

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 257 de 6 de enero de 2022

Ref. Expediente N° NC2019/0001169

Señor(a)
KALYPTON INTERNATIONAL LIMITED

TÍTULO DE LA SOLICITUD: **“SISTEMA DE AUTENTICACIÓN Y PROCESAMIENTO DE TRANSACCIÓN DISTRIBUIDA”**

NÚMERO DE SOLICITUD INTERNACIONAL: PCT/GB2017/052004

FECHA DE PRESENTACIÓN INTERNACIONAL: 7 de julio de 2017.

PRIORIDAD(ES): GB, 1611948.9, 8 de julio de 2016.

Como resultado del examen de patentabilidad realizado a la solicitud indicada en la referencia, atendiendo a lo consagrado en el artículo 45 de la Decisión 486 de 2000, se le comunica que esta Dirección ha encontrado que la materia objeto de solicitud no cumple con algunos requisitos establecidos en la Decisión, con fundamento en los siguientes aspectos:

1. Objeto de la invención

De acuerdo con lo establecido en el numeral 1.2.2.2 del Capítulo Primero del Título X de la Circular Única para efectos del examen de patentabilidad, cuando la solicitud contenga más de diez (10) reivindicaciones y no se haya pagado la tasa complementaria, sólo se estudiarán las cubiertas por la tasa pagada al momento de realizar el examen de patentabilidad consagrado en el artículo 45 de la Decisión 486. Por lo tanto, se estudiarán las reivindicaciones 1 a 10 del radicado N° NC2019/0001169 del 10 de junio de 2019.

El problema planteado en esta solicitud 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 en estudio 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.

2. De la solicitud de patente

2.1. Título

El nombre de la invención de que se trata en el artículo 27 literal d) de la Decisión 486 deberá reflejar el objeto y el campo industrial con el cual se relaciona la misma y ser concordante con la materia descrita y las reivindicaciones de la solicitud. El nombre no podrá referirse a nombres personales, marcas de productos o nombres de fantasía.

Oficio N° 257 de 6 de enero de 2022

Ref. Expediente N° NC2019/0001169

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”. Este título no se relaciona con el objeto de la solicitud contenido en la descripción y la modalidad descrita en las reivindicaciones, por lo cual se sugiere el título siguiente: “MÉTODO DE AUTENTICACIÓN Y PROCESAMIENTO DE TRANSACCIÓN DISTRIBUIDA”.

2.2. Reivindicaciones (Art. 30 Decisión 486)

Se sugiere incluir entre paréntesis () los números de referencia de cada uno de los elementos que hacen parte de la invención de acuerdo con la numeración empleada en los dibujos, con el fin, de hacer más fácil la comprensión de la materia reivindicada.

3. 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).

4. Examen de Patentabilidad (Art. 14 Decisión 486)

4.1. Novedad (Art 16 Decisión 486)

La reivindicación 1 consiste en: “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).

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

Características esenciales	D1
----------------------------	----

¹<https://patentimages.storage.googleapis.com/9c/08/2b/2f644446338aaf/EP2897051A2.pdf>
²<https://patentimages.storage.googleapis.com/22/7e/99/2339d4b9ad7ba5/US20150149781A1.pdf>

Ref. Expediente N° NC2019/0001169

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 primera transacción de datos.	(...) 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. (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).

Oficio N° 257 de 6 de enero de 2022

Ref. Expediente N° NC2019/0001169

	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.
(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

Oficio N° 257 de 6 de enero de 2022

Ref. Expediente N° NC2019/0001169

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.

4.2. Nivel Inventivo (Art. 18 Decisión 486)

La reivindicación 6 consiste en: *“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 las reivindicaciones 6 a 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 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 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



Oficio N° 257 de 6 de enero de 2022

Ref. Expediente N° NC2019/0001169

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

Adicionalmente, es conocido en el estado de la técnica el uso del protocolo de prueba de conocimiento cero para métodos criptográficos³.

