

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Resolución N° 73939

Ref. Expediente N° NC2019/0001169

Por la cual se deniega una Patente de Invención

EL SUPERINTENDENTE DE INDUSTRIA Y COMERCIO (E)
en ejercicio de sus facultades legales, en especial de las conferidas en el numeral 24 del artículo 3° del Decreto 4886 de 2011, y

CONSIDERANDO

Que mediante escrito radicado en esta Superintendencia el 8 de febrero de 2019, con el N° NC2019/0001169, por KALYPTON INTERNATIONAL LIMITED, entró a fase nacional la solicitud de patente de invención titulada “SISTEMA DE AUTENTICACIÓN Y PROCESAMIENTO DE TRANSACCIÓN DISTRIBUIDA”, que corresponde a la solicitud internacional PCT/GB2017/052004 del 7 de julio de 2017.

Que la solicitud fue publicada en la Gaceta de la Propiedad Industrial N° 864 el 28 de junio de 2019, sin que se hubieran presentado oposiciones por parte de terceros.

Que realizado el examen de fondo mediante Oficio N° 257, notificado el 7 de enero de 2022, se requirió al solicitante en los términos del artículo 45 de la Decisión 486 de la Comisión de la Comunidad Andina para que presentara respuesta a las observaciones de carácter técnico, relacionadas con la patentabilidad o cumplimiento de los requisitos establecidos por esta Decisión para la concesión de la patente.

Que el solicitante mediante escrito radicado bajo el N° NC2019/0001169 el 13 de mayo de 2022, respondió oportunamente el requerimiento formulado y presentó las reivindicaciones 1 a 10 que reemplazan las originalmente presentadas. Simultáneamente, mediante escrito radicado bajo el N° NC2022/0006306 el 13 de mayo de 2022, el solicitante presentó las reivindicaciones 1 a 10 para que sean tenidas en cuenta al momento de realizar el examen definitivo de la solicitud, de dichas reivindicaciones modificadas esta Superintendencia advirtió la incorporación de materia que no había sido objeto de búsqueda y estudio previamente.

Que con fundamento en lo anterior, así como, en lo establecido por el literal b) del numeral 1.2.2.5.1. del Capítulo Primero del Título X de la Circular Única de esta Superintendencia, se requirió al solicitante mediante el Oficio N° 12350 del 5 de agosto de 2022, en los términos del artículo 17 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo (Ley 1437 de 2011), para que acreditara el pago correspondiente a la tasa para el examen de patentabilidad, teniendo en cuenta que dicha reivindicación incluyó materia que no estaba incluida en los capítulos previamente estudiados, específicamente, en el fragmento: “(...) *la generación del primer resumen es contemporánea a la realización de la primera transacción de datos y el almacenamiento del registro de la primera transacción de datos y el primer resumen se realiza de manera simultánea (...)*”. Sin embargo, el solicitante no respondió a este último requerimiento y tampoco realizó el pago solicitado, por lo tanto, conviene ponerle de presente que la decisión que se adoptará por parte de esta Oficina será con ocasión del último capítulo reivindicatorio sobre el cual, se encuentra acreditado el pago de la tasa por concepto de examen de patentabilidad.

Que en virtud de lo dispuesto en el artículo 14 de la Decisión 486 expedida por la Comisión de la Comunidad Andina “*Los países miembros otorgarán patentes para las invenciones,*

Resolución N° 73939

Ref. Expediente N° NC2019/0001169

sean de producto o de procedimiento, en todos los campos de la tecnología, siempre que sean nuevas, tengan nivel inventivo y sean susceptibles de aplicación industrial”.

Que en el presente caso las reivindicaciones 1 a 10 incluidas en el radicado bajo el N° NC2019/0001169 del 10 de junio de 2019, no cumplen los requisitos indicados. Lo anterior, de acuerdo con las siguientes consideraciones:

Objeto de la invención

El problema técnico planteado consiste en la necesidad de diseñar e implementar métodos para realizar transacciones de todo tipo en una implementación única a escala, de forma segura y casi en tiempo real.

Para resolver este problema técnico, la solicitud proporciona un método para registrar una transacción de datos que comprende, en un dispositivo asociado con una primera entidad, determinar los primeros datos iniciales, generar un registro de una primera transacción entre la primera entidad y una segunda entidad, determinar los segundos datos iniciales combinando al menos los primeros datos iniciales y el registro de la primera transacción de datos, generando un primer resumen mediante la aplicación de la función de resumen a los segundos datos iniciales, en donde los primeros datos consisten en un historial de transacciones de datos que involucran a la primera entidad y almacenan el primer resumen contra el registro de la primera transacción de datos en una memoria.

Determinación del estado de la técnica

La fecha para determinar el estado de la técnica es el 8 de julio de 2016 que corresponde a la fecha de presentación de la solicitud de prioridad.

Consultadas las fuentes de información con que se cuenta, se encontró el siguiente documento que anticipa el objeto de esta solicitud:

Ítem	Documento	Título	Fecha de Publicación
D1	EP2897051	“Verifiable audit log”	22 de julio de 2015
D2	US20150149781	“Authenticated session establishment”	28 de mayo de 2015

El documento D1¹ divulga sistemas y técnicas para el registro de eventos. Más específicamente, la presente divulgación se refiere a la protección, verificación y redacción de registros generados por ordenador (Col. 1, Párr. 0001).

