(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 723 276**

(51) Int. CI.:

G08B 13/24 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **25.06.2013 PCT/US2013/047465**

(87) Fecha y número de publicación internacional: **27.03.2014 WO14046760**

(96) Fecha de presentación y número de la solicitud europea: **25.06.2013 E 13737725 (5)**

(97) Fecha y número de publicación de la concesión europea: **13.03.2019 EP 2909821**

(54) Título: **Plataforma periférica móvil de venta minorista para dispositivos portátiles**

(30) Prioridad:

21.09.2012 US 201261704061 P
28.05.2013 US 201313903282

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
23.08.2019

(73) Titular/es:

SENSORMATIC ELECTRONICS, LLC (100.0%)
6600 Congress Avenue
Boca Raton, FL 33487, US

(72) Inventor/es:

RASBAND, PAUL BRENT;
SEQUEIRA, MELWYN;
PATTERSON, HUBERT A. y
EASTER, RONALD B.

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Plataforma periférica móvil de venta minorista para dispositivos portátiles

Referencia cruzada a solicitudes relacionadas

Esta solicitud es una aplicación no provisional de la Solicitud Provisional de EE. UU. n.º 61/704.061 presentada el 21 de septiembre de 2012.

Antecedentes de la invención

Declaración del campo técnico

Los acuerdos de la invención se relacionan con los sistemas y métodos para desactivar una etiqueta de vigilancia electrónica de artículos ("EAS") en un punto de venta móvil ("POS"). Más particularmente, las disposiciones de la invención se refieren a sistemas y métodos para desactivar una etiqueta EAS utilizando un dispositivo periférico de un dispositivo móvil (por ejemplo, un teléfono móvil o dispositivo informático).

Descripción de la técnica relacionada

Un sistema EAS típico en un establecimiento al por menor puede comprender un sistema de monitoreo y al menos una etiqueta o marcador de seguridad adjunto a un artículo que se debe proteger contra la eliminación no autorizada. El sistema de monitoreo establece una zona de vigilancia en la que se puede detectar la presencia de etiquetas y/o marcadores de seguridad. La zona de vigilancia generalmente se establece en un punto de acceso para el área controlada (por ejemplo, adyacente a la entrada y/o salida de una tienda al por menor). Si un artículo ingresa a la zona de vigilancia con una etiqueta y/o marcador de seguridad activa, luego se puede activar una alarma para indicar una posible eliminación no autorizada de la misma del área controlada. En contraste, Si un artículo está autorizado para ser retirado del área controlada, entonces la etiqueta y/o marcador de seguridad del mismo puede desactivarse y/o separarse del mismo. En consecuencia, el artículo se puede transportar a través de la zona de vigilancia sin ser detectado por el sistema de monitoreo y/o sin disparar la alarma.

Actualmente, no hay una manera conveniente de desactivar una etiqueta EAS utilizando las unidades de POS móviles disponibles. Las opciones incluyen: el uso de una unidad de desactivación móvil además de una unidad de POS móvil; el uso de una unidad de desactivación fija ubicada dentro de una tienda al por menor que reduce la movilidad de la unidad móvil de POS; o el uso de una unidad de desactivación fija ubicada en una salida de una tienda al por menor que carga a los clientes con una tarea posterior al POS. Ninguna de estas opciones es satisfactoria para la adaptación de POS a gran escala en una industria al por menor.

También, no hay soporte general para la transferencia de datos de comunicación de campo cercano ("NFC") o de identificación por radiofrecuencia ("RFID") hacia y desde las unidades POS móviles. Incluso si algunos fabricantes comenzaran a implementar funciones NFC en algunos modelos de unidades móviles de POS, todavía habría algunas unidades de POS móviles que no son compatibles con NFC. Dichas unidades de POS móviles serían excluidas de consideración por cualquier al por menor que requiera soporte de NFC. Además, la funcionalidad y el soporte pasivos de RFID no se esperan de ninguno de los principales fabricantes de dispositivos de mano.

Adicionalmente, las unidades de POS móviles son frágiles y, por lo tanto, no cumplen con el nivel de protección y robustez necesario para las operaciones de tiendas minoristas normalmente rigurosas. Mantener la seguridad física de una unidad móvil de POS es un desafío que debe abordarse. Los dispositivos de mano y las tabletas representan una importante inversión de capital por parte de la empresa al por menor y pueden contener datos confidenciales de interés propietario para el al por menor. Por ello, Es importante prevenir el robo de tales dispositivos. Las soluciones adecuadas para prevenir dicho robo no están disponibles actualmente en el mercado. El documento US 5942978 revela un robo no está disponible actualmente en el mercado, el dispositivo de llave transmisora está anidado en una unidad de separación para indicar a la unidad de separación que retire las etiquetas duras reutilizables de los artículos de mercadería.

Un problema relacionado se relaciona con la búsqueda de hardware al por menor móvil perdido o fuera de lugar dentro de una tienda al por menor. Muchas tiendas minoristas son muy grandes. Por lo tanto, es posible que se requiera una cantidad significativa de mano de obra de los empleados para buscar ese hardware al por menor perdido o extraviado.

Sumario de la invención

La presente invención se refiere a sistemas y métodos para operar una etiqueta de seguridad de un sistema EAS. Los métodos implican ejecutar en un dispositivo móvil de POS una aplicación de software operativa para controlar las operaciones de un dispositivo periférico para facilitar el desempeño de una transacción de compra. Posteriormente, el dispositivo de POS móvil recibe una solicitud para separar la etiqueta de seguridad de un artículo.

En respuesta a la solicitud, un mensaje se comunica desde el dispositivo móvil POS al dispositivo periférico a través de una primera comunicación de corto alcance (por ejemplo, una comunicación Bluetooth). El mensaje está configurado para hacer que el dispositivo periférico realice operaciones para facilitar una separación de la etiqueta de seguridad del artículo. A continuación, una señal se comunica desde el dispositivo periférico de la etiqueta de seguridad. La señal provoca la activación de un mecanismo de separación de la etiqueta de seguridad y/o el calentamiento de un adhesivo dispuesto en la etiqueta de seguridad.

En algunos escenarios, el dispositivo periférico puede estar físicamente acoplado al dispositivo POS móvil. Por ejemplo, el dispositivo periférico puede incluir un espacio de inserción en el que el dispositivo de POS móvil puede estar dispuesto al menos parcialmente de manera que el dispositivo periférico puede envolverse alrededor de al menos una porción del dispositivo de POS móvil. Dichas configuraciones de acoplamiento permiten que el usuario o el vehículo lleven o usen fácilmente el dispositivo móvil POS y el dispositivo periférico.

En esos u otros escenarios, el método también implica: obtener acceso a un área segura de una tienda al por menor mediante la comunicación de una segunda comunicación de corto alcance (por ejemplo, una comunicación de campo cercano) desde el dispositivo periférico; y/u obtener acceso a equipos pesados mediante la comunicación de una tercera comunicación de corto alcance (por ejemplo, una comunicación de campo cercano) desde el dispositivo periférico. El dispositivo periférico también puede: obtener información del artículo para el artículo y/o información de identificación para la seguridad a través de una cuarta comunicación de corto alcance (por ejemplo, una comunicación de campo cercano o una comunicación de código de barras); y reenviar la información del artículo y/o la información de identificación al dispositivo móvil de POS a través de una quinta comunicación de corto alcance (por ejemplo, una comunicación Bluetooth). El dispositivo periférico puede además: obtener información de pago para el artículo utilizando un lector de tarjetas electrónico o una unidad de comunicación de corto alcance del mismo (por ejemplo, una unidad de comunicación de campo cercano o una unidad de comunicación de código de barras); y reenviar la información de pago al dispositivo móvil de POS a través de una sexta comunicación de corto alcance (por ejemplo, una comunicación Bluetooth). La información del artículo al por menor y/o la información del recibo pueden comunicarse desde el dispositivo periférico a un dispositivo de comunicación móvil mediante una comunicación de corto alcance (por ejemplo, una comunicación Bluetooth), también.

Breve descripción de los dibujos

Las realizaciones se describirán con referencia a las siguientes figuras de dibujo, en el que los números similares representan elementos similares en todas las figuras, y en los que:

La figura 1 es una ilustración esquemática de un sistema a modo de ejemplo que es útil para comprender la presente invención.
La figura 2 es un diagrama de bloques de una arquitectura a modo de ejemplo para una etiqueta de seguridad mostrada en la figura 1.
La figura 3 es un diagrama de bloques de una arquitectura a modo de ejemplo para un dispositivo de comunicación móvil mostrado en la figura 1.
La figura 4 es un diagrama de bloques de una arquitectura a modo de ejemplo para un dispositivo periférico mostrado en la figura 1.
La figura 5 es un diagrama de bloques de una arquitectura a modo de ejemplo para un sistema de desactivación de etiquetas mostrado en la figura 4.
La figura 6 es una vista en perspectiva de un dispositivo de comunicación móvil con un dispositivo periférico que es útil para comprender la presente invención.
La figura 7 es un diagrama de flujo de un método a modo de ejemplo para comprar un artículo de una tienda al por menor que es útil para comprender la presente invención.
La figura 8 es un diagrama de flujo de un proceso de transacción de compra a modo de ejemplo facilitado por un dispositivo de comunicación móvil (por ejemplo, una tableta o teléfono inteligente).
Las figuras 9A-9E proporcionan colectivamente un diagrama de flujo de un proceso a modo de ejemplo de separación de etiquetas de seguridad que es útil para comprender la presente invención.
La figura 10 es un diagrama de flujo de un proceso a modo de ejemplo para separar o desactivar una etiqueta de seguridad electromecánica utilizando un dispositivo periférico de un dispositivo de comunicación móvil.

Descripción detallada

Se entenderá fácilmente que los componentes de las realizaciones como se describen en general en este documento y se ilustran en las figuras adjuntas se podrían disponer y diseñar en una amplia variedad de configuraciones diferentes. Por ello, la siguiente descripción más detallada de varias realizaciones, como se representa en las figuras, no pretende limitar el ámbito de la presente invención, pero es meramente representativo de varias realizaciones. Mientras que los diversos aspectos de las realizaciones se presentan en dibujos, los dibujos no están necesariamente dibujados a escala a menos que se indique específicamente.

Las realizaciones descritas deben considerarse en todos los aspectos como ilustrativas. El alcance de la invención es, por lo tanto, indicado por las reivindicaciones adjuntas. Todos los cambios que se encuentren dentro del

significado y rango de equivalencia de las reclamaciones deben incluirse dentro de su alcance.

Referencia a través de esta especificación a las características, ventajas o un lenguaje similar no implica que todas las características y ventajas que pueden realizarse con la presente invención deban estar o estén en una forma de realización única de la invención. En su lugar, se entiende que el lenguaje que se refiere a las características y ventajas significa que una característica específica, ventaja o característica descrita en relación con una realización se incluye en al menos una realización de la presente invención. Por ello, discusiones de las características y ventajas, y lenguaje similar, a lo largo de la especificación podrá, pero no necesariamente, referirse a la misma realización.

Además, las características, ventajas y características de la invención descritas se pueden combinar de cualquier manera adecuada en una o más realizaciones. Un experto en la técnica relevante reconocerá, a la luz de la descripción aquí contenida, que la invención puede ponerse en práctica sin una o más de las características o ventajas específicas de una determinada realización. En otros casos, en ciertas realizaciones pueden reconocerse características y ventajas adicionales que pueden no estar presentes en todas las realizaciones de la invención.

Referencia a lo largo de esta especificación a "una realización", o lenguaje similar significa que un rasgo, estructura o característica particular descrita en relación con la realización indicada se incluye en al menos una realización de la presente invención. Por ello, las frases "en una realización", y un lenguaje similar a lo largo de esta especificación puede, pero no necesariamente, referirse todo a la misma realización.

Como se usa en este documento, la forma singular “un/a”, y "el/la" incluyen referencias plurales a menos que el contexto indique claramente lo contrario. A menos que se defina lo contrario, todos los términos técnicos y científicos utilizados en este documento tienen los mismos significados que entiende comúnmente un experto en la técnica. Como se usa en este documento, el término "que comprende" significa "que incluye, pero no se limita a”.

Ahora se describirán realizaciones con respecto a las figuras 1-10. Las realizaciones generalmente se relacionan con los sistemas y métodos para operar una etiqueta de seguridad de un sistema EAS. Los métodos implican el acoplamiento físico de un dispositivo periférico a un dispositivo de POS móvil. Por ejemplo, el dispositivo periférico puede incluir un espacio de inserción en el que el dispositivo de POS móvil puede estar dispuesto al menos parcialmente de manera que el dispositivo periférico puede envolverse alrededor de al menos una porción del dispositivo de POS móvil. Dichas configuraciones de acoplamiento permiten que un dispositivo o dispositivo móvil POS y un dispositivo periférico sean fácilmente adquiridos o usados por un usuario o vehículo. Los métodos también involucran: instalar una aplicación y/o complemento en un dispositivo móvil de POS que sea operativo para facilitar el control de un dispositivo periférico; recibir, mediante el dispositivo móvil de POS, una solicitud para separar la etiqueta de seguridad de un artículo; y comunicar un mensaje desde el dispositivo de POS móvil a su dispositivo periférico a través de una primera comunicación de corto alcance (por ejemplo, una comunicación Bluetooth). El mensaje generalmente está configurado para hacer que el dispositivo periférico realice operaciones para facilitar una separación de la etiqueta de seguridad del artículo. Posteriormente, se transmite una señal desde el dispositivo periférico a la etiqueta de seguridad para provocar la activación de un mecanismo de separación de la etiqueta de seguridad. El mecanismo de separación puede incluir, pero no se limita a, un mecanismo de separación electromecánico. La porción de separación mecánica del mecanismo de separación electromecánico puede incluir, pero no se limita a, un alfiler, un cordón, y/o un adhesivo.

A continuación, haciendo referencia a la figura 1, se proporciona una ilustración esquemática de un sistema a modo de ejemplo **100** que es útil para comprender la presente invención. El sistema **100** generalmente está configurado para permitir que un cliente compre un artículo **102** utilizando un dispositivo de comunicación móvil ("MCD") **104** y un dispositivo periférico ("PD") **190** de este. El PD **190** está diseñado para ser unido mecánicamente al MCD **104**. En algunos escenarios, el PD **190** envuelve al menos una porción del MCD **104**. Las comunicaciones entre MCD **104** y PD **190** se logran utilizando una tecnología de comunicación inalámbrica de corto alcance ("SRC"), tal como una tecnología Bluetooth. El PD **190** también emplea otras tecnologías SRC inalámbricas para facilitar la compra del artículo **102**. Las otras tecnologías inalámbricas SRC pueden incluir, pero no se limitan a, tecnología de comunicación de campo cercano (“NFC”), tecnología infrarroja (“IR”). tecnología de fidelidad inalámbrica (“Wi-Fi”), tecnología de identificación por radiofrecuencia ("RFID") y/o tecnología ZigBee, El PD **190** también puede emplear tecnología de código de barras, tecnología de lector de tarjeta electrónica y tecnología de comunicaciones de la red de sensores inalámbricos ("WSN").

Como se muestra en la figura 1, el sistema **100** comprende una instalación de tienda al por menor **150** que incluye un EAS **128**. El EAS **128** comprende un sistema de monitoreo **134** y al menos una etiqueta de seguridad **132**. Aunque no se muestra en la figura 1, la etiqueta de seguridad **132** se adjunta al artículo **102**, protegiendo así el artículo **102** de una remoción no autorizada de la tienda al por menor **150**. El sistema de monitoreo **134** establece una zona de vigilancia (no mostrada) dentro de la cual se puede detectar la presencia de la etiqueta de seguridad **132**. La zona de vigilancia se establece en un punto de acceso (no se muestra) para la tienda al por menor **150**. Si la etiqueta de seguridad **132** es llevada a la zona de vigilancia, luego se activa una alarma para indicar una posible eliminación no autorizada del artículo **102** de las instalaciones de la tienda al por menor **150**.
Durante las horas de la tienda, un cliente **140** puede desear comprar el artículo **102**. El cliente **140** puede comprar el

artículo **102** sin utilizar una estación POS tradicional fija (por ejemplo, un contador de pago y envío). En su lugar, la transacción de compra se puede lograr utilizando el MCD **104** y el PD **190**, como se ha mencionado anteriormente. El MCD **104** (por ejemplo, una tableta) puede estar en posesión del cliente **140** o de la tienda asociada **142** en el momento de la transacción de compra. Una arquitectura a modo de ejemplo del MCD **104** se describirá a continuación en relación con la figura 3. Una arquitectura a modo de ejemplo del PD **190** se describirá a continuación en relación con la figura 4. Todavía, debe entenderse que el MCD **104** tiene una aplicación de transacción al por menor instalada en la misma que está configurada para facilitar la compra del artículo **102** y la gestión/control de las operaciones del PD **190** para una unión/separación de la etiqueta de seguridad **132** al/del artículo **102**. La aplicación de transacción al por menor puede ser una aplicación preinstalada, una aplicación complementaria o una aplicación complementaria.

Para iniciar una transacción de compra, la aplicación de transacción al por menor se inicia a través de una interacción usuario-software. La aplicación de transacción al por menor facilita el intercambio de datos entre el artículo **102**, la etiqueta de seguridad **132**, el cliente **140**, la tienda asociada **142** y/o sistema de transacciones minoristas ("RTS") **118**. Por ejemplo, después del lanzamiento de la aplicación de transacción al por menor, se le solicita a un usuario **140**, **142** que comience un proceso de transacción al por menor para comprar el artículo **102**. El proceso de transacción al por menor puede iniciarse simplemente realizando una interacción de software de usuario, como presionar la tecla en un teclado del MCD **104** o tocar un botón en una pantalla táctil del MCD **104**.

Después, el usuario **140**, **142** puede ingresar manualmente en la información de artículos de la aplicación de transacción al por menor. Alternativa o adicionalmente, el usuario **140**, **142** coloca el MCD **104** en la proximidad del artículo **102**. Como resultado de esta colocación, el PD **190** obtiene información del artículo del artículo **102**. La información del artículo incluye cualquier información que sea útil para comprar el artículo **102**, como un identificador de artículo y un precio de compra de artículo. En algunos escenarios, La información del artículo puede incluir incluso un identificador de la etiqueta de seguridad **132** adjunta a la misma. La información del artículo se puede comunicar desde el artículo **102** al PD **190 a** través de una comunicación de corto alcance, tal como una comunicación de código de barras **122** o una NFC **120**.

En el caso de código de barras, el artículo **102** tiene un código de barras **128** unido a una superficie expuesta del mismo. El término "código de barras", como se usa en el presente documento, se refiere a un patrón o símbolo que contiene datos incrustados. Los códigos de barras pueden incluir, por ejemplo, códigos de barras unidimensionales, códigos de barras bidimensionales (como códigos de matriz). códigos de respuesta rápida ("QR"), códigos aztecas y similares), o códigos de barras tridimensionales. Los datos incrustados pueden incluir, pero no se limita a, un identificador único del artículo **102** y/o un precio de compra del artículo **102**. El código de barras **128** es leído por un escáner/lector de código de barras (no mostrado en la figura 1) del PD **190**. Los escáneres/lectores de códigos de barras son bien conocidos en la técnica. Cualquier escáner/lector de código de barras conocido o que se conozca se puede usar aquí sin limitación.

En los escenarios de NFC, el artículo **102** puede comprender un dispositivo **126** habilitado para NFC. El dispositivo **126** habilitado para NFC puede estar separado de la etiqueta de seguridad **132** o comprender la etiqueta de seguridad **132**. Se produce una comunicación NFC **120** entre el dispositivo **126** habilitado para NFC y el PD **190** en una distancia relativamente pequeña (por ejemplo, N centímetros o N pulgadas, donde N es un número entero como doce). La comunicación NFC **120** se puede establecer tocando los componentes **126**, **190** juntos o acercándolos a una proximidad tal que se produzca un acoplamiento inductivo entre sus circuitos inductivos. En algunos escenarios, la NFC funciona a 13,56 MHz y a tasas que van desde 06 kbit/s a **848** kbit/s. La NFC se puede lograr utilizando transceptores NFC configurados para permitir la comunicación sin contacto a 13,56 MHz. Los transceptores NFC son bien conocidos en la técnica y, por lo tanto, no se describirán en detalle en este documento. Cualquier transceptor NFC conocido o que se conozca se puede usar en este documento sin limitación.

Después de que el PD **190** obtiene la información del artículo, lo reenvía al MCD **104 a** través de un SRC inalámbrico, como una comunicación Bluetooth. Posteriormente, la información de pago se ingresa en la aplicación de transacción al por menor del MCD **104** por parte del usuario **140**, **142.** La información de pago puede incluir, pero no se limita a, un código de fidelidad del cliente, información de la tarjeta de pago, y/o información de la cuenta de pago. La información de pago se puede introducir manualmente, a través de un lector de tarjetas electrónico (por ejemplo, un lector de tarjetas de banda magnética), o mediante un lector de código de barras. Los lectores de tarjetas electrónicas y los lectores de códigos de barras son bien conocidos en la técnica y, por lo tanto, no se describen en este documento. Cualquier lector de tarjetas electrónicas y/o de códigos de barras conocido o que se conozca se puede usar en este documento sin limitación. La información de pago puede obtenerse de forma alternativa o adicional de un almacén de datos remoto basado en un identificador de cliente o un identificador de cuenta. En este caso, la información de pago se puede recuperar de los datos almacenados asociados a una venta anterior de un artículo al cliente **140**.