En consecuencia, la persona normalmente versada en la materia estaría motivada a incluir el 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 del documento D2 en el método de D1, para así llegar al objeto de la reivindicación 6. Por lo cual se considera obvia.

La reivindicación 7 consiste en: *“El método de la reivindicación 6, en donde proporcionar segundos datos (...)”* (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).

³ Wikipedia. “Prueba de conocimiento cero”. Tomado de: https://es.wikipedia.org/wiki/Prueba_de_conocimiento_cero.



Oficio N° 257 de 6 de enero de 2022

Ref. Expediente N° NC2019/0001169

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 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 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) 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).

Adicionalmente, es conocido en el estado de la técnica el uso del protocolo de prueba de conocimiento cero para métodos criptográficos³.

En consecuencia, la persona normalmente versada en la materia estaría motivada a incluir el 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 del documento D2 en el método de D1, para así llegar al objeto de la reivindicación 7. Por lo cual se considera obvia.

La reivindicación 8 consiste en: *“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.



Oficio N° 257 de 6 de enero de 2022

Ref. Expediente N° NC2019/0001169

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).

Adicionalmente, es conocido en el estado de la técnica el uso del protocolo de prueba de conocimiento cero para métodos criptográficos³ y el uso de datos aleatorios en criptografía⁴.

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.

La reivindicación 9 consiste en: *“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.

⁴ Wikipedia. “Generador de números pseudoaleatorios criptográficamente seguro”. Tomado de: https://es.wikipedia.org/wiki/Generador_de_n%C3%BAmeros_pseudoaleatorios_criptogr%C3%A1ficamente_seguro.



Oficio N° 257 de 6 de enero de 2022

Ref. Expediente N° NC2019/0001169

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).

Adicionalmente, es conocido en el estado de la técnica el uso del protocolo de prueba de conocimiento cero para métodos criptográficos³.

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.

La reivindicación 10 consiste en: *“El método de la reivindicación 7, en donde la tercera prueba de (...)”* (Reiv. 10) (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



Oficio N° 257 de 6 de enero de 2022

Ref. Expediente N° NC2019/0001169

(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).

Adicionalmente, es conocido en el estado de la técnica el uso del protocolo de prueba de conocimiento cero para métodos criptográficos³.

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.

5. Conclusión con respecto a novedad y/o nivel inventivo

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

Ítem	Documento	Reivindicaciones afectadas	Requisito que afecta
D1	EP2897051	1 a 5	Novedad
		6 a 10	Nivel Inventivo
D2	US20150149781	6 a 10	Nivel Inventivo

6. Respuesta a los argumentos del solicitante (

El solicitante argumenta que: “(...) *El Solicitante respetuosamente se encuentra en desacuerdo con la objeción al título, por las razones que se expondrán más adelante en el análisis de la novedad y nivel inventivo de la solicitud. Por lo anterior, no se modifica el título de la solicitud de patente y amablemente se solicita que se de por superada la objeción (...)*”

Esta Oficina reafirma la objeción hecha, puesto que en la materia técnica, se reitera la sugerencia en el cambio del título tal y como se evidencia en el numeral 2.1 del presente oficio, toda vez que las reivindicaciones mencionan: “*Un método para (...)*” (Reivindicación 1), “*El método de la reivindicación 1 (...)*” (Reivindicación 2), “*El método de la reivindicación 2 (...)*” (Reivindicaciones 3 y 4), “*El método de la reivindicación 4 (...)*” (Reivindicación 5), “*El método de cualquiera de las reivindicaciones precedentes (...)*” (Reivindicación 6), “*El método de la reivindicación 6 (...)*” (Reivindicación 7) y “*El método de la reivindicación 7 (...)*” (Reivindicaciones 8 a 10). De acuerdo con lo anterior, es evidente que todas y cada una de las reivindicaciones reclamadas en la solicitud hacen referencia a un método y no a un sistema.

