

**REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

Oficio N° 3112

Ref. Expediente N° 16145618

Señor(a)
MASTERCARD INTERNATIONAL INCORPORATED
tmtamayo@gmail.com

Asunto: PATENTE DE INVENCION - PCT

Patente de Invención	PT	Patente de Modelo de Utilidad			
Vía Nacional					
Vía PCT (Fase Nacional)	PCT	Capítulo I	X	Capítulo II	
No. Solicitud Internacional	PCT/US2014/068078				
Fecha de Presentación Internacional	2 de diciembre de 2014				

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	16-145618-0000-0000	2 de junio de 2016
Reivindicaciones:	16-145618-0000-0000	2 de junio de 2016
Reivindicaciones:	16145618	26 de agosto 2016
Reivindicaciones:	16145618	22 de febrero 2018
Dibujos:	16-145618-0000-0000	2 de junio de 2016
Respuesta del solicitante:	16145618	22 de febrero 2018
Prioridad(es):	País: US, ESTADOS UNIDOS DE AMÉRICA Número: 61/910,819 Fecha: 2 de diciembre de 2013	

**REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

Oficio N° 3112

Ref. Expediente N° 16145618

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

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 el 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 25 del capítulo reivindicatorio (Radicado No. 16145618 de 22 de febrero de 2018).

Título de la solicitud: "MÉTODO Y SISTEMA PARA LA TRANSMISIÓN SEGURA DE MENSAJES DEL SERVICIO DE NOTIFICACIÓN A DISTANCIA A DISPOSITIVOS MÓVILES SIN ELEMENTOS DE SEGURIDAD" (Radicado No. 16145618 de 02 de junio de 2016).

El problema planteado en esta solicitud consiste en la necesidad de soluciones técnicas para proporcionar aún más seguridad para la recepción y el almacenamiento de credenciales de pago en un dispositivo móvil que carezca de un elemento de seguridad, así como para proporcionar una mayor seguridad en la transmisión de credenciales de pago a un punto de venta desde el dispositivo móvil durante la realización de una transacción financiera.

Para resolver este problema técnico, la presente divulgación proporciona una descripción de los sistemas y métodos para el procesamiento de mensajes de servicio de notificación a distancia. Un método para recibir y procesar un mensaje de datos que permita realizar una transacción.

El objeto de la presente solicitud se relaciona con la Clasificación Internacional de Patentes (CIP): H04W 12/06, H04W 12/08.

Página 2 de 24

**REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

Oficio N° 3112

Ref. Expediente N° 16145618

5. De la solicitud de patente

Reivindicaciones (Art 30 D 486, Art 22 PCT)

Existe una falsa dependencia de la reivindicación 14 con la(s) predecesora(s), al hacer depender un producto (en este caso el sistema), de un método previo, ocasionando una combinación de categorías de reivindicaciones. Se sugiere corregir dado que la reivindicación 14 es una reivindicación independiente de producto no puede estar relacionada con ninguna reivindicación del método del capítulo reivindicatorio.

6. Determinación del Estado de la Técnica

El estado de la técnica se determinó con base en la fecha de presentación de la prioridad: 2 de diciembre de 2013, y se encontraron los siguientes documentos que anticipan el objeto de esta solicitud:

Ítem	Documento	Título	Fecha de Publicación
D1	US20130262317	"Systems and methods for processing mobile payments by provisioning credentials to mobile devices without secure elements"	3/octubre/2013
D2	JP2013081028	"Communication system, communication device, encryption communication method, and program"	02/mayo/2013
D3	JP2010206762	"Encryption communication system, encryption communication method, transmitting apparatus and receiving apparatus"	16/septiembre/2010

El documento D1¹ divulga un método para generar y aprovisionar credenciales de pago a un dispositivo móvil que carece de un elemento seguro incluye: generar un perfil de tarjeta asociado con una cuenta de pago, donde el perfil de tarjeta incluye al menos credenciales de pago correspondientes a la cuenta de pago asociada y un identificador de perfil; aprovisionamiento, a un dispositivo móvil que carece de un elemento seguro, del perfil de tarjeta generado; recibir, desde el dispositivo móvil, una solicitud de clave, en la que la solicitud de clave incluye al menos un número de identificación móvil (PIN) y el identificador de perfil; usando el PIN móvil; generar una clave de uso único, en la que la clave de uso único incluye al menos el identificador de perfil, un contador de transacción de aplicación y una clave de generación para

1 <https://patentimages.storage.googleapis.com/99/9d/39/acba960244065a/US20130262317A1.pdf>



**REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

Oficio N° 3112

Ref. Expediente N° 16145618

usar en la generación de un criptograma de pago válido para una única transacción financiera; y transmitir la clave de un solo uso generada al dispositivo móvil (Resumen).

El documento D2² divulga un sistema de comunicación, un aparato de comunicación, un método de comunicación criptográfica y un programa. Enviar una variedad de información de forma inalámbrica desde los terminales inalámbricos y recibirlos a través de una pluralidad de estaciones base que se han propuesto. En tales redes, a veces la señal de control a los terminales inalámbricos se transmite de acuerdo con la información recopilada. Por ejemplo, el terminal inalámbrico se instala en el aparato, como varios tipos de sensores y dispositivos, cada terminal inalámbrico transmite información representativa del estado y estado de cada dispositivo (Resumen).

El documento D3³ divulga sistema de comunicación criptográfica, método de comunicación criptográfica, un transmisor y un receptor. Al combinar un método de criptografía de clave común y clave pública, generalmente se conoce un sistema de comunicación de cifrado para proteger la confidencialidad del contenido que se va a transmitir y recibir. Se presenta un documento no de patente 1, un método para compartir de forma segura una clave común utilizando el criptosistema de clave pública. En lo sucesivo, se describe un método para combinar una criptografía de clave común y una criptografía de clave pública para la comunicación de cifrado (Resumen).

7. Examen de Patentabilidad (Art. 14 D486)

Novedad (Art 16 D486)

La reivindicación 1 consiste en: *“Un método para recibir y procesar un mensaje de datos, el método caracterizado porque comprende (...)”* (Radicado No. 16145618 de 22 de febrero de 2018).

Tabla 1. Comparación de las Características Técnicas Esenciales con las del estado de la Técnica.

