UN CHIP DE CIRCUITO Y UN MÉTODO PARA OPERARLO

ANTECEDENTES DE LA INVENCIÓN

[0001] La presente invención se refiere, en general, a chips de circuito integrados y, más particularmente, a la actualización segura del sistema operativo de chips de circuito integrados empotrados.

[0002] Los chips de circuito integrado seguros como, por ejemplo, los que se encuentran en las tarjetas inteligentes, son un mecanismo cada vez más importante para mejorar la seguridad de muchos dispositivos. Por ejemplo, todo el tiempo que los pasaportes han existido ha habido quienes los falsifiquen. En un antiguo juego del gato y el ratón, los emisores de pasaportes han tratado de mejorar la seguridad de estos documentos mediante la introducción de características de seguridad que son cada vez más difíciles de falsificar en tanto que los falsificadores buscan desarrollar técnicas para violar esas características de seguridad. Un mecanismo para mejorar la seguridad de los pasaportes ha sido la introducción de los pasaportes electrónicos, es decir, aquellos que contienen un chip de circuito integrado seguro.

[0003] Los chips de circuito integrados seguros son circuitos integrados resistentes a manipulaciones que incluyen muchas características de seguridad. A menudo, estos chips se utilizan para almacenar información confidencial, como números de cuenta, credenciales de inicio de sesión, claves criptográficas, información personal del usuario, incluida la biometría.

[0004] Aunque los chips de circuito integrado seguros contienen muchas características de seguridad para mejorar su resistencia a la manipulación, todavía están sujetos a ataques de falsificadores y piratas informáticos que buscan hacerse pasar por usuarios legítimos de los chips o acceder ilícitamente a la información almacenada en los chips. Por tanto, así como los fabricantes de documentos de seguridad de la vieja escuela agregaron nuevas características de seguridad, los fabricantes de chips de circuito integrado seguros de vez en cuando deben de añadir nuevas características de seguridad para mejorar la seguridad de sus chips de circuito integrados seguros. Por ejemplo, si una falla de seguridad se expone en un algoritmo criptográfico, es posible que el fabricante del chip tenga que proporcionar una corrección del algoritmo que corrige el falla de seguridad identificada.

[0005] Una ventaja de los documentos electrónicos y otros dispositivos computarizados es la posibilidad de agregar nuevas características y funcionalidades a un documento o dispositivo. Por ejemplo, si un banco introduce un nuevo servicio, puede ser necesario agregar una nueva característica correspondiente al nuevo servicio a una tarjeta bancaria en poder de los clientes del banco.

[0006] Los usuarios de los modernos computadores o dispositivos electrónicos en red están familiarizados, e incluso esto puede molestarles, con la invitación casi diaria a instalar un parche de software de algún tipo. De hecho, con frecuencia este tipo de parches son anunciados por el sistema operativo o el emisor del programa de aplicaciones como un “parche de seguridad crítico.” Este parcheo a través de la red es relativamente trivial para los dispositivos en red; un sistema operativo o programa de aplicaciones puede tener un mecanismo integrado para preguntar a través de la red con un servidor de parches para determinar si hay un parche disponible que debería o podría instalarse.

[0007] Sin embargo, en el caso de los dispositivos electrónicos que no se conectan a una red aplicar los parches de software es mucho más difícil. Considere, por ejemplo, una actualización crítica de seguridad de un pasaporte electrónico. El pasaporte electrónico, como muchos otros dispositivos, no suele estar en comunicación con un servidor a través de una red. Además, incluso si está conectado a una red, es esencial poder confiar en que cualquier parche propuesto no se haya originado en una fuente insegura o maliciosa.

[0008] De lo anterior resulta evidente que existe la necesidad de un método mejorado para proporcionar una actualización segura del sistema operativo y otros programas instalados en chips de circuito integrado seguros.

RESUMEN

[0009] 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. El servidor de la autoridad emisora transmite el segundo certificado digital que incluye el parche encriptado al terminal. El terminal se

comunica con el chip de circuito integrado tras la presentación del chip de circuito integrado al terminal.

[0010] Para lograr esas y otras ventajas, y de conformidad con el propósito de la invención tal como se realiza y describe ampliamente, la invención propone 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.

