

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° 699 de 25 de enero de 2021

Ref. Expediente N° NC2019/0007655

Señor(a)
LLC MICROSOFT TECHNOLOGY LICENSING

TÍTULO DE LA SOLICITUD: **“IDENTIDAD DE ENCLAVE MULTIPLATAFORMA”**
NÚMERO DE SOLICITUD INTERNACIONAL: PCT/US2018/014298
FECHA DE PRESENTACIÓN INTERNACIONAL: 19 de enero de 2018.
PRIORIDAD(ES): US, 15/414,421, 24 de enero de 2017.

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

1. Objeto de la invención

De acuerdo con lo establecido en el numeral 1.2.2.2 del Capítulo Primero del Título X de la Circular Única para efectos del examen de patentabilidad, cuando la solicitud contenga más de diez (10) reivindicaciones y no se haya pagado la tasa complementaria, sólo se estudiarán las cubiertas por la tasa pagada al momento de realizar el examen de patentabilidad consagrado en el artículo 45 de la Decisión 486. Por lo tanto, se estudiarán las reivindicaciones 1 a 15 del radicado N° NC2019/0007655 del 16 de julio de 2019.

El problema planteado en esta solicitud consiste en la necesidad de proporcionar un nivel adicional de seguridad y garantías de confidencialidad e integridad sobre los sistemas informáticos.

Para resolver este problema técnico, la solicitud en estudio proporciona sistemas y métodos para determinar la equivalencia de enclave de una identidad abstracta de enclave, donde un valor de identidad de enclave puede determinarse a partir de un tipo de identidad abstracta de enclave con respecto a un enclave instanciado. Puede utilizarse un valor de identidad abstracta para determinar la equivalencia de dos instancias de enclave que no son idénticas, como dos enclaves similares alojados en diferentes computadoras, dos enclaves alojados en diferentes plataformas de enclave nativas y dos enclaves instanciados a partir de diferentes versiones de las mismas imágenes binarias de enclave.

2. De la solicitud de patente

2.1. Título

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

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



Oficio N° 699 de 25 de enero de 2021

Ref. Expediente N° NC2019/0007655

reivindicaciones, por lo cual se sugiere el título siguiente: “SISTEMAS Y MÉTODO PARA DETERMINAR LA EQUIVALENCIA DE ENCLAVE DE UNA IDENTIDAD ABSTRACTA DE ENCLAVE”.

2.2. Reivindicaciones (Art. 30 Decisión 486)

- 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. Se sugiere aclarar cuáles son las características de las arquitecturas de enclave en cuestión.

3. 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 encontraron los siguientes documentos que anticipan el objeto de esta solicitud:

Ítem	Documento	Título	Fecha de Publicación
D1	US20150033012	“Secure processing environment measurement and attestation”	29 de enero de 2015
D2	US20150304736	“Technologies for hardening the security of digital information on client platforms”	22 de octubre 2015

El documento D1¹ divulga realizaciones de una invención para la medición y certificación de entornos de procesamiento seguros. En una realización, un procesador incluye una unidad de instrucción y una unidad de ejecución. La unidad de instrucción debe recibir una primera instrucción asociada con la construcción o reconstrucción de un enclave seguro. La unidad de ejecución es ejecutar la primera instrucción. La ejecución de la primera instrucción, cuando está asociada con la construcción, incluye el cálculo de una primera medición y una segunda medición del enclave seguro. La ejecución de la primera instrucción, cuando se asocia con la reconstrucción, incluye el cálculo de la segunda medición sin el cálculo de la primera medición (Resumen).

El documento D2² divulga tecnologías para fortalecer la seguridad de la información digital en un dispositivo cliente. En algunas realizaciones, el dispositivo cliente incluye un entorno de procesamiento seguro, como un enclave seguro, que puede usarse para proteger información digital en una plataforma cliente. Los entornos seguros también pueden proteger los activos que se pueden utilizar para acceder a la información digital. Usando el (los) entorno (s) de procesamiento seguro, las tecnologías descritas pueden proteger la información digital a medida que se proporciona, almacena, accede y / o procesa para su visualización en un dispositivo cliente, incluso si el dispositivo cliente puede estar infestado con malware o sujeto a ataque por otra entidad (Resumen)

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

4.1. Nivel Inventivo (Art. 18 Decisión 486)

¹<https://patents.google.com/patent/US20150033012A1/en?q=US2015033012>

²<https://patents.google.com/patent/US20150304736A1/en?q=US20150304736>

Oficio N° 699 de 25 de enero de 2021

Ref. Expediente N° NC2019/0007655

La reivindicación 1 consiste en: “Un método para determinar la equivalencia de enclave, que comprende (...)” (Radicado N° NC2019/0007655 del 16 de julio de 2019).

