(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 965 224**

(51) Int. Cl.:

H04B 5/00 (2006.01)
G06Q 20/32 (2012.01)
G06Q 20/40 (2012.01)
H04W 12/08 (2011.01)
H04W 12/06 (2011.01)
H04W 4/08 (2009.01)
G06Q 20/20 (2012.01)
G06Q 20/38 (2012.01)
H04L 9/40 (2012.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **29.10.2012 PCT/US2012/062443**

(87) Fecha y número de publicación internacional: **02.05.2013 WO13063583**

(96) Fecha de presentación y número de la solicitud europea: **29.10.2012 E 12843130 (1)**

(97) Fecha y número de publicación de la concesión europea: **29.11.2023 EP 2771978**

(54) Título: **Sistema y método para la presentación de múltiples credenciales NFC durante una única transacción NFC**

(30) Prioridad:

28.10.2011 US 201113284863

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
11.04.2024

(73) Titular/es:

TIS INC. (100.0%)
17-1, Nishishinjuku 8-chome, Shinjuku-ku
Tokyo 1600023, JP

(72) Inventor/es:

REISGIES, HANS;
BRUDNICKI, DAVID y
WEINSTEIN, ANDREW

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Sistema y método para la presentación de múltiples credenciales NFC durante una única transacción NFC

CAMPO TÉCNICO

La presente invención se refiere en general al uso de datos seguros para completar una transacción inalámbrica, y más particularmente a un sistema y procedimiento para la presentación de múltiples credenciales NFC durante una única transacción NFC.

ANTECEDENTES

Las transacciones inalámbricas con tarjetas de proximidad basadas en RFID son bastante habituales. Por ejemplo, muchos trabajadores utilizan tarjetas llave RFID para acceder a su lugar de trabajo y los conductores utilizan pases RFID para pagar los peajes en las autopistas. La RFID, cuya sigla significa identificación por radiofrecuencia, utiliza ondas electromagnéticas para intercambiar datos entre un terminal y algún objeto con fines de identificación. Más recientemente, las empresas han intentado utilizar la RFID con el apoyo de teléfonos móviles para implantar un producto de pago electrónico (es decir, una tarjeta de crédito y/o débito). Sin embargo, la tecnología RFID básica plantea una serie de problemas de seguridad que han impulsado modificaciones de la tecnología básica. Aun así, la adopción generalizada de la RFID como mecanismo de pagos electrónicos ha sido lenta.

La comunicación de campo cercano (NFC) es otra tecnología que utiliza ondas electromagnéticas para intercambiar datos. Las ondas NFC sólo se transmiten a corta distancia (del orden de unos pocos centímetros) y a altas frecuencias. Los dispositivos NFC ya se utilizan para realizar pagos en los puntos de venta. La NFC es una norma abierta (véase, por ejemplo, ISO/IEC 18092) que especifica esquemas de modulación, codificación, velocidades de transferencia e interfaz de radiofrecuencia. La adopción de la NFC como plataforma de comunicación se ha generalizado porque ofrece mayor seguridad para las transacciones financieras y el control de accesos. Otros protocolos de comunicación a corta distancia son conocidos y pueden ganar aceptación para su uso en el apoyo a las transacciones financieras y el control de acceso.

Independientemente del protocolo de comunicación inalámbrica seleccionado, es inevitable que se produzcan errores de funcionamiento tanto en los dispositivos en los que se implementa el protocolo (denominados "monederos inalámbricos" en la presente memoria descriptiva) como en las comunicaciones entre el monedero inalámbrico y los dispositivos anfitriones locales (por ejemplo, terminales de punto de venta, terminales de control de acceso con tarjeta), en los dispositivos anfitriones locales; en cualquier equipo del lado del servidor que deba interactuar con los dispositivos anfitriones locales (por ejemplo, para una confirmación o aprobación); y en las comunicaciones entre el monedero inalámbrico, su red móvil y más allá. Por ejemplo, un consumidor puede tener problemas para completar una compra utilizando la "tarjeta de crédito" integrada en su teléfono inteligente en una gran superficie en el punto de venta debido a uno o más problemas con (1) la conexión NFC entre el teléfono del consumidor y el POS (punto de venta); (2) los datos seguros están corruptos en el teléfono inteligente del consumidor; (3) la cuenta de monedero electrónico del consumidor ha sido desactivada por el emisor de la tarjeta; (4) el dispositivo POS tiene un software de comunicación NFC obsoleto; etc.

El problema es que actualmente no hay ninguna empresa que se encargue de coordinar la resolución de los problemas que plantean las transacciones fallidas con monedero electrónico. De este modo, a nuestro consumidor puede resultarle difícil determinar cuál de los problemas potenciales mencionados, si es que existe alguno, está impidiendo la transacción con monedero electrónico deseada. Por consiguiente, nuestro consumidor puede dejar de utilizar el monedero electrónico o puede no ser capaz de completar una transacción con ese minorista en particular, lo que lleva al consumidor a tratar de consumar una transacción similar con alguien de la competencia.

Uno de los problemas que pueden impedir que se complete con éxito una transacción se debe a la miríada de protocolos de comunicación asociados a los distintos terminales de punto de venta disponibles. Así, por ejemplo, el protocolo necesario para comunicarse con éxito de forma inalámbrica con un terminal de punto de venta IBM puede ser muy diferente del protocolo necesario para comunicarse con un terminal NCR. En consecuencia, es un objeto de la presente invención proporcionar un sistema y procedimiento para utilizar datos de geolocalización (cuando estén disponibles) para tratar de predeterminar el probable dispositivo terminal de punto de venta presente en el establecimiento minorista colocado con el dispositivo de comunicación portátil.

El documento US 2011/0244796 descripción un sistema para realizar múltiples transacciones a través de un único toque NFC.

En consecuencia, la presente invención pretende proporcionar una o más soluciones a los problemas anteriores y problemas relacionados, como lo entenderían aquellos con un conocimiento ordinario de la materia que accedan a la presente memoria descriptiva. Estos y otros objetos y ventajas de la presente descripción resultarán evidentes para aquellos con conocimientos ordinarios en la materia que tengan ante sí los presentes dibujos, especificaciones y reivindicaciones.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

Para una mejor comprensión de la presente descripción, se describen realizaciones no limitantes y no exhaustivas con referencia a los siguientes dibujos. En los dibujos, los números de referencia similares se refieren a partes similares en todas las figuras, a menos que se especifique lo contrario.

La FIGURA 1 ilustra un agente instalado en el dispositivo de comunicación portátil del usuario final que le pregunta si desea presentar varias credenciales en un punto de venta;
la FIGURA 2 es un diagrama de bloques que ilustra los bloques lógicos dentro de un dispositivo de comunicación portátil que puede ser relevante para el presente sistema; y
la FIGURA 3 es un diagrama de bloques que ilustra la configuración de la técnica anterior de un Entorno de Sistema de Pago por Proximidad (PPSE) en un elemento seguro 120 de un dispositivo de comunicación portátil para uso estándar con un lector heredado,
las FIGURAS 4 a 6 son diagramas de bloques que ilustran diversas configuraciones del Entorno de Sistema de Pago por Proximidad (PPSE) en el elemento seguro 120 del dispositivo de comunicación portátil para su uso en la presente invención.

