(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 388 695**

(51) Int. CI.:
H04M 1/725 (2006.01)
G06F 1/16 (2006.01)
H04M 1/02 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **08830698 .0**
(96) Fecha de presentación: **12.09.2008**
(97) Número de publicación de la solicitud: **2196010**
(97) Fecha de publicación de la solicitud: **16.06.2010**

(54) Título: **Actualización de dispositivos móviles con elementos adicionales**

(30) Prioridad:
12.09.2007 US 971813 P

(45) Fecha de publicación de la mención BOPI:
17.10.2012

(45) Fecha de la publicación del folleto de la patente:
17.10.2012

(73) Titular/es:
DEVICEFIDELITY, INC.
2201 NORTH CENTRAL EXPRESSWAY SUITE 260
RICHARDSON, TX 75080, US

(72) Inventor/es:
JAIN, Deepak y
DAO, Tuan Quoc

(74) Agente/Representante:
Carvajal y Urquijo, Isabel

DESCRIPCIÓN

Actualización de dispositivos móviles con elementos adicionales

REIVINDICACIÓN DE PRIORIDAD

Esta solicitud reivindica la prioridad de la solicitud de patente de EE. UU. con número de serie 60/971 813, presentada el 12 de septiembre de 2007.

CAMPO TÉCNICO

Esta invención se refiere a dispositivos móviles y, más en particular, a la actualización de dispositivos móviles con elementos adicionales.

ANTECEDENTES

Los dispositivos y testigos electrónicos portátiles se han convertido en parte integrante de la experiencia cotidiana de los usuarios. Existe una amplia variedad de dispositivos portátiles y de bolsillo habituales en poder de los usuarios, que incluyen dispositivos de comunicación, de negocio y de entretenimiento, tales como teléfonos móviles, reproductores de música, cámaras digitales, tarjetas inteligentes, testigos de memoria y diversas combinaciones posibles de los dispositivos y testigos mencionados. Todos estos dispositivos tienen en común que los consumidores están habituados a llevarlos consigo la mayor parte del tiempo y a la mayor parte de los lugares. Esto es cierto para los diversos grupos demográficos y de edad, independientemente del nivel de sofisticación como consumidor, de su grupo de edad, su nivel técnico o su formación.

Estos dispositivos de bolsillo habituales ofrecen opciones de memoria ampliable. Micro Secure Digital (microSD) es la interfaz más popular en todos los teléfonos móviles de alta gama, mientras que las interfaces SD y MultiMediaCard (MMC) están disponibles asimismo en modelos limitados. MicroSD es el mínimo común denominador soportado por la mayor parte de estos dispositivos y testigos (en términos de tamaño). Además, existen adaptadores disponibles para transformar una microSD en MiniSD, SD, MMC y USB. Si bien la mayor parte de los reproductores MP3 (iPOD) presentan una interfaz privada, existen diseños competidores que presentan interfaces estándar. Las cámaras digitales presentan principalmente SD y MMC, siendo otra opción Extreme Digital (xD). Las versiones Micro y Mini de estas interfaces están disponibles asimismo en varios modelos. Mini-USB está cada vez más disponible en teléfonos móviles, cámaras digitales y reproductores MP3 para la sincronización con ordenadores portátiles.

La publicación de patente de EE. UU. número 2006/0291483 describe una pasarela de teléfono móvil y un dispositivo de encaminamiento de comunicaciones (MPG) que está acoplado, a través de un medio eléctrico de transmisión de señalización, con un teléfono móvil operativo en una primera red de comunicación acorde con un primer protocolo de comunicación, para añadir capacidades de comunicación a través de, por lo menos, una segunda red de comunicación acorde con un segundo protocolo de comunicación. Asimismo, se describe un sistema de comunicación móvil. El sistema incluye MPG situado entre el teléfono móvil y la batería y la tarjeta del módulo de identificación de abonado. El MPG se conecta a la interfaz SIM del teléfono móvil, y utilizándola empaqueta las funcionalidades SIM y controla la gestión de llamadas. Éste conecta con la interfaz de datos/señalización del teléfono móvil, y utilizándola comunica con éste, comunicando al mismo tiempo con la segunda red utilizando otros medios de comunicación.

La publicación de patente de EE. UU. 2003/0064689 describe una cubierta intercambiable que está dotada de uno o varios puertos I/O y de electrónica complementaria para añadir dichos uno o varios puertos I/O a un dispositivo móvil, al que es acoplada la cubierta intercambiable. En diversas realizaciones, los puertos I/O pueden comprender un puerto de ratón PS/2, un puerto serie, un puerto paralelo, un puerto bus serie y así sucesivamente. En diversas realizaciones, la electrónica complementaria está empaquetada en un ASIC con pines de salida similares a los de una tarjeta inteligente, que puede incluir un procesador de protocolos equipado apropiadamente para empaquetar y desempaquetar datos que son introducidos/emitidos, de acuerdo con los protocolos I/O seleccionados. En una realización, la cubierta tiene forma de U. En una realización de teléfono móvil inalámbrico, la cubierta está acoplada a una subsección giratoria de una sección pivotante.

La patente de EE. UU. número 6 970 130 B1 da a conocer un aparato de navegación para acoplar con un dispositivo informático portátil de bolsillo y proporcionar capacidades de navegación al mismo. El aparato de navegación incluye un receptor de navegación para recibir señales de navegación procedentes de una serie de fuentes; un procesador acoplado al receptor de navegación para determinar la posición del aparato de navegación en función de las señales de navegación recibidas; y una interfaz/un conector.

RESUMEN

La invención se refiere a una cubierta para un dispositivo móvil de acuerdo con la reivindicación 1. En las reivindicaciones dependientes 2 a 19 se describen realizaciones preferidas.

Los detalles de una o varias realizaciones de la invención se exponen en los dibujos anexos y se describen a continuación. A partir de la descripción y los dibujos, y de las reivindicaciones, resultarán evidentes otras características, objetivos y ventajas de la invención.

DESCRIPCIÓN DE LOS DIBUJOS

La figura 1 es un sistema de actualización a modo de ejemplo, de acuerdo con algunas implementaciones de la presente exposición;

las figuras 2A a 2C muestran vistas en sección transversal, de algunas implementaciones de la cubierta de la figura 1;

las figuras 3A y 3B muestran ejemplos de ranuras en la cubierta de la figura 1;

la figura 4 muestra un ejemplo de módulo convertidor de la cubierta de la figura 1.

la figura 5 es un sistema de transacciones a modo de ejemplo, que transmite información de transacciones;

la figura 6 es un sistema de transacciones a modo de ejemplo, que transmite información de transacciones a través de la red celular;

la figura 7 es un ejemplo de tarjeta de transacciones de la figura 5, de acuerdo con algunas implementaciones de la presente exposición;

la figura 8 es un ejemplo de tarjeta inteligente que conmuta selectivamente una antena;

la figura 9 es otro ejemplo de sistema de transacciones;

la figura 10 es un diagrama esquemático que muestra procesos de personalización de tarjetas inteligentes;

la figura 11 es un diagrama de flujo que muestra un método de ejemplo para inicializar una tarjeta inteligente;

la figura 12 es un flujo de llamada a modo de ejemplo, que muestra sesiones de llamada con una tarjeta inteligente;

la figura 13 es un diagrama de flujo que muestra un ejemplo de método para activar una tarjeta de transacciones;

la figura 14 es un ejemplo de memoria segura de una tarjeta inteligente para almacenar múltiples credenciales de usuario; y

la figura 15 es un diagrama de flujo que muestra un método de ejemplo para la conmutación dinámica entre cuentas de usuario.

En los diversos dibujos, los mismos símbolos de referencia indican elementos iguales.

DESCRIPCIÓN DETALLADA

La figura 1 es un diagrama de bloques que muestra un sistema 100 a modo de ejemplo, para mejorar un dispositivo móvil, por ejemplo un iPhone, con dispositivos externos adicionales, que utiliza una cubierta para el dispositivo móvil. Por ejemplo, el sistema 100 puede añadir una ranura microSecureDigital (microSD) externa a un dispositivo anfitrión móvil, por ejemplo un iPhone, que utiliza una cubierta flexible que encierra por lo menos parte del dispositivo móvil y conecta a una parte del dispositivo móvil. Además de una microSD, el sistema 100 puede añadir un dispositivo externo de memoria a un dispositivo móvil utilizando otras interfaces tales como, por ejemplo, MultiMediaCard (MMC), SD, miniSD, Firewire y/u otros. Al añadir dispositivos externos (por ejemplo, memoria, tarjetas de transacciones), el sistema 100 puede actualizar un dispositivo móvil que no incluye ranuras de expansión, con dispositivos externos adicionales, al mismo tiempo manteniendo sustancialmente las dimensiones del dispositivo. Por ejemplo, la cubierta puede incrementar las dimensiones del dispositivo móvil en un 5 por ciento o menos. En otras palabras, la cubierta puede añadir ranuras de dispositivo para un dispositivo móvil, a la vez que mantiene

sustancialmente los atributos originales tales como las salidas de altavoz, la intensidad de la señal de red, las conexiones Jack de auriculares, la carga de la batería, los puertos de acoplamiento y otros. En algunas implementaciones, el sistema 100 puede actualizar dispositivos móviles con dispositivos de memoria externos, tarjetas de transacción y/u otros dispositivos. Por ejemplo, la tarjeta inteligente puede ejecutar de manera inalámbrica transacciones con diferentes empresas utilizando una sola tarjeta inteligente e independientemente del dispositivo anfitrión móvil. En otras palabras, una sola tarjeta inteligente comprendida en la cubierta puede ejecutar una transacción de pago con una institución financiera, una transacción de control de acceso con una red corporativa, una transacción de compra de billetes con una autoridad de transporte y/o una transacción de validación de identidad con un organismo estatal. En dichas implementaciones, cada una de las transacciones puede identificar de manera segura a un usuario y los privilegios del usuario con respecto a los servicios que son recibidos desde las diferentes empresas. De ese modo, la cubierta que incluye la tarjeta inteligente puede funcionar como una cartera lógica. En algunas de estas implementaciones, la cubierta puede incluir un circuito que transforma señales entre una forma compatible con un dispositivo de memoria externa (por ejemplo, microSD) y una forma compatible con el dispositivo móvil (por ejemplo, USB). Además, el sistema 100 puede incluir una tarjeta inteligente integrada en la cubierta, de tal modo que se evita que una tarjeta extraíble pueda dañar, por lo menos parcialmente, la cubierta.

A alto nivel, el sistema 100 incluye una cubierta 102, un dispositivo externo 104, un dispositivo móvil 106 y una red 108. La cubierta 102 incluye una ranura 110 para la conexión al dispositivo externo 104, un conector 112 para la conexión al dispositivo móvil 106, y un circuito 114 para conectar de manera comunicable la ranura 110, una antena 115 para amplificar la transmisión y recepción de señales de RF y el conector 112. La cubierta 102 puede actualizar el dispositivo móvil 106 con un dispositivo externo 104. Además, la cubierta 102 encierra por lo menos una parte del dispositivo móvil 106. En el caso de encerrar una parte del dispositivo móvil 106, la cubierta 102 puede incluir otras características que exponen puertos del dispositivo móvil 106 para conectar con periféricos externos, de tal modo que la cubierta 102 no interfiere sustancialmente con dichas conexiones. En otras palabras, la cubierta 102 puede incluir puertos sustancialmente alineados con puertos del dispositivo móvil 106, o proporcionar aberturas que permiten un acceso sustancialmente libre a los puertos originales del dispositivo 108 (ver figura 2C). El dispositivo móvil 106 puede estar acoplado de forma comunicable a la red 108. El dispositivo móvil 106 incluye una interfaz gráfica de usuario (GUI, Graphical User Interface) 116 para presentar información y/o recibir información procedente de los usuarios.

La cubierta 102 puede incluir cualquier soporte lógico, equipamiento físico y/o soporte lógico inalterable configurado para actualizar el dispositivo móvil 106 con una o varias ranuras de dispositivos externos. Por ejemplo, la cubierta 102 puede incluir una ranura microSD y una interfaz física para conectar a un puerto del dispositivo móvil. En este ejemplo, la cubierta 102 puede conectar la ranura microSD al dispositivo móvil 106 utilizando la interfaz física. En algunas implementaciones, la cubierta 102 puede incluir uno o varios de los siguientes: una o varias ranuras para dispositivos externos (por ejemplo, memoria, tarjetas de transacción inalámbrica); uno o varios conectores que conectan al dispositivo móvil 106; uno o varios circuitos para conectar dichas una o varias ranuras a dichos uno o varios conectores; un módulo de conversión que transforma señales entre formatos diferentes; un lector biométrico que determina información biométrica de un usuario del dispositivo móvil 106; y/u otros elementos. En algunas implementaciones, la cubierta 102 puede estar formada de un material flexible tal como, por ejemplo, goma de silicona, un neopreno suave y/u otros elementos. La abertura formada por la cubierta 102 puede ser sustancialmente igual o menor que las dimensiones del dispositivo móvil 106. En el caso de que la dimensiones de la abertura sean menores, la cubierta puede ser ligeramente flexible para abarcar el dispositivo móvil 106. La cubierta puede mantener sustancialmente los atributos del dispositivo móvil 106, tales como las dimensiones, la accesibilidad a periféricos proporcionada por el dispositivo, la recarga, la vida útil de la batería, la intensidad de la señal, el acceso a la pantalla y a todos los demás dispositivos de entrada, la conectividad a la red inalámbrica si la hay, la capacidad de interfaz con un PC si lo hay, y cualesquiera otras características proporcionadas por el dispositivo. Manteniendo los atributos, la funcionalidad añadida no puede degradar el funcionamiento del dispositivo de ninguna manera que comprometa la certificación por las autoridades reguladoras (por ejemplo, FCC) y la garantía del emisor del dispositivo 106.

En la implementación ilustrada, la cubierta 102 incluye la ranura 110, el conector 112 y el circuito 114. La ranura 110 puede comprender una ranura MMC, miniMMC, microMMC, SD, miniSD, microSD y/u otras. La ranura 110 puede incluir una abertura, de tal modo que el dispositivo externo 104 pueda ser insertado después de que el dispositivo móvil 106 ha sido insertado en la cubierta 102. En algunas implementaciones, la ranura 110 puede estar formada en la superficie posterior, de tal modo que la cubierta 102 es extraída, o por lo menos desplazada parcialmente de la superficie del dispositivo móvil 106, para insertar el dispositivo externo 104. En algunas implementaciones, la ranura 110 y el dispositivo externo 104 están integrados en la cubierta 102, y en este caso el dispositivo externo 104 puede no ser extraíble sin dañar la cubierta 102. El conector 112 incluye por lo menos una parte que conecta con un puerto del dispositivo móvil 106. El conector 112 puede incluir un conector USB, iDock, microUSB, Firewire, serie y/u otros que presente el dispositivo móvil 106. En algunas implementaciones, el conector 112 puede incluir una primera interfaz para conectar al dispositivo móvil 106 y una segunda interfaz para conectar con dispositivos externos. La segunda interfaz puede ser sustancialmente similar, en dimensiones y capacidades de la interfaz, al conector original del dispositivo móvil 106. En estos casos, el conector 112 puede pasar una o varias señales procedentes de dispositivos externos al dispositivo móvil 106, por ejemplo sin interferir con la conexión al dispositivo externo 104.

Por ejemplo, el conector 112 puede incluir una segunda interfaz que conecta con la fuente de alimentación del dispositivo móvil 106 y pasa la señal de recarga al dispositivo móvil 106. El circuito 114 puede incluir cualquier soporte lógico, equipamiento físico y soporte lógico inalterable para conectar de manera comunicable la ranura 110 con el conector 112. Por ejemplo, el circuito 114 puede incluir una o varias conexiones cableadas entre la ranura 110 y el conector 112. Además, el circuito 114 puede incluir asimismo una antena amplificadora que puede mejorar la capacidad de recepción de señal del dispositivo móvil 106 y/o la capacidad de recepción de señal de cualesquiera tarjetas de transacción inalámbrica insertadas en la ranura 110 (ver figura 2A). En algunas implementaciones, el circuito 114 puede ejecutar una o varias de las acciones siguientes: pasar señales entre la ranura 110 y el conector 112; traducir o transformar de otro modo señales entre formas compatibles con el dispositivo externo 114 y formas compatibles con el dispositivo móvil 106; detectar información biométrica de un usuario del dispositivo móvil 106; gestionar al acceso al dispositivo externo 104 en base, por lo menos en parte, a la información biométrica detectada; mejorar la recepción de señal del dispositivo anfitrión a través de una antena amplificadora integrada; mejorar la recepción de señal de una tarjeta de transacción inalámbrica insertada en la ranura; proporcionar acceso al soporte lógico y al sistema en el dispositivo insertado en la ranura, para una aplicación residente en el dispositivo móvil; y/u otros procesos.

El dispositivo externo 104 puede incluir cualquier soporte lógico, equipamiento físico y/o soporte lógico inalterable configurados para actualizar el dispositivo móvil 106 con una o varias características y/o funciones. Por ejemplo, el dispositivo externo 104 puede incluir memoria de estado sólido (por ejemplo, flash, EEPROM) para almacenar información recibida, por ejemplo, desde el dispositivo móvil 106. El dispositivo externo 104 puede actualizar el dispositivo móvil 106, por ejemplo, con memoria externa, una tarjeta de transacciones inalámbricas, un receptor de radiodifusión, un transceptor de banda ancha y/u otros elementos. En relación con la memoria, el dispositivo externo 104 puede ser un paquete de memoria flash, que es una memoria no volátil que puede ser borrada y reprogramada eléctricamente. El dispositivo externo 104 puede ser una tarjeta de memoria, unidades flash USB y/u otro dispositivo de memoria. Por ejemplo, el dispositivo externo 104 puede incluir memoria de sólo lectura programable y borrable eléctricamente (Electrically Erasable Programmable Read-Only Memory, EEPROM), que es borrada y programada en bloques. En relación con las tarjetas de memoria, el dispositivo externo 104 puede ser una tarjeta de memoria MMC, microMMC, miniMMC, SD, microSD, miniSD, Memory Stick, Memory Stick Duo, xD-Picture Card, Secure Digital de alta capacidad (SDHC, Secure Digital High Capacity) y/u otra tarjeta de memoria. En algunas implementaciones, el dispositivo externo 104 puede incluir una capacidad de memoria entre 1 MB y 1 TB. Alternativa o adicionalmente, el dispositivo externo 104 puede ser una tarjeta de transacciones, tal como la descrita con respecto a las figuras 5 a 14. En estas implementaciones, la tarjeta externa 104 puede ejecutar de manera inalámbrica transacciones, por ejemplo, con un dispositivo de punto de venta. En algunas implementaciones, la tarjeta externa 104 está integrada/incorporada en la cubierta 102. La tarjeta externa 104 puede almacenar credenciales de usuario para una tarjeta de crédito, una tarjeta de débito, una tarjeta de prepago, un cheque regalo, una cuenta corriente y/u otras cuentas de usuario. Además, la tarjeta inteligente puede almacenar asimismo credenciales de usuario para otras aplicaciones, tales como fidelidad (puntos por compra), línea aérea (acceso a clubs, registro), estado (permiso de conducción), membresía (clubs) y/u otros en los que se utilizan las credenciales del usuario para identificar al usuario con objeto de poder proporcionar bienes y/o servicios. Almacenando múltiples credenciales del usuario en una sola tarjeta externa 104, el sistema 100 puede ejecutar transacciones con instituciones diferentes sin requerir múltiples instrumentos, tal como se describe en mayor detalle en relación con las figuras 5 a 14.

El dispositivo móvil 106 comprende un dispositivo electrónico operativo para interactuar con la cubierta 102 utilizando uno o varios puertos. Por ejemplo, el dispositivo móvil 106 puede tener un puerto iDock que conecta con la cubierta 112. Tal como se utiliza en esta exposición, se contempla que el dispositivo móvil 106 abarque teléfonos móviles (por ejemplo, iPhone), teléfonos de datos, dispositivos de radiobúsqueda, ordenadores portátiles, teléfonos SIP, teléfonos inteligentes, asistentes personales de datos (PDA, personal data assistants), cámaras digitales, reproductores MP3, cámaras de video, uno o varios procesadores contenidos en estos u otros dispositivos, o cualesquiera otros dispositivos de procesamiento adecuados capaces de comunicar información con la cubierta 102 a través de uno o varios puertos, y puede tener o no una ranura para que la tarjeta externa 104 pueda ser conectada directamente. Dichos uno o varios puertos pueden incluir, por ejemplo, un puerto USB, un puerto iDock, un puerto Firewire, un puerto serie y/o cualquier otro puerto de interfaz proporcionado por el dispositivo móvil para la conectividad con periféricos, y/u otros puertos. En algunas implementaciones, los dispositivos móviles 106 pueden estar basados en tecnología radioeléctrica celular. Por ejemplo, el dispositivo móvil 106 puede ser una PDA para conectar de manera inalámbrica con una red externa o no segura. En otro ejemplo, el dispositivo móvil 106 puede comprender un reproductor multimedia digital que incluye un dispositivo de entrada, tal como un teclado numérico, una rueda de selección, un selector táctil, una pantalla táctil u otro dispositivo que pueda aceptar información o que permita la selección de elementos de la interfaz de usuario, y un dispositivo de salida que transporte información asociada con el sistema 100, incluyendo datos digitales, información visual, o GUI 116.

La GUI 116 comprende una interfaz gráfica de usuario operativa para permitir al usuario del dispositivo móvil 106 interactuar con, por lo menos, una parte del sistema 100 para cualquier finalidad adecuada, tal como ejecutar transacciones y/o presentar un historial de transacciones. Generalmente, la GUI 116 proporciona al usuario particular una presentación eficiente y amigable de los datos proporcionados por el sistema 100 o comunicados

dentro del mismo, y/o asimismo un medio eficiente y amigable para que el usuario gestione sus propias configuraciones y servicios de acceso ofrecidos por una institución. La GUI 116 puede comprender una serie de cuadros o vistas personalizables que tienen campos interactivos, listas desplegables y/o botones manejados por el usuario. El término interfaz gráfica de usuario puede utilizarse en singular o en plural, para describir una o varias interfaces gráficas de usuario y cada una de las pantallas de una interfaz gráfica de usuario concreta. La GUI 116 puede incluir cualquier interfaz gráfica de usuario tal como un navegador web genérico o una pantalla táctil, que procese información en el sistema 100 y presente los resultados al usuario.

La red 118 facilita la comunicación inalámbrica o cableada entre instituciones y cualquier otro ordenador local o remoto, tal como el dispositivo móvil 106. La red 108 puede ser la totalidad o una parte de una red corporativa o de seguridad. Si bien se ilustra como una sola red, la red 108 puede ser una red continua dividida lógicamente en varias subredes o redes virtuales, sin apartarse del alcance de esta exposición, siempre que por lo menos una parte de la red 108 pueda proporcionar comunicaciones con el dispositivo móvil 106. En algunas implementaciones, la red 108 abarca cualquier red, redes, subred o combinación de las mismas, internas o externas, operativas para facilitar las comunicaciones entre diversos componentes informáticos en el sistema 100. La red 108 puede comunicar, por ejemplo, paquetes de protocolo de internet (IP, Internet Protocol), tramas de Transmisión de Tramas, celdas de modo de transferencia asíncrono (ATM, Asynchronous Transfer Mode), voz, video, datos y cualquier otra información adecuada entre redes. La red 108 puede incluir una o varias redes de área local (LANs, local area networks), redes de acceso radioeléctrico (RANs, radio access networks), redes de área metropolitana (MANs, metropolitan area networks), redes de área extendida (WANs, wide area networks), la totalidad o una parte de la red global de ordenadores conocida como internet, y/o cualquier otro sistema o sistemas de comunicación en una o varias ubicaciones.

Las figuras 2A a 2C muestran vistas en sección transversal de la cubierta 102 de la figura 1. En particular, las vistas muestran los componentes de la cubierta 102 que, como mínimo, mejoran el dispositivo móvil 106 con la tarjeta 104. En la figura 2A, la cubierta 102 incluye un módulo convertidor 202 puerto a tarjeta (por ejemplo, USB a microSD), un lector 204 y una antena 206. El módulo convertidor 202 puede incluir cualquier soporte lógico, equipamiento físico y/o soporte lógico inalterable que transforme entre señales procesables por tarjeta y señales compatibles con el dispositivo móvil 106. En el ejemplo mostrado, el módulo convertidor 202 transforma señales SD y señales USB. El lector 204 puede incluir cualquier soporte lógico, equipamiento físico y/o soporte lógico inalterable que verifique o determine de otro modo información del usuario, tal como información biométrica. En el ejemplo mostrado, el lector 204 determina huellas digitales de un usuario, y puede verificar si el usuario tiene acceso a la tarjeta 104. Además, el lector 204 puede pasar la información biométrica a una aplicación en el dispositivo móvil 106 (a través del convertidor 202 y/o del conector), por ejemplo para verificar de manera segura la identidad del titular del dispositivo. El dispositivo anfitrión móvil 106 puede incluir la verificación de la identidad biométrica para aplicaciones tales como banca móvil. En algunas implementaciones, una aplicación puede utilizar un lector biométrico 204 para registrar en primer lugar la identidad biométrica del usuario en la primera utilización, y a continuación emparejar la identidad biométrica del titular del dispositivo con la identidad biométrica registrada. El almacenamiento seguro de la identidad biométrica para el usuario puede proporcionarse mediante la tarjeta segura extraíble 104, o podría emplazarse en una memoria segura especial incorporada en la cubierta. Por ejemplo, cuando el usuario cambia de dispositivo 106, la huella de identidad puede borrarse del dispositivo inicial (si el usuario extrae la cubierta y la tarjeta 104). Además, otra aplicación que corra sobre la CPU de la cubierta 102 puede utilizar asimismo los datos biométricos para el acceso seguro a ciertas características y/o servicios. La antena 206 puede transmitir y recibir de forma inalámbrica señales de RF asociadas a la tarjeta 104. En las implementaciones de la tarjeta de transacciones, la antena 206 puede extender el rango de transacciones de la tarjeta 104 para transacciones que se ejecutan de forma inalámbrica. La figura 2B es otra ilustración de una vista en sección transversal de la cubierta 102. En esta vista se muestra un conector 208 del dispositivo móvil 106. Por ejemplo, el conector 208 puede ser un conector iDock para un iPhone con 30 pines. La figura 2C es una vista en sección transversal de la cubierta 102. En esta vista, la cubierta 102 incluye las aberturas 214A y 214B para altavoces incluidos con el dispositivo móvil 106 y una cavidad 212 para conectar una fuente de alimentación al conector 112 y al conector 208. En este caso, el dispositivo móvil 106 puede ser cargado utilizando el conector 208 sin extraer la cubierta 102.

Las figuras 3A y 3B muestran diferentes implementaciones de la ranura 110. En la figura 3A, la ranura puede estar formada en la cubierta 102, de tal modo que una tarjeta 104 puede ser insertada y extraída sin levantar o retirar de otro modo una parte, por lo menos, de la cubierta 102. En la figura 3B, la ranura 110 está formada en el interior de la cubierta 102, de tal modo que la cubierta es levantada o retirada de otro modo, por lo menos parcialmente, para insertar y extraer la tarjeta 104.

La figura 4 muestra algunas implementaciones del módulo convertidor 202, que transforma entre señales USB y SD. Tal como se muestra, el módulo convertidor 202 puede recibir una serie de entradas asociadas con la tarjeta 104 y transformar las señales a una forma compatible con el conector 208 del dispositivo móvil 106. En algunas implementaciones, el módulo convertidor 202 puede realizar una conversión, por ejemplo, entre formatos de datos. En algunas implementaciones, el módulo convertidor 202 puede pasar entradas a correspondientes salidas, tal como para VDD y GND.