Al obtener la información de pago, el MCD **104** realiza automáticamente operaciones para establecer una sesión de transacción al por menor con el RTS **118**. La sesión de transacciones minoristas puede implicar: comunicar la información del artículo y la información de pago del MCD **104** al RTS **118 a** través de una comunicación RF **124** y una red pública **106** (por ejemplo, Internet); completar una transacción de compra por el RTS **118**; y comunicar un

mensaje de respuesta desde el RTS **118** al MCD **104** que indica que el artículo **102** se ha comprado con éxito o sin éxito. La transacción de compra puede implicar el uso de un sistema de pago autorizado, como un sistema de pago bancario de la Cámara de Compensación Automática ("ACH"), un sistema de autorización de tarjeta de crédito/débito, o un sistema de terceros (por ejemplo, PayPal®, SolidTrust Pay® o Google Wallet®).

Notablemente, Las comunicaciones entre MCD **104** y el dispositivo informático **108** pueden ser comunicaciones seguras en las que se emplea la criptografía. En tales escenarios, una clave criptográfica también se puede comunicar desde MCD **104** a RTS **118**, o viceversa. La clave criptográfica puede ser una clave criptográfica de un solo uso. Cualquier tipo de criptografía se puede emplear en este documento sin limitación.

El RTS **118** puede completar la transacción de compra utilizando la información del artículo y la información de pago. En este sentido, dicha información puede ser recibida por un dispositivo informático **108** del RTS **118** y reenviada a un subsistema de una red privada **100** (por ejemplo, una intranet). Por ejemplo, la información del artículo y la información de compra también pueden ser enviadas y procesadas por un subsistema de compra **112** para completar una transacción de compra. Cuando se completa la transacción de compra, se genera un mensaje y se envía al MCD **104** que indica si el artículo **102** se ha comprado con éxito o sin éxito.

Si el artículo **102** ha sido comprado con éxito, luego, el RTS **118** o el MCD **104** pueden iniciar automáticamente un proceso de separación de etiquetas de seguridad. Alternativamente, el usuario **140**, **142** puede iniciar el proceso de separación de la etiqueta de seguridad realizando una interacción de software de usuario utilizando el MCD **104**. En los tres escenarios, la información del artículo puede ser enviada y procesada por un subsistema de liberación de bloqueo **114** para recuperar una clave de separación o un código de separación que es útil para separar la etiqueta de seguridad **132** del artículo **102**. La clave o código de separación se envía desde el RTS **118** al MCD **104,** de modo que el MCD **104** puede hacer que el PD **190** realice operaciones de separación de etiquetas. Las operaciones de separación de etiquetas del PD **190** están configuradas generalmente para hacer que la etiqueta de seguridad **132** accione un mecanismo de separación (no mostrado en la figura 1). En este sentido, el PD **190** genera un comando de desconexión y envía una señal de desconexión inalámbrica que incluye el comando de desconexión a la etiqueta de seguridad **132**. La etiqueta de seguridad **132** autentica el comando de desconexión y activa el mecanismo de desconexión. Por ejemplo, el comando de separación hace que se libere un alfiler, un cordón para liberar, y/o un adhesivo para calentar de tal manera que la etiqueta de seguridad pueda separarse del artículo **102**. El adhesivo se puede calentar a través del calentamiento actual y/o del calentamiento por RF. Una vez que la etiqueta de seguridad **132** se ha separado del artículo **102**, el cliente **140** puede llevar el artículo **102 a** través de la zona de vigilancia sin activar la alarma.

Alternativa o adicionalmente en los tres escenarios de separación de etiquetas de seguridad, el MCD **104** puede indicar al usuario **140**, **142** para obtener un identificador único (no mostrado en la figura 1) para la etiqueta de seguridad **132**. El identificador único se puede obtener manualmente del usuario **140**, **142** o a través de una comunicación inalámbrica, tal como una comunicación de código de barras o una comunicación NFC.

En el caso de código de barras, la etiqueta de seguridad **132** tiene un código de barras **138** unido a una superficie expuesta del mismo. El código de barras comprende un patrón o símbolo que contiene datos incrustados. Los datos incrustados pueden incluir, pero no se limita a, un identificador único de la etiqueta de seguridad **132** y/o un identificador único del artículo **102** que está asegurado de ese modo. El código de barras **138** es leído por un escáner/lector de código de barras (no mostrado en la figura 1) del PD **190**.

En el escenario NFC, la etiqueta de seguridad **132** puede comprender un dispositivo **136** habilitado para NFC. Una comunicación NFC (no mostrada en la figura 1) ocurre entre el dispositivo **136** habilitado para NFC y el PD **190** en una distancia relativamente pequeña (por ejemplo, N centímetros o N pulgadas, donde N es un número entero como doce). La comunicación NFC se puede establecer tocando los componentes **136**, **190** juntos o acercándolos a una proximidad tal que se produzca un acoplamiento inductivo entre sus circuitos inductivos. La NFC se puede lograr utilizando transceptores NFC configurados para permitir la comunicación sin contacto a 13,56 MHz.

Una vez obtenido el identificador único para la etiqueta de seguridad **132**, El PD **190** comunica lo mismo al MCD **104**. A su vez, el MCD **104** comunica el identificador único al RTS **118** a través de la red **106** (por ejemplo, Internet o una red de telefonía móvil) y la comunicación por RF **124**. En el RTS **118**, el identificador único se procesa por varias razones. En este sentido, el dispositivo informático **108** puede recibir el identificador único y reenviarlo al subsistema de liberación de bloqueo **114** para recuperar la clave o código de separación que es útil para separar la etiqueta de seguridad **132** del artículo **102**. La clave o código de separación se envía desde el RTS **118** al MCD **104**. El MCD **104** reenvía la clave o código de separación a PD **190,** de modo que el PD **190** puede hacer que la etiqueta de seguridad **132** accione un mecanismo de separación (no mostrado en la figura 1) de la misma manera que se describió anteriormente.

En vista de lo anterior, el subsistema de liberación de bloqueo **114** puede comprender un almacén de datos en el que las claves de separación y/o los códigos de separación se almacenan en asociación con identificadores únicos para una pluralidad de artículos y/o etiquetas de seguridad, respectivamente. Cada llave de separación puede incluir, pero no se limita a, al menos un símbolo seleccionado para accionar un mecanismo de separación de una etiqueta

de seguridad respectiva. En algunos escenarios, la clave de separación puede ser una clave de separación de uso de una sola vez en la que permite la separación de una etiqueta de seguridad solo una vez durante un período de tiempo determinado (por ejemplo, N días, N semanas, N meses, o N años, donde N es un número entero igual o mayor que 1). Cada código de destacamento puede incluir, pero no se limita a, al menos un símbolo del cual se puede derivar o generar una clave de separación. La clave de separación puede ser derivada o generada por el MCD **104**, el RTS **118**, y/o el PD **190**. La clave y/o el código de separación pueden almacenarse de manera segura dentro del MCD **104**, PD **190** o el RTS **118**, como se discutirá a continuación. En el caso de que la clave sea generada por el MCD **104** o el PD **190**, Las operaciones de generación de claves se realizan de manera segura. Por ejemplo, el algoritmo para generar la clave puede ser realizado por un procesador con un gabinete a prueba de manipulaciones, de tal manera que si una persona intenta maliciosamente extraer el algoritmo del procesador, el algoritmo se borrará antes de cualquier acceso no autorizado al mismo.

Aunque la figura 1 se muestra con dos instalaciones (a saber, la instalación de la tienda al por menor **150** y la instalación corporativa **152**), La presente invención no está limitada a este respecto. Por ejemplo, las instalaciones **150**, **152** pueden residir en el mismo o diferente edificio o área geográfica. Alternativa o adicionalmente, las instalaciones **150**, **152** pueden ser las mismas o diferentes subpartes de una instalación más grande.

A continuación, haciendo referencia a la figura 2, se proporciona una ilustración esquemática de una arquitectura a modo de ejemplo para la etiqueta de seguridad **132**. La etiqueta de seguridad **132** puede incluir más o menos componentes que los que se muestran en la figura 2. Sin embargo, los componentes mostrados son suficientes para divulgar una realización ilustrativa que implementa la presente invención. Algunos o todos los componentes de la etiqueta de seguridad **132** pueden implementarse en hardware, software y/o una combinación de hardware y software. El hardware incluye, pero no se limita a, uno o más circuitos electrónicos.

La arquitectura de hardware de la figura 2 representa una realización de una etiqueta de seguridad representativa **132** configurada para facilitar la prevención de una eliminación no autorizada de un artículo (por ejemplo, el artículo **102** de la figura 1) de una tienda al por menor (por ejemplo, la instalación de la tienda al por menor **150** de la figura 1). En este sentido, la etiqueta de seguridad **132** puede tener un código de barras **138** pegado a la misma para permitir el intercambio de datos, un dispositivo externo (por ejemplo, PD **190** de la figura 1) a través de la tecnología de código de barras.

La etiqueta de seguridad **132** también incluye una antena **202** y un dispositivo habilitado para NFC **136** para permitir el intercambio de datos con el dispositivo externo a través de la tecnología NFC. La antena **202** está configurada para recibir señales NFC desde el dispositivo externo y transmitir señales NFC generadas por el dispositivo **136** habilitado para NFC. El dispositivo **136** habilitado para NFC comprende un transceptor NFC **204**, los transceptores NFC son bien conocidos en la técnica y, por lo tanto, no se describirán aquí. Sin embargo, debe entenderse que el transceptor NFC **204** procesa las señales NFC para extraer información en el mismo. Esta información puede incluir, pero no se limita a, una solicitud de cierta información (por ejemplo, un identificador único **210**), y/o un mensaje que incluye información que especifica una clave o código de separación para separar la etiqueta de seguridad **132** de un artículo. El transceptor NFC **204** puede pasar la información extraída al controlador **206**.

Si la información extraída incluye una solicitud de cierta información, luego, el controlador **206** puede realizar operaciones para recuperar un identificador único **210** y/o información de artículo **214** de la memoria **208**. La información del artículo **214** puede incluir un identificador único de un artículo y/o un precio de compra del artículo. La información recuperada se envía luego desde la etiqueta de seguridad **132** a un dispositivo externo solicitante (por ejemplo, PD **190** de la figura 1) a través de una comunicación NFC.

En contraste, si la información extraída incluye información que especifique una clave de uso único y/o instrucciones para programar la etiqueta de seguridad **132** para activar un mecanismo de separación **250** de un mecanismo de bloqueo electromecánico **216**, luego, el controlador **206** puede realizar operaciones para simplemente accionar el mecanismo de separación **250** usando la tecla de una sola vez. Alternativa o adicionalmente, el controlador **206** puede: analizar la información de un mensaje recibido; recuperar una clave/código de separación **212** de la memoria **208**; y compare la información analizada con el código/clave de separación para determinar si existe una coincidencia entre ellos. Si existe una coincidencia, luego, el controlador **206** genera y envía un comando al mecanismo de bloqueo electromecánico **216** para accionar el mecanismo de separación **250**. Una indicación auditiva o visual puede ser emitida por la etiqueta de seguridad **132** cuando se acciona el mecanismo de separación **250**. Si una coincidencia no existe, luego, el controlador **206** puede generar un mensaje de respuesta que indica que la clave/código de separación especificado en la información extraída no coincide con la clave/código **212** de separación almacenada en la memoria **208**. El mensaje de respuesta puede luego enviarse desde la etiqueta de seguridad **132** a un dispositivo externo solicitante (por ejemplo, PD **190** de la figura 1) a través de una comunicación inalámbrica de corto alcance o una comunicación por cable a través de la interfaz **260**. Un mensaje también puede comunicarse a otro dispositivo externo o nodo de red a través de la interfaz **260**.

En algunos escenarios, las conexiones entre los componentes **204**, **206, 208, 216, 260** son conexiones no seguras o conexiones seguras. La frase “conexión insegura”, como se usa en el presente documento, se refiere a una conexión en la que no se emplean medidas a prueba de manipulación o criptografía. La frase “conexión segura”, como se usa

en el presente documento, se refiere a una conexión en la que se emplean medidas a prueba de manipulación y criptografía. Tales medidas a prueba de manipulación indebida incluyen encerrar el enlace eléctrico físico entre dos componentes en una carcasa a prueba de manipulación indebida.

Notablemente, la memoria **208** puede ser una memoria volátil y/o una memoria no volátil. Por ejemplo, La memoria **208** puede incluir, pero no se limita a, una memoria de acceso aleatorio (“RAM”), una memoria de acceso aleatorio dinámico ("DRAM"), una memoria estática de acceso aleatorio ("SRAM"), una memoria de solo lectura (“ROM”) y una memoria flash. La memoria **208** también puede comprender memoria no segura y/o memoria segura. La frase "memoria insegura", como se usa en el presente documento, se refiere a la memoria configurada para almacenar datos en forma de texto simple. La frase "memoria segura", como se usa en el presente documento, se refiere a la memoria configurada para almacenar datos en una forma cifrada y/o memoria que tiene o está dispuesta en un recinto seguro o a prueba de manipulaciones.

El mecanismo de bloqueo electromecánico **216** es operable para accionar el mecanismo de separación **250**, El mecanismo de separación **250** puede incluir un bloqueo configurado para moverse entre un estado de bloqueo y un estado de desbloqueo. Tal bloqueo puede incluir, pero no se limita a, un alfiler o un cordón. En algunos escenarios, el mecanismo de separación **250** puede comprender adicional o alternativamente un adhesivo que puede calentarse mediante calentamiento por corriente o calentamiento por RF.
El mecanismo de bloqueo electromecánico **216** se muestra como acoplado indirectamente al transceptor NFC **204** a través del controlador **206**. La invención no está limitada a este respecto. El mecanismo de bloqueo electromecánico **216** se puede acoplar adicional o alternativamente directamente al transceptor NFC **204**, uno o más de los componentes **204**, **206** puede hacer que el bloqueo del mecanismo de separación **250** sea transicionado entre estados de acuerdo con la información recibida desde un dispositivo externo (por ejemplo, PD **190** de la figura 1), Los componentes **204** - **208**, **260** y una batería **220** pueden denominarse colectivamente en este documento como el dispositivo **136** habilitado para NFC.

El dispositivo **136** habilitado para NFC puede incorporarse a un dispositivo que también alberga el mecanismo de bloqueo electromecánico **216**, o puede ser un dispositivo separado que está en comunicación directa o indirecta con el mecanismo de bloqueo electromecánico **216**. El dispositivo **136** habilitado para NFC está acoplado a una fuente de alimentación. La fuente de alimentación puede incluir, pero no se limita a, batería **220** o una conexión de alimentación de A/C (no mostrada). Alternativa o adicionalmente, el dispositivo **136** habilitado para NFC está configurado como un dispositivo pasivo que deriva energía de una señal de RF acoplada inductivamente al mismo.

En algunos escenarios, también se puede proporcionar un mecanismo de bloqueo mecánico-magnético **222** con la etiqueta de seguridad **132**. Los mecanismos de bloqueo mecánico-magnético son bien conocidos en la técnica y, por lo tanto, no se describirán en detalle en este documento. Todavía, debe entenderse que tales mecanismos de bloqueo se separan utilizando herramientas magnéticas y mecánicas.

A continuación, haciendo referencia a la figura 3, se proporciona un diagrama de bloques más detallado de una arquitectura a modo de ejemplo para el MCD **104** de la figura 1. En algunos escenarios, dispositivo informático **108** de la figura 1 es igual o similar al MCD **104**. En consecuencia, la siguiente discusión del MCD **104** es suficiente para comprender el dispositivo informático **108** de la figura 1.

El MCD **104** puede incluir, pero no se limita a, un ordenador de tableta, un ordenador portátil, un asistente digital personal, un teléfono celular o un teléfono móvil con funcionalidad de dispositivo inteligente (por ejemplo, un teléfono inteligente). El MCD **104** puede incluir más o menos componentes que los mostrados en la figura 3. Sin embargo, los componentes mostrados son suficientes para divulgar una realización ilustrativa que implementa la presente invención. Algunos o todos los componentes del MCD **104** pueden implementarse en hardware, software y/o una combinación de hardware y software. El hardware incluye, pero no se limita a, uno o más circuitos electrónicos.

La arquitectura de hardware de la figura 3 representa una realización de un MCD **104** representativo configurado para facilitar el intercambio de datos (a) entre un artículo (por ejemplo, el artículo **102** de la figura 1) y un RTS (por ejemplo, un RTS **118** de la figura 1) a través de tecnología de comunicación de corto alcance y/o tecnología móvil y (b) entre una etiqueta de seguridad (por ejemplo, la etiqueta de seguridad **132** de la figura 1) y el RTS a través de tecnología de comunicación de corto alcance y/o tecnología móvil. En este sentido, el MCD **104** comprende una antena **302** para recibir y transmitir señales de RF. Un interruptor de recepción/transmisión ("Rx/Tx") **304** acopla selectivamente la antena **302** al circuito transmisor **306** y al circuito receptor **308** de una manera familiar para los expertos en la materia. El circuito receptor **308** demodula y decodifica las señales de RF recibidas desde una red (por ejemplo, la red **106** de la figura 1). El circuito receptor **308** está acoplado a un controlador (o microprocesador) **310** a través de una conexión eléctrica **334**. El circuito receptor **308** proporciona la información de la señal decodificada al controlador **310**. El controlador **310** utiliza la información de señal de RF descodificada de acuerdo con la función(es) del MCD **104**.

El controlador **310** también proporciona información al circuito transmisor **306** para codificar y modular información en señales de RF. En consecuencia, el control ler **310** está acoplado a la circuitería transmisora **306** a través de una conexión eléctrica **338**. El circuito transmisor **306** comunica las señales de RF a la antena **302** para su transmisión a

un dispositivo externo (por ejemplo, un nodo de una red **106** de la figura 1) a través del interruptor Rx/Tx **304**.

Una antena **340** puede estar acoplada a una unidad de comunicación SRC **314** para recibir señales SRC. En algunos escenarios, la unidad de comunicación SRC **314** implementa la tecnología Bluetooth. En consecuencia, La unidad de comunicación SRC **314** puede comprender un transceptor Bluetooth. Los transceptores Bluetooth son bien conocidos en la técnica y, por lo tanto, no se describirán en detalle en este documento. Sin embargo, se debe entender que el transceptor Bluetooth procesa las señales de Bluetooth para extraer información del mismo. El transceptor Bluetooth puede procesar las señales Bluetooth de una manera definida por una aplicación SRC **354** instalada en el MCD **104**. La aplicación SRC **354** puede incluir, pero no se limita a, una aplicación comercial fuera de la plataforma ("COTS"). El transceptor Bluetooth proporciona la información extraída al controlador **310**. En consecuencia, la unidad de comunicación SRC **314** está acoplada al controlador **310** a través de una conexión eléctrica **336**. El controlador **310** utiliza la información extraída de acuerdo con las funciones del MCD **104**. Por ejemplo, el MCD **104** puede utilizar la información extraída para generar una solicitud de una clave o código de separación asociado a una etiqueta de seguridad en particular (por ejemplo, etiqueta de seguridad **132** de la figura 1) de un RTS (por ejemplo, un RTS **118** de la figura 1). Posteriormente, el MCD **104** envía la solicitud al RTS a través de los circuitos de transmisión **306** y la antena **302**.

El controlador **310** puede almacenar la información recibida y extraída en la memoria **312** del MCD **104**. En consecuencia, la memoria **312** está conectada y es accesible por el controlador **310** a través de la conexión eléctrica **332**. La memoria **312** puede ser una memoria volátil y/o una memoria no volátil. Por ejemplo, La memoria **312** puede incluir, pero no está limitada a, una memoria RAM, una DRAM, una SRAM, una ROM y una memoria flash. La memoria **312** también puede comprender memoria no segura y/o memoria segura. La memoria **212** se puede usar para almacenar otros tipos de información en ella, como la información de autenticación, información criptográfica, información de ubicación e información varia relacionada con el servicio.

Como se muestra en la figura 3, uno o más conjuntos de instrucciones **350** se almacenan en la memoria **312**. Las instrucciones **350** pueden incluir instrucciones personalizables e instrucciones no personalizables. Las instrucciones **350** también pueden residir, total o al menos parcialmente, dentro del controlador **310** durante la ejecución del mismo por MCD **104**. En este sentido, la memoria **312** y el controlador **310** pueden constituir medios legibles por máquina. El término "medios legibles por máquina", como se usa en el presente documento, se refiere a un medio único o múltiple que almacena uno o más conjuntos de instrucciones **350**. El término "medios legibles por máquina", como se usa en el presente documento, también se refiere a cualquier medio que sea capaz de almacenar, codificar o transportar el conjunto de instrucciones **350** para su ejecución por el MCD **104** y que hace que el MCD **104** realice una o más de las metodologías de la presente divulgación.

El controlador **310** también está conectado a una interfaz de usuario **330**. La interfaz de usuario **330** comprende dispositivos de entrada **316**, los dispositivos de salida **324** y las rutinas de software (que no se muestran en la figura 3) están configurados para permitir que un usuario interactúe y controle las aplicaciones de software (por ejemplo, software de aplicación **352** - **356** y otras aplicaciones de software) instaladas en el MCD **104**. Tales dispositivos de entrada y salida pueden incluir, pero no se limitan a, una pantalla **328,** un altavoz **326**, un teclado **320**, una almohadilla direccional (no mostrada en la figura 3), un mando direccional (no mostrado en la figura 3), Un micrófono **322** y una cámara **318**. La pantalla **328** puede estar diseñada para aceptar entradas de pantalla táctil. En consecuencia, la interfaz de usuario **330** puede facilitar una interacción entre el usuario y el software para iniciar aplicaciones (por ejemplo, software de aplicación **352** - **356**) instalado en MCD **104**. La interfaz de usuario **330** puede facilitar una sesión interactiva de software de usuario para escribir datos en y leer datos de la memoria **312**.

