

Señores

Superintendencia de Industria y Comercio

Dirección de Nuevas Creaciones

E. S. D.

Ref: Expediente No. NC2019/0007651.

Solicitud de registro de Patente de Invención denominada “MÉTODO, SISTEMA Y DISPOSITIVO PARA IDENTIFICACIÓN DE ENCLAVE DE SELLADO”.

Entrada en fase nacional de la solicitud PCT/US2017/067451.

Solicitante: MICROSOFT TECHNOLOGY LICENSING, LLC.

Luz Helena Adarve, identificada como aparece al pie de mi firma, y obrando en mi condición de apoderada de **MICROSOFT TECHNOLOGY LICENSING, LLC**, solicitante de la patente en referencia, a continuación, doy respuesta al Oficio No. **6398** del 29 de abril de 2021.

1. Respecto al título de la solicitud

En el numeral 2.1 del oficio No. **6398**, se presentan las siguientes observaciones sobre el título de la solicitud:

“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:

El solicitante en el escrito radicado bajo el N° NC2019/0007651 el 16 de julio de 2019, tituló la invención como: ‘IDENTIDAD ABSTRACTA DE ENCLAVE’. Este título no se relaciona con el objeto de la solicitud contenido en la descripción y las modalidades descritas en las

reivindicaciones, por lo cual se sugiere el título siguiente: ‘MÉTODO, SISTEMA Y DISPOSITIVO PARA IDENTIFICACIÓN DE ENCLAVE DE SELLADO’”

Con el objetivo de superar esta objeción, es deseo del solicitante modificar el título de la solicitud de la siguiente forma:

“MÉTODO, SISTEMA Y DISPOSITIVO PARA IDENTIFICACIÓN ~~IDENTIDAD~~
ABSTRACTA DE ENCLAVE DE SELLADO”

Lo anterior, para que el título de la solicitud quede como se muestra a continuación:

**“MÉTODO, SISTEMA Y DISPOSITIVO PARA IDENTIFICACIÓN DE ENCLAVE
DE SELLADO”**

2. Respecto a las Objeciones a la Claridad y Concisión de las reivindicaciones (Artículo. 30 de la Decisión 486).

En el numeral 2.2 del oficio No. **6398**, se presentan la siguiente objeción a la claridad de las reivindicaciones:

- *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.*

Con el fin de superar las objeciones presentadas respecto a la claridad y concisión de las reivindicaciones, el solicitante presenta un nuevo capítulo reivindicatorio en donde se incluyen los números de referencia como lo sugiere el examinador.

3. Respecto a la Determinación del Estado de la Técnica y al Examen de Patentabilidad

En los numerales 3, 4 y 5 del oficio citado, ese Despacho concluye que las reivindicaciones de la presente solicitud de patente carecen de nivel inventivo

frente a las enseñanzas de los documentos titulados “**Intel® Software Guard Extensions Tutorial Series: Part 1, Intel® SGX Foundation**” (D1) y “**Sealing and Attestation in Intel® Software Guard Extensions (SGX)**” (D2).

3.1. Novedad

El nuevo capítulo reivindicatorio ahora presentado es novedoso de acuerdo con el análisis de patentabilidad presentado en el del oficio No. **6398** porque, de acuerdo con dicho análisis, ninguna de las anterioridades divulga completamente la materia reclamada en la solicitud. Teniendo en cuenta que las reivindicaciones del nuevo capítulo reivindicatorio que ahora se presenta mantienen al menos las mismas características que fueron estudiadas en dicho oficio, este nuevo capítulo reivindicatorio es novedoso al menos por dichas características reconocidas como novedosas por este Despacho.

3.2. Nivel inventivo

Aunque el Examinador haya citado los documentos D1 y D2 para objetar la altura inventiva de la presente invención, es posible afirmar que éstos no enseñan las características esenciales de la invención que ahora se reclama en el nuevo capítulo reivindicatorio modificado como se explica a continuación.

Con el fin de superar las objeciones presentadas respecto al nivel inventivo de las reivindicaciones, **es deseo del solicitante presentar un nuevo capítulo reivindicatorio compuesto por 14 reivindicaciones**, que encuentran su debido sustento en las reivindicaciones y la descripción originalmente presentadas, sin que ello conlleve ampliación de la invención.

Primero se indica que las antiguas reivindicaciones 1, 11 y 15, correspondientes a las nuevas reivindicaciones 1, 10 y 14, se modificaron con el objetivo de que sea aún más claro su nivel inventivo donde ahora incluyen las características de la antigua reivindicación 6 que no son divulgadas ni sugeridas por los documentos D1 o D2.

