(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 481 046**

(51) Int. CI.:

H04L 29/06 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **09.03.2007 E 12192326 (2)**

(97) Fecha y número de publicación de la concesión europea: **14.05.2014 EP 2560342**

(54) Título: **Método, sistema y aparato para proteger una entidad de función de servicio de inicialización, BSF, a los fines de prevención de ataques**

(30) Prioridad:

14.03.2006 CN 200610064822

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
29.07.2014

(73) Titular/es:

HUAWEI TECHNOLOGIES CO., LTD. (100.0%)
B1-3A, Bantian, Longgang District, Shenzhen Guangdong 518129, CN

(72) Inventor/es:

YANG, YANMEI

(74) Agente/Representante:

LEHMANN NOVO, María Isabel

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

DESCRIPCIÓN

Método, sistema y aparato para proteger una entidad de función de servicio de inicialización, BSF, a los fines de prevención de ataques

CAMPO DE LA INVENCIÓN

La presente invención se refiere a la tecnología de seguridad de arquitectura de autenticación genérica (GAA) y en particular, a un método, sistema y aparato para proteger una entidad de función de servicio de inicialización (BSF) contra un ataque y una entidad BSF.

ANTECEDENTES DE LA INVENCIÓN

En el estándar de telecomunicaciones inalámbricas de la tercera generación, la arquitectura GAA es una arquitectura genérica que se utiliza por múltiples entidades de servicio de aplicación para realizar la autenticación de la identidad del usuario. La arquitectura GAA puede utilizarse para comprobar y realizar la autenticación de la identidad de un usuario de un servicio de aplicación. Los anteriores servicios de aplicación múltiples incluyen servicios multidifusión/difusión, servicios de licencias de usuarios, servicios de mensajería instantánea y servicios de agentes.

La Figura 1 ilustra la arquitectura GAA en la técnica anterior. Según se ilustra en la Figura 1, la arquitectura GAA consiste en un usuario, una entidad BSF que realiza la autenticación inicial de la identidad del usuario, un servidor de abonado residencial (HSS) y una entidad de función de aplicación de red (NAF). En adelante, la entidad BSF se refiere como "BSF" y la entidad NAF se refiere como "NAF". La función BSF y el usuario realizan una autenticación mutua entre sí. Durante la autenticación mutua, la identidad se verifica mutuamente y se genera una clave compartida para BSF y el usuario. El proceso de autenticación mutua se conoce también como un proceso de inicialización o un proceso de GBA. El usuario capaz de poner en práctica el proceso de GBA con la función BSF se conoce como un usuario autorizado de GBA. El servidor HSS memoriza un perfil que describe la información del usuario (perfil de usuario) y proporciona también la función de generar información de autenticación. La función NAF puede representar diferentes entidades de función de aplicación de red. Para poner en práctica un servicio, el usuario debe acceder a la función NAF correspondiente al servicio y entrar en comunicación con NAF. Las interfaces entre las entidades se ilustran en la Figura 1. La función BSF está conectada a NAF por intermedio de una interfaz Zn; el usuario está conectado a la BSF o la NAF por intermedio de un equipo de usuario (UE); el equipo UE está conectado a la BSF por intermedio de una interfaz Ub y conectado a la NAF por intermedio de una interfaz Ua.

Para utilizar un servicio, esto es, para acceder a la NAF correspondiente al servicio, el usuario realiza el proceso de inicialización en la BSF por intermedio del UE si el usuario conoce que el servicio necesita una autenticación mutua en la BSF. De no ser así, el usuario origina primero una demanda de conexión a la NAF correspondiente al servicio. Si la NAF adopta una arquitectura GAA (a saber, soporta la función de GAA) y encuentra que el usuario que origina la demanda de conexión no ha realizado la autenticación mutua en la BSF, la NAF notifica al usuario la realización del proceso de inicialización en la BSF.

Posteriormente, el usuario realiza la autenticación mutua con la BSF poniendo en práctica un proceso de inicialización entre el UE y la BSF. El UE envía una demanda de autenticación a la BSF. La demanda de autenticación incluye la identidad privada del usuario (a modo de ejemplo, identidad privada multimedia IP, aquí referida como "IMPI") o incluye una identidad IMPI derivada de un identificador de abonado móvil internacional (IMSI). Después de recibir la demanda de autenticación desde el usuario, la BSF adquiere la información de autenticación del usuario desde el servidor HSS. El mensaje de demanda de autenticación enviado por la BSF al HSS incluye también un identificador IMPI. En función del IMPI del usuario, el servidor HSS busca la información de autenticación, genera vectores de autenticación y reenvía los vectores a la BSF. La BSF realiza la autenticación mutua y la negociación de claves con el UE en función de la información de autenticación adquirida. A la terminación del proceso de inicialización, el equipo UE y la función BSF realizan una autenticación mutua y generan una clave compartida "Ks". La BSF define un periodo de validez "Duración-clave" para la clave compartida "Ks" y asigna una identidad temporal, a modo de ejemplo, una entidad B-TID, para el usuario; la BSF y el UE memorizan la clave compartida "Ks", la denominada B-TID y el periodo de validez de forma correlativa. Cuando el usuario desea comunicarse con la NAF, el UE envía una demanda de conexión que incluye la B-TID a la NAF de nuevo. El equipo de usuario UE calcula la clave derivativa denominada "clave específica de NAF" mediante un algoritmo derivativo preestablecido en función de la clave compartida "Ks".