[0011] El terminal transmite el segundo certificado digital que incluye el parche encriptado al chip de circuito integrado.

[0012] El chip de circuito integrado desempaqueta el segundo certificado digital que incluye el parche encriptado para recuperar la extensión del segundo certificado digital y

verifica que la extensión al segundo certificado digital corresponde al sistema operativo del chip de circuito integrado. Si se verifica que la extensión corresponde al sistema operativo del chip de circuito integrado, el chip de circuito integrado desencripta la extensión al segundo certificado digital recuperando así el parche al sistema operativo del chip de circuito integrado e instalando el parche en el sistema operativo del chip de circuito integrado.

[0013] En un aspecto, el servidor de parches firma digitalmente el parche encriptado y 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.

[0014] En otro aspecto, se instala una clave 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 una clave del fabricante del chip de circuito integrado, y el chip de circuito integrado desencripta la extensión al certificado digital utilizando una clave del fabricante.

[0015] El segundo certificado digital de la autoridad emisora puede ser un certificado de enlace como, por ejemplo, un certificado de enlace de un país que verifica la autoridad del certificado, que enlaza con el primer certificado de la autoridad del certificado almacenado en el chip de circuito integrado.

[0016] En un aspecto, el chip de circuito integrado está empotrado en un documento de seguridad electrónico.

[0017] En otro aspecto, el documento electrónico de seguridad es un documento de viaje legible por una máquina.

[0018] En un aspecto, se instala 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.

[0019] En un aspecto, se instala 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.

[0020] La presente invención también está relacionada con 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 instalando el parche en el sistema operativo del chip de circuito integrado.

[0021] En un aspecto, 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.

[0022] En un aspecto, 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.

[0023] En un aspecto, 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.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

[0024] La FIG. 1 es una ilustración de una portada de una libreta de pasaporte.

[0025] La FIG. 2 es una ilustración de una página de un pasaporte electrónico que incluye un chip de circuito integrado como una incrustación en la página.
[0026] La FIG. 3 es un diagrama de bloques de alto nivel de una arquitectura del chip de circuito integrado de la FIG. 2.
[0027] La FIG. 4 es un diagrama de bloques que ilustra datos y programas almacenados en una memoria que corresponde a la memoria de la FIG. 3.
[0028] La FIG. 5 es un diagrama de red que ilustra el flujo de un parche de un servidor del fabricante a un dispositivo o documento que contiene un chip de circuito integrado 203 (que no se muestra) a través de una red.
[0029] La FIG. 6 es un esquema de programas y datos que pueden incluirse en una memoria de un chip de circuito integrado de un pasaporte electrónico.
[0030] La FIG. 7 es una ilustración esquemática de un certificado digital que tiene un cuerpo del certificado y una parte de extensiones del certificado.
[0031] La FIG. 8 es una ilustración esquemática de una parte de extensiones del certificado para una modalidad de pasaporte electrónico.
[0032] La FIG. 9 es un diagrama de flujo de datos que ilustra la población de claves requeridas en un chip de circuito integrado, correspondiente a un chip de circuito integrado de la FIG. 2.
[0033] La FIG. 10, que está compuesta por las FIG.10a y 10b, es un diagrama de flujo de datos de la fase de uso del ciclo de vida de un chip de circuito integrado.

DESCRIPCIÓN DETALLADA DE LA INVENCIÓN

[0034] En la siguiente descripción detallada se hace referencia a los dibujos que acompañan que muestran, a modo de ilustración, modalidades específicas en las que se puede practicar la invención. Estas modalidades se describen con suficiente detalle para permitir a la persona medianamente versada en la materia técnica correspondiente practicar la invención. Debe entenderse que las diversas modalidades de la invención, aunque diferentes, no por fuerza son mutuamente excluyentes. Por ejemplo, una característica, estructura o característica particular descrita en este documento en relación con una modalidad puede aplicarse dentro de otras modalidades sin apartarse del espíritu y el alcance de la invención. Además, debe entenderse que la ubicación o disposición de elementos individuales dentro de cada modalidad divulgada puede modificarse sin apartarse del espíritu y el alcance de la invención. Por consiguiente, la siguiente

descripción detallada no debe tomarse en un sentido limitante, y el alcance de la presente invención solo se define mediante las reivindicaciones anexadas, interpretadas adecuadamente, junto con toda la gama de equivalentes a los que las reivindicaciones tienen derecho. En los dibujos, los numerales iguales se refieren a la misma o similar funcionalidad en las varias vistas.