Características Esenciales	D1	D2	D3
Un método para recibir y procesar un mensaje de datos.	La descripción proporciona una descripción de un presente	La presente invención se refiere a un sistema de comunicación, un aparato de comunicación, un	Sistema de comunicación de cifrado, método de comunicación de cifrado,

2 <https://patentimages.storage.googleapis.com/42/62/3e/c312f34fcae427/JP2013081028A.pdf>

3

<https://worldwide.espacenet.com/publicationDetails/originalDocument?CC=JP&NR=2010206762A&KC=A&FT=D&ND=&date=20100916&DB=&locale=>

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 3112

Ref. Expediente N° 16145618

	sistema y métodos para la provisión de credenciales de pago a dispositivos móviles que carecen de elementos seguros para su uso en transacciones de pago móviles. (Fl. 21, Pág. 1, Párr. 0006). El servicio de gestión de credenciales de pago (112) puede generar un mensaje que incluye la clave de uso único cifrada con una clave aleatoria a proporcionar y puede encriptar el mensaje usando la clave móvil. (Pág. 5, Párr. 0059)	método de comunicación criptográfica y un programa (Pág. 2, Párr. 0001).	aparato de transmisión y aparato receptor (Título).
Almacenar, en una memoria, una llave de cifrado	Adicionalmente, "El sistema informático (1900) también puede incluir una memoria principal (1908) (por ejemplo, memoria de acceso aleatorio, memoria de solo lectura, etc.), y también puede incluir una memoria secundaria (1910). La memoria secundaria (1910) puede incluir la unidad de disco duro (1912) y una extraíble unidad de almacenamiento (1914), como una unidad de disquete, una unidad de cinta magnética, una unidad de disco óptico, una memoria flash, etc." (Pág. 13, Párr. 150).	Además, para la reducción de costos, capacidad de almacenamiento de datos en el terminal inalámbrico (memoria, ya sea volátil, como la duración de la batería), la capacidad de actualización de claves, la red se construye utilizando un dispositivo de capacidad de procesamiento aritmético pobre (Pág. 2, Párr. 0003).	(1) es un diagrama bloques que muestra una configuración de un sistema de comunicación cifrado de acuerdo con una realización de la presente invención. La figura 4 es un diagrama que muestra un ejemplo de una tabla almacenada en un dispositivo de almacenamiento (Traducción, Párr. 0024).
Recibir, mediante un dispositivo de recepción, un mensaje de datos, en donde el mensaje de datos incluye un mensaje cifrado y un código de autenticación del mensaje, en donde el	Método según la reivindicación 1, en el que aprovisionar el perfil de tarjeta generado al dispositivo móvil puede incluir construir un mensaje que incluye el perfil de	La figura 2 es un diagrama que muestra una estructura de datos en cada capa cuando el terminal inalámbrico (10) y el dispositivo de estación base (20) transmiten datos de	Cuando se notifica el número aleatorio al dispositivo receptor (2) desde el dispositivo transmisor (1), la firma del dispositivo transmisor (1) se agrega al mensaje que incluye el número aleatorio,

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 3112

Ref. Expediente N° 16145618

código de autenticación del mensaje se genera usando una parte del mensaje cifrado antes de descifrar el mensaje cifrado	tarjeta generado, generar una clave de cifrado, encriptar el mensaje usando la clave de cifrado generada y aprovisionar el mensaje cifrado al dispositivo móvil. (Fl.34, Pág. 14, Reivindicación 4). Método según la reivindicación 1, en el que la transmisión de la clave de uso único generada al dispositivo móvil puede incluir construir un mensaje que incluye la clave de uso único generada, generar una clave de cifrado, encriptar el mensaje usando la clave de cifrado generada y aprovisionar el mensaje cifrado al dispositivo móvil. (Fl.34, Pág. 14, Reivindicación 5).	usuario. Los datos de usuario generados por diversas aplicaciones de la capa de aplicación (la séptima capa en el modelo de referencia OSI) son datos transmitidos desde el terminal inalámbrico (10) o datos transmitidos al terminal inalámbrico (10). Capa 3 (tercera capa en el modelo de referencia OSI: en lo sucesivo también descrito como "L 3"). En el proceso de la capa CNT (control), el número de secuencia de seguridad y el encabezado L3 se agregan a los datos del usuario y, una vez encriptada la parte de datos del usuario, el código de autenticación de mensajes (MAC) se cifra según los datos de usuario cifrados: Código de autenticación de mensaje) se genera y agrega a los datos de usuario cifrados (Cifrado y MAC). El encabezado L3 contiene la longitud de los datos y la información sobre el tipo de mensaje. Además, el código de autenticación de mensaje es información para detectar la falsificación de datos en el lado de recepción. A continuación, los datos que incluyen un número de secuencia de seguridad, un encabezado L3, datos de usuario encriptados (en lo sucesivo denominados "datos de usuario encriptados") y un código de autenticación de mensaje se describen	y el dispositivo receptor (2) autentica el dispositivo transmisor (1) verificando la firma. Por el contrario, cuando el dispositivo receptor (2) notifica el número aleatorio al dispositivo transmisor (1), la firma del dispositivo receptor (2) se agrega al mensaje que incluye el número aleatorio, y el dispositivo transmisor (1) autentica el dispositivo receptor (2) verificando la firma (Traducción, Párr. 0033).
--	--	--	---

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 3112

Ref. Expediente N° 16145618

		como datos L3 (Pág. 16, Párr. 0034)	
Generar, mediante un dispositivo de procesamiento, un código de autenticación de referencia, utilizando una parte del mensaje cifrado incluido en el mensaje de datos recibido antes de descifrar el mensaje cifrado.	Un método para generar y aprovisionar credenciales de pago a un dispositivo móvil que carece de un elemento seguro incluye: generar, por un dispositivo de procesamiento, un perfil de tarjeta asociado con una cuenta de pago, donde el perfil de tarjeta incluye al menos credenciales de pago correspondientes a un identificador de perfil; aprovisionar, a un dispositivo móvil, el perfil de tarjeta generado; recibir, desde el dispositivo móvil, una solicitud de clave, en la que la solicitud de clave incluye al menos un número de identificación móvil (PIN) y el identificador de perfil; utilizando, mediante un dispositivo de autenticación, el PIN móvil; generar, por el dispositivo de procesamiento, una clave de uso único, en la que la clave de uso único incluye al menos el identificador de perfil, un contador de transacción de aplicación y una clave generadora para usar en la generación de un criptograma de pago válido para una única transacción financiera; y transmitir, mediante un dispositivo transmisor, la clave de	Un primer dispositivo de comunicación y el segundo aparato de comunicación, un sistema de comunicación que comunica utilizando una primera información de autenticación compartida para compartir la información de autenticación, donde el primer dispositivo de comunicación, cada vez dicha primera información de autenticación compartida el intercambio de autenticación entre dicho segundo aparato de comunicación, así como genera y transmite información de autenticación del lado de transmisión desde la primera información de autenticación compartida a dicho segundo dispositivo de comunicación; la segunda recibe la información de autenticación del dispositivo de comunicación, unidad de control de autenticación del lado transmisor para autenticar la información de autenticación del lado de recepción utilizando la primera información de autenticación compartida (Reiv. 1).	Con el fin de lograr el objeto anterior, el sistema de comunicación criptográfica de la presente invención tiene un primer dispositivo de comunicación que transmite contenido y un segundo dispositivo de comunicación que recibe el contenido del primer dispositivo de comunicación. Uno de los dispositivos de comunicación agrega una firma cifrada basada en un número aleatorio para ser notificado al otro dispositivo de comunicación a un mensaje que incluye un número aleatorio para ser notificado al otro dispositivo de comunicación y transmite la firma encriptada al otro dispositivo de comunicación. Verifica la firma sobre la base del número aleatorio incluido en el mensaje recibido y causa adicionalmente que el otro aparato de comunicación transmita un mensaje que incluye un número aleatorio para ser notificado al único aparato de comunicación al aparato de comunicación y un número aleatorio para ser notificado al otro aparato de comunicación y un número aleatorio ya notificado de un aparato de comunicación, y transmite el cifrado de firma al aparato de comunicación uno, y el aparato de comunicación único transmite el número aleatorio incluido en el mensaje recibido y se mantiene El primer



REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 3112

Ref. Expediente N° 16145618

	uso único generada al dispositivo móvil, en la que no se requiere que el dispositivo móvil tenga un elemento seguro (Pág. 1, Párr. 0007).		dispositivo de comunicación y el segundo dispositivo de comunicación comparten el número aleatorio notificado al dispositivo asociado y el número aleatorio notificado del dispositivo asociado entre sí verificando la firma sobre la base del primer número aleatorio y el segundo número aleatorio, 1 dispositivo de comunicación transmite contenido cifrado con una clave de sesión generada utilizando una pluralidad de números aleatorios compartidos al segundo dispositivo de comunicación, y el segundo el dispositivo de comunicación transmite el número aleatorio compartido al segundo dispositivo de comunicación Y descifra el contenido recibido del primer dispositivo de comunicación con la clave de sesión generada usando el primer dispositivo de comunicación (D3, Traducción, Párr. 0019).
Validar, mediante el dispositivo de procesamiento, el mensaje de datos recibido basándose en una comprobación del código de autenticación del mensaje incluido en el mensaje de datos recibido contra el código de autenticación de referencia generado.	Un método para generar un código de validación de tarjeta dinámico en un dispositivo móvil que carece de un elemento seguro incluye: recibir, por un dispositivo receptor, al menos una clave de almacenamiento, un componente de autenticación y credenciales de pago estáticas; recibir, por un dispositivo de entrada, al menos una credencial adicional; generar, mediante un	El aparato de estación base (20) autentica el autenticador del terminal recibido (Resumen). Además, la unidad de control de autenticación (104) realiza cálculos basados en MAC-ID, NET-ID, la información de clave de autenticación, el número aleatorio para autenticación NW, el número aleatorio para autenticación de terminal, etc., y realiza la autenticación NW Y verifica el aparato de estación base (20) comparando	Una vez completada la autenticación mutua mediante el certificado de clave pública, el aparato de transmisión genera la clave de cifrado de contenido del método de cifrado de clave común para encriptar el contenido. Además, el dispositivo de transmisión crea una firma que se utilizará para aclarar al emisor y confirmar que no se está realizando ninguna manipulación. El dispositivo de transmisión encripta la clave de cifrado de contenido generado con la clave pública del dispositivo

REPÚBLICA DE COLOMBIA

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 3112

Ref. Expediente N° 16145618

	dispositivo de procesamiento, un token de programa de autenticación de chip (CAP), en el que el token de CAP se basa en al menos el componente de autenticación y la al menos una credencial adicional; transmitir, mediante un dispositivo transmisor, el token CAP generado; recibir, por el dispositivo receptor, una carga útil encriptada, en el que la carga útil encriptada incluye al menos un código de validación de tarjeta dinámica suministrado, número impredecible de clave de sesión y contador de transacción de aplicación; (...) (Pág. 1, Párr. 0010).	(comprobando) con el vecindario de datos (Pág. 17, Párr. 0040).	receptor y encripta la firma con la clave secreta del dispositivo transmisor. El aparato de transmisión agrega una firma cifrada a la clave de cifrado de contenido cifrado y transmite la clave de cifrado de contenido cifrado al aparato de recepción (Traducción Párr. 0004).
Descifrar, mediante el dispositivo de procesamiento, el mensaje cifrado incluido en el mensaje de datos recibido, utilizando la llave de cifrado almacenada, para obtener un mensaje descifrado.	almacenar, en una base de datos, al menos una llave de almacenamiento, una pluralidad de llaves de código de validación dinámicas y un contador de transacciones de aplicaciones asociado con un programa de aplicación móvil; suministro, al dispositivo móvil, al menos la clave de almacenamiento, un componente de autenticación y credenciales de pago estáticas, en el que las credenciales de pago estáticas están asociadas con una cuenta de pago; recibir, desde un dispositivo	Una unidad de generación del contador del lado de recepción para actualizar el contador en la unidad de almacenamiento del lado de recepción cada vez que recibe los datos convertidos, una unidad de generación del contador del lado de recepción para recibir los datos cifrados recibidos por la unidad de procesamiento de recepción del contador Y una unidad de descifrado que descifra los datos descifrados mediante un proceso de descifrado que corresponde al proceso de cifrado predeterminado utilizando la clave de cifrado. Por ejemplo, cuando el primer dispositivo	Al recibir la clave de cifrado de contenido cifrado y la firma encriptada del dispositivo de transmisión, el dispositivo de recepción descifra primero la firma encriptada con la clave pública del dispositivo de transmisión y la verifica. Tras la verificación exitosa de la firma, el dispositivo receptor descifra la clave de cifrado de contenido cifrado con la clave secreta del dispositivo receptor y adquiere la clave de cifrado de contenido (Traducción, Párr. 0005).

**REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

Oficio N° 3112

Ref. Expediente N° 16145618

	móvil, un token de programa de autenticación de chip (CAP); validar, mediante un dispositivo de validación, la autenticidad del token CAP recibido; generar, por un dispositivo de procesamiento, un número impredecible de clave de sesión (KSUN); generando, por el dispositivo de procesamiento, un número impredecible de nubes (UNCLOUD); identificando, mediante el dispositivo de procesamiento (...) (Pág. 1, Párr. 0009).	comunicación corresponde al terminal inalámbrico (10) de la realización y el segundo dispositivo de comunicación corresponde al dispositivo de estación base (20) de la realización, la unidad de control de autenticación del lado de la transmisión notifica a la unidad de control de autenticación (104) del terminal inalámbrico (10) (Pág. 4, Párr. 0008).	
--	--	--	--

De acuerdo con la tabla anterior, las características esenciales del método de la reivindicación 1 habían sido divulgadas previamente en el documento D1, por lo tanto, la materia reivindicada no es nueva.

En consecuencia, la reivindicación 1 no es nueva, según lo divulgado en el documento D1.

