

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 15465 de 30 de septiembre 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 el 9 de junio de 2021 bajo el número NC2021/0007487, 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).

3. Reivindicaciones estudiadas



Oficio N° 15465 de 30 de septiembre de 2021

Ref. Expediente N° NC2018/0013079

El presente estudio se basa en el capítulo reivindicatorio presentado el 9 de junio 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 *"se compone de un código fuente protegido por una capa de seguridad para evitar la lectura por terceros no autorizados"* presente en las reivindicaciones independientes 1 y 7, hace referencia a materia no patentable de acuerdo con la decisión 486. Se sugiere eliminar esta característica esencial en las reivindicaciones o ubicar dicha característica en el preámbulo de la reivindicación.

Esta oficina informa que, el término *"transicionalmente"* presente en las reivindicaciones independiente 7, al parecer presenta un error de escritura. Se sugiere sustituirlo por el término *"transaccionalmente"* o aclarar la naturaleza de dicho término.

Esta oficina informa que, la frase *"leer al información"* presente en la reivindicación 1, tiene un error de escritura, Se solicita sustituirla por la frase *"leer la información"*.

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
D1	US20040127256	"Mobile device equipped with a contactless smart card reader/writer"	1 de junio de 2004
D2	US7729986	"Smart card transactions using wireless telecommunications network"	1 de julio de 2010

Oficio N° 15465 de 30 de septiembre de 2021

Ref. Expediente N° NC2018/0013079

El documento D1¹ divulga un dispositivo móvil inalámbrico está adaptado para acceder a una red inalámbrica e incluye una ranura para tarjeta de módulo de identificación de suscriptor (SIM) y un módulo de tarjeta inteligente sin contacto conectado eléctricamente a la ranura para tarjeta SIM y, por lo tanto, al teléfono móvil inalámbrico. El módulo de tarjeta inteligente sin contacto está adaptado para recibir y leer información almacenada en la tarjeta inteligente sin contacto y transmitir esta información a una entidad a través del dispositivo móvil inalámbrico y la red inalámbrica. El dispositivo móvil inalámbrico de esta invención se utiliza para realizar transacciones financieras utilizando la tarjeta inteligente sin contacto. Las transacciones financieras incluyen compras presenciales o remotas, pago con efectivo electrónico almacenado en la tarjeta inteligente sin contacto, o pago con la tarjeta inteligente sin contacto a través de una institución financiera, y descarga y almacenamiento de bienes o servicios digitales en la tarjeta inteligente sin contacto (Resumen).

El documento D2² divulga tarjetas inteligentes. Más específicamente, la presente invención se refiere al valor de carga y a realizar compras usando una tarjeta inteligente junto con un teléfono móvil (Col. 1, líneas 22 a 25).

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 (NC2021/0007487 del 9 de junio 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:

CARACTERÍSTICAS ESENCIALES	D1	D2
Un método para actualizar transaccionalmente la información en un chip de un dispositivo móvil usando un servidor de una red operacional que comprende.	(...) un método (...) (Párr. 0008). La institución financiera (112) procesa el pago, actualiza la cuenta del comerciante (...) (Párr. 0027). El dispositivo móvil inalámbrico de esta invención se utiliza para realizar transacciones financieras utilizando la tarjeta inteligente sin contacto (Resumen). (...) enviar (...) a un servidor de autenticación a través de dicha red inalámbrica (...) (Reiv. 19).	Un método (...) (Reiv. 1) Una transacción con tarjeta inteligente permite al consumidor cargar valor en una tarjeta inteligente y realizar compras utilizando una tarjeta inteligente con un teléfono móvil a través de la red de telecomunicaciones. (Resumen). La tarjeta inteligente (18) es típicamente una tarjeta de plástico del tamaño de una tarjeta de crédito ISO 7816 que incluye uno o más circuitos integrados de semiconductores.

