(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 640 471**

(51) Int. CI.:

H04L 9/08 (2006.01)
H04L 29/06 (2006.01)
H04W 12/06 (2009.01)
H04W 12/12 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **25.10.2004 PCT/CN2004/001209**

(87) Fecha y número de publicación internacional: **19.05.2005 WO05046118**

(96) Fecha de presentación y número de la solicitud europea: **25.10.2004 E 04789868 (9)**

(97) Fecha y número de publicación de la concesión europea: **21.06.2017 EP 1681793**

(54) Título: **Un procedimiento para verificar la validez del abonado**

(30) Prioridad:

07.11.2003 CN 200310113230

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
03.11.2017

(73) Titular/es:

SNAPTRACK, INC. (100.0%)
5775 Morehouse Drive
San Diego, CA 92121, US

(72) Inventor/es:

HUANG, YINGXIN

(74) Agente/Representante:

FORTEA LAGUNA, Juan José

DESCRIPCIÓN

Un procedimiento para verificar la validez del abonado

Campo de la invención

La presente invención se refiere a la tecnología de comunicación inalámbrica de tercera generación (3G) y, más específicamente, a un procedimiento para verificar la validez de un usuario.

Antecedentes de la invención

En las normas de comunicación inalámbrica 3G, la arquitectura de autenticación genérica describe una arquitectura genérica adoptada por varias funciones de aplicación de red (NAF) para verificar la validez de los usuarios. Mediante una arquitectura de autenticación genérica, es posible implementar la autenticación y la verificación de un usuario que pida un servicio. Las diversas funciones de aplicación anteriores pueden incluir servicio de difusión/multidifusión, servicio de certificados de abonados y servicio de suministro de mensajes instantáneos, así como servicio proxy, por ejemplo, múltiples entidades de funciones de servicios pueden conectarse con una entidad proxy. La arquitectura de autenticación genérica maneja el proxy como un tipo de servicio donde la construcción puede ser muy flexible. Además, la arquitectura de autenticación genérica puede adoptarse para la autenticación y la verificación de usuarios que pidan servicios recién desarrollados.

La Figura 1 es un diagrama de estructura esquemático de la arquitectura de autenticación genérica. Típicamente, la arquitectura de autenticación genérica incluye un equipo de usuario (UE) 101, una función de servidor de arranque (BSF) 102, un sistema de abonado doméstico (HSS) 103 y una NAF 104. La BSF 102 se usa para la autenticación mutua con el UE 101 y para generar de forma simultánea una clave secreta compartida con el UE 101. Un documento de perfil usado para describir la información de abonado se almacena en el HSS 103 que generará información de autenticación.

Cuando un UE pida un servicio, si el UE sabe que el servicio requiere un procedimiento de autenticación mutua en la BSF, el UE realizará una autenticación mutua en la BSF directamente. De lo contrario, el UE contactará primero con la NAF correspondiente al servicio. Si la NAF que aplica la arquitectura de autenticación genérica requiere que el UE realice una autenticación de arranque en la BSF, la NAF indicará al UE que realice una autenticación de arranque mediante la arquitectura de autenticación genérica. De lo contrario, la NAF ejecuta otro procesamiento apropiado.

La Figura 2 es un diagrama de flujo para la autenticación por la arquitectura de autenticación genérica en la técnica anterior.

Etapa 201: Un UE envía a una NAF un mensaje de petición de aplicación.

Etapa 202: Tras recibir el mensaje, la NAF detecta que el UE no ha realizado una autenticación mutua en una BSF, entonces indica al UE que realice una autenticación de arranque en la BSF.

Etapa 203: El UE envía al BSF un mensaje de petición de arranque.

Etapa 204: Tras recibir el mensaje de petición de arranque del UE, la BSF lleva a cabo la consulta de la información de autenticación necesaria del UE y el documento de perfil del mismo al HSS y recibe una respuesta del HSS.

Etapa 205: Tras recibir el mensaje de respuesta del HSS que contiene la información consultada, la BSF realiza una autenticación mutua basada en el protocolo de acuerdo de clave y autenticación (AKA) con el UE que use la información consultada. Cuando se complete la autenticación mutua basada en el protocolo AKA con el UE, es decir, pasando la autenticación mutua, la BSF genera una clave secreta compartida con el UE (K).

Etapa 206: La BSF asigna al UE un identificador de transacción (TID) que incluye solamente la identidad y es válido para una o más de una NAF. El TID está asociado con las K.

Etapa 207: Tras recibir el TID asignado por la BSF, el UE reenvía a la NAF un mensaje de petición de aplicación que contiene la información del TID.

Etapa 208: Tras recibir el mensaje de petición de aplicación que contiene la información del TID enviado desde el UE, la NAF llevará a cabo primero una consulta local: si la NAF detecta la información del TID localmente, procede directamente a la etapa 210. De lo contrario, envía a la BSF un mensaje de consulta TID que contiene la identidad local de la NAF y luego procede a la etapa 209.

Etapa 209: Tras recibir el mensaje de consulta TID de la NAF, la BSF, si detecta el TID consultado por la NAF, envía a la NAF un mensaje de respuesta de éxito. La NAF almacena el contenido del mensaje de respuesta y procede a la Etapa 210. De lo contrario, la BSF enviará a la NAF un mensaje de respuesta de fallo, notificando a la NAF que no

hay información del UE. La NAF indicará al UE que realice una autenticación en la BSF y finalice el procedimiento.

El mensaje de respuesta de éxito incluye el TID detectado, las K correspondientes al TID o una clave secreta derivada generada a partir de las K de acuerdo con el nivel de seguridad de la NAF. Siempre que se reciba un mensaje de respuesta de éxito de la BSF, la NAF creerá que el UE es un UE legítimo que pasa la autenticación por la BSF y comparte las K o la clave secreta derivada con el UE.

Etapa 210: La NAF hace comunicaciones normales con el UE, es decir, la transmisión de datos, y protege otras comunicaciones usando las K o la clave secreta derivada.

Después de finalizar el primer proceso de comunicación entre el UE y la NAF, el TID autenticado se usa para comunicaciones adicionales entre el UE y la NAF. Puesto que el TID puede usarse de forma repetida y cualquier NAF puede consultar el TID correspondiente de la BSF si no puede encontrar el TID localmente, siempre que obtenga un TID legítimo, el UE puede hacer comunicaciones con la NAF usando el TID durante un período indefinido.

