(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 753 388**

(51) Int. CI.:

H04W 12/00 (2009.01)
G06Q 20/32 (2012.01)
H04L 29/06 (2006.01)
G06Q 20/36 (2012.01)
G06Q 20/34 (2012.01)
G06Q 20/22 (2012.01)
G06Q 20/10 (2012.01)
H04W 12/12 (2009.01)
H04W 12/08 (2009.01)
G06Q 20/20 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **07.05.2015 PCT/US2015/029767**

(87) Fecha y número de publicación internacional: **12.11.2015 WO15171942**

(96) Fecha de presentación y número de la solicitud europea: **07.05.2015 E 15789702 (6)**

(97) Fecha y número de publicación de la concesión europea: **14.08.2019 EP 3140795**

(54) Título: **Interfaz de datos mejorada para comunicaciones sin contacto**

(30) Prioridad:

07.05.2014 US 201461989523 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
08.04.2020

(73) Titular/es:

VISA INTERNATIONAL SERVICE ASSOCIATION (100.0%)
P.O. Box 8999 MS M1-11F
San Francisco, CA 94128-8999, US

(72) Inventor/es:

SHARMA, SANJEEV;
MAKHOTIN, OLEG y
AABYE, CHRISTIAN

(74) Agente/Representante:

PONS ARIÑO, Ángel

DESCRIPCIÓN

Interfaz de datos mejorada para comunicaciones sin contacto

Referencias cruzadas a aplicaciones relacionadas

Antecedentes

La tecnología se ha desarrollado para permitir un mayor acceso a las interfaces de comunicación sin contacto por parte de los comercios y otros desarrolladores de aplicaciones que previamente no tenían permitido diseñar y desarrollar aplicaciones móviles configuradas para proporcionar capacidades de pago mediante comunicación sin contacto (por ejemplo, hardware de comunicaciones de campo cercano). Por lo tanto, los comercios están desarrollando aplicaciones de pago que son capaces de ofrecer servicios adicionales a los consumidores que usan interfaces de comunicación sin contacto o de campo cercano (NFC) que antes estaban fuera del alcance.

Sin embargo, junto con el aumento en el desarrollo de aplicaciones de pago móvil, ha habido una expansión en los intentos de los estafadores de usar aplicaciones de pago móvil de manera maliciosa. Por ejemplo, a medida que el ecosistema de pago de dispositivos móviles se ha expandido, los estafadores han utilizado dispositivos móviles (por ejemplo, teléfonos) para realizar transacciones fraudulentas robando tarjetas de crédito y agregando detalles de cuentas robadas a teléfonos no autorizados. Tradicionalmente, los desarrolladores de aplicaciones integraban sistemas de emisor de cuenta en un proceso de aprovisionamiento de cuenta o de inscripción de cuenta, de modo que el emisor de la cuenta accedió al aprovisionamiento y/o verificó la cuenta antes de agregar detalles de la cuenta a una aplicación de pago móvil. Esto permitió al emisor de la cuenta saber si se está agregando una cuenta a un teléfono desconocido y/o determinar si las actividades en una cuenta indican que la cuenta se está utilizando de manera fraudulenta. Por lo tanto, los emisores podrían rechazar una solicitud o autenticar a un usuario antes de permitir que la cuenta se agregue al teléfono. Sin embargo, a medida que los nuevos desarrolladores y emisores de aplicaciones del comercio adoptan el ecosistema móvil, integran cada uno de los millones de sistemas comerciales (u otros desarrolladores de aplicaciones) con cada uno de los cientos de sistemas emisores para obtener la aprobación antes de que se suministren las tarjetas en un teléfono para garantizar la tarjeta se agrega legítimamente al teléfono se ha vuelto excesivamente pesada y técnicamente difícil.

Como tal, muchos desarrolladores de aplicaciones han permitido que se agreguen cuentas a sus aplicaciones de pago móvil sin verificar u obtener la aprobación de los emisores de cuentas. Por lo tanto, debido a que no se contacta a los emisores durante el aprovisionamiento de la cuenta, los estafadores pueden ser capaces de aprovisionar los datos de la cuenta en un teléfono que de otro modo sería negado por un emisor.

Además, muchos desarrolladores de aplicaciones móviles no han informado a las partes confiantes (por ejemplo, comercios) durante las transacciones de que dichas cuentas agregadas a la aplicación no han sido verificadas por un emisor. Como tal, las partes confiantes no tienen medios para saber si una cuenta ha sido verificada antes de que se inicie una transacción. Por lo tanto, las partes confiantes no saben si confiar en la información de la cuenta que reciben durante las transacciones de pago móvil. En consecuencia, existe la necesidad de permitir que la información de cuenta no verificada se use en una transacción iniciada por una aplicación de pago móvil sin crear problemas de seguridad para las partes confiantes de la transacción.

Las modalidades de la invención abordan estos y otros problemas, individual y colectivamente.

La solicitud PCT 2012/002852 A1 divulga un servidor de seguridad dispuesto para establecer la comunicación entre un dispositivo del comercio y una aplicación de pago del cliente. La solicitud estadounidense 2012/109764 A1 divulga sistemas, métodos y medios legibles por ordenador para utilizar listas de aplicaciones preferidas en un lector de dispositivo inalámbrico.

Resumen

La invención está definida por las reivindicaciones independientes 1, 7, 8 y 14. Una modalidad de la invención está dirigida a un método. El método comprende un dispositivo móvil que recibe una solicitud de applets disponibles de un dispositivo de acceso y proporciona una lista de applets disponibles que incluyen identificadores de applets confiables e identificadores de applets no confiables para el dispositivo de acceso. El método comprende además recibir una selección de un identificador de applets no confiables de la lista y un identificador de entidad asociado con el dispositivo de acceso, validar que el dispositivo de acceso está autorizado para acceder a las credenciales asociadas con el identificador de applets no confiables seleccionado utilizando el identificador de entidad, y proporcionar el credenciales asociadas con el identificador de applets no confiables seleccionado para el dispositivo de acceso.

Otra modalidad de la invención está dirigida a un método. El método comprende enviar una solicitud de applets disponibles a un dispositivo móvil y recibir una lista de applets disponibles que incluyen identificadores de applets confiables e identificadores de applets no confiables. La lista de applets disponibles que incluye un identificador de cartera para cada uno de los applets disponibles que identifica una aplicación móvil que está asociada con cada uno

de los applets disponibles. El método comprende además determinar identificadores de applet compatibles de la lista de applets disponibles, determinar que un applet de máxima prioridad de los identificadores de applet compatibles incluye un identificador de applets no confiables y validar que el identificador de cartera esté asociado con una entidad confiable antes de seleccionar el applet no confiable de la lista. El método comprende además proporcionar una selección del identificador de applets no confiables de la lista y recibir credenciales asociadas con el identificador de applets no confiables seleccionado desde la aplicación móvil del dispositivo móvil.

Otra modalidad de la invención está dirigida a un sistema. El sistema comprende un dispositivo móvil y un dispositivo de acceso. El dispositivo móvil se configura para recibir una solicitud de applets disponibles de un dispositivo de acceso, proporcionar una lista de applets disponibles, incluidos identificadores de applets confiables e identificadores de applets no confiables para el dispositivo de acceso, recibir una selección de un identificador de applets no confiables de la lista y una identificador de entidad asociado con el dispositivo de acceso, validar que el dispositivo de acceso está autorizado para acceder a las credenciales asociadas con el identificador de applets no confiables seleccionado utilizando el identificador de entidad y proporcionar las credenciales asociadas con el identificador de applets no confiables seleccionado al dispositivo de acceso. El dispositivo de acceso se configura para enviar la solicitud de applets disponibles al dispositivo móvil, recibir la lista de applets disponibles, incluidos los identificadores de applets confiables y los identificadores de applets no confiables, proporcionar la selección del identificador de applets no confiables de la lista y recibir las credenciales asociadas con el identificador de applets no confiables seleccionado de la aplicación móvil del dispositivo móvil.

Estas y otras modalidades de la invención se describen con más detalle a continuación.

Breve descripción de los dibujos

La Figura 1 ilustra un diagrama de bloques ilustrativo de un sistema de interfaz de datos mejorado, de acuerdo con una modalidad de la presente invención.
La Figura 2 ilustra un ejemplo de protocolo de comunicación de corto alcance para una transacción entre un dispositivo móvil y un dispositivo de acceso, de acuerdo con una modalidad de la presente invención.
La Figura 3A ilustra una parte de un diagrama de flujo de interacción que incluye el procesamiento previo a la transacción y las etapas de inicio de la transacción, de acuerdo con una modalidad de la presente invención.
La Figura 3B ilustra una parte de un diagrama de flujo de interacción que incluye etapas de procesamiento de aplicaciones de servicios de valor agregado previos a la transacción, de acuerdo con una modalidad de la presente invención.
La Figura 3C ilustra una parte de un diagrama de flujo de interacción que incluye la selección del identificador de applets confiables y las etapas de procesamiento, de acuerdo con una modalidad de la presente invención.
La Figura 3D ilustra una parte de un diagrama de flujo de interacción que incluye la selección del identificador de applets no confiables y las etapas de procesamiento, de acuerdo con una modalidad de la presente invención.
La Figura 3E ilustra una parte de un diagrama de flujo de interacción que incluye las etapas de actualización de la aplicación de servicios de valor agregado posteriores a la transacción, de acuerdo con una modalidad de la presente invención.
La Figura 4 ilustra un sistema de procesamiento de transacciones, de acuerdo con una modalidad de la presente invención.
La Figura 5 ilustra un diagrama de bloques de un dispositivo móvil.
La Figura 6 ilustra un diagrama de bloques de un dispositivo portátil del consumidor.
La Figura 7 ilustra un diagrama de bloques de un aparato informático.

Descripción detallada

Las modalidades de la invención se refieren a métodos, sistemas, aparatos y medios legibles por ordenador para una interfaz de datos mejorada (EDI) que proporciona mecanismos de comunicación mejorados entre un dispositivo móvil y un dispositivo de acceso del comercio durante la transacciones sin contacto (u otra comunicación de corto alcance). La EDI proporciona validación de datos adicional, autenticación y controles de procesamiento de pagos durante las transacciones sin contacto (también conocidas como transacciones de comunicación de proximidad o de corto alcance).

Los comercios están desarrollando y proporcionando sus propias aplicaciones móviles (es decir, "aplicaciones móviles") a los consumidores que brindan capacidades de servicios de valor agregado (VAS) adicionales que incluyen interacciones adicionales de fidelidad, cupones y seguimiento de transacciones con los consumidores. Además, las aplicaciones móviles permiten la inscripción de cuentas de consumidores (por ejemplo, tarjetas de crédito, tarjetas de débito, etc.) para facilitar el procesamiento de transacciones utilizando la aplicación móvil. Para evitar transacciones fraudulentas y garantizar que una cuenta sea legítima, los proveedores de aplicaciones móviles generalmente obtienen la aprobación del emisor de la cuenta antes de agregar cuentas a sus aplicaciones móviles. Sin embargo, es difícil para los comercios integrar a cada emisor para obtener la verificación antes de permitir que una cuenta se aprovisione en una aplicación móvil en un dispositivo.

Por ejemplo, un comercio (por ejemplo, "Comercio A") puede desarrollar una aplicación móvil (o aplicación de cartera móvil) para un dispositivo móvil del consumidor (por ejemplo, teléfono móvil) que se utilizará durante las transacciones en sus ubicaciones (por ejemplo, "Comercio A" dispositivos de punto de venta (POS)). La aplicación móvil puede permitir a los usuarios inscribir información de cuenta registrada (por ejemplo, información de tarjeta de crédito) en su teléfono a través de la aplicación que se puede utilizar para pagar las compras realizadas en el comercio. Sin embargo, debido a que existen miles de emisores y millones de comercios, es complicado y técnicamente difícil para cada desarrollador de aplicaciones del comercio integrar cada sistema de emisor para validar una cuenta antes de agregar o aprovisionar las credenciales de la cuenta a través de la aplicación móvil. Por lo tanto, el comercio puede permitir a los consumidores agregar cuentas (es decir, tarjetas de crédito) a su teléfono a través de su aplicación móvil sin requerir que todos y cada uno de los emisores autentiquen y aprueben la tarjeta que se agrega a la aplicación móvil. Por ejemplo, el comercio puede obtener la aprobación de los emisores de cuentas más grandes (es decir, un banco nacional) pero no puede validar los datos de la cuenta para emisores más pequeños (es decir, un banco local) que tienen menos clientes, sistemas informáticos menos sofisticados o que son más difíciles de integrar con sus sistemas.

Sin embargo, debido a que el comercio no ha validado la cuenta con un emisor antes de agregar la tarjeta En la cuenta de la aplicación móvil, la aplicación móvil puede determinar que los datos de la tarjeta son "no confiables" o no han sido validados. Estas credenciales de la cuenta pueden clasificarse como "cuentas no confiables" cuando se agregan a través de la aplicación móvil y pueden tener restricciones de acceso adicionales que las cuentas confiables (es decir, cuentas validadas por el emisor). Por lo tanto, la aplicación móvil y un terminal POS que se basan en las "cuentas no confiables" pueden tratar los datos de cuentas de tarjetas no validadas o no aprobadas agregadas al dispositivo de manera diferente a los datos de cuenta que han sido validadas/aprobadas por un emisor de la cuenta.

Por ejemplo, la aplicación móvil solo puede permitir que las cuentas de tarjeta que no hayan sido validadas por el emisor se utilicen en las ubicaciones de los comercios del desarrollador de la aplicación móvil (por ejemplo ubicaciones del “comercio A”) (por ejemplo, aplicación móvil del "comercio A"). En consecuencia, una aplicación móvil puede determinar en qué comercio se encuentran y determinar si las credenciales de pago se pueden usar en ese comercio antes de permitir que se inicie una transacción.

Del mismo modo, un dispositivo de acceso del comercio (por ejemplo, un terminal POS) puede determinar el estado de los datos de la cuenta disponibles en un dispositivo móvil y puede verificar la identidad del desarrollador de la aplicación móvil o del propietario de la aplicación móvil antes de que acepten datos de tarjetas no confiables para una transacción porque un emisor de la cuenta no ha validado la tarjeta. En consecuencia, la aplicación móvil puede proporcionar un identificador diferente para cuentas confiables y cuentas no confiables almacenadas en el dispositivo móvil siempre que dicha información de cuenta se pase a un comercio para una transacción.

Por ejemplo, se le puede permitir al "Comercio A" iniciar una transacción utilizando credenciales de cuentas no confiables provistas a través de su aplicación móvil del "Comercio A" porque son responsables de permitir que se registre esa información, controlan la relación con el consumidor y pueden ser responsable de cualquier transacción fraudulenta asociada con las credenciales de cuentas no confiables. Sin embargo, "Comercio A" puede no permitir que la información de la cuenta registrada en una aplicación móvil de un comercio diferente (por ejemplo, "Comercio B") se use en su ubicación. Por lo tanto, si un consumidor intentó realizar una transacción utilizando credenciales de cuentas no confiables que se agregaron a través de una aplicación móvil del "Comercio B" en una ubicación del "Comercio A", el POS del "Comercio A" no puede aceptar credenciales de cuentas no confiables de la aplicación móvil del "Comercio B". Por lo tanto, la aplicación móvil y el POS del comercio pueden determinar la entidad asociada con el terminal POS y la aplicación móvil, respectivamente, para limitar el uso de las credenciales de cuentas no confiables.

Por lo tanto, la EDI utiliza la información adicional para facilitar la funcionalidad adicional y proporcionar ventajas adicionales sobre las interfaces de comunicación sin contacto anteriores. Por ejemplo, la EDI proporciona (i) validación del POS del comercio por una aplicación móvil, (ii) validación de aplicación móvil por parte de un POS del comercio, y (iii) proporciona la selección e integración de servicios de valor agregado (VAS) uniformes dentro de un protocolo de comunicación sin contacto.

Por ejemplo, para garantizar que una aplicación móvil no se utilice en otros comercios y para proteger la información del consumidor almacenada en la aplicación móvil (por ejemplo, información de cuenta registrada, historial de transacciones, etc.), la aplicación del comercio solo puede permitir transacciones y otras comunicaciones con un dispositivo de acceso del comercio que está asociado con el comercio. En consecuencia, la aplicación del comercio puede solicitar un identificador de entidad (por ejemplo, un identificador del comercio (MID)) durante una sesión de comunicación sin contacto con un dispositivo de acceso del comercio (por ejemplo, POS) y puede validar que el dispositivo de acceso del comercio sea operado por una entidad que es confiable para la aplicación del comercio.

Por ejemplo, una aplicación móvil puede solicitar un identificador del comercio (MID) en un mensaje de lista de objetos de datos de opciones de procesamiento (PDOL) de respuesta AID seleccionado. El dispositivo de acceso del comercio (por ejemplo, lector POS) puede enviar un MID preasignado en un comando de solicitud de obtención de opciones de procesamiento (GPO). Una aplicación móvil puede entonces verificar si el MID está autorizado para recibir datos de la tarjeta desde la aplicación móvil. Si un dispositivo de acceso del comercio (por ejemplo, lector POS) no admite la EDI, el lector puede no tener un MID en la solicitud de GPO y la Aplicación Móvil (MA) puede tratar la recepción no

tener MID, como una condición MID no válida. Además, en algunas modalidades, una aplicación móvil implementa la lógica de verificación del MID si un lector selecciona un identificador de applets no confiables (UAID), mientras que la verificación del MID es opcional si un lector selecciona un identificador de applets confiable (TAID).

Por lo tanto, algunas modalidades permiten que las aplicaciones móviles validen la identidad de un propietario u operador de un dispositivo de acceso antes de permitir que el dispositivo de acceso obtenga información confidencial de un applet de la cuenta. En consecuencia, la seguridad de la transacción sin contacto aumenta con respecto a las interacciones sin contacto preexistentes porque una aplicación móvil puede validar la identidad del dispositivo de acceso antes de proporcionar información potencialmente confidencial.

Además, en algunas modalidades, los comercios que reciben credenciales de pago durante las transacciones sin contacto pueden querer validar la identidad de una aplicación móvil utilizada por el consumidor para iniciar una transacción antes de permitir que se procese la transacción. El POS puede validar la aplicación móvil para cada tipo de transacción o puede validar la aplicación móvil donde un consumidor ha demostrado la intención de utilizar credenciales de cuentas no confiables. Por ejemplo, un POS del comercio puede iniciar transacciones utilizando credenciales de cuentas no confiables solo si un consumidor está usando una aplicación móvil autorizada por el comercio (por ejemplo, una aplicación desarrollada por el comercio o un socio).

En consecuencia, una ubicación del comercio puede validar al desarrollador de la cartera durante una transacción sin contacto. Por ejemplo, un comercio puede verificar un ID de la cartera (WID) de una aplicación de pago y un AID del applet de la cuenta para un pago. La aplicación móvil puede enviar el WID en una respuesta PPSE. La respuesta de PPSE también incluye los AID de los applets de las cuentas confiables y no confiables que el consumidor seleccionó para el pago. Por lo tanto, el dispositivo de acceso del comercio puede conocer las tarjetas disponibles para su uso en la transacción y la identidad de la aplicación de pago que se utiliza en una transacción.

Además, dado que los comercios solo tienen acceso a los datos que pasan a través de su cartera, el comercio que acepta el pago puede no recibir la información del consumidor asociada con la transacción porque no tiene acceso a la aplicación del comercio. En consecuencia, un comercio puede desear limitar el uso de otras aplicaciones del comercio en sus ubicaciones. Por lo tanto, una aplicación del comercio puede estar limitada a los dispositivos de acceso del comercio asociados con la ubicación del comercio. Alternativa y adicionalmente, si la cartera de comercio es una cartera de múltiples comercios y el comercio tiene una asociación con otro comercio o una colección de comercios, la cartera de múltiples comercios puede ser aceptable en múltiples ubicaciones.