Asimismo, los documentos D1, D2 y D3 divulgan las características de las reivindicaciones dependientes así:

- Reivindicación 2: Además, de acuerdo con la presente realización, en la notificación del número aleatorio después del segundo tiempo entre el dispositivo de transmisión y el dispositivo de recepción, no solo el número aleatorio a notificar, el número aleatorio notificado desde el dispositivo asociado o el número aleatorio desde la autenticación se realiza utilizando la firma cifrada utilizando el número aleatorio ya notificado al dispositivo asociado, se puede realizar la autenticación con mayor seguridad en comparación con la autenticación bidireccional simple (D 3, Traducción, Párr. 0166). La unidad de recepción de datos de recepción (105b) recibe los datos de comunicación de enlace descendente transmitidos desde el dispositivo terminal (50) por la unidad de comunicación (101) a través de la red (60), y descifra los datos de usuario cifrados incluidos en los datos de comunicación de enlace descendente. Cuando la información de identificación que indica el destino de la transmisión se establece en los datos de comunicación de

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 3112

Ref. Expediente N° 16145618

enlace descendente, MAC-ID se utiliza sin utilizar NET-ID. Por ejemplo, la unidad de obtención de datos recibida (105) recibe, desde el aparato de estación base (20), la asignación de ancho de banda incluyendo el MAC-ID asignado a sí mismo y sin incluir el NET-ID, y de acuerdo con esta notificación, la unidad de obtención de datos recibida (105b) del enlace descendente pueden recibirse en la banda. La unidad de adquisición de datos recibida (105b) emite los datos de usuario incluidos en los datos de comunicación de enlace descendente de adquisición al dispositivo externo Z (D2, Pág. 18, Párr. 0046).

- Reivindicación 3: La unidad de procesamiento de transmisión de capa 3 (110) incluye una unidad de generación de contador (111), una unidad de almacenamiento (112), una unidad de asignación de número de secuencia de seguridad (113), una unidad de encriptado (114) y una unidad de asignación de código de autenticación de mensaje (115) (D2, Pág. 18, Párr. 0048).
- Reivindicación 4: Además, de acuerdo con esta realización, la notificación del segundo y siguientes números aleatorios en los que un aparato transmisor y un aparato receptor se notifican mutuamente un número aleatorio entre sí, no solo el número aleatorio a notificar, el número aleatorio o más notificado desde la otra unidad, ya que se autentica utilizando una firma cifrada utilizando el número aleatorio y notifica al dispositivo asociado que puede realizar una mayor seguridad de autenticación que simplemente para autenticar cada uno bidireccional (D3, Traducción, Párr. 0166).
- Reivindicación 5: Para “**realizar**”: Con el fin de lograr el objeto anterior, el sistema de comunicación criptográfica de la presente invención tiene un primer dispositivo de comunicación que transmite contenido y un segundo dispositivo de comunicación que recibe el contenido del primer dispositivo de comunicación.

Para “**generar**”: Uno de los dispositivos de comunicación agrega una firma cifrada basada en un número aleatorio para ser notificado al otro dispositivo de comunicación a un mensaje que incluye un número aleatorio para ser notificado al otro dispositivo de comunicación y transmite la firma encriptada al otro dispositivo de comunicación.

Para “**Cifrar**”: Verifica la firma sobre la base del número aleatorio incluido en el mensaje recibido y causa adicionalmente que el otro aparato de comunicación transmita un mensaje que incluye un número aleatorio para ser notificado al único aparato de comunicación al aparato de comunicación y un número aleatorio para

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 3112

Ref. Expediente N° 16145618

ser notificado al otro aparato de comunicación y un número aleatorio ya notificado de un aparato de comunicación.

Para “**Generar**”: y transmite el cifrado de firma al aparato de comunicación uno, y el aparato de comunicación único transmite el número aleatorio incluido en el mensaje recibido y se mantiene.

Para “**Notificar**”: El primer dispositivo de comunicación y el segundo dispositivo de comunicación comparten el número aleatorio notificado al dispositivo asociado y el número aleatorio notificado del dispositivo asociado entre sí verificando la firma sobre la base del primer número aleatorio y el segundo número aleatorio, el dispositivo de comunicación transmite contenido cifrado con una clave de sesión generada utilizando una pluralidad de números aleatorios compartidos al segundo dispositivo de comunicación, y el segundo el dispositivo de comunicación transmite el número aleatorio compartido al segundo dispositivo de comunicación Y descifra el contenido recibido del primer dispositivo de comunicación con la clave de sesión generada usando el primer dispositivo de comunicación (D3, Traducción, Párr. 0019).

- Reivindicación 6: En la etapa (1506), se puede recibir una solicitud de clave desde el dispositivo móvil 104, en donde la solicitud de clave incluye al menos un número de identificación personal móvil (PIN) y el identificador de perfil. En la etapa (1508), un dispositivo de autenticación (por ejemplo, del servicio de gestión de credenciales de pago 112) puede usar el PIN móvil. En una realización, el dispositivo de autenticación puede usar el PIN móvil usando un método XOR. En la etapa (1510), el dispositivo de procesamiento puede generar una clave de uso único (por ejemplo, la clave de uso único 118), donde la clave de uso único (118) incluye al menos el identificador de perfil, un contador de transacción de aplicación y una clave generadora para su uso en generar un criptograma de pago válido para una sola transacción financiera. En algunas realizaciones, la clave de uso único (118) puede ser genuina si el PIN móvil se autentica satisfactoriamente en la etapa (1508), y falso si el PIN móvil se autentica sin éxito. En una realización, el método (1500) puede incluir además la transmisión de la clave (118) de uso único generada a un emisor asociado con la cuenta de pago. En algunas realizaciones, la clave (118) de uso único generada puede estar inactiva. (D1, Pág. 11, Párr. 0128).
- Reivindicación 7: En la etapa (1212), el mensaje de recepción puede ser recibido por el servicio de gestión de credenciales de pago (112) y puede ser descifrado usando la clave de sesión móvil y validada. Tras la validación exitosa, en el paso

Página 12 de 24

**REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

Oficio N° 3112

Ref. Expediente N° 16145618

(1214), el servicio de gestión de credenciales de pago (112) puede activar la clave de uso único (118) y puede actualizar el perfil de usuario en consecuencia. En la etapa (1216), el servicio de gestión de credenciales de pago (112) puede transmitir una notificación a la aplicación de pago móvil (106) de que la clave de uso único (118) se ha activado y puede borrar la clave de sesión móvil. En la etapa (1218), el servicio de gestión de credenciales de pago (112) puede sincronizar el perfil de usuario que indica la activación de la clave de uso único (118) con el emisor (108) para la gestión del fraude. (D1, Pág. 10, Párr. 0111).

En la etapa (508), el sistema SE remoto (110) puede transmitir el perfil de tarjeta (116) al dispositivo móvil (104). En una realización, el dispositivo móvil (104) puede recibir un mensaje de notificación remota para notificar al usuario (102) que la aplicación de pago móvil (106) debe conectarse con el sistema de SE remoto (110) que usa autenticación mutua (404). Una vez conectado, el sistema de SE remoto (110) puede transmitir el perfil de tarjeta que incluye credenciales de pago para la cuenta especificada por el usuario (102) en el paso (502), que luego puede ser almacenado por el pago móvil aplicación (106) en la base de datos cifrada local (304). (D1, Pág. 6, Párr. 0068).

