

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 17443

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
	16145618	26 de agosto de 2016
Reivindicaciones:	16-145618-0000-0000	2 de junio de 2016
	16145618	26 de agosto de 2016
Dibujos:	16-145618-0000-0000	2 de junio de 2016
Respuesta del solicitante:	16145618	26 de agosto de 2016
Prioridad(es):	País: US, ESTADOS UNIDOS DE AMÉRICA Número: 61/910,819 Fecha: 2 de diciembre de 2013	
	País: US, ESTADOS UNIDOS DE AMÉRICA Número: 61/951,842 Fecha: 12 de marzo de 2014	
	País: US, ESTADOS UNIDOS DE AMÉRICA Número: 61/955,716 Fecha: 19 de marzo de 2014	
	País: US, ESTADOS UNIDOS DE AMÉRICA Número: 61/979,113 Fecha: 14 de abril de 2014	
	País: US, ESTADOS UNIDOS DE AMÉRICA Número: 61/979,122 Fecha: 14 de abril de 2014	
	País: US, ESTADOS UNIDOS DE AMÉRICA Número: 61/979,132 Fecha: 14 de abril de 2014	
	País: US, ESTADOS UNIDOS DE AMÉRICA Número: 61/980,784 Fecha: 17 de abril de 2014	
	País: US, ESTADOS UNIDOS DE AMÉRICA Número: 61/996,665 Fecha: 14 de mayo de 2014	
	02/12/2013, US (ESTADOS UNIDOS DE AMÉRICA), 61/910,819	

Oficio N° 17443

Ref. Expediente N° 16145618

	12/03/2014, US (ESTADOS UNIDOS DE AMÉRICA), 61/951,842
	19/03/2014, US (ESTADOS UNIDOS DE AMÉRICA), 61/955,716
	14/04/2014, US (ESTADOS UNIDOS DE AMÉRICA), 61/979,113
	14/04/2014, US (ESTADOS UNIDOS DE AMÉRICA), 61/979,122
	14/04/2014, US (ESTADOS UNIDOS DE AMÉRICA), 61/979,132
	17/04/2014, US (ESTADOS UNIDOS DE AMÉRICA), 61/980,784
	14/05/2014, US (ESTADOS UNIDOS DE AMÉRICA), 61/996,665

2. Análisis de la Prioridad

Se aceptan las reivindicaciones 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 26 del capítulo reivindicatorio (Radicado No. 16145618 del 26 de agosto de 2016).

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. 16-145618-0000-0000 del 2 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.

5. De la solicitud de patente

Reivindicaciones (Art 30 D 486, Art 22 PCT)

Oficio N° 17443

Ref. Expediente N° 16145618

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.

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 encontró el siguiente documento que anticipa el objeto de esta solicitud:

7. Examen de Patentabilidad (Art. 14 D486)

Ítem	Documento	Título	Fecha
D1	US20130262317	“Systems and methods for processing mobile payments by provisioning credentials to mobile devices without secure elements”	3/octubre/2013

El documento D1¹ divulga un método para generar y aprovisionar credenciales de pago a un dispositivo móvil que carece de un elemento seguro que 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 usar en la generación de un criptograma de pago válido para una única transacción financiera; y transmitir la clave de uso único generada al dispositivo móvil.

Novedad (Art 16 D486)

La reivindicación 1 consiste en: “*Un método para recibir y procesar un mensaje de datos, el método caracterizado porque (...)*” (Radicado No. 16145618 del 26 de agosto de 2016).

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

Características Esenciales	D1
Método para recibir y procesar un mensaje de datos.	La presente descripción proporciona una descripción de un 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. (Fl. 25, Pág. 5, Párr. 0059)
Almacenar en una memoria una llave de 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

