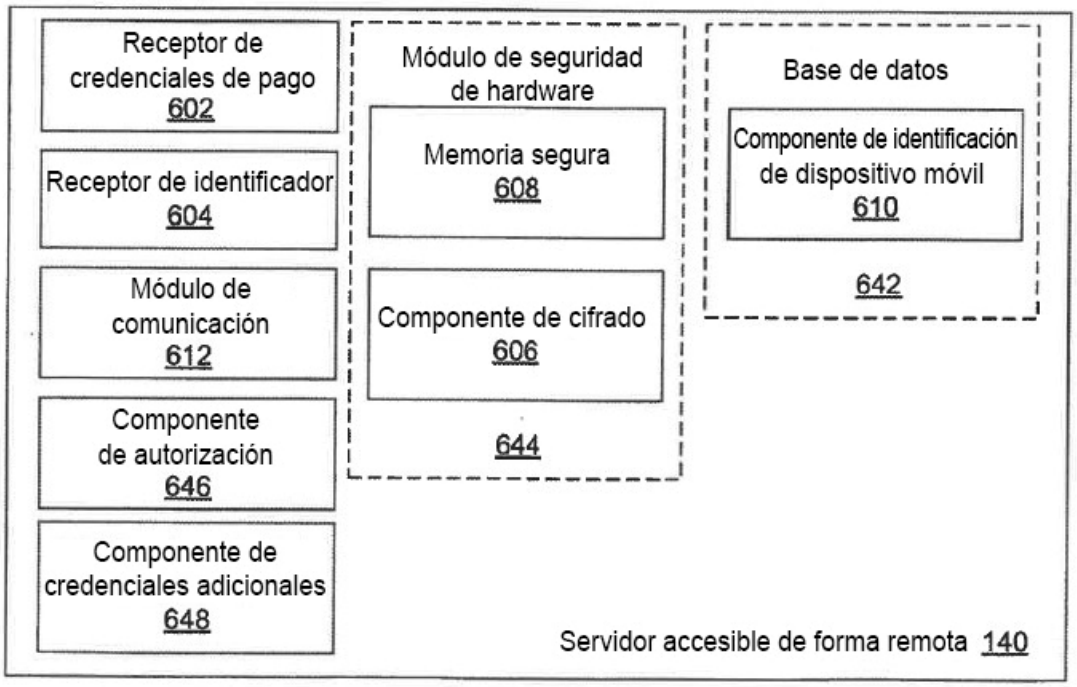

FIG. 6A

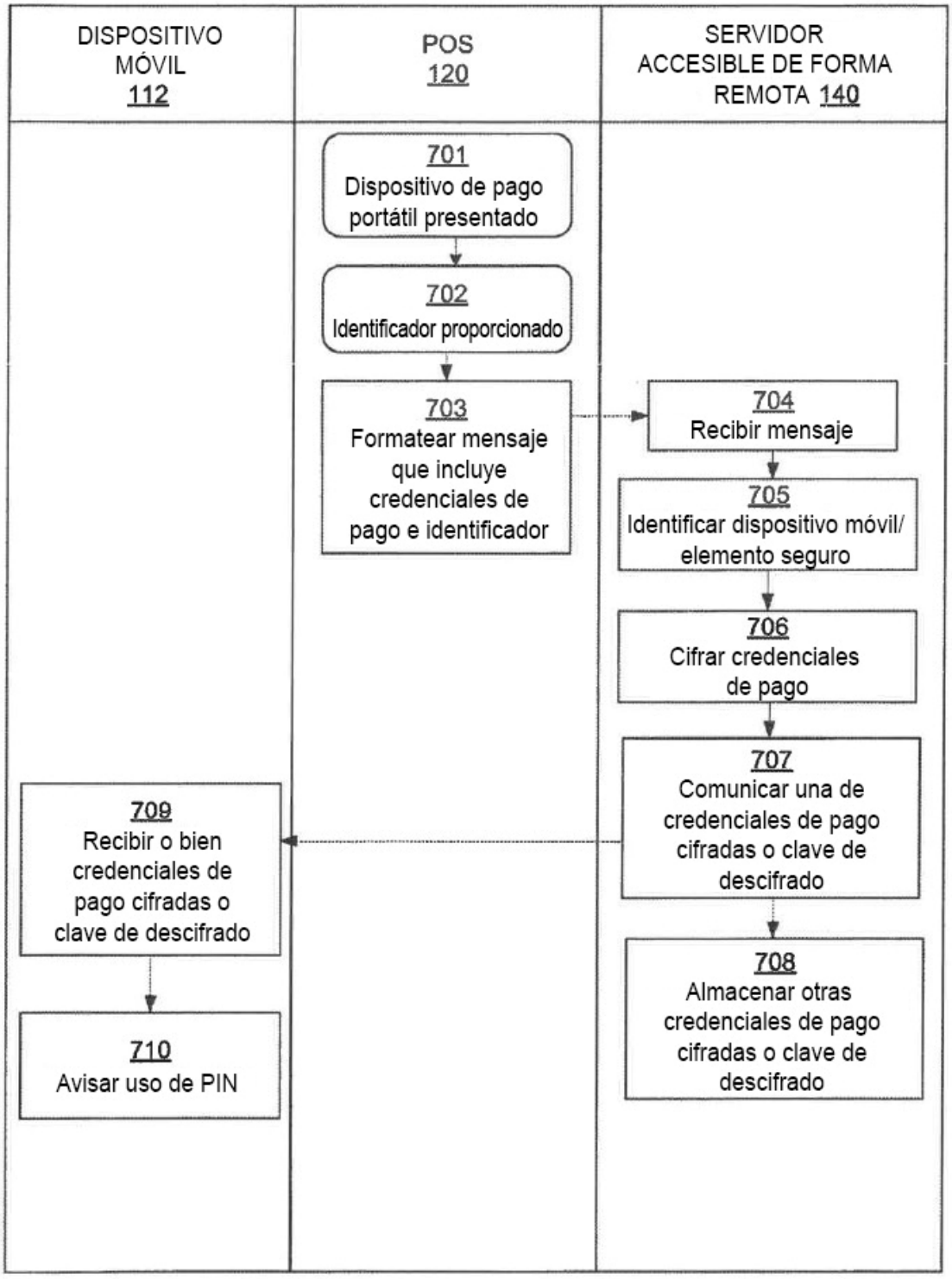
DISPOSITIVO MÓVIL 112
POS 120
SERVIDOR ACCESIBLE DE FORMA REMOTA 140
701 Dispositivo de pago portátil presentado
702 Identificador proporcionado
703 Formatear mensaje que incluye credenciales de pago e identificador
704 Recibir mensaje
705 Identificar dispositivo móvil/ elemento seguro
706 Cifrar credenciales de pago
707 Comunicar una de credenciales de pago cifradas o clave de descifrado
708 Almacenar otras credenciales de pago cifradas o clave de descifrado
709 Recibir o bien credenciales de pago cifradas o clave de descifrado
710 Avisar uso de PIN

