(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 359 774**

(51) Int. Cl.:
H04W 4/00 (2006.01)
H04W 88/02 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Número de solicitud europea: **08794721 .4**
(96) Fecha de presentación : **25.07.2008**
(97) Número de publicación de la solicitud: **2186356**
(97) Fecha de publicación de la solicitud: **19.05.2010**

(54) Título: **Activación de proveedor de servicios.**

(30) Prioridad: **01.09.2007 US 849286**

(45) Fecha de publicación de la mención BOPI:
26.05.2011

(45) Fecha de la publicación del folleto de la patente:
26.05.2011

(73) Titular/es: **APPLE Inc.**
1 Infinite Loop
Cupertino, California 95014, US

(72) Inventor/es: **De Atley, Dallas;**
Bush, Jeffrey;
Hauck, Jerry;
Huang, Ronald, Keryuan y
Sathianathan, Brainerd

(74) Agente: **Fàbrega Sabaté, Xavier**

DESCRIPCIÓN

Activación de proveedor de servicios.

Antecedentes

Los dispositivos móviles que se fabrican para utilizarse con la tecnología de telefonía celular digital del Sistema Global de Comunicaciones Móviles (GSM) están diseñados para funcionar con cualquier proveedor de servicios de red de comunicaciones móviles. El dispositivo requiere la utilización de un módulo de identidad de abonado (SIM), denominado como una tarjeta SIM, que debe estar insertado en el dispositivo GSM para iniciar una sesión en la red de proveedor de servicios del abonado. La tarjeta SIM es una pequeña placa de circuito que contiene, entre otras cosas, un identificador que identifica al proveedor de servicios con el que se permite utilizar la tarjeta SIM. Normalmente, cada proveedor de servicios, tal como AT&T o Verizon, tiene asignado su propio intervalo de identificadores de tarjeta SIM para utilizarse con sus redes.

La mayoría de dispositivos GSM se fabrican con un bloqueo de proveedor de servicios que limita el dispositivo a tarjetas SIM para un proveedor de servicios particular. Por ejemplo, un dispositivo móvil fabricado por Nokia y comercializado por un proveedor de servicios AT&T puede tener un bloqueo que limite el dispositivo a tarjetas SIM codificadas con identificadores que pertenezcan al intervalo de identificadores de tarjeta SIM asignados para utilizarse con la red de AT&T.

El procedimiento de aplicar el bloqueo de proveedor de servicios puede variar de un fabricante a otro. Cuando un dispositivo se fabrica con un bloqueo de servidor de servicios, el bloqueo se basa normalmente en un código que está almacenado en el dispositivo o que se obtiene utilizando un algoritmo. Sin embargo, los códigos y/o algoritmos pueden vulnerarse de manera que el dispositivo puede desbloquearse y utilizarse con tarjetas SIM que tienen identificadores asignados para utilizarse con otros proveedores de servicio. Esto da como resultado que el proveedor de servicios original obtenga menos ingresos ya que, presumiblemente, el dispositivo ya no está utilizándose en su red.

Desde el punto de vista del fabricante de dispositivos GSM, hay otros inconvenientes relacionados con la fabricación de dispositivos con bloqueos de proveedor de servicio. Por ejemplo, la fabricación de un dispositivo con un bloqueo de proveedor de servicios particular puede requerir que el fabricante mantenga diferentes números de pieza para los dispositivos móviles fabricados para los diferentes proveedores de servicio, ya que los códigos y/o algoritmos de bloqueo variarán dependiendo del proveedor de servicios. Esto puede aumentar la complejidad logística de la fabricación del dispositivo, así como añadir un coste de inventario significativo.

Desde el punto de vista de los consumidores, la mayoría prefiere tener libertad a la hora de comprar un dispositivo móvil sin estar limitado a un proveedor de servicios particular. Por ejemplo, puede ser deseable cambiar a un proveedor de servicios diferente cuando se viaja al extranjero o a diferentes partes del país. El documento US6879825 B1 divulga una activación en dos etapas donde el terminal se registra en la red utilizando un identificador temporal y se descarga un identificador permanente. El identificador permanente se utiliza en la segunda etapa para descargar datos de programación. Se recopila y se envía información personal. El documento no prevé la utilización de un ID de SIM ni verificación.

Resumen de la descripción detallada

Se describen procedimientos y sistemas para la activación de un proveedor de servicios en un dispositivo móvil.

Según un aspecto de la invención, un dispositivo móvil funciona en un modo de servicio limitado hasta que se activa para utilizarse con un proveedor de servicios particular. El dispositivo móvil puede estar preparado para activarse a través de la utilización de un proceso de firma de proveedor de servicios y, posteriormente, activarse para utilizarse con un proveedor de servicios particular a través de la utilización de un proceso de activación de proveedor de servicios. Los procesos de firma y de activación de proveedor de servicios se llevan a cabo según formas de realización de la invención.

Según un aspecto de la invención, el proceso de firma de proveedor de servicios prepara el dispositivo para su activación haciendo que una etiqueta de activación se almacene en el dispositivo, la cual incorpora de manera segura información tanto del dispositivo como de la tarjeta SIM que se insertó en el dispositivo durante el proceso de firma.

Según otro aspecto de la invención, el proceso de activación de proveedor de servicios verifica que una etiqueta de activación almacenada anteriormente en el dispositivo sea auténtica y corresponda tanto al dispositivo como a la tarjeta SIM insertada actualmente en el dispositivo antes de activar el dispositivo para utilizarse en la red del proveedor de servicios.

Según un aspecto de la invención, cuando se inserta una nueva tarjeta SIM en el dispositivo o cuando el dispositivo

se reinicia, los procesos de firma y de activación de proveedor de servicios se repiten según sea necesario para activar el dispositivo para utilizarse con el proveedor de servicios identificado en la tarjeta SIM actualmente insertada. Por ejemplo, cuando la tarjeta SIM actualmente insertada ya ha pasado por el proceso de firma durante una inserción anterior en el dispositivo, entonces solo se necesita el proceso de activación para activar el dispositivo. Cuando la tarjeta SIM es nueva para el dispositivo (es decir, no ha pasado todavía por el proceso de firma o de activación en este dispositivo), los procesos de firma y de activación se repiten para activar el dispositivo para utilizarse con el proveedor de servicios.

Según un aspecto de la invención, el proceso de firma de proveedor de servicio puede repetirse para diferentes tarjetas SIM, de manera que en el dispositivo puede haber almacenadas más de una etiqueta de activación. Cada etiqueta de activación almacenada en el dispositivo corresponde a una de las tarjetas SIM que se insertaron en el dispositivo durante el proceso de firma. De esta manera, el dispositivo móvil puede estar preparado para activarse con diferentes proveedores de servicio correspondientes a las diferentes tarjetas SIM utilizadas durante el proceso de firma (siempre que las cuentas de abonado con esos proveedores de servicios sean todavía válidas en el momento de la activación).

Según un aspecto de la invención, el proceso de firma de proveedor de servicios incluye generar una solicitud de activación en la que se introduce información tanto del dispositivo como de la tarjeta SIM actualmente insertada en el dispositivo. La información introducida incluye, entre otros datos, el ID de tarjeta de circuito integrado (ICCID) y el identificador internacional de abonado móvil (IMSI) de la tarjeta SIM actualmente insertada en el dispositivo, el identificador internacional de equipo móvil (IMEI) codificado en el dispositivo, y una huella digital de hardware del dispositivo.

Según un aspecto la invención, el proceso de firma de proveedor de servicios incluye además recibir la solicitud de activación en un servidor de activación, donde la solicitud de activación se retransmite normalmente al servidor de activación a través de un cliente de activación en comunicación con el dispositivo. El servidor de activación genera la etiqueta de activación basándose en la información que se introdujo en la solicitud de activación. El servidor de activación, en comunicación con servidores de procesamiento para el proveedor de servicios, puede verificar en primer lugar si el abonado especificado en el IMSI está asociado con una cuenta válida. En algunas formas de realización, el servidor de activación puede llevar a cabo otras determinaciones de política que controlan si generar una etiqueta de activación, incluyendo acciones como confirmar si el código de país de móvil (MCC) y el código de red móvil (MNC) especificados en el IMSI son compatibles con el canal de distribución esperado para el dispositivo, basándose en el IMEI del dispositivo.

Según un aspecto de la invención, durante el proceso de firma, el servidor de activación genera una etiqueta de activación firmada utilizando una clave privada de activación que está almacenada en, o que está accesible de otro modo para, el servidor de activación. La etiqueta de activación generada se formatea para incluir no solamente la información que se introdujo en la solicitud de activación, sino también una clave pública de activación que se utilizará posteriormente en el dispositivo para validar la firma de la etiqueta. Como una medida de seguridad adicional, el contenido de la etiqueta de activación se oscurece mediante cifrado antes de enviar la etiqueta de activación al dispositivo. El cifrado puede llevarse a cabo utilizando una clave simétrica por dispositivo que está almacenada en, o que está accesible de otro modo para, el dispositivo y el servidor de activación. Esta clave puede denominarse como la clave de oscurecimiento compartida.

Según un aspecto la invención, al finalizar el proceso de firma, la etiqueta de activación generada se recibe en el dispositivo desde el servidor de activación, normalmente a través de un cliente de activación en comunicación con el dispositivo. El dispositivo almacena la etiqueta de activación para su utilización durante un proceso de activación de proveedor de servicios posterior.