[0035] La siguiente descripción incluye referencias a varios métodos ejecutados por un procesador de un chip de circuito integrado. Como es común en el campo, puede haber frases aquí que indican que estos métodos o pasos del método son realizados por instrucciones de software o módulos de software. Como lo sabe la persona medianamente versada en la materia técnica correspondiente, tales descripciones deben tomarse como que significan que un procesador, de hecho, ejecuta los métodos, las instrucciones de software y los módulos de software.

[0036] La tecnología aquí descrita proporciona un mecanismo seguro de actualización de software en el campo para chips de circuito integrados seguros.

[0037] La FIG. 1 es una ilustración de una portada de una libreta de pasaporte 100. Un símbolo 101 indica que el pasaporte es un pasaporte electrónico que contiene un chip de circuito integrado que puede ser leído por una terminal en una estación fronteriza de control de pasaportes.

[0038] La FIG. 2 es una ilustración de una página 201 de un pasaporte electrónico 100 que incluye un chip de circuito integrado 203 como incrustación en la página 201. La página 201 también contiene una antena 205 conectada al chip de circuito integrado 203 a través de la cual el chip de circuito integrado 203 se comunica con las terminales.

[0039] La FIG. 3 es un diagrama de bloques de alto nivel de una arquitectura del chip de circuito integrado 203 y la antena 205. El chip de circuito integrado 203 contiene un procesador 301 y una estructura de memoria 303, la cual almacena datos y programas ejecutables por el procesador 301. La estructura de memoria 303 puede contener una o más de cada una de una memoria de acceso aleatorio (RAM) 305, memoria de solo lectura (ROM) 307 y memoria programable no volátil (NVM) 309. Los dispositivos de memoria 305, 307 y 309 están conectados al procesador 301 a través de un bus 311.

[0040] El chip de circuito integrado 203 contiene además una interfaz de entrada/salida 313 para comunicarse con dispositivos externos, por ejemplo, un terminal, a través de la antena 205. Para la comunicación sin contacto, la interfaz de entrada/salida 313 puede comunicarse con un terminal a través del protocolo ISO 14443.

[0041] En modalidades alternativas, el chip de circuito integrado 203 puede incluir contactos eléctricos (que no se muestran) para comunicarse a través de una interfaz de contacto con un terminal, por ejemplo, de acuerdo con el protocolo ISO-7816 o el protocolo de bus de serie universal (USB).

[0042] La FIG. 4 es un diagrama de bloques que ilustra datos y programas almacenados en una memoria 403 que corresponde a la memoria 303 de la FIG. 3. En una modalidad preferida, los datos y programas que se ilustran almacenados en la memoria 403 se almacenan en una NVM 409 que corresponde a la NVM 309 de la FIG. 3. Sin embargo, otras organizaciones de memoria son posibles.

[0043] La memoria 403 contiene programas 401 y datos de personalización 451. Los programas 401 son instrucciones de programas informáticos que hacen que el procesador 301 lleve a cabo ciertas acciones. Los programas 401 incluyen un sistema operativo 405 y programas de aplicaciones 407.

[0044] El sistema operativo 405, a su vez, contiene una variedad de funciones del sistema operativo 409 y un cargador de parches 411. Las funciones del sistema operativo 409 pueden incluir, por ejemplo, una máquina virtual para ejecutar los programas de aplicación 407 y las funciones de gestión de memoria.

[0045] El cargador de parches 411, que se describe con mayor detalle a continuación, realiza funciones relacionadas con recibir un parche, verificar que el parche tiene su origen en el fabricante del chip de circuito integrado 203 (o en otra fuente de confianza), desencriptar un parche encriptado e instalar el parche en el sistema operativo 405.