FIG. 7

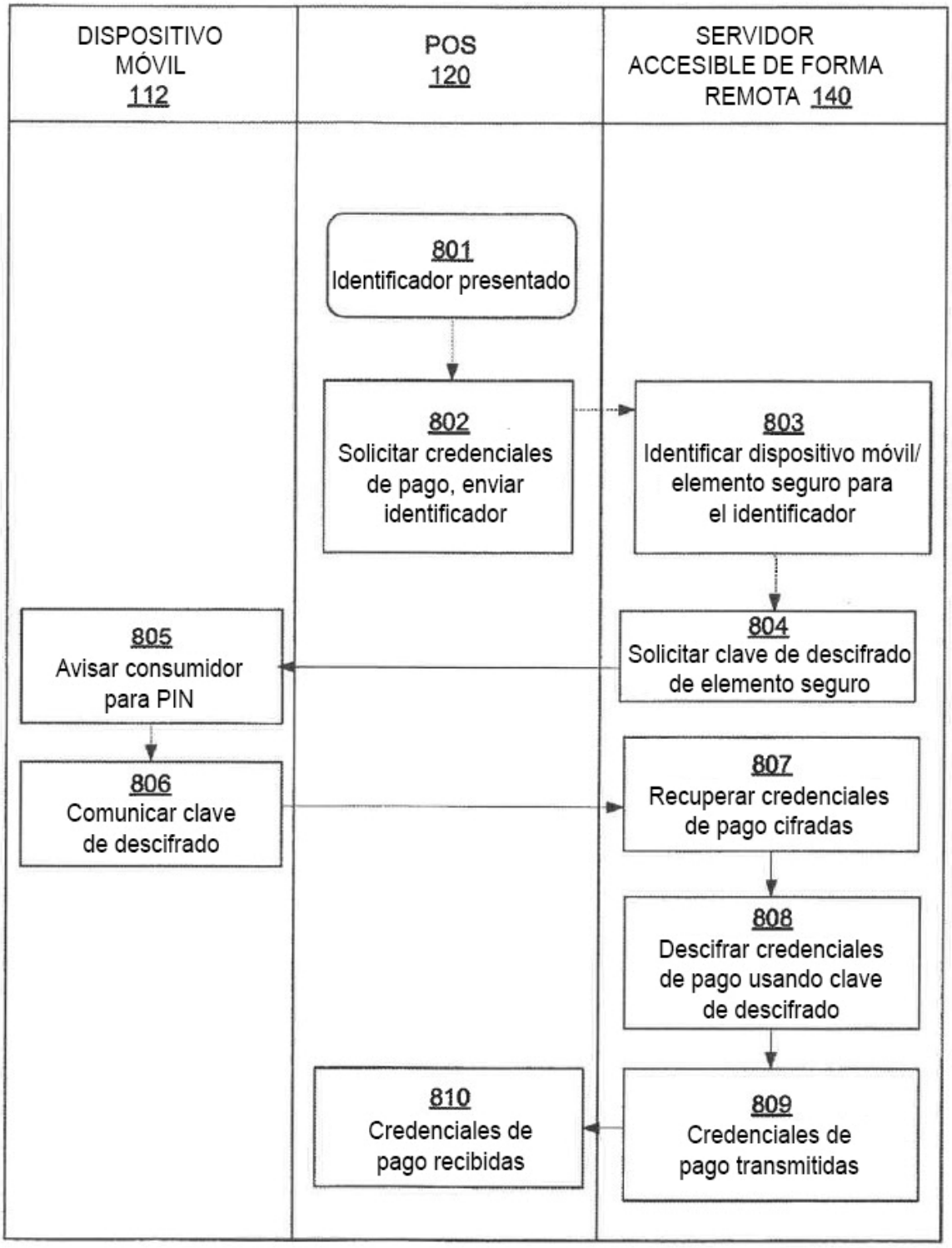
DISPOSITIVO MÓVIL 112
POS 120
SERVIDOR ACCESIBLE DE FORMA REMOTA 140
801 Identificador presentado
802 Solicitar credenciales de pago, enviar identificador
803 Identificar dispositivo móvil/ elemento seguro para el identificador
804 Solicitar clave de descifrado de elemento seguro
805 Avisar consumidor para PIN
806 Comunicar clave de descifrado
807 Recuperar credenciales de pago cifradas
808 Descifrar credenciales de pago usando clave de descifrado
809 Credenciales de pago transmitidas
810 Credenciales de pago recibidas

FIG. 8

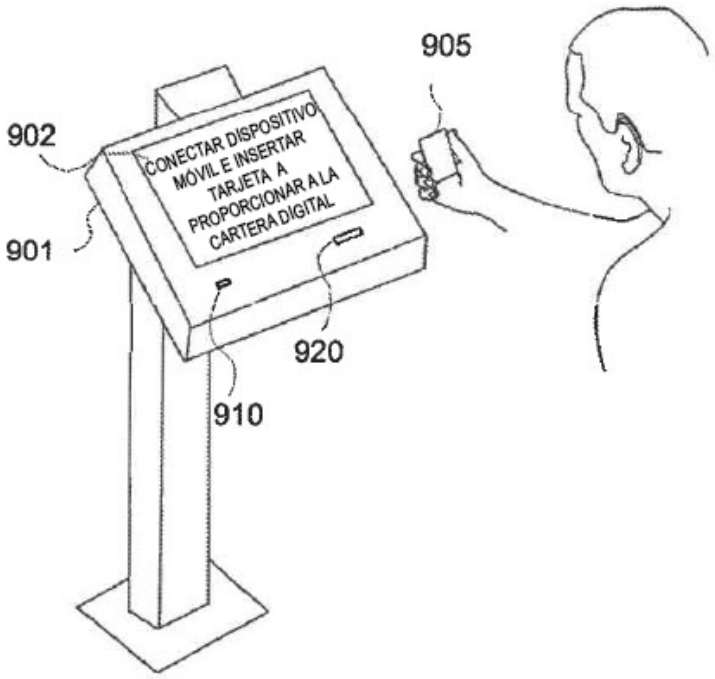
905
902
CONECTAR DISPOSITIVO MÓVIL E INSERTAR TARJETA A PROPORCIONAR A LA CARTERA DIGITAL
901
920
910