Según un aspecto de la invención, el proceso de activación de proveedor de servicios requiere el ICCID de la tarjeta SIM actualmente insertada en el arranque y utiliza este valor para determinar si se ha almacenado anteriormente una etiqueta de activación para esta tarjeta SIM. Si es así, el proceso de activación de proveedor de servicios emite un comando en el dispositivo para verificar la etiqueta de activación, incluyendo pero sin limitarse a, descifrar la etiqueta de activación utilizando la clave de oscurecimiento compartida, validar la clave de activación pública suministrada en la etiqueta por el servidor de activación y utilizar la clave validada para validar la firma de la etiqueta de activación.

Según un aspecto de la invención, el proceso de activación de proveedor de servicios verifica el contenido de la etiqueta de activación con respecto al dispositivo y a la tarjeta SIM actualmente insertada en el dispositivo, incluyendo verificar que el IMEI y las huellas digitales de hardware coinciden con los del dispositivo, y que el ICCID y el IMSI coinciden con los de la tarjeta SIM actualmente insertada. Si no puede verificarse que el contenido de la etiqueta de activación corresponde al dispositivo y a la tarjeta SIM, entonces la etiqueta de activación se trata como no válida y el dispositivo no se activa para su utilización con la red del proveedor de servicios. Si se verifica el contenido de la etiqueta de activación, entonces el dispositivo se activa para su utilización con la red del proveedor de servicios.

Breve descripción de los dibujos

La presente invención se ilustra a modo de ejemplo y de manera no limitativa en las figuras de los dibujos adjuntos, donde los números de referencia similares indican elementos similares.

La FIG. 1 es una visión general en forma de diagrama de bloques de una arquitectura para un sistema de activación de proveedor de servicios según una forma de realización a modo de ejemplo de la invención.

La FIG. 2 es una visión general en forma de diagrama de bloques de componentes seleccionados de un dispositivo móvil según una forma de realización a modo de ejemplo de la invención.

La FIG. 3 es una visión general en forma de diagrama de bloques de un sistema de activación de proveedor de servicios según una forma de realización a modo de ejemplo de la invención.

La FIG. 4 es un diagrama de flujo que ilustra determinados aspectos para llevar a cabo un procedimiento para un proceso de firma de proveedor de servicios según una forma de realización a modo de ejemplo de la invención.

Las FIGS. 5A y 5B son diagramas de flujo que ilustran determinados aspectos para llevar a cabo un procedimiento para un proceso de activación de proveedor de servicios según una forma de realización a modo de ejemplo de la invención.

La FIG. 6 es una visión general en forma de diagrama de bloques de una forma de realización a modo de ejemplo de un sistema informático de propósito general en el que determinados componentes de un sistema de activación de proveedor de servicios pueden implementarse según una forma de realización a modo de ejemplo de la invención, que incluyen pero sin limitarse a, componentes tales como el cliente de activación, el servidor de activación y otros servidores de procesamiento de los proveedores de servicios de redes de comunicaciones móviles.

Descripción detallada

Las formas de realización de la presente invención se describirán con referencia a numerosos detalles expuestos posteriormente, y los dibujos adjuntos ilustrarán las formas de realización descritas. Como tales, la siguiente descripción y los dibujos ilustran formas de realización de la presente invención y no deben considerarse que limiten la invención. Se describen numerosos detalles específicos para proporcionar un entendimiento minucioso de la presente invención. Sin embargo, en determinados casos, no se describen detalles convencionales o ampliamente conocidos para no oscurecer innecesariamente la presente invención.

La descripción puede incluir material protegido por derechos de autor, como ilustraciones de imágenes de interfaz gráfica de usuario. Los titulares de los derechos de autor, incluyendo el cesionario de la presente invención, reservan sus derechos por la presente, incluyendo derechos de autor, en estos materiales. El titular de los derechos de autor no se opone a la reproducción en facsímil del documento de patente o de la descripción de patente, tal y como aparece en el archivo o registros de la Oficina de Patentes y Marcas, pero reserva todos los derechos de autor. Copyright Apple Computer, Inc. 2007.

Pueden utilizarse varias arquitecturas de sistema diferentes para implementar las funciones y operaciones descritas en este documento, tal como llevar a cabo los procedimientos mostrados en las FIG. 4, 5A y 5B. El siguiente análisis proporciona un ejemplo de una arquitectura de este tipo, pero debe entenderse que también pueden utilizarse arquitecturas alternativas para conseguir resultados idénticos o similares. El sistema de bloqueo de proveedor de servicios 100 mostrado en la FIG. 1 es un ejemplo basado en el dispositivo iPhone comercializado por Apple Computer, Inc., y en clientes y servidores de procesamiento asociados con el dispositivo iPhone y las redes de comunicaciones móviles con las que puede utilizarse el dispositivo iPhone. Sin embargo, debe entenderse que la arquitectura 100 puede ser diferente y que puede utilizarse además con dispositivos y redes de comunicaciones móviles no relacionados con el dispositivo iPhone. La arquitectura 100 incluye un dispositivo móvil 102, tal como el dispositivo iPhone, y una o más tarjetas SIM 104 que pueden insertarse en el dispositivo móvil 102. Las tarjetas SIM 104 permiten al dispositivo registrarse con y utilizar una red de comunicaciones móviles 118 gestionada por un proveedor de servicios asociado con una de las tarjetas SIM 104 y/o el dispositivo 102.

El dispositivo móvil 102 puede comunicarse además con un cliente de activación 108 que funciona en un ordenador personal (PC) 106 u otro tipo de dispositivo informático con el que el dispositivo 102 está conectado. El cliente de activación 108 está en comunicación con uno o más servidores de activación 110, normalmente a través de una red 116. La red 116 puede ser cualquier inter-red privada o pública u otro tipo de trayectoria de comunicaciones a través de la cual pueden transmitirse las comunicaciones entre el cliente de activación 108 y el servidor de activación 110. El servidor de activación 110 puede comunicarse, a su vez, con servidores de procesamiento 112 del proveedor de servicios y con una base de datos de proveedor de servicio 114 que puede contener información relacionada con los abonados y dispositivos que pueden registrarse con y utilizar la red de comunicaciones móviles 118 del proveedor de servicios.

La FIG. 2 es una visión general en forma de diagrama de bloques de componentes 200 seleccionados de un dispositivo móvil 100 según una forma de realización a modo de ejemplo de la invención. El dispositivo móvil 100 puede incluir un procesador de aplicaciones (AP) 202 que se utiliza para llevar a cabo algunas de las funciones del sistema de activación de proveedor de servicios según una forma de realización de la invención. El AP 202 se implementa normalmente como firmware que funciona junto con un circuito integrado de banda base (BB) 204. Entre otras cosas, la BB 204 proporciona la plataforma de sistema operativo en la que se llevan a cabo las funciones del dispositivo móvil. En una forma de realización típica, la BB 204 incorpora un IMEI 206 almacenado que identifica de manera única el dispositivo móvil, así como una clave de oscurecimiento compartida 208, cuya utilización se describirá posteriormente en detalle con referencia al procesamiento de la etiqueta de activación. El dispositivo 100 incluye además un componente de memoria 210 que incluye una memoria volátil y una memoria no volátil que pueden utilizarse para almacenar, entre otras cosas, las etiquetas de activación utilizadas en el sistema de activación de proveedor de servicios que se describirá posteriormente en mayor detalle.

El dispositivo móvil 100 puede incluir además una ranura de tarjeta SIM en la que puede insertarse una tarjeta SIM 212. La tarjeta SIM 212 puede incluir un ICCID 214 que identifica de manera única la tarjeta SIM 212 y un IMSI 216 que designa al abonado y que se utiliza para proporcionar la red de comunicaciones móviles 118 con la que el dispositivo va a utilizarse.

La FIG. 3 es una visión general en forma de diagrama de bloques de un sistema de activación de proveedor de servicios según una forma de realización a modo de ejemplo de la invención. Tal y como se ilustra, con una BB 294 y un AP 208 puede haberse insertado una de tres tarjetas SIM 302, la tarjeta SIM A 302A, la tarjeta SIM B 302B y la tarjeta SIM C 302C. Debe entenderse que el dispositivo 100 puede utilizarse con una cualquiera de una pluralidad de tarjetas SIM, y que las tres tarjetas SIM se ilustran solamente como un ejemplo.

En una forma de realización, el dispositivo móvil 100 puede ser un dispositivo “genérico”, lo que quiere decir que se fabricó sin un bloqueo de proveedor de servicios. Un dispositivo sin un bloqueo de proveedor de servicios puede utilizarse con una cualquiera de las tarjetas SIM A, B y C, 302A, B y C. En otras formas de realización, el dispositivo móvil 100 puede haberse bloqueado anteriormente de manera que no puede utilizarse con las tarjetas SIM A, B y C a no ser que se desbloquee primero. Una vez que el dispositivo 100 está desbloqueado, por lo general puede funcionar solamente en un modo de servicio limitado, lo que quiere decir que sólo puede utilizarse para llamadas de emergencia y que todavía no está activado en una red de proveedor de servicios.

En una forma de realización, tras detectar la inserción de una de las tarjetas SIM A, B o C, 302, o, como alternativa, cuando la BB 204 arranca, el AP 208 determina si ya hay almacenada una etiqueta de activación 308 asociada con la tarjeta SIM A, B o C insertada. Si no es así, el AP 208 inicia un proceso de firma emitiendo una solicitud de activación 304 al servidor de activación 110. La solicitud de activación 304 comprende información del dispositivo 100 y de la tarjeta SIM 302 actualmente insertada, incluyendo, por ejemplo, los valores del IMEI 206, el IMSI 216 y el ICCID 214, que se introducen en la solicitud de activación 304.

