(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 698 434**

(51) Int. CI.:

H04W 12/04 (2009.01)
H04L 29/06 (2006.01)
H04L 29/08 (2006.01)
H04W 12/06 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **03.07.2007 PCT/CN2007/070217**

(87) Fecha y número de publicación internacional: **17.01.2008 WO08006312**

(96) Fecha de presentación y número de la solicitud europea: **03.07.2007 E 07764146 (2)**

(97) Fecha y número de publicación de la concesión europea: **22.08.2018 EP 2037620**

(54) Título: **Método de realización para servicio push de GAA y dispositivo**

(30) Prioridad:

04.07.2006 CN 200610101212
17.11.2006 CN 200610145188

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
04.02.2019

(73) Titular/es:

NOKIA TECHNOLOGIES OY (100.0%)
Karaportti 3
02610 Espoo, FI

(72) Inventor/es:

YANG, YANMEI

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Método de realización para servicio push de GAA y dispositivo

Campo de la invención

La presente invención se refiere al campo de las tecnologías de comunicación de red y, en particular, a un método y a un dispositivo para implementar un servicio push de la arquitectura de autenticación genérica.

Antecedentes de la invención

En los estándares de comunicación inalámbrica de tercera generación, diversas entidades de servicios de aplicaciones utilizan un marco genérico para llevar a cabo la autenticación de la identidad del usuario, lo que se conoce como la arquitectura de autenticación genérica (GAA). Una aplicación de la arquitectura de autenticación genérica puede verificar y autenticar la identidad de un usuario de un servicio de aplicación y proporcionar al usuario que accede al servicio de aplicación una clave para una comunicación segura. Los diversos servicios de aplicación pueden incluir un servicio de difusión o multidifusión, un servicio de certificado de usuario, un servicio de mensajería instantánea, etc., o un servicio proxy.

La figura 1 ilustra un diagrama esquemático de un marco del GAA.

La arquitectura de autenticación genérica generalmente consiste en un equipo de usuario (UE), una entidad de función de servidor de arranque (BSF) que inicialmente verifica y autentica la identidad de un usuario, un servidor de suscriptor doméstico (HSS), una entidad de función de localización de suscriptor (SLF) que localiza el HSS y una entidad de función de aplicación de red (NAF). El BSF se usa para la autenticación de identidad mutua con el UE y también para la generación de una clave compartida, Ks, que la BSF comparte con el usuario, y el HSS almacena un archivo de descripción que describe la información del usuario y también funciona para generar información de autenticación. Dz, Zh, Zn, Ub y Ua indican una interfaz entre las entidades respectivas.

Por lo general, se requiere que el equipo de usuario con la intención de acceder a un servicio entre en contacto con la NAF correspondiente al servicio, es decir, el UE es requerido para iniciar activamente una solicitud de conexión a la NAF. Si la NAF utiliza la arquitectura genérica de autenticación GAA, primero se requiere que el UE realice una autenticación mutua con la BSF para la autenticación de identidad. Tras la autenticación exitosa, el UE calcula una clave derivada Ks_NAF para la comunicación encriptada con la NAF desde la clave Ks compartida con la BSF y transmite un identificador de transacción de sesión de arranque (B-TID) a la NAF, y la NAF obtiene de la BSF la clave derivada Ks_NAF de la clave compartida Ks de acuerdo con el B-TID recibido. Por lo tanto, el UE y la NAF pueden utilizar la clave derivada Ks NAF para comunicación segura a través de la interfaz Ua.

Se requiere el lado de la red en algunos escenarios de aplicación para iniciar activamente una solicitud de comunicación al equipo de usuario, que se conoce como un servicio push. Un flujo push GAA existente es el siguiente.

La NAF en primer lugar se requiere para solicitar la BSF para la clave derivada Ks_NAF de Ks para la comunicación a través de la interfaz Ua antes de la transmisión de un mensaje push al usuario mediante el uso de la tecnología GAA.

Si la BSF no ha negociado con el UE sobre ninguna clave compartida Ks disponible al recibir la solicitud de clave de la NAF, entonces la BSF adquiere un conjunto de vectores de autenticación del HSS y calcula Ks y Ks NAF y transmite a la NAF una señal de autenticación (AUTN) en el conjunto de vectores de autenticación y la clave derivada Ks_NAF y también posiblemente un número aleatorio (RAND), un identificador de transacción de sesión de arranque (B-TID), una vida útil de la clave derivada Ks_NAF en los vectores de autenticación, etc. Luego, la NAF transmite, en un mensaje push transmitido al UE, la información de AUTN, RAND, B-TID, identificador de NAF (NAF_ID), etc., y también posiblemente datos cifrados. El UE autentica la red y calcula la clave compartida Ks y la clave derivada Ks_NAF de acuerdo con los valores de AUTN y RAND.

Si la BSF ha negociado con el UE acerca de las claves Ks compartidas disponibles a la recepción de la solicitud de clave de la NAF, entonces la BSF calcula la clave derivada Ks_NAF a partir de la clave compartida Ks y transmite el correspondiente B-TID y la duración de Ks_NAF a la NAF. La NAF transporta el B-TID y el NAF-ID y también posiblemente los datos cifrados en un mensaje push transmitido al UE. El UE calcula la clave derivada Ks_NAF a partir de la clave compartida Ks en el B-TID o busca localmente un Ks_NAF correspondiente al B-TID y usa la clave para descifrar los datos cifrados transportados.

En el caso de la arquitectura de autenticación de arranque genérico basada en UICC (GBA U), la BSF y el UE pueden derivar dos claves de la clave compartida Ks, es decir, la clave derivada Ks_int_NAF colocada en una tarjeta de circuito integrado universal (UICC) y la clave derivada Ks_ext_NAF colocada en un equipo móvil (ME). En este caso, se requiere que la NAF negocie con el UE una clave que se utilizará para comunicación segura.
En un servicio iniciado en el UE, el lado del UE decide la clave derivada para uso de acuerdo con la ubicación de una

aplicación: si se trata de una aplicación basada en UICC, a continuación, se usa la clave derivada Ks_int_NAF puesta en la UICC; y si se trata de una aplicación basada en ME, se usa la clave derivada Ks_ext_NAF puesta en el ME. Luego, el UE notifica a la NAF el tipo de clave seleccionada indicando a la NAF la ubicación donde reside la aplicación. La NAF determina si se debe permitir un tipo de clave seleccionada por el terminal de acuerdo con una política local o con una política de la BSF. Si está permitido, entonces la clave se utiliza para la comunicación; de lo contrario, se rechaza la solicitud del UE.

Sin embargo, en el servicio push, no hay ningún mensaje transmitido entre la NAF y el UE antes de que la NAF transmita el mensaje push al UE. Incluso en algunos casos, es posible que al UE no se le proporcione un canal de retroalimentación para la transmisión de un mensaje al lado de la red. Por lo tanto, es imposible para el UE notificar al lado de la red sobre un tipo de clave que selecciona. En consecuencia, este enfoque existente no puede ser aplicable en el proceso push de GAA.

El documento "Proyecto de asociación de tercera generación; Servicios de grupo de especificación técnica y aspectos del sistema; Arquitectura de autenticación genérica (GAA); Función push de arquitectura de arranque genérico (GBA) (Versión 7)" Estándar 3GPP, 3GPP TS 33.XXX, v 0.0.1 (2006-05) divulga contornos del flujo de mensajes para arquitectura push GBA, donde el UE no tiene un canal de retorno a la red y, por lo tanto, no puede realizar el procedimiento de arranque directamente con la BSF. En su lugar, el arranque entre el UE y la BSF pasa a través de una NAF.

El documento "Sistema de telecomunicaciones móviles universales (UMTS); Arquitectura de autenticación genérica (GAA); Arquitectura de arranque genérica (3GPP TS 33.220 versión 7.4.0 versión 7 (2006-06))" divulga un modo de referencia GAA y funciones de los elementos de red.

Sumario de la invención

Las realizaciones de la invención proporcionan un método y un dispositivo para implementar un servicio push de la arquitectura de autenticación genérica para superar la indisponibilidad de una aplicación de servicio push de GAA en el caso de GBA U en la técnica anterior para garantizar así la seguridad del servicio. Este objetivo se consigue mediante las características de acuerdo con las reivindicaciones independientes, y las realizaciones ventajosas se describen mediante sus reivindicaciones dependientes.

De acuerdo con una realización a modo de ejemplo, se proporciona un método para implementar un servicio push de la arquitectura de autenticación genérica. El método incluye:

determinar, en un lado de la red, una clave de servicio push; usar la clave de servicio push para proteger el servicio push; y
seleccionar, mediante el UE, una clave de servicio push cualificada compatible con la clave de servicio push determinada por el lado de la red de acuerdo con la indicación, y comunicarse con el lado de la red usando la clave de servicio push cualificada.

De acuerdo con una realización a modo de ejemplo, se proporciona otro método para implementar un servicio push de la arquitectura de autenticación genérica, que incluye lo siguiente.

Un método para implementar un servicio push de la arquitectura de autenticación genérica incluye:

recibir, por un equipo de usuario, UE, una indicación desde un lado de la red, indicando la indicación un tipo de clave de servicio push determinada por el lado de la red; y

determinar, por el UE, una clave de servicio push compatible con el lado de la red de acuerdo con la indicación, y utilizar la clave de servicio push para obtener el servicio push.

Se proporciona una entidad de función de aplicación de red NAF, que incluye:

una unidad de determinación de clave de servicio push, configurada para determinar una clave de servicio push según se requiera para su uso, y

una unidad de interacción, configurada para transmitir un mensaje push a un equipo de usuario, UE, incluyendo el mensaje push una indicación de un tipo de clave de servicio push determinada en el lado de la red y para enviar un servicio push protegido por seguridad con la clave de servicio push al UE.