Con respecto al análisis de patentabilidad, el solicitante reafirma que: “(...) 3.4. *La 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. Hasta ahora, cada sistema primero ha procesado una transacción o evento, y luego ha pasado un registro de esa transacción o evento al sistema de registro o auditoría, que luego crea un registro o auditoría de esa transacción o evento. Ese retraso representa la brecha temporal que elimina la invención en cuestión.* 3.5. *El estado de la técnica se ha centrado, hasta la presente solicitud, en asegurar una cadena de auditoría (ver, por ejemplo, el párrafo [0001] en D1) o en establecer un enlace de comunicaciones seguro entre dos o más dispositivos (ver, por ejemplo, el párrafo [0002]*



Oficio N° 257 de 6 de enero de 2022

Ref. Expediente N° NC2019/0001169

en D2). No se ha centrado en eliminar la brecha temporal (...) 3.6. Los documentos citados no implican que una auditoría pueda generarse al mismo tiempo que la transacción en sí (...) En ninguna parte se relacionan con el procesamiento de una pista de auditoría o con la eliminación de la brecha temporal entre una transacción o evento y la pista de auditoría de esa transacción o evento (...).

Cabe indicar que las características referidas a: “procesar una transacción y generar y grabar el registro o auditoría de esa transacción al mismo tiempo en el mismo proceso” y “Eliminar cualquier brecha temporal entre una transacción o evento, por un lado, y el registro o auditoría” las cuales el solicitante menciona en el radicado N° NC2019/0001169 del 23 de septiembre de 2021, no se encuentran divulgadas en las reivindicaciones del capítulo estudiado con radicado N° NC2019/0001169 del 10 de junio de 2019 y por lo tanto no son tenidas en cuenta para presente examen de patentabilidad. Resulta del caso señalar que, esta Oficina reafirma que la reivindicación 1 no es nueva de acuerdo con las características allegadas en el capítulo reivindicatorio, tal y como se evidencia en el numeral 4 del presente oficio.

Aunado a lo anterior, se menciona que: “(...) 3.9. El Examinador indica que las reivindicaciones 1 a 5 no definen una invención novedosa a la luz del documento D1. Para esto, el Examinador se refiere a los párrafos [0105], [0104], [0058], [0055], [0104], [0058], [0105], [0058], [0059], [0102], [0105], y [0059] en ese orden, en un intento de tratar de construir desde D1 una descripción que no existe. 3.10. Como bien lo indica el párrafo [0105] de D1 citado por el Examinador: **“Una vez que esta información 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”, es claro que el sistema reclamado en D1 procesa y calcula hashes y procesa los datos para la auditoría después de que la transacción ocurre en un servidor o sistema separado y se envía al servidor de registro. El hash no es contemporáneo de la transacción; no se calcula en el mismo flujo de procesamiento de mensajes que la transacción en sí, sino en un sistema separado después del evento (...) 3.12. El Examinador se refirió a estos dos párrafos anteriormente mencionados en ese orden para objetar la novedad de la reivindicación 1. Sin embargo, al leer los párrafos completos en su orden completo, [0104] y luego [0105], D1 claramente describe un sistema en el que un servidor de registros debe recibir primero una transacción o un mensaje antes de poder procesar el hash. En ninguna parte de la reivindicación 1 se reclama un sistema que primero debe recibir una transacción o mensaje antes de que pueda generar un hash o auditoría de esa transacción o mensaje (...) 3.13. A continuación, el examinador cita selectivamente el párrafo (...) 3.14. En otras palabras, el sistema de D1 solo puede procesar eventos o transacciones después de que el evento haya ocurrido (...) 3.15. Luego en su análisis, el Examinador se refiere a se refiere al párrafo [0058]. Sin embargo, este párrafo describe el método en D1 que se basa en un segundo hash de resumen que el sistema reclamado debe almacenar junto con el primer hash, como claramente se indica al principio del párrafo: “En el bloque 110, después de determinar un hash que depende tanto de la sal como del mensaje de registro actual, que se ingresará en el registro, **se puede calcular un segundo hash, denominado hash de resumen**”. 3.16. En D1, este hash conduce directamente desde el primer hash para ese mismo evento de registro, el “hash de registro actual” como se describe en [0057] y se almacena en la entrada junto con el primer hash [0059]. El párrafo [0058] no divulga “los primeros datos iniciales” o los “segundos datos iniciales” como afirma el Examinador (...)”**