En una forma de realización, tras recibir la solicitud de activación 304, el servidor de activación 110 determina si generar una etiqueta de activación 306 basándose en la información que se introdujo en la solicitud de activación 304. Una etiqueta de activación 306 incorpora información de identificación tanto del dispositivo 100 como de la tarjeta SIM A, B, o C insertada, utilizando una lógica de generación de etiquetas 310 y un par de claves pública/privada de activación 312 tal y como se describirá en mayor detalle con referencia a la FIG. 4.

En una forma de realización típica, la determinación de si generar una etiqueta de activación 306 dependerá, al menos en parte, de si el servidor de proveedor de servicios 112 y/o la base de datos de proveedor de servicios 114 indican que el IMSI 216 introducido en la solicitud de activación puede activarse en la red de comunicaciones 118 del proveedor de servicios. En algunas formas de realización, la determinación de si generar la etiqueta de activación dependerá de otras consideraciones de política, tales como si generar una etiqueta de activación 306 para un par IMEI/ICCID dado (utilizando el IMEI/ICCID que se introdujo en la solicitud de activación 304). Si el servidor de activación 110 determina que no puede generar una etiqueta de activación 306, entonces la solicitud de activación 304 se desestimará.

En una forma de realización, una vez que se ha generado la etiqueta de activación 306, el servidor de activación 110 oscurece el contenido de la etiqueta de activación 306 antes de enviar la etiqueta al dispositivo 100 para proteger los contenidos de la etiqueta de activación. En una forma de realización, la etiqueta de activación 306 se oscurece cifrándola con una clave simétrica por dispositivo. La clave simétrica por dispositivo puede obtenerse a partir de datos únicos relacionados con el dispositivo 100 y una clave compartida entre el dispositivo y el servidor de activación 110. En el ejemplo ilustrado se refiere a la clave compartida como una Clave de Oscurecimiento Compartida 208 en el dispositivo 100, y también se almacena como una de las Claves 312 definidas en el servidor de activación 110. Como un ejemplo, se refiere a la clave simétrica por dispositivo como una Clave de Oscurecimiento de Dispositivo y se obtiene utilizando la huella digital de hardware del dispositivo 100 y la Clave de Oscurecimiento Compartida almacenada en el servidor en las Claves 312 utilizando el siguiente algoritmo:

ClaveOscurecimientoDispositivo = SHA-1(HuellaDigitalHardware || ClaveOscurecimientoCompartida)

Después de que la etiqueta de activación 306 se haya generado y cifrado, la etiqueta de activación 306 está lista para enviarse al dispositivo 100, donde se almacena junto con cualquier otra etiqueta de activación 308 previamente almacenada. Las etiquetas de activación 308A, B y C almacenadas pueden utilizarse posteriormente por el AP 208 para iniciar el proceso de activación, tal y como se describirá en mayor detalle con referencia a las FIG. 5A y 5B.

En una forma de realización, el formato de la etiqueta de activación 306/308 es como se muestra en la Tabla 1. El formato de la clave pública de activación que está incluida en la etiqueta de activación es como se muestra en la Tabla 2.

Tabla 1 - Formato de Etiqueta de Activación

NOMBRE	TAMAÑO (Octetos)	CODIFICACIÓN
Versión	1	BCD
Activación ClavePública	N	Clave Pública
ICCID	10	BCD
IMSI	8	BCD
IMEI	8	BCD
Huella digital de hardware	20	Binaria
FirmaEtiqueta	Longitud de clave / 8	Binaria

Tabla 2 - Formato de Clave Pública de Activación

NOMBRE	TAMAÑO (Octetos)	CODIFICACIÓN
Longitud de Registro	4	Binaria
Número de Serie	4	Binaria
LongitudClave	4	Binaria
Exponente	4	Binaria
Módulo	Longitud de Clave / 8	Binaria
Factor de Montgomery	Longitud de Clave / 8	Binaria
FirmaClave	Longitud de Mclave / 8	Binaria

En una forma de realización, el campo Versión de la etiqueta de activación 306/308 permite que el procesamiento de las etiquetas de activación sea compatible hacia delante. En una forma de realización, el número entero codificado Versión permite futuras versiones de firmware en el dispositivo 100 para reconocer etiquetas de activación más antiguas y soportarlas. La Versión también está incluida en el compendio de la etiqueta de activación para verificar que no pueda alterarse. En una forma de realización, la BB 204 tendrá una versión de registro mínima incluida en la misma que puede impedir ataques de anulación si se ha vulnerado un formato de etiqueta de activación.

En una forma de realización, el campo Clave Pública de Activación de la etiqueta de activación 306/308 puede formatearse tal y como se muestra en la Tabla 2. Sin embargo, debe observarse que pueden utilizarse otros formatos de clave pública con apartarse del alcance de las reivindicaciones que siguen.

El ICCID (ID de tarjeta de circuito integrado) es un número de 20 dígitos, definido en la norma ISO/IEC 7812-1 que consiste en: un identificador de industria principal de 2 dígitos (89 para las SIM), un código de país de 1 a 3 dígitos (ITU-T E.164), un código de identificador de emisor, de 1 a 4 dígitos (dependiendo de la longitud del código de país), que contiene normalmente el MNC de la red de emisión, un número de identificación de cuenta individual, y una suma de control de 1 dígito.

El IMSI (identificador internacional de abonado móvil) es un número de 15 dígitos, definido en la norma 3GPP TS 23.003 que consiste en un código de país de móvil (MCC) de 3 dígitos, un código de red móvil (MNC) de 2 ó 3 dígitos y un número de identidad de abonado móvil (MSIN) de 9 ó 10 dígitos.

En una forma de realización, la huella digital de hardware es un valor que se obtiene normalmente a partir de datos que son únicos para el dispositivo, tales como los números de serie de los componentes de hardware del dispositivo y el IMEI, más una secuencia aleatoria definida. Por ejemplo, en una forma de realización, la huella digital puede calcularse de la siguiente manera:

HuellaDigitalHardware = SHA-1(SOro-NúmeroSerie || NúmeroSerieFlash || IMEI || Salt), donde Salt es una secuencia aleatoria.

En una forma de realización, la firma de la etiqueta se genera de la siguiente manera:

Mensaje = Versión || ICCID || IMSI || IMEI, || HuellaDigitalHardware

Hash = SHA-1(Mensaje)

MensajeCodificado = 0x00 || 0x04 || CadenaRelleno || 0x00 | Hash

FirmaEtiqueta = RSACifrar (ClavePrivadaActivación, MensajeCodificado)

Debe observarse que el formato descrito de la etiqueta de activación 306/308 expuesta en la Tabla 1 es solamente un ejemplo de un formato que puede utilizarse, y que otros formatos y campos de datos pueden comprender la etiqueta de activación sin apartarse del alcance de las reivindicaciones posteriores.

Las FIGS. 4, 5A y 5B son diagramas de flujo que ilustran determinados aspectos de la activación de proveedor de servicios según una forma de realización a modo de ejemplo de la invención. En la FIG. 4 se describe un procedimiento para un proceso de firma de proveedor de servicios 400. El procedimiento 400 que va a llevarse a cabo comienza en el bloque 402, en el que el dispositivo 100 detecta un arranque de banda base o la inserción de una nueva tarjeta SIM. En el bloque 404, el procedimiento 400 introduce el IMSI, el ICCID, el IMEI y una huella digital de hardware en una solicitud de activación, y envía la solicitud desde el dispositivo hasta un servidor de activación. En el bloque 406, el servidor de activación recibe la solicitud y determina si generar una etiqueta de activación como respuesta a la solicitud basándose en determinadas consideraciones de política, tal como si los servidores de procesamiento asociados con el proveedor de servicios confirman que la información IMSI es válida para la red de comunicaciones del proveedor de servicios.

En una forma de realización, en el bloque de proceso 408, el procedimiento 400 genera la etiqueta de activación utilizando la información de ICCID, de IMSI, de IMEI y de huella digital de hardware que se introdujo en la solicitud de activación. En una forma de realización, el procedimiento 400 incluye una clave pública de activación en la etiqueta, y en el bloque 410 firma la etiqueta utilizando una clave privada de activación correspondiente que está almacenada de manera segura en el servidor de activación. En el bloque 412, el procedimiento 400 oscurece los contenidos de la etiqueta de activación cifrando los contenidos con una clave de oscurecimiento de dispositivo que se obtiene a partir de información específica del dispositivo, tal como la huella digital de hardware prevista en la solicitud de activación, y una clave de oscurecimiento compartida que está disponible para el servidor de activación y para el dispositivo. En el bloque de proceso 414, el procedimiento 400 concluye con el envío de la etiqueta de activación al dispositivo para su almacenamiento. Por ejemplo, la etiqueta de activación puede almacenarse en la memoria del dispositivo que es accesible para la banda base del dispositivo.