Por lo tanto, la aplicación móvil puede recibir un identificador de entidad (por ejemplo, un identificador del comercio (MID)) desde el POS de comercio y puede usar el identificador de entidad para determinar si las credenciales de cuentas no confiables pueden usarse para una transacción, el nivel de riesgo asociado con la transacción y cualquier dato de servicios de valor agregado (VAS) que pueda enviarse con la transacción. Además, el POS del comercio puede recibir un identificador de cartera (WID) de la aplicación móvil para determinar si el POS del comercio debe permitir la transacción (por ejemplo, si las credenciales de pago se originan en la aplicación móvil del comercio o en una aplicación móvil en la que el comercio confía) y/o si se pueden seleccionar datos de cuenta no confiables para una transacción.

Otra modalidad de la EDI incluye proporcionar un identificador de applets de VAS uniforme (AID de VAS) para usar durante las transacciones. Los emisores, comercios y proveedores externos pueden ofrecer servicios VAS basados en AID de VAS uniforme. El AID de VAS uniforme (VAID) puede permitir a los usuarios de la aplicación VAS obtener una mayor interoperabilidad y adopción en múltiples comercios.

Como tal, la aplicación VAS puede realizar un seguimiento de la información de la cuenta de servicios de valor agregado de un usuario (por ejemplo, fidelidad, cupón, etc.) para una variedad de diferentes comercios y permitir una fácil integración de los datos VAS durante el procesamiento de la transacción. Por ejemplo, un usuario puede usar su aplicación móvil del "Comercio A" en una transacción de pago en una ubicación del "Comercio A" y pueden proporcionarse datos VAS (por ejemplo, un número de cuenta de fidelidad, un cupón, etc.) asociados con su cuenta durante la transacción automáticamente sin requerir que el consumidor seleccione o interactúe de otra manera con su cuenta de fidelidad o aplicación de pago.

La aplicación VAS puede seleccionar la información de fidelidad relevante basada en un identificador de entidad (por ejemplo, un identificador del comercio (MID)) recibido de un POS durante la interacción entre el dispositivo móvil y el dispositivo de acceso del comercio. Por ejemplo, si una aplicación VAS admite los datos de fidelidad del "Comercio A" y del "Comercio B", un consumidor puede usar la aplicación VAS en cualquier comercio para comprar bienes y la aplicación VAS puede seleccionar los datos de cuenta de fidelidad apropiados basados en el identificador del comercio (MID) asociado con el POS del comercio (por ejemplo, el número de cuenta de fidelidad del comercio A está asociado con el identificador del comercio del "Comercio A").
Antes de analizar modalidades y ejemplos específicos, a continuación se proporcionan algunas descripciones de los términos utilizados en este documento.

Una "aplicación" puede incluir cualquier módulo de software configurado para realizar una función o funciones específicas cuando es ejecutado por un procesador de un ordenador. Por ejemplo, una "aplicación móvil" puede incluir un módulo de software que se configura para ser operado por un dispositivo móvil. Las aplicaciones se pueden configurar para realizar muchas funciones diferentes. Por ejemplo, una "aplicación de pago" puede incluir un módulo de software que se configura para almacenar y proporcionar información de pago para una transacción. Una "aplicación de cartera" puede incluir un módulo de software con una funcionalidad similar a una aplicación de pago que tiene múltiples applets de la cuenta aprovisionadas o inscritas en la aplicación y que pueden utilizarse a través de la aplicación.

Una aplicación de pago puede almacenar credenciales de la cuenta (por ejemplo, identificador de la cuenta, fecha de vencimiento, valor de verificación de tarjeta (CW), etc.) en una memoria segura o entorno de ejecución confiable (por ejemplo, elemento seguro). Se puede acceder a la información de pago confidencial solicitando la información de pago de la aplicación de pago utilizando un identificador de applets (AID) u otra información de dirección para acceder a la aplicación de pago correcta. Se puede usar cualquier número de protocolos de comunicación para acceder a la información de pago desde la aplicación de pago y usar la información de pago recibida en una transacción de pago.

Las "credenciales" pueden incluir cualquier información que identifique una entidad, artículo, derecho o elemento en particular. Por ejemplo, una credencial de la cuenta puede identificar y proporcionar confirmación de que un dispositivo, persona o entidad tiene permiso para acceder a la cuenta. Las credenciales de la cuenta pueden incluir tan poca o tanta información como sea necesario. Por ejemplo, las credenciales de la cuenta pueden incluir un identificador de la cuenta, una fecha de vencimiento, un criptograma generado, un valor de verificación o cualquier combinación de los mismos.

La "información de pago" puede incluir cualquier información asociada con un pago. Por ejemplo, la información de pago puede incluir cualquier dato que pueda usarse para identificar una cuenta y usar la cuenta en una transacción de pago. Por ejemplo, la información de pago puede incluir credenciales de la cuenta (por ejemplo, identificador de la cuenta principal (PAN), fecha de vencimiento, valor de verificación de tarjeta (CW), información de autenticación del dispositivo (por ejemplo, criptograma de transacción), información de autenticación dinámica (por ejemplo, un criptograma dinámico), etc.), información personal asociada con un usuario o consumidor (por ejemplo, nombre, dirección de facturación, dirección residencial, fecha de nacimiento, etc.), información de la cuenta (por ejemplo, identificador del emisor (BIN), fecha de emisión de la cuenta, etc.), información de verificación del titular de la tarjeta (por ejemplo, código de acceso, contraseña, número de identificación personal (PIN), etc.), una indicación de un proceso de autenticación para el procesamiento de la transacción (por ejemplo, PIN en línea, firma, etc.) y/o cualquier otra información adecuada o relevante para realizar una transacción.

Un "applet" incluye cualquier aplicación que realiza una pequeña cantidad de tareas que se ejecutan dentro del alcance de un programa más grande. Por ejemplo, una aplicación móvil puede comprender múltiples applets de la cuenta que están diseñados para almacenar credenciales de la cuenta y permitir que la aplicación móvil use las credenciales de la cuenta en una transacción. En algunas modalidades, un applet puede estar asociado con un identificador de applets (AID) que identifica la ubicación y/o identidad del applet. En algunas modalidades, un applet puede configurarse para proporcionar cualquier información de pago asociada con credenciales de la cuenta almacenadas (por ejemplo, generar y proporcionar un criptograma dinámico, límites de transacción, etc.).

Un "identificador de applet" (AID) puede incluir cualquier información que pueda identificar un applet. Por ejemplo, un AID puede incluir una dirección de datos para un applet almacenado en un dispositivo móvil o puede ser utilizado por otro programa para hacer referencia a la ubicación del applet. El AID puede estar en cualquier formato adecuado. Por ejemplo, un AID puede incluir un conjunto de caracteres alfanuméricos. En algunas modalidades, un AID puede identificar una aplicación móvil, una aplicación de pago, applets dentro de una aplicación y/o cualquier combinación de los mismos.

Además, en algunas modalidades, un AID puede asociarse con un conjunto de características y/o servicios relacionados con la forma en que se procesa una transacción realizada utilizando la aplicación de pago correspondiente. En algunas modalidades, el AID puede estar asociado con la información de la cuenta provista en una aplicación móvil y el AID puede pasarse entre dispositivos como un medio para identificar un applet de la cuenta particular y/o opciones de procesamiento particulares para un applet de cuenta. Por ejemplo, en algunas modalidades, un AID puede indicar a un dispositivo de acceso cuya red de procesamiento de pagos (por ejemplo, VisaNet™) debe usarse para procesar una transacción realizada con el applet de pago correspondiente al AID; un tipo de cuenta o credenciales financieras asociadas con el applet (por ejemplo, débito, crédito, fidelidad, etc.); información relacionada con la cuenta (por ejemplo, cuenta de nivel platino, cuenta de nivel oro, etc.); un emisor de cuenta (por ejemplo, Banco A); y/o cualquier otra información sobre una aplicación móvil, un applet y/o datos de cuenta subyacentes asociados con el applet.
En algunas modalidades, el AID puede tener un formato estandarizado para incluir información sobre un proveedor de applet (por ejemplo, red de pago A, comercio B, etc.) y un tipo de aplicación (por ejemplo, tipo de cuenta o producto, emisor de cuenta, etc.) asociado con cada aplicación móvil o applet de cuenta. Por ejemplo, una primera parte de un AID puede identificar un proveedor de aplicaciones asociado con los datos de la tarjeta aprovisionados en un dispositivo y una segunda parte puede identificar un tipo de cuenta asociada con el proveedor de la aplicación. Por

ejemplo, el AID (por ejemplo, A000000031010) puede tener una primera porción (por ejemplo, A00000003) que identifica un proveedor de aplicaciones (por ejemplo, la red de pago A) y una segunda porción (por ejemplo, 1010) que identifica un tipo de cuenta aprovisionada en el applet identificado (por ejemplo, cuenta de débito o crédito). Además, en algunas modalidades, la segunda porción (o una tercera porción) también podría identificar un emisor asociado con la cuenta aprovisionada y/o el applet (por ejemplo, el Emisor B). Por lo tanto, el dispositivo de acceso puede usar la AID para determinar si el dispositivo de acceso puede admitir el procesamiento de una transacción iniciada utilizando el applet de pago o cuenta.

En algunas modalidades, la interfaz de datos mejorada (EDI) puede reclasificar los identificadores de applet (AID). Por ejemplo, los identificadores de applet pueden clasificarse como identificadores de applets confiables (TAID), identificadores de applets no confiables (UAID) e identificadores de applet/aplicación de servicios de valor agregado (VAID).

Un "identificador de applets confiables" (TAID) puede incluir un identificador para un applet o aplicación que incluye credenciales confiable que tienen un mayor nivel confiable que otros applets. Por ejemplo, un TAID puede identificar un applet de la cuenta donde el consumidor o la cuenta de consumidor fue verificada por el emisor durante la inscripción de la cuenta. Además, el TAID puede indicar que un sistema emisor estuvo involucrado o participó en el proceso de provisión de cuenta. Por ejemplo, un TAID puede ser similar a un AID tradicional para una aplicación de pago móvil que se aprovisiona en un elemento seguro u otro entorno de ejecución confiable en el que varias partes (incluido un emisor) participan en el proceso de aprovisionamiento antes de proporcionar la aprobación para la inscripción, entrega o aprovisionamiento de la aplicación de pago. Por lo tanto, un TAID puede indicar que el applet o aplicación de la cuenta identificada se aprovisionó con credenciales en las que un emisor de las credenciales participó durante el aprovisionamiento de la cuenta.

Un "identificador de applets no confiable" (UAID) puede identificar un applet o aplicación que incluye credenciales que tienen un nivel confiable más bajo que un identificador de applets confiable. Por ejemplo, un UAID puede identificar un applet de la cuenta donde las credenciales de la cuenta han sido inscritas por un comercio asociado con la aplicación móvil sin la participación del emisor o la verificación del consumidor o la cuenta del consumidor durante el suministro de las credenciales de la cuenta. Por ejemplo, algunas aplicaciones móviles pueden permitir que un consumidor agregue credenciales de pago de una cuenta de consumidor sin autenticar o contactar a un emisor asociado con la cuenta del consumidor durante la inscripción, el aprovisionamiento o la entrega del applet. Tenga en cuenta que el dispositivo móvil puede confiar en un applet y el nombre "applet no confiable" no indica que el dispositivo no confíe en el applet. En cambio, el identificador de applets no confiables puede identificar una applet en la que el dispositivo móvil y/o la aplicación móvil todavía confía, pero que incluye información que no puede confirmarse como confiable porque un emisor no participó en el proceso de inscripción o aprovisionamiento de credenciales almacenadas por el applet de la cuenta identificado por el UAID.

Una "aplicación de servicios de valor agregado" puede incluir una aplicación móvil que se refiere al almacenamiento y proporcionamiento de información de servicios de valor agregado (VAS). La aplicación VAS puede incluir información VAS para muchos comercios diferentes. Por ejemplo, la aplicación VAS puede incluir información asociada con múltiples identificadores de fidelidad (LID) donde cada identificador de fidelidad (LID) está asociado con un comercio o proveedor de servicios separado. Además, cada identificador de fidelidad puede tener múltiples datos de contenido de fidelidad que pueden asociarse con múltiples ofertas, valores o cualquier otra información que pueda pasarse y usarse durante una transacción sin contacto. En algunas modalidades, la aplicación de servicios de valor agregado puede denominarse un "identificador de applets de entidades múltiples" porque la aplicación VAS almacenó datos VAS para varias entidades diferentes (por ejemplo, comercios). Por ejemplo, la aplicación VAS puede usar un identificador de entidad (por ejemplo, un identificador del comercio (MID)) para determinar la información VAS relevante para una entidad (por ejemplo, un comercio) asociada con un dispositivo de acceso y puede proporcionar la información relevante en respuesta a la recepción del Identificador de entidad. La lógica de la aplicación VAS puede ser parte de una aplicación móvil que admite pagos o podría ser una aplicación ejecutable separada.

Un "identificador de applets de máxima prioridad" puede incluir un identificador de applets (AID) que se ha determinado que tiene la máxima prioridad. Por ejemplo, la AID de máxima prioridad puede ser determinada por un dispositivo móvil o un dispositivo de acceso. Por lo tanto, en algunas modalidades, el AID de máxima prioridad puede incluir solo aquellos AID que son compatibles con un dispositivo de acceso. La prioridad de cada AID se puede determinar mediante cualquier método adecuado. Por ejemplo, la prioridad de los AID puede basarse en los comentarios del consumidor (por ejemplo, un consumidor elige sus tres aplicaciones de pago compatibles principales), la coincidencia más cercana con las opciones de configuración para un dispositivo (por ejemplo, se dan aplicaciones asociadas con un tipo preferido de procesamiento por parte del dispositivo prioridad), seguridad de la transacción (por ejemplo, las aplicaciones que requieren un alto nivel de autenticación para procesar una transacción tienen mayor prioridad que otras aplicaciones, las redes de pago con un mejor historial de seguridad tienen prioridad), velocidad de procesamiento de la transacción (por ejemplo, las aplicaciones asociadas con una red de pago particular que es más rápida que otras redes de pago tienen mayor prioridad), y/o cualquier otra información o procesos pueden usarse para priorizar los AID asociados con aplicaciones en el dispositivo móvil.

Un "identificador de entidad" puede incluir cualquier dato que identifique a un propietario, operador, proveedor o parte responsable asociado con un dispositivo. Por ejemplo, para un terminal POS, un identificador de entidad puede incluir un identificador del comercio (MID) para el comercio que controla y/u opera el POS. Un MID puede incluir cualquier información relevante para identificar a un comercio. Por ejemplo, el MID puede incluir una cadena alfanumérica u otro valor de datos asociado con un comercio en particular. El identificador de entidad (por ejemplo, MID) puede ser compartido con otros dispositivos. Otros dispositivos pueden almacenar un directorio de entidades confiables (por ejemplo, comercios confiables) que incluye una lista de identificadores de entidades confiables que los dispositivos pueden comparar para garantizar que un dispositivo de acceso del comercio sea confiable.

Un "identificador de cartera (WID)" puede incluir cualquier dato que identifique a un proveedor de aplicaciones móviles, proveedor de carteras móviles o proveedor de aplicaciones. El WID puede incluir cualquier cantidad de información y puede pasarse entre dispositivos. Por ejemplo, el WID puede incluir una cadena alfanumérica u otro valor de datos asociado con un proveedor de cartera móvil o proveedor de aplicaciones móviles en particular. Un dispositivo puede incluir un directorio de proveedores de aplicaciones confiables o compatibles que se pueden comparar con el WID para garantizar que una entidad procesadora confíe en un proveedor de aplicaciones móviles.

Un "identificador de fidelidad" (LID) puede incluir cualquier dato que identifique información de fidelidad. Por ejemplo, un LID puede incluir una cadena alfanumérica de caracteres que identifica una cuenta particular del consumidor (por ejemplo, un número de tarjeta de fidelidad o una dirección de correo electrónico). Un LID puede incluir cualquier otra información adecuada que sea capaz de identificar información de fidelidad del consumidor. El LID puede almacenarse en una aplicación móvil y puede accederse cuando se valida un identificador de entidad (por ejemplo, identificador del comercio) que coincide con la ubicación de datos relevante para el LID. Además, cada comercio o entidad puede tener uno o más LID almacenados dentro de una aplicación móvil.

Los "datos del contenedor de fidelidad" (LCD) pueden incluir cualquier dato que identifique una oferta de fidelidad, un cupón o un beneficio de valor agregado en particular. Por ejemplo, una pantalla LCD puede incluir una cadena alfanumérica de caracteres que identifica un beneficio asociado con un comercio (por ejemplo, un número de cupón). La pantalla LCD puede almacenarse en una aplicación móvil y puede accederse cuando se valida un identificador de entidad (por ejemplo, identificador del comercio) que coincide con la ubicación de datos relevante para la pantalla LCD. Además, cada comercio o entidad puede tener uno o más LCD almacenados dentro de una aplicación móvil.

Un "módulo" puede incluir cualquier componente o subcomponente de un sistema. Por ejemplo, un módulo puede incluir un programa de software configurado para realizar una función particular cuando lo ejecuta un procesador.

A. Sistema de comunicación de interfaz de datos mejorada (EDI) ilustrativo

La Figura 1 muestra un sistema ilustrativo de interfaz de datos mejorada (EDI) que incluye un dispositivo móvil 110, un dispositivo de acceso 120 y un ordenador de aplicación móvil 170. El dispositivo móvil 110 y el dispositivo de acceso 120 están configurados para comunicarse utilizando un protocolo de comunicación EDI que permite que el dispositivo móvil 110 y el dispositivo de acceso 120 validen la identidad, los derechos de acceso y la compatibilidad entre una aplicación móvil 112 del dispositivo móvil 110 y el dispositivo de acceso del comercio 120. La ordenador de aplicación móvil 170 está configurada para comunicarse con la aplicación móvil 112 del dispositivo móvil 110 para proporcionar credenciales.

Un dispositivo móvil 110, también denominado "dispositivo electrónico portátil", puede ser, por ejemplo, un teléfono celular o inalámbrico (por ejemplo, un teléfono inteligente), un asistente digital personal (PDA), un ordenador portátil (por ejemplo, una tableta o un portátil), buscapersonas, dispositivo portátil (por ejemplo, reloj inteligente, gafas, etc.) u otro dispositivo portátil que lleve un titular de cuenta. Un dispositivo móvil 110 y un dispositivo portátil del consumidor (no mostrado) se describen más adelante con referencia a las Figuras 5 y 6, respectivamente.

Un dispositivo de acceso 120 puede incluir cualquier dispositivo que esté configurado para interactuar con un dispositivo móvil 110 y/o dispositivo portátil del consumidor (no mostrado) para iniciar una transacción. Los ejemplos de dispositivos de acceso 120 incluyen dispositivos de punto de venta (POS), teléfonos celulares, PDA, ordenadores personales, tabletas, lectores especializados de mano, decodificadores, cajas registradoras electrónicas, cajeros automáticos (ATM), cajas registradoras virtuales, quioscos, sistemas de seguridad, sistemas de acceso y similares. Los dispositivos de acceso 120 pueden usar medios tales como lectores de radiofrecuencia (RF) para interactuar con el dispositivo móvil 110 a través de la comunicación sin contacto (es decir, un lector sin contacto).

El dispositivo de acceso 120 puede incluir un módulo de selección de aplicaciones 121 que se configura para interactuar con el sistema operativo móvil 116 del dispositivo móvil 110 para identificar una aplicación móvil compatible presente en el dispositivo móvil 110. El módulo de selección de aplicaciones se configura para generar cualquier comunicación relevante para determinar las aplicaciones disponibles en un dispositivo móvil 110, seleccionar una aplicación móvil compatible, proporcionar cualquier información solicitada por el dispositivo móvil 110 y procesar una transacción usando credenciales asociadas con la aplicación móvil seleccionada 112.