"Handbook of Applied Cryptography" (Menezes, Oorschot, Vanstone, 1997) divulga problemas clave del ciclo de elevación. Los controles son necesarios para proteger las claves durante el uso y el almacenamiento. En cuanto al almacenamiento a largo plazo de claves, la duración de la protección requerida depende de la función criptográfica (por ejemplo, cifrado, firma, autenticación/integridad del origen de datos) y la sensibilidad temporal de los datos en cuestión. Excepto en sistemas simples donde las claves secretas permanecen fijas durante todo el tiempo, los criptoperiodos asociados con las claves requieren que las claves se actualicen de forma periódica.

El proyecto de asociación de 3ª generación "3GPP TS ab.cde V0.3.0:3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Bootstrapper of application security using AKA and Support for Subscriber Certificates; System Description" (3GPP TSG SA WG3 Security-S3 # 30, octubre de 2003) divulga las características de seguridad y un mecanismo para arrancar la autenticación y el acuerdo clave para la seguridad de las aplicaciones del mecanismo AKA 3GPP. Las aplicaciones candidatas para usar este mecanismo de arranque incluyen pero no están restringidas a la distribución de certificados de abonado, etc. El abonado certifica los servicios a cuya provisión asiste el operador móvil, así como servicios que proporciona operador móvil.

Puede verse a partir de la solución anterior que el TID asignado por la BSF para un UE es solamente un puente para establecer la confianza entre una NAF y el UE y, generalmente, existe solamente la información de identidad en un TID, es decir, no existe ninguna definición sobre cómo construir un TID y con qué información debe asociarse el TID. Mientras tanto, es poco probable que la NAF gestione el TID. Además, una vez que un UE obtiene un TID legítimo, el UE puede realizar comunicaciones con la NAF usando el TID durante un período indefinido, lo que perjudica la seguridad del sistema y aumenta la posibilidad de que se robe una clave secreta del UE.

Sumario de la invención

La presente invención proporciona un procedimiento para verificar la validez de un usuario por medio de la verificación de si es válido un TID de un usuario.

Las soluciones técnicas de acuerdo con los modos de realización de la presente invención se implementan de la manera siguiente:

De acuerdo con un aspecto de la presente invención, cuando una NAF recibe un mensaje de petición de aplicación que contiene información TID, determina si la información TID existe localmente; si existe, determina si caduca el TID. Si el TID no ha caducado, la NAF hará comunicaciones normales con el UE. Si el TID ha caducado, la NAF indicará al UE que realice una autenticación de arranque en una BSF de nuevo.

Si no hay ninguna información TID en la NAF, la NAF enviará a la BSF un mensaje de consulta TID que contenga la identidad de la NAF. Si la BSF detecta el TID consultado por la NAF, devolverá a la NAF un mensaje de respuesta de éxito que contenga el TID encontrado y el plazo de validez del TID; la NAF almacena primero el contenido en el mensaje de respuesta de la BSF y luego hace comunicaciones normales con el UE. Si la BSF no detecta el TID requerido por la NAF, devolverá a la NAF un mensaje de respuesta de fallo y la NAF indicará al UE que realice una autenticación de arranque en la BSF.

Puede observarse a partir del sistema mencionado anteriormente que la presente invención aprovecha plenamente que el TID es un puente para establecer la relación de confianza entre la NAF y el UE, a través de una BSF que asigna un plazo de validez para un TID, extiende las funciones del TID y permite que una NAF verifique el plazo de validez del TID usado por el UE, implementando de este modo una verificación adicional de la validez del UE. Mediante el procedimiento de la presente invención, es posible evitar la situación donde un TID sea válido de forma permanente para una NAF, mejorar la seguridad del sistema, disminuir la posibilidad de que se roben el TID de un UE y su clave secreta correspondiente e implementar la gestión de los TID por una NAF. Además, una combinación del procedimiento con el sistema de facturación facilitará la implementación de la carga de un usuario.

Breve descripción de los dibujos

La Figura 1 es un diagrama de estructura esquemático que ilustra la arquitectura de autenticación genérica.

La Figura 2 es un diagrama de flujo de una autenticación de UE que usa la arquitectura de autenticación genérica en la técnica anterior.

La Figura 3 es un diagrama de flujo que representa la validez de un UE de acuerdo con un modo de realización de la presente invención.

La Figura 4 es un diagrama de flujo de verificación de la validez de un UE de acuerdo con otro modo de realización de la presente invención.

La Figura 5 es un diagrama de flujo de verificación de la validez de un UE de acuerdo con otro modo de realización más de la presente invención.

Descripción detallada de la invención

Con el fin de hacer más evidente la solución técnica de la presente invención, se da una descripción adicional y detallada de la presente invención de aquí en adelante con referencia a los dibujos adjuntos y modos de realización específicos.

De acuerdo con un aspecto de la presente invención, cuando una NAF recibe un mensaje de petición de aplicación que contiene la información de un TID, determina si la información del TID existe localmente; si existe, determina si el UE es legítimo determinando si se supera un término preestablecido de validez para el TID usado por el UE. Si el UE es legítimo, la NAF hará comunicaciones normales con el UE. De lo contrario, la NAF indicará al UE que realice una autenticación de arranque en una BSF de nuevo.

Si no existe ninguna información del TID en la NAF, la NAF enviará a la BSF un mensaje de consulta TID que contenga la identidad de la NAF. Si la BSF detecta el TID consultado por la NAF, devolverá a la NAF un mensaje de respuesta de éxito que contenga el TID detectado y el plazo de validez del TID, la NAF almacena primero el contenido en el mensaje de respuesta de la BSF y luego hace comunicaciones normales con el UE. Si la BSF no logra detectar el TID requerido por la NAF, devolverá a la NAF un mensaje de respuesta de fallo y la NAF indicará al UE que realice una autenticación de arranque en la BSF.

La invención se describe de aquí en adelante con detalle mediante varios modos de realización específicos.

Primer modo de realización:

Una BSF asigna a un UE un TID que es válido para una o más NAF mientras no se cifra el TID.

La Figura 3 es un diagrama de flujo para verificar la validez de un UE de acuerdo con el primer modo de realización de la presente invención.

Etapa 301: Un UE envía un mensaje de petición de aplicación a una NAF.

Etapa 302: Tras recibir el mensaje, la NAF detecta que el UE no ha realizado una autenticación mutua con una BSF e indica luego al UE que realice una autenticación de arranque en la BSF.

Etapa 303: El UE envía al BSF un mensaje de petición de arranque.

Etapa 304: Tras recibir el mensaje de petición de arranque del UE, la BSF lleva a cabo una consulta de la información de autenticación y del perfil del UE hacia un HSS y recibe un mensaje de respuesta del HSS.