Haciendo referencia ahora a las FIGS. 5A y 5B se describe un procedimiento para un proceso de activación de proveedor de servicios 500. El procedimiento 500 que va a llevarse a cabo comienza en el bloque 502, en el que el dispositivo 100 consulta durante el arranque el ICCID de la tarjeta SIM actualmente insertada. En el bloque 504, el procedimiento 500 utiliza el ICCID para buscar una etiqueta de activación correspondiente al ICCID actual. En el bloque 506, el dispositivo emite un comando para iniciar la verificación del la etiqueta de activación. La verificación de la etiqueta de activación hará que la banda base del dispositivo salga del modo de servicio limitado y que se registre en una red de comunicaciones. El comando devolverá un código de error si la etiqueta no puede verificarse de manera satisfactoria.

En una forma de realización típica, el procedimiento 500 lleva a cabo la verificación de etiqueta después de determinar si la tarjeta SIM actualmente insertada en el dispositivo está en un estado preparado, es decir, si la SIM está desbloqueada. Si no, entonces el procedimiento 500 lleva a cabo la verificación de etiqueta después de que la tarjeta SIM se haya desbloqueado de manera satisfactoria.

El procedimiento 500 continúa en los bloques de proceso 508A a 508H para llevar a cabo los diversos aspectos de la verificación de etiqueta de activación. En el bloque 508A, el procedimiento 500 verifica en primer lugar que no se haya superado el cómputo de reintentos. Un contador de reintentos se incrementará para cada intento no satisfactorio de desbloquear y activar el servicio en el dispositivo utilizando el comando de verificación de etiqueta de activación. Solo se permite un número predefinido de intentos en la verificación para impedir ataques de fuerza bruta, donde se producen numerosos intentos de activar el dispositivo.

En una forma de realización, el procedimiento 500 continúa en los bloques 508B/508C para analizar la información de versión de la etiqueta de activación a partir de la información cifrada y para determinar si la versión de la etiqueta de activación que va a verificarse se soporta en la versión actual de la banda base del dispositivo.

En el bloque 508D, el procedimiento 500 descifra los contenidos de la etiqueta de activación utilizando una clave de

oscurecimiento de dispositivo que se obtiene a partir de la clave de oscurecimiento compartida almacenada en el dispositivo y de información que es específica del dispositivo, tal como la huella digital de hardware del dispositivo. En el bloque 508E, el procedimiento 500 valida la clave pública de activación suministrada en la etiqueta de activación, y en 508F utiliza la clave pública para validar la firma de etiqueta. En los bloques 508G/H, el procedimiento 500 finaliza el proceso de verificación de etiqueta verificando si el valor hash descrifrado de la etiqueta de activación se compara correctamente con el valor hash calculado. Si es así, el procedimiento continúa en el bloque de proceso 510; en caso contrario, la verificación de etiqueta falla y el procedimiento avanza hasta el bloque 516.

En el bloque de proceso 510, con el fin de impedir que una etiqueta de activación de un dispositivo se utilice en otro dispositivo, el IMEI de la etiqueta de activación se compara con el IMEI almacenado en el dispositivo. En una forma de realización, los 15 dígitos de los IMEI respectivos deben coincidir. Si no coinciden, la etiqueta de activación BB

En el bloque de proceso 512, el procedimiento 500 procede a verificar la etiqueta de activación determinando el valor de la huella digital de hardware contenida en la etiqueta de activación y comparándolo con la huella digital de hardware del dispositivo. Si no coinciden, la etiqueta de activación se trata como no válida.

En el bloque de proceso 514, el procedimiento 500 procede a verificar la etiqueta de activación comparando el valor del ICCID contenido en la etiqueta de activación con el ICCID de la tarjeta SIM actualmente insertada en el dispositivo. En casos especiales se omite la verificación del ICCID, como cuando el ICCID está codificado con 10 octetos 0xFF. Asimismo, en el bloque de proceso 516, el procedimiento 500 procede a verificar la etiqueta de activación comparando el valor del IMSI contenido en la etiqueta de activación con el IMSI de la tarjeta SIM actualmente insertada en el dispositivo. Nuevamente, en casos especiales, se omite la verificación del IMSI, como cuando el IMS está codificado con 10 octetos 0xFF.

En el bloque de proceso 516, el procedimiento incrementa el contador de reintentos y devuelve un error como respuesta al comando en caso de que falle alguno de los procesos de verificación de etiqueta de activación. En el bloque de proceso 518, si los procesos de verificación tienen éxito, entonces el dispositivo puede activar el servicio en el dispositivo iniciando el registro del dispositivo en la red de comunicaciones móviles del proveedor de servicios.

La FIG. 6 ilustra un ejemplo de un sistema informático típico en el que puede llevarse a la práctica algunos aspectos de la invención, tales como los clientes y servidores de procesamiento utilizados para proporcionar la activación de servicio de un dispositivo móvil. Debe observarse que aunque la FIG. 6 ilustra varios componentes de un sistema informático, no pretende representar ninguna arquitectura o manera particular de interconectar los componentes, ya que tales detalles no son pertinentes a la presente invención. Además, debe apreciarse que ordenadores de red y otros sistemas de procesamiento de datos que tengan menos componentes o quizás más componentes también pueden utilizarse con la presente invención. El sistema informático de la FIG. 6 puede ser, por ejemplo, un ordenador Macintosh de Apple Computer, Inc.

Tal y como se muestra en la FIG. 6, el sistema informático 601, que es una forma de un sistema de procesamiento de datos, incluye un bus 602 que está acoplado a un(os) microprocesador(es) 603, una ROM (memoria de solo lectura) 607, una RAM volátil 605 y una memoria no volátil 606. En una forma de realización, el microprocesador 603 puede ser un microprocesador G3 o G4 de Motorola, Inc., o uno o más microprocesadores G5 de IBM. El bus 602 interconecta estos diversos componentes entre sí y también interconecta estos componentes 603, 607, 605 y 606 a un controlador de visualización y dispositivo de visualización 604 y a dispositivos periféricos tales como dispositivos de entrada/salida (E/S) que pueden ser ratones, teclados, módems, interfaces de red, impresoras y otros dispositivos que son ampliamente conocidos en la técnica. Normalmente, los dispositivos de entrada/salida 609 se acoplan al sistema a través de controladores de entrada/salida 608. La RAM volátil (memoria de acceso aleatorio) 605 se implementa normalmente como una RAM dinámica (DRAM) que requiere energía continuamente para refrescar o mantener los datos en la memoria. El almacenamiento masivo 606 es normalmente un disco duro magnético, una unidad óptica magnética, una unidad óptica, una RAM de DVD u otros tipos de sistemas de memoria que mantienen datos (por ejemplo, grandes cantidades de datos) incluso después de apagar el sistema. Normalmente, el almacenamiento masivo 606 será además una memoria de acceso aleatorio, aunque esto no es necesario. Aunque la FIG. 6 muestra que el almacenamiento masivo 606 es un dispositivo local directamente acoplado al resto de los componentes del sistema de procesamiento de datos, debe apreciarse que la presente invención puede utilizar una memoria no volátil que sea remota al sistema, tal como un dispositivo de almacenamiento de red que esté acoplado al sistema de procesamiento de datos a través de una interfaz de red tal como un módem o una interfaz Ethernet. El bus 602 puede incluir uno o más buses conectados entre sí a través de varios puentes, controladores y/o adaptadores, tal y como se conoce ampliamente en la técnica. En una forma de realización, el controlador de E/S 608 incluye un adaptador USB (bus serie universal) para controlar dispositivos periféricos USB y un controlador IEEE 1394 para dispositivos periféricos compatibles con la norma IEEE 1394.

A partir de esta descripción resultará evidente que los aspectos de la presente invención pueden realizarse, al menos en parte, en software. Es decir, las técnicas pueden llevarse a cabo en un sistema informático o en otro sistema de procesamiento de datos como respuesta a su procesador, tal como un microprocesador, que ejecuta secuencias de instrucciones contenidas en una memoria, tal como la ROM 607, la RAM 605, el almacenamiento

masivo 606 o un dispositivo de almacenamiento remoto. En varias formas de realización, puede utilizarse un sistema de circuitos cableado en combinación con instrucciones de software para implementar la presente invención. Por lo tanto, las técnicas no están limitadas a ninguna combinación específica de software y sistemas de circuitos de hardware, ni a ninguna fuente particular para las instrucciones ejecutadas por el sistema de procesamiento de datos. Además, a través de esta descripción, varias funciones y operaciones se describen como llevadas a cabo o causadas por código de software para simplificar la descripción. Sin embargo, los expertos en la técnica reconocerán que lo indicado por tales expresiones es que las funciones resultan de la ejecución del código mediante un procesador, tal como el microprocesador 603.

REIVINDICACIONES

1. Un procedimiento implementado por máquina para activar un dispositivo móvil (100), comprendiendo el procedimiento:

emitir desde un dispositivo móvil que tiene una tarjeta SIM (302A, 302B, 302C) actualmente insertada una solicitud de activación, comprendiendo la solicitud de activación (304) datos que identifican de manera única el dispositivo y datos que identifican de manera única la tarjeta SIM actualmente insertada;
almacenar en el dispositivo móvil un registro de activación firmado (308) que comprende los datos de dispositivo y los datos de tarjeta SIM, habiéndose generado y firmado el registro de activación por un servidor de activación (110) respondiendo a la solicitud de activación (304);
verificar el registro de activación con respecto a la tarjeta SIM (302A, 302B, 302C) actualmente insertada; y
registrar el dispositivo con una red de comunicaciones después de verificar de manera satisfactoria el registro de activación.