La pantalla **328,** teclado **320**, la almohadilla direccional (no mostrada en la figura 3) y el botón direccional (no mostrado en la figura 3) pueden proporcionar colectivamente a un usuario un medio para iniciar una o más aplicaciones de software o funciones del MCD **104**. El software de aplicación **354** - **358** puede facilitar el intercambio de datos (a) entre un artículo (por ejemplo, el artículo **102** de la figura 1) y un RTS (por ejemplo, un RTS **118** de la figura 1) y (b) entre una etiqueta de seguridad (por ejemplo, etiqueta de seguridad **132** de la figura 1) y el RTS. En este sentido, el software de aplicación **354** - **358** realiza uno o más de los siguientes: verificar una identidad de un usuario del MCD **104 a** través de un proceso de autenticación; presentar información al usuario que indique que su identidad ha sido o no ha sido verificada; y/o determinar si el usuario se encuentra dentro de un área particular de una tienda al por menor en la que está autorizado a usar las funciones del MCD **104** de venta al por menor. Dicha determinación se puede lograr utilizando una señal de "mantener vivo" o "latido del corazón" que recibe el MCD **104** del sistema EAS. La señal "mantener vivo" o "latido del corazón" puede tener una cierta frecuencia, tensión, amplitud y/o información, que el MCD **104** puede detectar y comparar con valores almacenados previamente para determinar si existe una coincidencia entre ellos. Si un partido existe o no existe, luego, el MCD **104** realizará una o más operaciones predefinidas para habilitar o deshabilitar una o más funciones del mismo.

En algunos escenarios, la señal "mantener vivo" o "latido del corazón" puede hacer que una o más operaciones del MCD **104** se habiliten o deshabiliten, de modo que el usuario del MCD **104** pueda acceder y utilizar las funciones relacionadas con el comercio al por menor de manera controlada. Por ejemplo, un empleado de la tienda puede estar autorizado para completar una transacción de compra de artículos en un departamento electrónico de una tienda al por menor, pero no de artículos en una farmacia de la tienda al por menor. En consecuencia, las

operaciones de transacción de compra al por menor del MCD **104** se habilitan cuando la tienda asociada está en el departamento electrónico y se deshabilita cuando el empleado de la tienda está en la farmacia. La señal de "mantener vivo" o "latido del corazón" también puede hacer que una o más operaciones del MCD **104** se habiliten o deshabiliten, de manera que el MCD **104** no funcionará si se saca de la tienda para evitar su robo.

El software de aplicación **354** - **358** también puede realizar uno o más de los siguientes: generar una lista de tareas que debe realizar un empleado de tienda particular; mostrar la lista al empleado de tienda utilizando el MCD **104**; y/o actualice dinámicamente la lista en función de la información recibida del asociado de la tienda y del sistema EAS, una etiqueta de seguridad, y/o un RTS. Por ejemplo, la lista puede incluir una pluralidad de preguntas: manejar un cliente en la isla 7 de la tienda de comestibles; estantes de existencias en la isla 9 de la tienda de comestibles; y/o bloquear/desbloquear un gabinete o una pieza de equipo.

El software de aplicación **354** - **358** puede realizar además uno o más de los siguientes: presentar una interfaz gráfica de usuario ("GUI") para que el usuario pueda iniciar un proceso de transacción al por menor para comprar uno o más artículos (por ejemplo, el artículo **102** de la figura 1); y/o presentar una GUI al usuario para permitirle al usuario iniciar un proceso de separación para separar una etiqueta de seguridad (por ejemplo, etiqueta de seguridad **132** de la figura 1) de un artículo (por ejemplo, el artículo **102** de la figura 1).

El proceso de transacción al por menor generalmente puede implicar: pedirle a un usuario del MCD **104** que ingrese manualmente la información del artículo o pedirle al usuario del MCD **104** que coloque el MCD con el PD **190** adjunto al mismo cerca del artículo; obtener la información del artículo manualmente del usuario o automáticamente del artículo a través de una comunicación de corto alcance (por ejemplo, comunicación de código de barras o comunicación NFC) utilizando el PD **190**; solicitando al usuario información de pago; obtener información de pago manualmente del usuario del MCD o automáticamente de una tarjeta de pago a través de un lector de tarjeta electrónico o un lector de código de barras del PD **190**; y establecer una sesión de transacción al por menor con un RTS (por ejemplo, RTS **118** de la figura 1).

La sesión de transacciones cubierta generalmente implica: comunicar la información del artículo y la información de pago al RTS a través de una conexión de red pública; recibir un mensaje de respuesta del RTS que indica que el artículo se ha comprado con éxito o sin éxito; e iniciar automáticamente el proceso de separación o pedirle al usuario que inicie el proceso si el artículo se compró correctamente.

El proceso de desapego generalmente puede involucrar: obtener un identificador único (por ejemplo, identificador único **210** de la figura 2) del artículo (por ejemplo, el artículo **102** de la figura 1) y/o la etiqueta de seguridad (por ejemplo, etiqueta de seguridad **132** de la figura 1) a través del PD **190**; reenviando el identificador(es) único(s) al RTS; recibir un mensaje del RTS que incluye información que especifica una clave de separación o un código de separación asociado con el identificador único; opcionalmente derivar la clave de separación del código de separación; opcionalmente, generar instrucciones para programar la etiqueta de seguridad para desbloquear un mecanismo de bloqueo electrónico utilizando la tecla de separación una sola vez; ordenando a PD **190** que reenvíe la clave de separación y/o las instrucciones a la etiqueta de seguridad a través de una comunicación SRC. En algunos escenarios, el MCD simplemente envía la información recibida del RTS al PD **190**sin modificaciones. En otros escenarios, el MCD modifica la información antes de la comunicación con el PD **190**. Dichas modificaciones pueden ser realizadas por un procesador con un gabinete a prueba de manipulaciones, de manera tal que si una persona intenta obtener acceso maliciosamente a cualquier algoritmo utilizado para dichos fines de modificación, el (los) algoritmo(s) se borrarán antes de cualquier acceso al mismo. Esta configuración puede ser ventajosa cuando la criptografía no se emplea para las comunicaciones entre el MCD y el RTS. Todavía, esta configuración puede emplearse incluso cuando se utiliza dicha criptografía.

A continuación, haciendo referencia a la figura 4, se proporciona un diagrama de bloques de una arquitectura a modo de ejemplo para el PD **190** de la figura 1. El PD **190** comprende una fuente de energía interna **430** para suministrar energía a ciertos componentes **404**, **406, 410, 412, 418** - **428** de los mismos. La fuente de poder **430** puede comprender, pero no se limita a, una batería recargable, un puerto de conexión de recarga, filtros de aislamiento (por ejemplo, inductores y componentes a base de ferrita), un circuito regulador de tensión y un plano de potencia (por ejemplo, una capa de placa de circuito dedicada al poder). El PD **190** puede incluir más o menos componentes que los mostrados en la figura 4. Por ejemplo, el PD **190** puede incluir además una unidad de radio UHF. Sin embargo, los componentes mostrados son suficientes para divulgar una realización ilustrativa que implementa la presente invención. Algunos o todos los componentes del PD **190** pueden implementarse en hardware, software y/o una combinación de hardware y software. El hardware incluye, pero no se limita a, uno o más circuitos electrónicos.

Notablemente, el PD **190** es un dispositivo periférico del MCD **104**. En algunos escenarios, el PD **190** está diseñado para envolver al menos una parte del MCD **104**. Una ilustración esquemática de tal diseño del PD **190** se proporciona en la figura 6. Como se muestra en la figura 6, el PD **190** comprende una cubierta o un soporte para una tableta **104**. Las realizaciones de la presente invención no están limitadas a la arquitectura del PD a modo de ejemplo mostrada en la figura 6. El PD **190** puede tener otras arquitecturas para aplicaciones en las que se emplean diferentes tipos de MCD (por ejemplo, un teléfono inteligente). En tales aplicaciones, El PD aún puede diseñarse

para cubrir al menos una porción del MCD de modo que el PD proporcione un dispositivo de POS móvil relativamente pequeño que sea fácil de transportar en o sobre una persona o un vehículo. En todos esos escenarios, el PD **190** también está configurado para proteger el MCD de daños durante el uso del mismo.

El PD **190** también está configurado para proporcionar al menos algunas de las funciones periféricas críticas requeridas por una amplia variedad de aplicaciones minoristas móviles que no son proporcionadas por el MCD **104**. En consecuencia, el PD **190** comprende un controlador **406** y una unidad SRC **404** para coordinar sus actividades con las del MCD **104**. En algunos escenarios, la unidad **404** de SRC incluye, pero no se limita a, un transceptor Bluetooth y/o un transceptor NFC. Notablemente, el PD **190** actúa como un dispositivo esclavo del MCD **104** maestro. Por ello, las operaciones del PD **190** son administradas y/o controladas por MCD **104**. La manera en que las operaciones del PD **190** son administradas y/o controladas por el MCD **104** se hará más evidente a medida que avanza la discusión.

Las funciones periféricas críticas pueden incluir, pero no se limitan a, funciones de detección de etiquetas EAS, funciones de desactivación/separación de etiquetas EAS, funciones de lectura de etiquetas RFID, funciones de determinación/seguimiento/informe de la ubicación del dispositivo y/o funciones de comunicación SRC con etiquetas de seguridad EAS, equipo móvil de POS y dispositivos manejados por el cliente. En este sentido, el PD **190** comprende antenas **402**, **408,** la unidad SRC **404**, una unidad de determinación **410,** el controlador **406**, la memoria **412,** un sistema de detección de etiquetas **418**, un sistema de desactivación de etiquetas **420**, un lector de código de barras **422**, una unidad de determinación **424,** un lector de tarjetas electrónicas **426** y un sistema de comunicación de canal trasero WSN **428**. El PD **190** también puede comprender un mecanismo de separación mecánico-magnético **416** y un código de barras **438**. Los componentes enumerados **404** - **412** y **416** - **428** están alojados juntos en una cubierta protectora de peso ligero (por ejemplo, la cubierta **602** de la figura 6). La cubierta protectora puede estar hecha de una goma dura o plástico que puede proteger los componentes enumerados **404** - **412** y **416** - **428** y el MCD **104** contra daños como resultado de factores externos. La cubierta protectora también puede diseñarse para mejorar la ergonomía del MCD **104** al hacer que sea más fácil de sostener en las manos del usuario, adjuntar a un vehículo, o usarse en el cuerpo de un usuario cuando no esté en uso.

También, los componentes pueden disponerse dentro de la cubierta protectora de cualquier manera que sea adecuada para una aplicación particular. Por ejemplo, los componentes de detección y/o desactivación de etiquetas se pueden colocar dentro de una parte específica (por ejemplo, la porción **604** de la figura 6) la cubierta protectora que no está cubierta por el MCD acoplado al PD. Las antenas pueden colocarse en la cubierta protectora de manera que resida debajo del MCD acoplado al PD.

Cada componente **404** - **412** y **416** - **428** proporciona una o más capacidades requeridas por varias aplicaciones minoristas relacionadas con las operaciones de POS móviles. Por ejemplo, durante una transacción móvil de POS, la unidad SRC **404** se usa para obtener acceso a una vitrina cerrada u otra área segura de una tienda al por menor en la que se desecha un artículo(s) al por menor. En algunos escenarios, es posible que se necesite equipo pesado para adquirir los artículos de venta al por menor. El acceso a dicho equipo pesado puede obtenerse utilizando la unidad SRC **404**. La unidad SRC **404** y/o el lector de código de barras **422** se utilizan para obtener la información del artículo necesaria para una transacción de compra. La información del artículo se puede obtener directamente del artículo(s) al por menor o de una etiqueta/marcador dispuesto junto al borde de un estante en el que el artículo(s) al por menor está(n) dispuesto(s). De forma similar, el lector de tarjetas electrónicas **426** se utiliza para obtener información de pago del cliente. tras la compra exitosa de los artículos al por menor, el sistema de desactivación de etiquetas **420** se utiliza para desactivar cualquier mecanismo de bloqueo electromecánico (por ejemplo, el mecanismo de bloqueo **216** de la figura 2) presente en el artículo(s) al por menor. También, la unidad RFID **424** se puede usar para desactivar las etiquetas RFID presentes con los artículos al por menor (por ejemplo, escribir en el bit del artículo vendido en la memoria). Se puede usar un mecanismo de separación mecánico-magnético **416** para separar cualquier mecanismo de bloqueo mecánico-magnético (por ejemplo, mecanismo de bloqueo **222** de la figura 2) acoplado a los artículos al por menor. Después, la información del artículo al por menor y/o la información del recibo se comunican al propio dispositivo móvil del cliente a través de la unidad SRC **404**. En algunos escenarios, la unidad RFID **424** también se puede usar para encontrar artículos de venta al por menor con etiqueta RFID en un estante o en un estante de exhibición (por ejemplo, un estante de la ropa), escribir los datos del recibo en una etiqueta RFID incrustada en una tarjeta o papel del recibo de la transacción y/o realice el conteo del ciclo de inventario.

El sistema de comunicaciones de canal trasero WSN **428** permite que el PD funcione como un nodo en una red inalámbrica. En este sentido, el sistema **428** se puede utilizar como el enlace de datos principal entre PD **190** y un RTS (por ejemplo, RTS **118**). El sistema **428** también se puede usar para ubicar físicamente el MCD dentro de la tienda al por menor, monitorear las actividades del MCD, actualizar el software del PD y/o MCD, y/o bloquear físicamente el PD si se retira el PD de la tienda al por menor sin autorización. El sistema **428** también se puede usar para transferir directamente datos de transacciones y eventos a otros dispositivos en la tienda al por menor (por ejemplo, pedestales EAS inteligentes o sistemas de sincronización de pedestales EAS) que pueden estar desconectados de la red principal de la tienda al por menor (por ejemplo, intranet **110** de la figura 1).

En algunos escenarios, el sistema **428** comprende un transceptor WSN, una antena y un circuito de adaptación

adecuado para las bandas de frecuencia que se utilizan en la comunicación WSN. El sistema **428** también puede comprender un controlador, separado del controlador **406**, para facilitar el control de las operaciones del transceptor WSN del sistema **428**. Este controlador separado puede actuar como esclavo del controlador **406**. El sistema **428** puede comprender además un circuito de administración de energía que extrae energía de una fuente de energía interna separada de la fuente de energía interna **430**.

Utilizando el sistema **428**, el PD **190** puede comunicar su estado y actividad a través de la red de sensores inalámbricos, recibir actualizaciones de software y realizar tareas de administración (por ejemplo, tareas de localización). Usando la unidad SRC **404** y el sistema **428**, el MCD/PD tiene una forma de comunicarse con otras aplicaciones que se ejecutan en servidores remotos o nodos de red de una red pública (por ejemplo, red pública **106** de la figura 1), suponiendo que el sistema **428** esté conectado directamente o mediante enrutadores a esos servidores remotos o nodos de red. También, el MCD/PD puede usar las comunicaciones SRC y/o WSN para acceder a los recursos de un sistema RTS (por ejemplo, el sistema RTS **118** de la figura 1) o red pública si los canales de comunicación alternativos fallan o están demasiado ocupados. En algunos escenarios, el sistema **428** puede emplear cualquier número de canales de comunicación estándar, frecuencias y/o protocolos. Por ejemplo, el sistema **428** emplea bandas ISM (por ejemplo, **433** MHz, **902** - **928** MHz y 2,4 GHz). Por ello, una ventaja importante de incluir el sistema **428** como parte del PD **190** es mejorar la solidez de la conectividad general y las opciones de conexión de red del MCD.

Como se desprende de la discusión anterior, PD **190** comprende al menos cuatro sistemas separados **404**, **420, 424, 428** para la recopilación de datos inalámbricos y la interacción de etiquetas de seguridad. En algunos escenarios, estos sistemas **404**, **420, 424, 428** utilizan diferentes bandas de comunicación, frecuencias, y/o protocolos. Por ejemplo, el sistema de detección de etiquetas **420** está configurado para desactivar etiquetas de seguridad AcoustoMagnetic ("AM") con un pulso de alta energía en torno a los 58 KHz. La unidad SRC **404** puede comprender un transceptor NFC que opera a aproximadamente 13,56 MHz. La unidad RFID **424** y el sistema de comunicación de canal de retorno WSN **428** operan en la ultra alta frecuencia ("UHF") industrial, Bandas científicas y médicas (“ISM”) (es decir, **850** - **950** MHz). Los componentes **424**, **428** se puede combinar en una sola unidad utilizando una radio UHF que emplea dos funciones de software diferentes para implementar los dos protocolos RFID y WSN.

Como se señaló anteriormente, PD **190** comprende una unidad RFID **424**. En algunos escenarios, la unidad RFID **424** comprende una etiqueta activa del sistema de ubicación RFID o en tiempo real ("RTLS") que se utiliza junto con lectores y/o transceptores externos para ubicar el PD **190** y determinar su estado. La etiqueta activa RFID o RTLS está integrada en el PD **190** y se comunica con el controlador **406**. La etiqueta activa RFID o RTLS también permite que PD **190** comunique su estado y/o actividad a través de una red a la que está conectado un lector o transceptor. La unidad RFID **424** también incluye hardware y/o software configurado para recibir actualizaciones de software, realizar tareas de gestión (por ejemplo, tareas de determinación y/o reporte de ubicación), leer etiquetas RFID y/o escribir en etiquetas RFID.

Las operaciones de la unidad RFID **424** se pueden controlar mediante el MCD al que se adjunta el PD **190**. En este sentido, el MCD comprende software (por ejemplo, el software **358** de la figura 3) configurado para servir como una interfaz para la unidad RFID **424**. Las funciones RFID de la combinación MCD/PD se pueden utilizar en varias aplicaciones. Por ejemplo, las funciones de RFID se pueden utilizar en el proceso de mantenimiento de existencias en el que se cuentan varios artículos minoristas etiquetados con RFID presentes en una tienda al por menor. En este caso, el MCD comunica el comando al PD a través de los SRC (por ejemplo, comunicaciones Bluetooth) para iniciar tales actividades de mantenimiento de existencias RFID.

Claramente, componentes **406**, **424, 428** juntos forman un conjunto de enlaces que se puede usar para hacer que las etiquetas RFID sean visibles para aplicaciones externas que se ejecutan en la WSN o dispositivos en cualquier conexión de red a la WSN. Esta actividad puede ser administrada y/o activada por una aplicación de software que se ejecuta en el controlador **406** del PD **190** o por una aplicación de software que se ejecuta en el MCD a través de una conexión SRC (por ejemplo, una conexión Bluetooth).

En algunos escenarios, las etiquetas NFC minoristas pueden colocarse en artículos minoristas o en el entorno al por menor (por ejemplo, en los bordes de los estantes de venta cubierta o en carteles en lugares prominentes dentro de una tienda al por menor). La unidad SRC **404** se puede usar para obtener información de estas etiquetas NFC minoristas a través de comunicaciones NFC. Dicha información puede incluir, pero no se limita a, instrucciones de uso, información promocional, información de advertencia del producto, información del ingrediente del producto, información de precios de productos y/o información de disponibilidad de productos. Se produce una comunicación NFC entre la unidad SRC **404** y la etiqueta NFC al por menor en una distancia relativamente pequeña (por ejemplo, N centímetros o N pulgadas, donde N es un número entero como doce). La comunicación NFC puede establecerse tocando la unidad SRC **404** y la etiqueta al por menor NFC **190** juntas o acercándolas a la proximidad de la dosis de manera que se produzca un acoplamiento inductivo entre los circuitos inductivos de la misma. La información obtenida a través de estas comunicaciones NFC se puede reenviar desde la unidad SRC **404** al controlador **406**. A su vez, el controlador **406** envía la información al MCD a través de un SRC (por ejemplo, una comunicación Bluetooth). En el MCD, la información se procesa para determinar qué acción se debe tomar. En el caso de una búsqueda, un cierto tipo de información para el artículo al por menor en cuestión se puede recuperar de un RTS (por

ejemplo, RTS **118** de la figura 1). La información recuperada se puede mostrar a un usuario del MCD/PD.
Las comunicaciones NFC también se pueden utilizar para transferir datos de ventas desglosados o agregados, datos de actividad de los empleados u otros datos de operaciones de un MCD al que el PD **190** está acoplado a otro MCD de la tienda al por menor. Dicha transferencia de datos puede ser facilitada por los respectivos sistemas de comunicaciones de canal trasero WSN **428** y/o las unidades SRC **404** de los PD de los dos MCD. Antes de esta transferencia de datos WSN, las operaciones de identificación y/o autenticación se pueden realizar como un protocolo de seguridad de transferencia de datos MCD al MCD.

Uno o más conjuntos de instrucciones **414** se almacenan en la memoria **412**. Las instrucciones **414** pueden incluir instrucciones personalizables e instrucciones no personalizables. Las instrucciones **414** también pueden residir, total o al menos parcialmente, dentro del controlador **406** durante la ejecución del mismo por PD **190**. En este sentido, la memoria **412** y el controlador **406** pueden constituir medios legibles por máquina. El término "medios legibles por máquina", como se usa en el presente documento, se refiere a un medio único o múltiple que almacena uno o más conjuntos de instrucciones **414**. El término "medios legibles por máquina", como se usa en el presente documento, también se refiere a cualquier medio que sea capaz de almacenar, codificar o transportar el conjunto de instrucciones **414** para su ejecución por el PD **190** y que hace que el PD **190** realice una o más de las metodologías de la presente divulgación.

Notablemente, en algunos escenarios, la unidad GPS **410** se puede usar para facilitar la habilitación y deshabilitación de una o más operaciones del PD **190** y/o MCD **104**. Por ejemplo, la ubicación del PD **190** y/o MCD **104** se puede determinar utilizando la unidad de GPS **410**. La información que especifica la ubicación del PD **190** y/o MCD **104** se puede enviar al sistema EAS **130** y/o RTS **118** para su procesamiento. Basado en la información de ubicación, el sistema **118**, **130** puede generar y comunicar un comando al PD **190** y/o MCD **104** para habilitar o deshabilitar sus operaciones. Dicha configuración puede emplearse para garantizar que un usuario del PD **190** y/o MCD **104** pueda acceder y usar ciertas funciones de la misma solo dentro de un área específica de una tienda al por menor. También, dicha configuración puede evitar el robo del PD **190** y/o M CD **104,** ya que una o más operaciones del mismo pueden desactivarse cuando el equipo sale de las instalaciones de la tienda al por menor.

