

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. De conformidad con precisas instrucciones de mi representada se adjunta un nuevo capítulo reivindicatorio, el cual ha 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.

2. 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**

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

De Ustedes Atentamente,

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

Reivindicaciones Modificadas

1. Un sistema para parchear un sistema operativo de un chip de circuito integrado que comprende un primer certificado digital de una autoridad emisora, el cual sistema comprende:
 - un servidor de parches configurado para encriptar un parche al sistema operativo del chip de circuito integrado;
 - transmitir el parche encriptado al servidor de la autoridad emisora;
 - un servidor de la autoridad emisora configurado para anexar el parche encriptado dentro de un segundo certificado digital de la autoridad emisora en una extensión al segundo certificado digital;
 - transmitir el segundo certificado digital que incluye el parche encriptado al terminal;
 - una terminal para parchar de forma segura el sistema operativo del chip de circuito integrado, en donde el terminal está configurado para que se comuniquen con el chip de circuito integrado tras la presentación del chip de circuito integrado al terminal;
 - transmitir el segundo certificado digital que incluye el parche encriptado al chip de circuito integrado;
 - el chip de circuito integrado configurado para desempaquetar el segundo certificado digital que incluye el parche encriptado para recuperar la extensión del segundo certificado digital; y
 - verificar que la extensión al segundo certificado digital corresponde al sistema operativo del chip de circuito integrado; y si se verifica que la extensión corresponde al sistema operativo del chip de circuito integrado, desencriptar la extensión al segundo 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.
2. El sistema de acuerdo con la reivindicación anterior, que además comprende:
 - el servidor de parches configurado para firmar digitalmente el parche encriptado; y
 - el chip de circuito integrado configurado para verificar la firma digital del parche encriptado antes de instalar el parche en el sistema operativo del chip de circuito integrado.
3. El sistema de cualquiera de las reivindicaciones anteriores, que además comprende previamente la instalación de una clave privada del fabricante del chip de circuito integrado en el chip de circuito integrado; y que se caracteriza porque el servidor de parches encripta el parche utilizando la clave pública correspondiente a la clave privada

del fabricante del chip de circuito integrado, y que se caracteriza porque el chip de circuito integrado descripta la extensión al certificado digital utilizando la clave privada del fabricante.

4. El sistema de cualquiera de las reivindicaciones anteriores 1 a 2, que además comprende previamente la instalación de una clave secreta del fabricante del chip de circuito integrado en el chip de circuito integrado; y que se caracteriza porque el servidor de parches encripta el parche utilizando la clave secreta correspondiente a la clave secreta del fabricante del chip de circuito integrado, y que se caracteriza porque el chip de circuito integrado descripta la extensión al certificado digital utilizando la clave secreta del fabricante.
5. El sistema de cualquiera de las reivindicaciones anteriores, que se caracteriza porque el segundo certificado digital de la autoridad emisora es un certificado de enlace que enlaza con el primer certificado de la autoridad del certificado almacenada en el chip de circuito integrado.
6. El sistema de cualquiera de las notificaciones anteriores, que se caracteriza porque el certificado de enlace es un país que verifica el certificado de enlace de la autoridad de certificación y la extensión al certificado de enlace contiene un identificador de objeto que indica que el fabricante del chip de circuito integrado ha originado la extensión al certificado de enlace.
7. El sistema de cualquiera de las reivindicaciones anteriores, que se caracteriza porque el chip de circuito integrado está incrustado en un documento de seguridad electrónico.
8. El sistema de cualquiera de las reivindicaciones anteriores, que se caracteriza porque el documento de seguridad electrónico es un documento de viaje legible por máquina.
9. Un chip de circuito integrado que comprende:
 - 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: 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;
 - desempaquetar el certificado digital recuperando así la extensión al certificado digital;
 - verificar que la extensión al certificado digital corresponde al sistema operativo del chip de circuito integrado; y si se verifica que la extensión corresponde al sistema operativo del chip de circuito integrado, descriptar 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.

10. El chip de circuito integrado de la reivindicación 9, en donde las instrucciones del cargador de parches además comprenden instrucciones para hacer que el procesador verifique la firma digital del parche encriptado antes de instalar el parche en el sistema operativo del chip de circuito integrado.
11. El chip de circuito integrado de las reivindicaciones 9 o 10, que se caracteriza porque la memoria incluye además una clave privada del fabricante del chip de circuito integrado; y que se caracteriza porque el parche se encripta utilizando la clave pública correspondiente a la clave privada del fabricante del chip de circuito integrado, y que se caracteriza porque las instrucciones además comprenden instrucciones para hacer que el procesador descripte la extensión al certificado digital utilizando la clave privada del fabricante.
12. El chip de circuito integrado de las reivindicaciones 9 o 10, que se caracteriza porque la memoria incluye además una clave secreta del fabricante del chip de circuito integrado; y que se caracteriza porque el parche es encriptado usando la clave secreta compartida; y que se caracteriza porque las instrucciones además comprenden instrucciones para hacer que el procesador descripte la extensión al certificado digital utilizando la clave secreta compartida del fabricante.
13. El chip de circuito integrado de cualquiera de las reivindicaciones 9 a 12, que se caracteriza porque el segundo certificado digital de la autoridad emisora es un certificado de enlace que enlaza con el primer certificado de la autoridad del certificado almacenada en el chip de circuito integrado.
14. El chip de circuito integrado de la reivindicación 13, que se caracteriza porque el certificado de enlace es un certificado de enlace de autoridad del certificado que verifica el país y la extensión al certificado de enlace contiene un identificador de objeto que indica que el fabricante del chip de circuito integrado ha originado la extensión al certificado de enlace.
15. El chip de circuito integrado de cualquiera de las reivindicaciones 9 a 14, que se caracteriza porque el chip de circuito integrado está empotrado en un documento de seguridad electrónico.
16. El chip de circuito integrado de cualquiera de las reivindicaciones 9 a 15, que se caracteriza porque el documento electrónico de seguridad es un documento de viaje legible por máquina.