(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 751 081**

(51) Int. Cl.:

H04W 12/04	(2009.01)
H04W 12/06	(2009.01)
H04L 12/22	(2006.01)
H04L 29/06	(2006.01)
H04L 9/32	(2006.01)
G06Q 20/02	(2012.01)
G06Q 30/06	(2012.01)
G06Q 20/38	(2012.01)
G06Q 20/40	(2012.01)
G07F 7/10	(2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **31.03.2009** **PCT/KR2009/001629**

(87) Fecha y número de publicación internacional: **03.12.2009** **WO09145443**

(96) Fecha de presentación y número de la solicitud europea: **31.03.2009** **E 09754908 (3)**

(97) Fecha y número de publicación de la concesión europea: **25.09.2019** **EP 2260610**

(54) Título: **Procedimiento y sistema para registrar un terminal de tarjeta inteligente con un servidor de difusión**

(30) Prioridad:

31.03.2008 IN CH07922008
09.03.2009 IN CH07922009

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
30.03.2020

(73) Titular/es:

SAMSUNG ELECTRONICS CO., LTD. (100.0%)
129, Samsung-ro, Yeongtong-gu
Suwon-si, Gyeonggi-do, 443-742, KR

(72) Inventor/es:

LEE, BYUNG RAE;
VENKATESWAR, JEEDIGUNTA;
RAJENDRAN, PRATYUSHA y
RAJADURAI, RAJAVELSAMY

(74) Agente/Representante:

CARPINTERO LÓPEZ, Mario

ES 2 751 081 T3

Aviso: En el plazo de nueve meses a contar desde la fecha de publicación en el Boletín Europeo de Patentes, de la mención de concesión de la patente europea, cualquier persona podrá oponerse ante la Oficina Europea de Patentes a la patente concedida. La oposición deberá formularse por escrito y estar motivada; sólo se considerará como formulada una vez que se haya realizado el pago de la tasa de oposición (art. 99.1 del Convenio sobre Concesión de Patentes Europeas).

DESCRIPCIÓN

Procedimiento y sistema para registrar un terminal de tarjeta inteligente con un servidor de difusión

Antecedentes de la invención

1. Campo de la invención

La presente invención se refiere en general al campo de Subsistema Multimedia (IMS) basado en un Protocolo de Internet (IP), y más particularmente, a un procedimiento y un sistema para el registro de un terminal de tarjeta inteligente con un servidor de difusión.

2. Descripción de la técnica relacionada

Un terminal, por ejemplo, un dispositivo móvil, se conecta a un Subsistema Multimedia (IMS) basado en el Protocolo de Internet (IP) para habilitar un servicio de IP. El IMS autentica el terminal y luego lo registra para proporcionar el servicio IP. El subsistema IMS también es capaz de proporcionar servicios de transmisión de la Alianza Móvil Abierta (OMA), en los que el terminal se conecta al sistema de transmisión. Sin embargo, se realiza un procedimiento de autenticación y registro por separado durante este procedimiento. El procedimiento de registro y autenticación por separado conduce a una utilización ineficiente de los recursos. Además, el registro por separado también resulta en ineficiencia con respecto al coste. Además, cada vez que se requiere un servicio de red o se debe realizar un nuevo registro, también aumenta la utilización de recursos y el tiempo necesario para el registro por separado. Por lo tanto, la latencia aumenta al establecer las asociaciones de seguridad del terminal con el subsistema IMS o el sistema de difusión.

El documento US 2005/102501 A1 divulga la transferencia de información de rutina de arranque.

El documento US 2006/230436 A1 describe un procedimiento y un aparato para proporcionar un mecanismo genérico para un servidor de aplicaciones de red.

El documento WO 2007/062882 A2 describe un procedimiento para entregar una o varias claves de aplicación a un servidor de aplicaciones para su uso en la protección de datos intercambiados entre el servidor de aplicaciones y un equipo de usuario, el equipo de usuario accede a una red de comunicaciones a través de un dominio de acceso.

XP014040715, "Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); Generic Authentication Architecture (GAA); Generic bootstrapping architecture (3GPP TS 33.220 versión 7.10.0 Release 7); ETSI TS 133 220", IEEE, LIS, SOPHIA ANTIPOLIS CEDEX, FRANCE, vol. 3-SA3, n.º V7.10.0, 1 de Enero de 2008 (2008-0101), ISSN: 0000-0001, revela aspectos de un sistema de telecomunicaciones celulares digitales UMTS.

Sumario de la invención

La presente invención se ha llevado a cabo para es resolver sustancialmente al menos los problemas y/o desventajas anteriores y proporcionar al menos las ventajas descritas a continuación. Por consiguiente, un aspecto de la presente invención proporciona un procedimiento y un sistema para el registro en un servidor de difusión.

Según un aspecto de la presente invención se proporciona un procedimiento para el registro con un servidor de difusión. Se recibe una solicitud de un terminal de tarjeta inteligente para el registro con al menos uno de un servidor de Subsistema Multimedia (IMS) basado en el Protocolo de Internet (IP) y un servidor de difusión. El terminal de la tarjeta inteligente se autentica en función de la solicitud. Una Función de Aplicación de Red (NAF) de la Arquitectura de Rutina de Arranque Genérico (GBA) genera material clave específico Ks_NAF en respuesta a la solicitud. Se realiza al menos uno de registrar el terminal de tarjeta inteligente con el servidor IMS y con el servidor de difusión simultáneamente, y registrar el terminal de tarjeta inteligente con el servidor IMS y posteriormente con el servidor de difusión a través del servidor IMS. Se realiza al menos uno de notificar al servidor IMS del estado del registro por parte del servidor de difusión, y notificar al servidor de difusión el estado del registro por parte del servidor IMS.

De acuerdo con otro aspecto de la presente invención se proporciona un servidor de difusión que incluye un terminal de tarjeta inteligente para el envío de una solicitud de registro. El sistema incluye un generador de claves para generar un Ks_NAF y un servidor de Subsistema Multimedia IP (IMS) para la autenticación y el establecimiento de la asociación de seguridad con el terminal de tarjeta inteligente utilizando el Ks_NAF. El sistema también incluye un servidor de difusión para registrar el terminal de tarjeta inteligente a través del servidor IMS solicitando y recibiendo el Ks_NAF del servidor IMS.

Breve descripción de los dibujos

Los anteriores y otros aspectos, características y ventajas de la presente invención se entenderán más claramente a partir de la siguiente descripción detallada cuando se toma en conjunción con los dibujos adjuntos, en los que:

La **figura 1** es un diagrama de bloques de un entorno de servidor de tarjeta inteligente, de acuerdo con el cual

pueden implementarse diversas realizaciones de la presente invención;
La **figura 2** es un diagrama de flujo que ilustra un procedimiento para el registro con un servidor de difusión, de acuerdo con una realización de la presente invención;
La **figura 3** es un diagrama de flujo que representa un flujo de mensajes entre un terminal de tarjeta inteligente, un servidor IMS y un servidor de difusión para el registro del terminal de tarjeta inteligente con el servidor IMS y el posterior registro del terminal de tarjeta inteligente con el servidor de difusión, de acuerdo con una realización de la presente invención;
La **figura 4** es un diagrama de flujo que representa un flujo de mensajes entre un terminal de tarjeta inteligente, un servidor IMS y un servidor de difusión para el registro del terminal de tarjeta inteligente con el servidor IMS y el registro posterior del terminal de tarjeta inteligente con el servidor de difusión, de acuerdo con otra realización de la presente invención;
La **figura 5** es un diagrama de flujo que representa un flujo de mensajes entre un terminal de tarjeta inteligente, un servidor IMS y un servidor de difusión para el registro del terminal de tarjeta inteligente con el servidor IMS y el posterior registro del terminal de tarjeta inteligente con el servidor de difusión, de acuerdo con otra realización de la presente invención;
La **figura 6** es un diagrama de flujo que representa un flujo de mensajes entre un terminal de tarjeta inteligente, un servidor IMS y un servidor de difusión para el registro simultáneo del terminal de tarjeta inteligente con el servidor IMS y el servidor de difusión, de acuerdo con una realización de la presente invención;
La **figura 7** es un diagrama de flujo que representa un flujo de mensajes entre un terminal de tarjeta inteligente, un servidor IMS y un servidor de difusión para el registro simultáneo del terminal de tarjeta inteligente con el servidor IMS y el servidor de difusión, de acuerdo con otra realización de la presente invención; y
La **figura 8** es un diagrama de flujo que representa un flujo de mensajes entre un terminal de tarjeta inteligente, un servidor IMS y un servidor de difusión para el registro simultáneo del terminal de tarjeta inteligente con el servidor IMS y el servidor de difusión, de acuerdo con otra realización más de la presente invención.

Descripción detallada de realizaciones de la invención

Realizaciones de la presente invención se describen en detalle con referencia a los dibujos adjuntos. Los mismos componentes o similares pueden designarse con los mismos números de referencia o similares, aunque se ilustran en diferentes dibujos. Se pueden omitir descripciones detalladas de construcciones o procedimientos conocidos en la técnica para evitar oscurecer el objeto de la presente invención.

Las realizaciones de la presente descripción descritas en el presente documento proporcionan un procedimiento y un sistema para registrarse con un servidor de difusión.

La **figura 1** es un diagrama de bloques de un entorno **100** de servidor de tarjeta inteligente, de acuerdo con el cual pueden implementarse diversas realizaciones de la presente invención. El entorno **100** incluye un terminal **105** de tarjeta inteligente. Además, el terminal **105** de tarjeta inteligente incluye una tarjeta inteligente. La tarjeta inteligente corresponde a una tarjeta con chip o una Tarjeta de Circuito Integrado (ICC). El terminal **105** de tarjeta inteligente corresponde a un dispositivo electrónico. Los ejemplos del dispositivo electrónico incluyen, entre otros, un ordenador, un ordenador portátil, un dispositivo móvil, una unidad de procesamiento, un ordenador de mano y un Asistente Digital Personal (PDA).

