(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 986 847**

(51) Int. Cl.:

B42D 25/24 (2014.01)
B42D 25/305 (2014.01)
G06Q 10/10 (2013.01)
H04N 1/32 (2006.01)
G06Q 50/26 (2014.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **20.11.2019 PCT/EP2019/081955**

(87) Fecha y número de publicación internacional: **28.05.2020 WO20104537**

(96) Fecha de presentación y número de la solicitud europea: **20.11.2019 E 19804735 (9)**

(97) Fecha y número de publicación de la concesión europea: **22.05.2024 EP 3883782**

(54) Título: **Un chip de circuito integrado y un método para operarlo**

(30) Prioridad:

21.11.2018 EP 18306538

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
12.11.2024

(73) Titular/es:

THALES DIS FRANCE SAS (100.0%)
6, rue de la Verrerie
92190 Meudon, FR

(72) Inventor/es:

CHAPELLIER, SÉBASTIEN;
RANTI, MARIO-LOCAS;
WANG-ZW, JERVIS y
FOO, YONG JIE

(74) Agente/Representante:

DEL VALLE VALIENTE, Sonia

DESCRIPCIÓN

Un chip de circuito integrado y un método para operarlo

Antecedentes de la invención

La presente invención se refiere a un chip de circuito integrado y a un método para operarlo y, más particularmente, a la actualización segura del sistema operativo de los chips de circuito integrado integrados.

Los chips de circuito integrado seguros, p. ej., los que se encuentran en las tarjetas inteligentes, son un mecanismo cada vez más importante para mejorar la seguridad de muchos dispositivos. Por ejemplo, desde que ha habido pasaportes, ha habido falsificadores de pasaportes. Como en un antiguo juego del gato y el ratón, los emisores de pasaportes han intentado mejorar la seguridad de los pasaportes mediante la introducción de elementos de seguridad que son cada vez más difíciles de falsificar, mientras que los falsificadores buscan desarrollar técnicas para frustrar dichas características de seguridad. Un mecanismo para mejorar la seguridad de los pasaportes ha sido la introducción de los pasaportes electrónicos, es decir, pasaportes que contienen un chip de circuito integrado seguro.

Los chips de circuito integrado seguro son circuitos integrados a prueba de manipulaciones indebidas que incluyen muchas características de seguridad. Frecuentemente, dichos chips se utilizan para almacenar información confidencial, tal como números de cuenta, credenciales de inicio de sesión, claves criptográficas e información personal del usuario, incluida información biométrica.

Si bien los chips de circuito integrado seguros contienen muchas características de seguridad para mejorar su resistencia a la manipulación indebida, siguen siendo objeto de ataques por parte de falsificadores y piratas informáticos que buscan hacerse pasar por usuarios legítimos de los chips o acceder, de forma ilícita, a la información almacenada en los chips. Por lo tanto, al igual que los fabricantes de documentos de seguridad de la vieja escuela, que añadieron nuevas características de seguridad, los fabricantes de chips de circuito integrado seguros deben añadir de vez en cuando nuevas características de seguridad para mejorar la seguridad de sus chips de circuito integrado seguros. Por ejemplo, si se expone un fallo de seguridad en un algoritmo criptográfico, es posible que el fabricante del chip deba proporcionar una solución al algoritmo que corrija el fallo de seguridad identificado.

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

Los usuarios de ordenadores modernos o dispositivos electrónicos conectados en red están familiarizados con la invitación casi diaria a instalar algún tipo de parche de software, e incluso les puede molestar. De hecho, frecuentemente el emisor del sistema operativo o del programa de aplicación anuncia dichos parches como un “parche de seguridad crítico”. Dichos parches a través de la red son relativamente triviales para los dispositivos conectados en red; un sistema operativo o un programa de aplicación pueden tener un mecanismo incorporado para consultar a través de la red con un servidor de parches para determinar si hay un parche disponible que deba o podría instalarse.

Sin embargo, para los dispositivos electrónicos que no se conectan a una red, la aplicación de parches al software es mucho más difícil. Considérese, por ejemplo, una actualización de seguridad crítica de un pasaporte electrónico. El pasaporte electrónico, como muchos otros dispositivos, típicamente no se comunica con un servidor a través de una red. Además, incluso si se conecta a una red, es esencial que se pueda confiar en que cualquier parche propuesto no provenga de una fuente insegura o maliciosa.

La patente WO2016189488 se refiere a un sistema para detectar la manipulación indebida de un documento. En un aspecto, el sistema puede incluir el almacenamiento de un documento original junto con su al menos un certificado digital asociado de al menos una autoridad emisora en un servidor, y la asociación de un identificador único con el documento original, en donde el identificador único correspondiente al documento original también se almacena en el servidor. El sistema puede permitir además la creación de otra instancia del documento original, en donde la instancia del documento original incluye el identificador único, de modo que un usuario de la instancia del documento original verifique la fuente y la autenticidad de la instancia del documento original transmitiendo el identificador único al servidor para recuperar el al menos un certificado digital asociado basándose en el identificador único, y evalúa el certificado digital asociado recuperado.

La patente WO2017050739 describe un sistema para el marcado remoto de documentos de seguridad que comprende una interfaz adaptada para recibir, desde un equipo de campo y a través de una red, datos gráficos de una imagen escaneada de un documento de seguridad; un almacenamiento de datos adaptado para almacenar un registro de datos que comprende dichos datos de imagen recibidos y datos adicionales en relación con el propietario del documento de seguridad escaneado; un módulo de procesamiento gráfico de datos adaptado para superponer una imagen de una marca sobre la imagen del documento de seguridad y adaptado para generar datos gráficos adicionales

de la imagen escaneada del documento de seguridad con la marca; y un módulo de acceso adaptado para proporcionar acceso a dichos datos gráficos adicionales.

La patente WO2016073202 describe una tarjeta que incluye un sustrato, al menos un dispositivo de entrada de datos biométricos en el sustrato para recibir datos biométricos sobre un individuo que posee el sustrato, un componente de memoria en el sustrato y que contiene datos biométricos sobre un individuo que posee la tarjeta y al menos una clave privada, y un procesador configurado para comparar los datos biométricos recibidos a través del dispositivo de entrada de datos biométricos con los datos biométricos contenidos en el componente de memoria para determinar si coinciden. Cuando hay una coincidencia de datos biométricos, se inicia un proceso que requiere el uso de la(s) clave(s) privada(s) para el uso autorizado de la tarjeta. Un sistema detector de intrusos en el chasis detecta la manipulación indebida de la tarjeta y, tras dicha detección, provoca la eliminación de la(s) clave(s) privada(s) para evitar de este modo el uso no autorizado de la tarjeta.

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

Un método para parchar de forma segura un sistema operativo de un chip de circuito integrado incluye operar un servidor de parches para cifrar un parche en el sistema operativo, operar el servidor de parches para transmitir el parche cifrado al servidor de la autoridad emisora y operar el servidor de la autoridad emisora para añadir el parche cifrado a un segundo certificado digital de la autoridad emisora en una extensión al segundo certificado digital. El servidor de la autoridad emisora transmite el segundo certificado digital que incluye el parche cifrado al terminal. El terminal se comunica con el chip de circuito integrado tras la presentación del chip de circuito integrado al terminal.

Para lograr estas y otras ventajas, la invención propone un método para operar un chip de circuito integrado tal como se define en la reivindicación 1.

Preferiblemente, se instala una clave del fabricante del chip de circuito integrado en el chip de circuito integrado; y en donde el servidor de parches cifra el parche utilizando una clave del fabricante del chip de circuito integrado, y el chip de circuito integrado descifra la extensión al certificado digital utilizando una clave del fabricante.

El segundo certificado digital de la autoridad emisora puede ser un certificado de enlace, por ejemplo, un certificado de enlace de una autoridad certificadora de verificación del país, que vincula con el primer certificado de la autoridad certificadora almacenado en el chip de circuito integrado.

En un aspecto, el chip de circuito integrado se integra en un documento de seguridad electrónico.

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

En un aspecto, una clave privada del fabricante del chip de circuito integrado se instala en el chip de circuito integrado; y en donde el servidor de parches cifra el parche utilizando la clave pública correspondiente a la clave privada del fabricante del chip de circuito integrado, y en donde el chip de circuito integrado descifra la extensión al certificado digital utilizando la clave privada del fabricante.

En un aspecto, una clave secreta del fabricante del chip de circuito integrado se instala en el chip de circuito integrado; y en donde el servidor de parches cifra el parche utilizando la clave secreta correspondiente a la clave secreta del fabricante del chip de circuito integrado, y en donde el chip de circuito integrado descifra la extensión al certificado digital utilizando la clave secreta del fabricante.

La presente invención también se refiere a un chip de circuito integrado tal como se define en la reivindicación 8.

En un aspecto, la memoria incluye además una clave privada del fabricante del chip de circuito integrado; y en donde el parche se cifra utilizando la clave pública correspondiente a la clave privada del fabricante del chip de circuito integrado, y en donde las instrucciones comprenden además instrucciones para hacer que el procesador descifre la extensión al certificado digital utilizando la clave privada del fabricante.

En un aspecto, la memoria incluye además una clave secreta del fabricante del chip de circuito integrado; y en donde el parche se cifra utilizando la clave secreta compartida; y en donde las instrucciones comprenden además instrucciones para hacer que el procesador descifre la extensión al certificado digital utilizando la clave secreta compartida del fabricante.

Breve descripción de las figuras

La figura 1 es una ilustración de una portada de una libreta de pasaporte.

La figura 2 es una ilustración de una página de un pasaporte electrónico que incluye un chip de circuito integrado como incrustación en la página.

