

REPÚBLICA DE COLOMBIA

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 1730

Ref. Expediente N° NC2016/0001754

Señor(a)
MASTERCARD INTERNATIONAL INCORPORATED
notificaciones@clarkemodet.com.co

Asunto: PATENTE DE INVENCIÓN - PCT

Patente de Invención	PT	Patente de Modelo de Utilidad			
Vía Nacional					
Vía PCT (Fase Nacional)	PCT	Capítulo I		Capítulo II	
No. Solicitud Internacional	PCT/US2015/015546				
Fecha de Presentación Internacional	12 de febrero de 2015				

Como resultado del examen de fondo realizado, con fundamento en el Artículo 45 de la Decisión 486 de la Comisión de la Comunidad Andina, se comunica:

1. Documentos estudiados

Descripción	Radicado N° NC2016/0001754	9/Septiembre/2016
Reivindicaciones:	Radicado N° NC2016/0001754	9/Septiembre/2016
	Radicado N° NC2016/0001754	20/Diciembre/2016
Dibujos:	Radicado N° NC2016/0001754	9/Septiembre/2016
Prioridad(es):	Pais: US, ESTADOS UNIDOS DE AMÉRICA Número: 61/939,132 Fecha: 12 de febrero de 2014	
	Pais: US, ESTADOS UNIDOS DE AMÉRICA Número: 14/619,741 Fecha: 11 de febrero de 2015	

2. Análisis de la Prioridad

Se acepta la reivindicación de prioridad porque esta solicitud fue presentada dentro del plazo establecido y el contenido técnico de esta solicitud corresponde con el de la prioridad reivindicada.

3. Modificaciones presentadas (Art. 34 D 486 y Art. 19, 22 y 34 PCT)

Se aceptan las modificaciones presentadas comoquiera que se ajustan a las prescripciones contenidas en el reglamento del PCT y en el Art 34 de la Decisión 486.

Oficio N° 1730

Ref. Expediente N° NC2016/0001754

4. Objeto de la invención

De acuerdo con lo establecido en el numeral 1.2.2.2 del capítulo primero del Título X de la Circular Única para efectos del examen de patentabilidad, se tendrá en cuenta la tasa pagada por la solicitante al momento de comenzar el examen para las reivindicaciones adicionales; esto es que cuando la solicitud contenga más de diez (10) reivindicaciones y no se haya pagado la tasa complementaria, sólo se estudiarán las cubiertas por la tasa pagada. Por lo tanto, se estudiarán las reivindicaciones 1 a 22 del capítulo reivindicatorio (Radicado N° NC2016/0001754 del 20 de diciembre de 2016).

Título de la solicitud: “MÉTODO DE ACCESO, SISTEMA, MEDIO LEGIBLE Y APARATO PARA PERMITIR PAGOS DE TARIFAS DE RENDIMIENTOS ALTOS” (Ver página 1 del radicado bajo el N° NC2016/0001754 del 20 de diciembre de 2016).

El problema planteado en esta solicitud consiste en la necesidad de suministrar 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.

Para resolver este problema técnico, la solicitud en estudio proporciona un método y un sistema. El método 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. Además, 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.

El objeto de la presente solicitud se relaciona con la Clasificación Internacional de Patentes (CIP): G06Q 40/00.

5. De la solicitud de patente

Reivindicaciones (Art. 30 D 486, Art. 22 PCT)

- Las reivindicaciones 1, 3 a 8, 10 a 11, 15 a 22, no son claras debido a que poseen términos generales que no permiten establecer un concepto suficiente de la invención que se está reclamando. Estos términos se describen a continuación: reivs. 1, 3 a 8, 11, 15 a 19 y 21 a 22: “(...) *dispositivo electrónico portátil* (...)”; reivs. 1, 10 a 11, 16 a 18 y 21 a 22: “(...) *ficha electrónica* (...)”, reivs. 16, 18 a 20: “(...) *servidor* (...)”, reivs. 16 y 18: “(...) *transceptor* (...)”, reivs. 16 y 18: “(...) *red de comunicaciones* (...)”, reiv. 8: “(...) *cuneta* (...)”, reiv. 18: “(...) *servido* (...)”. Se sugiere hacer la aclaración respectiva.

Oficio N° 1730

Ref. Expediente N° NC2016/0001754

- Se sugiere al solicitante incluir entre paréntesis () los números de referencia de cada uno de los elementos que hacen parte de la invención de acuerdo con la numeración empleada en los dibujos, con el fin de hacer más fácil y sencilla la comprensión de la materia reivindicada.

6. Determinación del Estado de la Técnica

El estado de la técnica se determinó con base en la fecha de prioridad: febrero 12 de 2014 y se encontraron los siguientes documentos que anticipan el objeto de esta solicitud:

Ítem	Documento	Título	Fecha de Publicación
D1	US2013/325566	"Public transit system fare processor for multi-balance funding"	5/Diciembre/2013
D2	US 2013/275307	"Systems, methods, and computer readable media for conducting a transaction using cloud based credentials"	17/Octubre/2013

El documento D1¹ un sistema y método para procesar viajes de transferencia asociados con al menos una red de transporte público. El sistema y el método preprocesan transacciones para consolidar o eliminar transacciones innecesarias con una red de compensación y liquidación de una institución financiera. (Resumen).

El documento D2² divulga sistemas, métodos y medios legibles por computadora para realizar una transacción usando credenciales basadas en la nube. (Compendio).

7. Examen de Patentabilidad (Art. 14 D486)

La reivindicación 1 consiste en: *"Un método para permitir pagos de tarifas de rendimientos altos que comprende:(...)"* (Ver página 5 del radicado N° NC2016/0001754 del 20 de diciembre de 2016).

TABLA 1. Comparación de las características técnicas esenciales, con las del estado de la técnica:

Características esenciales	D1	D2
Detectar la presencia de un dispositivo electrónico portátil fuera de un punto de acceso a un área de acceso controlado	No se menciona.	En una realización alternativa, los datos en formato T1/T2 pueden ser proporcionados de manera inalámbrica por el dispositivo móvil (102) a un dispositivo de salto adicional a través de WiFi/ GPS/ Bluetooth/ Detección celular o

¹https://worldwide.espacenet.com/publicationDetails/description?CC=US&NR=2013325566A1&KC=A1&FT=D&ND=3&date=20131205&DB=&locale=en_EP

²https://worldwide.espacenet.com/publicationDetails/description?CC=US&NR=2013275307A1&KC=A1&FT=D&ND=3&date=20131017&DB=&locale=en_EP

