

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO	
RAD: 13-169786- -4	FECHA: 2014-07-09 09:01:44
DEP: 2020 DIRECCION DE NUEVAS CREACIONES	EVE: 378 FASE NACIONAL INCLUIDO CAPITULO I
TRA: 11 PCT-PATENTE DE INVENCION CAPITULOS I Y II	FOLIOS: 13
ACT: 519 PRESENTACION	

DIRECCIÓN DE NUEVAS CREACIONES

2020
Bogotá, D.C.,

Abogado(a)/Señor(a)
JUAN PABLO CADENA SARMIENTO

Asunto: Radicación: 13-169786- -4
 Trámite: 11
 Evento: 378
 Actuación: 519
 Oficio: 8113
 Folios: 13

Patente de Invención	X			Patente de Modelo de Utilidad	
Vía Nacional					
Vía PCT (Fase Nacional)	X	Capítulo I	X	Capítulo II	
No. Solicitud Internacional	PCT/US2011/066203				
Fecha de Presentación Internacional	22/12/2011				

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:	Rad. N° 13-169786-00000-0000	17/Julio/2013
Reivindicaciones:	Rad. N° 13-169786-00000-0000	17/Julio/2013
Dibujos:	Rad. N° 13-169786-00000-0000	17/Julio/2013
Prioridad(es):	US 12/975.502	22/Diciembre/2010

2. Análisis de la Prioridad

Se acepta la reivindicación de prioridad porque ésta solicitud fue presentada dentro del plazo establecido (Art. 9 D 486) y su contenido técnico corresponde con el de la prioridad reivindicada.

3. 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 35.

Título de la solicitud: "Sistema de pago en el surtidor de combustible para asegurar la evaluación de los datos del titular de la tarjeta" (Ver página 1 del radicado N°13-169786-00000-0000).

El problema planteado en esta solicitud consiste en la necesidad de realizar pagos de productos y servicios en puntos minoristas de forma segura.

Para resolver este problema técnico, la solicitud en estudio proporciona un sistema y método donde se encriptan los datos del titular de la tarjeta, de acuerdo con un primer método de encriptación, y se envían a un sistema de evaluación segura, donde se desencriptan y se evalúan con el obtivo de detrmnar si disco datos son datos de pago o datos no sensibles del titular. En caso de ser datos de pago estos se encriptan de nuevo.

El objeto de la presente solicitud se relaciona con la Clasificación Internacional de Patentes (CIP): G06Q 20/00.

4. De la solicitud de patente

Reivindicaciones (Art 30 D 486, Art 22 PCT)

Las reivindicaciones 2, 3, 6 a 10, 12 a 17, 20 y 24 a 26 no están caracterizadas por sus características esenciales sino por resultados a alcanzar y/o funcionalidades definidos por los términos: "...porque dicho sistema de evaluación segura transmite dichos datos no encriptados del titular de la tarjeta hacia un sistema de procesamiento local, en una forma no encriptada, si dichos datos no encriptados del titular de la tarjeta son los datos no sensibles del titular de la tarjeta...", "...porque dicho sistema de evaluación segura está implementado como a candado electrónico...", "...está adaptado para transmitir dichos segundos datos encriptados del titular de la tarjeta hacia un sistema procesador anfitrión remoto...", "...porque dichos primer y segundo métodos de encriptación son los mismos...", "...porque dichos primer y segundo métodos de encriptación son diferentes...", "...porque dicho primer método de encriptación comprende la encriptación triple DES de los datos del titular de la tarjeta...", "...porque dicho dispositivo de entrada es contra la manipulación indebida...", "...conteniendo dicha memoria del sistema de evaluación segura la información necesitada para desencriptar los datos encriptados, de acuerdo con un primer método de encriptación, y la información necesitada para encriptar los datos de acuerdo con un segundo método de encriptación; siendo dicha memoria del sistema de evaluación segura encriptada de acuerdo con un tercer método de encriptación...", "...está adaptada para desencriptar dicha memoria del sistema de evaluación segura...", "...está adaptada ulteriormente para desencriptar los datos encriptados del titular de la tarjeta, de acuerdo con dicho primer método de encriptación, con el fin de producir los datos no encriptados del titular de la tarjeta...", "...está adaptada ulteriormente para evaluar dichos datos no encriptados del titular de la tarjeta, y encriptar dichos datos no encriptados del titular de la tarjeta, de acuerdo con dicho segundo método de encriptación, si dichos datos no encriptados del titular de la tarjeta son los datos del titular de la tarjeta de pago...", "...porque dichos primer y segundo métodos de encriptación son diferentes...", "...porque dicha memoria del sistema de evaluación segura contiene la información necesitada para encriptar los datos, de acuerdo con más que un segundo método de encriptación...", "...porque dicha electrónica de control seguro selecciona el apropiado