Oficio N° 257 de 6 de enero de 2022

Ref. Expediente N° NC2019/0001169

Se aclara que, contrario a lo afirmado por el solicitante, dichas características si son anticipadas por el documento D1, toda vez que menciona: *“En el bloque (110), después de 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. Independientemente del nombre que se utilice, su función es ser la siguiente entrada de la cadena hash verificable. El hash de resumen puede depender del hash de registro actual, que a su vez depende de la sal y del mensaje de registro. 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 44 a 57), particularmente, el párrafo anterior detalla que se pueden obtener unos primeros datos iniciales, a los cuales el documento D1 hace referencia como *“hash de resumen anterior”* y unos segundos datos iniciales a los cuales se hace referencia mediante *“segundo hash o hash de resumen”* el cual se usa como una siguiente entrada a la cadena de hash.

El solicitante reitera que: *“(...) 3.17. El párrafo [0059] describe efectivamente cómo el sistema en D1 construye bloques de múltiples entradas de registro antes de que se comprometan con el registro (...) 3.18. Esto es lo opuesto al sistema reivindicado en la presente solicitud. Como se mencionó anteriormente, la invención reclamada procesa una transacción y genera y graba el registro o auditoría de esa transacción al mismo tiempo en el mismo proceso (...) 3.19. Los párrafos [0055] a [0059], cuando se leen juntos en su orden natural (...) 3.20. El párrafo [0102] establece que el sistema reivindicado en D1 puede utilizar uno o más registros. No se comprende la relevancia de ese párrafo para las reivindicaciones de la presente solicitud, ya que los registros en D1 no son contemporáneos a las transacciones (...) 3.21. En cuanto al párrafo [0109] (...) 3.22. La divulgación en el párrafo [0109] (...) Como se señaló anteriormente, en ninguna parte de la descripción o de las reivindicaciones, se reclama un sistema que primero debe almacenar una transacción antes de que el sistema pueda procesar esa transacción. El sistema, en cambio, elimina esa brecha de tiempo, a diferencia del de D1 (...)”*.

Se aclara nuevamente al solicitante que, la anterioridad sí afecta la reivindicación, y que de ninguna manera es una construcción de un nuevo invento a partir del documento. En primera instancia, es importante destacar que la anterioridad y la materia contenida en la presente solicitud corresponden a la misma modalidad toda vez que están referidas a un sistema. Adicionalmente, se indica que de acuerdo con el artículo 16 de la Decisión 486, toda invención se considera nueva cuando no está comprendida dentro del estado de la técnica, particularmente, en el numeral 4 del presente oficio se establece una comparación elemento por elemento en donde no se muestra de forma convincente cuál es dicha novedad. De igual manera, se reitera al solicitante que, las características referidas a: *“una transacción y genera y graba el registro o auditoría de esa transacción al mismo tiempo en el mismo proceso”*, la *“contemporaneidad de las transacciones”*, la *“brecha de tiempo”*, la reiterada referencia del solicitante respecto a que en las etapas en D1 se hagan una después de la otra, *“eliminar el lapso de tiempo”*, lo cual de acuerdo con el solicitante diferencia a la solicitud del documento D1, no se presentan de manera explícita en el pliego reivindicatorio allegado y por lo tanto nos son tenidas en cuenta en el presente examen.

