

Señores

Superintendencia de Industria y Comercio

Dirección de Nuevas Creaciones

E. S. D.

Ref: Expediente No. NC2019/0007655.

Solicitud de registro de Patente de Invención denominada “SISTEMA, MÉTODO Y MEDIO DE ALMACENAMIENTO PARA DETERMINAR LA EQUIVALENCIA DE ENCLAVE”.

Entrada en fase nacional de la solicitud PCT/US2018/014298.

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. **699** del 25 de enero de 2021.

1. Respecto al título de la solicitud

En el numeral 2.1 del oficio No. **699**, 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° NC2019/0007655 el 16 de julio de 2019, tituló la invención como: “IDENTIDAD DE ENCLAVE MULTIPLATAFORMA”. Este título no se relaciona con el

objeto de la solicitud contenido en la descripción y las reivindicaciones, por lo cual se sugiere el título siguiente: ‘SISTEMAS Y MÉTODO PARA DETERMINAR LA EQUIVALENCIA DE ENCLAVE DE UNA IDENTIDAD ABSTRACTA DE ENCLAVE’ ”.

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

“SISTEMA, MÉTODO Y MEDIO DE ALMACENAMIENTO PARA DETERMINAR LA EQUIVALENCIA DE ENCLAVE”

Sobre este nuevo título, se indica que difiere del título sugerido por el examinador en que menciona un *“medio de almacenamiento”* y en que no menciona *“de una identidad abstracta de enclave”*.

El nuevo título menciona un *“medio de almacenamiento”* con el objetivo de incluir la materia reclamada de la nueva reivindicación 23.

El nuevo título no menciona *“de una identidad abstracta de enclave”* debido a que dicha característica, aunque corresponde a la característica de una realización de la invención de acuerdo con la descripción de la presente solicitud, no es una característica estrictamente necesaria y, por lo tanto, no describiría la esencia de la presente solicitud.

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. **699**, se presentan la siguiente objeción a la claridad de las reivindicaciones:

“La reivindicación 6 hace referencia a ‘(...) arquitectura de enclave de extensiones de protección de software (SGX, por sus siglas en inglés) de Intel y (...) una arquitectura de enclave de modo seguro virtual (VSM, por sus siglas en inglés) de Microsoft (...)’, que es una marca registrada que no define el producto, porque sus características técnicas pueden cambiar con el paso del tiempo, aunque conserve el mismo nombre”.

Con el objetivo de superar esta objeción, la antigua reivindicación 6, que corresponde a la nueva reivindicación 7, se modificó para eliminar las expresiones objetadas y reemplazarlas por “*una primera arquitectura de enclave*” y “*una segunda arquitectura de enclave*”.

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 **US20150033012 (D1)** y **US20150304736 (D2)**.

3.1. Novedad y 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, como se explica a continuación.

Por ejemplo, ninguno de los documentos D1 o D2 enseña ni sugiere “*recibir un segundo informe de certificación a partir de un segundo enclave instanciado en una segunda plataforma de enclave nativa, en donde la primera plataforma de enclave nativa y la segunda plataforma de enclave nativa son diferentes*”, como lo requiere la reivindicación independiente 1.

En el examen de patentabilidad, el examinador se basa en el párrafo [0054] del documento D1 para supuestamente mostrar que esta característica fue previamente divulgada por dicho documento. Sin embargo, después de revisar dicha referencia, se afirma que nada en el párrafo citado (párrafo [0054] del documento D1) o en cualquier otra parte del documento D1 enseña o sugiere dicha característica.

El documento D1 da a conocer una técnica para la medición y certificación del entorno de procesamiento seguro (ver el Título y el Resumen del documento D1). El documento D1 describe una estructura de control de enclave seguro (SECS),