Las características de la antigua reivindicación 6 que se incluyeron son las siguientes:

- *“el valor de identidad se determina como una salida de una función hash; el enclave se sometió a la creación de instancias con una pluralidad de imágenes de enclave; y el tipo de identidad indica cuál de la pluralidad de imágenes de enclave se incluye, al menos en parte, en la función hash para determinar el valor de identidad”.*

Se reitera que las anteriores características no son divulgada ni sugeridas por los documentos D1 o D2. Ninguno de dichos documentos trata la determinación de una identidad como una salida obtenida de una función hash que incluye imágenes de enclave indicadas por el tipo de identidad.

Adicionalmente, la novedad y nivel inventivo de las anteriores características es reconocida por el análisis de patentabilidad del Oficio N° 6398 donde se evidencia que ninguno de los documentos D1 o D2 divulgan la antigua reivindicación 6 que contiene dichas características.

Por todo lo anterior se concluye que las reivindicaciones independientes en cuestión poseen características que no se dan a conocer de manera obvia para una persona versada en la materia por los documentos D1 o D2, por ende la presente invención debe ser considerada como novedosa y con nivel inventivo sobre el estado de la técnica presentado por el Examinador.

4. Conclusión

Las modificaciones realizadas a las reivindicaciones de la presente solicitud de patente y las aclaraciones presentadas a lo largo del presente escrito permiten superar completamente las objeciones realizadas a la claridad de las reivindicaciones, por lo cual, la presente solicitud cumple a cabalidad las exigencias establecidas por el artículo 30 de la Decisión 486 según los requerimientos del Examinador.

De otra parte, los argumentos expuestos en el numeral 3 del presente escrito ponen de manifiesto de una manera clara y contundente que lo revelado en las nuevas reivindicaciones de la presente solicitud resulta completamente NOVEDOSO E INVENTIVO sobre las enseñanzas del estado del arte más cercano representado por los documentos D1 y D2, toda vez que nada dentro de

dichos documentos revela en forma directa o al menos llega a sugerir la determinación de una identidad como una salida obtenida de una función hash que incluye imágenes de enclave indicadas por el tipo de identidad.

En consecuencia, me permito solicitar a ese Despacho, proceder con la revisión de las modificaciones y de los argumentos aquí presentados, para conceder el privilegio de patente solicitado para la materia objeto de las 14 reivindicaciones ahora presentadas en el capítulo reivindicatorio modificado, y que de subsistir alguna duda o inquietud respecto a la patentabilidad de la presente invención, a pesar de las modificaciones y argumentos técnicos ahora presentados, sin apartarse del espíritu inventivo originalmente revelado en la solicitud internacional, se le brinde la oportunidad al solicitante de aclararla o de limitar aún más la invención, mediante la emisión de un segundo examen de fondo, teniendo en cuenta el nuevo capítulo reivindicatorio que se somete a revisión, antes de que se emita una decisión definitiva por parte de ese Despacho, de conformidad con lo dispuesto en 1.2.2.5.1 del artículo primero de la Resolución 54093 de 2012.

5. Anexos

Junto con este escrito se incluye lo siguiente:

- Capítulo reivindicatorio modificado, en donde se han llevado a cabo las modificaciones mencionadas anteriormente.

6. Pagos

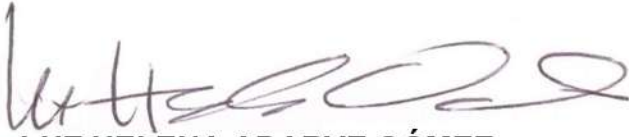
Junto con esta respuesta se paga la tasa correspondiente a la modificación del capítulo reivindicatorio.

Petición

Solicito al Despacho, y en el evento que el examinador considere que pese a las modificaciones presentadas aún existen objeciones, que proceda a emitir un segundo examen de fondo sobre el nuevo capítulo reivindicatorio presentado.

En este sentido requiero se me comunique a través del SIPI o cualquier otro medio la existencia de estas objeciones para, de esta manera, si procede, realizar el nuevo pago del examen de patentabilidad de la solicitud de la referencia.

Atentamente,



LUZ HELENA ADARVE GÓMEZ.

C.C 41.575.435 de Bogotá.

T.P. 14.884 C.S.J.

FJG

P-1072

REIVINDICACIONES (con marcas de modificación)

1. Un método de identificación de enclave realizado por un dispositivo informático que comprende un procesador y una memoria, el método comprende:

Recibir (1503) un tipo de identidad y una solicitud de una operación relacionada con un enclave instanciado;

determinar (1508) un valor de identidad para el enclave con base en el tipo de identidad y la información obtenida a partir de una imagen de enclave a partir de la cual se creó una instancia del enclave;

y

realizar (1512) la operación con el valor de identidad,

en donde:

el valor de identidad se determina como una salida de una función hash;

el enclave se sometió a la creación de instancias con una pluralidad de imágenes de enclave; y

el tipo de identidad indica cuál de la pluralidad de imágenes de enclave se incluye, al menos en parte, en la función hash para determinar el valor de identidad.