Se proporciona una entidad de función de servidor de protocolo de autenticación de arranque BSF, que incluye:

una unidad de determinación de clave de servicio push, configurada para determinar una clave de servicio push según se requiera para su uso; y
una unidad de interacción, configurada para transmitir un mensaje push a un equipo de usuario, UE, incluyendo el

mensaje push un tipo de clave de servicio push según se requiera para su uso.

Como puede verse a partir de las soluciones técnicas de acuerdo con las realizaciones de la invención que, en un servicio push de acuerdo con las realizaciones de la invención, el lado de red determina una clave de servicio push cualificada o la clave de servicio push y un tipo de clave y utiliza la clave para cifrar el servicio push para su transmisión al lado del usuario; y el lado del usuario selecciona una clave de servicio push con la que se puede reconocer el servicio push cifrado en el lado de la red y utiliza la clave para comunicación con el lado de la red. En una implementación práctica, una regla de selección de clave para su uso en el servicio push puede determinarse en una especificación de aplicación, por el operador de BSF o el operador de NAF, o conjuntamente por el usuario, el operador de BSF y el operador de NAF, adaptándose así convenientemente y de manera flexible a demandas en diferentes escenarios de aplicación. Una clave derivada correspondiente se selecciona según el tipo de clave determinado como clave de servicio push para garantizar la seguridad efectiva del servicio push.

Breve descripción de los dibujos

La figura 1 ilustra un diagrama esquemático de un marco de la arquitectura de autenticación genérica en la técnica anterior;

La figura 2 ilustra un diagrama de flujo de implementación de un método de acuerdo con una primera realización de la presente invención;

La figura 3 ilustra un diagrama de flujo del método de una implementación en la que una BSF y una NAF determinan conjuntamente un tipo de clave de acuerdo con una realización de la presente invención;

La figura 4 ilustra un diagrama de flujo del método de interacción de mensajes entre el lado de la red y el lado del usuario de acuerdo con una realización de la presente invención;

La figura 5 ilustra un diagrama de flujo del método de interacción de mensajes alternativo entre el lado de la red y el lado del usuario de acuerdo con una realización de la presente invención; y

La figura 6 ilustra un diagrama de flujo de implementación de un método de acuerdo con una segunda realización de la presente invención.

Descripción detallada de las realizaciones

En un servicio push de acuerdo con las realizaciones de la invención, el lado de red selecciona una clave de servicio push cualificada o la clave de servicio push y un tipo de clave y utiliza la clave para cifrar el servicio push para su transmisión al lado del usuario; y el lado del usuario selecciona una clave de servicio push con la que se puede reconocer el servicio push cifrado en el lado de la red y utiliza la clave para comunicación con el lado de la red. La clave de servicio push es la clave derivada de una clave Ks compartida por la BSF y el UE (Ks_int_NAF o Ks_ (ext) NAF). Como en el caso de GBA_U, la BSF y el UE pueden derivar dos claves de la clave compartida Ks, es decir, la clave derivada Ks_int_NAF colocada en la UICC y la clave derivada Ks_ext_NAF colocada en el ME. Por lo tanto, en vista de este caso, una regla de selección de un tipo de clave para uso en el servicio push puede determinarse en una especificación de la aplicación, por un operador de BSF o un operador de NAF, o conjuntamente por el usuario, el operador de BSF y el operador de NAF en las realizaciones de la invención.

Si la regla de selección de clave se determina conjuntamente por el usuario, el operador de BSF y el operador de NAF, a continuación, el usuario que suscribe un servicio que puede negociar con la red acerca de un tipo de clave, y un resultado de la negociación se puede poner en un archivo de suscripción de usuario. Alternativamente, el equipo móvil en el lado del usuario puede almacenar este resultado de selección.

Si el usuario y el operador de BSF negocian, entonces la información de la política de selección de clave en el lado de la red se puede colocar en un archivo de suscripción de usuario del HSS, por ejemplo, en la configuración de seguridad del usuario (USS) de los ajustes de seguridad del usuario de la arquitectura de autenticación genérica de arranque genérica (GUSS). La BSF puede decidir el tipo de clave que se utilizará para el servicio push y luego transmitir una clave disponible (Ks_int_NAF o Ks_ (ext) _NAF) a la NAF. Alternativamente, la BSF puede determinar el tipo de GBA de acuerdo con un atributo de UICC, calcular claves derivadas de Ks y transmitir todas las claves derivadas resultantes (dos claves derivadas de Ks_int_NAF Ks_ext_NAF) junto con la política de selección de clave en el archivo de suscripción del usuario para la NAF, y la NAF pueden decidir seleccionar un tipo de clave que se utilizará para el servicio push.

En este caso, el lado del usuario es solo necesario para seleccionar un tipo de clave para descifrar un mensaje push de acuerdo con un tipo de selección de clave almacenado localmente.

Si el usuario y el operador de NAF negocian, entonces se requiere que la NAF almacene la información de tipo de selección de clave correspondiente al usuario y use directamente una clave seleccionada al enviar el servicio al

usuario, y también el lado del usuario solo necesita seleccionar un tipo de clave para descifrar un mensaje de servicio push de acuerdo con un tipo de selección de clave almacenada localmente.

Si la regla de selección de clave se prescribe por la especificación de la aplicación, entonces puede prescribirse que: si la UICC es GBA activada, entonces se seleccionará la clave almacenada en la UICC; si la UICC no está habilitada para GBA, se seleccionará la clave almacenada en el ME. La BSF determina un tipo de clave para su uso a través de la interfaz Ua y selecciona una clave (en el ME o en el UICC) al recibir una solicitud de clave de servicio push de la NAF o de acuerdo con el atributo de UICC y la prescripción de la especificación de la aplicación y luego transmite la clave seleccionada a la NAF, o transmite el atributo de UICC junto con las dos claves a la NAF, y la NAF realiza la selección de acuerdo con la especificación de la aplicación.

En este caso, el lado del usuario, por supuesto, puede seleccionar una clave para ser utilizada para el descifrado de un mensaje push de acuerdo con su propio atributo de UICC y la prescripción de la especificación de la aplicación.

Si no hay una política de selección de clave prescrita en la especificación de la aplicación y en su lugar se prescribe solamente por el operador de BSF o el operador de NAF en el lado de la red, a continuación, la selección se puede hacer de las siguientes maneras.

1. El lado de la red selecciona y usa una clave de acuerdo con una o más información entre el atributo de UICC del usuario, la política del operador de red y la política del operador de NAF, y luego transmite en un mensaje push una indicación de un tipo de clave en uso. El lado del usuario selecciona una clave para descifrar de acuerdo con la indicación al recibir el mensaje push.

2. El lado de la red selecciona y usa una clave de acuerdo con el atributo de UICC del usuario, la política del operador de BSF o el operador de NAF en el lado de la red, pero no transmite ninguna indicación de tipo de clave al usuario, y en su lugar, el propio usuario hace un intento. En el caso de GBA_U, el equipo del usuario puede calcular dos claves y, en primer lugar, utilizar una de las claves para descifrar y luego utilizar la otra clave en caso de fallo.

3. La propia NAF determina qué parte de UE (ME o UICC) descifra los datos recibidos. Si es parte de la UICC, entonces la clave derivada de Ks almacenada en la UICC se usa para el cifrado, de lo contrario, se usa la clave derivada de Ks almacenada en el ME. El propio equipo de usuario también puede determinar si el ME o la UICC procesarán un mensaje push. Si el mensaje es procesado por el ME, entonces el ME utiliza la clave derivada en el ME; si el mensaje es procesado por la UICC, entonces la UICC usa la clave derivada en la UICC.

4. El lado de la red selecciona una clave de acuerdo con su propia política, la usa para cifrar el servicio push y luego la transmite al lado del usuario. El equipo del usuario de alguna manera ha obtenido previamente la política de selección de clave en el lado de la red, por ejemplo, mediante la descarga automática, desde un anuncio de servicio en el lado de la red, por el almacenamiento local de información de selección de clave cuando el usuario se suscribe a la red, etc. Al recibir un mensaje push, el lado del usuario selecciona una clave para descifrar el mensaje push de acuerdo con la política. Por ejemplo, un cliente de la aplicación capaz de recibir dicho mensaje se coloca en una ubicación cualificada de manera tal que el cliente de la aplicación se coloca en el ME si la clave derivada del ME se requiere para su uso o se coloca en la UICC si la clave derivada en la UICC se requiere para su uso. La política en el lado de la red puede variar, y, por lo tanto, en este caso, el usuario debe obtener dinámicamente la política más reciente de la red. Al cambiar la política en el lado de la red, se puede notificar al lado del usuario sobre la política, se puede transmitir un anuncio de servicio periódicamente al usuario para notificarle sobre la política más reciente en el lado de la red, o el usuario puede descargar periódicamente desde la red para actualización.

5. En analogía con la iniciación activa de un servicio desde el lado del usuario, un cliente de la aplicación se coloca previamente en una ubicación según sea necesario en vista de otras razones, y se decide un tipo de clave de acuerdo con la ubicación donde el cliente de la aplicación reside de una manera en que se selecciona la clave en el ME para una aplicación basada en ME o la clave en la UICC se selecciona para una aplicación basada en la UICC. La NAF en el lado de la red puede obtener la ubicación del cliente de la aplicación de las siguientes maneras posibles para determinar así un tipo de clave disponible.

(1) El usuario notifica al lado de la red al registrar un servicio para la suscripción. La información de suscripción se puede almacenar en el HSS, la BSF o la NAF. No se transmitirá ningún servicio push al usuario si una clave seleccionada de acuerdo con la ubicación del cliente de la aplicación no está calificada según lo requerido por el operador de NAF o BSF.