El documento D2² divulga métodos, dispositivos y medios legibles por máquina para proporcionar comunicaciones seguras entre entidades. Como se proporciona en esta divulgación, esto puede incluir recibir una solicitud para comenzar una nueva sesión de comunicación, determinar uno o más parámetros deseados de la sesión y determinar si los parámetros deseados del mensaje coinciden con los parámetros propuestos proporcionados por la entidad que solicita la nueva sesión de comunicación. Cuando uno o más parámetros propuestos coinciden con el uno o más parámetros deseados, se establece una sesión de comunicación segura entre las entidades (Resumen).

¹<https://patentimages.storage.googleapis.com/9c/08/2b/2f644446338aaf/EP2897051A2.pdf>

²<https://patentimages.storage.googleapis.com/22/7e/99/2339d4b9ad7ba5/US20150149781A1.pdf>

Resolución N° 73939

Ref. Expediente N° NC2019/0001169

Novedad (Art 16 Decisión 486)

Según lo dispuesto en el artículo 16 de la Decisión 486: *“Una invención se considerará nueva cuando no está comprendida en el estado de la técnica.*

El estado de la técnica comprenderá todo lo que haya sido accesible al público por una descripción escrita u oral, utilización, comercialización o cualquier otro medio antes de la fecha de presentación de la solicitud de patente o, en su caso, de la prioridad reconocida”.

En el presente caso, el método reclamado en la solicitud no es nuevo, teniendo en cuenta que la reivindicación 1 está referida a: *“Un método para registrar una transacción de datos que comprende, en un dispositivo asociado con una primera entidad (...)”* (Radicado N° NC2019/0001169 del 10 de junio de 2019).

La siguiente tabla presenta la comparación entre las características técnicas esenciales de la solicitud estudiada, mencionadas en la reivindicación 1, y las reveladas en el documento D1 que representa el estado de la técnica:

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

Características esenciales	D1
Un método para registrar una transacción de datos que comprende, en un dispositivo asociado con una primera entidad.	(...) se envía al servidor de registro, el servidor de registro puede almacenar y calcular los valores hash necesarios para implementar los registros descritos en este documento y almacenar esas entradas de registro en el almacenamiento de datos, como el almacenamiento de datos (760). Estas entradas de registro pueden contener información sobre la computadora, actividades de la red, transacciones financieras o cualquier otro evento electrónico. (Col. 26, Párr. 0105, líneas 12 a 18). El servidor de registro (758) puede ser uno o más servidores, cada servidor tiene uno o más procesadores que pueden ejecutar las instrucciones del software, como las instrucciones de la máquina, el código compilado o un lenguaje interpretado, para llevar a cabo los procesos descritos. (Col. 26, Párr. 0104, líneas 1 a 6).
Determinar primeros datos iniciales.	El hash de resumen también puede depender de los metadatos del mensaje de registro actual y del hash de resumen anterior del mensaje de registro anterior. Esto hace que el resumen hash dependa indirectamente tanto de la entrada del registro actual como de todas las entradas que aparecen en el registro antes de la entrada del registro actual. (Col. 14, Párr. 0058, líneas 51 a 57).
Generar un registro de una primera transacción de datos entre la primera entidad y una segunda entidad.	En el bloque (106), se puede recibir un nuevo mensaje de registro o evento para registrar. (Col. 13, Párr. 0055, línea 1 y Col. 14, Párr. 0055, línea 1). El servidor de registro puede recibir mensajes de dispositivos informáticos como el dispositivo informático (752). Estos mensajes de registro se pueden generar en función de una variedad de eventos y objetos, por ejemplo, actividades de la red informática, transacciones financieras y otros eventos (por ejemplo, el ejemplo de seguimiento de matrículas descrito anteriormente). (Col. 26, Párr. 0104, líneas 6 a 11).
Determinar segundos datos iniciales mediante la combinación de al menos los primeros datos iniciales y el registro de la	(...) determinar un hash que depende tanto de la sal como del mensaje de registro actual que se introducirá en el registro, se puede calcular un segundo hash, denominado hash de resumen (...) El hash de resumen puede depender del hash de registro actual, que a su vez depende de la sal y del mensaje de registro.