segundo método de encriptación, después de la evaluación de dichos datos no encriptados del titular de la tarjeta...”, “...porque dicha memoria del sistema de evaluación segura contiene un archivo de configuración del sitio...”, “...porque dicha electrónica de control seguro está contra la manipulación indebida...”, “...porque dicho tercer método de encriptación comprende el AES-128...”, “...porque dicha electrónica de control seguro transmite dichos datos no encriptados del titular de la tarjeta hacia un sistema de procesamiento local, en la forma no encriptada si dichos datos no encriptados del titular de la tarjeta son los datos no sensibles del titular de la tarjeta...”, “...está adaptada ulteriormente, para evaluar dichos datos no encriptados del titular de la tarjeta, con el fin de realizar la validación de la transacción...” y “...porque dicha memoria del sistema de evaluación segura contiene un archivo de registro de la transacción...”. Es así que estos términos no definen características estructurales esenciales, puesto que la reivindicación incluiría no sólo la solución propuesta por el solicitante, sino todas las alternativas presentes o futuras que lleguen a esos resultados. Se sugiere reemplazarlos por las características esenciales estructurales que contribuyen a la obtención de esos efectos. Es oportuno aclarar que, las funcionalidades pueden estar presente en la reivindicación pero no le pueden dar novedad y/o nivel inventivo a un producto, dado que, que cuando se reivindica un producto, las funcionalidades sirven para entender la relación que hay entre los diferentes elementos estructurales de un producto, pero son solo los elementos estructurales los que definen a dicho producto haciendo a las funcionalidades opcionales.

Las reivindicaciones 1 y 18 tienen funcionalidades definidas por los términos: “...configurado para recibir los datos del titular de la tarjeta, dicho dispositivo de entrada está operativo para encriptar dichos datos del titular de la tarjeta, de acuerdo con un primer método de encriptación, con el fin de producir los primeros datos encriptados del titular de la tarjeta...”, “...adaptada para desencriptar dichos primeros datos encriptados del titular de la tarjeta, con el fin de producir los datos no encriptados del titular de la tarjeta...”, “...donde dicha electrónica de control respecto a la manipulación indebida, de dicho sistema de evaluación segura, evalúa dichos datos no encriptados del titular de la tarjeta, con el fin de determinar si dichos datos no encriptados del titular de la tarjeta son los datos del titular de la tarjeta de pago, o los datos no sensibles del titular de la tarjeta; y donde, si dichos datos no encriptados del titular de la tarjeta son los datos del titular de la tarjeta de pago, dicha electrónica de control respecto a la manipulación indebida de dicho sistema de evaluación segura, está adaptada para encriptar dichos datos no encriptados del titular de la tarjeta, de acuerdo con un segundo método de encriptación, con el fin de producir los segundos datos encriptados del titular de la tarjeta...” y “...almacenando la información necesitada para desencriptar los datos encriptados, de acuerdo con dicho tercer método de encriptación...”. Estas funcionalidades pueden estar presente en las reivindicaciones pero, se aclara que, no le pueden dar novedad y/o nivel inventivo a un producto, dado que, que cuando se reivindica un producto, las funcionalidades sirven para entender la relación que hay entre los diferentes elementos estructurales de un producto, pero son solo los elementos estructurales los que definen a dicho producto haciendo a las funcionalidades opcionales.