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

Características esenciales	D1	D2
Recibir un primer informe de certificación a partir de un primer enclave instanciado en una primera plataforma de enclave nativa.	En el recuadro (410), comienza la construcción inicial de un enclave seguro en el sistema (100) (...) (Párr. 0040). Se puede realizar una certificación del contenido del enclave utilizando el hash de compilación. La certificación puede proporcionarse a una entidad externa como parte de la ejecución de una instrucción EREPORT (Párr. 0048).	El informe del enclave se puede firmar con una firma digital utilizando un primer protocolo de firma digital, como el protocolo de firma Rivest Shamir Adleman (RSA), el protocolo del algoritmo de firma digital (DSM), la Identificación de privacidad mejorada de Intel (EPID), combinaciones de los mismos y similar (...) (Párr. 0060).
Extraer un primer valor de identidad de enclave asociado con un tipo de identidad de enclave a partir del primer informe de certificación.	(...) La entidad puede obtener este hash leyendo una certificación de la compilación inicial (del recuadro (436)) o calculándola (p. Ej., En función de las páginas que se agregarán durante la reconstrucción) (...) (Párr. 0050).	(...) Tras la verificación de la firma digital aplicada al informe de enclave, el módulo de cotización puede generar una cotización de enclave y firmar la cotización con una clave de firma de cotización utilizando un segundo protocolo de firma digital que es igual o diferente al primer protocolo de firma digital (...) (Párr. 0060).
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.	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") (...) (Párr. 0054).	No se menciona.
Extraer un segundo valor de identidad de enclave asociado con el tipo de identidad de enclave a partir del segundo informe de certificación.	(...) En la casilla (446), el MAC de construcción final se obtiene, por ejemplo, al ser proporcionado por la entidad de reconstrucción (si se proporciona a la entidad en la casilla (434)) o al ser recuperado del almacenamiento (si se almacena en la casilla (434)) (Párr. 0050).	No se menciona.
Determinar que el primer valor de identidad de enclave es el mismo que el segundo valor de identidad de enclave.	Se puede realizar una certificación del contenido del enclave utilizando el hash esperado. La certificación puede proporcionarse a una entidad externa como parte de la ejecución de una instrucción EREPORT. Para una entidad externa, la certificación resultante de la casilla (468) es indistinguible de la certificación resultante de la casilla (436) (...) (Párr. 0059). (...) el MAC de reconstrucción final calculado en el cuadro (456) se compara con el MAC de	No se menciona.

Oficio N° 699 de 25 de enero de 2021

Ref. Expediente N° NC2019/0007655

	construcción final obtenido en el cuadro (446) (...) (Párr. 0056).	
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.	No se menciona	El servidor (102) puede condicionar la distribución de una licencia a la autenticación exitosa del cliente (101). A este respecto, el CEREM, cuando se ejecuta, puede hacer que el cliente (101) transmita las credenciales de autenticación al servidor (102). (...) El servidor (102) puede analizar las credenciales de autenticación recibidas del cliente (101) e intentar autenticar al cliente (101), por ejemplo, contra la política de acceso recibida del distribuidor (103), una lista preestablecida de plataformas confiables (por ejemplo, una lista blanca), combinaciones de las mismas y similar (Párr. 0044).

El documento D1 se considera el estado de la técnica más cercano a la invención definida en la reivindicación 1 porque divulga un método (400) que incluye la construcción de un enclave seguro utilizando las instrucciones ECREATE, EADD, EEXTEND y EINIT; sin embargo, las realizaciones de la presente invención no se limitan a estas instrucciones nombradas específicamente. En el método (400), estas instrucciones pueden ser emitidas, invocadas o utilizadas de otro modo por software de sistema privilegiado, como un sistema operativo o un monitor de máquina virtual. El método (400) también incluye el uso de una instrucción EREPORT, que puede ser emitida, invocada o utilizada de otro modo por software de aplicación sin privilegios que se ejecuta dentro del enclave (...) (Párr. 0039).

La diferencia entre la invención definida en la reivindicación 1 y el método divulgado de D1 consiste en que la invención incluye la etapa de 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

El efecto que se logra al incluir la etapa de 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 es proporcionar medición y certificación del entorno de procesamiento seguro.

Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así: ¿Cómo modificar el método conocido en D1 con el fin de proporcionar medición y certificación del entorno de procesamiento seguro?

