Superintendencia de Industria y Comercio

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Oficio N° **8039** de **26 de mayo de 2025**

Ref. Expediente N° NC2021/0008019

Señores
THALES DIS FRANCE SA

TÍTULO DE LA SOLICITUD: "UN CHIP DE CIRCUITO Y UN MÉTODO PARA OPERARLO"
NUMERO DE SOLICITUD INTERNACIONAL: PCT/EP2019/081955
FECHA DE PRESENTACIÓN INTERNACIONAL: 20 de noviembre de 2019.
PRIORIDAD: 21/11/2018, EP (EUROP PATENT ORGANIZATION(EPO)), 18306538.2

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. Modificaciones presentadas

Revisada la modificación a la solicitud objeto de estudio, la cual fue radicada el 18 de diciembre de 2024 bajo el número NC2021/0008019, y teniendo en cuenta lo señalado en el artículo 34 de la Decisión 486 de 2000 de la Comisión de la Comunidad Andina, esta oficina no acepta las modificaciones propuestas, por cuanto aquellas amplían la materia divulgada inicialmente.

Las reivindicaciones 1 a 8, no son aceptables porque incluyen "*Un sistema para parchear un sistema operativo de un chip de circuito integrado*", que no habían sido divulgados inicialmente, y que no se encuentra soporte en la descripción, por lo cual se amplía el objeto de la solicitud.

2. Objeto de la invención

El problema planteado consiste en la necesidad de proporcionar un método mejorado para proporcionar una actualización segura del sistema operativo y otros programas instalados en chips de circuito integrado seguros.

Para resolver dicho problema técnico, la solicitud en estudio proporciona un método para parchar de forma segura un sistema operativo de un chip de circuito integrado incluye operar un servidor de parches para encriptar un parche en el sistema operativo, operar el servidor de parches para transmitir el parche encriptado al servidor de la autoridad emisora y operar el servidor de la autoridad emisora para anexar el parche encriptado dentro de un segundo certificado digital de la autoridad emisora en una extensión del segundo certificado digital (...) (Resumen).

3. Reivindicaciones estudiadas

El presente estudio se basa en el capítulo reivindicatorio presentado el 18 de junio de 2021.

4. Reivindicaciones relativas a un uso

De conformidad con lo señalado en el artículo 14 de la Decisión 486 de 2000 de la Comisión de la Comunidad Andina solo son patentables las invenciones de producto o de procedimiento.

En consecuencia las reivindicaciones 1 a 8 no se consideran patentables, teniendo en cuenta que reclaman un uso.

Lo anterior se argumenta dado que la reivindicación independiente 1 se refiere a un método que reclama únicamente etapas de operación sobre el chip de circuito integrado, lo cual corresponde a un procedimiento que puede ser llevado a cabo por un usuario a quien se le asigne dicha labor, es decir, corresponde netamente al uso que se le dará a la invención como consecuencia del conocimiento propio del ejercicio intelectual.

Especificamente puede detallarse en la reivindicación 1 que las acciones de transmitir, anexar, comunicar con el chip desempaquetar, verificar las extensiones e instalar el parche dependen de la acción de “operar” que depende de un tercer. Adicionalmente, del párrafo 10 de la descripción puede evidenciarse que de los 10 pasos del método, cada uno de ellos depende de la “*operación*”, que como se indicó anteriormente, corresponde netamente al uso que se le dará a la invención como consecuencia del conocimiento propio del ejercicio intelectual que puede ser llevado a cabo por una persona.

5. De la solicitud de patente

5.1. Titulo

De conformidad con el literal d) del artículo 27 de la Decisión 486 de 2000 de la Comisión de la Comunidad Andina, el nombre de la invención de que se trata 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.

Analizado el título modificado en el escrito radicado bajo el N° NC2021/0008019 el 18 de diciembre de 2024, se encuentra que el título de la solicitud no refleja el objeto divulgado en la descripción y las reivindicaciones, por lo cual se sugiere el siguiente título: “CHIP DE CIRCUITO INTEGRADO Y PARCHE ENCRIPTADO”.

6. Determinación del Estado de la Técnica

La fecha para determinar el estado de la técnica es el 21 de noviembre de 2018, que corresponde a la fecha de presentación de prioridad de la solicitud.