La reivindicación 5 no es clara porque el término “...are...” no se entiende.

La reivindicación 5 no es clara porque hace referencia a USIP®, que es una marca registrada¹ y por tanto no definen al producto porque su composición puede cambiar con el paso del tiempo aunque conserve el mismo nombre. Se sugiere aclarar cuáles son las características del producto en cuestión.

¹ http://www.linux-mips.org/wiki/Innova_Card_SoC

Las reivindicaciones 16 y 26 no son claras porque presenta un archivo como características esenciales del aparato. Los archivos al no ser tangibles no pueden hacer parte de las características estructurales de un aparato y por lo tanto un aparato no puede caracterizarse por tener archivos.

5. Determinación del Estado de la Técnica

El estado de la técnica se determinó con base en la fecha de presentación de la solicitud de prioridad: diciembre 22 de 2010 y se encontraron los siguientes documentos que anticipan el objeto de esta solicitud:

Ítem	Documento	Título	Fecha de Publicación
D1	US 2010/0318468	“Tamper-Resistant Secure Methods, Systems and Apparatuses for Credit and Debit Transactions”	16/Diciembre/2010
D2	US 2008/0040287	“Fuel Dispenser Management”	14/Febrero/2008
D3	US 2008/0235140	“Digital Rights Management Dongle”	25/Septiembre/2008

El documento D1² divulga un procedimiento y dispositivos para el pago en transacciones electrónicas (Resumen).

El documento D2³ divulga un sistema y proceso para gestionar una gasolinera (Resumen).

El documento D3⁴ divulga un dispositivo de habilitación (Dongle) para gestionar la protección de derechos de autor que incluye un motor de encriptación (Resumen).

6. Examen de Patentabilidad (Art 14 D486)

Es importante mencionar que el siguiente análisis de patentabilidad se realizó teniendo en cuenta las objeciones del numeral 4 de la presente comunicación.

Novedad (Art 16 D486)

La reivindicación 1 consiste en “Un sistema usado en un entorno minorista para la provisión de la encriptación de extremo a extremo de los datos del titular de la tarjeta de pago...” (Ver página 34 del radicado N° 13-169786-00000-0000).

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

Características esenciales	D1
Un dispositivo de entrada.	Dispositivo del vendedor en el punto de venta (POS) (Fig. 1, zona 1) que tiene un lector de banda y un motor de encriptamiento (Fig. 2, elementos 201 y 205).
Un dispositivo de manipulación de los datos del titular de la tarjeta, en comunicación electrónica con dicho dispositivo de entrada.	CPU conectado al motor de encriptamiento (Fig. 2, elemento 215).
Un sistema de evaluación segura, operativamente conectado con dicho dispositivo de manipulación de los datos del	Entrada de la red de autorización (Fig. 1, zona 2).

2 http://worldwide.espacenet.com/searchResults?compact=false&PN=US2010318468&ST=advanced&locale=en_EP&DB=EPODOC

3 http://worldwide.espacenet.com/searchResults?compact=false&PN=US2008040287&ST=advanced&locale=en_EP&DB=EPODOC

4 http://worldwide.espacenet.com/searchResults?compact=false&PN=US2008235140&ST=advanced&locale=en_EP&DB=EPODOC

titular de la tarjeta.	
Comprendiendo dicho sistema de evaluación segura la electrónica de control respecto a la manipulación indebida.	Modulo de seguridad de resistencia a la manipulación (Pág. 3, Párr. 60; Fig. 1, elemento 101).

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

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

- Reivindicaciones 10 y 11: Dispositivo del vendedor en el punto de venta (POS) (Fig. 1, zona 1) que tiene un circuito de respuesta y detección de manipulación (Fig. 2, elementos 215 y 225) y modulo de seguridad de resistencia a la manipulación (Pág. 3, Párr. 60; Fig. 1, elemento 101).

De acuerdo con el análisis anterior, las reivindicaciones dependientes 10 y 11 no mencionan alguna característica que haga nuevo al sistema de la reivindicación 1, por lo cual, se considera que no son nuevas.