que “se crea mediante la ejecución de una instrucción ECREATE para contener metadatos para ser utilizados por hardware, y accesibles solo por hardware (...) para definir, mantener y proteger un enclave” (D1, párr. [0033]). El SECS “incluye un primer registro de medición (MRENCLAVE) (...) para almacenar el valor de medición de construcción del enclave (...) y un segundo registro de medición (MRSIGNER) (...) para almacenar una medición de un identificador, como una clave pública, de la entidad que verificó la creación del enclave” (D1, párr. [0033]). “La medida [del enclave] puede usarse como una huella dactilar del enclave...” (D1, párr. [0037]). La medición del enclave “puede generarse de dos formas diferentes, por ejemplo, calculando un hash (...) y calculando un MAC...” (D1, párr. [0038]). La técnica divulgada en el documento D1 “prevé que el enclave se mida de ambas formas la primera vez que [el enclave] se construye sobre una plataforma (por ejemplo, el sistema 100), y se mide de una sola manera (por ejemplo, por el cálculo de un MAC) cuando [el enclave] se construya posteriormente” (D1, párr. [0038]). El documento D1 explica que “el lanzamiento inicial de una aplicación de software que se ejecutará en un enclave seguro en el sistema 100 puede resultar en la generación de un hash y un MAC del enclave seguro a medida que se construye, y cualquier lanzamiento subsecuente de esa aplicación de software en el sistema 100 (por ejemplo, después de un reinicio o apagado) puede resultar en la generación del MAC pero no en el hash del enclave seguro tal como está construido” (D1, párr. [0038], subrayado fuera de texto).

Con referencia a la Figura 4, el documento D1 describe un método que incluye “una construcción inicial de un enclave seguro en el sistema 100” (ver, por ejemplo, D1, párr. [0040] y el recuadro 410 de la Figura 4) y “una construcción posterior del enclave seguro en el sistema 100” (ver, por ejemplo, D1, párr. [0050] y el recuadro 440 de la Figura 4). El documento D1 explica que “una o más páginas (...) se pueden agregar al enclave y medir (...) para reconstruir el enclave...” (D1, párr. [0051]).

De acuerdo con el análisis de patentabilidad del oficio en referencia, parece que el examinador se basa en la construcción inicial del enclave seguro en el sistema 100, como lo describe D1, para corresponder al primer enclave instanciado en una primera plataforma de enclave nativa, como se menciona en la reivindicación 1 de la solicitud. Adicionalmente, parece que el examinador se basa en la construcción posterior del enclave seguro en el sistema 100, como lo describe D1, para que corresponda al segundo enclave instanciado en una segunda plataforma de enclave nativa, como se menciona en la reivindicación 1 de la solicitud. De

acuerdo con lo anterior, el solicitante indica que la construcción inicial y la construcción subsiguiente descritas en D1 son del mismo enclave seguro. Independientemente, el documento D1 no sugiere de ninguna manera que la construcción inicial del enclave seguro se instancia en una primera plataforma de enclave nativa y que la construcción posterior del enclave seguro se instancia en una segunda plataforma de enclave nativa que sea diferente de la primera plataforma, como se sugiere en el análisis de patentabilidad del oficio en referencia. Por el contrario, el documento D1 establece específicamente que la construcción inicial del enclave seguro está en el sistema 100, y la construcción posterior del enclave seguro está en el sistema 100. La afectación de patentabilidad de la presente solicitud (y comunicada a través del oficio en referencia) se fundamenta en una invención en el que el sistema 100 corresponde a la primera plataforma de enclave nativa y a la segunda plataforma del enclave nativa. Sin embargo, la reivindicación independiente 1 requiere que "la primera plataforma de enclave nativa y la segunda plataforma de enclave nativa [sean] diferentes".

El párrafo [0054] del documento D1, en el que se basa la afectación del estudio de patentabilidad del oficio en referencia, explica que *"la ejecución de la instrucción EINIT puede incluir la actualización o extensión del MAC con una firma u otra certificación que represente la identidad del creador o verificador del enclave, junto con cualquier otra propiedad de seguridad del enclave, para generar el MAC final del enclave reconstruido (el 'MAC de reconstrucción final'). La firma puede ser proporcionada por el creador o verificador del enclave, verificada por el procesador 200 como parte de la ejecución de la instrucción EINIT y almacenada en MRSIGNER 314"* (D1, párr. [0054]). Sin embargo, nada en el párrafo [0054] o cualquier otra parte del documento D1 sugiere de ninguna manera que la construcción inicial del enclave seguro se instancia en una primera plataforma de enclave nativo y que la construcción posterior del enclave seguro se instancia en una segunda plataforma de enclave nativa que es diferente de dicha primera plataforma de enclave nativa.

Por al menos las anteriores razones, el documento D1 no enseña ni sugiere *"recibir un segundo informe de certificación a partir de un segundo enclave instanciado en una segunda plataforma de enclave nativa, en donde la primera plataforma de enclave nativa y la segunda plataforma de enclave nativa son diferentes"*, según lo reclamado por la reivindicación 1 de la presente solicitud.

Además, el documento D2 no menciona, ni subsana esta deficiencia del documento D1 respecto a la reivindicación 1.