(2) La ubicación se conoce a partir de la aplicación por sí misma. Por ejemplo, una aplicación solo se puede implementar en el ME o en la UICC. La información de ubicación de la aplicación en el equipo en el lado del usuario puede almacenarse en el archivo de suscripción del usuario y puede ser obtenida por la BSF leyendo el archivo de suscripción del usuario cuando sea necesario conocer la información de ubicación de la aplicación.

(3) El lado de la red no transporta datos encriptados con una clave derivada de Ks al transmitir el primer mensaje push, decide una clave derivada para su uso de acuerdo con una respuesta del lado del usuario o información indicativa de la ubicación donde reside una aplicación al recibir el mensaje de respuesta, y luego transmite los datos cifrados con la clave derivada correspondiente de Ks. Por supuesto, si el tipo de clave indicado desde el lado del usuario no está cualificado como requerido en el lado de la red, entonces la NAF no transmitirá más datos posteriores al usuario.

La invención se detalla adicionalmente a continuación con referencia a los dibujos y a las realizaciones de la misma para hacer que los expertos en la técnica entiendan mejor la solución de la invención.

Se hace referencia a la figura 2, que ilustra un flujo de ejecución de un método de acuerdo con una primera realización de la invención, y el método incluye las siguientes etapas.

Etapa 201: La NAF requerida para implementar un servicio push comprueba si una clave de servicio push relacionada con el lado del usuario ya existe localmente, y si es así, el proceso avanza a la etapa 202; de lo contrario, el proceso pasa a la etapa 203.

Etapa 202: Selecciona la clave almacenada localmente para su uso y determina un tipo de clave disponible y, a continuación, ejecuta la etapa 211.

Etapa 203: La NAF solicita a la BSF una clave de servicio push.

La información del identificador del usuario, la información del identificador de la NAF, etc., se puede transportar en el mensaje de solicitud. En particular, el identificador de usuario puede ser un identificador privado del identificador de identidad de suscriptor privado del subsistema multimedia IP (IMPI) o un identificador permanente de identificador de suscriptor móvil internacional (IMSI) para el usuario u otra información de identificación que pueda identificar al usuario de manera única.

Etapa 204: La BSF determina si la NAF ha sido autorizada para el servicio push, y si no es así, entonces el proceso pasa a la etapa 205; de lo contrario, el proceso pasa a la etapa 206.

La BSF puede determinar si la NAF ha sido autorizada de acuerdo con la información de suscripción del usuario o una relación de suscripción del operador de la NAF con el operador de la BSF.

Etapa 205: Se rechaza la solicitud de clave de la NAF y el flujo finaliza.

La etapa anterior 204 y la etapa 205 son etapas opcionales. En otras palabras, la BSF puede, alternativamente, no determinar si la NAF ha sido autorizada para el servicio push.

Etapa 206: La BSF verifica si una clave Ks para el cálculo de una clave de servicio push de la NAF existe localmente, y si no es así, entonces el proceso pasa a la etapa 207; de lo contrario, el proceso pasa a la etapa 208.

Como se ha mencionado anteriormente, la NAF puede incluir la información del identificador del usuario y la información de identificador de la NAF en la transmisión del mensaje de solicitud de clave de servicio push a la BSF, y por lo tanto la BSF puede comprobar con la información para ver si hay una de las claves disponibles almacenadas localmente que corresponde a la información, es decir, la clave Ks disponible para el cálculo de una clave de servicio push de la NAF.

Esta etapa se puede omitir si Ks en el push GAA no puede ser reutilizada, y el flujo pasa directamente a la etapa 207.

Etapa 207: La BSF obtiene nuevos vectores de autenticación y calcula la clave Ks que comparte con el usuario.

La información de suscripción del usuario se almacena en el HSS, como es conocido para los expertos en la técnica. Por lo tanto, la BSF puede obtener un conjunto de vectores de autenticación correspondientes al usuario del HSS de acuerdo con el identificador de usuario contenido en el mensaje de solicitud de clave de servicio push recibido, y calcular la clave compartida Ks y las claves derivadas Ks_NAF o Ks_(ext/int)_NAF de Ks.

Etapa 208: La BSF calcula las claves derivadas Ks_NAF/Ks_(ext/int)_NAF de Ks.

En el caso de la GBA_U, la BSF y el usuario pueden derivar dos claves de Ks, una de las cuales se pone en la tarjeta de circuito integrado universal (UICC), es decir, Ks_int_NAF, y la otra de las cuales se pone en el ME, es decir, Ks_ext_NAF. En este caso, se determinará un tipo de clave disponible para la NAF. En otras palabras, se determina si la NAF utilizará la clave derivada almacenada en la UICC o en el ME.
Si la BSF puede calcular las dos claves derivadas de Ks, a continuación, un tipo de clave requerida para la NAF se puede determinar por la BSF solamente o por la BSF y la NAF conjuntamente.

Etapa 209: La BSF transmite las claves derivadas obtenidas de Ks a la NAF.

La BSF también puede transmitir a la NAF la información de AUTN, B-TID, duración de la clave, etc., y también posiblemente otros parámetros para el cálculo de la clave de servicio push.

Puesto que la BSF puede determinar solamente un tipo de clave requerida para la NAF, a continuación, la BSF puede transmitir a la NAF solo la clave derivada seleccionada de Ks y también, posiblemente, el tipo de con la misma clave correspondiente. Alternativamente, la BSF puede transmitir a la NAF tanto la clave derivada obtenida de Ks como una política de selección de clave prescrita por la BSF (por ejemplo, una indicación del tipo de clave permitida para su uso), de modo que la NAF pueda determinar el tipo disponible de clave de acuerdo con la política. Por supuesto, también es posible que solo las dos claves derivadas obtenidas de Ks puedan transmitirse a la NAF, y la NAF puede seleccionar un tipo de clave para usarse de acuerdo con su propia política de selección de claves o un tipo de clave prescrito en la especificación de la aplicación y también posiblemente en relación con la información de capacidad del usuario.

Por supuesto, la propia BSF puede en primer lugar seleccionar una clave para el uso y luego calcular una clave derivada cualificada de Ks.

La selección de uno de los enfoques para el uso se puede determinar de acuerdo con el entorno de la aplicación del sistema, la información de suscripción del terminal, las capacidades del terminal, etc. Más adelante se detallará una forma específica para seleccionar un tipo de clave.

Etapa 210: La NAF determina la clave de servicio push disponible y el tipo de clave.

Etapa 211: La NAF transmite un mensaje push al lado del usuario.

La NAF puede transmitir una política de selección de clave en el lado de la red (simplemente una indicación del tipo de clave seleccionada por la NAF) en el mensaje.

Cabe señalar que los datos de aplicación a proteger con Ks_(ext/int)_NAF (por ejemplo, el cifrado, la integridad-protección, etc.) y la información PUSH_INFO (por ejemplo, AUTN, B-TID) requerido para el cálculo de Ks_(ext/int)_NAF se puede transmitir en el mismo mensaje o por separado. En el caso de una transmisión por separado, la política de selección de clave se puede transmitir junto con un mensaje de inserción que lleva PUSH_INFO o se puede colocar en un mensaje de inserción en el que los datos de la aplicación se transmiten y transmitirán con el mismo.

Etapa 212: El lado del usuario selecciona una clave derivada cualificada, que es una clave de servicio push compatible con el lado de la red, y usa la clave para la comunicación con el lado de la red.

Tras la recepción del mensaje push transmitido desde la NAF, el lado de usuario determina un tipo de clave para ser utilizado antes de su uso de la clave derivada de Ks para descifrar el servicio push. Por ejemplo, una clave derivada cualificada se puede seleccionar para su uso de las siguientes maneras.

(1) Si hay un tipo de indicación de clave, es decir, una política de selección de clave, en el mensaje push, entonces se puede usar la clave correspondiente para descifrar el servicio push.

(2) Si se ha prescrito una clave preferida para la aplicación, entonces la selección se puede hacer de manera que primero se seleccione una clave y luego se decida la ubicación de un punto de descifrado. El equipo del usuario puede seleccionar una clave derivada cualificada de acuerdo con la prescripción de la especificación de la aplicación y el atributo UICC (GBA habilitado o no) y usar la clave derivada para descifrar el servicio push.

(3) Se decide a partir de un atributo de la aplicación por sí mismo. Por ejemplo, si la aplicación solo se puede implementar en la UICC o en el ME, entonces se puede seleccionar una clave derivada calificada en un principio de que una clave debe almacenarse justo en el lugar donde se encuentra el cliente de la aplicación y luego se puede usar para descifrar el servicio push.

(4) Si el equipo del usuario tiene información de selección de clave preconfigurada correspondiente a la aplicación, entonces la selección se puede hacer según lo configurado.

(5) Se utiliza una forma adaptativa, es decir, en el caso de GBA_U, el equipo de usuario puede calcular dos claves y, en primer lugar, utilizar una de las claves para descifrar y luego usar la otra clave para descifrarla en caso de fallo.

Como se mencionó anteriormente, si dos claves derivadas de Ks están presentes en o calculadas por el BSF, a continuación, un tipo de clave requerida para la NAF se puede determinar por la BSF solamente o por la BSF y la NAF conjuntamente.

Según la invención, la BSF puede seleccionar un tipo de clave a disposición de la NAF en cualquiera de las siguientes maneras.

(1) La BSF determina un tipo de clave requerida para la NAF de acuerdo con una regla de selección de clave determinada por el usuario al suscribirse a la red.

(2) La BSF determina un tipo de clave requerida para la NAF de acuerdo con un atributo de la propia aplicación. Por ejemplo, la clave derivada almacenada en la tarjeta de circuito integrado universal UICC puede seleccionarse para usarse si la aplicación está en la UICC, y la clave derivada almacenada en el equipo móvil ME puede seleccionarse para usarse si la aplicación está en el ME.

