



No. 13-169786- -00005-0000

Fecha: 2014-10-08 16:13:45 Dep. 2020 DIR.NUEVASCR
Tra. 11 PATENTEIYII Eve: 378 FASENACIONALI
Act. 523 RESPUESTA Folios: 25

As. 125.085

Señor

**DIRECTOR DIVISIÓN DE NUEVAS CREACIONES
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO**

E. S. D.

REF: Expediente No. **13 169.786**– solicitud de patente de invención a favor de **GILBARCO INC. AND GILBARCO S.R.L.** Título: **SISTEMA DE PAGO EN EL SURTIDOR DE COMBUSTIBLE PARA ASEGURAR LA EVALUACIÓN DE LOS DATOS DEL TITULAR DE LA TARJETA.**

RESPUESTA A EXAMEN DE FONDO

JUAN PABLO CADENA SARMIENTO, portador de la tarjeta profesional No. 57.492 del C.S.J., obrando como apoderado de la sociedad solicitante me permito dar respuesta al Oficio No. 8113 relacionado con la patentabilidad de la presente invención y notificado por fijación en lista el 15 de Julio de 2014.

Atendiendo a las objeciones manifestadas por su Despacho, nos permitimos remitir un nuevo pliego reivindicatorio compuesto por treinta y cinco (35) reivindicaciones, las cuales encuentran total sustento en el capítulo descriptivo y no exceden en ningún momento el alcance de la invención inicialmente divulgada. Adjuntamos también el recibo correspondiente a la tasa de estudio de veinticinco (25) reivindicaciones adicionales.

Antes de proceder a presentar nuestros argumentos frente a las objeciones expuestas en el Oficio No. 8113, consideramos pertinente manifestar que las reivindicaciones

independientes del pliego reivindicatorio, es decir las reivindicaciones 1, 12 y 28, se modificaron para incluir que los datos del titular de la tarjeta *"comprenden por lo menos uno de datos de pago del titular de la tarjeta y datos no sensibles del titular de la tarjeta"*.

Esta modificación se realizó con el objetivo de puntualizar que los datos del titular de la tarjeta pueden incluir datos de pago, datos no sensibles o datos de pago y datos no sensibles del titular de la tarjeta. El debido soporte de tal modificación se encuentra en los párrafos [0021] y [0022] de la solicitud en inglés.

Claridad

Las reivindicaciones 1 y 18 fueron objetadas por incluir funcionalidades que no le dan novedad y/o nivel inventivo a un producto.

Frente a esta observación nos permitimos señalar que si bien las reivindicaciones 1 y 18 contienen algunas características funcionales, no todos los términos aludidos se deberían incluir en el grupo de funcionalidades que *"no le pueden dar novedad y/o nivel inventivo a un producto"*; puesto que algunas de las expresiones objetadas corresponden a limitaciones que contribuyen a definir el alcance de la presente invención, otorgándole novedad y nivel inventivo y permitiendo diferenciarla del estado de la técnica .

Para evidenciar lo anteriormente expuesto, nos permitimos presentar una porción de la reivindicación 1, donde los términos que el señor Examinador identificó como funcionalidades se encuentran subrayados,

un dispositivo de entrada configurado para recibir los datos del titular de la tarjeta, dichos datos del titular de la tarjeta comprenden por lo menos uno de datos de pago del titular de la tarjeta y datos no sensibles del titular de la tarjeta, dicho dispositivo de entrada opera 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;

Así, si por ejemplo se definiera simplemente un dispositivo de entrada y se ignorara que este opera para encriptar los datos del titular de la tarjeta, en efecto se estaría reivindicando cualquier dispositivo de entrada, tales como un micrófono, un teclado, un mouse, etc. Sin embargo, no todos los objetos que se pueden definir como dispositivo de entrada tienen la configuración necesaria para recibir datos de titular de la tarjeta.

De esta manera, cuando la reivindicación especifica que el dispositivo de entrada está *"configurado para recibir los datos del titular de la tarjeta..."* limita el alcance de la invención y reivindica únicamente aquellos dispositivos de entrada que permiten la recepción de datos de un titular de la tarjeta, no cualquier dispositivo de entrada indiscriminadamente. En concreto, tal expresión catalogada como funcionalidad que no aporta novedad ni nivel inventivo, permite definir el verdadero alcance de la invención.

Por otro lado, suponiendo que se incluyeran en la reivindicación la totalidad de las características estructurales de dicho dispositivo de entrada que le permiten recibir los datos del titular de la tarjeta, se tendría que restringir considerable e innecesariamente el alcance de la invención, puesto que sería necesario describir la configuración electrónica, las partes del dispositivo, la configuración del software, etc. De tal manera, consideramos que siempre y cuando se especifique el objeto de tal configuración, esto es, para recibir los datos de la tarjeta, la invención se define con la suficiente claridad para que el versado en la materia pueda entender el tipo particular de dispositivo que se está reivindicando y consecuentemente pueda diferenciar la invención del estado de la técnica.

Por consiguiente, dada la naturaleza intrínseca de la invención, es necesario recurrir a estos términos (configurado para...) para poder definir el verdadero alcance de la invención y por lo tanto estas expresiones deberían tenerse en cuenta en el análisis de patentabilidad, y no simplemente obviarse por incluir la palabra *para*.

Solicitamos entonces amablemente que el señor Examinador diferencie las características funcionales de la reivindicación, tales como *"con el fin de producir los primeros datos encriptados del titular de la tarjeta"*, *"con el fin de producir los datos no*

encriptados del titular de la tarjeta”...de las limitaciones que definen el alcance de la reivindicación, como por ejemplo, “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”, “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”.