Los documentos D1 y D2 tampoco enseñan ni sugieren *“realizar, con base en la determinación, una operación de computación al completar parcialmente la operación de computación en el primer enclave y al completar parcialmente la operación de computación en el segundo enclave”*, como lo requiere la reivindicación independiente 1. El análisis de la patentabilidad presentado en el oficio en referencia reconoce que el documento D1 no revela explícitamente esta característica. En cambio, dicho examen se basa en los párrafos [0044] y [0045] del documento D2 para afectar supuestamente el nivel inventivo de esta característica. Sin embargo, tras la debida inspección, nada en los párrafos citados o en cualquier otra parte del documento D2 enseña o sugiere dicha característica de la reivindicación independiente 1.

El documento D2 da a conocer un sistema para fortalecer la seguridad de la información digital en las plataformas de los clientes (ver D2, Título y párr. [0036]). El sistema incluye un cliente 101, un servidor 102 y un distribuidor opcional 103, en donde el cliente 101 se utiliza para consumir información digital recibida de una fuente, como el servidor 102 o el distribuidor 103 (D2, párr. [0036]). El *“distribuidor 103 puede ser el propietario/creador de información digital y puede desear compartir de forma segura dicha información con el cliente 101”* (D2, párr. [0037]). El distribuidor 103 puede proporcionar al *“servidor 102 una licencia que incluye una copia de [una clave] que se utilizó para cifrar la información digital proporcionada al cliente 101, así como una política de acceso a la información que rige dicha información”* (D2, párr. [0042]). *“El servidor 102 puede condicionar la distribución de una licencia a la autenticación exitosa del cliente 101”* (D2, párr. [0044]). Por ejemplo, el servidor puede analizar *“las credenciales de autenticación recibidas del cliente 101, por ejemplo, contra la política de acceso recibida del distribuidor 103, una lista preestablecida de plataformas confiables”* (D2, párr. [0044]). *“Si el servidor 102 autentica exitosamente al cliente 101, puede transmitir toda o una parte de la licencia que rige la información digital al cliente 101, incluyendo cualquier clave pertinente”* (D2, párr. [0045]) y potencialmente la política de acceso a la información. La política de acceso *“puede ser aplicada por un módulo de aplicación de políticas (PEM) (...) Si la política de acceso lo permite, el cliente 101 puede acceder y utilizar las claves proporcionadas con la licencia ... para descifrar la información digital cifrada”* (D2, párr. [0045]).

Sin embargo, parece que nada en los párrafos citados o en cualquier otra parte del documento D2 menciona nada sobre una operación de computación que se completa parcialmente en un primer enclave y que se completa parcialmente en un segundo enclave, como lo sugiere el examen de patentabilidad del oficio en referencia. En consecuencia, no es posible que el documento D2 enseñe o sugiera *"realizar, con base en la determinación, una operación de computación al completar parcialmente la operación de computación en el primer enclave y al completar parcialmente la operación de computación en el segundo enclave"*, como se reclama en la reivindicación independiente 1. Además, el documento D1 no menciona ni subsana esta deficiencia del documento D2 respecto a la reivindicación independiente 1 como se indicó anteriormente.

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 al Título y 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 *"recibir un segundo informe de certificación a partir de un segundo enclave instanciado en una segunda plataforma de enclave nativa, en donde la primera plataforma de enclave nativa y la segunda plataforma de enclave nativa son diferentes"*, ni tampoco *"realizar, con base en la determinación, una operación de computación al*

completar parcialmente la operación de computación en el primer enclave y al completar parcialmente la operación de computación en el segundo enclave”.

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 23 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

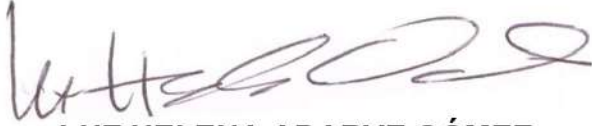
Junto con esta respuesta se paga la tasa correspondiente a la modificación y a 8 reivindicaciones adicionales.

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-1073

REIVINDICACIONES (con marcas de modificación)

1. Un método para determinar la equivalencia de enclave, que comprende
recibir un primer informe de certificación a partir de un primer enclave instanciado en una primera plataforma de enclave nativa;
extraer un primer valor de identidad de enclave asociado con un tipo de identidad de enclave a partir del primer informe de certificación;
recibir un segundo informe de certificación a partir de un segundo enclave instanciado en una segunda plataforma de enclave nativa, en donde la primera plataforma de enclave nativa y la segunda plataforma de enclave nativa son diferentes;
extraer un segundo valor de identidad de enclave asociado con el tipo de identidad de enclave a partir del segundo informe de certificación;
determinar que el primer valor de identidad de enclave es el mismo que el segundo valor de identidad de enclave; y
realizar, con base en la determinación, una operación de computación al completar parcialmente la operación de computación en el primer enclave y al completar parcialmente la operación de computación en el segundo enclave.

