

SOLUCIÓN BIOMÉTRICA QUE PERMITE PAGOS DE TARIFAS DE RENDIMIENTOS ALTOS Y ACCESO DE SISTEMA

Referencia Cruzada a Solicitudes Relacionadas

Esta solicitud de patente reivindica el beneficio de la Solicitud de Patente Provisional de Estados Unidos Serial No. 61/939,132 presentada el 12 de febrero de 2014 y titulada “SOLUCIÓN BIOMÉTRICA QUE PERMITE PAGOS DE TARIFAS DE RENDIMIENTOS ALTOS Y ACCESO DE SISTEMA”. La divulgación completa de la Solicitud de Patente Provisional de Estados Unidos Serial No. 61/939,132 mencionada anteriormente incluyendo los anexos de la misma se incorporan acá expresamente por referencia en su totalidad para todos los propósitos.

Campo de la Divulgación

La presente divulgación se relaciona generalmente con los artes de la electrónica y los computadores y, más particularmente, con el pago y/o control de acceso utilizando dispositivos inalámbricos y similares.

Antecedentes de la Divulgación

En comparación con los esquemas Registro Salida (también denominados de Ingreso Salida o Toque de Entrada Salida) que utilizan tarjetas inteligentes de proximidad, donde el usuario tiene que registrarse mientras ingresa o sale mientras que aterriza, Be-In Be-Out (BIBO) es el nombre común para las tecnologías de tiquetes que detectan y registran automáticamente la presencia de dispositivos inteligentes (teléfonos inteligentes o tabletas son ejemplos no limitantes) en un vehículo de transporte público. Los esquemas BIBO no requieren ninguna acción por parte del usuario y por lo tanto son “manos libres”.

Resumen de la Divulgación

Los principios de la divulgación suministran una solución biométrica que permite el pago de tarifas rendimientos altos y acceso de sistema. Algunas modalidades alternas utilizan una o más formas de autenticación diferentes a biométricos.

En un aspecto, un método ejemplar incluye detectar la presencia de un dispositivo electrónico portátil fuera de un punto de acceso a un área de acceso controlado; obtener, a partir del dispositivo electrónico portátil, una indicación que un usuario del dispositivo electrónico portátil se ha autenticado al dispositivo electrónico portátil; e iniciar un proceso de aprobación de pago asociado con una cuenta del usuario. El proceso de aprobación de pago se completa antes que el usuario busque pasar a través del punto de acceso. Pasos adicionales incluyen: con base por lo menos en parte en la obtención de la indicación de la autenticación y el éxito del proceso de aprobación de pago, suministrar al punto de acceso una ficha electrónica que indica que el usuario, que lleva el dispositivo electrónico portátil, se le debe permitir pasar a través del punto de acceso al área de acceso controlado; permitir al usuario, que lleva el dispositivo electrónico portátil, pasar a través del punto de acceso al área de acceso controlado, con base por lo menos en parte en la ficha electrónica; y hacer que la ficha electrónica expire después que el usuario pasa a través del punto de acceso al área de acceso controlado.

En otro aspecto, un sistema ejemplar incluye: un punto de acceso que controla el acceso a un área de acceso controlado; un servidor; un transceptor de comunicaciones inalámbricas de rango medio o largo; y una red de comunicaciones que ubica el punto de acceso, el servidor, y el transceptor en comunicación de datos. El transceptor se configura para detectar la presencia de un dispositivo electrónico portátil afuera del punto de acceso; el servidor se configura para obtener, del dispositivo electrónico portátil, por medio del

transceptor y la red de comunicaciones, una indicación que un usuario del dispositivo electrónico portátil se ha autenticado al dispositivo electrónico portátil; y el servidor se configura para iniciar un proceso de aprobación de pago asociado con una cuenta del usuario. El proceso de aprobación de pago se completa antes que el usuario busque pasar a través del punto de acceso. El servidor se configura para, con base por lo menos en parte en la indicación de autenticación y éxito del proceso de aprobación de pago, suministrar al punto de acceso una ficha electrónica que indica que el usuario, que lleva el dispositivo electrónico portátil, se debe permitir pasar a través de punto de acceso al área de acceso controlado; y el punto de acceso se configura para permitir que el usuario, que lleva el dispositivo electrónico portátil, pase a través del punto de acceso al área de acceso controlado, con base por lo menos en parte en la ficha electrónica.

Aspectos de la divulgación contemplan los métodos realizados por una o más entidades acá, así como facilitar uno o más pasos de método por la misma o por diferentes entidades. Como se utiliza acá, “facilitar” una acción incluye realizar la acción, hacer la acción más fácil, ayudar a llevar a cabo la acción, o hacer que la acción se realice. Así, a modo de ejemplo y no limitación, las instrucciones que se ejecutan en un procesador pueden facilitar una acción llevada a cabo por las instrucciones que se ejecutan en un procesador remoto, al enviar los datos o comandos adecuados para hacer o ayudar que la acción se realice. Para evitar la duda, cuando un actor facilita una acción por otra forma diferente a realizar la acción, la acción sin embargo es realizada por alguna entidad o combinación de entidades.

Una o más modalidades de la divulgación o elementos de la misma se pueden implementar en la forma de un producto de programa de computador que incluye un medio tangible de almacenamiento grabable legible por computador con código de programa usado en el computador para realizar los pasos del método indicados almacenados en el mismo en una forma no transitoria. Además, una o

más modalidades de la divulgación o elementos de la misma se pueden implementar en la forma de un sistema (o aparato) que incluye una memoria y por lo menos un procesador que se acopla a la memoria y opera para realizar los pasos de método ejemplares. Aún más, en otro aspecto, una o más modalidades de la divulgación o elementos de la misma se pueden implementar en la forma de medios para llevar a cabo uno o más de los pasos de método acá descritos; los medios pueden incluir (i) módulos de hardware especializados, (ii) módulos de software almacenados en una forma no transitoria en un medio tangible de almacenamiento grabable legible por computador (o múltiples de dichos medios) e implementados en un procesador de hardware, o (iii) una combinación de (i) y (ii); cualquiera de (i)-(iii) implementan las técnicas específicas definidas acá. Los medios de transmisión *per se* y las señales sin cuerpo *per se* se definen para estar excluidas de los medios reivindicados.

Una o más modalidades de la divulgación pueden suministrar efectos técnicos beneficiosos sustanciales, que incluyen:

- control del acceso a un sistema de tránsito o similar en una forma tal que al operador de tránsito se le garantiza el pago sin formar una cola de pasajeros que consume tiempo en el punto de acceso al tránsito
- permite que las agencias de tránsito apalanquen los dispositivos propiedad del consumidor y los protocolos y redes de comunicaciones estándar para gestionar el acceso a los ambientes de tránsito seguro
- permite identificar de forma confiable qué personas han ingresado el sistema de tránsito y sus puntos de entrada y/o salida, suministrando de esta forma seguridad mejorada y permitiendo que la agencia aumente el monitoreo y los sistemas de gestión de emergencia sin inversión adicional significativa en los sistemas actuales
- permite que la agencia de tránsito gestione mejor la adopción y el uso de nuevas tecnologías de consumidores al confiar en los estándares de

tecnología desplegados ampliamente en lugar de sistemas propietarios, lo cual reducirá costos y facilita la introducción de nuevos servicios y soluciones

- a diferencia de los sistemas actuales que manejan el acceso a áreas de tránsito seguras, los cuales requieren procesamiento extremadamente rápido y/o toma de decisiones (300 a 500 milisegundos), lo cual a su vez a menudo obliga a la agencia a comprometer los procesos de autenticación y autorización en favor de la velocidad de transacción requerida para acomodar estos ambientes de rendimiento alto, una o más modalidades minimizan dichas limitaciones al mover la iniciación de este proceso lejos de la puerta de tránsito y fuera de los límites de la red de área amplia en el sitio de tránsito
- iniciar el proceso lejos de la puerta permite a la agencia suministrar un mejor patrón de experiencia al identificar si hay una oportunidad de suministrar una alerta o guía temprana al patrón con base en la preferencia o los patrones del consumidor (por ejemplo, probabilidad de tomar un cierto tren que la agencia sabe que está retrasado) o conocimiento de condiciones del sistema (por ejemplo, plataforma llena de gente, escalera averiada, puerta con mal funcionamiento, etc.)
- iniciar el proceso lejos de la puerta también es útil cuando se utilizan las billeteras electrónicas para el pago ya que hay más tiempo disponible para desplegar y utilizar la billetera
- iniciar el proceso lejos de la puerta además es útil cuando se va a emplear procesamiento de tipo de evaluación de riesgo (alertas y controles) (por ejemplo, producto “inControl” de MasterCard), ya que hay más tiempo disponible para dicho procesamiento de tipo de evaluación de riesgo

Estas y otras características y ventajas de la presente divulgación se volverán evidentes a partir de la siguiente descripción detallada de las modalidades ilustrativas de la misma, la cual se debe leer en conexión con las figuras adjuntas.

Breve Descripción de las Figuras

La figura 1 muestra un ejemplo de un sistema y varios componentes del mismo que pueden implementar por lo menos porciones de al menos algunas técnicas de la divulgación;

La figura 2 ilustra una inter-relación ejemplar entre: (i) una red de pago configurada para facilitar las transacciones entre múltiples emisores y múltiples adquirentes, (ii) una pluralidad de usuarios, (iii) una pluralidad de comerciantes, (iv) una pluralidad de adquirentes, y (v) una pluralidad de emisores;

La figura 3 es un diagrama de bloque de un sistema de computador ejemplar útil en una o más modalidades de la divulgación;

La figura 4 es un diagrama de bloque de un teléfono “inteligente” o computador tableta configurado de acuerdo con otro aspecto de la divulgación;

La figura 5 es un diagrama de una estación de trenes con un sistema de acuerdo con un aspecto de la divulgación;

La figura 6 es un diagrama de flujo de un método ejemplar, de acuerdo con un aspecto de la divulgación;

Las figuras 7 y 8 suministran una vista ejemplar detallada de la operación de una red de tarjeta de pago, de acuerdo con un aspecto de la divulgación;

La figura 9 muestra un grupo de procesadores de interfaz de red de pago, tal como se puede utilizar con la red de las figuras 7 y 8;

La figura 10 muestra una disposición de puerto en un procesador de interfaz de red de pago, tal como se puede utilizar con la red de las figuras 7 y 8;

La figura 11 muestra una caja en donde un emisor tiene múltiples procesadores de interfaz de red de pago; y

La figura 12 muestra la lógica de control que se puede implementar por medio de un procesador de una puerta de acceso, de acuerdo con un aspecto de la divulgación.

Descripción Detallada de las Modalidades Preferidas

Una o más modalidades de la divulgación son generalmente aplicables a teléfonos celulares, tabletas de Internet, y otros dispositivos electrónicos móviles con capacidad de “Wi-Fi” y similares. Como se utiliza acá, “Wi-Fi” se define que incluye cualquier producto de red de área local inalámbrica (WLAN) que se basan en los estándares del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) 802.11, sin importar de si están habilitados para utilizar la marca “Wi-Fi” o el logo “CERTIFICADO Wi-Fi”.

Dispositivos de Pago y Redes de Procesamiento de Pago Asociadas

Ahora se debe dirigir la atención a la figura 1, la cual ilustra una modalidad ejemplar de un sistema 100 y varios componentes del mismo que pueden implementar por lo menos porciones de por lo menos algunas técnicas de la divulgación. El sistema 100 puede incluir uno o más tipos diferentes de dispositivos de pago portátiles. Por ejemplo, uno de dichos dispositivos puede ser un dispositivo de contacto tal como una tarjeta 102. La tarjeta 102 puede incluir un chip de circuito integrado (IC) 104 que tiene una porción de procesador 106 y una porción de memoria 108. Una pluralidad de contactos eléctricos 110 se pueden suministrar para propósitos de comunicación. Adicional o en lugar de la tarjeta 102, el sistema 100 también puede diseñarse para trabajar con un dispositivo sin contacto tal como una tarjeta 112. La tarjeta 112 puede incluir un chip IC 114 que tiene una porción de procesador 116 y una porción de memoria 118. Una antena

120 se puede suministrar para comunicación sin contacto, tal como, por ejemplo, utilizando ondas electromagnéticas de radiofrecuencia (RF). Se puede suministrar un oscilador u osciladores, y/o circuitos adecuados adicionales para uno o más de modulación, demodulación, conversión de bajada, y similares. Nótese que las tarjetas 102, 112 son ejemplares de una variedad de dispositivos que se pueden emplear. El sistema *per se* se puede funcionar con otros tipos de dispositivos en lugar de o adicional a tarjetas “inteligentes” o de “chip” 102, 112; por ejemplo, una tarjeta convencional 150 que tiene una banda magnética 152. Adicionalmente, un teléfono celular apropiadamente configurado, asistente digital personal (PDA), tableta, y similares se pueden utilizar para llevar a cabo los pagos sin contacto en algunos casos.

Los IC 104, 114 pueden contener unidades de procesamiento 106, 116 y unidades de memoria 108, 118. Preferiblemente, los IC 104, 114 también pueden incluir uno o más de lógica de control, un temporizador, y puertos de entrada/salida. Dichos elementos son bien conocidos en el arte de IC y no se ilustran de forma separada. Uno o ambos de los IC 104, 114 también pueden incluir un co-procesador, de nuevo, bien conocido y no ilustrado de forma separada. La lógica de control puede suministrar, en conjunto con las unidades de procesamiento 106, 116, el control necesario para manejar las comunicaciones entre la unidad de memoria 108, 118 y los puertos de entrada/salida. El temporizador puede suministrar una señal de referencia de tiempo de las unidades de procesamiento 106, 116 y la lógica de control. El co-procesador podría suministrar la capacidad de realizar cálculos complejos en tiempo real, tal como aquellos requeridos por algoritmos de criptografía.

Las porciones o unidades de memoria 108, 118 pueden incluir diferentes tipos de memoria, tal como memoria volátil y no volátil y memoria de sólo lectura y programable. Las unidades de memoria pueden almacenar datos de tarjeta de transacción tal como, por ejemplo, un número principal de la cuenta del usuario

("PAN") y/o el número de identificación personal ("PIN"). Las porciones o unidades de memoria 108, 118 pueden almacenar el sistema operativo de las tarjetas 102, 112. El sistema operativo carga y ejecuta las aplicaciones y suministra gestión de archivo u otros servicios básicos de tarjeta a las aplicaciones. Un sistema operativo que se puede utilizar es el sistema operativo MULTOS® licenciado por MAOSCO Limited. (MAOSCO Limited, St. Andrews House, The Links, Kelvin Close, Birchwood, Warrington, WA3 7PB, Reino Unido). Alternativamente, se podrían emplear los sistemas operativos basados en JAVA CARD™, basados en tecnología JAVA CARD™ (Licenciada por Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, CA 95054 USA), o sistemas operativos propietarios disponibles de un número de proveedores. Preferiblemente, el sistema operativo se almacena en la memoria de sólo lectura ("ROM") dentro de la porción de memoria 108, 118. En un acercamiento alterno, también se puede utilizar memoria flash u otros tipos de memoria no volátil y/o volátil en las unidades de memoria 108, 118.

Adicional a los servicios básicos suministrados por el sistema operativo, las porciones de memoria 108, 118 también pueden incluir una o más aplicaciones. Actualmente, una posible especificación a la cual se pueden conformar dichas aplicaciones es la especificación de pagos interoperable EMV establecida por EMVCo, LLC (901 Metro Center Boulevard, Mailstop M3-3D, Foster City, California, 94404, USA). Se apreciará que las aplicaciones se pueden configurar en una variedad de diferentes formas.

El experto en la materia también estará familiarizado con las especificaciones MasterCard® PayPass™, disponibles bajo licencia de MasterCard International Incorporated of Purchase, NY, USA (marcas de MasterCard International Incorporated of Purchase, NY, USA).

Como se notó, las tarjetas 102, 112 son ejemplos de una variedad de dispositivos de pago que se pueden emplear. La función principal de los

dispositivos de pago puede no ser el pago, por ejemplo, estos pueden ser teléfonos celulares que implementan técnicas de la divulgación. Dichos dispositivos pueden incluir tarjetas que tienen un factor de forma convencional, tarjetas más pequeñas o más grandes, tarjetas de diferentes formas, llaveros, asistentes digitales personales (PDA), teléfonos celulares adecuadamente configurados, tabletas, o de hecho cualquier dispositivo con las habilidades de implementar técnicas de la divulgación. En algunos casos, las tarjetas, u otros dispositivos de pago, pueden incluir porciones de cuerpo (por ejemplo, capas plástica laminadas de una tarjeta de pago, cubierta o gabinete de una tableta, PDA o teléfono celular, empaque de chip, y similares), memorias 108, 118 asociadas con las porciones de cuerpo, y procesadores 106, 116 asociados con las porciones de cuerpo y acoplados a las memorias. Las memorias 108, 118 pueden contener aplicaciones adecuadas. Los procesadores 106, 116 pueden ser operativos para facilitar la ejecución de uno o más pasos del método. Las aplicaciones pueden ser, por ejemplo, identificadores de aplicación (AID) vinculados a código de software en la forma de firmware más datos en una memoria de tarjeta tal como una memoria de sólo lectura programable borrable eléctricamente (EEPROM).

