

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Resolución N° **22687**

Ref. Expediente N° NC2019/0007656

Por la cual se otorga parcialmente una Patente de Invención

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 escrito radicado en esta Superintendencia el 16 de julio de 2019, con el N° NC2019/0007656, por LLC MICROSOFT TECHNOLOGY LICENSING, entró a fase nacional la solicitud de patente de invención titulada “SELLADO DE DATOS CON UN ENCLAVE DE SELLADO”, que corresponde a la solicitud internacional PCT/US2017/067455 del 20 de diciembre de 2017.

Que la solicitud fue publicada en la Gaceta de la Propiedad Industrial N° 867 el 31 de julio de 2019, sin que se hubieran presentado oposiciones por parte de terceros.

Que realizado el examen de fondo mediante Oficio N° 18680, notificado el 30 de noviembre de 2021, 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° NC2019/0007656 el 15 de febrero de 2022, respondió oportunamente el requerimiento formulado sin presentar nuevo capítulo reivindicatorio. Por lo tanto, se tendrá en cuenta el capítulo reivindicatorio presentado con el radicado N° NC2019/007656 el 22 de septiembre de 2021.

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, 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 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



Resolución N° 22687

Ref. Expediente N° NC2019/0007656

instancias de enclave, además de proporcionar equivalencia de reportes de afirmación para todos los enclaves con la misma identidad de nivel superior.

En consecuencia, las reivindicaciones 7 a 10 y 17 a 20 cumplen los requisitos de novedad, nivel inventivo y aplicación industrial establecidos en la normatividad citada en precedencia y este Despacho encuentra procedente conceder para las mismas la patente solicitada.

Que por otra parte, las reivindicaciones 1 a 6 y 11 a 16 incluidas en el radicado bajo el N° NC2019/0007656 el 22 de septiembre de 2021, 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 suministrar un método y sistema de aislamiento de un enclave local confiable de código local no confiable fuera del aislamiento del enclave, habilitando la informática confiable remota.

Para resolver este problema técnico, la solicitud proporciona técnicas para sellar y desellar de manera segura datos de enclave a través de plataformas. Los datos de enclave de un enclave de origen alojado en una primera computadora pueden sellarse de manera segura en un enclave de sellado en una segunda computadora, y pueden además desellarse de manera segura para un enclave de destino en una tercera computadora.

Determinación del estado de la técnica

La fecha para determinar el estado de la técnica es el 24 de enero de 2017 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	US 2015/347768	"Policy-Based Trusted Inspection of Rights Managed Content"	03 de diciembre de 2015

El documento D1¹ divulga 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 primer y segundo enclaves seguros tenga acceso a software y datos dentro del primer y segundo enclaves seguros (Pág. 1, Resumen).

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".

¹https://worldwide.espacenet.com/publicationDetails/biblio?CC=US&NR=2015347768A1&KC=A1&FT=D&ND=3&date=20151203&D=B=&locale=en_EP

Resolución N° 22687

Ref. Expediente N° NC2019/0007656

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 sellar datos de enclave, que comprende (...)” (Radicado N° NC2019/0007656 del 22 de septiembre de 2021).

