

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

Oficio N° 4234

Ref. Expediente N° NC2016/0006168

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	Capítulo II
No. Solicitud Internacional	PCT/US2014/068000		
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	Radicado N° NC2016/0006168	22 de julio de 2016
Reivindicaciones:	Radicado N° NC2016/0006168	22 de julio de 2016
	Radicado N° NC2016/0006168	2 de junio de 2017
Dibujos:	Radicado N° NC2016/0006168	22 de julio de 2016
Prioridad(es):	Pais: US, ESTADOS UNIDOS DE AMÉRICA Número: 61/979,113 Fecha: 14 de abril de 2014	

2. Análisis de la Prioridad

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

Oficio N° 4234

Ref. Expediente N° NC2016/0006168

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 24 del capítulo reivindicatorio (Radicado N° NC2016/0006168 del 2 de junio de 2017).

Título de la solicitud: “METODO Y SISTEMA PARA GENERAR UNA LLAVE DE ALMACENAMIENTO AVANZADA EN UN DISPOSITIVO MOVIL SIN ELEMENTOS DE SEGURIDAD” (Radicado N° NC2016/0006168 del 22 de julio de 2016).

El problema planteado en esta solicitud consiste en permitir que los usuarios de dispositivos móviles que no cuentan con elementos de seguridad puedan realizar transacciones de pago utilizando una llave de almacenamiento en lugar de estos elementos.

Para resolver este problema técnico, la solicitud en estudio proporciona un método para construir una llave de almacenamiento avanzada incluye: almacenar, en una memoria de un dispositivo móvil, al menos (i) información de dispositivo asociada con el dispositivo móvil, (ii) código de programa asociado con un primer programa, el código incluye un identificador de instancia y (iii) código de programa asociado con un segundo programa.

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

Oficio N° 4234

Ref. Expediente N° NC2016/0006168

El objeto de la presente solicitud se relaciona con la Clasificación Internacional de Patentes (CIP): G06Q 20/38.

5. De la solicitud de patente

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

- El término de las Reivindicaciones 1 y 13 "(...) *avanzada* (...)" es relativo por lo cual no permite distinguir la invención del estado de la técnica. Se sugiere sustituirlo por un término o rango concreto.
- Las reivindicaciones 1, 5 a 6, 8 a 10, 13, 17 y 20 a 22, no son claras debido a que poseen términos generales que no permiten establecer un concepto suficiente de la invención que se está reclamando. Estos términos se describen a continuación: Reivs. 1, 5, 8 a 10, 13, 17 y 20 a 22: "(...) *primer programa de aplicación* (...)", Reivs. 1, 6, 9 a 10, 13 y 21 a 22: "(...) *segundo programa de aplicación* (...)", Reivs. 1 y 13: "(...) *huella de dispositivo* (...)", Reivs. 1 y 13: "(...) *valor diversificador* (...)". Se sugiere hacer la aclaración respectiva.

6. Determinación del Estado de la Técnica

El estado de la técnica se determinó con base en la fecha de prioridad: 14 de abril de 2014, 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"	03/Octubre/2013
D2	US20130282589	"Multi-factor mobile transaction authentication"	24/Octubre/2013

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

Oficio N° 4234

Ref. Expediente N° NC2016/0006168

El documento D1¹ proporciona 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 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 (Resumen).

El documento D1² proporciona sistemas y técnicas de autenticación que pueden reconocer, validar y utilizar automáticamente diferentes tipos de información, incluida la información del usuario, la información del dispositivo y la información de la red. Cada uno de estos tipos de información se procesa con un algoritmo único y luego se cifra con fines de seguridad. La información procesada y encriptada se usa luego como componentes de un proceso de autenticación de múltiples factores (...) (Resumen).

7. Examen de Patentabilidad (Art. 14 D486)

Nivel Inventivo (Art 18 D486)

La reivindicación 1 consiste en: “*Un método para construir una llave de almacenamiento avanzada que comprende: (...)*” (Radicado N° NC2016/0006168 del 2 de junio de 2017).

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

Características esenciales	D1	D2
Almacenar, en una memoria de un dispositivo de	En la etapa (1702), al menos una clave de almacenamiento, una pluralidad de claves de código de	No se menciona.