Etapa 305: Tras recibir el mensaje de respuesta que contiene la información encontrada enviada desde el HSS, la BSF realiza una autenticación mutua basada en el protocolo AKA con el UE usando la información encontrada. Cuando se completa la autenticación mutua basada en el protocolo AKA con el UE, es decir, pasando la autenticación mutua, la BSF genera una clave secreta compartida con el UE (K).

Etapa 306: la BSF asigna al UE un TID que contiene solamente una identidad y es válido para una o más NAF al mismo tiempo.

Etapa 307: Tras recibir el TID asignado por la BSF, el UE reenvía a la NAF un mensaje de petición de aplicación que contiene la información del TID.

Etapa 308: Tras recibir el mensaje de petición de aplicación que contiene la información del TID enviado desde el UE, la NAF determina si la información del TID existe localmente; si existe, la NAF determina si se superan el tiempo de vida válido o los tiempos válidos de uso para el TID. Si se superan, procede a la Etapa 309. De lo contrario, procede a la Etapa 310.

Si no existe información del TID en la NAF, la NAF enviará a la BSF un mensaje de consulta TID que contiene la identidad de la NAF; si la BSF detecta el TID, la BSF generará primero una clave secreta derivada válida para la NAF de consulta en base a la identidad de usuario, la identidad NAF y la clave secreta de raíz correspondiente al TID y, entonces, asignará, de acuerdo con el nivel de seguridad de la NAF de consulta y la información de perfil del UE, un plazo de validez para la clave secreta derivada generada para el TID consultado, donde el plazo de validez sea un tiempo de vida válido y/o tiempos válidos de uso y sean válidos solamente para la NAF de consulta. A continuación, la BSF envía un mensaje de respuesta de éxito a la NAF y la NAF almacena el contenido del mensaje de respuesta de éxito y procede a la etapa 310. Si la BSF no logra detectar el TID, la BSF enviará a la NAF un mensaje de respuesta de fallo y procederá a la Etapa 309.

El mensaje de respuesta de éxito mencionado anteriormente incluye el TID consultado por la NAF, correspondiendo la clave secreta derivada al TID y generada para la NAF de consulta, así como el plazo de validez de la clave secreta derivada. La clave secreta derivada para la NAF de consulta se ha generado cuando el UE envía la petición de aplicación a la NAF usando el TID asignado por la BSF. Cuando la NAF recibe el mensaje de respuesta de éxito desde la BSF, la NAF comienza a compartir la clave secreta derivada generada para la NAF de consulta con el UE.

Etapa 309: la NAF indica al UE que realice una autenticación de arranque en la BSF y finaliza este procedimiento.

Etapa 310: la NAF hace comunicaciones normales con el UE, es decir, transmisión de datos, y protege otras comunicaciones usando la clave secreta derivada de las K.

Aunque el TID usado por un UE es válido para una o más NAF al mismo tiempo, son diferentes las claves secretas derivadas para NAF diferentes así como los plazos de validez de las mismas asignados por la BSF, es decir, el mismo TID, cuando se usa para NAF diferentes, corresponde a claves secretas derivadas diferentes y a plazos de validez diferentes de las mismas. Sin embargo, en términos de una NAF, son únicos el TID del UE y la clave secreta derivada correspondiente del mismo.

Cuando caducan el TID usado por el UE y la clave secreta correspondiente para una NAF determinada, el UE realizará de nuevo una autenticación de arranque en la BSF. Después de que la autenticación tenga éxito, la BSF asignará al UE un nuevo TID y generará una nueva clave secreta compartida (K) correspondiente al nuevo TID. Tras recibir el nuevo TID, el UE enviará un nuevo mensaje de petición de aplicación usando el nuevo TID mientras que el nuevo mensaje de petición contiene también la información del TID antiguo. Por lo tanto, no se verán afectadas la NAF que usa el TID antiguo y la clave secreta derivada del mismo y no se usará un TID nuevo a menos que el UE envíe una petición de aplicación de nuevo o la NAF requiera que el UE actualice el TID, evitando de este modo el impacto por la NAF que pida actualizar el TID en otras NAF que usen actualmente el TID.

Cuando una NAF reciba un nuevo TID, la NAF llevará a cabo siempre la consulta del TID en la BSF; si la consulta tiene éxito, la BSF devolverá a la NAF un mensaje de respuesta de éxito que incluya también el TID consultado por la NAF, la clave secreta derivada para el TID en base a dichos parámetros como la identidad de la NAF de consulta y la clave secreta de raíz y el plazo de validez correspondiente a la clave secreta derivada. Tras recibir el mensaje de respuesta de éxito de la BSF, la NAF almacenará el nuevo TID en el mensaje de respuesta de éxito, la clave secreta derivada correspondiente al TID y el plazo de validez del mismo. Al mismo tiempo, la NAF desactivará o borrará el TID antiguo almacenado en ella y la clave secreta correspondiente al TID antiguo.

Puesto que el TID antiguo usado por un UE corresponde a múltiples NAF al mismo tiempo, cuando el TID caduque para una NAF determinada, es muy posible que el TID siga siendo válido para otras NAF. Puesto que cada NAF que reciba un nuevo TID llevará a cabo una consulta en la BSF, en aras de la seguridad del sistema, cada NAF que reciba un nuevo TID reemplazará el TID antiguo y la información relativa del mismo con el nuevo TID del UE y la información relativa del mismo. De esta forma, no solamente la gestión TID se vuelve menos compleja, sino que se mejora la seguridad del TID y las claves secretas correspondientes.

En la Etapa 306 de este modo de realización, la BSF puede asignar al UE un TID válido solamente para una NAF determinada e incluyendo solamente una identidad. Por consiguiente, en la etapa 308, tras recibir del UE un mensaje de petición de aplicación que contenga la información del TID, la NAF determina primero si el TID es válido para la NAF: si no es válido, la NAF solicitará al UE un mensaje de error; si es válido, continúa con las etapas posteriores. Las demás etapas del procedimiento son las mismas que las mostradas en la Figura 3 y no se da más descripción por la presente.

El procedimiento para asignar a un UE un TID válido solamente para una NAF determinada y el procedimiento para determinar si el TID es válido para la NAF se han descrito con detalle en la solicitud de patente presentada por este inventor y titulada "procedimiento para asignar identidades de transacción" con el número de solicitud

"200310113233.4" y no se da más descripción por la presente.

En este modo de realización, el plazo de validez de la clave secreta correspondiente a un TID es en realidad el plazo de validez del TID, porque el TID está asociado con la clave secreta correspondiente al TID. Si caduca una clave secreta correspondiente a un TID, significa que caduca el plazo de validez del TID para una NAF.