La figura 5 es un diagrama de bloques que muestra un sistema 500 de transacciones, a modo de ejemplo, para ejecutar de manera inalámbrica transacciones con diferentes empresas utilizando una sola tarjeta inteligente. Por ejemplo, el sistema 500 puede incluir una sola tarjeta microSD que ejecuta transacciones con diferentes empresas (por ejemplo, instituciones financieras) independientemente del dispositivo anfitrión móvil. Por ejemplo, una sola tarjeta microSD puede ejecutar una transacción de pago con una institución financiera, una transacción de control de acceso con una red corporativa, una transacción de compra de billete con una autoridad de transporte y/o una transacción de validación de identidad con un organismo estatal. En dichas implementaciones, cada una de las transacciones puede identificar de manera segura a un usuario y los privilegios del usuario con respecto a los servicios que están siendo recibidos desde las diferentes empresas. Además de una microSD, el sistema 500 puede incluir otras interfaces de almacenamiento masivo que conectan una tarjeta inteligente a un dispositivo anfitrión tal como, por ejemplo, MMC, SD, USB, Firewire y/u otras. Un dispositivo anfitrión puede incluir un teléfono móvil, un teléfono inteligente, una PDA, un dispositivo MP3, una cámara digital, una cámara de video, un cliente, un ordenador y/u otros dispositivos que incluyen, por ejemplo, una interfaz de memoria masiva. En algunas implementaciones, una tarjeta inteligente puede ser una tarjeta que se inserta en un dispositivo anfitrión y ejecuta transacciones independientemente del dispositivo anfitrión. En la ejecución de transacciones, la tarjeta inteligente puede utilizar una interfaz doble que conecta al dispositivo anfitrión a través de una interfaz física (por ejemplo, SD, MMC, USB), y a dispositivos externos a través de la conexión inalámbrica (por ejemplo, NFC, ISO 14 443, Bluetooth). La tarjeta inteligente puede controlar, o en todo caso manejar, uno o varios componentes de equipamiento físico del dispositivo anfitrión móvil (por ejemplo, pantalla, tecnología radioeléctrica celular) utilizando la interfaz física, y comunicar de manera inalámbrica con terminales de acceso utilizando la interfaz inalámbrica. En algunas implementaciones, la tarjeta inteligente incluye una serie de credenciales de usuario con cada conjunto de identidad asociado con una institución diferente. Por ejemplo, la tarjeta inteligente puede almacenar credenciales de usuario para una tarjeta de crédito, una tarjeta de débito, una tarjeta de prepago, un cheque regalo, una cuenta corriente y/u otras cuentas de usuario. Además, la tarjeta inteligente puede almacenar asimismo credenciales del usuario para otras aplicaciones tales como fidelidad (puntos por compra), línea aérea (acceso a clubs, registro), estado (permiso de conducción), membresía (clubs) y/u otros en los que se utilizan las credenciales de usuario para identificar al usuario con objeto de poder proporcionar bienes y/o servicios. Almacenando múltiples credenciales de usuario en una sola tarjeta inteligente, el sistema 500 puede ejecutar transacciones con instituciones diferentes sin requerir múltiples instrumentos. En otras palabras, una sola tarjeta inteligente puede funcionar como una cartera lógica, que almacena localmente información para las diferentes cuentas de usuario y conmuta entre las diferentes cuentas de usuario en respuesta, por lo menos, a un evento. Proporcionando una tarjeta inteligente, el sistema 500 puede ejecutar de forma inalámbrica transacciones con instituciones sin requerir equipamiento físico, soporte lógico y/o soporte lógico inalterable adicionales, y/o sin requerir cambios en el equipamiento físico, el soporte lógico y/o el soporte lógico inalterable existentes, para que los terminales de lectura permitan a un usuario ejecutar de manera inalámbrica una transacción. Además, el sistema 500 puede eliminar, minimizar o sino reducir el número de instrumentos en posesión de un individuo para ejecutar transacciones utilizando diferentes cuentas de usuario. En otras palabras, la tarjeta inteligente puede funcionar como una serie de instrumentos diferentes pero implementados como un sólo dispositivo.

A alto nivel, el sistema 500 incluye una memoria 502 fuera de línea y clientes 504a y 504b acoplados a instituciones 506 a través de una red 108. Aunque no se ilustra, el sistema 500 puede incluir varias partes intermediarias entre la institución 506 y la red tales como, por ejemplo, un adquiriente de transacciones y/o un anfitrión de la red de pagos. La memoria 502 fuera de línea incluye un dispositivo móvil 106a que tiene una tarjeta 104a de transacciones y un dispositivo 514 de punto de venta (POS, Point of Sale) que ejecuta transacciones con los clientes. El punto de acceso 514 incluye una interfaz gráfica de usuario (GUI, Graphical User Interface) 509 para presentar información y/o recibir información procedente de los usuarios. En algunas implementaciones, el punto de acceso 514 puede transmitir a la tarjeta 104 de transacciones una petición de ejecutar una transacción. La tarjeta 104 de transacciones puede transmitir información de la transacción al punto de acceso 514. El cliente 504 incluye la GUI 505 para presentar información asociada con el sistema 500. El cliente 504a incluye un lector 516 de tarjetas que interconecta la tarjeta 104c de transacciones con el cliente 504a. La institución 506 puede autorizar la transacción, por lo menos en parte, en base a información transmitida mediante la tarjeta 104 de transacciones. El dispositivo móvil 106 incluye una GUI 116 para presentar información asociada con transacciones financieras.

Generalmente, la empresa 502 es, como mínimo, una parte de una empresa que tiene una presencia física (por ejemplo, un edificio) para operaciones. Por ejemplo, la empresa 502 puede vender bienes y/o servicios en un emplazamiento físico (por ejemplo, una tienda física) directamente a los clientes. En este ejemplo, la empresa 502 compra, o recibe de otro modo, bienes (por ejemplo, productos) de los distribuidores (no mostrados) y a continuación puede vender estos bienes a los clientes, tales como los usuarios del dispositivo móvil 106. En general, la empresa 502 puede ofrecer encuentros cara a cara con los clientes al proporcionar los bienes y/o servicios. Por ejemplo, la empresa 502 puede ser una tienda física, de tal modo que el usuario selecciona un bien o servicio utilizando la red internet, y compra y recibe el bien o servicio en la empresa 502. La empresa 502 puede proporcionar uno o varios de los servicios siguientes asociados con bienes: inventario, almacenaje, distribución y/o transporte. Por consiguiente, la empresa 502 puede no distribuir inmediatamente bienes recibidos de los distribuidores. La empresa 502 puede incluir un solo establecimiento minorista, uno o varios establecimientos minoristas en un solo emplazamiento geográfico, y/o una serie de establecimientos minoristas distribuidos geográficamente. En algunos casos, dos o más

entidades pueden representar partes de la misma entidad legal o filiales. Por ejemplo, la empresa 502 y los distribuidores pueden ser departamentos comprendidos en una empresa. En resumen, la empresa 502 puede ejecutar de manera inalámbrica transacciones financieras con el dispositivo móvil 106.

La tarjeta 104 de transacciones puede incluir cualquier soporte lógico, equipamiento físico y/o soporte lógico inalterable configurado para ejecutar de manera inalámbrica transacciones con el punto de acceso 514, utilizando una de una serie de cuentas de usuario seleccionables. Por ejemplo, la tarjeta 104 de transacciones puede seleccionar credenciales de usuario asociadas con una de la serie de cuentas de usuario seleccionables (por ejemplo, cuentas financieras) y ejecutar una transacción sin contacto con el punto de acceso 514 utilizando la cuenta seleccionada, e independientemente del dispositivo móvil 106a. En otras palabras, la tarjeta 104 de transacciones puede ejecutar de manera inalámbrica transacciones sin que haya partes de la transacción que sean ejecutadas por el dispositivo móvil 106. Además, la tarjeta 104 de transacciones puede almacenar localmente credenciales de usuario y/o aplicaciones (por ejemplo, aplicaciones de pago, aplicaciones de acceso) para una serie de cuentas de usuario seleccionables. Una tarjeta 104 de transacciones puede conmutar dinámicamente entre credenciales de usuario y aplicaciones de pago, por lo menos en respuesta a un evento. Un evento de conmutación puede incluir una selección procedente de un usuario a través de la GUI 116, la compleción de una transacción, la detección de un tipo de señal, la determinación de un tipo de compra (por ejemplo, comestibles, ropa), un cambio de área geográfica (por ejemplo, GPS) y/u otros eventos. Las diferentes cuentas de usuario pueden incluir una cuenta de tarjeta de crédito (por ejemplo, Visa, MasterCard), una cuenta minorista (por ejemplo, Target, Dillard's), una tarjeta de prepago, un cheque regalo, una tarjeta bancaria (por ejemplo, Banco de América), una tarjeta de líneas aéreas, una tarjeta de identidad, un permiso de conducción y/u otros. En algunas implementaciones, la tarjeta 104 de transacciones puede incluir credenciales de usuario para cualquier combinación de cuentas financieras, minoristas, de líneas aéreas, corporativas, de estado y/u otras. En algunas implementaciones, la tarjeta 104 de transacciones puede almacenar localmente aplicaciones para dicha serie de cuentas de usuario seleccionables. Por ejemplo, la tarjeta 104 de transacciones puede ejecutar una aplicación diferente para cada una de las diferentes credenciales de usuario. Las diferentes aplicaciones pueden ejecutar transacciones utilizando diferentes infraestructuras de lector, formatos, protocolos, cifrado, tipo/estructura de credenciales de usuario intercambiados con el terminal y/u otros aspectos.

La tarjeta 104 de transacciones puede ejecutar transacciones con el punto de acceso 514 utilizando señales de corto alcance, tales como NFC (por ejemplo, ISO 18092/ECMA 340), ISO 14443, ISO 15693, Felica, MiFARE, Bluetooth, banda ultra-ancha (UWB, Ultra-wideband), identificador por radiofrecuencia (RFID, Radio Frequency Identifier), y/u otras señales compatibles con terminales de pago minorista (por ejemplo, punto de acceso 514). En algunas implementaciones, la tarjeta 104 de transacciones puede incluir uno o varios conjuntos de chips que ejecutan un sistema operativo y procesos de seguridad para ejecutar independientemente la transacción. De este modo, el dispositivo móvil 106 no requiere equipamiento físico, soporte lógico y/o soporte lógico inalterable adicionales para ejecutar de manera inalámbrica una transacción con el punto de acceso 514, tal como una transacción NFC. En algunas implementaciones, la tarjeta 104 de transacciones puede ejecutar uno o varios de las siguientes acciones: conmutar dinámicamente entre credenciales de usuario y/o aplicaciones en respuesta, por lo menos, a uno o varios eventos; recibir de manera inalámbrica una petición procedente del punto de acceso 514 para ejecutar una transacción y/o transmitir una respuesta; traducir entre protocolos inalámbricos y protocolos compatibles con la tarjeta 104 de transacciones; traducir entre protocolos de tarjeta de transacciones y protocolos compatibles con el dispositivo móvil 106; presentar y recibir información (por ejemplo, petición de PIN, PIN) procedente del usuario a través de la GUI 116; descifrar y cifrar información transmitida de manera inalámbrica entre la tarjeta 104 de transacciones y el punto de acceso 514; ejecutar aplicaciones memorizadas localmente en la tarjeta 104 de transacciones; conectar y desconectar selectivamente la antena de la tarjeta 104 de transacciones en base, por lo menos en parte, a uno o varios eventos; ejecutar procesos de autenticación en base, por lo menos en parte, a la información recibida, por ejemplo, a través de la GUI 116; transmitir al punto de acceso 514 una firma del anfitrión en respuesta, por lo menos, a un intento de transacción; almacenar, por lo menos en parte, detalles de la transacción ejecutada entre la tarjeta 104 y el punto de acceso 514; generar y/o presentar alertas (por ejemplo, alertas audiovisuales) al usuario a través de la GUI 116; generar y/o transmitir alertas de mensaje inalámbrico a la institución 516 utilizando el dispositivo móvil 106 si tiene capacidad celular; y/u otros. En algunas implementaciones, la tarjeta 104 de transacciones puede iniciar una transacción en respuesta, por lo menos, a la selección un elemento gráfico en la GUI 116 por parte de un usuario. La tarjeta 104 de transacciones puede iniciar una transacción con el punto de acceso 514, en respuesta, por lo menos, a una petición inalámbrica transmitida mediante el punto de acceso 514. En algunas implementaciones, la tarjeta 104 de transacciones puede conmutar selectivamente la antena entre los estados conectado y desconectado, en respuesta a uno o varios eventos. Dichos uno o varios eventos pueden incluir una petición del usuario, la compleción de una transacción, la inserción de la tarjeta 104 en un dispositivo móvil diferente, un cambio de emplazamiento, eventos de temporizador, la detección de un PIN incorrecto introducido por el usuario, un cambio de la red inalámbrica a la que está conectado el dispositivo, un mensaje recibido desde la institución 506 utilizando métodos de comunicación inalámbricos tales como SMS, y/u otros eventos. Por ejemplo, la tarjeta 104 de transacciones puede recibir una o varias órdenes para desconectar la antena de una red celular (no ilustrada) a través del dispositivo móvil 106.

En algunas implementaciones, la tarjeta 104 de transacciones puede iniciar una transacción en respuesta, por lo menos, a un usuario seleccionando un elemento gráfico en la GUI 116. La tarjeta 104 de transacciones puede iniciar una transacción con el punto de acceso 514 en respuesta, por lo menos, a una petición inalámbrica transmitida por el punto de acceso 514. En algunas implementaciones, la tarjeta 104 de transacciones puede conmutar selectivamente la antena entre los estados conectado y desconectado, en respuesta a uno o varios eventos. Dichos uno o varios eventos pueden incluir una petición del usuario, la compleción de una transacción, la inserción de la tarjeta 104 en un dispositivo móvil diferente, un cambio de emplazamiento, eventos de temporizador, la detección de un PIN incorrecto introducido por el usuario, un cambio de la red inalámbrica a la que está conectado el dispositivo, un mensaje recibido desde la institución 506 utilizando métodos de comunicación inalámbricos tales como SMS, y/u otros eventos. Por ejemplo, la tarjeta 104 de transacciones puede recibir una o varias órdenes para desconectar la antena de una red celular (no mostrada) a través del dispositivo móvil 106. En algunas implementaciones, la tarjeta 104 de transacciones puede solicitar la identificación del usuario, tal como un PIN, una combinación de contraseña e ID de usuario, una firma biométrica y/u otras.

En relación con la traducción entre protocolos, la tarjeta 104 de transacciones puede procesar información, por ejemplo, en ISO 106416, un protocolo de seguridad estándar y/u otros. En este caso, la tarjeta 104 de transacciones puede traducir entre un protocolo NFC (por ejemplo, ISO 18092) y el protocolo de la tarjeta de transacciones. En algunas implementaciones, las órdenes ISO 106416 pueden ser encapsuladas dentro de órdenes de la interfaz utilizadas para transmitir datos entre el dispositivo anfitrión 514 y la tarjeta 104. Además, la tarjeta 104 de transacciones puede interactuar con el dispositivo móvil 106 a través de una interfaz física tal como MicroSD, Mini-SD, SD, MMC, miniMMC, microMMC, USB, miniUSB, microUSB, Firewire, Apple iDock y/u otras. En relación con los procesos de seguridad, la tarjeta 104 de transacciones puede implementar uno o varios algoritmos de cifrado para asegurar la información de la transacción, tal como el número de tarjeta (por ejemplo, número de tarjeta de crédito, número de tarjeta de débito, número de cuenta bancaria), PIN, y/u otra información relacionada con la seguridad. La información relacionada con la seguridad puede incluir una fecha de expiración, un código de verificación de la tarjeta, el nombre de usuario, el número de teléfono particular, el código postal y/u otra información del usuario asociada con la verificación de la identidad del titular de la tarjeta. En algunas implementaciones, la tarjeta 104 de transacciones puede ejecutar clave privada (algoritmos asimétricos), tal como DES, TDES y/u otros, o clave publica (algoritmos simétricos), tal como RSA, curvas elípticas y/u otros. Además, la tarjeta 104 de transacciones puede incluir memoria (por ejemplo, flash, EEPROM) para almacenar datos del usuario, aplicaciones, páginas web fuera de línea y/u otra información. En relación con las aplicaciones, la tarjeta 104 de transacciones puede ejecutar una aplicación almacenada localmente y presentar información al usuario y recibirla del mismo a través de la GUI 116. Por ejemplo, la tarjeta 104 de transacciones puede ejecutar una aplicación utilizada para sincronizar un saldo de cuentas con la institución 506, utilizando la GUI 116 y el dispositivo móvil 106. Alternativa o adicionalmente a las aplicaciones, la tarjeta 104 de transacciones puede presentar al usuario páginas web fuera de línea utilizando la GUI 116. En respuesta a iniciar una transacción, la tarjeta 104 de transacciones puede presentar automáticamente una página web fuera de línea a través de la GUI 116. En algunas implementaciones, la página web fuera de línea puede estar asociada con una institución 506. En algunas implementaciones, la tarjeta 104 de transacciones puede ser compatible con versiones anteriores y funcionar como un dispositivo de almacenamiento masivo. Por ejemplo, si la interfaz inalámbrica de la tarjeta 104 de transacciones no está disponible o está desactivada, la tarjeta 104 de transacciones puede funcionar como un dispositivo de almacenamiento masivo que permite a los usuarios acceder a datos memorizados en el componente de memoria (por ejemplo, flash). En algunas implementaciones, la tarjeta 104 de transacciones puede ejecutar un conjunto de órdenes de inicialización en respuesta, por lo menos, a la introducción en el dispositivo móvil 106. Estas órdenes de inicialización pueden incluir determinar información relacionada con el dispositivo para el dispositivo móvil 106 (por ejemplo, número de teléfono, firma, información de la red conectada, información de la posición y otras propiedades disponibles), determinar información relativa al usuario (por ejemplo, código PIN, código de activación), implementar contadores, establecer indicadores y activar/desactivar funciones en función de normas y/o algoritmos preexistentes.

En algunas implementaciones, la tarjeta 104 de transacciones puede ejecutar automáticamente uno o varios procesos de control de fraude. Por ejemplo, la tarjeta 104 de transacciones puede identificar un cambio operacional y transmitir automáticamente una notificación a la institución financiera en base, por lo menos en parte, al cambio identificado. La tarjeta 104 de transacciones puede ejecutar dos procesos de control del fraude: (1) determinar una infracción de una o varias normas; y (2) ejecutar automáticamente una o varias acciones en respuesta, por lo menos, a la infracción. En relación con las normas, la tarjeta 104 de transacciones puede almacenar localmente normas asociadas con actualizaciones de aspectos operativos de la tarjeta 104 de transacciones. Por ejemplo, la tarjeta 104 de transacciones puede almacenar una norma que indica que un cambio en el dispositivo anfitrión móvil 106 es una infracción operacional. En algunas implementaciones, la tarjeta 104 de transacciones puede almacenar normas basadas, por lo menos en parte, en actualizaciones de uno o varios de los siguientes: número telefónico del dispositivo anfitrión 106; dirección MAC del dispositivo anfitrión 106; red conectada de forma inalámbrica al dispositivo anfitrión 106; ubicación del dispositivo anfitrión; y/u otros aspectos. En respuesta a uno o varios eventos que se adecuan a las normas o bien las infringen, la tarjeta 104 de transacciones puede ejecutar uno o varios procesos para impedir sustancialmente, o si no notificar a las instituciones, una actividad potencialmente fraudulenta. Por ejemplo, la tarjeta 104 de transacciones puede ejecutar una orden para bloquear una cuenta de usuario asociada y/o la tarjeta 104 de transacciones. Alternativa o adicionalmente, la tarjeta 104 de transacciones puede

transmitir una orden a la institución 506 para llamar al dispositivo anfitrión móvil 106. En algunas implementaciones, la tarjeta 104 de transacciones puede ejecutar una orden basada, por lo menos en parte, en un tipo de evento. En algunos ejemplos, la tarjeta 104 de transacciones puede iniciar una llamada a la institución 506 en respuesta, por lo menos, a un cambio en el número del dispositivo anfitrión 106. En algunos ejemplos, la tarjeta 104 de transacciones puede volver a ejecutar un proceso de activación, en respuesta, por lo menos, a un tipo de evento especificado. Un proceso de activación puede incluir la activación de la tarjeta de transacciones y/o de la cuenta financiera, tal como se discute en mayor detalle en relación con la figura 13. En algunas implementaciones, la tarjeta 104 de transacciones puede ejecutar una orden para desconectar la GUI 116 respecto de la tarjeta 104 de transacciones. La tarjeta 104 de transacciones puede presentar una notificación de desconexión a través de la GUI 116, antes de la ejecución de la orden. En algunas implementaciones, la tarjeta 104 de transacciones puede transmitir una orden a la institución 506 para desactivar una cuenta asociada con la tarjeta 104.

En algunas implementaciones, el punto de acceso 514 puede transmitir una petición 517 de transacción a la tarjeta 512 de transacciones, de información para generar una petición 518 de autorización. En respuesta, por lo menos, a la petición de transacción, la tarjeta 512 de transacciones puede transmitir una o varias respuestas 519 de transacción, que identifican información asociada con una cuenta de usuario. En algunas implementaciones, el punto de acceso 514 puede transmitir a la institución 506 una petición 518 para autorizar una transacción. La información de autorización puede incluir un número de cuenta, el importe de la transacción, credenciales del usuario y/u otra información. En respuesta, por lo menos, a la petición 518 de transacción, la institución 506 puede transmitir una respuesta 520 de autorización al punto de acceso 514. En algunas implementaciones, el punto de acceso 114 puede transmitir la respuesta 520 a la tarjeta 512 de transacciones. La respuesta 520 de transacción puede incluir, por ejemplo, un recibo presentable al usuario a través de la GUI 116a. En algunas implementaciones, la institución 506 puede transmitir la respuesta 120 de autorización al dispositivo móvil, a través de una red central celular (ver figura 7). En esta implementación, la institución 506 puede haber memorizado la asociación entre el dispositivo móvil 106 y la tarjeta 104 de transacciones durante el proceso de registro del usuario, automáticamente al producirse la activación del usuario de la tarjeta 104 cuando, por ejemplo, la tarjeta 104 es insertada inicialmente en el dispositivo móvil 106, y/u en otro evento. En la implementación mostrada, el punto de acceso 514 incluye la GUI 509.

La GUI 509 comprende una interfaz gráfica de usuario operativa para permitir al usuario del punto de acceso 514 interactuar, por lo menos, con una parte del sistema 500 con cualquier propósito adecuado, tal como un usuario que introduce información de transacción (por ejemplo, PIN, aceptación de la transacción) y/o presenta información de la transacción (por ejemplo, importe de la transacción). Generalmente, la GUI 509 proporciona al usuario particular una presentación eficiente y amigable de los datos proporcionados mediante el sistema 500 o comunicados dentro del mismo, y/o asimismo un medio eficiente y amigable para que el usuario inicie una transacción inalámbrica con la tarjeta 104 de transacciones. La GUI 509 puede presentar una serie de pantallas al usuario para, por ejemplo, aceptar una transacción e introducir información de seguridad, tal como un PIN.

En algunas implementaciones, la tarjeta 104 de transacciones puede implementarse de manera diferente. La tarjeta 104 de transacciones puede ser implementada como un llavero de seguridad y permanece activa fuera de la dispositivo móvil 106, como un llavero. En este caso, la tarjeta 104 de transacciones puede estar pasiva y ser activada desde un campo magnético de inducción generado por el punto de acceso 514. La tarjeta 104 de transacciones puede implementarse en forma de chip industrial de circuitos integrados para su montaje en un PCB o un chip IC. En algunas implementaciones, la tarjeta 104 de transacciones puede implementarse en forma de unidad independiente de sobremesa autocontenida, alimentada mediante un adaptador externo de CA o una caja autónoma. En algunas implementaciones, la tarjeta 104 de transacciones puede implementarse como un accesorio externo del dispositivo móvil 106 (por ejemplo, una caja) y conectarse al dispositivo móvil utilizando una interfaz periférica tal como USB, puerto serie, la interfaz privada iDock Apple y/u otra interfaz.

En algunas implementaciones, la tarjeta 104 de transacciones puede funcionar de acuerdo con uno o varios de los modos siguientes: emulación de tarjeta activa; lector activo; auto-aprendizaje; anulada; memoria; inactiva; y/u otros modos. La tarjeta 104 de transacciones puede manejar el modo de emulación de tarjeta activa para transformar el dispositivo móvil 106 en un dispositivo de pago sin contacto, cargado con un vehículo financiero (financial vehicle, FV) que puede ser, por ejemplo, una tarjeta de crédito, una tarjeta de débito, un cheque regalo y/u otro producto de pago minorista. En este modo, la tarjeta 104 de transacciones puede ejecutar transacciones de pago en cualquier terminal de pago minorista (por ejemplo, punto de acceso 514) que acepte transacciones de pago sin contacto. Por ejemplo, dichos terminales pueden ser terminales con capacidad de pago sin contacto, instalados actualmente por los comerciantes bajo los programas Paypass de MasterCard, Paywave de Visa, Amex ExpressPay, Discover Zip y/u otros. Después de que la antena de la tarjeta 104 de transacciones es activada de este modo, un terminal del comerciante puede detectar la presencia de un dispositivo anfitrión con la tarjeta 104 de transacciones, y solicitar al usuario que autorice una transacción, por ejemplo introduciendo un PIN, registrándose en una interfaz de un terminal, confirmando el importe de la transacción y/o con otra acción. De este modo, dichas transacciones pueden manejarse como una transacción normal en presencia de la tarjeta. En otras palabras, el punto de acceso 514 puede percibir la tarjeta 104 de transacciones como una tarjeta de plástico de pago sin contacto y puede comunicar con la tarjeta 104 de transacciones como una tarjeta de plástico de pago sin contacto, para ejecutar las transacciones de pagos. En estas implementaciones, cuando la tarjeta 104 funciona en un modo de emulación de tarjeta activa, el

punto de acceso 514 puede comunicar de forma inalámbrica con la tarjeta 104 de transacciones utilizando las mismas señales utilizadas para comunicar con una tarjeta de plástico de pago sin contacto. En este modo de emulación de tarjeta activa, la tarjeta 104 de transacciones emula una tarjeta de plástico de pago sin contacto y puede ser compatible para versiones anteriores con el punto de acceso 514. En esta implementación, puede no ser necesario que el terminal ni la institución financiera requieran soporte lógico adicional para ejecutar la transacción. Además, en este modo la tarjeta 104 de transacciones puede utilizarse para otras aplicaciones tales como control de acceso físico (para abrir puertas, en un entorno corporativo o en un entorno de transporte), control de acceso lógico (para solicitar acceso a la red a través de un PC), control de acceso a aplicaciones (para comprar el acceso a servicios tales como transporte, películas o dondequiera que se requiera la realización de un pago para obtener acceso a un servicio) y/u otras aplicaciones.

En el modo de lector activo, la tarjeta 104 de transacciones puede transformar el dispositivo móvil 106 en un dispositivo lector sin contacto, capaz de recibir datos dentro del alcance de un terminal transmisor (por ejemplo, el punto de acceso 514). En algunas implementaciones, este modo puede requerir equipamiento físico NFC especial con capacidad de modo lector como parte de la tarjeta 104 de transacciones. En caso de que el dispositivo móvil 106 esté próximo (por ejemplo, a 10 cm o menos) a un terminal transmisor, puede activarse el modo lector de la tarjeta 104 de transacciones y solicitarse al usuario autorización para recibir datos a través de la GUI 116. Este modo puede ser adecuado solamente para dispositivos móviles 106 con un elemento de UI, tal como un botón de OK y una pantalla, un LED para indicar que se está solicitando la recepción de datos, y/u otras interfaces. Una vez que el usuario autoriza la transmisión, la tarjeta 104 de transacciones en este modo puede recibir y, localmente, almacenar, procesar y ejecutar una transacción y/o enviar a otra entidad datos recibidos. Por ejemplo, la tarjeta 104 de transacciones en este modo puede recibir contenido a través de carteles promocionales, validar la compra de un billete y/u otros. Por ejemplo, en este modo la tarjeta 104 de transacciones puede funcionar como un terminal POS móvil que recibe información de transacciones procedente de un llavero/tarjeta de plástico sin contacto, y ordena al punto de acceso 514 preparar una petición de autorización de transacción para la institución 506, a través de una red central celular. Una vez que la institución 506 autoriza la transacción, el dispositivo móvil 106 puede mostrar al usuario la confirmación de la transacción a través de la GUI 116.