Sin embargo, el incluir la etapa de 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 para proporcionar medición y certificación del entorno de procesamiento seguro, ya está divulgado en el documento D2 que se refiere a que el servidor (102) puede condicionar la distribución de una licencia a la autenticación exitosa del cliente (101). A este respecto, el CEREM, cuando se ejecuta, puede hacer que el cliente (101) transmita las credenciales de autenticación al servidor (102). Adicionalmente, el servidor (102) puede analizar las credenciales de autenticación recibidas del cliente (101) e intentar autenticar al cliente (101), por ejemplo, contra la política de acceso recibida del distribuidor (103), una lista

Oficio N° 699 de 25 de enero de 2021

Ref. Expediente N° NC2019/0007655

preestablecida de plataformas confiables (por ejemplo, una lista blanca), combinaciones de las mismas y similar (Párr. 0044).

En consecuencia, la persona normalmente versada en la materia estaría motivada a incluir la etapa de 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 del documento D2 en el método de D1, para así llegar al objeto de la reivindicación 1. Por lo cual se considera obvia.

Asimismo, el documento D2 divulga las características de las reivindicaciones dependientes así:

- Reivindicación 2: Una vez que se valida el informe de enclave firmado, las instrucciones del módulo de cotización pueden hacer que el cliente (101) genere una cotización de enclave segura que puede incluir diversa información como se discutió anteriormente. Las instrucciones del módulo de cotización pueden hacer además que el cliente (101) firme la cotización del enclave utilizando una clave de firma tal como la clave privada EPID del cliente, que puede haber sido previamente aprovisionada en el cliente (...) (Párr. 0109). (...) Si el cliente (101) cifró MSG3 con cifrado de clave pública y una clave pública de servidor (por ejemplo, Spub), las instrucciones de SPM pueden hacer que el servidor (102) descifre MSG3 usando un protocolo de descifrado y una clave privada de servidor correspondiente (por ejemplo, Spriv) (...) (Párr. 0110).
- Reivindicación 3: (...) Cuando MSG4 está firmado con la clave privada del servidor (102) (por ejemplo, Spriv), las instrucciones CPM cuando se ejecutan pueden hacer que el cliente (101) verifique la autenticidad de la firma usando una clave pública correspondiente (por ejemplo, Spub). Alternativa o adicionalmente, si MSG4 está cifrado con Cpub, las instrucciones CPM cuando se ejecutan pueden hacer que el cliente (101) descifre MSG4 dentro del enclave de memoria (304) usando una clave privada correspondiente (por ejemplo, Cpriv) (...) (Párr. 0115). (...) Si el cliente (101) cifró MSG3 con cifrado de clave pública y una clave pública de servidor (por ejemplo, Spub), las instrucciones de SPM pueden hacer que el servidor (102) descifre MSG3 usando un protocolo de descifrado y una clave privada de servidor correspondiente (por ejemplo, Spriv) (...) (Párr. 0110).
- Reivindicación 4: (...) Un TEE en un cliente puede usarse para proporcionar una fuente confiable de tiempo, por ejemplo, cuando el cliente puede no tener acceso a una fuente confiable de tiempo desde una entidad remota confiable. En otras palabras, un TEE puede usarse como una fuente de tiempo local confiable, que puede ser útil para el registro seguro, video seguro y otros procesos consistentes con la presente divulgación (Párr. 0063). La política de registro de actividades puede requerir además el registro de la hora de los eventos detectados asociados con la información digital. En tales casos, se puede usar una fuente confiable de tiempo para asegurar el registro preciso de la sincronización de los eventos detectados. En los casos en los que el servidor (102) es una plataforma confiable, puede servir como una fuente confiable de tiempo para el cliente (101). Por ejemplo, el servidor (102) puede comunicar la hora al cliente (101) a través de un canal de comunicaciones seguro (...) (Párr. 0174).
- Reivindicación 5: En respuesta al mensaje de respuesta, el CPM (306) puede hacer que el cliente (101) genere un par de claves asimétricas, tal como se puede utilizar en el cifrado de claves públicas Rivest, Shamir, Adleman (RSA) y / o un protocolo de firma digital. Más específicamente, CPM (306) puede configurarse para hacer que el cliente (101) genere un par de claves asimétricas que incluye una clave pública del cliente