(3) La BSF determina un tipo de clave requerida para la NAF de acuerdo con una regla de selección de clave prescrita en la especificación de la aplicación y en el atributo del usuario. Por ejemplo, si un tipo preferido de clave se prescribe en la especificación de la aplicación, entonces el tipo preferido de clave prescrito se puede seleccionar preferentemente como un tipo de clave requerido para la NAF; y si no se determina una prescripción de selección de clave en la especificación de la aplicación, entonces la BSF puede determinar un tipo de clave requerida para la NAF de acuerdo con un atributo de la propia aplicación.

Alternativamente, la BSF y la NAF pueden determinar conjuntamente una clave de servicio push o tanto una clave de servicio push y un tipo de clave requerida para la NAF de numerosas maneras.

Se hace referencia a la figura 3, que ilustra una BSF y una NAF que determinan conjuntamente un tipo de clave, y el flujo de aplicación incluye las siguientes etapas.

Etapa 301: La BSF obtiene una clave compartida con el usuario y calcula las claves derivadas de la clave compartida.

Etapa 302: La BSF responde a las claves derivadas calculadas de la clave compartida a la NAF en un mensaje que lleva una política de selección de clave o información de suscripción del usuario prescrita por la BSF.

La política de selección de clave prescrita por la BSF puede ser, por ejemplo, que solo Ks_int_NAF se puede permitir para el uso o ambas se puede permitir, con preferencia por Ks_int_NAF.

Etapa 303: La NAF selecciona un tipo de clave disponible de acuerdo con la política de selección de clave o la información de suscripción del usuario enviada desde la BSF.

Si la BSF no envía ninguna política de selección de clave, entonces la NAF selecciona un tipo de clave disponible de acuerdo con su propia política.

Etapa 304: Una clave derivada del tipo de clave seleccionado se toma como una clave de servicio push requerida por la NAF para su uso.

En la etapa 302 anterior, la BSF puede alternativamente devolver solo las claves derivadas calculadas de la clave compartida a la NAF, y luego la NAF puede seleccionar un tipo de clave de acuerdo con su propia política de selección de clave y también posiblemente en conexión con información de capacidad UICC del usuario. La NAF puede obtener las capacidades UICC del usuario tras la suscripción del usuario u obtener la información de capacidad del usuario de la BSF.

La política de selección de clave de la NAF puede ser, por ejemplo, que solo Ks_int_NAF se puede permitir para el uso o ambos se puede permitir con preferencia por Ks_int_NAF, es decir, si la tarjeta de usuario es capaz de soportar una función de derivación de claves de GBA, entonces Ks_int_NAF puede seleccionarse; de lo contrario, se puede seleccionar Ks _NAF.

A continuación, se darán descripciones detalladas de un flujo de mensajes cuando el lado de la red y el lado del usuario interactúan de acuerdo con la invención.

Se hace referencia a la figura 4, que ilustra un flujo de una realización en la que el lado de la red y el lado del usuario interactúan a través de mensajes.

1. La NAF pretende transmitir un mensaje push a un usuario. Si aún no hay ninguna clave de servicio push local, la NAF solicita a la BSF una clave de servicio push al llevar información de un identificador de usuario, un identificador de NAF (NAF_ID), etc., en un mensaje de solicitud. En particular, el identificador de usuario puede ser un identificador privado IMPI o un identificador permanente IMSI del usuario u otro identificador que pueda identificar de manera única al usuario. Si ya existe una clave de servicio push relacionada con el usuario en la NAF, entonces el flujo pasa directamente a la etapa 4.

2. La BSF verifica si la NAF ha sido autorizada para un servicio push. Si la NAF no ha sido autorizada para el servicio push, entonces la BSF procede a la etapa 3'; de lo contrario, la BSF obtiene Ks y calcula las claves derivadas Ks_ (ext/int)_push_NAF de Ks a partir de Ks. En primer lugar, la BSF busca un Ks disponible localmente correspondiente al usuario. Si ya existe Ks disponible, la BSF calcula las claves derivadas Ks_ (ext/int)_push_NAF de Ks a partir de Ks como una clave de servicio push de la NAF; de lo contrario, la BSF primero obtiene un conjunto de nuevos vectores de autenticación, obtiene Ks de los parámetros existentes, calcula las claves derivadas de Ks como una clave de servicio push Ks_(ext/int)_push_NAF de la NAF. Entonces, la BSF pasa a la etapa 3.

3'. La BSF responde a la NAF rechazando el mensaje de solicitud de clave de servicio push. Esta etapa es opcional.

3. La BSF transmite a la NAF el B-TID, la duración de la clave y las claves de servicio push calculadas Ks_(ext/int)_push_NAF de la NAF y también posiblemente AUTN y otros parámetros para el cálculo de una clave de servicio push. La BSF puede determinar un tipo de clave derivada de Ks que se utilizará para proteger el servicio push (especialmente en el caso de GBA U) y transmitir solamente una clave disponible a la NAF para su uso. Específicamente, se puede determinar qué tipo de clave utilizará la NAF como clave para el cifrado de la información de inserción de las siguientes maneras.

(1) Uso de qué tipo de clave se ha negociado entre el usuario y la red tras la suscripción y se coloca en un archivo de suscripción de usuario (por ejemplo, en GUSS del archivo de suscripción de usuario en el HSS), y luego la BSF puede hacer una determinación de acuerdo con la información de suscripción.

(2) La ubicación donde se encuentra el cliente de la aplicación en el lado del equipo (ME o UICC) se proporciona en la información de suscripción del usuario. La BSF puede hacer la selección en un principio de que una clave debe almacenarse justo en el lugar donde se encuentra el cliente de la aplicación.

(3) La determinación se realiza de acuerdo con un atributo de la aplicación por sí mismo. Por ejemplo, si la aplicación solo se puede implementar en la UICC o en el ME, entonces la BSF puede hacer la selección en un principio de que una clave debe almacenarse justo en el lugar donde se encuentra el cliente de la aplicación.

(4) Si se ha prescrito una clave preferida en la especificación de la aplicación, entonces la selección se puede hacer de manera que primero se seleccione una clave y luego se decida la ubicación de un punto de descifrado. La BSF puede realizar la selección de acuerdo con la prescripción de la especificación de la aplicación y un atributo UICC (GBA habilitado o no).

Alternativamente, la BSF no puede determinar un tipo de clave derivada de Ks que se utilizará para proteger el servicio push, pero puede transmitir solo la información de suscripción del usuario (por ejemplo, USS) a la NAF.

4. La NAF compone un mensaje push que puede transmitirse junto con el servicio push cifrado por la clave derivada de Ks. Se puede seleccionar un tipo de clave para su uso de las siguientes maneras.

(1) Si la BSF responde solo un tipo de clave, entonces se puede usar la clave.

(2) Si la BSF responde dos tipos de claves, así como una política de selección de claves o información de suscripción del usuario, la NAF puede realizar la selección de acuerdo con la política de selección de claves o la información de suscripción del usuario. Con respecto a la información de suscripción, el usuario y el operador pueden haber negociado previamente un tipo de clave para el uso o la ubicación de un punto de descifrado (ME o UICC).

(3) Si se ha prescrito una clave preferida en la especificación de la aplicación, entonces la selección se puede hacer de manera que primero se seleccione una clave y luego se decida la ubicación de un punto de descifrado. La NAF puede realizar la selección de acuerdo con la prescripción de la especificación de la aplicación y un atributo UICC (GBA habilitado o no).

(4) La NAF puede realizar la selección de acuerdo con su propia política o información de usuario almacenada localmente y también posiblemente en relación con un atributo UICC, que puede obtenerse en GUSS devuelto por la BSF.

(5) La determinación se realiza de acuerdo con un atributo de la aplicación por sí mismo. Por ejemplo, si la aplicación solo se puede implementar en la UICC o en el ME, entonces la NAF puede hacer la selección en un principio de que una clave debe almacenarse justo en el lugar donde se encuentra el cliente de la aplicación.

5. La NAF transmite al UE un mensaje push, que puede incluir la información de B-TID, NAF_ID, AUTN, etc., y también posiblemente un identificador de tipo de la clave derivada de Ks seleccionada por la NAF y también posiblemente un servicio push protegido con la clave derivada seleccionada de Ks. En el diagrama, "[]" en esta etapa indica un parámetro opcional y se aplicará igualmente a continuación. Cabe señalar que las descripciones anteriores son aplicables a un caso de transmisión de datos de aplicación e información requerida para el cálculo

de un Ks derivado (por ejemplo, AUTN) en el mismo mensaje. Además, como se mencionó anteriormente, los datos de la aplicación pueden transmitirse por separado de la información requerida para un Ks derivado. En el caso de una transmisión separada, se puede transmitir un identificador de tipo de clave al UE en un mensaje de inserción que lleve a cualquiera de los mismos.

6. Al recibir el mensaje push que contiene los datos de la aplicación, el UE determinará un tipo de clave derivada de Ks para usar antes del uso de la clave derivada para descifrar los datos push. Se puede determinar un tipo de clave para usar de las siguientes maneras.

(1) Si se proporciona una indicación de tipo de clave en el mensaje push, entonces se puede usar una clave correspondiente para el descifrado.

(2) Si se ha prescrito una clave preferida para la aplicación, entonces la selección se puede hacer de manera que primero se seleccione una clave y luego se decida la ubicación de un punto de descifrado. El UE puede realizar la selección de acuerdo con la prescripción de la especificación de la aplicación y un atributo UICC (GBA habilitado o no).

(3) La determinación se realiza de acuerdo con un atributo de la aplicación por sí mismo. Por ejemplo, si la aplicación solo se puede implementar en la UICC o en el ME, entonces la BSF puede hacer la selección en un principio de que una clave debe almacenarse justo en el lugar donde se encuentra el cliente de la aplicación.

