

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 18756 de 29 de noviembre de 2021

Ref. Expediente N° NC2018/0013079

Señores

RPC REDE PONTO CERTO TECNOLOGIA E SERVIÇOS LTDA

TÍTULO DE LA SOLICITUD: “SISTEMA MÓVIL PARA ACTUALIZACIÓN TRANSACCIONAL DE INFORMACIONES EN CHIPS DEL TIPO SIN CONTACTO”

NUMERO DE SOLICITUD INTERNACIONAL: PCT/BR2017/050171.

FECHA DE PRESENTACIÓN INTERNACIONAL: 30 de junio de 2017.

PRIORIDAD: 4/07/2016, BR (BRASIL), BR1020160156114.

Como resultado del examen de patentabilidad realizado a la solicitud indicada en la referencia, atendiendo a lo consagrado en el artículo 45 de la Decisión 486 de 2000, se le comunica que esta Dirección ha encontrado que la materia objeto de solicitud no cumple con algunos requisitos establecidos en la Decisión, con fundamento en los siguientes aspectos:

1. Modificaciones presentadas

Revisada la modificación a la solicitud objeto de estudio, la cual fue radicada 4 de noviembre de 2021 bajo el número NC2021/0014884, y teniendo en cuenta lo señalado en el artículo 34 de la Decisión 486 de 2000 de la Comisión de la Comunidad Andina, esta oficina acepta las modificaciones presentadas por ajustarse a los requisitos legales.

2. Objeto de la invención

El problema planteado en esta solicitud consiste en la necesidad de suministrar un sistema móvil para realizar transacciones mediante chips del tipo sin contacto a través de dispositivos móviles de forma remota.

Para resolver este problema técnico, la solicitud en estudio proporciona un sistema móvil para actualización transaccional de informaciones en chips del tipo sin contacto", caracterizado por permitir a los usuarios de chips la realización de operaciones transaccionales en tránsito, utilizando un aparato smartphone, tablet, notebook, smartwatch o cualquier otro dispositivo capaz de ejecutar aplicaciones móviles, compuesto por un proceso con 3 macro etapas comprendiendo: - Solicitud del usuario vía aplicación móvil; - Autenticación en el Servidor de la Red Operacional; - Autenticación con la clave del Emisor. Uno de los objetivos de la presente Patente de Invención reside en proveer una alternativa para que los usuarios de chips del tipo sin contacto realicen operaciones transaccionales en tránsito, utilizando un aparato smartphone, tablet o cualquier otro dispositivo capaz de ejecutar aplicaciones móviles. Esto permitirá al usuario total autonomía en el proceso de actualización o consulta del contenido de su chip, eliminando su dependencia con relación a la red de terminales fijos. Otro objetivo de la presente Patente de Invención reside en proveer una solución segura para tráfico de datos entre el dispositivo móvil del usuario y la red de autenticación de las transacciones de compra, atendiendo a las buenas prácticas de seguridad en criptografía de datos por la combinación de múltiples claves criptográficas de modo de garantizar la integridad de las informaciones y mitigar los riesgos de fraude (Resumen).

Oficio N° 18756 de 29 de noviembre de 2021

Ref. Expediente N° NC2018/0013079

3. Reivindicaciones estudiadas

El presente estudio se basa en el capítulo reivindicatorio presentado el 4 de noviembre de 2021.

4. De la solicitud de patente

4.1. Reivindicaciones

Teniendo en cuenta lo establecido en el artículo 30 de la Decisión 486 de 2000 de la Comisión de la Comunidad Andina:

"Las reivindicaciones definirán la materia que se desea proteger mediante la patente. Deben ser claras y concisas y estar enteramente sustentadas por la descripción. (...)"

Esta oficina informa que, el capítulo reivindicatorio carece de números de referencia. Se sugiere 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 la comprensión de la materia reivindicada.

Esta oficina informa que, la frase "código fuente" presente en el capítulo reivindicatorio puede hacer referencia a materia no patentable de acuerdo con la decisión 486. Se sugiere cambiar dicha frase por "instrucciones ejecutadas por computador", con el fin de evitar hacer referencia a materia no patentable.

En consecuencia, es necesario que allegue las aclaraciones o modificaciones correspondientes para dar cumplimiento a lo establecido en el citado artículo.

5. Determinación del Estado de la Técnica

La fecha para determinar el estado de la técnica es el 4 de julio de 2016, que corresponde a la fecha de presentación de la solicitud de prioridad.

Consultadas las fuentes de información con que se cuenta, se encontraron los siguientes documentos que anticipan el objeto de esta solicitud:

Ítem	Documento	Título	Fecha de publicación
D3	WO15061354	"Facilitating secure transactions using a contactless interface"	30 de abril de 2015
D4	US2016125355	"Systems for Secure Tracking Code Generation, Application, and Verification"	5 de mayo de 2016

D3¹ divulga un dispositivo que puede realizar una primera operación de autenticación, asociada con un dispositivo de medios sin contacto, utilizando una primera clave. La primera clave puede permitir modificar un modo de seguridad del dispositivo de medios sin contacto. El dispositivo puede hacer que el dispositivo de medios sin contacto establezca el modo de seguridad en un primer modo de seguridad que hace que el

¹ <https://patentimages.storage.googleapis.com/dc/f5/72/6af7a909ead999/WO2015061354A1.pdf>



Ref. Expediente N° NC2018/0013079

dispositivo de medios sin contacto asegure al menos una transmisión desde el dispositivo de medios sin contacto. El dispositivo puede realizar una segunda operación de autenticación, asociada con el dispositivo de medios sin contacto, utilizando una segunda clave que permite leer o escribir información en el dispositivo de medios sin contacto. El dispositivo puede leer la primera información protegida o escribir una segunda información protegida en el dispositivo de medios sin contacto. La primera información protegida o la segunda información protegida pueden protegerse basándose en el modo de seguridad del dispositivo de medios sin contacto que se establece en el primer modo de seguridad (Resumen).