[0046] La FIG. 5 es un diagrama de red que ilustra el flujo de un parche 507 de un fabricante 501 a un dispositivo o documento 503 que contiene un chip de circuito integrado 203 (que no se muestra) a través de una red 505. El fabricante, por ejemplo, el fabricante del chip de circuito integrado 203 crea un parche 507 para el sistema operativo 409. El fabricante encripta y firma el parche y transmite el parche encriptado firmado 509 a un emisor de dispositivos ICC 511, por ejemplo, una autoridad nacional de emisión de pasaportes.

[0047] El emisor del dispositivo ICC 513 incorpora el parche encriptado firmado 509 en un certificado digital 513, por ejemplo, un certificado de enlace que vincula un certificado digital vencido o expirado a un certificado digital de reemplazo, y transmite el certificado digital 513 a un terminal 515, por ejemplo, un terminal verificador de pasaportes operado en un control de pasaportes en una frontera nacional o puerto de entrada.

[0048] Un portador del dispositivo 503 como, por ejemplo, un viajero que lleva un pasaporte electrónico presenta el dispositivo 503 al terminal 515. Se establece un enlace de comunicaciones entre el dispositivo 503 y el terminal. El enlace de comunicaciones puede ser un enlace de comunicaciones basado en contacto que funcione, por ejemplo, con el protocolo ISO 7816 o el protocolo del bus de serie universal, o un enlace de comunicaciones sin contacto como, por ejemplo, comunicación de campo cercano (NFC) o comunicación a través del protocolo ISO/IEC 14443.

[0049] El terminal 515 entonces transmite el certificado digital 513 al dispositivo 503 como parte de un proceso de autenticación de terminal 517.

[0050] Volviendo ahora a la FIG. 4, el cargador de parches 411 recibe un parche que está firmado y encriptado por la autoridad del emisor a través de un terminal. Al recibir el parche firmado y encriptado, el cargador de parches 411 verifica el origen del parche, desencripta el parche e instala el parche en el sistema operativo 405.

[0051] Si bien los mecanismos descritos en este documento se aplican al parcheo del sistema operativo 405, los mecanismos también se pueden utilizar en los programas de aplicación de parches 407. De hecho, el límite entre los programas de aplicación 407 y el sistema operativo 405 puede ser bastante borroso en algunos entornos.

[0052] Los datos de personalización 451 pueden incluir datos de usuario 453, claves del sistema 455 y claves de parche 457. Los datos de usuario 453 pueden incluir información biográfica como nombre y fecha de nacimiento, datos biométricos como fotografías, huellas dactilares y escaneos de retina, información de la cuenta y claves de usuario. Las claves del sistema 455 pueden incluir certificados raíz. Las claves de parche 457 incluyen claves que se utilizan para comprobar el origen de un archivo de parche y desencriptar un archivo de parche.

[0053] La FIG. 6 es un esquema de programas y datos que pueden incluirse en una memoria 603 (por ejemplo, NVM 609) de un chip de circuito integrado de un pasaporte electrónico 100 en donde la memoria 603 y la NVM 609 corresponden a la memoria 303 y la NVM 309 de la FIG. 3, así como la memoria 403 y la NVM 409 de la FIG. 4, respectivamente, y contiene los programas 601, correspondientes a los programas 401 de la FIG. 4, incluido un sistema operativo 609.

[0054] Para un pasaporte electrónico, el sistema operativo 609 puede incluir varias funciones de pasaporte electrónico, como control de acceso básico (BAC) 613, autenticación activa 615, establecimiento de conexión de autenticación de contraseña 617, autenticación de chip 619 y autenticación de terminal 621. Estas funciones del

pasaporte electrónico se describen en Bundesamt für Sicherheit in der Informationstechnik, BSI TR- 03110 Technical Guideline Advanced Security Mechanisms for Machine Readable Travel Documents y el Token DAS, https://www.bsi.bund.de/EN/Publications/TechnicalGuidelines/TR03110/BSITR03110.html, que se consultó el 30 de octubre de 2018 (en lo sucesivo, "TR-03110") y en la Organización de Aviación Civil Internacional (OACI), Doc. 9303, Documentos de viaje legibles por máquina, https://www.icao.int/publications/pages/publication.aspx?docnum=9303, consultado el 30 de octubre de 2018.

[0055] El sistema operativo 609 incluye además el cargador de parches 611, que corresponde al cargador de parches 411 de la FIG. 4.