El terminal **105** de tarjeta inteligente envía una solicitud de registro a un servidor **125** de IMS a través de una red **110**. Los ejemplos de la red **110** incluyen, entre otros, un sistema basado en el Protocolo de Inicio de Sesión (SIP). El servidor **125** IMS proporciona servicios multimedia IP. El servidor **125** IMS utiliza protocolos de internet, por ejemplo, SIP. El Protocolo de Inicio de Sesión (SIP) es un protocolo de control de nivel de aplicación para establecer y finalizar sesiones con uno o más participantes. Los servicios facilitados por el servidor **125** IMS incluyen, pero no se limitan a, control de servicio, enrutamiento, registro, compresión SIP y soporte de calidad de servicio.

El servidor **125** IMS autentifica el terminal **105** de tarjeta inteligente basado en la solicitud de registro recibida desde el terminal **105** de tarjeta inteligente. El entorno **100** también incluye un generador **120** de claves para generar un Ks_NAF en respuesta a la recepción de la solicitud por el servidor **125** IMS. El terminal **105** de tarjeta inteligente está suscrito para servicios de difusión. El servidor **125** IMS verifica la suscripción del terminal de tarjeta inteligente para servicios de difusión. La generación de Ks_NAF se basa en el procedimiento GBA. El GBA es una tecnología utilizada para autenticar a un usuario utilizando el terminal **105** de tarjeta inteligente, para servicios de difusión. Además, el GBA verifica una identidad de usuario en la tarjeta inteligente del terminal **105** de tarjeta inteligente utilizando información almacenada en un Servidor **115** de Suscripción Doméstico (HSS). El HSS **115** almacena perfiles de usuario, genera vectores de autenticación para que la red realice la autenticación y la autorización de un usuario utilizando el terminal **105** de tarjeta inteligente. El HSS **115** también mantiene el perfil de suscripción del terminal de tarjeta inteligente.

En una realización de la presente invención, una clave de administración de sesión (SMK) es generado por el generador **120** de clave si el terminal **105** de tarjeta inteligente se suscribe para servicios de difusión de OMA.

El terminal **105** de tarjeta inteligente es entonces registrado con el servidor **125** IMS y los datos de registro del terminal **105** de tarjeta inteligente se actualizan en el HSS **115**. El terminal **105** de tarjeta inteligente también puede

solicitar el registro con un servidor **140** de difusión a través del servidor **125** IMS. Los ejemplos del servidor **140** de difusión incluyen, pero no se limitan a, un servidor de suite de habilitador de servicios de difusión móvil (BCAST) y un servidor del servicio de difusión multidifusión multimedia (MBMS). El servidor **140** de difusión funciona como un servidor de aplicaciones. Un servidor de aplicaciones aloja y ejecuta servicios en el entorno IMS.

El servidor **125** IMS incluye un módulo **130** de identificación y un módulo **135** de reenvío. El módulo **130** de identificación identifica una parte de la solicitud de registro asociada con el servidor **140** de difusión. El Ks_NAF se utiliza para registrar el terminal **105** de tarjeta inteligente con el servidor **140** de difusión. El módulo **135** de reenvío reenvía la porción asociada con el servidor **140** de difusión al servidor **140** de difusión. La porción asociada con el servidor **140** de difusión puede incluir, entre otros, el Ks_NAF, el identificador de función de aplicación de red asociado con el terminal **105** de tarjeta inteligente y una solicitud de carga de servicio.

La porción es recibida por el servidor **140** de difusión**.** El servidor **140** de difusión puede recibir o solicitar el Ks_NAF del servidor **125** IMS. La comunicación entre el servidor **125** IMS y el servidor **140** de difusión se basa en SIP.

El servidor **140** de difusión valida la Ks_NAF obtenida del servidor **125** IMS. El terminal **105** de tarjeta inteligente se registra luego con el servidor **140** de difusión y los detalles de registro se actualizan con el HSS **115**.

El servidor **140** de difusión incluye un módulo **150** de alerta para notificar el estado del registro al servidor **125** IMS.

En algunas realizaciones, el servidor **125** IMS y el servidor **140** de difusión forman juntos un sistema de difusión.

El servidor **125** IMS transmite la Ks_NAF al servidor **140** de difusión.

El servidor **140** de difusión incluye un módulo **145** de recuperación para recuperar el Ks_NAF desde el generador **120** de clave. El Ks_NAF generado por el generador **120** de claves se utiliza para autenticar y registrar el terminal **105** de tarjeta inteligente con el servidor **140** de difusión a través del servidor **125** IMS. Los detalles de registro del terminal **105** de tarjeta inteligente se actualizan luego con el HSS **115**.

En algunas realizaciones de la presente invención, el servidor **125** IMS y el servidor **140** de difusión forman juntos un servidor de difusión.

El entorno **100** puede incluir diversos otros elementos además de o en lugar de los mostrados en la **figura 1.** Por ejemplo, el servidor **125** IMS puede incluir una capa de Función de Control de Sesión de Llamada de Interrogación (I-CSCF), una capa CSCF proxy y una capa CSCF de servicio, y el servidor **140** de transmisión puede incluir una Distribución/Aplicación de Servicio de Transmisión (BSD/A), una Gestión de Suscripción de Difusión (BSM) y un Centro de servicios de difusión múltiple (BM-SC).

En una realización adicional de la presente invención, las funciones del servidor **125** IMS se realizan por la capa de CSCF de servicio.

En realizaciones adicionales de la presente invención, las funciones del servidor **135** de aplicaciones se realizan por el BSD/A, el BM-SC y el BSM.

La **figura 2** es un diagrama de flujo que ilustra un procedimiento para el registro con un servidor de difusión para un perfil de tarjeta inteligente, de acuerdo con una realización de la presente invención.

La metodología comienza en la etapa **205.**

En la etapa **210,** se recibe una petición desde un terminal de tarjeta inteligente para el registro en al menos uno de un servidor de IMS y un servidor de difusión.

El terminal de tarjeta inteligente puede solicitar el registro con el servidor de IMS para obtener uno o más servicios, por ejemplo, Presionar-para-hablar sobre los servicios celulares (PoC), proporcionado por el servidor IMS.

De manera similar, el terminal de la tarjeta inteligente puede solicitar el registro con el servidor de difusión a través del servidor IMS para obtener los uno o más servicios proporcionados por el servidor de difusión, por ejemplo, bajo demanda servicios de vídeo.

En la etapa **215,** el terminal de tarjeta inteligente se autentica basándose en la solicitud. Un usuario posee una identidad de usuario en el HSS. La autenticación se realiza mediante el intercambio de una clave ubicada en una tarjeta inteligente del terminal de tarjeta inteligente y una clave generada por el BSF. El terminal de tarjeta inteligente y BSF se autentican mutuamente en función del intercambio. El procedimiento de autenticación utiliza el Protocolo de Transferencia de Hipertexto (HTTP) Autenticación_Acceso_Resumen (AKA).

En la etapa **220,** un material de clave específica GBA NAF Ks_NAF se genera en respuesta a la solicitud. El Ks_NAF se genera ejecutando el GBA. El KS_NAF se representa como "Ks_NAF". El Ks derivado durante el procedimiento GBA se utiliza para derivar Ks_NAF.

En la etapa **225,** un terminal de tarjeta inteligente está registrado con un servidor de IMS y con un servidor de difusión simultáneamente.

La solicitud de porción asociada con el servidor de difusión se identifica y se remitió al servidor de difusión. Si la porción incluye el registro del servicio de difusión, el servidor IMS transmite el Ks_NAF en un mensaje SIP al servidor de difusión a través de un mensaje SIP. El Ks_NAF puede transmitirse al servidor de difusión antes del registro con el servidor IMS para facilitar el registro simultáneo del terminal de tarjeta inteligente con el servidor IMS y el servidor de difusión.

El BSM se encuentra en el servidor de difusión. Ks_NAF es validado por el servidor de difusión. El terminal de la tarjeta inteligente se registra con el servidor IMS y el servidor de transmisión simultáneamente.

Un reconocimiento del registro puede ser enviado a la terminal de tarjeta inteligente.

El registro con el servidor de difusión incluye el establecimiento de una sesión de seguridad para la comunicación entre el terminal de tarjeta inteligente y el servidor de difusión.

En una realización, la etapa **225** se pueden omitir y la etapa **230** se puede realizar.

En la etapa **230,** el terminal de tarjeta inteligente está registrado con el servidor IMS y posteriormente con el servidor de aplicaciones a través del servidor IMS.

El terminal de tarjeta inteligente envía una solicitud al servidor IMS para su registro. La solicitud incluye la identidad de usuario requerida para la autenticación mediante señalización basada en SIP. El servidor IMS responde señalando un reconocimiento de registro de IMS al terminal de la tarjeta inteligente. El terminal de tarjeta inteligente luego solicita el registro con el sistema de transmisión.

El servidor recupera la emisión Ks_NAF desde el servidor IMS si la solicitud se envía al servidor de difusión directa. El servidor IMS también puede reenviar el Ks_NAF directamente al servidor de difusión si la solicitud se reenvía al servidor IMS. Una vez, el servidor de transmisión recibe y valida el Ks_NAF, el terminal de tarjeta inteligente y el servidor de transmisión pueden comunicarse directamente. La autenticación del terminal de la tarjeta inteligente con el servidor de difusión se puede omitir ya que el terminal de la tarjeta inteligente se ha autenticado previamente con el servidor IMS. Se envía un acuse de recibo del registro de difusión al terminal de tarjeta inteligente.