En relación con el modo de auto-aprendizaje, la tarjeta 104 de transacciones puede ejecutar una versión del modo lector. En algunas implementaciones, el modo de auto-aprendizaje puede ser activado mediante una acción especial (por ejemplo, la presión de un punto de aguja sobre un pequeño conmutador, la introducción de una contraseña administrativa a través de la GUI 116). En respuesta, por lo menos, a la activación de este modo, la tarjeta 104 de transacciones puede configurarse para recibir datos de personalización sobre, por ejemplo, la interfaz inalámbrica de corto alcance, desde otra tarjeta homóloga de transacciones, tal como las tarjetas de plástico sin contacto compatibles con esta funcionalidad y emitidas por la institución 506, o una tarjeta administrativa preparada especialmente a tal efecto. Los datos de personalización recibidos en este modo pueden incluir información FV cifrada, que es almacenada en la memoria segura de la tarjeta 104 de transacciones. En algunas implementaciones, la tarjeta 104 de transacciones en este modo puede recibir la información FV a través de una interfaz sin contacto de un transmisor y/u otros. A continuación, la tarjeta 104 de transacciones puede sintetizar la información FV que corresponde a la cuenta de usuario y personalizar un modo de seguridad interno que incluye, por ejemplo, aplicaciones de pago para ejecutar transacciones con instituciones 506 y credenciales de usuario asociadas. El modo de auto-aprendizaje puede utilizarse para volver a personalizar la tarjeta 104 de transacciones sobre el terreno. En algunas implementaciones, pueden ser eliminados todos los datos anteriores si se activa el modo de auto-aprendizaje. El modo de auto-aprendizaje puede ser un modo de personalización entre pares, en el que la tarjeta 104 puede recibir información de personalización procedente de otra tarjeta 104 de transacciones. Este modo puede representar un modo de personalización adicional en comparación con los escenarios de personalización en la fábrica, la tienda y/o aérea (OTA, Over-The-Air), que pueden ser escenarios de personalización servidor a cliente. En algunas implementaciones, el modo de auto-aprendizaje puede ser un modo de personalización entre homólogos, en el que la tarjeta 104 de transacciones recibe información de personalización procedente de otra tarjeta de transacciones. Puesto que en este modo se utilizan dos tarjetas 104 de transacción, este modo puede ser diferente respecto de un escenario de personalización servidor a cliente, tal como con la personalización en fábrica, en tienda y OTA.

En relación con el modo inactivo, la tarjeta 104 de transacciones puede desactivar temporalmente la interfaz sin contacto. En algunas implementaciones, el modo inactivo puede activarse a través de la interfaz física con el dispositivo móvil 106, tal como una interfaz microSD. En respuesta, por lo menos, a la activación del modo inactivo, la tarjeta 104 de transacciones puede comportarse temporalmente como solamente una tarjeta de memoria masiva. En algunas implementaciones, la tarjeta 104 puede asimismo entrar en este estado cuando es presionado el punto de aguja de reseteo. En este modo, la tarjeta 104 de transacciones puede preservar información almacenada localmente, que incluye datos financieros del usuario. En este modo, la tarjeta 104 de transacciones puede ejecutar el proceso de activación y, en caso satisfactorio, puede volver al modo activo. Las instituciones 506 pueden utilizar este modo para impedir temporalmente la utilización en respuesta, por lo menos, a la identificación de actividad por lo menos potencialmente fraudulenta.

En relación con el modo anulado, la tarjeta 104 de transacciones puede desactivar permanentemente la interfaz sin contacto. En algunas implementaciones, el modo anulado se activa a través de la interfaz física con el dispositivo móvil 106, tal como una interfaz microSD. En respuesta, por lo menos, a la activación del modo anulado la tarjeta 104 de transacciones puede comportarse permanentemente como una barra de memoria masiva. En el caso de que se presione un punto de aguja de reseteo, en algunas implementaciones no puede hacerse entrar a la tarjeta 104 de transacciones en ningún otro modo. Además, la tarjeta 104 de transacciones puede eliminar el contenido financiero de la memoria en respuesta, por lo menos, a la activación de este modo. En algunas implementaciones, las instituciones 506 pueden utilizar este modo para eliminar datos de una tarjeta 104 de transacciones que está inutilizada físicamente pero sigue conectada a la red inalámbrica a través del dispositivo anfitrión 106.

En relación con el modo de memoria, la tarjeta 104 de transacciones puede funcionar como una barra de memoria masiva, de tal modo que la memoria es accesible a través de los métodos convencionales. En algunas implementaciones, la tarjeta 104 de transacciones puede activar automáticamente este modo en respuesta, por lo menos, a su extracción del dispositivo anfitrión, su inserción en un dispositivo anfitrión no autorizado, y/u otros eventos. La tarjeta 104 de transacciones puede conmutarse al modo activo desde el modo de memoria, por ejemplo, insertando la tarjeta en un dispositivo autorizado, o puede conmutarse desde este modo al modo de auto-aprendizaje para volver a personalizar el dispositivo para un nuevo dispositivo anfitrión o una nueva cuenta de usuario. En algunas implementaciones, el modo de memoria puede funcionar sustancialmente igual que el modo inactivo.

En algunas implementaciones, la tarjeta 104 de transacciones puede volver a personalizarse/actualizarse, tal como utilizando un proceso de gestión del dispositivo por soporte lógico y/o un reseteo de equipamiento físico. Por ejemplo, el usuario puede desear volver a personalizar la tarjeta 104 de transacciones para cambiar de dispositivos anfitriones, para tener múltiples dispositivos anfitriones y/o por otras razones. En relación con la gestión del dispositivo por soporte lógico, puede ser necesario que el usuario sitúe en un soporte conmutador el nuevo dispositivo anfitrión con la tarjeta 104 de transacciones insertada, para lanzar la aplicación de administración del dispositivo por soporte lógico. En algunas implementaciones, la aplicación de gestión por soporte lógico puede ser una aplicación instalada directamente en el cliente 504, estar integrada como un complemento en una aplicación de sincronización normal, tal como ActiveSync, estar disponible a través de un complemento del navegador que se ejecuta en el sitio web del proveedor del complemento, y/o mediante otras fuentes. El usuario puede ingresar en la aplicación y verificar su identidad y, en respuesta a la verificación, la aplicación puede permitir el acceso a una sección de dispositivos en la aplicación de gestión del dispositivo. La aplicación de gestión del dispositivo puede leer la tarjeta 104 de transacciones y mostrar las direcciones MAC, las firmas de los dispositivos en los que el usuario ha insertado su complemento, y/u otra información específica del dispositivo. El dispositivo móvil 106 puede marcarse como activo y el dispositivo anfitrión puede mostrarse como rechazado o inactivo. La aplicación puede permitir al usuario actualizar el estado del nuevo dispositivo anfitrión y, en respuesta como mínimo a la selección, la aplicación de gestión del dispositivo puede instalar la firma en el nuevo dispositivo anfitrión y marcar la actualización del estado como admisible en la memoria segura de la tarjeta 104 de transacciones. Asimismo, el usuario puede ser capaz de actualizar el estado del dispositivo móvil 106 como rechazado. De lo contrario, ambos dispositivos pueden estar activos y la tarjeta 104 de transacciones puede conmutarse entre los dos dispositivos. En relación con el proceso de reseteo del equipamiento físico, el usuario puede utilizar la presión en el punto de aguja de reseteo sobre la tarjeta 104 de transacciones física, para activar el modo de auto-aprendizaje. En este modo, los datos financieros pueden ser eliminados y han de ser recargados. Cuando la tarjeta 104 de transacción es insertada en el nuevo dispositivo anfitrión, puede comenzar el proceso de provisión, tal como se ha discutido anteriormente.

El punto de acceso 514 puede incluir cualquier soporte lógico, equipamiento físico y/o soporte lógico inalterable que reciba de forma inalámbrica información de la cuenta para ejecutar una transacción con una o varias instituciones 506. Por ejemplo, el punto de acceso 514 puede ser una caja registradora electrónica capaz de transmitir de forma inalámbrica información de transacciones con la tarjeta 104a de transacciones. El punto de acceso 514 puede transmitir información en uno o varios de los formatos siguientes: 14443 tipo A/B, Felica, MiFare, ISO 18092, ISO 15693; y/u otros. La información de la transacción puede incluir información de verificación, número de comprobación, número de encaminamiento, número de cuenta, importe de la transacción, fecha y hora, número de permiso de conducción, ID del comerciante, parámetros del comerciante, número de tarjeta de crédito, número de tarjeta de débito, firma digital y/u otra información. En algunas implementaciones, la información de la transacción puede cifrarse. En la implementación mostrada, el punto de acceso 514 puede recibir de forma inalámbrica desde la tarjeta 104 de transacciones información cifrada de la transacción, y enviar electrónicamente la información a una o varias de las instituciones 506 para su autorización. Por ejemplo, el punto de acceso 514 puede recibir una indicación de que ha sido aceptado o rechazado un importe de transacción para la cuenta identificada, y/o solicitar información adicional de la tarjeta 104 de transacciones.

Tal como se utiliza en esta exposición, se contempla que los clientes 504 incluyan un ordenador personal, un terminal de pantalla táctil, una estación de trabajo, un ordenador en red, un ordenador de sobremesa, un quiosco, un puerto inalámbrico de datos, un teléfono inteligente, una PDA, uno o varios procesadores en el interior de estos o de otros dispositivos, o cualquier otro dispositivo adecuado electrónico o de procesamiento, utilizado para examinar información de transacciones asociada con la tarjeta 104 de transacciones. Por ejemplo, el cliente 504 puede ser

una PDA operativa para conectar de forma inalámbrica con una red externa o no segura. En otro ejemplo, el cliente 504 puede comprender un ordenador portátil que incluye un dispositivo de entrada, tal como un teclado numérico, una pantalla táctil, un ratón u otro dispositivo que pueda recibir información, y un dispositivo de salida que transporta la información asociada a transacciones ejecutadas con las instituciones 506, que incluye datos digitales, información visual o GUI 515. En algunas implementaciones, el cliente 504b puede comunicar de forma inalámbrica con la tarjeta 104b de transacciones utilizando, por ejemplo, un protocolo NFC. En algunas implementaciones, el cliente 504a incluye un lector 516 de tarjetas que tiene una interfaz física para comunicar con la tarjeta 104c de transacciones. En algunas implementaciones, el lector 516 de tarjetas puede incluir, por lo menos, un adaptador que adapta la interfaz soportada por el cliente 504 (por ejemplo, USB, Firewire, Bluetooth, WiFi) a la interfaz física soportada por la tarjeta 104 (por ejemplo, SD/NFC). En este caso, el cliente 504a puede no incluir un transceptor para la comunicación inalámbrica.

La GUI 515 comprende una interfaz gráfica de usuario operativa para permitir al usuario del cliente 504 interactuar, por lo menos, con una parte del sistema 500 con cualquier fin adecuado, tal como examinar información de transacciones. Generalmente, la GUI 505 proporciona al usuario particular una presentación eficiente y amigable de los datos proporcionados por el sistema 500 o comunicados en el interior del mismo. La GUI 515 puede comprender una serie de cuadros o vistas personalizables que tienen campos interactivos, listas desplegables y/o botones manejados por el usuario. El término interfaz gráfica de usuario puede utilizarse en singular o en plural, para describir una o varias interfaces gráficas de usuario y cada una de las pantallas de una interfaz gráfica de usuario concreta. La GUI 515 puede incluir cualquier interfaz gráfica de usuario, tal como un navegador web genérico o una pantalla táctil, que procese información en el sistema 500 y presente los resultados al usuario. Las instituciones 506 pueden aceptar datos procedentes del cliente 504 utilizando, por ejemplo, el navegador web (por ejemplo, Microsoft Internet Explorer o Mozilla Firefox) y devolver las respuestas apropiadas (por ejemplo, HTML o XML) al navegador utilizando la red 108. En algunas implementaciones, la GUI 516 de la tarjeta 104c de transacciones puede presentarse a través de la GUI 515a del cliente 504a. En estas implementaciones, la GUI 515a puede recuperar credenciales del usuario desde la GUI 116c y documentar formularios financieros presentados en la GUI 515a. Por ejemplo, la GUI 515a puede presentar un formulario al usuario para introducir información de la tarjeta de crédito con objeto de comprar un bien a través de la red internet, y la GUI 515a puede documentar el formulario utilizando la GUI 116c en respuesta, por lo menos, a una petición del usuario.

Las instituciones 506a-c pueden incluir cualquier empresa que pueda autorizar transacciones recibidas a través de la red 108. Por ejemplo, la institución 506a puede ser un proveedor de tarjetas de crédito que determine si autorizar una transacción en base, al menos en parte, a la información recibida a través de la red 506. La institución 506 puede ser un proveedor de tarjetas de crédito, un banco, una asociación (por ejemplo, VISA), un comerciante minorista (por ejemplo, Target), un proveedor de cheques de regalo/prepago, un banco de internet, un ente público, un club y/u otros. En general, la institución 506 puede ejecutar una o varias de las siguientes acciones: recibir una petición para autorizar una transacción; identificar un número de cuenta y otra información de la transacción (por ejemplo, PIN); identificar fondos y/o un límite de crédito asociado con la cuenta identificada; identificar privilegios de acceso asociados con la cuenta de usuario; determinar si la petición de transacción excede los fondos y/o el límite de crédito y/o infringe cualesquiera otras normas asociadas con la cuenta; transmitir una indicación sobre si la transacción ha sido aceptada o rechazada; y/u otros procesos. En relación con la banca móvil, la institución 506 puede identificar un número de cuenta (por ejemplo, cuenta bancaria, número de tarjeta de crédito) e información de verificación asociada (por ejemplo, PIN, código postal) y determinar fondos disponibles para el titular de la cuenta. En base, por lo menos en parte, a los fondos identificados, la institución 506 puede aceptar o rechazar la transacción solicitada, o solicitar información adicional. En relación con el cifrado, la institución 506 puede utilizar un algoritmo de clave pública tal como RSA o curvas elípticas, y/o algoritmos de clave privada tales como TDES, para cifrar y descifrar datos.

La figura 6 es un diagrama de bloques que muestra un sistema de transacciones 600 a modo de ejemplo para comunicar de forma inalámbrica información de transacciones utilizando tecnología radioeléctrica celular. Por ejemplo, el sistema 600 puede comunicar de forma inalámbrica la recepción de una transacción a una tarjeta 104 de transacciones, utilizando el dispositivo anfitrión móvil 110 y tecnología radioeléctrica celular. En algunas implementaciones, la tecnología radioeléctrica celular puede incluir el sistema global para comunicaciones móviles (GSM, Global System for Mobile Communication), acceso múltiple por división de código (CDMA, Code Division Multiple Access), sistema universal de telecomunicaciones móviles (UMTS, Universal Mobile Telecommunications System) y/o cualquier otra tecnología celular. Las instituciones 106 pueden asignar uno o varios dispositivos anfitriones móviles 110 a una tarjeta 104 de transacciones, en respuesta a uno o varios eventos. En algunos ejemplos, el usuario puede registrar dichos uno o varios dispositivos móviles 106 con la institución 506, por ejemplo, en relación con la solicitud de la tarjeta 104 de transacciones asociada. En algunos ejemplos, la tarjeta 104 de transacciones puede registrar el dispositivo anfitrión móvil 110 con la institución 506 en respuesta, por lo menos, a la introducción inicial en el dispositivo 110. Independientemente del proceso de asociación, el sistema 500 puede utilizar las capacidades celulares de los dispositivos anfitriones 110 para comunicar información entre las instituciones 506 y la tarjeta 104 de transacciones. Utilizando la tecnología radioeléctrica celular del dispositivo anfitrión 110, el sistema 500 puede comunicar con la tarjeta 104 de transacciones cuando la tarjeta no está cerca de un dispositivo minorista, tal como el punto de acceso 514 de la figura 1.

En la implementación mostrada, la red central celular 602 incluye habitualmente diversos elementos de conmutación, pasarelas y funciones de control del servicio para proporcionar servicios celulares. La red central celular 602 proporciona frecuentemente estos servicios a través de una serie de redes de acceso celular (por ejemplo, RAN) que interactúan entre el sistema celular y otros sistemas de comunicación, tal como la red 108, a través de un MSC 606. De acuerdo con los estándares celulares, la red central celular 602 puede incluir una parte con conmutación de circuitos (o con conmutación de voz) para procesar llamadas de voz y una parte con conmutación de paquetes (o con conmutación de datos) para soportar transferencias de datos tales como, por ejemplo, mensajes de correo electrónico y navegación web. La parte con conmutación de circuitos incluye el MSC 606, que conmuta o conecta llamadas telefónicas entre la red de acceso radioeléctrico (RAN, radio access network) 604 y la red 108 u otra red, entre redes centrales celulares o entre otras redes. En caso de que la red central 602 sea una red central GSM, la red central 602 puede incluir una parte con conmutación de paquetes, conocida asimismo como servicio general de radiocomunicaciones por paquetes (GPRS, General Packet Radio Service), que incluye un nodo de soporte de servicios GPRS (SGSN, Serving GPRS Support Node) (no ilustrado), similar al MSC 606, para dar servicio a los dispositivos de comunicación 106 y rastrearlos, y un nodo de soporte de pasarela GPRS (GGSN, Gateway GPRS Support Node) (no ilustrado) para establecer conexiones entre redes con conmutación de paquetes y dispositivos de comunicación 110. La SGSN puede contener asimismo datos de abonado útiles para establecer y traspasar conexiones de llamada. La red central celular 602 puede incluir asimismo un registro de posición base (HLR, home location register) para mantener datos de abonados "permanentes" y un registro de posición de visitantes (VLR, visitor location registe) (y/o una SGSN) para mantener "temporalmente" datos de abonado extraídos del HLR y actualizar información sobre la posición de dichos dispositivos de comunicaciones 110 utilizando un método de comunicaciones inalámbrico. Además, la red central celular 602 puede incluir autenticación, autorización y contabilidad (AAA, Authentication, Authorization, and Accounting), que lleva a cabo la función de autenticar, autorizar y contabilizar los dispositivos 110 operativos para acceder a la red central GSM 602. Si bien la descripción de la red central 602 se realiza con respecto a redes GSM, la red central 602 puede incluir otras tecnologías de radio celular tales como UMTS, CDMA y otras, sin apartarse del alcance de esta exposición.

La RAN 604 proporciona una interfaz radioeléctrica entre dispositivos móviles y la red central celular 602, que puede proporcionar servicios de voz en tiempo real, de datos y multimedia (por ejemplo, una llamada) a los dispositivos móviles a través de una macrocelula 608. En general, la RAN 604 comunica tramas aéreas a través de enlaces de radiofrecuencia (RF). En particular, la RAN 604 transforma tramas aéreas en mensajes basados en enlace físico, para su transmisión a través de la red central celular 602. La RAN 604 puede implementar durante la transmisión, por ejemplo, uno de los siguientes estándares de interfaz inalámbrico: servicio telefónico móvil avanzado (AMPS, Advanced Mobile Phone Service), estándares GSM, acceso múltiple por división de código (CDMA), acceso múltiple por división de frecuencias (TDMA, Time Division Multiple Access), IS-54 (TDMA), servicio general de radiocomunicaciones por paquetes (GPRS), velocidades de datos mejoradas para evolución global (EDGE, Enhanced Data Rates for Global Evolution) o interfaces radioeléctricos privados. El usuario puede abonarse a la RAN 604, por ejemplo, para recibir el servicio telefónico celular, el servicio el sistema de posicionamiento global (GPS, Global Positioning System), el servicio radioeléctrico XM, etc.

La RAN 604 puede incluir estaciones base (BS, Base Stations) 610 conectadas a controladores de estación base (BSC, Base Station Controllers) 12. La BS 610 recibe y transmite tramas aéreas dentro de una zona geográfica de la RAN 604 y comunica con otros dispositivos móviles 106 conectados a la red central GSM 602. Cada BSC 612 está asociada con una o varias BS 610 y controla la BS asociada. Por ejemplo, el BSC 612 puede proporcionar funciones tales como traspaso, datos de configuración de células, control de niveles de potencia de RF o cualesquiera otras funciones adecuadas para gestionar los recursos radioeléctricos y encaminar señales hacía, y desde la BS 610. El MSC maneja el acceso al BSC 612 y a la red 108. El MSC 306 puede conectarse al BSC 612 a través de una interfaz estándar, tal como la interfaz-A. Si bien los elementos de la RAN 604 se describen con respecto a redes GSM, la RAN 604 puede incluir otras tecnologías celulares tales como UMTS, CDMA y/u otras. En el caso de UMTS, la RAN 604 puede incluir nodos B y controladores de red radioeléctrica (RNC, Radio Network Controllers).

La tarjeta inteligente inalámbrica 614 es una tarjeta de bolsillo con circuitos integrados incorporados que procesan información. Por ejemplo, la tarjeta inteligente 614 puede recibir de forma inalámbrica información de transacciones, procesar la información utilizando aplicaciones incorporadas y transmitir de forma inalámbrica una respuesta. La tarjeta inteligente inalámbrica 614 puede comunicar de forma inalámbrica con lectores de tarjeta a través de la tecnología de inducción RFID a velocidades de transferencia de datos de 106 a 848 kbit/s. La tarjeta 614 puede comunicar de forma inalámbrica con lectores próximos, a entre 10 cm (por ejemplo, ISO/IEC 14443) y 50 cm (por ejemplo, ISO 15693). La tarjeta inteligente inalámbrica 614 funciona independientemente de la fuente de alimentación interna, y capta energía de las señales incidentes de interrogación por radiofrecuencias para alimentar la electrónica incorporada. La tarjeta inteligente 614 puede ser una tarjeta de memoria o una tarjeta con microprocesador. En general, las tarjetas de memoria incluyen solamente componentes de almacenamiento de memoria no volátil, y pueden incluir alguna lógica de seguridad específica. Las tarjetas con microprocesador incluyen memoria volátil y componentes de microprocesador. En algunas implementaciones, la tarjeta inteligente 614 puede tener las dimensiones del tamaño habitual de una tarjeta de crédito (por ejemplo, 85,60 x 53,98 x 0,76 mm, 5 x 15 x 76 mm). En algunas implementaciones, la tarjeta inteligente 614 puede ser un llavero u otro testigo de seguridad. La tarjeta inteligente 614 puede incluir un sistema de seguridad con propiedades inviolables (por ejemplo,

un criptoprocesador de seguridad, un sistema de archivos seguro, características legibles por humanos) y/o puede configurarse para proporcionar servicios de seguridad (por ejemplo, confidencialidad de la información almacenada).

En algunas características de funcionamiento, la institución 506 puede comunicar de forma inalámbrica con el dispositivo anfitrión móvil 106 utilizando la red central celular 602. Por ejemplo, la institución 506 puede transmitir información al dispositivo anfitrión móvil 106 en respuesta, por lo menos, a un evento. La información puede incluir, por ejemplo, información de transacciones (por ejemplo, recepción de transacción, histórico de transacciones), archivos por lotes, aplicaciones, páginas web y/u otra información asociada con las instituciones 506. El evento puede incluir la compleción de la transacción, la determinación de que una tarjeta 104 de transacciones está fuera del rango operativo de un terminal de punto de acceso, la recepción de una petición procedente de un usuario del dispositivo anfitrión móvil y/u otros. Por ejemplo, la institución 506 puede identificar un dispositivo anfitrión móvil 106 asociado con una tarjeta 104 que ha ejecutado una transacción, y transmitir información de la transacción al dispositivo anfitrión móvil 106 utilizando la red central celular 602. Utilizando la red central celular 602, las instituciones 506 pueden transmitir información a la tarjeta 104 de transacciones sin requerir que haya un terminal de punto de acceso próximo a la tarjeta 104. Adicional o alternativamente, la institución 506 puede solicitar información al dispositivo anfitrión móvil 106, a la tarjeta 104 de transacciones y/o al usuario utilizando la red central celular 602. Por ejemplo, la institución 506 puede transmitir una solicitud del histórico de transacciones a la tarjeta 104, a través de la red central celular 602 y el dispositivo anfitrión móvil 106. En algunas implementaciones, el dispositivo anfitrión móvil 106c puede funcionar como un terminal de punto de venta (POS) móvil, configurado para ejecutar de forma inalámbrica transacciones con la tarjeta inteligente 614. Por ejemplo, un vendedor puede ser móvil (por ejemplo, un conductor de taxi) y puede incluir un dispositivo anfitrión móvil 106c con una tarjeta 104C de transacciones. En este ejemplo, la tarjeta 104C de transacciones puede recibir de forma inalámbrica información de la cuenta desde la tarjeta inteligente 614 y transmitir una petición de autorización a la institución 506 utilizando el dispositivo anfitrión móvil 106 y la red central celular 602.

En algunas implementaciones, el sistema 600 puede ejecutar uno o varios de los modos discutidos con respecto a la figura 5. Por ejemplo, la tarjeta 104 de transacciones puede volver a ser personalizada/ser actualizada utilizando la tecnología radioeléctrica celular del dispositivo anfitrión móvil 106. El usuario puede desear volver a personalizar la tarjeta 104 de transacciones para cambiar los dispositivos anfitriones, para tener múltiples dispositivos anfitriones y/o por otras razones. En relación con la gestión del dispositivo por soporte lógico, el usuario puede transmitir a la institución 506 una solicitud para volver a personalizar la tarjeta 104 de transacciones utilizando la tecnología radioeléctrica celular del dispositivo anfitrión 106.

La figura 7 es un diagrama de bloques que muestra un ejemplo de la tarjeta 104 de transacciones de la figura 1, de acuerdo con algunas implementaciones de la presente exposición. En general, la tarjeta 104 de transacciones incluye módulos personalizados que ejecutan transacciones financieras independientemente del dispositivo móvil 106. La tarjeta 104 de transacciones ilustrada tiene solamente una finalidad ejemplar, y la tarjeta 104 de transacciones puede incluir parte, la totalidad de los módulos, u otros diferentes sin apartarse del alcance de esta exposición.

En algunas implementaciones, la tarjeta 104 de transacciones puede incluir una capa 702 de interfaz, una API/UI 704, un servidor web 706, un marco de tiempo real 708, aplicaciones de transacciones 710, aplicaciones de valor añadido 712, credenciales de usuario 714, OS 716 de tiempo real, un conjunto de chips 718 para funcionamiento sin contacto, funciones 720 de control de la antena, la antena 722, una memoria 724 de instituciones y memoria libre 326. En algunas implementaciones, un controlador anfitrión incluye la capa 702 de interfaz, la API/UI 704, el servidor web 706, el marco 708 de tiempo real, el conjunto de chips 718 para funcionamiento sin contacto y las funciones 720 de control de la antena. En algunas implementaciones, un módulo de seguridad incluye las aplicaciones 710 de transacciones y las credenciales 714 del usuario. La memoria 724 de instituciones y la memoria libre 726 puede estar contenida en memoria flash. El algunas implementaciones, el conjunto de chips 718 para funcionamiento sin contacto puede estar integrado en el interior del módulo de seguridad o funcionar de forma independiente. La antena 722 puede consistir en circuitos electrónicos.

La capa 702 de interfaz incluye interfaces para el dispositivo anfitrión, es decir, conexión física, y para el mundo externo, es decir, conexión inalámbrica/sin contacto. En las implementaciones de pago, la conexión inalámbrica puede basarse en cualquier estándar inalámbrico adecuado, tal como sin contacto (por ejemplo, ISP 14443 A/B), de proximidad (por ejemplo, ISO 15693), NFC (por ejemplo, ISO 18092), y/u otros. En algunas implementaciones, la conexión inalámbrica puede utilizar otro protocolo inalámbrico de corto alcance, tal como Bluetooth, otras interfaces privadas utilizadas por terminales de pago minorista (Felica en Japón, MiFare en Asia, etc.) y/u otros. En relación con la interfaz física, la capa 702 de interfaz puede interactuar físicamente con el dispositivo móvil 106 utilizando un protocolo SD, tal como microSD, Mini-SD o SD (tamaño normal). En algunas implementaciones, la interfaz física puede incluir un convertidor/adaptador para la conversión entre dos protocolos diferentes en base, por lo menos en parte, al dispositivo móvil 106. En algunas implementaciones, el dispositivo móvil 106 puede comunicar utilizando protocolos tales como USB, MMC, interfaz privada iPhone u otras.