DESCRIPCIÓN DETALLADA

Ahora, se describirá la presente invención con más detalles, en adelante con la referencia a los dibujos adjuntos que forman una parte de la misma y muestran, a modo de ilustración, realizaciones ejemplares específicas mediante las cuales es posible llevar a la práctica la invención. Esta invención puede realizarse de muchas formas diferentes y esto no debe considerarse como limitante para las realizaciones establecidas en esta invención. Entre otras cosas, la presente invención puede materializarse como un sistema.

En consecuencia, la presente invención puede adoptar la forma de una realización totalmente de hardware, una realización totalmente de software o una realización que combine aspectos de software y hardware. Por lo tanto, la siguiente descripción detallada no debe tomarse en sentido limitante.

Dispositivos de comunicación portátiles

La presente invención proporciona un dispositivo de comunicación portátil según la reivindicación 1 y un dispositivo de comunicación portátil según la reivindicación 2. Dichos dispositivos de comunicación portátiles 50 incluyen, entre otros, PDA, teléfonos móviles, teléfonos inteligentes, ordenadores portátiles, tabletas y otros dispositivos móviles que incluyen servicios móviles de voz y datos, así como, preferentemente, acceso a aplicaciones que puede descargar el consumidor. Un dispositivo de comunicación portátil de este tipo podría ser un iPhone, un Motorola RAZR o un DROID; sin embargo, la presente invención preferentemente es independiente de la plataforma y del dispositivo. Por ejemplo, la plataforma tecnológica del dispositivo de comunicación portátil puede ser Microsoft Windows Mobile, Microsoft Windows Phone 7, Palm OS, RIM Blackberry OS, Apple OS, Android OS, Symbian, Java o cualquier otra plataforma tecnológica. A efectos de la presente descripción, la presente invención se ha descrito en general según características e interfaces optimizadas para un teléfono inteligente que utiliza una plataforma generalizada, aunque un experto en la materia entendería que todas estas características e interfaces también pueden utilizarse y adaptarse para cualquier otra plataforma y/o dispositivo.

El dispositivo de comunicación portátil 50 incluye uno o más dispositivos de comunicación electromagnética de corta proximidad, como un transceptor NFC, RFID o Bluetooth. Actualmente se prefiere utilizar una banda base NFC que cumpla las normas NFC IP 1 (www.nfcforum.org), que proporciona funciones estándar como el intercambio de datos entre pares, el modo lector-escritor (es decir, la recogida de información de las etiquetas RFID), y la emulación de tarjetas sin contacto (según las normas NFC IP 1 e ISO 14443) cuando se empareja con un elemento seguro 120 en el dispositivo de comunicación portátil 50 y se presenta delante de un "lector de pago sin contacto" (como se representa en la FIGURA 1). Como comprenderán en la técnica quienes tengan ante sí esta memoria descriptiva, sus figuras y reivindicaciones, las normas de NFC IP 1 son simplemente el ejemplo preferido en la actualidad, que podría exportarse, ya sea en su totalidad o en parte, para su uso en asociación con cualquier otra norma de comunicación de proximidad. Se prefiere además que el dispositivo de comunicación portátil incluya una antena NFC/RFID (conforme a las normas de NFC IP 1 e ISO 14443) para permitir las comunicaciones de campo cercano. Sin embargo, como se entiende en la técnica, las comunicaciones NFC/RFID pueden llevarse a cabo aunque a distancias aún más cortas y con posibles problemas de lectura.

El dispositivo de comunicación portátil 50 también incluye una interfaz de red móvil para establecer y gestionar comunicaciones inalámbricas con un operador de red móvil. La interfaz de red móvil utiliza uno o varios protocolos y tecnologías de comunicación, incluidos, entre otros, el sistema mundial de comunicaciones móviles (GSM), 3G, 4G, el acceso múltiple por división de código (CDMA), el acceso múltiple por división de tiempo (TDMA), el protocolo de datagramas de usuario (UDP), el protocolo de control de transmisión/protocolo de Internet (TCP/IP), SMS, el servicio general de radio por paquetes (GPRS), WAP, la banda ultraancha (UWB), IEEE 802.16 Worldwide Interoperability for Microwave Access (WiMax), SIP/RTP o cualquier otro protocolo de comunicación inalámbrica para comunicarse con la red móvil de un operador de red móvil. En consecuencia, la interfaz de red móvil puede incluir como un transceptor, dispositivo transceptor, o tarjeta de interfaz de red (NIC). Se contempla que la interfaz de red móvil y el dispositivo de comunicación electromagnética de proximidad corta podrían compartir un transceptor o dispositivo transceptor, como entenderían en la técnica quienes tuvieran ante sí la presente memoria descriptiva, sus figuras y reivindicaciones.

El dispositivo de comunicación portátil 50 incluye además una interfaz de usuario que proporciona algunos medios para que el consumidor reciba información, así como para introducir información o responder de otro modo a la información recibida. Como se entiende actualmente (sin pretender limitar la presente descripción a lo antedicho), esta interfaz de usuario puede incluir un micrófono, un altavoz de audio, una interfaz háptica, una pantalla gráfica y un teclado, un dispositivo señalador y/o una pantalla táctil. Como podrían entender aquellos con conocimiento en la materia que tengan la presente memoria descriptiva, sus figuras y reivindicaciones ante sí, el dispositivo de comunicación portátil 50 puede incluir además un transceptor de localización que puede determinar las coordenadas físicas del dispositivo en la superficie de la Tierra típicamente en función de su latitud, longitud y altitud. Este transceptor de localización utiliza preferentemente tecnología GPS, por lo que puede denominarse en el presente documento transceptor GPS; no obstante, debe entenderse que el transceptor de localización puede emplear adicionalmente (o alternativamente) otros mecanismos de geoposicionamiento, incluidos, entre otros, triangulación, GPS asistido (AGPS), E- OTD, CI, SAI, ETA, BSS o similares, para determinar la ubicación física del dispositivo de comunicación portátil en la superficie de la Tierra.

El dispositivo de comunicación portátil 50 también incluirá un microprocesador y una memoria masiva. La memoria masiva puede incluir ROM, RAM, así como una o más tarjetas de memoria extraíbles. La memoria masiva proporciona almacenamiento para instrucciones legibles por ordenador y otros datos, incluido un sistema básico de entrada/salida ("BIOS") y un sistema operativo para controlar el funcionamiento del dispositivo de comunicación portátil. El dispositivo de comunicación portátil también incluirá una memoria de identificación del dispositivo dedicada a identificar el dispositivo, como una tarjeta SIM. Como es sabido, las tarjetas SIM contienen un número de serie único del dispositivo (ESN), un número internacional único del usuario móvil (IMSI), información de autenticación y cifrado de seguridad, información temporal relacionada con la red local, una lista de los servicios a los que tiene acceso el usuario y dos contraseñas (un PIN para uso habitual y una PUK para desbloqueo). Como podrían comprender aquellos con conocimiento en la materia que tengan ante sí la presente memoria descriptiva, sus figuras y reivindicaciones, en la memoria de identificación del dispositivo puede mantenerse otra información en función del tipo de dispositivo, su tipo de red primaria, operador de red móvil de origen, etc.

