Superintendencia de Industria y Comercio

REPÚBLICA DE COLOMBIA
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO

Resolución N° **96986**

Ref. Expediente N° NC2021/0008019

Por la cual se deniega una Patente de Invención

LA SUPERINTENDENTE DE INDUSTRIA Y COMERCIO
en ejercicio de sus facultades legales, en especial de las conferidas en el numeral 24 del artículo 3° del Decreto 4886 de 2011, y

CONSIDERANDO

Que mediante escrito radicado en esta Superintendencia el 18 de junio de 2021 con el N° NC2021/0008019, por THALES DIS FRANCE SA, entró a fase nacional la solicitud de patente de invención titulada “UN CHIP DE CIRCUITO Y UN MÉTODO PARA OPERARLO”, que corresponde a la solicitud internacional PCT/EP2019/081955 del 20 de noviembre de 2019.

Que la solicitud fue publicada en la Gaceta de la Propiedad Industrial Nº 946 el 30 de noviembre de 2021, sin que se hubieran presentado oposiciones por parte de terceros.

Que realizado el examen de fondo mediante Oficio Nº 8039 de 26 de mayo de 2025, se requirió al solicitante en los términos del artículo 45 de la Decisión 486 de la Comisión de la Comunidad Andina para que presentara respuesta a las observaciones de carácter técnico, relacionadas con la patentabilidad o cumplimiento de los requisitos establecidos por esta Decisión para la concesión de la patente.

Que el solicitante mediante escrito radicado bajo el N° NC2021/0008019 el 26 de agosto de 2025, respondió oportunamente el requerimiento formulado sin presentar nuevo capítulo reivindicatorio. Por lo tanto, se tendrá en cuenta el capítulo reivindicatorio presentado con el radicado Nº NC2021/0008019 el 18 de junio de 2021.

Que en virtud de lo dispuesto en el artículo 14 de la Decisión 486 expedida por la Comisión de la Comunidad Andina *“Los países miembros otorgarán patentes para las invenciones, sean de producto o de procedimiento, en todos los campos de la tecnología, siempre que sean nuevas, tengan nivel inventivo y sean susceptibles de aplicación industrial."*

Que en el presente caso las reivindicaciones a 1 a 16 incluidas en el radicado bajo el N° NC2021/0008019 el 18 de junio de 2021, no cumplen los requisitos indicados. Lo anterior, de acuerdo con las siguientes consideraciones:

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 proporciona un dispositivo 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).

Reivindicaciones relativas a un uso (Art. 14 Decisión 486)

Tal como está contemplado en el artículo 14 de la Decisión 486, los usos no son susceptibles de protección, dado que se protegen productos y procedimientos. 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.

Específicamente 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 operativa de un tercero, tal y como lo indica el párrafo 10 de la descripción, los pasos del método reclamado, son producto de la "*operación*" del dispositivo, lo cual, 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 al realizar la ejecución del programa.

Con fundamento en las anteriores consideraciones, la Superintendente de Industria y Comercio,

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).

[1] https://patentimages.storage.googleapis.com/60/0c/94/eaa70f2da7de16/US20080022380A1.pdf

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).

Nivel Inventivo (Art. 18 Decisión 486)

Según lo dispuesto en el artículo 18 de la Decisión 486: *"Se considerará que una invención tiene nivel inventivo, si para una persona del oficio normalmente versada en la materia técnica correspondiente, esa invención no hubiese resultado obvia ni se hubiese derivado de manera evidente del estado de la técnica".*

En el presente caso, el chip reclamado en la solicitud no tiene nivel inventivo, teniendo en cuenta que la reivindicación 9 está referida a: *"Un chip de circuito integrado que comprende: (…)"* (Radicado Nº NC2021/0008019 del 18 de junio de 2021).

La siguiente tabla presenta la comparación entre las características técnicas esenciales de la solicitud estudiada, mencionadas en la reivindicación 1, y las reveladas en los documentos D1 y D2 que representan 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).
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	(…) 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)

[2] https://patentimages.storage.googleapis.com/65/fb/e8/45650905441d29/US20040198496A1.pdf

	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).	
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 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.	(…) 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.

D1 es considerado como el estado de la técnica más cercano a la invención definida en la reivindicación 9, 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 no mencionan alguna característica que, junto con las características de la reivindicación independiente, aporte nivel inventivo al chip de circuito de la reivindicación 9, por lo cual se considera que no tienen nivel inventivo.

Respuesta a los argumentos del solicitante

Argumentos relacionados con la no patentabilidad

El solicitante indica que "*Con respecto a la objeción del Examinador referente a que las reivindicaciones estudiadas 1-8 hacen referencia a un uso, y no a un producto o procedimiento, mi representada respetuosamente sostiene que no está de acuerdo con esa apreciación.*

El Examinador ha señalado que solo las invenciones de productos o procesos son patentables y ha argumentado que las reivindicaciones 1 a 8 son inadmisibles, alegando que se refieren a un mero "uso" y no a un proceso patentable."

Con respecto a lo anterior, es importante indicar que, las reivindicaciones 1 a 8 no logran cumplir con lo indicado en el artículo 14 de la Decisión 486. Lo anterior debido a que las acciones de transmitir, anexar, comunicar con el chip desempaquetar, verificar las extensiones e instalar el parche depende de la acción de "operar" que obedece a la intervención de un tercero quien resulta ser el responsable de realizar dichos pasos mientras manipula el dispositivo. Lo anterior puede evidenciarse en el párrafo 10 de la descripción en el cual se hace referencia a 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 al realizar la ejecución de las tareas en un orden específico.

Teniendo en cuenta las anteriores consideraciones, el argumento no es procedente y las reivindicaciones 1 a 8 no cumplen los requisitos de patentabilidad.