La figura 3 es un diagrama en bloque de alto nivel de una arquitectura del chip de circuito integrado de la figura 2.

La figura 4 es un diagrama en bloque que ilustra datos y programas almacenados en una memoria que corresponde a la memoria de la figura 3.

La figura 5 es un diagrama de red que ilustra el flujo de un parche desde un servidor del fabricante a un dispositivo o documento que contiene un chip 203 de circuito integrado (no mostrado) a través de una red.

La figura 6 es un esquema de programas y datos que pueden incluirse en una memoria de un chip de circuito integrado de un pasaporte electrónico.

La figura 7 es una ilustración esquemática de un certificado digital que tiene un cuerpo de certificado y una parte de extensiones de certificado.

La figura 8 es una ilustración esquemática de una parte de extensiones de certificado para una realización de pasaporte electrónico.

La figura 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 figura 2.

La figura 10, que está compuesta por las figuras 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

La siguiente descripción incluye referencias a varios métodos ejecutados por un procesador de un chip de circuito integrado. Como es habitual en este campo, puede haber frases en la presente memoria que indiquen que estos métodos o etapas del método se realizan mediante instrucciones de software o módulos de software. Como sabrá un experto en la técnica, dichas descripciones deben interpretarse en el sentido de que un procesador, de hecho, ejecuta los métodos, las instrucciones de software y los módulos de software.

La tecnología descrita en la presente memoria proporciona un mecanismo seguro de actualización de software in situ para chips de circuito integrado seguros.

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

La figura 2 es una ilustración de una página 201 de un pasaporte electrónico 100 que incluye un chip 203 de circuito integrado como incrustación en la página 201. La página 201 también contiene una antena 205 conectada al chip 203 de circuito integrado mediante la cual el chip 203 de circuito integrado se comunica con los terminales.

La figura 3 es un diagrama en bloque de alto nivel de una arquitectura del chip 203 de circuito integrado y la antena 205. El chip 203 de circuito integrado contiene un procesador 301 y una estructura 303 de memoria, que almacena datos y programas ejecutables por el procesador 301. La estructura 303 de memoria puede contener una o más de cada una de las siguientes: una memoria 305 de acceso aleatorio (RAM, en inglés), una memoria 307 de solo lectura (ROM, en inglés) y una memoria 309 programable no volátil (NVM, en inglés). Los dispositivos 305, 307 y 309 de memoria se conectan al procesador 301 a través de un bus 311.

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

En realizaciones alternativas, el chip 203 de circuito integrado puede incluir contactos eléctricos (no mostrados) para comunicarse a través de una interfaz de contacto con un terminal, por ejemplo, según el protocolo ISO-7816 o el protocolo de bus serie universal (USB).

La figura 4 es un diagrama en bloque que ilustra datos y programas almacenados en una memoria 403 que corresponde a la memoria 303 de la figura 3. En una realización preferida, los datos y programas ilustrados tal como se almacenan en la memoria 403 se almacenan en una NVM 409 que corresponde a la NVM 309 de la figura 3. Sin embargo, son posibles otras organizaciones de memoria.

La memoria 403 contiene programas 401 y datos 451 de personalización. Los programas 401 son instrucciones de programa informático que hacen que el procesador 301 realice ciertas acciones. Los programas 401 incluyen un sistema operativo 405 y programas 407 de aplicaciones.

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

El cargador 411 de parches, que se describe con mayor detalle más adelante, realiza funciones relacionadas con la recepción de un parche, la verificación de que el parche proviene del fabricante del chip 203 de circuito integrado (o de otra fuente confiable), el descifrado de un parche cifrado y la instalación del parche en el sistema operativo 405.

La figura 5 es un diagrama de red que ilustra el flujo de un parche 507 desde un fabricante 501 a un dispositivo o documento 503 que contiene un chip 203 de circuito integrado (no mostrado) a través de una red 505. El fabricante, p. ej., el fabricante del chip 203 de circuito integrado crea un parche 507 para el sistema operativo 409. El fabricante cifra y firma el parche y transmite el parche cifrado firmado 509 a un emisor 511 de dispositivos ICC, p. ej., una autoridad nacional emisora de pasaportes.

El emisor 513 del dispositivo ICC incorpora el parche cifrado firmado 509 en un certificado digital 513, p. ej., un certificado de enlace que vincula un certificado digital caducado o que está a punto de caducar a un certificado digital de reemplazo, y transmite el certificado digital 513 a un terminal 515, p. ej., un terminal verificador de pasaportes que funciona en un control de pasaportes en una frontera nacional o puerto de entrada.

Un portador del dispositivo 503, p. ej., un viajero que lleve 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 contactos que funcione, por ejemplo, a través del protocolo ISO 7816 o el protocolo de bus serie universal, o un enlace de comunicaciones sin contacto, p. ej., comunicación de campo cercano (NFC, por sus siglas en inglés) o comunicación a través del protocolo ISO/IEC 14443.

A continuación, el terminal 515 transmite el certificado digital 513 al dispositivo 503 como parte de un proceso 517 de autenticación del terminal.

Volviendo ahora a la figura 4, el cargador 411 de parches recibe un parche que está firmado y cifrado desde la autoridad emisora a través de un terminal. Tras la recepción del parche firmado y cifrado, el cargador 411 de parches verifica la fuente del parche, descifra el parche e instala el parche en el sistema operativo 405.

] Si bien los mecanismos descritos en la presente memoria se aplican para parchar el sistema operativo 405, los mecanismos también se pueden usar para parchar los programas 407 de aplicación. De hecho, el límite entre los programas 407 de aplicación y el sistema operativo 405 puede ser bastante borroso en algunos entornos.

Los datos 451 de personalización pueden incluir datos 453 de usuario, claves 455 de sistema y claves 457 de parche. Los datos 453 de usuario pueden incluir información biográfica, tal como nombre y fecha de nacimiento, datos biométricos, tales como fotografías, huellas dactilares y escaneos de retina, información de cuentas y claves de usuario. Las claves 455 de sistema pueden incluir certificados raíz. Las claves 457 de parche incluyen claves que se usan para verificar el origen de un archivo de parche y para descifrar un archivo de parche.

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

Para un pasaporte electrónico, el sistema operativo 609 puede incluir varias funciones de pasaporte electrónico, tales como 613 el control de acceso básico (BAC, por sus siglas en inglés), la autenticación 615 activa, el establecimiento 617 de conexión con autenticación de contraseña, la autenticación 619 con chip y la autenticación 621 de terminal. Estas funciones del pasaporte electrónico se describen en Bundesamt für Sicherheit in der Informationstechnik, Guía técnica BSI TR-03110 sobre mecanismos de seguridad avanzados para documentos de viaje legibles por máquina y token elDAS, https://www.bsi.bund.de/EN/Publications/TechnicalGuidelines/TR03110/BSITR03 110.html, consultada el 30 de octubre de 2018 (en adelante, “TR-03110”) y en la Organización de Aviación Civil Internacional (OACI, por sus siglas en inglés), Doc. 9303, Documentos de viaje legibles por máquina, https://www.icao.int/publications/pages/publication.aspx?docnum=9303, consultada el 30 de octubre de 2018.

El sistema operativo 609 incluye además el cargador 611 de parches, que corresponde al cargador 411 de parches de la figura 4.

Para un ejemplo de pasaporte electrónico, tal como se ilustra en la figura 6, el programa 407 de solicitud de la figura 4 puede ser una solicitud 607 de pasaporte, que puede conceder acceso a los datos 653 de usuario dependiendo del contexto 613, 617, 621 de autenticación.

Como se ha analizado junto con la figura 4, los datos de personalización pueden contener cierta información 653 personal. En el contexto de los pasaportes electrónicos, esta puede incluir el número de pasaporte y la información de viaje.

Un pasaporte electrónico realiza varias funciones de verificación, p. ej., la autenticación 621 de terminal, para verificar que la información confidencial almacenada en el mismo no sea obtenida por una entidad que no tenga la autorización requerida para acceder a la información. Un mecanismo consiste en verificar que los certificados proporcionados por el terminal hayan sido firmados por una autoridad de certificación confiable. Para ello, el chip de circuito integrado de un pasaporte electrónico contiene un certificado 659 de la *Autoridad certificadora de verificación del país* (C_{CVCA}) en las claves 655 del sistema.

El cargador 611 de parches verifica el parche cifrado firmado usando una clave de firma pública del fabricante ($PK_{ManSign}$) 661 y si la verificación es positiva, el cargador de parches descifra el parche 509 cifrado usando una clave secreta del fabricante (SK_{Man}) 663. La clave secreta del fabricante (SK_{Man}) 663 puede ser una clave secreta compartida o una clave privada de un par de claves PKI (Infraestructura de Clave Pública).

La autoridad emisora 511 incorpora el parche cifrado firmado en un certificado 513 digital. La figura 7 es una ilustración esquemática de un certificado digital 701 que tiene un cuerpo 703 de certificado y una parte 705 de extensiones de certificado.

El cuerpo 703 de certificado puede contener una clave pública de una autoridad de certificación y cierta otra información pertinente, p. ej., fechas de validez.

La parte 705 de extensiones de certificado contiene una o más extensiones 707 de certificado, cada una de las cuales sigue una plantilla prescrita. Una extensión 707 de certificado se introduce mediante un identificador 709 de objeto seguido de una secuencia de objetos 711 de datos dependientes del contexto. El identificador 709 de objeto puede identificar a qué chip de circuito integrado pertenece la extensión 707, p. ej., el fabricante del chip de circuito integrado, de modo que los chips de circuito integrado a los que no es aplicable la extensión 707 pueden ignorar la extensión 707.