FIG. 9A

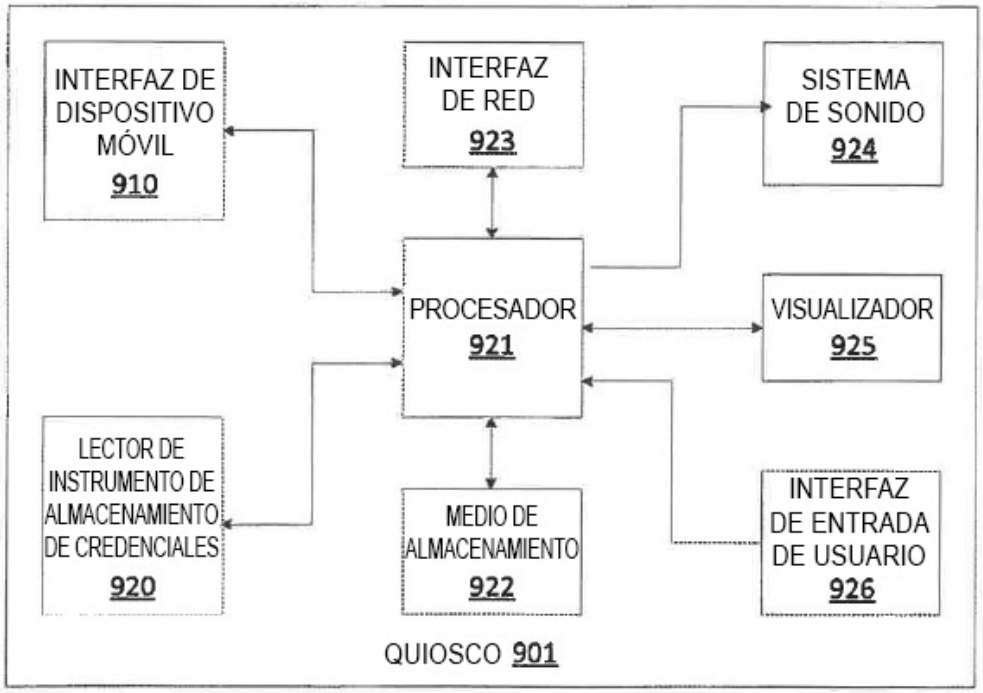
INTERFAZ DE DISPOSITIVO MÓVIL 910
INTERFAZ DE RED 923
SISTEMA DE SONIDO 924
PROCESADOR 921
VISUALIZADOR 925
LECTOR DE INSTRUMENTO DE ALMACENAMIENTO DE CREDENCIALES 920
MEDIO DE ALMACENAMIENTO 922
INTERFAZ DE ENTRADA DE USUARIO 926
QUIOSCO 901

