

Señores

Superintendencia de Industria y Comercio

Dirección de Nuevas Creaciones

E. S. D.

Ref: Expediente No. NC2019/0007656.

Solicitud de registro de Patente de Invención denominada “MÉTODO Y SISTEMA DE SELLADO DE DATOS CON UN ENCLAVE DE SELLADO”.

Fase nacional de la solicitud PCT/US2017/067455.

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. **9787** del 24 de junio de 2021.

1. Respecto al título de la solicitud

En el numeral 2.1 del oficio No. **9787**, 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° NC2019/0007656 el 16 de julio de 2019, tituló la invención como: ‘SELLADO DE DATOS CON UN ENCLAVE DE SELLADO’. 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 Y SISTEMA DE SELLADO DE DATOS CON UN ENCLAVE DE SELLADO’.

Con el objetivo de superar esta objeción, es deseo del solicitante modificar el título de la solicitud al siguiente de acuerdo con la sugerencia del examinador:

“MÉTODO Y SISTEMA DE SELLADO DE DATOS CON UN 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. **9787**, se presentan las siguientes objeciones a la claridad de las reivindicaciones:

- *Se solicita corregir los errores de redacción de la siguiente frase: “restringir el acceso de los datos de enclave enclaves con identidades autenticadas se permite de acuerdo con la lista permitida” (reivs. 1 y 6).*
- *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 modificado donde se resuelven dichas objeciones.

A continuación, se explicará cómo este nuevo capítulo reivindicatorio busca superar cada una de las objeciones de claridad expuestas previamente:

- Sobre la frase objetada de las reivindicaciones 1 y 6, se indica que fue modificada de la siguiente forma para corregir los errores de redacción: “restringir el acceso de los datos de enclave a enclaves con identidades autenticadas que se permite de acuerdo con la lista permitida” (se subrayan las modificaciones).

- Respecto a la sugerencia del examinador de incluir los números de referencia a los dibujos, se indica que dichos números de referencia fueron incluidos.

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 novedad y de nivel inventivo frente a las enseñanzas de los documentos **US 2015/347768 (D1)**, **US 2015/304736 (D2)** y **US 2013/198853 (D3)**.

3.1. Novedad y nivel inventivo

Aunque el Examinador haya citado los documentos D1, D2 y D3 para objetar la novedad y la altura inventiva de la presente invención, es posible afirmar que éstos no enseñan las características esenciales de la invención que se reclama en el nuevo capítulo reivindicatorio que ahora se presenta.

Con el fin de superar las objeciones presentadas respecto a la novedad y nivel inventivo de las reivindicaciones, **es deseo del solicitante presentar un nuevo capítulo reivindicatorio compuesto por 20 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 se añadió una nueva reivindicación 7 con características nuevas e inventivas, y que las anteriores reivindicaciones 1, 6 y 11, correspondientes a las reivindicaciones enmendadas 1, 11 y 17, se modificaron con el objetivo de que sea aún más clara su novedad y nivel inventivo donde ahora las reivindicaciones independientes incluyen las siguientes características que no son divulgadas ni sugeridas por los documentos D1, D2 o D3:

- Las reivindicaciones enmendadas 1 y 11 incluyen lo siguiente:
 - *“en donde el almacenado de manera segura incluye cifrar los datos de enclave con una clave asociada con el enclave de sellado, por parte*

del enclave de sellado, antes de recibir una petición por los datos de enclave de parte de un enclave de destino para crear datos de enclave sellados”; y