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

Oficio N° 17443

Ref. Expediente N° 16145618

	el mensaje usando la clave de cifrado generada y aprovisionar el mensaje cifrado al dispositivo móvil. (Fl. 34, Pág. 14, Reivindicación 2). 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.” (Fl.33, Pág. 13, Párr. 150).
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.	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. (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).
El código de autenticación del mensaje se genera usando una parte del mensaje cifrado.	En una realización a modo de ejemplo, mientras se realiza la conexión con el servicio de gestión de credenciales de pago (112) realizado al activar la gestión remota ilustrada en la FIG. 10, la clave (118) de uso único encriptada, puede transmitirse previamente a la aplicación de pago móvil (106) en un mensaje cifrado por la clave móvil (604). En la etapa (1202), el servicio de gestión de credenciales de pago (112) puede construir un mensaje con una acción para activar (por ejemplo, descifrar) la clave de uso único previamente provisionada (118), incluyendo el mensaje la clave aleatoria utilizada para encriptar la clave de uso único (118). El servicio de gestión de credenciales de pago (112) puede generar una clave de sesión móvil y luego cifrar el mensaje incluyendo la clave aleatoria usando la clave de la sesión móvil. El servicio (112) de gestión de credenciales de pago puede, en la etapa (1204), transmitir el mensaje que incluye la clave aleatoria a la aplicación 106 de pago móvil. (Fl. 29, Pág. 9, Párr. 0109).
Validar mediante el dispositivo de procesamiento el mensaje de datos recibidos basándose en una comprobación del código de identificación 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 dinámica 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 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; desencriptar, mediante el dispositivo de procesamiento, la carga cifrada usando al menos la clave de almacenamiento recibida; recibir, a través de una comunicación de campo cercana, un número impredecible para el lector desde un terminal de punto de venta; generar, por el dispositivo de procesamiento, un código de validación de tarjeta dinámica de pago basado en al menos el código de validación de tarjeta dinámica suministrado, el número impredecible de clave de sesión, el contador de transacción de la aplicación y el número impredecible del lector; y transmitir, a través de la comunicación de campo cercano, el código de validación de la tarjeta dinámica de pago generado y el contador de transacción de la aplicación al terminal del punto de venta

Oficio N° 17443

Ref. Expediente N° 16145618

	para incluir en una solicitud de autorización para una transacción financiera (Fl. 21, Pág. 1, Párr. 0010).
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.	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 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 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 derivada (KDCVC3), en la que la carga cifrada incluye al menos una clave de código de validación de tarjeta dinámica de la pluralidad de claves de código de validación dinámicas, el KSUN y el contador de transacciones de la aplicación; transmitir, mediante un dispositivo transmisor, la carga cifrada al dispositivo móvil para utilizarla en la generación de un código de validación de tarjeta dinámica para su uso en una transacción financiera; y transmitir, por el dispositivo transmisor, al menos el contador de transacciones KSUN, UNCLOUD y de la aplicación a un emisor asociado con la cuenta de pago para usar en la validación del código de validación de la tarjeta dinámica generado utilizado en la transacción financiera (Fl. 21, Pág. 1, Párr. 0009).

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, el documento D1 divulga las características de las reivindicaciones dependientes así:

- Reivindicación 2: 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. (Fl. 30, 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

Oficio N° 17443

Ref. Expediente N° 16145618

(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). (Fl. 26, Pág. 6, Párr. 0068).

- Reivindicación 3: 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. (Fl.31, Pág. 11, Párr. 0128).

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.” (Fl. 33, Pág. 13, Párr. 150)

- Reivindicación 4: Los avances en las tecnologías móviles y de comunicación han creado enormes oportunidades, una de las cuales es proporcionar al usuario de dispositivos informáticos móviles la capacidad de iniciar transacciones de pago utilizando su dispositivo móvil. Uno de estos enfoques para permitir que los dispositivos móviles realicen transacciones de pago ha sido el uso de la tecnología de comunicación de campo cercano (NFC) para transmitir de forma segura la información de pago a un terminal cercano de punto de venta sin contacto. Para lograr esto, los teléfonos móviles con hardware de elementos seguros (por ejemplo, un chip de Elemento seguro) se utilizan para almacenar de forma segura las credenciales de la cuenta de pago, como las credenciales de la tarjeta de crédito. (Fl. 21, Pág. 1, Párr. 0003).

El usuario (102) puede tener una cuenta de pago con un emisor (108), tal como una cuenta de tarjeta de crédito. El usuario (102) puede desear usar su dispositivo móvil 104 para realizar transacciones de pago usando su cuenta de pago con el emisor (108) para el financiamiento de las transacciones. Las credenciales de pago correspondientes a la cuenta de pago pueden almacenarse mediante un sistema remoto SE (elemento de seguridad remota) (110) para aprovisionar al dispositivo móvil (104). El sistema de SE remota (110) puede incluir al menos un servicio de gestión de credenciales de pago (112) y un control remoto servidor de notificaciones

Oficio N° 17443

Ref. Expediente N° 16145618

(114), cada uno de los cuales se trata con más detalle a continuación. (Fl. 24, pág. 4, Párr. 0042).