D4² divulga una plataforma de gestión implementada por ordenador para generar de forma segura códigos de seguimiento y para imprimir de forma verificable esos códigos de seguimiento en artículos físicos. En una realización, uno o más procesadores de hardware generan códigos de seguimiento y envían los códigos de seguimiento a una línea de producción automatizada controlada por computadora, y que imprimen físicamente cada código de seguimiento en un artículo correspondiente, y verifican físicamente la impresión física. . Si un código de seguimiento se imprimió correctamente en su artículo correspondiente, uno o más registros se registran en un medio de almacenamiento duradero, lo que indica que el código de seguimiento se imprimió en un artículo. Si un código de seguimiento se imprimió incorrectamente en su artículo correspondiente, la línea de fábrica rechaza físicamente el artículo correspondiente. Las realizaciones también incluyen la plataforma de gestión implementada por ordenador que gestiona de forma segura esos artículos físicos a lo largo de su ciclo de vida, basándose en los códigos de seguimiento generados de forma segura e impresos de forma verificable (Referencia).

6. Examen de Patentabilidad

De acuerdo con lo establecido en el artículo 14 de la Decisión 486 de 2000 de la Comisión de la Comunidad Andina, en el cual se establecen los requisitos de patentabilidad objeto de la solicitud en estudio, esta Oficina presenta a continuación el análisis de los requisitos de patentabilidad.

6.1. Nivel Inventivo

Teniendo en cuenta lo señalado en el artículo 18 de la Decisión 486 de 2000 de la Comisión de la Comunidad Andina, la reivindicación independiente 1 (NC2021/0014884 del 4 de noviembre de 2021) refiere a: *“Un método para actualizar transaccionalmente la información en un chip de un dispositivo móvil usando un servidor de una red operacional que comprende (...)”*. A continuación, se presenta la tabla comparativa entre el objeto reivindicado y los documentos encontrados en el estado de la técnica:

Tabla 1.

CARACTERÍSTICAS ESENCIALES	D3	D4
Un método para actualizar transaccionalmente la información en un chip de un dispositivo móvil usando un servidor de una red	Facilitar transacciones seguras mediante una interfaz sin contacto (Título).	Sistemas para la generación, aplicación y verificación de código de seguimiento seguro (Título).

² <https://patentimages.storage.googleapis.com/37/3c/1e/af37d247db6c00/US20160125355A1.pdf>

Oficio N° 18756 de 29 de noviembre de 2021

Ref. Expediente N° NC2018/0013079

operacional que comprende.	(...)un método puede incluir realizar, mediante un primer dispositivo, una primera operación de autenticación, asociada con un dispositivo de medios sin contacto, utilizando una primera clave (...) (Pág. 2, líneas 8 a 10). (Pág. 4, líneas 17 a 23).	(...) el sistema de gestión (101) puede comunicarse con más de una instalación de producción, y los puntos suspensivos (104a) indican que el sistema de gestión (101) puede comunicarse con una variedad de dispositivos de gestión (tanto en número como en tipo, como el ilustrado teléfono inteligente, tableta y computadora portátil) (Párr. 0019).
Recibir una solicitud por un usuario a través de una aplicación que corre en un dispositivo móvil para una operación transaccional.	Facilitar transacciones seguras mediante una interfaz sin contacto (Título). (...) Por ejemplo, un usuario puede interactuar con el dispositivo (220) de interfaz (por ejemplo, a través de una aplicación de medios sin contacto que se ejecuta en el dispositivo (220) de interfaz) para proporcionar una entrada que haga que la solicitud se envíe al dispositivo (230) remoto (Pág. 9, líneas 27 a 29).	No menciona.
Leer al información de un chip en respuesta a la solicitud de la aplicación móvil.	(...) El dispositivo (220) de interfaz puede configurarse para leer información de la tarjeta y/o escribir información de la tarjeta en el dispositivo (210) de medios sin contacto en proximidad comunicativa (por ejemplo, dentro de un rango particular, como unos pocos centímetros, diez metros, etc.) del dispositivo (220) de interfaz (Pág. 6, líneas 9 a 14).	Por ejemplo, la unidad de verificación de hardware (111b) puede leer una representación de código legible por máquina del código de seguimiento, puede realizar un reconocimiento óptico de caracteres (OCR) de una representación legible por humanos del código de seguimiento, etc. (...) (Párr. 0031).
Encriptar la información transaccional leída del chip.	El dispositivo (210) de medios sin contacto puede ser capaz de comunicarse utilizando múltiples modos de seguridad, como un modo de alta seguridad (por ejemplo, un modo encriptado, un modo encriptado simétricamente, un modo encriptado asimétricamente, un modo codificado, un modo de texto cifrado, etc.) (Pág. 5, líneas 23 a 28).	Estos códigos de seguimiento pueden estar protegidos criptográficamente por el componente de cifrado (105b) (...) (Párr. 0061).
Transferir la información transaccional encriptada remotamente al servidor de la red operacional.	El dispositivo (210) de medios sin contacto puede comunicar información con otros dispositivos aplicando diferentes protocolos de seguridad (por ejemplo, encriptación, encriptación simétrica, encriptación asimétrica, codificación, codificación de autenticación de mensajes (MAC), etc.) basados en el modo de seguridad (Pág. 5 línea 29 a Pág. 6 línea 2).	No menciona.