Después de recibir la demanda de conexión, la NAF envía un mensaje de mensaje de demanda de consulta a la BSF para la búsqueda de B-TID si falla en encontrar B-TID al nivel local, en donde el mensaje transmite la identidad de la NAF y esta B-TID. Si la BSF falla en encontrar a B-TID al nivel local, la BSF notifica a la NAF que no está disponible ninguna información sobre el usuario. En este caso, la NAF notifica al usuario la realización de la autenticación mutua en la BSF. Si la BSF encuentra a B-TID, la BSF calcula la clave derivativa de la clave compartida "Ks" utilizando el mismo algoritmo derivativo que se aplica en el lado del usuario y a continuación, envía un mensaje de respuesta de éxito operativo a la NAF. El mensaje de respuesta de éxito operativo transmite la B-TID,

la clave derivativa correspondiente a B-TID y el periodo de validez de la clave compartida "Ks". Después de recibir el mensaje de respuesta de éxito operativo desde la BSF, la NAF considera al usuario como un usuario legal que ha pasado la autenticación de BSF. La NAF comparte la clave derivativa calculada a partir de la clave compartida "Ks". Esta clave derivativa es la misma que la clave derivativa calculada por el usuario en función de la clave compartida "Ks". En el acceso posterior a la NAF, el usuario utiliza la clave derivativa para proteger las comunicaciones con la NAF.

Cuando el usuario descubre que la clave compartida "Ks" pronto caducará o la NAF requiere al usuario la realización de la autenticación mutua en la BSF de nuevo, el usuario repite las etapas de autenticación mutua anteriores en la BSF para obtener una nueva clave compartida "Ks" y una nueva "B-TID".

En la práctica actual, la IMPI transmitida en la demanda de autenticación se envía en la forma de texto no cifrado, que hace a la IMPI del usuario vulnerable a escucha ilegal. Para cada demanda re-autenticación recibida, la BSF adquiere un grupo de vectores de autenticación desde el servidor HSS. Después de que un atacante malicioso adquiera las IMPIs de múltiples usuarios mediante escucha ilegal, si el intruso utiliza dichas IMPIs para enviar demandas de re-autenticación a BSF, la BSF necesita adquirir vectores de autenticación desde el HSS continuamente después de recibir las IMPIs de múltiples usuarios. En tanto que el intruso utilice la IMPI para enviar continuamente demandas de re-autenticación, la BSF adquirirá vectores de autenticación desde el servidor HSS de forma continua, de modo que la BSF resultará atacada de forma maliciosa.

Una solución al problema anterior en la técnica anterior es: si el UE tiene una identidad temporal válida (tal como TMPI, B-TID), la identidad temporal se utilizará para sustituir la IMPI en la demanda, con el fin de reducir la frecuencia de utilizar la IMPI en la interfaz Ub y para evitar la interceptación de IMPI. Puesto que identidades temporales se utilizan frecuentemente en la interfaz Ua, sin embargo, los intrusos pueden interceptar las identidades temporales desde la interfaz Ua y utilizar las identidades temporales para atacar la BSF por intermedio de la interfaz Ub. Por lo tanto, la técnica anterior no protege efectivamente a la BSF contra un ataque malicioso.

La solicitud de patente internacional WO 2005/107213 A1, describe un método para la autenticación de la identidad del abonado en el marco de la Arquitectura de Autenticación Genérica.

El documento WO 2007/008120 A1 da a conocer un método y disposición para autenticación y privacidad. La función BSF genera claves Ks y Ks NAF, con la correspondiente clave identificando a B_TID y B_TID_NAF. Con el fin de impedir el seguimiento del usuario mediante la colusión entre varias entidades NAF, B_TID_NAF y el comprobante operativo Voucher pueden ser únicos para cada NAF. La interfaz Ua está protegida, además, mediante encriptación utilizando la clave Ks y la interfaz Ub está protegida, además, contra ataques de un intermediario, denominado 'man-in-the-middle' utilizando signaturas con la clave Ks y provisión de innovación en dicha operación.

SUMARIO DE LA INVENCIÓN

Las formas de realización de la presente invención dan a conocer un método, sistema y aparato para proteger contra ataques a una entidad de función de servicio de inicialización (BSF) y una entidad BSF, con miras a proteger efectivamente a la entidad BSF contra los posibles ataques.

Las formas de realización de la presente invención dan a conocer la solución técnica siguiente.