¹<https://patents.google.com/patent/US20130262317?q=US2013262317>

²<https://patents.google.com/patent/US20130282589A1/en?q=US2013282589>



REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 4234

Ref. Expediente N° NC2016/0006168

comunicación móvil, información de dispositivo asociada con el dispositivo de comunicación móvil, código de programa asociado con un primer programa de aplicación, en donde el código de programa incluye un identificador de instancia, y código de programa asociado con un segundo programa de aplicación, en donde el código de programa incluye una primera llave.	validación dinámico (CVC3) y un contador de transacción de aplicación asociado con un programa de aplicación móvil (por ejemplo, la aplicación de pago móvil (106)) pueden almacenarse en una base de datos (por ejemplo, el almacenamiento (304)). En la etapa (1704), al menos la clave de almacenamiento, un componente de autenticación y credenciales de pago estáticas pueden aprovisionarse en el dispositivo móvil (104), en el que las credenciales de pago estáticas están asociadas a una cuenta de pago (Pág. 12, Párr. 0138). Los datos almacenados en el sistema informático (1900) (por ejemplo, en la memoria principal (1908) y/o la memoria secundaria (1910)) se pueden almacenar en cualquier tipo de medio legible por computadora adecuado, como el almacenamiento óptico (por ejemplo, un disco compacto, disco versátil digital, Blu-ray disc, etc.) o almacenamiento en cinta magnética (por ejemplo, una unidad de disco duro). Los datos pueden configurarse en cualquier tipo de configuración de base de datos adecuada, como una base de datos relacional, una base de datos de lenguaje de consulta estructurado, una base de datos distribuida, una base de datos de objetos, etc. Las configuraciones adecuadas y los tipos de almacenamiento serán evidentes para las personas con	
---	--	--

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 4234

Ref. Expediente N° NC2016/0006168

	habilidades en la técnica relevante (Pág. 13, Párr. 0153).	
Generar, mediante un dispositivo de procesamiento, una huella de dispositivo asociada con el dispositivo de comunicación móvil con base en la información de dispositivo almacenada vía la ejecución del código de programa asociado con el primer programa de aplicación.	En la etapa (1710), un dispositivo de procesamiento (por ejemplo, el sistema de nube (302)) puede generar un número imprevisible de clave de sesión (KSUN). En la etapa (1712), el dispositivo de procesamiento (302) puede generar un número impredecible de nube (UNCLOUD) (...) (Pág. 12, Párr. 0140).	Una aplicación de servidor que recibe información específica del usuario (por ejemplo, nombre de usuario, número de móvil, límite de compra, fecha de vencimiento, PIN), información del dispositivo (por ejemplo, IMEI o número de serie del dispositivo) y/o información de red (por ejemplo, número de móvil, MSISDN), y genera una clave de aplicación única que se transmite de forma segura a la aplicación del usuario, donde se almacena de forma segura en una ubicación de memoria volátil (...) (Pág. 6, Párr. 0107).
Generar, mediante el dispositivo de procesamiento, un valor aleatorio vía ejecución del código de programa asociado con el primer programa de aplicación.	No se menciona.	(...) El servidor, para generar una nueva clave de aplicación, usará un generador de números pseudoaleatorio con una regla de negocios que garantiza que cada clave sea única (Pág. 6, Párr. 0107). (...) Un servidor de backend se comunica con ambos dispositivos para crear un proceso de autenticación de circuito cerrado altamente seguro. Este proceso de autenticación se puede utilizar para interactuar con otros procesos o sistemas para permitir la identificación del cliente, el procesamiento de pagos o cualquier otro proceso comercial que pueda beneficiarse de una capacidad de autenticación de identificación