Segundo modo de realización

Una BSF asigna a un UE un TID válido para solamente una NAF determinada y se cifra el TID.

La Figura 4 es un diagrama de flujo que verifica la validez de un UE de acuerdo con un segundo modo de realización de la presente invención.

Etapa 401: Un UE envía un mensaje de petición de aplicación a una NAF.

Etapa 402: Tras recibir el mensaje, la NAF detecta que el UE no ha realizado una autenticación mutua con la BSF, por lo tanto indica al UE que realice una autenticación de arranque en la BSF.

Etapa 403: El UE envía al BSF un mensaje de petición de arranque.

Etapa 404: Tras recibir del UE el mensaje de petición de arranque, la BSF lleva a cabo una consulta de la información de autenticación y del perfil del UE a un HSS y recibe un mensaje de respuesta del HSS.

Etapa 405: Tras recibir el mensaje de respuesta que contiene la información encontrada enviada desde el HSS, la BSF realiza una autenticación mutua basada en el protocolo AKA con el UE usando la información detectada. Al completar la autenticación mutua basada en el AKA con el UE, es decir, pasando la autenticación mutua, la BSF genera una clave secreta con el UE (K).

Etapa 406: la BSF asigna al UE una identidad válida solamente para una NAF determinada y luego, en base a la identidad o nombre de la NAF y a la información de perfil del UE, asigna un plazo de validez para la identidad del UE, donde el plazo de validez es un tiempo de vida válido y/o tiempos de uso válidos. La BSF cifra la identidad válida para la NAF y el plazo de validez de la identidad usando la clave secreta preestablecida compartida entre la BSF y la NAF (Knb), toma la información cifrada como un TID y envía el TID al UE. Puesto que el UE no tiene Knb, el UE no puede modificar el plazo de validez del TID.

Etapa 407: Tras recibir el TID asignado por la BSF, el UE envía a la NAF un mensaje de petición de aplicación que contiene el TID cifrado.

Etapa 408: Tras recibir el mensaje de petición de aplicación que contiene la información del TID enviada desde el UE, la NAF determina primero si la información del TID existe localmente; si existe, la NAF descifra el TID usando Knb y determina si se superan el tiempo de vida válido o los tiempos de uso válidos; si se superan, procede a la Etapa 409. De lo contrario, procede a la Etapa 410.

Si no existe información del TID en la NAF, la NAF descifrará primero el TID usando Knb y luego determinará si el TID es válido para la NAF, donde el procedimiento específico para realizar la determinación se ha descrito con detalle en la solicitud de patente presentada por este inventor y titulada "procedimiento para asignar identidades de transacción" con el número de solicitud "200310114069.9". Si el TID es válido para la NAF, la NAF enviará a la BSF un mensaje de consulta TID que contenga la identidad de la NAF. De lo contrario, la NAF solicitará al UE un mensaje de error.

Si la BSF detecta la información del TID, enviará a la NAF un mensaje de respuesta de éxito que contenga el TID consultado por la NAF y K, la clave secreta compartida entre el UE y la BSF y correspondiente al TID o una clave secreta generada a partir de K, es decir, la clave secreta derivada generada para la NAF de consulta. Tras recibir el mensaje de respuesta de éxito de la BSF, la NAF comienza a compartir con el UE la clave secreta derivada generada para la NAF de consulta. La clave secreta derivada correspondiente a la NAF de consulta se ha generado por el UE cuando el UE envió la petición de aplicación a la NAF usando el TID asignado por la BSF. Después de que la NAF almacena el contenido en el mensaje de respuesta de éxito de la BSF, procede a la etapa 410. Si la BSF no logra detectar la información, enviará un mensaje de respuesta de fallo a la NAF y procederá a la Etapa 409.

Etapa 409: la NAF indica al UE que realice una autenticación de arranque en la BSF y finaliza el procedimiento.

Etapa 410: la NAF hace comunicaciones normales con el UE, es decir, transmisión de datos, y protege las comunicaciones adicionales usando la K o la clave secreta derivada de K.

Cuando el TID usado por el UE ha caducado para una NAF determinada, el UE realizará la autenticación mutua en la BSF de nuevo. Después de que la autenticación tenga éxito, la BSF asignará al UE un nuevo TID y generará una

nueva clave secreta compartida, K, correspondiente al nuevo TID, donde el nuevo TID se cifra también. Cuando el UE envía una petición de aplicación a la NAF de nuevo, el mensaje de petición contiene la información tanto del nuevo TID como del TID antiguo.

Cuando una NAF reciba un nuevo TID, la NAF realizará siempre la consulta del TID en la BSF. Si la consulta tiene éxito, la BSF devolverá a la NAF un mensaje de respuesta de éxito que contenga también el TID consultado por la NAF y K o la clave secreta derivada generada a partir de K. Tras recibir el mensaje de respuesta de éxito de la BSF, la NAF comienza a compartir K o la clave secreta derivada a partir de K con el UE. El NAF almacenará el nuevo TID y las K y desactivará o borrará el TID antiguo almacenado localmente y las K.

Tercer modo de realización

La BSF asigna a un UE un TID válido solamente para una NAF determinada y no cifra el TID.

La Figura 5 es un diagrama de flujo que representa la validez de un UE de acuerdo con el tercer modo de realización de la presente invención.

Etapa 501: Un UE envía un mensaje de petición de aplicación a una NAF.

Etapa 502: Tras recibir el mensaje, la NAF detecta que el UE no ha realizado una autenticación mutua con la BSF, por lo tanto indica al UE que realice una autenticación de arranque en la BSF.

Etapa 503: El UE envía al BSF un mensaje de petición de arranque.

Etapa 504: Tras recibir el mensaje de petición de arranque del UE, la BSF lleva a cabo una consulta de la información de autenticación y el perfil del UE hacia un HSS y recibe un mensaje de respuesta del HSS.

Etapa 505: Tras recibir el mensaje de respuesta que contiene la información detectada enviada desde el HSS, la BSF realiza una autenticación mutua basada en el protocolo AKA con el UE usando la información encontrada. Al completar la autenticación mutua basada en la AKA con el UE, es decir, pasando la autenticación mutua, la BSF genera una clave secreta compartida con el UE (K).

Etapa 506: la BSF asigna al UE una identidad válida solamente para una NAF determinada y toma la identidad de un TID. Luego, en base a la identidad o al nombre de la NAF y a la información de perfil del UE, la BSF asigna y almacena un plazo de validez para el TID del UE, donde el plazo de validez es un tiempo de vida válido y/o tiempos de uso válidos y envía el TID asignado al UE.