Los componentes en el dispositivo móvil 110 pueden incluir hardware del dispositivo 118, un sistema operativo móvil (OS) 116 y un entorno de aplicaciones 111 en el que pueden residir una aplicación móvil 112 y una aplicación de servicios de valor agregado (VAS). El hardware del dispositivo 118 puede incluir una interfaz sin contacto 119 que puede interactuar con un lector sin contacto 123 de un dispositivo de acceso 120. Los ejemplos de la interfaz sin contacto 119 pueden incluir uno o más transceptores de radiofrecuencia (RF) que pueden enviar y recibir comunicaciones utilizando comunicaciones de campo cercano (NFC) u otros protocolos de comunicación de radiofrecuencia o inalámbrica como Bluetooth, Bluetooth de baja energía (BLE), Wi-Fi, iBeacon, etc.

El entorno de aplicaciones 111 del dispositivo móvil 110 puede alojar una aplicación móvil 112 y una aplicación de servicios de valor agregado (VAS) 114. La aplicación móvil 112 puede ser proporcionada, instalada y mantenida por un ordenador de aplicación móvil 170. La aplicación VAS puede ser proporcionada por el ordenador de aplicación móvil 170 o por un ordenador proveedora de servicios VAS (no mostrada). La ordenador de aplicación móvil 170 puede ser propiedad u operada por un desarrollador de aplicaciones móviles que incluye un comercio u otro proveedor de servicios. La aplicación móvil 112 puede ser la propia aplicación móvil de un comercio desde la cual los consumidores pueden realizar transacciones de comercio electrónico o punto de venta (POS) con ese comercio, o puede ser una aplicación de cartera móvil que admita múltiples comercios.

La aplicación 114 de servicios de valor agregado (VAS) puede incluir una aplicación que está configurada para administrar datos VAS para el consumidor a través de múltiples comercios, entidades y/o proveedores de servicios diferentes. La aplicación VAS 114 puede almacenar datos de fidelidad organizados por un identificador de entidad (por ejemplo, un identificador del comercio). El identificador del comercio puede incluir, por ejemplo, un identificador de fidelidad que sea uniforme en múltiples dispositivos móviles de modo que la aplicación VAS 114 conozca la ubicación apropiada de los datos VAS almacenados a través de la aplicación VAS 114 para un comercio particular. En algunas modalidades, la aplicación VAS 114 puede ser parte de la aplicación de pago 112 o podría ser una aplicación separada (como se muestra). La aplicación VAS 114 puede identificarse y seleccionarse usando un identificador de applets VAS (VAID) que informa al sistema operativo móvil para enviar una comunicación (es decir, una APDU) a la aplicación VAS 114.

Según algunas modalidades, la aplicación móvil 112 puede incluir applets con credenciales aprovisionadas 113. Los applets 113 pueden configurarse para realizar la funcionalidad de pago descrita en este documento. Por ejemplo, los applets 113 pueden obtener las credenciales aprovisionadas almacenadas en el dispositivo móvil 110, generar criptogramas de transacción y entregar cualquier otra información de pago al sistema operativo móvil 116 para su transmisión a través de la interfaz sin contacto 119 al lector sin contacto 123 del dispositivo de acceso 120. Cada uno de los applets 113 puede incluir datos de cuenta aprovisionados que están asociados con una o más cuentas. Como se describirá con más detalle a continuación, cada uno de los applets 113 puede identificarse mediante uno o más identificadores de applet de la cuenta (AID), incluidos identificadores de applets confiables (TAID) e identificadores de applets no confiables (UAID) basados en el estado de las credenciales de la cuenta almacenadas allí (es decir, dependiendo de si la cuenta fue validada por un emisor antes de que se aprovisionaran las credenciales de la cuenta). Por ejemplo, un applet 113 puede incluir un módulo de software o un conjunto de interfaces de programación de aplicaciones (API) proporcionadas por una red de pago (por ejemplo, VisaNet™) configurada para procesar credenciales de la cuenta asociadas con una cuenta aprovisionada a través de la aplicación móvil 112. Por lo tanto, cada cuenta aprovisionada en la aplicación móvil 112 puede tener un applet 113 asociado con el mismo o un único applet 113 puede configurarse para elegir entre varias credenciales de la cuenta diferentes asociadas con el mismo applet de la cuenta 113.

La aplicación móvil 112 también puede gestionar interacciones con el ordenador 170 de aplicación móvil, incluidas las comunicaciones de aprovisionamiento de cuenta y/o inscripción de cuenta, procesos de gestión del ciclo de vida y cualquier otro proceso de mantenimiento. La aplicación móvil 112 puede realizar un conjunto de funciones para inscribir o aprovisionar una cuenta con el ordenador de aplicación móvil 170.

El ordenador de aplicación móvil 170 puede incluir cualquier desarrollador de aplicaciones o propietario de la aplicación móvil 112 y/o la aplicación VAS 114. El ordenador de aplicación móvil 170 puede incluir un módulo de aprovisionamiento de credenciales 171 que puede configurarse para aprovisionar credenciales de la cuenta al dispositivo móvil 110 a través de la aplicación móvil 112. Se debe tener en cuenta que en algunas modalidades, la aplicación de pago 112 y la aplicación VAS 114 pueden ser aprovisionadas por cualquier entidad dentro de un ecosistema de comunicación móvil (por ejemplo, operador de red móvil, fabricante de dispositivo, red de procesamiento de pagos 150, etc.). El módulo de aprovisionamiento de credenciales 171 puede incluir cualquier módulo de software y hardware que permita que el ordenador de aplicación móvil 170 facilite el aprovisionamiento de información de cuenta en un dispositivo móvil 110. Además, en algunas modalidades, el aprovisionamiento de credenciales puede ser completado por un servicio de aprovisionamiento u otro tercero (no mostrado).

En implementaciones basadas en elementos seguros, una aplicación sin contacto (por ejemplo, una cartera móvil o una aplicación de pago para transacciones sin contacto) que usa una interfaz sin contacto 119 para comunicarse con un lector sin contacto 123 de un dispositivo de acceso 120 tendría que codificarse y ejecutarse en un entorno de ejecución confiable (por ejemplo, un elemento seguro) para obtener acceso a la interfaz sin contacto 119. En algunas modalidades, el dispositivo móvil 110 puede incluir un sistema operativo móvil (OS) 116 que implementa un conjunto

de interfaces de programación de aplicaciones de emulación de tarjeta (API) 117 tales como API de emulación de tarjeta servidor (HCE) para permitir que la aplicación móvil 112 obtenga acceso a la interfaz sin contacto 119 sin requerir el uso de un elemento seguro (no mostrado). Por ejemplo, las API de emulación de tarjeta 117 pueden codificarse y ejecutarse desde el OS móvil 116 del dispositivo móvil 110, y pueden incluir llamadas de función de programación para permitir que la aplicación móvil 112 para recibir, procesar y responder a comunicaciones de transacción tales como comandos de la unidad de datos del protocolo de aplicación (APDU) enviados desde el lector sin contacto 123 del dispositivo de acceso 120. De esta manera, el dispositivo móvil 110 puede realizar transacciones sin contacto sin requerir acceso a un elemento seguro (no mostrado) en el dispositivo móvil 110.

Una vez que el dispositivo móvil 110 y la aplicación móvil 112 han sido aprovisionados con las credenciales de la cuenta 113, el dispositivo móvil 110 puede realizar transacciones interactuando con el lector sin contacto 123 del dispositivo de acceso 120 (por ejemplo, en una ubicación del punto de venta (POS) del comercio). El lector sin contacto 123 puede incluir uno o más transceptores de radiofrecuencia (RF) que pueden enviar y recibir comunicaciones utilizando comunicación de campo cercano (NFC) u otros protocolos de comunicación de radiofrecuencia o inalámbrica como Bluetooth, BLE, Wi-Fi, iBeacon, etc..

Para realizar una transacción, un usuario del dispositivo móvil 110 puede colocar el dispositivo móvil 110 cerca del lector sin contacto 123 del dispositivo de acceso 120 para escanear por el lector sin contacto 123 del dispositivo de acceso 120. El dispositivo móvil 110 puede proporcionar al dispositivo de acceso 120 credenciales de la cuenta (por ejemplo, un identificador de la cuenta como un número de cuenta principal (PAN), un identificador de la cuenta alternativo como un PAN alternativo o un token, etc.) para identificar la cuenta del usuario e información adicional tal como un identificador de cartera (WID) asociado con el ordenador de aplicación móvil 170 u otro desarrollador de aplicaciones móviles. Por ejemplo, en algunas modalidades, las credenciales (por ejemplo, un identificador de la cuenta o token) e información adicional (por ejemplo, un criptograma de transacción, parámetros de cuenta, etc.) se pueden transmitir al dispositivo de acceso 120 en respuestas APDU que responden a una serie de comandos APDU recibidos del dispositivo de acceso 120. El dispositivo de acceso 120 o un ordenador del comercio (no mostrada) acoplada al dispositivo de acceso 120 puede generar un mensaje de solicitud de autorización que incluye el identificador o token de la cuenta, e información adicional como un criptograma de transacción y otros datos de transacción, y reenviar el mensaje de solicitud de autorización a una red de pago para el procesamiento de transacciones. Más detalles sobre el procesamiento de transacciones se describen a continuación en referencia a la Figura 4.

Como se explicó anteriormente y como puede describirse con más detalle a continuación, el dispositivo de acceso 120 puede comunicarse con el dispositivo móvil 110 para obtener información de pago. Sin embargo, ciertos dispositivos de acceso solo pueden configurarse para recibir y procesar tipos particulares de información asociados con aplicaciones de pago particulares. Por ejemplo, si el dispositivo de acceso 120 solo se configura para procesar transacciones utilizando una determinada red de procesamiento de pagos 150 (por ejemplo, VisaNet™), el dispositivo de acceso 120 no puede procesar la información de transacción que se origina en las aplicaciones de pago que están configuradas para proporcionar información en un formato de procesamiento de una red de procesamiento de pagos diferente 150 (por ejemplo, MasterCard™). En consecuencia, los dispositivos de acceso 120 y los dispositivos móviles 110 pueden realizar un proceso de selección de aplicaciones móviles antes de que se pueda iniciar una transacción. A continuación se proporciona más información con respecto a estos procesos en referencia a las Figuras 2-4.

La Figura 2 muestra un diagrama de flujo ilustrativo de un método para realizar una comunicación de corto alcance entre un dispositivo móvil 110 y un dispositivo de acceso 120 durante una transacción de pago, de acuerdo con una modalidad de la invención. Se debe tener en cuenta que la Figura 2 muestra una implementación ilustrativa de los conceptos descritos en este documento y las modalidades no se limitan a tales protocolos, métodos y etapas de comunicación. Por consiguiente, aunque la Figura 2 muestra una implementación de un protocolo de interfaz de datos mejorado para comunicar información de pago entre un dispositivo de acceso 120 y un dispositivo móvil 110, podrían implementarse muchos otros protocolos y técnicas de comunicación.

El lector sin contacto 123 del dispositivo de acceso 120 puede configurarse para identificar la presencia de un dispositivo móvil 110 dentro del rango de comunicación. Por ejemplo, la interfaz sin contacto 119 del dispositivo móvil 110 puede hacer ping o intentar encontrar dispositivos adecuados para comunicarse periódicamente. Cuando el dispositivo de acceso 120 detecta la presencia del dispositivo móvil 110 cerca del lector sin contacto 123 del dispositivo de acceso 120, el módulo de selección de aplicaciones 121 del dispositivo de acceso 120 puede iniciar una transacción enviando una solicitud de applets de la cuenta disponibles al dispositivo móvil 110. La solicitud de applets disponibles se envía para obtener información sobre qué aplicaciones móviles y applets de la cuenta correspondientes (por ejemplo, una lista de identificadores de applet de cuenta) pueden estar disponibles en el dispositivo móvil 110. En algunas modalidades, la solicitud de applets disponibles 201 puede tener la forma de un comando "seleccionar entorno de sistema de pago de proximidad (PPSE)". En tales modalidades, la solicitud de applets disponibles 201 puede incluir un identificador de entorno de pago (por ejemplo, un nombre PPSE tal como "2PAY.SYS.DDF01") para identificar el entorno de pago soportado por el dispositivo de acceso 120.

Al recibir la solicitud 201 de aplicaciones disponibles, el dispositivo móvil 110 puede identificar y procesar la solicitud al reconocer el identificador de entorno de pago (por ejemplo, el nombre PPSE) incluido en la solicitud, y responder

enviando una respuesta 202 de aplicaciones disponibles al dispositivo de acceso 120. La respuesta 202 de aplicaciones disponibles puede incluir una lista de identificadores de applet de la cuenta (AID) disponibles, un identificador de cartera asociado con la aplicación móvil 112, opciones de configuración de la aplicación asociadas con los AID disponibles, y puede incluir el identificador de entorno de pago de proximidad (por ejemplo, nombre PPSE) como el nombre de archivo dedicado.

En algunas modalidades, la respuesta 202 de aplicaciones disponibles puede tener la forma de una respuesta a "seleccionar PPSE" y puede incluir información de control de archivo PPSE (FCI). Por ejemplo, la respuesta 202 de aplicaciones disponibles puede incluir una entrada de directorio para cada AID disponible en el dispositivo móvil 110 con un identificador de cartera asociado con cada AID disponible. Cada entrada de directorio puede incluir información como el AID, una etiqueta de aplicación asociada con el AID (por ejemplo, un mnemotécnico asociado con el AID), un identificador de cartera (WID) asociado con la aplicación móvil, un indicador de prioridad de la aplicación que indica la prioridad del AID, un identificador de kernel que indica la preferencia de kernel de la aplicación y/o información adicional relacionada con el AID particular. La respuesta 202 de solicitudes disponibles también puede incluir otros datos, como datos discrecionales del emisor de FCI o cualquier otra información relevante.

El dispositivo de acceso 120 puede determinar un applet de la cuenta compatible en función de los identificadores de applet disponibles recibidos y puede enviar un comando 203 de "selección de aplicación" que incluye el AID seleccionado al dispositivo móvil 110.

Además, en algunas modalidades, al recibir el mensaje 203 de selección de aplicación, el dispositivo móvil 110 puede enviar una solicitud de datos de transacción de terminal 204 para solicitar datos de transacción del dispositivo de acceso 120 que puede ser necesario para ejecutar la transacción usando la aplicación seleccionada asociada con la AID seleccionado. En algunas modalidades, la solicitud 204 de datos de transacción de terminal puede tener la forma de una "Respuesta de AID Seleccionada" y puede incluir información de control de archivo (FCI) del identificador de applets (AID) con el AID seleccionado como el nombre de archivo dedicado. La solicitud de datos de transacción de terminal puede incluir una lista de identificadores de datos de transacción para solicitar los datos apropiados del dispositivo de acceso 120, y la lista de identificadores de datos de transacción puede tener la forma de una lista de objetos de datos de opciones de procesamiento (PDOL).

Los datos de transacción solicitados por la aplicación móvil 113 para la transacción pueden incluir un identificador de entidad asociado con el dispositivo de acceso 120 (por ejemplo, un identificador del comercio (MID)), opciones de procesamiento de terminal (TPO), cantidad autorizada, otra cantidad, código de país de terminal, resultados de verificación de terminal, código de moneda de transacción, datos de transacción, tipo de transacción y/o un número impredecible. La solicitud de datos de transacción de terminal también puede incluir otros datos, como datos discrecionales del emisor de FCI, identificador del programa de aplicación y preferencia de idioma. En otras modalidades, la información de transacción puede proporcionarse como parte del mensaje de selección de aplicación 203 y/o como parte del mensaje de solicitud de aplicaciones disponibles 201.

Después de recibir la solicitud 204 de datos de transacción de terminal, el dispositivo de acceso 120 puede enviar, a la aplicación móvil 112 del dispositivo móvil 110, los datos de transacción de terminal 205 solicitados por la aplicación móvil 113. En algunas modalidades, los datos de transacción de terminal 205 pueden enviarse en forma de un comando de obtención de opciones de procesamiento (GPO), y pueden incluir los datos de transacción de terminal solicitados 205 en una lista de objetos de datos de opciones de procesamiento (PDOL). En algunas modalidades, los datos de transacción de terminal 205 (por ejemplo, opciones de procesamiento de transacción (TPO)) pueden incluir un indicador de TPO que indica qué tipos de datos de transacción admite el dispositivo de acceso 120.

Debido a que la aplicación móvil agrega datos de la cuenta sin validar la cuenta con un emisor de la cuenta, diferentes niveles de seguridad de las transacciones (por ejemplo, transacción con tarjeta presente (CP), transacción sin tarjeta (CNP), transacción de autenticación avanzada (por ejemplo, verificación 3DS), etc.) puede proporcionarse en función del propietario/desarrollador de la aplicación móvil, el comercio y el estado del applet de la cuenta seleccionado provisto en el dispositivo móvil 110. Por ejemplo, dependiendo del tipo de credenciales seleccionadas, pueden existir diferentes niveles de seguridad para la transacción. Por lo tanto, si se selecciona un applet de la cuenta validado o confiable, la aplicación móvil puede iniciar una transacción de tarjeta presente (CP). Sin embargo, si se utilizan cuentas no confiables o no confiables, la aplicación móvil puede iniciar una transacción de tarjeta no presente (CNP). Además, cuando sea compatible con un POS del comercio, la aplicación móvil puede iniciar una transacción utilizando una carga útil de transacción de autenticación mejorada (por ejemplo, 3D-Secure). En consecuencia, el TPO (también denominado opciones de configuración del dispositivo de acceso) permite que el dispositivo móvil 110 determine si el dispositivo de acceso 120 se configura para procesar el tipo de transacción que está asociada con el applet de la cuenta seleccionado.

Una vez que el applet seleccionado 113 del dispositivo móvil 110 recibe los datos de transacción de terminal 205, el dispositivo móvil 110 obtiene las credenciales de la cuenta relevantes del applet seleccionado, así como cualquier otra información de pago relevante y puede enviar un conjunto de información de procesamiento de transacciones 206 que incluye el credenciales de la cuenta y cualquier otra información relevante de procesamiento de transacciones para el dispositivo de acceso 120. En algunas modalidades, la información de procesamiento de transacción 206 puede

enviarse en forma de una respuesta de la "obtención de opciones de procesamiento" (GPO). En algunas modalidades, la información de procesamiento de transacciones puede incluir uno o más ubicaciones de archivos de aplicación (AFL) que pueden ser utilizados como direcciones de archivo por el dispositivo de acceso 120 para leer los datos de la cuenta almacenados en el dispositivo móvil 110, y un perfil de intercambio de aplicaciones (AIP) que se puede usar para indicar las capacidades de la aplicación de pago.

Por ejemplo, la información de procesamiento de transacciones puede incluir cualquier credencial para la transacción, incluido un criptograma de transacción generado utilizando información de transacción, datos equivalentes de Track-2 y datos adicionales. Por ejemplo, la información de procesamiento de transacciones puede incluir un indicador de applet no confiable donde la transacción se origina usando un applet de la cuenta no confiable. Además, la información de procesamiento de transacciones puede incluir datos de la aplicación del emisor (IAD), un indicador de factor de forma (FFI), calificadores de transacciones de tarjetas (CTQ), datos de información de criptogramas (CID), un contador de transacciones de aplicaciones (ATC) y/o una número de secuencia de aplicación PAN (PSN). En algunas modalidades, los datos de la aplicación del emisor (IAD) pueden incluir un indicador de longitud que indica la longitud de la IAD, número de versión de criptograma (CVN) que indica la versión del criptograma de transacción, un indicador de clave derivada (DKI) que puede usarse para identificar una clave maestra (por ejemplo, una clave maestra asociada con el emisor), y/o resultados de verificación de tarjeta (CVR).

Debe entenderse que en algunas modalidades, la información de procesamiento de transacciones 206 que se envía desde el dispositivo móvil 110 al dispositivo de acceso 120 puede incluir parte o la totalidad de la información descrita anteriormente, y en algunas modalidades, puede incluir información adicional no específicamente descrita.