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 sellar datos de enclave, que comprende (...)	Un método ejecutado por al menos un procesador que comprende inicializar el primer y segundo enclaves seguros (Pág. 1, Resumen).
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).	(...) el CPM (306) puede hacer que el nodo (101) envíe un reporte de enclave a un módulo de cotización como el módulo de cotización (307) (Pág. 5, Párr. 058). Las instrucciones CPM también pueden hacer que el nodo (101) selle el ID de la lista blanca en el enclave de memoria (304) (Pág. 8, Párr. 085). (...) un primer enclave seguro que reconoce el segundo enclave seguro como un enclave confiable pero aún no “auténtica” el segundo enclave porque el segundo enclave no está en la lista blanca (Pág. 10, Párr. 113).
Recibir (2004) una lista permitida y datos de enclave asociados del enclave de origen en el enclave de origen, en donde la lista permitida incluye una lista de una o más identidades de enclave permitidas para desellar los datos de enclave.	(...) 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. 068).
Almacenar (2006) de manera segura los datos de enclave y la lista permitida.	Las instrucciones SPM también pueden hacer que el nodo (102) genere un ID de lista blanca para el nodo (101), que puede almacenarse en asociación con la información recibida en la cotización del enclave (101) (Pág. 7, Párr. 083).
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 sellado.	(...) CPM (306) puede configurarse para hacer que el nodo (101) genere un par de claves asimétricas que incluye una clave pública de nodo/cliente (Cpub) y una clave privada de cliente (Cpriv) (...) los cuales pueden almacenarse y/o sellarse en el enclave de memoria (304) (Pág. 5, Párr. 056). (...) un primer enclave seguro que reconoce el segundo enclave seguro como un enclave confiable pero aún no “auténtica” el segundo enclave porque el segundo enclave no está en la lista blanca (Pág. 10, Párr. 113).
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.	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 (...) el texto sin formato de dichos secretos puede protegerse de malware u otras entidades no autorizadas residentes en el cliente (101) (Pág. 6, Párr. 068).
En donde la restricción incluye determinar si enviar los datos de enclave desde el enclave sellado al enclave de destino, el cual es	(...) un primer enclave seguro que reconoce el segundo enclave seguro como un enclave confiable pero aún no

Resolución N° 22687

Ref. Expediente N° NC2019/0007656

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.	“autentica” el segundo enclave porque el segundo enclave no está en la lista blanca (Pág. 10, Párr. 113).
---	---

De acuerdo con la tabla anterior, las características esenciales del método de la reivindicación 1 habían sido divulgadas previamente en los 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: (...) un primer enclave seguro que reconoce el segundo enclave seguro como un enclave confiable pero aún no “autentica” el segundo enclave porque el segundo enclave no está en la lista blanca (Pág. 10, Párr. 113). El nodo (101) y el nodo (102), respectivamente, incluyen plataformas de dispositivos (301), (308). Sin limitación, las plataformas de dispositivos (301), (308) pueden correlacionarse con uno o más tipos de dispositivos, como servidores, clientes, nodos de computación móvil, teléfonos inteligentes, tabletas, computadoras portátiles, netbooks y similares (Pág. 4, Párr. 043).
- Reivindicación 3: A este respecto, el CPM (306) puede hacer que el nodo (101) envíe un reporte de enclave a un módulo de cotización como el módulo de cotización (307) (Pág. 5, Párr. 058). 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. Debido a que el nodo (101) puede revelar los secretos dentro del enclave de memoria (304), el texto sin formato de dichos secretos puede protegerse de malware u otras entidades no autorizadas residentes en el cliente (101) (Pág. 6, Párr. 068).
- Reivindicación 4: (...) un primer enclave seguro que reconoce el segundo enclave seguro como un enclave confiable pero aún no “autentica” el segundo enclave porque el segundo enclave no está en la lista blanca (Pág. 10, Párr. 113). (...) también obtiene la clave de descifrado del documento y transfiere la clave y el control al motor de inspección (120). El motor de inspección descifra el documento dentro de su enclave (...) (Pág. 8, Párr. 088).
- Reivindicación 5: Las instrucciones CPM también pueden hacer que el nodo (101) selle el ID de la lista blanca en el enclave de memoria (304), por ejemplo, cifrando el ID de la lista blanca con la clave del enclave de la memoria del enclave (304) (Pág. 8, Párr. 085). Las instrucciones SPM también pueden hacer que el nodo (102) genere un ID de lista blanca para el nodo (101), que puede almacenarse en asociación con la información recibida en la cotización del enclave. Por ejemplo, las instrucciones SPM pueden hacer que el nodo (102) almacene el ID de la lista blanca en la base de datos (314), en asociación con otra información recibida del nodo (101) (Pág. 7, Párr. 083). (...) memorias como memorias de estado sólido, discos ópticos y magnéticos, memoria de solo lectura (ROM), ROM programable (PROM), borrrable PROM (EPROM), EPROM eléctricamente (EEPROM), una unidad de disco, un disquete, un disco compacto ROM (CD-ROM), un disco versátil digital (DVD), memoria flash (...) (Pág. 11, Párr. 119). (...) un primer enclave seguro que reconoce el segundo enclave seguro como un enclave confiable pero aún no “autentica” el segundo enclave porque el segundo enclave no está en la lista blanca (Pág. 10, Párr. 113). El bloque (745) incluye