2. El procedimiento según reivindicación 1, en el que los datos que identifican de manera única el dispositivo incluyen un número de serie del dispositivo.

3. El procedimiento según reivindicación 2, en el que el número de serie del dispositivo es el identificador internacional de equipo móvil (IMEI) codificado en el dispositivo.

4. El procedimiento según reivindicación 1, en el que los datos que identifican de manera única el dispositivo incluyen una huella digital de hardware del dispositivo.

5. El procedimiento según reivindicación 4, en el que la huella digital de hardware del dispositivo se obtiene a partir de al menos uno de entre un número de serie de un componente de banda base del dispositivo, un número de serie de un componente de memoria del dispositivo, un número de serie del dispositivo, en combinación con un número aleatorio.

6. El procedimiento según reivindicación 1, en el que los datos que identifican de manera única la tarjeta SIM incluyen un número de serie de la tarjeta SIM.

7. El procedimiento según reivindicación 1, en el que los datos que identifican de manera única la tarjeta SIM incluyen un identificador de abonado asociado con la tarjeta SIM.

8. El procedimiento según reivindicación 1, en el que el registro de activación almacenado en el dispositivo comprende además una clave pública de activación, habiéndose firmado el registro de activación por el servidor de activación utilizando una clave privada de activación correspondiente a la clave pública de activación.

9. El procedimiento según reivindicación 1, en el que verificar el registro de activación almacenado en el dispositivo comprende además descifrar un contenido del registro de activación utilizando una clave de oscurecimiento de dispositivo que se obtiene a partir de una huella digital de hardware del dispositivo y una clave de oscurecimiento compartida.

10. El procedimiento según reivindicación 1, en el que verificar el registro de activación almacenado en el dispositivo comprende además validar una clave pública de activación contenida en el registro de activación.

11. El procedimiento según reivindicación 10, en el que verificar el registro de activación almacenado en el dispositivo comprende además validar una firma del registro de activación almacenado en el dispositivo utilizando la clave pública de activación validada.

12. El procedimiento según reivindicación 1, en el que verificar el registro de activación almacenado en el dispositivo comprende además verificar que un contador máximo de reintentos no haya alcanzado un cómputo máximo.

13. El procedimiento según reivindicación 1, que comprende además incrementar un contador máximo de reintentos cuando el registro de activación no se verifica de manera satisfactoria.

14. Un medio de almacenamiento legible por máquina que almacena instrucciones de programa que, cuando se ejecutan, hacen que un sistema de procesamiento de datos lleve a cabo un procedimiento según una cualquiera de las reivindicaciones 1 a 13.

15. Un sistema de procesamiento de datos, que comprende:

medios para emitir desde un dispositivo móvil que tiene una tarjeta SIM actualmente insertada una solicitud de activación, comprendiendo la solicitud de activación datos que identifican de manera única el dispositivo y datos que identifican de manera única la tarjeta SIM actualmente insertada;

medios para almacenar en el dispositivo móvil un registro de activación firmado que comprende los datos de dispositivo y los datos de tarjeta SIM, habiéndose generado y firmado el registro de activación por un servidor de activación respondiendo a la solicitud de activación;

medios para verificar el registro de activación con respecto a la tarjeta SIM actualmente insertada; y

medios para registrar el dispositivo con una red de comunicaciones después de verificar de manera satisfactoria el registro de activación.

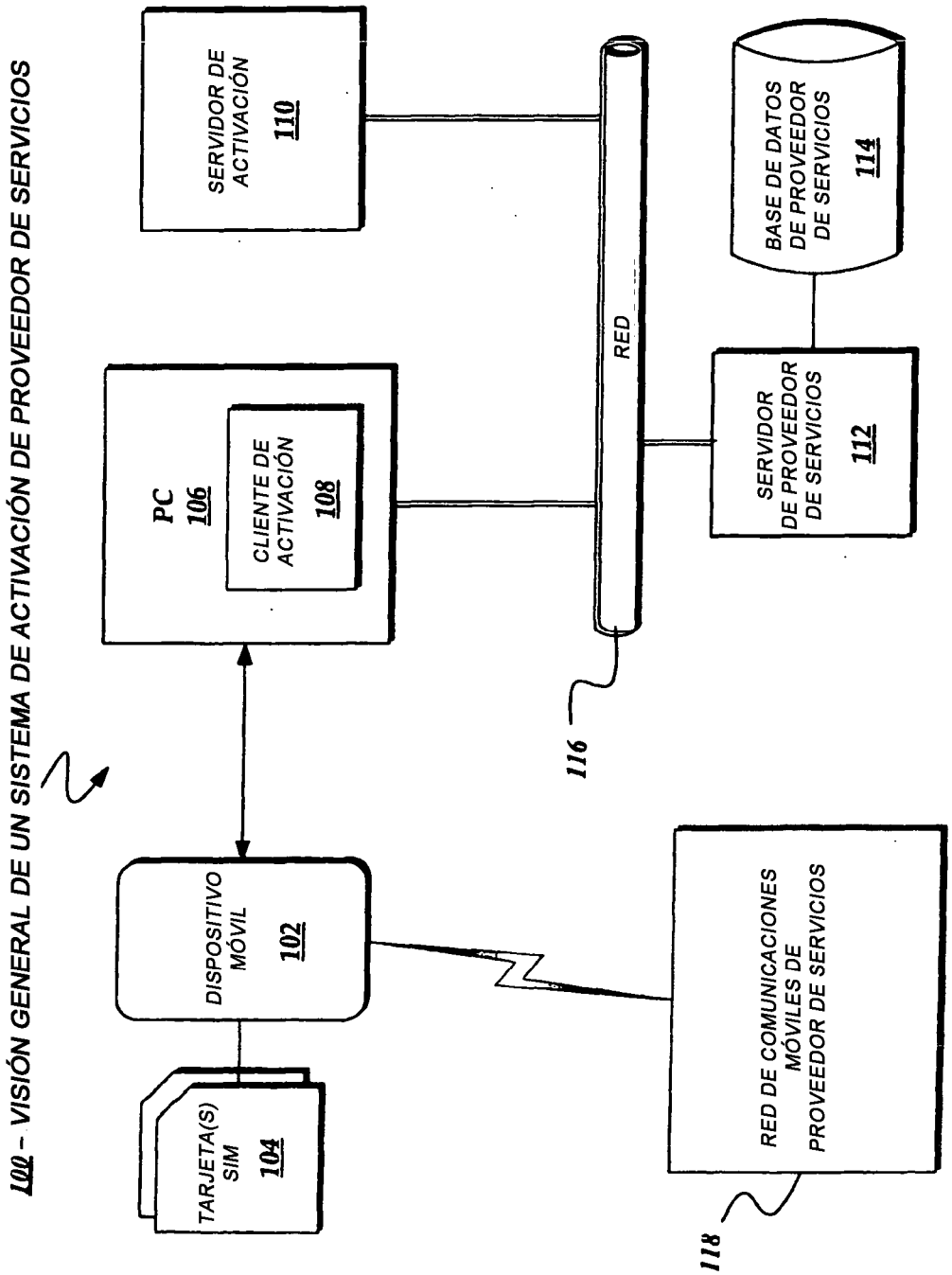
100 - VISIÓN GENERAL DE UN SISTEMA DE ACTIVACIÓN DE PROVEEDOR DE SERVICIOS
SERVIDOR DE ACTIVACIÓN 110
PC 106
CLIENTE DE ACTIVACIÓN 108
RED
BASE DE DATOS DE PROVEEDOR DE SERVICIOS 114
SERVIDOR DE PROVEEDOR DE SERVICIOS 112
116
DISPOSITIVO MÓVIL 102
TARJETA(S) SIM 104
RED DE COMUNICACIONES MÓVILES DE PROVEEDOR DE SERVICIOS
118

Fig. 1.

