

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Resolución N° 41327

Ref. Expediente N° NC2019/0007656

Por la cual se resuelve un recurso de reposición

EL SUPERINTENDENTE DE INDUSTRIA Y COMERCIO

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 Resolución No. 22687 de 25 de abril de 2022, la Superintendencia de Industria y Comercio concedió parcialmente patente de invención a la creación denominada: "MÉTODO Y SISTEMA DE SELLADO DE DATOS CON UN ENCLAVE DE SELLADO", para las reivindicaciones : 7 a 10 y 17 a 20, al considerar que cumplen con los requisitos de patentabilidad consagrados en el artículo 14 de la Decisión 486 de la Comisión de la Comunidad Andina. Asimismo, se niega el privilegio de patente para las reivindicaciones 1 a 6 y 11 a 16 al estimar que no cumplieron con el requisito de novedad, de acuerdo con lo establecido en el artículo 16 de la Decisión 486 de la Comisión de la Comunidad Andina.

Que mediante escrito radicado en esta Entidad el 7 de junio de 2022 con el N° NC2022/0008107, encontrándose dentro del término establecido para el efecto, LLC MICROSOFT TECHNOLOGY LICENSING, interpuso recurso de reposición contra la citada Resolución con fundamento en los argumentos que a continuación se exponen:

Sobre las modificaciones presentadas.

Inicialmente, la recurrente manifiesta que presenta junto con el memorial del recurso un nuevo capítulo reivindicatorio, bajo el radicado N° NC2022/0008093 el 07 de junio de 2022, el cual consta de 20 reivindicaciones, las cuales incluyen dentro de las reivindicaciones independientes 1 y 11 la característica *"en donde la lista permitida es una lista de tipos de identidad abstracta que corresponden a respectivos niveles de jerarquía de una jerarquía de identidad"* y reemplaza completamente el capítulo presentado anteriormente.

Sobre el análisis de novedad y nivel inventivo.

Luego de realizar un breve resumen del trámite administrativo, la recurrente manifiesta que *"En vista de lo que establece la Resolución impugnada, se puede apreciar que las reivindicaciones 1 a 6 y 11 a 16 fueron negadas debido a que no describen características que les proporcionen novedad frente al documento US 2015/347768 (D1).*

Aunque el solicitante está en desacuerdo con la decisión de esta oficina de negar las reivindicaciones 1 a 6 y 11 a 16 como se explica en la respuesta al Oficio No. 18680 presentada el 15 de febrero de 2022, el solicitante, con el ánimo de obtener todas las reivindicaciones concedidas, ha enmendado el capítulo reivindicatorio para incluir en las reivindicaciones independientes 1 y 11 la siguiente característica que no es divulgada ni sugerida por el documento D1.

Página 1 de 11



Ref. Expediente N° NC2019/0007656

‘en donde la lista permitida es una lista de tipos de identidad abstracta que corresponden a respectivos niveles de jerarquía de una jerarquía de identidad’.

Esta modificación la presenta el solicitante de forma separada a la presentación de este recurso de acuerdo con lo establecido en el Artículo 34 de la Decisión 486 de la comisión de la Comunidad Andina.”.

De la misma manera, la recurrente señala que “(...) indicamos que la resolución número 22687 reconoce la novedad y nivel inventivo cuando indica lo siguiente:

‘Que en el presente caso las reivindicaciones 7 a 10 y 17 a 20 incluidas en el radicado bajo el N° NC2019/0007656 el 22 de septiembre de 2021, cumplen los requisitos indicados en el considerando anterior, toda vez que refieren a un método y sistema de sellado de datos con un enclave de sellado que difiere del estado de la técnica más cercano, US2015/347768, en que la solicitud incluye que la lista permitida es una lista de tipos de identidad abstracta que corresponden a respectivos niveles de jerarquía de una jerarquía de identidad.