Resolución N° 22687

Ref. Expediente N° NC2019/0007656

el segundo enclave seguro que descifra el contenido cifrado para producir contenido descifrado e inspecciona el contenido descifrado (Pág. 10, Párr. 114).

- Reivindicación 6: (...) 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. 068). (...) CPM (306) puede configurarse para hacer que el nodo (101) genere un par de claves asimétricas que incluye una clave pública de nodo/cliente (Cpub) y una clave privada de cliente (Cpriv) (...) los cuales pueden almacenarse y/o sellarse en el enclave de memoria (304) (Pág. 5, Párr. 056).

Las reivindicaciones dependientes 2 a 6 tampoco cumplen con el requisito de novedad.

Por otra parte, el sistema reclamado en la solicitud no es nuevo, teniendo en cuenta que la reivindicación 11 está referida a: *“Un sistema que comprende al menos un procesador y memoria que almacena, en la misma, instrucciones que (...)”* (Radicado N° NC2019/0007656 del 22 de septiembre de 2021).

La siguiente tabla presenta la comparación entre las características técnicas esenciales de la solicitud estudiada, mencionadas en la reivindicación 11, y las reveladas en el documento D1 que representa el estado de la técnica:

Tabla 2. Comparación de las características técnicas esenciales, con las del estado de la técnica

Características esenciales	D1
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:	(...) un aparato que comprende: al menos una memoria; al menos un procesador, acoplado a la memoria, para realizar operaciones que comprenden (...) (Pág. 13, Párr. 150).
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).	(...) el CPM (306) puede hacer que el nodo (101) envíe un reporte de enclave a un módulo de cotización como el módulo de cotización (307) (Pág. 5, Párr. 058). Las instrucciones CPM también pueden hacer que el nodo (101) selle el ID de la lista blanca en el enclave de memoria (304) (Pág. 8, Párr. 085). (...) un primer enclave seguro que reconoce el segundo enclave seguro como un enclave confiable pero aún no “auténtica” el segundo enclave porque el segundo enclave no está en la lista blanca (Pág. 10, Párr. 113).
Recibir (2004) una lista permitida y datos de enclave asociados del enclave de origen, en donde la lista permitida incluye una lista de una o más identidades de enclave permitidas para desellar los datos de enclave.	(...) 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. 068).
Almacenar (2006) de manera segura los datos de enclave y la lista permitida.	Las instrucciones SPM también pueden hacer que el nodo (102) genere un ID de lista blanca para el nodo (101), que puede almacenarse en asociación con la información recibida en la cotización del enclave (101) (Pág. 7, Párr. 083).
En donde el almacenado incluye cifrar los datos de enclave con una clave asociada con	(...) CPM (306) puede configurarse para hacer que el nodo (101) genere un par de claves asimétricas que



Resolución N° 22687

Ref. Expediente N° NC2019/0007656

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.	incluye una clave pública de nodo/cliente (Cpub) y una clave privada de cliente (Cpriv) (...) los cuales pueden almacenarse y/o sellarse en el enclave de memoria (304) (Pág. 5, Párr. 056). (...) un primer enclave seguro que reconoce el segundo enclave seguro como un enclave confiable pero aún no “autentica” el segundo enclave porque el segundo enclave no está en la lista blanca (Pág. 10, Párr. 113).
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.	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 (...) el texto sin formato de dichos secretos puede protegerse de malware u otras entidades no autorizadas residentes en el cliente (101) (Pág. 6, Párr. 068). (...) un primer enclave seguro que reconoce el segundo enclave seguro como un enclave confiable pero aún no “autentica” el segundo enclave porque el segundo enclave no está en la lista blanca (Pág. 10, Párr. 113).
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.	(...) un primer enclave seguro que reconoce el segundo enclave seguro como un enclave confiable pero aún no “autentica” el segundo enclave porque el segundo enclave no está en la lista blanca (Pág. 10, Párr. 113).