En la presente invención se considera que cada dispositivo de comunicación portátil 50 tiene dos subsistemas: (1) un "subsistema inalámbrico" que permite la comunicación y otras aplicaciones de datos, como es habitual hoy en día entre los usuarios de teléfonos móviles, y (2) el "subsistema transaccional seguro", que también puede denominarse "subsistema de pago". Se contempla que este subsistema transaccional seguro incluya preferentemente un Elemento Seguro, similar (si no idéntico) al descrito como parte de Global Platform 2.1 .X, 2.2, o 2.2.X (www.globalplatform.org). El elemento seguro 120 se ha implementado como una memoria física especializada y separada utilizada para la práctica común de la industria de almacenar datos de seguimiento de tarjetas de pago utilizados con el punto de venta común de la industria; además, otras credenciales seguras que se pueden almacenar en el elemento seguro incluyen credenciales de credenciales de empleo (controles de acceso de la empresa), hotel y otros sistemas de acceso basados en tarjetas y credenciales de tránsito.

Operador de redes móviles

Cada uno de los dispositivos de comunicaciones portátiles está conectado al menos a un operador de red móvil. Por lo general, el operador de red móvil proporciona la infraestructura física que soporta los servicios de comunicación inalámbrica, las aplicaciones de datos y el subsistema transaccional seguro a través de una pluralidad de torres celulares que se comunican con una pluralidad de dispositivos de comunicación portátiles dentro de la celda asociada a cada torre celular. A su vez, las torres celulares pueden estar en comunicación operable con la red lógica del operador de red móvil, POTS e Internet para transmitir las comunicaciones y los datos dentro de la propia red lógica del operador de red móvil, así como a redes externas, incluidas las de otros operadores de red móvil. Por lo general, los operadores de redes móviles admiten uno o varios protocolos y tecnologías de comunicación, como, por ejemplo, el sistema mundial de comunicaciones móviles (GSM), 3G, 4G, el acceso múltiple por división de código (CDMA), el acceso múltiple por división de tiempo (TDMA)1 , el protocolo de datagramas de usuario (UDP) 1 , el protocolo de control de transmisión/protocolo de Internet (TCP/IP), SMS, el servicio general de radio por paquetes (GPRS), WAP, la banda ultraancha (UWB)1 , IEEE 802.16, la interoperabilidad mundial para el acceso por microondas (WiMax)1 , SIP/RTP o cualquier otro protocolo de comunicación inalámbrica para comunicarse con los dispositivos de comunicación portátiles.16 Worldwide Interoperability for Microwave Access (WiMax) 1 SIP/RTP, o cualquier otro protocolo de comunicación inalámbrica para comunicarse con los dispositivos de comunicación portátiles.

Subsistema de comercios minoristas

Lo habitual hoy en día en los comercios es un sistema de pago conectado al protocolo de Internet que permite procesar transacciones de productos de débito, crédito, prepago y regalo de bancos y proveedores de servicios comerciales. Al pasar una tarjeta con banda magnética por el lector magnético de un terminal de punto de venta, los datos de la tarjeta se transfieren al equipo del punto de venta y el banco emisor los utiliza para confirmar los fondos. Estos equipos de punto de venta han empezado a incluir como accesorios lectores de tarjetas sin contacto que permiten presentar los datos de la tarjeta de pago a través de una interfaz de radiofrecuencia, en lugar del lector magnético. Los datos se transfieren al lector a través de la interfaz de radiofrecuencia mediante la norma ISO 14443 y aplicaciones de pago patentadas como PayPass y Paywave1 , que transmiten los datos de la tarjeta sin contacto desde una tarjeta y, en el futuro, un dispositivo móvil que incluya un subsistema de pago.

Un dispositivo de punto de venta de un minorista 75 (véase la FIGURA 1) puede estar conectado a una red mediante una conexión inalámbrica o por cable. Esta red de puntos de venta puede incluir Internet, además de redes de área local (LAN), redes de área amplia (WAN), conexiones directas, como a través de un puerto de bus serie universal (USB), otras formas de medios legibles por ordenador, o cualquier combinación de los mismos. En un conjunto interconectado de redes LAN, incluidas las basadas en arquitecturas y protocolos diferentes, un rúter actúa como enlace entre las LAN, permitiendo el envío de mensajes de una a otra. Además, los enlaces de comunicación dentro de las LAN suelen incluir pares trenzados o cable coaxial, mientras que los enlaces de comunicación entre redes pueden utilizar líneas telefónicas analógicas, líneas digitales dedicadas completas o fraccionadas, incluidas T1, T2, T3 y T4, redes digitales de servicios integrados (RDSI), líneas de abonado digital (DSL), enlaces inalámbricos, incluidos enlaces por satélite, u otros enlaces de comunicación que conocen los expertos en la materia. Además, los ordenadores remotos y otros dispositivos electrónicos relacionados podrían conectarse a distancia a redes LAN o WAN a través de un módem y un enlace telefónico temporal. En esencia, la red del punto de venta puede utilizar cualquier procedimiento de comunicación que permita que la información viaje entre los dispositivos del punto de venta y los proveedores de servicios financieros con el fin de validar, autorizar y, en última instancia, capturar las transacciones financieras en el punto de venta para su pago a través de los mismos proveedores de servicios financieros.

Subsistema de pagos federados

Como se muestra en la FIGURA 2, cada dispositivo de comunicación portátil 50 puede contener una o más aplicaciones de terceros 200 (por ejemplo, seleccionadas por el consumidor), OpenWallet 100, bibliotecas de pago 110, elemento seguro 120, banda base NFC y un subsistema de pago 150 (es decir, el almacenamiento de datos seguro 115 y el elemento seguro 120). OpenWallet 100 es una aplicación informática que permite al consumidor ver todas las credenciales *(* por ejemplo, datos de tarjetas, cupones, controles de acceso y tickets) almacenadas en el dispositivo 50 (preferentemente en el subsistema de pago 150). OpenWallet 100 también rastrearía preferentemente los emisores de todas las credenciales almacenadas en el subsistema de pago 150 del dispositivo de comunicación portátil y determinaría, aplicación por aplicación, si esa aplicación de terceros debería tener permisos para ver, seleccionar y/o cambiar las credenciales almacenadas en el subsistema de pago. De este modo, OpenWallet 100 también impide que aplicaciones no autorizadas accedan a datos almacenados en el subsistema de pago 150, a los que actualmente no tienen permiso de acceso.

Las librerías de pago 110 son utilizadas por OpenWallet 100 para gestionar (y realizar tareas de mantenimiento) el elemento seguro 120, interactuar con el back-end de gestión del sistema, y realizar el aprovisionamiento over-the-air (OTA) a través del transceptor de comunicación de datos (incluyendo su canal SMS), en el dispositivo 50. Se contempla que las comunicaciones de datos OTA se encriptarán de alguna manera y se desplegará una clave de encriptación en el módulo de servicio de tarjeta 420. El subsistema de pago 150 puede utilizarse para almacenar credenciales como datos de tarjetas de pago, cupones, controles de acceso y entradas (por ejemplo, transporte, conciertos). Algunos de estos tipos de pago pueden ser añadidos al subsistema de pago por diferentes aplicaciones 200 para su uso por dichas aplicaciones. De este modo, se puede impedir que otras aplicaciones de terceros (no mostradas) accedan al subsistema de pago 150.