Adicionalmente, estas diferencias no se encuentran sugeridas en el estado de la técnica y, como consecuencia de ello, se evidencia el efecto de identificar de manera segura grupos de instancias de enclave, así como permitir interacciones entre grupos de instancias de enclave, además de proporcionar equivalencia de reportes de afirmación para todos los enclaves con la misma identidad de nivel superior’.

En vista de lo expuesto anteriormente, se puede concluir que la invención reclamada por las reivindicaciones 1 y 11 no se encuentran comprendidas dentro de las enseñanzas del documento D1, y adicionalmente son restricciones no evidentes para una persona versada en la materia, por lo que la solicitud cuenta con novedad y nivel inventivo”.

Finalmente, la recurrente solicita que se revoque la decisión impugnada en la Resolución No. 22687, la cual otorga parcialmente la solicitud; y acto seguido se conceda la totalidad de reivindicaciones presentadas.

Que para resolver el recurso interpuesto, de conformidad con el artículo 80 del Código de Procedimiento Administrativo y de lo Contencioso Administrativo, se atenderán “(...) todas las peticiones que hayan sido oportunamente planteadas y las que surjan con motivo del recurso”

Actuación administrativa.

Con el fin de verificar las razones que fundamentan la impugnación del acto administrativo por medio del cual se concedió parcialmente la solicitud radicada bajo el expediente de la referencia, se hizo una revisión de las actuaciones surtidas en este trámite administrativo encontrando que el 16 de julio de 2019 la sociedad MICROSOFT TECHNOLOGY LICENSING, presento la solicitud de patente de invención N° NC2019/0007656 titulada, “SELLADO DE DATOS CON UN ENCLAVE DE SELLADO”.

De igual manera, se observa que, mediante Oficio N° 9787 del 24 de junio de 2021, la Dirección de Nuevas Creaciones, con fundamento en lo dispuesto por el artículo 45 de

Resolución N° 41327

Ref. Expediente N° NC2019/0007656

la Decisión 486, requirió al solicitante para que se pronunciaran frente a las objeciones a la patentabilidad que fueron formuladas.

En efecto en dicho Oficio, se elevaron objeciones de claridad en relación al Artículo 30 de la Decisión 486, sugiriendo emendar los errores de redacción encontrados y sugiriendo la inclusión de los números de referencia al pliego reivindicatorio; de la misma manera, se sugirió el cambio de título de la solicitud de patente; Por otro lado, se encontró que los documento D1 a D3 anticipan el objeto de la invención, la cual fue afectada por novedad y nivel inventivo.

Frente al mencionado requerimiento, el solicitante presentó respuesta el 22 de septiembre de 2021, allegando modificaciones al pliego reivindicatorio y argumentos a favor de la novedad y el nivel inventivo de la solicitud, indicando que el concepto inventivo reclamado no se encuentra revelado dentro de los documento D1 a D3.

Posteriormente, se formularon objeciones de patentabilidad mediante el Oficio N° 18680 el 29 de noviembre de 2021, dentro de las cuales se le notificó a la recurrente que las modificaciones al pliego reclamatorio del 22 de septiembre de 2021 fueron aceptadas toda vez que se cancelaron las tasas de modificación correspondientes; de la misma manera, se encontró que, a pesar de los argumentos presentados por la recurrente, las reivindicaciones 1 a 6 y 11 a 16 no son consideradas novedosas a la luz de los documentos del estado de la técnica D1 y D2

Con respecto al Oficio emitido, el 15 de febrero de 2022, la recurrente dio respuesta a las objeciones formuladas, emitiendo argumentos a favor de la patentabilidad sin realizar modificaciones al pliego reivindicatorio.

No obstante, a pesar de las aclaraciones presentadas dentro de la respuesta al examen de patentabilidad, esta Oficina encontró que los argumentos revelados no son suficientes para superar las objeciones relacionadas con la novedad de la solicitud en relación al Artículo 16 de la Decisión 486. Por lo cual, subsistieron los impedimentos para la concesión de las reivindicaciones 1 a 6 y 11 a 16 y el derecho de exclusividad fue concedido parcialmente para las reclamaciones 7 a 10 y 17 a 20 mediante Resolución N° 22687 del 25 de abril de 2022, al considerar que la materia denegada no cumple con el requisito novedad de acuerdo con el documento del estado de la técnica D1.