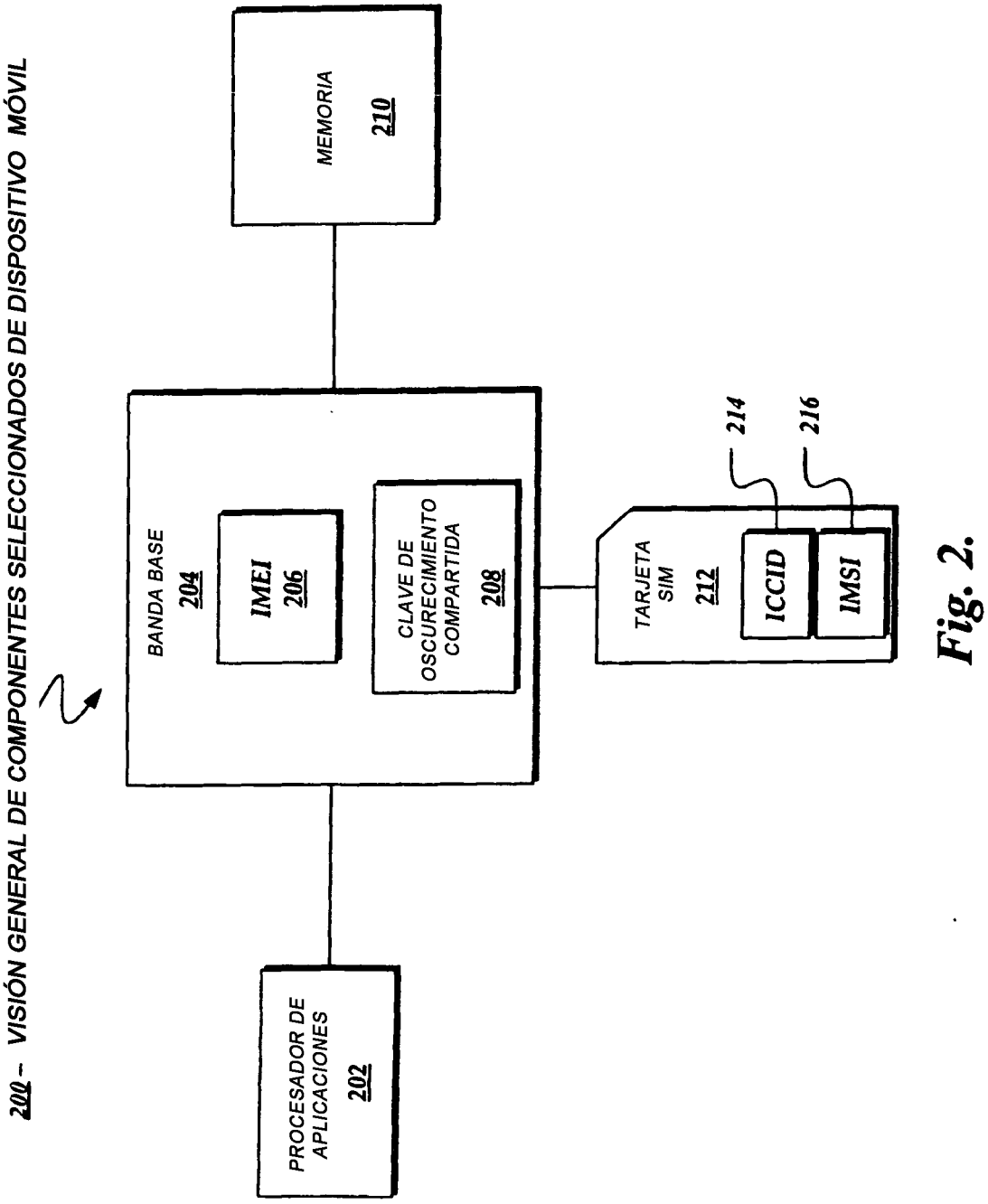
200 – VISIÓN GENERAL DE COMPONENTES SELECCIONADOS DE DISPOSITIVO MÓVIL
MEMORIA
210
BANDA BASE
204
IMEI
206
CLAVE DE OSCURECIMIENTO COMPARTIDA
208
PROCESADOR DE APLICACIONES
202
TARJETA SIM
212
214
216
ICCID
IMSI

Fig. 2.

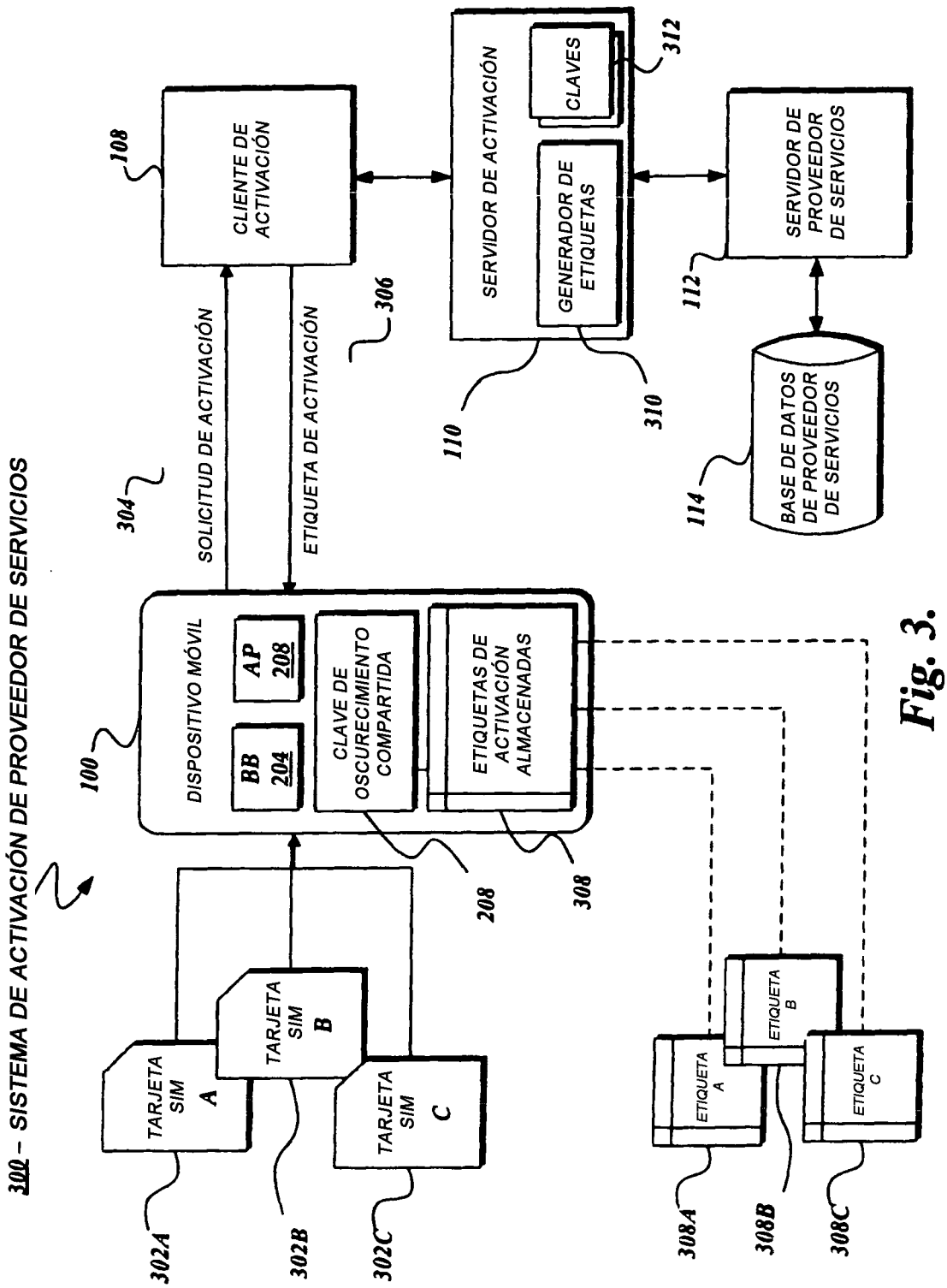
300 – SISTEMA DE ACTIVACIÓN DE PROVEEDOR DE SERVICIOS
100
DISPOSITIVO MÓVIL
BB 204
AP 208
CLAVE DE OSCURECIMIENTO COMPARTIDA
ETIQUETAS DE ACTIVACIÓN ALMACENADAS
208
308
304
SOLICITUD DE ACTIVACIÓN
ETIQUETA DE ACTIVACIÓN
306
108
CLIENTE DE ACTIVACIÓN
SERVIDOR DE ACTIVACIÓN
CLAVES
312
GENERADOR DE ETIQUETAS
110
310
SERVIDOR DE PROVEEDOR DE SERVICIOS
112
BASE DE DATOS DE PROVEEDOR DE SERVICIOS
114
TARJETA SIM A
TARJETA SIM B
TARJETA SIM C
302A
302B
302C
ETIQUETA A
ETIQUETA B
ETIQUETA C
308A
308B
308C

Fig. 3.