Oficio N° 18756 de 29 de noviembre de 2021

Ref. Expediente N° NC2018/0013079

Realizar una autenticación en el servidor de la red operacional.	Como se muestra en el número de referencia (850), suponga que el pago está validado (por ejemplo, por el dispositivo remoto (230) u otro dispositivo, como un servidor de autenticación de pago), y el monto de la transacción (por ejemplo, \$ 50,00) se proporciona al dispositivo remoto (230) (Pág. 22, líneas 17 a 20).	No menciona.
Realizar una autenticación con una primera llave de emisor.	Un dispositivo, que comprende: uno o más procesadores para realizar una primera operación de autenticación, asociado con un dispositivo de medios sin contacto, usando una clave de modo de seguridad; proporcionar una instrucción para hacer que el dispositivo de medios sin contacto establezca un modo de seguridad en un primer modo de seguridad basándose en la realización de la primera operación de autenticación (...) (Reiv. 1).	El componente de cifrado (105b) puede hacer prohibitivamente difícil (es decir, prácticamente imposible) que un tercero descifre los códigos de seguimiento generados por el componente de generación (105a), y los algoritmos utilizados por el componente de generación (105a) para producir los códigos de seguimiento, sin tener acceso a una clave criptográfica utilizada para cifrar los códigos de seguimiento (Pár. 0025).
Actualizar la información en el chip basado en una respuesta transaccional del servidor de la red operacional.	Como muestra el número de referencia (860), el dispositivo remoto (230) escribe un saldo actualizado de la tarjeta en la tarjeta de tarifa. Por ejemplo, el dispositivo remoto (230) puede proporcionar el saldo actualizado de la tarjeta a la tarjeta de tarifa y puede proporcionar una instrucción para actualizar el saldo de la tarjeta almacenado por la tarjeta de tarifa. Debido a que los dispositivos se han autenticado entre sí, la tarjeta de tarifa actualiza el saldo de la tarjeta almacenado (Pág. 22 líneas 22 a 26).	No menciona.
Encriptar, mediante una segunda llave, las llaves de lectura y escritura asociadas con un número de serie del chip en donde la aplicación móvil se compone de un código fuente protegido por una capa de seguridad para evitar la lectura por terceros no autorizados.	(...) una segunda clave que permite al dispositivo escribir la segunda información segura en el dispositivo de medios sin contacto (Reiv. 7) En algunas implementaciones, se puede generar una clave de autenticación a partir de una clave maestra asociada con un dispositivo (210) de medios sin contacto particular (por ejemplo, basado en un identificador de dispositivo, número de serie, firma de memoria, etc. asociado con el dispositivo (210) de medios sin contacto) (Pág. 6, líneas 18 a 0021). No menciona un código fuente protegido por una capa de seguridad para evitar la lectura por terceros no autorizados.	(...) de generación (105a), para cifrar los códigos de seguimiento que son generados por el generador de código (105) utilizando el componente de cifrado (105b), el módulo generador de código (105) puede generar códigos de seguimiento criptográficamente ofuscados que protegen la identidad del código de seguimiento que fue realmente generado por el componente de generación (105a). El componente de cifrado (105b) puede hacer prohibitivamente difícil (es decir, prácticamente imposible) que un tercero descifre los códigos de seguimiento generados por el componente de generación (105a) (...) Por tanto, el componente de cifrado (105b) puede ayudar de manera beneficiosa a evitar que

Oficio N° 18756 de 29 de noviembre de 2021

Ref. Expediente N° NC2018/0013079

		terceros no autorizados produzcan códigos de seguimiento falsificados, o anticipen códigos de seguimiento que puedan utilizarse a continuación, o similares (Párr. 0025).
--	--	---

D3 es considerado como el estado de la técnica más cercano a la invención definida en la reivindicación 1, ya que divulga facilitar transacciones seguras mediante una interfaz sin contacto (Título).

La diferencia entre la invención definida entre la reivindicación 1 y el método divulgado en D3, consiste en que la invención incluye un código fuente protegido por una capa de seguridad para evitar la lectura por terceros no autorizados.

El efecto que se logra al incluir específicamente un código fuente protegido por una capa de seguridad para evitar la lectura por terceros no autorizados es proporcionar mayor seguridad al método de transacciones.

Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así: ¿cómo modificar el método para proporcionar mayor seguridad a las transacciones al método divulgado en D3?

Sin embargo, el incluir un código fuente protegido por una capa de seguridad para evitar la lectura por terceros no autorizados para proporcionar mayor seguridad al método de transacciones, ya está divulgado en D4 que se refiere a: El componente de cifrado (105) b está configurado para implementar uno o más algoritmos de cifrado criptográfico (por ejemplo, clave pública, simétrica, asimétrica, etc.), en cooperación con el componente de generación (105a), para cifrar los códigos de seguimiento que son generados por el generador de código. módulo (105). Como tal, utilizando el componente de cifrado (105) b, el módulo generador de código (105) puede generar códigos de seguimiento criptográficamente ofuscados que protegen la identidad del código de seguimiento que fue realmente generado por el componente de generación (105a). El componente de cifrado (105b) puede hacer prohibitivamente difícil (es decir, prácticamente imposible) que un tercero descifre los códigos de seguimiento generados por el componente de generación (105a), y los algoritmos utilizados por el componente de generación (105a) para producir los códigos de seguimiento, sin tener acceso a una clave criptográfica utilizada para cifrar los códigos de seguimiento. Por tanto, el componente de cifrado (105b) puede ayudar de manera beneficiosa a evitar que terceros no autorizados produzcan códigos de seguimiento falsificados, o anticipen códigos de seguimiento que puedan utilizarse a continuación, o similares (Párr. 0025).