Resolución N° 73939

Ref. Expediente N° NC2019/0001169

primera transacción de datos.	(Col. 14, Párr. 0058, líneas 44 a 51). Estas entradas de registro pueden contener información sobre la computadora, actividades de la red, transacciones financieras o cualquier otro evento electrónico. (Col. 26, Párr. 0105, líneas 16 a 18).
Generar un primer resumen (hash) mediante la función de resumen (hashing) de los segundos datos iniciales, en donde el primer resumen comprende un historial de transacciones de datos que involucran a la primera entidad.	Por lo tanto, en el bloque (110), el resumen de hash se calcula a través de los datos dependientes descritos anteriormente, como el registro de hash, los metadatos para la entrada de registro actual y el resumen de hash anterior. (Col. 15, Párr. 0058, líneas 2 a 5). En cuyo caso, el servidor de registro puede recibir un nuevo evento y luego crear de nuevo para este nuevo evento otro hash de registro actual (bloque (108)) y otro hash de resumen (bloque (110)) dependiendo de la entrada de registro actual y las entradas de registro anteriores. (Col. 15, Párr. 0059, líneas 16 a 21). El anidamiento de entradas de registro, en algunas realizaciones, podría comprender mantener un registro separado para cada objeto. En esta realización, se pueden usar múltiples registros: un registro maestro, verificable y redactable, que registra todos los eventos / objetos, y un segundo registro que solo registra eventos para el objeto específico en un solo segmento. El uso de este tipo de estructura evita cualquier omisión de entradas de registro para el objeto registrándolas todas en un solo segmento que se puede voltear en una respuesta (Col. 25, Párr. 0102). Estas entradas de registro pueden contener información sobre la computadora, actividades de la red, transacciones financieras o cualquier otro evento electrónico. (Col. 26, Párr. 0105, líneas 16 a 18).
Almacenar el primer resumen contra el registro de la primera transacción de datos en una memoria.	En el bloque (112), se escribe una nueva entrada de registro en el registro que incluye, por ejemplo, datos que indican el tipo de mensaje de registro, el hash de resumen para ese mensaje de registro actual, el hash de registro para ese mensaje de registro actual, cualquier metadato asociado con el mensaje de registro actual, la sal y el mensaje de registro generado por el servidor de registro o el evento asociado con el evento actual. De esta manera, se puede ingresar un mensaje de registro tras otro (Col. 15, Párr. 0059, líneas 6 a 14). La (s) fuente (s) de datos (760) pueden estar incorporadas en unidades de disco duro, memorias de estado sólido y / o cualquier otro tipo de medio de almacenamiento no transitorio, legible por computadora, accesible de forma remota o local para el servidor de aplicaciones (758). (Col. 27, Párr. 0109, líneas 1 a 5).

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

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

- Reivindicación 2: El hash de resumen también puede depender de los metadatos del mensaje de registro actual y del hash de resumen anterior del mensaje de registro anterior.
(Col. 14, Párr. 0058, líneas 51 a 54).
- Reivindicación 3: Por tanto, en el bloque (110), el resumen de hash se calcula a través de los datos dependientes descritos anteriormente tales como el registro de hash, los metadatos para la entrada de registro actual y el resumen de hash anterior.

Resolución N° 73939

Ref. Expediente N° NC2019/0001169

(Col. 15, Párr. 0058, líneas 2 a 5).

En cuyo caso, el servidor de registro puede recibir un nuevo evento y luego crear de nuevo para este nuevo evento otro hash de registro actual (bloque (108)) y otro hash de resumen (bloque (110)) dependiendo de la entrada de registro actual y la anterior entrada de registro.

(Col. 15, Párr. 0059, líneas 16 a 21). Estas entradas de registro pueden contener información sobre la computadora, actividades de la red, transacciones financieras o cualquier otro evento electrónico.

(Col. 26, Párr. 0105, líneas 16 a 18).

- Reivindicación 4: Además, puede comprender un hash de registro que se calcula y depende del mensaje vacío/firma digital y aleatoria. También puede comprender un valor hash de resumen. El valor de resumen de hash puede depender del hash de registro original para el mensaje vacío y varios metadatos para el mensaje vacío. Dicho hash de resumen se puede considerar el inicio de la cadena de hash que se puede utilizar para verificar los mensajes de registro posteriores.

(Col. 12, Párr. 0049, líneas 47 a 55).

La entrada de registro (302), como otras entradas de registro en esta divulgación, puede comprender el hash de registro 1, que se puede calcular sobre el mensaje de registro, como la firma digital con marca de tiempo sobre el resumen de hash 0, y una que proporciona aleatorización.

(Col. 19, Párr. 0074, líneas 30 a 34).

- Reivindicación 5: Después del inicio de la cadena, puede ocurrir una segunda entrada de registro que firma y marca el tiempo de la cadena. Por ejemplo, en el bloque (104), se puede crear una segunda entrada de registro correspondiente a una entrada de confirmación que bloquea todas las entradas anteriores del registro. En este bloque, el servidor de registro puede recopilar y codificar una marca de tiempo firmada, consultando un servidor de hora, y solicitar una marca de tiempo firmada del servidor de hora. Esto puede incluir una solicitud para firmar, además de la marca de tiempo, un hash asociado con la entrada de registro anterior (en esta realización, el resumen de hash de la entrada de registro inicial). En algunas realizaciones, el servidor de registro puede entonces tratar esta información como el mensaje de registro, para lo cual se puede calcular un hash de registro.

(Col. 13, Párr. 0053).

Determinar una sal que comprende datos pseudoaleatorios, calcular un hash de entrada de registro asociado con la información del evento, el hash de entrada de registro dependiente de los datos del evento y la sal, calcular un hash de resumen de registro asociado con la información del evento, el hash de resumen de registro dependiente del registro hash de entrada, al menos un elemento de metadatos de uno o más elementos de metadatos, y un segundo hash de resumen de registro.

(Col. 3, líneas 18 a 25).

Las reivindicaciones dependientes 2 a 5 tampoco cumplen con el requisito de novedad.