2. El método de acuerdo con la reivindicación 1, en donde la operación de computación se realiza en serie con el primer y segundo enclave, y comprende, además:
codificar los datos de estado de enclave del primer enclave después de completar parcialmente la operación de computación en el primer enclave para producir los datos codificados, en donde los datos de estado se codifican para el tipo de identidad de enclave;
copiar los datos codificados desde el primer enclave al segundo enclave; y
decodificar los datos codificados en el segundo enclave.

3. El método de acuerdo con la reivindicación 1, en donde la operación de computación se realiza simultáneamente con el primer y segundo enclave, y comprende, además:
copiar una primera porción de un conjunto de datos en el primer enclave;
copiar una segunda porción de un conjunto de datos en el segundo enclave; y
en donde la operación de computación se completa parcialmente en el primer enclave utilizando la primera porción y se completa parcialmente en el segundo enclave utilizando la segunda porción.

4. El método de acuerdo con la reivindicación 1, en donde:
completar parcialmente la operación de computación en el primer enclave incluye la lectura, por el primer enclave, de un contador monotónico o un tiempo confiable asociado con el valor de identidad; y
completar parcialmente la operación de computación en el segundo enclave incluye la lectura, por el segundo enclave, del contador monotónico o del tiempo confiable asociado con el valor de identidad.

5. El método de acuerdo con la reivindicación 1, en donde:
completar parcialmente la operación de computación en el primer enclave incluye la lectura, por el primer enclave, de un un tiempo confiable asociado con el valor de identidad; y
completar parcialmente la operación de computación en el segundo enclave incluye la lectura, por el segundo enclave, del tiempo confiable asociado con el valor de identidad.

5-6. El método de acuerdo con la reivindicación 1, que comprende, además:
crear una firma para el primer informe de certificación al realizar al menos una primera operación

de plataforma nativa; y

crear una firma para el segundo informe de certificación al realizar al menos una segunda operación de plataforma nativa.

6.7. El método de acuerdo con la reivindicación 1, en donde la primera plataforma de enclave nativa se adapta a una primera arquitectura de enclave ~~de extensiones de protección de software (SGX, por sus siglas en inglés) de Intel~~ y la segunda plataforma de enclave nativa se adapta a una segunda arquitectura de enclave ~~de modo seguro virtual (VSM, por sus siglas en inglés) de Microsoft~~, y que comprende, además:

generar el primer informe de certificación al realizar al menos una operación nativa de ~~SGX~~ la primera arquitectura de enclave; y

generar el segundo informe de certificación al realizar al menos una operación nativa de la segunda arquitectura de enclave ~~VSM~~.

8. El método de acuerdo con la reivindicación 1, en donde:
la primera plataforma de enclave nativa y la segunda plataforma de enclave nativa son diferentes versiones de la misma arquitectura de enclave.

7.9. El método de acuerdo con la reivindicación 1, que comprende, además:
verificar una primera firma del primer informe de certificación con una clave pública asociada con la primera plataforma de enclave nativa; y

verificar una segunda firma del segundo informe de certificación con una clave pública asociada con la segunda plataforma del enclave nativa, en donde la primera clave pública y la segunda clave pública son diferentes.

8.10. El método de acuerdo con la reivindicación 1, que comprende, además:
verificar un primer certificado de aprobación de la primera plataforma nativa con una primera clave pública asociada con un fabricante de la primera plataforma de enclave nativa; y
verificar un segundo certificado de aprobación de la segunda plataforma de enclave nativa con una segunda clave pública asociada con el fabricante de la segunda plataforma de enclave nativa, en donde la primera clave pública y la segunda clave pública no son las mismas.

9.11. El método de acuerdo con la reivindicación 1, que comprende, además:
generar el primer informe de certificación al computar un valor *hash* con respecto a una primera porción de memoria en un contenedor seguro del primer enclave, en donde el contenido de la primera porción de memoria es independiente de la primera plataforma nativa; y
generar el segundo informe de certificación al computar un valor *hash* con respecto a una segunda porción de memoria en un contenedor seguro del segundo enclave, en donde el contenido de la segunda porción de memoria es independiente de la segunda plataforma nativa.