[0056] Para una modalidad de pasaporte electrónico como la que se ilustra en la FIG. 6, el programa de aplicación 407 de la FIG. 4 puede ser una aplicación de pasaporte 607, la cual puede conceder acceso a los datos de usuario 653 dependiendo del contexto de autenticación 613, 617, 621.

[0057] Como se discutió en relación con la FIG. 4, los datos de personalización pueden contener cierta información personal 653. En el contexto de los pasaportes electrónicos esto puede incluir el número de pasaporte, así como la información de viaje.

[0058] Un pasaporte electrónico realiza varias funciones de verificación como, por ejemplo, autenticación del terminal 621, para verificar que la información confidencial almacenada en este no es obtenida por una entidad que no tiene la autorización necesaria para tener acceso a esa información. Un mecanismo consiste en verificar que los certificados proporcionados por el terminal han sido firmados por una autoridad del certificado confiable. Para ello, el chip de circuito integrado de un pasaporte electrónico contiene un certificado de autoridad de certificación del país que verifica (CCVCA) 659 en las claves del sistema 655.

[0059] El cargador de parches 611 verifica el parche encriptado firmado utilizando una clave de firma pública del fabricante (PKMansign) 661 y si la verificación es positiva, el cargador de parches desencripta el parche encriptado 509 utilizando una clave secreta del fabricante (S KMan) 663. La clave secreta del fabricante (S KMan) 663 puede ser una clave secreta compartida o una clave privada de un clavedo PKI (Public Key Infrastructure).

[0060] La autoridad emisora 511 incorpora el parche encriptado firmado en un certificado digital 513. La FIG. 7 es una ilustración esquemática de un certificado digital 701 que tiene un cuerpo del certificado 703 y una parte de extensiones del certificado 705.

[0061] El organismo certificador 703 puede contener una clave pública de una autoridad del certificado y cierta otra información pertinente como, por ejemplo, fechas de validez.

[0062] La parte 705 de extensiones del certificado contiene una o más extensiones del certificado 707 cada una de las cuales se ciñe a una plantilla prestablecida. Una extensión del certificado 707 se introduce mediante un identificador de objeto 709 seguido de una secuencia de objetos de datos dependientes del contexto 711. El identificador de objeto 709 puede identificar a cuál chip de circuito integrado pertenece la extensión 707, por ejemplo, el fabricante del chip de circuito integrado, de modo que los chips de circuito integrados a los que no se aplica la extensión 707 puedan ignorar la extensión 707.

[0063] En una modalidad, la parte de extensiones del certificado 705 y las extensiones del certificado 707 se ciñen al formato descrito en Bundesamt für Sicherheit in der Informationstechnik, BSI TR-03110 Directriz técnica: Mecanismos avanzados de seguridad para documentos de viaje legibles por máquina y token elDAS, Parte 3: Especificaciones comunes, https://www.bsi.bund.de/EN/Publications/TechnicalGuidelines/TR03110/BSITR03110.html, consultadas el 30 de octubre de 2018 (incorporadas aquí mediante referencia) en las páginas 89-90.

[0064] La FIG. 8 es una ilustración esquemática de una parte de extensiones del certificado 805, correspondiente a la parte de extensiones del certificado 705 de la FIG. 7, por ejemplo, para una modalidad de pasaporte electrónico. La parte de extensiones del certificado 805 incluye una extensión de certificado 807 que tiene un identificador de objeto 809 que identifica la extensión como un parche que se origina en Claire Greystone Enterprises Corporation (CGE Corp., una sociedad ficticia). Los chips de circuito integrados que no se originan en CGE Corp. pueden ignorar la extensión 807. De hecho, estos otros ICC no tendrían las claves necesarias para desencriptar el parche. La extensión de certificado 807 incluye además el parche encriptado y la firma 811.