Oficio N° 1730

Ref. Expediente N° NC2016/0001754

		cualquier otro método de autodetección. (Pág. 5, Párr. 0031)
Obtener de dicho dispositivo electrónico portátil, una indicación que un usuario de dicho dispositivo electrónico portátil se ha autenticado con dicho dispositivo electrónico portátil;	El titular de una tarjeta bancaria puede registrar una tarjeta bancaria con el sistema de procesamiento (300) a través de una interfaz web, utilizando un sistema de respuesta de voz interactiva (IVR), en un quiosco interactivo o usando una máquina expendedora. El sistema de verificación de tarjeta bancaria (600), como las redes de liquidación y compensación utilizadas por las compañías de tarjetas de crédito, verifica que una tarjeta bancaria sea una tarjeta bancaria actualmente válida. (Pág. 4, Párr. 0042).	Inicialmente, un titular de cuenta nuevo o existente (es decir, el usuario consumidor) puede descargar una aplicación o tarjeta de software, tal como la aplicación (127), desde una tienda o servidor de aplicaciones en línea. Tras su uso inicial, la aplicación (127) puede establecer un secreto de datos compartidos con un sistema emisor (por ejemplo, el servidor emisor (106)) a través de una red celular o de Internet. En algunas realizaciones, la aplicación (127) también puede incluir un certificado digital de emisor que permite que la aplicación (127) y el servidor emisor (106) se autenticuen mutuamente durante todo el ciclo de gestión de vida de la aplicación (127). El certificado digital emisor también permite a la aplicación (127) y al servidor emisor (106) mutuamente autenticarse para una transacción de pago (por ejemplo, cuando se utiliza NFC). (Pág.3, Párr. 0020)
Iniciar un proceso de aprobación de pago asociado con una cuenta de dicho usuario, dicho proceso de aprobación de pago se completa antes que dicho usuario busque pasar a través de dicho punto de acceso.	El procesador de registro de presentación (300) está acoplado a una segunda interfaz (1005) para comunicarse con una pasarela de pago (410) para establecer la pluralidad de cuentas de tránsito. De forma similar, la segunda interfaz (1005) puede ser un bus de computadora. La pasarela de pago (410) está acoplada a una red de beneficios de cercanías (430) (por ejemplo, TransitChek®) para comunicar un primer conjunto de transacciones de liquidación (1007). La pasarela de pago (410) también está acoplada a una red (420) de compensación y liquidación de una institución financiera tradicional (por ejemplo, Base-II) para comunicar un segundo conjunto de transacciones de liquidación (1006). La pasarela de pago (410) primero liquida cuentas mediante la aplicación de fondos de la red (430) de beneficios de cercanías. La pasarela de pago (410) a continuación establece el saldo restante con la red (420) de compensación y liquidación (Pág. 8, Párr. 0079).	En una realización, la aplicación (127) puede utilizar la función criptográfica (126) para producir un resultado que puede usarse para autorizar un pago de compra (o alguna otra transacción electrónica) en el punto de venta. En una realización, la función criptográfica (126) puede recibir un número IMEI, un número de cuenta, un número UTV (almacenado en la memoria (124) o recibido en tiempo real) y datos hash para generar una salida como datos formateados de transacciones heredadas (por ejemplo, Datos de T1 y T2 o datos EMV). La aplicación (127) también puede construir una clave 3-DES basada en la contraseña ingresada y los datos secretos de la aplicación provistos previamente. En una realización, una parte de la salida de la función criptográfica (126) se convierte en datos de Pista 1 y Pista 2 (por ejemplo, caracteres hexadecimales). En este punto, la salida de la función criptográfica (126) está lista para la transmisión al dispositivo lector (104) cuando el teléfono móvil (102) está interconectado (por ejemplo, NFC) con el dispositivo lector (104). En una realización, al menos una parte del identificador de usuario y un BIN

Oficio N° 1730

Ref. Expediente N° NC2016/0001754

		permanece sin encriptar mientras que los datos restantes se encriptan como salida de la función criptográfica (126). (Pág. 26, Párr. 0026)
Suministrar a dicho punto de acceso una ficha electrónica que indica que a dicho usuario, que lleva dicho dispositivo electrónico portátil, se le debe permitir pasar a través de dicho punto de acceso al área de acceso controlado.	Las FIGS. 5A, 5B y 5C muestran el flujo de mensajes entre los componentes de la red, de acuerdo con las realizaciones de la presente invención. En la Fig. 5A, una tarjeta bancaria (100) es presentada actualmente por un titular de la misma (por ejemplo, un viajero de metro o un conductor de autobús). El lector (210) de tarjeta bancaria en el terminal (200) de tarjeta bancaria recibe datos de tarjeta bancaria que comprenden datos de la tarjeta bancaria actualmente presentada. El procesador (220) de terminal de tarjeta bancaria en el terminal (200) de tarjeta bancaria determina un identificador (por ejemplo, un valor hash o un número de tarjeta de crédito) de la tarjeta bancaria presentada. A continuación, el procesador (220) de terminal de tarjeta bancaria usa el identificador determinado para indicar que la tarjeta bancaria presentada actualmente está contenida en el conjunto de registros (230) de tarjeta bancaria. El procesador (220) terminal de tarjeta bancaria señala a la segunda interfaz (260) para comunicarse con el controlador (270) de acceso. El controlador (270) de acceso puede ser, por ejemplo, un conductor, una puerta del torniquete o un conductor de autobús u otro ser humano que proporcione supervisión o control. (Pág. 6, Párr. 0062).	No se menciona
Permitir a dicho usuario, que lleva dicho dispositivo electrónico portátil, pasar a través de dicho punto de acceso a dicha área de acceso controlado, con base en dicha ficha electrónica	Para ayudar al acceso de puerta, en algunas realizaciones la segunda interfaz (260) puede activar una barrera, mientras que otra segunda interfaz de realización (260) puede simplemente activar una luz roja o verde observable por un conductor, un operador de puerta y/o el conmutador. La segunda interfaz (260) puede proporcionar una señal para abrir el torniquete. La segunda interfaz (260) puede proporcionar una señal para activar un anuncio de audio y/o visual. Por ejemplo, la segunda interfaz (260) puede enviar una señal a una pantalla LCD o un LED en una unidad portátil que sea	No se menciona

Oficio N° 1730

Ref. Expediente N° NC2016/0001754

	observada por un conductor. (Pág. 6, Párr. 0063)	
Hacer que dicha ficha electrónica expire después que dicho usuario pase a través de dicho punto de acceso a dicha área de acceso controlado.	En algunas realizaciones, el primer registro de presentación resulta de una transacción entre un token de identificación y un lector de fichas, en el que el token de identificación no retiene información con respecto a la transacción. En otras realizaciones, la ficha de identificación solo conserva un contador ajustado como resultado de la transacción. De esta manera, los tokens de identificación son realmente sin memoria. (Pág. 9, Párr. 87)	No se menciona

El documento D1 se considera el estado de la técnica más cercano a la invención definida en la reivindicación 1 porque divulga la implementación de un sistema y método para procesar viajes de transferencia asociados con al menos una red de transporte público. El sistema y el método preprocesan transacciones para consolidar o eliminar transacciones innecesarias con una red de compensación y liquidación de una institución financiera. (Pág., 1, Resumen).

La diferencia entre la invención, definida en la reivindicación 1 y el método de D1 consiste en que en el método de la reivindicación 1 incluye la detección automática de un dispositivo electrónico portátil en un punto determinado de un área de acceso.

El efecto que logra la detección automática de un dispositivo electrónico portátil en un punto determinado de un área de acceso es permitir la autenticación e inicio la aprobación del proceso de pago antes de que el usuario pase a través de dicho punto de acceso completando así la transacción.

Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así: “¿cómo modificar el método conocido en D1 para permitir la autenticación e inicio de la aprobación del proceso de pago antes de que el usuario pase a través de dicho punto de acceso?”.