- *“en donde la restricción incluye determinar si enviar los datos de enclave desde el enclave sellado al enclave de destino, el cual es diferente del enclave de sellado, con base al menos en parte en si el enclave de destino está incluido en la lista de una o más identidades de enclave permitidas para desellar los datos de enclave”;*
- La nueva reivindicación 7 y la reivindicación enmendada 17 incluyen lo siguiente:
 - *“dicho envío comprende causar que el enclave de sellado determine si enviar los datos de enclave hacia el enclave de destino que es diferente del enclave de sellado con base al menos en parte en si el enclave de destino está incluido en la lista de una o más identidades de enclave permitidas para desellar los datos de enclave, en donde la lista permitida es una lista de tipos de identidad abstracta que corresponden a respectivos niveles de jerarquía de una jerarquía de identidad”; y*
 - *“enviar un reporte de afirmación de origen del enclave de origen hacia el enclave de sellado, en donde el reporte de afirmación de origen incluye al menos un valor de identidad del enclave de origen que corresponde a un tipo de identidad abstracta en la lista permitida”.*

El examinador se basa en los párrafos [0068] del documento D1, y en el párrafo [0098] del documento D2, para demostrar supuestamente la anticipada divulgación de la característica de *"Restringir el acceso de los datos de enclave a enclaves con identidades autenticadas que se permite de acuerdo con la lista permitida"*. Sin embargo, tras la detenida inspección, el solicitante afirma que nada en la combinación de los documentos D1, D2 y D3 enseña o sugiere la característica antes mencionada de las reivindicaciones independientes 1 y 11 enmendadas.

El documento D1 describe una técnica para la inspección confiable basada en políticas del contenido con derechos gestionados (ver título del documento D1). El documento D1 explica que una vez que se instancian los enclaves, los enclaves pueden autenticarse entre sí a través de una certificación, y se evitan los intentos de acceso a la memoria de los enclaves desde software no autorizado (ver documento

D1, párrafos [0038] y [0039]). La atestación puede usarse para permitir que *“una parte remota verifique que las medidas del enclave y los ajustes de la plataforma estén configurados como se esperaba...”* (D1, párrafo [0039]). Por ejemplo, *“SGX utiliza dos credenciales relacionadas para la certificación: informes y cotizaciones”* (D1, párrafo [0039]). De acuerdo con la técnica anterior, un primer enclave seguro puede recibir contenido e inspeccionar una política que corresponda al contenido. *“La política puede referirse a qué motores de inspección, si los hay, pueden tener acceso al contenido recibido por el primer enclave seguro”* (D1, párrafo [0111]). Por ejemplo, la política puede incluir una lista blanca que enumere un motor de inspección autorizado incluido en un segundo enclave seguro, y una identificación del segundo enclave seguro “puede compararse con la lista blanca para determinar si [una] aplicación del segundo nodo seguro debe inspeccionar los contenidos” (D1, párrafo [0113], énfasis añadido). Si es así, *“el primer enclave seguro autentica el segundo enclave seguro ‘en respuesta a’ inspeccionar la política”* (D1, párrafo [0113]). Cabe señalar que el documento D1 no sugiere de ninguna manera que la identificación del segundo enclave seguro se compare con la lista blanca para determinar si el contenido se enviará desde el primer enclave seguro al segundo enclave seguro. Más bien, el documento D1 establece específicamente que la identificación del segundo enclave seguro *“puede compararse con la lista blanca para determinar si la aplicación del segundo nodo seguro debe inspeccionar el contenido”*.

El documento D1 explica que, si el segundo enclave seguro se autentica con éxito, *“el primer nodo seguro [comunica] contenido cifrado al segundo enclave seguro ...”* (D1, párrafo [0114]). El segundo enclave seguro luego descifra *“el contenido cifrado para producir contenido descifrado”* e inspecciona el contenido descifrado. El segundo enclave seguro autentica el contenido descifrado y comunica un mensaje al primer enclave seguro. *“[E]l primer enclave seguro descifra el contenido cifrado para producir contenido descifrado adicional y procesa el contenido descifrado adicional (por ejemplo, procesa un documento, reproduce una canción)”* (D1, párrafo [0114]).