Etapa 507: Tras recibir el TID asignado por la BSF, el UE envía a la NAF un mensaje de petición de aplicación que contiene la información del TID de nuevo.

Etapa 508: Tras recibir el mensaje de petición de aplicación que contiene la información del TID enviada desde el UE, la NAF determina primero si el TID es válido para la NAF: si no es válido, la NAF solicitará al UE un mensaje de error; si es válido, la NAF determinará además si la información del TID existe localmente. Si existe la información del TID, la NAF determina si el tiempo de vida válido o los tiempos de uso válidos se superan; si se superan, procede a la Etapa 509. De lo contrario, procede a la Etapa 510.

Si no existe información del TID en la NAF, la NAF enviará a la BSF un mensaje de consulta TID que contenga la identidad de la NAF local. Si la BSF encuentra el TID, enviará a la NAF un mensaje de respuesta de éxito que contenga el TID consultado por la NAF, el plazo de validez correspondiente al TID y K, la clave secreta del TID compartida entre el UE y el BSF o la clave secreta derivada generada a partir de K, es decir, la clave secreta derivada generada para la NAF de consulta. Tras recibir el mensaje de respuesta de éxito de la BSF, la NAF comienza a compartir con el UE la clave secreta derivada generada de acuerdo con la NAF de consulta, que se ha generado por el UE cuando el UE envió la petición de aplicación a la NAF usando el TID asignado por la BSF. Después de que la NAF almacena el contenido en el mensaje de respuesta de éxito de la BSF, procede a la etapa 510. Si la BSF no logra detectar la información, enviará un mensaje de respuesta de fallo a la NAF, informa a la NAF de que no existe información del UE y procede a la Etapa 509.

Etapa 509: la NAF indica al UE que realice una autenticación de arranque en la BSF y finaliza este procedimiento.

Etapa 510: la NAF hace comunicaciones normales con el UE, es decir, transmisión de datos, y protege otras comunicaciones usando las K o la clave secreta derivada a partir de las K.

Cuando el TID usado por un UE ha caducado para una NAF determinada, el UE realizará una autenticación de arranque en la BSF de nuevo. Después de que la autenticación tenga éxito, la BSF asignará al UE un nuevo TID y generará una nueva clave secreta compartida, K, correspondiente al nuevo TID. Cuando el UE envíe una petición de aplicación de nuevo a la NAF, el mensaje de petición contendrá la información tanto del nuevo TID como del TID

antiguo.

Cuando una NAF reciba un nuevo TID, la NAF llevará a cabo la consulta del nuevo TID en la BSF. Si la consulta tiene éxito, la BSF devolverá a la NAF un mensaje de respuesta de éxito que contenga el TID consultado por la NAF, el plazo de validez correspondiente al TID y las K o la clave secreta derivada generada a partir de las K. Tras recibir el mensaje de respuesta de éxito de la BSF, la NAF comienza a compartir K o la clave secreta derivada a partir de K con el UE. El NAF almacenará el nuevo TID y la clave secreta asociada con el TID y desactivará o borrará el TID antiguo almacenado localmente y la clave secreta asociada con el TID antiguo.

En el tercer modo de realización, cuando se asigne un TID para un UE, la BSF puede no asignar el plazo de validez correspondiente al TID al principio. En cambio, la BSF puede asignar un plazo de validez correspondiente al TID de acuerdo con la identidad de la NAF y la información de perfil del UE cuando la NAF lleve a cabo la investigación del TID en la BSF.

El plazo de validez del TID puede usarse en la facturación. Si la facturación se basa en el tiempo, un TID puede tomarse como una unidad de tiempo y la carga de un día de uso puede hacerse siempre que se asigne un TID nuevo. Si la facturación se basa en los tiempos de uso, un TID puede cargarse de acuerdo con los tiempos de uso que se asignen. La operación de facturación puede implementarse cuando una BSF asigne un TID o se implemente cuando una NAF use un TID.

REIVINDICACIONES

1. Un procedimiento para verificar la validez de un usuario, aplicado a la tecnología de comunicación inalámbrica de 3ª generación, en el cual una función de aplicación de red (104), NAF, verifica la validez de un usuario mediante una arquitectura de autenticación, comprendiendo el procedimiento:

recibir de un equipo de usuario (101), UE, un mensaje de petición de aplicación que contenga un identificador de transacción, TID;

verificar si hay información TID almacenada en la NAF (104);

si se detecta la información TID, determinar si ha caducado el TID en base a un plazo de validez preestablecido para el TID,
si ha caducado el TID, indicar al UE (101) que se conecte a una función de servidor de arranque (102) BSF, para realizar una autenticación de arranque;

si no se detecta la información TID, la NAF (104) envía, al BSF (102), un mensaje de consulta TID que contiene una identidad de la NAF (104);

si se detecta el TID consultado por la NAF (104), la BSF (102) devuelve, a la NAF (104) un mensaje de respuesta de éxito que contiene la información del TID y el plazo de validez del TID en donde dicho plazo de validez se determina por la BSF (102) en base a la identidad o nombre de la NAF (104) y a la información de perfil del UE (101), y el procedimiento comprende además:

almacenar la información TID y el plazo de validez del TID en el mensaje de respuesta y realizar comunicaciones normales con el UE (101); o

si no se detecta la información TID consultada por la NAF, la BSF (102) devuelve a la NAF (104) un mensaje de respuesta de fallo, y el procedimiento comprende además:

indicar al UE (101) que realice una autenticación de arranque con la BSF (102).

2. El procedimiento de acuerdo con la reivindicación 1, que comprende además antes de que la NAF (104) verifique si existe la información TID:

una clave secreta compartida por el UE y la BSF (102), K, que se genera después de pasar una autenticación mutua entre el UE (101) y la BSF (102);

asignar la BSF (102) al UE (101) un TID que incluya solamente una identidad TID, que sea válida para una o más NAF al mismo tiempo y esté asociada con la clave secreta;

tras recibir el TID asignado por la BSF (102), enviar el UE (101) a la NAF (104) el mensaje de petición de aplicación de servicio que contiene el TID y verificar la NAF (104) si existe la información TID en la NAF (104);

que comprende además después de que la BSF (102) detecte el TID consultado por la NAF (104):

en base al TID detectado, la clave secreta asociada con el TID y la identidad de la NAF (104) de consulta, generar la BSF (102) una clave secreta derivada asociada con el TID y válida para la NAF (104) de consulta, asignar un plazo de validez para la clave secreta derivada y enviar un mensaje de respuesta de éxito a la NAF (104);

en donde el mensaje de respuesta de éxito comprende además la clave secreta derivada y el plazo de validez del TID en el mensaje de respuesta de éxito devuelto por la BSF (102) es el plazo de validez de la clave secreta derivada.