Igualmente, las reivindicaciones 2, 3, 6-10, 12-17, 20 y 24-26 fueron objetadas por estar caracterizadas por resultados a alcanzar o funcionalidades y no por características esenciales.

Al respecto, nuevamente indicamos que algunas de las expresiones consideradas por el señor Examinador como funcionalidades o resultados a alcanzar, que no otorgan novedad ni nivel inventivo al pliego reivindicatorio son, en efecto, características esenciales que limitan la reivindicación y por lo tanto permiten diferenciar la invención del estado de la técnica.

Por ejemplo, la expresión *“donde dicha electrónica de control seguro 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”* de la reivindicación 12, no corresponde solamente a un resultado a alcanzar o funcionalidad. Por el contrario, especifica, y por lo tanto limita la electrónica de control reivindicada, a aquella electrónica de control que permita evaluar los datos no encriptados y encripte solo aquellos datos que corresponden a datos de pago de acuerdo con una evaluación de dichos datos.

Tal y como se argumentó en párrafos anteriores, la evaluación de patentabilidad no debería excluir expresiones enteras solo por el hecho de comprender la palabra *para*. Por el contrario, el señor Examinador podría considerar que en algunas ocasiones, tal y como es el caso, es impráctico e incluso inaplicable poder reivindicar un sistema de otra forma que no sea mediante la actividad de sus partes dentro del sistema; y que

esta actividad de dichas partes corresponde a limitaciones sobre el sistema que aportan novedad y/o nivel inventivo a la reivindicación.

En conclusión, de acuerdo con los argumentos y ejemplos desarrollados, solicitamos amablemente que se tengan en cuenta aquellas expresiones catalogadas como funcionalidades que divulgan limitaciones y que por lo tanto, aportan novedad y/o nivel inventivo al pliego reivindicatorio.

Por otra parte, la reivindicación 5 fue objetada por hacer referencia a USIP®, el cual es una marca registrada. En respuesta a esta objeción, nos acogemos voluntariamente a la sugerencia del señor Examinador y reemplazamos el término USIP® por las características del producto en cuestión i.e. *circuito integrado de seguridad*.

Las reivindicaciones 16 y 26, objetadas por presentar un archivo como característica esencial del método, fueron modificadas de forma que ahora reivindican respectivamente *datos contra los cuales se comparan los datos no encriptados del titular de la tarjeta para determinar si dichos datos no encriptados corresponden a datos de pago; y datos representativos de un registro de la transacción contra los cuales se compara los datos de pago del titular de la tarjeta*, de tal manera que ya no se divulga un archivo.

Novedad

La novedad de las reivindicaciones independientes 1 y 12 fue afectada en vista de las enseñanzas del documento D1 *"Tamper-Resistant Secure Methods, Systems and Apparatuses for Credit and Debit Transactions"*.

Como punto de partida consideramos pertinente señalar que en el examen de patentabilidad no se tomaron en consideración algunos elementos de las reivindicaciones 1 y 12, los cuales limitan la materia reivindicada y por lo tanto son necesarios para diferenciarla del estado de la técnica.

Por ejemplo, el señor Examinador tomó en consideración únicamente los siguientes elementos de la reivindicación 1,

- Un dispositivo de entrada.
- Un dispositivo de manipulación en comunicación con el dispositivo de entrada.
- Un sistema de evaluación segura conectado con el dispositivo de manipulación.
- El sistema de manipulación segura comprende la electrónica de control respecto a la manipulación indebida.

No obstante, la reivindicación 1 no divulga un sistema de tal amplitud.

Primero, el sistema de la reivindicación 1 divulga que el dispositivo de entrada está configurado para recibir datos del titular de la tarjeta y que los datos del titular de la tarjeta comprenden *"por lo menos uno de datos de pago del titular de la tarjeta, y datos no sensibles del titular de la tarjeta."* Posteriormente, el dispositivo de entrada opera para encriptar los datos del titular de la tarjeta, de acuerdo a un primer método de encriptación para producir los primeros datos del titular de la tarjeta encriptados.

En otras palabras, el dispositivo de entrada recibe los datos del titular de la tarjeta y encripta todo este conjunto de datos, tanto los datos de pago como los datos no sensibles del titular de la tarjeta.

En contraste, en el sistema propuesto en D1, los datos no sensibles del titular de la tarjeta no se encriptan en el dispositivo de entrada. De hecho, en el sistema de D1, los datos no sensibles del titular de la tarjeta no se encriptan en absoluto.

Incluso, el documento D1 menciona explícitamente que el sistema de encriptación es un sistema de encriptación de extremo a extremo para proteger los "datos sensibles de pago y procesamiento" (Ver Párrafos [0044] a [0047]), pero no hace referencia alguna a la encriptación de los datos no sensibles.

Para demostrar con mayor certeza esta diferencia, consideramos que es necesario describir que el modelo descrito en la anterioridad D1 divide el sistema de extremo a extremo en cinco "zonas de pago", en las cuales, cuando los datos de transacción se mueven de una zona a otra, se pasan a través de un "módulo de seguridad de

hardware" (101), donde los datos de transacción se desenscriptan en la recepción y luego se re-enscriptan para su posterior transmisión o almacenamiento.