Sobre las modificaciones presentadas.

El artículo 34 de la Decisión 486 establece que:

“El solicitante de una patente podrá pedir que se modifique la solicitud en cualquier momento del trámite. La modificación no podrá implicar una ampliación de la protección que correspondería a la divulgación contenida en la solicitud inicial”.

En relación con el ámbito y alcance de la modificación, el Tribunal ha establecido lo siguiente: *“La única limitación impuesta al solicitante respecto de la modificación consiste en que ésta no debe implicar una ampliación del invento o de la divulgación contenida en la solicitud presentada. Contrario sensu, la modificación de la solicitud podrá concretar el invento o reducir el alcance de las reivindicaciones, sin importar cuál haya sido la redacción originariamente propuesta; por lo que aun cuando el cambio sea*

Resolución N° 41327

Ref. Expediente N° NC2019/0007656

sustancial con relación a las reivindicaciones iniciales, lo único relevante viene a ser que las nuevas reivindicaciones puedan seguir siendo sustentadas racionalmente con fundamento en la descripción contenida en la solicitud inicial”.

En el caso objeto de la presente revisión, la sociedad recurrente presenta en el memorial del recurso un nuevo capítulo reivindicatorio bajo el radicado N° NC2022/0008093 el 07 de junio de 2022, con el fin de que sea considerado al decidir sobre la patentabilidad de la materia, esta Oficina considera lo siguiente:

Se acepta la modificación allegada con el escrito del recurso, teniendo en cuenta que se ajusta a las prescripciones del artículo 34 de la Decisión 486, en la medida que no constituye ampliación de la protección que correspondería a la divulgación contenida en la solicitud inicial y se acompaña del pago de la tasa correspondiente por modificaciones voluntarias.

Sobre el análisis de novedad.

Por su parte, de acuerdo con el artículo 16 de la Decisión 486 para que una invención sea novedosa se requiere que no esté comprendida en el estado de la técnica; es decir, que antes de la fecha de presentación de la solicitud o de la prioridad reconocida, tanto la innovación como los conocimientos técnicos que de ella se desprenden no hayan sido accesibles al público. Una vez revisados los documentos aportados por la solicitante y teniendo en cuenta las modificaciones presentadas al objeto de las reivindicaciones 1 y 11, esta Superintendencia encuentra que a pesar de que el documento D1 revele que el nodo (101) puede autenticarse en el nodo (102) desellando los secretos dentro del enclave seguro (304) y enviando su ID de lista blanca al nodo (102), por ejemplo, en un mensaje firmado. El nodo (102) puede verificar la autenticidad del cliente verificando la firma aplicada al mensaje y comparando el ID de la lista blanca del cliente con los ID de la lista blanca de las plataformas aprobadas (Pág. 6, Párr. 0068), dentro de la mencionada anterioridad no se revela de forma específica que una lista permitida es una lista de tipos de identidad abstracta que corresponden a respectivos niveles de jerarquía de una jerarquía de identidad. Por lo tanto, la materia reclamada cumple con lo establecido en el mencionado artículo.

Sobre el análisis de Nivel Inventivo.

De acuerdo con 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 se advierte que el estado de la técnica puesto en consideración para apreciar el nivel inventivo no divulga un objeto concebido en el mismo campo técnico o está dirigido a alcanzar el mismo objetivo de la invención reivindicada, por lo tanto no es posible derivar sus características esenciales cumpliendo así con lo establecido en el mencionado artículo.