(4) Si el UE tiene información de selección de clave preconfigurada correspondiente a la aplicación, entonces la selección se puede hacer según lo configurado.

(5) Se utiliza una forma adaptativa, es decir, en el caso de GBA U, el equipo puede calcular dos claves y, en primer lugar, utilizar una de las claves para descifrar y luego usar la otra clave para descifrar si falla.

Se hace referencia a la figura 5, que ilustra un flujo de otra realización en la que el lado de la red y el lado del usuario interactúan a través de mensajes.

1. La NAF pretende transmitir un mensaje push a un usuario. Si aún no hay ninguna clave de servicio push local, la NAF solicita a la BSF una clave de servicio push al llevar información tal como un identificador de usuario, un identificador de NAF (NAF_ID), etc., en un mensaje de solicitud. En particular, el identificador de usuario puede ser un identificador privado IMPI o un identificador permanente IMSI del usuario u otro identificador que pueda identificar de manera única al usuario. Si ya existe una clave de servicio push relacionada con el usuario en la NAF, entonces el flujo pasa directamente a la etapa 4.

2. La BSF verifica si la NAF ha sido autorizada para un servicio push. Si la NAF no ha sido autorizada para el servicio push, entonces la BSF procede a la etapa 3'; de lo contrario, la BSF obtiene Ks y calcula las claves derivadas Ks_ (ext/int) _push_NAF de Ks a partir de Ks. En primer lugar, la BSF busca un Ks disponible localmente correspondiente al usuario. Si ya existe Ks disponible, la BSF calcula las claves derivadas Ks_ (ext/int)_push_NAF de Ks a partir de Ks como una clave de servicio push de la NAF; de lo contrario, la BSF primero obtiene un conjunto de nuevos vectores de autenticación, obtiene Ks de los parámetros existentes, calcula las claves derivadas de Ks como una clave de servicio push Ks_(ext/int)_push_NAF de la NAF. Entonces, la BSF pasa a la etapa 3. Por supuesto, si no se puede reutilizar ningún Ks, es posible que la BSF no necesite determinar si ya existe un Ks disponible, y en su lugar puede obtener nuevos vectores de autenticación directamente para Ks.

3'. La BSF responde a la NAF rechazando el mensaje de solicitud de clave de servicio push.

3. La BSF transmite a la NAF las claves de servicio push calculadas Ks_(ext/int)_push_NAF de la NAF y también posiblemente la duración de la clave y/u otros parámetros para el cálculo de una clave de servicio push, por ejemplo, AUTN, B-TID, etc. La BSF puede determinar un tipo de clave derivada de Ks que se utilizará para proteger el servicio push (especialmente en el caso de GBA U) y transmitir solamente una clave disponible a la NAF para su uso. Específicamente, se puede determinar qué tipo de clave utilizará la NAF como clave para el cifrado de la información de inserción de las siguientes maneras.

(1) Uso de qué tipo de clave se ha negociado entre el usuario y la red tras la suscripción y se coloca en un archivo de suscripción de usuario (por ejemplo, en GUSS del archivo de suscripción de usuario en el HSS), y luego la BSF puede hacer una determinación de acuerdo con la información de suscripción.

(2) La ubicación donde se encuentra el cliente de la aplicación en el lado del equipo (ME o UICC) se proporciona en la información de suscripción del usuario. La BSF puede hacer la selección en un principio de que una clave debe almacenarse justo en el lugar donde se encuentra el cliente de la aplicación.

(3) La determinación se realiza de acuerdo con un atributo de la aplicación por sí mismo. Por ejemplo, si la aplicación solo se puede implementar en la UICC o en el ME, entonces la BSF puede hacer la selección en un

principio de que una clave debe almacenarse justo en el lugar donde se encuentra el cliente de la aplicación.

(4) Si se ha prescrito una clave preferida en la especificación de la aplicación, entonces la selección se puede hacer de manera que primero se seleccione una clave y luego se decida la ubicación de un punto de descifrado. La BSF puede realizar la selección de acuerdo con la prescripción de la especificación de la aplicación y un atributo UICC (GBA habilitado o no).

Alternativamente, la BSF no puede determinar un tipo de clave derivada de Ks que se utilizará para proteger el servicio push, pero puede transmitir solo la información de suscripción del usuario (por ejemplo, USS) a la NAF.

4. La NAF compone un mensaje push que no contiene datos encriptados o protegidos con integridad con la clave derivada de Ks.

5. El primer mensaje push se transmite al UE. En este momento, también se puede transmitir una política de selección de claves en el lado de la red. La política puede ser una política prescrita por la propia NAF o por la BSF y puede indicar que solo se puede usar uno o ambos tipos de clave.

6. Al recibir el mensaje push, el UE verifica la legalidad del mensaje y el cliente de la aplicación selecciona un tipo de clave compatible.

7. El UE transmite un mensaje de respuesta a la red mientras notifica a la NAF el tipo de clave seleccionado (es decir, la ubicación del punto de descifrado en el cliente de la aplicación).

8. La NAF protege el servicio push con la clave seleccionada por el UE o finaliza el flujo si el lado del usuario devuelve un tipo no cualificado.

9. La NAF transmite los datos cifrados al UE.

10. El UE calcula una clave derivada de Ks y usa la clave apropiada para el descifrado.

Se hace referencia a la figura 6, que ilustra un flujo de implementación de un método de acuerdo con una segunda realización de la presente invención.

En esta realización, la BSF y el UE determinan conjuntamente un tipo de clave para un servicio push. El flujo incluye las siguientes etapas.

1. La NAF pretende transmitir un mensaje push a un usuario. Si aún no hay ninguna clave de servicio push local, la NAF solicita a la BSF una clave de servicio push al llevar información de un identificador de usuario, un identificador de NAF (NAF_ID), etc., en un mensaje. En particular, el identificador de usuario puede ser un identificador privado IMPI o un identificador permanente IMSI del usuario u otro identificador que pueda identificar de manera única al usuario. Si la NAF tiene su propio requisito sobre el tipo de clave, entonces el mensaje puede incluir además el tipo de clave requerido por la NAF para su uso.
2-3. La BSF ejecuta los procesos correspondientes que involucran principalmente los siguientes puntos a la recepción de la solicitud. La BSF primero obtiene un conjunto de nuevos vectores de autenticación del HSS y luego transmite un mensaje de inserción al UE al llevar el mensaje AUTN, RAND y/o B-TID y posiblemente también la NAF-ID. Además, la BSF puede determinar además un tipo de clave para su uso de acuerdo con el tipo de clave requerido por la NAF para su uso y también posiblemente con vistas a una cierta política del operador del BSF, si la hubiera. En este caso, el mensaje push incluirá además un tipo de clave seleccionado.
4. El UE verifica la red contra AUTN y RAND y calcula Ks al recibir el mensaje push.
5. El UE transmite un mensaje de respuesta a la BSF si hay un canal de retroalimentación del UE a la BSF. Si el UE no puede admitir el tipo de clave determinado por la BSF, entonces un tipo de clave seleccionado por el UE puede incluirse en el mensaje de respuesta, de modo que la BSF pueda volver a determinar un tipo de clave para el servicio push o determinar si transmitir un mensaje push al UE en vista de las capacidades del UE.
6. La BSF transmite las claves GBA calculadas (Ks_(ext/int)_NAF) a la NAF. En el caso de GBA_U, una clave del tipo de clave negociada puede transmitirse a la NAF, o ambas claves calculadas y el tipo de clave seleccionado por la BSF y/o el UE pueden transmitirse a la NAF, que a su vez puede hacer selección. Además, la BSF puede determinar además si el tipo de clave seleccionado por el UE se cualifica si el tipo de clave seleccionado por el UE se lleva en la etapa 5.
7. La NAF utiliza la clave GBA para cifrar el servicio push para la transmisión.
8. La NAF transmite al UE un mensaje push que contiene los datos y también posiblemente el tipo de clave de cifrado.
9. El UE utiliza la clave correspondiente para descifrar el mensaje push recibido.

Una realización de la presente invención además divulga una red de función de aplicación de entidad NAF, que incluye:

una unidad de determinación de clave de servicio push, adaptada para determinar una clave de servicio push

según se requiera para su uso; y
una unidad de interacción, adaptada para notificar al lado del usuario sobre la clave de servicio push determinada en el lado de la red y para el servicio push protegido por seguridad con la clave de servicio push al lado del usuario.

Una realización de la presente invención además da a conocer una entidad de función de servidor de protocolo de autenticación de arranque BSF, que incluye:

una unidad de determinación de clave de servicio push, adaptada para determinar una clave de servicio push según se requiera para su uso; y
una unidad de interacción, adaptada para notificar al lado del usuario y/o una entidad de función de aplicación de red NAF sobre la clave de servicio push determinada según se requiera para su uso.

Aunque la invención se ha descrito con referencia a las realizaciones, los expertos en la técnica podrán apreciar que son posibles numerosas modificaciones y variaciones a la misma. Las reivindicaciones adjuntas definen el alcance de la invención.

REIVINDICACIONES

1. Un método para implementar un servicio push de la arquitectura de autenticación genérica, que comprende:
determinar (210; 304), en el lado de la red, una clave de servicio push, y usar la clave de servicio push para proteger el servicio push para la transmisión a un equipo de usuario, UE, **caracterizado por que** el método comprende, además:

transmitir (211), mediante una función de aplicación de red, NAF, un mensaje push al UE, incluyendo el mensaje push una indicación de un tipo de clave de servicio push determinada por el lado de la red, en donde el tipo de clave de servicio push determinado por el lado de la red es una clave derivada Ks_int_NAF o una clave derivada Ks_ext_NAF;
seleccionar (212), mediante el UE, una clave de servicio push cualificada compatible con la clave de servicio push determinada por el lado de la red de acuerdo con la indicación, y comunicarse con el lado de la red usando la clave de servicio push cualificada.