Al final de la etapa **225** y la etapa **230,** el IMS y el servidor de difusión actualizan el estado del registro en un servidor de suscripción doméstico.

En la etapa **235,** el servidor IMS es notificado sobre el estado del registro con el servidor de difusión por el servidor de difusión. La notificación se puede realizar utilizando los mensajes SIP.

El servidor de difusión es notificado sobre el estado del registro con el servidor por el servidor IMS IMS. La notificación se puede realizar utilizando los mensajes SIP.

La metodología termina en la etapa **240.**

En algunas realizaciones de la presente invención, una o más de las etapas descritas anteriormente pueden implementarse utilizando un terminal de tarjeta inteligente. El terminal de tarjeta inteligente incluye un bus para comunicar información y un procesador junto con el bus para procesar información. El terminal de tarjeta inteligente también incluye una memoria, por ejemplo, una memoria de acceso aleatorio (RAM), acoplada al bus para almacenar la información requerida por el procesador. La memoria se puede utilizar para almacenar información temporal requerida por el procesador. El terminal de tarjeta inteligente incluye además una memoria de solo lectura (ROM) acoplada al bus para almacenar la información estática requerida por el procesador. Se puede proporcionar una unidad de almacenamiento del servidor, por ejemplo, un disco magnético, disco duro o disco óptico, y se puede acoplar al bus para almacenar información.

El terminal de tarjeta inteligente puede ser acoplado a través del bus a una pantalla, por ejemplo, un tubo de rayos catódicos (CRT) o pantalla de cristal líquido (LCD), para mostrar información. Un dispositivo de entrada, que incluye varias teclas, está acoplado al bus para comunicar información al procesador. En algunas realizaciones, también puede estar presente el control del cursor, por ejemplo, un ratón, una bola de seguimiento, un joystick o teclas de dirección del cursor, para comunicar información al procesador y para controlar el movimiento del cursor en la pantalla.

En una realización de la presente invención, las etapas de la figura 2 descritas anteriormente se llevan a cabo por el terminal de la tarjeta inteligente utilizando el procesador. La información se puede leer en la memoria desde un medio legible por máquina, por ejemplo, la unidad de almacenamiento del servidor. En realizaciones alternativas de la presente invención, los circuitos cableados pueden usarse en lugar de o en combinación con instrucciones de software para implementar diversas realizaciones de la presente invención.

El término medio legible por máquina puede definirse como un medio de proporcionar datos a una máquina para

permitir que la máquina para realizar una función específica. El medio legible por máquina puede ser un medio de almacenamiento. Los medios de almacenamiento pueden incluir medios no volátiles y medios volátiles. La unidad de almacenamiento del servidor puede ser un medio no volátil. La memoria puede ser un medio volátil. Todos estos medios deben ser tangibles para permitir que las instrucciones que llevan los medios sean detectadas por un mecanismo físico que lee las instrucciones en la máquina.

Los ejemplos del medio legible por máquina incluyen, pero no se limitan a, un disquete, un disco flexible, disco duro, cinta magnética, un CD-ROM, disco óptico, tarjetas perforadas, cinta de papel, una RAM, una PROM, EPROM y un FLASH-EPROM.

El medio legible por máquina también puede incluir enlaces en línea, enlaces de descarga, instalación y enlaces que facilitan la información al procesador.

El terminal de tarjeta inteligente también incluye una interfaz de comunicación acoplada al bus para permitir la comunicación de datos. Los ejemplos de la interfaz de comunicación incluyen, entre otros, una tarjeta de red digital de servicios integrados (ISDN), un módem, una tarjeta de red de área local (LAN), un puerto de infrarrojos, un puerto Bluetooth, un puerto zigbee y un puerto de conexión inalámbrica.

En realizaciones adicionales de la presente invención, el procesador puede incluir una o más unidades de procesamiento para realizar una o más funciones del procesador. Las unidades de procesamiento son circuitos de hardware que realizan funciones específicas.

Diversas realizaciones de la presente invención proporcionan una interfaz SIP entre el servidor de IMS y el servidor de difusión para ser reutilizado. Además, los servicios de difusión, que utilizan señalización basada en SIP, pueden converger. El tiempo de autenticación se optimiza al establecer la asociación de seguridad entre el terminal de tarjeta inteligente y el sistema de transmisión.

La **figura 3** es un diagrama de flujo que representa un flujo de mensajes entre un terminal **105** de tarjeta inteligente, un servidor **125** IMS y un servidor **140** de difusión para el registro del terminal **105** de tarjeta inteligente con el servidor **125** IMS y el registro posterior del terminal **105** de tarjeta inteligente con el servidor **140** de difusión, de acuerdo con una realización de la presente invención.

El terminal **105** de tarjeta inteligente realiza el procedimiento de GBA con el BSF. A continuación, se explica el flujo de detalles en los mensajes SIP para el registro posterior del terminal **105** de tarjeta inteligente con el servidor IMS y un servidor de aplicaciones:

IMS_Reg_Req: El terminal **105** de tarjeta inteligente envía la solicitud de registro de IMS al S-CSCF. El mensaje lleva la información de identidad del usuario necesaria para GBA. El valor de la identidad privada multimedia IP (IMPI) utilizado para el registro SIP se reutiliza aquí. El procedimiento de REGISTRO incluye:

```
REGISTER <domain name> SIP /2.0
Via:
   Forwards:
From:
To:
Authorization: .... Username= "user identity info for GBA/SIP registration" .....
Require: bcast_ext_profile=BCAST_EXT_PROFILE; bcast_ext_scard= "NAF_ID of
.
.
.
.
the NAF with which the terminal wishes to register"
   Content-Length: 0
```

IMS_Auth_Req: S-CSCF devuelve la respuesta de autenticación al terminal **105** de la tarjeta inteligente. El desafío aleatorio C (RAND) y el Identificador de Autenticación (AUTN) se comunican en este mensaje. El mensaje de desafío de autenticación incluye:

```
SIP/2.0 401 Authorization
.
WWW-Authenticate:
.
Content-Length: 0
```

IMS_Auth_Res: El terminal **105** de tarjeta inteligente envía la Respuesta de Autenticación a la S-CSCF. El procedimiento de REGISTRO incluye:

```
REGISTER <domain name> SIP /2.0
Via:
```

```
   Forwards:
From:
To:
Authorization: ......... Username= "user identity info for GBA/SIP registration" nonce
= "nonce value" response = "response value"
   Content-Length: 0
```

IMS_Reg_Res: El S-CSCF responde con el '200 OK' que sugiere un registro exitoso de IMS y una ejecución exitosa de GBA.

```
   SIP/2.0 200 OK

   .

   .

   Content-Length: 0
```

En este punto, la clave GBA se ha extraído entre el terminal **105** de la tarjeta inteligente y S-CSCF y se establece Ks entre el S-CSCF o el BSF y el terminal **105** de la tarjeta inteligente. Además, la S-CSCF o la BSF generan el Ks_NAF con el Ks que se ha establecido y el NAF_I D que se ha recibido en el mensaje de solicitud de registro inicial.

Entrega SMK: El S-CSCF genera y entrega el Ks_NAF al servidor 140 de difusión. Este Ks_NAF es el S MK para todas las comunicaciones posteriores entre el BSM y el terminal **105** de tarjeta inteligente.

200 OK: Después de recibir con éxito la SMK de la BSF, la BSM devuelve un mensaje de 200 OK a la BSF.

La **figura 4** es un diagrama de flujo que representa un flujo de mensajes entre un terminal **105** de tarjeta inteligente, un servidor **125** IMS y un servidor **140** de difusión para el registro del terminal de tarjeta inteligente **105** con el servidor **125** IMS y el registro posterior del terminal **105** de tarjeta inteligente con el servidor **140** de difusión, de acuerdo con otra realización de la presente invención.

El flujo de datos en los mensajes SIP para el registro subsiguiente de la terminal **105** de tarjeta inteligente tanto con el servidor **125** IMS y un servidor **140** de difusión se explica a continuación:

IMS_Reg_Req: El terminal **105** de tarjeta inteligente envía un mensaje IMS_Reg_Req para el registro de IMS con un S-CSCF. Además, el IMS_Reg_Req lleva la carga útil de aprovisionamiento del servicio para la solicitud de suscripción a un servicio. El procedimiento SIP utilizado es REGISTRO con extensiones. El S-CSCF reenvía la carga útil de suministro de servicios al servidor **140** de difusión. El procedimiento de REGISTRO incluye:

```
   REGISTER <domain name> SIP/2.0
   Via:
   Forwards:
   .Content-Length: <size of the service provisioning message>
   Require: bcast_ext_profile=BCAST_EXT_PROFILE; bcast_ext_scard= "NAF_ID of
   the NAF with which the terminal wishes to register"
   Content-Type: "application/vnd.oma.bcast.sprov + xml"
   <Service Provisioning Message>
```

IMS_Auth_Req: El S-CSCF envía una respuesta de autenticación al terminal **105** de la tarjeta inteligente. RAND y AUTN se comunican en el mensaje IMS_Auth_Req. El mensaje de desafío de autenticación incluye:

```
   SIP/2.0 401 Authorization
   WWW-Authenticate:
      Content-Length: 0
```

IMS_Auth_Res: El terminal **105** de tarjeta inteligente envía una respuesta de autenticación a la S-CSCF. El procedimiento de REGISTRO incluye:

```
   REGISTER <domain name> SIP /2.0
   Via:
   Forwards:
   From:
   To:
   Authorization: ......... Username= "user identity info for GBA/SIP registration"
   nonce = "nonce value" response = "response value"
   Content-Length: 0
```

IMS_Reg_Res: El S-CSCF responde con el '200 OK' que sugiere un registro exitoso de IMS y una ejecución exitosa de GBA.