Un número de diferentes tipos de terminales se pueden emplear con el sistema 100. Dichas terminales incluyen una terminal de contacto 122 configurada para interactuar con el dispositivo tipo contacto 102, una terminal inalámbrica 124 configurada para interactuar con el dispositivo inalámbrico 112, una terminal de banda magnética 125 configurada para interactuar con un dispositivo de banda magnética 150, o una terminal combinada 126. La terminal combinada 126 se diseña para interactuar con cualquier tipo de dispositivo 102, 112, 150. Algunas terminales pueden entrar en contacto con las terminales con lectores sin contacto de conexión. La terminal combinada 126 puede incluir una memoria 128, una porción de procesador 130, un módulo lector 132, y opcionalmente un módulo de

interfaz de artículo tal como un escáner de código de barras 134 y/o un lector de etiqueta de identificación por radiofrecuencia (RFID) 136. Los artículos 128, 132, 134, 136 se pueden acoplar al procesador 130. Nótese que los principios de construcción de la terminal 126 son aplicables a otros tipos de terminales y se describen en detalle para propósitos ilustrativos. El módulo lector 132 se puede, en general, configurar comunicación de contacto con la tarjeta o el dispositivo 102, comunicación sin contacto con la tarjeta o el dispositivo 112, lectura de la banda magnética 152, o una combinación de cualquier dos o más de los anteriores (se pueden suministrar diferentes tipos de lectores para interactuar con diferentes tipos de tarjetas, por ejemplo, con contacto, banda magnética, o sin contacto). Las terminales 122, 124, 125, 126 se pueden conectar a uno o más centros de procesamiento 140, 142, 144 por medio de una red de computador 138. La red 138 puede incluir, por ejemplo, el Internet, o una red propietaria (por ejemplo, una red privada virtual (VPN) tal como se describe con respecto a la figura 2 más adelante). Se puede emplear más de una red para conectar diferentes elementos del sistema. Por ejemplo, una red de área local (LAN) puede conectar una terminal a un servidor local u otro computador en el establecimiento de comercio. Una red de pago puede conectar los adquirentes y los emisores. Detalles adicionales con relación a una forma específica de la red de pago se suministrarán a continuación. Los centros de procesamiento 140, 142, 144 puede incluir, por ejemplo, un computador anfitrión de un emisor de un dispositivo de pago.

Varios diferentes comercios u otros establecimientos, representados por puntos-de-venta 146, 148, se pueden conectar a la red 138. Diferentes tipos de dispositivos de pago portátiles, terminales, u otros elementos o componentes pueden combinar o “mezclar y combinar” una o más características ilustradas en los dispositivos ejemplares de la figura 1.

Los dispositivos de pago portátiles pueden facilitar las transacciones por parte de un usuario con una terminal, tal como 122, 124, 125, 126, de un sistema

tal como el sistema 100. Dicho dispositivo puede incluir un procesador, por ejemplo, las unidades de procesamiento 106, 116 discutidas anteriormente. El dispositivo puede también incluir una memoria, tal como las porciones de memoria 108, 118 discutidas anteriormente, que se acoplan al procesador. Además, el dispositivo puede incluir un módulo de comunicaciones que se acopla al procesador y se configura para interactuar con una terminal tal como una de las terminales 122, 124, 125, 126. El módulo de comunicaciones puede incluir, por ejemplo, los contactos 110 o las antenas 120 junto con los circuitos adecuados (tal como el oscilador u osciladores mencionados anteriormente y los circuitos relacionados) que permite interactuar con los terminales por medio de comunicación con contacto o inalámbrica. El procesador del aparato puede operarse para realizar uno o más pasos de los métodos y técnicas. El procesador puede realizar dichas operaciones por medio de técnicas de hardware, y/o bajo la influencia de instrucciones de programa, tal como una aplicación, almacenada en una de las unidades de memoria.

El dispositivo portátil puede incluir una porción de cuerpo. Por ejemplo, este podría ser un cuerpo plástico laminado (como se discutió anteriormente) en el caso de tarjetas “inteligentes” o de “chip” 102, 112, o el chasis de teléfono y el cuerpo en el caso de un teléfono celular, tableta, o similar.

Se apreciará que las terminales 122, 124, 125, 126 son ejemplos de aparatos de terminal para interactuar con un dispositivo de pago de un propietario. El aparato puede incluir un procesador tal como el procesador 130, una memoria tal como la memoria 128 que se acopla al procesador, y un módulo de comunicaciones tal como 132 que se acopla al procesador y se configura para interactuar con los aparatos portátiles 102, 112, 1420. El procesador 130 se puede operar para comunicarse con los dispositivos de pago portátiles de un usuario por medio del módulo de comunicaciones 132. Los aparatos de terminal pueden funcionar por medio de técnicas de hardware en el procesador 130, o por

instrucciones de programa almacenadas en la memoria 128. Dicha lógica puede opcionalmente suministrarse desde una ubicación central tal como el centro de procesamiento 140 por la red 138. En un aspecto adicional, el escáner de código de barras 134 mencionado anteriormente y/o el lector de etiqueta RFID 136 se pueden suministrar, y se pueden acoplar al procesador, para reunir los datos de atributo, tal como una identificación de producto, de un código UPC o etiqueta RFID en un producto a comprar.

Los dispositivos 102, 112 anteriormente descritos pueden ser tarjetas o dispositivos de contacto que cumplen con ISO 7816 o NFC (Comunicaciones de Campo Cercano) o dispositivos o tarjetas de proximidad que cumplen con ISO 14443. En operación, la tarjeta 112 se puede tocar o golpear en la terminal 124 o 128 (o un lector asociado), el cual luego transmite sin contacto los datos electrónicos al chip de IC de proximidad en la tarjeta 112 u otro dispositivo inalámbrico.

Uno o más de los centros de procesamiento 140, 142, 144 pueden incluir una base de datos tal como la bodega de datos 154.

A menudo se emplea un dispositivo de interfaz dual 1302. El dispositivo 1302 se muestra más grande que los dispositivos 102, 112 por conveniencia de ilustración pero puede tener un factor de forma similar. El dispositivo 1302 incluye un chip IC 1304 que tiene una porción de procesador 1306 y una porción de memoria 1308. Una pluralidad de contactos eléctricos 1310, similares a los contactos 110, se pueden suministrar, así como una antena 1320 similar a la antena 120, junto con un oscilador u osciladores, y/o circuitos adecuados adicionales para uno o más de modulación, demodulación, conversión hacia abajo, y similares, como se describe con relación al dispositivo 112. Se puede suministrar un firmware adecuado para gestionar las dos interfaces disponibles, con la operación de otra forma siendo similar a los dispositivos 102, 112.

También se puede emplear un teléfono celular 1420 configurado de forma adecuada o dispositivo similar (por ejemplo, tableta) en un número de modalidades. El teléfono 1420 se ilustra en forma semi-esquemática en la figura 1, y puede incluir uno o más chips de IC tal como el chip 1440 que incluye una unidad de procesamiento 1460 y una unidad de memoria 1480. La comunicación inalámbrica con una terminal se puede suministrar por medio de la antena 1500 o con una segunda antena 1800 similar a la antena 120 descrita anteriormente (es decir, el teléfono puede tener una segunda antena para la aplicación de pago). Nótese que la antena 1800 se ilustra esquemáticamente, pero podría ser, por ejemplo, una antena en espiral como se usa en una tarjeta “inteligente” típica. Los teléfonos 1420 pueden estar cada uno equipado con una pantalla adecuada 1560. Además, también se puede suministrar una fuente de poder 1620 adecuada. Dichas fuentes de poder pueden incluir, por ejemplo, una batería y los circuitos adecuados. La pantalla y la fuente de poder se pueden interconectar con la porción de procesador. Diferentes tipos de dispositivos de pago portátiles pueden combinar o “mezclar y combinar” una o más características ilustradas en los dispositivos ejemplares de la figura 1. Se puede suministrar un teclado 1680 y un parlante 1740. Varios dispositivos actuales omiten el teclado 1680 y emplean una pantalla táctil. Ver la discusión de la figura 4 más adelante.

La descripción de los dispositivos, elementos, o componentes 102, 104, 106, 108, 110, 112, 114, 116, 118, 120 a lo largo de este documento es igualmente aplicable a los artículos correspondientes en la tarjeta de interfaz dual 1302 y el teléfono celular 1420.

Para completitud, se debe notar que el sistema ilustrado en la figura 1 puede involucrar no sólo transacciones convencionales en comercios de “cemento y ladrillo”, sino que también, transacciones con tarjeta no presentes, tal como transacciones con tarjeta no presentes por Internet o pagos recurrentes con tarjeta no presentes. En algunos casos, se puede capturar una dirección de Protocolo de

Internet (IP) durante las transacciones de tarjeta no presentes por Internet. En transacciones con tarjeta no presentes por internet ejemplares, un individuo utiliza su computador del hogar para comunicarse con un servidor de un establecimiento de comercio electrónico por Internet. El individuo suministra su PAN al servidor del comercio. El comercio utiliza el PAN para iniciar una solicitud de autorización, y al recibir una respuesta de la solicitud de autorización que indica la aprobación, completará la transacción de comercio electrónico. En pagos recurrentes con tarjeta no presentes ejemplares, un individuo suministra su PAN y los datos relacionados a un comercio (por ejemplo, por teléfono o correo postal). El comercio utiliza el PAN para iniciar una solicitud de autorización, y al recibir una respuesta a la solicitud de autorización que indica la aprobación, completará la transacción recurrente.

En algunos casos, puede haber cuentas de tarjeta de pago que no tienen tarjetas físicas u otros dispositivos de pago físicos asociados con las mismas; por ejemplo, un cliente puede contar con un PAN, fecha de vencimiento, y código de seguridad, pero no tiene un dispositivo de pago físico, y utiliza el mismo, por ejemplo, para transacciones con tarjeta no presentes por teléfono o internet. En este sentido, un “tarjetahabiente” debe entender que se refiere a un propietario de cuenta de una cuenta de tarjeta de pago, sin importar si el propietario actualmente tiene una tarjeta de pago física u otro dispositivo de pago físico.

Con referencia a la figura 2, se ilustra una relación ejemplar entre múltiples entidades. Un número de diferentes usuarios (por ejemplo, clientes) 2002, U_1 , $U_2 \dots U_N$, interactúan con un número de diferentes comercios 2004, P_1 , $P_2 \dots P_M$. Los comercios 2004 interactúan con un número de diferentes adquirentes 2006, A_1 , $A_2 \dots A_I$. Los adquirentes 2006 interactúan con un número de diferentes emisores 2010, I_1 , $I_2 \dots I_J$, a través de, por ejemplo, un operador simple 2008 de una red de pago configurado para facilitar transacciones entre múltiples emisores y múltiples adquirentes; por ejemplo, MasterCard International Incorporated,

operador de la red BANKNET® anteriormente mencionada, o Visa International Service Association, operador de la red VISANET® anteriormente mencionada. En general, N, M, I, y J son enteros que pueden ser iguales o no iguales. Nótese también que los elementos 2006, 2010 representan las entidades que actualmente lleva a cabo el procesamiento para los adquirentes y los emisores respectivamente; en algunos casos, estas entidades llevan a cabo su propio procesamiento; en otras entidades, ellos utilizan procesadores de adquirente y procesadores de emisor, respectivamente.

Durante un proceso convencional de autorización de crédito, el tarjetahabiente 2002 paga por la compra y el comercio 2004 envía la transacción al adquirente (banco que adquiere) 2006. El adquirente verifica el número de la tarjeta, el tipo de transacción y la cantidad con el emisor 2010 y reserva esa cantidad del límite de crédito del tarjetahabiente para el comercio. En este punto, la solicitud de autorización y la respuesta se han intercambiado, típicamente en tiempo real. Las transacciones autorizadas se almacenan en “lotes”, los cuales son enviados al adquirente 2006. Durante la posterior compensación y liquidación, el adquirente envía las transacciones de lote a través de la asociación de tarjeta de crédito, la cual debita al emisor 2010 para el pago y acredita el adquirente 2006. Una vez se le ha pagado al adquirente 2006, el adquirente 2006 le paga al comercio 2004.

Los mensajes dentro de una red tal como la red 138 y/o la red 2008, pueden, por lo menos en algunos casos, conformarse al Estándar 8583 de la Organización Internacional para Estandarización, *mensajes originados de tarjeta de transacción Financiera – especificaciones de mensaje de intercambio*, el cual es el estándar ISO para sistemas que intercambian transacciones electrónicas hechas por tarjetahabientes utilizando tarjetas de pago. Se debe notar que el experto en la materia estará familiarizado con los estándares ISO 8583. Sin embargo, de un exceso de precaución, los siguientes documentos se incorporan

acá expresamente por referencia en su totalidad para todos los propósitos (publicado por ISO, Ginebra, Suiza, y disponibles en la página web de ISO):

- ISO 8583 Parte 1: Mensajes, elementos de datos y valores de código (2003)
- ISO 8583 Parte 2: Procedimientos de aplicación y registro para Códigos de Identificación de Institución (IIC) (1998)
- ISO 8583 Parte 3: Procedimientos de mantenimiento para mensajes, elementos de datos y valores de código (2003)
- ISO 8583:1993 (1993)
- ISO 8583:1987 (1987)

Se apreciará que la red 2008 mostrada en la figura 2 es un ejemplo de una red de pago configurada para facilitar las transacciones entre múltiples emisores y múltiples adquirentes, la cual se puede pensar como un sistema “abierto”. En otros casos, se puede utilizar una red de pago configurada para facilitar las transacciones entre múltiples emisores y un adquirente simple. Algunas modalidades de la divulgación se pueden emplear con otros tipos de redes de pago, por ejemplo: redes de pago propietarias o cerradas con sólo un único emisor y adquirente; aplicaciones de etiquetas privadas; capacidades de etiqueta blanca; y similares. Además en este sentido, la figura 2 ilustra un modelo de cuatro partes, como será conocido para el experto en la materia; las cuatro partes son el consumidor 2002, el comercio 2004, el adquirente 2006, y el emisor 2010. Sin embargo, por lo menos algunas modalidades también son de uso con modelos de tres partes, en donde el adquirente y el emisor (y por lo menos en algunos casos, el operador de red, también) son la misma entidad.

Como se utiliza acá, una “red de tarjeta de pago” es una red de comunicaciones que utiliza números de cuenta de tarjeta de pago, tal como los números de cuenta principal (PAN), para autorizar, y para facilitar la

compensación y liquidación de, transacciones de tarjeta de pago – tal como para crédito, débito, valor almacenado y/o cuentas de tarjeta prepago. Las cuentas de tarjeta tienen números de cuenta de tarjeta de pago estandarizados asociados con ellas, lo cual permite el eficiente enrutamiento y liquidación de transacciones; por ejemplo, números de cuenta de estándar ISO tal como números de cuenta que cumplen con ISO/IEC 7812. Las cuentas de tarjeta y/o los números de cuenta pueden o no tener tarjetas físicas u otros dispositivos de pago físicos asociados con ellas. Por ejemplo, en algunos casos, las organizaciones tienen cuentas de tarjeta de compra a las cuales se les asigna un número de cuenta de tarjeta de pago, utilizado para hacer compras para la organización, pero no hay una correspondiente tarjeta física. En otros casos, se emplean números de cuenta “virtuales”; esto también es conocido como mapeo PAN. El proceso de mapeo PAN involucra tomar el Número de Cuenta Principal (PAN) original (el cual puede o no estar asociado con una tarjeta física) y emitir un pseudo-PAN (o número de tarjeta virtual) en su lugar. Las soluciones de mapeo PAN comercialmente disponibles incluyen aquellas disponibles de Orbiscom Ltd., Bloque 1, Blackrock Business Park, Carysfort Avenue, Blackrock, Co. Dublín, Irlanda (ahora parte de MasterCard International Incorporated of Purchase, New York, USA); a modo de ejemplo y no limitación, las técnicas de las Patentes de EE.UU. 6,636,833 y 7,136,835 de Flitcroft y otros, las divulgaciones completas de ambas se incorporan acá expresamente por referencia en su totalidad para todos los propósitos. Vale la pena anotar que en una o más modalidades, los datos asociados con las PANS de uso simple son valiosas si las PANS de uso simple se pueden re-mapear a la cuenta resaltada, el tarjetahabiente, o el domicilio (incluso cuando no se pueden mapear éstas aún son útiles ya que pueden ser un proxy para un tarjetahabiente y aún suministran inteligencia adicional).

Algunas redes de tarjeta de pago conectan múltiples emisores con múltiples adquirentes; otras usan un modelo de tres partes. Algunas redes de tarjeta de

pago utilizan mensajería ISO 8583. Ejemplos no limitantes de redes de tarjeta de pago que conectan múltiples emisores con múltiples adquirentes son la red BANKNET® y la red VISANET®. Una o más modalidades son aplicables a varios otros diferentes tipos de redes de tarjeta de pago también; la red AMERICAN EXPRESS® y la red DISCOVER® son ejemplos no limitantes.