- Reivindicación 8, 9, 10: El método de la reivindicación 11, donde recibir el perfil de tarjeta puede incluir recibir un mensaje cifrado que incluye el perfil de tarjeta, generar una clave de sesión móvil y descifrar el mensaje usando la clave de sesión móvil generada para obtener el perfil de tarjeta incluido. El método de la reivindicación 11, donde recibir la clave de uso único puede incluir recibir un mensaje cifrado que incluye la clave de uso único, generar una clave de sesión móvil y descifrar el mensaje usando la clave de sesión móvil generada para obtener la clave de uso único incluida. (D1, Pág. 15, Reivindicaciones 13 y 14).
- Reivindicación 11, 12 y 13: Un método para generar y aprovisionar credenciales de pago a un dispositivo móvil que carece de un elemento seguro, que comprende: generar, por un dispositivo de procesamiento, un perfil de tarjeta asociado con una cuenta de pago, en el que el perfil de tarjeta incluye al menos credenciales de pago correspondientes a la cuenta de pago asociada y un identificador de perfil; aprovisionar, a un dispositivo móvil, el perfil de tarjeta generado; recibir, desde el dispositivo móvil, una solicitud de clave, en el que la solicitud de clave incluye al menos un número de identificación personal móvil (PIN) y el identificador de perfil; utilizando, mediante un dispositivo de autenticación, el PIN móvil; generar, por el dispositivo de procesamiento, una sola tecla uso, en el que la tecla de un solo uso incluye al menos el identificador de perfil, un contador de transacción de aplicación, y una clave de generación para su uso en la generación de un criptograma de pago

Página 13 de 24

REPÚBLICA DE COLOMBIA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 3112

Ref. Expediente N° 16145618

válida para una sola transacción financiera; y transmitir, mediante un dispositivo de transmisión, la clave de uso único generada al dispositivo móvil, en la que no se requiere que el dispositivo móvil tenga un elemento seguro (D1, Pág. 14, Reivindicación 1).

Las reivindicaciones dependientes 2 a 13 no mencionan alguna característica que, junto con las características de la reivindicación independiente, aporten novedad al método de la reivindicación 1, por lo cual se considera que no son nuevas.

La reivindicación 14 consiste en: *“Un sistema para llevar a cabo el método de la reivindicación 1, el sistema caracterizado porque comprende: una memoria configurada para almacenar una llave de cifrado; (...)”* (Radicado No. 16145618 del 22 de febrero de 2018).

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

Características Esenciales	D1	D2	D3
Memoria configurada para almacenar una llave de cifrado.	El sistema informático (1900) también puede incluir una memoria principal (1908) (por ejemplo, memoria de acceso aleatorio, memoria de solo lectura, etc.), y también puede incluir una memoria secundaria (1910) (Párr. 150).	Además, para la reducción de costos, capacidad de almacenamiento de datos en el terminal inalámbrico (memoria, ya sea volátil, como la duración de la batería) (Pág. 2, Párr. 0003).	(1) es un diagrama bloques que muestra una configuración de un sistema de comunicación cifrado de acuerdo con una realización de la presente invención. La figura 4 es un diagrama que muestra un ejemplo de una tabla almacenada en un dispositivo de almacenamiento (Traducción, Párr. 0024).
Un dispositivo de recepción configurado para recibir un mensaje de datos, en donde el mensaje de datos incluye un mensaje cifrado y un código de autenticación del mensaje, en donde el código de autenticación del mensaje se genera utilizando una parte del mensaje cifrado antes de descifrar el mensaje cifrado.	Método según la reivindicación 1, en el que aprovisionar el perfil de tarjeta generado al dispositivo móvil puede incluir construir un mensaje que incluye el perfil de tarjeta generado, generar una clave de cifrado, encriptar el mensaje usando la clave de cifrado generada y aprovisionar el mensaje cifrado al dispositivo móvil. (Pág. 14, Reivindicación 4).	La figura 2 es un diagrama que muestra una estructura de datos en cada capa cuando el terminal inalámbrico (10) y el dispositivo de estación base (20) transmiten datos de usuario. Los datos de usuario generados por diversas aplicaciones de la capa de aplicación (la séptima capa en el modelo de	Cuando se notifica el número aleatorio al dispositivo receptor (2) desde el dispositivo transmisor (1), la firma del dispositivo transmisor (1) se agrega al mensaje que incluye el número aleatorio, y el dispositivo receptor (2) autentica el dispositivo transmisor (1) verificando la firma. Por

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 3112

Ref. Expediente N° 16145618

	Método según la reivindicación 1, en el que la transmisión de la clave de uso único generada al dispositivo móvil puede incluir construir un mensaje que incluye la clave de uso único generada, generar una clave de cifrado, encriptar el mensaje usando la clave de cifrado generada y aprovisionar el mensaje cifrado al dispositivo móvil. (Pág. 14, Reivindicación 5).	referencia OSI) son datos transmitidos desde el terminal inalámbrico (10) o datos transmitidos al terminal inalámbrico (10). Capa 3 (tercera capa en el modelo de referencia OSI: en lo sucesivo también descrito como "L 3"). En el proceso de la capa CNT (control), el número de secuencia de seguridad y el encabezado L3 se agregan a los datos del usuario y, una vez encriptada la parte de datos del usuario, el código de autenticación de mensajes (MAC) se cifra según los datos de usuario cifrados: (...) (Pág. 16, Párr. 0034).	el contrario, cuando el dispositivo receptor (2) notifica el número aleatorio al dispositivo transmisor (1), la firma del dispositivo receptor (2) se agrega al mensaje que incluye el número aleatorio, y el dispositivo transmisor (1) autentica el dispositivo receptor (2) verificando la firma (Traducción, Párr. 0033).
Un dispositivo de procesamiento configurado para: generar un código de autenticación de referencia utilizando una parte del mensaje cifrado incluido en el mensaje de datos recibidos antes de descifrar el mensaje cifrado.	Un método para generar y aprovisionar credenciales de pago a un dispositivo móvil que carece de un elemento seguro incluye: generar, por un dispositivo de procesamiento, un perfil de tarjeta asociado con una cuenta de pago, donde el perfil de tarjeta incluye al menos credenciales de pago correspondientes a un identificador de perfil; aprovisionar, a un dispositivo móvil, el perfil de tarjeta generado; recibir, desde el dispositivo móvil, una solicitud de clave, en la que la solicitud de clave incluye al menos un número de identificación móvil (PIN) y el identificador de perfil; utilizando, mediante un dispositivo de autenticación, el PIN móvil; generar, por el dispositivo de procesamiento, una clave de	Un primer dispositivo de comunicación y el segundo aparato de comunicación, un sistema de comunicación que comunica utilizando una primera información de autenticación compartida para compartir la autenticación, donde el primer dispositivo de comunicación, cada vez dicha primera información de autenticación compartida el intercambio de autenticación entre dicho segundo aparato de comunicación, así como genera y transmite información de autenticación del	Con el fin de lograr el objeto anterior, el sistema de comunicación criptográfica de la presente invención tiene un primer dispositivo de comunicación que transmite contenido y un segundo dispositivo de comunicación que recibe el contenido del primer dispositivo de comunicación. Uno de los dispositivos de comunicación agrega una firma cifrada basada en un número aleatorio para ser notificado al otro dispositivo de comunicación a un mensaje que incluye un número aleatorio para ser notificado al otro dispositivo de