3. El procedimiento de acuerdo con la reivindicación 1, que comprende además antes de que la NAF (104) verifique si existe la información TID:

después de que una clave secreta compartida entre el UE (101) y la BSF (102), K, se genere durante una autenticación mutua entre el UE (101) y la BSF (102), asignar la BSF (102) al UE (101) un TID que incluya solamente una identidad TID, que sea válida solamente para la NAF (104) y esté asociada con la clave secreta, y enviar el TID asignado al UE (101);

tras recibir un mensaje de petición de aplicación que contenga el TID del UE (101), determinar la NAF (104) si el TID es válido para la NAF (104); si es válido, verificar la NAF (104) si existe la información TID

en la NAF (104). De lo contrario, la NAF (104) solicita al UE (101) un mensaje de error;

que comprende además, después de que la BSF (102) detecte el TID consultado por la NAF (104):

en base a la información del TID detectado, la clave secreta asociada con la TID y una identidad de la NAF (104) de consulta, generar la BSF (102) una clave secreta derivada asociada con la TID y válida para la NAF (104) de consulta, asignar un plazo de validez para la clave secreta derivada y enviar un mensaje de respuesta de éxito a la NAF (104);

en donde el mensaje de respuesta de éxito comprende además la clave secreta derivada válida para la NAF de consulta (104) y el plazo de validez del TID en el mensaje de respuesta de éxito devuelto por la BSF (102) es el plazo de validez de la clave secreta derivada.

4. El procedimiento de acuerdo con la reivindicación 1, que comprende además antes de que la NAF (104) verifique si existe la información TID:

establecer una clave secreta compartida entre la BSF (102) y la NAF (104), Knb;

después de que se genere una clave secreta compartida entre el UE (101) y la BSF (102), K, durante una autenticación mutua entre el UE (101) y la BSF (102),
asignar el BSF (102) al UE (101) una identidad válida solamente para la NAF (104), así como el plazo de validez para usar la identidad, cifrar la identidad asignada y el plazo de validez de la misma usando el Knb, tomando la identidad cifrada de un TID asociado con la clave secreta y enviando el TID al UE (101);

tras recibir el TID asignado por la BSF (102), enviar el UE (101) a la NAF (104) un mensaje de petición de aplicación que contenga el TID y comprobar la NAF (104) si existe la información TID en la NAF (104);

que comprende además, antes de que la NAF (104) determine si caduca el TID: descifrar la NAF (104) el TID recibido usando el Knb;

que comprende además, antes de que la NAF (104) envíe al BSF (102) el mensaje de consulta TID: descifrar la NAF (104) el TID recibido usando el Knb y determinar si el TID es válido para la NAF (104); si es válido, enviar la NAF (104) al BSF (102) el mensaje de consulta TID. De lo contrario, solicitar al UE (101) un mensaje de error;

en donde el mensaje de respuesta de éxito devuelto por la BSF (102) comprende además la clave secreta asociada con el TID consultado por la NAF (104).

5. El procedimiento de acuerdo con la reivindicación 1, que comprende además antes de que la NAF (104) verifique si existe la información TID:

después de que se genere una clave secreta compartida entre el UE (101) y la BSF (102), K, a partir de una autenticación mutua entre el UE (101) y la BSF (102), asignar la BSF (102) al UE (101) un TID que incluya solamente la identidad válida para la NAF (104) y asignar un plazo de validez para el TID, en donde el TID esté asociado con la clave secreta, almacenar el TID asignado y el plazo de validez del mismo y enviar el TID asignado al UE (101);

tras recibir un mensaje de petición de aplicación que contenga el TID del UE (101), determinar la NAF (104) si el TID es válido para la NAF (104); si es válido, verificar la NAF (104) si existe la información TID en la NAF (104). De lo contrario, solicitar al UE (101) un mensaje de error;

en donde el mensaje de respuesta de éxito devuelto por la BSF (102) comprende además la clave secreta asociada con el TID consultado por la NAF (104).

6. El procedimiento de acuerdo con cualquiera de las reivindicaciones 1 a 5, que comprende además:

después de haber logrado realizar una autenticación de arranque en la BSF (102), recibir el UE (101) un nuevo TID asignado por la BSF (102) y generar una clave secreta, K, asociada al nuevo TID;

tras recibir un mensaje de petición de aplicación que contenga el nuevo TID y el TID antiguo del UE (101), llevar a cabo la NAF (104) la consulta en la BSF (102); tras recibir un

mensaje de respuesta de éxito desde la BSF (102), almacenar la NAF (104) el nuevo TID del UE (101) y la clave secreta asociada con el nuevo TID y borrar o desactivar el TID antiguo almacenado previamente en la NAF (104) y la clave secreta asociada con el TID antiguo.

7. El procedimiento de acuerdo con la reivindicación 6, en donde dicha clave secreta asociada con el TID es una clave secreta derivada que se deriva, en conexión con la NAF (104) de consulta, de una clave secreta raíz asociada con el TID.

8. El procedimiento de acuerdo con la reivindicación 2 o la reivindicación 3, en donde dicho plazo de validez se determina por la BSF (102) en base a un nivel de seguridad de la NAF de consulta (104) y la información de perfil del UE (101).

9. El procedimiento de acuerdo con la reivindicación 1, que comprende además: realizar la NAF (104) o la BSF (102) las operaciones de facturación de acuerdo con el plazo de validez del TID.

10. El procedimiento de acuerdo con la reivindicación 1, en donde dicho plazo de validez es un tiempo de vida útil válido.