Sin embargo, la detección automática de un dispositivo electrónico portátil en un punto determinado de un área de acceso para permitir la autenticación e inicio de la aprobación del proceso de pago antes de que el usuario pase a través de dicho punto, ya está divulgada en el documento D2 que se refiere a que los datos formateados pueden ser proporcionados de manera inalámbrica por el dispositivo móvil (102) a un dispositivo de salto adicional a través de WiFi/ GPS/ Bluetooth/ detección celular o cualquier otro método de autodetección. (Pág. 5, Párr. 0031).

En consecuencia, la persona del oficio normalmente versada en la materia, incluiría los métodos de autodetección de dispositivos electrónicos portátiles mencionados en documento D2 en el método divulgado en el documento D1 para llegar así al objeto de la reivindicación 1 de la solicitud. Por lo cual se considera obvia.

Asimismo, los documentos D1 y D2 divulgan las características de las siguientes reivindicaciones dependientes así:

Oficio N° 1730

Ref. Expediente N° NC2016/0001754

- Reivindicaciones 2 y 3: En una realización alternativa, los datos en formato T1/T2 pueden ser proporcionados de manera inalámbrica por el dispositivo móvil (102) a un dispositivo de salto adicional a través de WiFi/ GPS/ Bluetooth/ Detección celular o cualquier otro método de autodetección. El dispositivo alternativo puede entonces reenviar los datos formato T1/T2 al dispositivo POS 105. Además, el dispositivo móvil (102) puede configurarse para pulsar un cartel inteligente que permite al dispositivo móvil (102) para proporcionar los datos en formato T1/T2 con un servidor comercial en el servidor. El servidor comercial puede entonces reenviar los datos en formato T1/T2 al dispositivo POS (105) que posteriormente proporciona los datos al servidor emisor (106) sobre las bandas POS existentes. (D2, Pág. 5, Párr. 0031).
- Reivindicación 4: El contenido de datos del usuario puede incluir un número de cuenta asociado con un proveedor de servicio, un identificador de usuario único (por ejemplo, un número de teléfono, dirección de correo electrónico, identificador nacional, etc.), una contraseña de usuario (en combinación con información biométrica opcional en algunos casos) un identificador de módulo de identidad de abonado (SIM), un número de identificación patronal (EIN), un WIN, un número de identificación de equipo móvil internacional (IMEI), un número aleatorio y/o un valor de transacción único (por ejemplo, un número de secuencia). (D2, Pág. 3, Párr. 0025). (...) La contraseña puede incluir o utilizar una contraseña alfanumérica, datos biométricos o un mecanismo de desafío/respuesta. (D2, Pág. 5, Párr. 0035).
- Reivindicación 5: El contenido de datos del usuario puede incluir un número de cuenta asociado con un proveedor de servicio, un identificador de usuario único (por ejemplo, un número de teléfono, dirección de correo electrónico, identificador nacional, etc.), una contraseña de usuario (en combinación con información biométrica opcional en algunos casos) un identificador de módulo de identidad de abonado (SIM), un número de identificación patronal (EIN), un WIN, un número de identificación de equipo móvil internacional (IMEI), un número aleatorio y/o un valor de transacción único (por ejemplo, un número de secuencia). (D2, Pág. 3, Párr. 0025).
- Reivindicación 6: El procesador de registro de presentación (300) está acoplado a una segunda interfaz (1005) para comunicarse con una pasarela de pago (410) para establecer la pluralidad de cuentas de tránsito. De forma similar, la segunda interfaz (1005) puede ser un bus de computadora. La pasarela de pago (410) está acoplada a una red de beneficios de cercanías (430) (por ejemplo, TransitChek®) para comunicar un primer conjunto de transacciones de liquidación (1007). La pasarela de pago (410) también está acoplada a una red (420) de compensación y liquidación de una institución financiera tradicional (por ejemplo, Base-II) para comunicar un segundo conjunto de transacciones de liquidación (1006). La pasarela de pago (410) primero liquida cuentas mediante la aplicación de fondos de la red (430) de beneficios de cercanías. La pasarela de pago (410) a continuación establece el saldo restante con la red (420) de compensación y liquidación (D1, Pág. 8, Párr. 0079).
- Reivindicaciones 7 y 8: La FIG. 2 es un diagrama de flujo que ilustra un método (200) para llevar a cabo una transacción usando credenciales basadas en la nube de acuerdo con una realización del tema descrito en este documento. En el paso (202), se inicia una transacción electrónica. En una realización, un usuario de un

Oficio N° 1730

Ref. Expediente N° NC2016/0001754

dispositivo móvil usa un dispositivo móvil para seleccionar e iniciar una aplicación (por ejemplo, utilizar una billetera móvil para seleccionar una tarjeta de software). Después de seleccionar una aplicación, el usuario puede ingresar datos secretos compartidos (por ejemplo, una contraseña o clave de cifrado conocida por el usuario y la entidad emisora) asociados con la aplicación utilizando la interfaz de usuario (por ejemplo, pantalla táctil o teclas) del dispositivo móvil. (D2, Pág. 5, Párr. 0037).

- Reivindicación 9: En (402), el terminal (200) de tarjeta bancaria usa el identificador determinado para indicar si la tarjeta bancaria está o no contenida en un conjunto de registros de tarjeta bancaria y si la tarjeta bancaria es o no una tarjeta bancaria válida conocida. En algunas realizaciones del terminal (200) de tarjeta bancaria que tienen una interfaz con un sistema (600) de verificación de tarjeta bancaria, se intenta verificar la tarjeta bancaria en (404). En (405), el terminal (200) de tarjeta bancaria determina si la tarjeta bancaria se verificó satisfactoriamente o no. En (406), si la tarjeta bancaria se verificó con éxito, el conjunto de registros de la tarjeta bancaria (230) se actualiza con el identificador determinado para la tarjeta bancaria presentada actualmente. En (407), si la verificación no fue exitosa, se deniega el acceso, por ejemplo, al no abrir una puerta y/o al activar un indicador de audio y/o visual para el titular de la tarjeta bancaria y/o un conductor. En (403), si el identificador determinado ya estaba en el conjunto de registros de la tarjeta bancaria (230) como una tarjeta bancaria válida conocida o se agregó al conjunto de registros de la tarjeta bancaria (en (406)), se permite el acceso al sistema de tránsito, por ejemplo, abriendo la puerta y/o activando un indicador de audio y/o visual al titular de la tarjeta bancaria y/o a un conductor. (D1, Pág. 6, Párr. 0061).
- Reivindicaciones 10 y 11: En algunas realizaciones, el primer registro de presentación resulta de una transacción entre un token de identificación y un lector de fichas, en el que el token de identificación no retiene información con respecto a la transacción. En otras realizaciones, la ficha de identificación solo conserva un contador ajustado como resultado de la transacción. De esta manera, los tokens de identificación son realmente sin memoria. (D1, Pág. 9, Párr. 87).
- Reivindicación 12: Los terminales (200) de la tarjeta bancaria proporcionan una interfaz de front-end a las tarjetas bancarias. Un terminal de tarjeta bancaria (200A) puede tomar la forma de un torniquete en una puerta en el sistema de metro. Alternativamente, un terminal de tarjeta bancaria (200A) puede usarse en un sistema de tránsito que incorpore un sistema de autosupervisión o de honor (es decir, un pasajero puede ingresar al sistema de tránsito sin estar físicamente bloqueado por un torniquete; el pasajero proporciona voluntariamente su tarjeta bancaria al terminal de tarjeta bancaria (200A); en este caso, el enganche puede ser proporcionado simplemente por un indicador de audio y/o visual, que requiere que el pasajero lo respete). (D1, Pág. 4, Párr. 0041, Fig. 1)
- Reivindicaciones 13 a 15: Las realizaciones de la presente invención incluyen un método para controlar el acceso a una red de tránsito manteniendo una lista negra en la memoria en la que la lista negra identifica fichas, comprendiendo el método: (a) otorgar a un primer corredor potencial acceso a un sistema de tránsito previa presentación de una primera ficha de identificación, en la que el acto de otorgar comprende: (1) leer un primer conjunto de datos de ficha de la primera ficha de identificación usando un primer lector de ficha; (2) calcular un primer identificador