Oficio N° 699 de 25 de enero de 2021

Ref. Expediente N° NC2019/0007655

- (Cpub) y una clave privada del cliente (Cpriv), las cuales pueden almacenarse y/o sellarse en el enclave (304) de memoria (Párr. 0087). El informe del enclave se puede firmar con una firma digital utilizando un primer protocolo de firma digital, como el protocolo de firma Rivest Shamir Adleman (RSA), el protocolo del algoritmo de firma digital (DSM), la Identificación de privacidad mejorada de Intel (EPID), combinaciones de los mismos y similar (...) (Párr. 0060).
- Reivindicación 7: (...) El informe de enclave enviado al módulo de cotización (307) puede estar firmado con una firma digital y / o puede incluir otra información que el módulo de cotización (307) puede usar para verificar la autenticidad del informe de enclave. Por ejemplo, CPM (306) puede hacer que el cliente (101) firme el informe de enclave utilizando un protocolo de firma digital adecuado y la clave de enclave del enclave (304) de memoria antes de transmitir el informe del enclave al módulo de cotización (307) (Párr. 0089). En respuesta al mensaje de cotización, SPM (312) puede hacer que el servidor (102) verifique la autenticidad de la cotización de enclave incluida en un mensaje de enclave recibido del cliente (101). La verificación de la cotización de enclave puede realizarse de cualquier manera. Por ejemplo, SPM (312) puede hacer que el servidor (102) transfiera el mensaje de cotización al servicio de verificación (313), que puede ser local o remoto al servidor (102), como se ilustra en la FIG. 3 mediante el hash de la casilla (313). El servicio de verificación (313) puede verificar la cotización del enclave utilizando un protocolo de verificación adecuado (...) (Párr. 0094).
 - Reivindicación 9: Las instrucciones CPM pueden entonces hacer que el cliente (101) firme el informe de enclave (que incluye un hash de los datos del usuario y la información de identificación opcional), con una clave de firma. En algunas realizaciones, las instrucciones CPM pueden hacer que el cliente (101) firme el informe de enclave utilizando una clave de enclave (Ekey), que puede haber sido aprovisionada previamente dentro del enclave de memoria (304), por ejemplo, en el momento en que se estableció el enclave de memoria (304) en el cliente (101) (...) (Párr. 0107). (...) Las instrucciones de SPM pueden hacer que el servidor (102) almacene la medición del enclave (304), el nombre de usuario del cliente (si se incluye), la ID de la máquina del cliente (si se incluye), la información específica de la aplicación (si se incluye), el hash de los datos del usuario y el público del cliente. clave (Cpub) en la base de datos opcional (314) u otra estructura de datos. Las instrucciones de SPM también pueden hacer que el servidor (102) genere un ID de lista blanca para el cliente (101) (...) (Párr. 0113).

Las reivindicaciones dependientes 2 a 5, 7 y 9 no mencionan alguna característica que, junto con las características de la reivindicación independiente, aporte nivel inventivo al método de la reivindicación 1, por lo cual se considera que no tienen nivel inventivo.

La reivindicación 10 consiste en: “Un sistema que comprende (...)” (Radicado N° NC2019/0007655 del 16 de julio de 2019).

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

Características esenciales	D1	D2
----------------------------	----	----

Oficio N° 699 de 25 de enero de 2021

Ref. Expediente N° NC2019/0007655

Al menos un procesador.	(...) Todo o parte del método (400) puede estar incorporado en instrucciones de software o firmware que se almacenan en un medio legible por el procesador (110), que cuando es ejecutado por el procesador (110), hace que el procesador (110) ejecute una realización de la presente invención (...) (Párr. 0061).	(...) "Circuito", como se usa en cualquier realización en este documento, puede comprender, por ejemplo, individualmente o en cualquier combinación, circuitos cableados, circuitos programables tales como procesadores de computadora que comprenden uno o más núcleos de procesamiento de instrucciones individuales (...) (Párr. 0031).
Una memoria que almacena en la misma las instrucciones que, cuando se ejecutan por el sistema, producen al menos las etapas de.	(...) (Párr. 0061).	(...) El software puede incorporarse como un paquete de software, código, instrucciones, conjuntos de instrucciones y / o datos registrados en medios de almacenamiento no transitorios legibles por ordenador (...) (Párr. 0031).
Recibir un primer informe de certificación a partir de un primer enclave instanciado en una primera plataforma de enclave nativa.	En el recuadro (410), comienza la construcción inicial de un enclave seguro en el sistema (100) (...) (Párr. 0040). Se puede realizar una certificación del contenido del enclave utilizando el hash de compilación. La certificación puede proporcionarse a una entidad externa como parte de la ejecución de una instrucción EREPORT (Párr. 0048).	El informe del enclave se puede firmar con una firma digital utilizando un primer protocolo de firma digital, como el protocolo de firma Rivest Shamir Adleman (RSA), el protocolo del algoritmo de firma digital (DSM), la Identificación de privacidad mejorada de Intel (EPID), combinaciones de los mismos y similar (...) (Párr. 0060).
Extraer un primer valor de identidad de enclave asociado con un tipo de identidad de enclave a partir del primer informe de certificación.	(...) La entidad puede obtener este hash leyendo una certificación de la compilación inicial (del recuadro (436)) o calculándola (p. Ej., En función de las páginas que se agregarán durante la reconstrucción) (...) (Párr. 0050).	(...) Tras la verificación de la firma digital aplicada al informe de enclave, el módulo de cotización puede generar una cotización de enclave y firmar la cotización con una clave de firma de cotización utilizando un segundo protocolo de firma digital que es igual o diferente al primer protocolo de firma digital (...) (Párr. 0060).
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.	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") (...) (Párr. 0054).	No se menciona.
Extraer un segundo valor de identidad de enclave asociado con el tipo de identidad de enclave a partir del segundo informe de certificación.	(...) En la casilla (446), el MAC de construcción final se obtiene, por ejemplo, al ser proporcionado por la entidad de reconstrucción (si se proporciona a la entidad en la casilla (434)) o al ser recuperado del almacenamiento (si se almacena en la casilla (434)) (Párr. 0050).	No se menciona.
Comparar el primer valor de identidad de enclave con el segundo valor de identidad de enclave.	Se puede realizar una certificación del contenido del enclave utilizando el hash esperado. La certificación puede proporcionarse a una	No se menciona.