Como se ve en la figura 2, en algunos casos, el propietario o usuario de un teléfono inteligente 400, 1420 o dispositivo similar configurado de acuerdo con una o más modalidades de la divulgación accede a un sitio web o similar (por ejemplo, del operador de red de pago 2008 o un operador de sistema de tránsito) para descargar una aplicación adecuada 421, discutida anteriormente, al teléfono inteligente 400, 1420 o dispositivo similar. Esta característica es opcional. Nótese que la conexión entre el teléfono 1420 y el operador de red de pago 2008 puede ser muy bien indirecta; por ejemplo, el operador de red de pago 2008 o un operador de sistema de tránsito puede suministrar una “copia dorada” de la aplicación 421 a un tercero (por ejemplo, APPLE ITUNES STORE o el ANDROID MARKET de Google) y el teléfono 400, 1420 descarga por la web desde dicho tercero. El enlace mostrado entre el teléfono 400, 1420 y el operador de red de pago 2008 puede ser directo o indirecto; por ejemplo, por medio de una red celular y posiblemente con una o más partes intermediarias.

Aún con referencia a la figura 2, y con referencia también ahora a las figuras 7 y 8, a modo de revisión y provisión de detalle adicional, un consumidor 2002 efectivamente presenta su tarjeta 150 u otro dispositivo de pago (por ejemplo, presenta teléfono “inteligente” adecuadamente configurado o utiliza una billetera electrónica) a la terminal 126 de un comercio 2004. Una tarjeta de banda magnética 150 y la terminal combinada se muestran a modo de ejemplo, pero se pretende representar generalmente cualquier tipo de dispositivo de pago y cualquier tipo de terminal. La presentación efectiva puede suceder directamente (el usuario ingresa a una ubicación de ladrillo y cemento de un comercio 2004) o

virtualmente (el usuario ingresa a un sitio web de un comercio 2004 por medio de un navegador de un computador personal o similar, o llama por el teléfono, y suministra la información de la tarjeta, o envía un correo “caracol” con la información de cuenta de tarjeta de pago a un comercio). La terminal del comercio 126 captura la información de cuenta de tarjeta (al deslizar o comunicación inalámbrica si se presenta directamente; por ingreso manual o lectura de datos si es remoto) y remite la misma al adquirente 2006. La interacción entre el comercio y el tarjetahabiente es fuera del alcance de la red de tarjeta de pago *per se*. La red de tarjeta de pago se involucra en la conexión entre el adquirente 2006 y la red 2008; la línea punteada entre los puntos E y F en las figuras 7 y 8 abarca la red 2008. Nótese generalmente que los puntos A, B, C, E, y F en la figura 7 se conectan a los correspondientes puntos en la figura 8; toda la red y el ambiente asociado no son adecuados para ilustración en una sola hoja.

Más específicamente, el adquirente 2006, en el ejemplo más específico de las figuras 7 y 8, tiene en sus premisas un procesador de interfaz de red de pago (PNIP 2012). El Procesador de Interfaz de MasterCard o MIP es un ejemplo no limitante de un PNIP. En un ejemplo no limitante, el PNIP se implementa en un servidor montado en un estante. Los PNIP típicamente se ubican en los bordes de la red de tarjeta de pago. Por lo menos en algunos casos, la red de tarjeta de pago de la figura 2, es una red distribuida en donde cada adquirente y emisor tiene por lo menos un PNIP en sus premisas. Cada adquirente 2006 tendrá una relación con uno o más comercios 2004 e interactuará con las terminales del comercio 126 por medio del controlador de terminal 2014 (un adquirente también puede actuar como un adquirente para ellos mismos como un comercio). Adicionalmente en este sentido, las locaciones del comercio tendrán terminales donde se deslizan las tarjetas (o donde se están presentes dispositivos con contacto o sin contacto). El adquirente empleará el controlador de terminal 2014 para interactuar con esos terminales. El controlador de terminal 2014 es un bloque lógico que representa

software y/o hardware que permite que la plataforma de procesamiento de adquirente 2015 se comunice con los terminales de los comercios por medio de TCP, marcación, o similares (las interfaces TCP/IP 2016 se muestran en los ejemplos de las figuras). Cada comercio decidirá que adquirente utilizar para aceptar una o más marcas de tarjetas de pago, y el adquirente configurará al comercio con el software adecuado y/o el firmware para los dispositivos de punto de venta del comercio.

El adquirente 2006 presentará transacciones de varios diferentes comercios 2004 al operador de red de tarjeta de pago 2008 por medio de la interfaz PNIP 2012. La conexión entre los comercios 2004 y el adquirente 2006 es típicamente una interfaz TCP/IP 2016. El formato en el que está la transacción cuando se desliza la tarjeta en el comercio 2004 puede diferir del formato en el que está la transacción cuando actualmente se recibe por el operador de red de tarjeta de pago. El adquirente puede convertir la transacción en el formato ISO 8583 o en un formato que es una implementación específica del formato ISO 8583 (por ejemplo, el formato MASTERCARD CIS (especificación de interfaz de cliente). El mensaje de solicitud de autorización puede ser un mensaje de identificador tipo mensaje ISO 8583 (MTI) 0100, por ejemplo, enviado por la interfaz de comunicaciones 2016 entre el comercio 2004 y el adquirente 2006.

Una vez el mensaje 0100 es recibido en el PNIP 2012 del adquirente 2006, se pueden realizar una serie de ediciones en la transacción con respecto al formato, contenido, y/o contexto. Adicionalmente, se puede llevar a cabo filtrado para determinar si el mensaje se relaciona con algo más allá de una solicitud de autorización ordinaria, relacionada como un *servicio mejorado*. Los servicios mejorados se pueden filtrar a nombre de uno o más emisores 2010 y/o el operador de la red 2008 como tal. Se puede suministrar un sistema de parámetro de miembro centralizado (MPS) 2018 para alojar los parámetros utilizados para controlar el procesamiento de las transacciones de autorización de crédito. En una

o más modalidades, los extractos del sistema de parámetro de miembro centralizado 2018 se distribuyen a todos los PNIP del adquirente 2012 y los PNIP del emisor 2024 en la red 2008 en una base diaria para controlar el procesamiento de las transacciones de tarjeta de crédito.

Se debe notar en este punto que un “ICA” y un “BIN” se emplean en BANKNET de modo que un miembro puede realizar la emisión de tarjeta y/o adquirir actividades. Una ICA o Asociación de Tarjeta Interbancaria es una identificación de cuatro a seis dígitos asignada por MasterCard para uso por parte de un miembro para identificar de forma única la actividad por la que el miembro es responsable. Un BIN o Número de Identificación Bancaria es una serie única de números asignados por MasterCard a un miembro principal y utilizada como los primeros seis dígitos de un número de cuenta de tarjeta habiente. Otras redes de tarjeta de pago tienen tipos similares de números, como será evidente para un experto en la materia.

Por lo menos en algunas modalidades, el mismo extracto de parámetro de miembro se envía a todos los PNIP y las transacciones se enrutan utilizando las mismas. Por lo menos en algunas circunstancias, los números de cuenta o rangos de números de cuenta se usan en decidir cómo enrutar. En algunos casos, las transacciones se enrutan a un PNIP emisor con base en donde se “ingresa” en el rango de cuenta. Los emisores envían un mensaje de solicitud de ingreso MTI 0800 con un ID de grupo o el rango de cuenta. El ID de Miembro se saca de la configuración del puerto PNIP 2038 y las transacciones del rango de cuenta luego se enrutan al puerto del cual la solicitud de ingreso se recibe. Un ID de miembro puede estar presente en puertos en múltiples PNIP en el sitio del Emisor – ver la discusión de la figura 10 más adelante.

En una o más modalidades, con base en el rango de cuenta, los parámetros en MPS 2018 (o un extracto local del mismo) determinarán cómo procesar una transacción dada; por ejemplo, código de producto, código de país, código de

moneda, y similares, incluyendo que servicios mejorados (si los hay) se ha inscrito el emisor para un rango de cuenta particular. Esto es decir, los mensajes son interpretados y ciertos campos, incluyendo el rango de cuenta, se examinan; el rango de cuenta está asociado con un cierto emisor y con base en eso, el mensaje se puede tratar de forma diferente. Los mensajes se pueden interpretar, y convertir en un formato de dato interno de modo que se puede obtener acceso a todos los elementos de datos individuales. En una o más modalidades, el número de cuenta se utiliza como una llave para acceder al MPS 2018 (o un extracto local del mismo) y recuperar todos los parámetros que son adecuados para procesar la transacción dada. En un ejemplo no limitante, un analizador de mensaje adecuado 202 (y otros programas en el PNIP 2012) se pueden escribir en un lenguaje de alto nivel adecuado o similares.

En una modalidad ejemplar, el MPS central 2018 crea los extractos una vez al día que se distribuyen fuera a los puntos finales en la red (por ejemplo, los PNIP 2012), como se ve en 2022. Estos extractos incluyen la información pertinente necesaria para que el PNIP procese el mensaje y determine si requiere algún manejo especial. En algunos casos, los mensajes luego se enrutan a un sitio central 2009 para realizar servicios mejorados. Por otro lado, si no se requieren servicios especiales, el mensaje se puede enrutar directamente al PNIP emisor 2024 como se ve en 2026.

Mensajes enrutados directamente al PNIP emisor: En este aspecto, la transacción se enruta directamente al PNIP emisor 2024 con base en el extracto MPS 2022, como se ve en 2026. Cada rango de cuenta tendrá un único punto final de destino identificado en los parámetros (los rangos de cuenta se pueden agrupar y todos los miembros del grupo de rango de cuenta pueden tener un punto final de destino común). La *interfaz de miembro* se refiere a la conexión entre el procesador de adquisidor 2006 y el PNIP Adquisidor 2012. Este término también aplica a la interfaz entre el PINIP Emisor 2024 y el procesador emisor 2010. Las

conexiones entre y a lo largo del PNIP adquisidor 2012 y el PNIP emisor 2014, PNIP adquisidor 2012 y ASP 2050, y ASP 2050 y PNIP emisor 2024 se relacionan como *interfaz de red* en la red de tarjeta de pago como tal. En una o más modalidades, esta puede ser una conexión TCP/IP (como se ve en 2026) con capacidades de enrutamiento personalizadas que incluyen direcciones de grupo. Normalmente, las direcciones TCP/IP se refieren a un punto final simple. Las direcciones de grupo pueden estar dirigidas a un grupo de direcciones, y se enfocan en cualquiera de los computadores (por ejemplo, PNIP) en el grupo que usa una variedad de protocolos. Algunas usan un acercamiento round robin; otras pueden usar un acercamiento de primero en lista donde el mensaje siempre se enruta a un computador dado primero y luego a un segundo computador sólo si el primero no está disponible. El direccionamiento de grupo puede ser útil, por ejemplo, cuando un adquisidor o emisor tiene múltiples PNIP en la misma ubicación para tolerancia de redundancia/falla. También es posible combinar el acercamiento y establecer un round robin, en donde las direcciones dentro del round robin son primeras dirección de grupo de lista, o a la inversa, es posible establecer un primero-en-lista, en donde las direcciones dentro del primero-en-lista son direcciones de grupo round robin. Estas capacidades son útiles en caso de cortes, mantenimiento, y similares.

La figura 9 muestra un ejemplo no limitante con cuatro PNIP 2028-1 a 2028-4. En un acercamiento round robin, un primer mensaje se enruta primero a PNIP 2028-1, un segundo mensaje a PNIP 2028-2, un tercer mensaje a PNIP 2028-3, un cuarto mensaje a PNIP 2028-4, un quinto mensaje a PNIP 2028-1, y así sucesivamente. En un acercamiento de primero en lista, todos los mensajes se enrutan a PNIP 2028-1; si este no está disponible para un mensaje dado, el mensaje se enruta a PNIP 2028-2; si PNIP 2028-2 no está disponible, el mensaje se enruta a PNIP 2028-3; si PNIP 2028-3 no está disponible, el mensaje se enruta a PNIP 2028-4. Cada PNIP 2028-1 a 2028-4 en la figura 8 puede ser una máquina

sola o un grupo de máquinas direccionadas por primero en lista o round robin como se discutió justo antes. En una o más modalidades, la red física 2026 entre las PNIP 2012, 2024, y la red física 2030, 2032 entre las PNIP 2012, 2024 y el sitio central 2009 es una red de Conmutación de Etiqueta de Multiprotocolo privada (MPLS) TCP/IP y no es el Internet. Una vez la dirección de grupo de red del emisor se ha determinado por el PNIP 2012 (o ASP 2050), el mensaje se enruta al emisor PNIP 2024. Una vez el mensaje de autenticación 0100 llega al PNIP emisor 2024, se realizan ediciones adicionales para hacer doble chequeo y asegurar que el mensaje se ha enrutado a la ubicación correcta. Adicionalmente, el ID de miembro se examina, ya que algunos emisores pueden compartir un PNIP simple y es necesario determinar a cuales de los emisores (miembros) que comparten ese PNIP se debe enrutar la transacción en cuestión. Cada uno de los emisores que comparte el PNIP tendrá su propio puerto en el lado del miembro del PNIP; la transacción se enruta al puerto adecuado con base en los parámetros de miembro. Ver la figura 10 donde un PNIP generalizado 2028 tiene un lado de red 2034 y un lado de miembro 2036. El lado de miembro 2036 tiene N puertos 2038-1 a 2038-N a miembros 1 a N. N es utilizado acá como un entero arbitrario generalizado y el valor de N en la figura 10 no es necesariamente el mismo que el de N en conexión con los elementos 2002 en la figura 2, por ejemplo.

Como se ve en la figura 11, en algunos casos, un emisor tiene múltiples dispositivos PNIP 2028 en un sitio único, con una conexión de lado de red 2034, y con múltiples PNIP 2028 todos conectados al mismo sistema anfitrión (cada uno tiene el puerto 1 2038-1 asociado con el mismo miembro (emisor)).

En este punto, el mensaje 0100 se ha entregado al emisor 2010. El emisor 2010 luego lleva a cabo el procesamiento y las decisiones del emisor (por ejemplo, con la plataforma de procesamiento de emisor 2040) con base en las velocidades de transacción, abierto a comprar, protocolos de detección de fraude, etc., y suministra una respuesta de solicitud de autorización adecuada, ISO 8583 MTI

0110. Hay un número de diferentes posibles códigos de respuesta definidos dentro de ISO 8583 y sus implementaciones particulares. Cada transacción está hecha de múltiples elementos de dato; la respuesta del emisor está incluida en el elemento de dato 39. Una vez el mensaje 0110 es recibido en el PNIP emisor 2024 de la plataforma 2040 este se analiza y se edita para formato, contenido, y contexto, incluyendo validación de DE39 para asegurar que este es un valor válido.

Es importante notar que en una o más instancias, en cada punto donde una transacción afecta a un ordenador de la red de tarjetas de pago, ya sea un PNIP adquirente 2012, emisor PNIP 2024, o un equipo de servicios especiales o equipos 2050 en la ubicación central 2009 (véase más adelante), se conserva el contexto de la transacción. Es decir, antes de que el mensaje se envíe al siguiente nodo en la red, una copia se guarda en una cola de gestor de contexto 2042, 2046, 2058, de modo que cuando la respuesta de la transacción MTI 0110 regresa, la solicitud MTI 0100 puede ser igualada con la respuesta, con el fin de saber cómo encaminar la respuesta de vuelta al punto de la ruta anterior. Uno de los elementos guardados en la cola de gestor de contexto es la dirección del remitente del mensaje, de modo que pueda ser utilizado para información de las rutas de regreso. Una vez que la validación del emisor PNIP está completa, incluyendo el formato, contenido y edición de contexto, la transacción se extrae de la cola de gestor de contexto 2046 y la dirección de la ruta de devolución se recupera, y el mensaje de 0110 es enviado de vuelta de donde vino; en este caso, el adquirente PNIP 2012 (o ASP 2050). El adquirente PNIP 2012 luego recibe y analiza el mensaje y retira su solicitud original de su cola de gestor de contexto 2042. Tenga en cuenta que varios adquirentes pueden compartir una PNIP adquirente y por ello es necesario saber qué puerto del PNIP adquirente encamina la respuesta de vuelta (véase la discusión de la Fig. 10). La comprobación del

mensaje con la solicitud original en la cola de gestor de contexto permite que el mensaje se envíe de vuelta al puerto correcto.

Cada PNIP 2012, 2024 normalmente tiene muchos programas diferentes. Estos pueden incluir, por ejemplo, un analizador/editor 2020, 2043; un administrador de archivos de parámetros; un gestor de contexto de transacción; un programa de comunicaciones para miembros; un programa de comunicaciones de la red; y similares. Tenga en cuenta que para reducir el desorden, las figuras 7 y 8 muestran "extracto MPS" 2022, 2044; esto típicamente incluirá el propio extracto y el administrador de archivos de parámetros asociado que gestiona la obtención de los extractos desde MPS 2018. Del mismo modo, para reducir el desorden, las figuras 7 y 8 muestran la "cola de gestor de contexto" 2042, 2046; esto típicamente incluirá la cola en sí y el director asociado que administra el contenido de la cola. En una o más modalidades, también hay un programa de comunicación utilizado para la comunicación entre los otros programas (comunicaciones entre procesos) en el PNIP; esto se omite en las figuras 7 y 8 para evitar el desorden.