Después de que el dispositivo de acceso 120 recibe la información de procesamiento de transacciones 206, el dispositivo de acceso 120 puede enviar una solicitud de datos de la cuenta 207 al dispositivo móvil 110 para leer datos de cuenta adicionales 208 que pueden almacenarse en el dispositivo móvil 110. En algunas modalidades, la solicitud de datos de la cuenta 207 puede tener la forma de un comando de "registro de lectura", y puede incluir un localizador de archivos de aplicación (AFL) que indica la ubicación de los datos de cuenta que el dispositivo de acceso 120 está intentando leer. El AFL incluido en la solicitud de datos de la cuenta 207 puede corresponder a un AFL en la información de procesamiento de transacciones 206 que se proporcionó al dispositivo de acceso 120 desde el dispositivo móvil 110.

En respuesta a la recepción de la solicitud de datos de la cuenta 207 del dispositivo de acceso 120, el dispositivo móvil 110 puede enviar los datos de la cuenta 208 almacenados en la ubicación indicada por la AFL para acceder al dispositivo 120. En algunas modalidades, los datos 208 de la cuenta pueden enviarse en forma de una respuesta de "registro de lectura". Los datos de la cuenta 208 pueden incluir, por ejemplo, el control del uso de la aplicación que indica las restricciones del emisor sobre el uso y los servicios permitidos para la aplicación, el nombre del titular de la tarjeta, los datos exclusivos del cliente, el código del país del emisor y/u otros datos relacionados con la cuenta que sean accesibles en la ubicación AFL y se almacena en el dispositivo móvil 110.

Debe entenderse que en algunas modalidades, los datos de cuenta 208 que se envían desde el dispositivo móvil 110 al dispositivo de acceso 120 pueden incluir parte o la totalidad de la información descrita anteriormente, y en algunas modalidades, pueden incluir información adicional no específicamente descrita. Además, toda esta información se puede proporcionar en respuesta a la recepción de un mensaje de selección y/o la obtención de credenciales de pago como se describirá con más detalle a continuación.

B. Métodos ilustrativos que incorporan una interfaz de datos mejorada

Las Figuras 3A-3E ilustran un diagrama de flujo ilustrativo de una interacción entre un dispositivo móvil 110 que incluye una aplicación VAS 114 y una aplicación móvil 112 con applets de la cuenta 113, y un dispositivo de acceso del comercio 120 que usa una interfaz de datos mejorada para una transacción sin contacto.

1. Inscripción de tarjeta e inicio de transacción

Primero, las etapas 301-304 ocurren en algún momento antes de una transacción y pueden ocurrir antes de que un consumidor llegue a una ubicación del comercio. El consumidor puede aprovisionar cuentas de tarjeta usando la aplicación móvil antes de que se realice el proceso que se muestra en la Figura 3. Una vez que las credenciales de la cuenta de la tarjeta se aprovisionan en el dispositivo móvil 110 a través de la aplicación móvil, puede comenzar el proceso que se muestra en la Figura 3.

En la etapa 301, un consumidor selecciona una tarjeta o una prioridad de varias tarjetas para usar en una transacción a través de una aplicación móvil. Además, el consumidor puede establecer la prioridad para cada tarjeta que está inscrita en una aplicación móvil 112 de manera que el dispositivo móvil 110 (o el dispositivo de acceso del comercio 120) puede seleccionar una tarjeta preferida donde un dispositivo de acceso del comercio 120 admite múltiples opciones durante una transacción. Alternativa o adicionalmente, se puede solicitar al consumidor antes o durante una transacción sus preferencias para una transacción. Por ejemplo, el usuario puede abrir una aplicación móvil en su dispositivo antes de iniciar una transacción y las tarjetas disponibles se pueden proporcionar al usuario para su

selección. Alternativa o adicionalmente, las preferencias preconfiguradas del usuario pueden usarse para seleccionar la tarjeta o cuenta preferida. Además, en algunas modalidades, la aplicación móvil puede seleccionarse automáticamente por el dispositivo de acceso 120 de una variedad de aplicaciones móviles en el dispositivo móvil 110 durante el proceso de selección de la aplicación (por ejemplo, las etapas 201-203 de la Figura 2).

En la etapa 302, la aplicación móvil 112 determina si cada una de las tarjetas o cuentas seleccionadas (y sus credenciales de la cuenta correspondientes) corresponden a applets de las cuentas confiables o applets de las cuentas no confiables. Un applet de la cuenta puede tener identificadores de applet diferentes en función de si el applet de la cuenta se considera "confiable" o "no confiable". Como se explicó anteriormente, un applet de la cuenta no confiable puede identificarse utilizando un identificador de applets de la cuenta no confiable (UAID) que indica que el applet de la cuenta asociada se aprovisionó en el dispositivo sin ser autenticado, aprobado o validado por un emisor asociado con la cuenta. En contraste, un applet de la cuenta confiable se identifica usando un identificador de applets confiable (TAID) que indica que el applet de la cuenta asociada se aprovisionó con credenciales de la cuenta solo después de que un emisor asociado con la cuenta participó (es decir, aprobado, validado y/o acordado) en el aprovisionamiento de las credenciales de la cuenta con la aplicación móvil.

La aplicación móvil 112 puede determinar si el applet de la cuenta asociada con una tarjeta o cuenta seleccionada es confiable o no a través de cualquier método adecuado. Por ejemplo, la aplicación móvil puede determinar un estado para cada uno de los applets de la cuenta seleccionados por el consumidor como un applet confiable o un applet no confiable en función de un proceso de aprovisionamiento asociado con cada uno del uno o más applets. Por ejemplo, la aplicación móvil puede incluir una bandera u otro indicador junto con las credenciales de la cuenta almacenada o el applet de la cuenta asociada con cada cuenta para indicar si las credenciales de la cuenta asociadas con el applet fueron validadas por un emisor de cuenta asociada durante el aprovisionamiento. Alternativa o adicionalmente, la aplicación móvil puede comparar un emisor asociado con las credenciales de la cuenta con una lista de emisores integrados conocidos para la aplicación móvil y puede asignar al applet de la cuenta un estado de applet de la cuenta confiable o un estado de applet de la cuenta no confiable basado en la identidad del emisor de la cuenta.

Alternativa o adicionalmente, la aplicación móvil puede determinar el estado de un applet de la cuenta en función de la identidad de la aplicación móvil en general. Por ejemplo, si la aplicación móvil está configurada para validar todas las cuentas y/o ninguna solicitud de aprovisionamiento de cuenta con emisores, entonces el estado de los applets de la cuenta puede ser uniforme en todos los applets de la cuenta agregados a través de la aplicación móvil. Por lo tanto, el estado de cualquier applet de la cuenta aprovisionada a través de dicha aplicación móvil se determinaría en función de la configuración y/o identidad de la aplicación móvil que aprovisionó el applet de la cuenta.

En las etapas 303A-303B, la aplicación móvil clasifica los identificadores de applet asociados con las cuentas seleccionadas. Una vez que se ha determinado el estado de cada uno de los applets de la cuenta seleccionados, la aplicación móvil clasifica un identificador de applets para cada uno de los applets de la cuenta seleccionados por el consumidor como un identificador de applets confiable o un identificador de applets no confiables basado en el estado de cada cuenta applets. La aplicación móvil puede clasificar o determinar que el applet tiene un TAID o UAID a través de cualquier método adecuado.

Por ejemplo, la aplicación móvil puede proporcionar un identificador de applets confiables a cada applet de la cuenta aprovisionada a la aplicación móvil y la aplicación móvil puede asignar el identificador de applets de la cuenta de applet a un identificador de applets no confiables predeterminado asociado con el identificador de applets original cuando la aplicación móvil determina que el estado del applet no es confiable. En tal modalidad, el identificador de applets confiables sería el identificador de applets tradicional asociado con applets tradicionales y aplicaciones aprovisionadas para datos de cuenta. Por lo tanto, un nuevo identificador de applets de la cuenta solo puede asignarse a un applet de la cuenta cuando se determina que el applet de la cuenta no es confiable para una cuenta. Por ejemplo, la aplicación móvil puede aplicar una tabla de mapeo TAID a UAID para determinar las relaciones entre un identificador de applets confiable y no confiable y asignar un identificador de applets no confiables a un applet de cuenta.

Alternativa o adicionalmente, en algunas modalidades, la aplicación móvil puede haber provisto el applet de la cuenta con un UAID o TAID durante el aprovisionamiento basado en la participación del sistema emisor. Por lo tanto, la aplicación móvil puede clasificar los applets de la cuenta como que tienen un UAID o un TAID identificando un tipo de identificador de applets (por ejemplo, UAID, TAID) asociado con el applet de la cuenta. Por ejemplo, el UAID y el TAID pueden tener diferentes indicadores de datos o indicadores para indicar si una aplicación es confiable o no. Por ejemplo, un UAID puede tener un bit extra o puede tener un bit indicador mientras que un TAID puede no tener tales características, o viceversa. Además, se puede implementar cualquier otro método para identificar el caracter del identificador de applet.

En la etapa 303A, si la aplicación móvil determina que se selecciona una tarjeta confiable, la aplicación móvil 112 selecciona y llena un identificador de applets confiable (TAID) en una lista de applets disponibles junto con el identificador de cartera (WID) asociado con la aplicación móvil 112. Si se seleccionan varias tarjetas (no se muestran), las etapas pueden repetirse.

En la etapa 303B, si la aplicación móvil determina que se selecciona una tarjeta no confiable, la aplicación móvil 112 selecciona y llena un identificador de applets (UAID) no confiable junto con el identificador de cartera (WID) asociado con la aplicación móvil 112.

En las modalidades donde hay múltiples applets y credenciales de la cuenta asociadas con la aplicación móvil, el proceso que se muestra en las etapas 302-303 puede repetirse para cada uno de los applets de la cuenta con los identificadores de applet de la cuenta confiables y no confiables que se cargan en una lista de applet disponibles identificadores para una posible transacción.

En la etapa 304, la aplicación móvil 112 llena un entorno de sistema de pago de proximidad (PPSE) con la lista de TAID y/o UAID de los applets de la cuenta asociadas con la aplicación móvil junto con el identificador de cartera (WID) asociado con la aplicación móvil en preparación para la comunicación con un lector sin contacto.

En la etapa 305, el dispositivo móvil 110 informa al consumidor que el dispositivo móvil 110 está listo para que se inicie una transacción y que el usuario debe aprovechar el dispositivo móvil 110 al dispositivo de acceso del comercio 120. El consumidor toca el dispositivo 110 en el dispositivo de acceso del comercio 120 para iniciar una sesión de comunicación sin contacto con el dispositivo de acceso del comercio 120.

En la etapa 306, el dispositivo de acceso del comercio 120 identifica que un dispositivo sin contacto está dentro de la proximidad de comunicación y el dispositivo de acceso del comercio 120 solicita información de identificación del identificador de applets (AID) de la aplicación móvil. Por ejemplo, como se describió anteriormente en referencia a la etapa 201 de la Figura 2, el POS del comercio puede enviar un comando "solicitud de selección PPSE" al dispositivo móvil 110. El comando "seleccionar solicitud de PPSE" informa al dispositivo móvil 110 que el lector está dentro del rango de comunicación y que el lector está solicitando una lista de identificadores de applet en el PPSE que están disponibles para su uso en la modalidad de una transacción. En el presente ejemplo, el dispositivo de acceso del comercio (por ejemplo, POS) puede iniciar la comunicación. Sin embargo, en algunas modalidades, la aplicación móvil puede reconocer la presencia del dispositivo de acceso 120 y enviar el comando PPSE primero con todos los datos que se cargan en el PPSE.

En la etapa 307, la aplicación móvil 112 recibe la solicitud de identificación del identificador de applets y prepara la lista de identificadores de applet (AID) para enviar una respuesta. La lista de identificadores de applet disponibles ya puede estar preparada en respuesta a las tarjetas de aprovisionamiento del consumidor y/o seleccionar la aplicación para la transacción (como se describe en la etapa 304 anterior). Por lo tanto, la aplicación móvil 112 puede identificar los identificadores de applet (AID) que se han inscrito para la aplicación móvil 112, así como identificar el identificador de cartera (WID) asociado con la aplicación móvil 112 y generar una lista de identificadores de applet disponibles que incluyen UAID y TAID asociados con la aplicación móvil (u otras aplicaciones móviles en el dispositivo). La aplicación móvil 112 luego envía una respuesta de applet informando al lector sin contacto de qué aplicaciones están disponibles para la transacción. Por ejemplo, la aplicación móvil puede enviar una "respuesta de selección de PPSE" que incluye un VAID, TAID asociados con los applets de la cuenta que están inscritos con la aplicación móvil 112, y los UAID asociados con los applets de la cuenta que están inscritos con la aplicación móvil 112, junto con parámetros adicionales especificados (por ejemplo, WID asociados con los AID). Se pueden encontrar detalles adicionales en referencia a la etapa 202 de la Figura 2 descrita anteriormente.

En la etapa 308, el dispositivo de acceso 120 analiza y procesa la respuesta del identificador de applets para identificar si el lector se configura para procesar cualquiera de los AID recibidos en la respuesta de AID. Si el lector se configura para procesar un VAID identificado en la respuesta PPSE, se puede completar un procesamiento VAS de prepago. Si ninguno de los VAID es compatible con el dispositivo de acceso del comercio 120, el sistema puede omitir las etapas de la Figura 3B y pasar a la Figura 3C.

El módulo de selección de aplicación del dispositivo de acceso 120 puede determinar los identificadores de applet compatibles de la lista de applets disponibles comparando cada uno de los identificadores de applet en la lista de applets disponibles con una lista de identificadores de applet compatibles almacenados en el dispositivo de acceso 120. La lista de applets de cuenta admitidos puede almacenarse en un directorio de TAID y UAID que el dispositivo de acceso 120 se configura para admitir. Además, la lista puede estar separada por TAID y UAID.

Si hay una coincidencia, el módulo de selección de aplicaciones puede almacenar cada uno de los identificadores de applet coincidentes como uno de los AID compatibles en el orden de prioridad indicado por el dispositivo móvil 110 en la lista de applets de la cuenta disponibles. Por lo tanto, el dispositivo de acceso 120 puede tener una lista de applets de cuenta admitidos clasificados en orden de prioridad después de analizar la lista de applets de cuenta disponibles. En algunas modalidades, el dispositivo de acceso 120 puede seleccionar el applet de máxima prioridad de la lista de identificadores de applet compatibles tan pronto como se realiza una primera coincidencia. Sin embargo, en otras modalidades, todos los applets de cuenta disponibles pueden determinarse antes de seleccionar un applet de cuenta.

2. Procesamiento de VAS de prepago

En la etapa 309, el módulo de selección de aplicación del dispositivo de acceso 120 determina si el dispositivo de acceso 120 admite el identificador de applets VAS. Si el lector del comercio admite un AID de la aplicación VAS analizado a partir de la respuesta del identificador de applets (por ejemplo, "Seleccionar respuesta PPSE"), el lector envía un comando de selección a la aplicación VAS que el lector ha seleccionado la aplicación VAS. Por ejemplo, el dispositivo de acceso del comercio 120 puede enviar un comando "Seleccionar VAID VAS" que informa al dispositivo móvil 110 que el dispositivo de acceso del comercio 120 está seleccionando la aplicación VAS para la comunicación. Se pueden encontrar detalles adicionales en referencia a la etapa 203 de la Figura 2 descrita anteriormente.

En la etapa 310, la aplicación móvil VAS recibe la solicitud de selección y prepara una respuesta a la solicitud de selección. Por ejemplo, la aplicación VAS puede enviar una "Respuesta de seleccionar AID de VAS" que puede incluir una solicitud para recibir el identificador del comercio (MID) asociado con el dispositivo de acceso del comercio 120 para asegurarse de que el comercio que solicita los datos sea compatible con la aplicación VAS. La "Respuesta de AID de VAS" puede incluir además un estado VAS, así como parámetros adicionales. Se pueden encontrar detalles adicionales en referencia a la etapa 204 de la Figura 2 descrita anteriormente.

La información "Estado VAS" indica si la aplicación VAS está lista para enviar o recibir datos VAS. Por ejemplo, el estado de VAS podría ser un bit que es un 1 o un 0, donde cuando el estado de VAS es 1, la aplicación de VAS indica al lector que la aplicación de VAS está lista para enviar datos de VAS a un dispositivo de acceso 120. Después de que los datos de VAS se hayan entregado al lector y los datos de VAS se hayan procesado, el estado de VAS puede cambiar a 0, lo que significa que la aplicación VAS está lista para aceptar información del lector en la siguiente interacción (por ejemplo, procesamiento VAS de pago).

En la etapa 311, el dispositivo de acceso del comercio 120 recibe la respuesta VAS seleccionada en el PDOL que incluye la solicitud del identificador del comercio (MID) y responde al PDOL devolviendo el MID solicitado por la aplicación VAS. Por ejemplo, el dispositivo de acceso del comercio 120 puede enviar una "Solicitud de obtención de opciones de procesamiento (GPO)" que incluye el MID asociado con el dispositivo de acceso del comercio 120. Se pueden encontrar detalles adicionales en referencia a la etapa 205 de la Figura 2 descrita anteriormente.

En la etapa 312, la aplicación VAS recibe la "Solicitud de GPO" que incluye el MID asociado con el dispositivo de acceso del comercio 120 y determina si el dispositivo de acceso del comercio 120 es compatible o está asociado con alguna de la información de fidelidad almacenada en la aplicación VAS. Por ejemplo, la aplicación VAS puede determinar que el MID recibido es válido y que el MID está asociado con uno o más identificadores de fidelidad (LID) almacenados en la aplicación VAS. Luego, la aplicación VAS puede preparar y enviar cualquier LID (por ejemplo, un número de club de fidelidad) o información de datos del contenedor de fidelidad (LCD) (por ejemplo, un cupón, etc.) asociado con la información MID en la respuesta de GPO.

En consecuencia, la aplicación VAS responde con una "Respuesta de GPO" que incluye cualquier información relevante de fidelidad que podría ser: (1) datos de fidelidad "específicos" para un MID determinado (por ejemplo, cupones, número de tarjeta del club, etc.) o (2) "genérico "datos de fidelidad (por ejemplo, dirección de correo electrónico, número de teléfono, etc.) asociados con el consumidor. Por lo tanto, el dispositivo de acceso del comercio 120 ha sido validado como operado por una entidad con datos asociados almacenados por la aplicación VAS. Por lo tanto, la aplicación VAS envía cualquier identificador de fidelidad y datos del contenedor de fidelidad almacenados en el VAS al dispositivo de acceso del comercio 120. Se pueden encontrar detalles adicionales en referencia a las etapas 206 de la Figura 2 descritos anteriormente.

En la etapa 313, el dispositivo de acceso del comercio 120 puede recibir los datos, aplicar las reglas de aplicación VAS asociadas con la información de fidelidad recibida y aplicar toda la información LCD recibida (por ejemplo, cupones y descuentos) a la transacción. Por lo tanto, el proceso de solicitud de VAS previo a la transacción se ha completado y la transacción puede continuar hasta la etapa de pago.

3. El dispositivo de acceso del comercio admite un identificador de applets confiables

En la etapa 314, el dispositivo de acceso del comercio 120 puede decidir si selecciona el TAID o el UAID asociado con la aplicación móvil 112 que se recibió y analizó a partir de la respuesta PPSE en la etapa 308. Si el dispositivo de acceso del comercio 120 selecciona un TAID, el flujo se mueve a la etapa 315. De lo contrario, el diagrama de flujo se mueve a la etapa 317.

En la etapa 316, el dispositivo de acceso del comercio 120 selecciona un TAID asociado con un applet de la cuenta confiable. Esta es una transacción de pago sin contacto típica que existe actualmente y el dispositivo de acceso del comercio 120 envía un mensaje de comando "solicitud de selección de TAID" a la aplicación móvil 112 para preparar los datos apropiados para el procesamiento de la transacción. Por ejemplo, la aplicación móvil 112 puede responder con un comando "Seleccionar respuesta de TAID" y una transacción cara a cara de tarjeta presente típica puede iniciarse y procesarse como se describió anteriormente en referencia a las etapas 202-208 de la Figura 2.