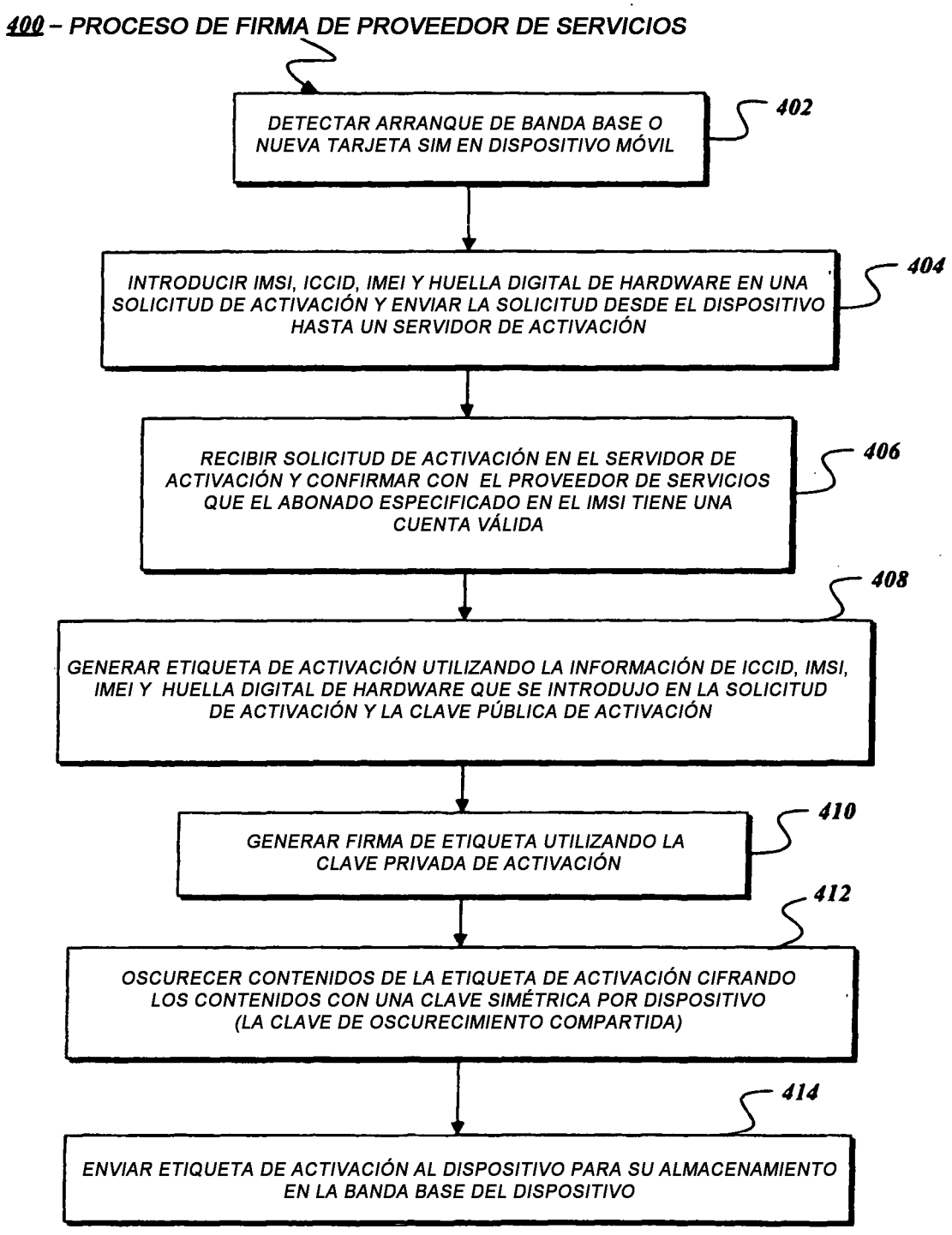
400 – PROCESO DE FIRMA DE PROVEEDOR DE SERVICIOS
DETECTAR ARRANQUE DE BANDA BASE O NUEVA TARJETA SIM EN DISPOSITIVO MÓVIL
402
INTRODUCIR IMSI, ICCID, IMEI Y HUELLA DIGITAL DE HARDWARE EN UNA SOLICITUD DE ACTIVACIÓN Y ENVIAR LA SOLICITUD DESDE EL DISPOSITIVO HASTA UN SERVIDOR DE ACTIVACIÓN
404
RECIBIR SOLICITUD DE ACTIVACIÓN EN EL SERVIDOR DE ACTIVACIÓN Y CONFIRMAR CON EL PROVEEDOR DE SERVICIOS QUE EL ABONADO ESPECIFICADO EN EL IMSI TIENE UNA CUENTA VÁLIDA
406
408
GENERAR ETIQUETA DE ACTIVACIÓN UTILIZANDO LA INFORMACIÓN DE ICCID, IMSI, IMEI Y HUELLA DIGITAL DE HARDWARE QUE SE INTRODUJO EN LA SOLICITUD DE ACTIVACIÓN Y LA CLAVE PÚBLICA DE ACTIVACIÓN
GENERAR FIRMA DE ETIQUETA UTILIZANDO LA CLAVE PRIVADA DE ACTIVACIÓN
410
412
OSCURECER CONTENIDOS DE LA ETIQUETA DE ACTIVACIÓN CIFRANDO LOS CONTENIDOS CON UNA CLAVE SIMÉTRICA POR DISPOSITIVO (LA CLAVE DE OSCURECIMIENTO COMPARTIDA)
414
ENVIAR ETIQUETA DE ACTIVACIÓN AL DISPOSITIVO PARA SU ALMACENAMIENTO EN LA BANDA BASE DEL DISPOSITIVO

Fig. 4.

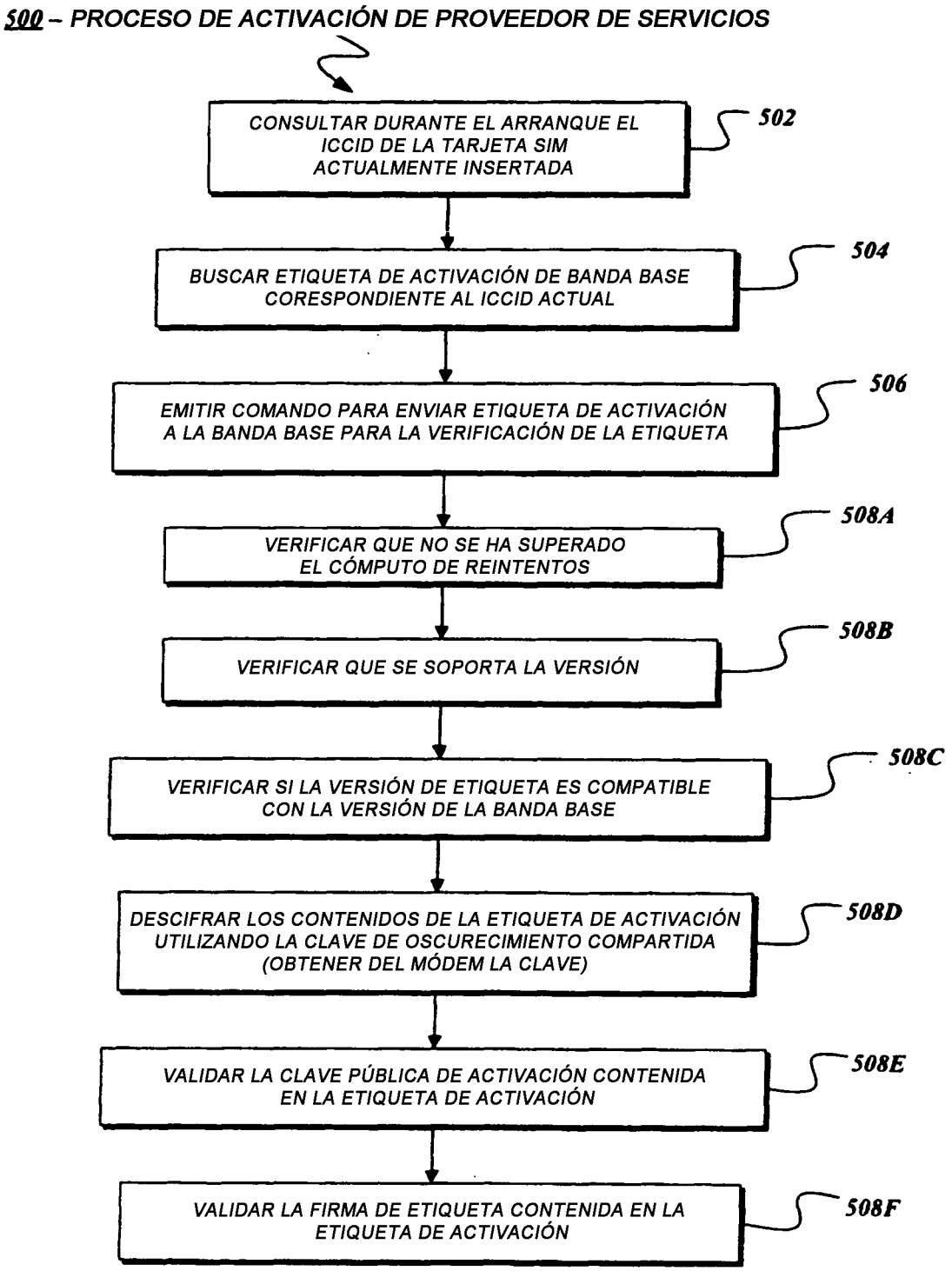
500 – PROCESO DE ACTIVACIÓN DE PROVEEDOR DE SERVICIOS
CONSULTAR DURANTE EL ARRANQUE EL ICCID DE LA TARJETA SIM ACTUALMENTE INSERTADA
502
BUSCAR ETIQUETA DE ACTIVACIÓN DE BANDA BASE CORESPONDIENTE AL ICCID ACTUAL
504
EMITIR COMANDO PARA ENVIAR ETIQUETA DE ACTIVACIÓN A LA BANDA BASE PARA LA VERIFICACIÓN DE LA ETIQUETA
506
VERIFICAR QUE NO SE HA SUPERADO EL CÓMPUTO DE REINTENTOS
508A
VERIFICAR QUE SE SOPORTA LA VERSIÓN
508B
VERIFICAR SI LA VERSIÓN DE ETIQUETA ES COMPATIBLE CON LA VERSIÓN DE LA BANDA BASE
508C
DESCIFRAR LOS CONTENIDOS DE LA ETIQUETA DE ACTIVACIÓN UTILIZANDO LA CLAVE DE OSCURECIMIENTO COMPARTIDA (OBTENER DEL MÓDEM LA CLAVE)
508D
VALIDAR LA CLAVE PÚBLICA DE ACTIVACIÓN CONTENIDA EN LA ETIQUETA DE ACTIVACIÓN
508E
VALIDAR LA FIRMA DE ETIQUETA CONTENIDA EN LA ETIQUETA DE ACTIVACIÓN
508F

Fig. 5A.