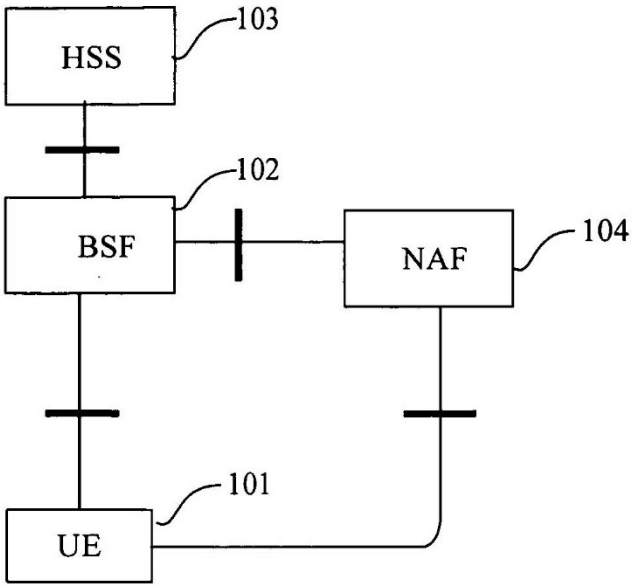

Figura 1

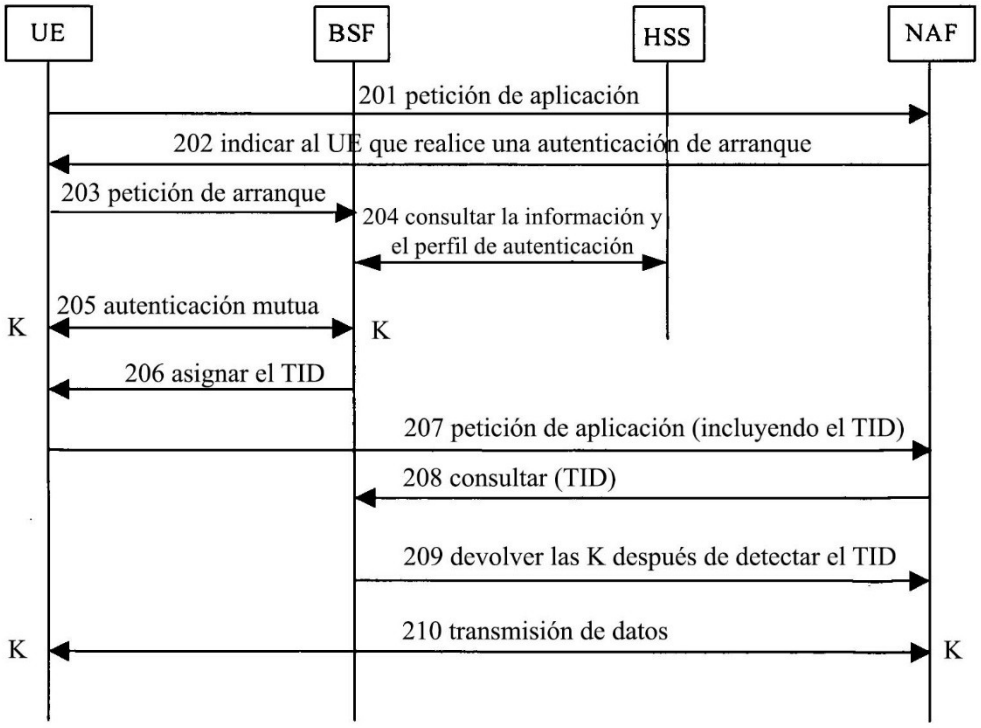

Figura 2

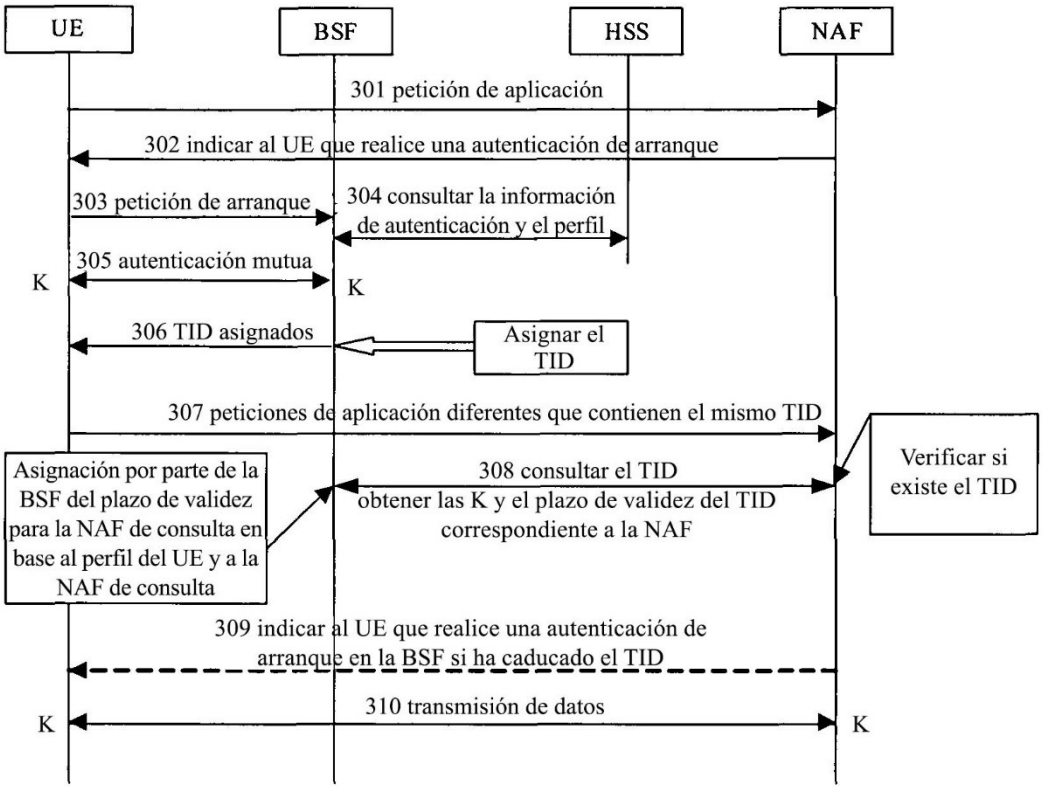
UE
BSF
HSS
NAF
301 petición de aplicación
302 indicar al UE que realice una autenticación de arranque
303 petición de arranque
304 consultar la información de autenticación y el perfil
305 autenticación mutua
K
K
306 TID asignados
Asignar el TID
307 peticiones de aplicación diferentes que contienen el mismo TID
Verificar si existe el TID
Asignación por parte de la BSF del plazo de validez para la NAF de consulta en base al perfil del UE y a la NAF de consulta
308 consultar el TID
obtener las K y el plazo de validez del TID correspondiente a la NAF
309 indicar al UE que realice una autenticación de arranque en la BSF si ha caducado el TID
310 transmisión de datos
K
K