Argumentos relacionados con el nivel inventivo

El solicitante indica que "*D1 no describe la incrustación del parche en una extensión de certificado de un certificado de enlace emitido por una autoridad, ni los mecanismos de desempaquetado y verificación vinculados a las extensiones de certificado. De igual forma, D2 enseña actualizaciones criptográficamente seguras de chips, pero estas se transmiten como objetos de datos cifrados independientes. Ni D1 ni D2 sugieren incrustar un parche cifrado en una extensión de certificado digital ni vincularlo a la infraestructura PKI de una autoridad emisora, como se exige en las presentes reivindicaciones*."

Con respecto a lo anterior, es importante indicar que, el argumento sobre el cual es señor solicitante basa su argumento hace parte de la reivindicación independiente 1, la cual, no logra superar los requisitos establecidos en el artículo 14 de la Decisión 486, en consecuencia, el argumento no es procedente.

El solicitante indica que "*Asimismo, las reivindicaciones 11 y 12 especifican que el chip de circuito integrado incluye claves de fabricante preinstaladas (ya sea una clave privada o una clave secreta compartida) que se utilizan para descifrar el parche contenido en la extensión del certificado. Las reivindicaciones D1 y D2 no divulgan dicho paso de personalización durante la fabricación para vincular el proceso de entrega del parche de extremo a extremo entre el fabricante y el chip. Esto representa una distinción técnica adicional con respecto a la técnica anterior citada*."

Con respecto a lo anterior, es fundamental indicar que la solicitud no logra superar el requisito de nivel inventivo, por lo tanto, el análisis va más allá de la simple comparación con los documentos D1 y D2. En análisis de nivel inventivo considera el aporte de la solicitud en el estado de la técnica, dicho aporte debe ir un paso más allá de lo que actualmente se conoce y que puede ser razonablemente entendible y aplicable por el técnico medio versado en la materia. De acuerdo con lo anterior, la reivindicación independiente 9 no logra superar el requisito de nivel inventivo toda vez que sus características técnicas esenciales no proporciona un efecto técnico sorprendente.

Adicionalmente, vale la pena resaltar que, el estado de la técnica representado por los documentos D1 y D2, sugiere las características técnicas esenciales reclamadas por el señor solicitante, de manera particular D1 sugiere las claves públicas, privadas y funcionalidades criptográficas en el párrafo 8 y 37. De igual manera, D2 menciona los certificados PKI para la instalación de parches en el párrafo 49, 53, 55 y en la reivindicación 6, en este punto es importante indicar que para el estado de la técnica no existe un efecto técnico sorprendente por el hecho de incluir que se desempaqueten y desencripten certificados digitales para su instalación, pues resultan ser inherentemente requeridos en el proceso y además son ampliamente utilizados. En consecuencia, el argumento no es procedente y la solicitud no cumple con los requisitos de patentabilidad.

El solicitante indica que "*Finalmente, las reivindicaciones 15 y 16 exigen que el chip de circuito integrado esté integrado en un documento electrónico de seguridad, específicamente un DVLM. Si bien las reivindicaciones D1 y D2 mencionan las tarjetas inteligentes en general, no abordan las restricciones particulares de los DVLM, que operan bajo estrictos procedimientos de validación de certificados de la OACI y la norma BSI TR-03110. La integración reivindicada de la aplicación de parches con las infraestructuras PKI de los MRTD proporciona, por lo tanto, una mejora técnica especialmente adecuada para entornos offline de alta seguridad, como los pasaportes electrónicos*."

Ref. Expediente N° NC2021/0008019

Con respecto a las reivindicaciones 15 y 16, es importante indicar que, dichas reivindicaciones no hacen referencia a tarjetas del tipo DVLM, OACI y la norma BSI TR-03110, por lo tanto, dichas características no son tenidas en cuenta en el momento de la presente decisión, adicionalmente, las reivindicaciones 15 y 16 son reivindicaciones que dependen de las reivindicaciones independiente 9 que, al no cumplir con los requisitos de patentabilidad, su afectación se extiende a aquellas reivindicaciones que dependan de ella. En consecuencia, el argumento no es procedente y la solicitud no cumple con los requisitos de patentabilidad.

Que de acuerdo con la modificación presentada por el solicitante en el escrito radicado bajo el N° NC2021/0008019 el 26 de agosto de 2025 y teniendo en cuenta el objeto de la solicitud, se modifica el título de la invención el cual quedará de la siguiente manera: “CHIP DE CIRCUITO INTEGRADO Y PARCHE ENCRIPTADO”.

En conclusión, teniendo en cuenta que los argumentos del solicitante no desvirtúan de manera alguna las objeciones a la patentabilidad ya sustentadas, el Superintendente de Industria y Comercio,

RESUELVE

ARTÍCULO 1: Denegar la patente de invención a la solicitud que entró en fase nacional en virtud del Tratado de Cooperación en Materia de Patentes (PCT), para la creación titulada:

“CHIP DE CIRCUITO INTEGRADO Y PARCHE ENCRIPTADO”

ARTÍCULO 2: Notificar el contenido de la presente resolución a THALES DIS FRANCE SA, advirtiendo que contra ella procede el recurso de reposición, ante la Superintendente de Industria y Comercio, el cual podrá ser interpuesto en el momento de la notificación o dentro de los diez (10) días hábiles siguientes a ella.

NOTIFÍQUESE Y CÚMPLASE

Dada en Bogotá D.C., el 24 de noviembre de 2025

LA SUPERINTENDENTE DE INDUSTRIA Y COMERCIO,

Firmado digitalmente por: CIELO ELAINNE RUSINQUE URREGO
Fecha: 2025.11.24 17:01:59 COT
Razón: Validez juridica.
Ubicación: Bogotá, Colombia.