La capa API/UI 704 puede incluir cualquier soporte lógico, equipamiento físico y/o soporte lógico inalterable que funcione como una API entre el dispositivo móvil 106 y la tarjeta 104 de transacciones y como la GUI 111. Antes de ejecutar las transacciones, la tarjeta 104 de transacciones puede instalar automáticamente controladores en el dispositivo móvil 106 en respuesta, por lo menos, a su inserción. Por ejemplo, la tarjeta 104 de transacciones puede instalar automáticamente un controlador de dispositivo microSD en el dispositivo 110 para permitir a la tarjeta 104 de transacciones interactuar con el dispositivo móvil 106. En algunas implementaciones, la tarjeta 104 de transacciones puede instalar un controlador de dispositivo mejorado, tal como la API de memoria masiva con radio (MMR, Mass Memory with Radio). En esta implementación, la interfaz puede controlar una clase de complementos que contienen memoria masiva así como una interfaz radioeléctrica. La API MMR puede ejecutar una o varias de las siguientes acciones: conectar/desconectar con el controlador MMR (microcontrolador en el complemento); transferir datos utilizando el protocolo MM (por ejemplo, SD, MMC, XD, USB, Firewire); enviar datos cifrados al controlador MMR; recibir acuse de éxito o de error; recibir una palabra de estado que indica la descripción de un error; conectar/desconectar la radio; enviar una instrucción a la tarjeta 104 de transacciones para conectar la antena especificando el modo de funcionamiento (por ejemplo, modo de envío, modo de escucha); transmitir datos, tal como enviar una instrucción al controlador para transmitir datos mediante la radio; escuchar datos, tal como enviar una instrucción al controlador para escuchar datos; leer datos, tal como enviar una instrucción al controlador para enviar los datos recibidos por la radio en escucha; y/u otros. En algunas implementaciones, MMR puede ser compatible con TCP/IP. El algunas implementaciones, además de otros comandos el módulo de seguridad puede procesar órdenes ISO 110416 encapsuladas en API.

En algunas implementaciones, el API puede funcionar de acuerdo con los dos procesos: (1) la tarjeta 104 de transacciones como maestro y el dispositivo móvil 106 como esclavo; y (2) la UI de la tarjeta como maestro. En el primer proceso, la tarjeta 104 de transacciones puede pasar una o varias órdenes al dispositivo móvil 106 en respuesta, por ejemplo, a la introducción de la tarjeta 104 de transacciones en una ranura del dispositivo móvil 106, a una transacción entre la tarjeta 104 de transacciones y el punto de acceso 514, y/o a otros eventos. En algunas implementaciones, la tarjeta 104 de transacciones puede solicitar al dispositivo móvil 106 que ejecute una o varias de las funciones siguientes: obtener la entrada del usuario; obtener firma; mostrar datos; enviar datos; recibir datos; y/u otras. La orden de obtener la entrada del usuario puede presentar una solicitud de datos del usuario a través de la GUI 111. En algunas implementaciones, obtener la entrada del usuario puede presentar una solicitud de múltiples entradas de datos. Las entradas de datos pueden ser cualquier formato adecuado tal como numérico, alfanumérico y/u otras cadenas de caracteres. La orden obtener firma puede solicitar al dispositivo móvil 106 que devuelva datos de identificación tales como, por ejemplo, un número de teléfono, un ID del dispositivo, tal como un código IMEI o una dirección MAC, un código de red, un ID de abono, tal como el número de tarjeta SIM, un estado de conexión, información de posición, balizas Wi-Fi, datos GPS y/u otra información específica del dispositivo. La orden mostrar datos puede presentar un diálogo al usuario a través de la GUI 111. En algunas implementaciones, el diálogo puede desaparecer después de un período de tiempo, una selección del usuario y/u otro evento. La orden enviar datos puede solicitar al dispositivo móvil 106 transmitir datos en paquetes utilizando su propia conexión al mundo externo (por ejemplo, SMS, celular, Wi-Fi). La orden recibir datos puede solicitar al dispositivo móvil 106 abrir un canal de conexión con ciertos parámetros, e identificar datos recibidos a través de la conexión. En algunas implementaciones, la orden puede solicitar al dispositivo móvil 106 enviar algunos datos (por ejemplo, SMS) que satisfacen ciertos criterios para ser enviados a la tarjeta 104 de transacciones.

En relación con la UI como maestra, la UI puede ejecutar una o varias de las siguientes órdenes: orden/respuesta del módulo de seguridad; activar/desactivar; leer/escribir memoria flash; enviar datos con o sin cifrado; recibir datos con o sin descifrado; obtener datos URL/presentar datos URL; y/u otros. Las órdenes del módulo de seguridad pueden referirse a funciones de seguridad proporcionadas por la tarjeta y están dirigidas al módulo de seguridad en el interior de la tarjeta 104 de transacciones (por ejemplo, orden ISO 110416 estándar, órdenes privadas). En algunas implementaciones, las órdenes pueden incluir cifrado, autenticación, suministro de datos, creación de dominios de seguridad, actualización de dominios de seguridad, actualización de credenciales del usuario después de verificación de clave, y/u otras. En algunas implementaciones, las órdenes pueden incluir órdenes de tarjeta inteligente no relacionadas con la seguridad, tales como, por ejemplo, leer órdenes del histórico de transacciones. La orden del histórico de transacciones puede realizar una lectura de la memoria segura 724 de la tarjeta 104 de transacciones. En algunas implementaciones, después de la verificación de seguridad puede escribirse en ciertos indicadores o áreas de la memoria segura 124. La orden activar/desactivar puede activar o desactivar ciertas funciones de la tarjeta 104 de transacciones. La orden leer/escribir memoria flash puede ejecutar una operación de lectura/escritura en un área especificada de la memoria no segura 726. La orden enviar datos con o sin cifrado puede ordenar a la tarjeta 104 de transacciones transmitir datos utilizando su conexión inalámbrica, por ejemplo, con el punto de acceso 514. Además, los datos pueden ser cifrados mediante la tarjeta 104 de transacciones antes de la transmisión utilizando, por ejemplo, claves y capacidad de cifrado almacenadas en el interior del módulo de seguridad. La orden recibir datos con o sin descifrado puede indicar a la tarjeta 104 de transacciones que conmute al modo de escucha para recibir datos desde su conexión inalámbrica con el terminal/lector (por ejemplo, el punto de acceso 514). En algunas implementaciones, el descifrado de los datos puede ser solicitado por el módulo de seguridad utilizando, por ejemplo, algoritmos de descifrado y claves disponibles en el módulo de seguridad, es decir, descifrado incorporado. La orden obtener datos URL/presentar datos URL puede ordenar al servidor web 706 volver a páginas, según instrucciones de obtener o presentar fuera de línea, utilizando, por ejemplo, URLs fuera de línea.

El servidor web 706, como parte del OS de la tarjeta 104 de transacciones, puede asignar o bien asociar direccionamiento de tipo URL a ciertos archivos almacenados en la memoria 726 (por ejemplo, flash) de la tarjeta 104 de transacciones. En algunas implementaciones, el servidor web 706 localiza un archivo utilizando la URL y devuelve el archivo a un navegador utilizando transferencia de tipo HTTP, HTTPS estándar. En algunas implementaciones, la definición de los archivos puede formatearse utilizando lenguajes estándar de tipo HTML, XHTML, WML y/o XML. El archivo puede incluir enlaces que apuntan a emplazamientos adicionales de almacenamiento fuera de línea en la memoria 726 y/o a sitios de internet a los que puede acceder el dispositivo móvil 106. En algunas implementaciones, el servidor web 706 puede soportar protocolos de seguridad, tales como SSL. El servidor web 706 puede transferir una aplicación de la memoria 726 al dispositivo móvil 106 para su instalación y ejecución. El servidor web 706 puede consultar las capacidades del navegador en el dispositivo 110 utilizando, por ejemplo, el perfil del agente de usuario del navegador, para personalizar la página web fuera de línea en función de las capacidades soportadas del dispositivo y el navegador, tales como, por ejemplo, lenguaje de marcado soportado, tamaño de la pantalla, resolución, colores y otras semejantes.

Como parte del OS de tiempo real, el marco 708 de tiempo real puede ejecutar una o varias funciones en base, por lo menos en parte, a uno o varios períodos de tiempo. Por ejemplo, el marco 708 de tiempo real puede permitir que un reloj interno disponible en la CPU proporcione marcas de tiempo en respuesta, por lo menos, a eventos solicitados. El marco 708 de tiempo real puede permitir que ciertas tareas sean preprogramadas, de tal modo que las tareas son ejecutadas en respuesta, por lo menos, a ciertos iniciadores basados en el tiempo y/o en eventos. En algunas implementaciones, el marco 708 de tiempo real puede permitir que la CPU inserte retardos en ciertas transacciones. En alguna implementación, puede implementarse una parte de los estándares WAP denominada WTAI (Wireless Telephony Application Interface, interfaz de aplicación de telefonía inalámbrica) para permitir que las páginas del navegador fuera de línea en la tarjeta 104 utilicen las funciones ofrecidas por el dispositivo móvil 106 (por ejemplo, enviar/recibir datos inalámbricos, enviar/recibir SMS, realizar una llamada de voz, reproducir un tono de llamada, etc.).

Las aplicaciones 710 de transacciones pueden incluir cualquier soporte lógico, equipamiento físico y/o soporte lógico inalterable que intercambie información de transacciones con instituciones utilizando, en algunos casos, un formato de datos y/o de secuencia predefinido. Por ejemplo, las aplicaciones 710 de transacciones pueden generar una respuesta a una solicitud de transacción seleccionando, extrayendo o sino incluyendo credenciales del usuario en la respuesta, en un formato compatible con una aplicación de procesamiento en los puntos de acceso. En algunas implementaciones, las aplicaciones 710 de transacciones pueden ejecutar una o varias de las siguientes acciones: transmitir propiedades de la tarjeta 104 de transacciones en respuesta, por lo menos, a una solicitud de identificación recibida desde el punto de acceso 514; recibir una solicitud para ejecutar una transacción, por ejemplo, desde el punto de acceso 514; identificar credenciales del usuario en la memoria 724 de instituciones en respuesta, por lo menos, a la solicitud; generar una respuesta de transacción en base, por lo menos en parte, a las credenciales del usuario; transmitir la respuesta de transacción al punto de acceso 514 utilizando, por ejemplo, un conjunto de chips para funcionamiento sin contacto; recibir datos libres, por ejemplo un numero aleatorio, desde el punto de acceso 514 y proporcionar una respuesta que contiene datos cifrados, mediante cifrar los datos libres utilizando las capacidades criptográficas del elemento seguro; transmitir los datos cifrados utilizando el conjunto de chips 718 para funcionamiento sin contacto; incrementar un contador de transacciones con cada solicitud de transacción recibida; transmitir un valor al contador de transacciones, en respuesta a una solicitud procedente del punto de acceso 514; memorizar detalles de la transacción solicitada recibida desde el punto de acceso 514, en el área del histórico de transacciones de la memoria 724 de instituciones; transmitir el histórico de transacciones a la CPU de la tarjeta inteligente 104, en respuesta a una solicitud de este tipo; recibir solicitudes ISO 110416 desde la CPU de la tarjeta inteligente 104; ejecutar transacciones correspondientes utilizando el OS del elemento seguro; devolver respuestas a la CPU; y/u otros procesos. En la generación de la respuesta a la transacción, la aplicación 710 de transacciones puede generar la respuesta en un formato especificado por la red asociada con una institución 506, o en un formato privado perteneciente a la institución 506 y definido por la misma, y procesable por el punto de acceso 514. La solicitud de transacción puede incluir uno o varios de los elementos siguientes: credenciales del usuario (por ejemplo, número de cuenta); datos de expiración, números de verificación de la tarjeta; cuenta de transacciones; y/u otra información de la tarjeta o el usuario. En algunas implementaciones, la aplicación 710 de transacciones puede comprender una aplicación de navegador para permitir las transacciones. La aplicación 710 de navegador puede consistir en un navegador que puede ser instalado si el dispositivo 106 carece de navegador o tiene uno incompatible con el servidor web 706 de la tarjeta 104. Después de la instalación de dicho navegador 710, las comunicaciones futuras entre el dispositivo móvil 106 y el servidor web 706 hacen uso del navegador recién instalado.

El OS 716 de tiempo real puede ejecutar, o en todo caso incluir, uno o varios de los siguientes: marco 708 de tiempo real; un procesador anfitrión que implementa la interfaz física entre la CPU de la tarjeta de transacciones y el dispositivo móvil 106; una interfaz que implementa la interfaz física entre la CPU de la tarjeta de transacciones y el módulo de seguridad; un proceso de gestión de memoria que implementa la interfaz física ISO 110416 entre la CPU de la tarjeta de transacciones y la memoria 724 y/o 726; un proceso de la capa de aplicaciones que implementa las capacidades API y UI; el servidor web 706; funciones 720 de control de la antena; gestión de la energía; y/u otros. En algunas implementaciones, el OS 716 de tiempo real puede gestionar la interfaz física entre la CPU de la tarjeta

de transacciones y la memoria segura 724, que incluye segmentación de la memoria para permitir que ciertas áreas de la memoria sean de acceso limitado y/o conductos/memorias intermedias de datos. En algunas implementaciones, el módulo de seguridad puede incluir un OS del módulo de seguridad proporcionado por el fabricante del módulo de seguridad y puede ser compatible con especificaciones Visa y MasterCard. El OS del módulo de seguridad puede estructurar los datos del módulo de seguridad para que sean compatibles con especificaciones Paypass y/o payWave o con cualesquiera otras especificaciones disponibles en la industria de pago minorista sin contacto. Además, el módulo de seguridad puede almacenar firmas del dispositivo anfitrión y permitir modos de la antena 722 en la memoria segura 724. En algunas implementaciones, el OS 716 de tiempo real puede incluir un OS del microcontrolador configurado para personalizar la memoria segura 724 tal como, por ejemplo, transformando datos FV en bruto (número de cuenta, fecha de expiración, número de verificación de la tarjeta (CVN, Card Verification Number), u otros detalles específicos de aplicación) en información cifrada segura. Además, el OS del microcontrolador puede presentar al dispositivo anfitrión la tarjeta 104 como un almacenamiento masivo microSD. El OS del microcontrolador puede dividir la memoria en una sección del usuario y una sección protegida para aplicaciones del dispositivo. En este ejemplo, la sección para aplicaciones del dispositivo puede utilizarse para almacenar aplicaciones específicas del proveedor que funcionan desde este segmento de la memoria o son instaladas en el dispositivo anfitrión desde este segmento de la memoria.

El chip del módulo de seguridad puede proporcionar funciones de seguridad del equipamiento físico antiviolación para cifrado, autenticación, gestión de credenciales de usuario utilizando múltiples dominios de seguridad, capacidades de procesamiento incorporadas para personalización, acceso y almacenamiento, y/u otras. En algunas implementaciones, el chip del módulo de seguridad puede incluir el conjunto de chips 718 para funcionamiento sin contacto.

El conjunto de chips 718 para funcionamiento sin contacto puede proporcionar la implementación del protocolo de equipamiento físico y/o controladores para la comunicación de RF. Por ejemplo, el conjunto de chips 718 para funcionamiento sin contacto puede incluir circuitos RF incorporados, para interactuar con una conexión con el mundo externo utilizando una conexión inalámbrica/sin contacto. La conexión sin contacto puede ser, por ejemplo, cliente a nodo (terminal/lector/estación base), nodo a cliente (etiqueta pasiva), o entre pares (otra tarjeta 104 de transacciones).

La función 720 de control de la antena puede controlar la disponibilidad de la antena de RF. Por ejemplo, la función 720 de control de la antena puede activar/desactivar la antena 722 en respuesta, por ejemplo, a una autenticación satisfactoria, a la compleción de una rutina establecida por el OS 716, y/o a otro evento. La antena 722 puede ser una antena inalámbrica de corto alcance conectada a un inserto NFC a través de un conmutador de soporte lógico, tal como una puerta NAND u otro elemento.

El sistema 728 de gestión de cartera puede conmutar selectivamente entre múltiples credenciales 714 cuando ejecuta transacciones. Por ejemplo, el sistema 728 de gestión de cartera puede identificar una cuenta por defecto, normas de conmutación y/u otra información. En algunas implementaciones, el sistema 728 de gestión de cartera puede conmutar automáticamente a credenciales de usuario por defecto en respuesta, por lo menos, a un evento tal como la compleción de una transacción utilizando credenciales no por defecto. Las normas de conmutación pueden identificar credenciales de usuario y eventos asociados, de tal modo que el sistema 728 de gestión de cartera conmuta a las credenciales de usuario en respuesta, por lo menos, a la determinación de un evento.

La figura 8 es un diagrama de bloques que muestra un ejemplo de tarjeta inteligente 800, de acuerdo con algunas implementaciones de la presente exposición. Por ejemplo, la tarjeta de transacciones de la figura 1 puede implementarse de acuerdo con la tarjeta inteligente 800 mostrada. En general, la tarjeta inteligente 800 puede acceder independientemente a servicios y/o transacciones. La tarjeta inteligente 800 tiene solamente propósitos ilustrativos y puede incluir parte, la totalidad de los elementos u otros diferentes, sin apartarse del alcance de la exposición.

Tal como se muestra, la tarjeta inteligente 800 incluye una antena 802, un circuito 804 de sintonización más conmutador, un conjunto de chips 806 para funcionamiento sin contacto y módulo de seguridad, una CPU 808 y la memoria 810. La antena 802 transmite y recibe de forma inalámbrica señales, tal como señales NFC. En algunas implementaciones, el circuito 804 de sintonización más conmutador puede ajustar dinámicamente la impedancia de la antena 802 para sintonizar la frecuencia de transmisión y/o recepción. Además, el circuito 804 de sintonización más conmutador puede selectivamente conectar y desconectar la antena 802 en respuesta, por lo menos, a una orden procedente de la CPU 808. En algunas implementaciones, la antena 802 puede ser una antena inalámbrica de corto alcance conectada a un inserto NFC a través de un conmutador de soporte lógico, tal como una puerta NAND u otro elemento, para permitir encender y apagar la antena 802 mediante código desde la CPU 808. En algunas implementaciones, la tarjeta 800 puede incluir un inserto NFC (no mostrado) que puede ser una implementación pasiva de tecnología inalámbrica de corto alcance NFC, que obtiene potencia del terminal lector para transmitir datos de vuelta, o una implementación más potente que utiliza un conjunto de chips eNFC para activar el modo de lector activo y el modo de auto-aprendizaje. Además, la tarjeta 800 puede incluir un reseteo externo por punta de aguja (no mostrado) que da lugar a que la CPU 808 despersonalice la memoria o el elemento seguro.

La CPU 808 puede transmitir el comando de conmutación en respuesta a un evento, tal como una solicitud del usuario, la compleción de una transacción y/u otros. Cuando es activado, el conjunto de chips 806 para funcionamiento sin contacto y módulo de seguridad es conectado a la antena 802 y ejecuta una o varias de las siguientes acciones: formatea señales para comunicación inalámbrica de acuerdo con uno o varios formatos; descifra mensajes recibidos y cifra mensajes transmitidos; auténtica credenciales de usuario almacenadas localmente en la memoria 810; y/u otros procesos. La memoria 810 puede incluir secciones seguras y no seguras. En esta implementación, la memoria segura 810 puede almacenar una o varias credenciales de usuario que no son accesibles por el usuario. Además, la memoria 810 puede almacenar páginas web fuera de línea, aplicaciones, histórico de transacciones y/u otros datos. En algunas implementaciones, la memoria 810 puede incluir memoria flash entre 64 MB y 32 GB. Además, la memoria 810 puede dividirse en memoria para el usuario y memoria para aplicaciones del dispositivo. El conjunto de chips 806 puede incluir un módulo de seguridad que está, por ejemplo, certificado por Visa y/o MasterCard para almacenar datos de vehículos financieros, y/o según estándares globales. Además de un vehículo financiero del usuario, el elemento seguro puede almacenar firmas de dispositivos anfitriones permitidos y/o modos de antena.

En algunas implementaciones, la CPU 808 puede conmutar la antena 802 entre un modo activo y otro inactivo en base, por lo menos en parte, a un parámetro de personalización definido, por ejemplo, por un usuario, un distribuidor (por ejemplo, una institución financiera, un proveedor de servicios) y/u otros. Por ejemplo, la CPU 808 puede activar la antena 802 cuando la tarjeta inteligente 800 está conectada físicamente a un dispositivo central y cuando se ejecuta satisfactoriamente un establecimiento de comunicación con el dispositivo anfitrión. En algunas implementaciones, la CPU 808 puede desactivar automáticamente la antena 802 cuando la tarjeta inteligente 800 es extraída del dispositivo anfitrión. En algunas implementaciones, la antena 802 está siempre activa, de tal modo que la tarjeta inteligente 800 puede utilizarse como un dispositivo de acceso independiente (por ejemplo, un dispositivo en un llavero). En relación con el proceso de establecimiento de la comunicación, la CPU 808 puede ejecutar uno o varios procesos de autenticación antes de la activación de la tarjeta inteligente 800 y/o de la antena 802, tal como se muestra en la figura 7. Por ejemplo, la CPU 808 puede ejecutar una autenticación física, una autenticación del dispositivo y/o un autenticación del usuario. Por ejemplo, la CPU 808 puede activar la antena 802 en respuesta, por lo menos, a la detección de una conexión a la interfaz física con el dispositivo anfitrión (por ejemplo, interfaz SD) y la instalación satisfactoria del controlador del dispositivo para el acceso de memoria masiva (por ejemplo, un controlador del dispositivo SD) en el dispositivo anfitrión. En algunas implementaciones, la autenticación del dispositivo puede incluir la autenticación física, además de una comparación de firmas entre una firma del dispositivo almacenada en la memoria (por ejemplo, módulo de seguridad (SE, security module)) que fue creada durante la primera utilización (entrega) y una firma en tiempo de ejecución calculada utilizando, por ejemplo, un parámetro único del dispositivo anfitrión. En el caso de que no exista ninguna firma del dispositivo anfitrión en la memoria, la CPU 808 puede ser vinculada al primer dispositivo anfitrión compatible en el que es insertada la tarjeta 800. Un dispositivo anfitrión compatible puede ser un dispositivo que consiga satisfactoriamente la autenticación física. Si en la memoria existe una firma del dispositivo anfitrión, la CPU 808 compara la firma almacenada con la firma en tiempo real del dispositivo anfitrión actual. Si las firmas coinciden, la CPU 808 puede completar la operación de inicialización. Si las firmas no coinciden, el dispositivo anfitrión es rechazado, la inicialización es abortada y la tarjeta 800 se devuelve al modo en el que estaba antes de ser insertada en el dispositivo.

La autenticación del usuario puede incluir la verificación de la conexión física con un usuario utilizando un PIN introducido por el usuario, un certificado de tipo x.509 que es único para el usuario y está almacenado en el dispositivo anfitrión, y/u otros procesos. La autenticación del dispositivo y del usuario puede verificar una conexión física con el dispositivo mediante la comparación de una firma del dispositivo y la autenticación del usuario mediante la verificación de un certificado o un PIN del usuario. En algunas implementaciones, el usuario puede seleccionar un PIN o un certificado en el momento del suministro. En este caso, la CPU 808 puede invocar un complemento de soporte lógico en el dispositivo anfitrión. Por ejemplo, un componente de soporte lógico puede solicitar el usuario su PIN en tiempo real, leer un certificado del usuario instalado en el dispositivo (por ejemplo, x.509), y/u otros. El funcionamiento del complemento de soporte lógico puede ser personalizado por el proveedor. Independientemente, los datos del usuario devueltos pueden compararse con los datos del usuario almacenados en la memoria. En el caso de una comparación satisfactoria, la antena 802 puede ser activada. En el caso de una comparación fallida de un certificado, la tarjeta 800 es desactivada. En caso de comparación de PIN fallida, puede solicitarse al usuario que repita intentos con el PIN hasta que se produce una comparación satisfactoria o el número de intentos supera un umbral. El proveedor del disco puede personalizar el umbral de intentos.

En relación con la autenticación de red, el dispositivo anfitrión puede ser un teléfono móvil, de tal modo que la tarjeta 800 puede solicitar la autenticación de red antes de la activación. Por ejemplo, la tarjeta 800 puede ser distribuida por un operador de red inalámbrica (WNO, Wireless Network Operator) que requiere autenticación de red. En este ejemplo, puede ser activado (ON) un indicador en memoria para indicar que es necesaria la autenticación de red. Si el indicador está activado, una identidad única relativa a la red permitida es almacenada localmente en la memoria, tal como un código de red móvil para redes GSM, un NID para redes CDMA, un SSID para redes de banda ancha y/u otros identificadores. Si el indicador está activado, la CPU 808, en respuesta por lo menos a la inserción, puede solicitar que sea descargado al dispositivo anfitrión un complemento especial de soporte lógico, e invocado. El complemento de soporte lógico puede solicitar al dispositivo anfitrión que responda con detalles de la red. En

algunos casos, la identidad de red única utilizada y el método para deducirla del dispositivo anfitrión pueden ser variables y dependientes del proveedor de red y de la capacidad del dispositivo anfitrión. Si el ID almacenado localmente coincide con el ID solicitado, la CPU 806 activa la antena 802 para permitir el acceso, y en caso contrario los servicios son denegados.

La figura 9 muestra un ejemplo del sistema 900 de transacciones para comunicar de forma inalámbrica información de transacciones utilizando una entre una serie de interfaces. Por ejemplo, el sistema 900 puede interactuar con la tarjeta 104 de transacciones utilizando una interfaz cableada o inalámbrica. En relación con las interfaces cableadas, el sistema 900 incluye un adaptador 904 y un receptor 906. El adaptador 904 puede incluir cualquier soporte lógico, equipamiento físico y/o soporte lógico inalterable configurado para traducir entre un formato compatible con la tarjeta 104 y un formato compatible con el cliente 504c. Por ejemplo, el adaptador 904 puede traducir entre protocolo microSD y un protocolo USB. El lector 906 puede incluir cualquier soporte lógico, equipamiento físico y/o soporte lógico inalterable configurado para interactuar directamente con la tarjeta 104b. Por ejemplo, el lector 906 puede ser un lector microSD, tal que el cliente 504d interactúa con la tarjeta 104b utilizando protocolo microSD. En relación con las interfaces inalámbricas, el sistema 900 puede incluir una interfaz celular 902 y una interfaz inalámbrica de corto alcance 908. En relación con la interfaz celular 902, las instituciones 106 pueden comunicar de forma inalámbrica con la tarjeta 104e de transacciones utilizando la tecnología radioeléctrica celular del dispositivo móvil 106e. Por ejemplo, la interfaz celular 902 puede ser una interfaz CDMA, una interfaz GSM, una interfaz UMTS y/u otras interfaces celulares. En relación con la interfaz inalámbrica de corto alcance 908, las instituciones 106 pueden comunicar de forma inalámbrica con la tarjeta 104f de transacciones utilizando, por ejemplo, tecnología Wi-Fi. La interfaz inalámbrica de corto alcance 908 puede ser una interfaz 1602.11, una interfaz Bluetooth y/u otra interfaz inalámbrica. En estas implementaciones, el cliente 504e puede incluir un transceptor utilizado para comunicación inalámbrica con la tarjeta 104f de transacciones.