FIG. 9B

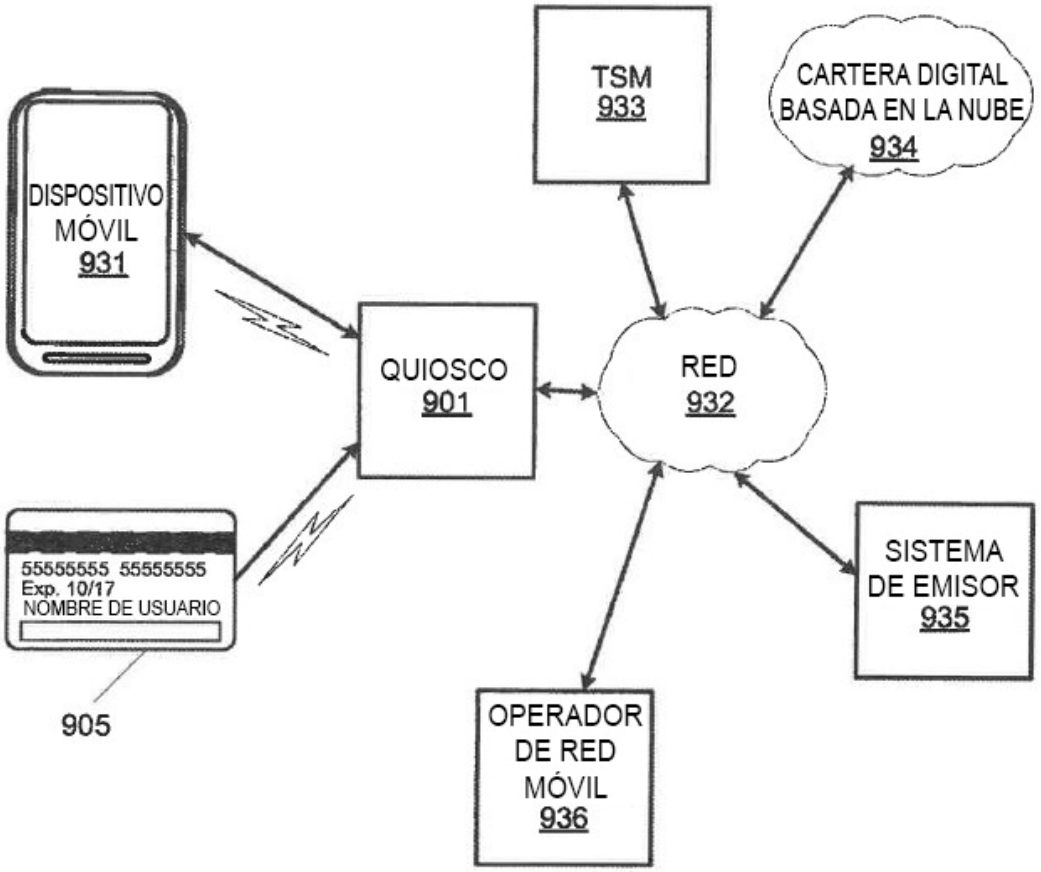
TSM
933
CARTERA DIGITAL BASADA EN LA NUBE
934
DISPOSITIVO MÓVIL
931
QUIOSCO
901
RED
932
55555555 55555555
Exp. 10/17
NOMBRE DE USUARIO
905
SISTEMA DE EMISOR
935
OPERADOR DE RED MÓVIL
936