Por lo anterior, como se evidenció en la resolución de negación impugnada, el estado de la técnica más cercano a la invención esta relacionado con el documento D1 el cual indica un método ejecutado por al menos un procesador que comprende inicializar el primer y segundo enclaves seguros, cada uno de los cuales comprende un entorno de ejecución de software confiable que evita que el software que se ejecuta fuera del

Resolución N° 41327

Ref. Expediente N° NC2019/0007656

primer y segundo enclaves seguros tenga acceso a software y datos dentro del primer y segundo enclaves seguros (Pág. 1, Resumen).

La diferencia entre la invención definida en las reivindicaciones 1 y 11, y el método - sistema de D1 consiste en que la solicitud señala que la lista permitida es una lista de tipos de identidad abstracta que corresponden a respectivos niveles de jerarquía de una jerarquía de identidad.

El efecto que se logra al señalar que la lista permitida es una lista de tipos de identidad abstracta que corresponden a respectivos niveles de jerarquía de una jerarquía de identidad, es que permite identificar de manera segura grupos de instancias de enclave, así como permitir interacciones entre grupos de instancias de enclave, además de proporcionar equivalencia de reportes de afirmación para todos los enclaves con la misma identidad de nivel superior

Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así: ¿Cómo modificar el método - sistema conocido en D1 con el fin de identificar de manera segura grupos de instancias de enclave, así como permitir interacciones entre grupos de instancias de enclave, además de proporcionar equivalencia de reportes de afirmación para todos los enclaves con la misma identidad de nivel superior?

Sin embargo, de acuerdo a la divulgación presentada en el documento D1, la materia consignada en la mencionada anterioridad no presenta indicaciones claras que proporcionen una lista permitida que es una lista de tipos de identidad abstracta que corresponden a respectivos niveles de jerarquía de una jerarquía de identidad es permite identificar de manera segura grupos de instancias de enclave.

En consecuencia, la persona normalmente versada en la materia, no estaría motivada a combinar el documento del estado de la técnica D1 para proporcionar una lista de tipos de identidad abstracta que corresponden a respectivos niveles de jerarquía de una jerarquía de identidad que permite identificar de manera segura grupos de instancias de enclave, para así llegar al objeto de la reivindicaciones 1 y 11. Por lo cual, la materia señalada cumple con el requisito de nivel inventivo.

Que de acuerdo con la modificación presentada por el solicitante y teniendo en cuenta el objeto concedido, se modifica el título de la invención el cual quedará de la siguiente manera: "MÉTODOS Y SISTEMAS DE SELLADO DE DATOS CON UN ENCLAVE DE SELLADO".

Con fundamento en las anteriores consideraciones,

RESUELVE

ARTÍCULO 1: Revocar la Resolución No. 22687 de 25 de abril de 2022, por medio de la cual se concedió parcialmente patente de invención a la creación titulada: "MÉTODO Y SISTEMA DE SELLADO DE DATOS CON UN ENCLAVE DE SELLADO", de acuerdo con las razones anteriormente expuestas.

Resolución N° 41327

Ref. Expediente N° NC2019/0007656

ARTÍCULO 2: Otorgar patente de Invención a la solicitud que entró en fase nacional en virtud del Tratado de Cooperación en Materia de Patentes (PCT), para la creación titulada:

“MÉTODOS Y SISTEMAS DE SELLADO DE DATOS CON UN ENCLAVE DE SELLADO”

Clasificación IPC: G06F 21/60, G06F 21/62.

Reivindicación(es): 1 a 20 incluidas en el radicado bajo el N° NC2022/0008093 el 07 de junio de 2022, de acuerdo con el anexo 1.

Titular(es): LLC MICROSOFT TECHNOLOGY LICENSING.

Dirección(es): ONE MICROSOFT WAY, REDMOND, WA 98052-6399, 98052-6399, ESTADOS UNIDOS DE AMÉRICA.

Inventor(es): Manuel COSTA.

Prioridad(es) N° 24/01/2017, US (ESTADOS UNIDOS DE AMÉRICA), 15/414,492.

Solicitud internacional N°: PCT/US2017/067455 **Fecha:** 20 de diciembre de 2017.