A continuación, haciendo referencia a la figura 5, se proporciona un diagrama de bloques de una arquitectura a modo de ejemplo para un sistema de desactivación de etiquetas **420** mostrado en la figura 4. El sistema **420** comprende un circuito de carga de condensador **504**, un condensador **512**, un interruptor de descarga **514** y una antena de desactivación **516**. El circuito de carga del condensador **504** incluye un interruptor de carga **508** y un monitor de carga del condensador **510**. Durante el funcionamiento, el sistema **420** recibe una señal de control desde el controlador **406** de la figura 4, la señal de control incluye información para cerrar el interruptor de carga **508**. Cuando el interruptor de carga **508** está cerrado, se suministra alimentación desde la entrada de potencia **502** al cargador de carga **512**. La carga en el condensador **512** es monitoreada por el monitor de carga del condensador **510**. El monitor **510** comunica la información de carga del condensador al controlador **406** de la figura 4 de manera que el controlador **406** pueda monitorear adicional o alternativamente la carga en el condensador **512**. Basado en la información de carga del condensador, se determina si el interruptor de carga **508** debe abrirse o cerrarse (es decir, para cargar o no cargar el condensador **512**). También se determina si un interruptor de descarga **514** debe abrirse o cerrarse (es decir, para descargar o no descargar el condensador **512**). Si se determina que el condensador **512** debe ser descargado, luego, el interruptor de descarga **514** se cierra de manera tal que el condensador **512** se descarga a través de la antena **516**. Como resultado de la descarga del condensador, la energía es pulsada a una frecuencia deseada desde la antena **516**.

A continuación, haciendo referencia a la figura 7, se proporciona un diagrama de flujo de un método a modo de ejemplo **700** para comprar un artículo (por ejemplo, el artículo **102** de la figura 1) de una tienda al por menor (por ejemplo, la instalación de la tienda al por menor **150** de la figura 1) que es útil para entender la presente invención. Aunque no se muestra en la figura 7, debe entenderse que las operaciones de autenticación de usuarios y/o las operaciones de habilitación de funciones se pueden realizar antes de la etapa **702**. Tales operaciones se describen arriba. Por ejemplo, un usuario del MCD puede ser autenticado, y por lo tanto, una o más operaciones de transacción al por menor del MCD pueden habilitarse en función del nivel de autorización del usuario y/o la ubicación del MCD dentro de una tienda al por menor. La ubicación del MCD se puede determinar utilizando la información del GPS. En algunos escenarios, se puede usar una señal de "latido cardíaco" para habilitar las operaciones de transacción al por menor del MCD y/o PD. La señal de "latido del corazón" puede comunicarse directamente al MCI) o indirectamente al MCD a través del PD.

Después de la etapa **702,** el método **700** continúa con la etapa **704** donde un cliente (por ejemplo, el cliente **140** de la figura 1) ingresa a la tienda al por menor y acumula uno o más artículos para comprar. En algunos escenarios, el cliente puede pedir a un empleado de la tienda (por ejemplo, tienda asociada **142** de la figura 1) asistir en la compra de los artículos acumulados, como se muestra en la etapa opcional **706**. La etapa **706** opcional se puede realizar cuando el cliente **140** no tiene un MCD (por ejemplo, MCD **104** de la figura 1) con una aplicación de transacción al por menor instalada allí y/o un PD (por ejemplo, dispositivo periférico **190** de la figura 1) acoplado al mismo. Si el cliente está en posesión de tal MCD, entonces el cliente no necesitaría la asistencia de un empleado de la tienda para completar una transacción de compra y/o separar las etiquetas de seguridad de los artículos.

En una etapa siguiente **708**, el cliente o el empleado de la tienda utiliza el PD de la MCI) para escanear cada artículo para la licitación. El escaneo se puede lograr utilizando un escáner de código de barras (por ejemplo, el lector de código de barras **422** de la figura 4), un escáner RFID (por ejemplo, la unidad de RFID **424** de la figura 4), un escáner de etiquetas NFC (por ejemplo, la unidad de SRC **404** de la figura 4), o cualquier otro medio de comunicación de corto alcance. Una vez escaneados los artículos, la información de pago se ingresa en la aplicación de transacción al por menor del MCD, como se muestra en las etapas **710** - **712**. La información de pago puede ser ingresada por la persona en posesión del MCD (es decir, el cliente o el asociado de la tienda). La información de pago puede incluir, pero no se limita a, un código de fidelidad del cliente, información de la tarjeta de pago, y/o información de la cuenta de pago. La información de pago se puede ingresar manualmente usando un dispositivo de entrada (por ejemplo, Los dispositivos de entrada **316** - **322** de la figura 3) del MCD, a través de un lector de tarjetas electrónico (por ejemplo, un lector de tarjetas de banda magnética) del PD (por ejemplo, lector de tarjetas electronico **426** de la figura 4), y/o mediante un lector de código de barras del PD (por ejemplo, el lector de código de barras **422** de la figura 4). En los escenarios de tarjeta/código de barras, el cliente puede proporcionar una tarjeta de pago al asociado de la tienda, como se muestra en la etapa opcional **710**.

Después de que la información de pago haya sido ingresada en la aplicación de transacción al por menor, se realiza una etapa de decisión **714** para determinar si se ha completado una transacción de compra. Esta determinación la realiza el MCD basándose en la información recibida de un RTS, como se ha descrito anteriormente. A continuación se describirá un proceso de transacción de compra a modo de ejemplo en relación con la figura 8. Si la transacción de compra no se completa [**714**: NO], entonces el método **700** vuelve a la etapa **714**. Si la transacción de compra se completa [**714**: SÍ], entonces se realiza una etapa de decisión **716**. En la etapa 716, se determina si los artículos han sido comprados con éxito. Si los artículos no se han comprado con éxito [**716**: NO], entonces el método **700** vuelve a la etapa **710**. En contraste, si los artículos se han comprado con éxito [**716**: SÍ], luego se realizan las etapas **718** - **722**.

La etapa **718** implica separar las etiquetas de seguridad (por ejemplo, etiqueta de seguridad **132** de la figura 1) de los artículos. Las etiquetas de seguridad son separadas por el cliente o el empleado de la tienda utilizando el MCD y/o PD. Un proceso de separación a modo de ejemplo se describirá a continuación en relación con las figuras 9A-9E. La etiqueta de seguridad separada se puede colocar en una bandeja de colección para su uso posterior, como se muestra en la etapa **720**. Después, la etapa **722** se realiza donde termina el método **700**.

A continuación, haciendo referencia a la figura 8, se proporciona un proceso a modo de ejemplo de transacción de compra **800** facilitado por un MCD (por ejemplo, MCD **104** de la figura 1) con un PD (por ejemplo, PD **190** de la figura 1) acoplado comunicativamente al mismo. El proceso **800** comienza con la etapa **802** y continúa con la etapa opcional **804**. en la etapa opcional **804**, la información de autenticación (por ejemplo, un nombre de usuario, una contraseña, o información biométrica) se obtiene de un usuario de la misma. La información de autenticación es utilizada por el MCD y/o PD para autenticar al usuario (por ejemplo, el cliente **140** de la figura 1 o empleado de tienda **142** de la figura 1).

En algunos escenarios, la información de autenticación se obtiene mediante dispositivos de entrada del MCD (por ejemplo, dispositivos de entrada **316** de la figura 3) y/o dispositivos de entrada del PD (por ejemplo, dispositivos de entrada **404**, **422, 424** y/o **426** de la figura 4). Por ejemplo, una unidad SRC (por ejemplo, la unidad de SRC **404** de la figura 4) del PD se utiliza para facilitar la seguridad y el acceso al MCD. Un problema general asociado con el uso del MCD orientados a operaciones minoristas es la seguridad física de los mismos. Es decir, el minorista debe asegurarse de que los empleados y clientes no autorizados no puedan usar el MCD para actividades no autorizadas, como una desactivación maliciosa de una etiqueta de seguridad y/o un acceso malicioso a la red general de la tienda al por menor (por ejemplo, red privada **110** de la figura 1). La unidad SRC del PD se puede utilizar junto con una etiqueta o etiqueta de seguridad SRC en el cliente autorizado **140** o el empleado de tienda **142** (por ejemplo, integrado con el distintivo del empleado o incluido con un llavero) para asegurar el MCD.

En estos y/u otros escenarios, una aplicación de transacción cubierta (por ejemplo, la solicitud **358** de la figura 3) puede estar en modo de suspensión segura para ahorrar energía. En el modo de suspensión segura, una pantalla de visualización (por ejemplo, pantalla **328** de la figura 3) se oscurece y todas las funciones innecesarias del procesador se detienen. También, un servicio de interrupción de entrada/salida ("IO") del MCD supervisa una interfaz SRC (por ejemplo, la unidad SRC **314** de la figura 3) para los SRC recibidos del PD. En este momento, El PD también puede estar en modo de reposo en el que solo ciertos componentes de los mismos están activos, como una unidad SRC (por ejemplo, La unidad de SRC **404** de la figura 4), un lector RFID (por ejemplo, la unidad de RFID **424** de la figura 4) o un lector de código de barras (por ejemplo, el lector de código de barras **422** de la figura 4). Cuando un empleado de tienda autorizado o un cliente retira el MCD, el PD se coloca muy cerca de un elemento de seguridad del mismo (por ejemplo, un llavero habilitado para NFC o una tarjeta de identificación). En consecuencia, el PD obtiene un número o código del elemento de seguridad a través de un SRC, escaneo de código de barras o lectura RFID. Esta actividad hace que el PD salga de su modo de suspensión. Luego, el PD o el MCD pueden analizar el número/código para determinar si el usuario actual está autorizado para realizar transacciones minoristas con el mismo.

Si el número/código debe ser analizado por el PD, luego el PD compara el número/código recibido con los códigos

autorizados almacenados en una memoria interna (por ejemplo, memoria **412** de la figura 4) del mismo o en una memoria externa (por ejemplo, una memoria de RTS **118** de la figura 1) a este respecto, el PD puede consultar códigos autorizados en la memoria externa a través de un sistema de comunicaciones de canal trasero WSN (por ejemplo, sistema **428** de la figura 4) de los mismos. Basado en los resultados de dicha comparación, el PD opcionalmente 'comunica un mensaje a través de un SRC (por ejemplo, una comunicación Bluetooth) al MCD. El mensaje incluye información que especifica si el uso actual está autorizado o no para realizar transacciones minoristas con el mismo. MCD puede entonces, opcionalmente, salir de su modo de suspensión en respuesta a la recepción de dicho mensaje. Por ejemplo, el MCD puede salir de su modo de suspensión cuando recibe un mensaje que indica que el usuario actual es un usuario autorizado del mismo.

En contraste, si el número/código debe ser analizado por el MCD, luego, el número/código se reenvía al MCD desde el PD a través de la unidad SRC. En respuesta a la recepción del número/código, el MCD sale de su modo de reposo utilizando una rutina de 10 servicios del mismo. Posteriormente, el MCD compara el número/código recibido con los códigos autorizados almacenados en una memoria interna (por ejemplo, la memoria **312** de la figura 3) del mismo o en una memoria externa (por ejemplo, una memoria de RTS **118** de la figura 1) de los mismos. En este sentido, el MCD puede consultar códigos autorizados en la memoria externa a través del sistema de comunicaciones de canal trasero WSN (por ejemplo, sistema **428** de la figura 4) del PD y/o mediante una comunicación segura a través de una red pública (por ejemplo, red pública **106** de la figura 1).

Haciendo referencia de nuevo a la figura 8, el método **800** continúa con la etapa **808** después de que el usuario haya sido autenticado. La etapa **806** se realiza cuando el MCD lanza una aplicación de transacción al por menor (por ejemplo, la solicitud de transacción **358** de la figura 3) configurado para facilitar la compra de uno o más artículos (por ejemplo, artículo **102** de la figura 1) de una tienda al por menor (por ejemplo, la instalación de la tienda al por menor **150** de la figura 1). La aplicación de transacción al por menor puede ser una aplicación preinstalada, una aplicación adicional, o una aplicación de complemento. La aplicación de transacción al por menor se puede descargar al MCD a través de un sitio web u otro medio electrónico de transferencia de datos antes de la etapa **806**. En algunos escenarios, la aplicación de transacción al por menor se inicia en respuesta a una interacción de usuario con software. Por ejemplo, la aplicación de transacción al por menor se inicia en respuesta a la interacción del cliente con un producto a través de un escaneo de código de barras, un escaneo NFC, escaneo de código QR de una etiqueta de precio o etiqueta de identificación del producto. En otros escenarios, la aplicación de transacción al por menor se inicia automáticamente en respuesta a la autenticación del usuario.

Posteriormente, el MCD recibe una entrada del usuario para iniciar un proceso de transacción al por menor para comprar un artículo (por ejemplo, el artículo **102** de la figura 1). A este respecto, se puede presentar una GUI al usuario del MCD. La GUI puede incluir un aviso para una interacción entre el usuario y el software para comenzar un proceso de compra al por menor. Al completar la etapa **808**, la etapa **810** se realiza cuando el MCD y/o el PD obtienen información del artículo que es útil para comprar el artículo. La información del artículo puede incluir, pero no se limita a, un identificador de artículo, un precio de compra del artículo y/o un identificador de etiqueta de seguridad. El MCD puede obtener información del artículo a través de la interacción del usuario con el software. En contraste, el PD puede obtener la información del artículo a través de un SRC. El SRC puede incluir, pero no se limita a, una comunicación de código de barras (por ejemplo, la comunicación de código de barras **122** de la figura 1) o una comunicación NFC (por ejemplo, la comunicación NFC **120** de la figura 1). Notablemente, el PD realiza operaciones para obtener la información del artículo de acuerdo con las instrucciones y/o comandos recibidos del MCD a través de un SRC (por ejemplo, una comunicación Bluetooth). También, el PD puede enviar la información obtenida del artículo al MCD a través del SRC.

Al recibir la información del artículo en el MCD, se realiza una etapa opcional **812** donde la información de pago se ingresa en la aplicación de transacción al por menor. La información de pago puede ingresarse en el software de transacción al por menor a través de una interacción del software del usuario con el MCD o un SRC (por ejemplo, un escaneo de código de barras o escaneo de tarjeta de pago) con el PD. En el escenario SRC, la información de pago se envía del PD al MCD a través de otro SRC (por ejemplo, una comunicación Bluetooth). La información de pago puede incluir, pero no se limita a, un código de fidelidad del cliente, información de la tarjeta de pago, y/o información de la cuenta de pago. Alternativa o adicionalmente, la etapa **812** puede implicar la activación de un proceso de pedido de un solo clic en el que la información de pago del cliente se almacena en línea para que el cliente no tenga que presentar una tarjeta de crédito o deslizar la tarjeta para ofrecer la transacción. Una vez que se activa el proceso de pedido de un solo clic, el usuario del MCD puede simplemente presionar una tecla en un teclado o tocar un botón en una pantalla táctil del MCD para ofrecer la transacción.

En una etapa siguiente **814**, el MCD realiza operaciones para establecer una sesión de transacción al por menor con un RTS (por ejemplo, RTS **118** de la figura 1). Después, la etapa **816** se realiza cuando la información del artículo y la información de pago se comunica desde el MCD al RTS a través de una red pública (por ejemplo, red pública **106** de la figura 1). En el RTS, la información del artículo y la información de pago se procesa, como se muestra en la etapa **818**. Esta información es procesada por el RTS para completar una transacción de compra.

Una vez completada la transacción de compra, la etapa **820** se realiza cuando el RTS genera un mensaje de respuesta. El mensaje de respuesta indica si los artículos se han comprado con éxito o sin éxito. El mensaje de

respuesta se comunica en la etapa **822** desde el RTS al MCD. Posteriormente, se realiza una etapa de decisión **824** donde el MCD determina si los artículos se compraron con éxito. Esta determinación se puede realizar en función del contenido del mensaje de respuesta. Si los artículos no fueron comprados con éxito [**824**: NO], luego se realiza la etapa **826** donde termina el método **800** u otro procesamiento. En contraste, si los artículos fueron comprados con éxito [**824**: SÍ], luego se realizan las etapas **828** - **830**. La etapa **828** implica iniciar automáticamente un proceso de separación de etiquetas de seguridad mediante el MCD, automáticamente por el RTS, o en respuesta a una interacción del software del usuario con el MCD. Un proceso a modo de ejemplo de separación de etiquetas de seguridad se describirá a continuación en relación con las figuras 9A-9E. Después de completar la etapa **828**, la etapa **830** se realiza cuando el método **800** finaliza o se realiza otro procesamiento.

haciendo referencia ahora a la figura 9A-9E, se proporciona un proceso de separación de etiqueta de seguridad a modo de ejemplo **900** que es útil para comprender la presente invención. El proceso **900** comienza con la etapa **902** y continúa con la etapa **904**. La etapa **904** implica mostrar una GUI al usuario del MCD (por ejemplo, MCD **104** de la figura 1). La GUI permite al usuario iniciar un proceso para eliminar una etiqueta de seguridad (por ejemplo, etiqueta de seguridad **132** de la figura 1) de un artículo (por ejemplo, el artículo **102** de la figura 1). Una vez que se ha iniciado el procedimiento, la etapa **905** se realiza cuando el MCD determina si un PD (por ejemplo, el PD **190** de la figura 1) del mismo está listo para desactivar la etiqueta de seguridad.

En algunos escenarios, la etapa **905** implica realizar operaciones por el MCD para comunicar un mensaje de comprobación de recursos de red al PD a través de un SRC (por ejemplo, una comunicación Bluetooth). El mensaje de comprobación de recursos de red puede tomar la forma de más o menos complejidad, pero el propósito básico del mensaje de comprobación de recursos de red es que el MCD determine si el PD está activada o no, así como determinar el estado del PD. El término "estado", como se usa en el presente documento, significa la ubicación del control en un algoritmo de máquina de estado utilizado para controlar el comportamiento de un controlador interno (por ejemplo, el controlador **406** de la figura, 4). Es decir, una máquina de estados con estados numerados discretamente se implementaría como código ejecutable en el controlador interno, y se implementarán algoritmos particulares como estados específicos en esa máquina de estados. La máquina de estado también puede incluir funciones (por ejemplo, funciones de comprobación de potencia y funciones de seguridad) no relacionadas con tales algoritmos. Cuando el MCD toca el PD, el PD responde con un mensaje de respuesta que indica su estado (es decir, dando su código de identificación de estado actual o número). El mensaje de respuesta se puede comunicar desde el PD al MCD a través de un SRC (por ejemplo, una comunicación bluetooth). Si el PD está listo, el MCD puede esperar un mensaje de evento del PD. El mensaje del invento incluye información (por ejemplo, información del artículo) que indica que una etiqueta de seguridad particular puede necesitar desactivarse. En contraste, del PD no está listo, luego, el MCD puede esperar a que caduque un período de tiempo predefinido, y luego volver a enviar el PD.

A continuación, el proceso **900** continúa con las etapas opcionales **906** - **910**. Las etapas opcionales **906** - **910** se pueden realizar cuando la información del artículo obtenida del artículo está ausente de un identificador de etiqueta de seguridad. Si la información del artículo incluye el identificador de la etiqueta de seguridad, luego el proceso **900** puede estar ausente de al menos las etapas **906** - **910**.

En la etapa opcional **906**, un usuario (por ejemplo, el cliente **140** de la figura 1 o asociado de ventas **142** de la figura 1) coloca un PD (por ejemplo, PD **190** de la figura 1) del MCD en la proximidad de una etiqueta de seguridad (por ejemplo, etiqueta de seguridad **132** de la figura 1). En consecuencia, el MCD puede opcionalmente controlar el PD para que realice operaciones para detectar cualquier etiqueta de seguridad activa en el artículo. Tales operaciones pueden ser realizadas por un sistema de detección de etiquetas (por ejemplo, sistema de detección de etiquetas **418** de la figura 4) del PD utilizando SRC (por ejemplo, comunicaciones de código de barras, comunicaciones RFID, comunicaciones NFC, y/o comunicaciones Bluetooth).

Cuando se ha detectado al menos una etiqueta de seguridad activa, el PD realiza la etapa opcional **908**. En la etapa 908, el PD obtiene al menos un identificador único de la etiqueta de seguridad a través de un SRC (por ejemplo, una comunicación de código de barras, una comunicación RFID, una comunicación NFC, y/o una comunicación Bluetooth). Un mensaje de evento que incluye el identificador único se comunica luego desde el PD al MCD a través de otro SRC (por ejemplo, una comunicación Bluetooth).
En algunos escenarios, este SRC es iniciado por el PD, pero en otros escenarios, el MCD inicia el segundo SRC a través de un proceso de sondeo. Se proporciona una indicación al usuario del MCD que indica que el identificador único se ha obtenido correctamente de la etiqueta de seguridad, como se muestra en la etapa opcional **910**.

En respuesta a la recepción del mensaje del evento, el MCD realiza varias operaciones para determinar si la etiqueta de seguridad particular debe ser desactivada o no. Por ejemplo, como se muestra en la etapa opcional **911**, el MCD puede realizar operaciones para determinar si un impulso de energía de desactivación podría interferir con otros dispositivos (por ejemplo, un pedestal de detección de etiquetas EAS) que se ejecuta en la tienda al por menor. Si se determina que tal impulso de energía de desactivación es poco probable que interfiera con las operaciones de otros dispositivos en la tienda al por menor, luego el proceso **900** puede continuar con la etapa **912**, de lo contrario, el proceso **900** puede finalizar o volver a una etapa anterior.