Nivel Inventivo (Art. 18 Decisión 486)

Según lo dispuesto en el artículo 18 de la Decisión 486: *“Se considerará que una invención tiene nivel inventivo, si para una persona del oficio normalmente versada en la materia técnica correspondiente, esa invención no hubiese resultado obvia ni se hubiese derivado de manera evidente del estado de la técnica”.*



Resolución N° 73939

Ref. Expediente N° NC2019/0001169

En el presente caso, el método reclamado en la solicitud no tiene nivel inventivo, teniendo en cuenta que la reivindicación 6 está referida a: *“El método de cualquiera de las reivindicaciones precedentes, (...)”* (Radicado N° NC2019/0001169 del 10 de junio de 2019).

El documento D1 se considera el estado de la técnica más cercano a la invención definida en la reivindicación 6 porque divulga sistemas y técnicas para el registro de eventos. Más específicamente, la presente divulgación se refiere a la protección, verificación y redacción de registros generados por ordenador (Col. 1, Párr. 0001).

La diferencia entre la invención definida en la reivindicación 6 y el método divulgado de D1 consiste en que, proporcionar segundos datos iniciales comprende además la combinación de una primera prueba de conocimiento cero y una segunda prueba de conocimiento cero con los primeros datos iniciales y el registro de la primera transacción de datos, en donde: la primera prueba de conocimiento cero comprende probar que el resumen inicial comprende el resumen verdadero de la transacción de datos anterior que involucra a la primera entidad; y la segunda prueba de conocimiento cero comprende probar que un segundo resumen comprende el resumen verdadero de una transacción de datos anterior que involucra a la segunda entidad.

El efecto que se logra al incluir el proporcionar segundos datos iniciales que comprende además la combinación de una primera prueba de conocimiento cero y una segunda prueba de conocimiento cero con los primeros datos iniciales y el registro de la primera transacción de datos, en donde: la primera prueba de conocimiento cero comprende probar que el resumen inicial comprende el resumen verdadero de la transacción de datos anterior que involucra a la primera entidad; y la segunda prueba de conocimiento cero comprende probar que un segundo resumen comprende el resumen verdadero de una transacción de datos anterior que involucra a la segunda entidad es autenticar cada uno de los pasos de la transacción de los datos mediante criptografía.

Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así: ¿Cómo modificar el método conocido en D1 con el fin de autenticar cada uno de los pasos de la transacción de los datos mediante criptografía?

Sin embargo, el incluir el proporcionar segundos datos iniciales que comprende además la combinación de una primera prueba de conocimiento cero y una segunda prueba de conocimiento cero con los primeros datos iniciales y el registro de la primera transacción de datos, en donde: la primera prueba de conocimiento cero comprende probar que el resumen inicial comprende el resumen verdadero de la transacción de datos anterior que involucra a la primera entidad; y la segunda prueba de conocimiento cero comprende probar que un segundo resumen comprende el resumen verdadero de una transacción de datos anterior que involucra a la segunda entidad para autenticar cada uno de los pasos de la transacción de los datos mediante criptografía, ya está divulgado en el documento D2 que se refiere a métodos, dispositivos y medios legibles por máquina para proporcionar comunicaciones seguras entre entidades (Resumen, líneas 1 a 2). El campo (1312) *zkp-x1-gr* almacena el valor g^r asociado con la prueba de conocimiento cero de x_1 , representado como un entero de longitud variable en formato big-endian. El campo (1314) *zkp-x1-b* almacena el valor b asociado con la prueba de conocimiento cero de x_1 , representado como un entero de longitud variable en formato big-endian. El campo *zkp-x2-gr* (1316) contiene el valor g^r asociado con la prueba de conocimiento cero de x_2 ,

Resolución N° 73939

Ref. Expediente N° NC2019/0001169

representado como un entero de longitud variable en formato big-endian (Pág. 16, Párr. 0146, líneas 7 a 15).

En consecuencia, la persona normalmente versada en la materia estaría motivada a incluir el proporcionar segundos datos iniciales que comprende además la combinación de una primera prueba de conocimiento cero y una segunda prueba de conocimiento cero con los primeros datos iniciales y el registro de la primera transacción de datos, en donde: la primera prueba de conocimiento cero comprende probar que el resumen inicial comprende el resumen verdadero de la transacción de datos anterior que involucra a la primera entidad; y la segunda prueba de conocimiento cero comprende probar que un segundo resumen comprende el resumen verdadero de una transacción de datos anterior que involucra a la segunda entidad del documento D2 en el método de D1, para así llegar al objeto de la reivindicación 6. Por lo cual se considera obvia.

Según lo dispuesto en el artículo 18 de la Decisión 486: *“Se considerará que una invención tiene nivel inventivo, si para una persona del oficio normalmente versada en la materia técnica correspondiente, esa invención no hubiese resultado obvia ni se hubiese derivado de manera evidente del estado de la técnica”*.

En el presente caso, el método reclamado en la solicitud no tiene nivel inventivo, teniendo en cuenta que la reivindicación 7 está referida a: *“El método de la reivindicación 6, en donde proporcionar segundos datos iniciales comprende además (...)”* (Radicado N° NC2019/0001169 del 10 de junio de 2019).

El documento D1 se considera el estado de la técnica más cercano a la invención definida en la reivindicación 7 porque divulga sistemas y técnicas para el registro de eventos. Más específicamente, la presente divulgación se refiere a la protección, verificación y redacción de registros generados por ordenador (Col. 1, Párr. 0001).