FIG. 9C

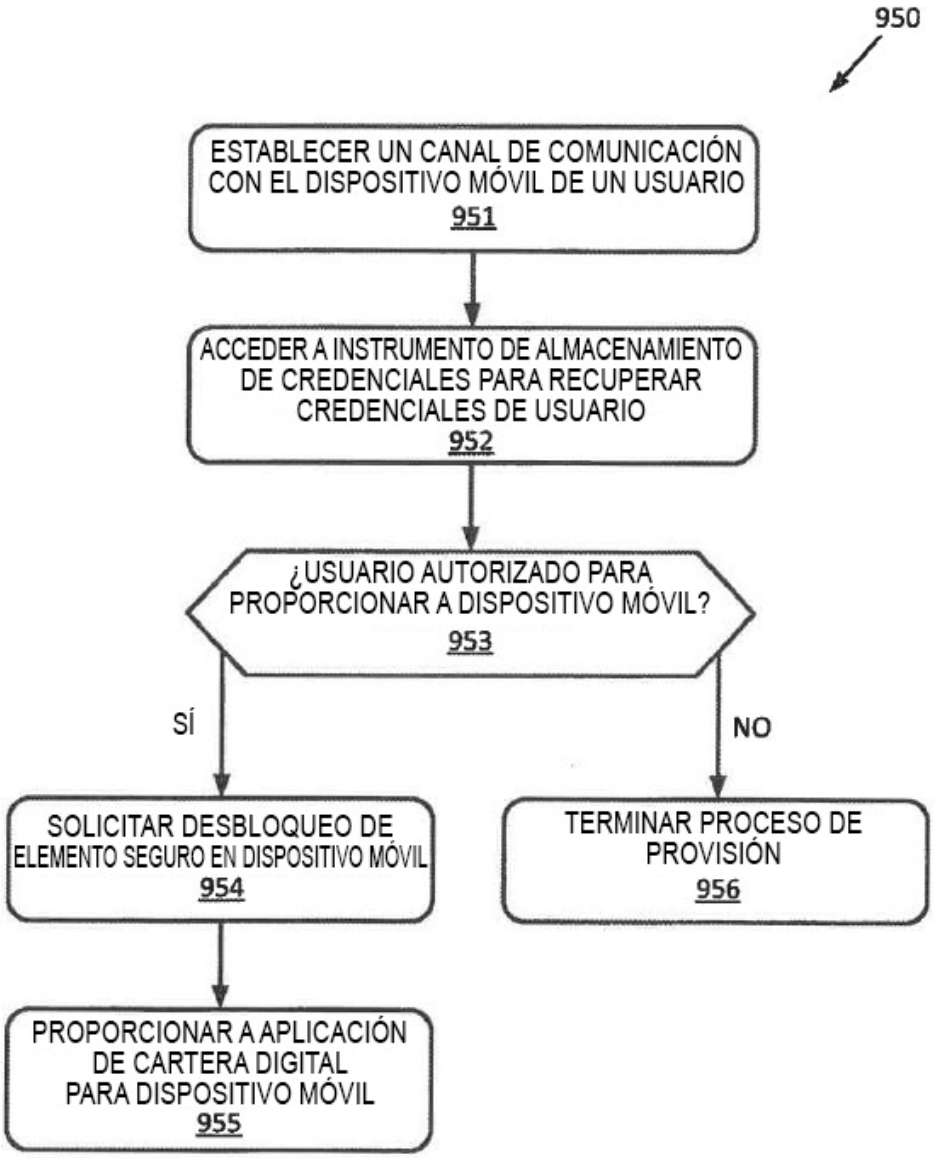
950
ESTABLECER UN CANAL DE COMUNICACIÓN CON EL DISPOSITIVO MÓVIL DE UN USUARIO
951
ACCEDER A INSTRUMENTO DE ALMACENAMIENTO DE CREDENCIALES PARA RECUPERAR CREDENCIALES DE USUARIO
952
¿USUARIO AUTORIZADO PARA PROPORCIONAR A DISPOSITIVO MÓVIL?
953
SÍ
NO
SOLICITAR DESBLOQUEO DE ELEMENTO SEGURO EN DISPOSITIVO MÓVIL
954
TERMINAR PROCESO DE PROVISIÓN
956
PROPORCIONAR A APLICACIÓN DE CARTERA DIGITAL PARA DISPOSITIVO MÓVIL
955