¹ <https://patentimages.storage.googleapis.com/53/26/9f/79fed8190258c6/US20040127256A1.pdf>
² <https://patentimages.storage.googleapis.com/9a/e2/e1/c7eb69335ddefc/US7729986.pdf>

Oficio N° 15465 de 30 de septiembre de 2021

Ref. Expediente N° NC2018/0013079

	Para un técnico medio versado en la materia es conocido que una tarjeta sin contacto tenga embebido un chip con información ³ .	También denominadas "tarjetas con chip" (Col. 4, líneas 47 a 49). El servidor (106) incluye hardware y software para procesar transacciones con tarjetas inteligentes y puede ser cualquier ordenador adecuado que implemente cualquier sistema operativo adecuado (Col. 6, líneas 15 a 18).
Recibir una solicitud por un usuario a través de una aplicación que corre en un dispositivo móvil para una operación transaccional.	(...) un primer programa de aplicación asociado con la memoria y la CPU y que está adaptado para recibir y transmitir instrucciones desde el módulo de tarjeta inteligente sin contacto al teléfono móvil inalámbrico y viceversa (Párr. 0007).	No menciona.
Leer la información de un chip en respuesta a la solicitud de la aplicación móvil.	El módulo de tarjeta inteligente sin contacto está adaptado para recibir y leer información almacenada en la tarjeta inteligente sin contacto y transmitir esta información a una entidad a través del dispositivo móvil inalámbrico y la red inalámbrica (Resumen).	A continuación, se solicita al titular de la tarjeta que proporcione información sobre la cuenta. El número de cuenta del usuario (de la cual se retirarán los fondos) puede ser ingresado por el usuario en este punto (en un escenario de financiamiento de banca desde casa) o el número de cuenta de financiamiento puede leerse en la tarjeta inteligente (Col. 8, líneas 15 a 19). La tarjeta inteligente puede programarse con varios tipos de funciones, como una aplicación de valor almacenado, una aplicación de crédito o débito, una aplicación de fidelización, información del titular de la tarjeta, etc. (Col. 4, líneas 53 a 56).
Encriptar la información transaccional leída del chip.	El teléfono móvil (110) cifra la información de la transacción y envía un mensaje al servidor de autenticación (107) a través de la red inalámbrica GSM (90) (...) (Párr. 0027). Para un técnico medio versado en la materia es conocido que una tarjeta sin contacto tenga embebido un chip con información transaccional ⁴ .	(...) las firmas S1, S2 y/o S3 se crean utilizando una clave criptográfica compartida entre la tarjeta y el emisor, datos exclusivos de la transacción actual (incluido el número aleatorio) y datos exclusivos de la tarjeta (Col. 8, líneas 50 a 55). El ARPC es un criptograma que utiliza una clave conocida solo por la aplicación de tarjeta

³ Wolfgang Rankl. Smart Card Applications. Design Models for using and programming smart cards. Wiley. 2007 Disponible en : <https://www.wiley.com/en-us/Smart+Card+Applications%3A+Design+models+for+using+and+programming+smart+cards-p-9780470511947>.
⁴ Wolfgang Rankl. Smart Card Applications. Design Models for using and programming smart cards. Wiley. 2007 Disponible en : <https://www.wiley.com/en-us/Smart+Card+Applications%3A+Design+models+for+using+and+programming+smart+cards-p-9780470511947>.

Oficio N° 15465 de 30 de septiembre de 2021

Ref. Expediente N° NC2018/0013079

		inteligente (Col. 10, líneas 21 y 22).
Transferir la información transaccional encriptada remotamente al servidor de la red operacional.	Usando el lector sin contacto en el teléfono móvil (110), la aplicación de pago en el dispositivo móvil envía los comandos apropiados a la tarjeta inteligente para deducir de la tarjeta inteligente el monto de la compra. El teléfono móvil (110) cifra la información de la transacción y envía un mensaje al servidor de autenticación (107) a través de la red inalámbrica GSM (90) (...) El servidor de autenticación (107) valida la información de la transacción del dispositivo móvil, descifra la información de la transacción y enruta la información de la transacción al servidor de pago (106) a través de la red de comunicación (80) (Párr. 0027). Dispositivo móvil inalámbrico según la reivindicación 13, en el que dichas transacciones financieras entre dicho usuario y dicha entidad son remotas (Reiv. 14).	En el paso (538), la pasarela (106) pasa el mensaje de confirmación al servidor comercial 410 (Col. 12, líneas 29 y 30). (...) La rutina de validación toma el identificador de transacción junto con el mensaje de confirmación cifrado para descifrar el mensaje de confirmación (Col 12, líneas 33 a 35). La figura 3 ilustra un sistema distribuido en el que el lector de tarjetas está presente dentro del teléfono (102) y el procesamiento ocurre en una ubicación remota en el servidor (106) o en otro lugar (Col. 4, líneas 23 a 26).
Realizar una autenticación en el servidor de la red operacional.	(...) un servidor de autenticación a través de la red inalámbrica, y autenticando y enviando la información de compra y el monto de efectivo electrónico por el servidor de autenticación a una cuenta comercial del comerciante en una institución financiera (Párr. 0010).	No menciona.
Realizar una autenticación con una primera llave de emisor.	No menciona.	(...) las firmas S1, S2 y/o S3 se crean utilizando una clave criptográfica compartida entre la tarjeta y el emisor, datos exclusivos de la transacción actual (incluido el número aleatorio) y datos exclusivos de la tarjeta (Col. 8, líneas 50 a 55). El ARPC es un criptograma que utiliza una clave conocida solo por la aplicación de tarjeta inteligente (Col. 10, líneas 21 y 22).