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 3112

Ref. Expediente N° 16145618

	uso único, en la que la clave de uso único incluye al menos el identificador de perfil, un contador de transacción de aplicación y una clave generadora para usar en la generación de un criptograma de pago válido para una única transacción financiera; y transmitir, mediante un dispositivo transmisor, la clave de uso único generada al dispositivo móvil, en la que no se requiere que el dispositivo móvil tenga un elemento seguro (Pág. 1, Párr. 0007).	lado de transmisión desde la primera información de autenticación compartida a dicho segundo dispositivo de comunicación; la segunda recibe la información de autenticación del dispositivo de comunicación, unidad de control de autenticación del lado transmisor para autenticar la información de autenticación del lado de recepción utilizando la primera información de autenticación compartida (Reiv. 1).	comunicación y transmite la firma encriptada al otro dispositivo de comunicación. Verifica la firma sobre la base del número aleatorio incluido en el mensaje recibido y causa adicionalmente que el otro aparato de comunicación transmita un mensaje que incluye un número aleatorio para ser notificado al único aparato de comunicación al aparato de comunicación y un número aleatorio para ser notificado al otro aparato de comunicación y un número aleatorio ya notificado de un aparato de comunicación, y transmite el cifrado de firma al aparato de comunicación uno, y el aparato de comunicación único transmite el número aleatorio incluido en el mensaje recibido (...) (Párr. 0019).
Validar los datos recibidos basándose en una comprobación del código de autenticación del mensaje incluido en el mensaje de datos recibido contra el código de autenticación de referencia generado.	Otro método para generar y aprovisionar credenciales de pago a un dispositivo móvil sin un elemento seguro incluye: almacenar, en una base de datos, al menos una llave de almacenamiento, una pluralidad de llaves de código de validación dinámicas y un contador de transacciones de aplicaciones asociado con un programa de aplicación móvil; suministro, al dispositivo móvil, al menos la clave de almacenamiento, un	El aparato de estación base (20) autentica el autenticador del terminal recibido (Resumen). Además, la unidad de control de autenticación 104 realiza cálculos basados en MAC-ID, NET-ID, la información de clave de autenticación, el número aleatorio para autenticación NW, el número aleatorio para autenticación de	Una vez completada la autenticación mutua mediante el certificado de clave pública, el aparato de transmisión genera la clave de cifrado de contenido del método de cifrado de clave común para encriptar el contenido. Además, el dispositivo de transmisión crea una firma que se utilizará para aclarar al emisor y confirmar que no se está realizando

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 3112

Ref. Expediente N° 16145618

	componente de autenticación y credenciales de pago estáticas, en el que las credenciales de pago estáticas están asociadas con una cuenta de pago; recibir, desde un dispositivo móvil, un token ⁴ de programa de autenticación de chip (CAP); validar, mediante un dispositivo de validación, la autenticidad del token CAP recibido; generar, por un dispositivo de procesamiento, un número impredecible de clave de sesión (KSUN); generando, por el dispositivo de procesamiento, un número impredecible de nubes (UNCLOUD); identificando, mediante el dispositivo de procesamiento, una carga cifrada basada en una clave de código de validación de tarjeta dinámica. (...) (Fl. 21, Pág. 1, Párr. 0009).	terminal, etc., y realiza la autenticación NW Y verifica el aparato de estación base 20 comparando (comprobando) con el vecindario de datos (Pág. 17, Párr. 0040).	ninguna manipulación. El dispositivo de transmisión encripta la clave de cifrado de contenido generado con la clave pública del dispositivo receptor y encripta la firma con la clave secreta del dispositivo transmisor. El aparato de transmisión agrega una firma cifrada a la clave de cifrado de contenido cifrado y transmite la clave de cifrado de contenido cifrado al aparato de recepción (Traducción Párr. 0004).
Descifrar el mensaje cifrado incluido en el mensaje de datos recibido utilizando la llave de cifrado almacenada para obtener un mensaje descifrado.	(...) El dispositivo de recepción está configurado además para recibir una carga útil encriptada, en el que la carga útil encriptada incluye al menos un código de validación de tarjeta dinámica suministrado, número impredecible de clave de sesión y contador de transacción de aplicación. El dispositivo de procesamiento está configurado además para descifrar la carga cifrada usando al menos la clave de almacenamiento recibida. El dispositivo receptor está configurado además para recibir, a través de la comunicación de campo cercano, un número de lector impredecible de un terminal	Una unidad de generación del contador del lado de recepción para actualizar el contador en la unidad de almacenamiento del lado de recepción cada vez que recibe los datos convertidos, una unidad de generación del contador del lado de recepción para recibir los datos cifrados recibidos por la unidad de procesamiento de recepción del contador Y una unidad de descifrado que descifra los datos descifrados mediante un proceso de descifrado que	Al recibir la clave de cifrado de contenido cifrado y la firma encriptada del dispositivo de transmisión, el dispositivo de recepción descifra primero la firma encriptada con la clave pública del dispositivo de transmisión y la verifica. Tras la verificación exitosa de la firma, el dispositivo receptor descifra la clave de cifrado de contenido cifrado con la clave secreta del dispositivo receptor y adquiere la clave de cifrado de contenido

⁴ https://es.wikipedia.org/wiki/Token_de_seguridad

**REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

Oficio N° 3112

Ref. Expediente N° 16145618

	de punto de venta (...) (Fl. 22, Pág. 2, Párr. 0014).	corresponde al proceso de cifrado predeterminado utilizando la clave de cifrado. Por ejemplo, cuando el primer dispositivo de comunicación corresponde al terminal inalámbrico 10 de la realización y el segundo dispositivo de comunicación corresponde al dispositivo de estación base 20 de la realización, la unidad de control de autenticación del lado de la transmisión notifica a la unidad de control de autenticación 104 del terminal inalámbrico 10 (Pág. 4, Párr. 0008).	(Traducción, 0005). Párr.
--	---	--	---------------------------

De acuerdo con la tabla anterior, las características esenciales del sistema de la reivindicación 14 habían sido divulgadas previamente en el documento D1, por lo tanto, la materia reivindicada no es nueva.

En consecuencia, la reivindicación 14 no es nueva, según lo divulgado en el documento D1.