En consecuencia, la persona normalmente versada en la materia estaría motivada a incluir un código fuente protegido por una capa de seguridad para evitar la lectura por terceros no autorizados del D4 en el método de D3, para así llegar al objeto de la reivindicación 1. Por lo cual se considera obvia.

Así mismo, D3 divulga las características de las reivindicaciones dependientes de la siguiente manera:

- Reivindicación 2: En algunas implementaciones, el dispositivo (220) de interfaz puede incluir una memoria de almacenamiento de clave segura, que puede almacenar una o

Oficio N° 18756 de 29 de noviembre de 2021

Ref. Expediente N° NC2018/0013079

más claves de autenticación (por ejemplo, una clave de modo de seguridad, una clave de transacción, etc.) en una ubicación de memoria segura. En algunas implementaciones, se puede generar una clave de autenticación a partir de una clave maestra asociada con un dispositivo 210 de medios sin contacto particular (por ejemplo, basado en un identificador de dispositivo, número de serie, firma de memoria, etc. asociado con el dispositivo 210 de medios sin contacto). De esta manera, un sistema de transacciones puede no verse comprometido si un atacante conoce la clave de autenticación, ya que la clave de autenticación sólo puede funcionar con el dispositivo 210 de medios sin contacto particular con el que está asociada la clave de autenticación (Pág. 6, líneas 18 a 26).

- Reivindicación 3: De esta forma, el dispositivo (220) de interfaz puede proporcionar de forma segura el saldo de la tarjeta con un riesgo reducido de que el saldo de la tarjeta sea interceptado por un dispositivo atacante de terceros (Pág. 20, línea 30 a Pág. 21, línea 2).

- Reivindicación 5: (...) una segunda clave que permite al dispositivo escribir la segunda información segura en el dispositivo de medios sin contacto (Reiv. 7). En algunas implementaciones, se puede generar una clave de autenticación a partir de una clave maestra asociada con un dispositivo (210) de medios sin contacto particular (por ejemplo, basado en un identificador de dispositivo, número de serie, firma de memoria, etc. asociado con el dispositivo (210) de medios sin contacto) (Pág. 6, líneas 18 a 0021). Para un técnico medio versado en la materia resulta implícito que los chips vengan con un número de serie determinado por el agente emisor.

De igual manera, D4 divulga las características de las reivindicaciones dependientes así:

- Reivindicación 4: El componente de cifrado (105) b está configurado para implementar uno o más algoritmos de cifrado criptográfico (por ejemplo, clave pública, simétrica, asimétrica, etc.), en cooperación con el componente de generación (105a), para cifrar los códigos de seguimiento que son generados por el generador de código. módulo (105). Como tal, utilizando el componente de cifrado (105) b, el módulo generador de código (105) puede generar códigos de seguimiento criptográficamente ofuscados que protegen la identidad del código de seguimiento que fue realmente generado por el componente de generación (105a). El componente de cifrado (105b) puede hacer prohibitivamente difícil (es decir, prácticamente imposible) que un tercero descifre los códigos de seguimiento generados por el componente de generación (105a), y los algoritmos utilizados por el componente de generación (105a) para producir los códigos de seguimiento, sin tener acceso a una clave criptográfica utilizada para cifrar los códigos de seguimiento. Por tanto, el componente de cifrado (105b) puede ayudar de manera beneficiosa a evitar que terceros no autorizados produzcan códigos de seguimiento falsificados, o anticipen códigos de seguimiento que puedan utilizarse a continuación, o similares (Párr. 0025).

Las reivindicaciones dependientes 2 a 5 no mencionan alguna característica que, junto con las características de la reivindicación independiente, aporte nivel inventivo al método de la reivindicación 1, por lo cual se considera que carece de nivel inventivo.

Teniendo en cuenta lo señalado en el artículo 18 de la Decisión 486 de 2000 de la Comisión de la Comunidad Andina, la reivindicación independiente 6 (NC2021/0014884 del 4 de noviembre de 2021) refiere a: *“Un método para actualizar transicionalmente actualizar la información en un chip de un dispositivo móvil utilizando un servidor de una*



Oficio N° 18756 de 29 de noviembre de 2021

Ref. Expediente N° NC2018/0013079

red operacional que comprende. (...)”. A continuación, se presenta la tabla comparativa entre el objeto reivindicado y los documentos encontrados en el estado de la técnica:

Tabla 2.