La diferencia entre la invención definida en la reivindicación 7 y el método divulgado de D1 consiste en que, proporcionar segundos datos iniciales comprende además combinar una tercera prueba de conocimiento cero con los primeros datos iniciales, el registro de la primera transacción de datos, la primera prueba de conocimiento cero y la segunda prueba de conocimiento cero.

El efecto que se logra al incluir el proporcionar segundos datos iniciales que comprende además combinar una tercera prueba de conocimiento cero con los primeros datos iniciales, el registro de la primera transacción de datos, la primera prueba de conocimiento cero y la segunda prueba de conocimiento cero es autenticar cada uno de los pasos de la transacción de los datos mediante criptografía.

Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así: ¿Cómo modificar el método conocido en D1 con el fin de autenticar cada uno de los pasos de la transacción de los datos mediante criptografía?

Sin embargo, el incluir el proporcionar segundos datos iniciales que comprende además combinar una tercera prueba de conocimiento cero con los primeros datos iniciales, el registro de la primera transacción de datos, la primera prueba de conocimiento cero y la segunda prueba de conocimiento cero para autenticar cada uno de los pasos de la transacción de los datos mediante criptografía, ya está divulgado en el documento D2 que se refiere a métodos, dispositivos y medios legibles por máquina para proporcionar comunicaciones seguras entre entidades (Resumen, líneas 1 a 2). El mensaje (1204)



Resolución N° 73939

Ref. Expediente N° NC2019/0001169

contiene una multitud de campos útiles para un establecimiento de claves basado en J-PAKE. Por ejemplo, el mensaje (1204) puede incluir un campo gx3 (1400), un campo gx4 (1402), un campo zkp-x3-gr (1404), un campo zkp-x3-b (1406) (Pág. 16, Párr. 0148, líneas 1 a 4).

En consecuencia, la persona normalmente versada en la materia estaría motivada a incluir el proporcionar segundos datos iniciales que comprende además combinar una tercera prueba de conocimiento cero con los primeros datos iniciales, el registro de la primera transacción de datos, la primera prueba de conocimiento cero y la segunda prueba de conocimiento cero del documento D2 en el método de D1, para así llegar al objeto de la reivindicación 7. Por lo cual se considera obvia.

Según lo dispuesto en el artículo 18 de la Decisión 486: *“Se considerará que una invención tiene nivel inventivo, si para una persona del oficio normalmente versada en la materia técnica correspondiente, esa invención no hubiese resultado obvia ni se hubiese derivado de manera evidente del estado de la técnica”*.

En el presente caso, el método reclamado en la solicitud no tiene nivel inventivo, teniendo en cuenta que la reivindicación 8 está referida a: *“El método de la reivindicación 7, en donde la tercera prueba de conocimiento cero se (...)”* (Radicado N° NC2019/0001169 del 10 de junio de 2019).

El documento D1 se considera el estado de la técnica más cercano a la invención definida en la reivindicación 8 porque divulga sistemas y técnicas para el registro de eventos. Más específicamente, la presente divulgación se refiere a la protección, verificación y redacción de registros generados por ordenador (Col. 1, Párr. 0001).

La diferencia entre la invención definida en la reivindicación 8 y el método divulgado de D1 consiste en que, la tercera prueba de conocimiento cero se genera a partir de datos aleatorios.

El efecto que se logra al incluir que la tercera prueba de conocimiento cero se genere a partir de datos aleatorios es mejorar la calidad criptográfica en la autenticación de cada uno de los pasos de la transacción de los datos.

Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así: ¿Cómo modificar el método conocido en D1 con el fin de mejorar la calidad criptográfica en la autenticación de cada uno de los pasos de la transacción de los datos mediante criptografía?

Sin embargo, el incluir que la tercera prueba de conocimiento cero se genere a partir de datos aleatorios para mejorar la calidad criptográfica en la autenticación de cada uno de los pasos de la transacción de los datos mediante criptografía, ya está divulgado en el documento D2 que se refiere a métodos, dispositivos y medios legibles por máquina para proporcionar comunicaciones seguras entre entidades (Resumen, líneas 1 a 2). Utilizando las funciones hash (1108) y/o (1110), la sal (1112) puede incluir tanto un elemento de aleatoriedad (por ejemplo, de los datos de clave pública), reforzando aún más las derivaciones de la clave maestra (Pág. 15, Párr. 0136, líneas 11 a 14). El mensaje (1204) contiene una multitud de campos útiles para un establecimiento de claves basado en J-PAKE. Por ejemplo, el mensaje (1204) puede incluir un campo gx3 (1400), un campo gx4 (1402), un campo zkp-x3-gr (1404), un campo zkp-x3-b (1406) (Pág. 16, Párr. 0148, líneas 1 a 4).



Resolución N° 73939

Ref. Expediente N° NC2019/0001169

En consecuencia, la persona normalmente versada en la materia estaría motivada a incluir que la tercera prueba de conocimiento cero se genere a partir de datos aleatorios del documento D2 en el método de D1, para así llegar al objeto de la reivindicación 8. Por lo cual se considera obvia.

Según lo dispuesto en el artículo 18 de la Decisión 486: *“Se considerará que una invención tiene nivel inventivo, si para una persona del oficio normalmente versada en la materia técnica correspondiente, esa invención no hubiese resultado obvia ni se hubiese derivado de manera evidente del estado de la técnica”*.