Vigente desde: 20 de diciembre de 2017 **Hasta:** 20 de diciembre de 2037.

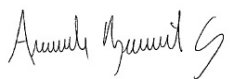
ARTÍCULO 3: El titular tendrá los derechos y las obligaciones establecidos en la Decisión 486 de la Comisión de la Comunidad Andina y en las demás disposiciones legales vigentes sobre propiedad industrial, precisando que para mantener vigente la patente se deberá cancelar la tasa anual de mantenimiento, conforme lo dispone el artículo 80 de la referida norma comunitaria.

ARTÍCULO 4: Notificar el contenido de la presente Resolución a LLC MICROSOFT TECHNOLOGY LICENSING, advirtiéndole que contra ella no procede recurso alguno.

NOTIFÍQUESE Y CÚMPLASE

Dada en Bogotá D.C., a los 29 de junio de 2022

EL SUPERINTENDENTE DE INDUSTRIA Y COMERCIO,



ANDRÉS BARRETO GONZÁLEZ
SUPERINTENDENTE DE INDUSTRIA Y COMERCIO

Firmado digitalmente
por: ANDRÉS
BERNARDO BARRETO
GONZÁLEZ
Fecha: 2022.06.29
17:00:37 COT
Razón: Validez jurídica.
Ubicación: Bogotá,
Colombia.

ANEXO 1

REIVINDICACIONES CONCEDIDAS

1. Un método para sellar datos de enclave, que comprende:

enviar (2002), a un enclave de origen (1912) alojado en una primera plataforma de enclave nativa (1916), un primer reporte de afirmación de un enclave de sellado (1932) alojado en una segunda plataforma de enclave nativa (1936);

recibir (2004) una lista permitida y datos de enclave asociados del enclave de origen en el enclave de origen, en donde la lista permitida es una lista de tipos de identidad abstracta que corresponden a respectivos niveles de jerarquía de una jerarquía de identidad e incluye una lista de una o más identidades de enclave permitidas para desellar los datos de enclave;

almacenar (2006) de manera segura los datos de enclave y la lista permitida, en donde el almacenado de manera segura incluye cifrar los datos de enclave con una clave asociada con el enclave de sellado, por parte del enclave de sellado, antes de recibir una petición por los datos de enclave de parte de un enclave de destino para crear datos de enclave sellados; y

restringir (2008, 2010, 2012) el acceso de los datos de enclave a enclaves con identidades autenticadas que se permite de acuerdo con la lista permitida, en donde la restricción incluye determinar si enviar los datos de enclave desde el enclave sellado al enclave de destino, el cual es diferente del enclave de sellado, con base al menos en parte en si el enclave de destino está incluido en la lista de una o más identidades de enclave permitidas para desellar los datos de enclave.

2. El método de acuerdo con la reivindicación 1, en donde:

la primera plataforma de enclave nativa está en una primera computadora y la segunda plataforma de enclave nativa está alojada en una segunda computadora.

3. El método de acuerdo con la reivindicación 1 que comprende además:
recibir un reporte de afirmación de origen del enclave de origen; y

derivar un valor de identidad permitida a partir del reporte de afirmación de origen y un tipo de identidad abstracta en la lista permitida.

3. El método de acuerdo con la reivindicación 1, en donde se cifran los datos de enclave recibidos, y que comprende además:

ejecutar un proceso de afirmación entre el enclave de origen y el enclave de sellado; y

descifrar los datos de enclave cifrados con una clave generada durante el proceso de afirmación.

5. El método de acuerdo con la reivindicación 1, en donde almacenar de manera segura los datos de enclave incluye:

Ref. Expediente N° NC2019/0007656

almacenar los datos de enclave sellados en almacenamiento persistente; y

en donde restringir el acceso de los datos de enclave a enclaves con identidades autenticadas adicionalmente incluye:

después de determinar que los datos de enclave son enviados desde el enclave sellado al enclave de destino con base al menos en parte en que el enclave de destino está incluido en la lista de una o más identidades de enclave permitidas para desellar los datos de enclave, descifrar los datos de enclave sellados en respuesta a recibir la petición por los datos de enclave de parte de un enclave de destino.