CARACTERÍSTICAS ESENCIALES	D3	D4
Un método para actualizar transicionalmente actualizar la información en un chip de un dispositivo móvil utilizando un servidor de una red operacional que comprende.	Facilitar transacciones seguras mediante una interfaz sin contacto (Título). (...)un método puede incluir realizar, mediante un primer dispositivo, una primera operación de autenticación, asociada con un dispositivo de medios sin contacto, utilizando una primera clave (...) (Pág. 2, líneas 8 a 10). (Pág. 5, líneas 8 a 13).	Sistemas para la generación, aplicación y verificación de código de seguimiento seguro (Título). (...) el sistema de gestión (101) puede comunicarse con más de una instalación de producción, y los puntos suspensivos (104a) indican que el sistema de gestión (101) puede comunicarse con una variedad de dispositivos de gestión (tanto en número como en tipo, como el ilustrado teléfono inteligente, tableta y computadora portátil) (Párr. 0019).
Recibir una solicitud por un usuario a través de una aplicación móvil que corre en un dispositivo móvil para una operación transaccional.	Facilitar transacciones seguras mediante una interfaz sin contacto (Título). Un dispositivo móvil (por ejemplo, un dispositivo móvil que ejecuta una aplicación de tarjeta de tarifa, como una billetera móvil (Pág. 5, líneas 12 a 13). (...) Por ejemplo, un usuario puede interactuar con el dispositivo (220) de interfaz (por ejemplo, a través de una aplicación de medios sin contacto que se ejecuta en el dispositivo (220) de interfaz) para proporcionar una entrada que haga que la solicitud se envíe al dispositivo (230) remoto (Pág. 9, líneas 27 a 29).	No menciona.
Leer información del chip en respuesta a la solicitud de la aplicación móvil.	Un dispositivo móvil (por ejemplo, un dispositivo móvil que ejecuta una aplicación de tarjeta de tarifa, como una billetera móvil (Pág. 5, líneas 12 a 13). (...) El dispositivo (220) de interfaz puede configurarse para leer información de la tarjeta y/o escribir información de la tarjeta en el dispositivo (210) de medios sin contacto en proximidad comunicativa (por ejemplo, dentro de un rango particular, como unos pocos centímetros, diez metros, etc.) del dispositivo (220) de interfaz (Pág. 6, líneas 9 a 14).	Por ejemplo, la unidad de verificación de hardware (111b) puede leer una representación de código legible por máquina del código de seguimiento, puede realizar un reconocimiento óptico de caracteres (OCR) de una representación legible por humanos del código de seguimiento, etc. (...) (Párr. 0031).
Generar una primera llave encriptada para asegurar la integridad de la información transaccional leída del chip.	En algunas implementaciones, se puede generar una clave de autenticación a partir de una clave maestra asociada con un dispositivo (210) de medios sin contacto particular (por ejemplo, basado	No menciona.

Oficio N° 18756 de 29 de noviembre de 2021

Ref. Expediente N° NC2018/0013079

	en un identificador de dispositivo, número de serie, firma de memoria, etc. asociado con el dispositivo (210) de medios sin contacto).	
Encriptar la información transaccional para transferencia remota.	El dispositivo (210) de medios sin contacto puede ser capaz de comunicarse utilizando múltiples modos de seguridad, como un modo de alta seguridad (por ejemplo, un modo encriptado, un modo encriptado simétricamente, un modo encriptado asimétricamente, un modo codificado, un modo de texto cifrado, etc.) (Pág. 5, líneas 23 a 28).	Estos códigos de seguimiento pueden estar protegidos criptográficamente por el componente de cifrado (105b). Además, el módulo generador de código (105) puede producir diferentes codificaciones (por ejemplo, código QR, ASCII, etc.) de cada código de seguimiento usando el componente de codificación (105c) (...) (Párr. 0061).
Transferir la información transaccional encriptada remotamente al servidor de la red operacional	El dispositivo (210) de medios sin contacto puede comunicar información con otros dispositivos aplicando diferentes protocolos de seguridad (por ejemplo, encriptación, encriptación simétrica, encriptación asimétrica, codificación de autenticación de mensajes (MAC), etc.) basados en el modo de seguridad (Pág. 5 línea 29 a Pág. 6 línea 2).	No menciona.
Devolver una respuesta transaccional a la aplicación móvil que corre en el dispositivo móvil por el servidor de la red operacional	El dispositivo (300) puede realizar estos procesos en respuesta a que el procesador (320) ejecute instrucciones de software almacenadas por un medio legible por computadora (Pág. 8, línea 3 a Pág. 9, línea 1). Como se muestra en el número de referencia (850), suponga que el pago está validado (por ejemplo, por el dispositivo remoto (230) u otro dispositivo, como un servidor de autenticación de pago), y el monto de la transacción (por ejemplo, \$ 50,00) se proporciona al dispositivo remoto (230) (Pág. 22, líneas 17 a 20).	No menciona.
Actualizar la información en el chip en base a la respuesta transaccional del servidor en la red operacional.	Como muestra el número de referencia (860), el dispositivo remoto (230) escribe un saldo actualizado de la tarjeta en la tarjeta de tarifa. Por ejemplo, el dispositivo remoto (230) puede proporcionar el saldo actualizado de la tarjeta a la tarjeta de tarifa y puede proporcionar una instrucción para actualizar el saldo de la tarjeta almacenado por la tarjeta de tarifa. Debido a que los dispositivos se han autenticado entre sí, la tarjeta de tarifa actualiza el saldo de la tarjeta almacenado (Pág. 22 líneas 22 a 26).	No menciona.
Utilizar una segunda llave encriptada enlazada a la	(...) una segunda clave que permite al dispositivo escribir la segunda	No menciona.