Sin embargo, si la autenticación del segundo enclave seguro o el contenido descifrado no tiene éxito, esto *“lleva a ... impedir que el primer enclave seguro procese el contenido no cifrado, derivado del contenido cifrado, en respuesta a que el segundo enclave seguro inspecciona el descifrado contenido”* (D1, párrafo [0114]). Así, el documento D1 indica claramente que incluso si la autenticación mencionada no tiene éxito, el segundo enclave seguro inspecciona el contenido descifrado, que se deriva del contenido cifrado que el segundo enclave seguro recibe del primer

enclave seguro. Por lo tanto, el primer enclave seguro comunica el contenido cifrado al segundo enclave seguro independientemente de si la autenticación es exitosa, lo que significa que el primer enclave seguro comunica el contenido cifrado al segundo enclave seguro independientemente de si la aplicación del segundo enclave seguro es incluida en la lista blanca.

Por al menos las anteriores razones, el documento D1 no enseña ni sugiere “restringir (2008, 2010, 2012) el acceso de los datos de enclave a enclaves con identidades autenticadas que se permite de acuerdo con la lista permitida, en donde la restricción incluye determinar si enviar los datos de enclave desde el enclave sellado al enclave de destino, el cual es diferente del enclave de sellado, con base al menos en parte en si el enclave de destino está incluido en la lista de una o más identidades de enclave permitidas para desellar los datos de enclave”, según se indica en las reivindicaciones independientes enmendadas 1 y 11. Por ejemplo, el documento D1 no sugiere de ninguna manera que se tome una determinación sobre si enviar el contenido cifrado descrito en el mismo desde el primer enclave seguro al segundo enclave seguro basándose al menos en parte en si el segundo enclave seguro está incluido en la lista blanca. De hecho, el Documento D1 se aleja de dicha característica que requieren las reivindicaciones independientes 1 y 11 enmendadas, porque indica que el primer enclave seguro descrito en el documento D1 comunica el contenido cifrado al segundo enclave seguro independientemente de si la aplicación del segundo enclave seguro está incluida en la lista blanca.

Además, el documento D2 no corrige esta deficiencia del documento D1 con respecto a las reivindicaciones independientes 1 y 11 enmendadas. Por ejemplo, el documento D2 no revela explícitamente una lista de enclaves autenticados, ni tampoco la determinación de “*enviar los datos de enclave desde el enclave sellado al enclave de destino, el cual es diferente del enclave de sellado, con base al menos en parte en si el enclave de destino está incluido en la lista de una o más identidades de enclave permitidas para desellar los datos de enclave*”. En consecuencia, el documento D2 no sugiere de ninguna manera la restricción del acceso de los datos de enclave a enclaves con identidades autenticadas que se permite de acuerdo con la lista permitida que comprende dicha determinación como se requiere en las reivindicaciones independientes enmendadas 1 y 11.

Por su parte, el documento D3 tampoco subsana esta deficiencia de los documentos D1 y D2 con respecto a las reivindicaciones independientes 1 y 11 modificadas.

En consecuencia, el solicitante sostiene que las reivindicaciones independientes 1 y 11 enmendadas son patentables sobre la combinación de los documentos D1, D2 y D3. Además, las reivindicaciones 2 a 6, que dependen de la reivindicación independiente 1, y las reivindicaciones 12 a 16, que dependen de la reivindicación independiente 11, son patentables sobre la combinación de los documentos D1, D2 y D3 por al menos las mismas razones que las reivindicaciones independientes 1 y 11, y además en vista de sus propias características respectivas.

Con respecto a las reivindicaciones 7 a 10 y 17 a 20, los documentos D1, D2 y D3 no enseñan ni sugieren *“enviar una lista permitida y datos de enclave asociados hacia el enclave de sellado, en donde la lista permitida incluye una lista de una o más identidades de enclave permitidas para desellar los datos de enclave, dicho envío comprende causar que el enclave de sellado determine si enviar los datos de enclave hacia el enclave de destino que es diferente del enclave de sellado con base al menos en parte en si el enclave de destino está incluido en la lista de una o más identidades de enclave permitidas para desellar los datos de enclave”*, según lo reclamado por las reivindicaciones independientes 7 y 17 por las mismas razones expuestas previamente donde se demostró que dichos documentos no enseñan ni sugiere dicha determinación y que en cambio alejan a la persona del oficio de la invención reclamada en la presente solicitud.