Por ejemplo, el intercambio de datos de pago puede incluir una carga útil de datos configurada para al menos tres tipos diferentes de transacciones dependiendo de la aplicación móvil 112, el dispositivo de acceso del comercio 120 y

las tarjetas seleccionadas. Las cargas útiles pueden incluir al menos una de las tres opciones (CP, CNP o 3D-Secure) en función de las opciones de configuración del dispositivo de acceso (es decir, TPO o información de configuración del dispositivo de acceso) transmitidas durante el intercambio de comunicación sin contacto. También se pueden capturar opciones de carga útil de pago adicionales como reconocería una persona con habilidades normales.

4. El dispositivo de acceso del comercio admite el identificador de applets no confiable

Sin embargo, algunos comercios pueden optar por utilizar el UAID porque proviene de una aplicación móvil en la que confían y/o porque no hay TAID presentes. En consecuencia, en la etapa 317, el dispositivo de acceso del comercio 120 puede determinar que el identificador de cartera (WID) asociado con la aplicación móvil 112 está asociado con una aplicación que el dispositivo de acceso del comercio 120 admite. Por lo tanto, el dispositivo de acceso del comercio 120 puede determinar que la aplicación móvil es su aplicación móvil y/o fue desarrollada por una parte en la que confían. Como tal, el dispositivo de acceso 120 puede determinar que el identificador del comercio (MID) está asociado con una entidad confiable antes de seleccionar el identificador de applets no confiables de la lista de applets disponibles.

Sin embargo, si el dispositivo de acceso del comercio 120 determina que confía en la aplicación móvil asociada con el MID, el dispositivo de acceso del comercio 120 puede generar un mensaje de "seleccionar solicitud de UAID" y enviar el mensaje de "seleccionar solicitud de UAID" a la aplicación móvil 112. En algunas modalidades, el dispositivo de acceso del comercio 120 puede enviar el comando "solicitud de selección de UAID" suponiendo que el comercio admite transacciones de tarjeta no presente (CNP) (mediante la selección de UAID) y que el comercio reconoció su WID (recibido en "Seleccionar respuesta PPSE") o decidió aceptar los datos de pago de la aplicación móvil de otra persona en la que confían.

En la etapa 318, la aplicación móvil 112 recibe la "solicitud de selección de UAID" y llena un PDOL con la información relevante. Sin embargo, la aplicación móvil 112 puede solicitar al dispositivo de acceso del comercio 120 el MID para que la aplicación móvil 112 no proporcione información a un dispositivo de acceso del comercio 120 que no admite. En consecuencia, antes de que la aplicación del comercio proporcione la información de pago al dispositivo de acceso del comercio 120, la aplicación móvil 112 puede solicitar la MID del dispositivo del comercio. Por lo tanto, la aplicación móvil puede garantizar que el dispositivo de acceso del comercio 120 esté asociado con un comercio que desarrolló la aplicación móvil 112 o sea un socio del desarrollador de la aplicación antes de proporcionar información de pago al dispositivo de acceso del comercio 120. Se pueden encontrar detalles adicionales en referencia a la etapa 203 de la Figura 2 descrita anteriormente.

Además, la aplicación móvil también puede solicitar información de configuración del dispositivo de acceso (también denominada "opciones de procesamiento de transacciones" (TPO)) desde el dispositivo de acceso del comercio 120 para determinar qué opciones de procesamiento admite el dispositivo de acceso del comercio. En consecuencia, la "respuesta de selección de UAID" puede incluir dos preguntas diferentes para el dispositivo de acceso del comercio 120, (1) ¿qué es ese MID? y (2) ¿qué tipo de modos de procesamiento admite?

En la etapa 319, el dispositivo de acceso del comercio 120 puede recibir la "respuesta de selección de UAID" que incluye la solicitud para el TPO y el MID y puede enviar una "Solicitud de GPO" con el MID y el TPO que son compatibles con la aplicación móvil 112. El TPO puede incluir una máscara de bits del dispositivo de acceso 120 opciones de pago sin contacto compatibles. Por ejemplo, el TPO puede incluir un indicador de 3 dígitos de "XYZ", donde X indica si el lector es capaz de aceptar una carga útil de la transacción de tarjeta chip presente (CP) de la aplicación móvil 112, Y indica una transacción de tarjeta no presente (CNP) carga útil, y Z indica una transacción de tarjeta de autorización avanzada no presente (por ejemplo, 3D-Secure).

El tipo de información preparada y pasada por la aplicación móvil 112 durante la transacción puede depender de la TPO. Por ejemplo, si X==1 para la TPO, entonces la aplicación móvil puede establecer un indicador CNP en la información de pago para que un emisor o una red de pago que procese la información de la transacción pueda reconocer que la transacción que se parece a una tarjeta regular presente (CP) La transacción es de hecho una transacción CNP. Además, si Y==1, la aplicación móvil puede responder con datos CNP (por ejemplo, PAN, fecha de vencimiento, CW2) y un comercio envía la transacción utilizando sistemas de procesamiento de transacciones CNP en lugar de sistemas CP. Finalmente, si Z==1, la aplicación móvil responde con datos 3DS (por ejemplo, un valor de verificación autenticado del titular de la tarjeta (CAW)) y el comercio puede procesar la transacción utilizando los datos 3DS. Los datos 3DS pueden ser validados por una red de pago para garantizar que el CAW incluido coincida con un valor generado por la red de pago.

En la etapa 320, la aplicación móvil recibe el mensaje "Solicitud de GPO" que incluye el MID solicitado y el TPO del dispositivo de acceso del comercio 120. La aplicación móvil 112 recibe la información y comprueba si el dispositivo de acceso del comercio 120 está asociado con un comercio válido para acceder al applet de la cuenta asociada con el UAID.

En la etapa 321, la aplicación móvil compara el identificador de entidad (por ejemplo, MID) con el directorio de identificador de entidad almacenado (por ejemplo, directorio de identificador del comercio) para garantizar que el MID

sea correcto y que el propietario y/u operador del dispositivo de acceso esté asociado con el móvil aplicación 112. Si no es así, se genera un mensaje de error y se envía al dispositivo de acceso del comercio 120. Por lo tanto, la aplicación móvil valida que el dispositivo de acceso 120 esté autorizado para acceder a las credenciales de la cuenta asociadas con los UAID seleccionados utilizando el identificador de entidad (por ejemplo, MID) comparando el identificador de entidad (por ejemplo, MID) con una lista de identificadores de entidad confiables (por ejemplos, MID) asociados y almacenados en la aplicación móvil.

En la etapa 322, la aplicación móvil determina si el dispositivo de acceso 120 soporta el TPO del UAID que está seleccionado. Por ejemplo, si la aplicación móvil solo puede procesar transacciones CNP, pero el dispositivo de acceso 120 no se configura para procesar ese tipo de transacciones, se produciría un error y la transacción finalizaría. Por lo tanto, la aplicación móvil puede validar que el dispositivo de acceso 120 se configura para admitir transacciones iniciadas utilizando identificadores de applets no confiables basados en la información de configuración del dispositivo de acceso.

Como otro ejemplo, si la TPO indica que el dispositivo de acceso del comercio 120 solo admite transacciones de tarjeta presente, pero se está seleccionando un UAID, entonces la aplicación móvil 112 puede determinar que los datos de transacción de UAID no son compatibles con el dispositivo de acceso del comercio 120. En consecuencia, se puede enviar una "Respuesta de GPO" al dispositivo de acceso del comercio 120 que incluye un código de error. Un TPO que indica solo que se permite una transacción de tarjeta presente puede crear un error porque el UAID no es confiable y los datos de la transacción CNP pueden usarse para procesar la transacción. Por lo tanto, la aplicación móvil 112 puede determinar que solo está configurada para transacciones con tarjeta no presente y que la aplicación móvil no está lista para una transacción con tarjeta presente porque se seleccionó un UAID. Por lo tanto, la aplicación móvil 112 verifica que el MID sea válido y que la TPO del dispositivo de acceso del comercio 120 soporte el tipo de datos de transacción asociados con el applet del UAID.

En la etapa 323, si el dispositivo de acceso del comercio 120 recibe mensajes de error de las etapas 321 o 322 anteriores, la transacción finaliza. Se puede mostrar un mensaje de error informando al usuario y/o comercio del problema.

En la etapa 324A, el dispositivo de acceso del comercio 120 recibe una "Respuesta de GPO" apropiada de la aplicación móvil y la transacción se procesa según lo indicado por el tipo de información de pago pasada de acuerdo con las opciones de TPO proporcionadas por el dispositivo de acceso del comercio 120. En consecuencia, la aplicación móvil 112 ha determinado que el dispositivo de acceso del comercio 120 está listo para tomar los datos de pago y que el dispositivo de acceso del comercio 120 está asociado con un comercio válido. Por lo tanto, se realiza una acción de pago normal.

La transacción puede procesarse utilizando cualquier proceso adecuado. Por ejemplo, en la etapa 324B, el dispositivo de acceso 120 y la aplicación móvil 112 pueden realizar un intercambio de datos de pago para permitir que se procese la transacción. El intercambio de datos de pago puede incluir cualquier paso relevante para permitir que el dispositivo de acceso 120 genere y envíe un mensaje de solicitud de autorización apropiado para la transacción. Como se describió anteriormente en referencia a la etapa 316 de la Figura 3C, el mensaje de solicitud de autorización puede incluir diferentes cargas útiles basadas en la opción de procesamiento de transacciones (TPO) del dispositivo de acceso 120. Por ejemplo, las cargas útiles pueden incluir al menos una de las tres opciones (CP, CNP o 3D-Secure) en función de las opciones de configuración del dispositivo de acceso (es decir, TPO o información de configuración del dispositivo de acceso) transmitidas durante el intercambio de comunicación sin contacto. Detalles adicionales con respecto al procesamiento de la transacción se pueden encontrar anteriormente en referencia al intercambio de datos de pago que pueden incluir una funcionalidad similar a la encontrada en las etapas 206-208 de la Figura 2 descritos anteriormente.

5. Procesamiento de VAS posterior al pago

En algunas modalidades, se puede usar un proceso de pago posterior para pasar información sobre la transacción, obtener datos VAS de la transacción o para cualquier otro propósito. El procesamiento de VAS posterior al pago puede ocurrir cuando el dispositivo móvil 110 interactúa con el dispositivo de acceso del comercio 120 a través de un segundo toque o iniciación de comunicación sin contacto con el dispositivo de acceso del comercio 120. Durante el segundo toque, la aplicación VAS puede completar los mismos etapas de identificación descritos anteriormente con respecto a las etapas 309-313 descritos anteriormente. Sin embargo, en lugar de obtener información de fidelidad para la aplicación de la transacción, el dispositivo de acceso del comercio 120 puede pasar recibos y/o información actualizada de cupones/fidelidad al dispositivo móvil 110. Además, el MID se puede pasar con la pantalla LCD y el recibo para garantizar que el dispositivo móvil 110 acceda a la LID correcta. La aplicación VAS puede guardar la información del LCD en la memoria del dispositivo móvil 110.

En la etapa 325, el dispositivo de acceso del comercio 120 (si es compatible con VAS para solicitudes de interacción posteriores al pago) puede solicitar al consumidor que presente nuevamente su dispositivo móvil 110 y puede enviar un comando "solicitud de selección VAID". Se puede realizar una verificación similar usando el MID como se describe anteriormente en referencia a la Figura 3B.

En la etapa 326, la aplicación VAS responde con "Seleccionar respuesta VAID" e incluye una solicitud de LCD, recibos, estado VAS y cualquier otra información de fidelidad en un comando PDOL. Sin embargo, en el proceso posterior al pago, el estado de VAS debe establecerse, por ejemplo, en 0, lo que indica que la aplicación VAS está lista para aceptar información del lector.

En la etapa 327, el lector envía datos VAS en un comando de solicitud de GPO. El comando de solicitud de GPO puede incluir pantallas LCD, un recibo o cualquier otro dato relevante para la aplicación VAS. Los datos, como las pantallas LCD y un recibo, también podrían ser URL que indiquen dónde se pueden descargar dichos datos de la web.

En la etapa 328, la aplicación móvil responde con una respuesta de GPO que incluye la confirmación de una interacción exitosa.

En la etapa 329, el dispositivo de acceso 120 recibe la respuesta de GPO y determina que la transacción se ha completado.

C. Sistema de procesamiento de transacciones ilustrativo

La Figura 4 ilustra un sistema de procesamiento de transacciones ilustrativo 400 de acuerdo con una modalidad ilustrativa de la invención. La Figura 4 muestra un diagrama de bloques funcional que ilustra los elementos funcionales principales de un sistema de procesamiento de transacciones ilustrativo que incorpora un dispositivo de comunicación portátil y un dispositivo de acceso 120 que incluye una funcionalidad de interfaz de datos mejorada. Debe entenderse que las modalidades de la invención pueden incluir más de uno de los componentes mostrados individualmente en la Figura 4. Además, algunas modalidades de la invención pueden incluir menos que todos los componentes mostrados en la Figura 4.

El sistema de procesamiento de transacciones ilustrativo puede incluir un consumidor (no mostrado), un dispositivo móvil 110 asociado con el consumidor (u otro titular de la cuenta), un dispositivo de acceso 120, un ordenador del comercio 130, un ordenador receptor 140, un ordenador 150 de red de procesamiento de pagos y un ordenador emisor 160. Los diversos ordenadores pueden configurarse para comunicarse de cualquier manera adecuada utilizando cualquier red de comunicación adecuada. Aunque las entidades se muestran como acopladas a entidades particulares, las entidades pueden configurarse para comunicarse a través de cualquier otra interfaz adecuada y algunas entidades pueden eliminarse y/o agregarse al sistema dependiendo de la configuración del sistema.

En la siguiente descripción, un "receptor" es típicamente una entidad comercial (por ejemplo, un banco comercial) que tiene una relación comercial con un comercio en particular. Un "emisor" es típicamente una entidad comercial (por ejemplo, un banco o cooperativa de crédito) que emite un dispositivo de pago (como una tarjeta de crédito, tarjeta de débito, tarjeta inteligente, dispositivo prepago o dispositivo sin contacto) al propietario de una cuenta y que proporciona y funciones de gestión para la cuenta de pago. Algunas entidades pueden realizar funciones tanto de emisor como de receptor. Una cuenta de pago puede ser cualquier cuenta utilizable en una transacción, como una cuenta de crédito, débito o prepaga.

En una transacción típica, un dispositivo de pago tal como un dispositivo móvil 110 (también denominado "dispositivo de comunicación portátil") o un dispositivo portátil del consumidor, interactúa con un dispositivo de acceso 120 (o, en algunas modalidades, con el ordenador del comercio 130) para iniciar una transacción. Los ejemplos específicos de dispositivos portátiles del consumidor incluyen tarjetas de pago como tarjetas inteligentes con chips, dispositivos de débito (por ejemplo, una tarjeta de débito), dispositivos de crédito (por ejemplo, una tarjeta de crédito) o dispositivos de valor almacenado (por ejemplo, una tarjeta de valor almacenado o tarjeta "prepago").

Como se describió anteriormente en referencia a las Figuras 1-3E, el dispositivo móvil 110 y el dispositivo de acceso 120 utilizan un protocolo de comunicación de interfaz de datos mejorado para seleccionar y obtener credenciales y/o información de cuenta (por ejemplo, identificador de la cuenta de pago, criptograma, información de fidelidad, etc.) asociada con una aplicación móvil seleccionada 112 y/o aplicación de servicios de valor agregado (VAS) 114.

Después de que el dispositivo de acceso 120 recibe las credenciales (por ejemplo, el identificador de la cuenta de pago), el dispositivo de acceso 120 o el ordenador del comercio 130 en comunicación con el dispositivo de acceso 120 genera un mensaje de solicitud de autorización para la transacción. Los datos incluidos en el mensaje de solicitud de autorización (también denominado "solicitud de autorización") pueden incluir datos obtenidos de un dispositivo de comunicación portátil 110, así como otros datos relacionados con la transacción, el titular de la cuenta de pago o el comercio, como uno o más de un número de cuenta de pago, la fecha de vencimiento del dispositivo de pago, un código de moneda, el monto de la venta, un sello de transacción comercial, la ciudad aceptora, el estado/país aceptor, etc.

Un mensaje de solicitud de autorización puede protegerse utilizando un método de cifrado seguro (por ejemplo, SSL de 128 bits o equivalente) para evitar que los datos se vean comprometidos. En una modalidad, el mensaje de solicitud de autorización es un mensaje de intercambio estandarizado tal como un mensaje 8583 de la Organización

Internacional de Normalización (ISO). Un mensaje ISO 8583 incluye un indicador de tipo de mensaje; uno o más mapas de bits que indican qué elementos de datos están presentes en el mensaje y los elementos de datos del mensaje. El mensaje de solicitud de autorización puede comprender información de enrutamiento como parte o además del mensaje de intercambio. Como parte de la generación del mensaje de solicitud de autorización, el ordenador del comercio 130 puede comunicarse con una base de datos que almacena datos tales como datos relacionados con el titular de la cuenta, el dispositivo de pago o el historial de transacciones del titular de la cuenta con el comercio. La ordenador del comercio 130 (o dispositivo de acceso 120) transmite el mensaje de solicitud de autorización a el ordenador receptor 140. La ordenador receptor 140 luego transmite la solicitud de autorización a una red de procesamiento de pagos 150.

Una red de procesamiento de pagos 150, también conocida como "red de pago", es un sistema que puede comprender uno o más servidores, subsistemas de procesamiento de datos, redes y operaciones utilizadas para soportar y entregar servicios de autorización, servicios de archivos de excepción y compensación y servicios de liquidación. Una red de procesamiento de pagos puede procesar una o más transacciones con tarjeta de crédito, transacciones con tarjeta de débito o cualquier otro tipo de transacción comercial. Una red de procesamiento de pagos ilustrativo puede incluir, por ejemplo, VisaNet™. Aunque el sistema de la Figura 4 solo muestra una red de procesamiento de pagos, se puede implementar cualquier número de redes de procesamiento de pagos en el ecosistema de transacciones para permitir que el ordenador del comercio 130 determine la red de procesamiento de pagos 150 que admiten y seleccione la aplicación móvil apropiada 112 asociada con la una o más redes de procesamiento de pagos.

La red de procesamiento de pagos 150 transmite el mensaje de solicitud de autorización a un ordenador emisor 160. La ordenador emisor 160 genera un mensaje de respuesta de autorización que indica si la transacción fue autorizada. El mensaje de respuesta de autorización se enruta de nuevo a el ordenador del comercio 130. La respuesta de autorización puede ser visualizada por el dispositivo de acceso 120 (por ejemplo, un terminal POS), transferida al dispositivo de comunicación portátil 110, impresa en un recibo o transmitida de otro modo al titular de la cuenta de pago.

Al final del día, cada una de las redes de procesamiento de pagos puede llevar a cabo un proceso normal de compensación y liquidación. Un proceso de compensación es un proceso de intercambio de detalles financieros entre un receptor y un emisor para facilitar la publicación en la cuenta del titular de la cuenta de pago y la conciliación de la posición de liquidación del consumidor. La compensación y la liquidación pueden ocurrir simultáneamente.

El término "ordenador", como se usa en el presente documento, se refiere a un sistema que comprende un procesador y un medio legible por ordenador, tal como memoria de ordenador u otro dispositivo de almacenamiento de datos, acoplado al procesador. El medio legible por ordenador almacena el código ejecutable por el procesador.