[0065] La FIG. 9 es un diagrama de flujo de datos que ilustra la población de claves requeridas en un chip de circuito integrado 907, correspondiente a un chip de circuito integrado 203 de la FIG. 2. Como se señaló anteriormente, el parcheo de un chip de circuito integrado incluye cuatro nodos: El servidor de fabricación 901 operado por un fabricante 501, un servidor de la autoridad emisora 903 operado por el emisor de chip de

circuito integrado 511, el terminal 905 correspondiente al terminal 515, y el chip de circuito integrado 907 correspondiente al chip de circuito integrado 203. Los chips de circuito integrados pasan por varias fases durante su ciclo de vida. Una primera fase es la fase de fabricación 909 durante la cual el fabricante genera claves de encriptado, desencriptado y firma, paso 911.

[0066] El chip de circuito integrado 907 desencripta el parche encriptado 509 utilizando la clave de desencriptado del fabricante. El encriptado y desencriptado del parche puede basarse en criptografía secreta compartida o PKI. En cualquiera de las dos, la clave de desencriptado es una clave secreta del fabricante y por tanto se representa aquí como SKMan 913. En una modalidad alternativa, el encriptado se realiza mediante una clave pública. En tal modalidad, el fabricante también puede generar y almacenar una clave pública del fabricante (PKMan) 915.

[0067] La firma del parche encriptado 509 y la verificación de la firma se realizan mediante PKI. Así, el fabricante genera un papel clave PKI, la clave de firma pública del fabricante (PKMansign) 917 y la correspondiente clave de firma secreta del fabricante (SKMansign) 919. El servidor del fabricante 901 transmite la clave PKManSign 917 y la clave SKMan 913 al chip de circuito integrado 907, paso 921, y el chip de circuito integrado 907 almacena las claves en la memoria del chip de circuito integrado 907, paso 923. Los pasos 921 y 923 de transmisión y almacenamiento se pueden realizar mediante una operación de escritura en la que el servidor del fabricante 901 escribe directamente en la memoria del chip de circuito integrado 907.

[0068] La fase de personalización y emisión 951 sigue la fase de fabricación 909 en el ciclo de vida de un chip de circuito integrado 203. Durante la personalización 951 el servidor de la autoridad emisora 903 obtiene información del usuario, paso 953, como, por ejemplo, información biográfica y biométrica asociada con el titular de la tarjeta, paso 955, la cual luego se transmite al chip de circuito integrado 907, que a su vez almacena la información del usuario, paso 957.

[0069] El servidor de la autoridad emisora 903 también transmite la clave pública (PKi_{SSAuth}) 959 de la autoridad emisora al chip de circuito integrado 907, paso 961. El chip de circuito integrado 907 almacena la clave PKi_{SSAuth} 959, paso 963. La clave pública PKi_{SSAuth} 959 puede ser un certificado digital. En una modalidad de pasaporte electrónico, la clave pública puede ser el certificado de la Autoridad de Certificación de País (CCVCA), como se describe en el documento TR-31110.

[0070] Las FIG. 10a y 10b se combinan para formar un diagrama de flujo de datos de la fase de uso 971 (que consiste en una primera porción 971a de la FIG. 10a y una segunda porción 971b de la FIG. 10b) del ciclo de vida de un chip de circuito integrado 907. Durante la fase de uso 971, el chip de circuito integrado 907 se ha incorporado a un dispositivo, por ejemplo, una tarjeta inteligente o un pasaporte electrónico. A su debido tiempo durante la fase de uso 971, el usuario, por ejemplo, un viajero, puede presentar el chip de circuito integrado 907, o más el dispositivo en el que se incorpora, a un terminal 905.

[0071] Durante el uso de un chip de circuito integrado 907, puede haber la necesidad o el deseo de actualizar el sistema operativo del chip de circuito integrado 907 mediante el desarrollo de parches del sistema operativo, paso 973.

[0072] Para asegurarse de que ese parche solo está disponible para un chip de circuito integrado autorizado 907 y no es accesible para ninguna otra parte, el servidor del fabricante 901 encripta el parche, paso 975. El encriptado puede estar utilizando una clave secreta compartida (SKMan) del fabricante:

$PATCH_{ENC} = E(SK_{MAN}, PATCH)$

O, de acuerdo con PKI, utilizando una clave pública (PKMan) del fabricante:

$PATCH_{ENC} = E(PK_{MAN}, PATCH)$

[0073] El servidor del fabricante 901 también firma el parche encriptado PA TCHENC produciendo un parche encriptado firmado (PA TCHSIGN), paso 977. El parche encriptado firmado se produce usando PKI mediante la firma con la clave de firma secreta del fabricante (SKMansign):

$PATCH_{SIGN}$ $SIGN(SK_{MANSIGN}PATCH_{ENC})$

[0074] El servidor del fabricante 901 transmite el parche encriptado firmado (PATCHSIGN) al servidor de la autoridad emisora 903, paso 979.