Oficio N° 18756 de 29 de noviembre de 2021

Ref. Expediente N° NC2018/0013079

transacción para encriptar las llaves de lectura y escritura asociadas con el número de serie del chip y proporcionada por el agente emisor.	información segura en el dispositivo de medios sin contacto (Reiv. 7) En algunas implementaciones, se puede generar una clave de autenticación a partir de una clave maestra asociada con un dispositivo (210) de medios sin contacto particular (por ejemplo, basado en un identificador de dispositivo, número de serie, firma de memoria, etc. asociado con el dispositivo (210) de medios sin contacto) (Pág. 6, líneas 18 a 0021).	
En donde la aplicación móvil comprende un código fuente protegido por una capa de seguridad para evitar la lectura por terceros no autorizados.	No menciona.	(...) de generación (105a), para cifrar los códigos de seguimiento que son generados por el generador de código (105) utilizando el componente de cifrado (105b), el módulo generador de código (105) puede generar códigos de seguimiento criptográficamente ofuscados que protegen la identidad del código de seguimiento que fue realmente generado por el componente de generación (105a). El componente de cifrado (105b) puede hacer prohibitivamente difícil (es decir, prácticamente imposible) que un tercero descifre los códigos de seguimiento generados por el componente de generación (105a) (...) Por tanto, el componente de cifrado (105b) puede ayudar de manera beneficiosa a evitar que terceros no autorizados produzcan códigos de seguimiento falsificados, o anticipen códigos de seguimiento que puedan utilizarse a continuación, o similares (Párr. 0025).

D3 es considerado como el estado de la técnica más cercano a la invención definida en la reivindicación 6, ya que divulga facilitar transacciones seguras mediante una interfaz sin contacto (Título).

La diferencia entre la invención definida entre la reivindicación 1 y el método divulgado en D3, consiste en que la invención incluye un código fuente protegido por una capa de seguridad para evitar la lectura por terceros no autorizados.

El efecto que se logra al incluir específicamente un código fuente protegido por una capa de seguridad para evitar la lectura por terceros no autorizados es proporcionar mayor seguridad al método de transacciones.

Oficio N° 18756 de 29 de noviembre de 2021

Ref. Expediente N° NC2018/0013079

Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así: ¿cómo modificar el método para proporcionar mayor seguridad a las transacciones al método divulgado en D3?

Sin embargo, el incluir un código fuente protegido por una capa de seguridad para evitar la lectura por terceros no autorizados para proporcionar mayor seguridad al método de transacciones, ya está divulgado en D4 que se refiere a: El componente de cifrado (105) b está configurado para implementar uno o más algoritmos de cifrado criptográfico (por ejemplo, clave pública, simétrica, asimétrica, etc.), en cooperación con el componente de generación (105a), para cifrar los códigos de seguimiento que son generados por el generador de código. módulo (105). Como tal, utilizando el componente de cifrado (105) b, el módulo generador de código (105) puede generar códigos de seguimiento criptográficamente ofuscados que protegen la identidad del código de seguimiento que fue realmente generado por el componente de generación (105a). El componente de cifrado (105b) puede hacer prohibitivamente difícil (es decir, prácticamente imposible) que un tercero descifre los códigos de seguimiento generados por el componente de generación (105a), y los algoritmos utilizados por el componente de generación (105a) para producir los códigos de seguimiento, sin tener acceso a una clave criptográfica utilizada para cifrar los códigos de seguimiento. Por tanto, el componente de cifrado (105b) puede ayudar de manera beneficiosa a evitar que terceros no autorizados produzcan códigos de seguimiento falsificados, o anticipen códigos de seguimiento que puedan utilizarse a continuación, o similares (Párr. 0025).

En consecuencia, la persona normalmente versada en la materia estaría motivada a incluir un código fuente protegido por una capa de seguridad para evitar la lectura por terceros no autorizados del D4 en el método de D3, para así llegar al objeto de la reivindicación 6. Por lo cual se considera obvia.

Así mismo, D3 divulga las características de las reivindicaciones dependientes de la siguiente manera:

- Reivindicación 7: En algunas implementaciones, el dispositivo remoto 230 (y/o el dispositivo de interfaz 220) y el dispositivo de medios sin contacto 210 pueden intercambiar una o más claves de modo de seguridad para autenticarse entre sí. Por ejemplo, la operación de autenticación puede incluir un intercambio de claves criptográficas simétricas, un intercambio de claves asimétricas (por ejemplo, mediante criptografía de clave pública, donde cada dispositivo usa una clave privada para descifrar la clave pública), o similares (Pág. 11, líneas 3 a 7).

- Reivindicación 8: Las transacciones anteriores pueden tener lugar mediante comunicaciones seguras (por ejemplo, en el modo de alta seguridad). Cuando se han completado las transacciones, el dispositivo de medios sin contacto y el dispositivo remoto pueden comunicarse nuevamente, a través del dispositivo de interfaz, para autenticarse entre sí usando la clave de modo de seguridad. Después de una autenticación exitosa, el dispositivo remoto (o el dispositivo de interfaz, en algunas implementaciones) puede configurar el dispositivo de medios sin contacto en un modo de baja seguridad para permitir la comunicación con otros dispositivos (Pág. 4, líneas 24 a 29).

De igual manera, D4 divulga las características de las reivindicaciones dependientes así:



Oficio N° 18756 de 29 de noviembre de 2021

Ref. Expediente N° NC2018/0013079

- Reivindicación 8: (...) una segunda clave que permite al dispositivo escribir la segunda información segura en el dispositivo de medios sin contacto (Reiv. 7). En algunas implementaciones, se puede generar una clave de autenticación a partir de una clave maestra asociada con un dispositivo (210) de medios sin contacto particular (por ejemplo, basado en un identificador de dispositivo, número de serie, firma de memoria, etc. asociado con el dispositivo (210) de medios sin contacto) (Pág. 6, líneas 18 a 0021).