Mensajes en caso de Servicios Mejorados: En una o más instancias, una arquitectura especial se utiliza para facilitar la prestación de servicios mejorados (la ASP 2050 en las figuras 7 y 8 es un ejemplo no limitativo). Ejemplos de servicios mejorados incluyen los productos "enControl" de MasterCard que proporcionan control de gastos y/o números de tarjetas virtuales. Otros ejemplos son las recompensas de fidelidad, cancelaciones de pagos recurrentes, y similares. Una o más instancias no despliegan esta lógica compleja hacia el borde de la red. Además, en este sentido, el emisor y adquirente PNIPs 2012, 2024 se conocen por estar en el borde porque residen en las instalaciones del cliente 2006, 2010. Puede haber más de 2000 PNIPs en una red típica. La arquitectura especial que se utiliza en una o más instancias es una arquitectura de tipo de sitio central asociada con la ubicación 2009. En el sitio central 2009, algunos equipos se conocen como procesadores de servicios de autorización o ASPs 2050.

En el adquirente PNIP 2012, cuando se comprueba el archivo de parámetros de miembro para un rango de cuentas, se determina si la transacción requiere servicios mejorados. Si es así, las transacciones se enrutan al sitio central ASPs 2050, que tienen interfaces para todos los sistemas de proveedores de servicio - los ASP no proporcionan necesariamente los mismos servicios (a pesar de que pueden en algunas modalidades), pero pueden mediar entre la red (por ejemplo, Banknet) y los proveedores de servicios reales 2051-1 a través de 2051-N. Un ASP tendrá típicamente conexiones 2053 a un servidor 2052 a través de conexión DB2 u otro tipo de conexión adecuado. Si una transacción se ha de enriquecer con datos adicionales, se hará una llamada a la base de datos a la unidad central 2052 para recuperar la información de base de datos de la unidad central 2054 de modo que se puede insertar en la transacción antes de que la transacción se envíe a los emisores. Las interfaces también se pueden proporcionar a un sistema de gestión de riesgos, un sistema de gestión de toma de decisiones, control, recompensas, y similares. Los proveedores de servicios 2051-1 a través de 2051-N representan generalmente cualquiera de los servicios mejorados, ejemplos no limitativos de los cuales se han dado en este documento.

Una capa de comunicación 2056 se utiliza para comunicarse con los proveedores de servicios en una o más modalidades, un ejemplo no limitativo de una implementación adecuada es la serie IBM MQ. El mensaje 0100 puede ser enviado a los proveedores de servicios, opcionalmente encapsulados dentro de un encabezado de "servicios mejorados" especiales (ES) que envuelve el mensaje con toda la información adicional necesaria para cumplir con el servicio. El proveedor de servicios envía una respuesta. El ASP toma la respuesta y enriquece la transacción 0100 con la respuesta del servicio, y luego envía el paquete completo al emisor PNIP 2024. Algunos servicios mejorados son procesados en los mensajes de solicitud (0100) y otros se procesan en los mensajes de respuesta (0110). Una vez que el mensaje de respuesta se procesa en el ASP, el

mensaje original se retira de la cola de gestor de contexto 2058 en el ASP para determinar el adquirente apropiado PNIP 2012 para enrutar el mensaje de vuelta. A partir de ahí, el adquirente PNIP se comportará igual que en el caso de "mensajes enrutados directamente al emisor PNIP" discutido anteriormente. Algunas modalidades de la arquitectura especial utilizan un bus de servicios empresariales para mediar y facilitar algunos de los servicios 2051. Por ejemplo, el servicio de EN CONTROL se puede acceder a través de una instancia de un bus de servicios empresariales.

Introducción de datos en el almacén de datos: En una o más instancias, cada transacción que fluye a través del emisor PNIP 2012, adquirente PNIP 2024, y/o ASPs 2050 se registra en todos los puntos al escribir registros. Varias veces al día (por ejemplo, seis), un sistema de transferencia de archivos global 2059 mueve los registros de cada nodo y los recoge en un sistema de archivos de soporte 2060 en la unidad central 2052. El registro de archivos se analiza y se recogen en un archivo general diario. El archivo general diario se depura y se modifica para crear un archivo consolidado en la unidad central que luego se lleva en el almacén de datos 2062, donde la manipulación de datos adicionales y la limpieza se llevan a cabo antes de que se almacenen las transacciones. El almacén de datos 2062 se encuentra en un nodo intermedio (ubicación 2009) conectado a los PNIPs de los adquirentes y emisores 2012, 2024. A modo de aclaración, en una o más modalidades, el nodo 2009 está conectado directamente a los PNIPs 2012, 2024 pero el almacén de datos no está conectado directamente a los dispositivos 2012 y 2024; en cambio, los datos fluyen a través de sistemas SF y GT 2059, 2060 y terminan en el almacén de datos. El almacén de datos 2062 debería distinguirse de un almacén de datos 154 que podrían ser mantenidos por un emisor.

Compensación y Liquidación: Una o más instancias emplean un sistema de compensación y liquidación 2074. En compensación, a través de transferencia de

archivos global 2059, los adquirentes remiten los archivos de compensación en un formato de mensaje adecuado (en un ejemplo no limitativo, los formatos de Mensajes de Productos Integrados (IPM)). Los archivos contienen, desde la perspectiva de los adquirentes, lo que creen que deben ser pagados. En una o más instancias, la autorización no mueve ningún dinero; la autorización sólo valida que el titular de la tarjeta es un titular válido reconocido por el banco, que honrará el pago al comerciante por los bienes o servicios. Por ejemplo, en una visita típica a un restaurante, la tarjeta se pasa por el importe del recibo, pero luego se añade una propina. El mensaje de liberación tendrá la cantidad real de alimentos más la propina. En una o más instancias, la compensación no mueve el dinero; simplemente resuelve las cantidades reales. El sistema de solución de hecho inicia el movimiento del dinero. Además, en este sentido, el sistema de solución en realidad le dice a los bancos la cantidad de dinero a mover, pero en realidad no mueve el dinero. Dentro de compensación, incluyen procesos de resolución de conflictos, de cargo, y similares. Durante la compensación, los archivos son enviados desde los adquirentes a la red de tarjetas de pago; la red de tarjetas de pago, con el sistema de compensación y liquidación 2074, a continuación, toma los archivos y los divide y los ordena según el emisor. Los archivos de respuestas se reciben después por cada emisor, y estos archivos de respuesta son divididos nuevamente y se vuelven a clasificar de nuevo a los compradores correctos. Con el tiempo, los datos fluyen en el sistema de liquidación y el dinero se mueve. Por lo tanto, en un nivel alto, la solicitud de autenticación y la respuesta de la solicitud de autenticación son en tiempo real, y la compensación y liquidación son en modo en serie.

A modo de revisión y provisión de detalles adicionales, al menos en algunos casos, de un modo discontinuo, la compensación se inicia a través de un mensaje ISO 8583 MTI 1240 que tiene un valor de 200 de código de función DE24 para una primera presentación. Una vez obtenido este mensaje por parte del adquirente, la

red de tarjetas de pago, con el sistema de compensación y liquidación 2074, llevará a cabo las modificaciones sintácticas, ediciones, ediciones de formato de contenido y ediciones de contexto (típicamente aplicado a cada transacción). Si se pasan esas ediciones, se calcularán el intercambio y las tarifas asociadas con la transacción. Sobre la base de los cálculos, el mensaje también puede ser enriquecido con información adicional antes de pasar al emisor. A continuación se determina el importe de la liquidación. Dentro del ciclo de compensación, las cantidades de dinero que se debe a cada miembro determinado (por ejemplo, emisor o adquirente) se acumulan, y éstas se resumen en un archivo de solución que se remitirá a su debido tiempo.

Aspectos criptográficos: Hay que tener en cuenta los conceptos de *datos en reposo* y *datos en movimiento*. Un ejemplo de datos en reposo son los archivos de registro que en realidad residen en los mismos PNIPS - información de configuración que contiene los números de tarjeta o información de identificación personal (PII). En una o más modalidades, todos los datos sensibles en reposo se cifran antes de ser plasmados en el disco. Los datos de movimiento se refieren a los datos que de hecho se mueven sobre un medio de transmisión (por ejemplo, alambres, cable coaxial, cable de fibra óptica, enlace RF). Todos los datos PCI-sensibles (Consejo de Normas de Seguridad PCI, LLC, Wakefield, MA, Estados Unidos) están cifrados, ya sean plasmados en el disco o enviados a través de una red. Al menos en algunos casos, los enlaces internos dentro de las instalaciones de los adquirentes y emisores no están cifrados ya que se supone que las instalaciones del cliente son instalaciones físicamente seguras que confían en la seguridad física del hardware. Por otra parte, al menos en algunos casos, los enlaces externos (por ejemplo, enlaces 2026, 2030 y 2032) están todos codificados tanto para el tráfico de autorización y las transferencias de archivos a granel.

Una o más modalidades tendrán interfaz o interfaces 2068 para otras marcas de red de procesamiento de tarjeta de pago. Por ejemplo, una red de procesamiento de tarjetas de pago de marca MASTERCARD puede tener interfaces a redes tales como American Express, Visa, JCB, Discover, y similares. Las capas de traducción adecuadas se pueden proporcionar para actuar como intermediarias entre el formato y los formatos utilizados por otras redes, en su caso MASTERCARD (u otro). En una o más modalidades, las interfaces 2068 a otras redes de pago se proporcionan a través de una máquina, que se encuentra en 2009, pero en general análoga a un Emisor PNIP 2024 con capas de mediación agregadas cargadas como es requerido por otros formatos de red de pago. Algunos comerciantes pueden tener sólo una única interfaz para, por ejemplo, la red MASTERCARD - todas las transacciones de ese comerciante pueden ser dirigidas a MASTERCARD, independientemente de la tarjeta que se utilizó - MASTERCARD procesará las transacciones y las encaminará a las redes correspondientes.

Dispositivos informáticos portátiles

Figura 4 es un diagrama en bloque de un dispositivo informático de tableta ejemplar, "netbook" , "Ultrabook" u otros sub-portátiles, ordenador portátil, dispositivo electrónico móvil, teléfono inteligente 400 o similares; algunas modalidades pueden emplear una exhibición de la tarjeta "inteligente" con capacidad biométrica (ejemplos no limitantes incluyen productos disponibles de IDEX ASA, Fornebu, Noruega; productos de NagralD SA - Kudelski Group, La Chaux-de-Fonds, Suiza pueden también ser útiles en algunos casos). La unidad 400 incluye un procesador adecuado; por ejemplo, un microprocesador 402. Un módulo transceptor celular 404 acoplado al procesador 402 incluye una antena y sus circuitos apropiados para enviar y recibir señales de telefonía celular, por ejemplo, 3G o 4G. Un módulo transceptor Wi-Fi 406 acoplado al procesador 402

incluye una antena y circuitos apropiados para permitir que la unidad 400 pueda conectarse a Internet a través de un punto de acceso de red inalámbrica o punto de acceso. El experto en la técnica apreciará que "Wi-Fi" es una marca registrada de la Alianza Wi-Fi y el nombre de marca para los productos que utilizan la familia de estándares IEEE 802.11. Un módulo transceptor Bluetooth 429 acoplado al procesador 402 incluye una antena y circuitos apropiados para permitir que la unidad 400 pueda conectarse a otros dispositivos a través del estándar de tecnología inalámbrica Bluetooth. Un módulo transceptor NFC 431 acoplado al procesador 402 incluye una antena y circuitos apropiados para permitir que la unidad 400 pueda establecer la comunicación por radio a través de comunicaciones de campo cercano.

Una o más modalidades incluyen una aplicación de tránsito 421 en la memoria 412, que cuando es ejecutada hace que el procesador 402 implemente al menos una parte de la funcionalidad descrita en este documento. El sistema operativo 427 orquesta el funcionamiento de la unidad 400. iOS de Apple y Android de Google son ejemplos no limitantes de los sistemas operativos adecuados.

La pantalla táctil 410 acoplada al procesador 402 también es generalmente indicativa de una variedad de dispositivos de entrada/salida (I/O) tales como un teclado, otro tipo de pantalla, un ratón u otro dispositivo señalador, y así sucesivamente, todos los cuales pueden o no puede estar presentes en una o más modalidades. El módulo de audio 418 acoplado al procesador 402 incluye, por ejemplo, un codificador/decodificador de audio (códec), altavoz, conector para auriculares, un micrófono, y sucesivamente. El sistema de gestión de energía 416 puede incluir un cargador de batería, una interfaz a una batería, y sucesivamente. La memoria 412 está acoplada al procesador 402. La memoria 412 puede incluir, por ejemplo, memoria volátil tal como la RAM y la memoria no volátil, tal como ROM, flash, o cualquier medio de almacenamiento grabable legible por un

ordenador tangible que almacena la información de una manera no transitoria. El procesador 402 típicamente también tendrá una memoria en chip.

El escáner de huellas dactilares 437 está acoplado al procesador 402 para fines de autenticación biométrica. Una aplicación de software correspondiente apropiada (no representada por separado) puede residir en la memoria 412 en algunos casos. Muchos teléfonos móviles están equipados con una cámara digital 439, que se muestra acoplada al procesador 402. En algunas modalidades, la cámara 439 se utiliza en conjunción con una aplicación de reconocimiento facial 435 en la memoria 412 para la verificación biométrica. En algunas modalidades, un micrófono en el módulo de audio 418 se utiliza en conjunción con una aplicación de reconocimiento de altavoz 433 en la memoria 412 para la verificación biométrica; un extremo delantero acústico adecuado puede ser proporcionado. Algunas modalidades incluyen una aplicación de cartera 423 como se discute en otra parte en este documento.

Un módulo receptor GPS 499 acoplado al procesador 402 incluye una antena y circuitos apropiados para permitir que el dispositivo 400 pueda calcular su posición al calcular con precisión las señales enviadas por los satélites GPS por encima de la Tierra. El software correspondiente reside opcionalmente en la memoria 412.

La memoria 412 también puede incluir, por ejemplo, un PIN almacenado para la comparación con un PIN introducido a través de la pantalla táctil 410; extrae los rasgos faciales del dueño legítimo del teléfono para la comparación con los rasgos faciales extraídos de una imagen tomada por la cámara 439; la huella digital se obtiene del propietario legítimo del teléfono para la comparación con las características de huellas dactilares obtenidas a partir de un análisis llevado a cabo por el escáner 437; y/o las características de voz son extraídas del propietario legítimo del teléfono para la comparación con las características de voz extraídas de una muestra de voz proporcionada por un micrófono de audio en el

módulo 418. Tenga en cuenta que los elementos en la figura 4 se muestran conectados directamente al procesador 402; sin embargo, una o más estructuras de bus se pueden emplear en una o más modalidades. Además, los elementos que se muestran como implementados en el software se pueden implementar al menos en parte en el hardware para la velocidad, si se desea.

El programa navegador 497 en la memoria 412 descifra el html dado por un servidor como 506 o 510 para la visualización en la pantalla 410 o similares.

Solución de Control de Acceso

Una o más modalidades proporcionan una solución que incorpora Wi-Fi, emparejamiento Bluetooth de dispositivos de entrada a un ambiente de tránsito (u otro acceso controlado), una cartera basada en un dispositivo o basada en la nube, y/o autenticación biométrica para crear una experiencia de rendimiento de fricción baja/alta para el pago de tarifas y/o control de acceso. En una o más modalidades, el sistema reconoce un dispositivo electrónico portátil (por ejemplo, teléfono celular, tableta) al entrar en una zona, examina las características del dispositivo y/o preferencias del usuario, autentica al usuario con soluciones biométricas (reconocimiento de huellas dactilares, reconocimiento de voz, reconocimiento facial, y similares), y ofrece un acceso y/o ficha de aprobación a un punto de control (por ejemplo, un torniquete u otra puerta de salida) antes de que el usuario entre en la puerta con tarifa. La ficha está emparejado con el dispositivo cuando el dispositivo entra dentro del rango del punto de control, y luego se permite a la ficha caducar a la salida del punto de acceso o después de un período de tiempo predeterminado.

Tal como se usa en este documento, comunicaciones inalámbricas de "proximidad" se refiere a las comunicaciones inalámbricas con un alcance máximo de unos diez a veinte centímetros, como la comunicación de campo cercano (NFC); comunicaciones inalámbricas de "corto alcance" se refiere a las

comunicaciones inalámbricas con un alcance máximo de unos cincuenta a cien metros, tales como Bluetooth; y las comunicaciones inalámbricas "rango medio-largo" se refiere a tecnologías de comunicaciones inalámbricas, como Wi-Fi y 3G o 4G y redes celulares LTE.

