REIVINDICACIONES

1. Un método para operar un chip de circuito integrado que comprende un primer certificado digital de una autoridad emisora, un servidor de parches, un servidor de la autoridad emisora y un terminal para parchar de forma segura un sistema operativo del chip de circuito integrado, el cual método comprende:

   operar el servidor de parches para encriptar un parche al sistema operativo del chip de circuito integrado;

   operar el servidor de parches para transmitir el parche encriptado al servidor de la autoridad emisora;

   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 al segundo certificado digital;

   operar el servidor de la autoridad emisora para transmitir el segundo certificado digital que incluye el parche encriptado al terminal;

   operar el terminal para que se comunique con el chip de circuito integrado tras la presentación del chip de circuito integrado al terminal;

   operar el terminal para transmitir el segundo certificado digital que incluye el parche encriptado al chip de circuito integrado;

   operar el chip de circuito integrado para desempaquetar el segundo certificado digital que incluye el parche encriptado para recuperar la extensión del segundo certificado digital; y

   operar el chip de circuito integrado para 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 método de acuerdo con la reivindicación anterior, que además comprende:

   operar el servidor de parches para firmar digitalmente el parche encriptado; y

   operar el chip de circuito integrado para verificar la firma digital del parche encriptado antes de instalar el parche en el sistema operativo del chip de circuito integrado.

3. El método de cualquiera de las reivindicaciones anteriores, que además comprende una medida preliminar de 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 desencripta la extensión al certificado digital utilizando la clave privada del fabricante.

4. El método de cualquiera de las reivindicaciones anteriores 1 a 2, que además comprende un paso preliminar de 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 desencripta la extensión al certificado digital utilizando la clave secreta del fabricante.
5. El método 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 método 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 método 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 método 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, 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.

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 desencripte 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 desencripte 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.