Las reivindicaciones dependientes 7 y 8 no mencionan alguna característica que, junto con las características de la reivindicación independiente, aporte nivel inventivo al método de la reivindicación 6, por lo cual se considera que carece de nivel inventivo.

7. Conclusión

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

Ítem	Documento	Reivindicaciones afectadas	Requisito que afecta
D3	WO15061354	1 a 3 y 5 a 8	Nivel inventivo
D4	US2016125355	1, 4, 6 y 8	Nivel inventivo

8. Respuesta a los argumentos del solicitante

Es importante aclarar que los argumentos presentados por el señor solicitante frente a los documentos D1 y D2 son procedentes. Sin embargo, se ha realizado una nueva búsqueda encontrando los documentos D3 y D4 que anticipan el Nivel inventivo de la solicitud como se muestra en el presente Oficio.

El solicitante indica que: *“El solicitante considera que ninguna de las características identificadas en el arte previo corresponde a la aplicación móvil compuesta por un código fuente protegido por una capa de seguridad para evitar la lectura de terceros no autorizados. Si bien D1 anticipa las aplicaciones almacenadas en la CPU del dispositivo móvil, nada en dicha anterioridad enseña incorporar en la aplicación una capa de seguridad para evitar la lectura de terceros no autorizados; de hecho, nada en D1 enseña o sugiere proteger o cifrar la información financiera contenida en la aplicación. Por su parte, D2 enseña cifrar la información desde que sale del dispositivo móvil hasta que llega a la entidad financiera y de regreso, pero nada en D2 enseña o sugiere algún tipo de programa que corresponda a una aplicación y mucho menos un cifrado adaptado directamente sobre el dispositivo móvil”*.

Con respecto a lo anterior se le indica al señor solicitante que el documento D4 menciona *“El componente de cifrado (105) b está configurado para implementar uno o más algoritmos de cifrado criptográfico (por ejemplo, clave pública, simétrica, asimétrica, etc.), en cooperación con el componente de generación (105a), para cifrar los códigos de seguimiento que son generados por el generador de código. módulo (105) (...) Por tanto, el componente de cifrado (105b) puede ayudar de manera beneficiosa a evitar que terceros no autorizados produzcan códigos de seguimiento falsificados, o anticipen códigos de seguimiento que puedan utilizarse a continuación, o similares”* (Párr. 0025). De acuerdo con lo mencionado en el documento D4, la característica técnica esencial es anticipada y junto a lo divulgado por D3, la solicitud no logra superar el requisito de Nivel inventivo. Por lo tanto, se trasladan nuevas objeciones referentes a este requisito como se muestra en el presente Oficio.



Oficio N° 18756 de 29 de noviembre de 2021

Ref. Expediente N° NC2018/0013079

El solicitante indica que: *“La reivindicación 1 claramente se relaciona con “Un método para actualizar transaccionalmente la información en un chip de un dispositivo móvil usando un servidor de una red operacional que comprende (...)” (Resaltado fuera del texto (...)) basa todo su análisis en esta comparación”, “El examinador equipara el método (...) reclamado la presencia de una tarjeta física” y “La interpretación errada de las (...) para poder llevar a cabo la transacción y todo el método subyacente” y “El argumento del examinador de que “D1 es considerado (...) sin contacto (Título).” No tiene sustento, ya que la materia reclamada (...) con una primera llave de emisor”.*

Con respecto a lo anterior es importante aclarar que los argumentos presentados son procedentes frente a los documentos D1 y D2, sin embargo, frente a los Documentos D3 y D4 la solicitud no logra superar el requisito de Nivel inventivo por las razones expuestas anteriormente. Es importante aclararle al señor solicitante que el argumento presentado está orientado mas hacia el uso que se le da a la solicitud. El documento D3 incluye dentro de sus características una aplicación de billetera móvil, por lo que le permite pagar (transferir información) o recibir un pago (recibir y procesar información). De acuerdo con lo anterior y con las divulgaciones de los documentos D3 y D4, las características técnicas esenciales de la solicitud han sido anticipadas y por tal razón se trasladan las objeciones mostradas en el presente Oficio.

Con respecto a lo anterior es importante aclararle al señor solicitante que las tarjetas sin contacto³ son un tipo de tarjetas que utilizan un chip para llevar a cabo procesos y/o procedimientos que usan tecnologías como RFID para intercambiar la información necesaria y protocolos de seguridad que permiten que la transacción se realice. Es importante aclararle al señor solicitante que cuando indica *“El examinador, de manera errónea, equipara el chip de un dispositivo móvil con el chip de una tarjeta inteligente sin contacto y basa todo su análisis en esta comparación”* está haciendo referencia al uso que se le dará al chip y no a las características técnicas esenciales de los chips sin importar su aplicación. Adicionalmente, el documento D3 menciona: *“Un dispositivo móvil (por ejemplo, un dispositivo móvil que ejecuta una aplicación de tarjeta de tarifa, como una billetera móvil”* (Pág. 5, líneas 12 a 13). En este párrafo resulta claro que el documento D3 incluye aplicaciones móviles como una billetera móvil que requiere del chip del teléfono para llevar a cabo las transacciones requeridas. Cabe aclarar que el termino sin contacto, no solo hace referencia a las “tarjetas bancarias”, debido a que los teléfonos inteligentes actuales incluyen tecnologías que permiten este tipo de interacciones. Adicionalmente, el documento D3 divulga *“facilitar transacciones seguras mediante una interfaz sin contacto”* en el título y los sistemas y métodos allí presentados junto a lo divulgado por el documento D4 anticipan el nivel inventivo de la solicitud debido a que los documentos D3 y D4 hacen parte del estado de la técnica y anticipan las características técnicas esenciales de la materia reclamada.