La figura 10 es un diagrama esquemático 1000 de personalización de una tarjeta inteligente (por ejemplo, tarjeta de transacciones, tarjeta de memoria). En particular, la tarjeta inteligente puede ser personalizada antes de su emisión a un usuario, es decir, pre-emisión, o después de ser emitida un usuario, es decir, post-emisión. En relación con la pre-emisión, las tarjetas inteligentes pueden ser personalizadas en masa por lotes, por ejemplo en una fábrica. En este ejemplo, cada tarjeta inteligente puede ser cargada con credenciales del usuario, marco de seguridad, aplicaciones, páginas web fuera de línea y/u otros datos. En algunas implementaciones, una tarjeta inteligente puede personalizarse individualmente, por ejemplo, en una sucursal bancaria. En este caso, una tarjeta inteligente puede ser cargada individualmente con datos asociados con un usuario, por ejemplo, después de la compra del disco. En relación con la post-personalización, la tarjeta inteligente puede ser personalizada de forma inalámbrica. Por ejemplo, la tarjeta 104 de transacciones puede ser personalizada a través de una conexión celular establecida utilizando el dispositivo móvil 106. En algunas implementaciones, una tarjeta inteligente puede ser personalizada mediante su sincronización con un ordenador, tal como el cliente 504. La tarjeta 104 de transacciones puede recibir de, por lo menos, una empresa asociada con la institución 506, aquellos datos de personalización previos a la activación que incluyen credenciales del usuario, aplicación de pago y, por lo menos, uno entre indicadores operacionales, lista de normas o interfaz del usuario. Los datos de personalización presentes en la tarjeta pueden ser actualizados después de la activación utilizando, por lo menos, uno entre los métodos siguientes: mensajes inalámbricos o aéreos que contienen instrucciones de actualización especiales y seguras; aplicación cliente de internet que se ejecuta en un PC conectado a la tarjeta 104 de transacciones a través del dispositivo anfitrión o de un lector de tarjetas; aplicación de internet que se conecta de forma inalámbrica a la tarjeta 104 de transacciones a través del dispositivo móvil anfitrión o aplicación de interfaz del usuario de la propia tarjeta 104 de transacciones; y/u otros métodos.

En algunas implementaciones, la provisión de la tarjeta inteligente puede basarse, por lo menos en parte, en la entidad de distribución (por ejemplo, institución financiera, operador inalámbrico, usuario). Por ejemplo, la tarjeta inteligente puede ser distribuida mediante una institución financiera, tal como un banco. En la implementación por banco, la tarjeta inteligente puede ser provisionada por adelantado con las cuentas del usuario. En este caso, la tarjeta inteligente puede ser activada en respuesta, por lo menos, a su inserción inicial en un dispositivo anfitrión. El modo de antena puede configurarse como autenticación física solamente por defecto. En algunos ejemplos, el usuario puede auto-seleccionar una autenticación por PIN para impedir el uso no autorizado, o mediante un soporte conmutador de PC y un soporte lógico de administración de complementos, si el dispositivo anfitrión no tiene una pantalla y un teclado. En la implementación por operador-inalámbrica, la tarjeta inteligente puede requerir autenticación del dispositivo antes de la activación. En algunos ejemplos, el usuario puede proporcionar datos financieros (por ejemplo, crédito o débito) utilizando uno entre varios métodos. Además, el usuario puede añadir autenticación de usuario. En la implementación proporcionada por el usuario, el usuario puede adquirir la tarjeta inteligente, por ejemplo, en un comercio minorista o través de otros canales tales como fabricantes de dispositivos anfitriones OEM. En este caso, el usuario puede activar la tarjeta mediante una serie de diferentes dispositivos con provisionamiento seleccionado por operador.

En relación con la activación para transacciones financieras, la tarjeta inteligente puede estar configurada en el modo memoria cuando el usuario adquiere el disco, por ejemplo en un banco, en un operador inalámbrico, en un proveedor de tercera parte y/o en otros. La activación de la tarjeta puede incluir los siguientes dos niveles: 1)

físicamente, especificando la disponibilidad de la antena bajo un conjunto específico de circunstancias deseadas por el proveedor; y 2) lógicamente, en la institución financiera que representa la activación del vehículo financiero soportado en la tarjeta. En algunas implementaciones, la activación puede basarse, por lo menos en parte, en el distribuidor del dispositivo, en la selección de disponibilidad de la antena, y/o en el tipo de dispositivo anfitrión, tal como se muestra en la siguiente tabla 1.

Tabla 1:

Vendedor del complemento y modo de distribución	Estado inicial del complemento y opción de la disponibilidad de la antena	El dispositivo no tiene pantalla/teclado	El dispositivo tiene pantalla y teclado
FI: la institución financiera (banco o minorista) envía el complemento directamente al abonado a través de revendedores/ distribuidores/ etc. participantes.	El complemento está en modo de memoria. Está completamente personalizado con la información de cuenta (FV) del usuario y el modo de antena está configurado para autenticación física	Manual: el usuario tiene que llamar al número de la FI para activar su cuenta, el dispositivo puede solamente funcionar con una sola cuenta. El usuario puede acceder asimismo al sitio de la FI en internet utilizando otro PC para activar su cuenta.	Si el dispositivo está capacitado para acceso inalámbrico, tras la inserción el complemento genera una página web y lleva el usuario al sitio web de la FI. El propio usuario activa su cuenta introduciendo su número de cuenta y proporcionando información personal secreta (últimos 4 dígitos del SSN o del número de teléfono de su domicilio, por ejemplo). Opcionalmente, el usuario puede asimismo seleccionar un PIN (cambiar disponibilidad de la antena a autenticación de usuario) al mismo tiempo. Si no está disponible una conexión a internet, el dispositivo puede marcar automáticamente una llamada de voz al número de la FI para la activación de la cuenta. Si no está disponible tampoco una conexión inalámbrica (el dispositivo es solamente una PDA), el usuario tiene que recurrir a la activación manual (de la izquierda).

Vendedor del complemento y modo de distribución	Estado inicial del complemento y opción de la disponibilidad de la antena	El dispositivo no tiene pantalla/teclado	El dispositivo tiene pantalla y teclado
WNO: el operador de la red inalámbrica (Wireless Network Operator) envía el complemento conjuntamente con el dispositivo anfitrión. El usuario puede seleccionar su dispositivo anfitrión preferido y el complemento es acoplado con éste si el usuario lo desea, para aprovechar este servicio.	El complemento está en modo memoria, está parcialmente personalizado (la firma de dispositivo del dispositivo anfitrión está cargada para impedir que el usuario cambie de dispositivo anfitrión) no estando cargada la información de FV. La disponibilidad de la antena está configurada como autenticación del dispositivo (el complemento puede ser utilizado solamente con el dispositivo anfitrión con el que es enviado).	No aplicable	Hipótesis: el dispositivo tiene una conexión inalámbrica funcional. El operador ofrece una aplicación de gestión de cartera incorporada. Cuando el usuario hace clic sobre la aplicación de gestión de cartera, el usuario es invitado a registrarse con la FI asociada del operador para una nueva cuenta. Cuando el registro se ha realizado satisfactoriamente, los datos de la cuenta son descargados al complemento de manera aérea o a través de internet, y se activa la utilización del mismo. El dispositivo puede utilizar múltiples FI en este escenario, y almacenar múltiples FVs. El usuario puede seleccionar introducir un PIN para un FV en la aplicación de gestión de cartera, para transformar la disponibilidad de la antena a autenticación del usuario y del dispositivo para dicho FV. El complemento está supeditado a la firma del dispositivo. Cuando es extraído del dispositivo, la antena se desconecta y el complemento se transforma en una simple barra de memoria masiva. Cuando el complemento es insertado en otro dispositivo anfitrión, la firma no coincide y la antena permanece desconectada.

Vendedor del complemento y modo de distribución	Estado inicial del complemento y opción de la disponibilidad de la antena	El dispositivo no tiene pantalla/teclado	El dispositivo tiene pantalla y teclado
WNO: el operador de red inalámbrica envía un complemento como accesorio, con un aviso sobre los dispositivos compatibles. El usuario puede seleccionar su dispositivo anfitrión preferido, e intentar que funcione su complemento con el mismo, para hacer uso del servicio.	El complemento está en modo memoria, no está personalizado. La disponibilidad de la antena está configurada como autenticación de red. El complemento estará ligado al primer dispositivo en el que es insertado y en el que su autenticación es satisfactoria.	No aplicable	Hipótesis: el dispositivo tiene conexión inalámbrica funcional. El complemento generará una conexión de internet con un portal del operador y, tras la conformación del usuario, se descargará la aplicación de gestión de cartera. El usuario puede rechazar la descarga y elegir la provisión manual de datos FV yendo a un proveedor de cartera de tercera parte, o directamente al sitio de la FI. El complemento está supeditado al dispositivo y a la red del proveedor de red. Si el mismo dispositivo es desbloqueado y utilizado en otra red, el complemento dejará de funcionar y volverá al modo memoria. Cuando es extraído del dispositivo, el complemento volverá al modo memoria.
OEM 1: fabricante del teléfono móvil	Autenticación del dispositivo (el dispositivo viene acoplado a un teléfono móvil)	No aplicable	Opción A: el fabricante del dispositivo presenta una aplicación de gestión de cartera, el resto de los procesos son como en el caso de arriba. Opción B: el operador inalámbrico ofrece una aplicación de gestión de cartera. El usuario se dirige al portal del operador inalámbrico y descarga esta aplicación de manera aérea. El resto del proceso es igual que el caso de arriba. Opción C: el usuario navega a una aplicación de gestión de cartera de tercera parte (por ejemplo, Paypal o Google). Se ofrece el registro a las FI participantes y se personalizan los FV en el complemento sobre la red internet. Opción D: el usuario navega al sitio web de la FI y activa una nueva cuenta, que es personalizada por internet en el complemento.

Vendedor del complemento y modo de distribución	Estado inicial del complemento y opción de la disponibilidad de la antena	El dispositivo no tiene pantalla/teclado	El dispositivo tiene pantalla y teclado
OEM 2: otro fabricante	Autenticación del dispositivo	El usuario tiene que conectar mediante un soporte conmutador el dispositivo al PC con conexión a internet, y registrarse en el PC yendo para ello directamente al sitio web de una FI. La cuenta es descargada por internet a través del soporte conmutador, y a continuación el dispositivo es activado. En este proceso, el complemento queda supeditado a la firma del dispositivo. Cuando es extraído del dispositivo anfitrión, las antena se desconecta. Cuando es conectado en otro dispositivo, la firma del dispositivo falla y éste se comporta solamente como un dispositivo de memoria masiva.	Si el dispositivo tiene conexión inalámbrica (es una PDA inalámbrica): igual que el caso de arriba. Si el dispositivo no tiene conexión inalámbrica (es una PDA sin conexión): igual que el caso de la izquierda.

El diagrama mostrado es solamente a modo de ejemplo. El usuario puede activar una tarjeta inteligente utilizando todos, algunos de los anteriores o diferentes procesos, sin apartarse del alcance de esta exposición.

En las implementaciones mostradas, la tarjeta 104 de transacciones puede ser mejorada para ejecutar un sistema de cartera utilizando múltiples credenciales de usuario. Por ejemplo, la tarjeta 104 de transacciones puede ser mejorada con el sistema 728 de gestión de cartera, a través de una conexión inalámbrica o cableada. Además de mejorar la tarjeta 104 de transacciones, pueden cargarse en la memoria credenciales de usuario adicionales. En este caso, la tarjeta 104 de transacciones puede conmutar selectivamente entre diferentes credenciales de usuario en base, por lo menos en parte, a normas, selecciones del usuario, eventos y/u otros aspectos.

La figura 11 es un diagrama de flujo que muestra un método 1100, a modo de ejemplo, para la inicialización automática de la tarjeta inteligente en respuesta, por lo menos, a su introducción en un dispositivo anfitrión. En general, una tarjeta inteligente puede ejecutar uno o varios procesos de autenticación antes de la activación. Muchas de las etapas en este diagrama de flujo pueden tener lugar simultáneamente y/o en órdenes diferentes a los mostrados. El sistema 500 o el sistema 600 pueden utilizar métodos con etapas adicionales, menos etapas y/o etapas diferentes, siempre que los métodos sigan siendo apropiados.

El método 1100 comienza en la etapa 1102, en la que se detecta una cubierta acoplada a un dispositivo anfitrión. Por ejemplo, la tarjeta 104 de transacciones puede detectar la inserción en el dispositivo móvil 106. Si no se requiere autenticación para ningún aspecto de la tarjeta inteligente, la ejecución finaliza en la etapa de decisión 1104. Si se requiere autenticación por lo menos para un aspecto, entonces la ejecución pasa a la etapa de decisión 1106. Si la comunicación con el dispositivo anfitrión incluye uno o varios errores, entonces se indica un fallo al usuario en la etapa 1108. En el ejemplo, la tarjeta 104 de transacciones puede presentar al usuario una indicación de un error de comunicación utilizando la GUI 111. Si no se detecta un error de comunicación en la etapa de decisión 1106, entonces la ejecución pasa a la etapa de decisión 1110. En algunas implementaciones, la tarjeta inteligente carga un controlador de SD en el dispositivo anfitrión. Si la tarjeta inteligente requiere solamente autenticación física, entonces la ejecución pasa a la etapa de decisión 1104. Si el indicador de autenticación de red no está activado entonces, en la etapa 1114, la antena es conectada y la tarjeta inteligente es actualizada con la firma del dispositivo anfitrión. A modo de ejemplo, la tarjeta 104 de transacciones puede activar la antena para transacciones inalámbricas y actualizar la memoria local con la firma del dispositivo anfitrión. Si el indicador de autenticación de red está activado en la etapa de decisión 1104 entonces, en la etapa 1116, la tarjeta inteligente transmite una solicitud del ID de red al dispositivo anfitrión. A continuación, en la etapa 1118, la tarjeta inteligente recibe un ID de red almacenado localmente. Si en la etapa de decisión 1120 el ID de red almacenado y el ID de red solicitado coinciden, entonces el disco es activado en la etapa 1122. Si los dos ID de red no coinciden, entonces la antena es desactivada en la etapa 1114.

Haciendo referencia a la etapa de decisión 1110, si la autenticación es no solamente autenticación física, entonces la ejecución pasa a la etapa de decisión 1124. Si el proceso de autenticación incluye autenticación del dispositivo entonces, en la etapa 1126, la tarjeta inteligente transmite una petición de un ID de red al dispositivo anfitrión. En la etapa 1128, la tarjeta inteligente recupera firmas de dispositivo almacenadas localmente. Si la tarjeta inteligente no incluye por lo menos una firma del dispositivo, entonces la ejecución pasa a la etapa de decisión 1134. Si la tarjeta inteligente incluye una o varias firmas de dispositivo, entonces la ejecución pasa a la etapa de decisión 1132. Si una de las firmas del dispositivo coincide con el ID de red solicitado, entonces la ejecución pasa a la etapa de decisión 1134. Si las firmas y el ID de red solicitado no coinciden, entonces la ejecución pasa a la etapa 1122 para la desactivación. Si la autenticación de usuario no está incluida en el proceso de autenticación, entonces la ejecución pasa a la etapa de decisión 1112 para la autenticación física. Si la autenticación del usuario está incluida en la etapa de decisión 1134, entonces la ejecución pasa a la etapa 1138.

De nuevo haciendo referencia a la etapa de decisión 1124, si el proceso de autenticación no incluye autenticación del dispositivo, entonces la ejecución pasa a la etapa de decisión 1136. Si la autenticación del usuario no está incluida en el proceso entonces, en la etapa 1122, la tarjeta inteligente es desconectada. Si la autenticación del usuario está incluida entonces, en la etapa 1138, la tarjeta inteligente solicita un número de PIN al usuario utilizando el dispositivo anfitrión. Si bien la autenticación del usuario se describe con respecto a la introducción de un PIN a través del dispositivo anfitrión móvil, el usuario puede ser autenticado utilizando otra información tal como información biométrica (por ejemplo, huellas digitales). De nuevo haciendo referencia al ejemplo, la tarjeta 104 de transacciones puede presentar una solicitud al usuario para introducir un PIN a través de la GUI 111. En la etapa 1140, la tarjeta inteligente recupera un PIN almacenado localmente. Si en la etapa de decisión 1142 el PIN solicitado y el PIN almacenado coinciden, entonces la ejecución pasa a la etapa de decisión 1104 para la autenticación física. Si en la etapa de decisión 1142 el PIN solicitado y el PIN almacenado no coinciden, entonces la ejecución pasa a la etapa de decisión 1124. Si el número de intentos no ha superado un umbral especificado, entonces la ejecución vuelve a la etapa 1138. Si el número de intentos ha superado el umbral, entonces la antena es desactivada en la etapa 1122. En el ejemplo, en el caso de que la tarjeta 104 de transacciones no consiga autorizar el dispositivo, la red y/o el usuario, la tarjeta 104 de transacciones puede transmitir de forma inalámbrica una indicación a la institución financiera asociada, utilizando la tecnología radioeléctrica celular del dispositivo anfitrión móvil 110. En este caso, el método mostrado 1100 puede ser implementado como un proceso de control de fraude, para impedir sustancialmente la utilización no autorizada de la tarjeta 104 de transacciones.

La figura 12 es un flujo de llamada 1200 a modo de ejemplo, acorde con algunas implementaciones de la presente exposición. Tal como se muestra, el flujo 1200 incluye una red 1202, un dispositivo anfitrión 1204, una tarjeta inteligente 1206 y un terminal 1208. El dispositivo anfitrión 1204 está configurado para comunicar con la red 1202 e incluye una ranura para la inserción de la tarjeta inteligente 1206. La tarjeta inteligente 1206 está configurada para transmitir órdenes a, y recibir datos desde, una aplicación 1210 de la interfaz de usuario ejecutada por el dispositivo anfitrión 1210, y ejecutar transacciones independientemente del dispositivo anfitrión 1210. La tarjeta 1206 incluye una CPU 1212 para ejecutar transacciones, y un conjunto de chips 1214 para funcionamiento inalámbrico, para comunicar con el terminal 1208. La CPU 1212 ejecuta una interfaz API/controlador del anfitrión 1216 configurada para transmitir órdenes en un formato compatible con el dispositivo anfitrión 1204, y transformar datos procedentes del dispositivo anfitrión 1204 a un formato compatible con la CPU 1212.

Tal como se muestra, el flujo 1200 puede incluir múltiples sesiones 1220 entre el dispositivo anfitrión 1204 y la tarjeta 1206, y entre la tarjeta 1206 y el terminal 1208. La sesión 1220a muestra una sesión gestionada por la tarjeta 1206 utilizando las capacidades de red del dispositivo anfitrión 1210. En este ejemplo, la tarjeta 1206 transmite datos de transmisión a través de una red celular conectada al dispositivo anfitrión 1204, y después de recibir los datos celulares, el dispositivo anfitrión 1204 transmite los datos a la red 1202. En respuesta a la recepción de datos desde la red 1202, el dispositivo anfitrión 1204 puede transmitir automáticamente a la tarjeta 1206 los datos recibidos. En algunas implementaciones, la tarjeta 1206 puede transmitir al dispositivo anfitrión 1204 una solicitud de una firma del dispositivo, tal como se muestra en la sesión 1220b. Por ejemplo, la tarjeta 1206 puede solicitar la firma del dispositivo durante un proceso de inicialización. La sesión 1220c muestra que un usuario puede presentar órdenes a la tarjeta 1206 a través de la interfaz del dispositivo anfitrión 1204. Por ejemplo, el usuario puede solicitar que el disco presente el histórico de transacciones de usuario a través de la interfaz del dispositivo anfitrión 1204.

En algunas implementaciones, la tarjeta 1206 puede recibir una orden para activar o desactivar la antena a través del dispositivo anfitrión 1204, tal como se muestra en la sesión 1220d. Por ejemplo, una institución financiera puede identificar transacciones irregulares y transmitir una orden a través de la red 1202, para desactivar la tarjeta 1206. La tarjeta 1206 puede autorizar a un usuario mediante solicitar un PIN utilizando el dispositivo anfitrión 1204. Tal como se muestra en la sesión 1220e, el usuario puede presentar un PIN a la tarjeta 1206 utilizando la interfaz del dispositivo anfitrión 1204, y en respuesta a una evaluación del PIN presentado, la tarjeta 1206 puede presentar, a través del dispositivo anfitrión 1204, una indicación de que la verificación del usuario es satisfactoria o fallida. En algunas implementaciones, un usuario y/o una institución financiera pueden solicitar un histórico de transacciones de la tarjeta 1206, tal como se muestra en la sesión 1220f. Por ejemplo, una institución financiera puede transmitir una solicitud del histórico de transacciones a través de la red 1202 conectada al dispositivo anfitrión 1204 y en respuesta, por lo menos, a la solicitud, la tarjeta 1206 puede transmitir el histórico de transacciones a la institución financiera

utilizando la red 1202 conectada al dispositivo anfitrión 1204. En algunas implementaciones, el usuario puede presentar páginas web fuera de línea almacenadas en la tarjeta 1206, tal como se muestra en la sesión 1220g. Por ejemplo, la tarjeta 1206 puede recibir de un usuario que utiliza el dispositivo anfitrión 1204 una solicitud para presentar una página web fuera de línea, y presentar la página fuera de línea utilizando la URL de la solicitud. En algunas implementaciones, los datos almacenados en la memoria de la tarjeta 1206 pueden presentarse, por ejemplo, a través del dispositivo anfitrión 1204, tal como se muestra en la sesión 1220h. Por ejemplo, el usuario puede solicitar información específica asociada con una transacción sobre unos datos concretos, y la tarjeta 1206 puede recibir los datos y presentarlos al usuario utilizando el dispositivo anfitrión 1204. Además, el usuario puede escribir datos en la memoria de la tarjeta 1206, tal como se muestra en la sesión 1220i. Por ejemplo, el usuario puede actualizar datos de transacción con una anotación y en respuesta, por lo menos, a la solicitud, la tarjeta 1206 puede indicar si la actualización ha sido satisfactoria o fallida.

En relación con la sesión entre la tarjeta 1206 y el terminal, el flujo 1200 muestra la sesión de personalización 1220k y la sesión de transacción 1220l. En relación con la personalización, una institución financiera puede personalizar la tarjeta 1206 con credenciales del usuario, aplicaciones del usuario, páginas web y/u otra información, tal como se muestra en la sesión 1220k. Por ejemplo, el terminal 1208 puede transmitir una solicitud de provisión a la tarjeta 1206 incluyendo datos asociados. La traducción 1218 de protocolos puede traducir la solicitud de personalización a un formato compatible con la tarjeta 1206. En respuesta, por lo menos, a dicha solicitud, la CPU 1212 transmite una indicación sobre si la personalización ha sido o no satisfactoria, utilizando la traducción 1218 de protocolos. Antes de que el terminal ejecute la transacción, el terminal 1208 puede presentar un intento de transacción a la tarjeta 1206, tal como se muestra en la sesión 1220l. En este caso, la tarjeta 1206 puede identificar una firma de dispositivo del dispositivo anfitrión 1204, presentar los datos asociados al usuario a través del dispositivo anfitrión 1204 y transmitir la firma al terminal 1208 utilizando la traducción 1218 de protocolos.

La figura 13 es un diagrama de flujo que muestra un método 1300 a modo de ejemplo, para la activación de un sistema de transacciones inalámbricas que incluye una tarjeta inteligente. En general, una tarjeta inteligente puede ejecutar uno o varios procesos de activación en respuesta, por ejemplo, a una selección de un usuario. Muchas de las etapas en este diagrama de flujo pueden tener lugar simultáneamente y/o en órdenes diferentes a los mostrados. El sistema 500 o el sistema 600 pueden utilizar métodos con etapas adicionales, menos etapas y/o etapas diferentes, siempre que los métodos sigan siendo apropiados.

El método 1300 comienza en la etapa 1302, en la que se recibe una solicitud para activar una tarjeta de transacciones. Por ejemplo, el usuario puede seleccionar un elemento gráfico mostrado a través de la GUI 116 de un dispositivo anfitrión móvil 106 de la figura 1. Si se incluye una activación de cuenta, en la etapa 1304, entonces en la etapa 1306 es transmitida de forma inalámbrica a la institución financiera una solicitud de activar la cuenta financiera asociada utilizando tecnología radioeléctrica celular del dispositivo anfitrión. Por ejemplo, la tarjeta 104d de transacciones de la figura 5 puede transmitir de forma inalámbrica una solicitud de activación a la institución 506 utilizando la tecnología radioeléctrica celular del dispositivo anfitrión móvil 106d. Si no se incluye una activación de cuenta, entonces la ejecución pasa a la etapa de decisión 1308. Si no se incluye una activación de tarjeta, entonces la ejecución finaliza. Si se incluye activación de tarjeta, entonces la ejecución pasa a la etapa de decisión 1310. Si no se incluye un código de activación entonces, en la etapa 1312, se presentan al usuario una o varias preguntas previamente programadas utilizando la GUI del dispositivo anfitrión. Volviendo al ejemplo inicial, la tarjeta 104 de transacciones puede identificar preguntas almacenadas localmente, y presentar las preguntas al usuario utilizando la GUI 116 del dispositivo anfitrión móvil 106. En la etapa 1314, se identifican respuestas almacenadas localmente para las cuestiones programadas. De nuevo haciendo referencia a la etapa de decisión 1310, si se incluye un código de activación, entonces la ejecución pasa a la etapa de decisión 1316. Si el código de activación es introducido manualmente por el usuario entonces, en la etapa 1318, se presenta al usuario una solicitud del código de activación a través de la GUI del dispositivo anfitrión móvil. En el ejemplo inicial, la tarjeta 104 de transacciones puede presentar al usuario una solicitud para un código de activación, tal como una cadena de caracteres, a través de la GUI 116 del dispositivo anfitrión móvil 106. Si el código de activación no es introducido manualmente por el usuario entonces, en la etapa 1320, la tarjeta de transacciones transmite de forma inalámbrica una solicitud del código de activación utilizando la tecnología radioeléctrica celular del dispositivo anfitrión. En el ejemplo celular, la tarjeta 104 de transacciones puede transmitir una solicitud a la institución financiera utilizando la red central celular 602. En cualquier caso, en la etapa 1322 se identifica el código de activación almacenado localmente. Si la información almacenada localmente coincide con la información proporcionada en la etapa de decisión 1324, entonces, la tarjeta de transacciones es activada en la etapa 1326. Por ejemplo, la tarjeta 104 de transacciones puede activarse en respuesta, por lo menos, a la introducción por parte de un usuario de un código de activación coincidente a través de la GUI 116. Si la información proporcionada no coincide con la información almacenada localmente, entonces la ejecución finaliza.

La figura 14 muestra un ejemplo de memoria segura 1400 de acuerdo con algunas implementaciones de la presente exposición. En general, la memoria segura 1400 está configurada para almacenar credenciales de usuario para una serie de diferentes instituciones financieras. Por ejemplo, cada credencial puede estar asociada con una cuenta de usuario diferente (por ejemplo, tarjeta de crédito, cuenta bancaria). En la implementación mostrada, la memoria de seguridad 1400 incluye credenciales de usuario 1402a-c y marcos de seguridad asociados 1406a-c separados por

barreras lógicas 1410a-c. Además, la memoria segura incluye credenciales maestras 1404 y un marco de seguridad maestro 1408. Cada una de las credenciales de usuario 1402 puede estar asociada con una cuenta de usuario y/o una institución diferentes. Para cada usuario, una credencial 1402 de usuario es asignada o bien asociada con un marco de seguridad 1406. El marco de seguridad 1406 puede ser una aplicación de pago ejecutada por la tarjeta inteligente en respuesta, por lo menos, a una selección de la cuenta de usuario. Por ejemplo, el marco de seguridad 1406 puede ejecutar transacciones de acuerdo con un formato, protocolo, cifrado y/u otros aspectos especificados en una solicitud de autorización. En algunas implementaciones, el marco de seguridad 1406 puede impedir sustancialmente el acceso no autorizado a credenciales de usuario. Por ejemplo, cada marco de seguridad 1406 puede contener múltiples clases que proporcionan niveles de acceso diferentes. Cada aplicación dentro del marco 1406 puede configurarse para ser accesible en función de niveles de seguridad concretos. En algunas implementaciones, los marcos de seguridad 1406 pueden incluir diferentes versiones de una aplicación de pago para un tipo de instrumento financiero (por ejemplo, Visa). En algunas implementaciones, el marco de seguridad 1406 puede identificarse utilizando un ID de la aplicación.

La credencial maestra 1404 y el marco de seguridad maestro 1408 pueden permitir a las instituciones financieras almacenar o actualizar credenciales de usuario 1402 y marcos de seguridad asociados 1406. Por ejemplo, la creación de una nueva clave dentro de un marco de seguridad 1406 puede estar protegida por la clave raíz del marco maestro. Las barreras 1410 pueden generar dominios de seguridad entre las diferentes credenciales de usuario seleccionables 1402 y el marco de seguridad asociado 1406. Por ejemplo, una institución financiera puede acceder a credenciales 1402 de usuario y el marco de seguridad asociado 1406 para una cuenta de usuario gestionada, pero puede impedirse sustancialmente que acceda o las credenciales de usuario 1402 y el marco de seguridad asociado 1406 para instituciones financieras diferentes.