Algunas modalidades usan una forma alternativa de autenticación, en lugar de los datos biométricos; por ejemplo, la entrada de un número de identificación personal (PIN). En algunos casos, dependiendo de la capacidad del dispositivo y/o los resultados de la autenticación y/o autorización y/o el método de autenticación (por ejemplo, PIN frente al biométrico), el soporte del dispositivo puede ser enviado a un punto de control diferente (por ejemplo, a la puerta estándar de 524 en lugar de la puerta rápida 522, o viceversa, como se discute más adelante).

Son posibles una variedad de diferentes casos de uso con una o más modalidades de la divulgación. Algunos aspectos son aplicables en el caso de un dispositivo 400 con capacidad biométrica de autenticación (por ejemplo, 437 con cualquier software necesario, 439 más 435, 418 más 433, y cualquier parte de hardware implementado correspondientes) y una aplicación de cartera 423, pero sin capacidad de NFC 431. Algunos aspectos son aplicables en el caso de un dispositivo 400 con capacidad de autenticación biométrica, una aplicación de cartera, y con capacidad de NFC 431. Algunos aspectos son aplicables en el caso de un dispositivo 400 sin capacidad de autenticación biométrica, pero con una aplicación de cartera, y con capacidad de NFC 431. Algunos aspectos son aplicables en el caso de un dispositivo 400 con capacidad de autenticación biométrica, pero con una cartera basada en la nube en lugar de una aplicación de cartera, y sin capacidad de NFC 431.

La figura 5 muestra un sistema ejemplar en el contexto de un área de estación de ferrocarril 502, con el entendimiento de que una o más modalidades son aplicables para controlar el acceso a una variedad de diferentes localizaciones, tales como terminales de autobuses, terminales de metro, estadios,

fiestas, pubs, clubes nocturnos, entornos corporativos o educativos de campus, parques temáticos, hoteles, centros comerciales y parques de vacaciones. La zona de la estación 502 incluye al menos un transceptor Wi-Fi 504, así como una puerta de acceso “rápida” 522 usando los aspectos de una o más modalidades de la divulgación. Los componentes opcionales incluyen un servidor local 506 con la base de datos 508; una interfaz de red de pagos 516; y una puerta de acceso estándar 524. Las puertas, 522, 524 están opcionalmente equipadas con barreras 528, 530 para evitar el acceso no autorizado a los trenes alcanzados a través de la región 520. En lugar de barreras 528, 530, técnicas de audio (por ejemplo, zumbador) y o visuales (por ejemplo, técnicas de parpadeo de luz) se podrían utilizar para llamar la atención de alguien que intenta atravesar sin autenticación y/o autorización correspondiente.

En un ejemplo no limitativo, la interfaz 516 puede incluir una interfaz tal como 2016, y elementos relacionados, como se ve en la figura 7 (por ejemplo, conexión TCP/IP entre la LAN 526 y el adquirente con el router apropiado y/u otro hardware).

Los elementos 504, 506, 516, 522, 524 se colocan en la comunicación de datos a través de una red de área local adecuada (LAN) 526, que en general puede ser una red Wi-Fi para el cual el transceptor 504 proporciona un punto de acceso; otra red inalámbrica; y/o una red cableada, tal como una de Ethernet cableada. Opcionalmente, una red de área amplia (WAN) 514 (por ejemplo, Internet) se proporciona a un servidor remoto 510 con la base de datos 512. La interfaz 516 puede proporcionar la conectividad, por ejemplo, a un adquirente 518 de la agencia de transporte u otra entidad que opera el sistema en la figura 5. Véase la discusión de los adquirentes con respecto a las figuras 2 y 7-11.

En general, al entrar en una zona de conexión Wi-Fi en una instalación (por ejemplo, la región en la estación 502 en rango del transceptor 504), el dispositivo 400 del usuario 532 se descubre, y se descubren las capacidades del dispositivo

400 y preferencias del usuario 532. En una o más modalidades, una aplicación en el dispositivo 400 gestiona (en el dispositivo) estas preferencias o inicia una solicitud a un sistema anfitrión 506, 510 que gestiona la base de datos 508, 512 de las preferencias del cliente. En al menos algunos casos, esta base de datos incluye un perfil del cliente mantenido por la agencia (como se hace actualmente para los clientes registrados), con la información adicional que es apropiada para una o más modalidades de la invención; por ejemplo, firmas biométricas almacenadas de los clientes para facilitar la verificación de las preferencias del cliente y/o la gestión de riesgos que especifican una jerarquía de técnicas de verificación. Alternativamente, una transacción "pago por uso" se puede realizar en algunas modalidades, permitiendo que el usuario permanezca en el anonimato hacia la agencia, pero el usuario es conocido por el emisor de la credencial de pago seleccionada. El usuario 532 se autentica al dispositivo 400 a través de una técnica biométrica y/o mediante la introducción de un PIN. Se hace un intento para autorizar el pago. Tenga en cuenta que algunos sistemas de transporte tienen una única tarifa (por ejemplo, el sistema de metro de Nueva York), mientras que otros tienen una tarifa basada en la distancia (por ejemplo, el Sistema de Metro de Washington, D.C.). En este último caso, en algunos casos, la autorización puede ser para una cantidad predeterminada. La inclusión de una capacidad de comunicación similar a la mostrada en la figura 5 en los puntos de salida del sistema permite a la agencia proporcionar una experiencia de baja fricción similar a la salida del sistema. Si la autenticación y la autorización son exitosas, se envía una ficha de autorización (por ejemplo, del servidor local 506) a la puerta 522. El usuario 532 pasa por la puerta 522 (abierta) y es reconocido cuando el dispositivo 400 se empareja con la puerta 522 cuando se acerca (por ejemplo, a través de la asociación Bluetooth como se ve en 534). La ficha se confirma y el usuario continúa a través de la puerta 522 (típicamente sin paradas).

En algunas modalidades, tales como parques temáticos, se emplean fichas con un lapso de tiempo determinado donde al usuario se le carga en función del tiempo que permanencia en el parque - la ficha expira después de la salida y el costo para el día se calcula basándose en el tiempo transcurrido, con capacidad de pre-autorización.

Continuando ahora con respecto a la referencia a una puerta "abierta", la puerta está abierta, si se retiran las barreras 528. En otros casos, las barreras 528 solamente se abren cuando el dispositivo 400 especificado por una ficha dado se acerca estrechamente. Por razones de seguridad, la agencia deseará típicamente una solución que mantenga las puertas y/u otras barreras de algún tipo. Al menos en algunos casos, este tipo de puertas u otras barreras permanecen abiertas hasta que un usuario anticipado no autorizado se identifica dentro de un rango predeterminado (en un ejemplo no limitativo unos 15 pies o 4.6 metros). Por ejemplo, al detectar la presencia de un individuo usando un detector de movimiento 598 o similar, y si ese individuo no puede ser ligado a una ficha, se cierra la puerta. Haciendo referencia al diagrama de flujo 1200 de la figura 12, que comienza en 1202, la puerta rápida 522 puede incluir un procesador para controlar las barreras 528. El procesador, en algunas modalidades, implementa la lógica en la figura 12. Las barreras se mantienen inicialmente en una posición abierta en el paso 1204. El proceso continúa en 1205. En el bloque de decisión 1206, la entrada de detector de movimiento 598 o similares permite determinar si una persona ha sido detectada cerca de la puerta 522. Si no, como por la rama "N", se hace un bucle de nuevo a 1205 y se continúa a la comprobación. Si es así, por la rama "Y", el control lógico se mueve al bloque de decisión 1208, y se determina si la persona detectada está vinculado a una ficha. Por ejemplo, ¿lleva la persona un dispositivo con un identificador que coincide con un identificador de una ficha válido en la puerta 522? Si es así, según la rama "Y", se hace un bucle y se continua a la comprobación. En caso negativo, según la rama "N", se cierra la

barrera en la etapa 1210 y se investiga; se continua en ese estado, como en el paso 1212, hasta que el problema se ha resuelto y se consideré otra vez oportuno el abrir la barrera.

Algunas modalidades tienen la puerta u otra barrera abierta por defecto, y cierran la puerta u otra barrera cuando una persona no autorizada se detecta en el entorno; otras modalidades tienen la puerta u otra barrera cerradas por defecto, y abren la puerta u otra barrera cuando una persona autorizada se acerca, sin que haya ninguna persona no autorizada en las proximidades.

Algunos usuarios son redirigidos a una línea de puerta estándar asociada con la puerta estándar 524 (por ejemplo, cuando la autenticación falla, es autenticado pero no autorizado). Dichos usuarios deberán presentar el pago. El uso de un dispositivo 400 para el cual falla la autenticación puede ser negado por lo menos en algunos casos. Por lo tanto, si se deniega la cuenta seleccionada o de pago por defecto de un usuario (y el usuario no puede seleccionar una que será autorizada), el usuario será redirigido a otra ubicación de puerta donde él o ella puedan presentar un dispositivo de pago alternativo.

Casos de Uso Ejemplares

A continuación se discuten los casos no limitativos de uso ejemplares.

Caso A - Dispositivo con biométrica y cartera (sin NFC): Como se ha señalado, algunos aspectos son aplicables en el caso de un dispositivo 400 con capacidad de autenticación biométrica (por ejemplo, 437 con cualquier software necesario, 439 más 435, 418 más 433, y cualquier porción implementada por hardware correspondiente) y una aplicación de cartera 423, pero sin capacidad de NFC 431. Con referencia ahora al diagrama de flujo 600 de la figura 6, que comienza en 602, en el paso 604, entran en una zona inalámbrica de rango medio-largo (por ejemplo, una zona Wi-Fi, tal como una región de la estación 502 en el rango del transceptor 504). El sistema (transceptor 504 acoplado al servidor

506 a través de LAN 526 y/o al servidor 510 a través de LAN 526 y WAN 514) detecta la presencia de un teléfono 400 que se puede detectar. En algunos casos, esta detección se lleva a cabo aprovechando el mismo tipo de capacidades que emplean dispositivos para identificar que se encuentran en el alcance de una red inalámbrica. Además, en una o más modalidades, el software en el servidor local 506 identifica no sólo que el dispositivo 400 está presente, sino también si el dispositivo tiene una aplicación 421 cargada en el mismo y/o registrada en el sistema (y si no, pregunta al usuario 532 si se desea tal registro). En el bloque de decisión 606, se realiza una determinación en cuanto a si el usuario 532 ha optado por no participar. Si es así, por la rama Y de bloque 606, este paso a través del flujo lógico termina en 622. Si no, procede al bloque de decisión 608 y determina si el usuario 532 ha optado por este. Estos pasos pueden llevarse a cabo a través de la lógica del programa en el servidor 506 y/o el servidor 510, por ejemplo. Si no se optó adentro o afuera, según la rama N de bloques 608, se indicará al usuario 532 configurar su teléfono 400 para ser detectable en el paso 624. Estos pasos se pueden llevar a cabo, por ejemplo, a través de la lógica del programa en el servidor 506 y/o el servidor 510, el envío de un mensaje al teléfono 400 a través del transceptor 504, LAN 526, y, si se emplea el servidor 510, a través de la WAN 514. Si se opta, según la rama Y de bloque 608, o si las prontas 624 provoca una respuesta favorable, como en el paso 610, se despierta la aplicación 421; el Blue Tooth u otro protocolo alerta que el dispositivo se acerca a la puerta (si el BlueTooth empareja los dispositivos o re-establece un vínculo previo). En algunas modalidades, una señal al teléfono 400 despierta la aplicación 421, si está presente. En un enfoque alternativo, que se discute más en otras partes del presente documento, el usuario 532 accede a una página web local en el dispositivo 400, en lugar de o además de usar la aplicación 421. En algunos casos, la página web local toma el lugar de la aplicación. En algunos casos, la página web local permite al usuario descargar la aplicación. La página web local

puede ser dirigida a un navegador del teléfono 400 mediante, por ejemplo, el servidor 506 o el servidor 510.

En el paso 612, si la capacidad biométrica está presente, se autentica al usuario 532 con la misma (algunas modalidades alternativas usan un PIN en lugar de o junto con la autenticación biométrica) y después se autoriza el pago en el paso 614. Más particularmente con respecto a la autenticación, si falla la autenticación, como por la rama N del bloque de decisión 612, este paso a través del flujo lógico termina en 622. Estos pasos se pueden implementar a través de la lógica del programa en el servidor 506 y/o el servidor 510, por ejemplo; tal lógica puede interconectarse con una API o similares para obtener los resultados de la autenticación desde 433, 435, o una aplicación asociada con 437. Además el uso del dispositivo 400 puede, en algunos casos, estar prohibido dentro de la zona 502. En algunos casos, esto puede llevarse a cabo mediante el uso de un identificador del dispositivo 400 en un "ficha negativo" enviado a las puertas 522 y/o 524. Si la autenticación tiene éxito, según la rama Y del bloque de decisión 612, se continúa con el bloque de decisión de autorización 614. Más detalles acerca de un proceso de autenticación ejemplar no limitativo se describen más adelante. Una vez más, esta porción del flujo lógico se puede implementar a través de la lógica del programa en el servidor 506 y/o el servidor 510, por ejemplo.

Si la autorización no tiene éxito, según la rama N del bloque 614, el usuario emplea un procedimiento de entrada estándar 626 (por ejemplo, comprar una tarjeta de tarifa convencional y entrar por la puerta 524). Entonces, este paso a través del flujo lógico termina en 622. El usuario puede verse obligado a utilizar la puerta estándar 524. Estos pasos se pueden implementar, por ejemplo, a través de la lógica del programa en el servidor 506 y/o el servidor 510, al enviar mensajes apropiados al teléfono 400. Opcionalmente, una ficha de "rechazo" se envía a la puerta 528. Por lo menos en algunos casos, se envía un mensaje al teléfono, una

ficha de rechazo se envía a la puerta, y la desaprobación se registra en una aplicación disponible para los agentes de servicios locales para alertar de posibles problemas. Si la autorización es exitosa, según la rama Y del bloque 614, el servidor 506 (o servidor 510) envía una ficha de autorización a la puerta rápida 522, como en el paso 616. A medida que el usuario sale de la puerta 522 en la zona 520, la salida se confirma y la ficha se retira, según el bloque de decisión 618 (rama S) y los pasos 620 (usuario permitido a través de la puerta 522) y 628. Si el usuario no pasa a través de la puerta 522 dentro de un tiempo predeterminado desde que la señal se generó, la ficha se retira en el paso 628 (y se registra un mensaje para que los agentes de servicios locales lo tengan en cuenta). Entonces, este paso a través del flujo lógico termina en 622. Por supuesto, las etapas de la figura 6 se pueden repetir muchas veces diferentes para muchos usuarios y dispositivos diferentes. Una vez más, estas porciones del flujo lógico se pueden implementar a través de la lógica del programa en el servidor 506 y/o el servidor 510, por ejemplo.

En algunos casos, los usuarios tales como el usuario 532 se canalizan (por ejemplo, a través de las barreras 536) para asegurar el flujo secuencial y esto se valida utilizando múltiples sensores antes y después de la puerta 522. Véase, por ejemplo, la discusión, a continuación, de una modalidad con dos transceptores Bluetooth. En algunos casos, un usuario autenticado y autorizado como el usuario 532 se acerca a la puerta 522, donde el dispositivo 400 se empareja con la puerta 522, como se muestra en 534, y el dispositivo 400 se reconoce a corta distancia de la puerta 522. Una vez más, algunas modalidades tienen la puerta u otra barrera abierta por defecto, y cierre la puerta u otra barrera cuando una persona no autorizada se detecta en el entorno; otras modalidades tienen la puerta u otra barrera cerrada por defecto, y abren la puerta u otra barrera cuando una persona autorizada se acerca, sin que haya ninguna persona no autorizada en las proximidades. Cuando el acceso a la región 520 por la puerta 522 es apropiado

para el usuario 532, en algunos casos, una luz verde se puede mantener o algún otro indicador de flujo abierto se puede emplear.

En algunos casos, si un usuario entra en las cercanías (véase la discusión del detector de movimiento 598 y la Fig. 12) de la puerta rápida 522, pero no hay una ficha de aprobación vigente para ese usuario en particular (por ejemplo, el usuario fallo en la autenticación o autorización), la barrera 528 es habilitada y / o un asistente recibe una alerta, o alguna otra indicación podrá ser, por ejemplo, el encendido de la luz en rojo y/o el sonido de la alarma. Esto puede llevarse a cabo a través de instrucciones enviadas a la puerta rápida 522 por el servidor 506 y/o el servidor 510, o por la capacidad de procesamiento local en la puerta 522, o por alguna combinación de los mismos.

A continuación se proporcionan más detalles con respecto a un proceso de autorización ejemplar. Sin embargo, vale la pena señalar primero que hasta ahora los intentos de utilizar dispositivos de pago, tales como tarjetas de pago, teléfonos celulares configurados apropiadamente, y similares para aplicaciones de transporte o similares generalmente no se han implementado con una solicitud de autorización en tiempo real y una respuesta de autorización de solicitud a y desde el dispositivo de pago desencadenada por la presentación del dispositivo en el torniquete o de otra puerta de salida. Esto es porque el tiempo consumido en tal solicitud de autorización y la respuesta de la autorización de solicitud hacia y desde el dispositivo de pago generalmente se ha considerado intolerablemente largo para aplicaciones de tránsito o aplicaciones similares. Véase, por ejemplo, la Patente de Estados Unidos No. 7.828.204 y la Publicación de Patente de Estados Unidos No. 2008-0033880 (ahora patente de EE.UU. 8.584.936). La patente de Estados Unidos No. 7.828.204 y la Publicación de Patente de Estados Unidos No. 2008-0033880 (ahora patente de EE.UU. 8.584.936) se incorporan expresamente por referencia en el presente documento en su totalidad para todos los propósitos.

