Señores
DIRECCION DE NUEVAS CREACIONES
SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO
Bogotá, D.C.

Re.: Expediente No. NC2021/0008019
Fase nacional de Solicitud PCT
THALES DIS FRANCE SA

En relación con el expediente de la referencia y dando cumplimiento a la última providencia recaída sobre este asunto por medio del presente escrito me permito manifestarles lo siguiente:

1. Mi representada acepta la sugerencia del Examinador para modificar el título de esta solicitud, por lo que el mismo queda como

CHIP DE CIRCUITO INTEGRADO Y PARCHE ENCRIPTADO

2. 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.

La reivindicación independiente 1 se refiere a un método para operar un chip de circuito integrado que comprende pasos técnicos definidos, incluyendo el cifrado de un parche, la transmisión del parche cifrado, su incorporación a un certificado digital, la comunicación con un terminal, el desempaquetado, la verificación de extensiones, el descifrado y la instalación del parche en el sistema operativo del chip de circuito integrado. Estos pasos no constituyen un "uso" abstracto ni un ejercicio intelectual, sino operaciones técnicas concretas realizadas por los componentes de hardware y software de un servidor de parches, un servidor de la autoridad emisora, un terminal y el propio chip de circuito integrado.

Contrariamente a la opinión del Examinador, los pasos reivindicados son ejecutados por el chip de circuito integrado y la infraestructura del sistema asociada, no simplemente por la actividad intelectual de un usuario externo. El término "operar", tal como se utiliza en las reivindicaciones, no implica intervención humana manual, sino que se refiere a la ejecución de operaciones técnicas definidas por los procesadores y las unidades de memoria de los dispositivos involucrados, como se describe expresamente en los párrafos [0009]-[0013] y se detalla en las figuras 3-10 de la descripción. El chip de circuito integrado realiza de forma autónoma el desempaquetado, la verificación, el descifrado y la instalación del parche basándose en claves criptográficas preinstaladas, lo cual constituye claramente un proceso técnico en el ámbito de aplicación del Artículo 14.

En consecuencia, las reivindicaciones 1-8 no buscan protección para un mero "uso", sino para una invención de proceso que proporciona un mecanismo seguro y verificable para aplicar parches al sistema operativo de un chip de circuito integrado mediante validación criptográfica basada en certificados. Este

proceso técnico produce un efecto técnico tangible —a saber, la actualización segura en terreno de los chips de los documentos de seguridad electrónicos, como los documentos de viaje legibles por máquina— que no se puede lograr mediante la mera actividad intelectual humana.

3. **Nivel Inventivo**

Mi representada rechaza respetuosamente las objeciones sobre las reivindicaciones 9 a 16 en vista de D1 (US2008022380A1) y D2 (US2004198496A1). Si bien tanto D1 como D2 describen técnicas de actualización segura para chips de circuitos integrados, ninguna de las referencias, por sí sola ni en combinación, enseña ni sugiere las características específicas requeridas por las presentes reivindicaciones.

La reivindicación independiente 9 describe un chip de circuito integrado configurado para recibir un certificado digital que incluye una extensión con un parche cifrado, descomprimir el certificado, verificar la correspondencia de la extensión con su sistema operativo, descifrar la extensión e instalar el parche. Las reivindicaciones dependientes 10 a 16 especifican además la verificación de una firma digital antes de la instalación del parche, el uso de claves de fabricante preinstaladas (ya sea un par de claves privadas y públicas o una clave secreta compartida), la incorporación del parche cifrado en un certificado de enlace con un identificador de objeto que especifica el fabricante, y la integración del chip de circuito integrado en un documento de seguridad electrónico, en particular un documento de viaje legible por máquina (MRTD).

D1 generalmente describe la actualización de chips IC seguros y menciona el uso de cifrado y firmas digitales para autenticar parches. Sin embargo, 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.

Por el contrario, la presente invención exige explícitamente que el parche cifrado se inserte en una extensión de un certificado digital, como un certificado de enlace de una autoridad de certificación de verificación de país (CCVCA). Este mecanismo garantiza que la entrega del parche se valide inherentemente dentro de la cadena de confianza de certificados existente utilizada en los MRTD, algo que ni D1 ni D2 abordan. Además, la reivindicación 14 exige la inclusión de un identificador de objeto en la extensión del certificado que identifique de forma única al fabricante, garantizando así que solo los chips autorizados apliquen el parche, mientras que los chips no autorizados lo ignoren. Esta característica de aplicabilidad selectiva no se encuentra en la técnica citada.

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.

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.

Por consiguiente, la combinación de D1 y D2 no hace evidente el objeto reivindicado. Las características distintivas —a saber, la entrega de parches cifrados dentro de las extensiones de certificado, el uso de identificadores de objeto específicos del fabricante, la dependencia de claves de fabricante preinstaladas y la adaptación a los MRTD— proporcionan, en conjunto, una solución segura y eficiente al problema de la aplicación de parches in situ en documentos electrónicos seguros. Por lo tanto, las reivindicaciones 9 a 16 implican actividad inventiva.

En consecuencia, de conformidad con los argumentos arriba expuestos se puede concluir que la materia reclamada en las reivindicaciones 1-16 cumplen con los requisitos de patentabilidad exigidos por la Decisión 486.

Renuncio al término faltante de traslado, y les solicito otorgar el privilegio de patente de invención aquí tramitado.

De Ustedes Atentamente,

LUIS FELIPE CASTILLO GIBSONE
T.P. No. 68995 del C.S.J.