Carga de solicitud de servicio: Al final del establecimiento de Ks entre la BSF y el terminal **105** de tarjeta inteligente, la BSF reenvía un mensaje de provisión de servicio al BSM.

Solicitud de petición de clave: El BSM recibe la carga útil de provisión de servicios de la BSF. El BSM envía una solicitud SMK al BSF. La solicitud SMK contiene un NAF_ID correspondiente al BSM. La solicitud SMK es una solicitud GBA por la cual la NAF especifica su NAF_ID correspondiente y solicita una Ks_NAF.

Solicitud de respuesta clave: El BSF genera el Ks_NAF y lo envía al BSM. El Ks_NAF funciona como SMK para futuras comunicaciones entre el BSM y el terminal **105** de tarjeta inteligente.

200 OK: El BSM responde al BSF con un 200 OK para indicar la recepción exitosa del SMK.

La **figura 5** es un diagrama de flujo que representa un flujo de mensajes entre un terminal **105** de tarjeta inteligente, un servidor **125** IMS y un servidor **140** de difusión para el registro del terminal **105** de tarjeta inteligente con el servidor **125** IMS y el registro posterior del terminal **105** de tarjeta inteligente con el servidor **140** de difusión, de acuerdo con otra realización más de la presente invención.

El flujo de datos en los mensajes SIP para el registro subsiguiente de la terminal **105** de tarjeta inteligente tanto con el servidor **125** IMS y un servidor **140** de difusión se explica a continuación:

IMS_Reg_Req: El terminal **105** de tarjeta inteligente envía una solicitud de registro de IMS a un S-CSCF. El mensaje IMS_Reg_Req lleva la información de identidad del usuario necesaria para GBA. El valor IMPI utilizado para el registro SIP se reutiliza. El procedimiento de REGISTRO incluye:

```
REGISTER <domain name> SIP /2.0
Via:
Forwards:
From:
To:
Authorization: .... Username= "user identity info for GBA/SIP registration" .....
Content-Length: 0
```

IMS_Auth_Req: El S-CSCF envía una respuesta de autenticación al terminal **105** de la tarjeta inteligente. RAND y AUTN se comunican en el mensaje IMS_Auth_Req. El mensaje de desafío de autenticación incluye:

```
SIP/2.0 401 Authorization
WWW-Authenticate:
Content-Length: 0
```

IMS_Auth_Res: El terminal **105** de tarjeta inteligente envía una respuesta de autenticación a la S-CSCF. La respuesta de autorización va del terminal **105** de la tarjeta inteligente al S-CSCF. El procedimiento de REGISTRO incluye:

```
REGISTER <domain name> SIP /2.0
Via:
Forwards:
From:
To:
Authorization: ......... Username= "user identity info for GBA/SIP registration"
nonce = "nonce value" response = "response value"
Content-Length: 0
```

IMS_Reg_Res: El S-CSCF responde con el '200 OK' que significa un registro exitoso de IMS y una ejecución exitosa de GBA.

```
SIP/2.0 200 OK
Content-Length: 0
```

El GBA ejecutado entre el terminal **105** de la tarjeta inteligente y el BSF (puede ubicarse junto con el S-CSCF) ya se habría completado y se ha establecido Ks entre el BSF y el terminal **105** de la tarjeta inteligente.

Req Aprovisionamiento de Servicios: El terminal **105** de tarjeta inteligente intenta contactar directamente con el servidor **140** de difusión. En este punto, el Ks_NAF se transmite al BSM desde el S-CSCF. Además, el terminal **105** de tarjeta inteligente envía una solicitud de servicio BCAST que incluye un NAF_ID correspondiente al BSM.

Req Clave de Aplicación: El BSM envía el NAF_ID a través de un mensaje SIP para recuperar el Ks NAF del BSF.

Res Clave de Aplicación: El BSF envía una respuesta con el Ks_NAF al BSM a través de un mensaje SIP.

Res Aprovisionamiento de Servicios: El BSM recibe el Ks_NAF del BSF. Además, el terminal **105** de tarjeta inteligente y el BSM se comunican directamente.

La **figura 6** es un diagrama de flujo que representa un flujo de mensajes entre un terminal **105** de tarjeta inteligente, un servidor **125** IMS y un servidor **140** de difusión para el registro simultáneo del terminal **105** de tarjeta inteligente con el servidor **125** IMS y el servidor **140** de difusión, de acuerdo con una realización de la presente invención.

El flujo de datos en los mensajes SIP para el registro simultáneo de la terminal **105** de tarjeta inteligente tanto con el servidor **125** IMS y un servidor de aplicaciones se explica a continuación:

IMS_Reg_Req: El terminal **105** de tarjeta inteligente envía la solicitud de registro del servidor **125** IMS al S-CSCF del servidor **125** IMS. Este mensaje lleva la información de identidad del usuario necesaria para GBA. El valor IMPI utilizado para el registro SIP se reutiliza aquí. El S-CSCF verifica la suscripción del terminal de tarjeta inteligente para los servicios de difusión.
IMS_Auth_Req: El S-CSCF del servidor **125** IMS envía la respuesta de autenticación al terminal **105** de la tarjeta inteligente.
IMS_Auth_Res: El terminal **105** de tarjeta inteligente envía la respuesta de autenticación al S-CSCF del servidor **125** IMS.
IMS_Reg_Res: S-CSCF responde con el '200 OK' sugiriendo el registro exitoso de IMS del terminal **105** de tarjeta inteligente con el servidor **125** IMS y la ejecución exitosa de GBA. El K se deriva entre S-CSCF o BSF y el terminal **105** de tarjeta inteligente. Ahora el S-CSCF o el BSF genera el Ks_NAF con los K establecidos y la identidad de función de aplicación de red (NAF_ID) que ha recibido en el mensaje de solicitud de registro inicial.
Carga de Solicitud de Servicio: Al establecer Ks_NAF entre la BSF y el terminal **105** de tarjeta inteligente, la S-CSCF reenvía el mensaje de aprovisionamiento del servicio al BSM para la autorización del servicio.
Solicitud de solicitud: Cuando el terminal **105** de tarjeta inteligente intenta ponerse en contacto con el Servidor de aplicaciones - BSM, entonces el KS_NAF necesita comunicarse al BSM desde el S-CSCF o BSF del servidor **125** IMS.
SMK Req: El BSM proporciona su NAF_ID para recuperar el SMK del BSF o el S-CSCF a través de un procedimiento SIP.
Res SMK: El BSF o S-CSCF envía la respuesta como SMK al BSM y, por lo tanto, la clave SMK se comunica al BSM.
Appln Res: Una vez que el BSM ha adquirido la clave, se pueden realizar más comunicaciones entre el terminal **105** de la tarjeta inteligente y el BSM directamente o a través de la red IMS.

La **figura 7** es un diagrama de flujo que representa un flujo de mensajes entre un terminal **105** de tarjeta inteligente, un servidor **125** IMS y un servidor **140** de difusión para el registro simultáneo del terminal **105** de tarjeta inteligente con el servidor **125** IMS y el servidor **140** de difusión, de acuerdo con con otra realización de la presente invención.

El flujo de datos en los mensajes SIP para el registro simultáneo de la terminal **105** de tarjeta inteligente tanto con el servidor **125** IMS y un servidor **140** de difusión se explica a continuación:

IMS_Reg_Req: El terminal **105** de tarjeta inteligente envía la solicitud de registro del servidor IMS a un S-CSCF. El mensaje IMS_Reg_Req lleva una información de identidad de usuario necesaria para GBA. Se reutiliza un valor IMPI utilizado para el registro SIP. El procedimiento de REGISTRO incluye:

```
REGISTER <domain name> SIP /2.0
Via:
Forwards:
From:
To:
Authorization: .... Username= "user identity info for GBA/SIP registration" .....
Require: bcast_ext_profile=BCAST_EXT_PROFILE; bcast_ext_scard= "NAF_ID of
the NAF with which the smartcard terminal 105 wishes to register"
Content-Length: 0
```

IMS_Auth_Req: El S-CSCF envía una respuesta de autenticación al terminal **105** de la tarjeta inteligente. Además, se comunican el RAND y el AUTN. El mensaje de desafío de autenticación incluye:

```
SIP/2.0 401
Authorization WWW-Authenticate:
Content-Length: 0
```

IMS_Auth_Res: El terminal **105** de tarjeta inteligente envía una respuesta de autenticación a la S-CSCF. La respuesta de autorización se transmite desde el terminal **105** de tarjeta inteligente al S-CSCF. El procedimiento de REGISTRO incluye:

```
REGISTER <domain name> SIP /2.0
Via:
Forwards:
From:
To:
Authorization: ......... Username= "user identity info for GBA/SIP registration"
nonce = "nonce value" response = "response value"
Content-Length: 0
```

Entrega SMK: El BSF recibe el paquete de respuesta de autenticación y se genera el Ks. El BSF genera y transmite un Ks_NAF al BSM.

200 OK: El BSM responde con el 200 OK después de recibir el Ks_NAF.

IMS_Reg_Res: El BSF responde con el 200 OK indicando la finalización exitosa del registro IMS y el registro de difusión.

La **figura 8** es un diagrama de flujo que representa un flujo de mensajes entre un terminal **105** de tarjeta inteligente, un servidor **125** IMS y un servidor **140** de difusión para el registro simultáneo del terminal **105** de tarjeta inteligente con el servidor **125** IMS y el servidor **140** de difusión, de acuerdo con con otra realización más de la presente invención.