En este sentido, la *zona 1* de D1 representa el paso de una tarjeta de pago por un dispositivo de un establecimiento comercial que comprende un terminal (200), el cual puede ser un terminal de punto de venta (POS). Cuando se inicia una transacción en el terminal (200) *"los datos sensibles del titular de la tarjeta se reciben"* (Párr. [0078]) y *"son encriptados usando la clave simétrica específica del dispositivo del establecimiento comercial"* (Párr. [0079]). En algunos casos, los datos sensibles, que no corresponden a datos del usuario, tales como una *"identificación del comerciante"* también se reciben en el procesamiento de la solicitud; estos datos sensibles se encriptan mediante la clave simétrica específica del dispositivo. Sin embargo, los datos no sensibles "pueden permanecer en forma de texto" (Párr. [0081])

Por lo tanto, la *zona 1* o el terminal (200) de D1, comunica los datos encriptados de las transacciones y los datos de texto, en el caso en que haya alguno, de la transacción a un dispositivo de puerta de enlace de la *Zona 2* (400) del sistema de pago electrónico (Párr. [0087]).

De esta manera, cuando los datos se reciben en el dispositivo de entrada o terminal (200) de D1, los datos de pago se encriptan, mientras que aquellos **datos no sensibles no son encriptados, sino que se presentan en forma de texto.**

En definitiva, el documento D1 falla en divulgar una encriptación tanto de los datos de pago como de los datos no sensibles del titular de la tarjeta; por lo tanto, la reivindicación 1 es diferente de la anterioridad al menos por esta razón.

Por otra parte, el sistema de la reivindicación 1 también requiere un sistema de evaluación segura, conectado con un dispositivo de manipulación, el cual a su vez está conectado con el dispositivo de entrada.

Dicho sistema de evaluación segura, además de comprender una electrónica de control respecto a la manipulación indebida, está configurado para realizar:

- i. La desenscriptación de los datos inicialmente encriptados.

- ii. La evaluación de dichos datos descriptados.
- iii. Diferenciar los datos de pago de los datos no sensibles del titular de la tarjeta.
- iv. La encriptación, mediante un segundo método de encriptación, de los datos de descriptados si estos datos corresponden a datos de pago.

En otras palabras, a electrónica de control para evitar la manipulación indebida, de la reivindicación 1, evalúa los datos descriptados del titular de la tarjeta y determina si dichos datos son datos de pago o datos no sensibles del titular de la tarjeta. Adicionalmente, si los datos descriptados corresponden a los datos de pago, la electrónica de control encripta dichos datos descriptados de acuerdo con un segundo método de encriptación para producir datos encriptados.

Por el contrario, el documento D1 no divulga un sistema de evaluación segura que esté configurado para realizar todos estos pasos. De hecho, un sistema de evaluación segura en el documento D1 no podría razonablemente comprender la misma configuración; ya que el primer paso corresponde a la descriptación de los datos encriptados (los cuales incluyen tanto datos sensibles como datos no sensibles), pero debido a que nunca se encriptaron los datos no sensibles del titular de la tarjeta, estos físicamente no pueden descriptarse.

Para precisar lo anterior, procedemos a explicar el funcionamiento de *"la entrada a de la red de autorización"* de D1, la cual según consideración del señor Examinador, anticipa el sistema de evaluación segura de la reivindicación 1. Estas *"puertas de entrada de la red de autorización"* realmente corresponden a la zona 2 del sistema de encriptación descrito en la anterioridad. Los datos de transacción encriptados, enviados desde la zona 1, necesariamente deben ser enviados a dicha zona 2; puesto que los datos encriptados en la zona 1 son encriptados bajo protocolos diferentes a los protocolos del resto del sistema.

Así, la zona 2 del sistema de D1, permite que los datos de la transacción sean re-encriptados bajo un esquema coherente con el resto del sistema descrito en D1 (Párr. [0089]). La transición de un esquema de encriptación al otro sistema de encriptación, se realiza en el módulo de seguridad de hardware (101), el cual cuenta con protección

contra la manipulación, de manera que la información confidencial permanece protegida.

En general, el dispositivo de salida (400) de la zona 2 recibe los datos encriptados de la zona 1 y los comunica con el módulo de seguridad de hardware (101). Los datos encriptados de la zona 1 se desencriptan en el módulo de seguridad de hardware (101) y luego se re-encriptan de acuerdo con un esquema que es consistente con las zonas 2 a 4 y los datos encriptados de la zona 2 se emiten mediante el módulo de seguridad de hardware (101) al dispositivo de salida (400).

De acuerdo con lo anterior, puede afirmarse que el módulo de seguridad de hardware (101) de D1, “equivalente” a la electrónica de control respecto a la manipulación indebida de dicho sistema de evaluación segura de la reivindicación 1, no evalúa los datos no encriptados, con el fin de determinar si dichos datos no encriptados corresponden a datos de pago o a los datos no sensibles del titular de la tarjeta.

Incluso, D1 no podría divulgar tal limitación porque los datos de transacción que se encriptan en D1, no incluyen datos no sensibles, y por lo tanto, tales datos no sensibles nunca se podrían transmitir al módulo de seguridad de hardware (101).

Más aun, la reivindicación 1 requiere que la electrónica de control en contra de la manipulación esté adaptada para encriptar 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 solo si “*dichos datos no encriptados del titular de la tarjeta son los datos del titular de la tarjeta de pago*”.

Nuevamente, la anterioridad no puede en esencia cumplir con tal limitación, porque la re-encriptación divulgada en D1 no requiere una evaluación para decidir qué datos se re-encriptan, como si lo requiere la reivindicación 1; Sino que re-encripta la totalidad de los datos provenientes de la terminal, o dispositivo de entrada.