En algunas implementaciones, la tarjeta inteligente (por ejemplo, tarjeta 104 de transacciones) puede conmutar dinámicamente las credenciales de usuario 1402 y los marcos de seguridad 1406 en respuesta, por lo menos, a un evento. Por ejemplo, la tarjeta inteligente puede conmutar a credenciales de usuario por defecto y al marco de seguridad correspondiente 1406 tras la compleción de una transacción. En algunas implementaciones, la tarjeta inteligente puede conmutar credenciales de usuario 1402 y marcos de seguridad 1406 en respuesta a la selección de un usuario, por ejemplo, a través de la GUI 116 de la figura 1. Habitualmente, la tarjeta inteligente puede conmutar entre diferentes cuentas de usuario en base, por lo menos en parte, a circunstancias diferentes. En relación con añadir cuentas de usuario adicionales, un usuario puede introducir manualmente credenciales 1402 del usuario utilizando la GUI de un dispositivo anfitrión. En algunas implementaciones, la memoria 1400 puede ser actualizada OTA utilizando la tecnología radioeléctrica celular del dispositivo anfitrión.

La figura 15 es un diagrama de flujo que muestra un método de ejemplo 1500 para la conmutación dinámica entre cuentas de usuario. En general, una tarjeta inteligente puede conmutar dinámicamente entre una serie de credenciales de usuario seleccionables y marcos de seguridad asociados en respuesta, por lo menos, a un evento. Muchas de las etapas en este diagrama de flujo pueden tener lugar simultáneamente y/o en órdenes diferentes a los mostrados. El sistema 100 puede utilizar métodos con etapas adicionales, menos etapas y/o etapas diferentes, siempre que los métodos sigan siendo adecuados.

El método 1500 comienza en la etapa 1502, en la que es identificado un evento. Por ejemplo, la tarjeta 104 de transacciones de la figura 1 puede determinar que han sido actualizados uno o varios de los siguientes: ID de red, número de teléfono, dirección MAC y/u otra información. En algunas implementaciones, el evento puede incluir identificar uno o varios aspectos de una transacción o transacción potencial. Por ejemplo, la tarjeta 104 de transacciones puede determinar una empresa, un tipo de empresa, bienes y/o servicios, tipos de bienes y/o servicios, y/u otros aspectos. En la etapa 1504, se determina la cuenta de usuario seleccionada actualmente. En el ejemplo, la tarjeta 104 de transacciones puede determinar las credenciales de usuario y el marco de seguridad seleccionados actualmente. Si se conmutan las cuentas de usuario en la etapa de decisión 1506, entonces en la etapa 1500 la tarjeta inteligente puede conmutar dinámicamente la cuenta de usuario seleccionada actualmente, a una cuenta de usuario diferente en base, por lo menos en parte, al evento identificado. De nuevo en el ejemplo, la tarjeta 104 de transacciones puede conmutar dinámicamente entre la serie de cuentas de usuario seleccionables, en base, por lo menos en parte, a uno o varios eventos. A continuación, en la etapa 1510 se recibe una solicitud de ejecución. A modo de ejemplo, la tarjeta 104 de transacciones puede recibir directamente una solicitud inalámbrica para ejecutar una transacción con el punto de acceso 514. En respuesta, por lo menos, a la solicitud, se presenta al usuario una solicitud para ejecutar la transacción, en la etapa 1512. En el ejemplo, la tarjeta 104 de transacciones puede presentar la solicitud al usuario a través de la GUI 116 del dispositivo anfitrión móvil 106. En algunas implementaciones, la tarjeta 104 de transacciones puede presentar al usuario la cuenta de usuario seleccionada actualmente, a través de la GUI 116. En la etapa 1504, la solicitud de transacción es ejecutada utilizando las credenciales de usuario seleccionadas y el marco de seguridad correspondiente, en respuesta, por lo menos, a una selección del usuario. De nuevo en el ejemplo, la tarjeta 104 de transacciones puede ejecutar la solicitud de transacción en respuesta, por lo menos, a la selección por parte de un usuario de un elemento gráfico en la GUI 116 del dispositivo anfitrión móvil 106, y transmitir de forma inalámbrica la solicitud de autorización directamente al punto de acceso 514. Si la selección de cuenta se conmuta a una cuenta por defecto en la etapa de decisión 1516, la tarjeta inteligente conmuta automáticamente la cuenta de usuario seleccionada a las credenciales de usuario por

defecto y al marco de seguridad correspondiente. Si la selección no se conmuta a una cuenta por defecto, entonces la ejecución finaliza.

REIVINDICACIONES

1. Una cubierta (102) para un dispositivo móvil, que comprende:

superficies laterales configuradas para ser adyacentes, por lo menos, a una parte de una o varias superficies laterales del dispositivo móvil (106);

una superficie posterior configurada para ser adyacente, por lo menos, a una parte de una superficie posterior del dispositivo móvil (106) y estar conectada a las superficies laterales, formando las superficies laterales y la superficie posterior una abertura que recibe, por lo menos, una parte del dispositivo móvil (106), una primera parte de, por lo menos, una de las superficies incluyendo un conector (112) para conectar a un puerto del dispositivo móvil (106);

una interfaz física (110) incluida, por lo menos, en una de las superficies, y

un circuito (114) configurado para conectar la interfaz física (110) al conector (112); y

una tarjeta de transacciones (104), **caracterizada por**:

una interfaz física configurada para la conexión a un puerto de un dispositivo móvil, en la que el dispositivo móvil incluye una interfaz gráfica de usuario (116);

un módulo de comunicaciones configurado para recibir de forma inalámbrica señales de radiofrecuencia desde un terminal de acceso, y transmitir señales de radiofrecuencia al mismo;

una memoria segura (1400) configurada para almacenar una serie de credenciales de usuario seleccionables (714), en la que las credenciales de usuario ejecutan transacciones con terminales de acceso y están, cada una, asociadas con diferentes instituciones;

un módulo (704) de interfaz de usuario, configurado para presentar y recibir información a través de la interfaz gráfica de usuario (116) del dispositivo anfitrión móvil; y

un módulo de transacciones configurado para conmutar dinámicamente entre la serie de credenciales de usuario seleccionables, en respuesta, por lo menos, a un evento y para transmitir de forma inalámbrica al terminal de acceso una respuesta a una transacción solicitada que incluye credenciales de usuario seleccionadas entre dicha serie de credenciales de usuario seleccionables.

2. La cubierta acorde con la reivindicación 1, en la que la interfaz física (110) configurada para recibir la tarjeta (104) de transacciones comprende una ranura SecureDigital o microSD.

3. La cubierta acorde con la reivindicación 1, en la que la tarjeta (104) de transacciones está integrada en la cubierta (102).

4. La cubierta acorde con la reivindicación 1, comprendiendo además el circuito (114) un módulo (202) de conversión configurado para transformar señales entre una forma compatible con la tarjeta (104) de transacciones y una forma compatible con el dispositivo móvil (106), en la que opcionalmente el módulo (202) de conversión realiza una conversión entre una señal SD y una señal de bus en serie universal.

5. La cubierta acorde con la reivindicación 1, en la que el conector (116) incluye una primera interfaz configurada para conectar al puerto del dispositivo móvil (106) y una segunda interfaz configurada para duplicar sustancialmente un puerto original del dispositivo móvil (106).

6. La cubierta acorde con la reivindicación 1, en la que la interfaz física comprende, por lo menos una entre una interfaz SecureDigital, una interfaz miniSD, una interfaz microSD, una interfaz MMC, una miniMMC, una microMMC, una interfaz Firewire o una interfaz Apple iDock, o una interfaz de bus en serie universal.

7. La cubierta acorde con la reivindicación 1, en la que el módulo de comunicaciones ejecuta la transacción independientemente del dispositivo móvil (106).

8. La cubierta acorde con la reivindicación 1, en la que la memoria segura (1400) almacena una serie de marcos de seguridad (1406) para dicha serie de credenciales (1402) de usuario, y el módulo de comunicaciones ejecuta la transacción solicitada utilizando un marco de seguridad de entre dicha serie de marcos de seguridad (1406), correspondiente a las credenciales de usuario seleccionadas (1402).

9. La cubierta acorde con la reivindicación 1, en la que el módulo (704) de interfaz de usuario presenta información asociada con la transacción solicitada, a través de la interfaz gráfica de usuario (116) del dispositivo móvil; opcionalmente

en el que la información presentada se basa, por lo menos en parte, por lo menos en uno entre el contenido en tiempo real durante la transacción, el contenido fuera de línea almacenado localmente o el contenido en línea asociado con la institución financiera; o

en el que el módulo (704) de la interfaz de usuario está configurado además para presentar una solicitud para la identificación del usuario que incluye, por lo menos, uno entre un número de identificación personal, un ID del usuario y una contraseña, o una firma biométrica a través de la interfaz gráfica de usuario (116) del dispositivo móvil, estando configurado además el módulo de procesamiento para comprobar la identificación del usuario presentada con la identificación del usuario almacenada localmente en la memoria segura, antes de la ejecución de la transacción solicitada.

10. La cubierta acorde con la reivindicación 1, en la que el módulo de comunicaciones conmuta selectivamente una antena de RF entre un estado activo y un estado inactivo en respuesta, por lo menos, a un evento.

11. La cubierta acorde con la reivindicación 1, en la que las señales de radiofrecuencia inalámbricas comprenden, por lo menos, una entre señales sin contacto, señales de proximidad, señales de comunicación por campo cercano, señales Bluetooth, señales de banda ultra-ancha o señales de identificador de radiofrecuencia.

12. La cubierta acorde con la reivindicación 1, en la que el módulo de comunicaciones comprende además un módulo de traducción de protocolos configurado además para traducir señales entre protocolos inalámbricos compatibles con el terminal minorista y una aplicación de transacciones interna.

13. La cubierta la reivindicación 1, que comprende además un módulo criptográfico configurado para descifrar señales recibidas, antes de su procesamiento mediante el módulo de transacciones, y para descifrar por lo menos parte de la respuesta de transacción antes de la transmisión inalámbrica.

14. La cubierta acorde con la reivindicación 1, que comprende además un módulo de autenticación configurado para autenticar, por lo menos, uno entre una red del dispositivo anfitrión móvil, el dispositivo móvil o un usuario.

15. La cubierta acorde con la reivindicación 1, que comprende además un módulo de inicialización configurado para ejecutar uno o varios procesos de autenticación en respuesta, por lo menos, a la introducción en el puerto del dispositivo móvil.

16. La cubierta acorde con la reivindicación 1, que comprende además un módulo de activación configurado para activar el acceso a unas credenciales de usuario entre la serie de credenciales de usuario seleccionables, y transmitir a una institución financiera asociada una solicitud de activación de una cuenta de usuario asociada.

17. La cubierta acorde con la reivindicación 1, estando configurado además el módulo de transacciones para recibir las selecciones del usuario a través de la interfaz gráfica de usuario (116), para las diferentes cuentas de usuario asociadas con dicha serie de credenciales de usuario seleccionables.

18. La cubierta acorde con la reivindicación 1, estando configurado además el módulo de comunicaciones para recibir solicitudes de actualización de dicha serie de credenciales de usuario seleccionables (1402), a través de una conexión inalámbrica con una red central celular o de una conexión cableada con una red de banda ancha y estando además configurado opcionalmente para, por lo menos, añadir nuevos conjuntos de credenciales de usuario o borrar credenciales de usuario existentes en base, por lo menos en parte, a las solicitudes de actualización.

19. La cubierta acorde con la reivindicación 1, en la que dicha serie de credenciales de usuario seleccionables (1402) incluyen credenciales de usuario por defecto, estando configurado además el módulo de comunicaciones para conmutar las credenciales de usuario por defecto en respuesta, por lo menos, a la compleción de la transacción solicitada, utilizando una credencial diferente de entre dicha serie de credenciales de usuario seleccionables; o

en el que dicha serie de credenciales de usuario seleccionables (1402) incluyen credenciales de usuario por defecto, estando configurado además el módulo de seguridad para conmutar a unas credenciales de usuario por defecto en respuesta, por lo menos, a la expiración de un periodo de tiempo para completar una transacción utilizando credenciales de usuario no por defecto; o en la que cada una que dicha serie de credenciales seleccionables (1402) es carga en el módulo seguro (1400) desde una institución diferente.