En una realización, la parte 705 de extensiones de certificado y las extensiones 707 de certificado siguen el formato descrito en Bundesamt für Sicherheit en der Informationstechnik, Guía técnica BSI TR-03110 sobre mecanismos de seguridad avanzados para documentos de viaje legibles por máquina y token eIDAS, Parte 3: Especificaciones comunes, https://www.bsi.bund.de/EN/Publications/TechnicalGuidelines/TR03110/BSITR03 110.html, consultada el 30 de octubre de 2018 (incorporadas en la presente memoria como referencia) en las páginas 89-90.

La figura 8 es una ilustración esquemática de una parte 805 de extensiones de certificado, que corresponde a la parte 705 de extensiones de certificado de la figura 7, por ejemplo, para una realización de pasaporte electrónico. La parte 805 de extensiones de certificado incluye una extensión 807 de certificado que tiene un identificador 809 de objeto que identifica la extensión como un parche originado en Claire Greystone Enterprises Corporation (CGE Corp., una corporación ficticia). Los chips de circuito integrado que no se originan en CGE Corp. pueden ignorar la extensión 807. De hecho, dichos otros ICC no tendrían las claves necesarias para descifrar el parche. La extensión 807 de certificado incluye además el parche cifrado y la firma 811.

La figura 9 es un diagrama de flujo de datos que ilustra la población de claves requeridas en un chip 907 de circuito integrado, correspondiente a un chip 203 de circuito integrado de la figura 2. Como se indicó anteriormente, el parcheo de un chip de circuito integrado incluye cuatro nodos: el servidor 901 de fabricación operado por un fabricante 501, un servidor 903 de la autoridad emisora operado por el emisor 511 de chips de circuito integrado, el terminal 905 correspondiente al terminal 515 y el chip 907 de circuito integrado correspondiente al chip 203 de circuito integrado. Los chips de circuito integrado pasan por varias fases durante su ciclo de vida. Una primera fase es la fase 909 de fabricación durante la cual el fabricante genera claves de cifrado, descifrado y firma, etapa 911.

El chip 907 de circuito integrado descifra el parche cifrado 509 utilizando la clave de descifrado del fabricante. El cifrado y el descifrado del parche pueden basarse en la criptografía secreta compartida o en la PKI. En cualquiera de los dos casos, la clave de descifrado es una clave secreta del fabricante y, por lo tanto, se representa aquí como SK_{Man} 913. En una realización alternativa, el cifrado se realiza utilizando una clave pública. En dicha realización, el fabricante también puede generar y almacenar una clave pública del fabricante (PK_{Man}) 915.

La firma del parche cifrado 509 y la verificación de la firma se realizan mediante PKI. Por lo tanto, el fabricante genera un par de claves PKI, la clave de firma pública del fabricante ($PK_{ManSign}$) 917 y la correspondiente clave de firma secreta del fabricante ($SK_{ManSign}$) 919. El servidor 901 del fabricante transmite la clave *PKManSign* 917 y la clave SK_{Man} 913 al chip 907 de circuito integrado, etapa 921, y el chip 907 de circuito integrado almacena las claves en la memoria del chip 907 de circuito integrado, etapa 923. Las etapas 921 y 923 de transmisión y almacenamiento pueden realizarse

usando una operación de escritura en la que el servidor 901 del fabricante escribe directamente en la memoria del chip 907 de circuito integrado.

La fase 951 de personalización y emisión sigue a la fase 909 de fabricación en el ciclo de vida de un chip 203 de circuito integrado. Durante la personalización 951, el servidor 903 de la autoridad emisora obtiene la información del usuario, etapa 953, p. ej., información biográfica y biométrica asociada con el titular de la tarjeta, etapa 955, que a continuación se transmite al chip 907 de circuito integrado, que a su vez almacena la información del usuario, etapa 957.

El servidor 903 de la autoridad emisora también transmite la clave pública ($PK_{IssAuth}$) 959 de la autoridad emisora al chip de circuito integrado 907, etapa 961. El chip 907 de circuito integrado almacena la clave $PK_{IssAuth}$ 959, etapa 963. La clave pública $PK_{IssAuth}$ 959 puede ser un certificado digital. En una realización de pasaporte electrónico, la clave pública puede ser el certificado de la Autoridad certificadora de verificación del país (C_{CVCA}), tal como se describe en el TR-31110.

Las figuras 10a y 10b se combinan para formar un diagrama de flujo de datos de la fase 971 de uso (que consiste en una primera porción 971a de la figura 10a y una segunda porción 971b de la figura 10b) del ciclo de vida de un chip 907 de circuito integrado. Durante la fase 971 de uso, el chip 907 de circuito integrado se ha incorporado a un dispositivo, por ejemplo, una tarjeta inteligente o un pasaporte electrónico. De vez en cuando, durante la fase 971 de uso, el usuario, p. ej., un viajero, puede presentar el chip 907 de circuito integrado, o más el dispositivo en el que está incorporado, a un terminal 905.

Durante el uso de un chip 907 de circuito integrado, puede existir la necesidad o el deseo de actualizar el sistema operativo del chip 907 de circuito integrado mediante el desarrollo de parches de sistema operativo, etapa 973.

Para garantizar que ese parche solo esté disponible para un chip 907 de circuito integrado autorizado y no sea accesible para ninguna otra parte, el servidor 901 del fabricante cifra el parche, etapa 975. El cifrado puede estar utilizando una clave secreta compartida (SK_{Man}) del fabricante:

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

O, según PKI, utilizando una clave pública (PK_{Man}) del fabricante:

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

El servidor 901 del fabricante también firma el parche cifrado $PATCH_{ENC}$ produciendo un parche cifrado firmado ($PATCH_{SIGN}$), etapa 977. El parche cifrado firmado se produce mediante PKI firmando con la clave de firma secreta del fabricante ($SK_{ManSign}$):

$$PATCH_{SIGN} = SIGN(SK_{ManSign}, PATCH_{ENC})$$

El servidor 901 del fabricante transmite el parche cifrado firmado ($PATCH_{SIGN}$) al servidor 903 de la autoridad emisora, etapa 979.

Opcionalmente, el servidor 903 de la autoridad emisora verifica la firma del parche cifrado firmado, etapa 981. Si la verificación falla (ruta no ilustrada), se marca una condición de error y se toma una medida correctiva del error, p. ej., terminar el proceso o alertar a las autoridades pertinentes de un posible intento de violación de la seguridad.

Alternativamente, el servidor 903 de la autoridad emisora simplemente transmite (como se describe a continuación) el parche cifrado firmado a la ICC sin verificar la firma de la autoridad emisora.

Si la verificación de firma de la etapa 981 tiene éxito (o no se realiza), la autoridad emisora añade el parche cifrado firmado ($PATCH_{SIGN}$) a un certificado digital, p. ej., como una extensión de certificado a un certificado de enlace ($CERT_{LINK}$), etapa 983, como se describió anteriormente.

Continuando ahora con la figura 10B. El servidor 903 de la autoridad emisora transmite el certificado digital ($CERT_{LINK}$) al terminal 905, etapa 985.

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

Durante una fase 989 de autenticación del terminal, el terminal 905 transmite el certificado digital al chip 907 del circuito integrado, etapa 991.

El chip 907 de circuito integrado desempaqueta el certificado digital, etapa 993, para recuperar la extensión 707 de certificado.

El chip de circuito integrado lee la etiqueta 709 de identificación de objeto de la extensión 707 de certificado. Si la etiqueta 709 de identificación de objeto corresponde a la fabricación del chip 907 de circuito integrado, el chip de circuito integrado continúa con la instalación del parche de sistema operativo incluido en el certificado digital. De lo contrario, si la etiqueta 709 de identificación de objeto no corresponde a la fabricación del chip 907 de circuito integrado, el chip 907 de circuito integrado ignora la extensión 707.

El chip 907 de circuito integrado verifica que el certificado digital 991 coincida con el fabricante 901 y esté firmado por una autoridad certificadora confiable, etapa 993. Si la verificación no se realiza correctamente, se marca una condición de error y se toman medidas correctivas (no ilustradas).

La firma digital coincide con la del fabricante del chip 907 de circuito integrado, el chip 907 de circuito integrado descifra el parche cifrado, etapa 997:

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

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

A partir de lo anterior, será evidente que se proporciona un mecanismo eficiente y seguro para la instalación in situ de parches de sistema operativo en un sistema operativo de un chip de circuito integrado.

La invención está limitada únicamente por las reivindicaciones.

REIVINDICACIONES

1. Un método para operar un chip (203) de circuito integrado que comprende un primer certificado digital de una autoridad emisora, un servidor (501) de parches, un servidor (511) de autoridad emisora, y un terminal (515) para parchar de forma segura un sistema operativo (409) del chip de circuito integrado, comprendiendo el método:

operar el servidor (501) de parches para cifrar un parche (507) para el sistema operativo del chip de circuito integrado;
operar el servidor de parches para transmitir el parche cifrado (509) al servidor de la autoridad emisora;

en donde el método **se caracteriza por que**

se opera el servidor de la autoridad emisora para adjuntar el parche cifrado a un segundo certificado digital (513) de la autoridad emisora en una extensión al segundo certificado digital;
se opera el servidor de la autoridad emisora para transmitir el segundo certificado digital que incluye el parche cifrado al terminal;
se opera el terminal para que se comunique con el chip de circuito integrado tras la presentación del chip de circuito integrado al terminal;
se opera el terminal para transmitir el segundo certificado digital que incluye el parche cifrado al chip de circuito integrado;
se opera el chip de circuito integrado para desempaquetar el segundo certificado digital que incluye el parche cifrado para recuperar la extensión al segundo certificado digital; y
se opera el chip de circuito integrado para verificar que la extensión al segundo certificado digital corresponda al sistema operativo del chip de circuito integrado; y si se verifica que la extensión corresponde al sistema operativo del chip de circuito integrado, se descifra la extensión al segundo certificado digital, recuperando de este modo el parche en el sistema operativo del chip de circuito integrado, e instalando el parche en el sistema operativo del chip de circuito integrado,
se opera el servidor de parches para firmar digitalmente el parche cifrado; y
se opera el chip de circuito integrado para verificar la firma digital del parche cifrado antes de instalar el parche en el sistema operativo del chip de circuito integrado.