Ventajosamente, en una o más modalidades, ya que el teléfono 400 de usuario 532 se detecta a la entrada de la zona 502, si es necesario, hay tiempo para llevar a cabo una solicitud de autorización y una respuesta de autorización de solicitud en tiempo real hacia y desde el dispositivo emisor del pago, a través de elementos 516, 518, antes de que el usuario 532 se acerca a la puerta 522. En algunos casos, la solicitud de autorización es un mensaje de solicitud de autorización ISO 8583/0100 y la respuesta de solicitud de autorización es un mensaje de respuesta de autorización ISO8583/0110.

En una o más modalidades, el bloque de decisión de autorización 614 incluye los siguientes sub-pasos:

- Determinar si el usuario 532 es un cliente registrado de la vía férrea u otra autoridad. Por ejemplo, un identificador permanente de teléfono 400 y/o aplicación 421 y/o 423 pueden ser almacenados en la base de datos 508 y/o base de datos 512 en relación con otros datos relacionados con el usuario 532. La lógica en el servidor 506 y/o el servidor 510 obtiene el identificador a través del transceptor 504, LAN 526 (y WAN 514 en el caso de servidor 510) y hace una consulta apropiada a la base de datos correspondiente. Además, en este sentido, si los dispositivos 400 son aparatos de telefonía celular (es decir, teléfonos y/o tabletas que se pueden conectar a una red celular) entonces la Identidad Internacional de Equipo Móvil (IMEI) es un ejemplo no limitante de un identificador permanente adecuado para identificar un determinado dispositivo. Tenga en cuenta que los dispositivos que solo usan Wi-Fi normalmente no tienen un número IMEI. Como alternativa al IMEI, o para dispositivos que no tienen una IMEI, un único ID de software (o prácticamente único, es decir, muy poco probable que sea duplicado), tal como un UUID (Identificador único universal,) se puede utilizar para identificar la aplicación 421 y/o 423.

- Si se ha registrado el usuario 532, puede haber opcionalmente una preferencia almacenada con respecto a qué modo de pago a utilizar. Por ejemplo, el usuario 532 puede tener una cuenta con el ferrocarril u otra autoridad establecida en el servidor 506 y/o servidor 510. En algunos casos, este modo se utiliza como valor predeterminado; en otros casos, se solicita al usuario confirmar el modo por defecto que se debe utilizar. El usuario puede confirmar o podría sugerir otro modo de pago para ser utilizado con el dispositivo 400, o puede indicar que se desea utilizar una puerta convencional 524, en cuyo caso esto se reconoce y el flujo lógico procede a 622.
- Si la preferencia almacenada se utiliza por defecto o por la confirmación del usuario, o si otro modo compatible con el proceso 600 fue elegido por el usuario, se hace una determinación con respecto a los derechos y/o productos del usuario (pase, pre-financiado, y similares) y la autorización es llevada a cabo. Por ejemplo, la base de datos 508 y/o base de datos 512 se comprueban para determinar si el usuario tiene un pase ilimitado o una cuenta pre-financiada. En el primer caso, si éste no está vencido, el usuario está autorizado. En el último caso, un cierto número de viajes o un cierto valor monetario puede ser almacenado en el servidor 506 y/o el servidor 510. Se hace una comprobación de si hay un viaje restante o suficiente valor monetario almacenado para permitir el viaje actual; si es así, el usuario está autorizado. Estos tipos de procesos generalmente no requieren una solicitud de autorización y una respuesta de autorización de solicitud en tiempo real hacia y desde el dispositivo de emisión de pago. Sin embargo, es concebible que el usuario podría tener como valor predeterminado, o podría seleccionar como alternativa, un enfoque de "pago por uso" donde una cuenta de tarjeta de pago asociada a la cartera 423 o una cartera basada en la nube puede ser empleada. Si es así, una

solicitud de autorización y una respuesta de autorización de solicitud en tiempo real hacia y desde el emisor correspondiente se llevan a cabo en este punto; si tiene éxito, el usuario está autorizado.

- En el caso de la autorización, el servidor 506 y/o el servidor 510 genera una aprobación dla ficha y envía la misma a la puerta 522.
- Si la autorización con un modo de pago falla, opcionalmente, busca una fuente registrada secundaria y vuelve a autorizar.
- Si todas las fuentes de pago son declinadas (o si las primera fuente de pago se declina y el paso anterior no es implementado), se alerta al usuario 532 y se envía una ficha de declinado a la puerta 522; por ejemplo, utilizando el ID de dispositivo o el ID residente en la aplicación del dispositivo 421 (si está presente). Preguntar al usuario 532 para proceder a la puerta 524 con un dispositivo de pago alternativo. En algunos casos, se envía una ficha de declinación al dispositivo 400 para advertir al usuario 532 de un problema, o utilizar el aspecto dla ficha de declinación para las personas que representen un riesgo para la seguridad.
- Si el usuario 532 no está registrado, se indicará al usuario que seleccione un modo de pago de la cartera 423 o una cartera basada en la nube 595. Se inicia una solicitud de autorización y una respuesta de solicitud de autorización en tiempo real desde y hacia el emisor correspondiente; si tiene éxito, el usuario está autorizado. Tal como se usa en este documento, una cartera basada en la nube (por ejemplo, sistema de pago móvil Google Wallet de Google Inc., Mountain View, CA, EE.UU. o plataforma digital MasterPass™ de MasterCard International Incorporated, Purchase, Nueva York, EE.UU.) es una donde los datos de las tarjetas de pago se almacenan en servidores seguros basados en nube, en lugar de un área de almacenamiento seguro en el teléfono u otro dispositivo móvil. La cartera basado en la nube 595 se puede acceder en una variedad de formas; por

ejemplo, conexión de red de área amplia (WAN) 514 (por ejemplo, Internet); una conexión 3G o 4G u otra conexión móvil desde el dispositivo 400, o similares.

En algunos casos, en otro aspecto, como parte del Caso A, solo se aceptan los usuarios registrados con una cuenta prepago en el servidor 506 y/o el servidor 510, y periódicamente recargan dicha cuenta prepago.

Caso B - Dispositivo con biométricas, NFC y cartera: Como se ha señalado, algunos aspectos son aplicables en el caso de un dispositivo 400 con capacidad de autenticación biométrica, aplicación de monedero, y con capacidad de NFC 431. En tales casos, los pasos 602 a 614, 624 y 626 pueden seguir las indicaciones anteriores. Si el usuario de la cuenta 532 registrado ha sido declinado y la aplicación o cartera del usuario de 532 no da acceso al usuario 532 a una alternativa, el usuario 532 puede, en algunos casos, iniciar una transacción similar a MPOS (MPO = punto de venta móvil) con un dispositivo de pago diferente (por ejemplo, una tarjeta sin contacto), mientras se dirige a la zona de la puerta (en algunos casos, a través de la capacidad de NFC) - este proceso permite la generación de una aprobación dla ficha y el acceso a la puerta rápida 522. De lo contrario, el organismo puede decidir si quieren correr el riesgo de permitir que el usuario pase a través de la puerta rápida y sin certeza de pago. Si el usuario se ha autenticado con éxito con un sistema biométrico, pero no se ha aprobado la capacidad de pago a través de la cartera o el perfil registrado del usuario, el usuario, en algunos casos, es dirigido a agregar valor prepagado, aprovechando así la instalación de la puerta rápida o las otras puertas a través de NFC. El NFC ofrece la capacidad de "emparejamiento aprovechado". Por lo tanto, en algunos casos, un teléfono de emparejamiento aprovechado proporciona una modalidad alternativa donde un lector físico está espaciado lejos de la puerta y un emparejamiento aprovechado se inicia utilizando NFC. Dicho de otra manera, cuando la etapa 614 da como resultado una declinación, el usuario puede, por

ejemplo, (i) cambiar su dispositivo de pago por defecto en su cartera, o puede (ii) recurrir a su tarjeta de red inalámbrica (asociado con una cuenta de tarjeta de pago válida) en un teléfono con NFC y así iniciar un nuevo proceso de autorización con la cuenta correspondiente. En el enfoque (i), al entrar en la estación, se reconoce a una persona registrada, se comprueba que la cuenta predeterminada sigue siendo válida, y se asesora a la persona cuando no lo es. El sistema informa a la persona para actualizar el dispositivo de pago por defecto en su cartera, y para informar al sistema cuando se completa (se podría decir a la persona que escriba "sí" cuando se realiza la actualización (o utilizar el correo electrónico, la notificación de inserción, u otra técnica)). Entonces, el sistema vuelve a intentar la autorización con la nueva información de la cuenta. Opción (i) no requiere necesariamente la capacidad de NFC; por ejemplo, el usuario puede iniciar sesión en el sitio web de la cartera y actualizar la fecha de caducidad o cambiar la tarjeta por defecto o añadir una nueva tarjeta y hacer que la tarjeta sea la opción predeterminada. La opción (ii) implica NFC o capacidad similar en el teléfono u otro dispositivo de manera que la nueva tarjeta pueda ser aprovechada.

Caso C - Dispositivo con NFC y cartera (no biométrica): Como se ha señalado, algunos aspectos son aplicables en el caso de un dispositivo 400 sin capacidad de autenticación biométrica, pero con una aplicación de cartera, y con capacidad de NFC 431. En tales casos, el proceso puede llevarse a cabo de la misma manera como se muestra en la figura 6 y descrito anteriormente, excepto que el paso de autenticación 612 se puede llevar a cabo mediante la introducción de un PIN o similar (o en otro aspecto, la autenticación biométrica basada en la nube externa 593 puede ser empleada - la autenticación biométrica basada en la nube 593 se puede acceder en una variedad de formas, por ejemplo, red de área amplia (WAN) 514 (por ejemplo, Internet); una conexión 3G o 4G u otra conexión celular desde el dispositivo 400, o similar. En algunos casos, se causa que el usuario use el carril normal 524, pero que use una ficha en la puerta estándar 524 y que pueda tener la

ventaja de la autorización completa. En este aspecto, la agencia no puede querer enviar a alguien a la puerta rápida 522 sin la seguridad de los datos biométricos. Si alguien está potencialmente haciendo algo fraudulento, algún nivel de control es deseable - en algunos casos, el requerimiento de presionar en la puerta 524 señala al usuario que hay un mayor grado de escrutinio (actuando de este modo como un elemento disuasorio para alguien con intención ilícita).

Caso D - Dispositivo con cartera biométrica basada en la nube (sin NFC): En algunos casos, es deseable dar cabida a una persona que tiene el dispositivo y el monedero para el pago, pero no tiene ningún deseo de ser registrado en el sistema de la agencia - por lo tanto, se puede permitir una transacción de pago por uso. Como se ha señalado, algunos aspectos son aplicables en el caso de un dispositivo 400 con capacidad de autenticación biométrica, pero con una cartera basada en la nube en lugar de una aplicación de cartera, y sin capacidad de NFC 431. En tales casos, el procesamiento puede llevarse a cabo de la misma manera como se muestra en la figura 6 y como se ha descrito anteriormente, excepto que en la determinación de las opciones de pago disponibles, la comunicación es con una cartera basada en la nube 595 (por ejemplo, a través de WAN 514) en lugar de aplicación de cartera 423. Vale la pena señalar que para algunos clientes, la agencia puede desear la flexibilidad de tomar algún riesgo en función de la situación (tipo de declinación, perfil de usuario, etc.).

Solución de Control de Acceso - Comentarios adicionales

Por lo tanto, una o más modalidades proporcionan una o más características biométricas emparejadas con la entrega de fichas de aprobación entregados a través de Wi-Fi o de otra red de comunicaciones adecuada (s) y reconocida y actuada sobre el uso de Bluetooth u otro protocolo adecuado para la comunicación de alta velocidad de rango medio-corto. En una o más modalidades, el Wi-Fi es utilizado para entregar fichas a los dispositivos 400 mientras que el

LAN 526 es utilizado para entregar fichas a la puerta rápida 522 y/o la puerta estándar 524. Por otra parte, una o más modalidades permiten el rendimiento de baja fricción de alta seguridad, el aprovechamiento de una combinación de protocolos de comunicaciones y las tecnologías de autorización y/o de autenticación.

Adicionalmente, una o más modalidades permiten un rendimiento rápido en un tránsito o entorno similar con una experiencia de usuario de baja fricción. Una o más modalidades emplean un dispositivo de mano detectable (por ejemplo, teléfonos inteligentes) 400 con capacidad biométrica. Un usuario 532 con un dispositivo de este tipo entra en un entorno de tránsito 502 o similares (las modalidades de la divulgación, como se señaló, no se limitan a aplicaciones de tránsito; otras aplicaciones ejemplares no limitativas se discuten en otra parte en este documento). El usuario 532 entra al entorno 502 y su teléfono 400 (o dispositivo similar) se descubre. En algunas modalidades, esto causa que una aplicación en el teléfono 421 despierte. El usuario 532 se autentifica a sí mismo al dispositivo mediante un sistema biométrico (o PIN). En un ejemplo no limitativo, este proceso de detección y autenticación puede ocurrir mientras el usuario se encuentra aproximadamente a cien yardas (aproximadamente noventa y un metros) de la puerta 522. De este modo, el dispositivo 400 del usuario 532 ha sido reconocido y el usuario 532 ha sido autenticado con el dispositivo 400. En algunos casos, se hace entonces una investigación para determinar si el usuario 532 se ha registrado en algún tipo de producto de tránsito. Por ejemplo, ¿el usuario 532 tiene un pase mensual o una cuenta de pre-financiado con el suficiente valor almacenado para permitir al usuario 532 el acceso a los trenes? Si es así, ¿es el pase mensual o la cuenta pre-financiada válida? Tenga en cuenta que esta consulta se puede hacer, por ejemplo, a la base de datos 508 de servidor local 506 o a la base de datos 512 del servidor remoto 510.

Si el pase mensual o la cuenta pre-financiada es válida y se sabe a dónde el usuario 532 está viajando (por ejemplo, en base a los puntos finales del pase mensual en un escenario de tren de cercanías donde el pasajero compra un pase mensual entre dos ubicaciones fijas), se envía una ficha (por ejemplo, desde el servidor 506) a la puerta rápida 522. La ficha indica a la puerta rápida 522 que el usuario 532 se acerca, que él o ella ha sido autenticada, que su producto es válido, y que, cuando él o ella se acerca, la puerta 522 debe dejar que él o ella pase a través. Si, durante la autenticación, se determina que el usuario 532 tiene varios productos de pases de tránsito y no se sabe cuál él o ella va a utilizar, puede haber un paso intermedio en donde se hace una pregunta al usuario 532 para determinar qué producto utilizar.

Cuando el usuario 532 se aproxima a la puerta actual 522, la comunicación Bluetooth o similar se lleva a cabo entre el dispositivo 400 y la puerta 522. Típicamente, un emparejamiento de Bluetooth entre el dispositivo 400 y la puerta 522 se produce cuando el usuario 532 se aproxima a la puerta 522, que, en efecto, aconseja a la puerta 522 que el dispositivo 400 se acerca. En algunos casos, como el usuario 532 se acerca a la puerta 522, la puerta 522 detecta el dispositivo 400 a través de Bluetooth, digamos, a unos diez pies (unos 3 metros) de distancia. Una ficha de entrada para el usuario 532 ya ha sido enviado a la puerta 522 ya que el usuario 532 ya ha sido autenticado y autorizado. En algunos casos, una luz verde que se encuentra en la puerta 522 a permite al usuario 532 caminar a través de ésta sin obstáculos y abordar el tren deseado, en la región 520. Si el usuario 532 no pasa a través de la puerta 522 en un periodo de tiempo predeterminado, la señal caduca. Puramente a modo de ejemplo y no de limitación, en algunas modalidades, la expiración es una cuestión de horas. Sin embargo, es de destacar que la expiración es típicamente variable en función de la instalación. Por ejemplo, en la Terminal Central de Nueva York, el proceso puede ocurrir antes de que el usuario salga de la zona donde hay restaurantes y lugares

de compras. Por otra parte, en algunas modalidades, el usuario se aproxima a la zona de la puerta y ve que él o ella ha perdido el último tren antes de pasar por la puerta rápida 522. El usuario puede entonces optar por salir de la instalación - si él o ella salen del campo de la conexión Wi-Fi y se ha reconocido que se han marchado, en tales casos la ficha expira.