Oficio N° 1730

Ref. Expediente N° NC2016/0001754

de token a partir del primer token de identificación; (3) verificar el primer token contra la lista negra en la memoria; y (4) usar el primer identificador de token para permitir el acceso del primer usuario potencial a la red de tránsito, si el primer token de usuario no está en la lista negra; (b) denegar a un segundo corredor potencial el acceso al sistema de tránsito con la presentación de una segunda ficha de identificación, en el que el acto de denegación comprende: (1) leer un segundo conjunto de datos de ficha desde la segunda ficha de identificación, utilizando un segundo lector de ficha; (2) calcular un segundo identificador de token a partir del segundo token de identificación; (3) verificar el segundo token de identificación contra la lista negra en la memoria; y (4) denegar el acceso al segundo corredor potencial a la red de tránsito, si el segundo token de usuario está en la lista negra; (c) agregar un tercer token de identificación a la lista negra si el saldo pendiente no se paga, en donde el acto de agregar comprende: (1) cobrar sin éxito una o más cuentas de pago asociadas con el tercer token de identificación; y (2) agregar la tercera ficha de usuario a la lista negra; y (d) eliminar un cuarto token de identificación de la lista negra después de que se acredita una cuenta monetaria asociada, en donde el acto de eliminar comprende: (1) cargar con éxito una cuenta de pago asociada con el cuarto token de identificación; (2) acreditando la cuenta monetaria asociada; y (3) eliminar el cuarto token de usuario de la lista negra. (D1, Pág. 12, Párr. 0102)

- Reivindicación 16: En una realización alternativa, los datos en formato T1/T2 pueden ser proporcionados de manera inalámbrica por el dispositivo móvil (102) a un dispositivo de salto adicional a través de WiFi/ GPS/ Bluetooth/ Detección celular o cualquier otro método de autodetección. El dispositivo alternativo puede entonces reenviar los datos formato T1/T2 al dispositivo POS 105. Además, el dispositivo móvil (102) puede configurarse para pulsar un cartel inteligente que permite al dispositivo móvil (102) para proporcionar los datos en formato T1/T2 con un servidor comercial en el servidor. El servidor comercial puede entonces reenviar los datos en formato T1/T2 al dispositivo POS (105) que posteriormente proporciona los datos al servidor emisor (106) sobre las bandas POS existentes. (D2, Pág. 5, Párr. 0031)

La reivindicación 18 consiste en: *“Un sistema para permitir pagos de tarifas de rendimientos altos que comprende:(...)”* (Ver página 8 del radicado N° NC2016/0001754 del 20 de diciembre de 2016).

TABLA 2. Comparación de las características técnicas esenciales, con las del estado de la técnica:

Características esenciales	D1	D2
Dicho transceptor se configura para detectar la presencia de un dispositivo electrónico portátil por fuera de dicho punto de acceso.	No se menciona.	En una realización alternativa, los datos en formato T1/T2 pueden ser proporcionados de manera inalámbrica por el dispositivo móvil (102) a un dispositivo de salto adicional a través de WiFi/ GPS/ Bluetooth/ Detección celular o cualquier otro método de autodetección. (Pág. 5, Párr. 0031)

Oficio N° 1730

Ref. Expediente N° NC2016/0001754

Dicho servidor se configura para obtener, del dispositivo electrónico portátil, por medio de dicho transceptor y dicha red de comunicaciones, una indicación que un usuario de dicho dispositivo electrónico portátil se ha autenticado a dicho dispositivo electrónico portátil.	El titular de una tarjeta bancaria puede registrar una tarjeta bancaria con el sistema de procesamiento (300) a través de una interfaz web, utilizando un sistema de respuesta de voz interactiva (IVR), en un quiosco interactivo o usando una máquina expendedora. El sistema de verificación de tarjeta bancaria (600), como las redes de liquidación y compensación utilizadas por las compañías de tarjetas de crédito, verifica que una tarjeta bancaria sea una tarjeta bancaria actualmente válida. (Pág. 4, Párr. 0042).	Inicialmente, un titular de cuenta nuevo o existente (es decir, el usuario consumidor) puede descargar una aplicación o tarjeta de software, tal como la aplicación (127), desde una tienda o servidor de aplicaciones en línea. Tras su uso inicial, la aplicación (127) puede establecer un secreto de datos compartidos con un sistema emisor (por ejemplo, el servidor emisor (106)) a través de una red celular o de Internet. En algunas realizaciones, la aplicación (127) también puede incluir un certificado digital de emisor que permite que la aplicación (127) y el servidor emisor (106) se autenticuen mutuamente durante todo el ciclo de gestión de vida de la aplicación (127). El certificado digital emisor también permite a la aplicación (127) y al servidor emisor (106) mutuamente autenticarse para una transacción de pago (por ejemplo, cuando se utiliza NFC). (Pág.3, Párr. 0020)
Dicho servidor se configura para iniciar un proceso de aprobación de pago asociado con una cuenta de dicho usuario, dicho proceso de aprobación de pago se completa antes que dicho usuario busque pasar a través de dicho punto de acceso.	El procesador de registro de presentación (300) está acoplado a una segunda interfaz (1005) para comunicarse con una pasarela de pago (410) para establecer la pluralidad de cuentas de tránsito. De forma similar, la segunda interfaz (1005) puede ser un bus de computadora. La pasarela de pago (410) está acoplada a una red de beneficios de cercanías (430) (por ejemplo, TransitChek®) para comunicar un primer conjunto de transacciones de liquidación (1007). La pasarela de pago (410) también está acoplada a una red (420) de compensación y liquidación de una institución financiera tradicional (por ejemplo, Base-II) para comunicar un segundo conjunto de transacciones de liquidación (1006). La pasarela de pago (410) primero liquida cuentas mediante la aplicación de fondos de la red (430) de beneficios de cercanías. La pasarela de pago (410) a continuación establece el saldo restante con la red (420) de compensación y liquidación (Pág. 8, Párr. 0079).	En una realización, la aplicación (127) puede utilizar la función criptográfica (126) para producir un resultado que puede usarse para autorizar un pago de compra (o alguna otra transacción electrónica) en el punto de venta. En una realización, la función criptográfica (126) puede recibir un número IMEI, un número de cuenta, un número UTV (almacenado en la memoria (124) o recibido en tiempo real) y datos hash para generar una salida como datos formateados de transacciones heredadas (por ejemplo, Datos de T1 y T2 o datos EMV). La aplicación (127) también puede construir una clave 3-DES basada en la contraseña ingresada y los datos secretos de la aplicación provistos previamente. En una realización, una parte de la salida de la función criptográfica (126) se convierte en datos de Pista 1 y Pista 2 (por ejemplo, caracteres hexadecimales). En este punto, la salida de la función criptográfica (126) está lista para