2. El método de acuerdo con la reivindicación 1, que comprende, además:

verificar la integridad del valor de identidad al verificar una firma en la imagen de enclave con una clave pública relacionada con un autor de la imagen de enclave.

3. El método de acuerdo con la reivindicación 1, ~~en donde el valor de identidad se determina como una salida de una función hash, y que~~ comprende, además:

determinar, con base, al menos en parte, en el tipo de identidad, una porción de identidad de la imagen de enclave; y

computar la función hash con respecto a la porción de identidad.

4. El método de acuerdo con la reivindicación 3, en donde la imagen de enclave incluye referencias a imágenes de enclave dependientes adicionales, y que comprende, además:

determinar, con base, al menos en parte, en el tipo de identidad, qué imágenes de enclave dependientes adicionales se incluyen como entrada a la función hash.

5. El método de acuerdo con la reivindicación 3, en donde la porción de identidad incluye uno o más de: código binario copiado en un contenedor de enclave seguro durante la creación de instancias del enclave instanciado, y uno o más identificadores que no son código ejecutable.

~~6. El método de acuerdo con la reivindicación 1, en donde:~~
~~el valor de identidad se determina como una salida de una función hash;~~
~~el enclave se sometió a la creación de instancias con una pluralidad de imágenes de enclave; y~~
~~el tipo de identidad indica cuál de la pluralidad de imágenes de enclave se incluye, al menos en parte, en la función hash para determinar el valor de identidad.~~

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

la operación incluye generar un informe de certificación con el valor de identidad.

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

la operación incluye codificar los datos en el enclave al codificar los datos con el valor de identidad.

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

la operación incluye incrementar un contador monótonico, en donde el contador monótonico se identifica por el valor de identidad.

~~109~~. El método de acuerdo con la reivindicación 1, en donde:
la operación incluye realizar una medición de tiempo confiable, en donde el tiempo confiable se determina de acuerdo con el valor de identidad.

~~110~~. Un sistema que comprende al menos un procesador y una memoria que almacena en la misma las instrucciones que, cuando se ejecutan por el sistema, producen al menos las etapas de:

recibir ~~(1503)~~ un tipo de identidad y una solicitud de una operación relacionada con un enclave instanciado;

determinar ~~(1508)~~ un valor de identidad para el enclave con base en el tipo de identidad y la información obtenida a partir de una imagen de enclave a partir de la cual se creó una instancia del enclave;
y

realizar ~~(1512)~~ la operación con el valor de identidad.

en donde:

el valor de identidad se determina como una salida de una función hash;

el enclave se sometió a la creación de instancias con una pluralidad de imágenes de enclave; y

el tipo de identidad indica cuál de la pluralidad de imágenes de enclave se incluye, al menos en parte, en la función hash para determinar el valor de identidad.

~~1211~~. El sistema de acuerdo con la reivindicación ~~1110~~, en donde las instrucciones producen, además, al menos las etapas de:

verificar la integridad del valor de identidad al verificar una firma en la imagen de enclave con una clave pública relacionada con un autor de la imagen de enclave.

~~1312~~. El sistema de acuerdo con la reivindicación ~~1110~~, en donde el valor de identidad se determina como una salida de una función hash, y en donde las instrucciones producen, además, al menos las etapas de:

determinar, con base, al menos en parte, en el tipo de identidad, una porción de identidad de la imagen de enclave; y

computar la función hash con respecto a la porción de identidad.

~~1413~~. El sistema de acuerdo con la reivindicación ~~1312~~, en donde la imagen de enclave incluye referencias a las imágenes de enclave dependientes adicionales, y en donde las instrucciones producen, además, al menos las etapas de:

determinar, con base, al menos en parte, en el tipo de identidad, qué imágenes de enclave dependientes adicionales se incluyen como entrada a la función hash.

~~1514~~. Un dispositivo informático configurado para:

recibir un tipo de identidad y una solicitud de una operación relacionada con un enclave instanciado;

determinar un valor de identidad para el enclave con base en el tipo de identidad y los datos almacenados en un contenedor de enclave; y

realizar la operación con el valor de identidad.

en donde:

el valor de identidad se determina como una salida de una función hash;

el enclave se sometió a la creación de instancias con una pluralidad de imágenes de enclave; y

el tipo de identidad indica cuál de la pluralidad de imágenes de enclave se incluye, al menos en parte, en la función hash para determinar el valor de identidad.