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 4234

Ref. Expediente N° NC2016/0006168

		segura y positiva (Pág. 4, Párr. 0052).
Construir, mediante el dispositivo de procesamiento, un valor diversificador con base en la huella de dispositivo generada, el valor aleatorio generado y el identificador de instancia incluido en el código de programa asociado con el primer programa de aplicación.	(...) En la etapa (1816), el dispositivo de procesamiento puede generar un valor CVC3 de pago basado en al menos el valor CVC3 suministrado, el número impredecible de la clave de sesión, el contador de transacciones de la aplicación y el número impredecible del lector (...) (Pág. 13, Párr. 0145).	(...) El servidor, para generar una nueva clave de aplicación, usará un generador de números pseudoaleatorio con una regla de negocios que garantiza que cada clave sea única (Pág. 6, Párr. 0107).
Descifrar, mediante el dispositivo de procesamiento, el valor diversificador construido con la primera llave almacenada en el código de programa asociado con el segundo programa de aplicación vía la ejecución del código de programa asociado con el segundo programa de aplicación para obtener una llave de almacenamiento.	(...) En la etapa (1714), el dispositivo de procesamiento (302) puede identificar una carga útil encriptada basada en una clave CVC3 derivada (KDCVC3), donde la carga útil encriptada incluye al menos una clave CVC3 de la pluralidad de claves CVC3, el KSUN y el contador de transacción de la aplicación. En una realización, el KDCVC3 puede ser genuino si el token de CAP recibido se valida con éxito, y puede ser falso si el token de CAP recibido se valida sin éxito. En alguna realización, la carga útil puede encriptarse usando al menos la clave de almacenamiento (Pág. 12, Párr. 0140). (...) En la etapa (1812), el dispositivo de procesamiento puede descifrar la carga útil encriptada usando al	No se menciona.

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

Oficio N° 4234

Ref. Expediente N° NC2016/0006168

	menos la clave de almacenamiento recibida (Pág. 13, Párr. 0144).	
--	--	--

El documento D1 se considera el estado de la técnica más cercano a la invención definida en la reivindicación 1 porque 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 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 (Resumen).

La diferencia entre la invención, definida en la reivindicación 1 y el método de D1 consiste en que en el método de la reivindicación 1, el dispositivo de procesamiento genera un valor aleatorio asociado con el primer programa de aplicación.

El efecto que logra que el dispositivo de procesamiento genere un valor aleatorio asociado con el primer programa de aplicación es generar una llave de almacenamiento.

Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así: “¿cómo modificar el método conocido en D1 para generar una llave de almacenamiento?”.

Sin embargo, el generar un valor aleatorio a través del dispositivo de procesamiento, ya está divulgado en el documento D2 que hace referencia a que (...) el servidor, para generar una nueva clave de aplicación, usará un generador de números pseudoaleatorio con una regla de negocios que garantiza que cada clave sea única (Pág. 6, Párr. 0107).

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

Oficio N° 4234

Ref. Expediente N° NC2016/0006168

En consecuencia, la persona del oficio normalmente versada en la materia, incluiría la generación de un valor aleatorio a través del dispositivo de procesamiento del documento D2 en el método divulgado en el documento D1 para llegar así al objeto de la reivindicación 1 de la solicitud. Por lo cual se considera obvia.

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

- Reivindicación 2: En la etapa (1702), al menos una clave de almacenamiento, una pluralidad de claves de código de validación dinámico (CVC3) y un contador de transacción de aplicación asociado con un programa de aplicación móvil (por ejemplo, la aplicación de pago móvil (106)) pueden almacenarse en una base de datos (por ejemplo, el almacenamiento (304)) (...) (D1, Pág. 12, Párr. 0138). (...) El servicio de gestión de credenciales de pago (112) puede generar entonces una clave de sesión móvil y luego puede encriptar el mensaje que incluye la clave aleatoria usando la clave de sesión móvil (...) (D1, Pág. 9, Párr. 0109). (...) en el que la carga útil encriptada incluye al menos un código de validación de tarjeta dinámica suministrado, un número impredecible de clave de sesión y un contador de transacción de aplicación (...) (D1, Pág. 1, Párr. 0010).
- Reivindicación 3: En la etapa (1702), al menos una clave de almacenamiento, una pluralidad de claves de código de validación dinámico (CVC3) y un contador de transacción de aplicación asociado con un programa de aplicación móvil (por ejemplo, la aplicación de pago móvil (106)) pueden almacenarse en una base de datos (por ejemplo, el almacenamiento (304)). En la etapa (1704), al menos la clave de almacenamiento, un componente de autenticación y credenciales de pago estáticas pueden aprovisionarse en el dispositivo móvil (104), en el que las credenciales de pago estáticas están asociadas a una cuenta de pago (D1, Pág. 12, Párr. 0138).
- Reivindicación 4: (...) El servidor, para generar una nueva clave de aplicación, usará un generador de números pseudoaleatorio con una regla de negocios que garantiza que cada clave sea única (D2, Pág. 6, Párr. 0107).