En síntesis, el documento D1 divulga un sistema tradicional de encriptación de extremo a extremo, en el cual nunca se encriptan los datos no sensibles del titular de la tarjeta, de forma que D1 tampoco podría describir todas las características del

sistema que se refieren a la descriptación y evaluación de tales datos no sensibles inicialmente encriptados.

Por lo tanto, la reivindicación 1, junto con sus respectivas reivindicaciones dependientes, comprenden condiciones técnicas y limitaciones no divulgadas en la anterioridad y por lo tanto cumplen con el requisito de novedad.

Ahora, en cuanto a la reivindicación independiente 12, esta reivindicación divulga un sistema de evaluación segura que comprende una electrónica de control seguro adaptada para descriptar los datos encriptados del titular de la tarjeta, de acuerdo con un primer método de encriptación. De forma similar que la reivindicación independiente 1, la reivindicación 12 específicamente requiere que los datos encriptados del titular de la tarjeta comprendan por lo menos uno de *"datos de pago del titular de la tarjeta"* y *"datos no sensibles del titular de la tarjeta"*.

Además, la reivindicación 12 requiere adicionalmente que la electrónica de control de seguridad esté adaptada ulteriormente para evaluar los datos no encriptados del titular de la tarjeta, para luego encriptar dichos datos no encriptados del titular de la tarjeta, de acuerdo con un segundo método de encriptación, sólo si dichos datos no encriptados son los datos de pago del titular de la tarjeta.

Por el contrario, y tal y como se discutió en párrafos anteriores, el documento D1 no divulga tales limitaciones, puesto que nunca se encriptan los datos no sensibles del titular de la tarjeta; de modo que estos no pueden evaluarse ni mucho menos re-encriptarse.

Adicionalmente la reivindicación 12 requiere una memoria del sistema de evaluación de seguridad que está encriptada de acuerdo con un tercer método de encriptación. Más aún, la electrónica de control de seguridad del sistema de la reivindicación 12 está adaptada para descriptar dicha memoria del sistema de evaluación segura.

En contraste, el documento D1 no divulga que la memoria (405) (la cual fue identificada en el examen de novedad como la memoria del sistema de evaluación de

seguridad de la reivindicación 12), está encriptada, o que el módulo de seguridad de hardware (411) opera para desencriptar dicha memoria (405).

Por consiguiente, basándose en los argumentos aquí expuestos, el requisito de novedad de la reivindicación 12 y sus respectivas reivindicaciones dependientes 13 a 27, no se ven afectadas por las enseñanzas del documento D1.

Nivel Inventivo

Si bien el Oficio presenta el examen de nivel inventivo sobre las reivindicaciones dependientes 3, 5, 19 y 21 y sobre la reivindicación independiente 28, consideramos pertinente aclarar que nuestros argumentos se van a enfocar en demostrar el nivel inventivo de las reivindicaciones independientes.

En este orden de ideas, comenzaremos por argumentar la reivindicación 28, para luego desarrollar sobre las reivindicaciones 1 y 12, ya que si se demostrara que estas últimas no son obvias, quedaría por consiguiente superada la objeción sobre las reivindicaciones dependientes 3, 5, 19 y 21.

El requisito de nivel inventivo de la reivindicación independiente 28 fue afectado en vista de las enseñanzas de los documentos D1 *"Tamper-Resistant Secure Methods, Systems and Apparatuses for Credit and Debit Transactions"* y D2 *"Fuel Dispenser Management"*.

En cuanto a esta objeción, el señor Examinador considera que el documento D1 divulga todas las limitaciones de la reivindicación 28, con excepción de la etapa que corresponde a *"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"*, la cual se encuentra divulgada en el documento D2 y por lo tanto, una persona normalmente en la materia hubiera modificado el sistema de D1 para incluir la etapa divulgada en D2 obteniendo el método reivindicado.

Sin embargo, la combinación de los documentos D1 y D2 no hubiera derivado en el método tal y como se reivindica, debido a que la reivindicación 28 requiere la encriptación de los datos del titular de la tarjeta, donde los datos encriptados comprenden tanto datos no sensibles, como datos de pago del titular de la tarjeta. Por el contrario, y tal como fue explicado en detalle en los párrafos anteriores, D1 describe únicamente la encriptación de la información sensible del titular de la tarjeta, y no divulga o sugiere la encriptación de la información no sensible del titular de la tarjeta.

Por su parte, el documento D2 no remedia tal deficiencia de D1, puesto que tampoco divulga la encriptación de los datos no sensibles junto con los datos sensibles del titular de la tarjeta.

Más aún, el documento D2 no divulga la encriptación de los datos del titular de la tarjeta en el mismo contexto de la reivindicación 28. En efecto, el documento D2 se relaciona con un sistema (100) en el manejo de la administración de combustible, en el cual los dispensadores de combustible (110) están bajo el control de un controlador de la instalación (120). Dichos dispensadores de combustible, están en comunicación con el controlador de instalación mediante una red de comunicación (130). Los dispensadores de combustible pueden obtener información de pago de un cliente y reenviar dicha información al controlador de la instalación mediante la red de comunicación. Seguidamente, el controlador de la instalación puede llevar a cabo comprobaciones de la validez y autorización de la información de pago del portador de la tarjeta, antes de autorizar la transacción a los dispensadores de combustible.