Oficio N° 699 de 25 de enero de 2021

Ref. Expediente N° NC2019/0007655

	entidad externa como parte de la ejecución de una instrucción EREPORT. Para una entidad externa, la certificación resultante de la casilla (468) es indistinguible de la certificación resultante de la casilla (436) (...) (Párr. 0059). (...) el MAC de reconstrucción final calculado en el cuadro (456) se compara con el MAC de construcción final obtenido en el cuadro (446) (...) (Párr. 0056).	
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.	No se menciona	El servidor (102) puede condicionar la distribución de una licencia a la autenticación exitosa del cliente (101). A este respecto, el CEREM, cuando se ejecuta, puede hacer que el cliente (101) transmita las credenciales de autenticación al servidor (102). (...) El servidor (102) puede analizar las credenciales de autenticación recibidas del cliente (101) e intentar autenticar al cliente (101), por ejemplo, contra la política de acceso recibida del distribuidor (103), una lista preestablecida de plataformas confiables (por ejemplo, una lista blanca), combinaciones de las mismas y similar (Párr. 0044).

El documento D1 se considera el estado de la técnica más cercano a la invención definida en la reivindicación 10 porque divulga un sistema de procesamiento de información para la medición y certificación del entorno de procesamiento seguro según una realización de la presente invención. El sistema (100) puede representar cualquier tipo de sistema de procesamiento de información, como un servidor, una computadora de escritorio, una computadora portátil, un decodificador, un dispositivo de mano como una tableta o un teléfono inteligente, o un sistema de control integrado (...) (Párr. 0015).

La diferencia entre la invención definida en la reivindicación 10 y el sistema divulgado de D1 consiste en que la invención incluye 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.

El efecto que se logra al incluir la realización de 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 es proporcionar medición y certificación del entorno de procesamiento seguro.

Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así: ¿Cómo modificar el sistema conocido en D1 con el fin de proporcionar medición y certificación del entorno de procesamiento seguro?

Sin embargo, el incluir la realización de 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 es proporcionar medición y certificación del entorno de procesamiento seguro, ya está divulgado en el documento D2 que se refiere a que el servidor (102) puede condicionar la distribución de

Oficio N° 699 de 25 de enero de 2021

Ref. Expediente N° NC2019/0007655

una licencia a la autenticación exitosa del cliente (101). A este respecto, el CEREM, cuando se ejecuta, puede hacer que el cliente (101) transmita las credenciales de autenticación al servidor (102). Adicionalmente, el servidor (102) puede analizar las credenciales de autenticación recibidas del cliente (101) e intentar autenticar al cliente (101), por ejemplo, contra la política de acceso recibida del distribuidor (103), una lista preestablecida de plataformas confiables (por ejemplo, una lista blanca), combinaciones de las mismas y similar (Párr. 0044).

En consecuencia, la persona normalmente versada en la materia estaría motivada a incluir la realización de 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 del documento D2 en el sistema de D1, para así llegar al objeto de la reivindicación 10. Por lo cual se considera obvia.