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	US2008022380	“Method of patching applications on small resource-constrained secure devices”	24 de enero de 2008
D2	US2004198496	“Dynamic configuration of a gaming system”	7 de octubre de 2004

D1[1] divulga una aplicación de software se almacena en una tarjeta inteligente en forma de particiones y se carga desde la tarjeta inteligente a la memoria de un ordenador host al que está conectada. La aplicación de software se ejecuta en el ordenador host, el cual, mediante sus instrucciones, establece un canal de comunicación entre la aplicación y un servidor de parches remoto que contiene un parche para al menos una partición de la aplicación. Al detectar un parche disponible para al menos una partición de la aplicación, se descarga dicha partición del servidor remoto a la memoria volátil asignada a la aplicación en el ordenador host a través del primer canal de comunicación, y se carga dicha partición desde la memoria volátil asignada a la aplicación a la tarjeta inteligente. Se describen otros sistemas y métodos (Resumen).

D2[2] divulga un método para habilitar la configuración dinámica de terminales de juego instaladas en una o varias instalaciones de juego, mediante el cual los juegos certificados, los archivos de datos certificados y los componentes de software de soporte certificados se activan según un programa predeterminado o automáticamente en respuesta a la actividad de juego observada. El método puede incluir la asignación de un certificado PKI individual a cada componente de software ejecutable y a cada una de sus versiones, la vinculación del certificado PKI al software ejecutable, la asociación de una política distintiva para cada certificado y la aplicación de las políticas de ejecución del software según la configuración y el programa de juego autorizados deseados. El "Nombre del sujeto" del certificado PKI (o el campo "Emitido a" o "Nombre común") puede ser una concatenación de la identificación del componente de software, su número de versión y, opcionalmente, otros caracteres de identificación. El método se aplica igualmente a otros subsistemas de juego conectados a la red. El método permite un control preciso y seguro de los componentes de software autorizados y, por lo tanto, la flexibilidad para configurar de forma segura el sistema de juego según un programa o en bucle cerrado para cumplir los objetivos comerciales. Además, se describe un método que permite a la autoridad de certificación vincular los certificados al código probado (Resumen).

7. Examen de Patentabilidad

De acuerdo con lo establecido en el artículo 14 de la Decisión 486 de 2000 de la Comisión de la Comunidad Andina, en el cual se establecen los requisitos de patentabilidad objeto de la solicitud en estudio, esta Oficina presenta a continuación el análisis de los requisitos de patentabilidad.

7.1. Nivel Inventivo

Teniendo en cuenta lo señalado en el artículo 18 de la Decisión 486 de 2000 de la Comisión de la Comunidad Andina, la reivindicación independiente 9 (NC2021/0008019 del 18 de junio de 2021) refiere a: *“Un chip de circuito integrado que comprende: (…)”*. A continuación, se presenta la tabla comparativa entre el objeto reivindicado y los documentos encontrados en el estado de la técnica:

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

CARACTERÍSTICAS ESENCIALES	D1	D2
Un chip de circuito integrado que comprende:	(…) La tarjeta inteligente (101) contiene una unidad central de procesamiento (201) (…) (Párr. 0030).	(…) Componentes de hardware (en cada uno de los chipsets principales) (…) (Párr. 0065).

[1] https://patentimages.storage.googleapis.com/60/0c/94/eaa70f2da7de16/US20080022380A1.pdf
[2] https://patentimages.storage.googleapis.com/65/fb/e8/45650905441d29/US20040198496A1.pdf