FIG. 9D

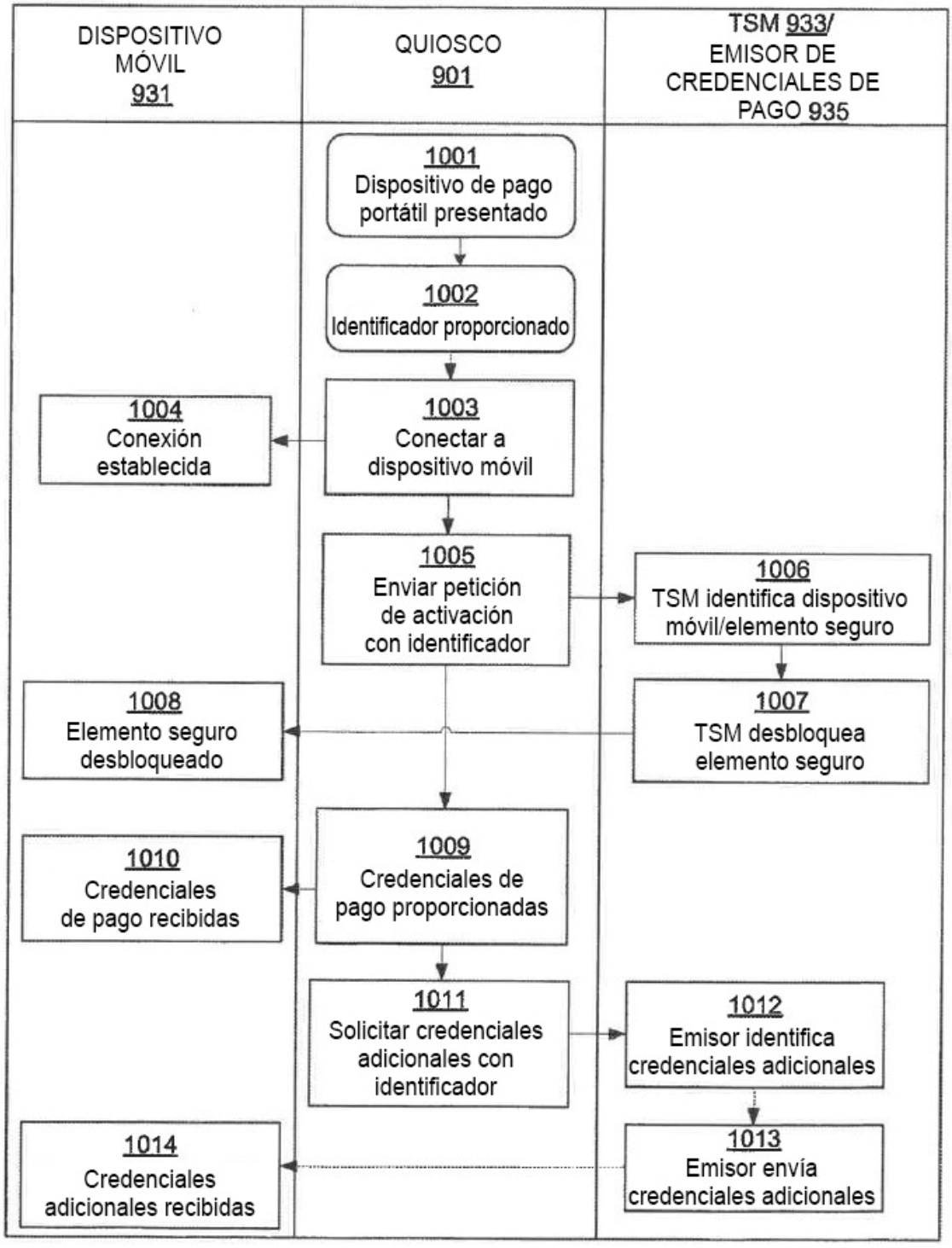
DISPOSITIVO MÓVIL 931
QUIOSCO 901
TSM 933/ EMISOR DE CREDENCIALES DE PAGO 935
1001 Dispositivo de pago portátil presentado
1002 Identificador proporcionado
1003 Conectar a dispositivo móvil
1004 Conexión establecida
1005 Enviar petición de activación con identificador
1006 TSM identifica dispositivo móvil/elemento seguro
1007 TSM desbloquea elemento seguro
1008 Elemento seguro desbloqueado
1009 Credenciales de pago proporcionadas
1010 Credenciales de pago recibidas
1011 Solicitar credenciales adicionales con identificador
1012 Emisor identifica credenciales adicionales
1013 Emisor envía credenciales adicionales
1014 Credenciales adicionales recibidas