El almacenamiento de datos seguro 115 puede incluirse para proporcionar almacenamiento seguro adicional en el dispositivo de comunicación portátil 50. Se pueden proporcionar varios niveles de seguridad dependiendo de la naturaleza de los datos destinados a ser almacenados en el almacenamiento de datos seguro 115. Por ejemplo, el almacenamiento de datos seguro 115 puede simplemente estar protegido por contraseña a nivel del sistema operativo del dispositivo 50. Como es conocido en estos sistemas operativos, la contraseña puede ser un simple código alfanumérico o hexadecimal que se almacena en algún lugar del dispositivo 50. De manera alternativa, los datos en el almacenamiento seguro de datos 115 están preferentemente encriptados. Sin embargo, lo más probable es que el almacenamiento seguro de datos 115 se configure como un elemento seguro virtual de la manera descrita en la solicitud de patente co-pendiente (propiedad del cesionario de la presente solicitud) titulada "System and Method for Providing A Virtual Secure Element on a Portable Communication Device" depositada el 21 de octubre de 2011.

OpenWallet 100 elimina preferentemente la complejidad que implica el almacenamiento, mantenimiento y uso de credenciales como tarjetas, cupones, billetes, datos de control de acceso de una o múltiples fuentes o emisores en asociación con el subsistema de pago 150. OpenWallet 100 también aplica preferentemente un control de acceso a los datos almacenados en el subsistema de pago 150 y a las funciones permitidas por cada aplicación. En una estrategia, OpenWallet 100 verifica el autor/emisor de cada aplicación de terceros almacenada en el dispositivo de comunicación portátil 50. Esta verificación puede realizarse accediendo a una base de datos de autorización local de aplicaciones permitidas (es decir, de confianza). Con esta estrategia, sólo las aplicaciones que están firmadas con un ID de emisor conocido y el ID de compilación correctamente asociado pueden acceder y/o manipular los datos almacenados en el subsistema de pago 150 y/o el repositorio de metadatos 125 (que almacena, entre otras cosas, los datos de la imagen de la tarjeta y cualquier dato de la tarjeta en relieve).

En otras palabras, cuando una aplicación 200 o interfaz de usuario de monedero 410 necesita interactuar con el subsistema de pago 150, lo hace pasando un identificador digital (como su ID de emisor o ID de aplicación), un token digital (es *decir,* ID de compilación o ID de token secreto), la acción deseada y cualquier argumento asociado necesario para la acción al módulo de servicios de tarjeta 420. El módulo de servicios de tarjeta 420 verifica que el par

identificador digital-token digital coincide con los datos de aplicación de confianza de la tabla de datos seguros y, a continuación, emitiría uno o varios comandos necesarios para ejecutar la acción deseada. Entre las posibles acciones que pueden utilizar las aplicaciones 200 o la interfaz de usuario de monedero 410 se encuentran las asociadas a:

a. la gestión del monedero (por ejemplo, establecer, restablecer o activar los códigos de acceso del monedero; obtener la URL del servidor OTA; aprovisionamiento del registro OTA; establecer el calendario de pagos; aumentar el calendario de pagos; establecer la tarjeta predeterminada; enumerar los emisores, enumerar las credenciales admitidas; establecer la secuencia de visualización de las credenciales; establecer la prioridad de almacenamiento de las credenciales; crear categorías/carpetas; asociar credenciales a categorías; auditoría de memoria; determinar SE para el almacenamiento de credenciales; obtener ofertas; actualizar el estado del monedero);
b. la gestión de credenciales (por ejemplo, añadir credencial; ver detalles de la credencial; eliminar credencial; activar credencial (para canje/pago); desactivar credencial; buscar credenciales; listar capacidad de credencial; establecer credencial por defecto; bloquear/desbloquear credencial; requerir acceso con contraseña; obtener imagen de credencial; establecer contraseña de acceso);
c. la gestión de elementos seguros (SE) (por ejemplo, obtención de credenciales; actualización de credenciales; actualización de metadatos; supresión de credenciales; bloqueo/desbloqueo de monederos; bloqueo/desbloqueo de SE);
d. la personalización (por ejemplo, añadir credencial; eliminar credencial; suspender/anular credencial; notificación de actualización de metadatos del emisor; notificación de actualización de metadatos de la tarjeta).

Las funciones de "OpenWallet" 100 pueden integrarse en un único módulo dedicado que proporcione una interfaz de usuario estrechamente vinculada a los servicios de la tarjeta. En otro aspecto que se ilustra en la FIGURA 4, las capacidades y funcionalidades de OpenWallet 100 pueden estar distribuidas entre una Interfaz de Usuario de Cartera 410 y un Módulo de Servicios de Tarjeta 420. La estrategia distribuida permitiría a las aplicaciones tener acceso directo al Módulo de Servicios de Tarjeta 420 sin tener que utilizar la interfaz de usuario proporcionada por la Interfaz de Usuario de Cartera 410. El módulo de servicios de tarjeta 420 puede estar configurado para rastrear el emisor de todos los datos de tarjeta, cupón, acceso y ticket almacenados en el subsistema de pago 150 del dispositivo de comunicación portátil 50 y determinar, aplicación por aplicación, si una aplicación debe tener permisos para ver, seleccionar, utilizar y/o cambiar datos seguros almacenados en el subsistema de pago. La interfaz de usuario del monedero 410 proporciona una interfaz de usuario a través de la cual un usuario puede registrarse, aprovisionar, acceder y/o utilizar la información almacenada de forma segura en asociación con el módulo de servicios de tarjeta 420 relativa a las credenciales del usuario. Dado que la interfaz de usuario del monedero 410 está separada del módulo de servicios de tarjeta 420, el usuario puede optar por utilizar una de las aplicaciones de terceros 200 para gestionar la información en el módulo de servicios de tarjeta 420. Como se muestra adicionalmente en la FIGURA 2, los metadatos (como logotipos de credenciales (por ejemplo, Amtrak®, MasterCard®, TicketMaster® y Visa®) e imágenes de afinidad (por ejemplo, AA Advantage® y United Mileage Plus®)) pueden almacenarse en la memoria 125 para que las aplicaciones de terceros 200 o la interfaz de usuario de monedero 410 los utilicen para ofrecer una experiencia de usuario más sencilla. Como estos metadatos se pueden compartir entre aplicaciones, se puede minimizar el almacenamiento necesario para implementar una transacción segura.

Cuando el elemento seguro 120 tiene múltiples credenciales, es probable que surja el deseo e incluso la necesidad de presentar una de esas credenciales en una sola transacción. Por ejemplo, un usuario puede querer dividir el coste de una transacción entre dos tarjetas de crédito, una tarjeta de crédito y una de débito, o similares. En otro ejemplo, cuando el elemento seguro también almacena cupones u otras ofertas de descuento, el usuario puede desear utilizar los cupones y luego cargar el saldo restante en una tarjeta de crédito. Como comprenderán quienes tengan ante sí la presente memoria descriptiva, las permutaciones posibles son infinitas.