Sin embargo, y de acuerdo con D2, los dispensadores de combustible *“pueden operar independientemente del controlador de la instalación, por lo menos para ciertas funciones y/o periodos de tiempo”* en caso tal en que la red de comunicación del controlador de la instalación haya fallado o este en un modo de inoperatividad (Ver párrafo [0047]).

Esta operación independiente descrita en D2 *“puede incluir la habilidad de proveer operaciones en el punto de venta (POS)”* (Párr. [0048]). Específicamente, de acuerdo con la Figura 15 de D2, el dispensador de combustible puede recibir *“una porción de los datos de transacción”*, tales como *“el número de cuenta del cliente, el código de*

identificación, el código de autorización, y/o la información de compra” de un cliente (Párr. [0164]). En el caso tal en que no haya disponible un link de comunicación, el dispensador está en capacidad de determinar si los datos necesitan almacenarse en el dispensador por un periodo determinado de tiempo (Párr. [0165]) y en tales casos, el dispensador de combustible determina si los datos, o la porción de datos, que se van a almacenar, requieren *“una medida de seguridad”* (Párr. [0166]).

De acuerdo con lo anterior, D2 es específico al mencionar que la porción de datos almacenados requiere una medida de seguridad, solo si *“se ha designado como una porción de información sensible”*. Adicionalmente, D2 divulga que en caso tal en que se requiera dicha medida de seguridad, el dispensador de combustible encripta la porción de datos, para luego almacenarlos. Por el contrario, si no se requiere dicha medida de seguridad, la porción de datos simplemente se almacena (Párr. [0167] a [0169]).

Así, a partir de una lectura detallada del funcionamiento del sistema descrito en D2, es posible concluir que en este sistema, al igual que el descrito en D1, los datos no sensibles del portador de la tarjeta nunca se encriptan, de forma que ninguno de los documentos por separado, ni su combinación, hubieran llevado al versado en la materia a obtener el método de la reivindicación 28.

Del mismo modo, D2 tampoco divulga una etapa relativa a determinar si los datos encriptados del titular de la tarjeta corresponden a los datos de pago o a los datos no sensibles del titular de la tarjeta. Esta etapa, al igual que las demás etapas del método reivindicado, es necesaria para llegar a la solución del problema técnico propuesto. Por consiguiente, dado que el método que resulta de la combinación de D1 y D2 no incluye esta etapa, no podría dar solución al problema técnico planteado en la presente solicitud.

Más aun, la reivindicación 28 requiere las etapas de *“la evaluación de dichos datos no encriptados del titular de la tarjeta en una electrónica de control seguro, con el fin de determinar si dichos datos no encriptados del titular de la tarjeta son los datos de pago del titular de la tarjeta, o los datos no sensibles del titular de la tarjeta”;* y *“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”.

Por consiguiente, partiendo del hecho que los datos no sensibles del titular de la tarjeta nunca se encriptan, no es posible una posterior evaluación de los datos del titular de la tarjeta para determinar si estos corresponden a datos de pago o datos no sensibles, y mucho menos, una segunda encriptación de los datos de pago, de acuerdo con los resultados obtenidos de tal evaluación.

Por lo tanto, el método de la reivindicación 28 no se hubiera podido obtener de forma evidente a partir de los documentos D1 y D2, ni de su combinación, ya que ninguno de estos documentos divulga una encriptación de los datos no sensibles del titular de la tarjeta, siendo esta una condición técnica esencial que es indispensable para que se puedan llevar a cabo los otros pasos del método de la reivindicación 28.

Este argumento se puede exponer de forma más clara de acuerdo con las siguientes figuras,