De acuerdo con la tabla anterior, las características esenciales del sistema de la reivindicación 11 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 12: (...) un primer enclave seguro que reconoce el segundo enclave seguro como un enclave confiable pero aún no “autentica” el segundo enclave porque el segundo enclave no está en la lista blanca (Pág. 10, Párr. 113). El nodo (101) y el nodo (102), respectivamente, incluyen plataformas de dispositivos (301), (308). Sin limitación, las plataformas de dispositivos (301), (308) pueden correlacionarse con uno o más tipos de dispositivos, como servidores, clientes, nodos de computación móvil, teléfonos inteligentes, tabletas, computadoras portátiles, netbooks y similares (Pág. 4, Párr. 043).
- Reivindicación 13: A este respecto, el CPM (306) puede hacer que el nodo (101) envíe un reporte de enclave a un módulo de cotización como el módulo de cotización (307) (Pág. 5, Párr. 058). 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. Debido a que el nodo (101) puede revelar los secretos dentro del enclave de memoria (304), el texto sin formato de dichos secretos puede protegerse de malware u otras entidades no autorizadas residentes en el cliente (101) (Pág. 6, Párr. 068).
- Reivindicación 14: (...) un primer enclave seguro que reconoce el segundo enclave seguro como un enclave confiable pero aún no “autentica” el segundo enclave porque

Resolución N° 22687

Ref. Expediente N° NC2019/0007656

el segundo enclave no está en la lista blanca (Pág. 10, Párr. 113). (...) también obtiene la clave de descifrado del documento y transfiere la clave y el control al motor de inspección (120). El motor de inspección descifra el documento dentro de su enclave (...) (Pág. 8, Párr. 088).

- Reivindicación 15: Las instrucciones CPM también pueden hacer que el nodo (101) selle el ID de la lista blanca en el enclave de memoria (304), por ejemplo, cifrando el ID de la lista blanca con la clave del enclave de la memoria del enclave (304) (Pág. 8, Párr. 085). Las instrucciones SPM también pueden hacer que el nodo (102) genere un ID de lista blanca para el nodo (101), que puede almacenarse en asociación con la información recibida en la cotización del enclave. Por ejemplo, las instrucciones SPM pueden hacer que el nodo (102) almacene el ID de la lista blanca en la base de datos (314), en asociación con otra información recibida del nodo (101) (Pág. 7, Párr. 083). (...) memorias como memorias de estado sólido, discos ópticos y magnéticos, memoria de solo lectura (ROM), ROM programable (PROM), borrrable PROM (EPROM), EPROM eléctricamente (EEPROM), una unidad de disco, un disquete, un disco compacto ROM (CD-ROM), un disco versátil digital (DVD), memoria flash (...) (Pág. 11, Párr. 119). (...) un primer enclave seguro que reconoce el segundo enclave seguro como un enclave confiable pero aún no “autentica” el segundo enclave porque el segundo enclave no está en la lista blanca (Pág. 10, Párr. 113). El bloque (745) incluye el segundo enclave seguro que descifra el contenido cifrado para producir contenido descifrado e inspecciona el contenido descifrado (Pág. 10, Párr. 114).
- Reivindicación 16: (...) 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. 068). (...) CPM (306) puede configurarse para hacer que el nodo (101) genere un par de claves asimétricas que incluye una clave pública de nodo/cliente (Cpub) y una clave privada de cliente (Cpriv) (...) los cuales pueden almacenarse y/o sellarse en el enclave de memoria (304) (Pág. 5, Párr. 056).

Las reivindicaciones dependientes 12 a 16 tampoco cumplen con el requisito de novedad.

Respuesta a los argumentos del solicitante

El solicitante argumenta que los documentos D1 y D2 no mencionan ni sugieren “(...) *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 (...)*”.