2. El método de la reivindicación 1, que comprende además una etapa preliminar de instalación de una clave privada del fabricante del chip de circuito integrado en el chip de circuito integrado; y en donde el servidor de parches cifra el parche utilizando la clave pública correspondiente a la clave privada del fabricante del chip de circuito integrado, y en donde el chip de circuito integrado descifra la extensión al certificado digital utilizando la clave privada del fabricante.

3. El método de la reivindicación 1, que comprende además una etapa preliminar de instalación de una clave secreta del fabricante del chip de circuito integrado en el chip de circuito integrado; y en donde el servidor de parches cifra el parche utilizando la clave secreta correspondiente a la clave secreta del fabricante del chip de circuito integrado, y en donde el chip de circuito integrado descifra la extensión al certificado digital utilizando la clave secreta del fabricante.

4. El método de cualquiera de las reivindicaciones anteriores, en donde el segundo certificado digital de la autoridad emisora es un certificado de enlace que vincula con el primer certificado de la autoridad certificadora almacenado en el chip de circuito integrado.

5. El método de cualquiera de las reivindicaciones anteriores, en donde el certificado de enlace es un certificado de enlace de una autoridad certificadora de verificación del 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.

6. El método de cualquiera de las reivindicaciones anteriores, en donde el chip de circuito integrado está integrado en un documento de seguridad electrónico.

7. El método de cualquiera de las reivindicaciones anteriores, en donde el documento de seguridad electrónico es un documento de viaje legible por máquina.

8. Un chip (203) de circuito integrado que comprende:

un procesador (301); y
una memoria (303) conectada al procesador y que contiene instrucciones ejecutables por procesador que incluye un sistema operativo; y

en donde el chip de circuito integrado **se caracteriza por que** las instrucciones hacen que el procesador:

reciba un certificado digital (513) desde un servidor (501) de parches a través de un terminal verificador (515), incluyendo el certificado digital una extensión que contiene un parche cifrado (509) para el sistema operativo (409);
desempaquete el certificado digital recuperando de este modo la extensión al certificado digital;
verifique que la extensión al certificado digital corresponda al sistema operativo del chip de circuito integrado; y si se verifica que la extensión corresponde al sistema operativo del chip de circuito integrado, descifre la extensión al certificado digital, recuperando de este modo el parche en el sistema operativo del chip de circuito integrado, e instalando el parche en el sistema operativo del chip de circuito integrado;

en donde las instrucciones del cargador de parches comprenden además instrucciones para hacer que el procesador verifique la firma digital del parche cifrado antes de instalar el parche en el sistema operativo del chip de circuito integrado.

9. El chip de circuito integrado de la reivindicación 8, en donde la memoria incluye además una clave privada del fabricante del chip de circuito integrado; y en donde el parche se cifra utilizando la clave pública correspondiente a la clave privada del fabricante del chip de circuito integrado, y en donde las instrucciones comprenden además instrucciones para hacer que el procesador descifre la extensión al certificado digital utilizando la clave privada del fabricante.

10. El chip de circuito integrado de la reivindicación 8, en donde la memoria incluye además una clave secreta del fabricante del chip de circuito integrado; y en donde el parche se cifra utilizando la clave secreta compartida; y en donde las instrucciones comprenden además instrucciones para hacer que el procesador descifre la extensión al certificado digital utilizando la clave secreta compartida del fabricante.

11. El chip de circuito integrado de cualquiera de las reivindicaciones 8 a 10, en donde el segundo certificado digital de la autoridad emisora es un certificado de enlace que vincula con el primer certificado de la autoridad certificadora almacenado en el chip de circuito integrado.

12. El chip de circuito integrado de la reivindicación 11, en donde el certificado de enlace es un certificado de enlace de una autoridad certificadora de verificación del 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.

13. El chip de circuito integrado de cualquiera de las reivindicaciones 8 a 12, en donde el chip de circuito integrado está integrado en un documento de seguridad electrónico.

14. El chip de circuito integrado de cualquiera de las reivindicaciones 8 a 13, en donde el documento de seguridad electrónico es un documento de viaje legible por máquina.