2. El método según la reivindicación 1, en el que la etapa de determinar en el lado de la red una clave de servicio push comprende:

determinar, mediante una función de servidor de arranque, BSF, la clave de servicio push; o
determinar (210, 204), mediante la NAF, la clave de servicio push.

3. El método según la reivindicación 2, en el que la etapa de determinar mediante la BSF la clave de servicio push comprende:

seleccionar, mediante la BSF, un tipo de clave disponible para la NAF, obteniendo una clave Ks para el cálculo de la clave de servicio push de la NAF, y calcular claves derivadas de Ks;
tomar una entre las claves derivadas del tipo de clave seleccionado como la clave de servicio push como lo requiere la NAF para su uso; y
transmitir a la NAF, mediante la BSF, la clave de servicio push del tipo seleccionado de clave.

4. El método según la reivindicación 3, en el que la etapa de seleccionar mediante la BSF el tipo de clave disponible para la NAF comprende:

determinar, mediante la BSF, el tipo de clave de acuerdo con una regla de selección de clave determinada cuando el usuario se suscribe a la red; o
determinar, mediante la BSF, el tipo de clave de acuerdo con un atributo de una aplicación; o
determinar, mediante la BSF, el tipo de clave de acuerdo con una regla de selección de claves prescrita en una especificación de aplicación y un atributo de usuario; o
determinar, mediante la BSF, el tipo de clave de acuerdo con una o ambas políticas propias y el tipo de clave.

5. El método según la reivindicación 2, en el que la etapa de determinar mediante la NAF la clave de servicio push comprende:

obtener, mediante la BSF, una clave compartida con el UE, y calcular claves derivadas de la clave compartida;
devolver a la NAF las claves derivadas calculadas de la clave compartida;
seleccionar, mediante la NAF, un tipo de clave disponible; y
tomar una entre las claves derivadas del tipo de clave seleccionado como la clave de servicio push requerida por la NAF para su uso.

6. El método según la reivindicación 5, en el que la etapa de devolver a la NAF las claves derivadas calculadas de la clave compartida comprende, además:

transportar, mediante la BSF, una indicación de la política de selección de clave o información de suscripción del usuario prescrita por la BSF en un mensaje que devuelve las claves derivadas a la NAF; y
la etapa de seleccionar mediante la NAF el tipo de clave disponible comprende:
seleccionar, mediante la NAF, el tipo de clave disponible de acuerdo con una indicación de la política de selección de clave o la información de suscripción del usuario devuelta por la BSF.

7. El método según la reivindicación 5, en el que la etapa de seleccionar mediante la NAF el tipo de clave disponible comprende:

seleccionar, mediante la NAF, el tipo de clave disponible de acuerdo con su propia política de selección de clave; o
seleccionar, mediante la NAF, el tipo de clave disponible de acuerdo con un tipo de clave prescrito en una especificación de aplicación.

8. El método según la reivindicación 1, en el que la clave de servicio push cualificada se obtiene mediante el siguiente método:
recibir, mediante el UE, un tipo de clave de servicio push según una indicación del lado de la red, y obtener una clave derivada como clave de servicio push cualificada compatible con el lado de la red.

9. Un método para implementar un servicio push de arquitectura de autenticación genérica, que comprende:

recibir, mediante un equipo de usuario, UE, una indicación desde un lado de la red, indicando la indicación un tipo de clave de servicio push determinada por el lado de red, en donde el tipo de clave de servicio push determinado por el lado de la red es una clave derivada Ks_int_NAF o una clave derivada Ks_ext_NAF; y
determinar, por el UE, una clave de servicio push compatible con el lado de la red de acuerdo con la indicación y utilizar la clave de servicio push para obtener el servicio push.

10. El método según la reivindicación 9, en el que la etapa de recibir mediante un UE, una indicación desde un lado de la red comprende:
recibir, mediante el UE, una indicación de una función de aplicación de red, NAF.

11. El método según la reivindicación 10, en el que la etapa de recibir mediante un UE, una indicación desde un lado de la red comprende:
recibir, mediante el UE, un mensaje push que incluye una indicación de la NAF.

12. El método según la reivindicación 9, en el que la clave de servicio push compatible con el lado de la red está determinada por el UE que comprende:
obtener, mediante el UE, el tipo de clave que requiere el lado de la red para su uso, y determinar la clave derivada de Ks asociada al tipo de clave como la clave de servicio push.

13. Una entidad de función de aplicación de red NAF, que comprende:
una unidad de determinación de clave de servicio push, configurada para determinar una clave de servicio push según se requiere para su uso, **caracterizada por que** la NAF comprende, además:
una unidad de interacción, configurada para transmitir un mensaje push a un equipo de usuario, UE, incluyendo el mensaje push una indicación de un tipo de clave de servicio push determinado en el lado de la red y para enviar al UE un servicio push protegido por seguridad con la clave de servicio push, en donde el tipo de clave de servicio push determinado por el lado de la red es una clave derivada Ks_int_NAF o una clave derivada Ks_ext_NAF.

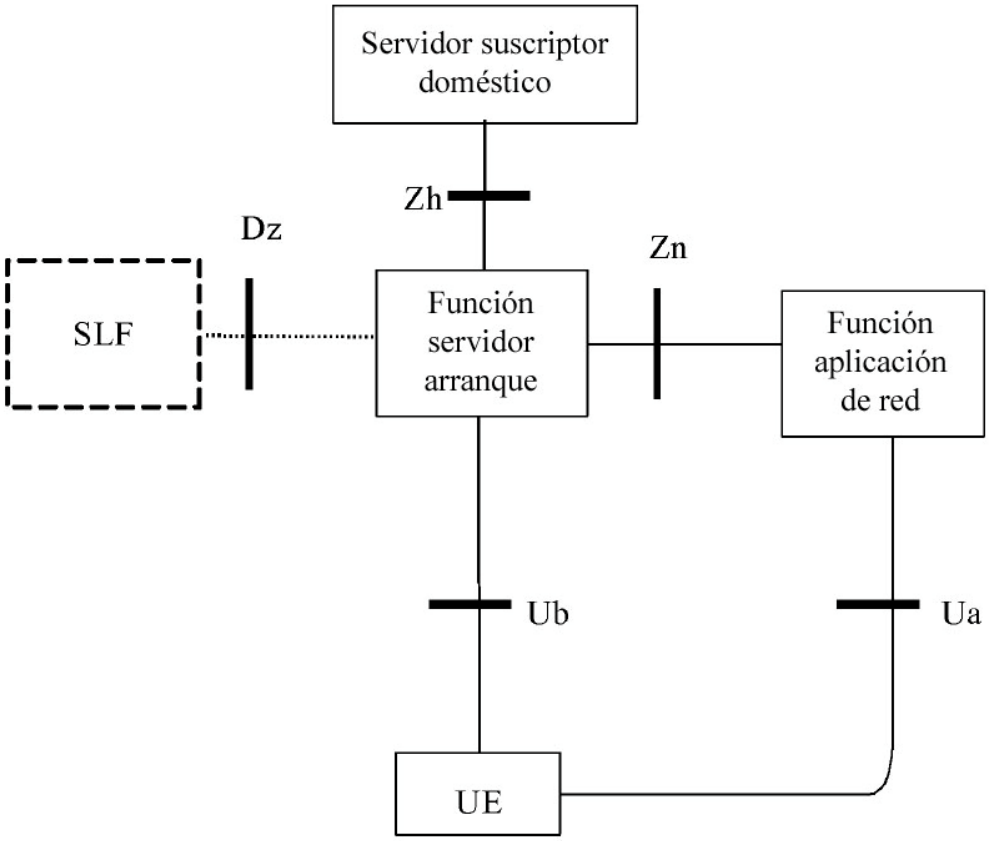
Servidor suscriptor doméstico
Zh
Dz
Zn
SLF
Función servidor arranque
Función aplicación de red
Ub
Ua
UE