Un procesador.	(…) La tarjeta inteligente (101) contiene una unidad central de procesamiento (201) (…) (Párr. 0030).	Para el técnico medio versado en la materia resulta evidente el uso de un procesador.
Y una memoria conectada al procesador y que contiene instrucciones ejecutables por el procesador, incluido un sistema operativo; e instrucciones para hacer que el procesador.	(…) una RAM (203) y una memoria no volátil (205). Estos componentes están conectados mediante un bus (207). También se conecta al bus (207) una interfaz de hardware de comunicaciones (209) para proporcionar una conexión entre el bus (207) y, en consecuencia, la CPU (201), la RAM (203) y la memoria no volátil (205), y el conector (105) (Párr. 0030). (…) en donde la aplicación de software comprende instrucciones que, cuando se cargan y se ejecutan en la computadora host, hacen que la computadora host (…) (Reiv. 10).	(…) Cada carpeta contiene los recursos informáticos y las instrucciones para realizar cada paso. Las carpetas están claramente identificadas con el número de paso y la descripción del título del procedimiento (1108) (Párr. 0075)
Reciba un certificado digital de un servidor de parches a través de un terminal verificador, el cual certificado digital incluye una extensión que contiene un parche encriptado para el sistema operativo.	(…) los parches o instaladores están firmados con un certificado digital y se le pide al usuario que valide el certificado de firma (…) (Párr. 0003). (…) el agente host (211) establece una sesión SSL/TLS segura con el servidor de parches remoto (601) mediante autenticación mutua (paso (703)). El certificado del dispositivo para esta autenticación mutua reside en la tarjeta inteligente (101) y se libera solo después de que la tarjeta haya confirmado la validez del agente host (211) (es decir, paso (701)) (Párr. 0063). (…) la comunicación está cifrada por los dos agentes (211) y (213) para evitar el acceso de un tercero a lo largo de una ruta de comunicaciones desde la tarjeta inteligente (101) a un servidor remoto (109) (…) (Párr. 0047).	(…) la pestaña "Detalles" (404) del certificado (402) y seleccionando "Solo extensiones", como se muestra en (406). La información intrínseca que identifica de forma única cada componente de software ejecutable se puede introducir en los atributos extendidos de un certificado PKI para lograr el mismo propósito que se describe para la FIG. 3 como alternativa a introducir la información en el nombre del sujeto del certificado (…) (Párr. 0049). Una arquitectura de certificado PKI según la reivindicación 1, en la que el al menos un campo comprende al menos uno de los campos y extensiones de campo (Reiv. 6). (…) configurar el registro de Windows, configurar accesos directos e instalar parches de software (…) (Párr. 0055).
Desempaquetar el certificado digital recuperando así la extensión al certificado digital.	No menciona.	(…) la pestaña "Detalles" (404) del certificado (402) y seleccionando "Solo extensiones", como se muestra en (406). La información intrínseca que identifica de forma única cada componente de software ejecutable se puede introducir en los atributos extendidos de un certificado PKI (…) (Párr. 0049).

		Una arquitectura de certificado PKI según la reivindicación 1, en la que el al menos un campo comprende al menos uno de los campos y extensiones de campo (Reiv. 6). Los componentes de software ejecutables firmados pueden empaquetarse en paquetes de instalación MSI firmados con código de una manera sustancialmente idéntica a los componentes de software ejecutables, es decir, con un certificado PKI único cuyo nombre de sujeto contiene el número de pieza, la versión y los identificadores de nombre descriptivo para el paquete MSI (Párr. 0053). Para el técnico medio versado en la materia resulta evidente que la arquitectura PKI y los paquetes de instalación MSI se encargan de desempaquetar y desencriptar el certificado digital y de su instalación.
Verificar que la extensión al certificado digital corresponde al sistema operativo del chip de circuito integrado.	(…) operar la tarjeta inteligente para autenticar el programa de descarga verificando que la clave secreta transmitida corresponde a una clave esperada por la tarjeta inteligente (…) (Reiv. 9) (…) el agente host (211) establece una sesión SSL/TLS segura con el servidor de parches remoto (601) mediante autenticación mutua (paso (703)) (…)(Párr. 0063). No menciona la extensión.	(…) la pestaña "Detalles" (404) del certificado (402) y seleccionando "Solo extensiones", como se muestra en (406). La información intrínseca que identifica de forma única cada componente de software ejecutable se puede introducir en los atributos extendidos de un certificado PKI para lograr el mismo propósito que se describe para la FIG. 3 como alternativa a introducir la información en el nombre del sujeto del certificado (…) (Párr. 0049).
Y si se verifica que la extensión corresponde al sistema operativo del chip de circuito integrado, desencriptar la extensión al certificado digital recuperando así el parche al sistema operativo del chip de circuito integrado, e instalar el parche en el sistema operativo del chip de circuito integrado.	(…) operar la tarjeta inteligente para autenticar el programa de descarga verificando que la clave secreta transmitida corresponde a una clave esperada por la tarjeta inteligente (…) (Reiv. 9). (…) Tras la validación, se instala el parche o se ejecuta el instalador. En el improbable caso de que el ordenador se quede sin energía durante la instalación, no suele haber ningún mecanismo de recuperación ni necesidad de un proceso de recuperación. En su lugar, se espera que el usuario	(…) la pestaña "Detalles" (404) del certificado (402) y seleccionando "Solo extensiones", como se muestra en (406). La información intrínseca que identifica de forma única cada componente de software ejecutable se puede introducir en los atributos extendidos de un certificado PKI para lograr el mismo propósito que se describe para la FIG. 3 como alternativa a introducir la información en el nombre del sujeto del certificado (…) (Párr. 0049).