Oficio N° 1730

Ref. Expediente N° NC2016/0001754

		la transmisión al dispositivo lector (104) cuando el teléfono móvil (102) está interconectado (por ejemplo, NFC) con el dispositivo lector (104). En una realización, al menos una parte del identificador de usuario y un BIN permanece sin encriptar mientras que los datos restantes se encriptan como salida de la función criptográfica (126). (Pág. 26, Párr. 0026)
Dicho servidor se configura para, con base en dicha indicación de autenticación y éxito de dicho proceso de aprobación de pago, suministrar a dicho punto de acceso una ficha electrónica que indica que el usuario, que lleva el dispositivo electrónico portátil, se debe permitir el paso a través de dicho punto de acceso a dicha área de acceso controlado.	Las FIGS. 5A, 5B y 5C muestran el flujo de mensajes entre los componentes de la red, de acuerdo con las realizaciones de la presente invención. En la Fig. 5A, una tarjeta bancaria (100) es presentada actualmente por un titular de la misma (por ejemplo, un viajero de metro o un conductor de autobús). El lector (210) de tarjeta bancaria en el terminal (200) de tarjeta bancaria recibe datos de tarjeta bancaria que comprenden datos de la tarjeta bancaria actualmente presentada. El procesador (220) de terminal de tarjeta bancaria en el terminal (200) de tarjeta bancaria determina un identificador (por ejemplo, un valor hash o un número de tarjeta de crédito) de la tarjeta bancaria presentada. A continuación, el procesador (220) de terminal de tarjeta bancaria usa el identificador determinado para indicar que la tarjeta bancaria presentada actualmente está contenida en el conjunto de registros (230) de tarjeta bancaria. El procesador (220) terminal de tarjeta bancaria señala a la segunda interfaz (260) para comunicarse con el controlador (270) de acceso. El controlador (270) de acceso puede ser, por ejemplo, un conductor, una puerta del torniquete o un conductor de autobús u otro ser humano que proporcione supervisión o control. (Pág. 6, Párr. 0062).	No se menciona
Dicho punto de acceso se configura para permitir que el usuario, que lleva el dispositivo electrónico portátil, pase a través de dicho punto de acceso a dicha área de acceso controlado, con base en dicha ficha electrónica.	Para ayudar al acceso de puerta, en algunas realizaciones la segunda interfaz (260) puede activar una barrera, mientras que otra segunda interfaz de realización (260) puede simplemente activar una luz roja o verde observable por un conductor, un operador de puerta y/o el conmutador. La segunda interfaz (260) puede proporcionar una señal para abrir el torniquete. La segunda	No se menciona

Oficio N° 1730

Ref. Expediente N° NC2016/0001754

	interfaz (260) puede proporcionar una señal para activar un anuncio de audio y/o visual. Por ejemplo, la segunda interfaz (260) puede enviar una señal a una pantalla LCD o un LED en una unidad portátil que sea observada por un conductor. (Pág. 6, Párr. 0063)	
--	--	--

El documento D1 se considera el estado de la técnica más cercano a la invención definida en la reivindicación 18 porque divulga la implementación de un sistema y método para procesar viajes de transferencia asociados con al menos una red de transporte público. El sistema y el método preprocesan transacciones para consolidar o eliminar transacciones innecesarias con una red de compensación y liquidación de una institución financiera. (Pág. 1, Resumen).

La diferencia entre la invención, definida en la reivindicación 18 y el sistema de D1 consiste en que en el sistema de la reivindicación 18 incluye la detección automática de un dispositivo electrónico portátil en un punto determinado de un área de acceso.

El efecto que logra la detección automática de un dispositivo electrónico portátil en un punto determinado de un área de acceso es permitir la autenticación e inicio la aprobación del proceso de pago antes de que el usuario pase a través de dicho punto de acceso completando así la transacción.

Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así: “¿cómo modificar el sistema conocido en D1 para permitir la autenticación e inicio de la aprobación del proceso de pago antes de que el usuario pase a través de dicho punto de acceso?”.

Sin embargo, la detección automática de un dispositivo electrónico portátil en un punto determinado de un área de acceso para permitir la autenticación e inicio de la aprobación del proceso de pago antes de que el usuario pase a través de dicho punto, ya está divulgada en el documento D2 que se refiere a que los datos formateados pueden ser proporcionados de manera inalámbrica por el dispositivo móvil (102) a un dispositivo de salto adicional a través de WiFi / GPS / Bluetooth / detección celular o cualquier otro método de autodetección. (Pág. 5, Párr. 0031)

En consecuencia, la persona del oficio normalmente versada en la materia, incluiría los métodos de autodetección de dispositivos electrónicos portátiles mencionados en documento D2 en el sistema divulgado en el documento D1 para llegar así al objeto de la reivindicación 18 de la solicitud. Por lo cual se considera obvia.

Asimismo, el documento D2 divulga las características de las siguientes reivindicaciones dependientes así:

Reivindicaciones 19 y 20: una vez que el usuario/ consumidor verifica y las credenciales de la cuenta son validadas, el servidor emisor (106) proporciona una instrucción (por ejemplo, un mensaje de confirmación o notificación) al dispositivo de POS (105) y/o lector de dispositivo inalámbrico (104) para proceder con la transacción electrónica (es decir, autorizar transacción electrónica en el punto de venta). En una realización, la instrucción se proporciona a través del servidor de aprovisionamiento OTA (110). El dispositivo POS (105) puede entonces llevar a cabo/ completar la transacción electrónica tras la recepción del mensaje de notificación. (D2, Pág. 5, Párr.

Oficio N° 1730

Ref. Expediente N° NC2016/0001754

0036). En la etapa (212), se envía un mensaje de notificación. En algunas realizaciones, el servidor emisor puede utilizar un servidor de aprovisionamiento OTA para proporcionar una instrucción (por ejemplo, un mensaje de confirmación o notificación) al dispositivo de punto de venta y/o al dispositivo lector para proceder con la transacción electrónica (es decir, autorizar la transacción en el punto de venta). En una realización, el servidor emisor o el servidor de aprovisionamiento OTA puede, después de verificar al usuario, validar la cuenta del usuario consultando un servidor de cuenta que gestiona la cuenta del usuario (por ejemplo, una cuenta de tarjeta de crédito, una cuenta de tarjeta de fidelidad, etc.) antes de enviar el mensaje de notificación. (D2, Pág. 6, Párr. 0044).

En la etapa (214), se lleva a cabo la transacción electrónica. En algunas realizaciones, el dispositivo lector de POS puede entonces llevar a cabo/completar la transacción electrónica al recibir el mensaje de notificación. (D2, Pág. 6, Párr. 0045)

La reivindicación 21 consiste en: “*Un medio legible por computador no transitorio que comprende instrucciones ejecutables por computador el cual cuando se ejecuta por un computador hace que el computador realice el método de: (...)*” (Ver página 10 del radicado N° NC2016/0001754 del 20 de diciembre de 2016).