El solicitante menciona que: *“3.24. En cuanto a la novedad de las reivindicaciones 2 a 5 (...) 3.25. Asimismo, el Solicitante no se encuentra de acuerdo con el Examinador en que*



Oficio N° 257 de 6 de enero de 2022

Ref. Expediente N° NC2019/0001169

el párrafo [0053] en D1 divulga la materia de las reivindicaciones 4 o 5 (...) 3.26. Esto no es lo que se reclama en las reivindicaciones 4 y 5 (...) en D1 describen una versión de Blockchain que procesa, aplica hash y registra transacciones después de que han ocurrido (...) 3.27. Por su parte, el párrafo [0049] se refiere a las figuras 1 y 2 en D1, que describen en forma gráfica cómo el sistema de D1 inicia una cadena de auditoría después de haber recibido el primer evento de hash (...) 3.29. El texto al que se refiere el Examinador no se puede leer de forma aislada. Cuando se lee con el párrafo [0048] (...) No hacen nada para eliminar el lapso de tiempo entre una transacción y la auditoría de esa transacción (...) 3.31. De nuevo, al igual que con las otras reivindicaciones en D1, nada en los párrafos [0073] a [0074] describe un método para procesar y auditar una transacción al mismo tiempo. Todas las auditorías son posteriores al evento (...) 3.33. La redacción y la eliminación son actividades independientes. La presentación de registros redactados no elimina ni destruye el original (...).

Se indica al solicitante que la materia reclamada en las reivindicaciones dependientes 1 a 5 tampoco superan el requisito de novedad, toda vez que la comparación realizada con el documento D1 permiten anticipar las características reclamadas mediante los siguientes fragmentos: “(...) *mensaje de registro actual y del hash de resumen anterior* (...)” (Col. 14, Párr. 0058) el cual permite anticipar la materia divulgada en la reivindicación 2 referida a datos iniciales los primeros datos iniciales y al resumen inicial, “(...) *datos dependientes descritos anteriormente tales como el registro de hash, los metadatos para la entrada de registro actual* (...)” (Col. 15, Párr. 0058) el cual permite anticipar la materia divulgada en la reivindicación 3 referida a la función de resumen de un registro de una transacción, “(...) *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* (...)” (Col. 12, Párr. 0049) el cual permite anticipar la materia divulgada en la reivindicación 4 referida a un resumen aleatorio, el cual puede depender del registro adicional y varios metadatos y “(...) *firma y marca el tiempo de la cadena* (...)” (Col. 13, Párr. 0053) el cual permite anticipar la materia divulgada en la reivindicación 5 referida a una firma del dispositivo y a la fecha y/u hora en la que se genera el resumen.

Frente al análisis de Nivel Inventivo de las reivindicaciones dependientes 6 a 10, se expone que: “(...) 3.35. Ahora, el Examinador en su análisis, también indica que las reivindicaciones 6 a 10 serían obvias para una persona versada en la materia a la luz de las enseñanzas de D1 y D2. El Solicitante respetuosamente se encuentra en desacuerdo (...) 3.37. El examinador afirma que el problema técnico objetivo que la invención en las reivindicaciones 6 a 10 busca resolver se puede formular como: “Cómo modificar el método conocido en D1 para autenticar cada uno de los pasos de la transacción de datos usando criptografía”. 3.38. El Solicitante se encuentra en desacuerdo. La invención, como se discutió anteriormente, es resolver el problema técnico de cómo procesar una transacción y la auditoría de esa transacción simultáneamente en el mismo flujo de procesamiento de mensajes para eliminar el lapso de tiempo entre una transacción y su auditoría. No es utilizar ni modificar el método conocido en D1 ya que eso impediría lograr el objetivo de la presente invención. Las divulgaciones en D1 y D2 no mencionan nada similar al respecto. 3.39. El documento D2 simplemente describe un método para establecer comunicaciones seguras entre dos dispositivos mediante el uso de un sistema de clave pública o el uso de un algoritmo J-Pake. No hace nada más (...) la descripción en uno de los dos primeros borradores iniciales de su especificación (ver draft-hao-jpake-00 (ietf.org) y draft-hao-jpake-01 (ietf.org) (...) 3.40. El Examinador correctamente afirma que: (...) 3.41. Si bien el Solicitante no discute con esa afirmación (...) 3.42. Las reivindicaciones 6 a 10 no son para un mecanismo de intercambio de claves (...) Las