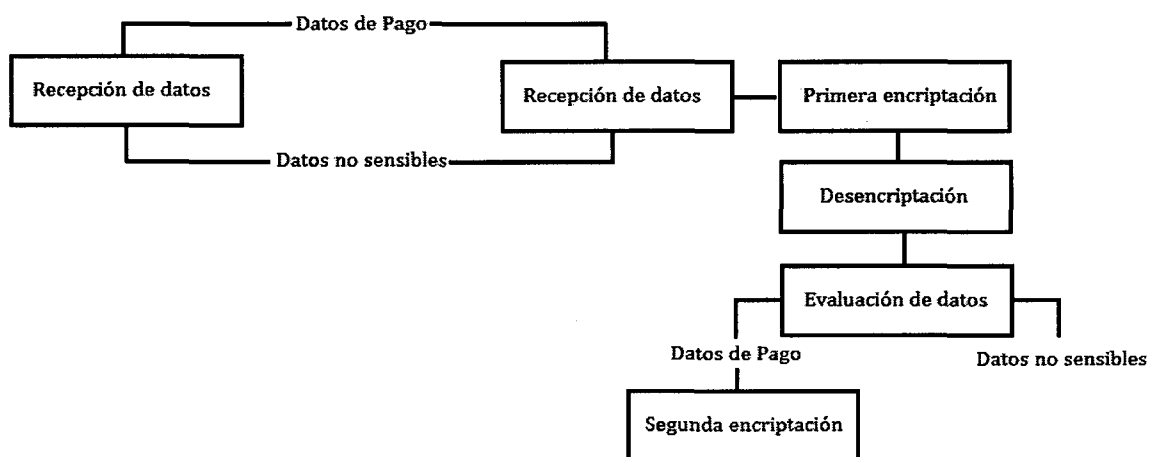


Figura 1. Método de la reivindicación 28

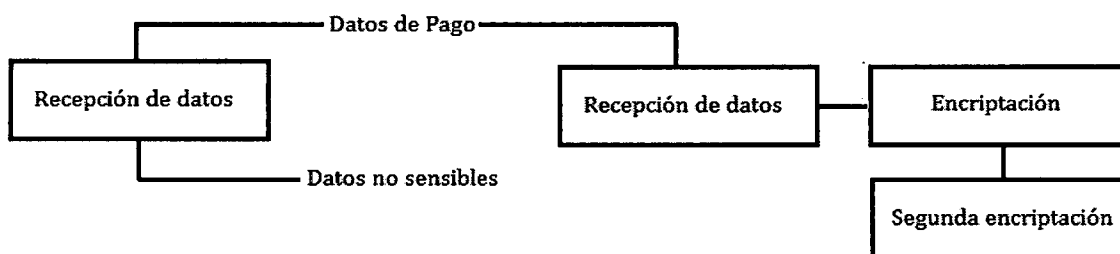


Figura 2. Método resultante de la combinación de D2 y D2.

Así, es evidente que dado que en el método que resulta de la combinación de las enseñanzas de los documentos citados nunca se encriptan los datos no sensibles, los datos no sensibles no pueden ser una entrada para las siguientes etapas del método, de forma que no es posible obtener el método de la presente invención tal y como se reivindica.

En cuanto a los sistemas de las reivindicaciones independientes 1 y 12, y tal y como se argumentó con respecto al requisito de novedad, el documento D1 no puede anticipar todas las limitaciones de la invención, porque el sistema divulga en este documento no requiere que los datos de transacción que se encriptan, incluyan datos no sensibles. Por consiguiente, un sistema que se obtenga a partir de las enseñanzas de D1, no puede incluir la posterior evaluación de tales datos no sensibles encriptados, ni una segunda etapa de encriptación de acuerdo con los “resultados” de dicha evaluación.

De igual manera, en coherencia con la naturaleza de funcionamiento del sistema descrito en D2, este documento tampoco puede divulgar tales limitaciones, dado que el sistema descrito en la anterioridad, no requiere la encriptación de los datos del titular de la tarjeta que comprende datos de pago del titular de la tarjeta, datos no sensibles del titular de la tarjeta, o las dos.

Como resultado, ni D1 ni D2, ni su combinación, pueden llevar al sistema de las reivindicaciones 1 y 12, con todas sus limitaciones, y por lo tanto, estas reivindicaciones, junto con sus respectivas reivindicaciones dependientes, cumplen con el requisito de nivel inventivo.

Más aún, el versado en la materia no llegaría a los sistemas de las reivindicaciones 1 y 12, ni al método de la reivindicación 28 modificando D1 con las enseñanzas de D2. El señor Examinador expone que la persona normalmente versada en la materia llevaría a cabo tal combinación para permitir *“proteger la información sensible necesaria para transacciones comerciales y dejar disponible la demás información”*. Esta afirmación es incorrecta, ya que este problema técnico objetivo **no existe** en el sistema divulgado en D1. Tal y como se mencionó en párrafos anteriores, la información no sensible nunca se encripta en el sistema de D1, y por lo tanto esta **siempre disponible**.

Ahora, las ventajas asociadas a encriptar la información no sensible es que el comerciante puede acceder a la información no sensible encriptada mediante el sistema de pago, y así, obtener o recuperar dicha información, la cual en el estado de la técnica, no se procesaba en el sistema de pago, sino que simplemente se presentaba como forma de texto, o no se presentaba en absoluto.

Por ejemplo mediante la presente invención, los comerciantes pueden acceder a los datos del titular de la tarjeta después de que son encriptados en un dispositivo de entrada, de forma que si un cliente reclama una transacción, el comerciante puede verificar el PAN, con el fin de probar que la transacción tuvo lugar.

De igual modo, el comerciante puede por ejemplo dar crédito a una cuenta del cliente o completar manualmente una transacción que previamente se rechazó debido a un error.

Así, la presente invención da solución a un problema técnico que no había sido resuelto, ni siquiera planteado, en el estado de la técnica, lo cual es un fuerte indicio de la presencia de nivel inventivo.

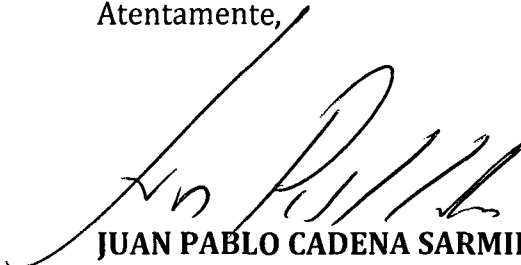
En conclusión, dado que la materia divulgada en las reivindicaciones 1, 12 y 28, no se hubiera podido derivar a partir de la combinación de las enseñanzas del estado de la técnica, ni se hubiera obtenido de manera evidente de los conocimientos de la persona normalmente versada en la materia, el pliego reivindicatorio cumple con el requisito de nivel inventivo.

En vista de lo anteriormente expuesto, respetuosamente solicitamos el retiro de las objeciones de la presente solicitud y la concesión del privilegio solicitado, ya que en opinión del solicitante cumple con todos los requisitos establecidos en la Decisión 486.

Anexos

Nuevo pliego reivindicatorio.

Atentamente,



JUAN PABLO CADENA SARMIENTO

T.P. No. 57.492 del C.S.J.

C.C. 80.410.337 de Usaquén

Calle 70 A No. 4 - 41

125085

18

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

NIT : 800.176.089-2

- / -



Industria y Comercio
SUPERINTENDENCIA

RECIBO DE CAJA

No. 14 - 0099012

Bogotá D.C., Septiembre 16 de 2014 - 17:29:59

RECIBIDO DE : BRIGARD & CASTRO S.A.