Oficio N° 15465 de 30 de septiembre de 2021

Ref. Expediente N° NC2018/0013079

Y actualizar la información en el chip basado en una respuesta transaccional del servidor de la red operacional.	La institución financiera (112) procesa el pago, actualiza la cuenta del comerciante y envía una confirmación del pago al servidor de pago (106) (Párr. 0027).	Esta validación asegura que cuando se cargue la tarjeta inteligente se actualicen los totales financieros en la tarjeta de seguridad (Col. 11, líneas 54 a 56). La red GSM (202) es un canal de comunicaciones que conecta el teléfono (102), el servidor comercial (410) y el servidor de pago (412), a través de la pasarela (106) (Col. 10, líneas 43 a 46).
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.	Los programas de aplicación primero y segundo pueden almacenarse en la CPU, la tarjeta SIM, una tarjeta SIM externa, la tarjeta inteligente sin contacto o una tarjeta externa (Párr. 0007).	La tarjeta inteligente puede programarse con varios tipos de funciones, como una aplicación de valor almacenado, una aplicación de crédito o débito, una aplicación de fidelización, información del titular de la tarjeta, etc (Col. 4, líneas 53 a 56).

D1 es considerado como el estado de la técnica más cercano a la invención definida en la reivindicación 1, ya que divulga un dispositivo móvil equipado con un lector/escritor de tarjetas inteligentes sin contacto (Título).

La diferencia entre la invención definida entre la reivindicación 1 y el método divulgado en D1, consiste en que la solicitud en estudio incluye la etapa de realizar una autenticación con una primera llave de emisor.

El efecto que se logra al incluir específicamente la etapa de realizar una autenticación con una primera llave de emisor es que se proporciona mayor seguridad al método de transacciones.

Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así: ¿cómo modificar método divulgado en D1 para proporcionar mayor seguridad al método de transacciones.

Sin embargo, el incluir la etapa de realizar una autenticación con una primera llave de emisor para proporcionar mayor seguridad al método de transacciones, ya está divulgado en D2 que se refiere a: (...) las firmas S1, S2 y/o S3 se crean utilizando una clave criptográfica compartida entre la tarjeta y el emisor, datos exclusivos de la transacción actual (incluido el número aleatorio) y datos exclusivos de la tarjeta (Col. 8, líneas 50 a 55). El ARPC es un criptograma que utiliza una clave conocida solo por la aplicación de tarjeta inteligente (Col. 10, líneas 21 y 22).

En consecuencia, la persona normalmente versada en la materia estaría motivada a incluir la etapa de realizar una autenticación con una primera llave de emisor del D2 en el método de D1, para así llegar al objeto de la reivindicación 1. Por lo cual se considera obvia.