10.12. 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:~~
memoria; y

uno o más procesadores acoplados a la memoria, los uno o más procesadores configurados para:

recibir un primer informe de certificación a partir de un primer enclave instanciado en una primera plataforma de enclave nativa;

extraer un primer valor de identidad de enclave asociado con un tipo de identidad de

enclave a partir del primer informe de certificación;

recibir un segundo informe de certificación a partir de un segundo enclave instanciado en una segunda plataforma de enclave nativa, en donde la primera plataforma de enclave nativa y la segunda plataforma de enclave nativa son diferentes;

extraer un segundo valor de identidad de enclave asociado con el tipo de identidad de enclave a partir del segundo informe de certificación;

comparar el primer valor de identidad de enclave con el segundo valor de identidad de enclave; y

realizar una operación de computación al completar parcialmente la operación de computación en el primer enclave y al completar parcialmente la operación de computación en el segundo enclave.

13. El sistema de acuerdo con la reivindicación ~~10~~12, en donde el uno o más procesadores están configurados para realizar la operación de computación ~~se realiza~~ en serie con el primer y segundo enclave; ~~y~~

en donde el uno o más procesadores están adicionalmente configurados para las instrucciones producen, además, al menos las etapas de:

codificar los datos de estado de enclave del primer enclave después de completar parcialmente la operación de computación en el primer enclave para producir los datos codificados, en donde los datos de estado se codifican para el tipo de identidad de enclave;

copiar los datos codificados desde el primer enclave al segundo enclave; y

decodificar los datos codificados en el segundo enclave.

14. El sistema de acuerdo con la reivindicación ~~10~~12, en donde el uno o más procesadores están configurados para realizar la operación de computación se realiza simultáneamente con el primero y segundo enclave; ~~y~~

en donde el uno o más procesadores están adicionalmente configurados para las instrucciones producen, además, al menos las etapas de:

copiar una primera porción de un conjunto de datos en el primer enclave; ~~y~~

copiar una segunda porción de un conjunto de datos en el segundo enclave; y

en donde el uno o más procesadores están configurados para completar parcialmente la operación de computación ~~se completa parcialmente~~ en el primer enclave utilizando la primera porción y ~~se completa~~ parcialmente la operación de computación en el segundo enclave utilizando la segunda porción.

15. El sistema de acuerdo con la reivindicación 12, en donde el uno o más procesadores están configurados para:

completar parcialmente la operación de computación en el primer enclave al causar que el primer enclave lea un contador monotónico asociado con el valor de identidad; y

completar parcialmente la operación de computación en el segundo enclave al causar que el segundo enclave lea el contador monotónico asociado con el valor de identidad.

16. El sistema de acuerdo con la reivindicación 12, en donde el uno o más procesadores están configurados para:

completar parcialmente la operación de computación en el primer enclave al causar que el primer enclave lea un tiempo confiable asociado con el valor de identidad; y

completar parcialmente la operación de computación en el segundo enclave al causar que el

segundo enclave lea el tiempo confiable asociado con el valor de identidad.

17. El sistema de acuerdo con la reivindicación 12, en donde el uno o más procesadores están configurados adicionalmente para:

crear una firma para el primer informe de certificación al realizar al menos una primera operación de plataforma nativa; y

crear una firma para el segundo informe de certificación al realizar al menos una segunda operación de plataforma nativa.

18. El sistema de acuerdo con la reivindicación 12, en donde la primera plataforma de enclave nativa se adapta a una primera arquitectura de enclave y la segunda plataforma de enclave nativa se adapta a una segunda arquitectura de enclave; y

en donde el uno o más procesadores están adicionalmente configurados para:

generar el primer informe de certificación al realizar al menos una operación nativa de la primera arquitectura de enclave; y

generar el segundo informe de certificación al realizar al menos una operación nativa de la segunda arquitectura de enclave.

19. El sistema de acuerdo con la reivindicación 12, en donde la primera plataforma de enclave nativa y la segunda plataforma de enclave nativa son diferentes versiones de la misma arquitectura de enclave.

20. El sistema de acuerdo con la reivindicación 12, en donde el uno o más procesadores están configurados adicionalmente para:

verificar una primera firma del primer informe de certificación con una clave pública asociada con la primera plataforma de enclave nativa; y

verificar una segunda firma del segundo informe de certificación con una clave pública asociada con la segunda plataforma del enclave nativa, en donde la primera clave pública y la segunda clave pública son diferentes.