TABLA 3. Comparación de las características técnicas esenciales, con las del estado de la técnica:

Características esenciales	D1	D2
Detectar la presencia de un dispositivo electrónico portátil fuera de un punto de acceso a un área de acceso controlado.	No se menciona.	En una realización alternativa, los datos en formato T1/T2 pueden ser proporcionados de manera inalámbrica por el dispositivo móvil (102) a un dispositivo de salto adicional a través de WiFi/ GPS/ Bluetooth/ Detección celular o cualquier otro método de autodetección. (Pág. 5, Párr. 0031)
Obtener, de dicho dispositivo electrónico portátil, una indicación que un usuario de dicho dispositivo electrónico portátil se ha autenticado con dicho dispositivo electrónico portátil.	El titular de una tarjeta bancaria puede registrar una tarjeta bancaria con el sistema de procesamiento (300) a través de una interfaz web, utilizando un sistema de respuesta de voz interactiva (IVR), en un quiosco interactivo o usando una máquina expendedora. El sistema de verificación de tarjeta bancaria (600), como las redes de liquidación y compensación utilizadas por las compañías de tarjetas de crédito, verifica que una tarjeta bancaria sea una tarjeta bancaria actualmente válida. (Pág. 4, Párr. 0042).	Inicialmente, un titular de cuenta nuevo o existente (es decir, el usuario consumidor) puede descargar una aplicación o tarjeta de software, tal como la aplicación (127), desde una tienda o servidor de aplicaciones en línea. Tras su uso inicial, la aplicación (127) puede establecer un secreto de datos compartidos con un sistema emisor (por ejemplo, el servidor emisor (106)) a través de una red celular o de Internet. En algunas realizaciones, la aplicación (127) también puede incluir un certificado digital de emisor que permite que la aplicación (127) y el servidor emisor (106) se autenticuen mutuamente durante todo el ciclo de gestión de vida de la aplicación (127). El certificado digital emisor también permite

Oficio N° 1730

Ref. Expediente N° NC2016/0001754

		a la aplicación (127) y al servidor emisor (106) mutuamente autenticarse para una transacción de pago (por ejemplo, cuando se utiliza NFC). (Pág.3, Párr. 0020)
Iniciar un proceso de aprobación de pago asociado con una cuenta de dicho usuario, dicho proceso de aprobación de pago se completa antes que dicho usuario busque pasar a través de dicho punto de acceso.	El procesador de registro de presentación (300) está acoplado a una segunda interfaz (1005) para comunicarse con una pasarela de pago (410) para establecer la pluralidad de cuentas de tránsito. De forma similar, la segunda interfaz (1005) puede ser un bus de computadora. La pasarela de pago (410) está acoplada a una red de beneficios de cercanías (430) (por ejemplo, TransitChek®) para comunicar un primer conjunto de transacciones de liquidación (1007). La pasarela de pago (410) también está acoplada a una red (420) de compensación y liquidación de una institución financiera tradicional (por ejemplo, Base-II) para comunicar un segundo conjunto de transacciones de liquidación (1006). La pasarela de pago (410) primero liquida cuentas mediante la aplicación de fondos de la red (430) de beneficios de cercanías. La pasarela de pago (410) a continuación establece el saldo restante con la red (420) de compensación y liquidación (Pág. 8, Párr. 0079).	En una realización, la aplicación (127) puede utilizar la función criptográfica (126) para producir un resultado que puede usarse para autorizar un pago de compra (o alguna otra transacción electrónica) en el punto de venta. En una realización, la función criptográfica (126) puede recibir un número IMEI, un número de cuenta, un número UTV (almacenado en la memoria (124) o recibido en tiempo real) y datos hash para generar una salida como datos formateados de transacciones heredadas (por ejemplo, Datos de T1 y T2 o datos EMV). La aplicación (127) también puede construir una clave 3-DES basada en la contraseña ingresada y los datos secretos de la aplicación provistos previamente. En una realización, una parte de la salida de la función criptográfica (126) se convierte en datos de Pista 1 y Pista 2 (por ejemplo, caracteres hexadecimales). En este punto, la salida de la función criptográfica (126) está lista para la transmisión al dispositivo lector (104) cuando el teléfono móvil (102) está interconectado (por ejemplo, NFC) con el dispositivo lector (104). En una realización, al menos una parte del identificador de usuario y un BIN permanece sin encriptar mientras que los datos restantes se encriptan como salida de la función criptográfica (126). (Pág. 26, Párr. 0026)
Suministrar a dicho punto de acceso una ficha electrónica que indica que a dicho usuario, que lleva dicho dispositivo electrónico portátil, se le debe permitir pasar a través de dicho	Las FIGS. 5A, 5B y 5C muestran el flujo de mensajes entre los componentes de la red, de acuerdo con las realizaciones de la presente invención. En la Fig. 5A, una tarjeta bancaria (100) es presentada actualmente por un titular de la	No se menciona

Oficio N° 1730

Ref. Expediente N° NC2016/0001754

punto de acceso al área de acceso controlado.	misma (por ejemplo, un viajero de metro o un conductor de autobús). El lector (210) de tarjeta bancaria en el terminal (200) de tarjeta bancaria recibe datos de tarjeta bancaria que comprenden datos de la tarjeta bancaria actualmente presentada. El procesador (220) de terminal de tarjeta bancaria en el terminal (200) de tarjeta bancaria determina un identificador (por ejemplo, un valor hash o un número de tarjeta de crédito) de la tarjeta bancaria presentada. A continuación, el procesador (220) de terminal de tarjeta bancaria usa el identificador determinado para indicar que la tarjeta bancaria presentada actualmente está contenida en el conjunto de registros (230) de tarjeta bancaria. El procesador (220) terminal de tarjeta bancaria señala a la segunda interfaz (260) para comunicarse con el controlador (270) de acceso. El controlador (270) de acceso puede ser, por ejemplo, un conductor, una puerta del torniquete o un conductor de autobús u otro ser humano que proporcione supervisión o control. (Pág. 6, Párr, 0062).	
Permitir a dicho usuario, que lleva dicho dispositivo electrónico portátil, pasar a través de dicho punto de acceso a dicha área de acceso controlado, con base en dicha ficha electrónica.	Para ayudar al acceso de puerta, en algunas realizaciones la segunda interfaz (260) puede activar una barrera, mientras que otra segunda interfaz de realización (260) puede simplemente activar una luz roja o verde observable por un conductor, un operador de puerta y/o el conmutador. La segunda interfaz (260) puede proporcionar una señal para abrir el torniquete. La segunda interfaz (260) puede proporcionar una señal para activar un anuncio de audio y/o visual. Por ejemplo, la segunda interfaz (260) puede enviar una señal a una pantalla LCD o un LED en una unidad portátil que sea observada por un conductor. (Pág. 6, Párr. 0063)	No se menciona
Hacer que dicha ficha electrónica expire después que dicho usuario pase a través de dicho punto de acceso a dicha área de acceso controlado.	En algunas realizaciones, el primer registro de presentación resulta de una transacción entre un token de identificación y un lector de fichas, en el que el token de identificación no retiene información con respecto a la transacción. En otras realizaciones, la ficha de identificación solo conserva un contador ajustado como resultado de la transacción. De esta manera, los tokens de identificación	No se menciona

Oficio N° 1730

Ref. Expediente N° NC2016/0001754

	son realmente sin memoria. (Pág. 9, Párr. 87)	
--	---	--

El documento D1 se considera el estado de la técnica más cercano a la invención definida en la reivindicación 21 porque divulga la implementación de un sistema y método para procesar viajes de transferencia asociados con al menos una red de transporte público. El sistema y el método preprocesan transacciones para consolidar o eliminar transacciones innecesarias con una red de compensación y liquidación de una institución financiera. (Pág. 1, Resumen).