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 4234

Ref. Expediente N° NC2016/0006168

- Reivindicación 5: (...) En la etapa (1702), al menos una clave de almacenamiento, una pluralidad de claves de código de validación dinámico (CVC3) y un contador de transacción de aplicación asociado con un programa de aplicación móvil (por ejemplo, la aplicación de pago móvil (106)) pueden almacenarse en una base de datos (por ejemplo, el almacenamiento (304)). En la etapa (1704), al menos la clave de almacenamiento, un componente de autenticación y credenciales de pago estáticas pueden aprovisionarse en el dispositivo móvil (104), en el que las credenciales de pago estáticas están asociadas a una cuenta de pago (D1, Pág. 12, Párr. 0138).
- Reivindicación 6: (...) El servicio de gestión de credenciales de pago (112) puede generar entonces una clave de sesión móvil y luego puede encriptar el mensaje que incluye la clave aleatoria usando la clave de 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 (...) (D1, Pág. 9, Párr. 0109).
- Reivindicación 7: (...) En la etapa (1702), al menos una clave de almacenamiento, una pluralidad de claves de código de validación dinámico (CVC3) y un contador de transacción de aplicación asociado con un programa de aplicación móvil (por ejemplo, la aplicación de pago móvil (106)) pueden almacenarse en una base de datos (por ejemplo, el almacenamiento (304)) (...) (D1, Pág. 12, Párr. 0138).
- Reivindicación 8: (...) En la etapa (1702), al menos una clave de almacenamiento, una pluralidad de claves de código de validación dinámico (CVC3) y un contador de transacción de aplicación asociado con un programa de aplicación móvil (por ejemplo, la aplicación de pago móvil (106)) pueden almacenarse en una base de datos (por ejemplo, el almacenamiento (304)) (...) (D1, Pág. 12, Párr. 0138). (...) El servidor, para generar una nueva clave de aplicación, usará un generador de números pseudoaleatorio con una regla de negocios que garantiza que cada clave sea única (D2, Pág. 6, Párr. 0107).
- Reivindicación 9 y 10: (...) En la etapa (1702), al menos una clave de

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

Oficio N° 4234

Ref. Expediente N° NC2016/0006168

almacenamiento, una pluralidad de claves de código de validación dinámico (CVC3) y un contador de transacción de aplicación asociado con un programa de aplicación móvil (por ejemplo, la aplicación de pago móvil (106)) pueden almacenarse en una base de datos (por ejemplo, el almacenamiento (304)) (...) (D1, Pág. 12, Párr. 0138).

- Reivindicación 11: En la etapa (1808), el token de CAP generado puede ser transmitido por un dispositivo de transmisión. En la etapa (1810), el dispositivo receptor puede recibir una carga cifrada, en la que la carga cifrada incluye al menos un valor CVC3 suministrado, un número impredecible de la clave de sesión y un contador de transacción de la aplicación. En la etapa (1812), el dispositivo de procesamiento puede descifrar la carga útil encriptada usando al menos la clave de almacenamiento recibida (D1, Pág. 13, Párr. 0144). (...) En la etapa (10), la carga útil encriptada puede descifrarse usando KSTORAGE y almacenarse en el almacenamiento (304) (D1, Pág. 7, Párr. 0085).
- Reivindicación 12: En la etapa (1716), un dispositivo transmisor puede transmitir la carga útil encriptada al dispositivo móvil (104) para su uso en la generación de un valor CVC3 para uso en una transacción financiera (...) (D1, Pág. 12, Párr. 0141).

Las reivindicaciones dependientes 2 a 12 no mencionan alguna característica que, junto con las características de la reivindicación independiente, aporte nivel inventivo al método de la reivindicación 1, por lo cual se considera que no tienen nivel inventivo.

La reivindicación 13 consiste en: *“Un sistema para construir una llave de almacenamiento avanzada, que comprende: (...)”* (Radicado N° NC2016/0006168 del 2 de junio de 2017).

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

Características esenciales	D1	D2
Una memoria de un dispositivo de comunicación móvil	En la etapa (1702), al menos una clave de almacenamiento, una pluralidad de claves de código de	No se menciona.