De igual manera, las reivindicaciones dependientes 2 y 6 a 9 no mencionan características técnicas tangibles adicionales que puedan brindarle novedad al sistema de la reivindicación 1, puesto que se encuentran redactadas en términos de usos, resultados y/o funcionalidades.

La reivindicación 12 consiste en *“Un sistema de evaluación segura, en el cual una comunicación encriptada de los datos del titular de la tarjeta, desde un dispositivo de entrada hacia un sistema procesador anfitrión remoto, puede ser evaluada de forma segura...”* (Ver página 36 del radicado N° 13-169786-00000-0000).

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

Características esenciales	D1
Una electrónica de control seguro.	Modulo de seguridad de resistencia a la manipulación (Pág. 3, Párr. 60; Fig. 1, elemento 101; Fig. 4, elemento 411).
Una memoria del sistema de evaluación segura.	Memoria en la entrada de la red de autorización (Fig. 4, elemento 405).

De acuerdo con la tabla anterior, las características esenciales del sistema de la reivindicación 12 habían sido divulgadas previamente en el documento D1, por lo tanto, la materia reivindicada no es nueva.

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

- Reivindicación 17: Modulo de seguridad de resistencia a la manipulación (Pág. 3, Párr. 60; Fig. 1, elemento 101).
- Reivindicación 18: Modulo de seguridad de resistencia a la manipulación con memoria (Fig. 4, elementos 411 y 415).
- Reivindicaciones 22 y 23: Dispositivo del vendedor en el punto de venta (POS) (Fig. 1, zona 1) que tiene un lector de banda, un motor de encriptamiento y CPU conectados a la entrada de la red de autorización (Fig. 1, Zona 1 y 2; Fig. 2,

- elementos 201, 205 y 215).
- Reivindicación 27: Dispositivo del vendedor en el punto de venta (POS) (Fig. 1, zona 1) con CPU (Fig. 2, elemento 215) y entrada de la red de autorización con CPU (Fig. 4, elemento 403).

De acuerdo con el análisis anterior, las reivindicaciones dependientes 17, 18, 22, 23 y 27 no mencionan alguna característica que haga nuevo al sistema de la reivindicación 12, por lo cual, se considera que no son nuevas.

De igual manera, las reivindicaciones dependientes 13 a 16, 20 y 24 a 26 no mencionan características técnicas tangibles adicionales que puedan brindarle novedad al sistema de la reivindicación 12, puesto que se encuentran redactadas en términos de usos, resultados y/o funcionalidades.

Nivel inventivo (Art18 D486)

La reivindicación 3 consiste en “*Un sistema como en la reivindicación 2...*” (Ver página 35 del radicado N° 13-169786-00000-0000).

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

R*	Características esenciales	D1	D3
1	Un dispositivo de entrada.	Dispositivo del vendedor en el punto de venta (POS) (Fig. 1, zona 1) que tiene un lector de banda y un motor de encriptamiento (Fig. 2, elementos 201 y 205).	Entrada de recursos encriptados (Pág. 1, Párr. 3; Fig. 1, elemento 150).
	Un dispositivo de manipulación de los datos del titular de la tarjeta, en comunicación electrónica con dicho dispositivo de entrada.	CPU conectado al motor de encriptamiento (Fig. 2, elemento 215).	Chip set (Fig. 1, elemento 155)
	Un sistema de evaluación segura, operativamente conectado con dicho dispositivo de manipulación de los datos del titular de la tarjeta.	Entrada de la red de autorización (Fig. 1, zona 2).	Dongle (Fig. 1, elemento 160).
	Comprendiendo dicho sistema de evaluación segura la electrónica de control respecto a la manipulación indebida.	Modulo de seguridad de resistencia a la manipulación (Pág. 3, Párr. 60; Fig. 1, elemento 101).	No menciona.
3	Sistema de evaluación segura está implementado como a candado electrónico.	No menciona.	Dongle (Fig. 1, elemento 160).

Los documentos D1 y D3 se consideran el estado de la técnica cercano a la invención definida en la reivindicación 3 porque divulgan un procedimiento y dispositivos para el pago en transacciones electrónicas (D1, Resumen) y un dispositivo de habilitación (Dongle) para gestionar la protección de derechos de autor que incluye un motor de encriptación (D2, Resumen).