El elemento seguro 120 suele cumplir las especificaciones EMVCo. Los elementos seguros que siguen las especificaciones EMVCo emplean el Entorno del Sistema de Pago de Proximidad (PPSE), donde el PPSE es un directorio de credenciales disponibles almacenadas actualmente en los elementos seguros. A cada credencial almacenada en un elemento seguro de este tipo se le asigna un identificador de aplicación (AID) (preferentemente registrado por una autoridad de registro ISO/IEC 7816-5), y se almacena en el PPSE. Estos AID se almacenan en orden de prioridad en el PPSE, el primer AID teniendo la prioridad más alta, el segundo AID la siguiente prioridad más baja, y así sucesivamente.

Cuando el dispositivo de comunicación portátil 50 se acerca a un lector sin contacto, el lector examina la primera credencial en el PPSE. Si el lector sin contacto es capaz de leer la primera credencial, lee la credencial y una vez leída con éxito esa credencial generalmente proporciona alguna indicación de éxito perceptible por el usuario (por ejemplo, haciendo sonar un pitido agradable y/o iluminando un LED en la carcasa del lector) y, a continuación, completa la transacción con el proveedor de servicios financieros apropiado (a través de la red conectada al dispositivo de punto de venta 75 del minorista). Si el lector sin contacto no reconoce la primera credencial, lee la siguiente credencial subsiguiente en el PPSE hasta que encuentra una credencial que reconoce. Estos ejemplos pueden ilustrarse con las credenciales representadas en el PPSE 121 de la FIGURA 3. En particular, la FIGURA 3 representa un ejemplo de una PPSE 121 que tiene una primera credencial, a la que por razones de ilustración nos referiremos como una tarjeta de crédito MasterCard con el código A0000000041010, una segunda credencial a la que llamaremos un cupón digital

con el código A0000001234, una tercera credencial a la que llamaremos otro cupón digital con el código A0000005678, una cuarta credencial a la que nos referiremos como una tarjeta de crédito Visa con el código A0000000031010) y una quinta credencial que llamaremos tarjeta de crédito American Express con el código A00000002501. Como comprenderán los expertos en la materia que tengan ante sí la presente memoria descriptiva, dibujos y reivindicaciones, estos códigos son meras ilustraciones de los tipos de códigos que pueden almacenarse en un PPSE/elemento seguro. Además, pueden incluirse menos credenciales o credenciales adicionales en un elemento seguro, en el extremo superior, sujeto a cualquier limitación de tamaño del elemento seguro seleccionado. En el modo de funcionamiento heredado, la disposición de la PPSE que se representa en la FIGURA 3, indicaría que el monedero se configuró para presentar la tarjeta de crédito MasterCard como credencial principal del monedero electrónico (ya que se encuentra en la parte superior del PPSE 121). Tras examinar el PPSE, un lector sin contacto que admita la credencial MasterCard deberá intentar aceptar la credencial de tarjeta MasterCard (es decir, A0000000041010) del dispositivo de comunicación portátil 50. Según las especificaciones EMVCo existentes, una vez completado el intento de aceptar la credencial MasterCard, finalizaría la comunicación entre la tarjeta y el lector. Si el lector no es capaz de leer la credencial MasterCard, a continuación intentará leer la segunda credencial en el PPSE, que ha sido ilustrada con el código A0000001234 y descrita como un cupón digital. Como pocos lectores, si es que algunos han sido programados para aceptar cupones digitales, es probable que el lector no acepte esta credencial y continúe "bajando" por el PPSE 121 leyendo la tercera credencial sin éxito hasta llegar a la cuarta credencial, por ejemplo, A0000000031010, que se ha descrito en la presente memoria descriptiva como una credencial de tarjeta de crédito VISA. En nuestro ejemplo, el lector sería capaz de leer una credencial VISA, por lo que esta cuarta credencial en el PPSE se leería con éxito, con una indicación de éxito dada por el lector, y la comunicación entre el elemento seguro 120 y el lector de tarjetas sin contacto terminaría.

A pesar del ejemplo anterior, en casi todos los cientos de millones de tarjetas inteligentes y dispositivos de comunicación portátiles con monedero que se utilizan hoy en día, sólo hay un conjunto de datos de tarjeta dentro del elemento seguro y, por lo tanto, sólo un AID en el PPSE. En este caso común, un lector sin contacto examina el PPSE, encuentra el único AID y, a continuación, utiliza ese único AID para comunicarse con las credenciales de la tarjeta inteligente. Si el lector no reconoce el único AID, el intento de transacción sin contacto fracasa.

Con una interfaz de usuario y una memoria de mayor tamaño, un elemento seguro en un dispositivo de comunicación portátil podría utilizarse fácilmente para almacenar y gestionar varios conjuntos de credenciales. Por ejemplo, estas credenciales pueden incluir varias tarjetas de crédito, tarjetas de débito y cupones digitales. Se pueden programar nuevos tipos de credenciales en los lectores heredados de la misma forma que se han programado anteriormente las tarjetas de crédito (y débito) en los lectores (y los elementos seguros asociados). Sin embargo, la mera programación de tipos de credenciales adicionales en los lectores no será del todo útil porque los lectores seguirán leyendo únicamente el PPSE de "arriba" a "abajo" hasta que la primera credencial reconocida se lea con éxito y, entonces, finalizarían las comunicaciones entre el elemento seguro y el lector. Y un segundo intento de comunicación posterior entre el dispositivo de comunicación portátil y el lector sólo daría lugar a que el lector leyera la misma credencial desde la parte superior del PPSE 121 por segunda vez.

El presente sistema y procedimiento establece además AID creados de forma única que se definen para ordenar a los lectores de tarjetas heredados que ejecuten funciones avanzadas, como la presentación de credenciales múltiples y la provisión de capacidad de impresión de recibos digitales a través del elemento seguro. Al utilizar los AID para representar instrucciones en lugar de sólo las credenciales que los AID estaban destinados a representar, el PPSE 121 actuaría como una simple interfaz de mensajería entre el elemento seguro 120 y un lector. Cada lector heredado se actualizaría para reconocer los AID de comandos recién creados de la misma manera general en que se actualizan ahora los lectores sin contacto (por ejemplo, un técnico descarga localmente un nuevo archivo en el lector utilizando un dispositivo de memoria USB). Por supuesto, después de la introducción de esta idea a la marca los lectores de tarjetas sin contacto se diseñarán/programarán inicialmente para reconocer el comando AID que se establecerá dentro de la industria de pago sin contacto basado en la presente invención.

Así, a efectos ilustrativos, supongamos que el lector sin contacto de la FIGURA 1 ha sido reprogramado para reconocer los identificadores de comandos, así como los identificadores de diversas credenciales, incluidos, entre otros, cupones y tarjetas de pago. Si un usuario desea enviar su credencial MasterCard y las dos credenciales de cupón digital al lector (estas credenciales ya se han descrito en relación con la FIGURA 3 anterior), el usuario indicaría este deseo al dispositivo 50. En la FIGURA 1, se ilustra una estrategia potencial. Si el usuario selecciona "sí" en la interfaz de usuario a la pregunta sobre la presentación de múltiples credenciales, la interfaz de usuario ofrecería un listado de las credenciales disponibles en el PPSE 121 para que el usuario las seleccione para su presentación en la transacción. Basándose en esas selecciones, las librerías de pago 110 en combinación con el subprograma de gestión en el elemento seguro 120 reorganizarán las credenciales en el PPSE 121 según las selecciones del usuario para facilitar la presentación de dos o más credenciales NFC en una única transacción. La simplicidad de la gestión de memoria en los elementos seguros actuales requiere el uso de una o más posiciones de memoria en el PPSE para intercambiar credenciales de un lado a otro para reordenar el PPSE.