En la etapa 912, el MCD obtiene un número de teléfono, una dirección electrónica (por ejemplo, una dirección de protocolo de internet ("IP") de un dispositivo informático (por ejemplo, dispositivo informático **108** de la figura 1) de un RTS (por ejemplo, RTS **118** de la figura 1), y/o una dirección de correo electrónico del usuario del dispositivo de computación RTS. El número de teléfono, la dirección electrónica y/o la dirección de correo electrónico se pueden obtener del usuario del MCD o de un directorio almacenado en un almacén de datos (por ejemplo, memoria **312** de la figura 3) del MCD.

El número de teléfono o la dirección electrónica se usa luego en la etapa **914** para establecer un enlace de comunicación entre el MCD y el dispositivo de computación RTS. El enlace de comunicación puede incluir, pero no se limita a, un enlace de comunicación RE (por ejemplo, el enlace de comunicación RE **124** de la figura 1). En algunos escenarios, el MCD y/o el dispositivo de computación RTS comprenden una tableta o un teléfono móvil que utiliza tecnología inteligente. Dichas tabletas y teléfonos móviles se mencionan en la técnica como dispositivos inteligentes. Los dispositivos inteligentes son bien conocidos en la técnica y, por lo tanto, no se describirán aquí.

Adicional o alternativamente, la etapa **914** puede involucrar el envío de correo electrónico al usuario del dispositivo de computación RTS que indica que se ha realizado una solicitud de acceso. En este escenario, el correo electrónico puede incluir, pero no se limita a, un medio para lanzar una solicitud para otorgar/denegar la solicitud de acceso, un identificador único de la etiqueta de seguridad, un identificador único del objeto/elemento protegido por la etiqueta de seguridad, un identificador único del usuario del MCD (por ejemplo, un nombre de usuario), y/o un identificador único del MCD (por ejemplo, un número de teléfono).

Al completar la etapa **914**, se realiza la etapa opcional **916**. La etapa opcional **916** se puede realizar si se estableció un enlace de comunicación entre el MCD y el dispositivo informático RTS en la etapa **914** a través del número de teléfono o la dirección electrónica. La etapa opcional **916** no se puede realizar cuando el correo electrónico se emplea en la etapa **914**.

En la etapa opcional **916**, un primer mensaje se comunica desde el MCD al dispositivo de computación RTS. El primer mensaje puede indicar que un usuario del MCD solicita la separación de una etiqueta de seguridad de un artículo. En este sentido, el mensaje puede incluir, pero no se limita a, un identificador único de la etiqueta de seguridad, un identificador único del artículo protegido por la etiqueta de seguridad, un identificador único del usuario del MCD (por ejemplo, un nombre de usuario) y/o un identificador único del MCD (por ejemplo, un número de teléfono). En algunos escenarios, el primer mensaje es un mensaje de texto o un mensaje de voz pregrabado.

Posteriormente, el proceso **900** continúa con la etapa **918**. La etapa **918** implica el lanzamiento de una aplicación preinstalada, aplicación adicional y/o una aplicación de complemento del dispositivo informático RTS. La aplicación se puede iniciar en respuesta a la recepción del primer mensaje del MCD o del mensaje de correo electrónico del MCD. La aplicación preinstalada, la aplicación adicional y/o la aplicación complementaria se pueden iniciar automáticamente en respuesta a la recepción del primer mensaje o mensaje de correo electrónico. Alternativamente, la aplicación preinstalada, la aplicación adicional y/o la aplicación complementaria se pueden iniciar en respuesta a una interacción del usuario con el software. La aplicación preinstalada, la aplicación adicional y/o la aplicación complementaria están configuradas para facilitar el control del acceso al área y/o al objeto. También se puede emitir opcionalmente una indicación audible desde el dispositivo de computación RTS en respuesta a la recepción del primer mensaje o correo electrónico en el mismo, como se muestra en la etapa **920**.

A continuación, se realiza una etapa de decisión opcional **922** para determinar si se permite que la etiqueta de seguridad se separe del artículo. Esta determinación se puede hacer utilizando la información contenida en el mensaje recibido (es decir, el primer mensaje o el mensaje de correo electrónico) y/o la información almacenada en un almacén de datos del RTS. Por ejemplo, se puede determinar que la etiqueta de seguridad se puede separar del artículo cuando (a) el artículo se compró con éxito y/o (b) un identificador del usuario y/o MCD coincida con el almacenado en el almacén de datos del RTS. Alternativa o adicionalmente, tal determinación se puede hacer cuando un nivel de clasificación asignado al usuario es el mismo que el del artículo protegido por la etiqueta de seguridad. El nivel de clasificación puede incluir, pero no se limita a, un personal de piso de minorista, un gerente de tienda al por menor, un propietario de una tienda al por menor, un cliente privilegiado, un nivel secreto, un nivel de alto secreto, un nivel clasificado, y/o un nivel no clasificado.

Si se determina que la etiqueta de seguridad no se puede eliminar del artículo [**922**: NO], luego el proceso **900** continúa con las etapas **924** - **930** de la figura 9B. La etapa **924** implica proporcionar automáticamente una indicación al usuario del dispositivo informático RTS de que la etiqueta de seguridad no puede separarse del artículo. También, se genera un segundo mensaje y se envía al MCD que indica que se ha denegado la solicitud del usuario para separar la etiqueta de seguridad del artículo, como se muestra en la etapa **926**. Al recibir el segundo mensaje en el MCD, se proporciona una indicación al usuario de que su solicitud ha sido denegada. Después, la etapa **930** se realiza donde termina el proceso **900**, se realiza otro procesamiento, o el proceso **900** vuelve a la etapa **902**.

Si se determina que el usuario de la etiqueta de seguridad puede separarse del artículo [**922**: SÍ], entonces el proceso **900** continúa con la etapa **932** de la figura 9C. Como se muestra en la figura 9C, la etapa **932** implica mostrar automáticamente información al usuario del dispositivo de computación RTS que indica que el usuario del

MCD está solicitando la separación de una etiqueta de seguridad de un artículo. En este sentido, La información mostrada puede incluir, pero no se limita a, información que identifica al usuario del MCD, información que identifica el MCD, información de contacto del usuario y/o MCD, información que identifica el artículo, información que identifica la etiqueta de seguridad y/o información que indica que se está solicitando una separación de la etiqueta de seguridad. Posteriormente, se realiza una etapa opcional **934** para obtener una confirmación verbal del usuario del MCD de que está buscando la separación de la etiqueta de seguridad del artículo.

En una etapa siguiente **936**, el dispositivo de computación RTS realiza operaciones para obtener una clave o código de separación de un almacén de datos que está asociado con el identificador del artículo y/o el identificador de la etiqueta de seguridad. Si se obtiene un código de separación en la etapa **936**, luego se puede realizar una etapa opcional **938** donde la clave de separación es generada por el dispositivo de computación RTS. En una etapa siguiente **940**, la clave o código de separación se comunica desde el dispositivo informático RTS al MCD. Si el MCD recibe el código de separación, entonces puede generar la clave de separación usando el código de separación, como se muestra en la etapa opcional **942**.

Una vez que el MCD posee la clave de separación, se toma una decisión en la etapa opcional **944** para determinar si la clave de separación es una clave de uso de una sola vez. Si se determina que la clave de separación no es una clave de uso de una sola vez [**944**: NO], luego se realizan las etapas **946** - **952**. La etapa **946** implica la comunicación de un mensaje de activación que incluye la clave de separación del MCD al PD a través de un SRC (por ejemplo, una comunicación Bluetooth). El MCD también puede inicializar un contador a cero, de manera que puede esperar un período de tiempo predefinido para recibir un mensaje de respuesta del PD que indique que la etiqueta de seguridad se ha desconectado o desactivado con éxito o sin éxito.

En el PD, las operaciones se realizan para separar o desactivar la etiqueta de seguridad. Un método a modo de ejemplo de las operaciones del PD para separar o desactivar una etiqueta de seguridad electromecánica se describirá en detalle a continuación en relación con la figura 10. Todavía, debe entenderse que tales operaciones generalmente implican: comunicar una señal a la etiqueta de seguridad para hacer que abra una bloqueo electrónica, retirar una tachuela/pasador/acollador y/o calentar un adhesivo con la llave de separación; recibir información de la etiqueta de seguridad que indica si el bloqueo electrónico fue desbloqueado o no, la tachuela/alfiler/o el cordón se retiró con éxito, y/o el adhesivo se calentó con éxito; y/o reenviar dicha información en un mensaje de respuesta desde el PD al MCD,

Si el MCD no recibe el mensaje de respuesta dentro del período de tiempo predefinido [**950**: NO], luego, el MCD informa al usuario y/o RTS que la separación/desactivación de la etiqueta de seguridad ha fallado. En contraste, si el MCD recibe el mensaje de respuesta dentro del período de tiempo predefinido [**950**: SÍ], luego, el MCD informa al usuario y/o RTS de que la separación/desactivación de la etiqueta de seguridad fue exitoso. Al completar la etapa **952** o **954**, la etapa **956** se realiza donde termina el proceso **900**, se realiza otro procesamiento, o el proceso **900** vuelve a la etapa **902**.

Si se determina que la clave de separación es una clave de uso de una sola vez [**944**: SÍ], luego el proceso **900** continúa con las etapas **958** - **970** de la figura 9D o las etapas **972** - **984** de la figura 9E, Dependiendo de la aplicación particular. como se muestra en la figura 9D, la etapa **658** implica generar instrucciones para programar el PD y/o la etiqueta de seguridad para abrir una bloqueo electrónica, retire una tachuela/pasador/acollador y/o calentar un adhesivo con la llave de separación solo una vez. Un mensaje de activación con la tecla de separación y las instrucciones se envían en la etapa **660** desde el MCD al PD a través de un SRC (por ejemplo, una comunicación NFC). El MCD también puede inicializar un contador a cero, de modo que puede esperar un período de tiempo predeterminado para recibir un mensaje de respuesta del PD que indique que la etiqueta de seguridad se ha desconectado o desactivado con éxito o sin éxito.

En el PD, las operaciones se realizan para separar o desactivar la etiqueta de seguridad usando las instrucciones y/o la tecla de separación. Un método a modo de ejemplo de las operaciones del PD para separar o desactivar una etiqueta de seguridad electromecánica se describirá en detalle a continuación en relación con la figura 10. Todavía, debe entenderse que tales operaciones generalmente implican: comunicar una señal a la etiqueta de seguridad para hacer que abra una bloqueo electrónica, retirar una tachuela/alfiler/pasador, y/o calentar un adhesivo usando la llave de separación usando las instrucciones y/o la llave de separación; recibir información de la etiqueta de seguridad que indica si el bloqueo electrónico fue desbloqueado o no, la tachuela/alfiler/acollador se retiró con éxito y/o el adhesivo se calentó con éxito; y/o reenviando dicha información en un mensaje de respuesta desde el PD al MCD.

Si el MCD no recibe el mensaje de respuesta dentro del período de tiempo predefinido [**964**: NO], luego, el MCD informa al usuario y/o RTS que la separación/desactivación de la etiqueta de seguridad ha fallado. En contraste, si el MCD recibe el mensaje de respuesta dentro del período de tiempo predefinido [**964**: SÍ], luego, el MCD informa al usuario y/o RTS que la separación de la etiqueta de seguridad/desactivación fue exitosa. Al completar la etapa **966** o **968**, la etapa **970** se realiza donde termina el proceso **900**, se realiza otro procesamiento, o el proceso **900** vuelve a la etapa **902**.

Como se muestra en la figura 6E, la etapa **672** implica mostrar opcionalmente la cantidad de veces que se puede

desbloquear el bloqueo, se puede soltar/retirar una tachuela/pasador/acollador, y/o se puede calentar un adhesivo con la tecla de separación en una pantalla de visualización del MCD. En una etapa siguiente **674**, el MCD simplemente envía la información recibida de RTS a PD sin modificación. La información puede incluir, pero no se limita a, una clave/código de separación, tiempo de espera de información, y/o información que especifique el número de veces que se puede usar la clave/código de separación. La información se puede enviar en una o más transmisiones desde el MCD al PD.

En el PD, las operaciones se realizan para separar o desactivar la etiqueta de seguridad utilizando la clave de separación y/u otra información. Un método a modo de ejemplo de las operaciones del PD para separar o desactivar una etiqueta de seguridad electromecánica se describirá en detalle a continuación en relación con la figura 10. Todavía, debe entenderse que tales operaciones generalmente implican: comunicar una señal a la etiqueta de seguridad para hacer que se abra un bloqueo electrónico, retirar una tachuela/pasador/acollador y/o calentar un adhesivo con la tecla de separación utilizando las instrucciones y/o la clave de separación; recibir información de la etiqueta de seguridad que indica si el bloqueo electrónico fue desbloqueado o no, la tachuela/alfiler/acollador se retiró con éxito y/o el adhesivo se calentó con éxito; y/o reenviando dicha información en un mensaje de respuesta desde el PD al MCD.

Si el MCD no recibe el mensaje de respuesta dentro del período de tiempo predefinido [**978**: NO], luego, el MCD informa al usuario y/o RTS que la separación/desactivación de la etiqueta de seguridad ha fallado. En contraste, si el MCD recibe el mensaje de respuesta dentro del período de tiempo predefinido [**978**: SÍ], luego, el MCD informa al usuario y/o RTS de que la separación/desactivación de la etiqueta de seguridad fue exitoso. Al completar la etapa **980** o **982**, la etapa **984** se realiza donde termina el proceso **900**, se realiza otro procesamiento, o el proceso **900** vuelve a la etapa **902**.

Como se señaló anteriormente, la etiqueta de seguridad se puede colocar en una bandeja de recolección una vez que se ha separado del artículo. Posteriormente, la etiqueta de seguridad se puede adjuntar a otro artículo. En este sentido, el bloqueo electrónico de la etiqueta de seguridad se puede bloquear en respuesta a la recepción de un código de bloqueo de un dispositivo externo (por ejemplo, el PD **190** de la figura 1, el MCD **104** de la figura 1 o el RTS **118** de la figura 1). También, la etiqueta de seguridad puede enviar un mensaje de respuesta al dispositivo externo que indica que el bloqueo electrónico se ha bloqueado una vez más. Este proceso de bloqueo puede ser activado por otra lectura del identificador único (por ejemplo, identificador único **210** de la figura 2) almacenados en la etiqueta de seguridad. Alternativa o adicionalmente, el bloqueo electrónico, tachuela, alfiler y/o el cordón de seguridad se pueden asegurar automáticamente cuando el tiempo expire según lo especificado por la información de límite de tiempo recibida desde el dispositivo externo. También, un mecanismo de tiempo de espera de la etiqueta de seguridad puede comenzar después de que haya expirado el período de tiempo predeterminado programado en la etiqueta de seguridad.

Haciendo referencia ahora a la figura 10, se proporciona un diagrama de flujo de un proceso a modo de ejemplo 1000 para separar o desactivar una etiqueta de seguridad electromecánica utilizando un PD (por ejemplo, PD **190** de la figura 1) de un MCD (por ejemplo, MCD **104** de la figura 1). Más específicamente, el proceso 1000 es el algoritmo de control básico que puede ser ejecutado por un controlador (por ejemplo, controlador **406** de la figura 4) del PD para controlar las operaciones del sistema de desactivación de etiquetas (por ejemplo, el sistema de desactivación de etiquetas **420** de la figura 4) del PD.

Como se muestra en la figura 10, el proceso 1000 comienza con la etapa 1002 y continúa con la etapa 1004. La etapa 1004 implica realizar las operaciones con un controlador de un PD para determinar si un capacitor (por ejemplo, El condensador **512** de la figura 5) de un sistema de desactivación de etiquetas (por ejemplo, sistema **420** de la figura 4) está suficientemente cargado. Por ejemplo, el PD determina si el condensador está cargado a una tensión en o por encima de un nivel mínimo de carga efectiva. Si el condensador está suficientemente cargado [1006: SÍ], luego se realizan las etapas 1024-1032. Las etapas 1024-1032 se describirán a continuación. En contraste, si el condensador no está suficientemente cargado [1006: NO], luego se realizan las etapas 1008-1022.

Como se muestra en la figura 10, la etapa 1008 es una etapa de decisiones en el que se determina si una fuente de alimentación interna (por ejemplo, la fuente de alimentación interna **430** de la figura 4) del PD está suficientemente cargada (por ejemplo, tiene un nivel de tensión por encima de un nivel de tensión de umbral). Si la fuente de alimentación interna está suficientemente cargada [1008: SÍ], luego un circuito de carga del condensador (por ejemplo, el circuito **504** de la figura 5) se activa para que el condensador se recargue desde la fuente de alimentación interna, como se muestra en la figura 1010. En este sentido, la etapa 1010 implica cerrar un interruptor (por ejemplo, el interruptor **508** de la figura 5). Posteriormente, el proceso 1000 vuelve a la etapa 1006. En contraste, de la fuente de alimentación interna no está suficientemente cargada [1008: NO], luego se realiza la etapa 1012 cuando se comunica un mensaje de notificación desde el PD al MCD a través de un SRC (por ejemplo, una comunicación Bluetooth). El mensaje de notificación indica que la fuente de alimentación interna debe ser recargada. Después, un mensaje de apagado se comunica desde el PD al MCD a través de un SRC (por ejemplo, una comunicación Bluetooth) para ejecutar un apagado suave, como se muestra en la figura 1014. En una próxima etapa 1016, cualquier parámetro necesario se escribe en una memoria (por ejemplo, la memoria **412** de la figura 4) del PD y/o una memoria (por ejemplo, **312** de la figura 3) del MCD para su almacenamiento. La DP luego pasa a un modo

de suspensión, como se muestra en la figura 1018. En modo de suspensión, el PD espera un período de tiempo predeterminado para expirar. En este sentido, se está ejecutando un tiempo de baja potencia dentro de el PD durante el modo de suspensión. Cuando el período de tiempo predeterminado ha expirado [1020: SÍ], el proceso 100 vuelve a la etapa 1002, como se muestra en la figura 1022.

Como también se muestra en la figura 10, el PD espera un mensaje de activación del MCD como se muestra en las etapas 1024 y 1026. Cuando el mensaje de activación es recibido por el PD [1026: SÍ], luego se realizan las etapas 1028-1032. En la etapa 1028, el condensador se descarga a través de una antena (por ejemplo, la antena **516** de la figura 5) produciendo así una serie de alta energía de pulsos electromagnéticos a una frecuencia sintonizada con la frecuencia de una etiqueta de seguridad. A continuación, un mensaje se comunica en la etapa **130** desde el PD al MCD a través de un SRC (por ejemplo, una comunicación Bluetooth). El mensaje indica la finalización del evento de desactivación. Después, la etapa 1032 se realiza donde termina el proceso 1000, se realiza otro procesamiento, o el proceso 1000 vuelve a la etapa 1002.

Todos los aparatos, los métodos y algoritmos descritos y reivindicados en este documento pueden elaborarse y ejecutarse sin experimentación excesiva a la luz de la presente descripción. Si bien la invención se ha descrito en términos de realizaciones preferidas, Será evidente para los expertos en la técnica que pueden aplicarse variaciones al aparato, Métodos y secuencia de etapas del método sin apartarse del concepto espíritu y alcance de la invención. Más específicamente, Será evidente que ciertos componentes pueden ser agregados a, combinados con, o sustituidos por los componentes descritos en este documento, mientras que se obtendrían resultados iguales o similares. Todos estos sustitutos y modificaciones similares evidentes para los expertos en la técnica se consideran dentro del alcance y concepto de la invención tal como se define.

REIVINDICACIONES

1. Un método para operar una etiqueta de seguridad (132) de un sistema de vigilancia electrónica de artículos ("EAS") (100), que comprende:

ejecutar en un dispositivo móvil de punto de venta ("POS") una aplicación operativa para controlar las operaciones de un dispositivo periférico (190) conectado mecánicamente al dispositivo móvil de POS para facilitar el desempeño de una transacción de compra;
recibir, mediante el dispositivo móvil de POS, una solicitud para separar de un artículo (102) una etiqueta de seguridad que tiene un identificador único (132);
en respuesta a la solicitud, comunicar un mensaje desde el dispositivo móvil de POS de POS al dispositivo periférico (190) a través de una primera comunicación de corto alcance, estando el mensaje configurado para hacer que el dispositivo periférico (190) realice operaciones para facilitar una separación de la etiqueta de seguridad (132) del artículo (102); y
provocar un accionamiento de un mecanismo de separación de la etiqueta de seguridad (132) o un calentamiento de un adhesivo dispuesto en la etiqueta de seguridad (132) al comunicar una señal desde el dispositivo periférico (190) a la etiqueta de seguridad (132).

2. El método de acuerdo con la reivindicación 1, en el que el dispositivo periférico (190) envuelve al menos una porción del dispositivo móvil de POS.

3. El método de acuerdo con la reivindicación 1, que comprende además obtener acceso a un área segura de una tienda al por menor comunicando una segunda comunicación de corto alcance desde el dispositivo periférico (190).

4. El método de acuerdo con la reivindicación 1, que comprende además obtener acceso a equipo pesado comunicando una segunda comunicación de corto alcance desde el dispositivo periférico.

5. El método de acuerdo con la reivindicación 1, que comprende, además:

obtener, mediante el dispositivo periférico (190), información del artículo para el artículo (102) a través de una segunda comunicación de corto alcance; y
reenviar la información del artículo desde el dispositivo periférico (190) al dispositivo móvil de POS a través de una tercera comunicación de corto alcance.