Los documentos D1, D2 y D3 tampoco mencionan que *“la lista permitida es una lista de tipos de identidad abstracta que corresponden a respectivos niveles de jerarquía de una jerarquía de identidad”*.

En consecuencia, el solicitante sostiene que las reivindicaciones independientes 7 y 17 modificadas son patentables sobre la combinación de los documentos D1, D2 y D3. Además, las reivindicaciones 8 a 10, que dependen de la reivindicación independiente 7, y las reivindicaciones 18 a 20, que dependen de la reivindicación independiente 17, son patentables sobre la combinación de los documentos D1, D2 y D3 por al menos las mismas razones que las reivindicaciones independientes 7 y 17, y además en vista de sus propias características respectivas.

Por lo tanto, el solicitante solicita respetuosamente que el rechazo de las reivindicaciones de la presente solicitud se reconsidere y retire.

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, D2 o D3, 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, D2 y D3, toda vez que nada dentro de dichos documentos revela en forma directa o al menos llega a sugerir todas las características de la materia reclamada en las reivindicaciones independientes. Por consiguiente, no se puede derivar la inexistencia de los requisitos de ley para la concesión del privilegio de patentabilidad.

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 20 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 las tasas correspondientes a la modificación de capítulo descriptivo y a 5 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-1074

REIVINDICACIONES (con marcas de cambios)

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

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

recibir (2004) una lista permitida y datos de enclave asociados del enclave de origen en el enclave de origen, en donde la lista permitida incluye una lista de una o más identidades de enclave permitidas para desellar los datos de enclave;

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

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

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

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

3. El método de acuerdo con la reivindicación 1, en donde la lista permitida es una lista de tipos de identidad abstracta; y que comprende además:

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

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

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

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

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

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

~~cifrar los datos de enclave con una clave asociada con el enclave de sellado para crear datos de enclave sellados;~~

almacenar los datos de enclave sellados en almacenamiento persistente; y

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

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

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

7. Un método para sellar datos de enclave, que comprende:
recibir, en un enclave de origen (1912) alojado en una primera plataforma de enclave nativa (1916), un primer reporte de afirmación de un enclave de sellado (1932) alojado en una segunda plataforma de enclave nativa (1936);
verificar la confianza en el enclave de sellado; y
enviar una lista permitida y datos de enclave asociados hacia el enclave de sellado, en donde la lista permitida incluye una lista de una o más identidades de enclave permitidas para desellar los datos de enclave, dicho envío comprende causar que el enclave de sellado determine si enviar los datos de enclave hacia el enclave de destino que es diferente del enclave de sellado con base al menos en parte en si el enclave de destino está incluido en la lista de una o más identidades de enclave permitidas para desellar los datos de enclave, en donde la lista permitida es una lista de tipos de identidad abstracta que corresponden a respectivos niveles de jerarquía de una jerarquía de identidad; y
enviar un reporte de afirmación de origen del enclave de origen hacia el enclave de sellado, en donde el reporte de afirmación de origen incluye al menos un valor de identidad del enclave de origen que corresponde a un tipo de identidad abstracta en la lista permitida.

8. El método de acuerdo con la reivindicación 7 que comprende además:
un proceso de afirmación entre el enclave de sellado y el enclave de origen;
generar datos de enclave cifrados por medio de cifrar los datos de enclave con una clave generada durante el proceso de afirmación; y
en donde los datos de enclave enviados hacia el enclave de sellado son los datos de enclave cifrados.

9. El método de acuerdo con la reivindicación 7, en donde:
la primera plataforma de enclave nativa está en una primera computadora y la segunda plataforma de enclave nativa está alojada en una segunda computadora.

