

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. 18680** del 29 de noviembre de 2021.

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

En los numerales 4, 5 y 6 del oficio citado, ese Despacho concluye que las reivindicaciones de la presente solicitud de patente carecen de novedad frente a las enseñanzas de los documentos **US 2015/347768** (D1) y **US 2015/304736** (D2).

1.1. Novedad y nivel inventivo

Aunque el Examinador haya citado los documentos D1 y D2 para objetar la novedad de la presente invención, es posible afirmar que éstos no enseñan las características esenciales de la invención, como se explica a continuación.

Ninguno de los documentos D1 o D2 menciona o 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 1 y 11.

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 inspeccionarlo dependiendo de una política relativa 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”*.

Aunque el documento D1 menciona en efecto el uso de una lista blanca, dicha lista blanca no se utiliza para *“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”.

El uso de la lista blanca que se enseña en el documento D1 es diferente a lo reclamado en las actuales reivindicaciones 1 y 11. Sin duda el documento D1 sí menciona el uso de una lista blanca, pero no menciona **determinar si enviar los datos de enclave** desde el enclave sellado al enclave de destino **con base en dicha lista**.

Las enseñanzas del documento D1 son diferentes a la invención que se reclama en la presente solicitud porque la lista blanca en el documento D1 se utiliza de forma diferente a la invención reclamada en la presente solicitud.

Aunque el método divulgado en el documento D1, de acuerdo con el párrafo [0068], verifica la autenticidad del cliente comparando el ID de la lista blanca del cliente con los ID de la lista blanca de las plataformas probadas, dicha comparación con la lista blanca no involucra una restricción de acceso que determine el envío de los datos desde el enclave sellado al enclave de destino como lo requiere la invención que actualmente se reclama.

Aunque según el examinador, de acuerdo con las tablas 1 y 2 del oficio N° 18680, dichas características de restricción de acceso reclamadas en las reivindicaciones 1 y 11 de la presente solicitud y que corresponden a “*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*” están divulgadas en el párrafo [0113] del documento D1, amablemente se aclara que dicho párrafo, y nada en el documento D1, divulga o sugiere dichas características de restricción de acceso.

El párrafo [0113] del documento D1 divulga que “*La autenticación puede incluir además la política que incluye una lista blanca (bloque 735) que enumera un motor de inspección autorizado incluido en el segundo enclave seguro*” donde, “*Por ejemplo, una vez que el primer nodo seguro comprende “quién”, la identificación del segundo enclave seguro (o alguna derivación de la misma) puede compararse con la lista blanca para determinar si la aplicación del segundo*

nodo seguro debe inspeccionar el contenido”, en donde, no se sugiere, ni divulga un envío condicionado de datos correspondiente a la restricción de acceso que se reclama en la presente solicitud. El párrafo [0113] se refiere a una inspección de contenido condicionada con base en una lista blanca (que, de acuerdo con el párrafo [0068], involucra un desellado (descifrado) de los datos, no corresponde a un envío de datos), donde dicha inspección de contenido condicionada (del documento D1) es diferente a un envío de datos condicionado como el que se reclama en la presente solicitud.

De acuerdo con lo anterior, aunque el oficio N° 18680, en su sección 7, indica que, refiriéndose a los párrafos [0068] y [0113] del documento D1, *“En estos párrafos se puede evidenciar que de acuerdo con la lista blanca que contiene los ID autorizados, se puede autenticar o no autorizar a un enclave para comunicación con un enclave de origen”* (énfasis añadido), los párrafos [0068] y [0113] no menciona nada sobre la autorización para comunicación de los enclaves, sino, como se mencionó anteriormente, se refieren a la autorización de inspeccionar los datos, lo que es diferente a una autorización de comunicación y/o envío de datos condicionado que se requiere en la invención de la presente solicitud.

Ahora bien, el documento D1 no solo no divulga la restricción de acceso reclamada en la solicitud, sino que enseña un método contrario, porque el envío de datos, según el documento D1, se realiza sin importar el contenido de la lista blanca de acuerdo con lo divulgado en el párrafo [0114] que divulga que, 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 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, en el documento D1, el primer enclave seguro comunica el contenido cifrado al segundo enclave seguro independientemente de si la autenticación es exitosa, y, por lo tanto, independientemente de si la aplicación del segundo enclave seguro esté incluida en la lista blanca.

Por otra parte, el documento D2 no corrige las deficiencias del documento D1 en mencionar que *“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” y, por lo tanto, una persona del oficio medianamente versada en la materia y en conocimiento de los documentos D1 y D2, no llegaría a, ni concluiría, las invenciones reclamadas en las reivindicaciones 1 y 11. 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”.

Aunque según el examinador, de acuerdo con las tablas 1 y 2 del oficio N° 18680, dichas características de restricción reclamadas en las reivindicaciones 1 y 11 de la presente solicitud y que corresponden a “*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*” están divulgadas en los párrafos [0061] y [0098] del documento D2, amablemente se aclara que dichos párrafos, y nada en el documento D2, divulga o sugiere dichas características de restricción de acceso.

El párrafo [0061] del documento D2 divulga que un dispositivo remoto (por ejemplo, un servidor) puede estar habilitado para verificar la autenticidad o integridad de memoria del enclave y/o de su contenido en memoria, en donde, por ejemplo, un servidor autentica una memoria de enclave por medio de verificar que el enclave está corriendo en una plataforma segura; o verificar mediciones y/o información de identidad incluida en el mismo enclave. El párrafo [0061] se refiere a la autenticación de un enclave por un servidor (no corresponde a un envío de datos condicionada con base en una lista blanca) lo que es diferente a la restricción que involucra un envío de datos condicionado que se reclama en la presente solicitud.

Aunque el documento D2 menciona el uso de una lista blanca según lo divulgado en su párrafo [0098], dicha lista blanca no se utiliza para “*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". Aunque el método divulgado en el documento D2, de acuerdo con el párrafo [0098], verifica la autenticidad del cliente comparando el ID de la lista blanca del cliente con los ID de la lista blanca de las plataformas probadas, dicha comparación con la lista blanca no involucra una restricción que determine el envío de los datos desde el enclave sellado al enclave de destino como lo requiere la invención que actualmente se reclama.

De acuerdo con lo anterior, aunque el oficio N° 18680, en su sección 7, indica que, refiriéndose a los párrafos [0061] y [0098] del documento D2, *"En estos párrafos se puede evidenciar nuevamente que la comunicación entre un origen y un destino, como es el caso de dos enclaves, se puede autenticar o restringir de acuerdo con la comparación de identificaciones de +una lista blanca"* (énfasis añadido), los párrafos [0061] y [0098] no menciona nada sobre la restricción para comunicación entre los enclaves, sino, como se mencionó anteriormente, se refieren a la verificación de autenticidad del enclave, lo que es diferente a una autorización de comunicación y/o envío de datos condicionado que se requiere en la invención de la presente solicitud.

Por 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.

2. Conclusión

Los argumentos expuestos en el numeral 1 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 una restricción de acceso que incluya determinar si enviar los datos de enclave desde el enclave sellado al enclave de destino 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 como lo hace la presente solicitud. 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 los argumentos aquí presentados, para conceder el privilegio de patente solicitado para la materia objeto de las actuales 20 reivindicaciones y que de subsistir alguna duda o inquietud respecto a la patentabilidad de la presente invención, a pesar de los 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 la invención, mediante la emisión de un segundo examen de fondo, teniendo en cuenta los argumentos aquí presentados, 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.

Petición

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

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