La diferencia entre la invención, definida en la reivindicación 3 y el sistema de D1 consiste en la implementación utilizando un candado electrónico (Dongle).

La diferencia entre la invención, definida en la reivindicación 3 y el procedimiento de D3

consiste en la electrónica de control respecto a la manipulación indebida.

El efecto que logra el incluir un candado electrónico es que facilita la distribución y portabilidad de las funcionalidades del sistema impidiendo uso no autorizado.

Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así: “¿cómo modificar el sistema conocido en D1 para facilitar la distribución y portabilidad de las funcionalidades del sistema impidiendo uso no autorizado?”.

Sin embargo, la utilización de dispositivos de habilitación (Dongle) para facilitar la distribución y portabilidad de las funcionalidades del sistema impidiendo uso no autorizado, ya está divulgada en el documento D3 que se refiere a un Dongle (Fig. 1, elemento 160). Adicionalmente se indica que la utilización de dispositivos de habilitación hace parte del conocimiento de la persona del oficio medianamente versada en la materia, la cual conoce el uso de Dongles, incluyendo los que se conectan por USB, para facilitar la distribución y portabilidad de las funcionalidades del sistema impidiendo uso no autorizado⁵.

En consecuencia, la persona del oficio normalmente versada en la materia, incluiría los dispositivos de habilitación (Dongle) del documento D3, en el sistema divulgado en el documento D1 para llegar así al objeto de la reivindicación 3 de la solicitud. Por lo cual, se considera obvia.

Asimismo, el documento D3 divulga las características de las reivindicaciones dependientes así:

- Reivindicación 4: Dongle que se acopla por el puerto serial (Pág. 2, Párr. 15).

De acuerdo con el análisis anterior, la reivindicación dependiente 4 no menciona alguna característica que le dé nivel inventivo al objeto de la reivindicación 3, por lo cual, se considera que no tienen nivel inventivo.

La reivindicación 5 consiste en “Un sistema como en la reivindicación 2...” (Ver página 35 del radicado N° 13-169786-00000-0000).

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

R*	Características esenciales	D1
1	Un dispositivo de entrada.	Dispositivo del vendedor en el punto de venta (POS) (Fig. 1, zona 1) que tiene un lector de banda y un motor de encriptamiento (Fig. 2, elementos 201 y 205).
	Un dispositivo de manipulación de los datos del titular de la tarjeta, en comunicación electrónica con dicho dispositivo de entrada.	CPU conectado al motor de encriptamiento (Fig. 2, elemento 215).
	Un sistema de evaluación segura, operativamente conectado con dicho dispositivo de manipulación de los datos del titular de la tarjeta.	Entrada de la red de autorización (Fig. 1, zona 2).
	Comprendiendo dicho sistema de evaluación segura la electrónica de control respecto a la manipulación indebida.	Modulo de seguridad de resistencia a la manipulación (Pág. 3, Párr. 60; Fig. 1, elemento 101).

⁵ http://en.wikipedia.org/w/index.php?title=Software_protection_dongle&oldid=402885209

5	Electrónica de control respecto a la manipulación indebida es implementada como un chip USIP.	No menciona.
---	---	--------------

El documento D1 se considera el estado de la técnica cercano a la invención definida en la reivindicación 5 porque divulgan un procedimiento y dispositivos para el pago en transacciones electrónicas (D1, Resumen).

La diferencia entre la invención, definida en la reivindicación 5 y el sistema de D1 consiste en la implementación utilizando un chip USIP.

El efecto que logra el incluir un chip USIP es que facilita la implementación de terminales confiables.

Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así: “¿cómo modificar el sistema conocido en D1 para facilita la implementación de terminales confiables?”.

Sin embargo, la utilización de chips USIP para facilita la implementación de terminales confiables, hace parte del conocimiento de la persona del oficio medianamente versada en la materia^{6 7}.