Oficio N° 257 de 6 de enero de 2022

Ref. Expediente N° NC2019/0001169

reivindicaciones 6 a 10 se refieren a métodos que utilizan una prueba de conocimiento cero, no a un algoritmo de intercambio de claves (...) 3.43. Las reivindicaciones 6-10 van más allá del progreso normal de la tecnología (...) 3.44. Si, como afirma el Examinador, D2 revela el material de la invención en cuestión, entonces D2 reclamaría un método para utilizar una prueba de conocimiento cero para eliminar la brecha temporal entre una transacción y la auditoría de esa transacción (...) 3.45. Si, como afirma el Examinador las reivindicaciones 6 a 10 fueran obvias para una persona experta en la técnica anterior, los incentivos económicos para eliminar la brecha temporal habrían resultado en un sistema que lo hizo (...) 3.46. Por lo tanto, el Solicitante sostiene que el mismo hecho de que D2 no mencione ningún uso de J-PAKE o la prueba de conocimiento cero para procesar una transacción y la auditoría de esa transacción simultáneamente en el mismo flujo de procesamiento de mensajes para eliminar la brecha de tiempo entre una transacción y su auditoría, solo confirma el nivel inventivo que tiene la invención en cuestión frente al estado de la técnica existente (...)."

Sin embargo, se indica que el estudio de nivel inventivo realizado sobre las reivindicaciones 6 a 10 se realiza mediante la combinación de las enseñanzas de los documentos D1 y D2. 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). Es importante destacar 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 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, que para el caso particular si se considera obvia dicha evaluación toda vez que corresponde a etapas de autenticación lo cual es conocido en el campo técnico y adicionalmente se encuentra divulgado de manera explícita por el documento D2, adicionalmente, es ampliamente conocido el uso del protocolo de prueba de conocimiento cero y por lo tanto es posible anticipar la materia reclamada en la



Oficio N° 257 de 6 de enero de 2022

Ref. Expediente N° NC2019/0001169

presente solicitud, tal y como se evidencia en el numeral 5 del presente oficio. Finalmente, de acuerdo con las pruebas allegadas por el solicitante, particularmente referidas al algoritmo J-PAKE: *“la descripción en uno de los dos primeros borradores iniciales de su especificación (ver [draft-hao-jpake-00 \(ietf.org\)](#) y [draft-hao-jpake-01 \(ietf.org\)](#)”* se indica que las mismas son especificaciones propias al protocolo, las cuales son conocidas en el campo técnico y anticipadas por el documento D2 porque menciona: *“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)”* (D2, Pág. 16, Párr. 0148, líneas 1 a 4), de acuerdo con el párrafo anterior dicha característica es anticipada por el documento D2 y por lo tanto es procedente la combinación de sus enseñanzas con las enseñanzas del documento D1 para realizar el análisis de Nivel Inventivo sobre la materia reclamada en la presente solicitud, tal y como se evidencia en el numeral 4 del presente oficio.

El estado de la técnica cercano es un documento que se encuentra en el mismo campo técnico que la invención o trata de solucionar el mismo problema o uno semejante. Suele ser el que tiene más características en común con la invención o presenta leves modificaciones de estructura e indica la misma función, propósito o efectos.

En cumplimiento del artículo 45 de la Decisión 486 de 2000, se le indica que debe dar respuesta dentro del término de sesenta (60) días contados a partir de la fecha de notificación de la presente comunicación. En caso de no dar respuesta al presente requerimiento, o si a pesar de la respuesta subsistieran los impedimentos para la concesión, se denegará la patente.