El flujo de datos en los mensajes SIP para el registro simultáneo de la terminal **105** de tarjeta inteligente tanto con el servidor **125** IMS y un servidor **140** de difusión se explica a continuación:

IMS_Reg_Req: El terminal **105** de tarjeta inteligente envía un mensaje IMS_Reg_Req para el registro de IMS con un S-CSCF. Además, el IMS_Reg_Req lleva la carga útil de aprovisionamiento del servicio para la solicitud de suscripción a un servicio. El procedimiento SIP utilizado es REGISTRO con extensiones. El S-CSCF reenvía la carga útil de suministro de servicios al servidor **140** de difusión**.** El procedimiento de REGISTRO incluye:

```
REGISTER <domain name> SIP/2.0
Via:
Forwards:
Content-Length: <size of the service provisioning message>
Require: bcast_ext_profile=BCAST_EXT_PROFILE; bcast_ext_scard= "NAF ID of
the NAF with which the terminal wishes to register"
Content-Type: "application/vnd.oma.bcast.sprov + xml"
<Service Provisioning Message>
```

IMS_Auth_Req: El S-CSCF envía una respuesta de autenticación al terminal **105** de la tarjeta inteligente. RAND y AUTN se comunican en el mensaje IMS_Auth_Req. El mensaje de desafío de autenticación incluye:

```
SIP/2.0 401 Authorization
WWW-Authenticate:
   Content-Length: 0
```

IMS_Auth_Res: El terminal **105** de tarjeta inteligente envía una respuesta de autenticación a la S-CSCF. La respuesta de autorización va del terminal **105** de la tarjeta inteligente al S-CSCF. El procedimiento de REGISTRO incluye:

```
REGISTER <domain name> SIP /2.0
Via:
Forwards:
From:
```

```
To: Authorization: ......... Username= "user identity info for GBA/SIP registration"
nonce = "nonce value" response = "response value" Content-Length: 0
```

Carga de Solicitud de Servicio: Al final del establecimiento de Ks entre el BSF y el terminal **105** de tarjeta inteligente, el BSF reenvía el mensaje de provisión de servicio al BSM.

Solicitud de Clave de Aplicación: Al recibir los datos de carga útil del BSF, el BSM envía una solicitud SMK al BSF. Esta solicitud contiene el NAF_ID del BSM.

Respuesta Clave de la Aplicación: El Ks_NAF es generado por el BSF y se envía al BSM. Esto sirve como SMK para futuras comunicaciones entre el BSM y el terminal **105** de tarjeta inteligente.

200 OK: Después de recibir el SMK del BSF, el BSM responde al BSF con 200 OK para indicar la recepción exitosa del SMK.

IMS_Reg_Res: El S-CSCF responde con el '200 OK' sugiriendo el registro exitoso de IMS y el registro de transmisión.

Aunque la presente invención se ha mostrado y descrito con referencia a ciertas realizaciones de la misma, se entenderá por los expertos en la técnica que diversos cambios en forma y detalles pueden hacerse en la misma sin apartarse del ámbito de la invención como se define en las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un procedimiento para registrar un terminal de tarjeta inteligente mediante un servidor IMS de Subsistema Multimedia basado en Protocolo de Internet en un sistema de comunicación móvil, el procedimiento comprende:

recibir, por el servidor IMS, desde el terminal de tarjeta inteligente, una solicitud de registro para registrarse con el servidor IMS y con un servidor de difusión;
autenticar el terminal de tarjeta inteligente basado en la solicitud de registro;
generar material clave específico NAF de función genérica de aplicación de red GBA de arquitectura de rutina de arranque, Ks_NAF; y
realizar un registro del terminal de tarjeta inteligente con el servidor IMS y el servidor de difusión,
en el que el Ks_NAF se transmite al servidor de difusión utilizando un mensaje SIP de protocolo de inicio de sesión,
en el que realizar el registro del terminal de tarjeta inteligente con el servidor de difusión comprende que el servidor IMS reenvía una porción asociada con el servidor de difusión de la solicitud de registro al servidor de difusión, y
en el que la porción comprende Ks_NAF.

2. El procedimiento de la reivindicación 1, que además comprende:
notificar al servidor de difusión del estado del registro por parte del servidor IMS.

3. El procedimiento de la reivindicación 1, en el que:
el reenvío de una porción de la solicitud de registro al servidor de difusión se realiza después de realizar una verificación basada en la información de suscripción en un servidor de suscripción doméstico HSS.

4. El procedimiento de la reivindicación 1, en el que el registro se realiza usando mensajes SIP del protocolo de inicio de sesión.

5. El procedimiento de la reivindicación 1, en el que la solicitud de registro desde el terminal de tarjeta inteligente comprende una carga útil de suministro de servicio para una solicitud de suscripción a un servicio de difusión.

6. El procedimiento de la reivindicación 1,
en el que Ks_NAF es una clave de gestión de sesión para una comunicación adicional entre el servidor de difusión y el terminal de tarjeta inteligente.

7. El procedimiento de la reivindicación 1, que además comprende:
actualizar un servidor de suscripción doméstico el registro del terminal de tarjeta inteligente en al menos uno del servidor IMS y el servidor de difusión.

8. Un servidor IMS de subsistema multimedia basado en protocolo de internet para registrar un terminal de tarjeta inteligente en un sistema de comunicación móvil, el servidor IMS comprende:

un transceptor configurado para comunicarse con otro nodo de red; y
un controlador configurado para recibir desde un terminal de tarjeta inteligente, una solicitud de registro para registrarse con el servidor IMS y con un servidor de difusión, para autenticar el terminal de tarjeta inteligente en función de la solicitud de registro, generar material clave específico NAF de función genérica de aplicación de red GBA de arquitectura de rutina de arranque, Ks_NAF, y para realizar un registro del terminal de tarjeta inteligente con el servidor IMS y el servidor de difusión,
en el que el Ks_NAF se transmite al servidor de difusión utilizando un mensaje SIP de protocolo de inicio de sesión,
en el que para realizar el registro del terminal de tarjeta inteligente con el servidor de transmisión, el servidor IMS está configurado para reenviar una porción asociada con el servidor de transmisión de la solicitud de registro al servidor de transmisión, y
en el que la porción comprende Ks_NAF.

9. El servidor IMS de la reivindicación 8, en el que el controlador está configurado además para notificar al servidor de difusión un estado del registro por parte del servidor IMS.

10. El servidor IMS de la reivindicación 8, en el que el reenvío de la parte de la solicitud de registro al servidor de difusión se realiza después de realizar una verificación basada en la información de suscripción en un servidor de suscripción doméstico HSS.

11. El servidor IMS de la reivindicación 8, en el que el registro se realiza utilizando mensajes de protocolo de inicio de sesión (SIP).

12. El servidor IMS de la reivindicación 8, en el que la solicitud de registro desde el terminal de tarjeta inteligente comprende una carga útil de suministro de servicio para una solicitud de suscripción a un servicio de difusión.

13. El servidor IMS de la reivindicación 8, en el que Ks_NAF es una clave de gestión de sesión para una comunicación adicional entre el servidor de difusión y el terminal de tarjeta inteligente.

14. El servidor IMS de la reivindicación 8, en el que el controlador está configurado además para actualizar un servidor de suscripción doméstico con respecto al registro del terminal de tarjeta inteligente en al menos uno del servidor IMS y el servidor de difusión.

FIG. 1

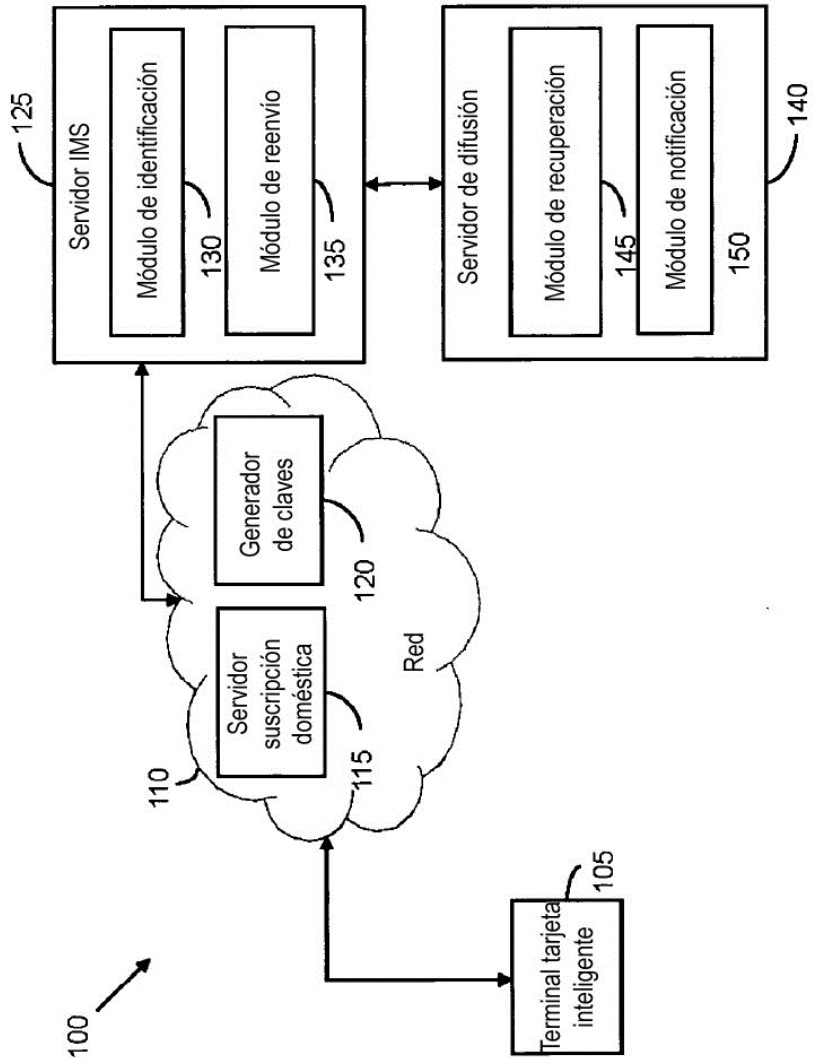

100
Terminal tarjeta inteligente
105
110
Servidor suscripción doméstica
115
Generador de claves
120
Red
125
Servidor IMS
Módulo de identificación
130
Módulo de reenvío
135
Servidor de difusión
Módulo de recuperación
145
Módulo de notificación
150
140