Al respecto, es pertinente aclarar que el documento D1 hace referencia a que (...) un primer enclave seguro que reconoce el segundo enclave seguro como un enclave confiable pero aún no “autentica” el segundo enclave porque el segundo enclave no está en la lista blanca (Pág. 10, Párr. 113). En estos párrafos se puede evidenciar que de acuerdo a lista blanca que contiene los ID autorizados, se puede autenticar o no autorizar a un enclave para comunicación con un enclave de origen. Adicionalmente, tal como se describe el párrafo 113 de este documento, esta acción se puede visualizar en el bloque

Resolución N° 22687

Ref. Expediente N° NC2019/0007656

(735) de la figura 7, donde una vez se autentica el segundo enclave como seguro mediante la lista blanca, se determina que se puede realizar el envío de los datos de enclave desde el primer enclave a este segundo enclave, contrario a lo que sucede cuando el segundo enclave no se autentica como seguro, donde en este caso se restringe y no se determina que se puede realizar el envío de estos datos de enclave, por lo que este argumento no resulta procedente para desvirtuar el análisis de novedad realizado para las reivindicaciones independiente 1 y 11 de acuerdo a lo estipulado en el artículo 16 de la Decisión 486.

El solicitante argumenta *“Solicito al Despacho, y en el evento que el examinador considere que pese a los argumentos presentados aún existen objeciones, que proceda a emitir un examen de fondo adicional sobre el nuevo capítulo reivindicatorio presentado”*.

Esta Oficina aclara que ya se han realizado dos exámenes de patentabilidad de la presente solicitud, y que esta Oficina no considera necesario realizar un tercer examen de patentabilidad teniendo en cuenta que no se presentó una modificación sustancial del capítulo reivindicatorio, ni el pago de la tasa correspondiente a un nuevo examen de patentabilidad; además de que es posible seguir empleando los documentos citados en el Oficio N° 18680, ante los cuales el solicitante ya tuvo la oportunidad de exponer sus argumentos.

Que de acuerdo con la modificación presentada por el solicitante en el escrito radicado bajo el N° NC2019/0007656 el 22 de septiembre de 2021 y teniendo en cuenta el objeto concedido, se modifica el título de la invención el cual quedará de la siguiente manera: **“MÉTODO Y SISTEMA DE SELLADO DE DATOS CON UN ENCLAVE DE SELLADO”**.

Con fundamento en las anteriores consideraciones, el Superintendente de Industria y Comercio,

RESUELVE

ARTÍCULO 1: 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:

“MÉTODO Y SISTEMA DE SELLADO DE DATOS CON UN ENCLAVE DE SELLADO”

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

Reivindicación(es): 7 a 10 y 17 a 20 incluidas en el radicado bajo el No NC2019/0007656 el 22 de septiembre de 2021, de acuerdo con el anexo 1.

Titular(es): LLC MICROSOFT TECHNOLOGY LICENSING.

Domicilio(s): 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.



Resolución N° 22687

Ref. Expediente N° NC2019/0007656

Vigente desde: 20 de diciembre de 2017

Hasta: 20 de diciembre de 2037.

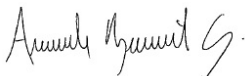
ARTÍCULO 2: Denegar la patente de invención solicitada para las reivindicaciones 1 a 6 y 11 a 16 incluidas en el radicado bajo el N° NC2019/0007656 el 22 de septiembre de 2021, de acuerdo con las razones expuestas en la parte considerativa de la presente resolución.

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 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., a los 25 de abril de 2022



ANDRÉS BARRETO GONZÁLEZ
SUPERINTENDENTE DE INDUSTRIA Y COMERCIO

Firmado digitalmente
por: ANDRÉS
BERNARDO BARRETO
GONZALEZ
Fecha: 2022.04.25
17:00:32 COT
Razón: Validez jurídica.
Ubicación: Bogotá,
Colombia.

ANEXO 1

REIVINDICACIONES CONCEDIDAS

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:
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.

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

Resolución N° **22687**

Ref. Expediente N° NC2019/0007656

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.

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.