Algunas modalidades emparejan el dispositivo 400 con dos receptores Bluetooth 597, 599 - uno en cada lado de la puerta 522 - para asegurarse de que el usuario 532 ha atravesado. Esto sirve para cerrar la transacción - verificar que el usuario 532 ha tomado el servicio que él o ella ha pagado. En este aspecto, el receptor 599 está situado de tal manera que el usuario sólo entra en rango después de que él o ella pasa a través de la barrera 528 y entra en la zona de tren 520. Algunas modalidades tienen múltiples opciones de pago: abono mensual, transacción de una sola vez, o cartera 423 integrada con el teléfono 400 (por ejemplo, servicio de monedero digital MASTERPASS disponible de MasterCard International Incorporated, Purchase, Nueva York, EE.UU., billetera móvil ISIS disponible de JVL Ventures, LLC, New York, NY, EE.UU., o Google Wallet disponible de Google Inc., Mountain View, CA, EE.UU.). Con respecto a una transacción de una sola vez, un usuario 532 puede estar caminando en la estación 502 por primera vez, no tiene un pase, y desea montar los trenes.

Como se ha indicado, algunas modalidades utilizan barreras 536 o similares para físicamente canalizar a los usuarios. Por ejemplo, las barreras 536 pueden ser usadas en conjunción con la señalización adecuada o similar para asegurar que las personas que no están autenticados y autorizadas a usar la puerta rápida 522 no se acerquen a la puerta rápida 522, sino más bien utilicen la puerta convencional 524. Los usuarios autenticados y autorizados se dirigen adecuadamente de modo que hay espacio suficiente para establecer la vinculación Bluetooth.

El dispositivo 400 puede ser descubierto a la entrada a la zona 502 utilizando una variedad de técnicas. Los teléfonos celulares suelen tener una configuración que permite al usuario decidir si su teléfono puede ser detectado a las redes; cuando se selecciona el dispositivo transmite su ubicación para que una red Wi-Fi sepa que está presente. El módulo receptor GPS 499 podría ser utilizado en algunas modalidades alternativas.

En una o más modalidades, la ficha de aprobación antes mencionada es un certificado de aprobación previa digital que indica que el usuario 532, en virtud de la autenticación y la autorización, en asociación con el dispositivo 400, se dispone a pasar a través de la puerta 522. En algunas modalidades, el elemento está cifrado. La ficha puede identificar el teléfono utilizando, por ejemplo, el IMEI, como se discutió anteriormente, o una única (o prácticamente única, es decir, muy poco probable que sea duplicada) ID de software tal como un UUID para identificar la aplicación 421 y/o 423, como también se discutió anteriormente. Otros identificadores de teléfono y/o software podrían utilizarse en otros casos, como la Identidad Internacional del Abonado a un Móvil (IMSI), o la Identidad del Abonado Móvil Temporal (TMSI), por ejemplo, sin perjuicio de las pautas de uso aplicables para la misma. De este modo, en una o más modalidades la ficha de aprobación declara cómo una persona fue autenticada (por ejemplo, para la gestión de riesgos y/o funciones de control), para que él o ella se autenticó, y enlaza a la persona 532 al dispositivo 400.

En el caso de uso de tránsito, también existe la posibilidad de una persona que viaja con su familia; es decir, un caso de uso con más de un viajero. Algunas modalidades enlazan una o más personas a uno o más teléfonos pagados todos en la misma cuenta. Es decir, una única cuenta de tránsito en el extremo posterior puede estar vinculada a varios dispositivos (por ejemplo, teléfonos, tabletas, etc.) vinculados a dicha cuenta. La cuenta podría ser financiada por múltiples dispositivos de pago. En algunos casos, si un usuario está viajando con otros y

paga por ellos, dos opciones ejemplares están disponibles. En una opción, si todos los viajeros tienen un dispositivo inteligente, los dispositivos inteligentes de los demás viajeros se combinan con el dispositivo principal (a través de Bluetooth) y los dispositivos inteligentes adicionales se les permiten ser "enlaces" adicionales en una cadena que incluye al usuario primario. Tenga en cuenta que esta opción potencialmente impacta la seguridad en una o más modalidades; por ejemplo, si la agencia solo eligiera permitir únicamente a los clientes autenticados biométricamente en el sistema de puerta rápida. En otra opción, permiten a los viajeros adicionales pagar por adelantado en la cuenta del usuario principal con el sistema descrito en el presente documento. El usuario principal identifica, a través de la aplicación para dispositivo 421 que él o ella está viajando con los demás. Entonces, el número apropiado de fichas se envían a la puerta alternativa (rápido) 522 y el número apropiado de aberturas de puerta secuenciales se admiten.

En algunos casos, la autoridad de tránsito u otra entidad que opera el ferrocarril u otra área de acceso limitado es habilitada por cartera (por ejemplo, una cartera específica de autoridad de tránsito, donde una o más tarjetas de pago están registradas con la autoridad de tránsito, en contraposición a una tercera cartera como Google Wallet). En una o más modalidades, el usuario 532 entra en la estación 502 y se conecta para indicar su presencia. En algunas modalidades, el usuario pre-matricula con la autoridad de tránsito; en otras modalidades, no se requiere pre-inscripción; en aún otras modalidades, ambos casos son posibles. En el caso de un usuario que no se ha registrado previamente, una o más modalidades están abiertas a cualquier persona con un teléfono inteligente detectable que puede comunicarse con los sistemas de autoridad de tránsito a través del transceptor Wi-Fi 504 y con la puerta rápida 522 a través de Bluetooth o similares. Así, al menos algunas modalidades son adecuadas para "pago por uso" de tránsito sin necesidad de registrarse ante la autoridad de tránsito u organismo similar.

Una o más modalidades emplean una aplicación específica de tránsito 421 o una página web local visible en un navegador de dispositivo 400 y servidas desde, por ejemplo, el servidor de aplicaciones 506. La aplicación 421 o la página web local 532 consulta al usuario si él o ella desea el acceso a trenes en 520 y si es así, cómo él o ella le gustaría pagar (por ejemplo, él o ella desea pagar por una tarifa de una sola vez o usar su pase mensual). Si el usuario tiene un pase mensual, el pago podrá ser efectuado mediante la comprobación del pase en el servidor local 506 o servidor remoto 510; si ésta misma es ilimitada, se limita a comprobar que sea válida; si una cierta cantidad de valor se almacena o un determinado número de viajes se han pagado por adelantado, el mismo se puede disminuir en el servidor 506 o 510.

Por otro lado, si el usuario no tiene un pase o cuenta ya establecidos, o los tiene pero sin embargo desea un enfoque de una sola vez, la verificación está ligada a una aplicación de cartera 423 o una cartera basada en la nube. Por ejemplo, la aplicación de cartera 423 o cartera basada en la nube suministra el número de tarjeta y fecha de expiración del usuario para una determinada tarjeta de pago en la cartera; el servidor local 506 formatea una solicitud de autorización al adquirente de la autoridad de tránsito a través de la interfaz 516, como se ve en 518. Debido a que esto se produce poco después de que el usuario 532 entra en la estación 502, hay tiempo para llevar a cabo una solicitud de autorización/respuesta de autorización plena para y desde el emisor de la cuenta de tarjeta de pago particular que se use, a diferencia del caso del acercamiento del usuario de su tarjeta u otro dispositivo de pago en una puerta convencional 524, este es el primer aviso del sistema que tiene el usuario.

Como se ha señalado, en una o más modalidades, el sistema se comunica con el dispositivo 400 a través de la aplicación 423 o mediante la carga de una página web local en un navegador del dispositivo 400 (por lo general no a través de la banda ancha inalámbrica, sino a través de una conexión Wi-Fi con el

transceptor 504). En algunos casos, al usuario 532 se le puede solicitar que descargue la aplicación 421 si no está presente. En algunas modalidades, la conexión Wi-Fi con el transceptor 504 resulta en que la página local sea la página por defecto para cargar cuando el navegador del teléfono 400 se abre dentro del entorno 502. De este modo, en una o más modalidades, algún acto afirmativo por parte del usuario 532 se requiere - él o ella debe descargar la aplicación 421, como se muestra y se describe en relación con la figura 2 y/o acceder a la web a través del transceptor Wi-Fi local 504 y ver la página local que "aparece" como resultado.

En una o más modalidades, un usuario que ha “optado por entrar” y/o quien ha establecido su teléfono u otro dispositivo para que pueda ser descubierto por una red de Wi-Fi puede ser alertado para iniciar una sesión – recibe un mensaje de texto diciéndole que abra su navegador o active su aplicación 421. Cualquier técnica adecuada de mensajería puede utilizarse; por ejemplo, un servicio de notificaciones por empuje, un mensaje de texto o similares.

Más aún, respecto al registro, la opción para salir, la opción para entrar y los bloques de decisión 606, 608, en algunos casos puede no ser deseable tener que consultar a todos los que caminan dentro de una instalación de transporte tal como 503 con un dispositivo de mano que se puede descubrir como 400. Siendo así, en algunos casos el sistema solo se pone a disposición de aquellos que han indicado que quieren usar el sistema (por ejemplo, al descargar la aplicación 421). De otro lado, como en 606, 608, en algunos casos los usuarios que no han optado explícitamente por salirse pero quienes tampoco se han registrado afirmativamente puede enviárseles un mensaje cuando entran por primera vez a una región como 502, tras lo cual pueden decidir por expresamente optar por entrar, expresamente optar por salir, o permanecer sin registrar pero sin optar por salir, en cuyo caso tienen la opción para una carrera de “un solo uso” mediante una solicitud de autorización en tiempo real y una respuesta a la solicitud de

autorización desde y hacia el dispositivo de pago emisor; tales usuarios recibirán un mensaje similar cuando ingresan nuevamente a un ambiente tal como 502. En algunos casos, la agencia tiene la oportunidad de ganar ingresos ofreciendo acceso a la puerta rápida 522 como un servicio superior a aquellos dispuestos a pagar una tasa o una tarifa más alta.

Entonces, una o más modalidades permiten un rendimiento de baja fricción en un ambiente de tránsito u otra área de acceso limitado, utilizando conceptos de interacción con un consumidor, apareando dispositivos mediante Bluetooth o similares, y proporcionando una ficha a una puerta rápida 522 tal que a medida que el usuario se acerca, puede caminar derecho independiente de si tiene o no un teléfono equipado con NFC.

Además, una o más modalidades proporcionan una solución de tránsito de pague-cuando-pasa; una solución de pase de tránsito; una solución de tarifa de tránsito por distancia; y/o varias soluciones de control de acceso sin tránsito.

Iniciando el proceso lejos de la puerta es además de ayuda cuando deben emplearse procesamientos de evaluación de riesgo (alertas y controles) (por ejemplo, MasterCard inControl), ya que hay más tiempo disponible para tales tipos de procesamiento con evaluación de riesgo. MasterCard inControl es un servicio que proporciona alertas en tiempo real por correo electrónico y aplicaciones móviles que mantienen a un tarjetahabiente informado de donde y como se están usando sus tarjetas. Donde está la función inControl o similares, una respuesta de solicitud de autorización puede enrutarse mediante ASPs 2050 como se describe arriba en lugar de directamente de regreso al que la adquiere; el tiempo adicional asociado con la iniciación del proceso lejos de la puerta puede ser entonces particularmente beneficioso en tales casos.

Este importante notar que en algunas modalidades, el paso de autenticación 614 en y por sí mismo puede ser con un PAN real o con una ficha generada por una aplicación de billetera en el dispositivo de la persona que está

siendo usado para acceder a su cuenta de tarjeta de pago. El sistema Mastercard Digital Anablement System (MDES) es un ejemplo de un sistema que usa una ficha en forma de un PAN alternativo asociado con el PAN primario. La ficha del MDES no debe confundirse con la ficha en una o más modalidades, la cual es una credencial de acceso que debe ser enviada a la puerta.

También vale la pena notar que en algunas modalidades la puerta rápida 522 puede configurarse para funcionar como una puerta estándar siempre que se prefiera una segunda puerta convencional. Dependiendo del caso particular, esto puede ser durante periodos de bajo volumen, durante periodos de alto volumen, o durante tiempos cuando regularmente se esperan menos usuarios regulares (por ejemplo, en un escenario de tránsito los usuarios regulares tienen más posibilidad que los usuarios casuales de ser ofrecidos una puerta rápida; en los fines de semana, cuando se esperan más pasajeros casuales, la puerta rápida puede configurarse para funcionar como una puerta regular).

Finalmente, debe nuevamente reiterarse que si bien se ha proporcionado un ejemplo no limitante en el contexto del tránsito, pueden emplearse otras modalidades en otros escenarios, por ejemplo, para controlar el acceso a conciertos u otros entretenimientos como se discute aquí en otra parte.

Recapitulación

Dada la discusión hasta este punto, se puede apreciar que, en términos generales, un método ejemplar (por ejemplo 600) de acuerdo con un aspecto de la invención, incluye el paso de detectar la presencia de un dispositivo electrónico portátil 400 fuera de un punto de acceso a un área de acceso controlado 520 (referirse al paso 604). Un paso adicional 612 incluye obtener, del dispositivo electrónico portátil, un indicio de que el usuario del dispositivo electrónico portátil ha sido autenticado al dispositivo electrónico portátil (algunas modalidades alternativamente o adicionalmente incluyen el paso afirmativo de autenticar el

usuario del dispositivo electrónico portátil al dispositivo electrónico portátil). Un paso adicional 614 incluye iniciar un proceso de aprobación del pago asociado con una cuenta del usuario (el paso 614 puede, pero no necesariamente, responder a la obtención de un indicio de autenticación – los pasos 612 y 614 pueden revertirse en algunas instancias). El proceso de aprobación del pago es completado antes que el usuario busque pasar a través del punto de acceso. Un paso adicional 616 incluye, basado al menos en parte en obtener un indicio de la autenticación y el éxito del proceso de aprobación del pago (la rama Y de los bloques de decisión 612 y 614), proporcionando al punto de acceso una ficha electrónica que indica que el usuario, que lleva el dispositivo electrónico portátil, debe permitírsele pasar a través del punto de acceso dentro del área de acceso controlado, basado al menos en parte en la ficha electrónica. Aún otro paso 628 incluye causar que la ficha electrónica expire después que el usuario ha pasado a través del punto de acceso dentro del área de acceso controlado.

El paso de detectar la presencia del dispositivo electrónico portátil puede llevarse a cabo, por ejemplo, mediante comunicaciones inalámbricas de rango medio-largo. Por ejemplo, como se anota arriba, el sistema (el transceptor 504 acoplado al servidos 506 mediante LAN 526 y/o al servidor 510 mediante LAN 526 y WAN 514) detecta la presencia de un teléfono o un dispositivo similar 400 que se puede descubrir. En algunos casos, esta detección se lleva a cabo apalancándose en el mismo tipo de capacidades que los dispositivos utilizan para identificar que están dentro del rango de una red inalámbrica. En otra aproximación, el paso de detectar la presencia de un dispositivo electrónico portátil puede llevarse a cabo, por ejemplo, utilizando una unidad del sistema de posicionamiento global 499 en el dispositivo electrónico portátil.

El paso de autenticación puede llevarse a cabo, por ejemplo, autenticando biométricamente al usuario del dispositivo electrónico portátil al dispositivo electrónico portátil (por ejemplo, mediante un análisis de la huella dactilar,

reconocimiento del habla, reconocimiento facial, o similares). Alternativamente, o además, el paso de autenticación puede llevarse a cabo mediante el ingreso de un número de identificación personal mediante I/O 410 para compararlo con un número almacenado en la memoria 412. El servidor 506 o 510, por ejemplo, obtiene la indicación de éxito de la autenticación de la aplicación 421 en el dispositivo 400 mediante un transceptor 504 y una red 526 (también la red 514 en el caso del servidor 510).

En algunos casos, el paso de iniciar el proceso de aprobación del pago puede llevarse a cabo mediante el servidor 506 utilizando la interfaz 516 para enviar una solicitud de autorización dentro de una red de pago con tarjeta mediante el adquirente 518. En algunos casos, el servidor remoto puede configurarse para llevar a cabo este paso. En otros casos, el servidor 506 o el servidor 510 revisan una cuenta mantenida por el usuario con la entrada asociada con el área de acceso controlado (por ejemplo, en la base de datos 508 o 512) por al menos uno de fondos adecuados, número adecuado de entradas restantes, y el no vencimiento de un pase de acceso con límite de tiempo.

El paso de enviar la ficha de aprobación puede llevarse a cabo, por ejemplo, enviándolo desde el servidor local 506 a la puerta 522 sobre la red 526.

Como se anotó, en una o más modalidades, la ficha de aprobación antes mencionada es un certificado digital de aprobación previa indicando que el usuario 532, por virtud de la autenticación y aprobación, en asociación con el dispositivo 400, es autorizado para pasar a través de la puerta 522. En algunas modalidades, la ficha está encriptada. La ficha puede identificar el teléfono utilizando, por ejemplo, el IMEI, como se discutió arriba, o una ID de software única (o prácticamente única, o sea con una muy baja posibilidad de ser duplicada) tal como una UUID para identificar la aplicación 421 y/o 423, como también se discutió arriba. La capacidad de procesamiento en la puerta rápida 522 compara el identificador del dispositivo 400 con el identificador de la ficha; si empatan, se

genera una señal para causar que la puerta se abra (en el caso de un estado cerrado por defecto); el caso de un estado abierto por defecto se discutió en conexión con la FIGURA 12.