Asimismo, el documento D2 divulga las características de las reivindicaciones dependientes así:

- Reivindicación 11: Una vez que se valida el informe de enclave firmado, las instrucciones del módulo de cotización pueden hacer que el cliente (101) genere una cotización de enclave segura que puede incluir diversa información como se discutió anteriormente. Las instrucciones del módulo de cotización pueden hacer además que el cliente (101) firme la cotización del enclave utilizando una clave de firma tal como la clave privada EPID del cliente, que puede haber sido previamente aprovisionada en el cliente (...) (Párr. 0109). (...) Si el cliente (101) cifró MSG3 con cifrado de clave pública y una clave pública de servidor (por ejemplo, Spub), las instrucciones de SPM pueden hacer que el servidor (102) descifre MSG3 usando un protocolo de descifrado y una clave privada de servidor correspondiente (por ejemplo, Spriv) (...) (Párr. 0110).
- Reivindicación 12: (...) Cuando MSG4 está firmado con la clave privada del servidor (102) (por ejemplo, Spriv), las instrucciones CPM cuando se ejecutan pueden hacer que el cliente (101) verifique la autenticidad de la firma usando una clave pública correspondiente (por ejemplo, Spub). Alternativa o adicionalmente, si MSG4 está cifrado con Cpub, las instrucciones CPM cuando se ejecutan pueden hacer que el cliente (101) descifre MSG4 dentro del enclave de memoria (304) usando una clave privada correspondiente (por ejemplo, Cpriv) (...) (Párr. 0115). (...) Si el cliente (101) cifró MSG3 con cifrado de clave pública y una clave pública de servidor (por ejemplo, Spub), las instrucciones de SPM pueden hacer que el servidor (102) descifre MSG3 usando un protocolo de descifrado y una clave privada de servidor correspondiente (por ejemplo, Spriv) (...) (Párr. 0110).
- Reivindicación 14: Las instrucciones CPM pueden entonces hacer que el cliente (101) firme el informe de enclave (que incluye un hash de los datos del usuario y la información de identificación opcional), con una clave de firma. En algunas realizaciones, las instrucciones CPM pueden hacer que el cliente (101) firme el informe de enclave utilizando una clave de enclave (Ekey), que puede haber sido aprovisionada previamente dentro del enclave de memoria (304), por ejemplo, en el momento en que se estableció el enclave de memoria (304) en el cliente (101) (...) (Párr. 0107). (...) Las instrucciones de SPM pueden hacer que el servidor (102) almacene la medición del enclave (304), el nombre de usuario del cliente (si se incluye), la ID de la máquina del cliente (si se incluye), la información específica de la aplicación (si se incluye), el hash de los datos del usuario y el público del cliente. clave (Cpub) en la base de datos opcional (314) u otra estructura de datos. Las instrucciones de SPM también pueden hacer que el servidor (102) genere un ID de lista blanca para



Oficio N° 699 de 25 de enero de 2021

Ref. Expediente N° NC2019/0007655

el cliente (101) (...) (Párr. 0113).

Las reivindicaciones dependientes 11, 12 y 14 no mencionan alguna característica que, junto con las características de la reivindicación independiente, aporte nivel inventivo al sistema de la reivindicación 10, por lo cual se considera que no tienen nivel inventivo.

La reivindicación 15 consiste en: “Un sistema que comprende: (...)” (Radicado N° NC2019/0007655 del 16 de julio de 2019).

Tabla 3. Comparación de las características técnicas esenciales, con las del estado de la técnica:

Características esenciales	D1	D2
Medios para recibir un primer informe de certificación desde un primer enclave instanciado en una primera plataforma de enclave nativa.	En el recuadro (410), comienza la construcción inicial de un enclave seguro en el sistema (100) (...) (Párr. 0040). Se puede realizar una certificación del contenido del enclave utilizando el hash de compilación. La certificación puede proporcionarse a una entidad externa como parte de la ejecución de una instrucción EREPORT (Párr. 0048).	El informe del enclave se puede firmar con una firma digital utilizando un primer protocolo de firma digital, como el protocolo de firma Rivest Shamir Adleman (RSA), el protocolo del algoritmo de firma digital (DSM), la Identificación de privacidad mejorada de Intel (EPID), combinaciones de los mismos y similar (...) (Párr. 0060).
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.	(...) La entidad puede obtener este hash leyendo una certificación de la compilación inicial (del recuadro (436)) o calculándola (p. Ej., En función de las páginas que se agregarán durante la reconstrucción) (...) (Párr. 0050).	(...) Tras la verificación de la firma digital aplicada al informe de enclave, el módulo de cotización puede generar una cotización de enclave y firmar la cotización con una clave de firma de cotización utilizando un segundo protocolo de firma digital que es igual o diferente al primer protocolo de firma digital (...) (Párr. 0060).
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.	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") (...) (Párr. 0054).	No se menciona.
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.	(...) En la casilla (446), el MAC de construcción final se obtiene, por ejemplo, al ser proporcionado por la entidad de reconstrucción (si se proporciona a la entidad en la casilla (434)) o al ser recuperado del almacenamiento (si se almacena en la casilla (434)) (Párr. 0050).	No se menciona.
Medios para comparar el primer valor de identidad de enclave con el segundo valor de identidad de enclave.	Se puede realizar una certificación del contenido del enclave utilizando el hash esperado. La certificación puede proporcionarse a una entidad externa como parte de la ejecución de una instrucción EREPORT. Para una entidad externa, la certificación resultante	No se menciona.