- Reivindicación 5, 6: El adquirente (122) puede presentar una solicitud de autorización para la transacción de pago a una red de pago (124). La red de pago (124) puede configurarse para procesar la solicitud de autorización, por ejemplo, preguntando al emisor (108) por la aprobación de la transacción de pago (por ejemplo, en base a fondos o créditos en la cuenta de pago). La red de pago (124) puede entonces presentar una respuesta de autorización a la adquirente (122) y / o al comerciante, que luego puede finalizar la transacción de pago con el usuario (102). Los métodos y sistemas adecuados para el procesamiento de una transacción financiera serán evidentes para las personas con habilidades en la técnica relevante. (Fl. 24, Pág. 4, Párr. 0045).

La clave de uso único (118) también puede incluir un identificador utilizado para identificar el perfil de tarjeta (116) al que corresponde. En algunas realizaciones, la clave de uso único (118) puede protegerse basándose en un valor de número de identificación personal (PIN) móvil. En dicha realización, el usuario (102) puede proporcionar un PIN móvil para la autenticación. Si el PIN móvil proporcionado es incorrecto, la aplicación de pago móvil (106) puede usar un valor incorrecto de la clave de uso único. En tal caso, el emisor (108) no autorizará la transacción de pago. Tal realización puede dar como resultado una seguridad adicional para el usuario (102), el emisor (108) y el comerciante involucrado en la transacción de pago. (Fl. 24, Pág. 4, Párr. 0051).

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. (Fl.31, 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 (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

Oficio N° 17443

Ref. Expediente N° 16145618

usuario que indica la activación de la clave de uso único (118) con el emisor (108) para la gestión del fraude. (Fl. 30, 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). (Fl. 26, 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. (Fl. 35, 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 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 (Fl. 34, Pág. 14, Reivindicación 1).

Las reivindicaciones dependientes 2 a 13 no mencionan alguna característica que haga nuevo 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 26 de agosto de 2016).*

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

Características Esenciales	D1
----------------------------	----

Oficio N° 17443

Ref. Expediente N° 16145618

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). 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. (Párr. 150). 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 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 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 derivada (KDCVC3), en la que la carga cifrada incluye al menos una clave de código de validación de tarjeta dinámica de la pluralidad de claves de código de validación dinámicas, el KSUN y el contador de transacciones de la aplicación; transmitir, mediante un dispositivo transmisor, la carga cifrada al dispositivo móvil para utilizarla en la generación de un código de validación de tarjeta dinámica para su uso en una transacción financiera; y transmitir, por el dispositivo transmisor, al menos el contador de transacciones KSUN, UNCLOUD y de la aplicación a un emisor asociado con la cuenta de pago para usar en la validación del código de validación de la tarjeta dinámica generado utilizado en la transacción financiera (Fl. 21, Pág. 1, Párr. 0009)
Un dispositivo de recepción configurado para recibir un mensaje de datos en donde el mensaje incluye un mensaje de datos cifrado y un código de autenticación del mensaje.	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 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 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 (Fl. 34, Pág. 14, Reiv. 1).
El código de autenticación se genera utilizando una parte del	Un sistema para generar un código de validación de tarjeta dinámico en un dispositivo móvil que carece de un elemento

Oficio N° 17443

Ref. Expediente N° 16145618

mensaje cifrado. 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 recibido.	seguro incluye un dispositivo receptor, un dispositivo de entrada, un dispositivo de procesamiento y un dispositivo transmisor. El dispositivo receptor está configurado para recibir al menos una clave de almacenamiento, un componente de autenticación y credenciales de pago estáticas. El dispositivo de entrada está configurado para recibir al menos una credencial adicional. El dispositivo de procesamiento está configurado para generar 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. El dispositivo de transmisión está configurado para transmitir el token CAP generado. 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 de punto de venta. El dispositivo de procesamiento está configurado además para generar un código de validación de tarjeta dinámica de pago basado en al menos el código de validación de tarjeta dinámico suministrado, el número impredecible de clave de sesión, el contador de transacción de la aplicación y el número impredecible del lector. El dispositivo transmisor está configurado además para transmitir, a través de comunicación de campo cercano, el código de validación de la tarjeta dinámica de pago generado y el contador de transacción de la aplicación al terminal del punto de venta para incluir en una solicitud de autorización para una transacción financiera (FI. 22, Pág. 2, Párr. 0014).
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 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 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 derivada (KDCVC3), en la que la carga cifrada incluye al menos una clave de código de validación de tarjeta dinámica de la pluralidad de claves de código de validación dinámicas, el KSUN y el contador de transacciones de la aplicación; transmitir, mediante un dispositivo transmisor, la carga cifrada al dispositivo móvil para utilizarla en la generación de un código de validación de tarjeta dinámico para su uso en una transacción financiera; y transmitir, por el dispositivo transmisor, al menos el contador de transacciones KSUN, UNCLOUD y de la aplicación a un emisor asociado con la cuenta de pago para usar en la validación del código de validación de la tarjeta dinámica