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 4234

Ref. Expediente N° NC2016/0006168

configurada para almacenar, información de dispositivo asociada con el dispositivo de comunicación móvil, código de programa asociado con un primer programa de aplicación, en donde el código de programa incluye un identificador de instancia, y código de programa asociado con un segundo programa de aplicación, en donde el código de programa incluye una primera llave.	validación dinámico (CVC3) y un contador de transacción de aplicación asociado con un programa de aplicación móvil (por ejemplo, la aplicación de pago móvil (106)) pueden almacenarse en una base de datos (por ejemplo, el almacenamiento (304)). En la etapa (1704), al menos la clave de almacenamiento, un componente de autenticación y credenciales de pago estáticas pueden aprovisionarse en el dispositivo móvil (104), en el que las credenciales de pago estáticas están asociadas a una cuenta de pago (Pág. 12, Párr. 0138). Los datos almacenados en el sistema informático (1900) (por ejemplo, en la memoria principal (1908) y/o la memoria secundaria (1910)) se pueden almacenar en cualquier tipo de medio legible por computadora adecuado, como el almacenamiento óptico (por ejemplo, un disco compacto, disco versátil digital, Blu-ray disc, etc.) o almacenamiento en cinta magnética (por ejemplo, una unidad de disco duro). Los datos pueden configurarse en cualquier tipo de configuración de base de datos adecuada, como una base de datos relacional, una base de datos de lenguaje de consulta estructurado, una base de datos distribuida, una base de datos de objetos, etc. Las configuraciones adecuadas y los tipos de almacenamiento serán evidentes	
---	--	--

Página 12 de 19



REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 4234

Ref. Expediente N° NC2016/0006168

	para las personas con habilidades en la técnica relevante (Pág. 13, Párr. 0153).	
Un dispositivo de procesamiento configurado para, generar una huella de dispositivo asociada con el dispositivo de comunicación móvil con base en la información de dispositivo almacenada vía ejecución del código de programa asociado con el primer programa de aplicación.	En la etapa (1710), un dispositivo de procesamiento (por ejemplo, el sistema de nube (302)) puede generar un número imprevisible de clave de sesión (KSUN). En la etapa (1712), el dispositivo de procesamiento (302) puede generar un número impredecible de nube (UNCLOUD) (...) (Pág. 12, Párr. 0140).	Una aplicación de servidor que recibe información específica del usuario (por ejemplo, nombre de usuario, número de móvil, límite de compra, fecha de vencimiento, PIN), información del dispositivo (por ejemplo, IMEI o número de serie del dispositivo) y/o información de red (por ejemplo, número de móvil, MSISDN), y genera una clave de aplicación única que se transmite de forma segura a la aplicación del usuario, donde se almacena de forma segura en una ubicación de memoria volátil (...) (Pág. 6, Párr. 0107).
Un dispositivo de procesamiento configurado para, generar un valor aleatorio vía ejecución del código de programa asociado con el primer programa de aplicación.	No se menciona.	(...) El servidor, para generar una nueva clave de aplicación, usará un generador de números pseudoaleatorio con una regla de negocios que garantiza que cada clave sea única (Pág. 6, Párr. 0107). (...) Un servidor de backend se comunica con ambos dispositivos para crear un proceso de autenticación de circuito cerrado altamente seguro. Este proceso de autenticación se puede utilizar para interactuar con otros procesos o sistemas para permitir la identificación del cliente, el procesamiento de pagos o cualquier otro proceso comercial que pueda beneficiarse de una capacidad de autenticación de identificación

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 4234

Ref. Expediente N° NC2016/0006168

		segura y positiva (Pág. 4, Párr. 0052).
Un dispositivo de procesamiento configurado para, construir un valor diversificador con base en la huella de dispositivo generada, el valor aleatorio generado y el identificador de instancia incluido en el código de programa asociado con el primer programa de aplicación.	(...) En la etapa (1816), el dispositivo de procesamiento puede generar un valor CVC3 de pago basado en al menos el valor CVC3 suministrado, el número impredecible de la clave de sesión, el contador de transacciones de la aplicación y el número impredecible del lector (...) (Pág. 13, Párr. 0145).	(...) El servidor, para generar una nueva clave de aplicación, usará un generador de números pseudoaleatorio con una regla de negocios que garantiza que cada clave sea única (Pág. 6, Párr. 0107).
Un dispositivo de procesamiento configurado para, descifrar el valor diversificador construido con la primera llave almacenada en el código de programa asociado con el segundo programa de aplicación vía ejecución del código de programa asociado con el segundo programa de aplicación para obtener una llave de almacenamiento.	(...) En la etapa (1714), el dispositivo de procesamiento (302) puede identificar una carga útil encriptada basada en una clave CVC3 derivada (KDCVC3), donde la carga útil encriptada incluye al menos una clave CVC3 de la pluralidad de claves CVC3, el KSUN y el contador de transacción de la aplicación. En una realización, el KDCVC3 puede ser genuino si el token de CAP recibido se valida con éxito, y puede ser falso si el token de CAP recibido se valida sin éxito. En alguna realización, la carga útil puede encriptarse usando al menos la clave de almacenamiento (Pág. 12, Párr. 0140). (...) En la etapa (1812), el dispositivo de procesamiento puede descifrar la carga útil encriptada usando al menos la	No se menciona.