[0075] Opcionalmente, el servidor de la autoridad emisora 903 verifica la firma del parche encriptado firmado, paso 981. Si se produce un error en la verificación (ruta no ilustrada), se marca una condición de error y se realiza una acción correctiva de error como, por ejemplo, terminar el proceso o alertar a las autoridades pertinentes de un posible intento de infracción de seguridad.

[0076] Como alternativa, el servidor de la autoridad emisora 903 simplemente transmite (como se describe a continuación) el parche encriptado firmado a la ICC sin verificar la firma de la autoridad emisora.

[0077] Si la verificación de firma del paso 981 se realiza correctamente (o no se realiza), la autoridad emisora agrega el parche encriptado firmado (PATCHSIGN) a un certificado digital, por ejemplo, como extensión de certificado a un certificado de enlace (CERTUNK), paso 983, como se describe aquí arriba.

[0078] Continuando ahora con la FIG. 10B, el servidor de la autoridad emisora 903 transmite el certificado digital (CERTUNK) al terminal 905, paso 985.

[0079] Un usuario presenta el chip de circuito integrado 907 al terminal 905, paso 987. El terminal y el chip de circuito integrado 907 establecen un canal de comunicación.

[0080] Durante una fase de autenticación de terminal 989, el terminal 905 transmite el certificado digital al chip de circuito integrado 907, paso 991.

[0081] El chip de circuito integrado 907 desempaqueta el certificado digital, paso 993, para recuperar la extensión de certificado 707.

[0082] El chip de circuito integrado lee la etiqueta de identificador de objeto 709 de la extensión de certificado 707. Si la etiqueta de identificador de objeto 709 corresponde a la fabricación del chip de circuito integrado 907, el chip de circuito integrado continúa con la instalación del parche del sistema operativo que porta el certificado digital. De lo contrario, si la etiqueta de identificador de objeto 709 no corresponde a la fabricación del chip de circuito integrado 907, el chip de circuito integrado 907 ignora la extensión 707.

[0083] El chip de circuito integrado 907 verifica que el certificado digital 991 coincida con el fabricante 901 y que está firmado por una autoridad del certificado de confianza, paso 993. Si la verificación no tiene éxito, se marca una condición de error y se toman medidas correctivas (que no se ilustran).

[0084] La firma digital es una coincidencia para el fabricante del chip de circuito integrado 907, el chip de circuito integrado 907 desencripta el parche encriptado, paso 997:

$PATCH = D\ (SK_{MAN}PATCH_{ENC})$

[0085] Finalmente, el chip de circuito integrado 907 instala el parche en el sistema operativo 405.

[0086] De lo anterior se desprende que se proporciona un mecanismo eficiente y seguro para la instalación en el campo de parches del sistema operativo en un sistema operativo de un chip de circuito integrado.

[0087] Aunque se han descrito e ilustrado modalidades específicas de la invención, la invención no debe limitarse a las formas o disposiciones específicas de las partes así descritas e ilustradas. La invención solo está limitada por las reivindicaciones.

[0088] Lo que se reivindica es:

RESUMEN

Parcheo seguro de un sistema operativo del chip de circuito integrado. Un servidor de parches encripta un parche al sistema operativo del chip de circuito integrado y transmite el parche encriptado a un servidor de la autoridad emisora. El servidor de entidad de emisión anexa el parche encriptado a un certificado digital en una extensión del certificado digital y transmite el certificado digital que incluye el parche encriptado a un terminal. El terminal transmite el certificado digital del chip de circuito integrado. El chip de circuito integrado recupera la extensión al segundo certificado digital y desencripta la extensión utilizando una clave de desencriptado del fabricante del chip de circuito integrado recuperando así el parche al sistema operativo del chip de circuito integrado e instala el parche en el sistema operativo del chip de circuito integrado.