El término "ordenador servidor" puede incluir un ordenador poderosa o un grupo de ordenadores. Por ejemplo, el ordenador servidor puede ser una unidad central grande, un clúster de miniordenador o un grupo de servidores que funcionan como una unidad. En un ejemplo, el ordenador servidor puede ser un servidor de base de datos acoplado a un servidor web. El ordenador servidor puede estar acoplado a una base de datos y puede incluir cualquier hardware, software, otra lógica o combinación de las anteriores para atender las solicitudes de una o más ordenadores cliente. El ordenador servidor puede comprender uno o más aparatos informáticos y puede usar cualquiera de una variedad de estructuras informáticas, arreglos y compilaciones para atender las solicitudes de una o más ordenadores cliente.

D. Dispositivos del sistema

La Figura 5 es un diagrama de bloques funcional que ilustra un dispositivo de comunicación portátil 502 que puede usarse para realizar operaciones de banca móvil, tales como iniciar transacciones y recibir y mostrar alertas de transacciones, de acuerdo con algunas modalidades de la presente invención. El dispositivo de comunicación portátil 502 puede incluir circuitos que se utilizan para habilitar ciertas funciones del dispositivo, como la telefonía. Los elementos funcionales responsables de habilitar esas funciones pueden incluir un procesador 504 que está programado para ejecutar instrucciones que implementan las funciones y operaciones del dispositivo. El procesador 504 puede acceder al almacenamiento de datos 512 (u otra región o elemento de memoria adecuado) para recuperar instrucciones o datos utilizados en la ejecución de las instrucciones. Los elementos de entrada/salida de datos 508 pueden usarse para permitir que un usuario ingrese datos (a través de un micrófono o teclado, por ejemplo) o reciba datos de salida (a través de un altavoz, por ejemplo). La pantalla 506 también se puede usar para enviar datos a un usuario. El elemento de comunicaciones 510 puede usarse para permitir la transferencia de datos entre el dispositivo 502 y una red inalámbrica (a través de la antena 518, por ejemplo) para ayudar a habilitar la telefonía y las funciones de transferencia de datos. El dispositivo 502 también puede incluir la interfaz de elemento sin contacto 514 para permitir la transferencia de datos entre el elemento sin contacto 516 y otros elementos del dispositivo, donde el elemento sin contacto 516 puede incluir una memoria segura y un elemento de transferencia de datos de comunicaciones de campo cercano (u otra forma de tecnología de comunicaciones de corto alcance). Como se señaló, un teléfono móvil o dispositivo similar es un ejemplo de un dispositivo de comunicación portátil que puede usarse para mostrar alertas como se describe con referencia a las modalidades de la presente invención. Sin embargo, se pueden usar otras formas o tipos de dispositivos sin apartarse de los conceptos subyacentes de la invención. Además, los

dispositivos que se usan para mostrar alertas pueden no requerir la capacidad de comunicarse usando una red celular para ser adecuados para su uso con modalidades de la presente invención.

La Figura 6 es un diagrama de un dispositivo portátil del consumidor 600 en forma de una tarjeta que incluye un elemento de pago sin contacto 602, y que puede usarse para iniciar una transacción, de acuerdo con algunas modalidades de la presente invención. El dispositivo de pago representado en la Figura 6 puede ser una "tarjeta inteligente" o un dispositivo similar, como una tarjeta de crédito o débito en la que está integrado un chip. Una forma de dicho dispositivo se conoce como una tarjeta EMV (Europay™, MasterCard™ y Visa™). En el contexto de la presente invención, EMV se refiere a un estándar para la interoperación de tarjetas IC ("tarjetas con chip") y terminales POS y cajeros automáticos con capacidad de tarjeta IC, y se utiliza para autenticar pagos con tarjeta de crédito y débito. El estándar EMV define las interacciones a nivel físico, eléctrico, de datos y de aplicación entre las tarjetas IC y los dispositivos de procesamiento de tarjetas IC para su uso en transacciones financieras.

La Figura 6 muestra un sustrato 604 que proporciona el factor de forma para el dispositivo 600. Un elemento sin contacto 602 para interactuar con un dispositivo de acceso o transferencia de datos puede estar presente o integrado dentro del sustrato 604. El elemento sin contacto 602 puede incluir un chip u otra forma de elemento de almacenamiento de datos. El elemento sin contacto 602 puede incluir la capacidad de comunicarse y transferir datos utilizando una tecnología de comunicaciones de campo cercano (NFC) u otra tecnología de comunicaciones de corto alcance. La información del consumidor 606, como el número de cuenta, la fecha de vencimiento y el nombre del consumidor, se pueden imprimir o grabar en la tarjeta. Aunque no es necesario para funcionar como un dispositivo de pago sin contacto, el dispositivo 600 puede incluir una banda magnética 608 sobre el sustrato 604, donde la banda magnética 608 permite el acceso al elemento sin contacto 602. Esto puede usarse para proporcionar acceso a los datos almacenados en, o las funciones, del chip que es parte del elemento sin contacto por un terminal que usa un lector de banda magnética.

Los diversos participantes y elementos descritos aquí con referencia a las Figuras 1-4 puede operar uno o más aparatos informáticos para facilitar las funciones descritas en este documento. Cualquiera de los elementos en las Figuras 1-4, incluidos los servidores o las bases de datos, pueden usar cualquier número adecuado de subsistemas para facilitar las funciones descritas en este documento.

Ejemplos de tales subsistemas o componentes se muestran en la Figura 7. Los subsistemas mostrados en la Figura 7 están interconectados a través de un bus de sistema 702. Se muestran subsistemas adicionales tales como una impresora 704, teclado 706, disco fijo 708 (u otra memoria que comprende medios legibles por ordenador), pantalla 710, que está acoplado al adaptador de pantalla 712, y otros. Los dispositivos periféricos y de entrada/salida (E/S), que se acoplan al controlador de E/S 714 (que puede ser un procesador u otro controlador adecuado), se pueden conectar al sistema informático por cualquier cantidad de medios conocidos en la técnica, como puerto serie 716. Por ejemplo, el puerto serie 716 o la interfaz externa 718 se pueden usar para conectar el aparato informático a una red de área amplia como Internet, un dispositivo de entrada de un ratón o un escáner. La interconexión a través del bus del sistema permite que el procesador central 720 se comunique con cada subsistema y controle la ejecución de instrucciones desde la memoria del sistema 722 o el disco fijo 708, así como el intercambio de información entre subsistemas. La memoria del sistema 722 y/o el disco fijo 708 pueden incorporar un medio legible por ordenador.

Las modalidades de la invención no se limitan a las modalidades descritas anteriormente. Por ejemplo, aunque se muestran bloques funcionales separados para un emisor, una red de procesamiento de pagos y un receptor, algunas entidades realizan todas estas funciones y pueden incluirse en modalidades de la invención.

Los detalles específicos con respecto a algunos de los aspectos antes descritos se proporcionan anteriormente. Los detalles específicos de los aspectos específicos se pueden combinar de cualquier manera adecuada. Por ejemplo, el procesamiento de respaldo, el análisis de datos, la recopilación de datos y otras transacciones pueden combinarse en algunas modalidades de la invención. Sin embargo, otras modalidades de la invención pueden dirigirse a modalidades específicas relacionadas con cada aspecto individual, o combinaciones específicas de estos aspectos individuales.

Debe entenderse que la presente invención como se describe anteriormente puede implementarse en forma de lógica de control usando software informático (almacenado en un medio físico tangible) de manera modular o integrada. En base a la divulgación y las enseñanzas proporcionadas en el presente documento, un experto en la técnica puede conocer y apreciar otras formas y/o métodos para implementar la presente invención utilizando hardware y una combinación de hardware y software.

Cualquiera de los componentes o funciones de software descritos en esta aplicación, puede implementarse como código de software para ser ejecutado por un procesador usando cualquier lenguaje de ordenador adecuado como, por ejemplo, Java, C ++ o Perl usando, por ejemplo, técnicas convencionales u orientado a objetos. El código de software puede almacenarse como una serie de instrucciones o comandos en un medio legible por ordenador, como una memoria de acceso aleatorio (RAM), una memoria de solo lectura (ROM), un medio magnético como un disco duro o un disquete disco, o un medio óptico como un CD-ROM. Cualquiera de estos medios legibles por ordenador puede residir en o dentro de un solo aparato computacional, y puede estar presente en o dentro de diferentes aparatos informáticos dentro de un sistema o red.

La descripción anterior es ilustrativa y no es restrictiva. Muchas variaciones de la invención pueden resultar evidentes para los expertos en la materia tras la revisión de la divulgación. Por lo tanto, el alcance de la invención no debe determinarse con referencia a la descripción anterior, sino que debe determinarse con referencia a las reivindicaciones pendientes junto con su alcance completo o equivalentes.

Una o más características de cualquier modalidad pueden combinarse con una o más características de cualquier otra modalidad sin apartarse del alcance de la invención.

Una mención de "un", "uno" o "el" pretende significar "uno o más" a menos que se indique específicamente lo contrario.

Todas las patentes, solicitudes de patentes, publicaciones y descripciones mencionadas anteriormente se incorporan aquí como referencia en su totalidad para todos los fines. Ninguno es admitido como arte previo.

REIVINDICACIONES

1. Un método que comprende:
recibir, por un dispositivo móvil (110), una solicitud de applets disponibles (113) desde un dispositivo de acceso (120);
proporcionar, mediante el dispositivo móvil (110), una lista de applets disponibles (113) que incluye identificadores de applets confiables e identificadores de applets no confiables para el dispositivo de acceso (120), la lista de applets disponibles (113) que incluye un identificador de cartera para cada uno de los applets disponibles, los identificadores de applets confiables que identifican applets que tienen credenciales aprovisionadas con participación del emisor, y los identificadores de applets no confiables que identifican applets que tienen credenciales aprovisionadas sin participación del emisor, en donde el identificador de cartera identifica una aplicación móvil (112) que está asociada con cada una de las aplicaciones disponibles (113);
recibir, por el dispositivo móvil (110), una selección de un identificador de applets de la lista;
cuando el identificador de applets seleccionado es un identificador de applets confiables:
proporcionar, por el dispositivo móvil (110), las credenciales asociadas con el identificador de applets confiables seleccionado al dispositivo de acceso (120); y cuando el identificador de applets seleccionado es un identificador de applets no confiable:
solicitar, por el dispositivo móvil (110), un identificador de entidad del dispositivo de acceso (120);
recibir, por el dispositivo móvil (110), el identificador de entidad asociado con el dispositivo de acceso (120);
validar, mediante el dispositivo móvil (110), que el dispositivo de acceso (120) está autorizado para acceder a las credenciales asociadas con el identificador de applets no confiables seleccionado utilizando el identificador de entidad; y
proporcionar, por el dispositivo móvil (110), las credenciales asociadas con el identificador de applets no confiables seleccionado al dispositivo de acceso (120).

2. El método de la reivindicación 1, en donde antes de recibir la solicitud de applets disponibles (113), el método comprende:
recibir, por el dispositivo móvil (110), una selección prioritaria de uno o más applets, en el que cada uno de los applets está asociado con credenciales almacenadas en el dispositivo móvil (110); determinar, por el dispositivo móvil (110), un estado para cada uno de los applets como un applet confiable o un applet no confiable basado en un proceso de aprovisionamiento asociado con cada uno de los applets;
categorizar, por el dispositivo móvil (110), un identificador de applets para cada uno del uno o más applets como identificadores de applets confiables o identificadores de applets no confiables según el estado de cada uno del uno o más applets; y
generar, mediante el dispositivo móvil (110), la lista de applets disponibles, incluidos los identificadores de applets confiables y los identificadores de applets no confiables.

3. El método de la reivindicación 1 o la reivindicación 2, en donde validar que el dispositivo de acceso (120) está autorizado para usar el applet no confiable seleccionado comprende además:
comparar, mediante el dispositivo móvil (110), el identificador de entidad con una lista de identificadores de entidad confiables asociados con la aplicación móvil (112).

4. El método de cualquier reivindicación anterior, en donde el dispositivo de acceso (120) valida que el identificador de cartera está asociado con una entidad confiable antes de seleccionar el identificador de applets no confiables de la lista de applets disponibles (113).

5. El método de cualquier reivindicación anterior, en donde antes de proporcionar las credenciales, el método comprende además:
recibir, por el dispositivo móvil (110), información de configuración del dispositivo de acceso; y
validar, mediante el dispositivo móvil (110), que el dispositivo de acceso (120) se configura para soportar transacciones iniciadas usando identificadores de applets no confiables basados en la información de configuración del dispositivo de acceso.

6. El método de cualquier reivindicación anterior, en donde las credenciales proporcionadas asociadas con el applet no confiable seleccionado incluyen un indicador de applet no confiable, en donde el indicador de applet no confiable permite a las entidades que dependen de la información de transacción dentro de una carga útil de transacción identificar la transacción como iniciada usando un applet no confiable.

7. Un dispositivo móvil (502), que comprende:
un procesador (504); y
un código de almacenamiento de memoria (512), que cuando es ejecutado por el procesador, implementa el método de cualquier reivindicación anterior.

8. Un método que comprende:
enviar, mediante un dispositivo de acceso (120), una solicitud de applets disponibles a un dispositivo móvil;

recibir, por el dispositivo de acceso, una lista de applets disponibles (113) incluyendo identificadores de applets confiables e identificadores de applets no confiables, la lista de applets disponibles (113) incluyendo un identificador de cartera para cada uno de los applets disponibles (113), los identificadores de applets confiables identificar applets que tienen credenciales aprovisionadas con participación del emisor, y los identificadores de applets no confiables que identifican applets que tienen credenciales aprovisionadas sin participación del emisor, en donde el identificador de cartera identifica una aplicación móvil (112) que está asociada con cada uno de los applets disponibles (113);
determinar, por el dispositivo de acceso (120), identificadores de applet compatibles de la lista de applets disponibles (113);
determinar, por el dispositivo de acceso, un applet de máxima prioridad de los identificadores de applet compatibles; cuando el applet de máxima prioridad corresponde a un identificador de applets confiables en un directorio de identificadores de applets confiables almacenados en el dispositivo de acceso (120):
proporcionar, mediante el dispositivo de acceso (120), una selección del identificador de applets confiables al dispositivo móvil (110); y
recibir, por el dispositivo de acceso (120), credenciales asociadas con el identificador de applets confiables seleccionado desde la aplicación móvil (112) del dispositivo móvil (110);
cuando el applet de máxima prioridad corresponde a un identificador de applets no confiables listado en un directorio de identificadores de applets no confiables almacenados en el dispositivo de acceso (120):
validar, mediante el dispositivo de acceso (120), que el identificador de cartera está asociado con una entidad confiable antes de seleccionar el applet no confiable de la lista;
proporcionar, mediante el dispositivo de acceso (120), una selección del identificador de applets no confiables de la lista y un identificador de entidad asociado con el dispositivo de acceso (120); y
recibir, por el dispositivo de acceso (120), las credenciales asociadas con el identificador de applets no confiables seleccionado desde la aplicación móvil (112) del dispositivo móvil (110).

9. El método de la reivindicación 8, en donde determinar identificadores de applet compatibles de la lista de applets disponibles comprende:
hacer coincidir, mediante el dispositivo de acceso (120), cada uno de los identificadores de applet en la lista de applets disponibles (113) con una lista de identificadores de applet compatibles almacenados en el dispositivo de acceso (120); y
almacenar, mediante el dispositivo de acceso (120), cada uno de los identificadores de applet coincidentes como uno de los identificadores de applet compatibles en orden de prioridad indicado por el dispositivo móvil (110).

10. El método de cualquiera de las reivindicaciones 8 a 9, en donde la aplicación móvil (112) del dispositivo móvil (110) valida que el dispositivo de acceso (120) está autorizado para acceder a las credenciales asociadas con el identificador de applets no confiables seleccionado utilizando el identificador de entidad.

11. El método de cualquiera de las reivindicaciones 8 a 10, en donde antes de recibir las credenciales asociadas con el identificador de applets no confiables seleccionado, el método comprende además:
proporcionar, mediante el dispositivo de acceso (120), información de configuración del dispositivo de acceso, en donde la aplicación móvil (112) valida que el dispositivo de acceso (120) se configura para soportar transacciones iniciadas utilizando identificadores de applets no confiables basados en la información de configuración del dispositivo de acceso.

12. El método de cualquiera de las reivindicaciones 8 a 11, en donde las credenciales recibidas asociadas con el identificador de applets no confiables seleccionado incluyen un indicador de applet no confiable, en donde el indicador de applet no confiable permite a las entidades identificar las credenciales como asociadas con un applet no confiable.

13. El método de cualquiera de las reivindicaciones 8 a 12, en donde la lista de applets disponibles comprende además un identificador de applets de múltiples entidades, en donde el método comprende además:
determinar, por el dispositivo de acceso (120), que el identificador de applets de entidades múltiples es compatible con el dispositivo de acceso (120);
proporcionar, mediante el dispositivo de acceso (120), una selección del applet de múltiples entidades al dispositivo móvil (110);
proporcionar, mediante el dispositivo de acceso (120), un identificador de entidad asociado con el dispositivo de acceso (120), en donde el applet de entidad múltiple asociado con el identificador de applets de entidad múltiple usa el identificador de entidad para determinar información relevante para la entidad asociada con el dispositivo de acceso (120); y
recibir, por el dispositivo de acceso (120), la información relevante.

14. Un dispositivo de acceso (120), que comprende:
un procesador y
un código de almacenamiento de memoria, que cuando es ejecutado por el procesador, implementa el método de cualquiera de las reivindicaciones 8 a 13.