Asimismo, los documentos D1, D2 y D3 divulgan las características de las reivindicaciones dependientes así:

- Reivindicación 15, 17: En la etapa (1212), el mensaje de recepción puede ser recibido por el servicio de gestión de credenciales de pago (112) y puede ser descifrado usando la clave de sesión móvil y validada. Tras la validación exitosa, en el paso (1214), el servicio de gestión de credenciales de pago (112) puede activar la clave de uso único (118) y puede actualizar el perfil de usuario en consecuencia. En la etapa (1216), el servicio de gestión de credenciales de pago (112) puede transmitir una notificación a la aplicación de pago móvil 106 de que la clave de uso único (118) se ha activado y puede borrar la clave de sesión móvil. En la etapa (1218), el servicio de gestión de credenciales de pago (112) puede sincronizar el perfil de usuario que indica la activación de la clave de uso único (118) con el emisor (108) para la gestión del fraude. (D1, Pág. 10, Párr. 0111).

Página 18 de 24

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 3112

Ref. Expediente N° 16145618

En la etapa (508), el sistema SE remoto (110) puede transmitir el perfil de tarjeta (116) al dispositivo móvil (104). En una realización, el dispositivo móvil (104) puede recibir un mensaje de notificación remota para notificar al usuario (102) que la aplicación de pago móvil (106) debe conectarse con el sistema de SE remoto (110) que usa autenticación mutua (404). Una vez conectado, el sistema de SE remoto (110) puede transmitir el perfil de tarjeta que incluye credenciales de pago para la cuenta especificada por el usuario (102) en el paso (502), que luego puede ser almacenado por el pago móvil aplicación (106) en la base de datos cifrada local (304). (D1, Pág. 6, Párr. 0068).

- Reivindicación 16 y 19: En la etapa (1506), se puede recibir una solicitud de clave desde el dispositivo móvil⁵ (104), en donde la solicitud de clave incluye al menos un número de identificación personal móvil (PIN) y el identificador de perfil. En la etapa (1508), un dispositivo de autenticación (por ejemplo, del servicio de gestión de credenciales de pago 112) puede usar el PIN móvil. En una realización, el dispositivo de autenticación puede usar el PIN móvil usando un método XOR. En la etapa (1510), el dispositivo de procesamiento puede generar una clave de uso único (por ejemplo, la clave de uso único 118), donde la clave de uso único (118) incluye al menos el identificador de perfil, un contador de transacción de aplicación y una clave generadora para su uso en generar un criptograma de pago válido para una sola transacción financiera. En algunas realizaciones, la clave de uso único (118) puede ser genuina si el PIN móvil se autentica satisfactoriamente en la etapa (1508), y falso si el PIN móvil se autentica sin éxito. En una realización, el método (1500) puede incluir además la transmisión de la clave (118) de uso único generada a un emisor asociado con la cuenta de pago. En algunas realizaciones, la clave (118) de uso único generada puede estar inactiva. (D1, Pág. 11, Párr. 0128).
- Reivindicación 18: Para “**realizar**”: Con el fin de lograr el objeto anterior, el sistema de comunicación criptográfica de la presente invención tiene un primer dispositivo de comunicación que transmite contenido y un segundo dispositivo de comunicación que recibe el contenido del primer dispositivo de comunicación. Para “generar”: Uno de los dispositivos de comunicación agrega una firma cifrada basada en un número aleatorio para ser notificado al otro dispositivo de comunicación a un mensaje que incluye un número aleatorio para ser notificado al otro dispositivo de comunicación y transmite la firma encriptada al otro dispositivo de comunicación.

5 https://es.wikipedia.org/wiki/Dispositivo_m%C3%B3vil

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 3112

Ref. Expediente N° 16145618

Para “**Cifrar**”: Verifica la firma sobre la base del número aleatorio incluido en el mensaje recibido y causa adicionalmente que el otro aparato de comunicación transmita un mensaje que incluye un número aleatorio para ser notificado al único aparato de comunicación al aparato de comunicación y un número aleatorio para ser notificado al otro aparato de comunicación y un número aleatorio ya notificado de un aparato de comunicación.

Para “**Generar**”: y transmite el cifrado de firma al aparato de comunicación uno, y el aparato de comunicación único transmite el número aleatorio incluido en el mensaje recibido y se mantiene.

Para “**Notificar**”: El primer dispositivo de comunicación y el segundo dispositivo de comunicación comparten el número aleatorio notificado al dispositivo asociado y el número aleatorio notificado del dispositivo asociado entre sí verificando la firma sobre la base del primer número aleatorio y el segundo número aleatorio, el dispositivo de comunicación transmite contenido cifrado con una clave de sesión generada utilizando una pluralidad de números aleatorios compartidos al segundo dispositivo de comunicación, y el segundo el dispositivo de comunicación transmite el número aleatorio compartido al segundo dispositivo de comunicación Y descifra el contenido recibido del primer dispositivo de comunicación con la clave de sesión generada usando el primer dispositivo de comunicación (D3, Traducción, Párr. 0019).

- Reivindicación 20: La unidad de almacenamiento (102) funciona como la unidad de almacenamiento de información de identificación del terminal (102a) y la unidad de almacenamiento de información clave (102b). La unidad de almacenamiento de información de identificación de terminal (102a), el autodispositivo (el terminal inalámbrico (10)) y el MAC-ID y NET-ID asignados a la ID de estación base de aparato propio que es información de identificación del dispositivo de estación base (20) a la comunicación inalámbrica (la segunda identificación y almacena la información). La ID de estación base es información de identificación utilizada únicamente por la comunicación inalámbrica entre el aparato de estación base (20). La unidad de almacenamiento de información clave (102b), la información de clave de autenticación por el aparato local (terminal inalámbrico (10)) se utiliza en el procesamiento de autenticación y comunicación con la base aparato de estación (20), y la información de clave de cifrado utilizada para el cifrado y descifrado de datos de usuario, alteración de los datos de usuario que almacenan una información de clave de autenticación de mensaje utilizada en la generación de código de autenticación de mensaje para su detección (D2, Pág. 17, Párr. 0039).

**REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

Oficio N° 3112

Ref. Expediente N° 16145618

- Reivindicación 21: El método de la reivindicación 11, donde recibir el perfil de tarjeta puede incluir recibir un mensaje cifrado que incluye el perfil de tarjeta, generar una clave de sesión móvil y descifrar el mensaje usando la clave de sesión móvil generada para obtener el perfil de tarjeta incluido. El método de la reivindicación 11, donde recibir la clave de uso único puede incluir recibir un mensaje cifrado que incluye la clave de uso único, generar una clave de sesión móvil y descifrar el mensaje usando la clave de sesión móvil generada para obtener la clave de uso único incluida. (D1, Pág. 15, Reivindicaciones 13 y 14).
- Reivindicación 22: Método según la reivindicación 1, en el que aprovisionar el perfil de tarjeta generado al dispositivo móvil puede incluir construir un mensaje que incluye el perfil de tarjeta generado, generar una clave de cifrado, encriptar el mensaje usando la clave de cifrado generada y aprovisionar el mensaje cifrado al dispositivo móvil. (D1, Pág. 14, Reivindicación 2.)
- Reivindicación 23, 24: En algunas realizaciones, la transacción de pago puede realizarse mediante el uso de autenticación de datos local (LDA). En algunos casos, el almacenamiento de credenciales de pago recibidas por el dispositivo móvil (104) en el almacenamiento local cifrado (304) (por ejemplo, y no en un elemento seguro) puede ser tal que CDA (generación de criptograma de aplicación / autenticación de datos dinámicos combinados) no esté disponible para respaldar los métodos tradicionales de verificación de tarjetas para verificar las credenciales de pago utilizadas en la transacción financiera. Como resultado, el terminal de punto de venta (120) puede configurarse de manera que puede requerir autenticación por el usuario 102 tanto en el dispositivo móvil (104) (por ejemplo, ingresando el PIN móvil) como en el terminal de punto de venta (120) (por ejemplo, ingresar un PIN o firma en línea). (D1, Pág. 11, Párr. 0123).
- Reivindicación 25: Método según la reivindicación 1, en el que aprovisionar el perfil de tarjeta generado al dispositivo móvil puede incluir construir un mensaje que incluye el perfil de tarjeta generado, generar una clave de cifrado, encriptar el mensaje usando la clave de cifrado generada y aprovisionar el mensaje cifrado al dispositivo móvil. (D1, Pág. 14, Reivindicación 2.)
- Reivindicación 26: El usuario (102) puede registrarse con el sistema (110) de SE remoto. El sistema (110) de SE remoto puede almacenar la información de registro de usuario (por ejemplo, información de cuenta de pago) en una base de datos (602) y puede devolver un código de activación al usuario (102). El usuario (102) luego puede instalar la aplicación de pago móvil (106) en el dispositivo móvil (104) y activar la aplicación de pago móvil (106) usando el código de activación. Como

Página 21 de 24



**REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

Oficio N° 3112

Ref. Expediente N° 16145618

parte de la activación, el sistema de SE remoto (110) puede transmitir una clave móvil compartida (604) a la aplicación de pago móvil (106). La aplicación de pago móvil (106) también puede generar una clave de cifrado de almacenamiento local y puede encriptar el almacenamiento (304) en el dispositivo móvil (104). La clave móvil (604) puede almacenarse en la base de datos cifrada local (304). (D1, Pág. 6, Párr. 0073).

Las reivindicaciones dependientes 15 a 26 no mencionan alguna característica que haga nuevo al sistema de la reivindicación 14, por lo cual se considera que no son nuevas.

8. Conclusión

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

Ítem	Documento	Reivindicaciones afectadas	Requisito que afecta
D1	US20130262317	1, 6, 7, 8, 9, 10 a 17, 19, 21 a 26	Novedad
D2	JP2013081028	1 a 3, 14 y 20	Novedad
D3	JP2010206762	1, 4, 5, 14 y 18	Novedad

9. Respuesta a los argumentos del señor solicitante

El señor solicitante argumenta que “(...) es el mensaje mientras todavía se encuentra en su formato cifrado el que se usa para generar el código de autenticación de referencia” se le aclara al solicitante que: En criptografía, el **cifrado**⁶ es un procedimiento que utiliza un algoritmo de cifrado con cierta clave (clave de cifrado) para transformar un mensaje, sin atender a su estructura lingüística o significado, de tal forma que sea incomprensible o, al menos, difícil de comprender a toda persona que no tenga la clave secreta (clave de descifrado) del algoritmo. Las claves de cifrado y de descifrado pueden ser iguales (criptografía simétrica), distintas (criptografía asimétrica) o de ambos tipos (criptografía híbrida). El juego de caracteres (alfabeto) usado en el mensaje sin cifrar puede no ser el mismo que el juego de caracteres que se usa en el mensaje cifrado. A veces el texto cifrado se escribe en bloques de igual longitud. A estos bloques se les denomina *grupos*. Estos grupos proporcionaban una forma de verificación adicional, ya que el texto cifrado obtenido debía tener un número entero de grupos. Si al cifrar el texto plano no se tiene ese número entero de grupos, entonces se suele rellenar al final con ceros o con caracteres sin sentido. Aunque el cifrado pueda volver secreto el contenido de un

⁶ [https://es.wikipedia.org/wiki/Cifrado_\(criptograf%C3%ADa\)](https://es.wikipedia.org/wiki/Cifrado_(criptograf%C3%ADa))



**REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

Oficio N° 3112

Ref. Expediente N° 16145618

documento, es necesario complementarlo con otras técnicas criptográficas para poder comunicarse de manera segura. Puede ser necesario garantizar la integridad la autenticación de las partes, etcétera. Por lo tanto, toda la información está contenida en el mensaje y hasta que no se tenga en mensaje no se puede iniciar la autenticación del dispositivo.

El señor solicitante argumenta que las reivindicaciones 4 y 5 y el párrafo (0109), “solo indican que se puede generar un mensaje y que el mensaje puede incluir claves y se puede encriptar o cifrar. No hay ninguna divulgación o sugerencia en las reivindicaciones de que se genere un código usando un mensaje o de que el mensaje esté cifrado y que ese mensaje cifrado se use para generar el código, como se menciona en las presentes reivindicaciones. El párrafo [0109] es simplemente una descripción más detallada de lo que se enumera en las reivindicaciones 4 y 5, y por lo tanto revela solo que se puede generar un mensaje que incluye una clave y ese mensaje cifrado”. Frente a estos argumentos, este Despacho reitera que el documento D1 afecta la novedad de la invención dado que el documento pertenece al estado de la técnica y aplica para tal fin, ya que continúa anticipando las características reclamadas en las cláusulas respectivas, por lo que esta Oficina mantiene el documento D1 en el actual examen de patentabilidad. Además, como resultado de la búsqueda adicional, se encontraron los documentos D2 y D3, para ser trasladados, con el fin de igualmente objetar la novedad de la materia reclamada.

Con respecto a la falsa dependencia de la reivindicación 14, se le indica al señor solicitante que realizar una combinación de categorías no es una forma correcta de presentar una reivindicación dado le resta claridad al pliego reivindicatorio. Para el caso de una invención implementada por computadora se entiende que el Hardware y el Software no pueden estar sin una relación por lo tanto no es necesario hacer mención que la reivindicación 14 se relaciona con la reivindicación 1.

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 el 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

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 3112

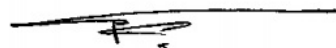
Ref. Expediente N° 16145618

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 al 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 al 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,



[DirectorName]
DIRECTOR DE NUEVAS CREACIONES

Elaborado: JUAN SEBASTIAN RONCANCIO AREVALO
Revisado: RACHID PONCE VERJEL
Aprobado: JOSÉ LUIS SALAZAR LÓPEZ