Oficio N° 699 de 25 de enero de 2021

Ref. Expediente N° NC2019/0007655

	de la casilla (468) es indistinguible de la certificación resultante de la casilla (436) (...) (Párr. 0059). (...) el MAC de reconstrucción final calculado en el cuadro (456) se compara con el MAC de construcción final obtenido en el cuadro (446) (...) (Párr. 0056).	
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.	No se menciona	El servidor (102) puede condicionar la distribución de una licencia a la autenticación exitosa del cliente (101). A este respecto, el CEREM, cuando se ejecuta, puede hacer que el cliente (101) transmita las credenciales de autenticación al servidor (102). (...) El servidor (102) puede analizar las credenciales de autenticación recibidas del cliente (101) e intentar autenticar al cliente (101), por ejemplo, contra la política de acceso recibida del distribuidor (103), una lista preestablecida de plataformas confiables (por ejemplo, una lista blanca), combinaciones de las mismas y similar (Párr. 0044).

El documento D1 se considera el estado de la técnica más cercano a la invención definida en la reivindicación 15 porque divulga un sistema de procesamiento de información para la medición y certificación del entorno de procesamiento seguro según una realización de la presente invención. El sistema (100) puede representar cualquier tipo de sistema de procesamiento de información, como un servidor, una computadora de escritorio, una computadora portátil, un decodificador, un dispositivo de mano como una tableta o un teléfono inteligente, o un sistema de control integrado (...) (Párr. 0015).

La diferencia entre la invención definida en la reivindicación 15 y el sistema divulgado de D1 consiste en que la invención incluye 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.

El efecto que se logra al incluir la realización de 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 es proporcionar medición y certificación del entorno de procesamiento seguro.

Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así: ¿Cómo modificar el sistema conocido en D1 con el fin de proporcionar medición y certificación del entorno de procesamiento seguro?

Sin embargo, el incluir la realización de 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 es proporcionar medición y certificación del entorno de procesamiento seguro, ya está divulgado en el documento D2 que se refiere a que el servidor (102) puede condicionar la distribución de una licencia a la autenticación exitosa del cliente (101). A este respecto, el CEREM, cuando se ejecuta, puede hacer que el cliente (101) transmita las credenciales de autenticación al servidor (102). Adicionalmente, el servidor (102) puede analizar las

Oficio N° 699 de 25 de enero de 2021

Ref. Expediente N° NC2019/0007655

credenciales de autenticación recibidas del cliente (101) e intentar autenticar al cliente (101), por ejemplo, contra la política de acceso recibida del distribuidor (103), una lista preestablecida de plataformas confiables (por ejemplo, una lista blanca), combinaciones de las mismas y similar (Párr. 0044).

En consecuencia, la persona normalmente versada en la materia estaría motivada a incluir la realización de 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 del documento D2 en el sistema de D1, para así llegar al objeto de la reivindicación 15. Por lo cual se considera obvia.

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

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

Ítem	Documento	Reivindicaciones afectadas	Requisito que afecta
D1	US20150033012	1, 10 y 15	Nivel inventivo
D2	US20150304736	1 a 5, 7, 9 a 12, 14 y 15	Nivel inventivo