En consecuencia, la persona del oficio normalmente versada en la materia, incluiría un chip USIP, en el sistema divulgado en el documento D1 para llegar así al objeto de la reivindicación 5 de la solicitud. Por lo cual, se considera obvia.

La reivindicación 19 consiste en “*Un sistema de evaluación segura como en la reivindicación 18...*” (Ver página 37 del radicado N° 13-169786-00000-0000).

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

R*	Características esenciales	D1
12	Una electrónica de control seguro.	Modulo de seguridad de resistencia a la manipulación (Pág. 3, Párr. 60; Fig. 1, elemento 101; Fig. 4, elemento 411).
	Una memoria del sistema de evaluación segura.	Memoria en la entrada de la red de autorización (Fig. 4, elemento 405).
19	Dicha electrónica de control seguro está implementada como un chip USIP.	No menciona.

El documento D1 se considera el estado de la técnica cercano a la invención definida en la reivindicación 19 porque divulgan un procedimiento y dispositivos para el pago en transacciones electrónicas (D1, Resumen).

La diferencia entre la invención, definida en la reivindicación 19 y el sistema de D1 consiste en la implementación utilizando un chip USIP.

El efecto que logra el incluir un chip USIP es que facilita la implementación de terminales confiables.

Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así: “¿cómo modificar el sistema conocido en D1 para facilita la implementación de terminales confiables?”.

6 http://www.innova-card.com/upload/gestionFichiers/CNA0107_chip_vendor_focus_838.pdf
 7 <http://fixunix.com/linux/263234-%5Bnews%5D-linux-continues-march-into-points-sale.html>

Sin embargo, la utilización de chips USIP para facilita la implementación de terminales confiables, hace parte del conocimiento de la persona del oficio medianamente versada en la materia^{8 9}.

En consecuencia, la persona del oficio normalmente versada en la materia, incluiría un chip USIP, en el sistema divulgado en el documento D1 para llegar así al objeto de la reivindicación 19 de la solicitud. Por lo cual, se considera obvia.

La reivindicación 21 consiste en “*Un sistema de evaluación segura como en la reivindicación 18...*” (Ver página 37 del radicado N° 13-169786-00000-0000).

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

R*	Características esenciales	D1
12	Una electrónica de control seguro.	Modulo de seguridad de resistencia a la manipulación (Pág. 3, Párr. 60; Fig. 1, elemento 101; Fig. 4, elemento 411).
	Una memoria del sistema de evaluación segura.	Memoria en la entrada de la red de autorización (Fig. 4, elemento 405).
21	Una interfaz USB.	No menciona.

El documento D1 se considera el estado de la técnica cercano a la invención definida en la reivindicación 21 porque divulgan un procedimiento y dispositivos para el pago en transacciones electrónicas (D1, Resumen).

La diferencia entre la invención, definida en la reivindicación 21 y el sistema de D1 consiste en una interfaz USB.

El efecto que logra el incluir una interfaz USB es que permite el uso de periféricos tales con un dispositivo de habilitación (Dongle).

Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así: “¿cómo modificar el sistema conocido en D1 para permitir el uso de periféricos tales con un dispositivo de habilitación (Dongle)?”.

Sin embargo, la de la interfaz USB para permitir el uso de periféricos tales con un dispositivo de habilitación (Dongle), hace parte del conocimiento de la persona del oficio medianamente versada en la materia^{5 10}.

En consecuencia, la persona del oficio normalmente versada en la materia, incluiría una interfaz USB, en el sistema divulgado en el documento D1 para llegar así al objeto de la reivindicación 21 de la solicitud. Por lo cual, se considera obvia.

La reivindicación 28 consiste en “*Un método para el procesamiento de una transacción, involucrando los datos del titular de la tarjeta en un sistema de pago minorista...*” (Ver página 38 del radicado N° 13-169786-00000-0000).

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

Características esenciales	D1	D2
La recepción de los datos del titular de la tarjeta en un dispositivo de entrada.	Recepción de los datos de usuario (Pág. 4, Párr. 78; Fig. 3, elemento 305).	Recibir información de transacción de un cliente (Pág. 1, Párr. 7).