	reinstale la versión original del programa y repita el proceso de instalación del parche (Párr. 0003). (…) La tarjeta inteligente (101) contiene una unidad central de procesamiento (201) (…) (Párr. 0030). No menciona la etapa de desencriptar.	Una arquitectura de certificado PKI según la reivindicación 1, en la que el al menos un campo comprende al menos uno de los campos y extensiones de campo (Reiv. 6). Los componentes de software ejecutables firmados pueden empaquetarse en paquetes de instalación MSI firmados con código de una manera sustancialmente idéntica a los componentes de software ejecutables, es decir, con un certificado PKI único cuyo nombre de sujeto contiene el número de pieza, la versión y los identificadores de nombre descriptivo para el paquete MSI (Párr. 0053). (…) configurar el registro de Windows, configurar accesos directos e instalar parches de software (…) (Párr. 0055). Para el técnico medio versado en la materia resulta evidente que la arquitectura PKI y los paquetes de instalación MSI se encargan de desempaquetar, y desencriptar el certificado digital y de su instalación.

D1 es considerado como el estado de la técnica más cercano a la invención definida en la reivindicación 1, ya que divulga un método para aplicar parches a aplicaciones en dispositivos pequeños y seguros con recursos limitados (Título).

La diferencia entre la invención definida entre la reivindicación 9 y el circuito divulgado en D1, consiste en que la solicitud incluye las etapas de desempaquetar y desencriptar el certificado digital recuperando así la extensión al certificado digital.

El efecto que se logra al incluir las etapas de desempaquetar y desencriptar el certificado digital recuperando así la extensión al certificado digital es recuperar la extensión del certificado digital para mejorar la seguridad del chip.

Por lo tanto, el problema técnico objetivo que pretende resolver esta invención se puede formular así : ¿cómo modificar el circuito integrado divulgado en D1 para recuperar la extensión del certificado digital y mejorar la seguridad del chip?

Sin embargo, el incluir las etapas de desempaquetar y desencriptar datos es recuperar la extensión del certificado digital, ya está divulgado en D2 que se refiere a: (…) la pestaña "Detalles" (404) del certificado (402) y seleccionando "Solo extensiones", como se muestra en (406). La información intrínseca que identifica de forma única cada componente de software ejecutable se puede introducir en los atributos extendidos de un certificado PKI (…) (Párr. 0049). Una arquitectura de certificado PKI según la reivindicación 1, en la que el al menos un campo comprende al menos uno de los campos y extensiones de campo (Reiv. 6). Los componentes de software ejecutables firmados

pueden empaquetarse en paquetes de instalación MSI firmados con código de una manera sustancialmente idéntica a los componentes de software ejecutables, es decir, con un certificado PKI único cuyo nombre de sujeto contiene el número de pieza, la versión y los identificadores de nombre descriptivo para el paquete MSI (Párr. 0053).

Adicionalmente, para el técnico medio versado en la materia resulta evidente que la arquitectura PKI y los paquetes de instalación MSI se encargan de desempaquetar y desencriptar el certificado digital y de su instalación.

En consecuencia, la persona normalmente versada en la materia al verse enfrentada al problema técnico objetivo de recuperar la extensión del certificado digital y mejorar la seguridad del chip estaría motivada a incluir las etapas de desempaquetar y desencriptar el certificado digital recuperando así la extensión al certificado digital del D2 en el circuito de D1, para así llegar al objeto de la reivindicación 9. Por lo cual se considera obvia.

Así mismo, D1 divulga las características de las reivindicaciones dependientes de la siguiente manera:

- Reivindicación 10: (…) operar la tarjeta inteligente para verificar la autenticidad de la firma aplicada al parche para al menos una partición de la aplicación de software (Reiv. 3). (…) operar la tarjeta inteligente para autenticar el programa de descarga verificando que la clave secreta transmitida corresponde a una clave esperada por la tarjeta inteligente (Reiv. 9).