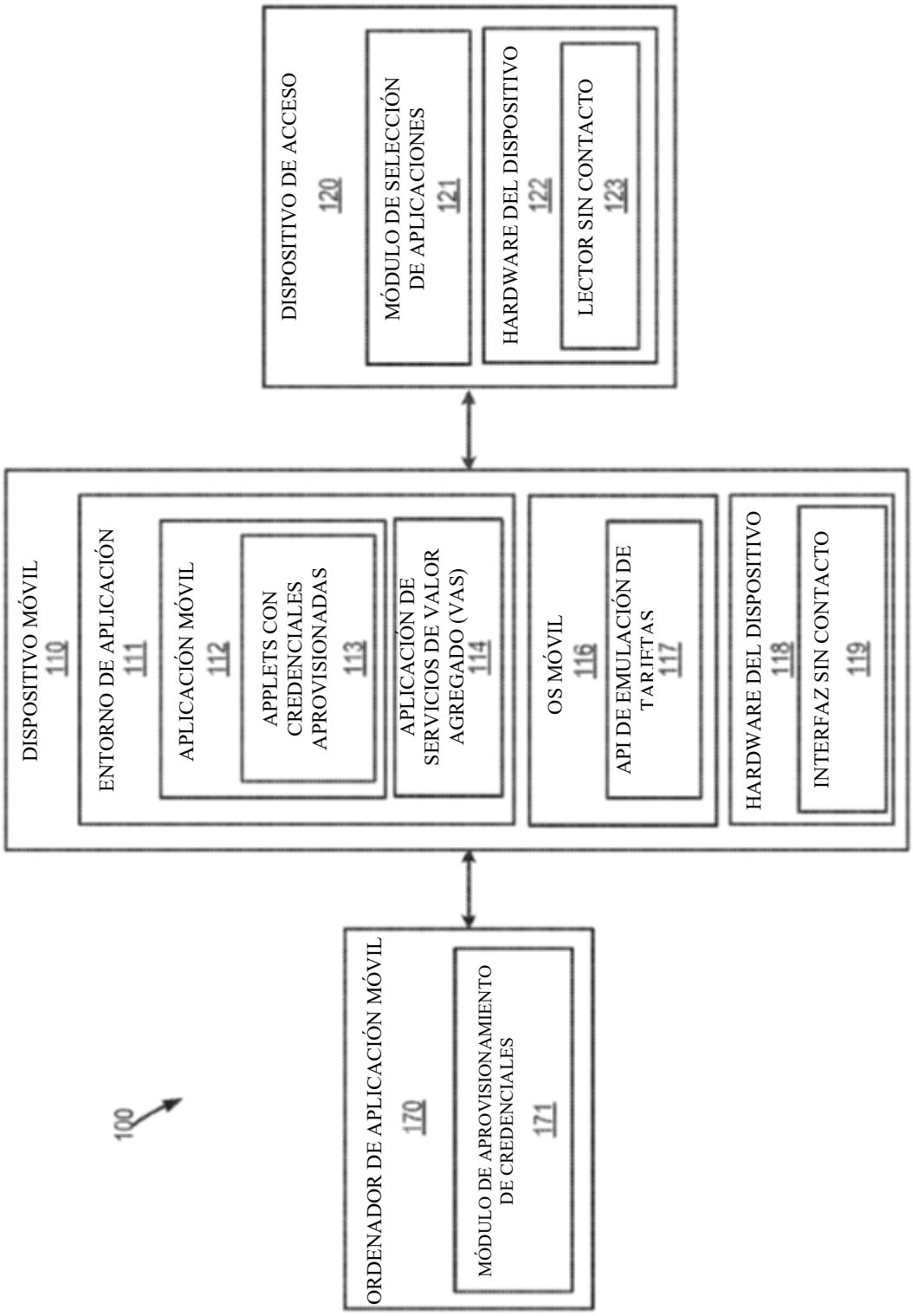
100
ORDENADOR DE APLICACIÓN MÓVIL
170
MÓDULO DE APROVISIONAMIENTO DE CREDENCIALES
171
DISPOSITIVO MÓVIL
110
ENTORNO DE APLICACIÓN
111
APLICACIÓN MÓVIL
112
APPLETS CON CREDENCIALES APROVISIONADAS
113
APLICACIÓN DE SERVICIOS DE VALOR AGREGADO (VAS)
114
OS MÓVIL
116
API DE EMULACIÓN DE TARJETAS
117
HARDWARE DEL DISPOSITIVO
118
INTERFAZ SIN CONTACTO
119
DISPOSITIVO DE ACCESO
120
MÓDULO DE SELECCIÓN DE APLICACIONES
121
HARDWARE DEL DISPOSITIVO
122
LECTOR SIN CONTACTO
123

Figura 1

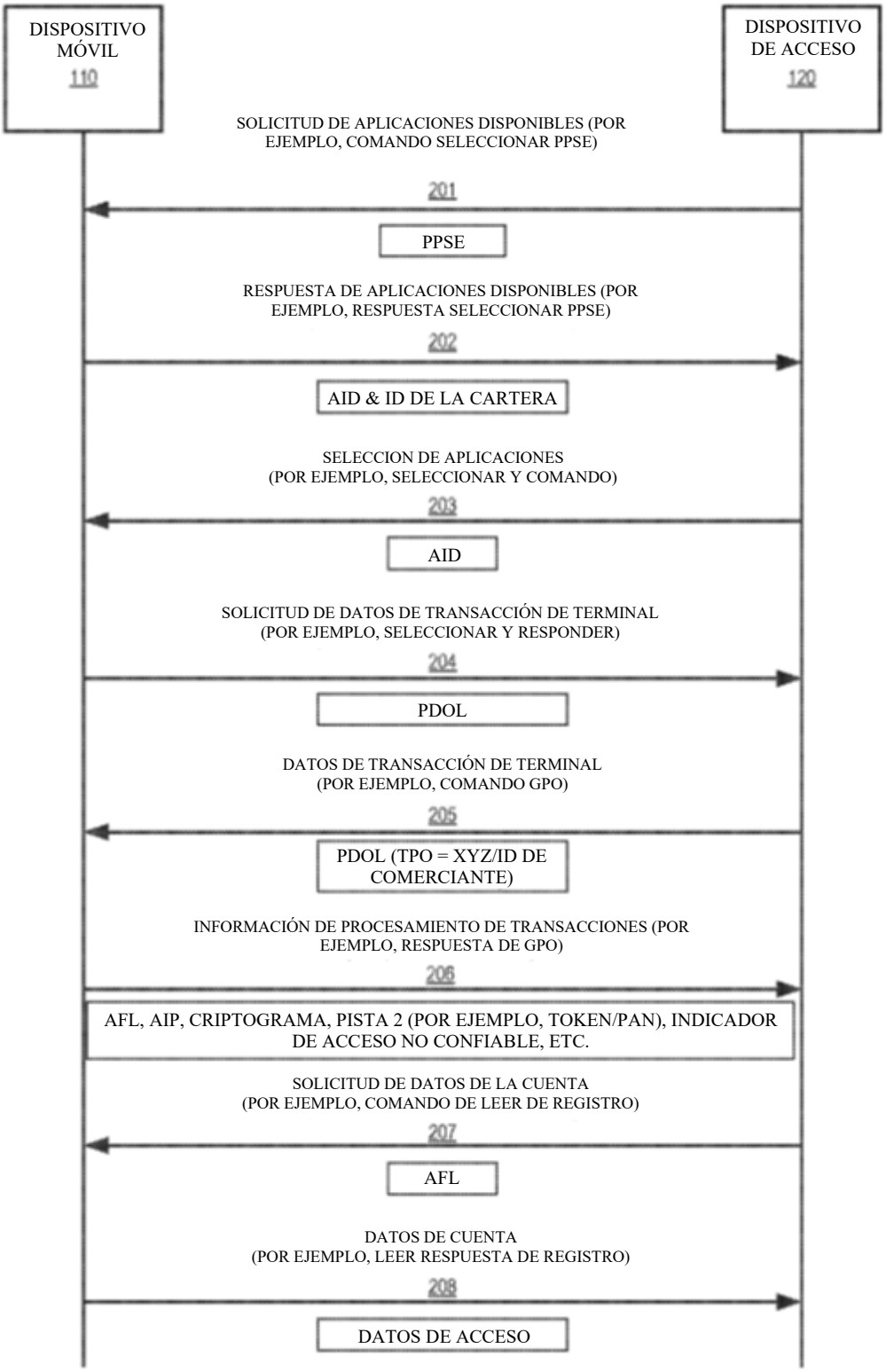
DISPOSITIVO MÓVIL
110
DISPOSITIVO DE ACCESO
120
SOLICITUD DE APLICACIONES DISPONIBLES (POR EJEMPLO, COMANDO SELECCIONAR PPSE)
201
PPSE
RESPUESTA DE APLICACIONES DISPONIBLES (POR EJEMPLO, RESPUESTA SELECCIONAR PPSE)
202
AID & ID DE LA CARTERA
SELECCION DE APLICACIONES (POR EJEMPLO, SELECCIONAR Y COMANDO)
203
AID
SOLICITUD DE DATOS DE TRANSACCIÓN DE TERMINAL (POR EJEMPLO, SELECCIONAR Y RESPONDER)
204
PDOL
DATOS DE TRANSACCIÓN DE TERMINAL (POR EJEMPLO, COMANDO GPO)
205
PDOL (TPO = XYZ/ID DE COMERCIANTE)
INFORMACIÓN DE PROCESAMIENTO DE TRANSACCIONES (POR EJEMPLO, RESPUESTA DE GPO)
206
AFL, AIP, CRIPTOGRAMA, PISTA 2 (POR EJEMPLO, TOKEN/PAN), INDICADOR DE ACCESO NO CONFIABLE, ETC.
SOLICITUD DE DATOS DE LA CUENTA (POR EJEMPLO, COMANDO DE LEER DE REGISTRO)
207
AFL
DATOS DE CUENTA (POR EJEMPLO, LEER RESPUESTA DE REGISTRO)
208
DATOS DE ACCESO

Figura 2

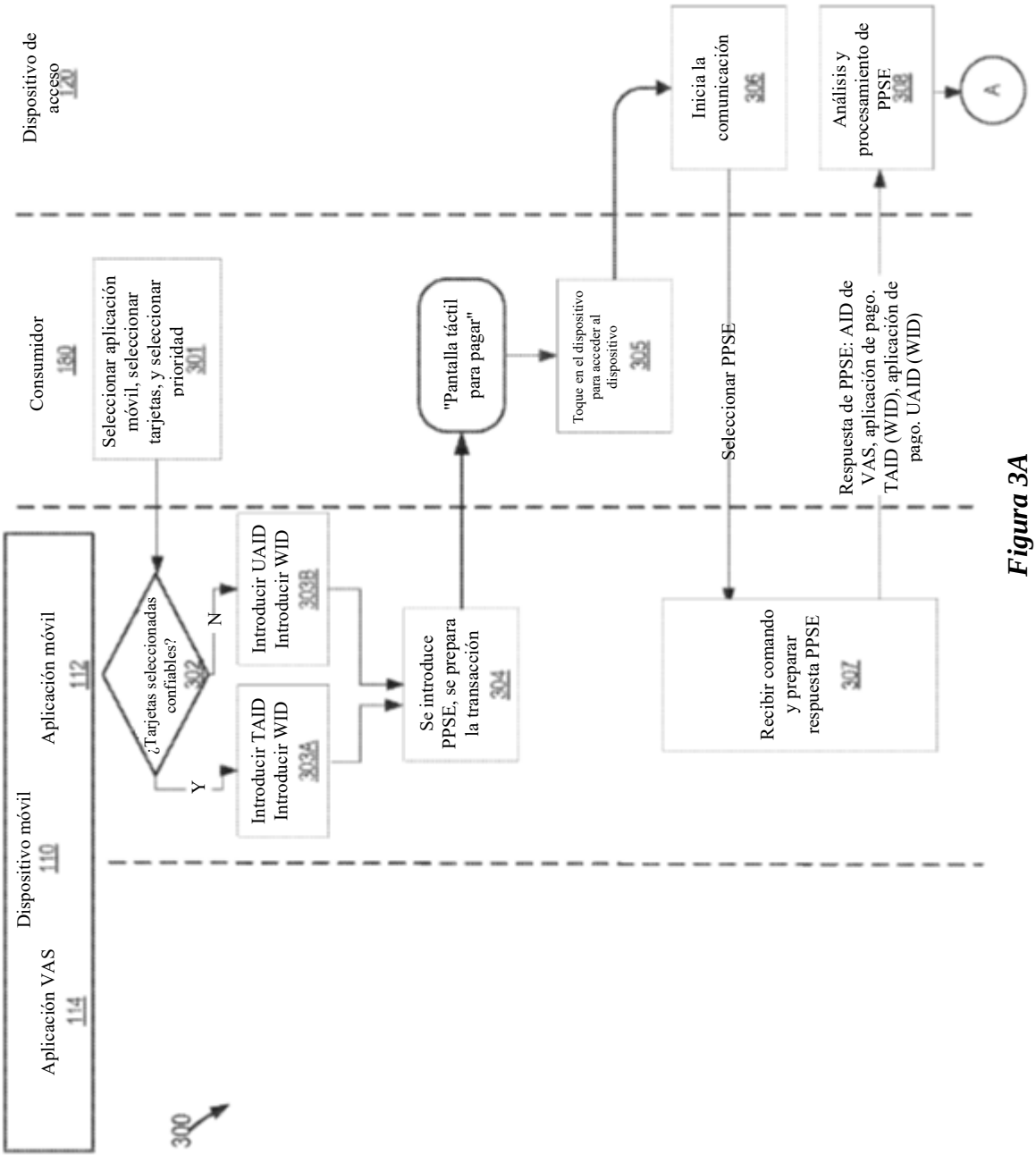
Dispositivo de acceso 120
Consumidor 160
Dispositivo móvil 110
Aplicación VAS 114
Aplicación móvil 112
Seleccionar aplicación móvil, seleccionar tarjetas, y seleccionar prioridad 301
¿Tarjetas seleccionadas confiables? 302
Y
N
Introducir TAID Introducir WID 303A
Introducir UAID Introducir WID 303B
Se introduce PPSE, se prepara la transacción 304
"Pantalla táctil para pagar"
Toque en el dispositivo para acceder al dispositivo 305
Inicia la comunicación 306
Seleccionar PPSE
Recibir comando y preparar respuesta PPSE 307
Respuesta de PPSE: AID de VAS, aplicación de pago. TAID (WID), aplicación de pago. UAID (WID)
Análisis y procesamiento de PPSE 308
A
300

Figura 3A

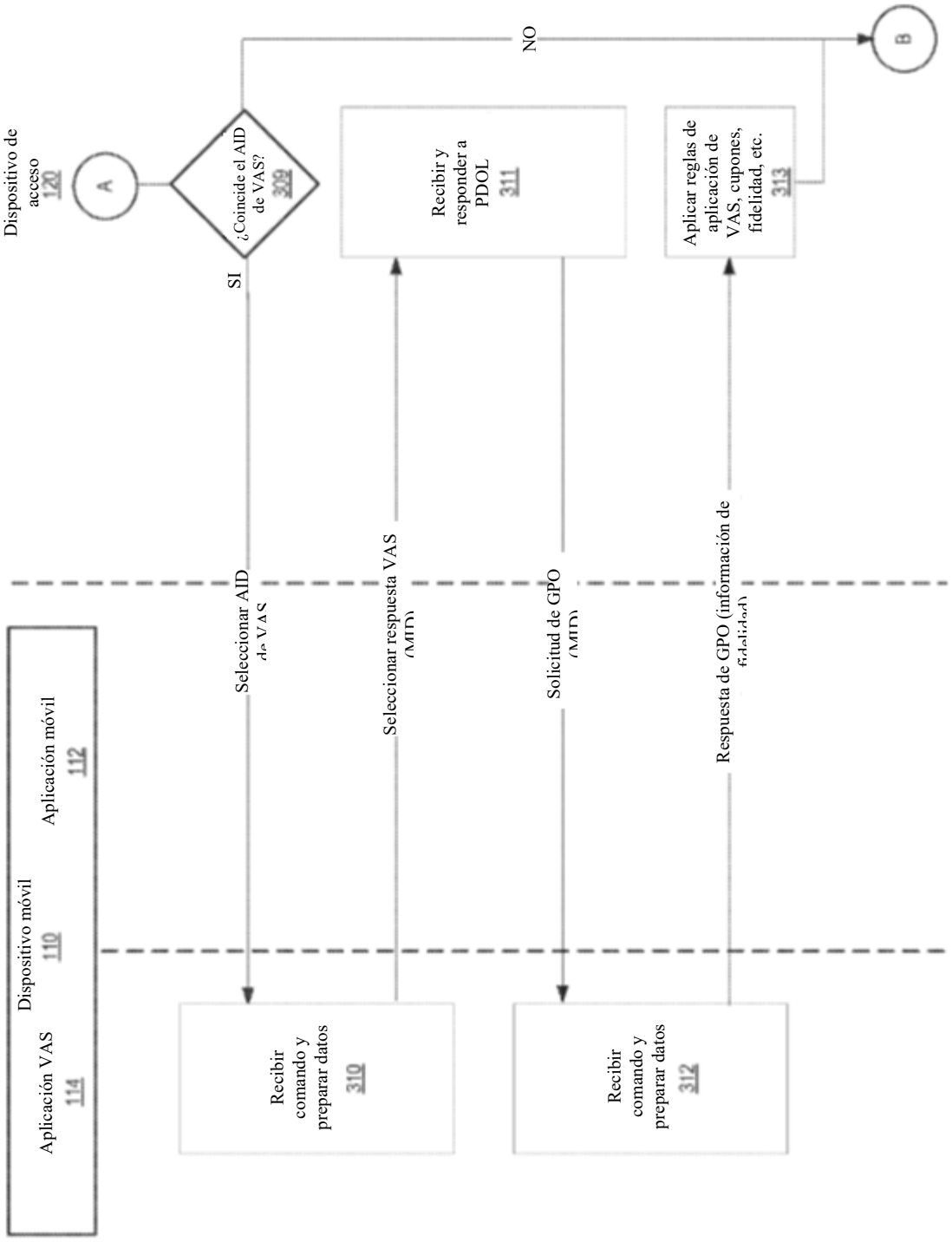
Dispositivo de acceso
120
A
¿Coincide el AID de VAS?
309
NO
B
SI
Recibir y responder a PDOL
311
Aplicar reglas de aplicación de VAS, cupones, fidelidad, etc.
313
Seleccionar AID de VAS
Seleccionar respuesta VAS (MTM)
Solicitud de GPO (MTM)
Respuesta de GPO (información de fidelidad)
Dispositivo móvil
110
Aplicación VAS
114
Aplicación móvil
112
Recibir comando y preparar datos
310
Recibir comando y preparar datos
312

Figura 3B

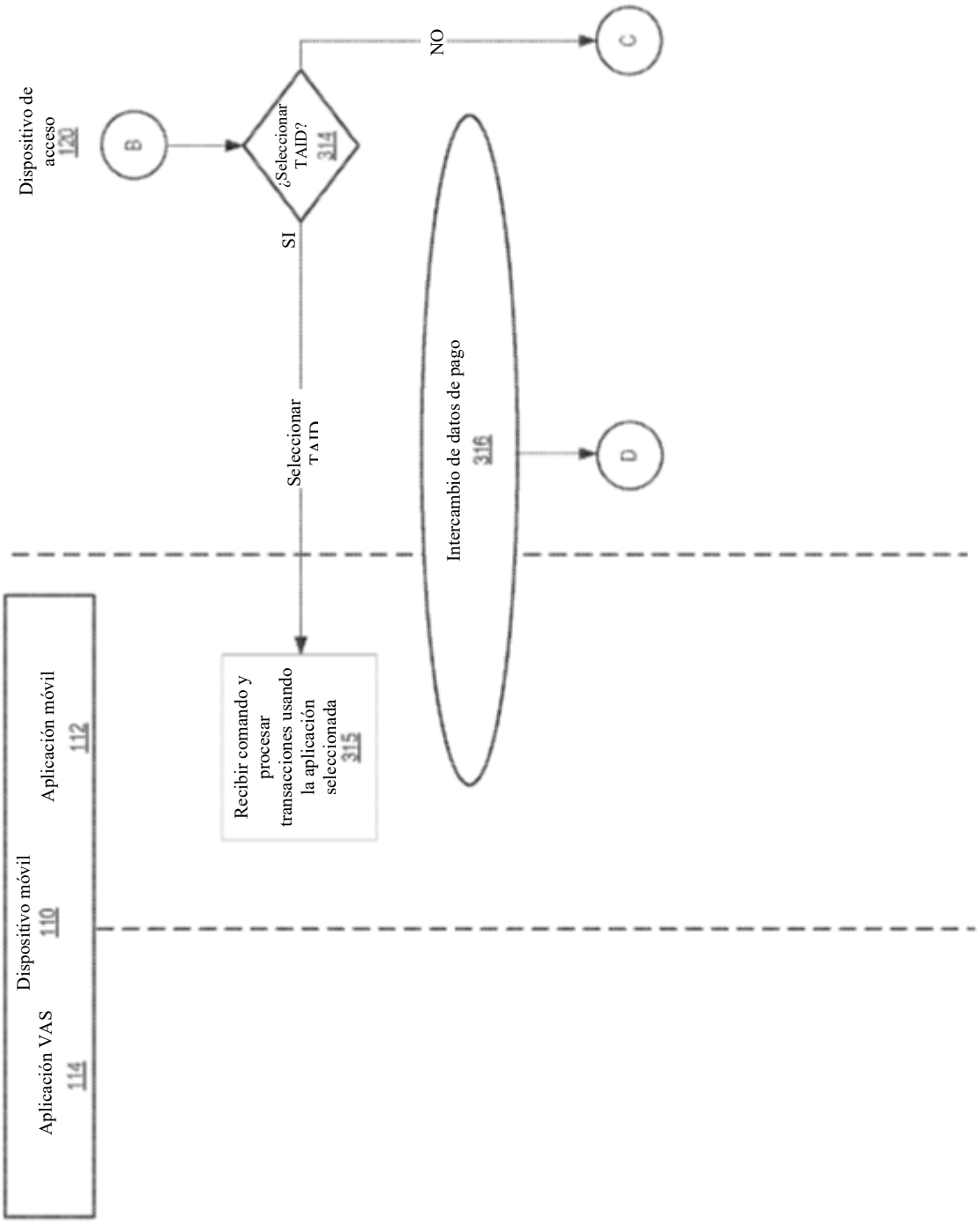
Dispositivo de acceso
120
B
¿Seleccionar TAID?
314
NO
C
SI
Seleccionar TAID
Intercambio de datos de pago
316
D
Recibir comando y procesar transacciones usando la aplicación seleccionada
315
Dispositivo móvil
110
Aplicación VAS
114
Aplicación móvil
112