8 http://www.innova-card.com/upload/gestionFichiers/CNA0107_chip_vendor_focus_838.pdf

9 <http://fixunix.com/linux/263234-%5Bnews%5D-linux-continues-march-into-points-sale.html>

10 <http://en.wikipedia.org/w/index.php?title=USB&oldid=403474890>

La encriptación de dichos datos del titular de la tarjeta, de acuerdo con un primer método de encriptación, con el fin de producir los primeros datos encriptados del titular de la tarjeta.	Encriptación de los datos de usuario (Pág. 4, Párr. 79; Fig. 3, elemento 307).	No menciona.
La recepción de dichos primeros datos encriptados del titular de la tarjeta en un sistema de evaluación segura, acoplado a un dispositivo de manipulación de los datos del titular de la tarjeta.	Recepción de los datos de transacción encriptados en la zona 2 (Pág. 5, Párr. 87; Fig. 3, elemento 307).	No menciona.
La desencriptación de dichos primeros datos encriptados del titular de la tarjeta, con el fin de producir los datos no encriptados del titular de la tarjeta.	Desencriptar datos de la transacción (Pág. 7, Párr. 98; Fig. 5, elemento 507).	No menciona.
La evaluación de dichos datos no encriptados del titular de la tarjeta en a una electrónica de control seguro, con el fin de determinar si dichos datos no encriptados del titular de la tarjeta son los datos del titular de la tarjeta de pago, o los datos no sensibles del titular de la tarjeta.	No menciona.	Se determina si una porción de los datos requiere medidas de seguridad (Pág. 1, Párrs. 7 y 8).
Si dichos datos no encriptados del titular de la tarjeta son los datos del titular de la tarjeta de pago, encriptando dichos datos no encriptados del titular de la tarjeta, de acuerdo con un segundo método de encriptación, con el fin de producir los segundos datos encriptados del titular de la tarjeta.	Re-encripta los datos de transacción (Pág. 7, Párr. 98; Fig. 5, elemento 509).	Se encripta la porción de datos que requieren medidas de seguridad (Pág. 1, Párrs. 7 y 8).

Los documentos D1 y D2 se consideran el estado de la técnica cercano a la invención definida en la reivindicación 28 porque divulgan un procedimiento y dispositivos para el pago en transacciones electrónicas (D1, Resumen) y un sistema y proceso para gestionar una gasolinera (D2, Resumen).

La diferencia entre la invención, definida en la reivindicación 28 y el método de D1 consiste en el paso de evaluación de datos del titular de la tarjeta con el fin de determinar si dichos datos son los datos de pago o datos no sensibles y en caso de ser datos de pago, encriptar dichos datos.

La diferencia entre la invención, definida en la reivindicación 28 y el método de D2 consiste en los pasos de encriptación y desencriptación anteriores a la determinación de una porción de datos que requieren medidas de seguridad.

El efecto que logra el incluir el paso de evaluación de datos del titular de la tarjeta con el fin de determinar si dichos datos son los datos de pago o datos no sensibles y en caso de ser datos de pago, encriptar dichos datos, es que permite proteger la información sensible necesaria para transacciones comerciales y dejar disponible la demás información.

Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así: “¿cómo modificar el método conocido en D1 para permitir proteger la información sensible necesaria para transacciones comerciales y dejar disponible la demás información?”.

Sin embargo, el paso de evaluación de datos del titular de la tarjeta con el fin de determinar si dichos datos son los datos de pago o datos no sensibles y en caso de ser datos de pago, encriptar dichos datos, para permitir proteger la información sensible necesaria para transacciones comerciales y dejar disponible la demás información, hace parte del conocimiento de la persona del oficio medianamente versada en la

materia⁵ ¹¹.

Sin embargo, la utilización del paso de evaluación de datos del titular de la tarjeta con el fin de determinar si dichos datos son los datos de pago o datos no sensibles y en caso de ser datos de pago, encriptar dichos datos, para permitir proteger la información sensible necesaria para transacciones comerciales y dejar disponible la demás información, ya está divulgada en el documento D2 que se refiere a pasos de determina si una porción de los datos requiere medidas de seguridad (Pág. 1, Párrs. 7 y 8) y encriptar la porción de datos que requieren medidas de seguridad (Pág. 1, Párrs. 7 y 8).