FIG. 2

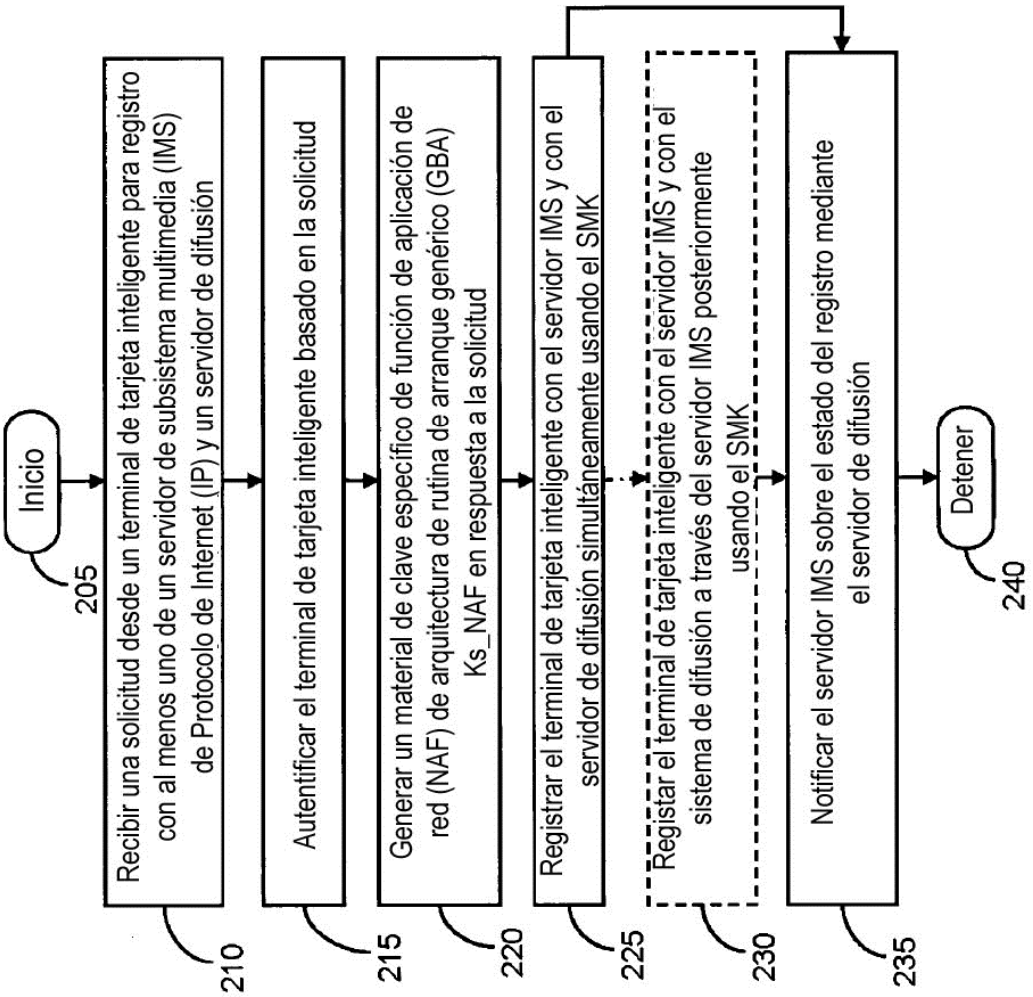

Inicio
205
Recibir una solicitud desde un terminal de tarjeta inteligente para registro con al menos uno de un servidor de subsistema multimedia (IMS) de Protocolo de Internet (IP) y un servidor de difusión
210
Autentificar el terminal de tarjeta inteligente basado en la solicitud
215
Generar un material de clave específico de función de aplicación de red (NAF) de arquitectura de rutina de arranque genérico (GBA) Ks_NAF en respuesta a la solicitud
220
Registrar el terminal de tarjeta inteligente con el servidor IMS y con el servidor de difusión simultáneamente usando el SMK
225
Registar el terminal de tarjeta inteligente con el servidor IMS y con el sistema de difusión a través del servidor IMS posteriormente usando el SMK
230
Notificar el servidor IMS sobre el estado del registro mediante el servidor de difusión
235
Detener
240

FIG. 3

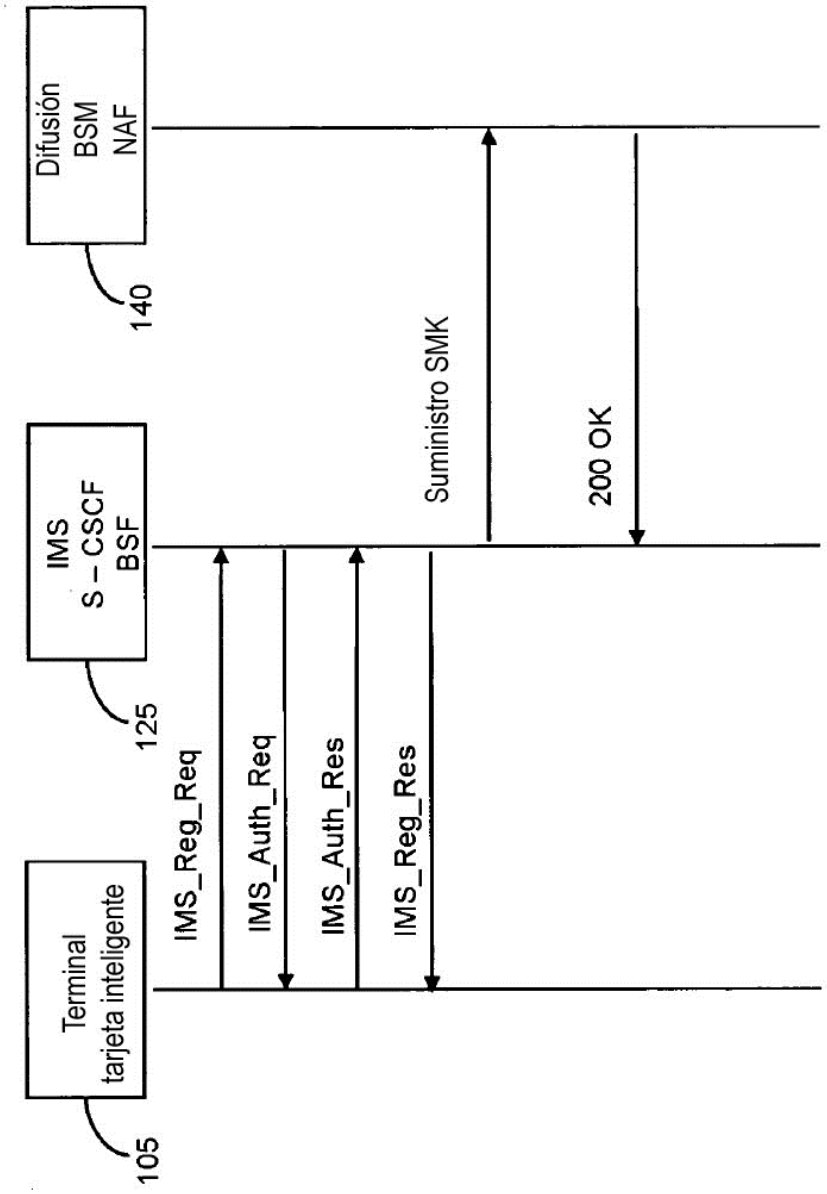

Terminal
tarjeta inteligente
105
IMS
S – CSCF
BSF
125
Difusión
BSM
NAF
140
IMS_Reg_Req
IMS_Auth_Req
IMS_Auth_Res
IMS_Reg_Res
Suministro SMK
200 OK