En el presente caso, el método reclamado en la solicitud no tiene nivel inventivo, teniendo en cuenta que la reivindicación 9 está referida a: *“El método de la reivindicación 7, en donde la tercera prueba de conocimiento (...)”* (Radicado N° NC2019/0001169 del 10 de junio de 2019).

El documento D1 se considera el estado de la técnica más cercano a la invención definida en la reivindicación 9 porque divulga sistemas y técnicas para el registro de eventos. Más específicamente, la presente divulgación se refiere a la protección, verificación y redacción de registros generados por ordenador (Col. 1, Párr. 0001).

La diferencia entre la invención definida en la reivindicación 9 y el método divulgado de D1 consiste en que la tercera prueba de conocimiento cero es una repetición de la primera prueba de conocimiento cero o la segunda prueba de conocimiento cero.

El efecto que se logra al incluir que la tercera prueba de conocimiento cero sea una repetición de la primera prueba de conocimiento cero o la segunda prueba de conocimiento cero es autenticar cada uno de los pasos de la transacción de los datos mediante criptografía.

Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así: ¿Cómo modificar el método conocido en D1 con el fin de autenticar cada uno de los pasos de la transacción de los datos mediante criptografía?

Sin embargo, el incluir que la tercera prueba de conocimiento cero sea una repetición de la primera prueba de conocimiento cero o la segunda prueba de conocimiento cero para autenticar cada uno de los pasos de la transacción de los datos mediante criptografía, ya está divulgado en el documento D2 que se refiere a métodos, dispositivos y medios legibles por máquina para proporcionar comunicaciones seguras entre entidades (Resumen, líneas 1 a 2). El mensaje (1204) contiene una multitud de campos útiles para un establecimiento de claves basado en J-PAKE. Por ejemplo, el mensaje (1204) puede incluir un campo gx3 (1400), un campo gx4 (1402), un campo zkp-x3-gr (1404), un campo zkp-x3-b (1406) (Pág. 16, Párr. 0148, líneas 1 a 4).

En consecuencia, la persona normalmente versada en la materia estaría motivada a incluir que la tercera prueba de conocimiento cero sea una repetición de la primera prueba de conocimiento cero o la segunda prueba de conocimiento cero del documento D2 en el método de D1, para así llegar al objeto de la reivindicación 9. Por lo cual se considera obvia.

Según lo dispuesto en el artículo 18 de la Decisión 486: *“Se considerará que una invención tiene nivel inventivo, si para una persona del oficio normalmente versada en la materia*



Resolución N° 73939

Ref. Expediente N° NC2019/0001169

técnica correspondiente, esa invención no hubiese resultado obvia ni se hubiese derivado de manera evidente del estado de la técnica”.

En el presente caso, el método reclamado en la solicitud no tiene nivel inventivo, teniendo en cuenta que la reivindicación 10 está referida a: *“El método de la reivindicación 7, en donde la tercera prueba de (...)”* (Radicado N° NC2019/0001169 del 10 de junio de 2019).

El documento D1 se considera el estado de la técnica más cercano a la invención definida en la reivindicación 10 porque divulga sistemas y técnicas para el registro de eventos. Más específicamente, la presente divulgación se refiere a la protección, verificación y redacción de registros generados por ordenador (Col. 1, Párr. 0001).

La diferencia entre la invención definida en la reivindicación 10 y el método divulgado de D1 consiste en que la tercera prueba de conocimiento cero se construye utilizando un segundo registro de la primera transacción de datos que corresponde a la segunda prueba de conocimiento cero.

El efecto que se logra al incluir que la tercera prueba de conocimiento cero se construya utilizando un segundo registro de la primera transacción de datos que corresponde a la segunda prueba de conocimiento cero es mejorar la autenticación de cada uno de los pasos de la transacción de los datos mediante criptografía.

Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así: ¿Cómo modificar el método conocido en D1 con el fin de mejorar la autenticación de cada uno de los pasos de la transacción de los datos mediante criptografía?

Sin embargo, el incluir que la tercera prueba de conocimiento cero se construya utilizando un segundo registro de la primera transacción de datos que corresponde a la segunda prueba de conocimiento cero para mejorar la autenticación de cada uno de los pasos de la transacción de los datos mediante criptografía, ya está divulgado en el documento D2 que se refiere a métodos, dispositivos y medios legibles por máquina para proporcionar comunicaciones seguras entre entidades (Resumen, líneas 1 a 2). El campo zkp-x3-b (1406) contiene el valor b asociado con la prueba de conocimiento cero de x3, representado como un entero de longitud variable en formato big-endian (Pág. 17, Párr. 0149, líneas 7a 9).

En consecuencia, la persona normalmente versada en la materia estaría motivada a incluir que la tercera prueba de conocimiento cero se construya utilizando un segundo registro de la primera transacción de datos que corresponde a la segunda prueba de conocimiento cero del documento D2 en el método de D1, para así llegar al objeto de la reivindicación 10. Por lo cual se considera obvia.