10. El método de acuerdo con la reivindicación 7, que comprende además:
completar parcialmente una operación de procesamiento seguro en el enclave de origen; y
en donde los datos de enclave incluyen datos de estado del enclave de origen suficientes para permitir que otra instanciación de enclave continúe la operación de procesamiento seguro completada parcialmente.

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

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

recibir (2004) una lista permitida y datos de enclave asociados del enclave de origen, en donde la lista permitida incluye una lista de una o más identidades de enclave permitidas para desellar los datos de enclave;

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

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

712. El sistema de acuerdo con la reivindicación 611, en donde:

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

813. El sistema de acuerdo con la reivindicación 611, en donde la lista permitida es una lista de tipos de identidad abstracta, y las instrucciones provocan además al menos:

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

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

914. El sistema de acuerdo con la reivindicación 611, en donde se cifran los datos de enclave recibidos, y las instrucciones provocan además al menos:

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

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

1015. El sistema de acuerdo con la reivindicación 611, en donde almacenar de manera segura los datos de enclave además incluye:

cifrar los datos de enclave con una clave asociada con el enclave de sellado para crear datos de enclave sellados;

almacenar los datos de enclave sellados en almacenamiento persistente; y

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

después de determinar que los datos de enclave son enviados desde el enclave sellado al enclave de destino con base al menos en parte en que el enclave de destino está incluido en la lista de una o más identidades de enclave permitidas para desellar los datos de enclaves se permite el acceso a una

~~identidad autenticada~~, descifrar los datos de enclave sellados en respuesta a recibir la petición por los datos de enclave de parte de un enclave de destino.

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

~~1117.~~ Un sistema que comprende al menos un procesador y memoria que almacena en la misma instrucciones que, cuando son ejecutadas por el sistema, provocan al menos:

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

verificar la confianza en el enclave de sellado; y

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

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

~~1218.~~ El sistema de acuerdo con la reivindicación ~~1117~~, en donde las instrucciones provocan además al menos:

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

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

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

~~1319.~~ El sistema de acuerdo con la reivindicación ~~1117~~, en donde:

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

~~14. El sistema de acuerdo con la reivindicación 11, en donde la lista permitida es una lista de tipos de identidad abstracta; y en donde, las instrucciones provocan además al menos:~~

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

~~1520.~~ El sistema de acuerdo con la reivindicación ~~1117~~, en donde las instrucciones provocan además al menos:

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

REIVINDICACIONES

1. Un método para sellar datos de enclave, que comprende:
enviar (2002), a un enclave de origen (1912) alojado en una primera plataforma de enclave nativa (1916), un primer reporte de afirmación de un enclave de sellado (1932) alojado en una segunda plataforma de enclave nativa (1936);
recibir (2004) una lista permitida y datos de enclave asociados del enclave de origen en el enclave de origen, en donde la lista permitida incluye una lista de una o más identidades de enclave permitidas para desellar los datos de enclave;
almacenar (2006) de manera segura los datos de enclave y la lista permitida, en donde el almacenado de manera segura incluye cifrar los datos de enclave con una clave asociada con el enclave de sellado, por parte del enclave de sellado, antes de recibir una petición por los datos de enclave de parte de un enclave de destino para crear datos de enclave sellados; y
restringir (2008, 2010, 2012) el acceso de los datos de enclave a enclaves con identidades autenticadas que se permite de acuerdo con la lista permitida, en donde la restricción incluye determinar si enviar los datos de enclave desde el enclave sellado al enclave de destino, el cual es diferente del enclave de sellado, con base al menos en parte en si el enclave de destino está incluido en la lista de una o más identidades de enclave permitidas para desellar los datos de enclave.
2. El método de acuerdo con la reivindicación 1, en donde:
la primera plataforma de enclave nativa está en una primera computadora y la segunda plataforma de enclave nativa está alojada en una segunda computadora.
3. El método de acuerdo con la reivindicación 1, en donde la lista permitida es una lista de tipos de identidad abstracta; y que comprende además:
recibir un reporte de afirmación de origen del enclave de origen; y
derivar un valor de identidad permitida a partir del reporte de afirmación de origen y un tipo de identidad abstracta en la lista permitida.
4. El método de acuerdo con la reivindicación 1, en donde se cifran los datos de enclave recibidos, y que comprende además:
ejecutar un proceso de afirmación entre el enclave de origen y el enclave de sellado; y
descifrar los datos de enclave cifrados con una clave generada durante el proceso de afirmación.
5. El método de acuerdo con la reivindicación 1, en donde almacenar de manera segura los datos de enclave incluye:
almacenar los datos de enclave sellados en almacenamiento persistente; y
en donde restringir el acceso de los datos de enclave a enclaves con identidades autenticadas adicionalmente incluye:
después de determinar que los datos de enclave son enviados desde el enclave sellado al enclave de destino con base al menos en parte en que el enclave de destino está incluido en la lista de una o