FIG. 4

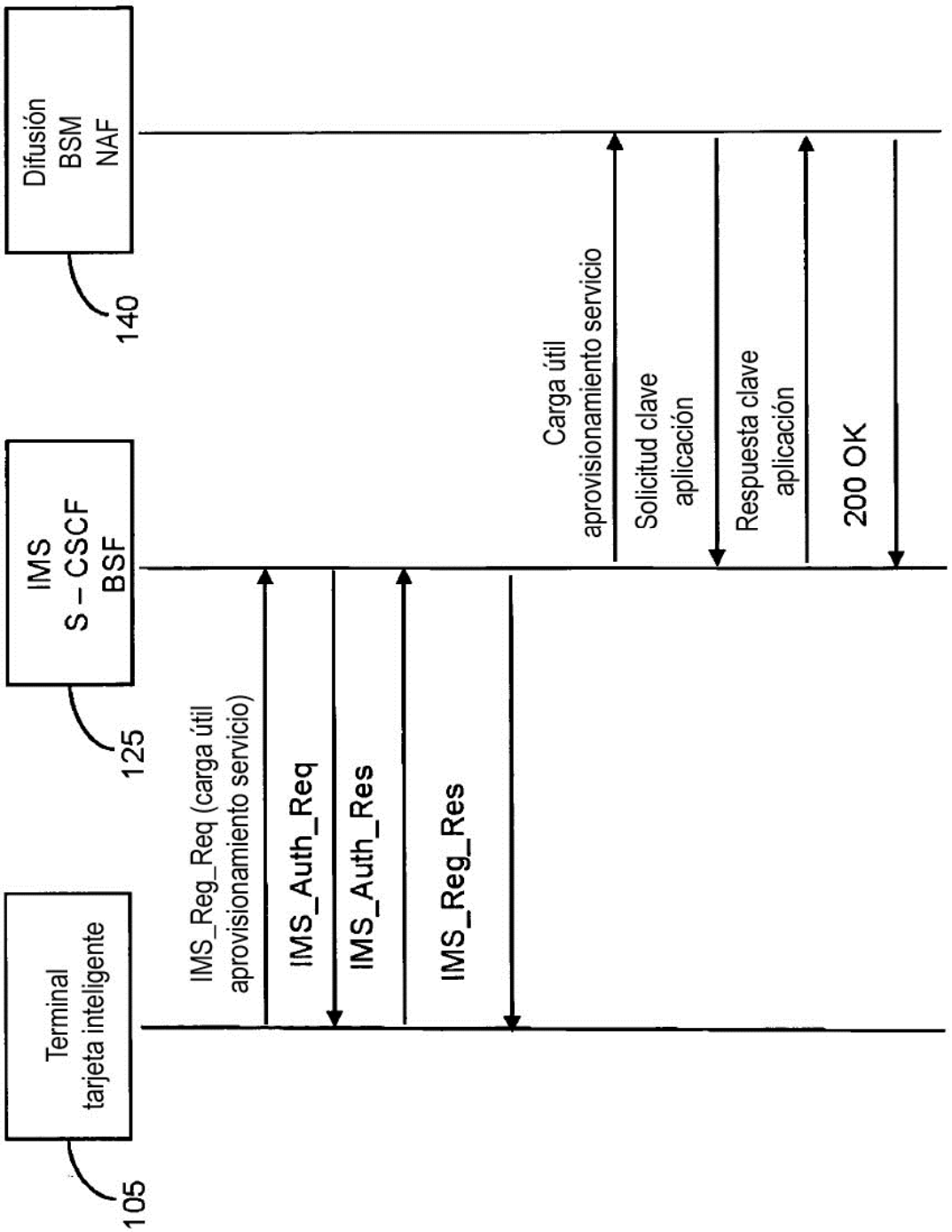

Terminal
tarjeta inteligente
105
IMS
S – CSCF
BSF
125
Difusión
BSM
NAF
140
IMS_Reg_Req (carga útil
aprovisionamiento servicio)
IMS_Auth_Req
IMS_Auth_Res
IMS_Reg_Res
Carga útil
aprovisionamiento servicio
Solicitud clave
aplicación
Respuesta clave
aplicación
200 OK

FIG. 5

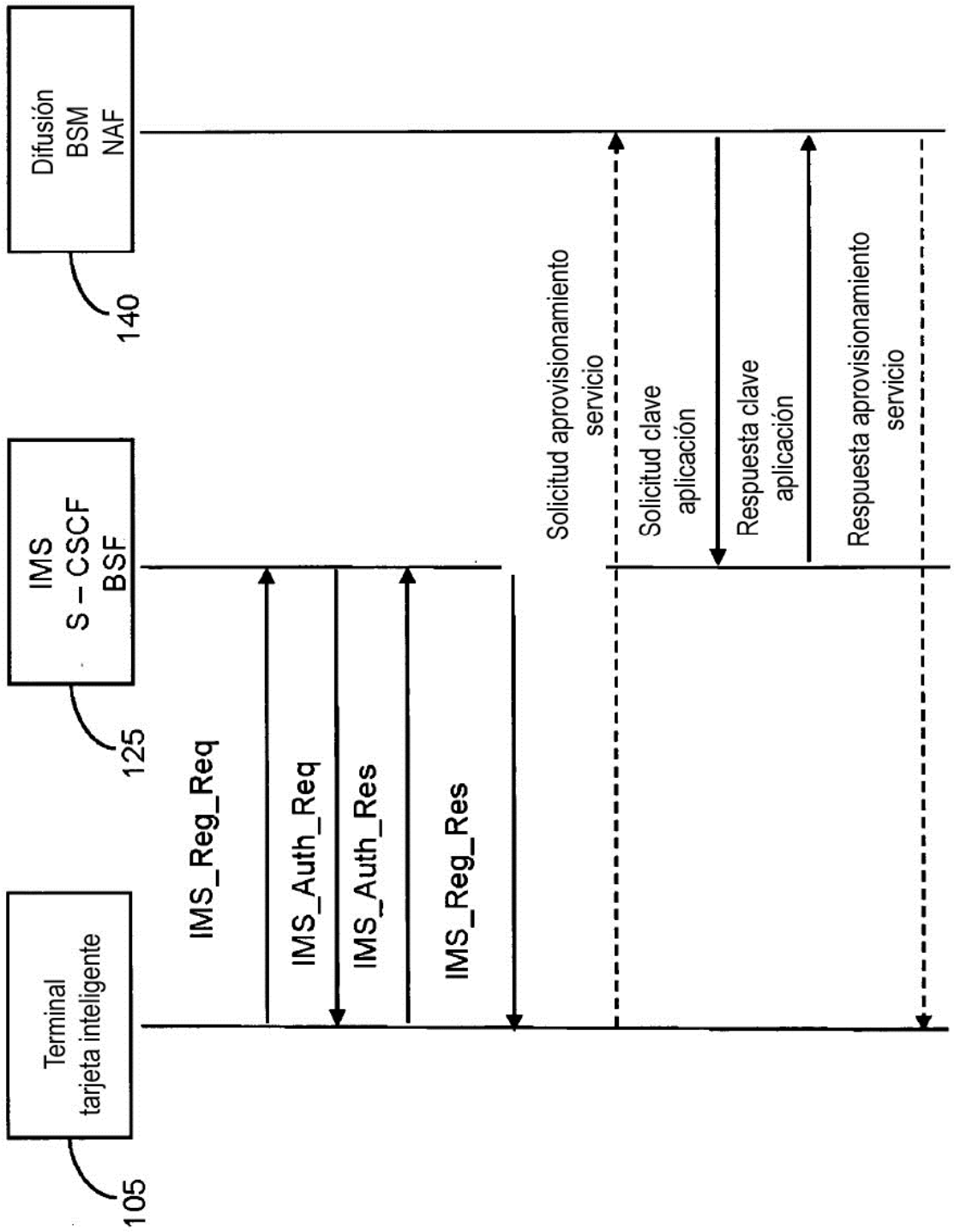

Terminal
tarjeta inteligente
105
IMS
S – CSCF
BSF
125
Difusión
BSM
NAF
140
IMS_Reg_Req
IMS_Auth_Req
IMS_Auth_Res
IMS_Reg_Res
Solicitud aprovisionamiento servicio
Solicitud clave aplicación
Respuesta clave aplicación
Respuesta aprovisionamiento servicio