La diferencia entre la invención, definida en la reivindicación 21 y el método de D1 consiste en que en el sistema de la reivindicación 21 incluye la detección automática de un dispositivo electrónico portátil en un punto determinado de un área de acceso.

El efecto que logra la detección automática de un dispositivo electrónico portátil en un punto determinado de un área de acceso es permitir la autenticación e inicio la aprobación del proceso de pago antes de que el usuario pase a través de dicho punto de acceso completando así la transacción.

Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así: “¿cómo modificar las instrucciones de un medio legible por computador conocido en D1 para permitir la autenticación e inicio de la aprobación del proceso de pago antes de que el usuario pase a través de dicho punto de acceso?”.

Sin embargo, la detección automática de un dispositivo electrónico portátil en un punto determinado de un área de acceso para permitir la autenticación e inicio de la aprobación del proceso de pago antes de que el usuario pase a través de dicho punto, ya está divulgada en el documento D2 que se refiere a que los datos formateados pueden ser proporcionados de manera inalámbrica por el dispositivo móvil 102 a un dispositivo de salto adicional a través de WiFi / GPS / Bluetooth / detección celular o cualquier otro método de autodetección. (Pág. 5, Párr. 0031)

En consecuencia, la persona del oficio normalmente versada en la materia, incluiría las instrucciones de autodetección de dispositivos electrónicos portátiles mencionados en documento D2 en las instrucciones del medio legible por computador divulgado en el documento D1 para llegar así al objeto de la reivindicación 21 de la solicitud. Por lo cual se considera obvia.

La reivindicación 22 consiste en: “*Un aparato para permitir pagos de tarifas de rendimientos altos que comprende: (...)*” (Ver página 10 del radicado N° NC2016/0001754 del 20 de diciembre de 2016).

TABLA 4. Comparación de las características técnicas esenciales, con las del estado de la técnica:

Características esenciales	D1	D2
Medios para detectar la presencia de un dispositivo electrónico portátil fuera de un punto de acceso a un área de acceso controlado.	No se menciona.	En una realización alternativa, los datos en formato T1/T2 pueden ser proporcionados de manera inalámbrica por el dispositivo móvil (102) a un dispositivo de salto adicional a través de WiFi/ GPS/ Bluetooth/ Detección celular o cualquier

Oficio N° 1730

Ref. Expediente N° NC2016/0001754

		otro método de autodetección. (Pág. 5, Párr. 0031)
Medios para obtener, de dicho dispositivo electrónico portátil, una indicación que un usuario de dicho dispositivo electrónico portátil se ha autenticado con dicho dispositivo electrónico portátil.	El titular de una tarjeta bancaria puede registrar una tarjeta bancaria con el sistema de procesamiento (300) a través de una interfaz web, utilizando un sistema de respuesta de voz interactiva (IVR), en un quiosco interactivo o usando una máquina expendedora. El sistema de verificación de tarjeta bancaria (600), como las redes de liquidación y compensación utilizadas por las compañías de tarjetas de crédito, verifica que una tarjeta bancaria sea una tarjeta bancaria actualmente válida. (Pág. 4, Párr. 0042).	Inicialmente, un titular de cuenta nuevo o existente (es decir, el usuario consumidor) puede descargar una aplicación o tarjeta de software, tal como la aplicación (127), desde una tienda o servidor de aplicaciones en línea. Tras su uso inicial, la aplicación (127) puede establecer un secreto de datos compartidos con un sistema emisor (por ejemplo, el servidor emisor (106)) a través de una red celular o de Internet. En algunas realizaciones, la aplicación (127) también puede incluir un certificado digital de emisor que permite que la aplicación (127) y el servidor emisor (106) se autenticuen mutuamente durante todo el ciclo de gestión de vida de la aplicación (127). El certificado digital emisor también permite a la aplicación (127) y al servidor emisor (106) mutuamente autenticarse para una transacción de pago (por ejemplo, cuando se utiliza NFC). (Pág.3, Párr. 0020)
Medios para iniciar un proceso de aprobación de pago asociado con una cuenta de dicho usuario, dicho proceso de aprobación de pago se completa antes que dicho usuario busque pasar a través de dicho punto de acceso.	El procesador de registro de presentación (300) está acoplado a una segunda interfaz (1005) para comunicarse con una pasarela de pago (410) para establecer la pluralidad de cuentas de tránsito. De forma similar, la segunda interfaz (1005) puede ser un bus de computadora. La pasarela de pago (410) está acoplada a una red de beneficios de cercanías (430) (por ejemplo, TransitChek®) para comunicar un primer conjunto de transacciones de liquidación (1007). La pasarela de pago (410) también está acoplada a una red (420) de compensación y liquidación de una institución financiera tradicional (por ejemplo, Base-II) para comunicar un segundo conjunto de transacciones de liquidación (1006). La pasarela de pago (410) primero liquida cuentas mediante la aplicación de fondos de la red (430) de beneficios de cercanías. La pasarela de pago (410) a continuación establece el saldo restante con la red (420) de	En una realización, la aplicación (127) puede utilizar la función criptográfica (126) para producir un resultado que puede usarse para autorizar un pago de compra (o alguna otra transacción electrónica) en el punto de venta. En una realización, la función criptográfica (126) puede recibir un número IMEI, un número de cuenta, un número UTV (almacenado en la memoria (124) o recibido en tiempo real) y datos hash para generar una salida como datos formateados de transacciones heredadas (por ejemplo, Datos de T1 y T2 o datos EMV). La aplicación (127) también puede construir una clave 3-DES basada en la contraseña ingresada y los datos secretos de la aplicación provistos previamente. En una realización, una parte de la salida de la función criptográfica (126) se convierte