Así mismo, D1 divulga las características de las reivindicaciones dependientes de la siguiente manera:

Oficio N° 15465 de 30 de septiembre de 2021

Ref. Expediente N° NC2018/0013079

- Reivindicaciones 3 y 5: La identificación de la tarjeta de pago puede ocurrir a través del número de la tarjeta de pago o mediante una firma de transacción cifrada que solo puede ser descifrada por la institución financiera que emitió la tarjeta de pago. El servidor de autenticación también puede utilizar una contraseña, firma digital o un identificador biométrico, es decir, escaneo de retina, huella digital, características de voz, para autenticar la transacción de pago. El instrumento de autenticación de pago puede estar contenido en la tarjeta inteligente sin contacto, en las tarjetas inteligentes SIM dentro del teléfono móvil 110 o dentro de otra tarjeta inteligente de tamaño completo que necesita ser insertada en una ranura de lector de tarjetas inteligentes (Párr. 0030).

De igual manera, D2 divulga las características de las reivindicaciones dependientes así:

- Reivindicación 2: (...) las firmas S1, S2 y/o S3 se crean utilizando una clave criptográfica compartida entre la tarjeta y el emisor, datos exclusivos de la transacción actual (incluido el número aleatorio) y datos exclusivos de la tarjeta (Col. 8 líneas 50 a 55).

- Reivindicaciones 3 : Las firmas criptográficas son bien conocidas en la técnica y pueden crearse de cualquier manera adecuada. Preferiblemente, las firmas S1, S2 y / o S3 se crean utilizando una clave criptográfica compartida entre la tarjeta y el emisor, datos exclusivos de la transacción actual (incluido el número aleatorio) y datos exclusivos de la tarjeta. Preferiblemente, el número de cuenta de fondos, número de tarjeta, PIN o contraseña, y todas las firmas S1, S2 o S3 están encriptados bajo DES triple de 128 bits entre la SIM y la puerta de enlace de procesamiento, y nuevamente con diferentes claves DES triple de 128 bits entre el procesamiento. pasarela 106 y los sistemas de autenticación de emisor y emisor de fondos (Col. 8, líneas 50 a 60). El teléfono recibe un mensaje de respuesta que incluye una firma criptográfica y una aprobación para cargar. Finalmente, el teléfono valida la segunda firma criptográfica y carga el valor en la tarjeta inteligente (Col. 2, líneas 47 a 51).

- Reivindicación 5: En el paso (316), también se solicita al usuario que introduzca un número de código (número de identificación personal) o contraseña que se introduce en el paso (318). En el paso (320), la tarjeta inteligente emite una solicitud de un número aleatorio desde el servidor de procesamiento (106). Este número aleatorio se utilizará para formar una firma criptográfica dentro de la tarjeta que se puede utilizar para autenticar la tarjeta. El número aleatorio se solicita a la puerta de enlace de procesamiento para mayor seguridad. En el paso (321), se devuelve un número aleatorio adecuado a la SIM en el teléfono. En el paso (326), el SIM envía un comando de inicialización para carga a la tarjeta que contiene el número aleatorio que crea una firma criptográfica S1 y la devuelve al SIM (Col. 8, líneas 28 a 39).

Las reivindicaciones dependientes 2, 3 y 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 7 (NC2021/0007487 del 9 de junio de 2021) refiere a: *“Un método para actualizar transicionalmente actualizar la información en un chip de un dispositivo móvil utilizando 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:



Oficio N° 15465 de 30 de septiembre de 2021

Ref. Expediente N° NC2018/0013079

CARACTERÍSTICAS ESENCIALES	D1	D2
Un método para actualizar transicionalmente actualizar la información en un chip de un dispositivo móvil utilizando un servidor de una red operacional que comprende.	(...) un método (...) (Párr. 0008). La institución financiera (112) procesa el pago, actualiza la cuenta del comerciante (...) (Párr. 0027). El dispositivo móvil inalámbrico de esta invención se utiliza para realizar transacciones financieras utilizando la tarjeta inteligente sin contacto (Resumen). (...) enviar (...) a un servidor de autenticación a través de dicha red inalámbrica (...) (Reiv. 19). Para un técnico medio versado en la materia es conocido que una tarjeta sin contacto tenga embebido un chip con información⁵.	Un método (...) (Reiv. 1) Una transacción con tarjeta inteligente permite al consumidor cargar valor en una tarjeta inteligente y realizar compras utilizando una tarjeta inteligente con un teléfono móvil a través de la red de telecomunicaciones. (Resumen). La tarjeta inteligente (18) es típicamente una tarjeta de plástico del tamaño de una tarjeta de crédito ISO 7816 que incluye uno o más circuitos integrados de semiconductores. También denominadas "tarjetas con chip" (Col. 4, líneas 47 a 49). El servidor (106) incluye hardware y software para procesar transacciones con tarjetas inteligentes y puede ser cualquier ordenador adecuado que implemente cualquier sistema operativo adecuado (Col. 6, líneas 15 a 18).
Recibir una solicitud por un usuario a través de una aplicación móvil que corre en un dispositivo móvil para una operación transaccional	(...) un primer programa de aplicación asociado con la memoria y la CPU y que está adaptado para recibir y transmitir instrucciones desde el módulo de tarjeta inteligente sin contacto al teléfono móvil inalámbrico y viceversa (Párr. 0007).	No menciona.
Leer información del chip en respuesta a la solicitud de la aplicación móvil	El módulo de tarjeta inteligente sin contacto está adaptado para recibir y leer información almacenada en la tarjeta inteligente sin contacto y transmitir esta información a una entidad a través del dispositivo móvil inalámbrico y la red inalámbrica (Resumen). (...) un primer programa de aplicación asociado con la memoria y la CPU y que está adaptado para recibir y transmitir instrucciones desde el módulo de tarjeta inteligente sin contacto al teléfono móvil inalámbrico y viceversa (Párr. 0007).	A continuación, se solicita al titular de la tarjeta que proporcione información sobre la cuenta. El número de cuenta del usuario (de la cual se retirarán los fondos) puede ser ingresado por el usuario en este punto (en un escenario de financiamiento de banca desde casa) o el número de cuenta de financiamiento puede leerse en la tarjeta inteligente (Col. 8, líneas 15 a 19). La tarjeta inteligente puede programarse con varios tipos de funciones, como una aplicación de valor almacenado, una aplicación de crédito o débito, una aplicación de fidelización,

⁵ Wolfgang Rankl. Smart Card Applications. Design Models for using and programming smart cards. Wiley. 2007 Disponible en : <https://www.wiley.com/en-us/Smart+Card+Applications%3A+Design+models+for+using+and+programming+smart+cards-p-9780470511947>

Oficio N° 15465 de 30 de septiembre de 2021

Ref. Expediente N° NC2018/0013079

		información del titular de la tarjeta, etc. (Col. 4, líneas 53 a 56).
Generar una primera llave encriptada para asegurar la integridad de la información transaccional leída del chip.	No menciona.	(...) las firmas S1, S2 y/o S3 se crean utilizando una clave criptográfica compartida entre la tarjeta y el emisor, datos exclusivos de la transacción actual (incluido el número aleatorio) y datos exclusivos de la tarjeta (Col. 8, líneas 50 a 55). El ARPC es un criptograma que utiliza una clave conocida solo por la aplicación de tarjeta inteligente (Col. 10, líneas 21 y 22). Para un técnico medio versado en la materia resulta evidente que encriptar datos se usa para asegurar la integridad de la información.
Encriptar la información transaccional para transferencia remota.	El teléfono móvil (110) cifra la información de la transacción y envía un mensaje al servidor de autenticación (107) a través de la red inalámbrica GSM (90) (...) (Párr. 0027). Dispositivo móvil inalámbrico según la reivindicación 13, en el que dichas transacciones financieras entre dicho usuario y dicha entidad son remotas (Reiv. 14).	(...) las firmas S1, S2 y/o S3 se crean utilizando una clave criptográfica compartida entre la tarjeta y el emisor, datos exclusivos de la transacción actual (incluido el número aleatorio) y datos exclusivos de la tarjeta (Col. 8, líneas 50 a 55). El ARPC es un criptograma que utiliza una clave conocida solo por la aplicación de tarjeta inteligente (Col. 10, líneas 21 y 22). La figura 3 ilustra un sistema distribuido en el que el lector de tarjetas está presente dentro del teléfono (102) y el procesamiento ocurre en una ubicación remota en el servidor (106) o en otro lugar (Col. 4, líneas 23 a 26).
Transferir la información transaccional encriptada remotamente al servidor de la red operacional	Usando el lector sin contacto en el teléfono móvil (110), la aplicación de pago en el dispositivo móvil envía los comandos apropiados a la tarjeta inteligente para deducir de la tarjeta inteligente el monto de la compra. El teléfono móvil (110) cifra la información de la transacción y envía un mensaje al servidor de autenticación (107) a través de la red inalámbrica GSM 90 (...) El servidor de autenticación (107) valida la información de la transacción del dispositivo móvil, descifra la información de la transacción y	En el paso (538), la pasarela (106) pasa el mensaje de confirmación al servidor comercial 410 (Col. 12, líneas 29 y 30). (...) La rutina de validación toma el identificador de transacción junto con el mensaje de confirmación cifrado para descifrar el mensaje de confirmación (Col 12, líneas 33 a 35). La figura 3 ilustra un sistema distribuido en el que el lector de tarjetas está presente dentro del teléfono (102) y el