FIG. 6

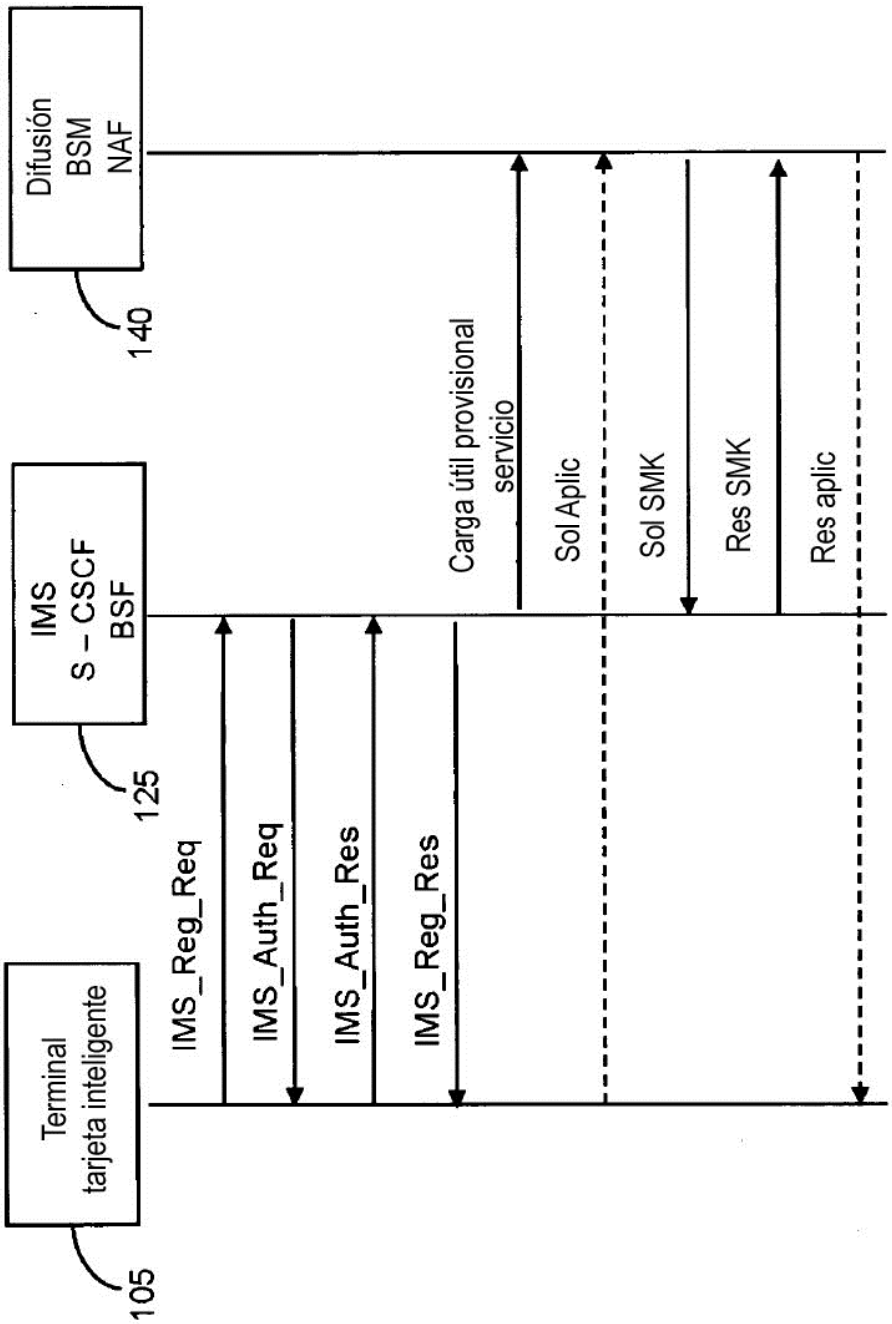

Terminal
tarjeta inteligente
105
IMS
S – CSCF
BSF
125
Difusión
BSM
NAF
140
IMS_Reg_Req
IMS_Auth_Req
IMS_Auth_Res
IMS_Reg_Res
Carga útil provisional
servicio
Sol Aplic
Sol SMK
Res SMK
Res aplic

FIG. 7

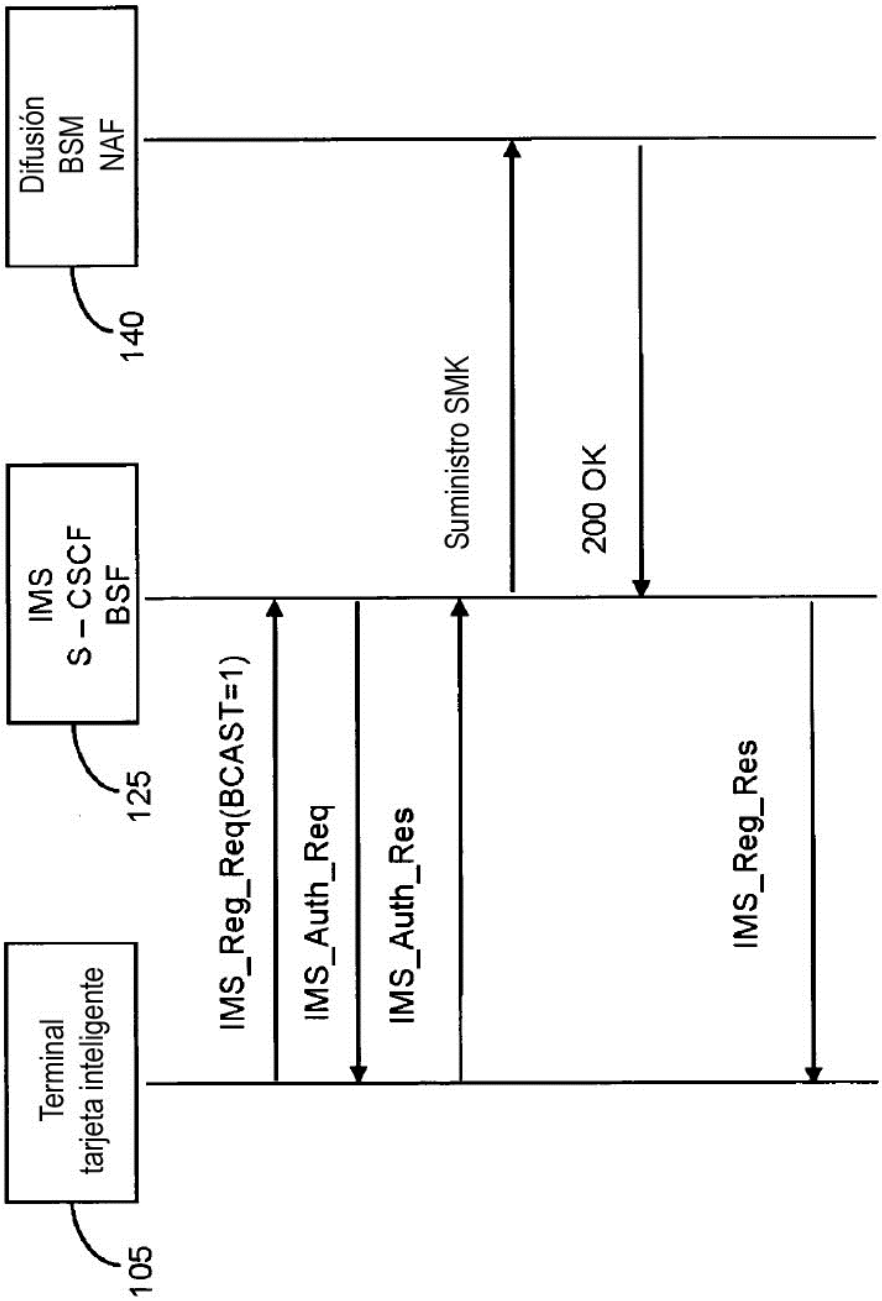
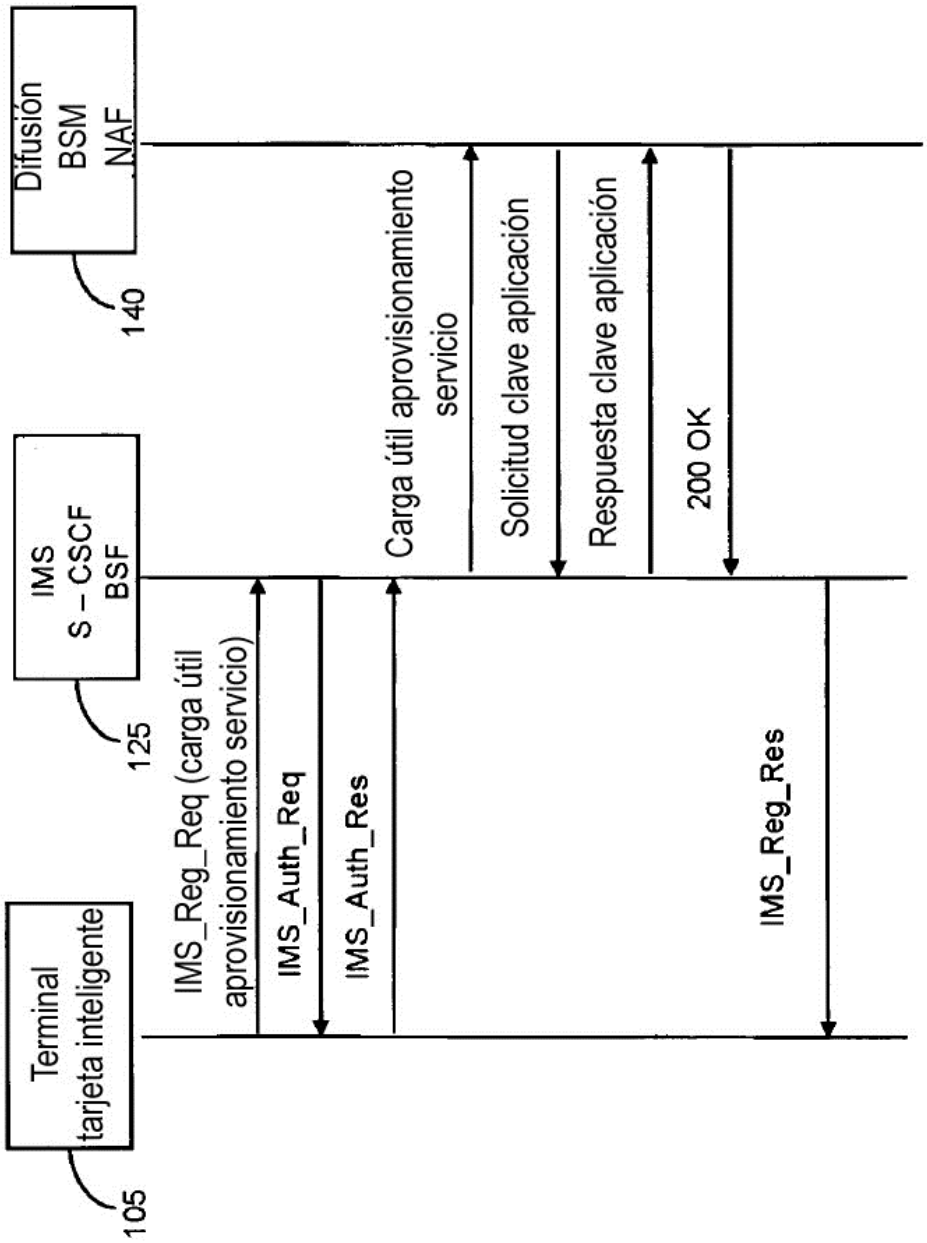

Terminal
tarjeta inteligente
105
IMS
S – CSCF
BSF
125
Difusión
BSM
NAF
140
IMS_Reg_Req(BCAST=1)
IMS_Auth_Req
IMS_Auth_Res
Suministro SMK
200 OK
IMS_Reg_Res

FIG. 8


Terminal
tarjeta inteligente
105
IMS
S – CSCF
BSF
125
Difusión
BSM
NAF
140
IMS_Reg_Req (carga útil aprovisionamiento servicio)
IMS_Auth_Req
IMS_Auth_Res
Carga útil aprovisionamiento servicio
Solicitud clave aplicación
Respuesta clave aplicación
200 OK
IMS_Reg_Res