Si como respuesta a este requerimiento, el solicitante modifica el capítulo reivindicatorio, deberá observar las instrucciones contenidas en el numeral 1.2.2.1.1., del Capítulo Primero del Título X de la Circular Única de esta Superintendencia. De igual forma, deberá tener presente que de conformidad con el literal a) del numeral 1.2.2.5.1., de la norma ibidem, será necesario acreditar el pago de la tasa por concepto de modificación a solicitudes en trámites, de conformidad con el valor establecido en la resolución de tasas vigentes.

Notifíquese el presente oficio conforme a lo dispuesto en el numeral 6.2 del Capítulo Sexto del Título I de la Circular Única, informándoles que contra el mismo no procede recurso alguno en actuación administrativa.



Edna Marcela Ramirez Orozco
DIRECTORA DE NUEVAS CREACIONES



Oficio N° 257 de 6 de enero de 2022

Ref. Expediente N° NC2019/0001169

INFORME DE BÚSQUEDA
EXAMEN DE PATENTABILIDAD

Solicitud No.		Examen de patentabilidad							
NC2019/0001169		1°		2°	X	3°		Revoca	
Solicitud Internacional No.		Fecha solicitud internacional: (DD/MM/AÑO)							
PCT/GB2017/052004		7 de julio de 2017							
Fecha de determinación estado de la técnica (DD/MM/AÑO)				Prioridad		Presentación			
8/07/2016				X					
Solicitante									
KALYPTON INTERNATIONAL LIMITED									
Reivindicaciones que no son objeto de búsqueda por:									
Art. 14	-	Art. 15	-	Art. 20	-	Art. 25 (Falta de unidad de invención)		-	

CRITERIOS DE BÚSQUEDA	
Reivindicaciones objeto de búsqueda	1 a 10
Palabras clave utilizadas	First, second, log, time, real, secur*, verif*, logs, hash, values, entry, sever, confidenti*, digital, segments, messages, ZKP, random.
Clasificaciones utilizadas para la búsqueda	CIP: H04L 9/32

DOCUMENTOS CONSIDERADOS RELEVANTES (Documentos patente, Literatura no patente (LNP): Artículos, catálogos, etc.)					
Informes de búsqueda / Bases de datos consultadas	N° de solicitud de patente / N° de patente / Autor LNP ⁽¹⁾	Fecha de Publicación /Presentación (DD/MM/AAAA)	Reivindicaciones /Secuencias afectadas	Citas relevantes del estado de la técnica	Categoría del documento citado ⁽²⁾
SIPI	NC2020/0000950	15/05/2020	-	-	E
ISA	EP2897051	22/07/2015	1 a 5	1 Col. 26, Párr. 0105, líneas 1 a 6; Col. 26, Párr. 0104, líneas 1 a 6; Col. 14, Párr. 0058, líneas 51 a 57; Col. 13, Párr. 0055, línea 1 y Col. 14, Párr. 0055, línea 1; Col. 26, Párr. 0104, líneas 6 a 11; Col. 14, Párr. 0058, líneas 44 a 51; Col. 15, Párr. 0058, líneas 2 a 5; Col. 15, Párr. 0059, líneas 16 a 21; Col. 25, Párr. 0102; Col. 15, Párr. 0059, líneas 6 a 14; Col. 26, Párr. 0105, líneas 16 a 18. 2 Col. 14, Párr. 0058, líneas 51 a 54 3 Col. 15, Párr. 0058, líneas 2 a 5; Col. 15, Párr. 0059, líneas 16 a 21; Col. 26, Párr. 0105, líneas 16 a 18. 4 Col. 12, Párr. 0049, líneas 47 a 55; Col. 19, Párr. 0074, líneas 30 a 34. 5 Col. 13, Párr. 0053.	X