Oficio N° 15465 de 30 de septiembre de 2021

Ref. Expediente N° NC2018/0013079

	enruta la información de la transacción al servidor de pago (106) a través de la red de comunicación (80) (Párr. 0027). Dispositivo móvil inalámbrico según la reivindicación 13, en el que dichas transacciones financieras entre dicho usuario y dicha entidad son remotas (Reiv. 14).	procesamiento ocurre en una ubicación remota en el servidor (106) o en otro lugar (Col. 4, líneas 23 a 26).
Devolver una respuesta transaccional a la aplicación móvil que corre en el dispositivo móvil por el servidor de la red operacional.	(...)crear un pedido digital que comprende información de compra y dicho número de identificación para dicho dispositivo móvil inalámbrico por dicho servidor comercial; solicitar y recibir autorización de pago del cliente a través de dicho dispositivo móvil inalámbrico (...) (reiv. 22) (...) un primer programa de aplicación asociado con la memoria y la CPU y que está adaptado para recibir y transmitir instrucciones desde el módulo de tarjeta inteligente sin contacto al teléfono móvil inalámbrico y viceversa (Párr. 0007).	Primero, el teléfono envía un mensaje de solicitud de pedido a una computadora servidor comercial y, a cambio, recibe un mensaje de instrucción de compra. El teléfono procesa el mensaje de instrucción de compra localmente y luego envía un mensaje de solicitud de retiro a través de la red de telecomunicaciones a una computadora servidor de pago. La computadora del servidor de pagos envía un mensaje de débito que incluye una firma gráfica criptográfica y una aprobación para debitar la tarjeta inteligente (Col. 2, líneas 54 a 61).
Y actualizar la información en el chip en base a la respuesta transaccional del servidor en la red operacional;	La institución financiera (112) procesa el pago, actualiza la cuenta del comerciante y envía una confirmación del pago al servidor de pago (106) (Párr. 0027).	Esta validación asegura que cuando se cargue la tarjeta inteligente se actualicen los totales financieros en la tarjeta de seguridad (Col. 11, líneas 54 a 56). La red GSM (202) es un canal de comunicaciones que conecta el teléfono (102), el servidor comercial (410) y el servidor de pago (412), a través de la pasarela (106) (Col. 10, líneas 43 a 46).
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.	Los programas de aplicación primero y segundo pueden almacenarse en la CPU, la tarjeta SIM, una tarjeta SIM externa, la tarjeta inteligente sin contacto o una tarjeta externa (Párr. 0007).	La tarjeta inteligente puede programarse con varios tipos de funciones, como una aplicación de valor almacenado, una aplicación de crédito o débito, una aplicación de fidelización, información del titular de la tarjeta, etc (Col. 4, líneas 53 a 56).

D1 es considerado como el estado de la técnica más cercano a la invención definida en la reivindicación 7, ya que divulga un dispositivo móvil equipado con un lector/escritor de tarjetas inteligentes sin contacto (Título).

Oficio N° **15465** de **30 de septiembre de 2021**

Ref. Expediente N° NC2018/0013079

La diferencia entre la invención definida entre la reivindicación 7 y el método divulgado en D1, consiste en que la solicitud en estudio incluye la etapa de generar una primera llave encriptada para asegurar la integridad de la información transaccional leída del chip.

El efecto que se logra al incluir específicamente la etapa de realizar una autenticación con una primera llave de emisor es que se proporciona mayor seguridad al método de transacciones.

Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así: ¿cómo modificar método divulgado en D1 para proporcionar mayor seguridad al método de transacciones.