REIVINDICACIONES

1. Un método de identificación de enclave realizado por un dispositivo informático que comprende un procesador y una memoria, el método comprende:

Recibir (1503) un tipo de identidad y una solicitud de una operación relacionada con un enclave instanciado;

determinar (1508) un valor de identidad para el enclave con base en el tipo de identidad y la información obtenida a partir de una imagen de enclave a partir de la cual se creó una instancia del enclave; y

realizar (1512) la operación con el valor de identidad,

en donde:

el valor de identidad se determina como una salida de una función hash;

el enclave se sometió a la creación de instancias con una pluralidad de imágenes de enclave; y

el tipo de identidad indica cuál de la pluralidad de imágenes de enclave se incluye, al menos en parte, en la función hash para determinar el valor de identidad.

2. El método de acuerdo con la reivindicación 1, que comprende, además:

verificar la integridad del valor de identidad al verificar una firma en la imagen de enclave con una clave pública relacionada con un autor de la imagen de enclave.

3. El método de acuerdo con la reivindicación 1 que comprende, además:

determinar, con base, al menos en parte, en el tipo de identidad, una porción de identidad de la imagen de enclave; y

computar la función hash con respecto a la porción de identidad.

4. El método de acuerdo con la reivindicación 3, en donde la imagen de enclave incluye referencias a imágenes de enclave dependientes adicionales, y que comprende, además:

determinar, con base, al menos en parte, en el tipo de identidad, qué imágenes de enclave dependientes adicionales se incluyen como entrada a la función hash.

5. El método de acuerdo con la reivindicación 3, en donde la porción de identidad incluye uno o más de: código binario copiado en un contenedor de enclave seguro durante la creación de instancias del enclave instanciado, y uno o más identificadores que no son código ejecutable.

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

la operación incluye generar un informe de certificación con el valor de identidad.

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

la operación incluye codificar los datos en el enclave al codificar los datos con el valor de identidad.

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

la operación incluye incrementar un contador monotónico, en donde el contador monotónico se identifica por el valor de identidad.

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

la operación incluye realizar una medición de tiempo confiable, en donde el tiempo confiable se determina de acuerdo con el valor de identidad.

10. Un sistema que comprende al menos un procesador y una memoria que almacena en la misma las instrucciones que, cuando se ejecutan por el sistema, producen al menos las etapas de:

recibir (1503) un tipo de identidad y una solicitud de una operación relacionada con un enclave

instanciado;

determinar (1508) un valor de identidad para el enclave con base en el tipo de identidad y la información obtenida a partir de una imagen de enclave a partir de la cual se creó una instancia del enclave;

y

realizar (1512) la operación con el valor de identidad,

en donde:

el valor de identidad se determina como una salida de una función hash;

el enclave se sometió a la creación de instancias con una pluralidad de imágenes de enclave; y

el tipo de identidad indica cuál de la pluralidad de imágenes de enclave se incluye, al menos en parte, en la función hash para determinar el valor de identidad.

11. El sistema de acuerdo con la reivindicación 10, en donde las instrucciones producen, además, al menos las etapas de:

verificar la integridad del valor de identidad al verificar una firma en la imagen de enclave con una clave pública relacionada con un autor de la imagen de enclave.

12. El sistema de acuerdo con la reivindicación 10, en donde el valor de identidad se determina como una salida de una función hash, y en donde las instrucciones producen, además, al menos las etapas de:

determinar, con base, al menos en parte, en el tipo de identidad, una porción de identidad de la imagen de enclave; y

computar la función hash con respecto a la porción de identidad.

13. El sistema de acuerdo con la reivindicación 12, en donde la imagen de enclave incluye referencias a las imágenes de enclave dependientes adicionales, y en donde las instrucciones producen, además, al menos las etapas de:

determinar, con base, al menos en parte, en el tipo de identidad, qué imágenes de enclave dependientes adicionales se incluyen como entrada a la función hash.

14. Un dispositivo informático configurado para:

recibir un tipo de identidad y una solicitud de una operación relacionada con un enclave instanciado;

determinar un valor de identidad para el enclave con base en el tipo de identidad y los datos almacenados en un contenedor de enclave; y

realizar la operación con el valor de identidad,

en donde:

el valor de identidad se determina como una salida de una función hash;

el enclave se sometió a la creación de instancias con una pluralidad de imágenes de enclave; y

el tipo de identidad indica cuál de la pluralidad de imágenes de enclave se incluye, al menos en parte, en la función hash para determinar el valor de identidad.