6. El método de acuerdo con la reivindicación 1, que comprende, además:

obtener información de pago para el artículo (102) utilizando un lector de tarjeta electrónico o una unidad de comunicación de corto alcance del dispositivo periférico (190); y
reenviar la información de pago desde el dispositivo periférico (190) al dispositivo móvil de POS a través de una segunda comunicación de corto alcance.

7. El método de acuerdo con la reivindicación 1, que comprende además comunicar información de artículos de venta al por menor o información de recibos desde el dispositivo periférico (190) a un dispositivo de comunicación móvil (104) a través de una segunda comunicación de corto alcance.

8. El método de acuerdo con la reivindicación 1, que comprende, además:

obtener, mediante el dispositivo periférico (190), un identificador único para la etiqueta de seguridad (132) a través de una segunda comunicación de corto alcance; y
reenviar el identificador único desde el dispositivo periférico (190) al dispositivo móvil de POS a través de una tercera comunicación de corto alcance.

9. El método de acuerdo con la reivindicación 9, en donde la segunda comunicación de corto alcance es una comunicación de código de barras o una comunicación de campo cercano.

10. Un sistema de vigilancia electrónica de artículos ("EAS") (100), que comprende: una etiqueta de seguridad (132) unida a un artículo (102);

un dispositivo móvil de punto de venta ("POS") configurado para controlar las operaciones de un dispositivo periférico (190) para facilitar el desempeño de una transacción de compra, y
recibir una solicitud para separar del artículo (102) una etiqueta de seguridad que tiene un identificador único (132); y
el dispositivo periférico (190) acoplado físicamente al dispositivo móvil de POS y configurado para recibir un mensaje, desde el dispositivo móvil de POS a través de una primera comunicación de corto alcance, que está configurado para hacer que el dispositivo periférico (190) realice operaciones para facilitar una separación de la etiqueta de seguridad (132) del artículo (102), y

comunicar una señal a la etiqueta de seguridad (132) para provocar la activación de un mecanismo de separación de la etiqueta de seguridad (132) o el calentamiento de un adhesivo dispuesto en la etiqueta de seguridad (132).

11. El sistema de acuerdo con la reivindicación 10, en el que el dispositivo periférico (190) envuelve al menos una porción del dispositivo móvil de POS.

12. El sistema de acuerdo con la reivindicación 10, en el que el dispositivo periférico (190) está configurado además para comunicar una segunda comunicación de corto alcance desde el mismo para hacer que un área segura de una tienda al por menor sea accesible para un empleado de tienda.

13. El sistema de acuerdo con la reivindicación 10, en el que el dispositivo periférico (190) está configurado además para comunicar una segunda comunicación de corto alcance desde el mismo para hacer que el equipo pesado sea accesible para un empleado de tienda.

14. El sistema de acuerdo con la reivindicación 10, en el que el dispositivo periférico (190) está configurado además para obtener información del artículo para el artículo (102) a través de una segunda comunicación de corto alcance, y reenviar la información del artículo al dispositivo móvil de POS a través de una tercera comunicación de corto alcance.

15. El sistema de acuerdo con la reivindicación 10, en el que el dispositivo periférico (190) está configurado además para obtener información de pago para el artículo (102) usando un lector de tarjetas electrónico o una unidad de comunicación de corto alcance del dispositivo periférico (190), y reenviar la información de pago al dispositivo móvil de POS a través de una segunda comunicación de corto alcance.

16. El sistema de acuerdo con la reivindicación 10, en el que el dispositivo periférico (190) está configurado además para comunicar información de artículos minoristas o información de recibos a un dispositivo de comunicaciones móviles (104) a través de una segunda comunicación de corto alcance.

17. El sistema de acuerdo con la reivindicación 10, en el que el dispositivo periférico (190) está configurado además para obtener un identificador único para la etiqueta de seguridad (132) a través de una segunda comunicación de corto alcance; y reenviar el identificador único al dispositivo móvil de POS a través de una tercera comunicación de corto alcance.

18. El sistema de acuerdo con la reivindicación 17, en donde la segunda comunicación de corto alcance es una comunicación de código de barras o una comunicación de campo cercano.

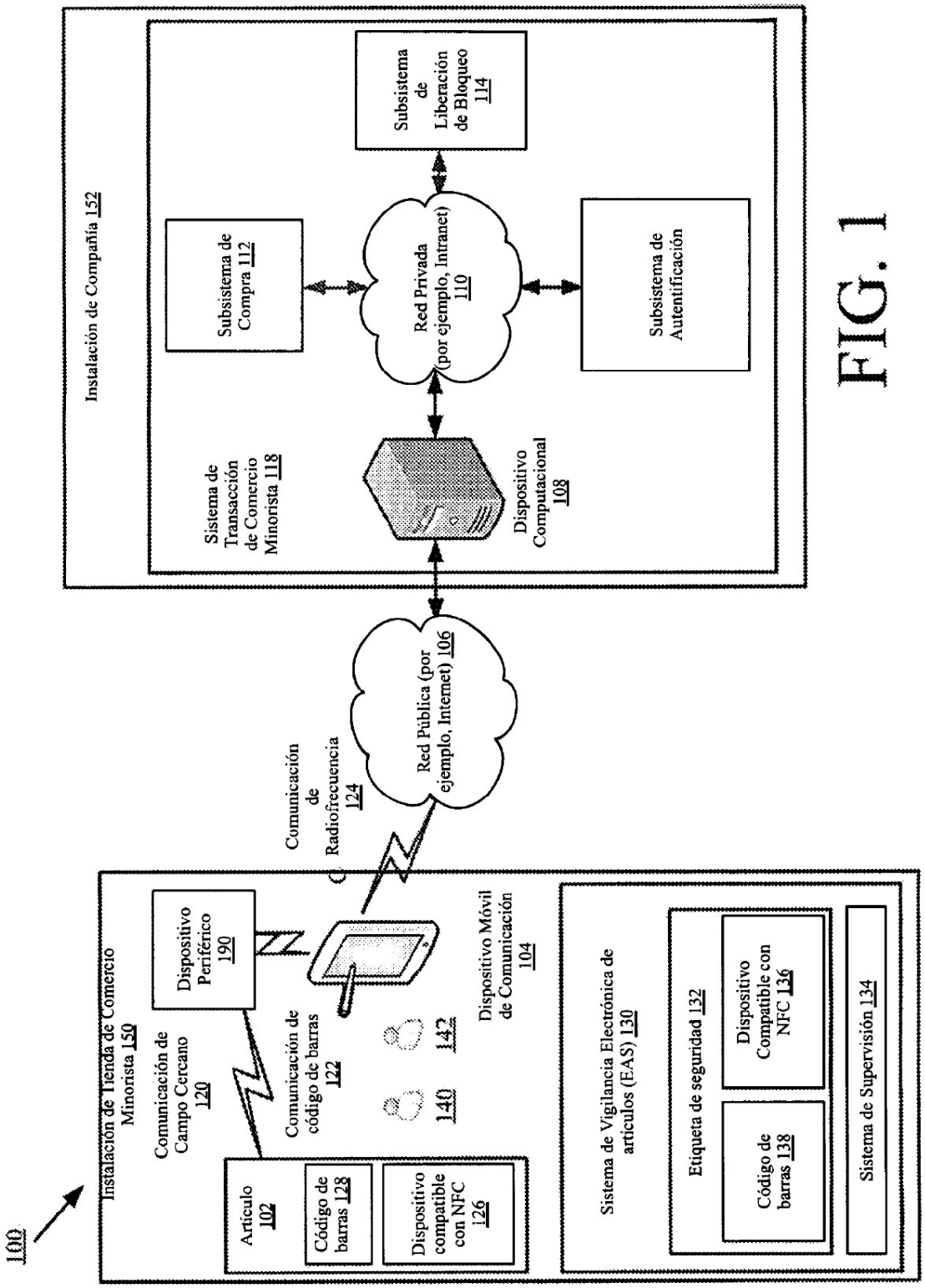
100
Instalación de Tienda de Comercio Minorista 150
Artículo 102
Código de barras 128
Dispositivo compatible con NFC 126
Comunicación de Campo Cercano 120
Dispositivo Periférico 190
Comunicación de código de barras 122
140
142
Dispositivo Móvil de Comunicación 104
Comunicación de Radiofrecuencia 124
Red Pública (por ejemplo, Internet) 106
Sistema de Vigilancia Electrónica de artículos (EAS) 130
Etiqueta de seguridad 132
Código de barras 138
Dispositivo Compatible con NFC 136
Sistema de Supervisión 134
Instalación de Compañía 152
Sistema de Transacción de Comercio Minorista 118
Dispositivo Computacional 108
Red Privada (por ejemplo, Intranet) 110
Subsistema de Compra 112
Subsistema de Liberación de Bloqueo 114
Subsistema de Autentificación

FIG. 1

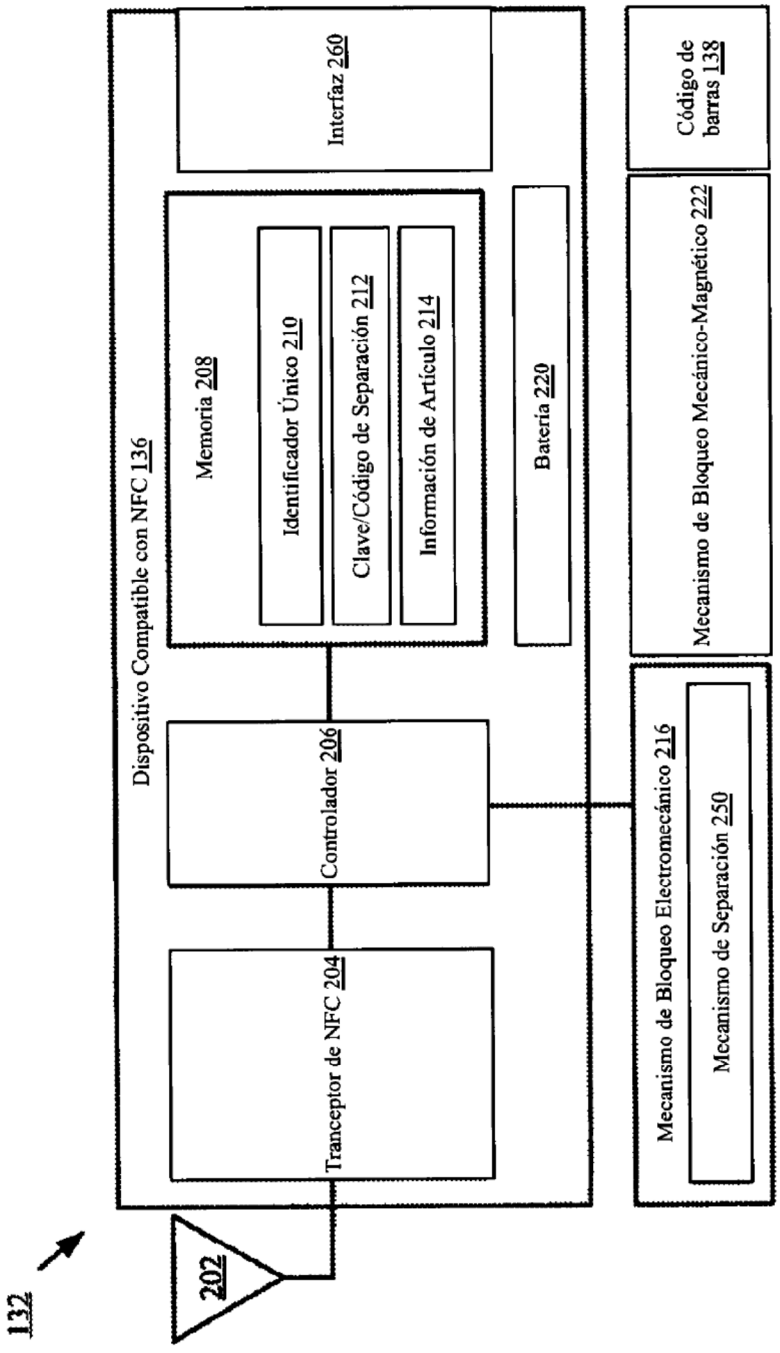
132
202
Dispositivo Compatible con NFC 136
Tranceptor de NFC 204
Controlador 206
Memoria 208
Identificador Único 210
Clave/Código de Separación 212
Información de Artículo 214
Batería 220
Interfaz 260
Mecanismo de Bloqueo Electromecánico 216
Mecanismo de Separación 250
Mecanismo de Bloqueo Mecánico-Magnético 222
Código de barras 138

FIG. 2

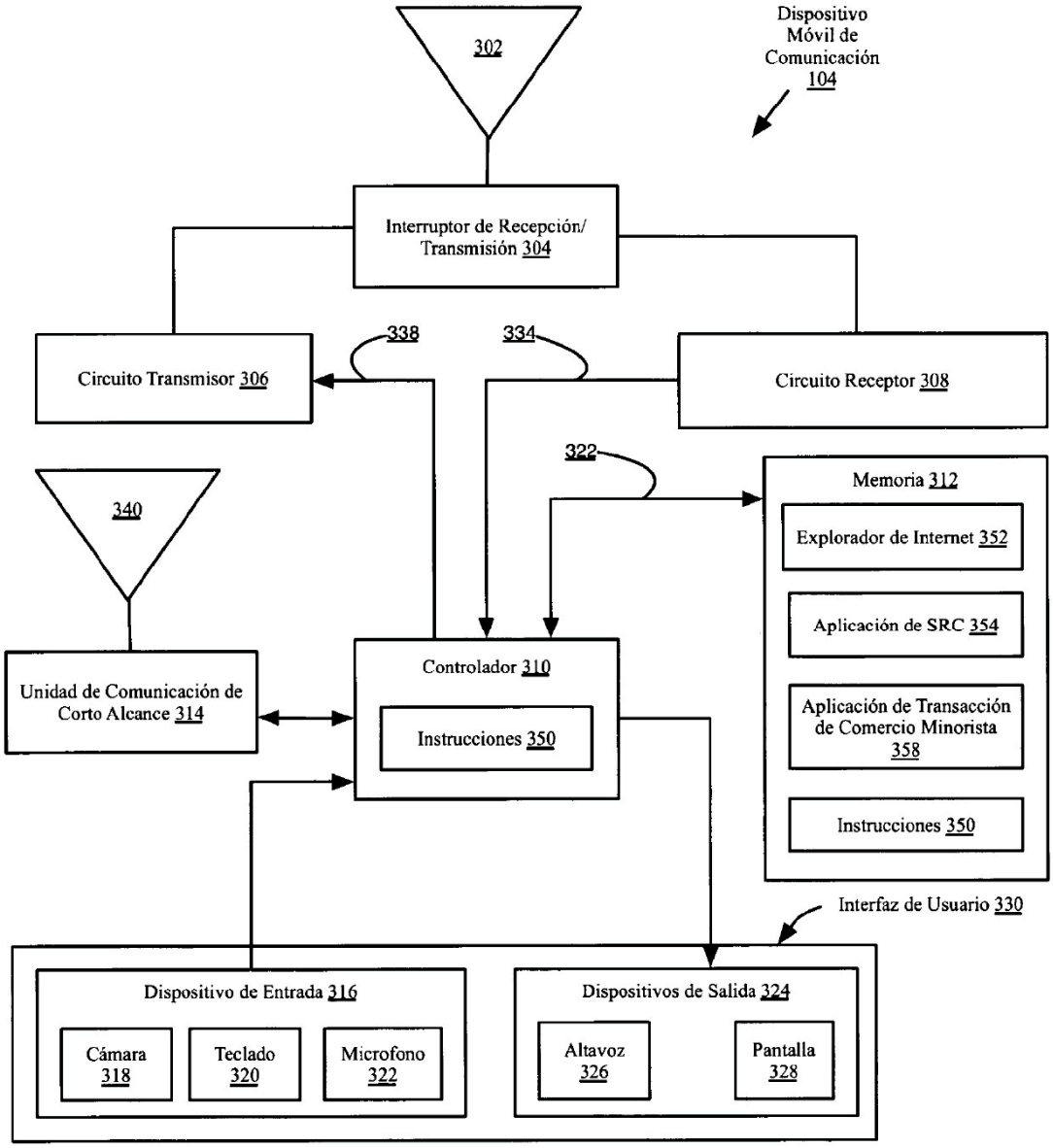
Dispositivo Móvil de Comunicación 104
302
Interruptor de Recepción/ Transmisión 304
338
334
Circuito Transmisor 306
Circuito Receptor 308
322
Memoria 312
Explorador de Internet 352
Aplicación de SRC 354
Aplicación de Transacción de Comercio Minorista 358
Instrucciones 350
340
Unidad de Comunicación de Corto Alcance 314
Controlador 310
Instrucciones 350
Interfaz de Usuario 330
Dispositivo de Entrada 316
Cámara 318
Teclado 320
Microfono 322
Dispositivos de Salida 324
Altavoz 326
Pantalla 328

FIG. 3

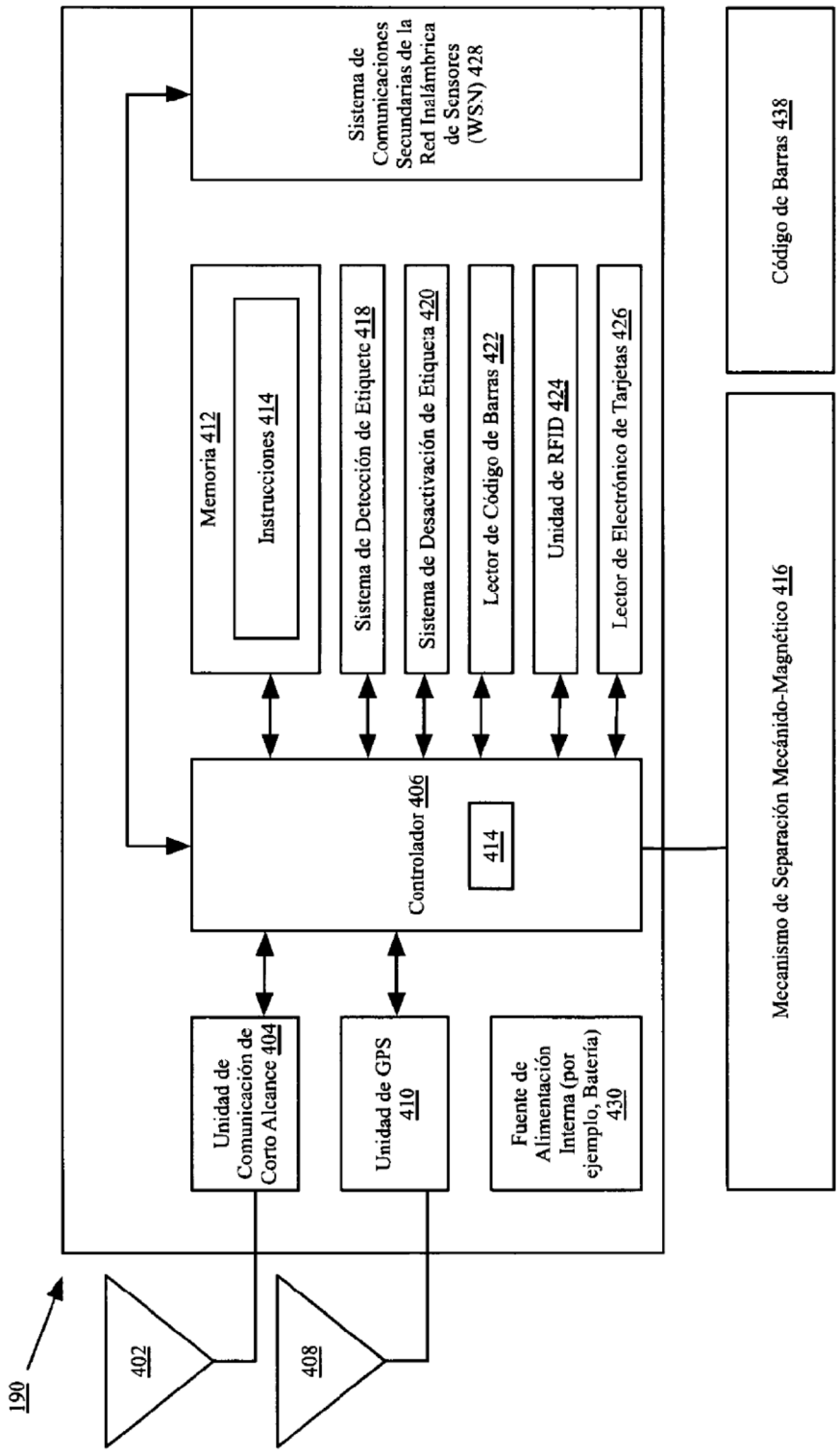
190
402
408
Unidad de Comunicación de Corto Alcance 404
Unidad de GPS 410
Fuente de Alimentación Interna (por ejemplo, Batería) 430
Controlador 406
414
Memoria 412
Instrucciones 414
Sistema de Detección de Etiquete 418
Sistema de Desactivación de Etiqueta 420
Lector de Código de Barras 422
Unidad de RFID 424
Lector de Electrónico de Tarjetas 426
Sistema de Comunicaciones Secundarias de la Red Inalámbrica de Sensores (WSN) 428
Mecanismo de Separación Mecánido-Magnético 416
Código de Barras 438