En cumplimiento del artículo 45 de la Decisión 486 de 2000, 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, el solicitante modifica el capítulo reivindicatorio, deberá observar las instrucciones contenidas en el numeral 1.2.2.1.1., del Capítulo Primero del Título X de la Circular Única de esta Superintendencia. De igual forma,

³ https://es.wikipedia.org/wiki/Tarjeta_sin_contacto

Oficio N° 18756 de 29 de noviembre de 2021

Ref. Expediente N° NC2018/0013079

deberá tener presente que de conformidad con el literal a) del numeral 1.2.2.5.1. de la norma ibidem, será necesario acreditar el pago de la tasa por concepto de modificación a solicitudes en trámites, de conformidad con el valor establecido en la resolución de tasas vigentes.

Notifíquese el presente oficio conforme a lo dispuesto en el numeral 6.2 del Capítulo Sexto del Título I de la Circular Única, informándoles que contra el mismo no procede recurso alguno en actuación administrativa.



Edna Marcela Ramirez Orozco
DIRECTORA DE NUEVAS CREACIONES



Oficio N° 18756 de 29 de noviembre de 2021

Ref. Expediente N° NC2018/0013079

INFORME DE BÚSQUEDA
EXAMEN DE PATENTABILIDAD

Solicitud No.		Examen de patentabilidad							
NC2018/0013079		1°		2°	X	3°		Revoca	
Solicitud Internacional No.		Fecha solicitud internacional: (DD/MM/AÑO)							
PCT/BR2017/050171		30 de junio de 2017							
Fecha de determinación estado de la técnica (DD/MM/AÑO)				Prioridad		Presentación			
4/07/2016				X					
Solicitante									
RPC REDE PONTO CERTO TECNOLOGIA E SERVIÇOS LTDA									
Reivindicaciones que no son objeto de búsqueda por:									
Art. 14	-	Art. 15	-	Art. 20	-	Art. 25 (Falta de unidad de invención)		-	

CRITERIOS DE BÚSQUEDA	
Reivindicaciones objeto de búsqueda	1 a 8
Palabras clave utilizadas	chip, update, transaction, third party, smart phone, secure, server, source code, write, read, NFC, encrypt
Clasificaciones utilizadas para la búsqueda	CIP: G06Q 20/32, G06Q 20/34

DOCUMENTOS CONSIDERADOS RELEVANTES (Documentos patente, Literatura no patente (LNP): Artículos, catálogos, etc.)					
Informes de búsqueda / Bases de datos consultadas	N° de solicitud de patente / N° de patente / Autor LNP ⁽¹⁾	Fecha de Publicación /Presentación (DD/MM/AAAA)	Reivindicaciones /Secuencias afectadas	Citas relevantes del estado de la técnica	Categoría del documento citado ⁽²⁾
SIPI	96003406	26/01/2996	-	-	A
WO	US20040127256	1/06/2004	-	-	Y
	US7729986	1/07/2010	-	-	Y
	WO2016076812	19/05/2016	-	-	A
	US2015332247	19/11/2015	-	-	A
Patbase	US2014108786	17/04/2014	-	-	A
	WO15061354	30/04/2015	1 a 3 y 5 a 8	Todo el documento	Y
	US2016125355	05/05/2016	1, 4, 6 y 8	Todo el documento	Y
Epoque	US2006218064	28/09/2006	-	-	A
	CA2844231	14/08/2015	-	-	A

⁽¹⁾ Cita completa literatura no patente (LNP)

Apellido, A. A. (Fecha). Título del artículo. Nombre de la revista. Volumen(Número), pp-pp.

O

Apellido, A. A. (Fecha). Título del artículo. Nombre de la revista. Recuperado de <http://xxxxxxx>.

⁽²⁾ Categorías de documentos citados	
“A” Documento que define el estado general de la técnica no considerado como particularmente relevante.	“T” Documento publicado en fecha posterior a la de presentación o la de prioridad de la solicitud internacional y no entra en conflicto con dicha solicitud, pero puede ser útil para la mejor comprensión del principio o

Oficio N° 18756 de 29 de noviembre de 2021

Ref. Expediente N° NC2018/0013079

“E” Solicitud de patente o patente anterior pero publicada en la fecha de presentación internacional o en fecha posterior. “L” Documento citado para llamar la atención sobre por ejemplo, dudas acerca de una reivindicación de prioridad o para determinar la fecha de publicación de otra cita, siempre van acompañados de una explicación, por la cual se citan. “O” Documento del tipo actas de conferencia, este tipo de documentos siempre estará acompañado por otra letra que indique la pertinencia del documento, por ejemplo, O,X, O,Y o bien O,A. “P” Documento publicado antes de la fecha de presentación internacional pero con posterioridad a la fecha de prioridad reivindicada.	teoría en que se basa la invención, o para demostrar que el razonamiento o los hechos en los que se basa dicha invención son incorrectos. “X” Documento particularmente relevante; la invención reivindicada no puede considerarse nueva o que implique una actividad inventiva por referencia al documento aisladamente considerado. “Y” Documento particularmente relevante; la invención reivindicada no puede considerarse que implique una actividad inventiva cuando el documento se asocia a otro u otros documentos de la misma naturaleza, cuya combinación resulta evidente para un experto en la materia.
Fecha del reporte de búsqueda: (17/11/2021)	
Examinador: JUAN SEBASTIAN RONCANCIO AREVALO	