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

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

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



Edna Marcela Ramirez Orozco
DIRECTORA DE NUEVAS CREACIONES



Oficio N° 699 de 25 de enero de 2021

Ref. Expediente N° NC2019/0007655

INFORME DE BÚSQUEDA
EXAMEN DE PATENTABILIDAD

Solicitud No.		Examen de patentabilidad							
NC2019/0007655		1°	X	2°		3°		Revoca	
Solicitud Internacional No.		Fecha solicitud internacional: (DD/MM/AÑO)							
PCT/US2018/014298		19 de enero de 2018							
Fecha de determinación estado de la técnica (DD/MM/AÑO)				Prioridad		Presentación			
24/01/2017				X					
Solicitante									
LLC MICROSOFT TECHNOLOGY LICENSING									
Reivindicaciones que no son objeto de búsqueda por:									
Art. 14	-	Art. 15	-	Art. 20	-	Art. 25 (Falta de unidad de invención)		-	
CRITERIOS DE BÚSQUEDA									
Reivindicaciones objeto de búsqueda				1 a 15					
Palabras clave utilizadas				Enclave, Identity, Attestation, Report, Equivalence, Sealing, Secure, Encryption, Hash, Public Key, Native Platform, Certificate.					
Clasificaciones utilizadas para la búsqueda				CIP:	G06F 21/57				
DOCUMENTOS CONSIDERADOS RELEVANTES (Documentos patente, Literatura no patente (LNP): Artículos, catálogos, etc.)									
Informes de búsqueda / Bases de datos consultadas	N° de solicitud de patente / N° de patente / Autor LNP ⁽¹⁾	Fecha de Publicación /Presentación (DD/MM/AAAA)	Reivindicaciones /Secuencias afectadas	Citas relevantes del estado de la técnica			Categoría del documento citado ⁽²⁾		
SIPI	00065033	31/07/2003	-	-			A		
USPTO	US20150033012	29/01/2015	1, 10 y 15	1 Párr. 0040, Párr. 0048, Párr. 0050, Párr. 0054, Párr. 0059, Párr.0056. 10 Párr. 0061, Párr. 0040, Párr. 0048, Párr. 0050, Párr. 0054, Párr. 0059, Párr.0056. 15 Párr. 0040, Párr. 0048, Párr. 0050, Párr. 0054, Párr. 0059, Párr.0056.			Y		
	US20150304736	22/10/2015	1 a 5, 7, 9 a 12, 14 y 15	1 Párr. 0060, Párr. 0044. 2 Párr. 0109, Párr. 0110. 3 Párr. 0115, Párr. 0110. 4 Párr. 0063, Párr. 0174. 5 Párr. 0087, Párr. 0060. 7 Párr. 0089, Párr. 0094. 9 Párr. 0107, Párr. 0113. 10 Párr. 0031, Párr. 0060, Párr. 0044. 11 Párr. 109, Párr. 0110. 12 Párr. 0115, Párr. 0110.			Y		

Oficio N° 699 de 25 de enero de 2021

Ref. Expediente N° NC2019/0007655

				14 Párr. 0107, Párr. 0113. 15 Párr. 0060, Párr. 0044.	
	US2017002456	05/01/2017	-	-	A
	US2015033012	29/01/2015	-	-	A
	US2015304736	22/10/2015	-	-	A
Patbase	US2012163589	28/06/2012	-	-	A
Epoquenet	US2010281273	04/11/2010	-	-	A
(1) Cita completa literatura no patente (LNP)					
Apellido, A. A. (Fecha). Título del artículo. Nombre de la revista. Volumen(Número), pp-pp.					
O					
Apellido, A. A. (Fecha). Título del artículo. Nombre de la revista. Recuperado de http://xxxxxxx .					
(2) Categorías de documentos citados					
“A” Documento que define el estado general de la técnica no considerado como particularmente relevante. “E” Solicitud de patente o patente anterior pero publicada en la fecha de presentación internacional o en fecha posterior. “L” Documento citado para llamar la atención sobre por ejemplo, dudas acerca de una reivindicación de prioridad o para determinar la fecha de publicación de otra cita, siempre van acompañados de una explicación, por la cual se citan. “O” Documento del tipo actas de conferencia, este tipo de documentos siempre estará acompañado por otra letra que indique la pertinencia del documento, por ejemplo, O,X, O,Y o bien O,A. “P” Documento publicado antes de la fecha de presentación internacional pero con posterioridad a la fecha de prioridad reivindicada. “T” Documento publicado en fecha posterior a la de presentación o la de prioridad de la solicitud internacional y no entra en conflicto con dicha solicitud, pero puede ser útil para la mejor comprensión del principio o teoría en que se basa la invención, o para demostrar que el razonamiento o los hechos en los que se basa dicha invención son incorrectos. “X” Documento particularmente relevante; la invención reivindicada no puede considerarse nueva o que implique una actividad inventiva por referencia al documento aisladamente considerado. “Y” Documento particularmente relevante; la invención reivindicada no puede considerarse que implique una actividad inventiva cuando el documento se asocia a otro u otros documentos de la misma naturaleza, cuya combinación resulta evidente para un experto en la materia.					
Fecha del reporte de búsqueda: (10/11/2020)					
Examinador: CARLOS EDUARDO GUEVARA NICHÓY					