Respuesta a los argumentos del solicitante

El solicitante manifiesta que: *“(...) El solicitante aporta un nuevo capítulo reivindicatorio, conformado por 10 reivindicaciones, en el que se han realizado las siguientes modificaciones: • Se ha modificado la reivindicación independiente 1 con el fin de limitar su alcance respecto las etapas del método para registrar una transacción de datos. Esta modificación cuenta con pleno sustento en la antigua reivindicación 1 y a lo largo de capítulo descriptivo. Estas modificaciones se ajustan al artículo 34 de la Decisión 486 de 2000, toda vez que no amplían el alcance de protección de la solicitud presentada*



Resolución N° 73939

Ref. Expediente N° NC2019/0001169

originalmente y además encuentran soporte en la descripción de la solicitud (...).

Sin embargo, esta oficina reafirma el argumento expuesto referente al literal b) del numeral 1.2.2.5.1. del Capítulo Primero del Título X de la Circular Única de esta Superintendencia, en los términos del artículo 17 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo (Ley 1437 de 2011), referido a la acreditación del pago correspondiente a la tasa para el examen de patentabilidad, teniendo en cuenta que en la modificación al pliego reivindicatorio mencionada, se incluyó materia que no estaba incluida en los capítulos previamente estudiados, específicamente, en el fragmento: “(...) *la generación del primer resumen es contemporánea a la realización de la primera transacción de datos y el almacenamiento del registro de la primera transacción de datos y el primer resumen se realiza de manera simultánea (...)*”, sobre el cual no se realizó el pago solicitado. Por lo anterior dichas modificaciones no son tenidas en cuenta para la presente resolución.

Con respecto al análisis de patentabilidad, el solicitante reafirma que: “*Como se ha venido argumentando a lo largo del trámite administrativo, no existe nada en los documentos citados que de a conocer un sistema que elimine la brecha temporal para un sistema que procesa los hashes en el mismo flujo de mensajes que también procesa la transacción o el mensaje. Es claro que el documento D1 no revela ni sugiere el objeto de que se desea proteger en la nueva reivindicación 1*”.

Cabe indicar que dicha característica, no se encuentra divulgada en las reivindicaciones del capítulo estudiado con radicado N° NC2019/0001169 del 10 de junio de 2019 y por lo tanto no es tenida en cuenta para la presente resolución. Resulta del caso señalar que, esta Oficina reafirma que la reivindicación 1 no es nueva de acuerdo con las características allegadas en este capítulo reivindicatorio.

Aunado a lo anterior, se menciona que: “(...) *En conexión con lo anterior, el resumen del documento D1 deja absolutamente claro que sus enseñanzas se refieren a “la seguridad, verificación y redacción de registros generados por computador”. En consecuencia, la persona medianamente versada en la materia estaría en capacidad de entender que realmente no existe conexión ni relación entre la invención de la presente solicitud y las enseñanzas de D1, toda vez que no tiene nada que ver con un sistema que procesa los hashes en el mismo flujo de mensajes que también procesa la transacción o el mensaje (...)*”

Se aclara que, contrario a lo afirmado por el solicitante, sí existe relación entre la solicitud y el documento D1, toda vez que ambos pertenecen al campo técnico. Particularmente el documento D1 menciona: “*sistemas y técnicas para el registro de eventos. Más específicamente, la presente divulgación se refiere a la protección, verificación y redacción de registros generados por ordenador*” (Col. 1, Párr. 0001). De acuerdo con el párrafo anterior, es claro que el documento D1 está referido a sistemas para tratamiento, verificación y/o procesamiento de datos en un ordenador, razón por la cual se mantiene la objeción.

El solicitante reitera que: “(...) *Así mismo, D1 no revela ni tiene un indicio en el que se procese de manera contemporánea ninguna de las actividades allí descritas. Tan es así que la Figura 1. a la que se refiere el párrafo [0055], ilustra que el sistema puede recibir varios eventos y luego generar los registros de esos eventos antes de consignar un lote de ellos en la entrada del registro (bloque 116). El párrafo [0059] confirma lo mencionado anteriormente (...)*”.



Resolución N° 73939

Ref. Expediente N° NC2019/0001169

Se aclara nuevamente al solicitante que, dicha característica referida al “procesamiento de manera contemporánea”, no se presenta de manera explícita en el pliego reivindicatorio radicado bajo el número N° NC2019/0001169 del 10 de junio de 2019, el cual fue el último capítulo aceptado y, por lo tanto, nos son tenidas en cuenta en la presente resolución.

El solicitante menciona que: *“Por otro lado, y como se ha manifestado a lo largo del trámite administrativo, el documento D2 tampoco revela todas y cada una de las características técnicas esenciales de la invención tal y como se reclama actualmente, ni mucho menos motiva a la persona medianamente versada en la materia a derivar de manera obvia el objeto de la presente invención (...) En conexión con lo anterior, es evidente que el estado de arte citado no revela, divulga o sugiere que el primer resumen se crea contemporáneamente con la realización de la primera transacción de datos y se registra contemporáneamente con esa primera transacción de datos (...) 3.11. La presente invención reclamada por el Solicitante procesa una transacción y genera y graba el registro o auditoría de esa transacción al mismo tiempo en el mismo proceso. Elimina cualquier brecha temporal entre una transacción o evento, por un lado, y el registro o auditoría, por el otro (...) los documentos citados no revelan todas y cada una de las características técnicas esenciales de la invención reclamada, y aun así la persona medianamente versada en la técnica combinando las enseñanzas de D1 y D2 tampoco derivaría de manera obvia el objeto de la presente solicitud (...)”.*