13.21. El sistema de acuerdo con la reivindicación 1012, en donde uno o más procesadores están configurados adicionalmente para las instrucciones producen, además, al menos las etapas de:

verificar un primer certificado de aprobación de la primera plataforma nativa con una primera clave pública asociada con un fabricante de la primera plataforma de enclave nativa; y

verificar un segundo certificado de aprobación de la segunda plataforma de enclave nativa con una segunda clave pública asociada con el fabricante de la segunda plataforma de enclave nativa, en donde la primera clave pública y la segunda clave pública no son las mismas.

14.22. El sistema de acuerdo con la reivindicación 1012, en donde el uno o más procesadores están configurados adicionalmente para las instrucciones producen, además, al menos las etapas de:

generar el primer informe de certificación al computar un valor *hash* con respecto a una primera porción de memoria en un contenedor seguro del primer enclave, en donde el contenido de la primera porción de memoria es independiente de la primera plataforma nativa; y

generar el segundo informe de certificación al computar un valor *hash* con respecto a una segunda porción de memoria en un contenedor seguro del segundo enclave, en donde el contenido de la segunda porción de memoria es independiente de la segunda plataforma nativa.

15-23. Un medio de almacenamiento legibles por computadora que tiene instrucciones almacenadas en el mismo para permitir a un sistema basado en procesador para determinar una equivalencia de enclaveque, las operaciones comprenden:

~~medios para~~ recibir un primer informe de certificación desde un primer enclave instanciado en una primera plataforma de enclave nativa;

~~medios para~~ extraer un primer valor de identidad de enclave asociado con un tipo de identidad de enclave a partir del primer informe de certificación;

~~medios para~~ recibir un segundo informe de certificación desde un segundo enclave instanciado en una segunda plataforma de enclave nativa, en donde la primera plataforma de enclave nativa y la segunda plataforma de enclave nativa son diferentes;

~~medios para~~ extraer un segundo valor de identidad de enclave asociado con el tipo de identidad de enclave a partir del segundo informe de certificación;

~~medios para~~ comparar el primer valor de identidad de enclave con el segundo valor de identidad de enclave; y

~~medios para~~ realizar una operación de computación al completar parcialmente la operación de computación en el primer enclave y al completar parcialmente la operación de computación en el segundo enclave.

REIVINDICACIONES

1. Un método para determinar la equivalencia de enclave, que comprende
recibir un primer informe de certificación a partir de un primer enclave instanciado en una primera plataforma de enclave nativa;
extraer un primer valor de identidad de enclave asociado con un tipo de identidad de enclave a partir del primer informe de certificación;
recibir un segundo informe de certificación a partir de un segundo enclave instanciado en una segunda plataforma de enclave nativa, en donde la primera plataforma de enclave nativa y la segunda plataforma de enclave nativa son diferentes;
extraer un segundo valor de identidad de enclave asociado con el tipo de identidad de enclave a partir del segundo informe de certificación;
determinar que el primer valor de identidad de enclave es el mismo que el segundo valor de identidad de enclave; y
realizar, con base en la determinación, una operación de computación al completar parcialmente la operación de computación en el primer enclave y al completar parcialmente la operación de computación en el segundo enclave.
2. El método de acuerdo con la reivindicación 1, en donde la operación de computación se realiza en serie con el primer y segundo enclave, y comprende, además:
codificar los datos de estado de enclave del primer enclave después de completar parcialmente la operación de computación en el primer enclave para producir los datos codificados, en donde los datos de estado se codifican para el tipo de identidad de enclave;
copiar los datos codificados desde el primer enclave al segundo enclave; y
decodificar los datos codificados en el segundo enclave.
3. El método de acuerdo con la reivindicación 1, en donde la operación de computación se realiza simultáneamente con el primer y segundo enclave, y comprende, además:
copiar una primera porción de un conjunto de datos en el primer enclave;
copiar una segunda porción de un conjunto de datos en el segundo enclave; y
en donde la operación de computación se completa parcialmente en el primer enclave utilizando la primera porción y se completa parcialmente en el segundo enclave utilizando la segunda porción.
4. El método de acuerdo con la reivindicación 1, en donde:
completar parcialmente la operación de computación en el primer enclave incluye la lectura, por el primer enclave, de un contador monotónico o un tiempo confiable asociado con el valor de identidad; y
completar parcialmente la operación de computación en el segundo enclave incluye la lectura, por el segundo enclave, del contador monotónico o del tiempo confiable asociado con el valor de identidad.
5. El método de acuerdo con la reivindicación 1, en donde:
completar parcialmente la operación de computación en el primer enclave incluye la lectura, por el primer enclave, de un un tiempo confiable asociado con el valor de identidad; y
completar parcialmente la operación de computación en el segundo enclave incluye la lectura, por el segundo enclave, del tiempo confiable asociado con el valor de identidad.
6. El método de acuerdo con la reivindicación 1, que comprende, además:
crear una firma para el primer informe de certificación al realizar al menos una primera operación