NI 860.047.372

*** Soporte del Pago ***

TIPO PAGO	BANCO	CUENTA	No. PAGO	FECHA PAGO	VR PAGO
CONSIGNACION	BANCO DE BOGOTA	062754387	610779315	16/09/2014	54.594.000.00

*** Conceptos Pagados ***

CANT.	RENTISTICO	CONCEPTO	Vr.UNDITARIO	Vr.CONCEPTO
5	50005-01-01 SOLICITUDES	1607 REIVINDICACION PATENTE UNITARIA ADICIONAL A LAS 10 INIC	31.000.00	155.000.00
				\$155.000.00

SON: **CIENTO CINCUENTA Y CINCO MIL PESOS MONEDA CORRIENTE***

Responsable: _____

Recibo de Caja Aplicado al Expediente No. _____

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO



No. 13-169786-00005-0000

Fecha: 2014-10-08 16:13:45 Dep. 2020 DIR.NUEVASCR
Tra. 11 PATENTEIYII Eve: 378 FASENACIONALI
Act. 523 RESPUESTA Folios: 25

Sede Centro: Carrera 13 No. 27 - 00 Pisos 3,4,5 y 10 Bogotá, D.C.- Colombia

Web: www.sic.gov.co e-mail: info@sic.gov.co Conmutador: (571) 5870000 Fax: (571) 5870284 Línea: 018000-910165 Call Center: (571) 6513240

, Septiembre 16 de 2014 - 17:30:23

125085

19

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

NIT : 800.176.089-2

- / -

Industria y Comercio
SUPERINTENDENCIA

RECIBO DE CAJA

No. 14 - 0010261

Bogotá D.C., Enero 29 de 2014 - 16:30:20

RECIBIDO DE : BRIGARD & CASTRO S.A.

NI 860.047.372

*** Soporte del Pago ***

TIPO PAGO	BANCO	CUENTA	No. PAGO	FECHA PAGO	VR PAGO
CONSIGNACION	BANCO DE BOGOTA	062754387	650529541	29/01/2014	27.663.000.00

*** Conceptos Pagados ***

CANT.	RENTISTICO	CONCEPTO	Vr. UNDITARIO	Vr. CONCEPTO
20	50005-01-01 SOLICITUDES	1607 REIVINDICACION PATENTE UNITARIA ADICIONAL A LAS 10 INIC	31.000.00	620.000.00
				\$620.000.00
			=====	

SON: **SEISCIENTOS VEINTE MIL PESOS MONEDA CORRIENTE***

Responsable: _____

Recibo de Caja Aplicado al Expediente No. _____

SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO



No. 13-169786- -00005-0000

Fecha: 2014-10-08 16:13:45 Dep. 2020 DIR.NUEVASCR
Tra. 11 PATENTEIYII Eve: 378 FASENACIONALI
Act. 523 RESPUESTA Folios: 25

Sede Centro: Carrera 13 No. 27 - 00 Pisos 3,4,5 y 10 Bogotá, D.C.- Colombia

Web: www.slc.gov.co e-mail: info@slc.gov.co Conmutador: (571) 5870000 Fax: (571) 5870284 Línea: 018000-910165 Call Center: (571) 6513240

Enero 29 de 2014 - 16:30:25

REIVINDICACIONES MODIFICADAS

1. 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, caracterizado porque dicho sistema comprende:

un dispositivo de entrada configurado para recibir los datos del titular de la tarjeta, dichos datos del titular de la tarjeta comprenden por lo menos uno de datos de pago del titular de la tarjeta y datos no sensibles del titular de la tarjeta, dicho dispositivo de entrada opera 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;

un dispositivo de manipulación de los datos del titular de la tarjeta, en comunicación electrónica con dicho dispositivo de entrada;

un sistema de evaluación segura, operativamente conectado con dicho dispositivo de manipulación de los datos del titular de la tarjeta, comprendiendo dicho sistema de evaluación segura la electrónica de control respecto a la manipulación indebida, adaptada para desenscriptar 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 de pago del titular de la tarjeta, 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 de pago del titular de la tarjeta, 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.

2. Un sistema como en la reivindicación 1, caracterizado 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.

3. Un sistema como en la reivindicación 2, caracterizado porque dicho sistema de evaluación segura está implementado como a candado electrónico.
4. Un sistema como en la reivindicación 3, caracterizado porque dicho candado electrónico comprende una interfaz USB.
5. Un sistema como en la reivindicación 2, caracterizado porque dicha electrónica de control respecto a la manipulación indebida es implementada como un circuito integrado de seguridad.
6. Un sistema como en la reivindicación 1, caracterizado porque dicho sistema de evaluación segura está adaptado para transmitir dichos segundos datos encriptados del titular de la tarjeta hacia un sistema procesador anfitrión remoto.
7. Un sistema como en la reivindicación 1, caracterizado porque dichos primer y segundo métodos de encriptación son los mismos.
8. Un sistema como en la reivindicación 1, caracterizado porque dichos primer y segundo métodos de encriptación son diferentes.
9. Un sistema como en la reivindicación 1, caracterizado porque dicho primer método de encriptación comprende la encriptación triple DES de los datos del titular de la tarjeta.
10. Un sistema como en la reivindicación 9, caracterizado porque dicho dispositivo de entrada es contra la manipulación indebida.
11. Un sistema como en la reivindicación 1, caracterizado porque dicho dispositivo de manipulación de los datos del titular de la tarjeta, es seleccionado entre el grupo que consta de un sistema de control del surtidor de combustible, un POS y un controlador de sitio.
12. 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, caracterizado porque comprende:

una electrónica de control seguro; y

una memoria del sistema de evaluación segura, conteniendo dicha memoria del sistema de evaluación segura la información necesitada para descriptar 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;

donde dicha electrónica de control seguro está adaptada para descriptar dicha memoria del sistema de evaluación segura;

donde dicha electrónica de control seguro está adaptada ulteriormente para descriptar 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, dichos datos del titular de la tarjeta comprende por lo menos uno de datos de pago del titular de la tarjeta y datos no sensibles del titular de la tarjeta;

donde dicha electrónica de control seguro 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 de pago del titular de la tarjeta.