Oficio N° 257 de 6 de enero de 2022

Ref. Expediente N° NC2019/0001169

				6 a 10 Col. 1, Párr. 0001	
	US2016063100	3/03/2016	6 a 10	- - -	Y
	US2015269570	24/09/2015	-	-	A
	US2011099277	28/04/2011	-	-	A
	US2012150750	14/06/2012	-	-	A
	US2015142650	21/05/2015	-	-	A
	US8250640	21/08/2012	-	-	A
	US9241004	19/01/2016	-	-	A
	EP2028794	25/02/2009	-	-	A
	US2015371216	24/12/2015	-	-	A
	US2008077979	27/03/2008	-	-	A
	US2010049975	25/02/2010	-	-	A
	US2005025091	3/02/2005	-	-	A
	US2014379576	25/12/2014	-	-	A
	US2011093939	21/04/2011	-	-	A
	US2013046690	21/02/2013	-	-	A
	US5617537	1/04/1997	-	-	A
	US6026474	15/02/2000	-	-	A
	US2013232217	5/09/2013	-	-	A
	Da Mendonça (2011) ¹	31/12/2011	-	-	A
Patbase	WO21022369	11/02/2021	-	-	E
Googlepatent	US20150149781	28/05/2015	6 a 10	6 Resumen; Pág. 16, Párr. 0146, líneas 7 a 15. 7 Resumen; Pág. 16, Párr. 0148, líneas 1 a 4. 8 Resumen; Pág. 15, Párr. 0136, líneas 11 a 14; Pág. 16, Párr. 0148, líneas 1 a 4. 9 Resumen; Pág. 16, Párr. 0148, líneas 1 a 4. 10 Resumen; Pág. 17, Párr. 0149, líneas 7 a 9.	Y
	EP2836956	18/02/2015	-	-	A
	CN106301788	19/03/2019	-	-	E
	WO2019034589	21/02/2019	-	-	E
	⁽¹⁾ Cita completa literatura no patente (LNP) Apellido, A. A. (Fecha). Título del artículo. Nombre de la revista. Volumen(Número), pp-pp. O Apellido, A. A. (Fecha). Título del artículo. Nombre de la revista. Recuperado de http://xxxxxxx.		¹ Faculdade De Ciências, Margarida Paula, Da Mendonça, Cravo Silva; “UNIVERSIDADE DE LISBOA SECURING USSD IN MOBILE FINANCIAL TRANSACTIONS (A PRACTICAL PROPOSAL FOR M-FINANCE)”; Tomado de: http://repositorio.ul.pt/bitstream/10451/8707/1/ulfc104212_tm_Paula_Cravo.pdf		
⁽²⁾ Categorías de documentos citados					
“A” Documento que define el estado general de la técnica no considerado como particularmente relevante.			“T” Documento publicado en fecha posterior a la de presentación o la de prioridad de la solicitud internacional y no entra en conflicto con dicha solicitud, pero puede ser útil para la mejor comprensión del principio o teoría en que se basa la invención, o para demostrar que el razonamiento o los hechos en los que se basa dicha invención son incorrectos.		
“E” Solicitud de patente o patente anterior pero publicada en la fecha de presentación internacional o en fecha posterior.					
“L” Documento citado para llamar la atención sobre por ejemplo, dudas acerca de una reivindicación de prioridad o para determinar la					

Oficio N° 257 de 6 de enero de 2022

Ref. Expediente N° NC2019/0001169

fecha de publicación de otra cita, siempre van acompañados de una explicación, por la cual se citan. “O” Documento del tipo actas de conferencia, este tipo de documentos siempre estará acompañado por otra letra que indique la pertinencia del documento, por ejemplo, O,X, O,Y o bien O,A. “P” Documento publicado antes de la fecha de presentación internacional pero con posterioridad a la fecha de prioridad reivindicada.	“X” Documento particularmente relevante; la invención reivindicada no puede considerarse nueva o que implique una actividad inventiva por referencia al documento aisladamente considerado. “Y” Documento particularmente relevante; la invención reivindicada no puede considerarse que implique una actividad inventiva cuando el documento se asocia a otro u otros documentos de la misma naturaleza, cuya combinación resulta evidente para un experto en la materia.
Fecha del reporte de búsqueda: (24/11/2021)	