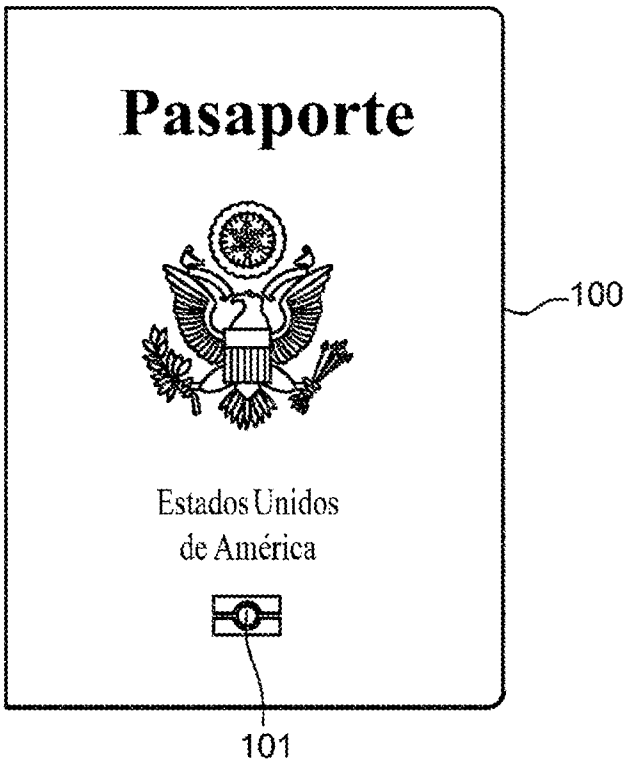

Figura 1

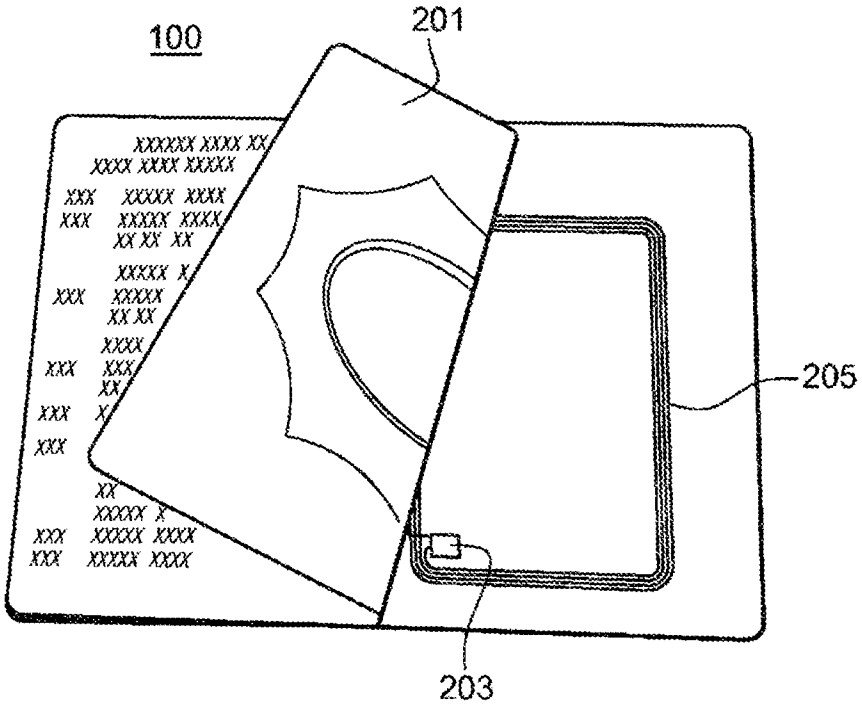

Figura 2

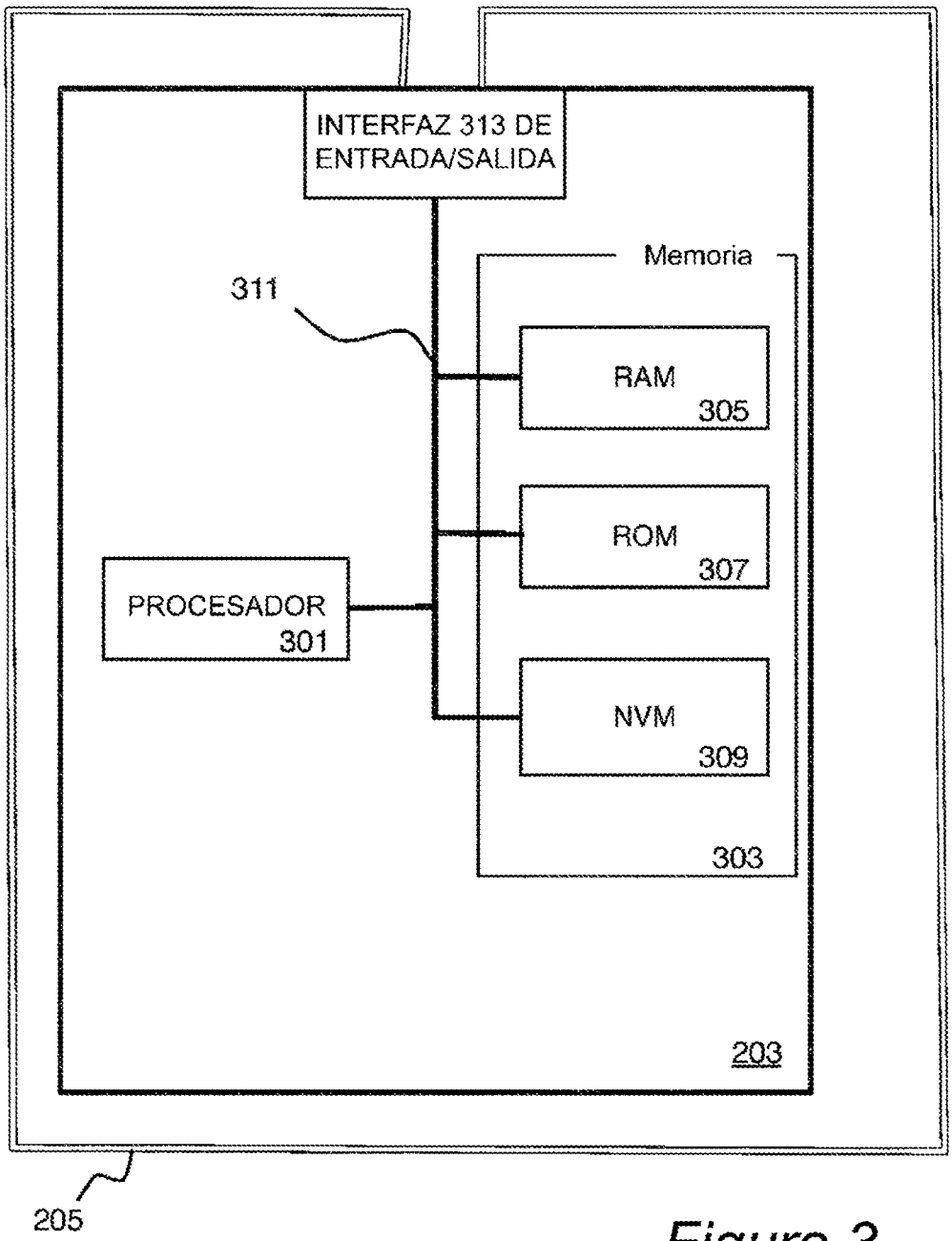
INTERFAZ 313 DE ENTRADA/SALIDA
Memoria
311
RAM 305
ROM 307
PROCESADOR 301
NVM 309
303
203
205

Figura 3

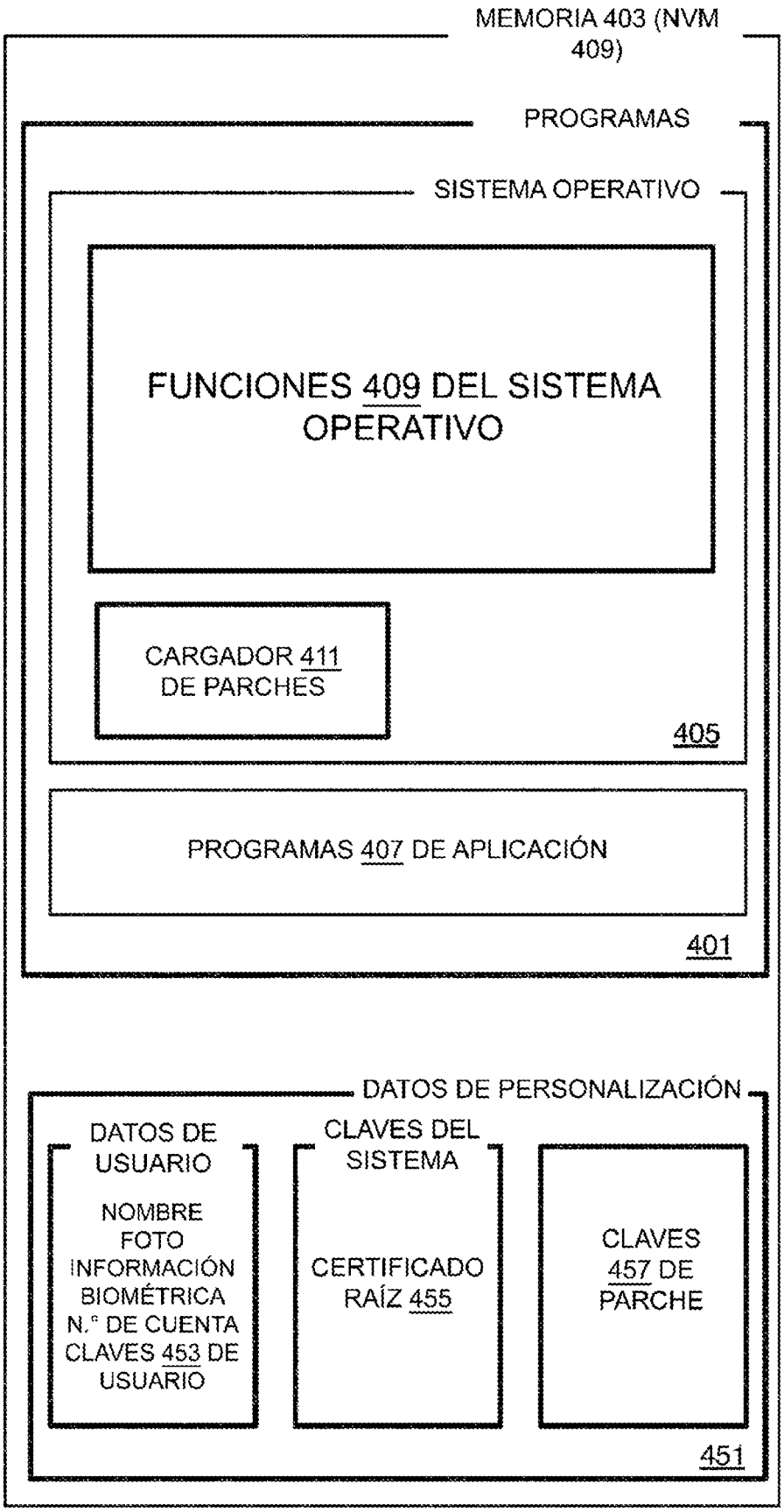
MEMORIA 403 (NVM 409)
PROGRAMAS
SISTEMA OPERATIVO
FUNCIONES 409 DEL SISTEMA OPERATIVO
CARGADOR 411 DE PARCHES
405
PROGRAMAS 407 DE APLICACIÓN
401
DATOS DE PERSONALIZACIÓN
DATOS DE USUARIO
NOMBRE
FOTO
INFORMACIÓN BIOMÉTRICA
N.º DE CUENTA
CLAVES 453 DE USUARIO
CLAVES DEL SISTEMA
CERTIFICADO RAÍZ 455
CLAVES 457 DE PARCHE
451

Figura 4

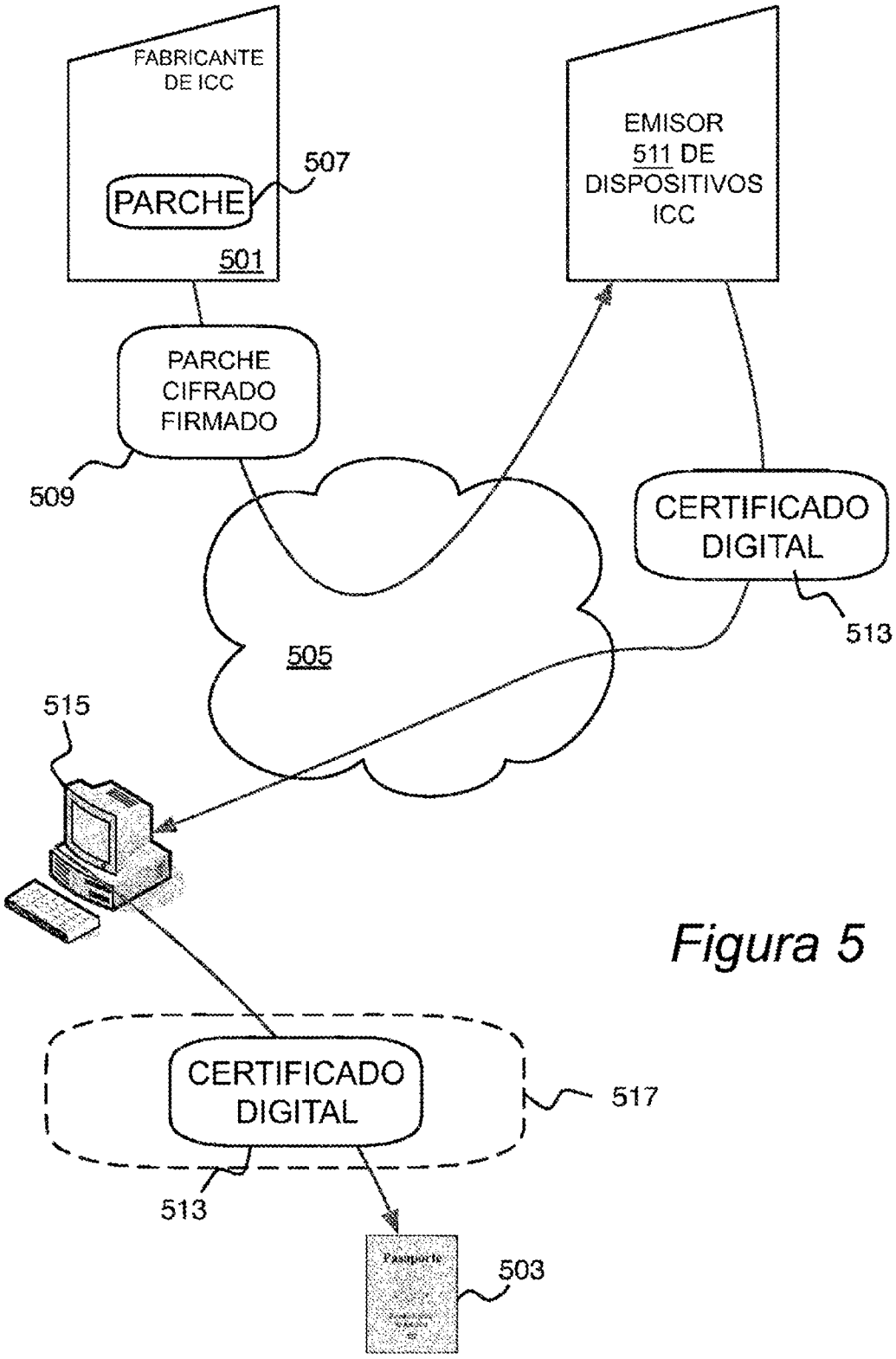
FABRICANTE DE ICC
PARCHE
507
501
EMISOR 511 DE DISPOSITIVOS ICC
PARCHE CIFRADO FIRMADO
509
505
CERTIFICADO DIGITAL
513
515
CERTIFICADO DIGITAL
517
513
Pasaporte
503