FIG. 4

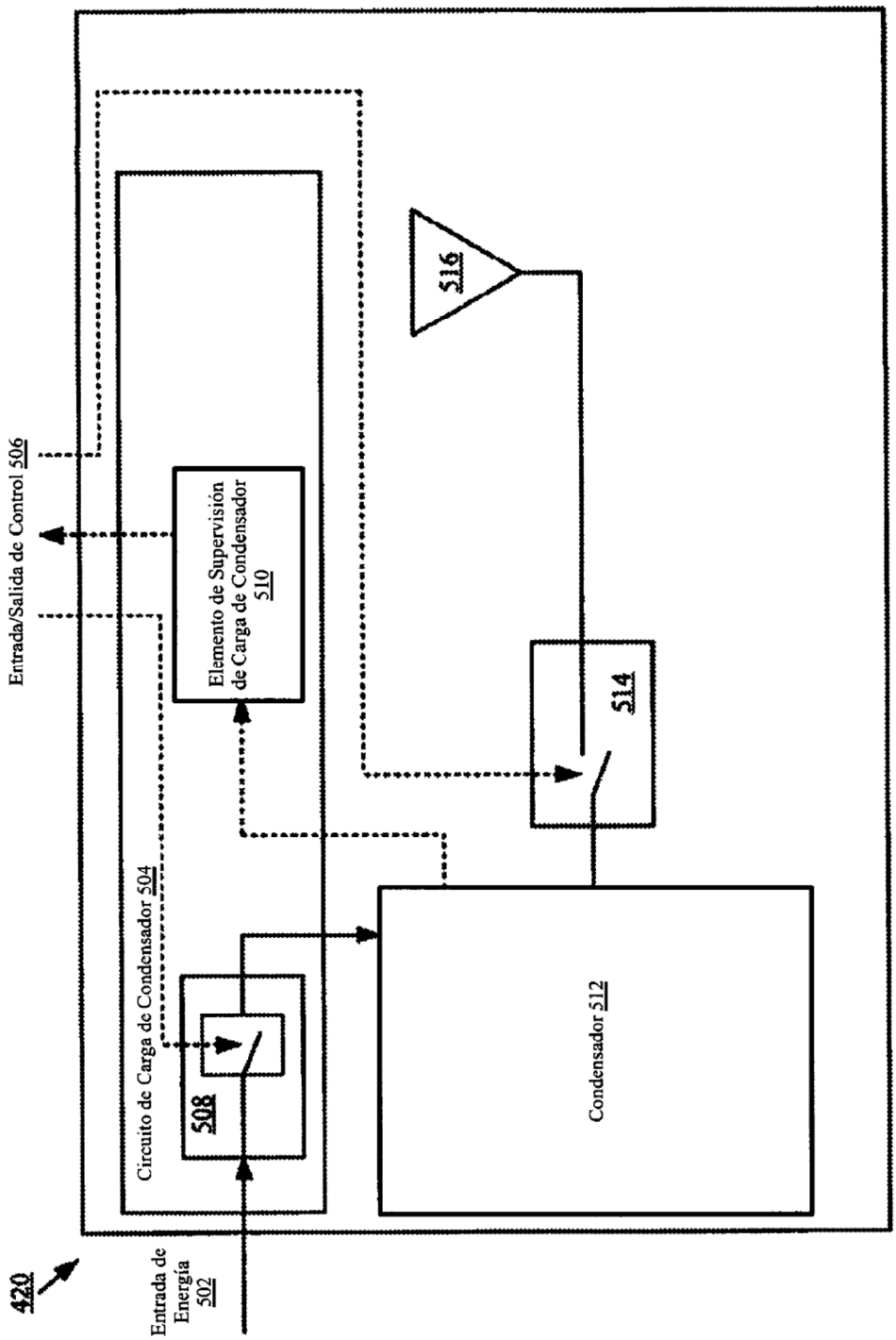
420
Entrada de Energía 502
Circuito de Carga de Condensador 504
508
Condensador 512
514
516
Elemento de Supervisión de Carga de Condensador 510
Entrada/Salida de Control 506

FIG. 5

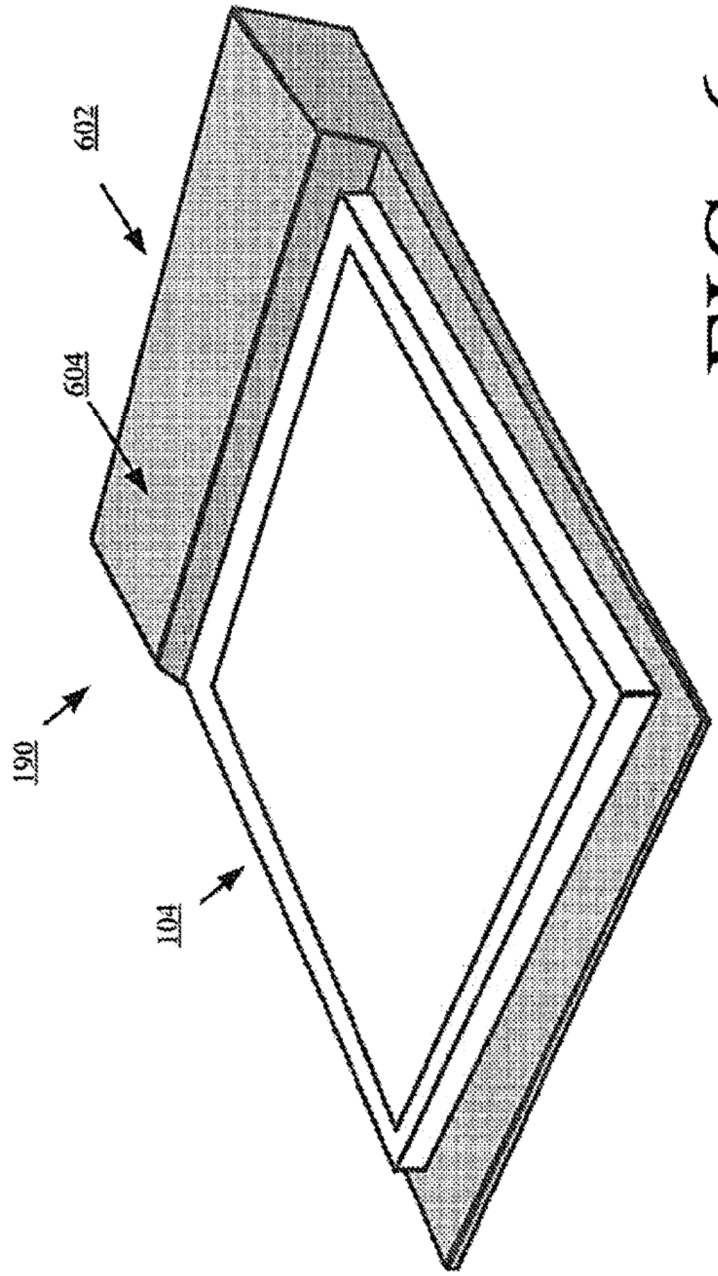

FIG. 6

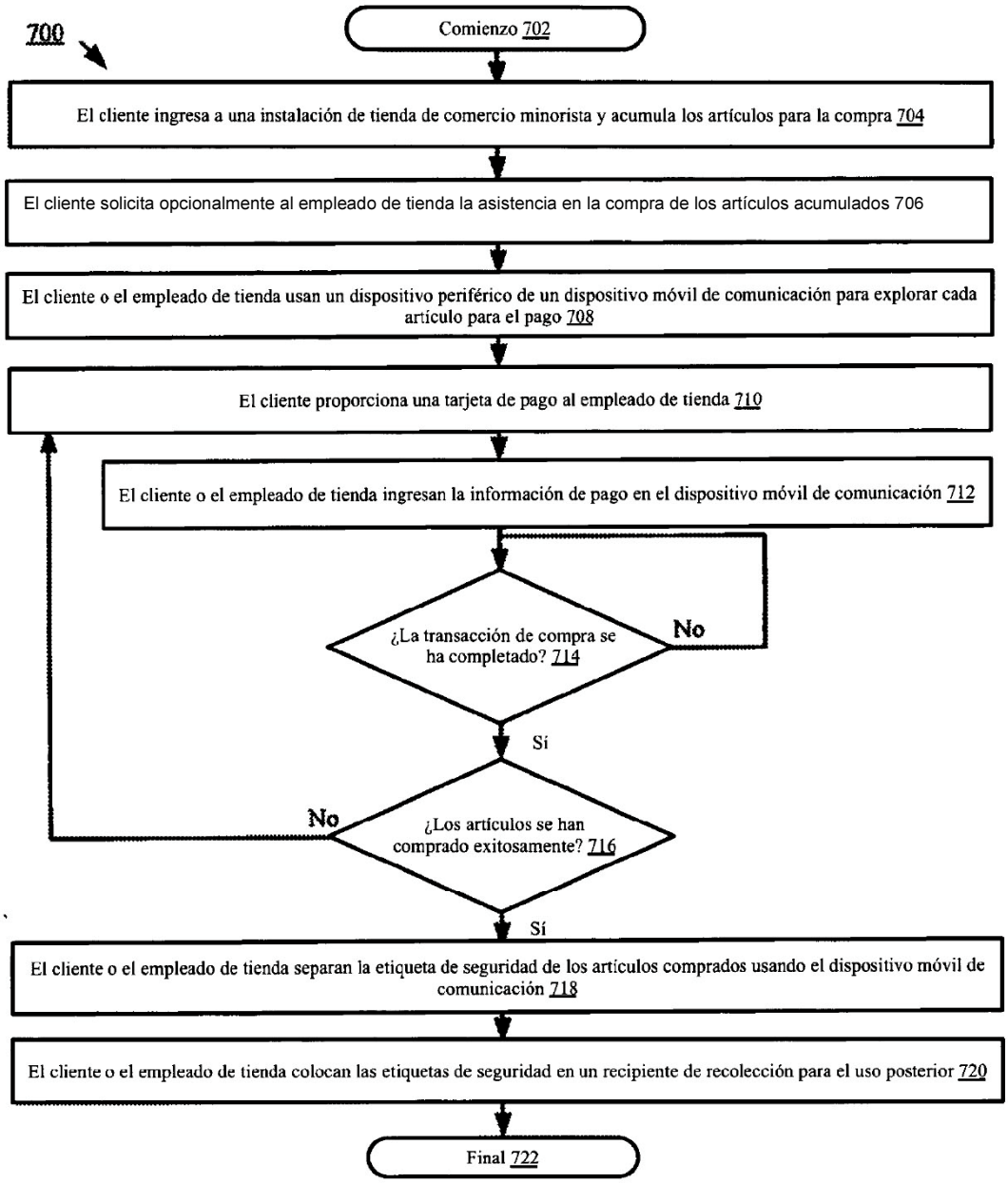
700
Comienzo 702
El cliente ingresa a una instalación de tienda de comercio minorista y acumula los artículos para la compra 704
El cliente solicita opcionalmente al empleado de tienda la asistencia en la compra de los artículos acumulados 706
El cliente o el empleado de tienda usan un dispositivo periférico de un dispositivo móvil de comunicación para explorar cada artículo para el pago 708
El cliente proporciona una tarjeta de pago al empleado de tienda 710
El cliente o el empleado de tienda ingresan la información de pago en el dispositivo móvil de comunicación 712
¿La transacción de compra se ha completado? 714
No
Sí
¿Los artículos se han comprado exitosamente? 716
No
Sí
El cliente o el empleado de tienda separan la etiqueta de seguridad de los artículos comprados usando el dispositivo móvil de comunicación 718
El cliente o el empleado de tienda colocan las etiquetas de seguridad en un recipiente de recolección para el uso posterior 720
Final 722

FIG. 7

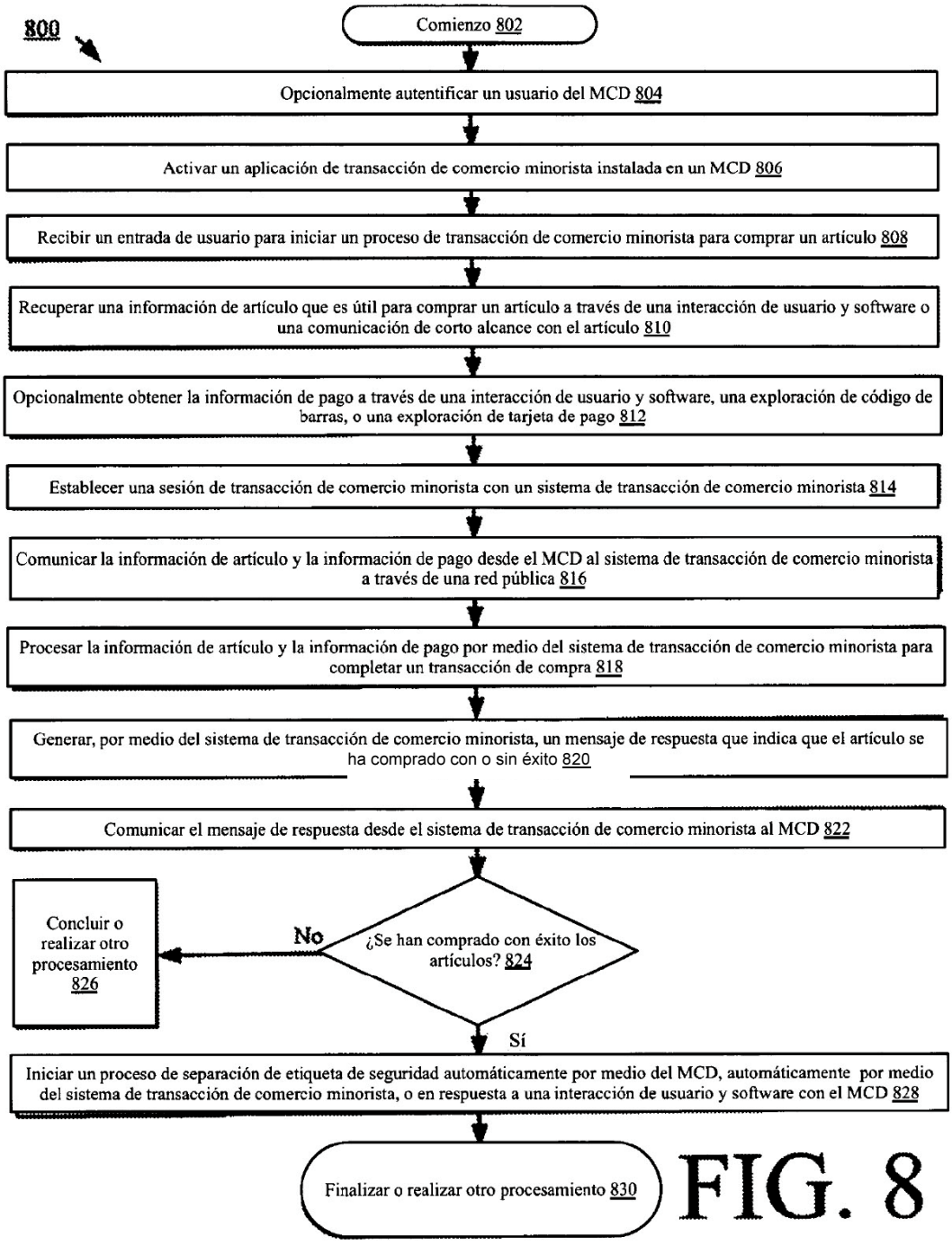
800
Comienzo 802
Opcionalmente autentificar un usuario del MCD 804
Activar un aplicación de transacción de comercio minorista instalada en un MCD 806
Recibir un entrada de usuario para iniciar un proceso de transacción de comercio minorista para comprar un artículo 808
Recuperar una información de artículo que es útil para comprar un artículo a través de una interacción de usuario y software o una comunicación de corto alcance con el artículo 810
Opcionalmente obtener la información de pago a través de una interacción de usuario y software, una exploración de código de barras, o una exploración de tarjeta de pago 812
Establecer una sesión de transacción de comercio minorista con un sistema de transacción de comercio minorista 814
Comunicar la información de artículo y la información de pago desde el MCD al sistema de transacción de comercio minorista a través de una red pública 816
Procesar la información de artículo y la información de pago por medio del sistema de transacción de comercio minorista para completar un transacción de compra 818
Generar, por medio del sistema de transacción de comercio minorista, un mensaje de respuesta que indica que el artículo se ha comprado con o sin éxito 820
Comunicar el mensaje de respuesta desde el sistema de transacción de comercio minorista al MCD 822
¿Se han comprado con éxito los artículos? 824
No
Concluir o realizar otro procesamiento 826
Sí
Iniciar un proceso de separación de etiqueta de seguridad automáticamente por medio del MCD, automáticamente por medio del sistema de transacción de comercio minorista, o en respuesta a una interacción de usuario y software con el MCD 828
Finalizar o realizar otro procesamiento 830

FIG. 8

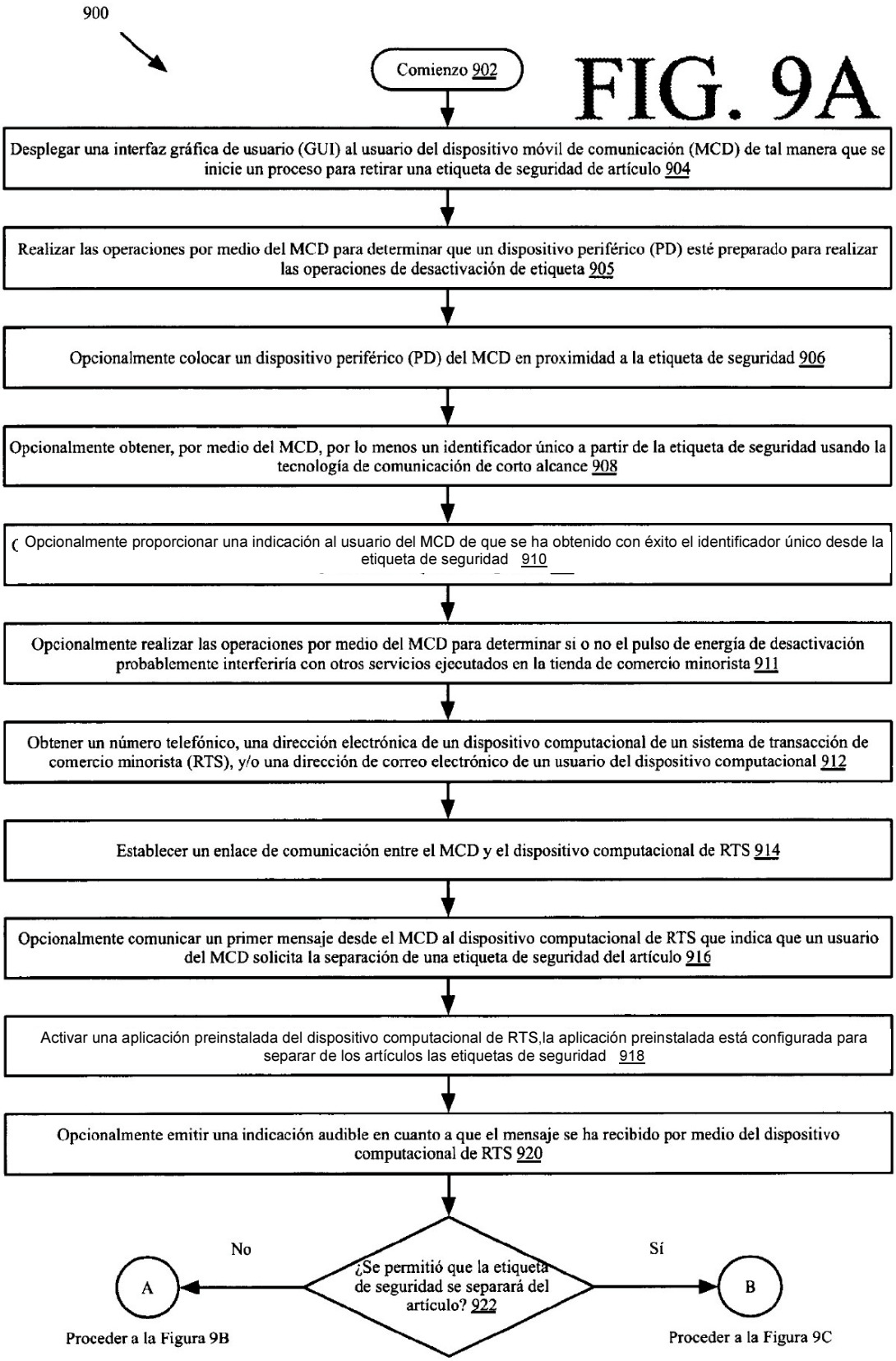
900
Comienzo 902
Desplegar una interfaz gráfica de usuario (GUI) al usuario del dispositivo móvil de comunicación (MCD) de tal manera que se inicie un proceso para retirar una etiqueta de seguridad de artículo 904
Realizar las operaciones por medio del MCD para determinar que un dispositivo periférico (PD) esté preparado para realizar las operaciones de desactivación de etiqueta 905
Opcionalmente colocar un dispositivo periférico (PD) del MCD en proximidad a la etiqueta de seguridad 906
Opcionalmente obtener, por medio del MCD, por lo menos un identificador único a partir de la etiqueta de seguridad usando la tecnología de comunicación de corto alcance 908
Opcionalmente proporcionar una indicación al usuario del MCD de que se ha obtenido con éxito el identificador único desde la etiqueta de seguridad 910
Opcionalmente realizar las operaciones por medio del MCD para determinar si o no el pulso de energía de desactivación probablemente interferiría con otros servicios ejecutados en la tienda de comercio minorista 911
Obtener un número telefónico, una dirección electrónica de un dispositivo computacional de un sistema de transacción de comercio minorista (RTS), y/o una dirección de correo electrónico de un usuario del dispositivo computacional 912
Establecer un enlace de comunicación entre el MCD y el dispositivo computacional de RTS 914
Opcionalmente comunicar un primer mensaje desde el MCD al dispositivo computacional de RTS que indica que un usuario del MCD solicita la separación de una etiqueta de seguridad del artículo 916
Activar una aplicación preinstalada del dispositivo computacional de RTS,la aplicación preinstalada está configurada para separar de los artículos las etiquetas de seguridad 918
Opcionalmente emitir una indicación audible en cuanto a que el mensaje se ha recibido por medio del dispositivo computacional de RTS 920
¿Se permitió que la etiqueta de seguridad se separará del artículo? 922
No
Sí
A
B
Proceder a la Figura 9B
Proceder a la Figura 9C