Oficio N° 17443

Ref. Expediente N° 16145618

	generado utilizado en la transacción financiera (Fl. 21, Pág. 1, Párr. 0009).
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 de punto de venta (...) (Fl. 22, Pág. 2, Párr. 0014).

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, el documento D1 divulga 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. (Fl. 30, 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). (Fl. 26, Pág. 6, Párr. 0068).

- Reivindicación 16 y 19: El adquirente (122) puede presentar una solicitud de autorización para la transacción de pago a una red de pago (124). La red de pago (124) puede configurarse para procesar la solicitud de autorización, por ejemplo, preguntando al emisor (108) por la aprobación de la transacción de pago (por ejemplo, en base a fondos o créditos en la cuenta de pago). La red de pago (124) puede entonces presentar una respuesta de autorización a la adquirente (122) y / o al comerciante, que luego puede finalizar la transacción de pago con el usuario

Oficio N° 17443

Ref. Expediente N° 16145618

(102). Los métodos y sistemas adecuados para el procesamiento de una transacción financiera serán evidentes para las personas con habilidades en la técnica relevante. (Fl. 24, Pág. 4, Párr. 0045).

La clave de uso único (118) también puede incluir un identificador utilizado para identificar el perfil de tarjeta (116) al que corresponde. En algunas realizaciones, la clave de uso único (118) puede protegerse basándose en un valor de número de identificación personal (PIN) móvil. En dicha realización, el usuario (102) puede proporcionar un PIN móvil para la autenticación. Si el PIN móvil proporcionado es incorrecto, la aplicación de pago móvil (106) puede usar un valor incorrecto de la clave de uso único. En tal caso, el emisor 108 no autorizará la transacción de pago. Tal realización puede dar como resultado una seguridad adicional para el usuario (102), el emisor (108) y el comerciante involucrado en la transacción de pago. (Fl. 24, Pág. 4, Párr. 0051).

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. (Fl.31, Pág. 11, Párr. 0128).

- Reivindicación 18, 20, 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 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). (Fl. 26, Pág. 6, Párr. 0073).
- 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

Oficio N° 17443

Ref. Expediente N° 16145618

móvil y descifrar el mensaje usando la clave de sesión móvil generada para obtener la clave de uso único incluida. (Fl. 35, 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. (Fl. 34, 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). (Fl. 31, 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. (Fl. 34, Pág. 14, Reivindicación 2.)

Las reivindicaciones dependientes 15 a 26 no mencionan alguna característica que haga nuevo al método 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 a 26	Novedad

9. Respuesta a las objeciones realizadas en el examen de forma

De acuerdo a la respuesta al oficio 8142 suministrada por el solicitante con radicado 16145618, del 26 de agosto de 2016, se acepta la respuesta superando de esta forma las objeciones de claridad que les fueron trasladadas en su momento.

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

Oficio N° 17443

Ref. Expediente N° 16145618

reivindicatorio, ii) la descripción de la invención a proteger, iii) o presente un nuevo capítulo reivindicatorio, y desee que se realice un nuevo examen de patentabilidad a esta modificación, no deberá pagar la tasa de modificación voluntaria pero sí la correspondiente a la tasa de examen de patentabilidad. En todo caso, el número de requerimientos por no patentabilidad estará supeditado a que el término del estudio de patentabilidad no sea superior a 18 meses, contados desde la publicación de la solicitud de patente de invención. Adicionalmente, se le recuerda 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,



OLGA ROSA GONZÁLEZ FONSECA
DIRECTORA DE NUEVAS CREACIONES (E)

Elaborado: JUAN SEBASTIAN RONCANCIO AREVALO

Revisado: RACHID PONCE VERJEL

Aprobado: OLGA ROSA GONZÁLEZ FONSECA