- Reivindicación 11: (…) La tarjeta inteligente almacena todos los datos confidenciales, como las claves privadas y las credenciales de usuario, en un sistema de archivos seguro. Además, proporciona funcionalidades criptográficas relacionadas con los datos confidenciales (…) (Párr. 0008). Los archivos de almacenamiento masivo son archivos de acceso público expuestos por la tarjeta inteligente (101) y visibles desde el ordenador host (103). El agente host (211) tiene acceso directo a estos archivos. Algunos ejemplos de estos archivos son HTML, imágenes, JavaScript, CSS y certificados de clave pública. Todos los archivos visibles a través de la interfaz de almacenamiento masivo son de solo lectura para el ordenador host (103). La única excepción es un conjunto de archivos de comunicaciones (217) en la partición de lectura y escritura (223) del almacenamiento masivo; por ejemplo, según una realización de la invención, el canal de comunicación entre el agente host (211) y el agente de tarjeta (213) se basa en archivos de almacenamiento masivo. Estos archivos son de lectura y escritura (Párr. 0037).

- Reivindicación 12: (…) el agente host busca nuevos componentes y los descarga si es necesario. El servidor de parches firma todos los parches que se descargan con su clave privada (…) (Párr. 0063). Los archivos de almacenamiento masivo son archivos de acceso público expuestos por la tarjeta inteligente (101) y visibles desde el ordenador host (103). El agente host (211) tiene acceso directo a estos archivos. Algunos ejemplos de estos archivos son HTML, imágenes, JavaScript, CSS y certificados de clave pública. Todos los archivos visibles a través de la interfaz de almacenamiento masivo son de solo lectura para el ordenador host (103). La única excepción es un conjunto de archivos de comunicaciones (217) en la partición de lectura y escritura (223) del almacenamiento masivo; por ejemplo, según una realización de la invención, el canal de comunicación entre el agente host (211) y el agente de tarjeta (213) se basa en archivos de almacenamiento masivo. Estos archivos son de lectura y escritura (Párr. 0037). (…) La tarjeta inteligente almacena todos los datos confidenciales, como las claves privadas y las credenciales de usuario, en un sistema de archivos seguro. Además, proporciona funcionalidades criptográficas relacionadas con los datos confidenciales (…) (Párr. 0008).

- Reivindicación 15: (…) El servidor de parches (601) integra la clave de descarga en el programa de descarga (paso (1109)). De este modo, la instancia específica del programa de descarga se personaliza para asociarse con un agente de tarjeta específico (213) y, en consecuencia, con una tarjeta inteligente específica (101) (…) (Párr. 0085). (…) La incrustación de secretos y el cálculo de valores hash también se aplican al agente host particionado. La figura 13 es un diagrama de secuencia temporal que ilustra el mecanismo para usar valores hash de secretos incrustados para verificar la autenticidad del agente host 211 y las particiones que lo conforman (…) (Párr. 0102).

- Reivindicación 16: (…) La tarjeta inteligente (101) contiene una unidad central de procesamiento (201) (…) (Párr. 0030). Para el técnico medio versado en la materia resulta evidente que la tarjeta inteligente puede ser incrustada en un documento de viaje.

De igual manera , D2 divulga las características de las reivindicaciones dependientes de la siguiente manera.

- Reivindicaciones 11 y 12: (…) la pestaña "Detalles" (404) del certificado (402) y seleccionando "Solo extensiones", como se muestra en (406). La información intrínseca que identifica de forma única cada componente de software ejecutable se puede introducir en los atributos extendidos de un certificado PKI para lograr el mismo propósito que se describe para la FIG. 3 como alternativa a introducir la información en el nombre del sujeto del certificado (…) (Párr. 0049). Una arquitectura de certificado PKI según la reivindicación 1, en la que el al menos un campo comprende al menos uno de los campos y extensiones de campo (Reiv. 6). Los componentes de software ejecutables firmados pueden empaquetarse en paquetes de instalación MSI firmados con código de una manera sustancialmente idéntica a los componentes de software ejecutables, es decir, con un certificado PKI único cuyo nombre de sujeto contiene el número de pieza, la versión y los identificadores de nombre descriptivo para el paquete MSI (Párr. 0053). (…) configurar el registro de Windows, configurar accesos directos e instalar parches de software (…) (Párr. 0055). Para el técnico medio versado en la materia resulta evidente que la arquitectura PKI y los paquetes de instalación MSI se encargan de desempaquetar, y desencriptar el certificado digital y de su instalación.

- Reivindicación 15: (…) Windows XP Embedded, así como en futuras versiones de Windows (al momento de redactar este documento, la próxima versión se denomina "Longhorn") para garantizar que solo se puedan ejecutar componentes de software ejecutables de un editor confiable, por ejemplo, "Microsoft" (…) (Párr. 0013).