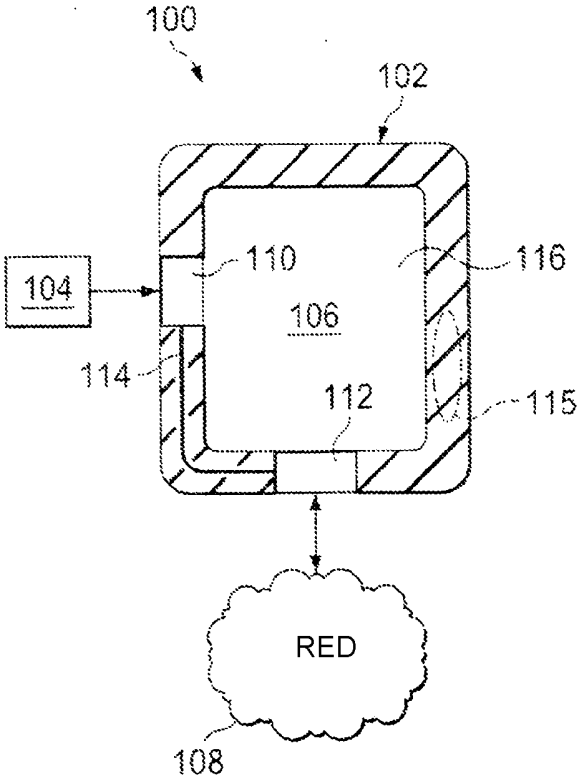

100
102
104
110
116
106
114
112
115
RED
108

FIG. 1

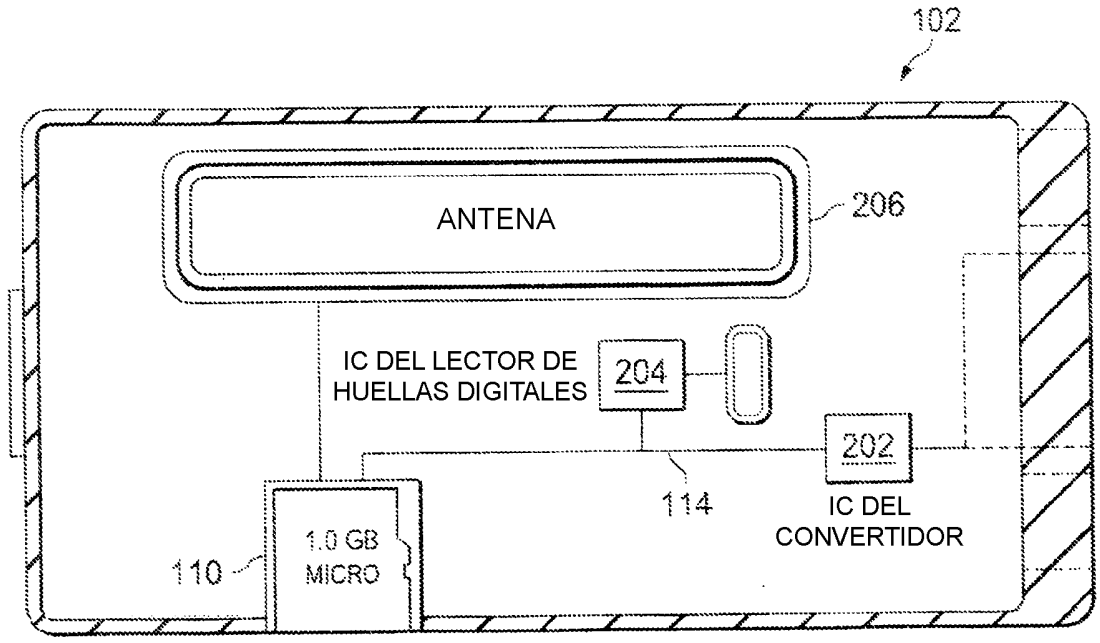

102
ANTENA
206
IC DEL LECTOR DE HUELLAS DIGITALES
204
202
114
IC DEL CONVERTIDOR
110
1.0 GB MICRO

FIG. 2A

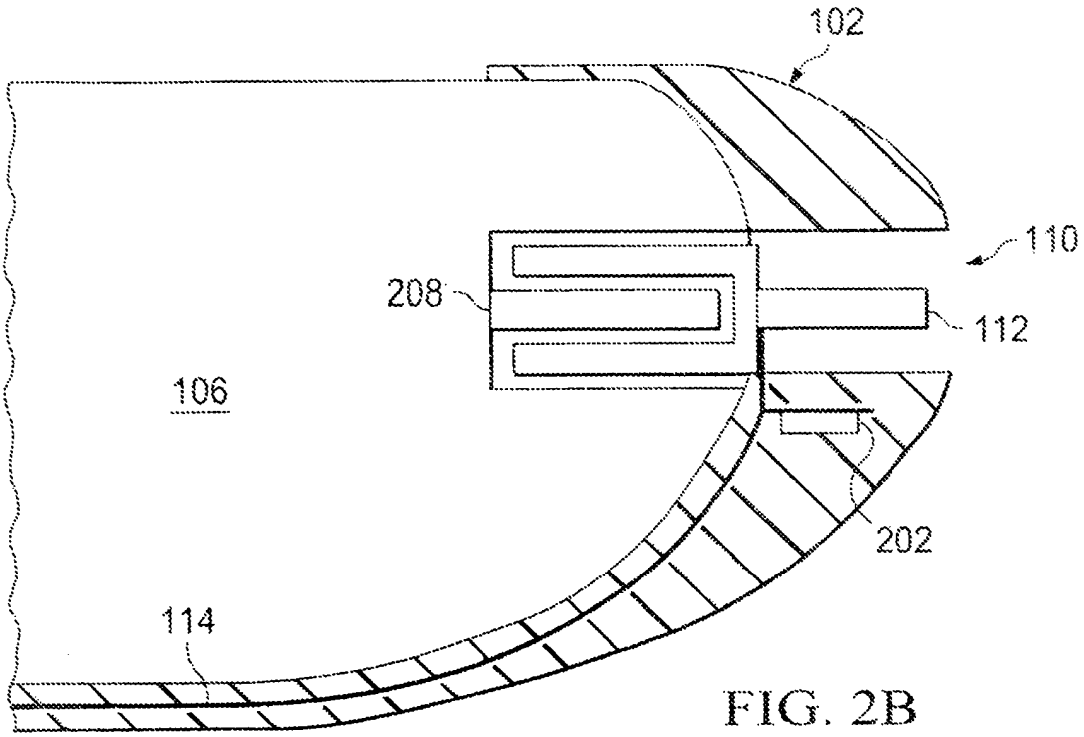


FIG. 2B

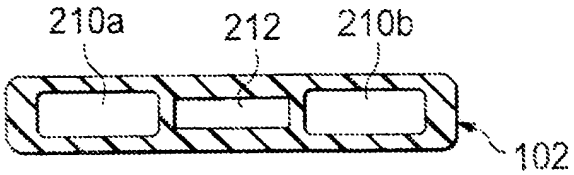


FIG. 2C

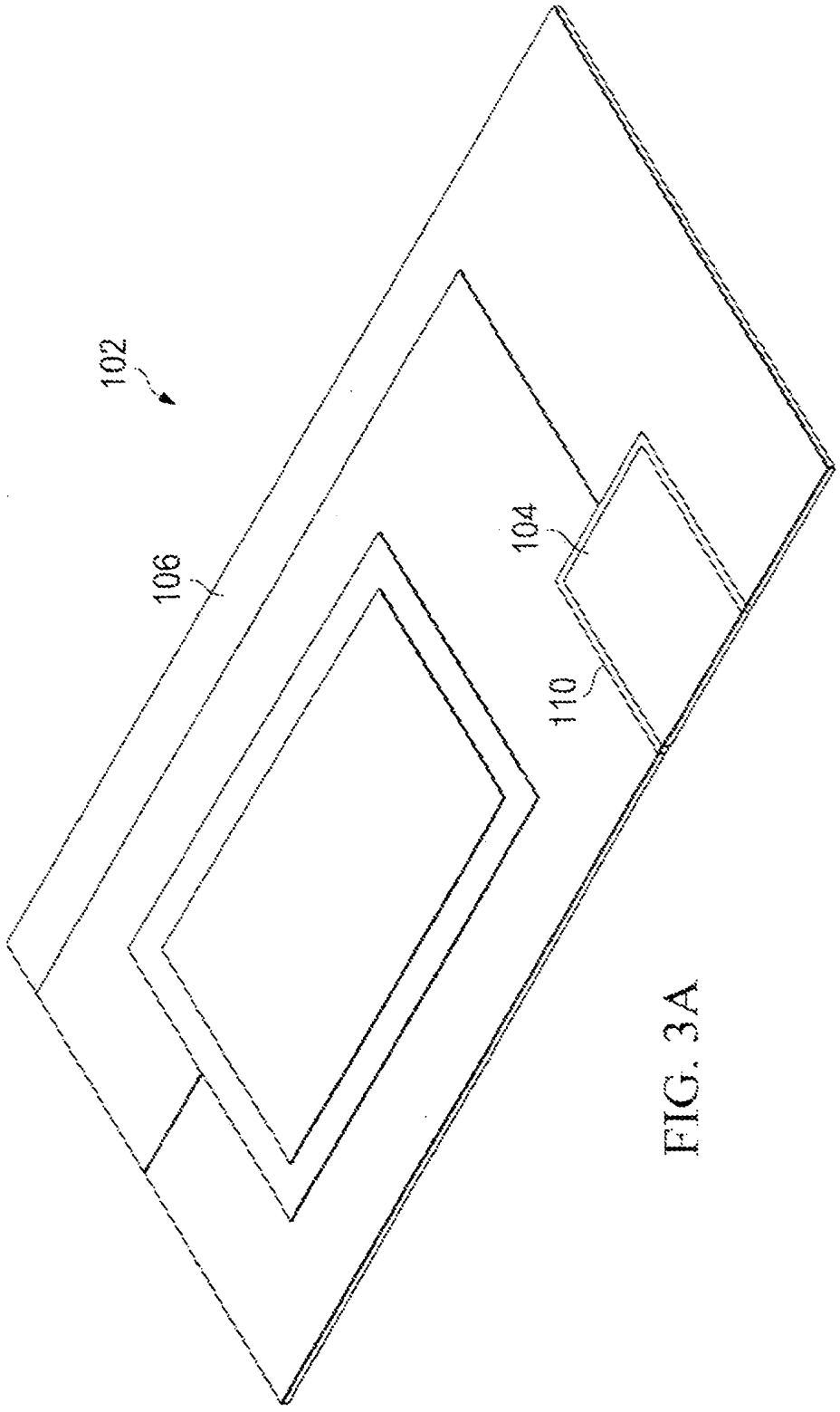


FIG. 3A

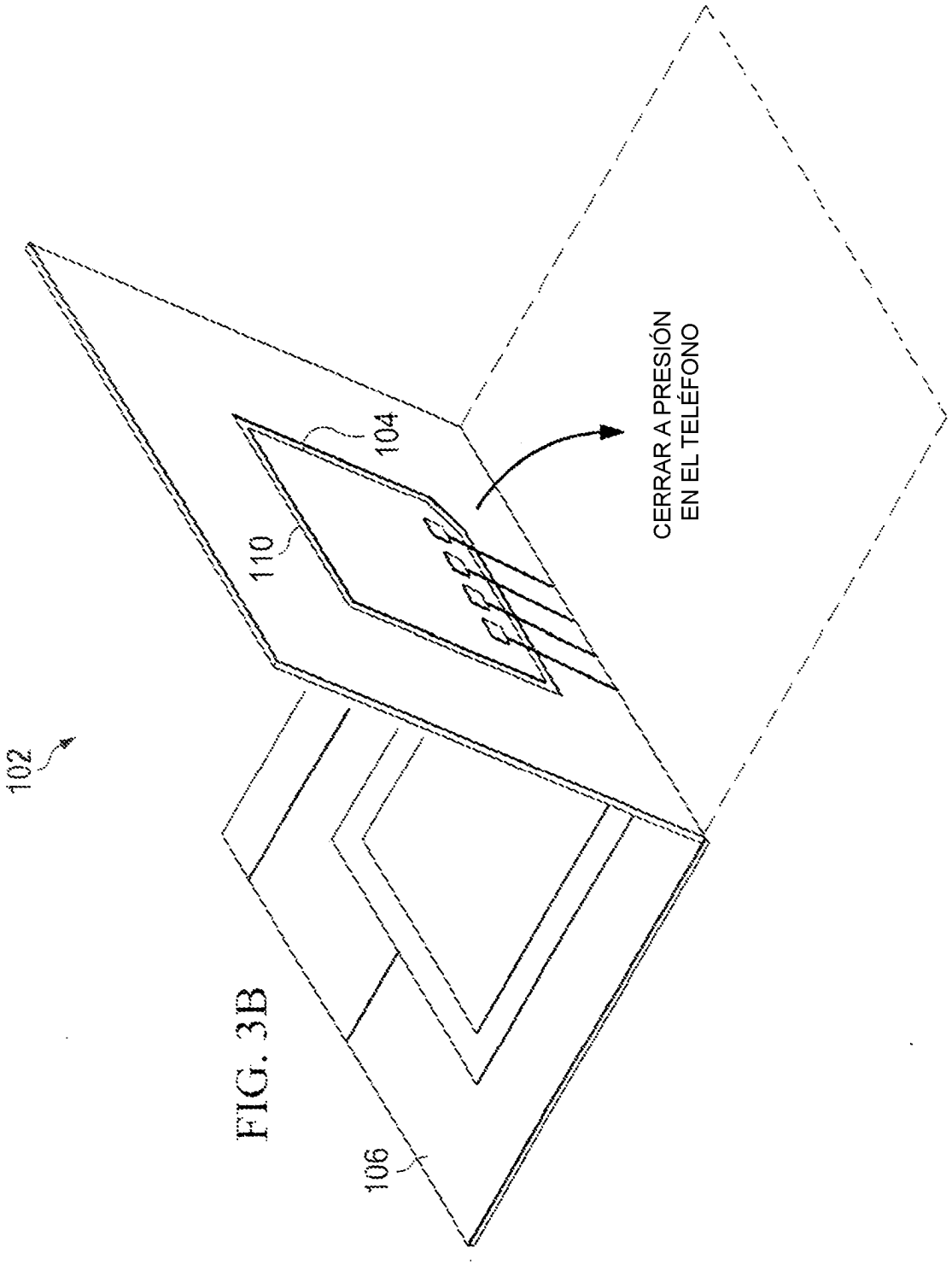


FIG. 3B

FIG. 4

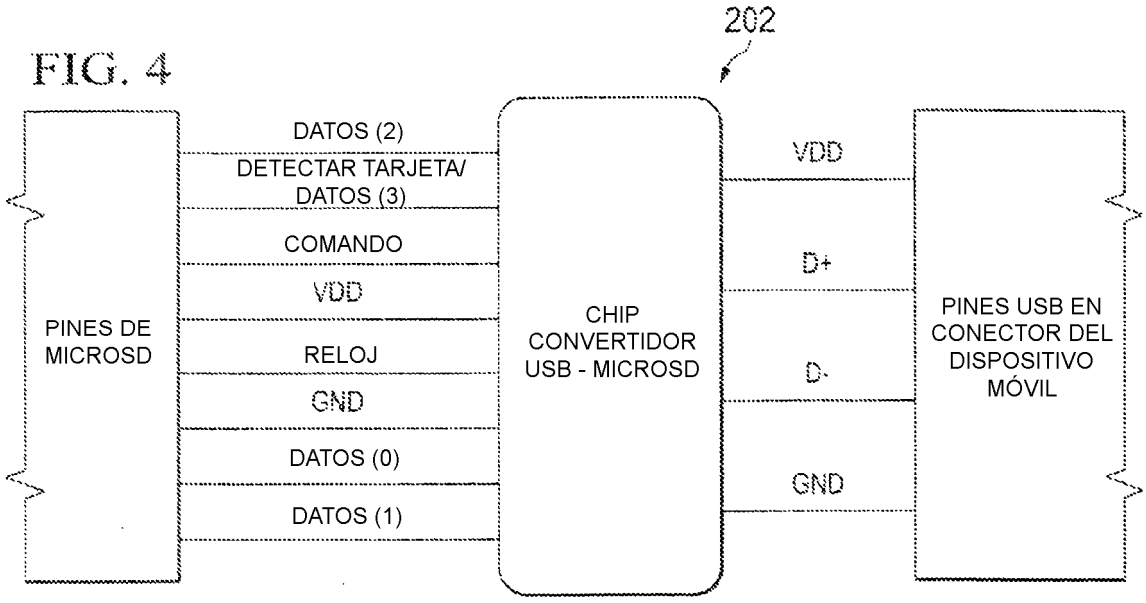
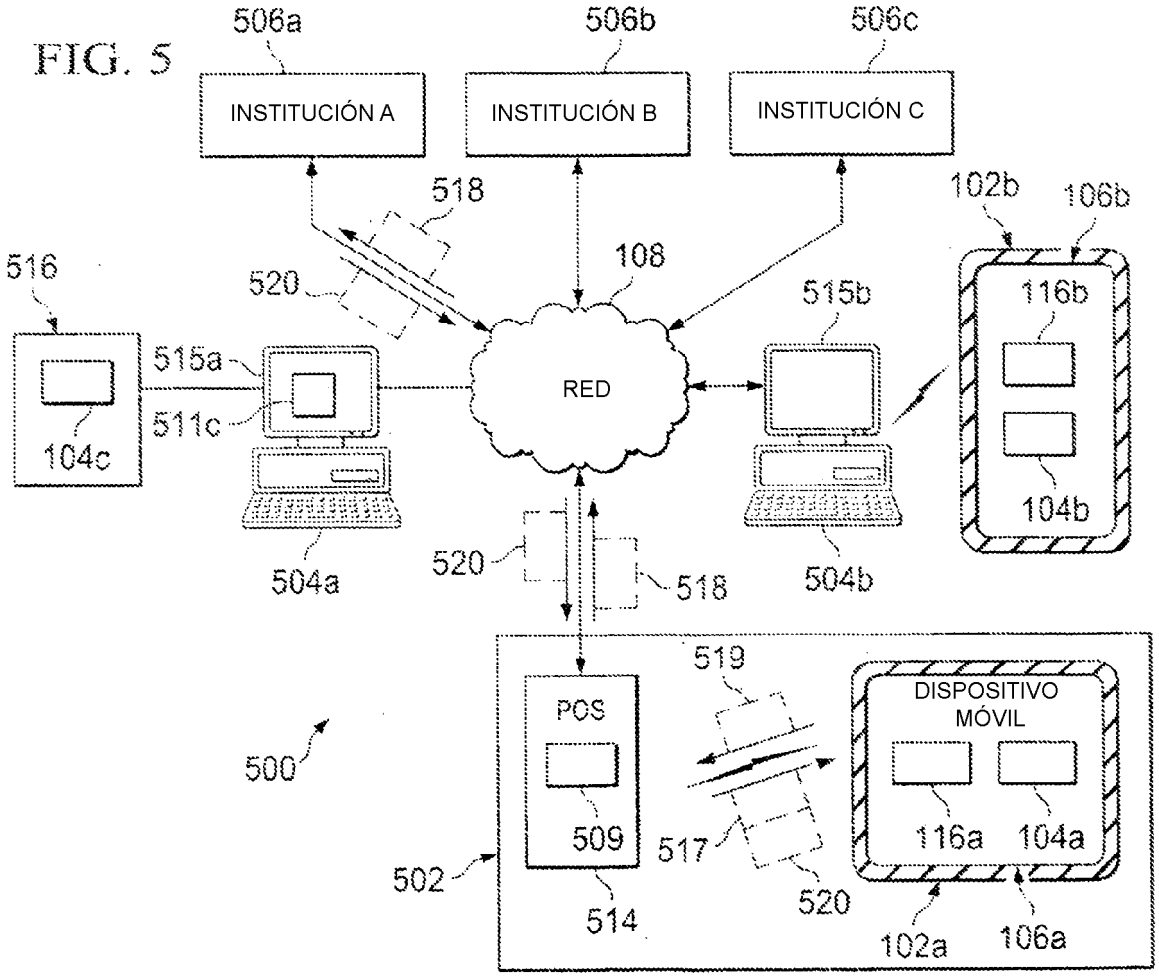

202
PINES DE MICROSD
DATOS (2)
DETECTAR TARJETA/ DATOS (3)
COMANDO
VDD
RELOJ
GND
DATOS (0)
DATOS (1)
CHIP CONVERTIDOR USB - MICROSD
VDD
D+
D-
GND
PINES USB EN CONECTOR DEL DISPOSITIVO MÓVIL

FIG. 5


506a
506b
506c
INSTITUCIÓN A
INSTITUCIÓN B
INSTITUCIÓN C
518
520
108
516
515a
511c
104c
RED
515b
102b
106b
116b
104b
504a
504b
520
518
519
PCS
509
514
DISPOSITIVO MÓVIL
116a
104a
517
520
502
500
102a
106a

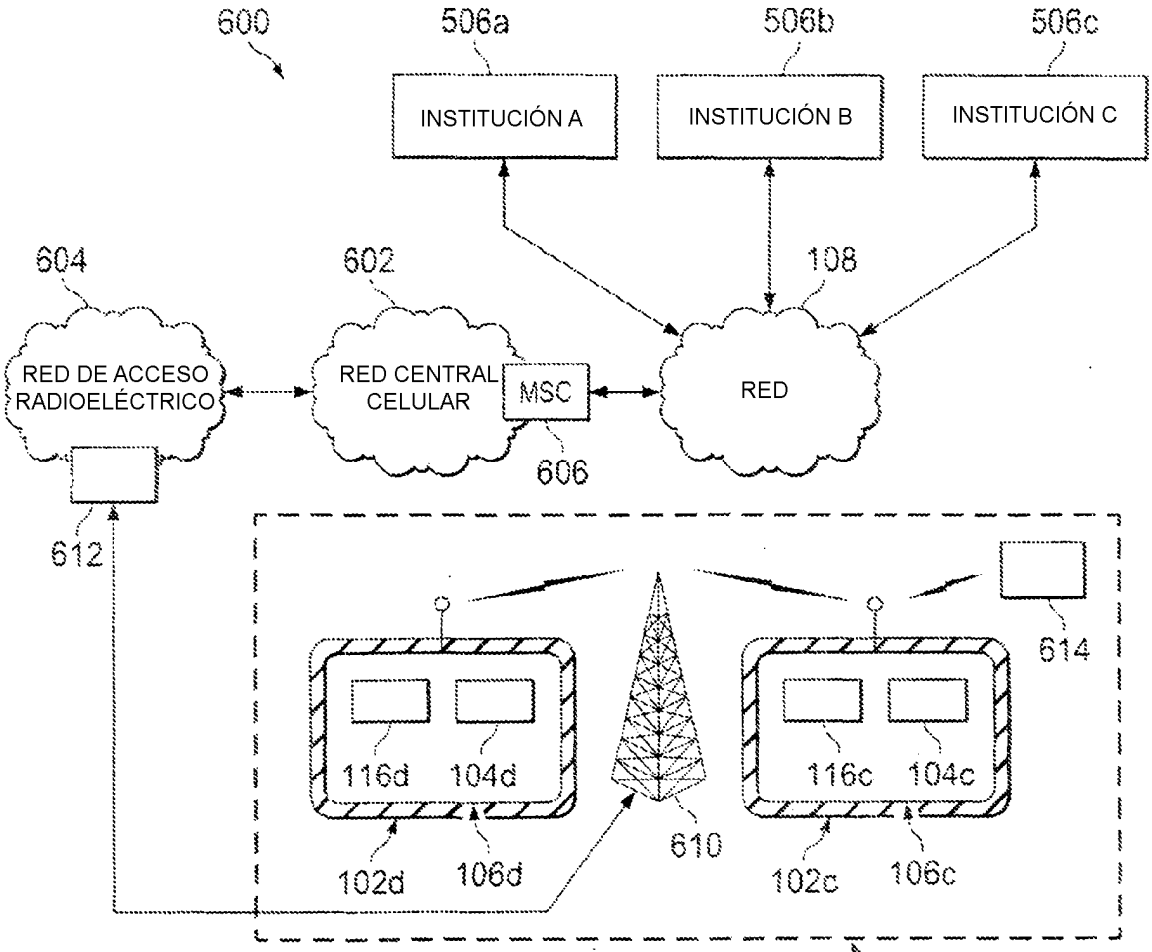

600
506a
506b
506c
INSTITUCIÓN A
INSTITUCIÓN B
INSTITUCIÓN C
604
602
108
RED DE ACCESO RADIOELÉCTRICO
RED CENTRAL CELULAR
MSC
RED
606
612
614
116d
104d
116c
104c
610
102d
106d
102c
106c
608

FIG. 6

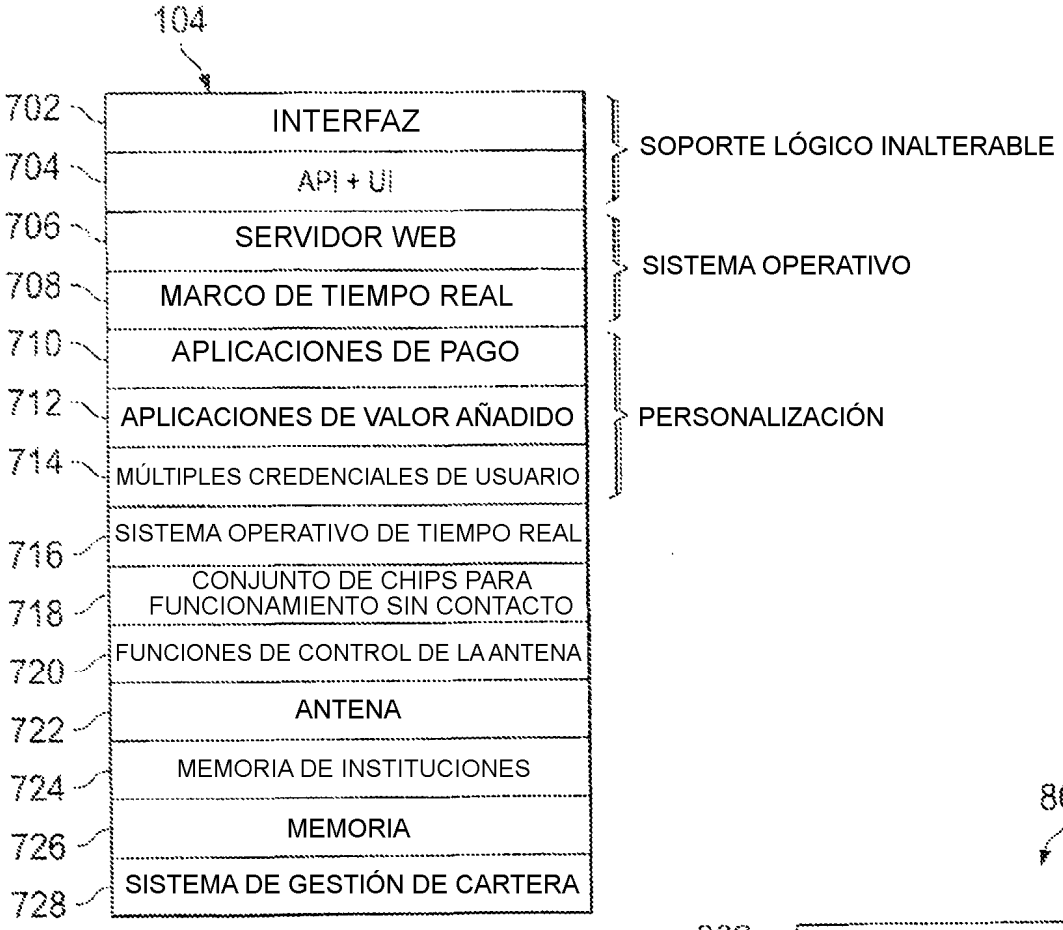

104
702
INTERFAZ
704
API + UI
706
SERVIDOR WEB
708
MARCO DE TIEMPO REAL
710
APLICACIONES DE PAGO
712
APLICACIONES DE VALOR AÑADIDO
714
MÚLTIPLES CREDENCIALES DE USUARIO
716
SISTEMA OPERATIVO DE TIEMPO REAL
718
CONJUNTO DE CHIPS PARA FUNCIONAMIENTO SIN CONTACTO
720
FUNCIONES DE CONTROL DE LA ANTENA
722
ANTENA
724
MEMORIA DE INSTITUCIONES
726
MEMORIA
728
SISTEMA DE GESTIÓN DE CARTERA
SOPORTE LÓGICO INALTERABLE
SISTEMA OPERATIVO
PERSONALIZACIÓN

FIG. 7

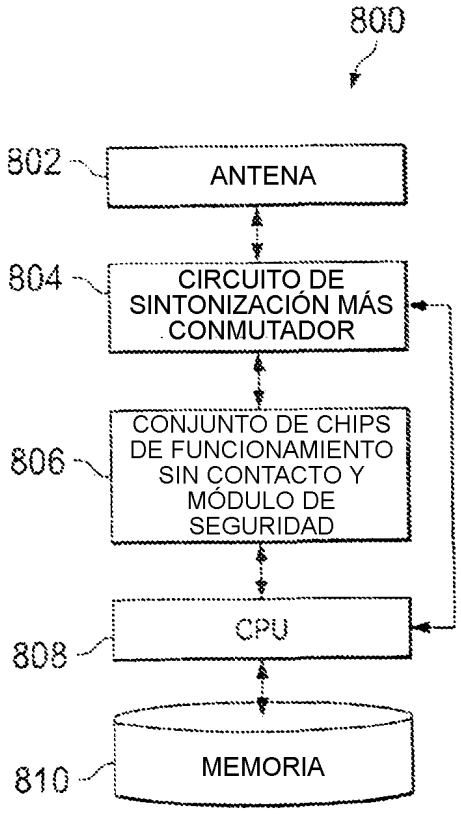

800
802
ANTENA
804
CIRCUITO DE SINTONIZACIÓN MÁS CONMUTADOR
806
CONJUNTO DE CHIPS DE FUNCIONAMIENTO SIN CONTACTO Y MÓDULO DE SEGURIDAD
808
CPU
810
MEMORIA

FIG. 8

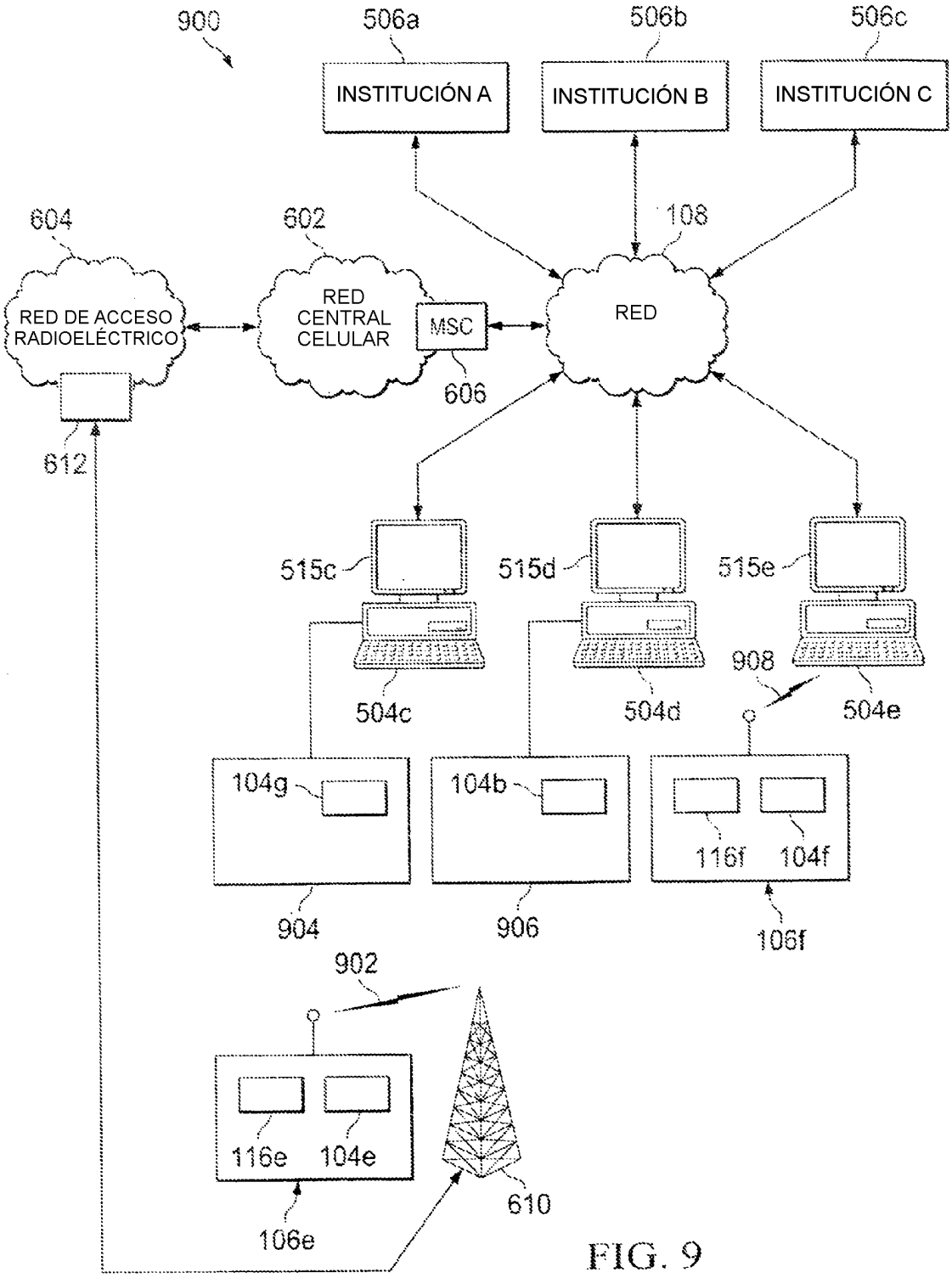

900
506a
506b
506c
INSTITUCIÓN A
INSTITUCIÓN B
INSTITUCIÓN C
604
602
108
RED DE ACCESO RADIOELÉCTRICO
RED CENTRAL CELULAR
MSC
606
RED
612
515c
515d
515e
504c
504d
908
504e
104g
104b
116f
104f
904
906
106f
902
116e
104e
106e
610

FIG. 9

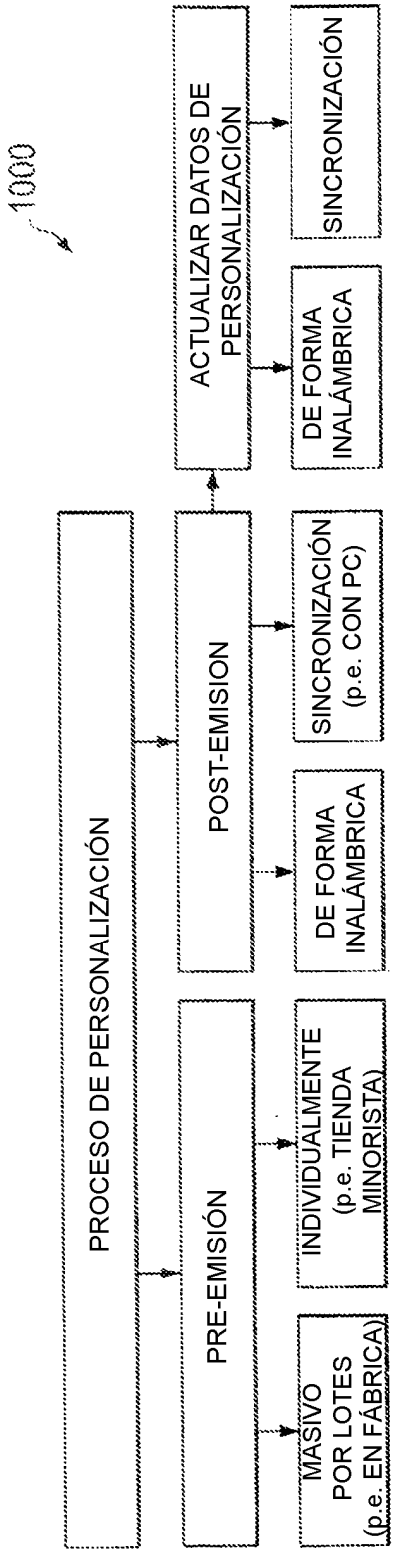

1000
PROCESO DE PERSONALIZACIÓN
PRE-EMISIÓN
MASIVO POR LOTES (p.e. EN FÁBRICA)
INDIVIDUALMENTE (p.e. TIENDA MINORISTA)
POST-EMISION
DE FORMA INALÁMBRICA
SINCRONIZACIÓN (p.e. CON PC)
ACTUALIZAR DATOS DE PERSONALIZACIÓN
DE FORMA INALÁMBRICA
SINCRONIZACIÓN

FIG. 10

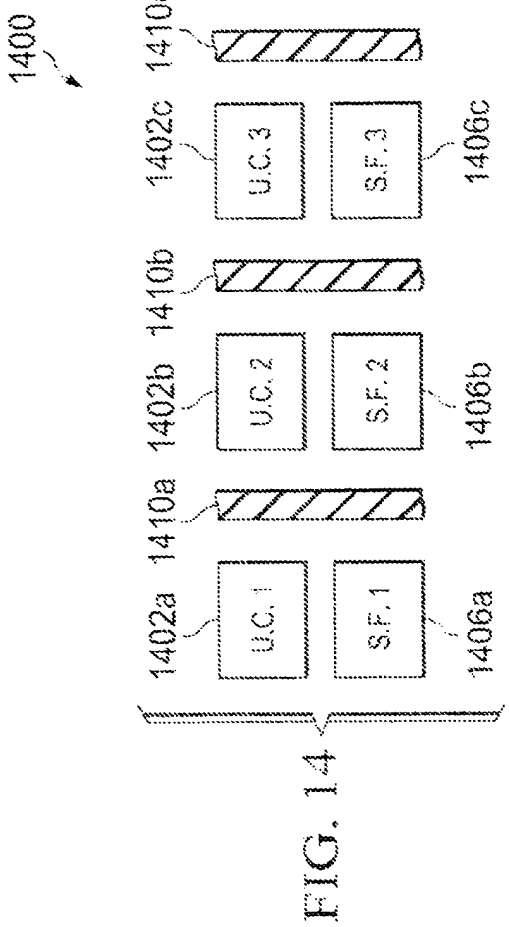

1400
1402a
U.C. 1
1410a
1402b
U.C. 2
1410b
1402c
U.C. 3
1410c
1404
M.C.
S.F. 1
1406a
S.F. 2
1406b
S.F. 3
1406c
M.S.F.
1408

FIG. 14

FIG. 11A

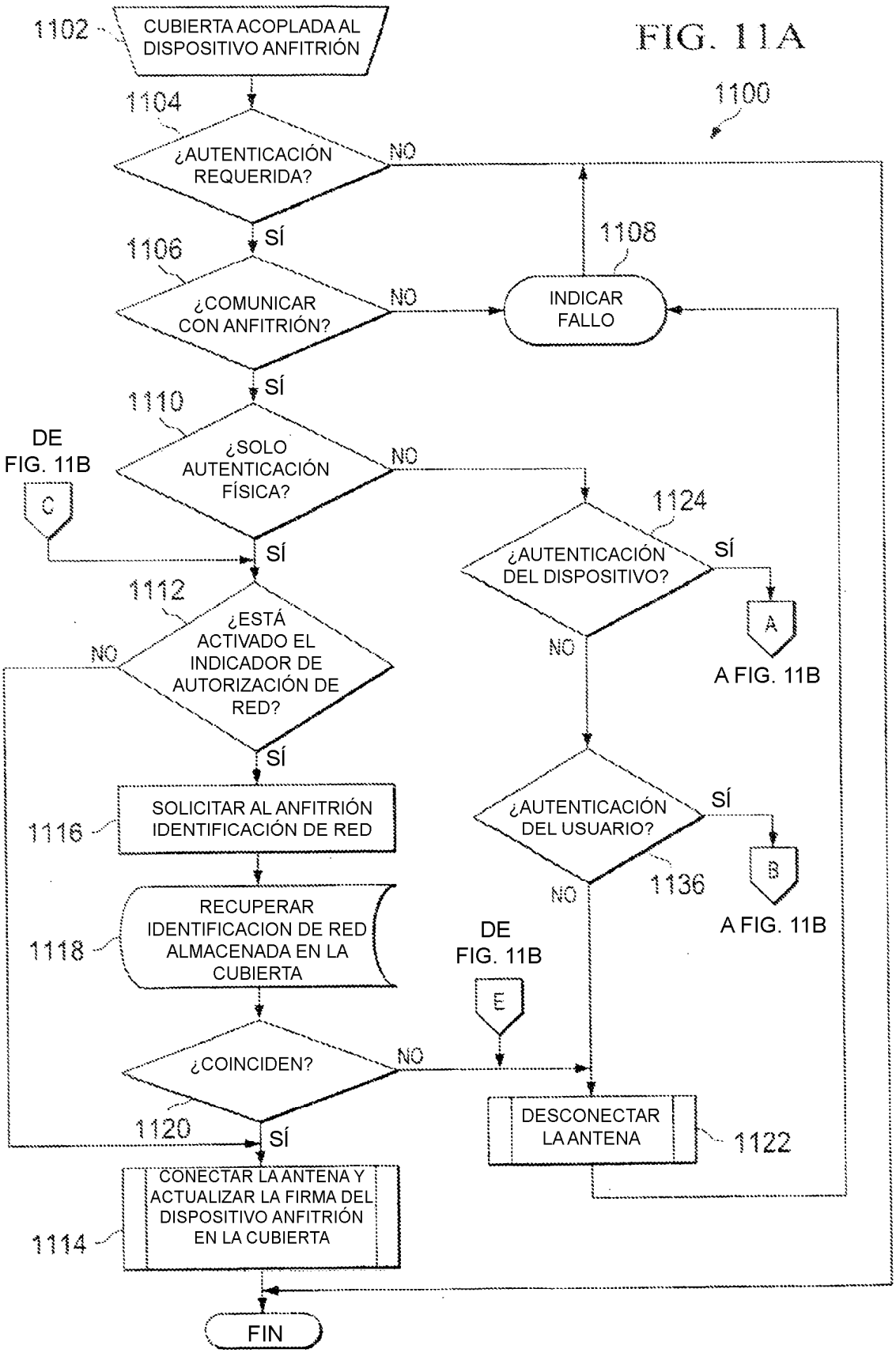

1100
1102
CUBIERTA ACOPLADA AL DISPOSITIVO ANFITRIÓN
1104
¿AUTENTICACIÓN REQUERIDA?
NO
SÍ
1106
¿COMUNICAR CON ANFITRIÓN?
NO
1108
INDICAR FALLO
SÍ
1110
¿SOLO AUTENTICACIÓN FÍSICA?
NO
DE FIG. 11B
C
SÍ
1112
¿ESTÁ ACTIVADO EL INDICADOR DE AUTORIZACIÓN DE RED?
NO
SÍ
1116
SOLICITAR AL ANFITRIÓN IDENTIFICACIÓN DE RED
1118
RECUPERAR IDENTIFICACION DE RED ALMACENADA EN LA CUBIERTA
1120
¿COINCIDEN?
NO
SÍ
1114
CONECTAR LA ANTENA Y ACTUALIZAR LA FIRMA DEL DISPOSITIVO ANFITRIÓN EN LA CUBIERTA
FIN
1124
¿AUTENTICACIÓN DEL DISPOSITIVO?
SÍ
A
A FIG. 11B
NO
¿AUTENTICACIÓN DEL USUARIO?
SÍ
B
A FIG. 11B
1136
NO
DE FIG. 11B
E
DESCONECTAR LA ANTENA
1122