6. El método de acuerdo con la reivindicación 1, en donde una o más identidades de enclave en la lista permitida son especificadas por una o más claves públicas del respectivo uno o más enclaves.

7. Un método para sellar datos de enclave, que comprende:

recibir, en un enclave de origen (1912) alojado en una primera plataforma de enclave nativa (1916), un primer reporte de afirmación de un enclave de sellado (1932) alojado en una segunda plataforma de enclave nativa (1936);

verificar la confianza en el enclave de sellado; y

enviar una lista permitida y datos de enclave asociados hacia el enclave de sellado, en donde la lista permitida incluye una lista de una o más identidades de enclave permitidas para desellar los datos de enclave, dicho envío comprende causar que el enclave de sellado determine si enviar los datos de enclave hacia el enclave de destino que es diferente del enclave de sellado con base al menos en parte en si el enclave de destino está incluido en la lista de una o más identidades de enclave permitidas para desellar los datos de enclave, en donde la lista permitida es una lista de tipos de identidad abstracta que corresponden a respectivos niveles de jerarquía de una jerarquía de identidad; y.

enviar un reporte de afirmación de origen del enclave de origen hacia el enclave de sellado, en donde el reporte de afirmación de origen incluye al menos un valor de identidad del enclave de origen que corresponde a un tipo de identidad abstracta en la lista permitida.

8. El método de acuerdo con la reivindicación 7 que comprende además:

un proceso de afirmación entre el enclave de sellado y el enclave de origen;

generar datos de enclave cifrados por medio de cifrar los datos de enclave con una clave generada durante el proceso de afirmación; y

en donde los datos de enclave enviados hacia el enclave de sellado son los datos de enclave cifrados.

9. El método de acuerdo con la reivindicación 7, en donde:

Resolución N° 41327

Ref. Expediente N° NC2019/0007656

la primera plataforma de enclave nativa está en una primera computadora y la segunda plataforma de enclave nativa está alojada en una segunda computadora.

10. El método de acuerdo con la reivindicación 7, que comprende además:

completar parcialmente una operación de procesamiento seguro en el enclave de origen; y

en donde los datos de enclave incluyen datos de estado del enclave de origen suficientes para permitir que otra instanciación de enclave continúe la operación de procesamiento seguro completada parcialmente.

11. Un sistema que comprende al menos un procesador y memoria que almacena, en la misma, instrucciones que, cuando son ejecutadas por el sistema, provocan al menos:

Enviar (2002), a un enclave de origen (1912) alojado en una primera plataforma de enclave nativa (1916), un primer reporte de afirmación de un enclave de sellado (1932) alojado en una segunda plataforma de enclave nativa (1936);

recibir (2004) una lista permitida y datos de enclave asociados del enclave de origen, en donde la lista permitida es una lista de tipos de identidad abstracta que corresponden a respectivos niveles de jerarquía de una jerarquía de identidad e incluye una lista de una o más identidades de enclave permitidas para desellar los datos de enclave;

almacenar (2006) de manera segura los datos de enclave y la lista permitida, en donde el almacenado incluye cifrar los datos de enclave con una clave asociada con el enclave de sellado, por parte del enclave de sellado, antes de recibir una petición por los datos de enclave de parte de un enclave de destino para crear datos de enclave sellados; y

restringir (2008, 2010, 2012) el acceso de los datos de enclave a enclaves con identidades autenticadas que se permite de acuerdo con la lista permitida, en donde la restricción incluye determinar si enviar los datos de enclave desde el enclave sellado al enclave de destino, el cual es diferente del enclave de sellado, con base al menos en parte en si el enclave de destino está incluido en la lista de una o más identidades de enclave permitidas para desellar los datos de enclave.