más identidades de enclave permitidas para desellar los datos de enclave, descifrar los datos de enclave sellados en respuesta a recibir la petición por los datos de enclave de parte de un enclave de destino.

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

7. Un método para sellar datos de enclave, que comprende:
recibir, en un enclave de origen (1912) alojado en una primera plataforma de enclave nativa (1916), un primer reporte de afirmación de un enclave de sellado (1932) alojado en una segunda plataforma de enclave nativa (1936);
verificar la confianza en el enclave de sellado; y
enviar una lista permitida y datos de enclave asociados hacia el enclave de sellado, en donde la lista permitida incluye una lista de una o más identidades de enclave permitidas para desellar los datos de enclave, dicho envío comprende causar que el enclave de sellado determine si enviar los datos de enclave hacia el enclave de destino que es diferente del enclave de sellado con base al menos en parte en si el enclave de destino está incluido en la lista de una o más identidades de enclave permitidas para desellar los datos de enclave, en donde la lista permitida es una lista de tipos de identidad abstracta que corresponden a respectivos niveles de jerarquía de una jerarquía de identidad; y
enviar un reporte de afirmación de origen del enclave de origen hacia el enclave de sellado, en donde el reporte de afirmación de origen incluye al menos un valor de identidad del enclave de origen que corresponde a un tipo de identidad abstracta en la lista permitida.

8. El método de acuerdo con la reivindicación 7 que comprende además:
un proceso de afirmación entre el enclave de sellado y el enclave de origen;
generar datos de enclave cifrados por medio de cifrar los datos de enclave con una clave generada durante el proceso de afirmación; y
en donde los datos de enclave enviados hacia el enclave de sellado son los datos de enclave cifrados.

9. El método de acuerdo con la reivindicación 7, en donde:
la primera plataforma de enclave nativa está en una primera computadora y la segunda plataforma de enclave nativa está alojada en una segunda computadora.

10. El método de acuerdo con la reivindicación 7, que comprende además:
completar parcialmente una operación de procesamiento seguro en el enclave de origen; y
en donde los datos de enclave incluyen datos de estado del enclave de origen suficientes para permitir que otra instanciación de enclave continúe la operación de procesamiento seguro completada parcialmente.

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

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

recibir (2004) una lista permitida y datos de enclave asociados del enclave de origen, en donde la lista permitida incluye una lista de una o más identidades de enclave permitidas para desellar los datos de enclave;

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

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

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

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

13. El sistema de acuerdo con la reivindicación 11, en donde la lista permitida es una lista de tipos de identidad abstracta, y las instrucciones provocan además al menos:

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

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

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

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

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

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

almacenar los datos de enclave sellados en almacenamiento persistente; y

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

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

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

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

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

verificar la confianza en el enclave de sellado;

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

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

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

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

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

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

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

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

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

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

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