de plataforma nativa; y

crear una firma para el segundo informe de certificación al realizar al menos una segunda operación de plataforma nativa.

7. El método de acuerdo con la reivindicación 1, en donde la primera plataforma de enclave nativa se adapta a una primera arquitectura de enclave y la segunda plataforma de enclave nativa se adapta a una segunda arquitectura de enclave, y que comprende, además:

generar el primer informe de certificación al realizar al menos una operación nativa de la primera arquitectura de enclave; y

generar el segundo informe de certificación al realizar al menos una operación nativa de la segunda arquitectura de enclave.

8. El método de acuerdo con la reivindicación 1, en donde:
la primera plataforma de enclave nativa y la segunda plataforma de enclave nativa son diferentes versiones de la misma arquitectura de enclave.

9. El método de acuerdo con la reivindicación 1, que comprende, además:
verificar una primera firma del primer informe de certificación con una clave pública asociada con la primera plataforma de enclave nativa; y

verificar una segunda firma del segundo informe de certificación con una clave pública asociada con la segunda plataforma del enclave nativa, en donde la primera clave pública y la segunda clave pública son diferentes.

10. El método de acuerdo con la reivindicación 1, que comprende, además:
verificar un primer certificado de aprobación de la primera plataforma nativa con una primera clave pública asociada con un fabricante de la primera plataforma de enclave nativa; y

verificar un segundo certificado de aprobación de la segunda plataforma de enclave nativa con una segunda clave pública asociada con el fabricante de la segunda plataforma de enclave nativa, en donde la primera clave pública y la segunda clave pública no son las mismas.

11. El método de acuerdo con la reivindicación 1, que comprende, además:
generar el primer informe de certificación al computar un valor *hash* con respecto a una primera porción de memoria en un contenedor seguro del primer enclave, en donde el contenido de la primera porción de memoria es independiente de la primera plataforma nativa; y

generar el segundo informe de certificación al computar un valor *hash* con respecto a una segunda porción de memoria en un contenedor seguro del segundo enclave, en donde el contenido de la segunda porción de memoria es independiente de la segunda plataforma nativa.

12. Un sistema que comprende:

memoria; y

uno o más procesadores acoplados a la memoria, los uno o más procesadores configurados para:

recibir un primer informe de certificación a partir de un primer enclave instanciado en una primera plataforma de enclave nativa;

extraer un primer valor de identidad de enclave asociado con un tipo de identidad de enclave a partir del primer informe de certificación;

recibir un segundo informe de certificación a partir de un segundo enclave instanciado en una segunda plataforma de enclave nativa, en donde la primera plataforma de enclave nativa y la

segunda plataforma de enclave nativa son diferentes;

extraer un segundo valor de identidad de enclave asociado con el tipo de identidad de enclave a partir del segundo informe de certificación;

comparar el primer valor de identidad de enclave con el segundo valor de identidad de enclave; y

realizar una operación de computación al completar parcialmente la operación de computación en el primer enclave y al completar parcialmente la operación de computación en el segundo enclave.

13. El sistema de acuerdo con la reivindicación 12, en donde el uno o más procesadores están configurados para realizar la operación de computación en serie con el primer y segundo enclave;

en donde el uno o más procesadores están adicionalmente configurados para:

codificar los datos de estado de enclave del primer enclave después de completar parcialmente la operación de computación en el primer enclave para producir los datos codificados, en donde los datos de estado se codifican para el tipo de identidad de enclave;

copiar los datos codificados desde el primer enclave al segundo enclave; y

decodificar los datos codificados en el segundo enclave.

14. El sistema de acuerdo con la reivindicación 12, en donde el uno o más procesadores están configurados para realizar la operación de computación se realiza simultáneamente con el primero y segundo enclave;

en donde el uno o más procesadores están adicionalmente configurados para:

copiar una primera porción de un conjunto de datos en el primer enclave; y

copiar una segunda porción de un conjunto de datos en el segundo enclave; y

en donde el uno o más procesadores están configurados para completar parcialmente la operación de computación en el primer enclave utilizando la primera porción y completar parcialmente la operación de computación en el segundo enclave utilizando la segunda porción.