La FIGURA 4 representa una configuración ejemplar de la PPSE 121 para facilitar la presentación de múltiples credenciales en una única transacción NFC. En primer lugar, la FIGURA 4 ilustra la adición de un AID de código inicial y credenciales múltiples predeterminado 700 al PPSE 121. Como su nombre indica, el AID de código inicial 700

indicará a los lectores de tarjetas sin contacto actualizados el inicio de una transmisión de datos de credenciales múltiples. Como se muestra en la FIGURA 4, al AID de código inicial y credenciales múltiples 700 se le podría asignar un código predeterminado A11111111111. Sin embargo, como comprenderán los expertos en la materia que tengan ante sí la presente memoria descriptiva, los dibujos y las reivindicaciones, puede utilizarse cualquier constante predeterminada para este fin, siempre que la constante sea única. Lo más preferente es que el AID 700 no sea el mismo valor que ninguna credencial emitida de manera válida. A la inversa, cualquier constante que se seleccione para el AID de código inicial y credenciales múltiples 700 predeterminado debe reservarse para los fines descritos en esta invención. La FIGURA 4 también muestra que, a la vez, se ha ilustrado un AID de código final y credenciales múltiples predeterminado 750. Como su nombre indica, el AID de código final 750 indicará a los lectores de tarjetas sin contacto actualizados el final de los datos de transmisión de credenciales múltiples. Como se muestra en la FIGURA 4, al AID 750 se le ha dado el valor constante A22222222222. También en este caso, los diseñadores deben preseleccionar el valor para el AID de código final y credenciales múltiples 750 a fin de impedir la duplicación de códigos de credencial asignados y, en última instancia, el AID de código final seleccionado debe reservarse para este uso. Se contempla que los AID de comandos predeterminados podrían resultar dinámicamente alteradas por el elemento seguro de una manera preproducible que también sería conocida por los lectores, con el fin de mejorar la seguridad de la transacción de comandos.

Como en la técnica anterior, el PPSE 121 todavía contiene credenciales. En el ejemplo de la FIGURA 4, porque se presentan entre los códigos de comando A11111111111 y A2222222222222 AID, la credencial MasterCard (terminada en 010), y dos credenciales de cupón digital (terminadas en 234 y 678) se presentarían al lector de tarjetas sin contacto durante la misma transacción NFC. Para ilustrar mejor los puntos relativos a la presentación y reorganización de credenciales dentro del PPSE 121, la Figura 4 muestra dos credenciales NFC más después del AID de código final predeterminado 750 (A2222222222222). Estas dos credenciales no se presentarán a la banda base NFC durante la transacción única porque se cargan en el PPSE 121 después del comando de AID final. Por consiguiente, un lector que soporte el nuevo procedimiento reconocería el indicador AID de código inicial 700 (A11111111111) y entendería que el usuario de este elemento seguro 120 ha indicado que se deben transferir múltiples credenciales al lector en la misma sesión. El lector aceptaría la credencial de la tarjeta MasterCard, la credencial del cupón digital 1234 y la credencial del cupón digital 5678. Al detectar el AID final, el lector dejaría de intentar leer más credenciales y finalizaría la sesión con el elemento seguro.

Tanto este sistema como este procedimiento también son compatibles con lectores antiguos que no han sido reprogramados con AID de comandos. Por ejemplo, con referencia a la ilustración de la FIGURA 4, un lector desactualizado intentaría leer el indicador AID de código inicial 700 A11111111111 porque está en la parte superior del PPSE 121. Por definición, el lector desactualizado no reconocerá esta credencial AID y entonces leerá la siguiente credencial en el PPSE 121, que, en el ejemplo de la FIGURA 4, es la credencial MasterCard (terminada en 010). El lector reconocería la credencial MasterCard y tal como se ilustra en el ejemplo de la FIGURA 3, ejecutaría sobre la misma. Para apoyar aún más esta compatibilidad con versiones anteriores, la interfaz de usuario puede obligar al usuario a enumerar varias credenciales para su presentación según la probabilidad de que un lector reconozca la credencial. Por ejemplo, las credenciales NFC de tarjetas de crédito son conocidas desde hace tiempo en esta técnica, por lo que se verían obligadas a figurar en primer lugar en cualquier selección de credenciales múltiples por parte del usuario.

En la FIGURA 5, se ilustra una estrategia alternativa. Aquí, sólo se utiliza una constante de AID de código inicial. Esta "constante" tiene un dígito final que varía para reflejar el número de credenciales que el lector debe esperar que se presenten durante la transacción única. Como se ilustra, la palabra de inicio predeterminada para varias credenciales se ha modificado ligeramente a fin de indicar que se pretende transferir tres credenciales (por ejemplo, A11111111113). (El subrayado es meramente para enfatizar y en realidad no se produciría en el PPSE). Así, el lector estaría programado para esperar tres credenciales durante la transacción única y, por consiguiente, ejecutará su ciclo de lectura-aceptación tres veces viajando por el PPSE 121. El resultado será que el lector recibirá las credenciales A0000001234 (un cupón digital), A000005678 (otro cupón digital) y A0000000031010 (una credencial de tarjeta Visa) en tres lecturas separadas de la única transacción NFC.

Los dispositivos NFC 50 son fundamentalmente capaces de transferir información del lector al dispositivo. Los ejemplos de este ejemplo de uso incluyen: el envío de recibos digitales de vuelta desde el lector al dispositivo de comunicación portátil 50 al final de la transacción. La FIGURA 6 ilustra un procedimiento para lograr este ejemplo con la adición de otra constante AID predeterminada 770 {A7777777777) que estaría predeterminada para instruir al lector que envíe los datos de nuevo al elemento seguro 120, el cual lee los datos del lector NFC en el dispositivo 50 a través de la banda base NFC.