Oficio N° 1730

Ref. Expediente N° NC2016/0001754

	compensación y liquidación (Pág. 8, Párr. 0079).	en datos de Pista 1 y Pista 2 (por ejemplo, caracteres hexadecimales). En este punto, la salida de la función criptográfica (126) está lista para la transmisión al dispositivo lector (104) cuando el teléfono móvil (102) está interconectado (por ejemplo, NFC) con el dispositivo lector (104). En una realización, al menos una parte del identificador de usuario y un BIN permanece sin encriptar mientras que los datos restantes se encriptan como salida de la función criptográfica (126). (Pág. 26, Párr. 0026)
Medios para, basado en obtener dicha indicación de autenticación y el éxito de dicho proceso de aprobación de pago, suministrar a dicho punto de acceso una ficha electrónica que indica que a dicho usuario, que lleva dicho dispositivo electrónico portátil, se le debe permitir pasar a través de dicho punto de acceso al área de acceso controlado.	Las FIGS. 5A, 5B y 5C muestran el flujo de mensajes entre los componentes de la red, de acuerdo con las realizaciones de la presente invención. En la Fig. 5A, una tarjeta bancaria (100) es presentada actualmente por un titular de la misma (por ejemplo, un viajero de metro o un conductor de autobús). El lector (210) de tarjeta bancaria en el terminal (200) de tarjeta bancaria recibe datos de tarjeta bancaria que comprenden datos de la tarjeta bancaria actualmente presentada. El procesador (220) de terminal de tarjeta bancaria en el terminal (200) de tarjeta bancaria determina un identificador (por ejemplo, un valor hash o un número de tarjeta de crédito) de la tarjeta bancaria presentada. A continuación, el procesador (220) de terminal de tarjeta bancaria usa el identificador determinado para indicar que la tarjeta bancaria presentada actualmente está contenida en el conjunto de registros (230) de tarjeta bancaria. El procesador (220) terminal de tarjeta bancaria señala a la segunda interfaz (260) para comunicarse con el controlador (270) de acceso. El controlador (270) de acceso puede ser, por ejemplo, un conductor, una puerta del torniquete o un conductor de autobús u otro ser humano que proporcione supervisión o control. (Pág. 6, Párr. 0062).	No se menciona
Medios para permitir a dicho usuario, que lleva dicho dispositivo electrónico portátil, pasar a través de	Para ayudar al acceso de puerta, en algunas realizaciones la segunda interfaz (260) puede activar una barrera, mientras que otra segunda	No se menciona

Oficio N° 1730

Ref. Expediente N° NC2016/0001754

dicho punto de acceso a dicha área de acceso controlado, con base en dicha ficha electrónica.	interfaz de realización (260) puede simplemente activar una luz roja o verde observable por un conductor, un operador de puerta y/o el conmutador. La segunda interfaz (260) puede proporcionar una señal para abrir el torniquete. La segunda interfaz (260) puede proporcionar una señal para activar un anuncio de audio y/o visual. Por ejemplo, la segunda interfaz (260) puede enviar una señal a una pantalla LCD o un LED en una unidad portátil que sea observada por un conductor. (Pág. 6, Párr. 0063)	
Medios para hacer que dicha ficha electrónica expire después que dicho usuario pase a través de dicho punto de acceso a dicha área de acceso controlado.	En algunas realizaciones, el primer registro de presentación resulta de una transacción entre un token de identificación y un lector de fichas, en el que el token de identificación no retiene información con respecto a la transacción. En otras realizaciones, la ficha de identificación solo conserva un contador ajustado como resultado de la transacción. De esta manera, los tokens de identificación son realmente sin memoria. (Pág. 9, Párr. 87)	No se menciona

El documento D1 se considera el estado de la técnica más cercano a la invención definida en la reivindicación 22 porque divulga la implementación de un sistema y método para procesar viajes de transferencia asociados con al menos una red de transporte público. El sistema y el método preprocesan transacciones para consolidar o eliminar transacciones innecesarias con una red de compensación y liquidación de una institución financiera. (Pág., 1, Resumen).

La diferencia entre la invención, definida en la reivindicación 22 y el sistema de D1 consiste en que en el aparato de la reivindicación 22 incluye la detección automática de un dispositivo electrónico portátil en un punto determinado de un área de acceso.

El efecto que logra la detección automática de un dispositivo electrónico portátil en un punto determinado de un área de acceso es permitir la autenticación e inicio de la aprobación del proceso de pago antes de que el usuario pase a través de dicho punto de acceso completando así la transacción.

Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así: “¿cómo modificar el sistema conocido en D1 para permitir la autenticación e inicio de la aprobación del proceso de pago antes de que el usuario pase a través de dicho punto de acceso?”.

Sin embargo, la detección automática de un dispositivo electrónico portátil en un punto determinado de un área de acceso para permitir la autenticación e inicio de la aprobación del proceso de pago antes de que el usuario pase a través de dicho punto, ya está divulgada en el documento D2 que se refiere a que los datos formateados pueden ser proporcionados de manera inalámbrica por el dispositivo móvil 102 a un

Oficio N° 1730

Ref. Expediente N° NC2016/0001754

dispositivo de salto adicional a través de WiFi / GPS / Bluetooth / detección celular o cualquier otro método de autodetección. (Pág. 5, Párr. 0031)

En consecuencia, la persona del oficio normalmente versada en la materia, incluiría los métodos de autodetección de dispositivos electrónicos portátiles mencionados en documento D2 en el sistema divulgado en el documento D1 para llegar así al objeto de la reivindicación 22 de la solicitud. Por lo cual se considera obvia.

8. Conclusión

Los requisitos de Patentabilidad de la presente solicitud están afectados así:

Ítem	Documento	Reivindicaciones afectadas	Requisito que afecta
D1	US 2013/325566	1, 6, 9 a 15, 18, 21 y 22.	Nivel Inventivo
D2	US 2013/275307	1 a 8, 16 y 18 a 22	Nivel Inventivo

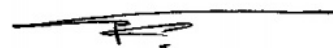
En cumplimiento del artículo 45, de la Decisión 486 de la Comisión de la Comunidad Andina, se le indica que debe dar respuesta dentro del término de sesenta (60) días contados a partir de la fecha de notificación de la presente comunicación. En caso de no dar respuesta al presente requerimiento, o si a pesar de la respuesta subsistieran los impedimentos para la concesión, se denegará la patente.

Si como respuesta a este requerimiento la solicitante llegara a modificar: i) el capítulo reivindicatorio, ii) la descripción de la invención a proteger, iii) o presente un nuevo capítulo reivindicatorio, y desee que se realice un nuevo examen de patentabilidad a esta modificación, no deberá pagar la tasa de modificación voluntaria pero sí la correspondiente a la tasa de examen de patentabilidad. En todo caso, el número de requerimientos por no patentabilidad estará supeditado a que el término del estudio de patentabilidad no sea superior a 18 meses, contados desde la publicación de la solicitud de patente de invención. Adicionalmente, se le recuerda a la solicitante que si como respuesta a este requerimiento llegara a modificar el capítulo reivindicatorio y éste contenga más de diez (10) reivindicaciones deberá pagar la tasa por reivindicación adicional.

Se invita a la solicitante se sirva indicar, si así lo considera, su renuncia al término faltante para los sesenta (60) días.

Notifíquese el presente oficio conforme a lo dispuesto en el Título I, Actuaciones ante la Superintendencia de Industria y Comercio; Capítulo sexto, publicación, comunicación, notificación y ejecutoria de las decisiones de la Superintendencia de Industria y Comercio, informándoles que contra el mismo no procede el recurso de la vía gubernativa.

Atentamente,



JOSÉ LUIS SALAZAR LÓPEZ
DIRECTOR DE NUEVAS CREACIONES (C)

Elaborado: CARLOS EDUARDO GUEVARA NICHÓY

Oficio N° 1730

Ref. Expediente N° NC2016/0001754

Revisado: SONIA ANDREA DÍAZ PIRAZÁN

Aprobado: JOSÉ LUIS SALAZAR LÓPEZ