Sin embargo, en primera instancia se indica al solicitante que el documento D2 es utilizado para el estudio de nivel inventivo sobre las reivindicaciones 6 a 10 mediante la combinación de las enseñanzas con el documento D1. De acuerdo con lo anterior, es importante destacar que el análisis de nivel inventivo es procedente toda vez que ambos documentos pertenecen al campo técnico porque mencionan: *“sistemas y técnicas para el registro de eventos. Más específicamente, la presente divulgación se refiere a la protección, verificación y redacción de registros generados por ordenador”* (D1, Col. 1, Párr. 0001) y *“métodos, dispositivos y medios legibles por máquina para proporcionar comunicaciones seguras entre entidades. Como se proporciona en esta divulgación, esto puede incluir recibir una solicitud para comenzar una nueva sesión de comunicación, determinar uno o más parámetros deseados de la sesión y determinar si los parámetros deseados del mensaje coinciden con los parámetros propuestos proporcionados por la entidad que solicita la nueva sesión de comunicación. Cuando uno o más parámetros propuestos coinciden con el uno o más parámetros deseados, se establece una sesión de comunicación segura entre las entidades”* (D2, Resumen). Adicionalmente, se indica que, el examen de nivel inventivo se basa en un juicio de valor y un análisis objetivo de las divulgaciones previas del estado de la técnica, los cuales no deben verse influenciados por el conocimiento que ya se tiene de la invención que se está evaluando. Así que para minimizar la subjetividad y evitar que se realice un análisis en retrospectiva (“hindsight” ó “a posteriori”), esto es, partiendo de lo divulgado en la invención, el examen de nivel inventivo debe relacionar la invención con la solución de un problema técnico, mediante el Método “Problema - Solución”, el cual consta de las siguientes etapas: a) Identificar el estado de la técnica más cercano a la invención reivindicada, que para el caso en particular corresponde al documento D1 tal y como se expuso anteriormente, b) Determinar la diferencia entre la invención y estado de la técnica más cercano, es decir, las características que hacen nueva la invención, que para el caso particular corresponde a la prueba de conocimiento cero, c) Definir el efecto técnico causado y atribuible al elemento diferencial, que para el caso particular el efecto técnico corresponde a autenticar cada uno de los pasos de la transacción mediante criptografía, d) Deducir el



Resolución N° 73939

Ref. Expediente N° NC2019/0001169

problema técnico objetivo, que para el caso particular corresponde a autenticar cada uno de los pasos de la transacción de los datos mediante criptografía, e) Evaluar si la invención reivindicada, partiendo del estado de la técnica más cercano y del problema técnico objetivo, habría sido obvia para la persona versada en la materia. Por lo anterior es procedente realizar la combinación de las enseñanzas entre los documentos D1 y D2 para realizar el análisis de Nivel Inventivo sobre la materia reclamada en la presente solicitud. Ahora bien, en segunda instancia se reitera al solicitante que las características referidas a *“se crea contemporáneamente (...) y se registra contemporáneamente” “el mismo tiempo en el mismo proceso” y “brecha temporal”* no se presentan de manera explícita en el capítulo reivindicatorio radicado bajo el número N° NC2019/0001169 del 10 de junio de 2019, el cual fue el último capítulo aceptado, y por lo tanto no hace parte de la decisión contenida en la presente resolución.

Que el solicitante en el escrito radicado bajo el N° NC2019/0001169 el 8 de febrero de 2019, tituló la invención como: “SISTEMA DE AUTENTICACIÓN Y PROCESAMIENTO DE TRANSACCIÓN DISTRIBUIDA”. Sin embargo, no se acepta porque no se relaciona con la materia reclamada en el pliego reivindicatorio, la cual corresponde a la modalidad de método, y de acuerdo con el objeto de la solicitud, el título de la invención quedará de la siguiente manera: “MÉTODO DE AUTENTICACIÓN Y PROCESAMIENTO DE TRANSACCIÓN DISTRIBUIDA”.

En conclusión, teniendo en cuenta que los argumentos del solicitante no desvirtúan de manera alguna las objeciones a la patentabilidad ya sustentadas, el Superintendente de Industria y Comercio (E),

RESUELVE

ARTÍCULO 1: Denegar la patente de invención a la creación titulada “MÉTODO DE AUTENTICACIÓN Y PROCESAMIENTO DE TRANSACCIÓN DISTRIBUIDA”.

ARTÍCULO 2: Notificar el contenido de la presente resolución a KALYPTON INTERNATIONAL LIMITED, advirtiéndole que contra ella procede el recurso de reposición, ante el Superintendente de Industria y Comercio, el cual podrá ser interpuesto en el momento de la notificación o dentro de los diez (10) días hábiles siguientes a ella.

NOTIFÍQUESE Y CÚMPLASE

Dada en Bogotá D.C., el 24 de octubre de 2022

EL SUPERINTENDENTE DE INDUSTRIA Y COMERCIO (E),



Firmado digitalmente
por: JUAN CAMILO
DURAN TELLEZ
Fecha: 2022.10.24
09:03:07 COT
Razón: Validez jurídica.
Ubicación: Bogotá,
Colombia.