Figura 1

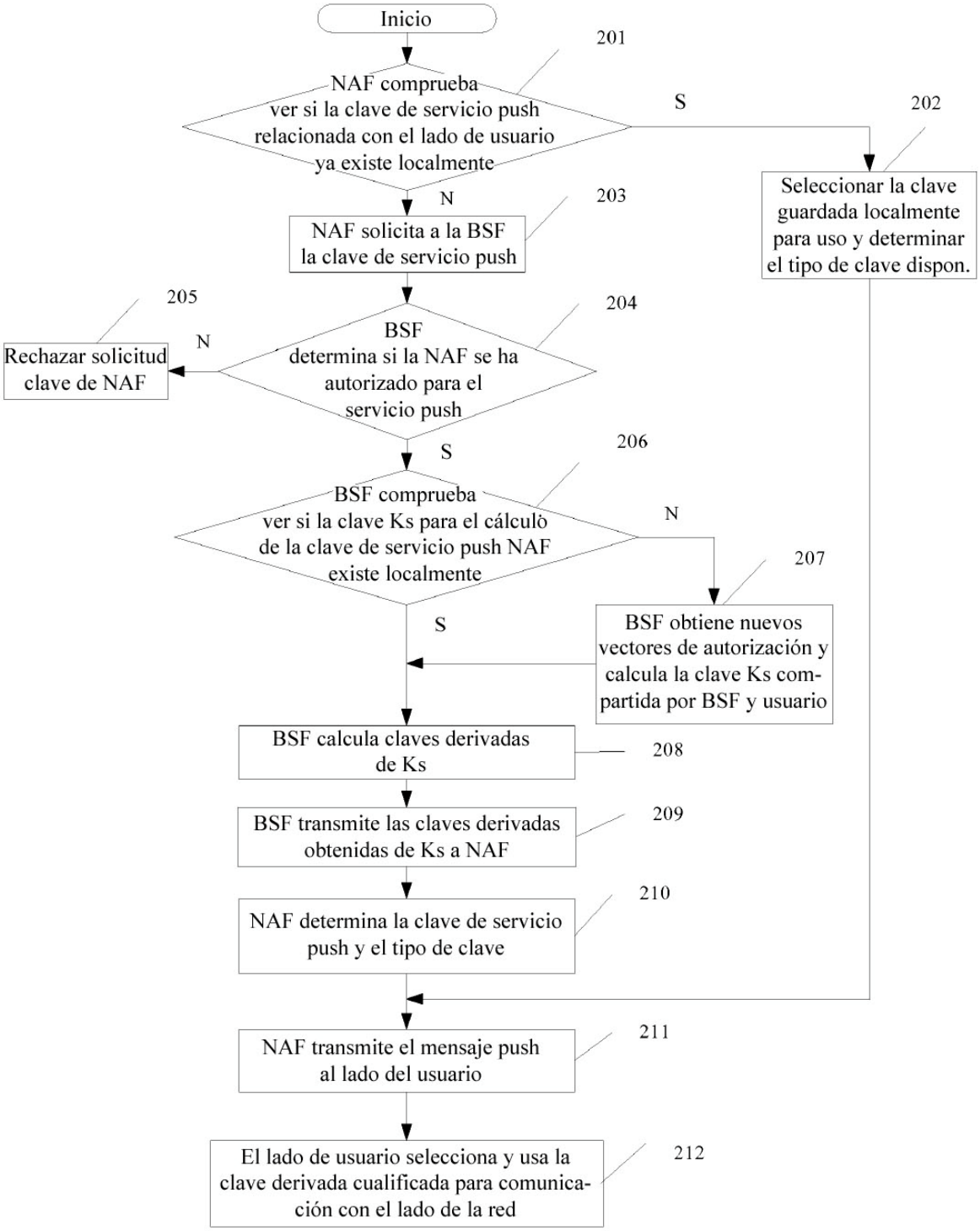
Inicio
201
NAF comprueba ver si la clave de servicio push relacionada con el lado de usuario ya existe localmente
S
202
Seleccionar la clave guardada localmente para uso y determinar el tipo de clave dispon.
N
203
NAF solicita a la BSF la clave de servicio push
205
204
Rechazar solicitud clave de NAF
N
BSF determina si la NAF se ha autorizado para el servicio push
S
206
BSF comprueba ver si la clave Ks para el cálculo de la clave de servicio push NAF existe localmente
N
207
S
BSF obtiene nuevos vectores de autorización y calcula la clave Ks compartida por BSF y usuario
BSF calcula claves derivadas de Ks
208
BSF transmite las claves derivadas obtenidas de Ks a NAF
209
NAF determina la clave de servicio push y el tipo de clave
210
NAF transmite el mensaje push al lado del usuario
211
El lado de usuario selecciona y usa la clave derivada cualificada para comunicación con el lado de la red
212

Figura 2

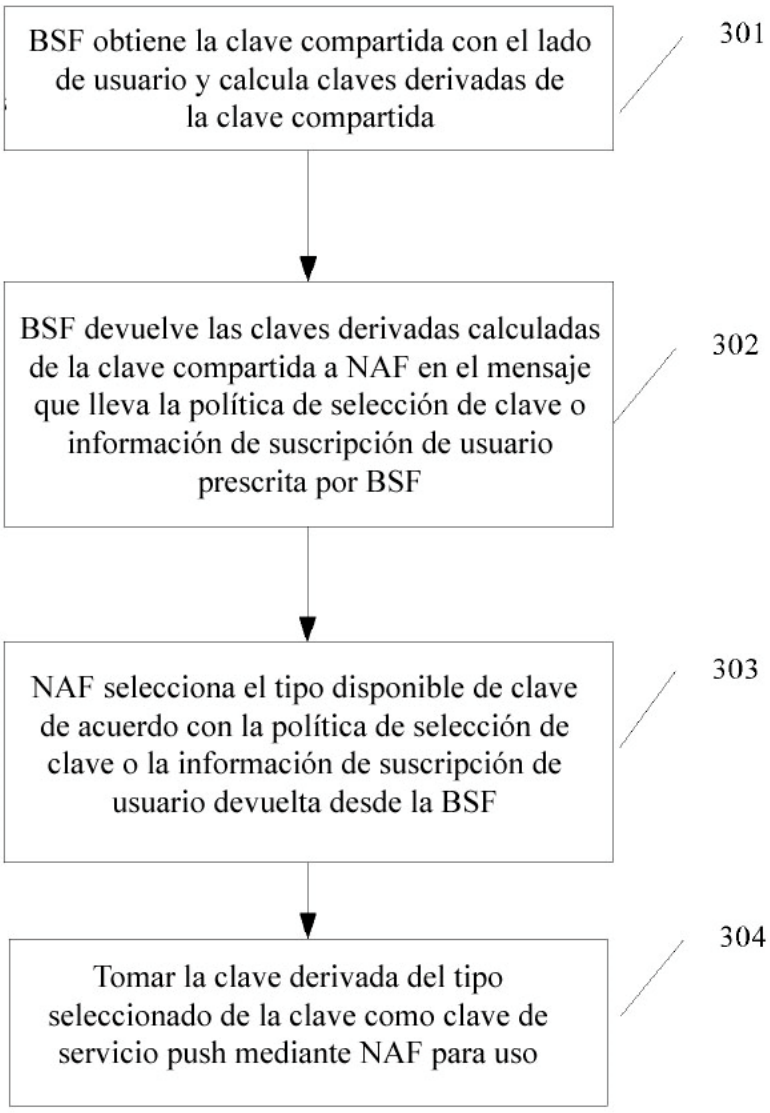
BSF obtiene la clave compartida con el lado de usuario y calcula claves derivadas de la clave compartida
301
BSF devuelve las claves derivadas calculadas de la clave compartida a NAF en el mensaje que lleva la política de selección de clave o información de suscripción de usuario prescrita por BSF
302
NAF selecciona el tipo disponible de clave de acuerdo con la política de selección de clave o la información de suscripción de usuario devuelta desde la BSF
303
Tomar la clave derivada del tipo seleccionado de la clave como clave de servicio push mediante NAF para uso
304

Figura 3

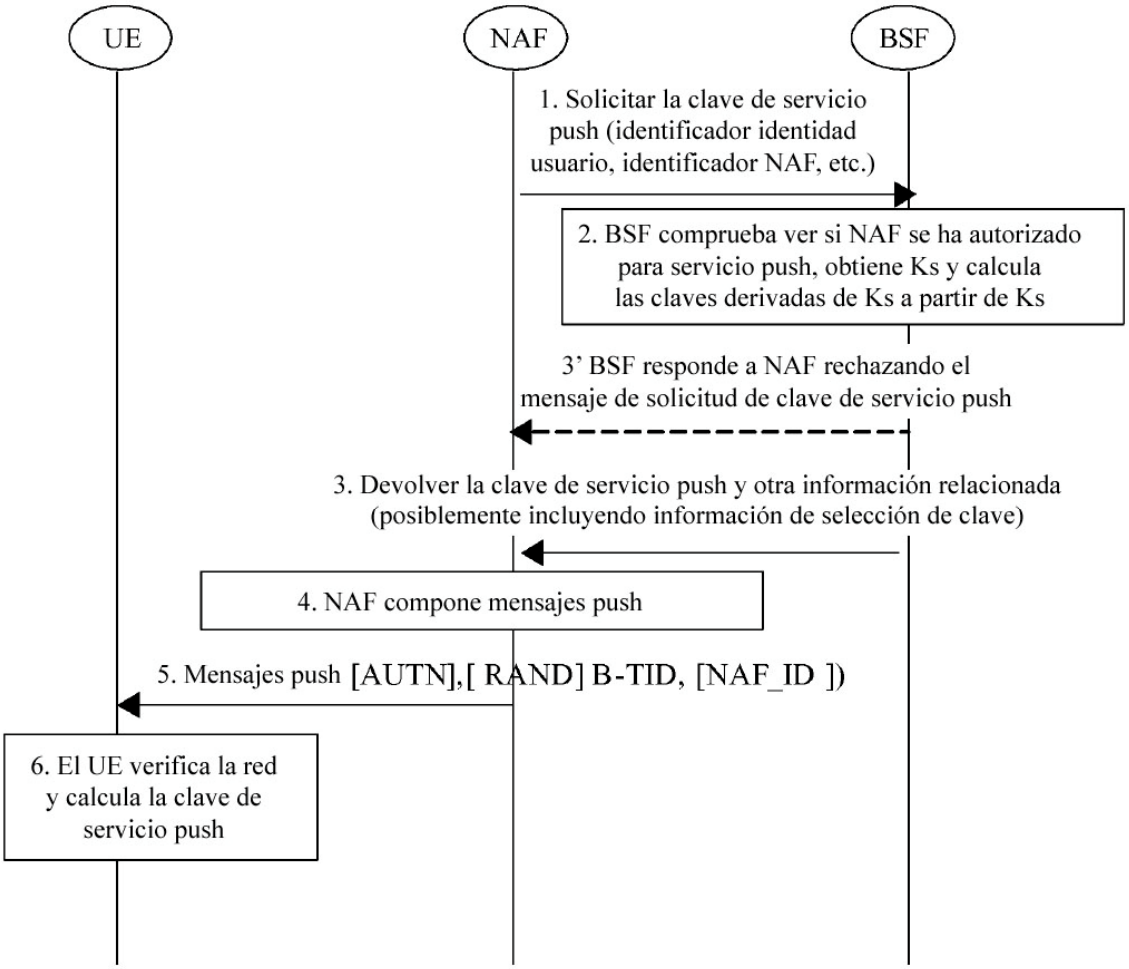
UE
NAF
BSF
1. Solicitar la clave de servicio push (identificador identidad usuario, identificador NAF, etc.)
2. BSF comprueba ver si NAF se ha autorizado para servicio push, obtiene Ks y calcula las claves derivadas de Ks a partir de Ks
3' BSF responde a NAF rechazando el mensaje de solicitud de clave de servicio push
3. Devolver la clave de servicio push y otra información relacionada (posiblemente incluyendo información de selección de clave)
4. NAF compone mensajes push
5. Mensajes push [AUTN],[RAND] B-TID, [NAF_ID])
6. El UE verifica la red y calcula la clave de servicio push