Figura 5

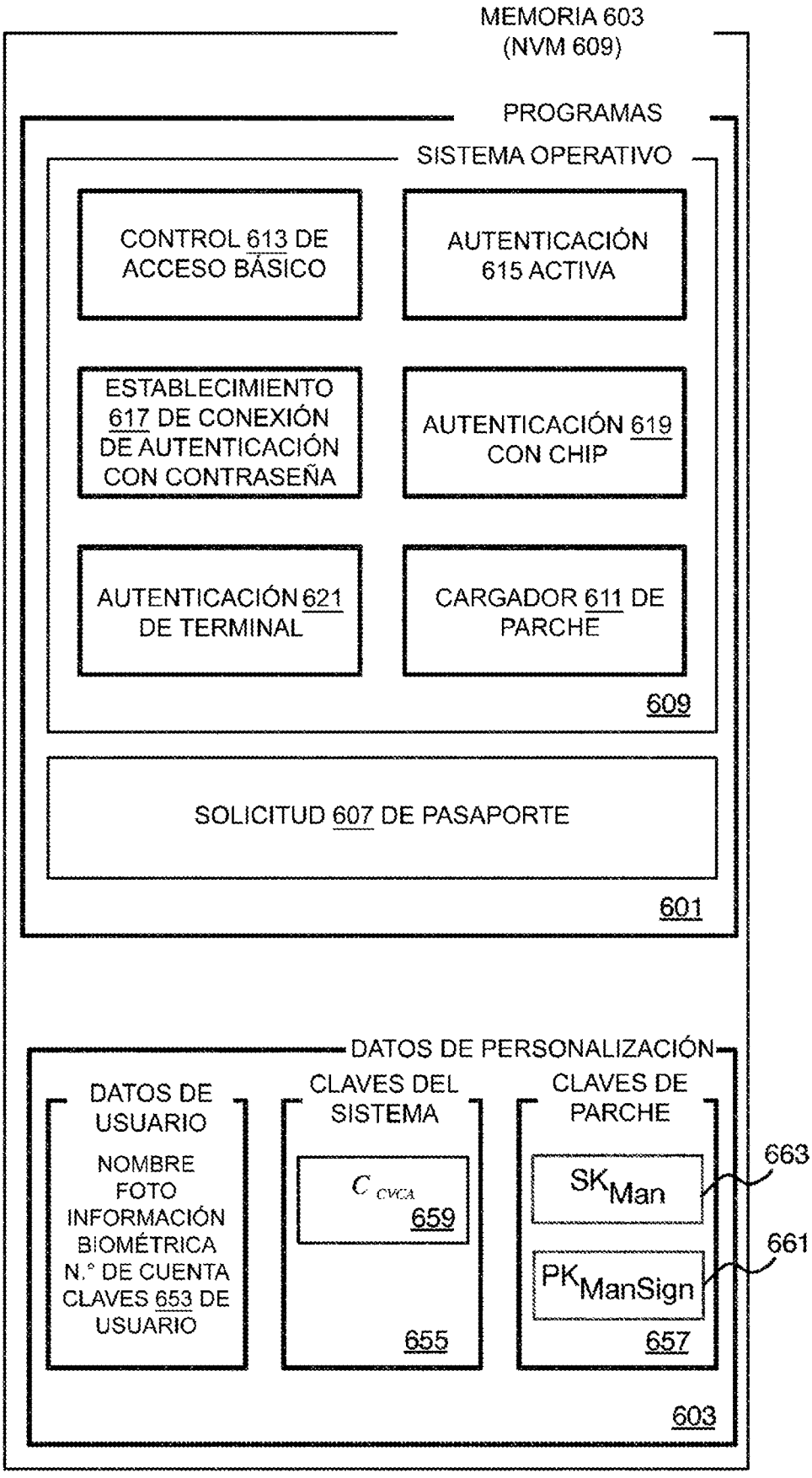
MEMORIA 603
(NVM 609)
PROGRAMAS
SISTEMA OPERATIVO
CONTROL 613 DE ACCESO BÁSICO
AUTENTICACIÓN 615 ACTIVA
ESTABLECIMIENTO 617 DE CONEXIÓN DE AUTENTICACIÓN CON CONTRASEÑA
AUTENTICACIÓN 619 CON CHIP
AUTENTICACIÓN 621 DE TERMINAL
CARGADOR 611 DE PARCHE
609
SOLICITUD 607 DE PASAPORTE
601
DATOS DE PERSONALIZACIÓN
DATOS DE USUARIO
NOMBRE
FOTO
INFORMACIÓN BIOMÉTRICA
N.° DE CUENTA
CLAVES 653 DE USUARIO
CLAVES DEL SISTEMA
C_{CVCA} 659
655
CLAVES DE PARCHE
SK_{Man}
663
$PK_{ManSign}$
661
657
603

Figura 6

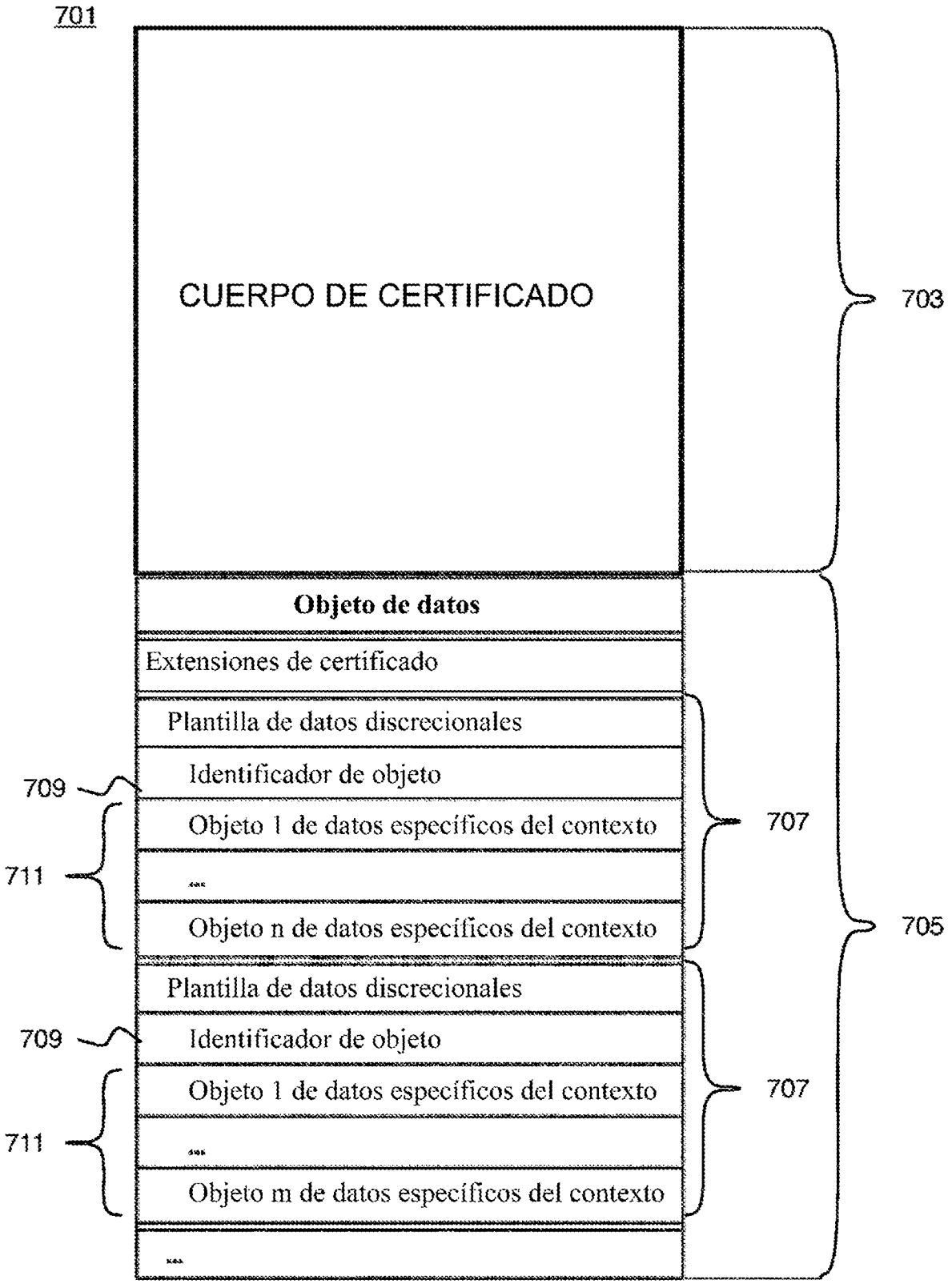
701
CUERPO DE CERTIFICADO
703
Objeto de datos
Extensiones de certificado
Plantilla de datos discrecionales
Identificador de objeto
709
Objeto 1 de datos específicos del contexto
711
...
Objeto n de datos específicos del contexto
707
705
Plantilla de datos discrecionales
Identificador de objeto
709
Objeto 1 de datos específicos del contexto
711
...
Objeto m de datos específicos del contexto
707
...