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 4234

Ref. Expediente N° NC2016/0006168

	clave de almacenamiento recibida (Pág. 13, Párr. 0144).	
--	--	--

El documento D1 se considera el estado de la técnica más cercano a la invención definida en la reivindicación 13 porque divulga un sistema para generar y aprovisionar credenciales de pago a un dispositivo móvil que carece de un elemento seguro incluye un dispositivo transmisor, un dispositivo de procesamiento, un dispositivo de aprovisionamiento, un dispositivo receptor y un dispositivo de autenticación (Pág. 2, Párr. 0011).

La diferencia entre la invención, definida en la reivindicación 13 y el sistema de D1 consiste en que en el sistema de la reivindicación 13, el dispositivo de procesamiento está configurado para generar un valor aleatorio asociado con el primer programa de aplicación.

El efecto que logra que el dispositivo de procesamiento está configurado para generar un valor aleatorio asociado con el primer programa de aplicación es generar una llave de almacenamiento.

Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así: “¿cómo modificar el sistema conocido en D1 para generar una llave de almacenamiento?”.

Sin embargo, el generar un valor aleatorio a través del dispositivo de procesamiento, ya está divulgado en el documento D2 que hace referencia a que (...) el servidor, para generar una nueva clave de aplicación, usará un generador de números pseudoaleatorio con una regla de negocios que garantiza que cada clave sea única (Pág. 6, Párr. 0107).

En consecuencia, la persona del oficio normalmente versada en la materia, incluiría la generación de un valor aleatorio a través del dispositivo de procesamiento del documento D2 en el sistema divulgado en el documento D1 para llegar así al objeto de la reivindicación 13 de la solicitud. Por lo cual se considera obvia.

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

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

Oficio N° 4234

Ref. Expediente N° NC2016/0006168

- Reivindicación 14: En la etapa (1702), al menos una clave de almacenamiento, una pluralidad de claves de código de validación dinámico (CVC3) y un contador de transacción de aplicación asociado con un programa de aplicación móvil (por ejemplo, la aplicación de pago móvil (106)) pueden almacenarse en una base de datos (por ejemplo, el almacenamiento (304)) (...) (D1, Pág. 12, Párr. 0138). El servicio de gestión de credenciales de pago (112) puede generar entonces una clave de sesión móvil y luego puede encriptar el mensaje que incluye la clave aleatoria usando la clave de sesión móvil (...) (D1, Pág. 9, Párr. 0109). (...) en el que la carga útil encriptada incluye al menos un código de validación de tarjeta dinámica suministrado, un número impredecible de clave de sesión y un contador de transacción de aplicación (...) (D1, Pág. 1, Párr. 0010).
- Reivindicación 15: En la etapa (1702), al menos una clave de almacenamiento, una pluralidad de claves de código de validación dinámico (CVC3) y un contador de transacción de aplicación asociado con un programa de aplicación móvil (por ejemplo, la aplicación de pago móvil (106)) pueden almacenarse en una base de datos (por ejemplo, el almacenamiento (304)). En la etapa (1704), al menos la clave de almacenamiento, un componente de autenticación y credenciales de pago estáticas pueden aprovisionarse en el dispositivo móvil (104), en el que las credenciales de pago estáticas están asociadas a una cuenta de pago (D1, Pág. 12, Párr. 0138).
- Reivindicación 16: (...) El servidor, para generar una nueva clave de aplicación, usará un generador de números pseudoaleatorio con una regla de negocios que garantiza que cada clave sea única (D2, Pág. 6, Párr. 0107).
- Reivindicación 17: (...) En la etapa (1702), al menos una clave de almacenamiento, una pluralidad de claves de código de validación dinámico (CVC3) y un contador de transacción de aplicación asociado con un programa de aplicación móvil (por ejemplo, la aplicación de pago móvil (106)) pueden almacenarse en una base de datos (por ejemplo, el almacenamiento (304)). En la etapa (1704), al menos la clave de almacenamiento, un componente de autenticación y credenciales de pago estáticas pueden aprovisionarse en el

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

Oficio N° 4234

Ref. Expediente N° NC2016/0006168

dispositivo móvil (104), en el que las credenciales de pago estáticas están asociadas a una cuenta de pago (D1, Pág. 12, Párr. 0138).