Figura 4

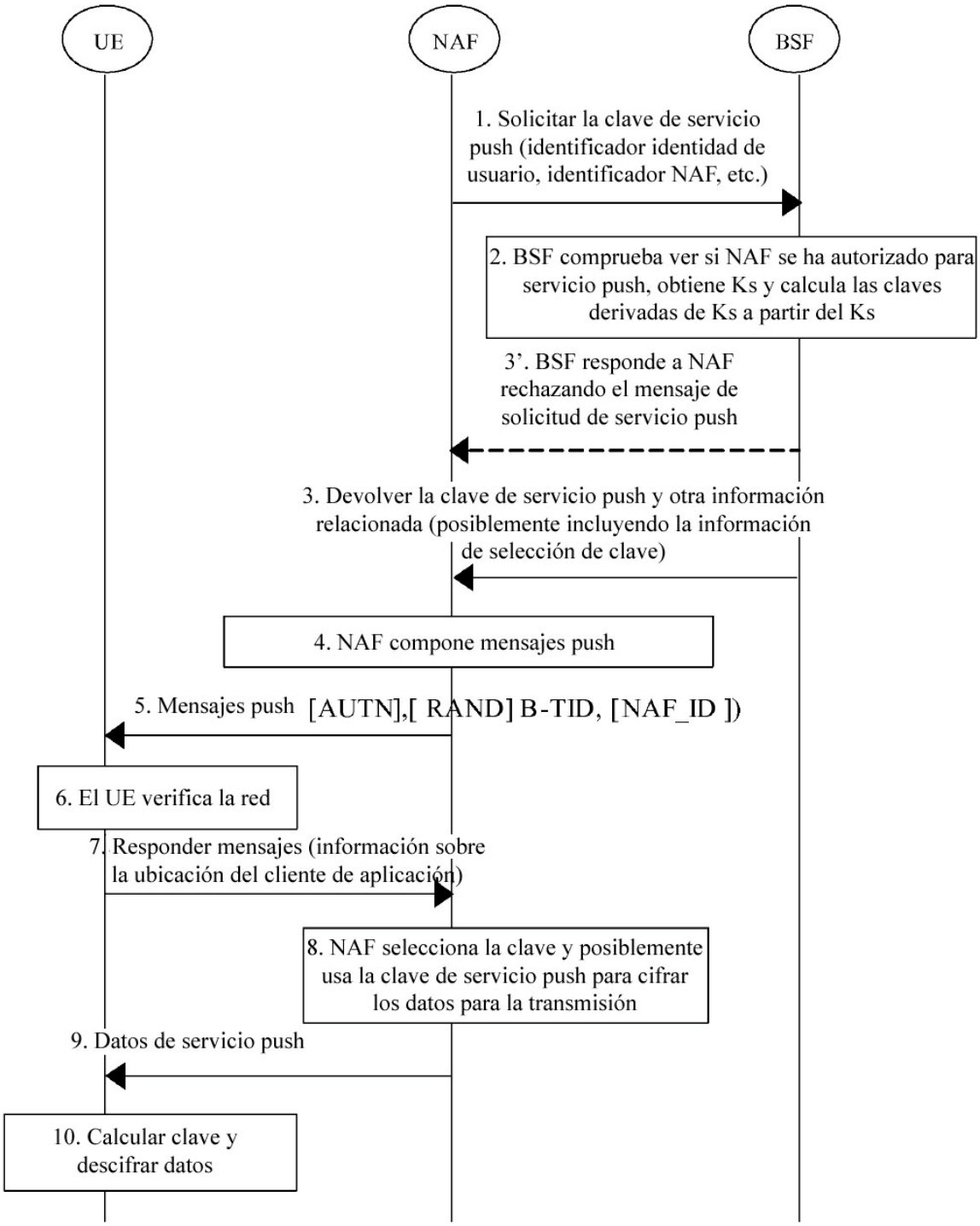
UE
NAF
BSF
1. Solicitar la clave de servicio push (identificador identidad de usuario, identificador NAF, etc.)
2. BSF comprueba ver si NAF se ha autorizado para servicio push, obtiene Ks y calcula las claves derivadas de Ks a partir del Ks
3'. BSF responde a NAF rechazando el mensaje de solicitud de servicio push
3. Devolver la clave de servicio push y otra información relacionada (posiblemente incluyendo la información de selección de clave)
4. NAF compone mensajes push
5. Mensajes push [AUTN],[RAND] B-TID, [NAF_ID])
6. El UE verifica la red
7. Responder mensajes (información sobre la ubicación del cliente de aplicación)
8. NAF selecciona la clave y posiblemente usa la clave de servicio push para cifrar los datos para la transmisión
9. Datos de servicio push
10. Calcular clave y descifrar datos

Figura 5

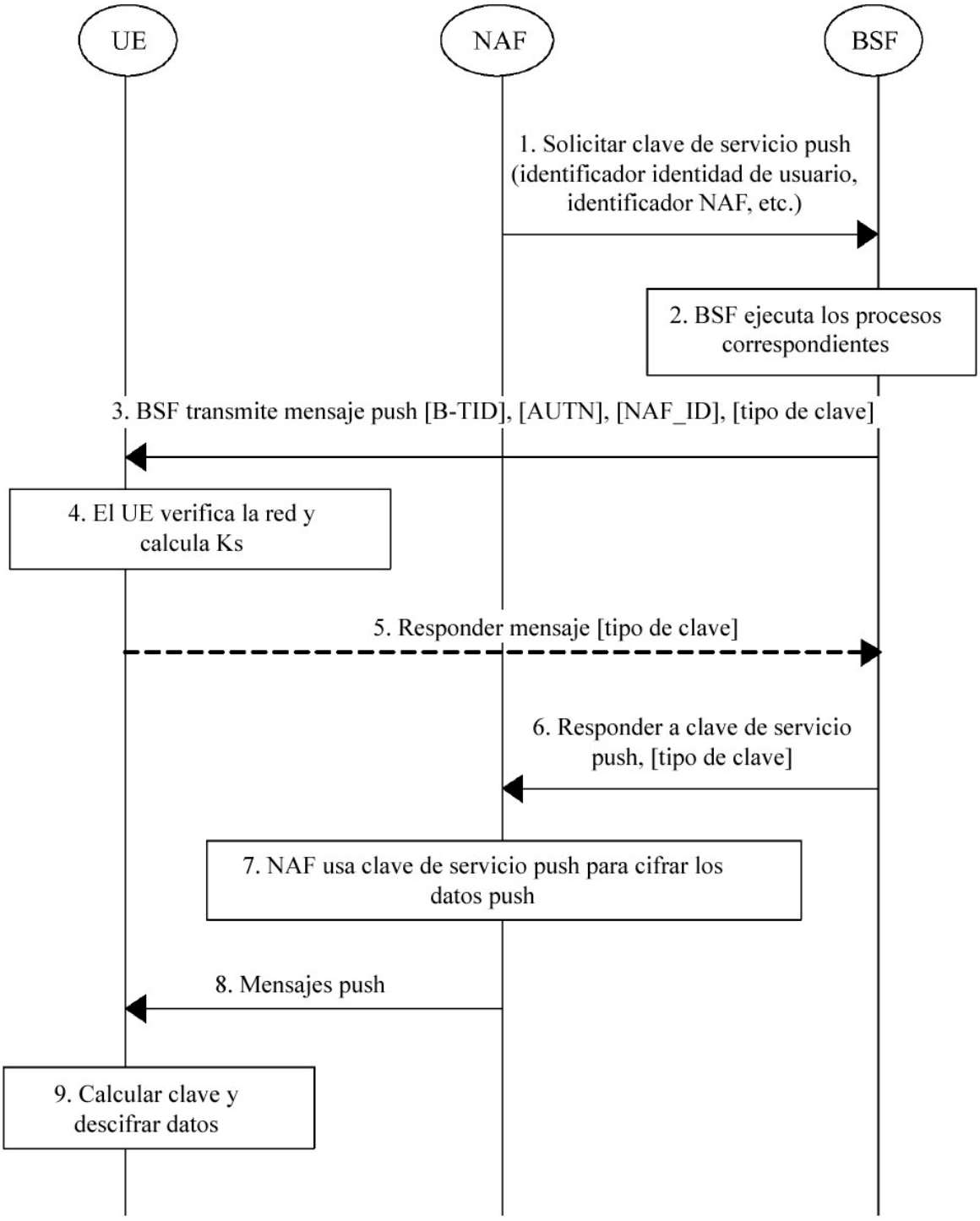
UE
NAF
BSF
1. Solicitar clave de servicio push (identificador identidad de usuario, identificador NAF, etc.)
2. BSF ejecuta los procesos correspondientes
3. BSF transmite mensaje push [B-TID], [AUTN], [NAF_ID], [tipo de clave]
4. El UE verifica la red y calcula Ks
5. Responder mensaje [tipo de clave]
6. Responder a clave de servicio push, [tipo de clave]
7. NAF usa clave de servicio push para cifrar los datos push
8. Mensajes push
9. Calcular clave y descifrar datos

Figura 6