Figura 3

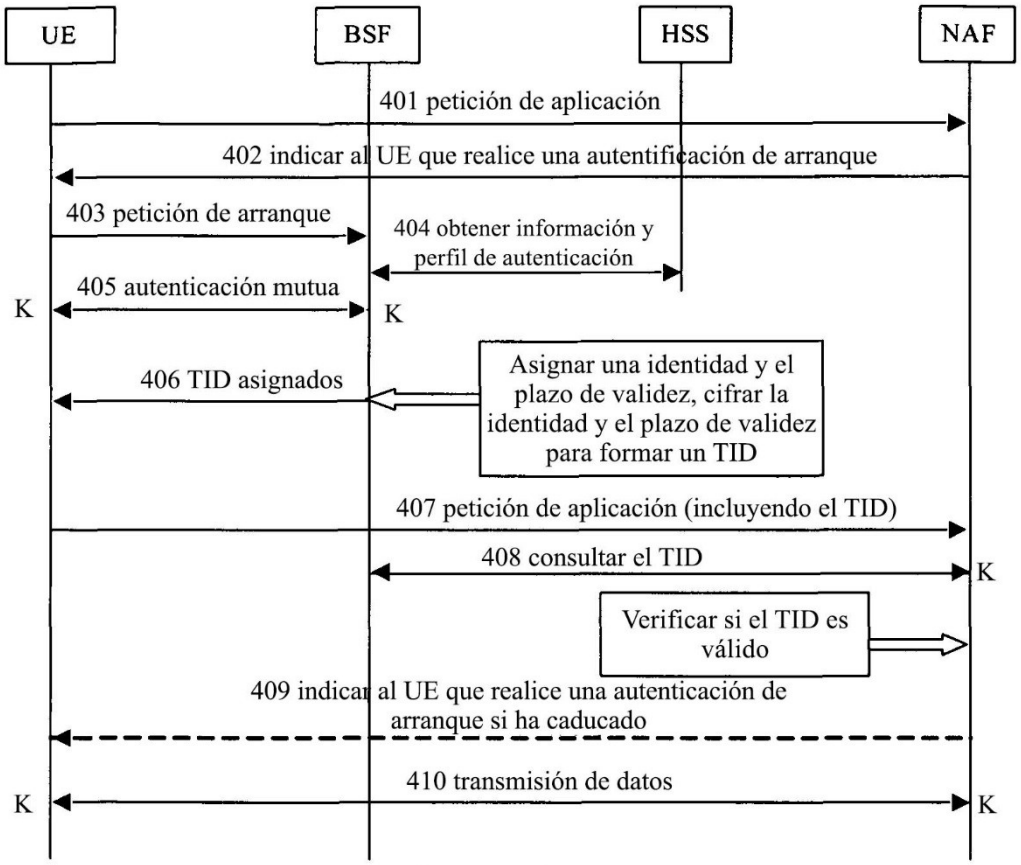
UE
BSF
HSS
NAF
401 petición de aplicación
402 indicar al UE que realice una autentificación de arranque
403 petición de arranque
404 obtener información y perfil de autenticación
405 autenticación mutua
K
K
406 TID asignados
Asignar una identidad y el plazo de validez, cifrar la identidad y el plazo de validez para formar un TID
407 petición de aplicación (incluyendo el TID)
408 consultar el TID
K
Verificar si el TID es válido
409 indicar al UE que realice una autenticación de arranque si ha caducado
410 transmisión de datos
K
K

Figura 4

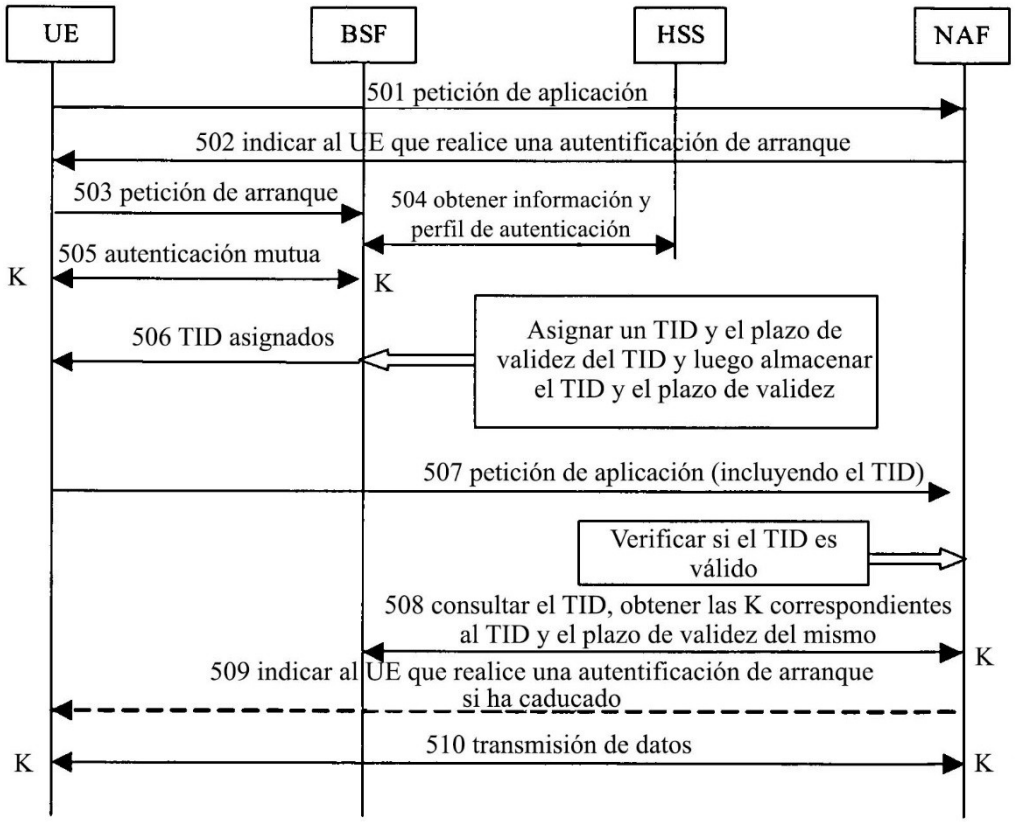
UE
BSF
HSS
NAF
501 petición de aplicación
502 indicar al UE que realice una autentificación de arranque
503 petición de arranque
504 obtener información y perfil de autenticación
505 autenticación mutua
K
K
506 TID asignados
Asignar un TID y el plazo de validez del TID y luego almacenar el TID y el plazo de validez
507 petición de aplicación (incluyendo el TID)
Verificar si el TID es válido
508 consultar el TID, obtener las K correspondientes al TID y el plazo de validez del mismo
K
509 indicar al UE que realice una autentificación de arranque si ha caducado
510 transmisión de datos
K
K

Figura 5