- Reivindicación 16: (…) un marco llamado Nexus profundamente integrado directamente dentro de los componentes de hardware (en cada uno de los chipsets principales) y el BIOS, que constituye un mecanismo para autenticar la confiabilidad de la configuración del software y del hardware, se inicia antes de verificar la integridad del marco de firma de controladores, el marco de protección de archivos de Windows y el marco de políticas de restricción de software (Párr. 0065).

Las reivindicaciones dependientes 10 a 16 tampoco cumplen con el requisito de nivel inventivo.

8. Conclusión

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

Ítem	Documento	Reivindicaciones afectadas	Requisito que afecta
D1	US2008022380	9 a 16	Nivel inventivo

D2	US2004198496	9 a 16	Nivel inventivo

9. Respuesta a los argumentos del solicitante

Argumentos con respecto a las modificaciones presentadas

El solicitante indica que "*De conformidad con precisas instrucciones de mi representada se adjunta un nuevo capítulo reivindicatorio, el cual has sido debidamente revisado y modificado. La modificación efectuada a las reivindicaciones 1 a 8 consiste en cambiar las reivindicaciones de método por reivindicaciones para un sistema, todo lo cual está íntegramente soportado en la descripción*."

Con respecto a lo anterior, se le aclara al señor solicitante que las modificaciones presentadas no están sustentadas en la descripción, toda vez que la frase "*un sistema para parchear un sistema operativo de un chip de circuito integrado"* no es divulgada en el capítulo descriptivo, por lo tanto, la modificación no puede ser sustentada y es causa de ampliación de la materia presentada inicialmente. Teniendo en cuenta las anteriores consideraciones, el estudio realizado se basa en el capítulo reivindicatorio NC2021/0008019 del 18 de junio de 2021.

El solicitante indica que "*Ahora bien, con respecto al título, éste se modifica en los siguientes términos. SISTEMA PARA PARCHAR UN SISTEMA OPERATIVO DE UN CHIP DE CIRCUITO INTEGRADO Y UN CHIP DE CIRCUITO INTEGRADO RELACIONADO*".

En relación con la modificación realizada al título, se indica al señor solicitante que no es aceptable, toda vez que el capítulo reivindicatorio objeto de estudio solo considera la modalidad relacionada con el circuito integrado, toda vez que "*el sistema para parchar*" no corresponde a una modalidad del capítulo reivindicatorio, por lo tanto, no puede hacer parte del título de la solicitud.

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.

Sandra Isabel Calderon Rodriguez
DIRECTORA DE NUEVAS CREACIONES

Superintendencia de Industria y Comercio

Oficio N° **8039** de **26 de mayo de 2025**

Ref. Expediente N° NC2021/0008019

INFORME DE BÚSQUEDA
EXAMEN DE PATENTABILIDAD

Solicitud No.	Examen de patentabilidad							
NC2021/0008019	1°	-	2°	X	3°	-	Revoca	-
Solicitud Internacional No.	Fecha solicitud internacional: (DD/MM/AÑO)							
PCT/EP2019/081955	20 de noviembre de 2019							

Fecha de determinación estado de la técnica (DD/MM/AÑO)	Prioridad	Presentación
21/11/2018	X	-

Solicitante
THALES DIS FRANCE SA

Reivindicaciones que no son objeto de búsqueda por:							
Art. 14	1 a 8	Art. 15	-	Art. 20	-	Art. 25 (Falta de unidad de invención)	-

CRITERIOS DE BÚSQUEDA		
Reivindicaciones objeto de búsqueda	9 a 16	
Palabras clave utilizadas	Patch, server, encryption, server, issuing, operating system, unpack, chip, processor, memory, verifier terminal, decrypt, authority, install, update, "digital certificate", "patch server".	
Clasificaciones utilizadas para la búsqueda	CIP:	B42D 25/24, B42D 25/305, G06Q 10/10, H04N 1/32, G06Q 50/26

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	05006630	31/07/2006	-	-	A
WO	US2007005955	04/01/2007	-	-	A
	WO2016073202	12/05/2016	-	-	A
	WO2016189488	01/12/2016	-	-	A
	WO2017050739	30/03/2017	-	-	A
Patbase	US2008022380	24/01/2008	9 a 16	Todo el documento	Y
	US2012190354	26/07/2012	-	-	A
Orbit	US8589541	19/11/2013	-	-	A
Google patents	US2004198496	07/10/2004	9 a 16	Todo el documento	Y

([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://xxxxxxxx.	-
	-
	-
	-
	-

([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

"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.

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.	**"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: (18/05/2025)	