La descripción y los dibujos precedentes se limitan a explicar e ilustrar la invención, sin que esta última tenga carácter limitante. Si bien la memoria descriptiva se describe en relación con determinadas implementaciones o realizaciones, se exponen muchos detalles con fines ilustrativos. Por consiguiente, lo anterior no hace sino ilustrar los principios de la invención. Las disposiciones descritas son ilustrativas y no restrictivas. Para los expertos en la materia, la invención es susceptible de implementaciones o realizaciones adicionales y algunos de los detalles descritos en esta solicitud pueden variar de manera considerable sin apartarse de los principios básicos de la invención, tal como lo definen las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un dispositivo de comunicación portátil (50) para la presentación de múltiples credenciales NFC a un lector de tarjetas sin contacto a través de una banda base NFC durante una única transacción NFC, donde el dispositivo de comunicación portátil (50) comprende:

- la banda base NFC;
- un elemento seguro (120) conectado de manera operable conectado a la banda base NFC;
- un directorio de Entorno de Sistema de Pago de Proximidad (PPSE) (121) de credenciales disponibles almacenadas en el elemento seguro, donde el orden de las credenciales disponibles en el directorio de PPSE suele indicar la prioridad, donde las credenciales disponibles incluyen un ID de Aplicación (AID) inicial de credenciales múltiples predeterminado;
- bibliotecas de pago (110); y
- un subprograma de gestión, programado para intercambiar las credenciales disponibles una y otra vez entre el directorio de PPSE y una o más ubicaciones de memoria dentro del elemento seguro, a fin de reordenar, en combinación con las librerías de pago (110), las credenciales disponibles en el directorio de PPSE, de modo tal que el directorio de PPSE contiene una pluralidad de credenciales NFC reorganizadas según las selecciones de un usuario después del AID inicial de múltiples credenciales predeterminado, donde la comunicación inalámbrica del AID inicial de credenciales múltiples indica al lector de tarjetas sin contacto el inicio de la transmisión de la pluralidad de credenciales NFC en orden desde el directorio de PPSE para completar la transacción NFC única, y donde el AID inicial de credenciales múltiples predeterminado es una constante que indica un número de credenciales que el lector debe esperar recibir operativamente durante la transacción NFC única.

2. Un dispositivo de comunicación portátil (50) para la presentación de múltiples credenciales NFC a un lector de tarjetas sin contacto a través de una banda base NFC durante una única transacción NFC, donde el dispositivo de comunicación portátil (50) comprende:

- la banda base NFC;
- un elemento seguro (120) conectado de manera operable conectado a la banda base NFC;
- un directorio de Entorno de Sistema de Pago de Proximidad (PPSE) (121) de credenciales disponibles almacenadas en el elemento seguro, donde el orden de las credenciales disponibles en el directorio PPSE suele indicar la prioridad, donde las credenciales disponibles incluyen un ID de Aplicación (AID) inicial de credenciales múltiples predeterminado;
- bibliotecas de pago (110); y

un subprograma de gestión, programado para intercambiar las credenciales disponibles una y otra vez entre el directorio de PPSE y una o más ubicaciones de memoria dentro del elemento seguro, a fin de reordenar, en combinación con las librerías de pago (110), las credenciales disponibles en el directorio de PPSE, de modo tal que el directorio de PPSE contiene una pluralidad de credenciales NFC reorganizadas según las selecciones de un usuario después del AID inicial de múltiples credenciales predeterminado, donde la comunicación inalámbrica del AID inicial de credenciales múltiples indica al lector de tarjetas sin contacto el inicio de la transmisión de la pluralidad de credenciales NFC en orden desde el directorio de PPSE para completar la transacción NFC única, donde las credenciales disponibles además incluyen un ID de aplicación final de múltiples credenciales (AID), el directorio de PPSE conteniendo además el AID final de credenciales múltiples predeterminado después de la pluralidad de credenciales NFC, donde el AID final de credenciales múltiples indica al lector de tarjetas sin contacto que deje de leer más credenciales NFC del directorio de PPSE para la transacción NFC única.

3. El dispositivo de comunicación portátil (50) según la reivindicación 2, donde la ID de aplicación (AID) final de credenciales múltiples predeterminada es una constante.