15. El sistema de acuerdo con la reivindicación 12, en donde el uno o más procesadores están configurados para:

completar parcialmente la operación de computación en el primer enclave al causar que el primer enclave lea un contador monotónico asociado con el valor de identidad; y

completar parcialmente la operación de computación en el segundo enclave al causar que el segundo enclave lea el contador monotónico asociado con el valor de identidad.

16. El sistema de acuerdo con la reivindicación 12, en donde el uno o más procesadores están configurados para:

completar parcialmente la operación de computación en el primer enclave al causar que el primer enclave lea un tiempo confiable asociado con el valor de identidad; y

completar parcialmente la operación de computación en el segundo enclave al causar que el segundo enclave lea el tiempo confiable asociado con el valor de identidad.

17. El sistema de acuerdo con la reivindicación 12, en donde el uno o más procesadores están configurados adicionalmente para:

crear una firma para el primer informe de certificación al realizar al menos una primera operación de plataforma nativa; y

crear una firma para el segundo informe de certificación al realizar al menos una segunda operación de plataforma nativa.

18. El sistema de acuerdo con la reivindicación 12, en donde la primera plataforma de enclave nativa se adapta a una primera arquitectura de enclave y la segunda plataforma de enclave nativa se adapta a una segunda arquitectura de enclave; y

en donde el uno o más procesadores están adicionalmente configurados para:

generar el primer informe de certificación al realizar al menos una operación nativa de la primera arquitectura de enclave; y

generar el segundo informe de certificación al realizar al menos una operación nativa de la segunda arquitectura de enclave.

19. El sistema de acuerdo con la reivindicación 12, en donde la primera plataforma de enclave nativa y la segunda plataforma de enclave nativa son diferentes versiones de la misma arquitectura de enclave.

20. El sistema de acuerdo con la reivindicación 12, en donde el uno o más procesadores están configurados adicionalmente para:

verificar una primera firma del primer informe de certificación con una clave pública asociada con la primera plataforma de enclave nativa; y

verificar una segunda firma del segundo informe de certificación con una clave pública asociada con la segunda plataforma del enclave nativa, en donde la primera clave pública y la segunda clave pública son diferentes.

21. El sistema de acuerdo con la reivindicación 12, en donde uno o más procesadores están configurados adicionalmente para:

verificar un primer certificado de aprobación de la primera plataforma nativa con una primera clave pública asociada con un fabricante de la primera plataforma de enclave nativa; y

verificar un segundo certificado de aprobación de la segunda plataforma de enclave nativa con una segunda clave pública asociada con el fabricante de la segunda plataforma de enclave nativa, en donde la primera clave pública y la segunda clave pública no son las mismas.

22. El sistema de acuerdo con la reivindicación 12, en donde el uno o más procesadores están configurados adicionalmente para:

generar el primer informe de certificación al computar un valor *hash* con respecto a una primera porción de memoria en un contenedor seguro del primer enclave, en donde el contenido de la primera porción de memoria es independiente de la primera plataforma nativa; y

generar el segundo informe de certificación al computar un valor *hash* con respecto a una segunda porción de memoria en un contenedor seguro del segundo enclave, en donde el contenido de la segunda porción de memoria es independiente de la segunda plataforma nativa.

23. Un medio de almacenamiento legibles por computadora que tiene instrucciones almacenadas en el mismo para permitir a un sistema basado en procesador para determinar una equivalencia de enclave, las operaciones comprenden:

recibir un primer informe de certificación desde un primer enclave instanciado en una primera plataforma de enclave nativa;

extraer un primer valor de identidad de enclave asociado con un tipo de identidad de enclave a partir del primer informe de certificación;

recibir un segundo informe de certificación desde un segundo enclave instanciado en una segunda plataforma de enclave nativa, en donde la primera plataforma de enclave nativa y la segunda plataforma de enclave nativa son diferentes;

extraer un segundo valor de identidad de enclave asociado con el tipo de identidad de enclave a partir del segundo informe de certificación;

comparar el primer valor de identidad de enclave con el segundo valor de identidad de enclave; y

realizar una operación de computación al completar parcialmente la operación de computación en el primer enclave y al completar parcialmente la operación de computación en el segundo enclave.