13. Un sistema de evaluación segura como en la reivindicación 12, caracterizado porque dichos primer y segundo métodos de encriptación son diferentes.
14. Un sistema de evaluación segura como en la reivindicación 13, caracterizado 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.
15. Un sistema de evaluación segura como en la reivindicación 14, caracterizado porque dicha electrónica de control seguro selecciona el segundo método de encriptación apropiado, después de la evaluación de dichos datos no encriptados del titular de la tarjeta.

16. Un sistema de evaluación segura como en la reivindicación 14, caracterizado porque dicha memoria del sistema de evaluación segura contiene datos con los cuales dichos datos no encriptados del titular de la tarjeta se comparan para determinar si dichos datos no encriptados del titular de la tarjeta corresponde a datos de pago del titular de la tarjeta.
17. Un sistema de evaluación segura como en la reivindicación 12, caracterizado porque dicha electrónica de control seguro está contra la manipulación indebida.
18. Un sistema de evaluación segura como en la reivindicación 12, caracterizado porque dicha electrónica de control seguro comprende una memoria interna, almacenando la información necesitada para desenscriptar los datos encriptados, de acuerdo con dicho tercer método de encriptación.
19. Un sistema de evaluación segura como en la reivindicación 18, caracterizado porque dicha electrónica de control seguro está implementada como un circuito de seguridad integrado.
20. Un sistema de evaluación segura como en la reivindicación 18, caracterizado porque dicho tercer método de encriptación comprende el AES-128.
21. Un sistema de evaluación segura como en la reivindicación 12, caracterizado porque comprende, además, una interfaz USB.
22. Un sistema de evaluación segura como en la reivindicación 21, caracterizado porque dicho sistema de evaluación segura está ubicado en un dispositivo de manipulación de los datos del titular de la tarjeta.
23. Un sistema de evaluación segura como en la reivindicación 22, caracterizado porque dicho dispositivo de manipulación de los datos del titular de la tarjeta, es seleccionado entre el grupo que consta de un sistema de control del surtidor de combustible, un POS y un controlador de sitio.
24. Un sistema de evaluación segura como en la reivindicación 12, caracterizado 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.

25. Un sistema de evaluación segura como en la reivindicación 12, caracterizado porque dicha electrónica de control seguro está adaptada ulteriormente, para evaluar dichos datos no encriptados del titular de la tarjeta, con el fin de realizar la validación de la transacción.
26. Un sistema de evaluación segura como en la reivindicación 25, caracterizado porque dicha memoria del sistema de evaluación segura contiene datos representativos de un registro de la transacción contra los cuales se compara dichos datos de pago del titular de la tarjeta.
27. Un sistema de evaluación segura como en la reivindicación 12, caracterizado porque dicho sistema de evaluación segura está implementado como una CPU contra la manipulación indebida.
28. Un método para el procesamiento de una transacción, involucrando los datos del titular de la tarjeta en un sistema de pago minorista, caracterizado porque comprende los pasos de:

la recepción de los datos del titular de la tarjeta en un dispositivo de entrada, dichos datos del titular de la tarjeta comprenden por lo menos uno de datos de pago del titular de la tarjeta y datos sensibles del titular de la tarjeta;

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;

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;

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;

la evaluación de dichos datos no encriptados del titular de la tarjeta en una electrónica de control seguro, con el fin de determinar si dichos datos no encriptados del titular de la tarjeta son los datos de pago del titular de la tarjeta, o los datos no sensibles del titular de la tarjeta; y

si dichos datos no encriptados del titular de la tarjeta son los datos de pago del titular de la tarjeta, 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.

29. El método según la reivindicación 28, caracterizado porque comprende, además, la transmisión de 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.
30. El método según la reivindicación 28, caracterizado porque dicha electrónica de control seguro está contra la manipulación indebida.
31. El método según la reivindicación 28, caracterizado porque dichos primer y segundo métodos de encriptación son diferentes.
32. El método según la reivindicación 31, caracterizado porque comprende, además, la transmisión de dichos segundos datos encriptados del titular de la tarjeta hacia un sistema procesador anfitrión remoto.
33. El método según la reivindicación 28, caracterizado porque dicho dispositivo de manipulación de los datos del titular de la tarjeta, es seleccionado entre el grupo que consta de un sistema de control del surtidor de combustible, un POS y un controlador de sitio.
34. El método según la reivindicación 28, caracterizado porque comprende, además, la evaluación de dichos datos no encriptados del titular de la tarjeta en dicha electrónica de control seguro, con el fin de realizar la validación de la transacción.
35. El método según la reivindicación 28, caracterizado porque dicho sistema de evaluación segura está implementado como un candado electrónico teniendo una interfaz USB.