El paso de hacer que la ficha electrónica expire después que el usuario pasa por el punto de acceso al interior del área de acceso controlado puede incluir hacer que la ficha electrónica expire después de un tiempo predeterminado. Por ejemplo, la ficha puede tener un sello de tiempo y la lógica en la puerta rápida 522 puede causar la expiración una vez a pasado tiempo real en el reloj, el sello de tiempo de la ficha puede ser una cantidad predeterminada. Una ficha vencida puede señalarse con una bandera de “expirado” o borrarse de la memoria en la puerta rápida 522. La ficha electrónica típicamente se hace expirar mediante una lógica en el punto de acceso.

Vale la pena notar que cualquier lógica descrita como que reside en la puerta rápida puede encontrarse en el servidor 506, 510 si las conexiones de la red son suficientemente rápidas.

El paso de causar que la ficha electrónica expire una vez el usuario pasa a través del punto de acceso al interior del área de acceso controlado puede, en otros casos, incluir el detectar que el dispositivo electrónico portátil ha pasado a través del punto de acceso al interior del área de acceso controlado (por ejemplo con la unidad 599).

En algunos casos, el inicio del proceso de autorización de pago incluye enviar una solicitud de autorización en tiempo real al emisor de una cuenta del dispositivo de pago asociada con el dispositivo electrónico portátil. El proceso de aprobación del pago es completado antes que el usuario busque pasar a través del punto de acceso al recibir, del emisor de la cuenta del dispositivo de pago asociada con el dispositivo electrónico portátil, en tiempo real, una respuesta a la solicitud de autorización en tiempo real, antes que el usuario busque pasar a través del punto de acceso (nuevamente, mediante la interfaz 518). Como se

emplea aquí, una cuenta del dispositivo de pago está “asociada con” un dispositivo electrónico portátil cuando la información de la cuenta está almacenada en el dispositivo o en una billetera basada en la nube a la que puede acceder el usuario del dispositivo.

En algunos casos, el inicio del proceso de aprobación del pago incluye enviar la solicitud de autorización en tiempo real basada en información de la cuenta del dispositivo de pago contenida en una aplicación de billetera electrónica 423 en el dispositivo electrónico portátil; de otro lado, en algunos casos, el inicio del proceso de aprobación del pago incluye enviar la solicitud de autorización en tiempo real basada en información de la cuenta del dispositivo de pago contenida en una aplicación de billetera basada en la nube 595 a la que accede el dispositivo electrónico portátil.

En algunos casos, el usuario está registrado con una entidad asociada con el área de acceso controlado (por ejemplo, el sistema de ferrocarril o tránsito); y el iniciar el proceso de autorización del pago incluye verificar una cuenta mantenida por el usuario con la entidad asociada con el área de acceso controlado por al menos uno de fondos adecuado, número adecuado de entradas restante, y no vencimiento de un pase de acceso con límite de tiempo (por ejemplo, en el servidor local 506 o en el servidor remoto 510). Tal verificación debe asumirse de manera amplia como que incluye verificar cantidades reales en dólares, un número restante de abordajes u otro contador, y demás.

En un ejemplo no limitante, el área de acceso controlado incluye u sistema de tránsito de ferrocarril, el punto de acceso incluye una puerta de tarifa 522, y el permitir incluye permitir al usuario pasar el interior de la región 520 en donde los trenes pueden ser abordados.

En algunos casos, el punto de acceso compromete un punto de acceso rápido 522 y el usuario incluye un primer usuario. Los pasos adicionales incluyen repetir el paso de detección y el paso de obtener el indicio de autenticación para

un segundo usuario; que responde, al menos en parte, al éxito de la repetida obtención de un indicio de autenticación, iniciar un proceso de aprobación de pago asociado con una cuenta del segundo usuario; y, que responde, al menos en parte, a la falla en el proceso de aprobación de pago asociado con la cuenta del segundo usuario, dirigiendo al segundo usuario lejos del punto de acceso rápido a un punto de acceso convencional 524. Referirse al paso 626.

En alguno de estos casos, un paso adicional incluye enviar una ficha de desaprobación al punto de acceso rápido, que responde, al menos en parte, al fallo del proceso de aprobación de pago asociado con la cuenta del segundo usuario (rama N del bloque 614).

En algunos casos, el punto de acceso compromete un punto de acceso rápido 522, el usuario incluye un primer usuario y el área de acceso controlado tiene un punto de acceso convencional 524 en adición al punto de acceso rápido. Un paso adicional incluye en respuesta, al menos en parte, a la falla del segundo usuario a autenticarse a un segundo dispositivo electrónico portátil correspondiente, enviar una ficha de desaprobación al punto de acceso rápido 522 y al punto de acceso convencional 524.

En algunos casos, el punto de acceso está configurado para permitir al usuario, que lleva el dispositivo electrónico portátil, el paso a través del punto de acceso al área de acceso controlado, basado la menos en parte en la ficha electrónica, utilizando apareamiento por comunicaciones inalámbricas de rango corto (por ejemplo, Bluetooth) entre el punto de acceso y el dispositivo electrónico portátil.

En otro aspecto, un sistema ejemplar incluye un punto de acceso 522 que controla el acceso a un área de acceso controlado 520; un servidor 506; un transceptor 504 de comunicaciones inalámbricas de rango medio; y una red de comunicaciones 526 que coloca el punto de acceso, el servidor y el transceptor en comunicación de datos. El transceptor está configurado para detectar la presencia

de un dispositivo electrónico portátil 400 fuera del punto de acceso. El dispositivo electrónico portátil puede ser visto como una pieza de trabajo sobre la cual actúa el sistema, o en otras modalidades puede ser parte del sistema *per se*. El servidor 506 está configurado para obtener, del dispositivo electrónico portátil, mediante el transceptor y la red de comunicaciones, un indicio de que el usuario del dispositivo electrónico portátil ha sido autenticado al dispositivo electrónico portátil (por ejemplo, la aplicación de tránsito 421 tiene una interfaz con la aplicación que proporciona la autenticación biométrica o por PIN) y se comunica con el servidor 506. El servidor también está configurado para iniciar un proceso de aprobación de pago asociado con una cuenta del usuario (el inicio de la aprobación del pago puede, pero no necesariamente necesita, responder a la obtención de un indicio de autenticación como se discute arriba). El proceso de aprobación de pago es completado antes que el usuario busque pasar a través del punto de acceso. El servidor está configurado para, basado al menos en parte en el indicio de autenticación y el éxito en el proceso de aprobación de pago, proporcionar al punto de acceso una ficha electrónica que indica que el usuario, que lleva el dispositivo electrónico portátil, está autorizado para pasar a través del punto de acceso al interior del área de acceso controlado. El punto de acceso está configurado para permitir al usuario, que lleva el dispositivo electrónico portátil, el paso a través del punto de acceso al interior del área de acceso controlado, basado al menos en parte en la ficha electrónica.

El servidor puede ser configurado para iniciar el proceso de autorización de pago enviando una solicitud de autorización en tiempo real a un emisor de una cuenta de dispositivo de pago asociado con el dispositivo electrónico portátil, mediante un procesador de interfaz de red de pago, o, donde el usuario está registrado con una entidad asociada con el área de acceso controlado, verificando una cuenta mantenida por el usuario como se describe aquí en otra parte.

Detalles del Sistema y Artículo de Manufactura

Las modalidades de la divulgación pueden emplear aspectos de equipos y/o equipos y programas. Los programas incluyen, pero no se limitan a programas de firmado, programas residentes, microcódigo, etc. Los programas pueden ser utilizados, por ejemplo, en conexión con uno o más de un teléfono inteligente, una tableta u otro dispositivo portátil 400, 1420, una terminal 122, 124, 125, 126, un lector 132, una puerta 522, 524, dispositivos de pago tales como tarjetas 102, 112, 400, 1302, 1420, un anfitrión, servidor, y/o centro de procesamiento 140, 142, 144 (opcionalmente con una bodega de datos 154), 506, 510 de un comerciante, emisor, adquisidor, procesador, operador de sistema de tránsito u operador de un área de acceso limitado similar (por ejemplo, terminales de buses, terminales de tren subterráneo, estadios, festivales, pubs, clubes nocturnos, ambientes de campus educativos o corporativos, parques temáticos, hoteles, centros comerciales, y parques vacacionales), operadores de una red 2008 que operan de acuerdo con un estándar (y/o especificación) de sistema de pago, y similares. El programa de firmado puede emplearse, por ejemplo, en conexión con dispositivos de pago tales como tarjetas 102, 112, 1302, 1420 y el lector 132. El programa de firmado proporciona un número básico de funciones (por ejemplo, muestra, imprime y acepta presiones de teclado) que por sí mismas no las proporciona la aplicación de uso final, sino que por el contrario son bloques de construcciones; los programas enlazan los bloques de construcción entre sí para entregar una solución utilizable.

La FIGURA 3 es un diagrama de bloques de un sistema 300 que puede implementar parte o la totalidad de uno o más aspectos o procesos de la divulgación. Como se muestra en la FIGURA 3, la memoria 330 configura el procesador 320 (el cual corresponde, por ejemplo, a las porciones del procesador 106, 116, 130; al procesador de un lector 132; al procesador de los anfitriones remotos en los centros 140, 142, 144; los procesadores de los anfitriones y/o los

servidores 506, 510 que implementan varias funcionalidades; un procesador de una puerta 522; un procesador de un computador de escritorio; un procesador 402; y similares) para implementar uno o más aspectos de los métodos, pasos y funciones divulgados aquí (colectivamente mostrados como el proceso 380 en la FIGURA 3). Diferentes pasos del método pueden llevarse a cabo por diferentes procesadores. La memoria 330 puede ser distribuida o local y el procesador 320 puede ser distribuido o singular. La memoria 330 puede implementarse como una memoria eléctrica, magnética u óptica, o cualquier combinación de estas u otros tipos de dispositivos de almacenamiento (incluyendo porciones de memorias como se describe arriba respecto a las tarjetas 102, 112). Debe anotarse que si se emplean los procesadores distribuidos, cada procesador distribuido que conforma el procesador 320 generalmente contiene su propio espacio de memoria direccionable. También debe anotarse que algunos o todos los sistemas de computador 300 pueden incorporarse en un circuito integrado de aplicación específica o uso general. Por ejemplo, pueden implementarse uno o más pasos del método en equipos en un circuito integrado de aplicación específica (ASIC) o una disposición de puerta que puede programarse en campo (FPGA) en lugar de utilizar programas de firmware. La pantalla 340 representa una pluralidad de dispositivos posibles de entrada/salida.

Como es sabido en el arte, parte o la totalidad de uno o más aspectos de los métodos y aparatos discutidos aquí pueden distribuirse como un artículo de manufactura que por sí mismo comprende un medio de almacenamiento tangible legible y grabable por un computador que tiene medios de código legibles y grabables por computador alojados allí. El código de programa legible y grabable por computador significa que es operado, en conjunción con un sistema de computador, para llevar a cabo todos o algunos de los pasos para realizar los métodos o crear los aparatos discutidos acá. Un medio utilizable por computador puede, en general, ser un medio grabable (por ejemplo, discos blandos, discos

duros, discos compactos, EEPROMs o tarjetas de memoria) o puede ser un medio de transmisión (por ejemplo, una red que comprende fibra óptica, la red global, cables, o un canal inalámbrico que emplea acceso múltiple con división de tiempo, acceso múltiple con división de código, u otro canal de radiofrecuencia). Cualquier medio conocido o desarrollado que puede almacenar información adecuado para uso con un computador, puede ser empleado. Los medios de código legible por computador es cualquier mecanismo para permitirle a un computador leer instrucciones y datos, tal como variaciones magnéticas en un medio magnético o variaciones de altura en una superficie de un disco compacto. El medio puede ser distribuido en múltiples dispositivos físicos (o sobre múltiples redes). Como se utiliza acá, in medio tangible de almacenamiento grabable legible por computador se define como que abarca un medio grabable, ejemplos del cual se dan arriba, pero se define para excluir un medio de transmisión *per se* o una señal incorpórea *per se*.

Los sistemas de computador y servidores descritos acá contienen cada uno una memoria que configurará procesadores asociados para implementar los métodos, pasos y funciones descritos aquí. Tales métodos, pasos y funciones pueden llevarse a cabo, a modo de ejemplo y no de limitación, por la capacidad de procesamiento de los procesadores 402, 320 o por cualquier combinación de los anteriores u otros procesadores aquí descritos. Las memorias pueden ser distribuidas o locales y los procesadores pueden ser distribuidos o singulares. Las memorias pueden implementarse como memorias eléctricas, magnéticas u ópticas, o cualquier combinación de estas y otros tipos de dispositivos de almacenamiento. Más aún, el término “memoria” debe interpretarse como que abarca de manera suficientemente amplia cualquier información capaz de ser leída de o escrita una dirección en el espacio direccionable accesado por un procesador asociado. Con esta definición, la información en una red aun cae

dentro de memoria porque el procesador asociado puede recuperar la información de la red.

Siendo así, los elementos de una o más modalidades de la divulgación, tal como, por ejemplo, 300, 400, 506, 510, 522 pueden hacer uso de tecnología de computador con instrucciones apropiadas para implementar pasos del método descrito aquí. Algunos aspectos pueden implementarse, por ejemplo, utilizando uno o más servidores los cuales incluyen una memoria y al menos un procesador acoplado a la memoria. La memoria puede cargar los programas apropiados. El procesador puede ser operativo para realizar uno o más de los pasos del método descrito aquí o de otra forma facilitar su realización. La unidad 300 representa un servidor y también un computador portátil, una tableta o un computador de escritorio de un usuario.

En concordancia, se apreciará que una o más de las modalidades de la divulgación pueden incluir un programa de computador que comprende medios de código de programa de computador adaptados para realizar uno o todos los pasos de cualquier método o reivindicaciones establecidos aquí cuando tal programa se corre en un computador, y que tal programa puede estar en forma de un medio legible por computador. Además, una o más modalidades de la presente divulgación pueden incluir un computador que comprende código adaptado para causar que el computador lleve a cabo uno o más pasos de los métodos o reivindicaciones establecidos aquí, junto con uno o más elementos o características de aparatos como se muestran y describen aquí.

Como se usa aquí, incluyendo en las reivindicaciones, un “servidor” incluye un sistema físico de procesamiento de datos (por ejemplo, el sistema 300 como se muestra en la FIGURA 3) que corre un programa de servidor. Se entenderá que tal servidor físico puede o no incluir una pantalla, un teclado u otros componentes de entrada/salida. Un “anfitrión” incluye un sistema físico de procesamiento de datos

(por ejemplo, el sistema 300 como se muestra en la FIGURA 3) que corre un programa apropiado.

Además, debe notarse que cualquiera de los métodos descritos aquí incluye un paso adicional de proporcionar un sistema que comprende módulos de programas separados configurados en uno o más medios tangibles de almacenamiento legibles por computador. Todos los módulos (o cualquier subconjunto de los mismos) puede estar en el mismo medio, o cada uno puede estar en un medio diferente, por ejemplo. Los módulos pueden incluir uno o todos los elementos mostrados en las figuras (por ejemplo, diferentes aplicaciones en la memoria 412, módulos para implementar la funcionalidad descrita en los elementos 506, 510, 522, 524, 593, 595, en las FIGS. 7 – 11, y similares). Los pasos del método pueden llevarse a cabo utilizando los módulos de software independientes del sistema, como se describe arriba, ejecutándose en uno o más procesadores del teléfono 400, el servidor 506, la puerta 522, y demás. Además, un producto de programa de computador puede incluir un medio de almacenamiento tangible grabable legible por computador con código adaptado para ser ejecutado para llevar a cabo uno o más pasos del método descritos aquí, incluyendo el proporcionar un sistema con módulos de programas independientes.

Los computadores, tabletas, teléfonos inteligentes, puertas y/u otros elementos con capacidad de procesamiento como se divulgan aquí pueden estar interconectados, por ejemplo, mediante uno o más de la red 138, 2008, otra red privada virtual (VPN), la Internet, una red local y/o una red de área amplia (LAN tal como 526 y/o WAN tal como 514), mediante una capa EDI, mediante una red Wi-Fi de la cual es parte el transceptor 504, mediante Bluetooth, mediante NFC, i demás. Los computadores pueden programarse, por ejemplo, en lenguajes compilados, orientados a objetos, ensamblados y/o lenguajes de máquina, por ejemplo, uno o más de C, C++, Java, Visual Basic, COBOL, y similares (una lista ejemplar y no limitante), y también pueden hacer uso de, por ejemplo, Lenguaje de

Marcado Extensible (XML), programas de aplicaciones conocidas tales como aplicaciones de bases de datos relacionables, hojas de cálculo y similares. Los computadores pueden programarse para implementar la lógica mostrada en los diagramas de flujo y otras figuras.

Aunque las modalidades ilustrativas de la presente divulgación han sido descritas aquí con referencia a los dibujos acompañantes, debe entenderse que la divulgación no se limita a estas modalidades y que pueden hacer diferentes cambios y modificaciones por aquel con habilidad en el arte sin alejarse del alcance y el espíritu de la divulgación.