Figura 7

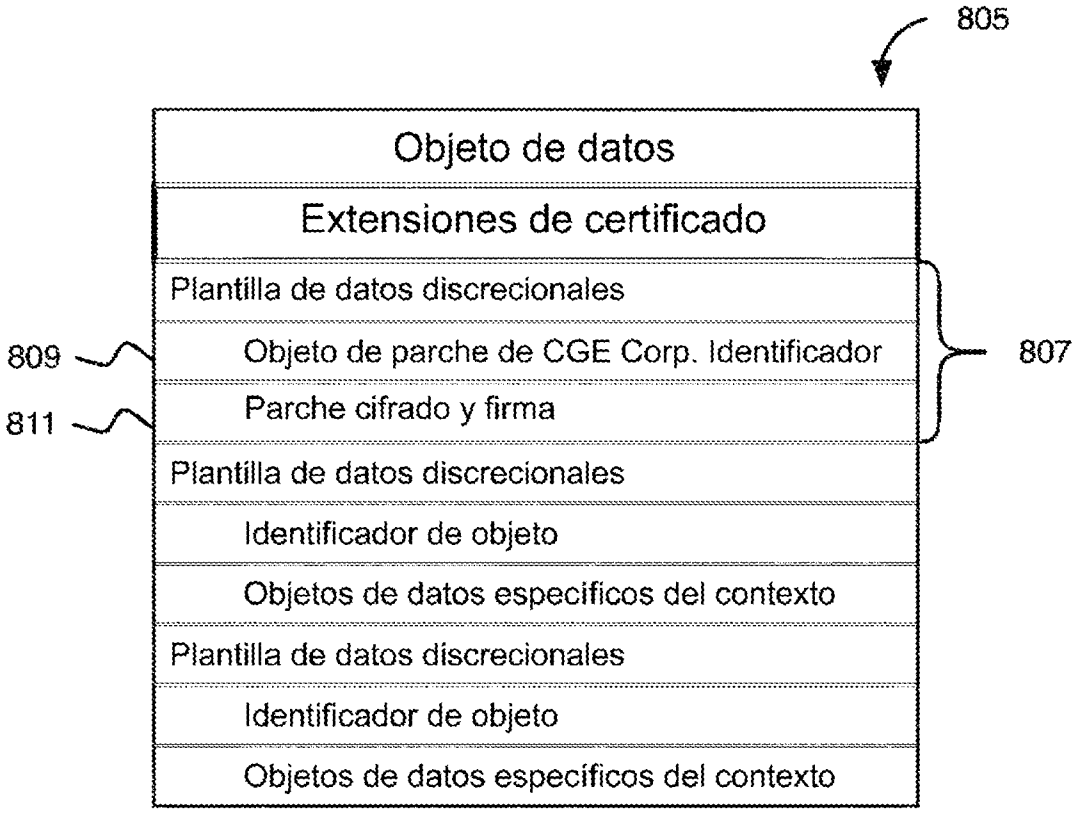
805
Objeto de datos
Extensiones de certificado
Plantilla de datos discrecionales
809
Objeto de parche de CGE Corp. Identificador
807
811
Parche cifrado y firma
Plantilla de datos discrecionales
Identificador de objeto
Objetos de datos específicos del contexto
Plantilla de datos discrecionales
Identificador de objeto
Objetos de datos específicos del contexto

Figura 8

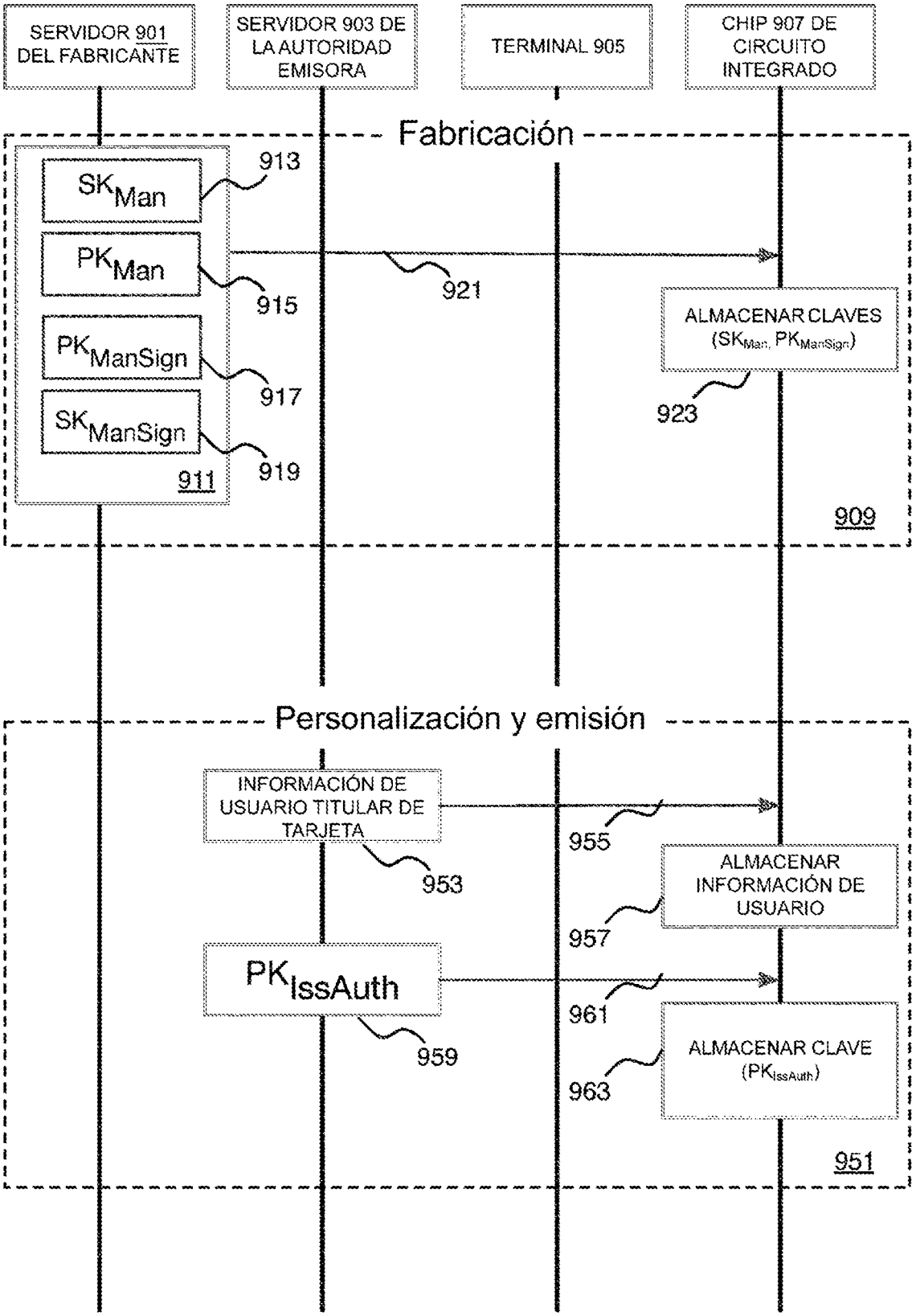
SERVIDOR 901 DEL FABRICANTE
SERVIDOR 903 DE LA AUTORIDAD EMISORA
TERMINAL 905
CHIP 907 DE CIRCUITO INTEGRADO
Fabricación
SKMan
PKMan
PKManSign
SKManSign
911
913
915
917
919
921
ALMACENAR CLAVES (SKMan, PKManSign)
923
909
Personalización y emisión
INFORMACIÓN DE USUARIO TITULAR DE TARJETA
953
955
ALMACENAR INFORMACIÓN DE USUARIO
957
PKIssAuth
959
961
ALMACENAR CLAVE (PKIssAuth)
963
951