12. El sistema de acuerdo con la reivindicación 11, en donde:

la primera plataforma de enclave nativa está en una primera computadora y la segunda plataforma de enclave nativa está alojada en una segunda computadora.

13. El sistema de acuerdo con la reivindicación 11, en donde las instrucciones provocan además al menos:

recibir un reporte de afirmación de origen del enclave de origen; y

derivar un valor de identidad permitida a partir del reporte de afirmación de origen y un tipo de identidad abstracta en la lista permitida.

Ref. Expediente N° NC2019/0007656

14. El sistema de acuerdo con la reivindicación 11, en donde se cifran los datos de enclave recibidos, y las instrucciones provocan además al menos:

ejecutar un proceso de afirmación entre el enclave de origen y el enclave de sellado; y

descifrar los datos de enclave cifrados con una clave generada durante el proceso de afirmación.

15. El sistema de acuerdo con la reivindicación 11, en donde almacenar de manera segura los datos de enclave además incluye:

almacenar los datos de enclave sellados en almacenamiento persistente; y
en donde restringir el acceso de los datos de enclave a enclaves con identidades autenticadas adicionalmente incluye:

después de determinar que los datos de enclave son enviados desde el enclave sellado al enclave de destino con base al menos en parte en que el enclave de destino está incluido en la lista de una o más identidades de enclave permitidas para desellar los datos de enclave, descifrar los datos de enclave sellados en respuesta a recibir la petición por los datos de enclave de parte de un enclave de destino.

16. El sistema de acuerdo con la reivindicación 11, en donde una o más identidades de enclave en la lista permitida son especificadas por una o más claves públicas de los respectivos uno o más enclaves.

17. Un sistema que comprende al menos un procesador y memoria que almacena en la misma instrucciones que, cuando son ejecutadas por el sistema, provocan al menos:

recibir, en un enclave de origen (1912) alojado en una primera plataforma de enclave nativa (1916), un primer reporte de afirmación de un enclave de sellado (1932) alojado en una segunda plataforma de enclave nativa (1936);

verificar la confianza en el enclave de sellado;

enviar una lista permitida y datos de enclave asociados hacia el enclave de sellado, en donde la lista permitida incluye una lista de una o más identidades de enclave permitidas para desellar los datos de enclave, dicho envío comprende causar que el enclave de sellado determine si enviar los datos de enclave hacia el enclave de destino que es diferente del enclave de sellado con base al menos en parte en si el enclave de destino está incluido en la lista de una o más identidades de enclave permitidas para desellar los datos de enclave, en donde la lista permitida es una lista de tipos de identidad abstracta que corresponden a respectivos niveles de jerarquía de una jerarquía de identidad; y.

enviar un reporte de afirmación de origen del enclave de origen hacia el enclave de sellado, en donde el reporte de afirmación de origen incluye al menos un valor de identidad del enclave de origen que corresponde a un tipo de identidad abstracta en la lista permitida.



Resolución N° 41327

Ref. Expediente N° NC2019/0007656

18. El sistema de acuerdo con la reivindicación 17, en donde las instrucciones provocan además al menos:

un proceso de afirmación entre el enclave de sellado y el enclave de origen;

generar datos de enclave cifrados al cifrar los datos de enclave con una clave generada durante el proceso de afirmación; y

en donde los datos de enclave enviados al enclave de sellado son los datos de enclave cifrados.

19. El sistema de acuerdo con la reivindicación 17, en donde:

la primera plataforma de enclave nativa está en una primera computadora y la segunda plataforma de enclave nativa está alojada en una segunda computadora.

20. El sistema de acuerdo con la reivindicación 17, en donde las instrucciones provocan además al menos:

completar parcialmente una operación de procesamiento seguro en el enclave de origen; y

en donde los datos de enclave incluyen datos de estado del enclave de origen suficientes para permitir que otra instanciación de enclave continúe la operación de procesamiento seguro completada parcialmente.