Figura 3C

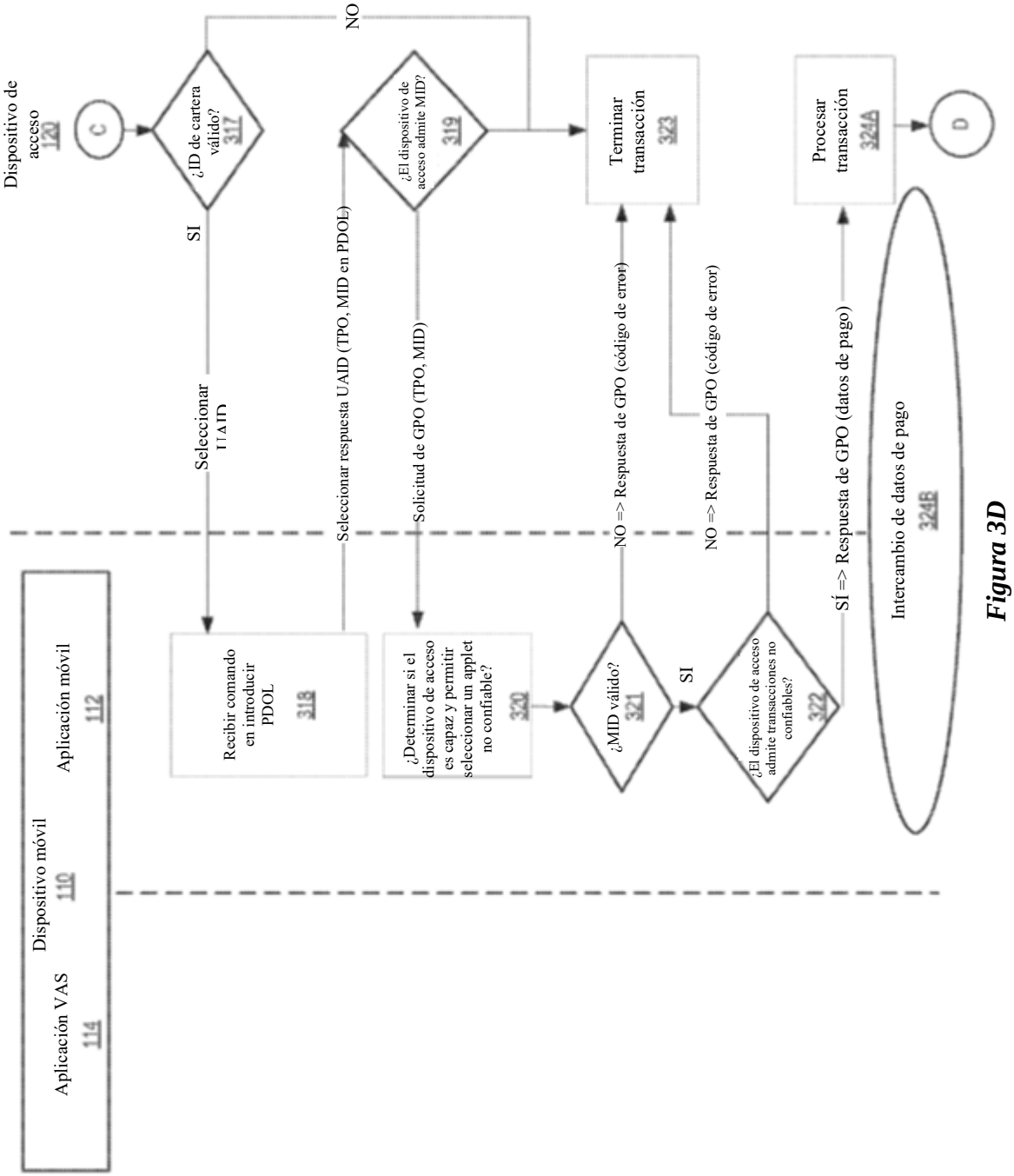
Dispositivo de acceso
120
C
¿ID de cartera válido?
317
NO
SI
Seleccionar UAID
¿El dispositivo de acceso admite MID?
319
Seleccionar respuesta UAID (TPO, MID en PDOL)
Solicitud de GPO (TPO, MID)
Terminar transacción
323
Procesar transacción
324A
D
Dispositivo móvil
110
Aplicación VAS
114
Aplicación móvil
112
Recibir comando en introducir PDOL
318
¿Determinar si el dispositivo de acceso es capaz y permitir seleccionar un applet no confiable?
320
¿MID válido?
321
NO => Respuesta de GPO (código de error)
SI
¿El dispositivo de acceso admite transacciones no confiables?
322
NO => Respuesta de GPO (código de error)
SÍ => Respuesta de GPO (datos de pago)
Intercambio de datos de pago
324B

Figura 3D

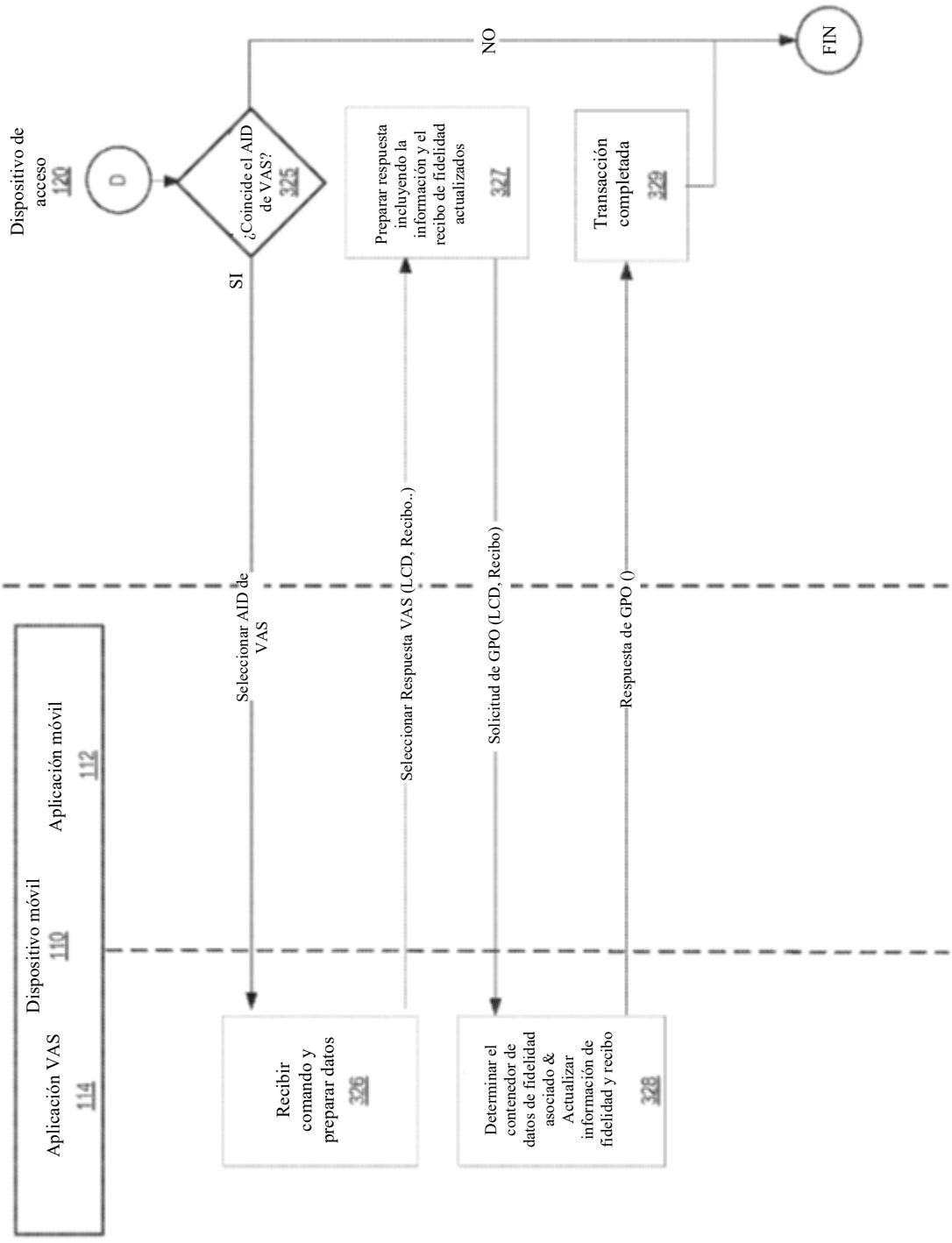
Dispositivo de acceso
120
D
¿Coincide el AID de VAS?
325
NO
FIN
SI
Preparar respuesta incluyendo la información y el recibo de fidelidad actualizados
327
Transacción completada
329
Dispositivo móvil
110
Aplicación VAS
114
Aplicación móvil
112
Seleccionar AID de VAS
Seleccionar Respuesta VAS (LCD, Recibo..)
Solicitud de GPO (LCD, Recibo)
Respuesta de GPO ()
Recibir comando y preparar datos
326
Determinar el contenedor de datos de fidelidad asociado & Actualizar información de fidelidad y recibo
328

Figura 3E

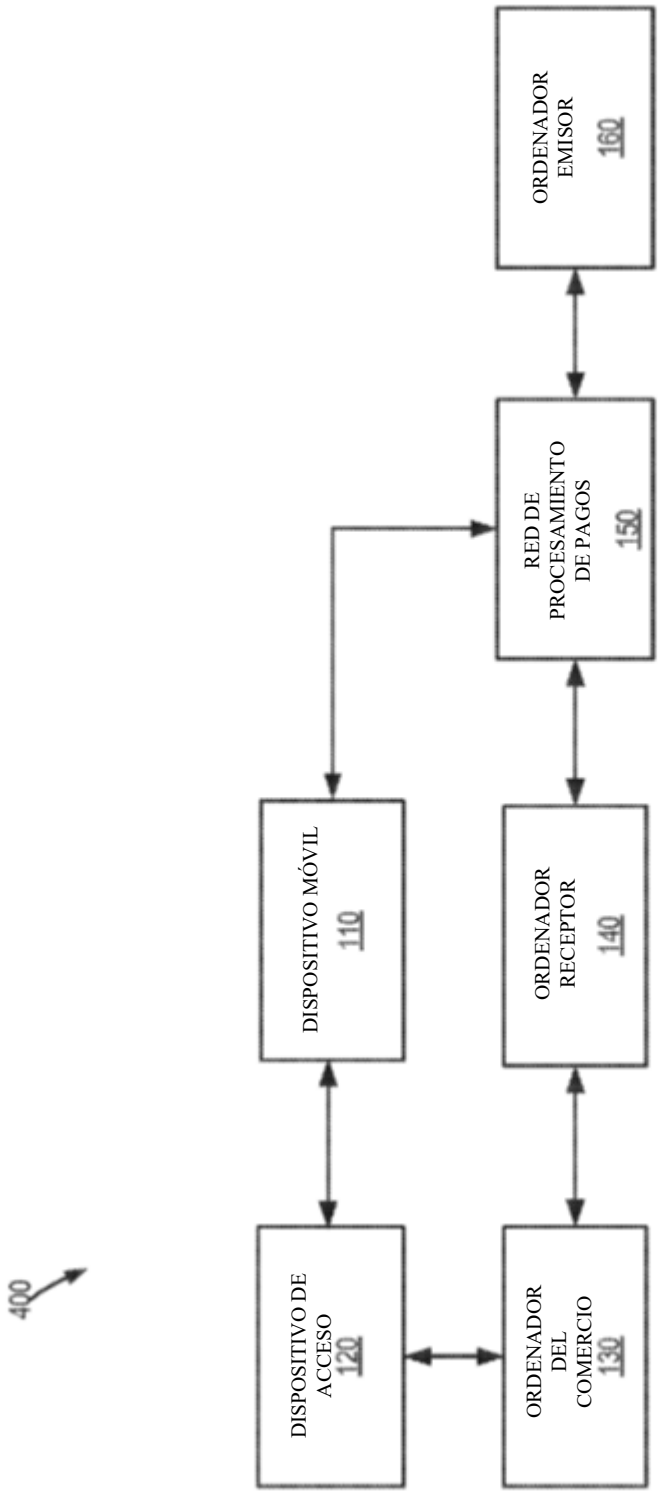
400
DISPOSITIVO DE ACCESO 120
DISPOSITIVO MÓVIL 110
ORDENADOR DEL COMERCIO 130
ORDENADOR RECEPTOR 140
RED DE PROCESAMIENTO DE PAGOS 150
ORDENADOR EMISOR 160

Figura 4

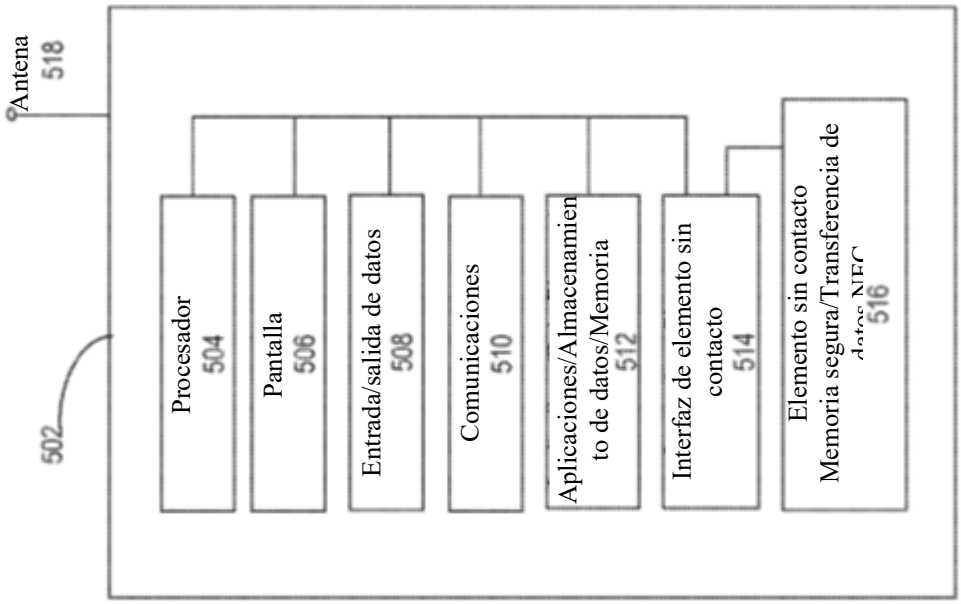

Figura 5

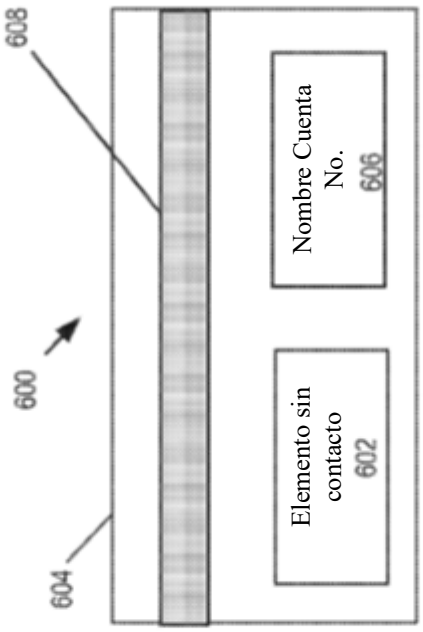

Figura 6

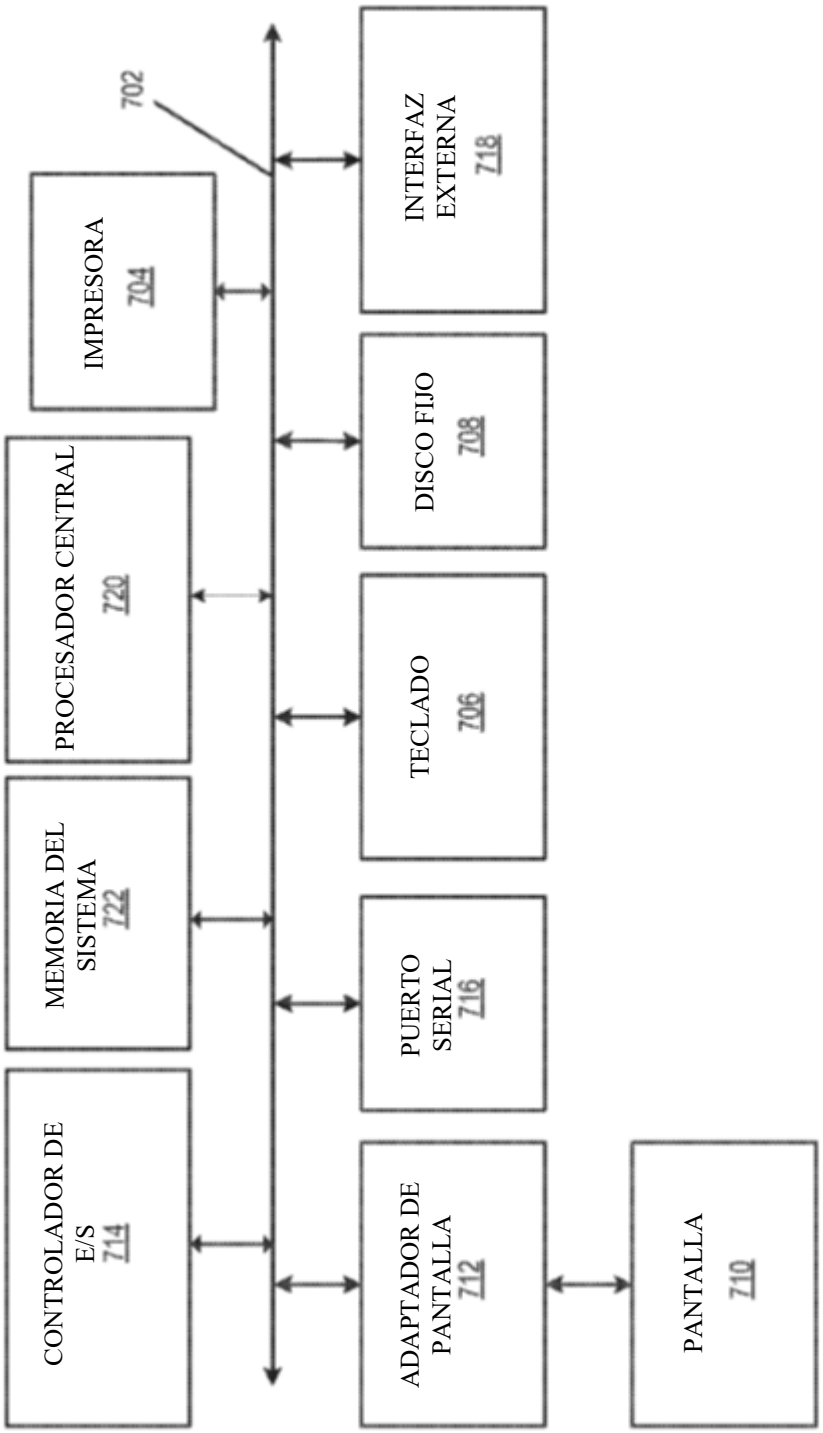
702
INTERFAZ EXTERNA 718
IMPRESORA 704
DISCO FIJO 708
PROCESADOR CENTRAL 720
TECLADO 706
MEMORIA DEL SISTEMA 722
PUERTO SERIAL 716
CONTROLADOR DE E/S 714
ADAPTADOR DE PANTALLA 712
PANTALLA 710

Figura 7