Sin embargo, el incluir la etapa de generar una primera llave encriptada para asegurar la integridad de la información transaccional leída del chip. para proporcionar mayor seguridad al método de transacciones, ya está divulgado en D2 que se refiere a: (...) las firmas S1, S2 y/o S3 se crean utilizando una clave criptográfica compartida entre la tarjeta y el emisor, datos exclusivos de la transacción actual (incluido el número aleatorio) y datos exclusivos de la tarjeta (Col. 8, líneas 50 a 55). El ARPC es un criptograma que utiliza una clave conocida solo por la aplicación de tarjeta inteligente (Col. 10, líneas 21 y 22).

En consecuencia, la persona normalmente versada en la materia estaría motivada a incluir la etapa de generar una primera llave encriptada para asegurar la integridad de la información transaccional leída del chip. del D2 en el método de D1, para así llegar al objeto de la reivindicación 7. Por lo cual se considera obvia.

Así mismo, D1 divulga las características de las reivindicaciones dependientes de la siguiente manera:

- Reivindicación 9: La identificación de la tarjeta de pago puede ocurrir a través del número de la tarjeta de pago o mediante una firma de transacción cifrada que solo puede ser descifrada por la institución financiera que emitió la tarjeta de pago. El servidor de autenticación también puede utilizar una contraseña, firma digital o un identificador biométrico, es decir, escaneo de retina, huella digital, características de voz, para autenticar la transacción de pago. El instrumento de autenticación de pago puede estar contenido en la tarjeta inteligente sin contacto, en las tarjetas inteligentes SIM dentro del teléfono móvil 110 o dentro de otra tarjeta inteligente de tamaño completo que necesita ser insertada en una ranura de lector de tarjetas inteligentes (Párr. 0030).

De igual manera, D2 divulga las características de las reivindicaciones dependientes así:

- Reivindicación 9: En el paso (316), también se solicita al usuario que introduzca un número de código (número de identificación personal) o contraseña que se introduce en el paso (318). En el paso (320), la tarjeta inteligente emite una solicitud de un número aleatorio desde el servidor de procesamiento (106). Este número aleatorio se utilizará para formar una firma criptográfica dentro de la tarjeta que se puede utilizar para autenticar la tarjeta. El número aleatorio se solicita a la puerta de enlace de procesamiento para mayor seguridad. En el paso (321), se devuelve un número aleatorio adecuado a la SIM en el teléfono. En el paso (326), el SIM envía un comando de inicialización para carga a la tarjeta que contiene el número aleatorio que crea una firma criptográfica S1 y la devuelve al SIM (Col. 8, líneas 28 a 39).



Oficio N° **15465** de **30 de septiembre de 2021**

Ref. Expediente N° NC2018/0013079

La reivindicación dependiente 9 no menciona alguna característica que, junto con las características de la reivindicación independiente, aporte nivel inventivo al método de la reivindicación 7, 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
D1	US20040127256	1, 3, 5, 7 y 9	Nivel inventivo
D2	US7729986	1, 2, 3, 5, 7 y 9	Nivel inventivo

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, 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° 15465 de 30 de septiembre de 2021

Ref. Expediente N° NC2018/0013079

**INFORME DE BÚSQUEDA
EXAMEN DE PATENTABILIDAD**

Solicitud No.		Examen de patentabilidad							
NC2018/0013079		1°		2°		3°		Revoca	X
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 9
Palabras clave utilizadas	Application, device, method, system, portable, transaction, contactless, chips.
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	1, 3, 5, 7 y 9	Todo el documento	Y
	US7729986	1/07/2010	1, 2, 3, 5, 7 y 9	Todo el documento	Y
	WO2016076812	19/05/2016	-	-	A
	US2015332247	19/11/2015	-	-	A
Patbase	US2014108786	17/04/2014	-	-	A
Epoquenet	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 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.		
“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			“X” Documento particularmente relevante; la invención reivindicada no puede considerarse nueva o que implique una actividad inventiva por referencia al documento aisladamente considerado.		

Oficio N° 15465 de 30 de septiembre de 2021

Ref. Expediente N° NC2018/0013079

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.	“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: (25/08/2021)	
Examinador: JUAN SEBASTIAN RONCANCIO AREVALO	