FIG. 10

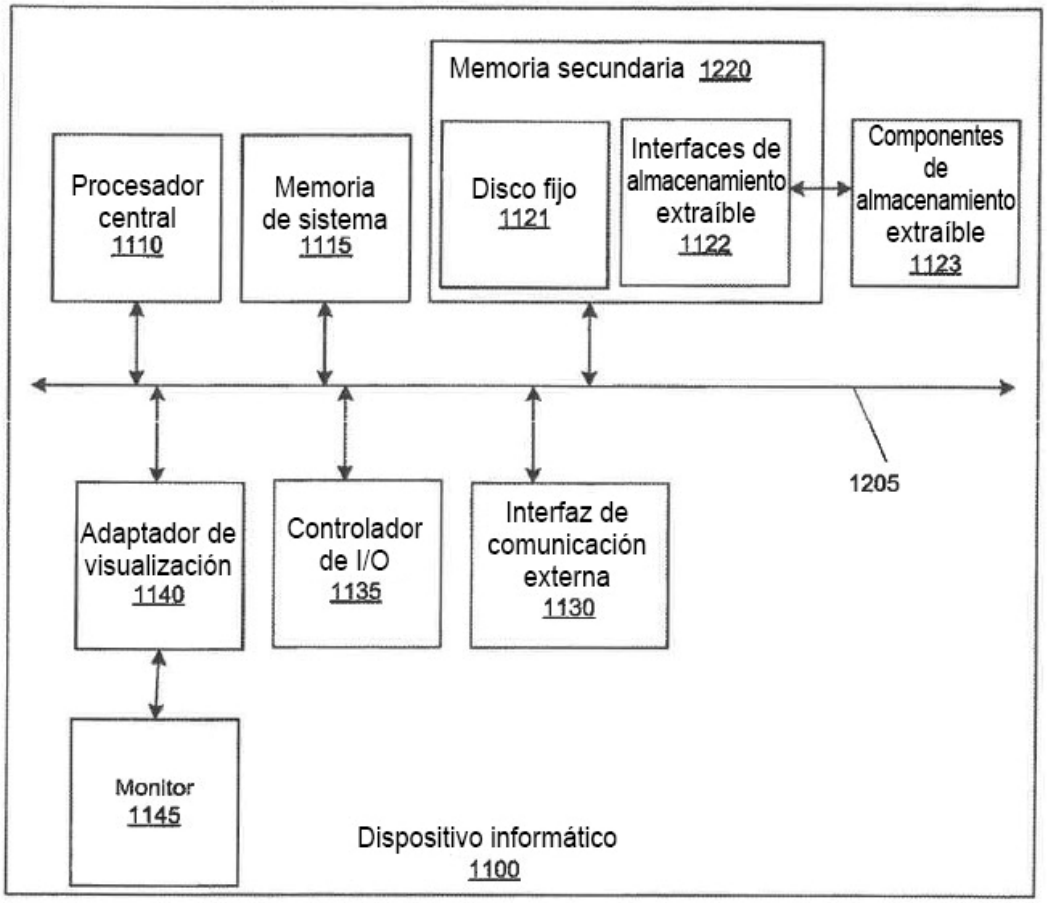
Memoria secundaria 1220
Procesador central 1110
Memoria de sistema 1115
Disco fijo 1121
Interfaces de almacenamiento extraíble 1122
Componentes de almacenamiento extraíble 1123
1205
Adaptador de visualización 1140
Controlador de I/O 1135
Interfaz de comunicación externa 1130
Monitor 1145
Dispositivo informático 1100

FIG. 11

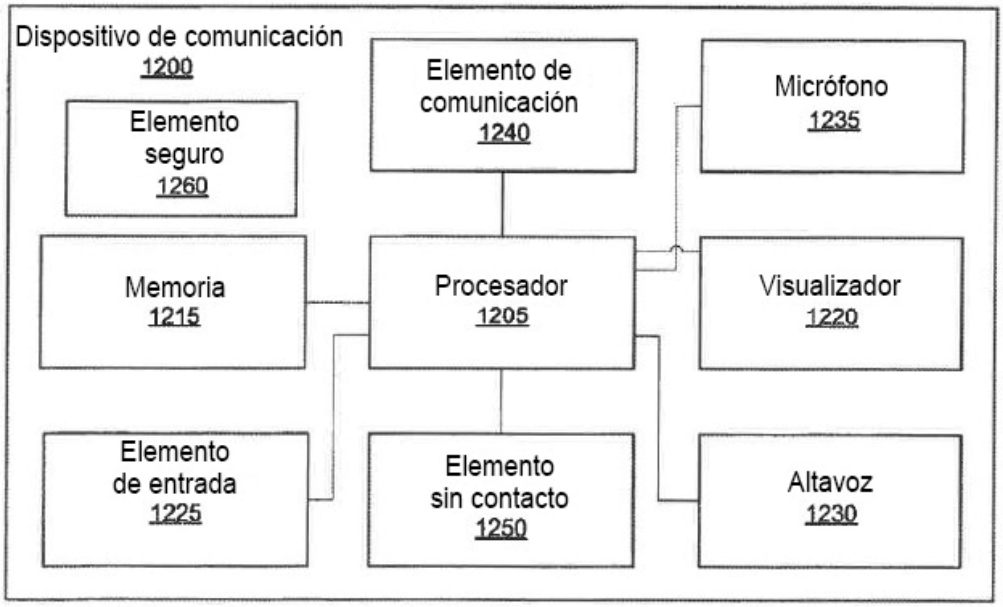
Dispositivo de comunicación 1200
Elemento de comunicación 1240
Micrófono 1235
Elemento seguro 1260
Memoria 1215
Procesador 1205
Visualizador 1220
Elemento de entrada 1225
Elemento sin contacto 1250
Altavoz 1230

FIG. 12