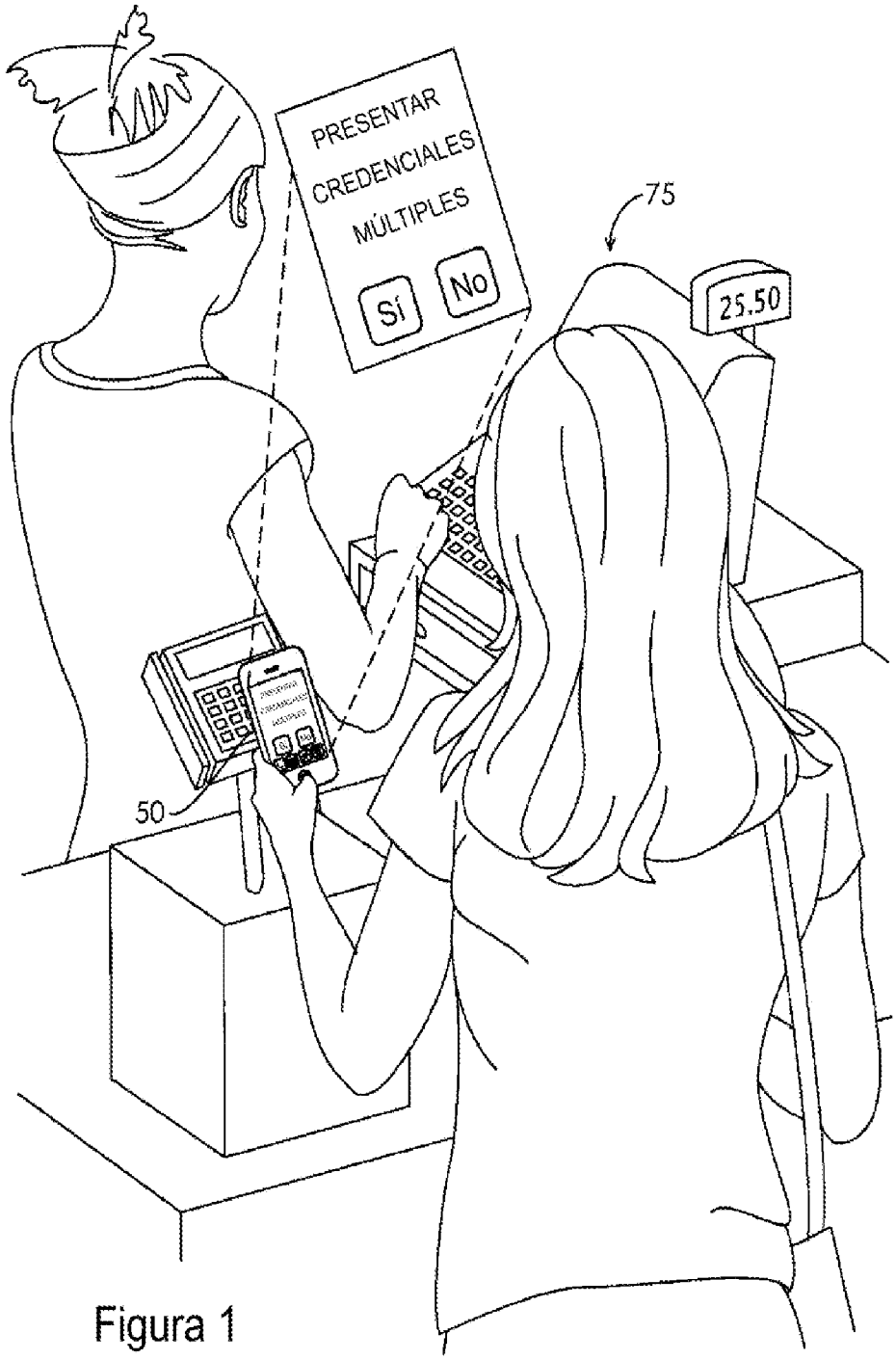

Figura 1

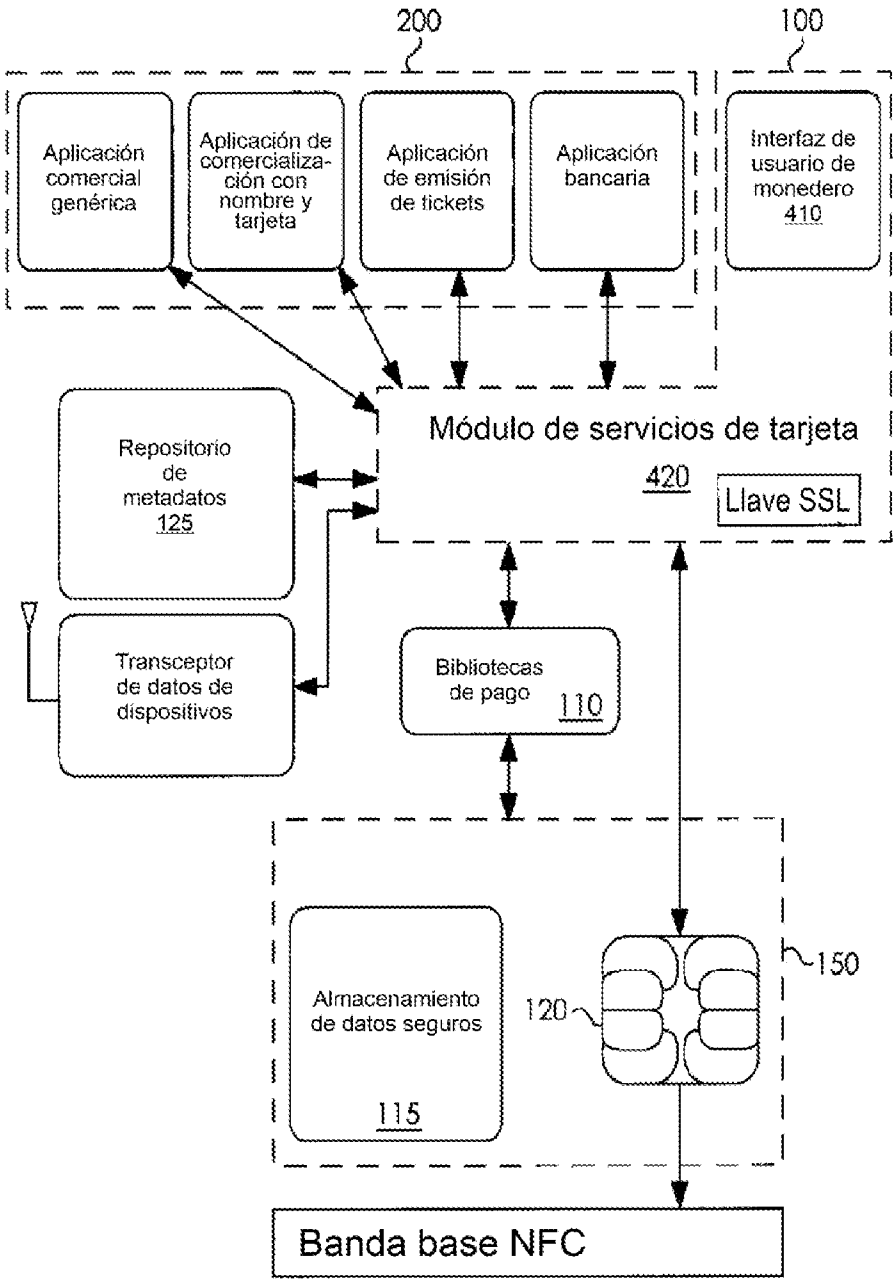
200
100
Aplicación comercial genérica
Aplicación de comercializa-ción con nombre y tarjeta
Aplicación de emisión de tickets
Aplicación bancaria
Interfaz de usuario de monedero 410
Módulo de servicios de tarjeta
420
Llave SSL
Repositorio de metadatos 125
Transceptor de datos de dispositivos
Bibliotecas de pago 110
Almacenamiento de datos seguros 115
120
150
Banda base NFC

Figura 2

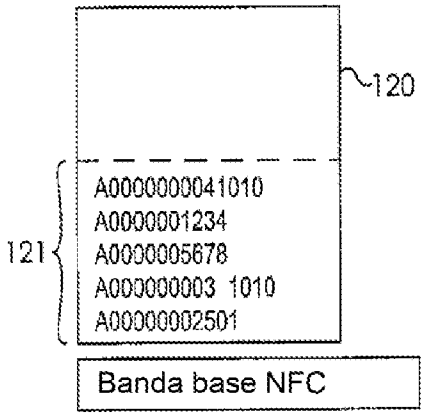

Figura 3

(Técnica anterior)

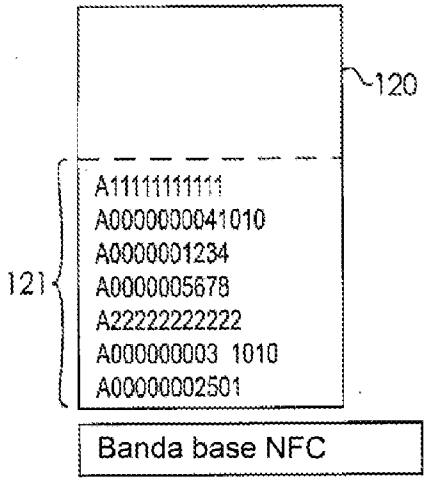

Figura 4

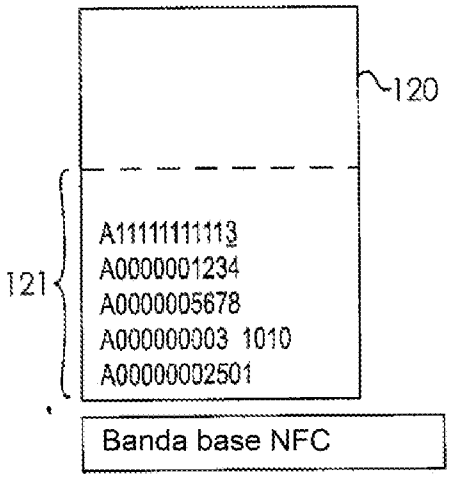

Figura 5

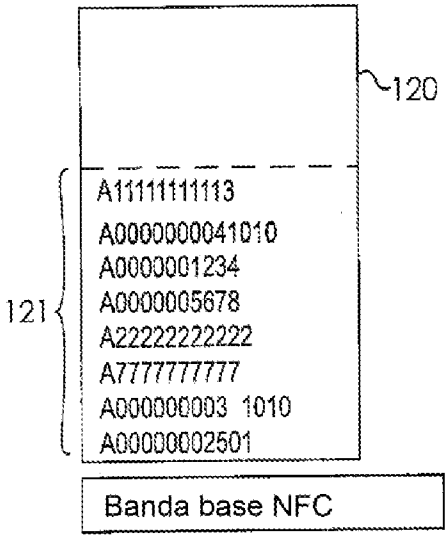

Figura 6