- Reivindicación 18: (...) El servicio de gestión de credenciales de pago (112) puede generar entonces una clave de sesión móvil y luego puede encriptar el mensaje que incluye la clave aleatoria usando la clave de 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 (...) (D1, Pág. 9, Párr. 0109).
- Reivindicación 19: (...) En la etapa (1702), al menos una clave de almacenamiento, una pluralidad de claves de código de validación dinámico (CVC3) y un contador de transacción de aplicación asociado con un programa de aplicación móvil (por ejemplo, la aplicación de pago móvil (106)) pueden almacenarse en una base de datos (por ejemplo, el almacenamiento (304)) (...) (D1, Pág. 12, Párr. 0138).
- Reivindicación 20: (...) En la etapa (1702), al menos una clave de almacenamiento, una pluralidad de claves de código de validación dinámico (CVC3) y un contador de transacción de aplicación asociado con un programa de aplicación móvil (por ejemplo, la aplicación de pago móvil (106)) pueden almacenarse en una base de datos (por ejemplo, el almacenamiento (304)) (...) (D1, Pág. 12, Párr. 0138). (...) El servidor, para generar una nueva clave de aplicación, usará un generador de números pseudoaleatorio con una regla de negocios que garantiza que cada clave sea única (D2, Pág. 6, Párr. 0107).
- Reivindicación 21 y 22: (...) En la etapa (1702), al menos una clave de almacenamiento, una pluralidad de claves de código de validación dinámico (CVC3) y un contador de transacción de aplicación asociado con un programa de aplicación móvil (por ejemplo, la aplicación de pago móvil (106)) pueden almacenarse en una base de datos (por ejemplo, el almacenamiento (304)) (...) (D1, Pág. 12, Párr. 0138).
- Reivindicación 23: En la etapa (1808), el token de CAP generado puede ser

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

Oficio N° 4234

Ref. Expediente N° NC2016/0006168

transmitido por un dispositivo de transmisión. En la etapa (1810), el dispositivo receptor puede recibir una carga cifrada, en la que la carga cifrada incluye al menos un valor CVC3 suministrado, un número impredecible de la clave de sesión y un contador de transacción de la aplicación. En la etapa (1812), el dispositivo de procesamiento puede descifrar la carga útil encriptada usando al menos la clave de almacenamiento recibida (D1, Pág. 13, Párr. 0144). (...) En la etapa (10), la carga útil encriptada puede descifrarse usando KSTORAGE y almacenarse en el almacenamiento (304) (D1, Pág. 7, Párr. 0085).

- Reivindicación 24: En la etapa (1716), un dispositivo transmisor puede transmitir la carga útil encriptada al dispositivo móvil (104) para su uso en la generación de un valor CVC3 para uso en una transacción financiera (...) (D1, Pág. 12, Párr. 0141).

Las reivindicaciones dependientes 14 a 24 no mencionan alguna característica que, junto con las características de la reivindicación independiente, aporte nivel inventivo al sistema de la reivindicación 13, por lo cual se considera que no tienen nivel inventivo.

8. Conclusión

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

Ítem	Documento	Reivindicaciones afectadas	Requisito que afecta
D1	US20130262317	1 a 3, 5 a 15, 17 a 19 a 24	Nivel Inventivo
D2	US20130282589	1, 4, 8, 13, 16 y 20	Nivel Inventivo

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

Si como respuesta a este requerimiento el solicitante llegara a modificar: i) el capítulo

Página 18 de 19

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 4234

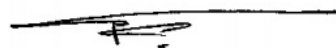
Ref. Expediente N° NC2016/0006168

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,



[DirectorName]

DIRECTOR DE NUEVAS CREACIONES

Elaborado: CARLOS EDUARDO GUEVARA NICHÓY

Revisado: SONIA ANDREA DÍAZ PIRAZÁN

Aprobado: JOSÉ LUIS SALAZAR LÓPEZ