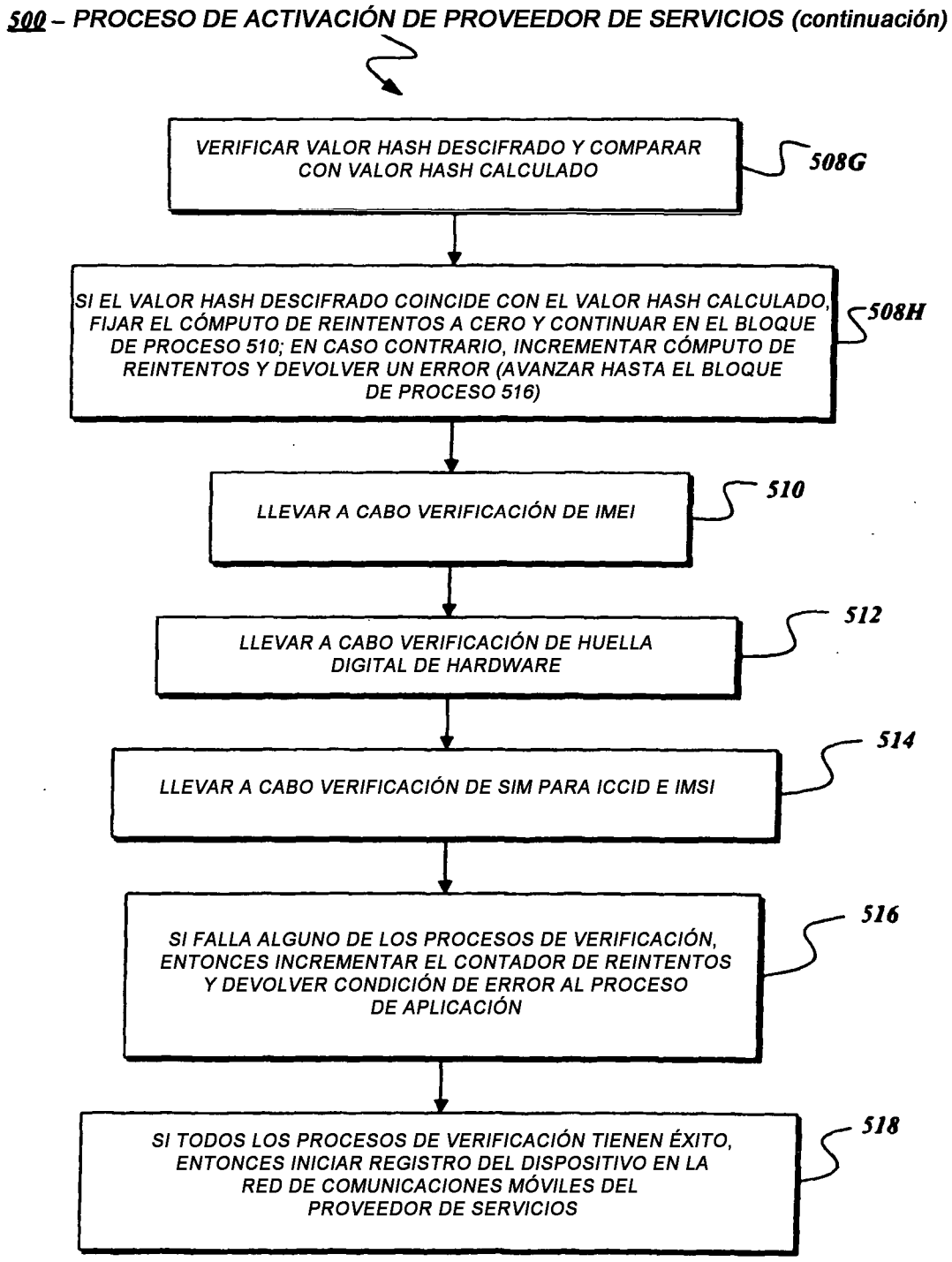
500 – PROCESO DE ACTIVACIÓN DE PROVEEDOR DE SERVICIOS (continuación)
VERIFICAR VALOR HASH DESCIFRADO Y COMPARAR CON VALOR HASH CALCULADO
508G
SI EL VALOR HASH DESCIFRADO COINCIDE CON EL VALOR HASH CALCULADO, FIJAR EL CÓMPUTO DE REINTENTOS A CERO Y CONTINUAR EN EL BLOQUE DE PROCESO 510; EN CASO CONTRARIO, INCREMENTAR CÓMPUTO DE REINTENTOS Y DEVOLVER UN ERROR (AVANZAR HASTA EL BLOQUE DE PROCESO 516)
508H
LLEVAR A CABO VERIFICACIÓN DE IMEI
510
LLEVAR A CABO VERIFICACIÓN DE HUELLA DIGITAL DE HARDWARE
512
LLEVAR A CABO VERIFICACIÓN DE SIM PARA ICCID E IMSI
514
SI FALLA ALGUNO DE LOS PROCESOS DE VERIFICACIÓN, ENTONCES INCREMENTAR EL CONTADOR DE REINTENTOS Y DEVOLVER CONDICIÓN DE ERROR AL PROCESO DE APLICACIÓN
516
SI TODOS LOS PROCESOS DE VERIFICACIÓN TIENEN ÉXITO, ENTONCES INICIAR REGISTRO DEL DISPOSITIVO EN LA RED DE COMUNICACIONES MÓVILES DEL PROVEEDOR DE SERVICIOS
518

Fig. 5B.

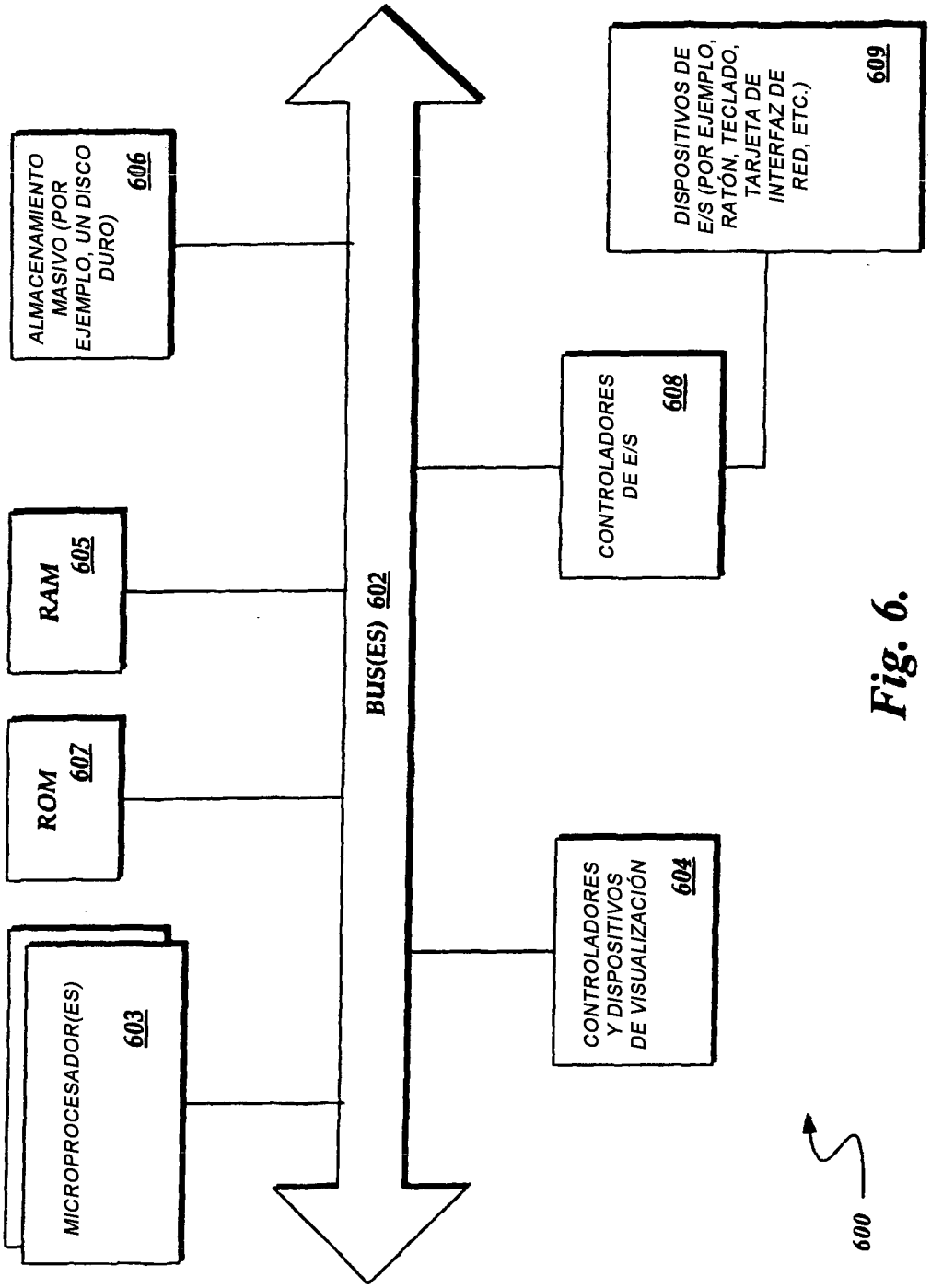
MICROPROCESADOR(ES) 603
ROM 607
RAM 605
ALMACENAMIENTO MASIVO (POR EJEMPLO, UN DISCO DURO) 606
BUS(ES) 602
CONTROLADORES Y DISPOSITIVOS DE VISUALIZACIÓN 604
CONTROLADORES DE E/S 608
DISPOSITIVOS DE E/S (POR EJEMPLO, RATÓN, TECLADO, TARJETA DE INTERFAZ DE RED, ETC.) 609
600

Fig. 6.