En consecuencia, la persona del oficio normalmente versada en la materia, incluiría el paso de evaluación de datos del titular de la tarjeta con el fin de determinar si dichos datos son los datos de pago o datos no sensibles y en caso de ser datos de pago, encriptar dichos datos, en el método divulgado en el documento D1 para llegar así al objeto de la reivindicación 28 de la solicitud. Por lo cual, se considera obvia.

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

- Reivindicación 30: Modulo de seguridad de resistencia a la manipulación (Pág. 3, Párr. 60; Fig. 1, elemento 101).
- Reivindicación 31: La información cifrada en la zona 1 es descriptada y re-encryptada en el formato de la zona 2 (Pág. 6, Párr. 90), donde los datos de la zona 1 están encriptados bajo parámetros y protocolos diferentes y la zona 2 permite una re-encryptación bajo un esquema consistente (Pág. 6, Párr. 89).
- Reivindicación 32: Los datos de transacción re-encryptados y transmitidos a la zona 3 (Pág. 7, Párr. 98).
- Reivindicación 33: Dispositivo del vendedor en el punto de venta (POS) (Fig. 1, zona 1).
- Reivindicación 34: Modulo de seguridad de resistencia a la manipulación con funcionalidad de autenticación (Fig. 4, elemento 411; Pág. 6, Párr. 93).

Asimismo, el documento D2 divulga las características de las reivindicaciones dependientes así:

- Reivindicación 29: Transmisión de los datos que no requieren medidas de seguridad (Pág. 1, Párr. 13).
- Reivindicación 32: Transmisión de los datos que requieren medidas de seguridad (Pág. 1, Párr. 13).
- Reivindicación 33: Sistema en una gasolinera (Resumen).

De acuerdo con el análisis anterior, la reivindicación dependiente 29 a 34 no menciona alguna característica que le dé nivel inventivo al objeto de la reivindicación 28, por lo cual, se considera que no tienen nivel inventivo.

De igual manera, la reivindicación dependiente 35 no menciona alguna característica que le dé nivel inventivo al objeto de la reivindicación 28, puesto que la implementación de sistemas como candados electrónicos hace parte del conocimiento de la persona del oficio medianamente versada en la materia. La persona del oficio medianamente versada en la materia conoce el uso de Dongles, incluyendo los que se conectan por USB, para facilitar la distribución y portabilidad de las funcionalidades del sistema impidiendo el uso no autorizado⁵.

¹¹ <http://en.wikipedia.org/w/index.php?title=USB&oldid=403474890>

7. Conclusión

Los requisitos de patentabilidad de la presente solicitud están afectados de acuerdo a las objeciones del numeral 4 y así:

Ítem	Documento	Reivindicaciones afectadas	Requisito que afecta
D1	US 2010/0318468	1, 2, 6 a 18, 20 y 22 a 27 3, 5, 19, 21, 28 y 30 a 35	Novedad/Nivel Inventivo Nivel inventivo
D2	US 2008/0040287	28, 29, 32, 33 y 35	Nivel inventivo
D3	US 2008/0235140	3 y 4	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 del día siguiente 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.

Se invita al solicitante se sirva indicar, si así lo considera, su renuncia al término faltante de sesenta (60) días para dar respuesta a este requerimiento y presentarla por escrito.

Finalmente, 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, no pagará la tasa de modificación voluntaria pero sí la correspondiente al pago por reivindicación adicional.

Notifíquese el presente oficio conforme a lo dispuesto en el numeral 5.2, literal e), del capítulo quinto del título primero de la Circular Única No. 10 de 2001.



JOSÉ LUIS SALAZAR LÓPEZ
Director de Nuevas Creaciones (c)

El anterior requerimiento fue notificado por fijación en lista, de fecha 2014-07-15

Elaboró: Francisco Javier Gonzalez Paez
Revisó: Rosa Patricia Tellez Chavarro