Figura 9

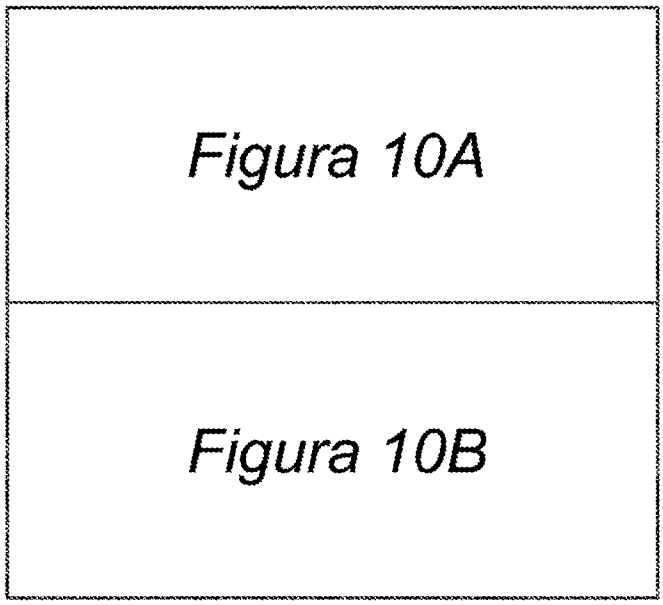

Figura 10

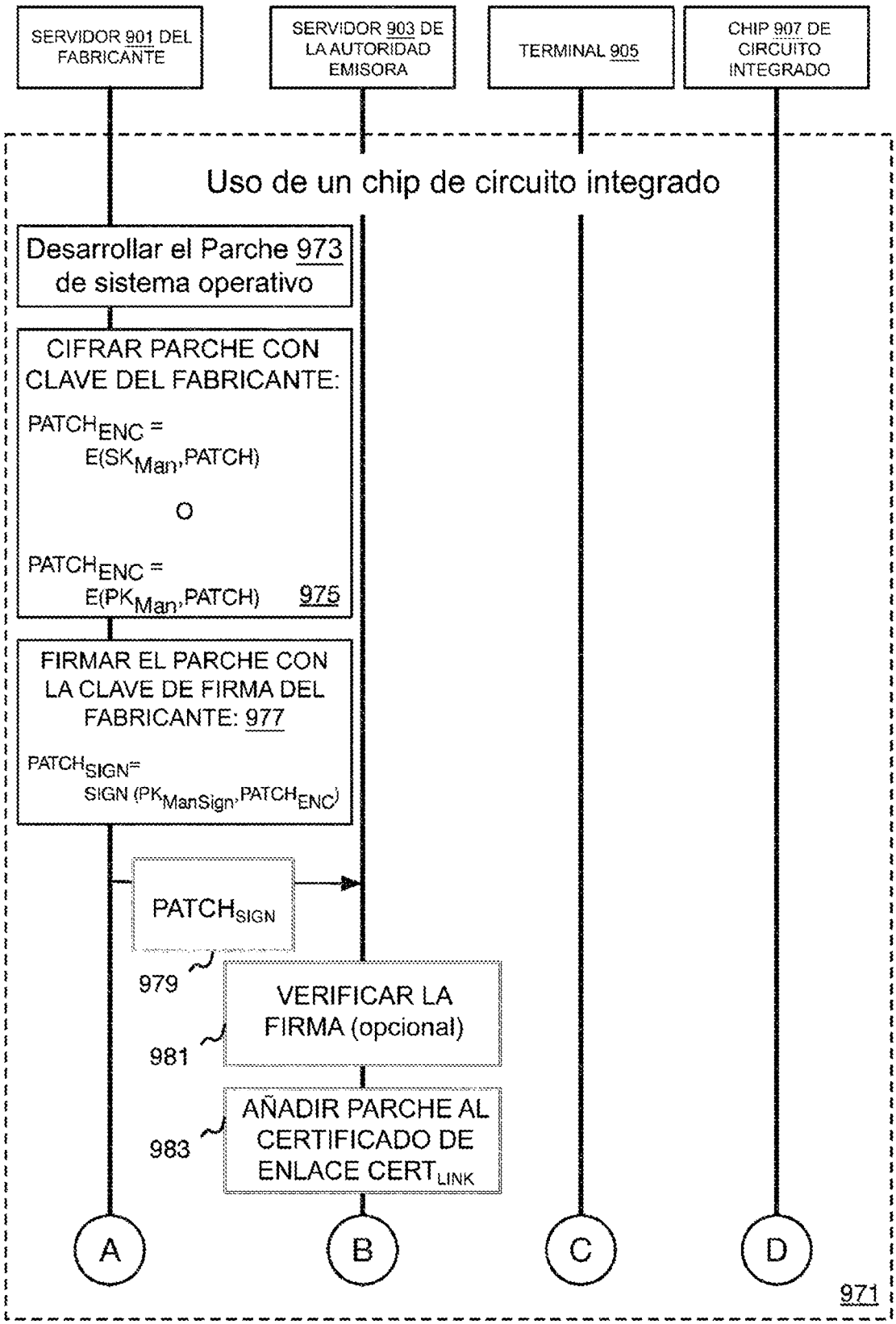
SERVIDOR 901 DEL FABRICANTE
SERVIDOR 903 DE LA AUTORIDAD EMISORA
TERMINAL 905
CHIP 907 DE CIRCUITO INTEGRADO
Uso de un chip de circuito integrado
Desarrollar el Parche 973 de sistema operativo
CIFRAR PARCHE CON CLAVE DEL FABRICANTE:
PATCH_ENC = E(SK_Man,PATCH)
O
PATCH_ENC = E(PK_Man,PATCH) 975
FIRMAR EL PARCHE CON LA CLAVE DE FIRMA DEL FABRICANTE: 977
PATCH_SIGN= SIGN (PK_ManSign,PATCH_ENC)
PATCH_SIGN
979
VERIFICAR LA FIRMA (opcional)
981
AÑADIR PARCHE AL CERTIFICADO DE ENLACE CERT_LINK
983
A
B
C
D
971

Figura 10A

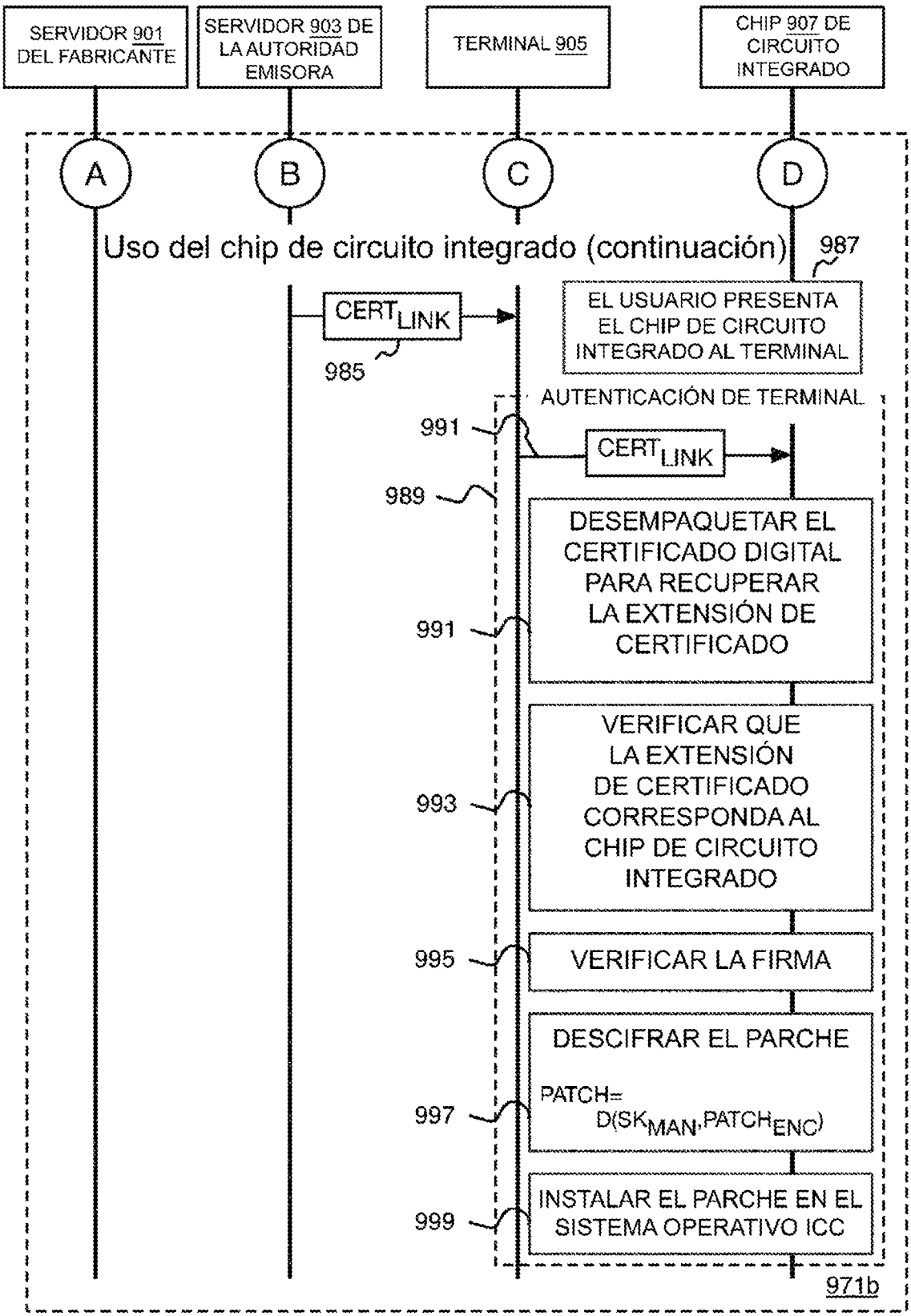
SERVIDOR 901 DEL FABRICANTE
SERVIDOR 903 DE LA AUTORIDAD EMISORA
TERMINAL 905
CHIP 907 DE CIRCUITO INTEGRADO
A
B
C
D
Uso del chip de circuito integrado (continuación)
987
CERT LINK
985
EL USUARIO PRESENTA EL CHIP DE CIRCUITO INTEGRADO AL TERMINAL
AUTENTICACIÓN DE TERMINAL
991
CERT LINK
989
DESEMPAQUETAR EL CERTIFICADO DIGITAL PARA RECUPERAR LA EXTENSIÓN DE CERTIFICADO
991
VERIFICAR QUE LA EXTENSIÓN DE CERTIFICADO CORRESPONDA AL CHIP DE CIRCUITO INTEGRADO
993
995
VERIFICAR LA FIRMA
DESCIFRAR EL PARCHE
PATCH= D(SK MAN, PATCH ENC)
997
INSTALAR EL PARCHE EN EL SISTEMA OPERATIVO ICC
999
971b

Figura 10B