FIG. 9A

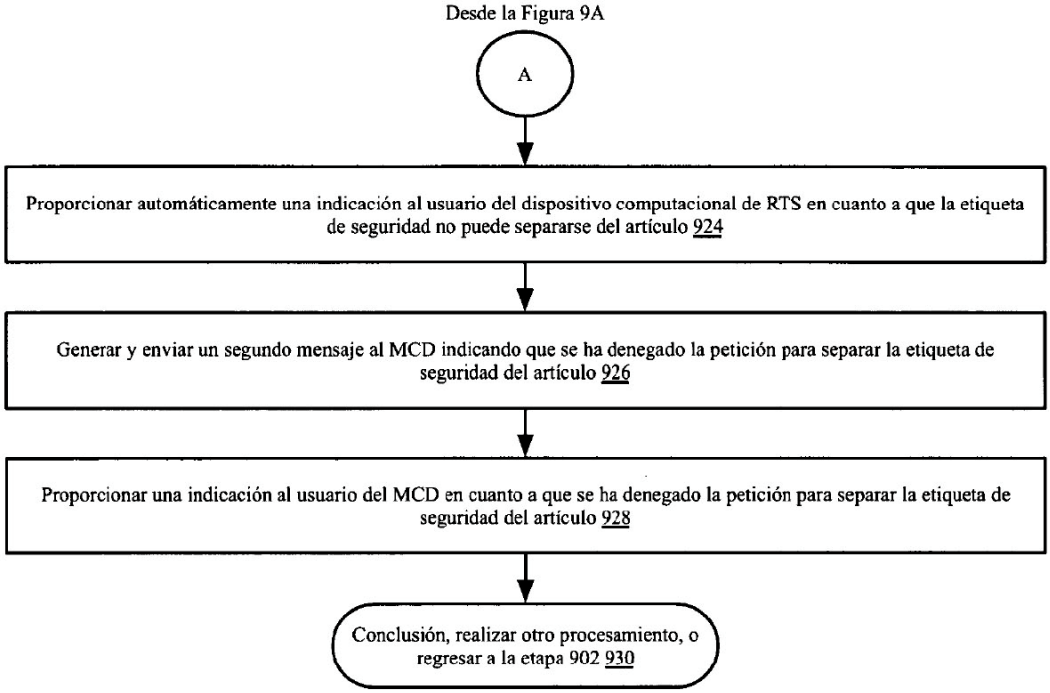
Desde la Figura 9A
A
Proporcionar automáticamente una indicación al usuario del dispositivo computacional de RTS en cuanto a que la etiqueta de seguridad no puede separarse del artículo 924
Generar y enviar un segundo mensaje al MCD indicando que se ha denegado la petición para separar la etiqueta de seguridad del artículo 926
Proporcionar una indicación al usuario del MCD en cuanto a que se ha denegado la petición para separar la etiqueta de seguridad del artículo 928
Conclusión, realizar otro procesamiento, o regresar a la etapa 902 930

FIG. 9B

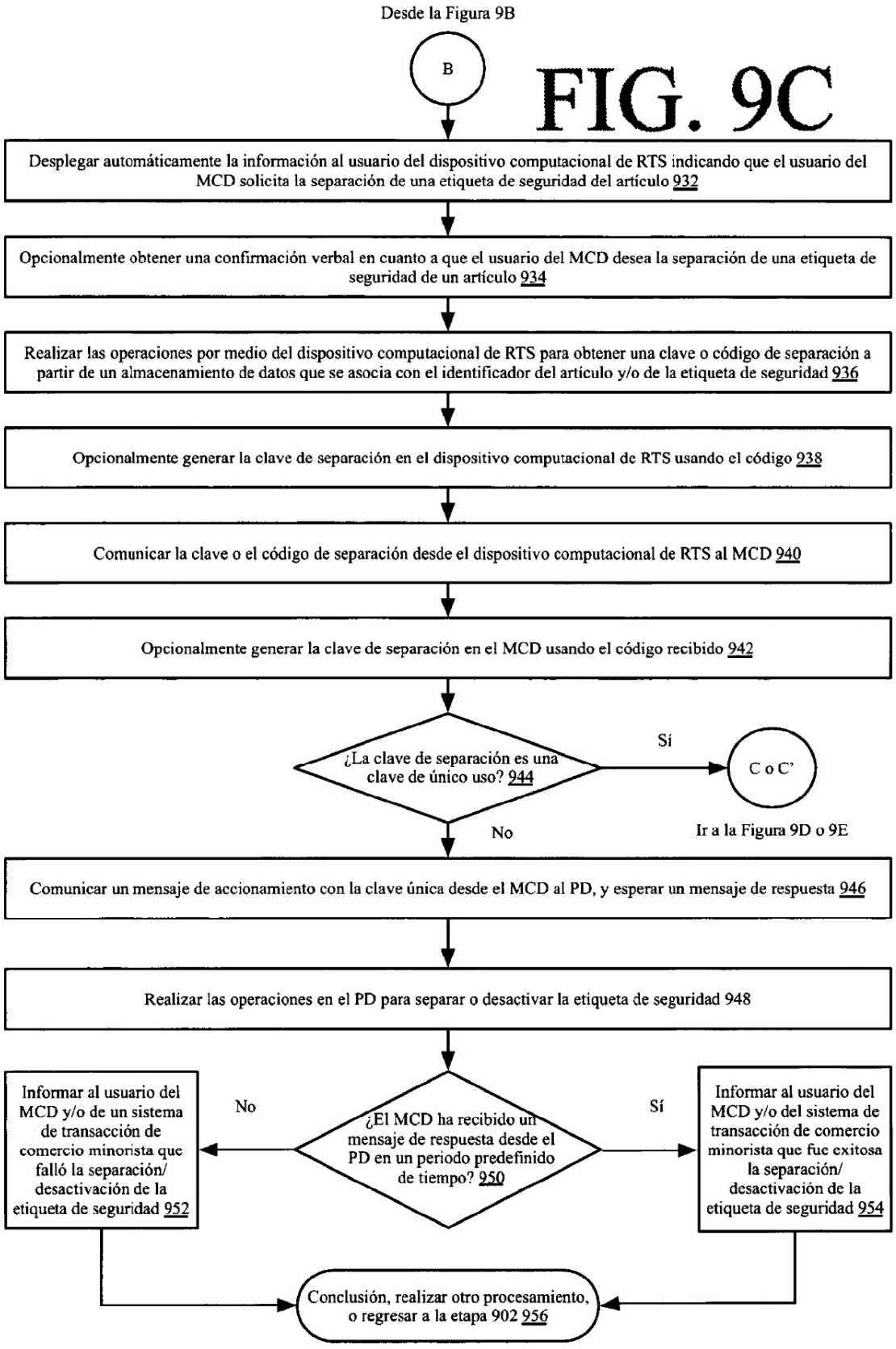
Desde la Figura 9B
B
Desplegar automáticamente la información al usuario del dispositivo computacional de RTS indicando que el usuario del MCD solicita la separación de una etiqueta de seguridad del artículo 932
Opcionalmente obtener una confirmación verbal en cuanto a que el usuario del MCD desea la separación de una etiqueta de seguridad de un artículo 934
Realizar las operaciones por medio del dispositivo computacional de RTS para obtener una clave o código de separación a partir de un almacenamiento de datos que se asocia con el identificador del artículo y/o de la etiqueta de seguridad 936
Opcionalmente generar la clave de separación en el dispositivo computacional de RTS usando el código 938
Comunicar la clave o el código de separación desde el dispositivo computacional de RTS al MCD 940
Opcionalmente generar la clave de separación en el MCD usando el código recibido 942
¿La clave de separación es una clave de único uso? 944
Sí
C o C'
Ir a la Figura 9D o 9E
No
Comunicar un mensaje de accionamiento con la clave única desde el MCD al PD, y esperar un mensaje de respuesta 946
Realizar las operaciones en el PD para separar o desactivar la etiqueta de seguridad 948
¿El MCD ha recibido un mensaje de respuesta desde el PD en un periodo predefinido de tiempo? 950
No
Sí
Informar al usuario del MCD y/o de un sistema de transacción de comercio minorista que falló la separación/ desactivación de la etiqueta de seguridad 952
Informar al usuario del MCD y/o del sistema de transacción de comercio minorista que fue exitosa la separación/ desactivación de la etiqueta de seguridad 954
Conclusión, realizar otro procesamiento, o regresar a la etapa 902 956

FIG. 9C

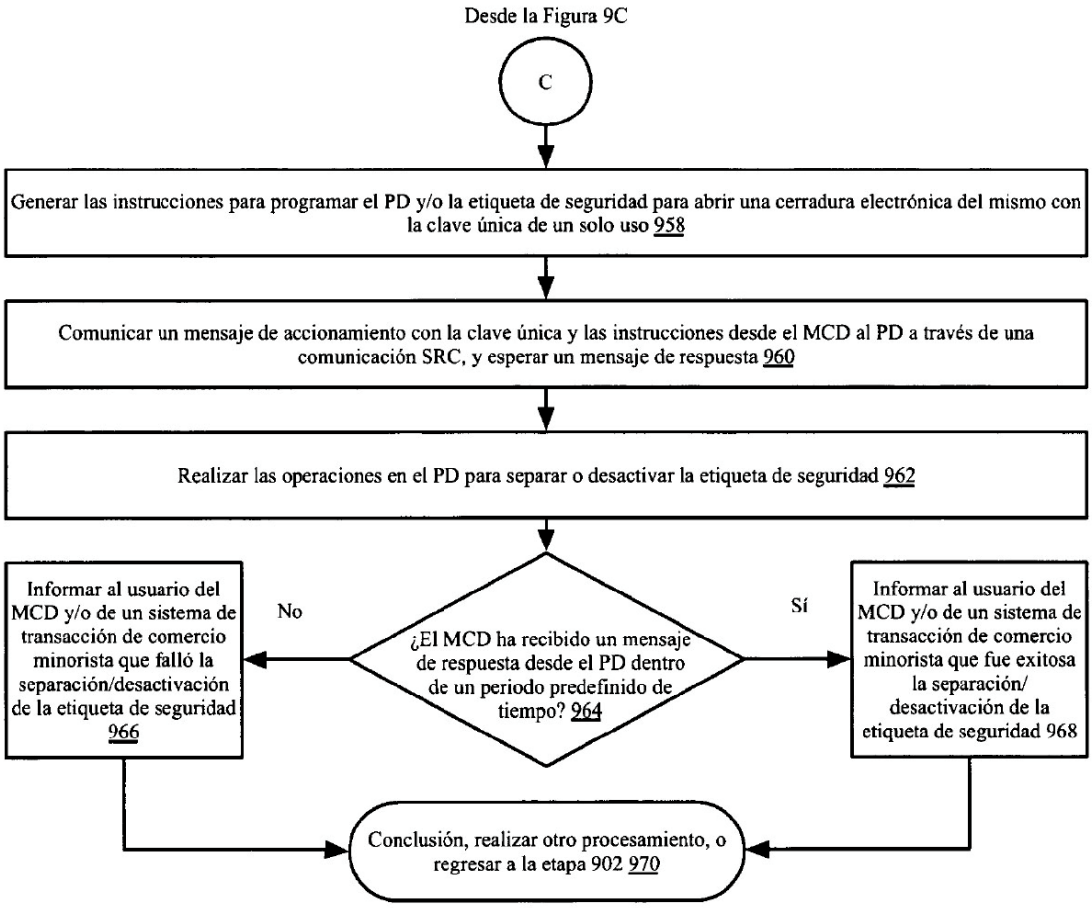
Desde la Figura 9C
C
Generar las instrucciones para programar el PD y/o la etiqueta de seguridad para abrir una cerradura electrónica del mismo con la clave única de un solo uso 958
Comunicar un mensaje de accionamiento con la clave única y las instrucciones desde el MCD al PD a través de una comunicación SRC, y esperar un mensaje de respuesta 960
Realizar las operaciones en el PD para separar o desactivar la etiqueta de seguridad 962
¿El MCD ha recibido un mensaje de respuesta desde el PD dentro de un periodo predefinido de tiempo? 964
No
Sí
Informar al usuario del MCD y/o de un sistema de transacción de comercio minorista que falló la separación/desactivación de la etiqueta de seguridad 966
Informar al usuario del MCD y/o de un sistema de transacción de comercio minorista que fue exitosa la separación/ desactivación de la etiqueta de seguridad 968
Conclusión, realizar otro procesamiento, o regresar a la etapa 902 970

FIG. 9D

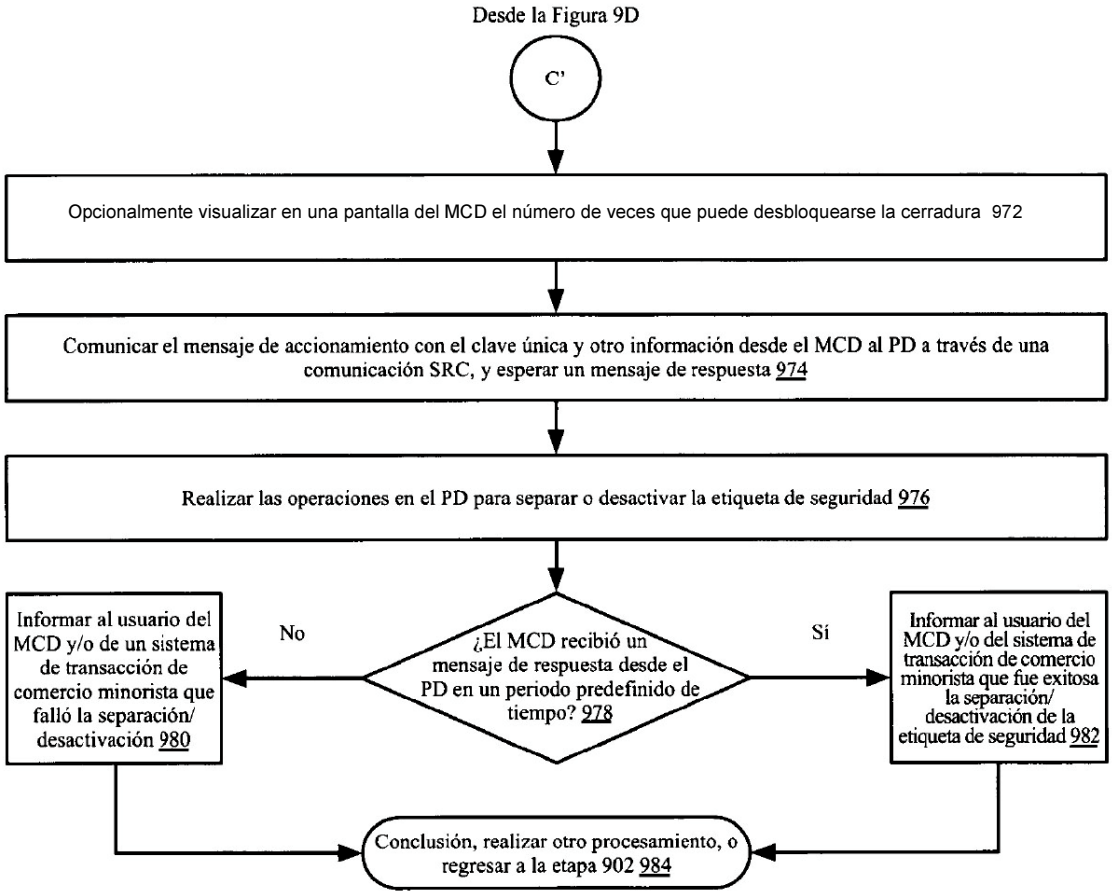
Desde la Figura 9D
C'
Opcionalmente visualizar en una pantalla del MCD el número de veces que puede desbloquearse la cerradura 972
Comunicar el mensaje de accionamiento con el clave única y otro información desde el MCD al PD a través de una comunicación SRC, y esperar un mensaje de respuesta 974
Realizar las operaciones en el PD para separar o desactivar la etiqueta de seguridad 976
¿El MCD recibió un mensaje de respuesta desde el PD en un periodo predefinido de tiempo? 978
No
Sí
Informar al usuario del MCD y/o de un sistema de transacción de comercio minorista que falló la separación/ desactivación 980
Informar al usuario del MCD y/o del sistema de transacción de comercio minorista que fue exitosa la separación/ desactivación de la etiqueta de seguridad 982
Conclusión, realizar otro procesamiento, o regresar a la etapa 902 984

FIG. 9E

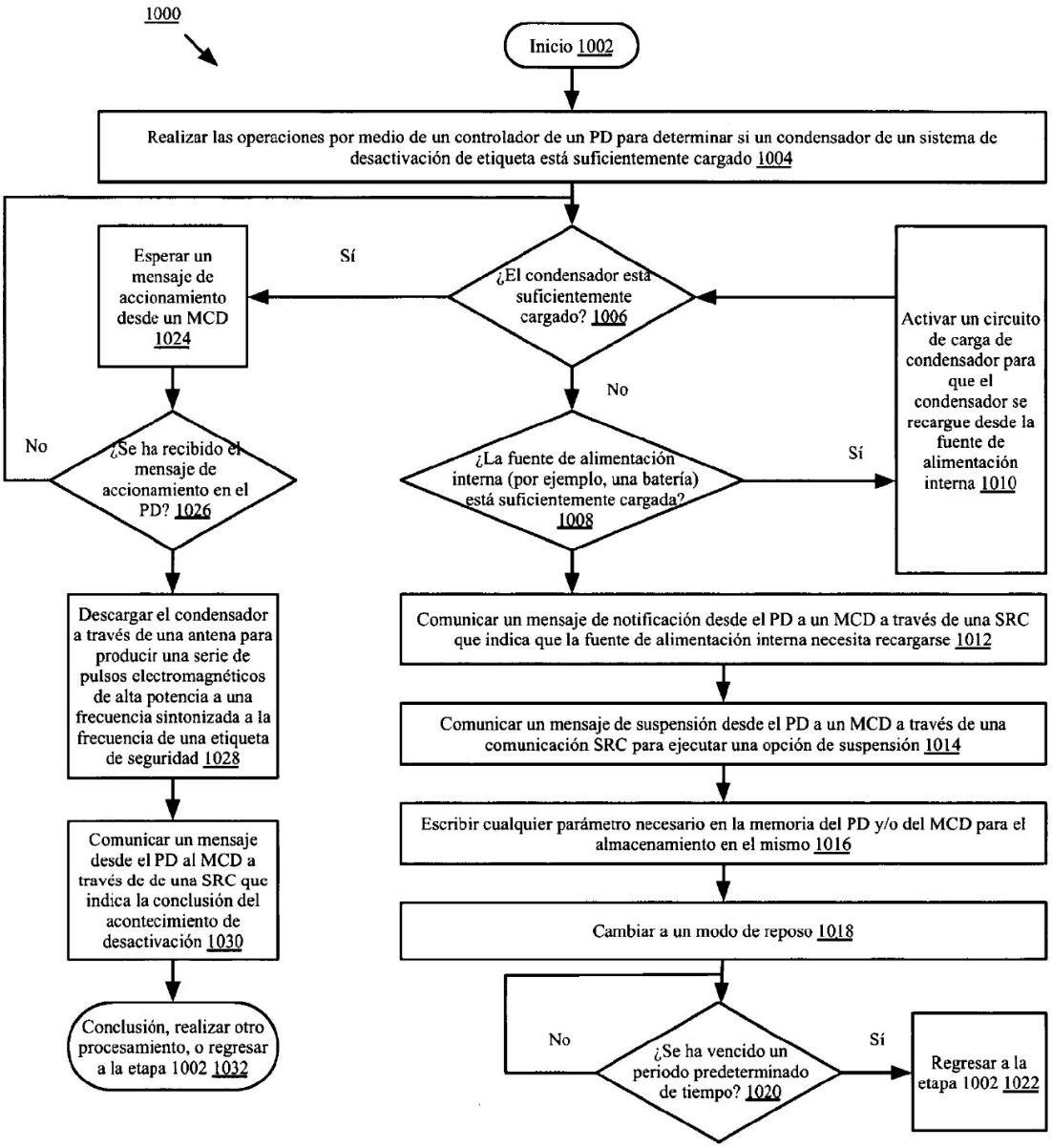
1000
Inicio 1002
Realizar las operaciones por medio de un controlador de un PD para determinar si un condensador de un sistema de desactivación de etiqueta está suficientemente cargado 1004
¿El condensador está suficientemente cargado? 1006
Sí
Esperar un mensaje de accionamiento desde un MCD 1024
Activar un circuito de carga de condensador para que el condensador se recargue desde la fuente de alimentación interna 1010
No
¿La fuente de alimentación interna (por ejemplo, una batería) está suficientemente cargada? 1008
Sí
No
¿Se ha recibido el mensaje de accionamiento en el PD? 1026
Descargar el condensador a través de una antena para producir una serie de pulsos electromagnéticos de alta potencia a una frecuencia sintonizada a la frecuencia de una etiqueta de seguridad 1028
Comunicar un mensaje desde el PD al MCD a través de de una SRC que indica la conclusión del acontecimiento de desactivación 1030
Conclusión, realizar otro procesamiento, o regresar a la etapa 1002 1032
Comunicar un mensaje de notificación desde el PD a un MCD a través de una SRC que indica que la fuente de alimentación interna necesita recargarse 1012
Comunicar un mensaje de suspensión desde el PD a un MCD a través de una comunicación SRC para ejecutar una opción de suspensión 1014
Escribir cualquier parámetro necesario en la memoria del PD y/o del MCD para el almacenamiento en el mismo 1016
Cambiar a un modo de reposo 1018
No
¿Se ha vencido un periodo predeterminado de tiempo? 1020
Sí
Regresar a la etapa 1002 1022

FIG. 10