FIG. 11B

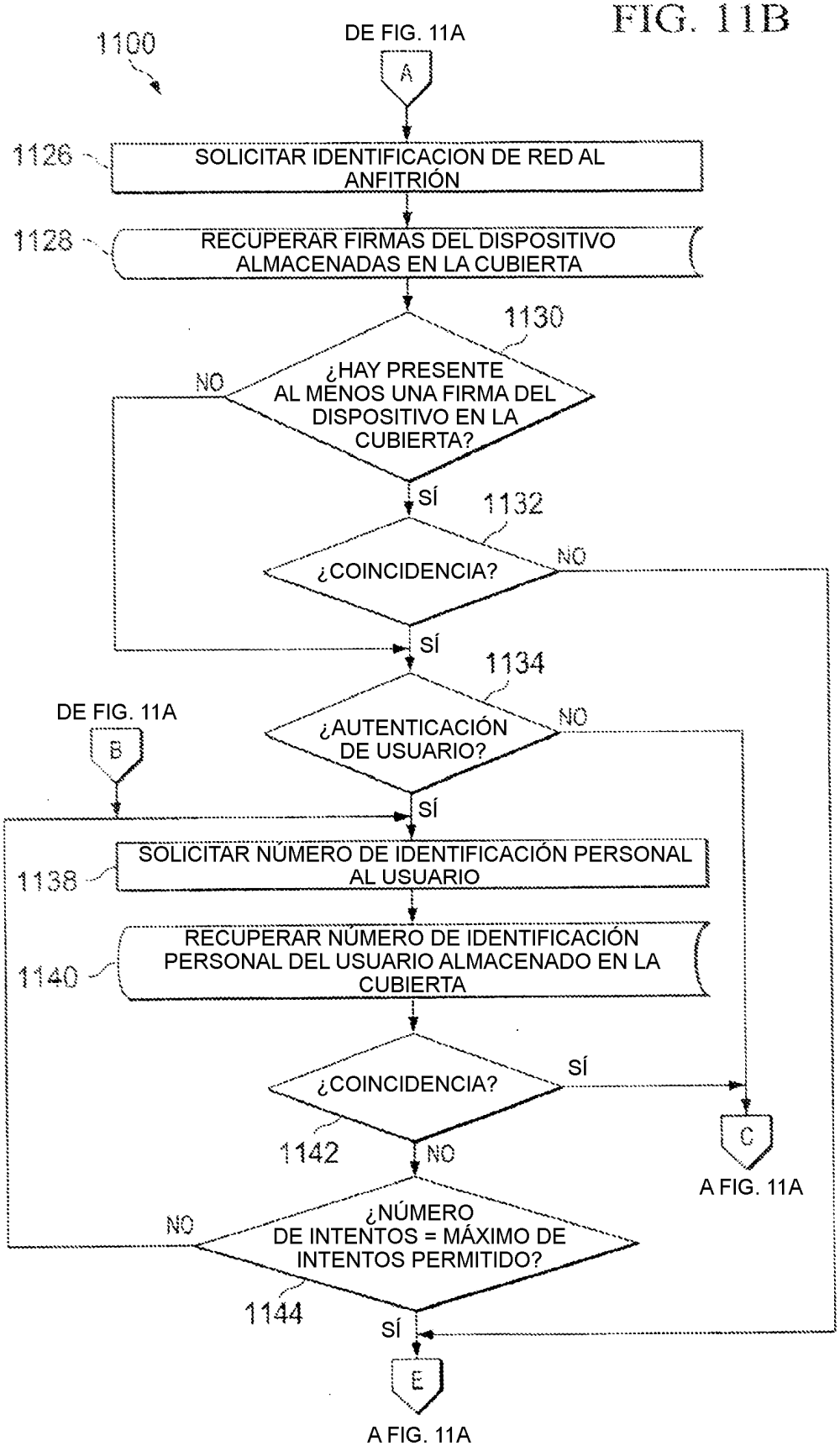

1100
DE FIG. 11A
A
1126
SOLICITAR IDENTIFICACION DE RED AL ANFITRIÓN
1128
RECUPERAR FIRMAS DEL DISPOSITIVO ALMACENADAS EN LA CUBIERTA
1130
¿HAY PRESENTE AL MENOS UNA FIRMA DEL DISPOSITIVO EN LA CUBIERTA?
NO
SÍ
1132
¿COINCIDENCIA?
NO
SÍ
1134
¿AUTENTICACIÓN DE USUARIO?
NO
SÍ
DE FIG. 11A
B
1138
SOLICITAR NÚMERO DE IDENTIFICACIÓN PERSONAL AL USUARIO
1140
RECUPERAR NÚMERO DE IDENTIFICACIÓN PERSONAL DEL USUARIO ALMACENADO EN LA CUBIERTA
¿COINCIDENCIA?
SÍ
1142
NO
C
A FIG. 11A
NO
¿NÚMERO DE INTENTOS = MÁXIMO DE INTENTOS PERMITIDO?
1144
SÍ
E
A FIG. 11A

FIG. 12A

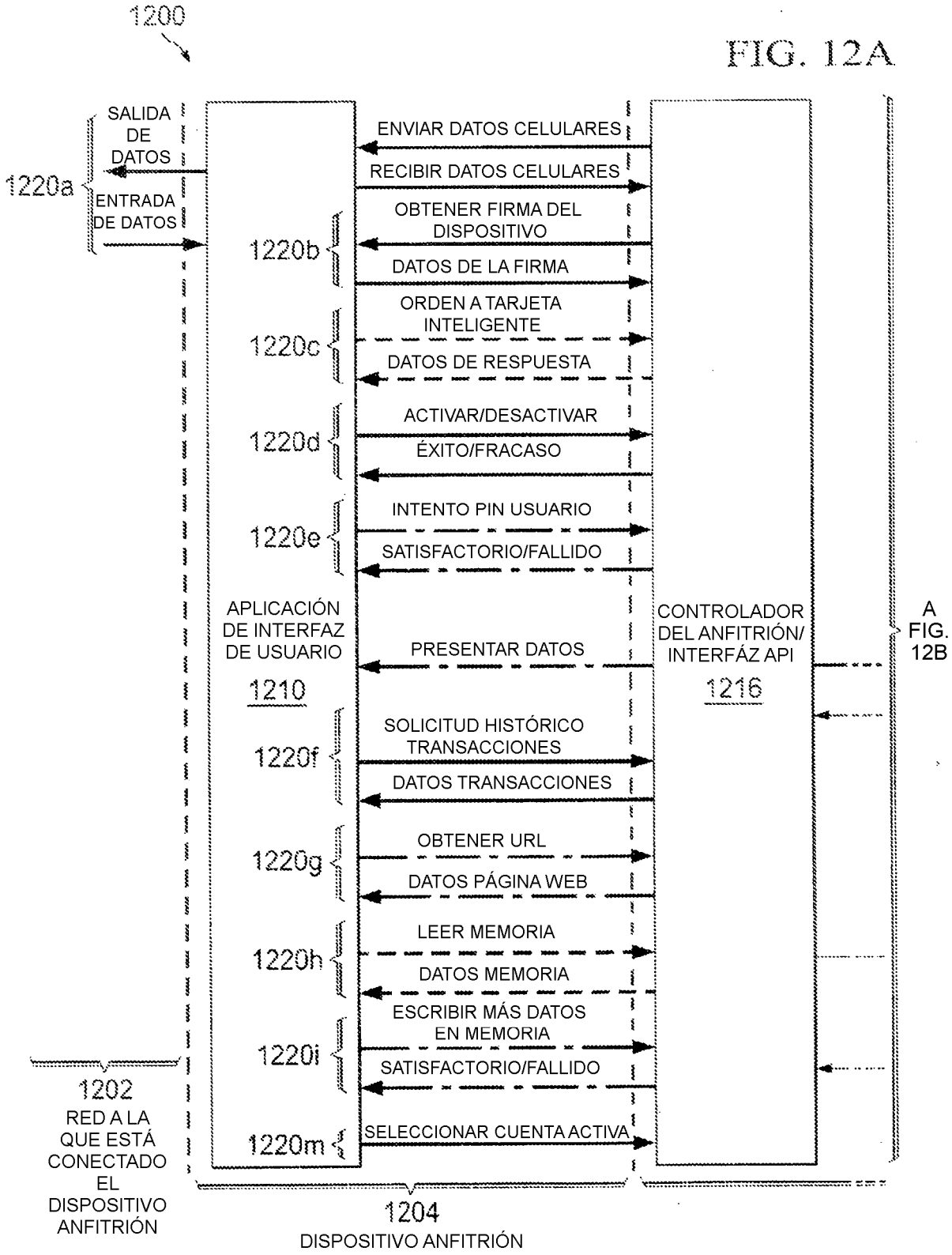

1200
SALIDA DE DATOS
1220a
ENTRADA DE DATOS
ENVIAR DATOS CELULARES
RECIBIR DATOS CELULARES
OBTENER FIRMA DEL DISPOSITIVO
1220b
DATOS DE LA FIRMA
ORDEN A TARJETA INTELIGENTE
1220c
DATOS DE RESPUESTA
ACTIVAR/DESACTIVAR
1220d
ÉXITO/FRACASO
INTENTO PIN USUARIO
1220e
SATISFACTORIO/FALLIDO
APLICACIÓN DE INTERFAZ DE USUARIO
1210
PRESENTAR DATOS
CONTROLADOR DEL ANFITRIÓN/ INTERFÁZ API
1216
A FIG. 12B
SOLICITUD HISTÓRICO TRANSACCIONES
1220f
DATOS TRANSACCIONES
OBTENER URL
1220g
DATOS PÁGINA WEB
LEER MEMORIA
1220h
DATOS MEMORIA
ESCRIBIR MÁS DATOS EN MEMORIA
1220i
SATISFACTORIO/FALLIDO
SELECCIONAR CUENTA ACTIVA
1220m
1202
RED A LA QUE ESTÁ CONECTADO EL DISPOSITIVO ANFITRIÓN
1204
DISPOSITIVO ANFITRIÓN

FIG. 12B

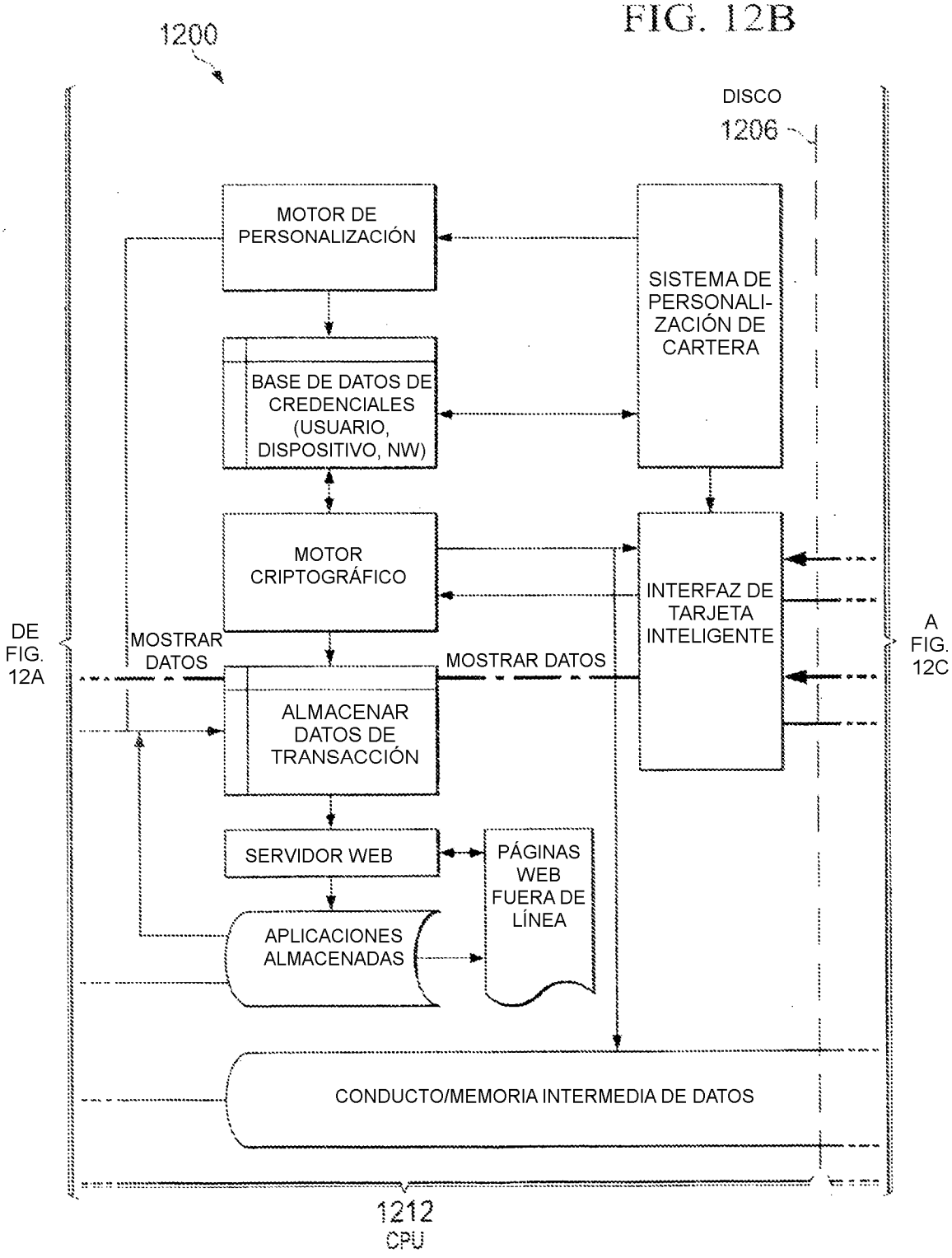
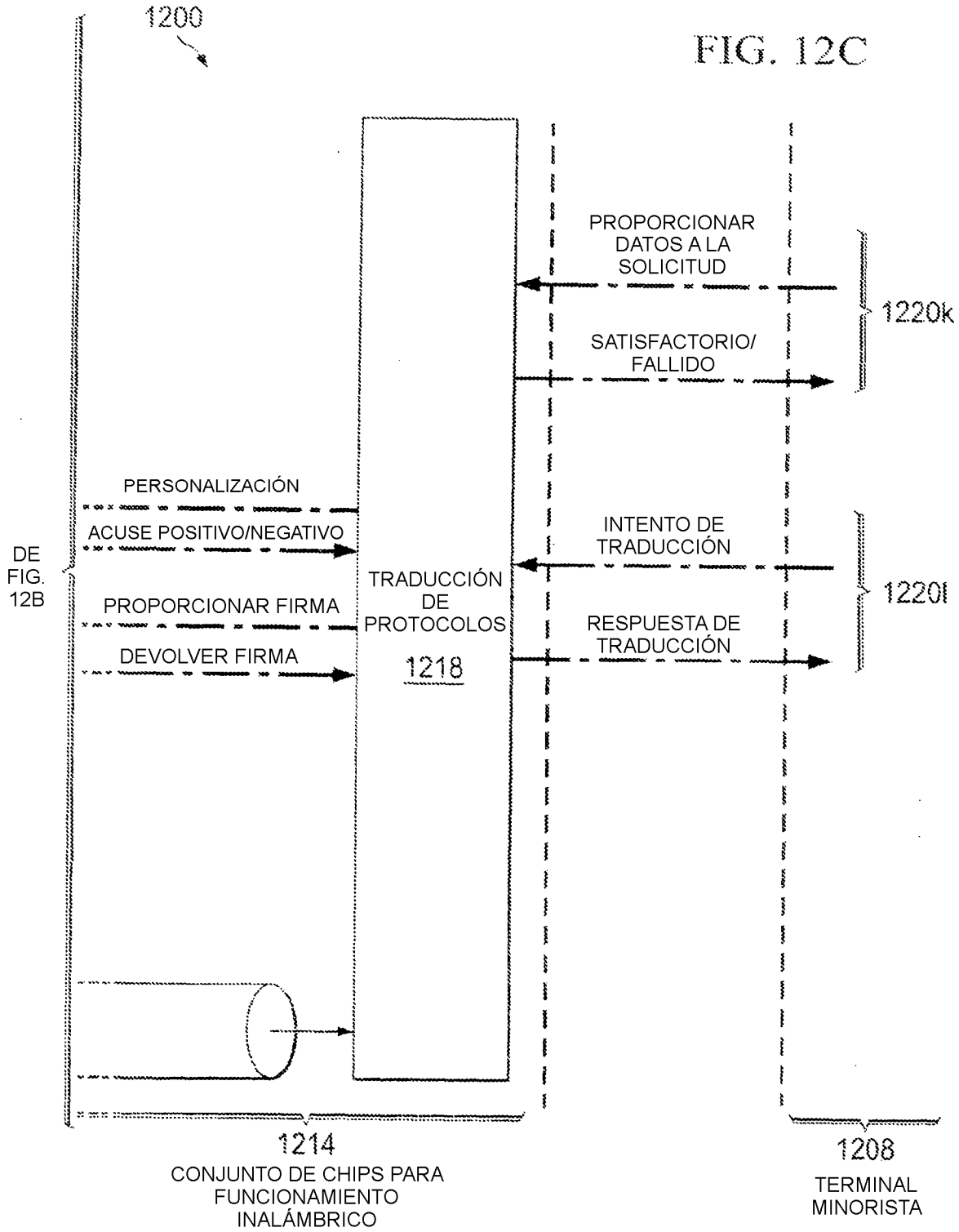

1200
DISCO
1206
MOTOR DE PERSONALIZACIÓN
SISTEMA DE PERSONALI-ZACIÓN DE CARTERA
BASE DE DATOS DE CREDENCIALES (USUARIO, DISPOSITIVO, NW)
MOTOR CRIPTOGRÁFICO
INTERFAZ DE TARJETA INTELIGENTE
DE FIG. 12A
A FIG. 12C
MOSTRAR DATOS
MOSTRAR DATOS
ALMACENAR DATOS DE TRANSACCIÓN
SERVIDOR WEB
PÁGINAS WEB FUERA DE LÍNEA
APLICACIONES ALMACENADAS
CONDUCTO/MEMORIA INTERMEDIA DE DATOS
1212
CPU

FIG. 12C


1200
PROPORCIONAR DATOS A LA SOLICITUD
SATISFACTORIO/ FALLIDO
1220k
PERSONALIZACIÓN
ACUSE POSITIVO/NEGATIVO
DE FIG. 12B
PROPORCIONAR FIRMA
DEVOLVER FIRMA
TRADUCCIÓN DE PROTOCOLOS
1218
INTENTO DE TRADUCCIÓN
RESPUESTA DE TRADUCCIÓN
1220l
1214
CONJUNTO DE CHIPS PARA FUNCIONAMIENTO INALÁMBRICO
1208
TERMINAL MINORISTA

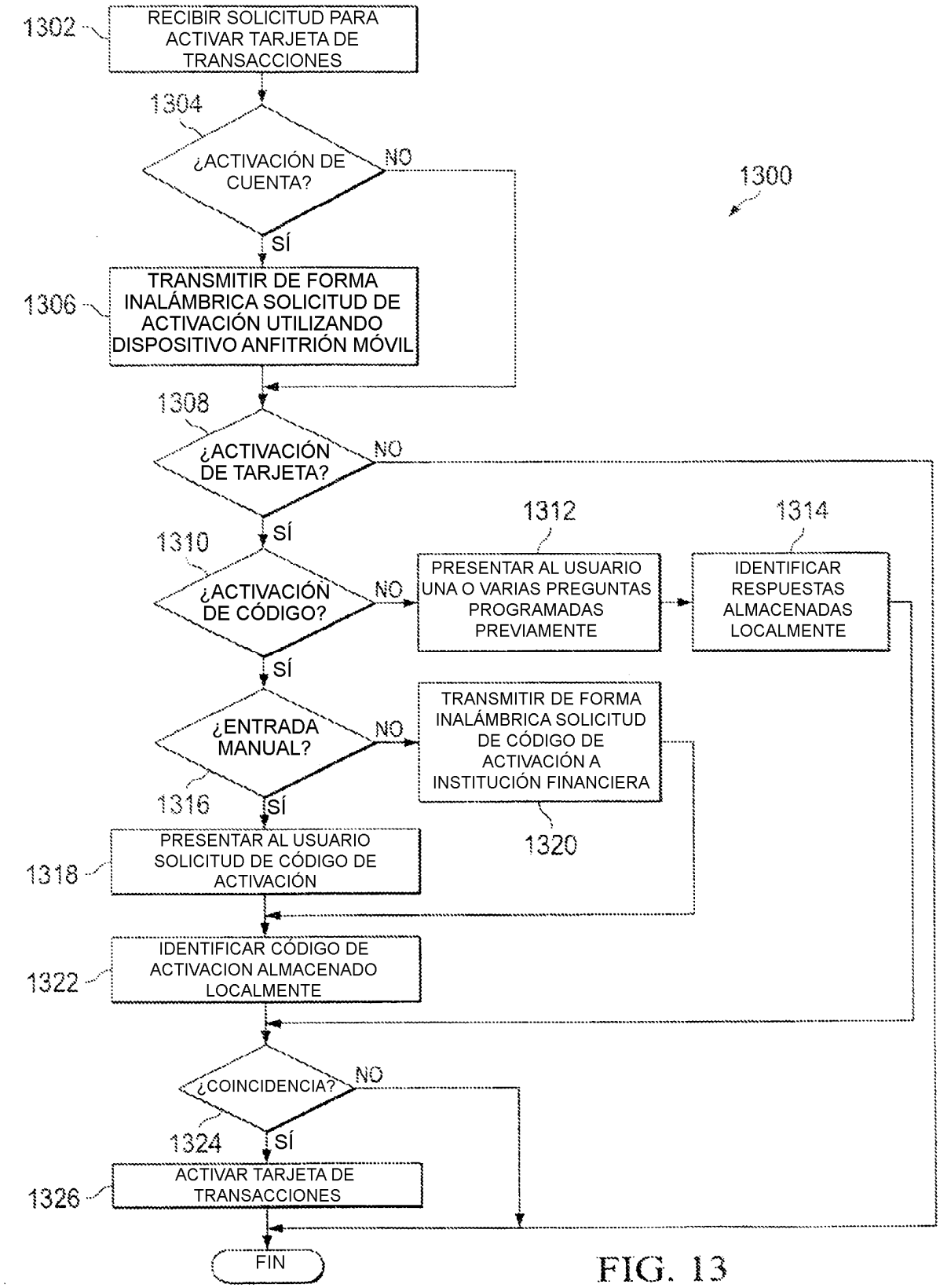

1302
RECIBIR SOLICITUD PARA ACTIVAR TARJETA DE TRANSACCIONES
1304
¿ACTIVACIÓN DE CUENTA?
NO
SÍ
1300
1306
TRANSMITIR DE FORMA INALÁMBRICA SOLICITUD DE ACTIVACIÓN UTILIZANDO DISPOSITIVO ANFITRIÓN MÓVIL
1308
¿ACTIVACIÓN DE TARJETA?
NO
SÍ
1310
¿ACTIVACIÓN DE CÓDIGO?
NO
SÍ
1312
PRESENTAR AL USUARIO UNA O VARIAS PREGUNTAS PROGRAMADAS PREVIAMENTE
1314
IDENTIFICAR RESPUESTAS ALMACENADAS LOCALMENTE
¿ENTRADA MANUAL?
NO
SÍ
1316
TRANSMITIR DE FORMA INALÁMBRICA SOLICITUD DE CÓDIGO DE ACTIVACIÓN A INSTITUCIÓN FINANCIERA
1320
1318
PRESENTAR AL USUARIO SOLICITUD DE CÓDIGO DE ACTIVACIÓN
1322
IDENTIFICAR CÓDIGO DE ACTIVACION ALMACENADO LOCALMENTE
¿COINCIDENCIA?
NO
SÍ
1324
1326
ACTIVAR TARJETA DE TRANSACCIONES
FIN

FIG. 13

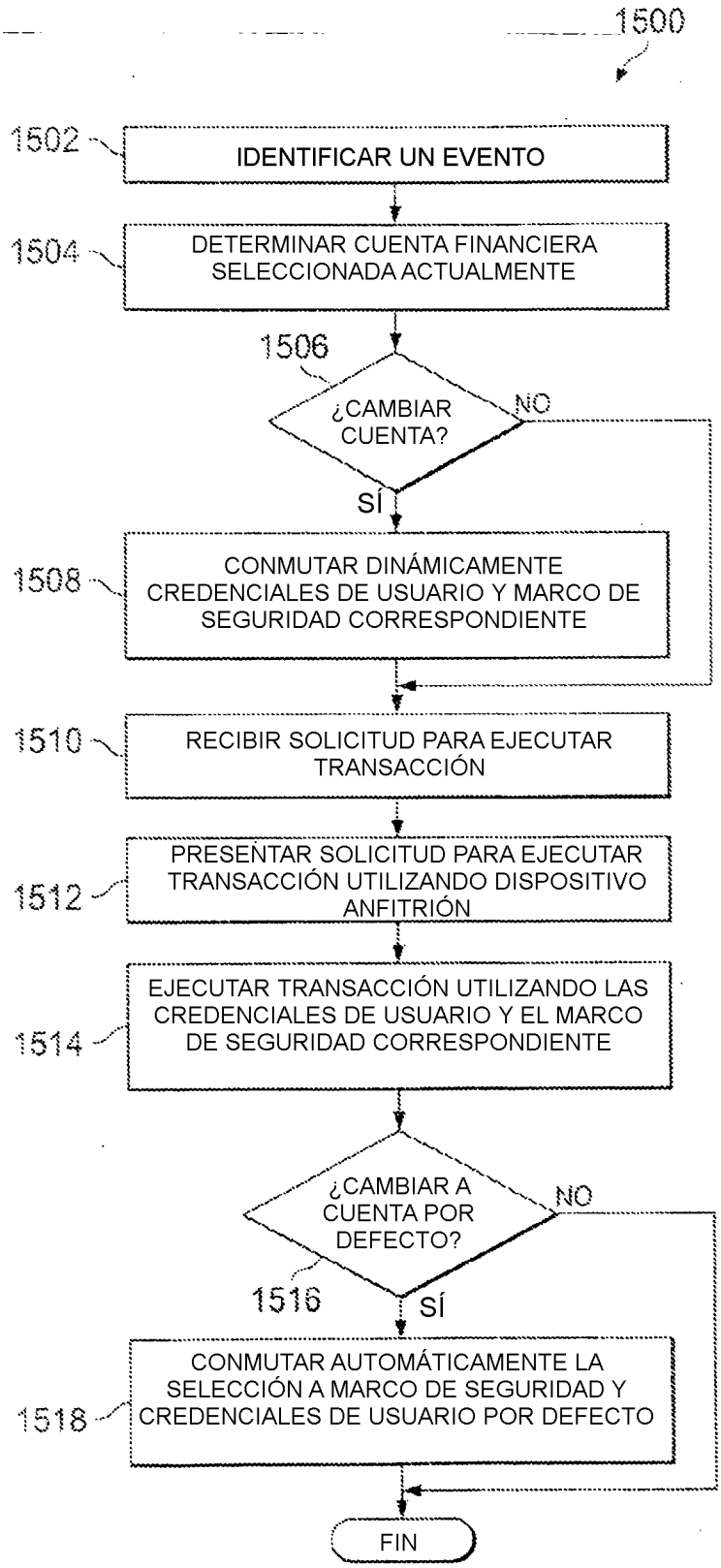

1500
1502
IDENTIFICAR UN EVENTO
1504
DETERMINAR CUENTA FINANCIERA SELECCIONADA ACTUALMENTE
1506
¿CAMBIAR CUENTA?
NO
SÍ
1508
CONMUTAR DINÁMICAMENTE CREDENCIALES DE USUARIO Y MARCO DE SEGURIDAD CORRESPONDIENTE
1510
RECIBIR SOLICITUD PARA EJECUTAR TRANSACCIÓN
1512
PRESENTAR SOLICITUD PARA EJECUTAR TRANSACCIÓN UTILIZANDO DISPOSITIVO ANFITRIÓN
1514
EJECUTAR TRANSACCIÓN UTILIZANDO LAS CREDENCIALES DE USUARIO Y EL MARCO DE SEGURIDAD CORRESPONDIENTE
¿CAMBIAR A CUENTA POR DEFECTO?
NO
1516
SÍ
1518
CONMUTAR AUTOMÁTICAMENTE LA SELECCIÓN A MARCO DE SEGURIDAD Y CREDENCIALES DE USUARIO POR DEFECTO
FIN

FIG. 15