Una forma de realización de la presente invención da a conocer un método para proteger a una entidad BSF contra posibles ataques, incluyendo: obtener una primera identidad temporal y una segunda identidad temporal, después de que un equipo de usuario (UE) realice una autenticación mutua con la entidad BSF, en donde la primera identidad temporal es diferente de la segunda identidad temporal; mediante el equipo de usuario UE, enviar una demanda que incluye la primera identidad temporal a la entidad BSF; y mediante el UE, el envío de una demanda de servicio que incluye la segunda identidad temporal a una entidad de función de aplicación de red (NAF).

Una forma de realización de la presente invención da a conocer un sistema para proteger una entidad BSF contra posibles ataques, incluyendo: un equipo de usuario (UE) está adaptado para obtener una primera identidad temporal y una segunda identidad temporal, en donde la primera identidad temporal es diferente de la segunda identidad temporal; y el UE está adaptado para enviar una demanda de la primera identidad temporal a la entidad BSF y para enviar una demanda de servicio de la segunda identidad temporal a la NAF.

Una forma de realización de la presente invención da a conocer, además, un aparato para proteger a una entidad BSF de un posible ataque, incluyendo: un primer módulo, adaptado para obtener una primera identidad temporal y una segunda identidad temporal; y un segundo módulo, adaptado para enviar una demanda que incluye la primera identidad temporal a una entidad BSF obtenida por el primer módulo y para enviar una demanda de servicio que incluye la segunda identidad temporal a una entidad NAF obtenida por el primer módulo.

Una entidad BSF incluye: un primer módulo, adaptado para generar una primera identidad temporal que se utiliza por un UE para originar una demanda de re-autenticación y una segunda identidad temporal que se utiliza por el UE

para originar una demanda de servicio.

Según se deduce de la solución técnica anterior, después de que el equipo UE termine la autenticación mutua con la BSF, las formas de realización de la presente invención generan dos identidades temporales diferentes para la autenticación mutua y el proceso de negociación de claves, una para el UE para originar una demanda de re-autenticación a la BSF y otra para el UE para originar una demanda de servicio para la NAF. Por lo tanto, las formas de realización de la presente invención pueden impedir que los intrusos intercepten, en su ataque, a identidades temporales (tales como TMPI y B-TID) en la interfaz Ua y utilizando las identidades temporales para originar las demandas de re-autenticación en la interfaz Ub, con lo que se protege efectivamente a la BSF contra posibles ataques, evitando una carga innecesaria en la BSF y ahorrando recursos.

BREVE DESCRIPCIÓN DE LOS DIBUJOS

La Figura 1 ilustra la arquitectura de GAA en la técnica anterior;

La Figura 2 es un diagrama de flujo de protección de la BSF contra posibles ataques según una forma de realización de la presente invención; y

La Figura 3 es un diagrama de flujo de protección de la BSF contra posibles ataques según otra forma de realización de la presente invención.

DESCRIPCIÓN DETALLADA DE LAS FORMAS DE REALIZACIÓN DE LA INVENCIÓN

En las formas de realización de la presente invención, después que el UE termine la autenticación mutua con la BSF, pueden generarse dos identidades temporales diferentes para la autenticación mutua, una para el UE para originar una demanda de re-autenticación a la BSF y otra para el equipo UE para originar una demanda de servicio para la NAF.

Con el fin de hacer más evidentes los objetivos y las ventajas de la solución técnica según la presente invención, se describe, a continuación, en detalle, la presente invención haciendo referencia a los dibujos adjuntos y a las formas de realización preferidas.

La Figura 2 es un diagrama de flujo de protección de la BSF contra ataques según una forma de realización de la presente invención. Esta forma de realización incluye las etapas siguientes:

Etapa 200: La BSF demandas al servidor HSS información de autenticación después de recibir una demanda de autenticación desde el UE.

Si el usuario ha adquirido una identidad temporal válida (tal como TMPI y B-TID), la demanda de autenticación incluye la identidad temporal; si el usuario no tiene ninguna identidad temporal válida, la demanda de autenticación incluye la identidad privada del usuario tal como una IMPI. Con la identidad temporal incluida en la demanda de autenticación, se impide que se intercepte la identidad privada del usuario.

Si la demanda de autenticación recibida por la BSF incluye la identidad privada del usuario, tal como IMPI, se utiliza la identidad privada para demandar al servidor HSS información de autenticación tal como vectores de autenticación.

Si la demanda de autenticación recibida por la BSF incluye una identidad temporal, la BSF comprueba, además, si la propia BSF memoriza cualquier registro que se memorice correlativamente con la identidad temporal. Si es así, la BSF busca la identidad privada del usuario tal como una IMPI memorizada correlativamente con la identidad temporal y demanda al servidor HSS para información de autenticación, tal como vectores de autenticación a través de la identidad privada. Si ningún registro se memoriza correlativamente con la identidad temporal, la BSF termina el proceso de autenticación o la BSF reenvía una indicación de error al UE para notificar al usuario el fallo de la autenticación y termina el proceso de autenticación. La indicación de error puede incluir causas de error. De este modo, aun cuando un intruso en ataque intercepte la identidad temporal cuando el UE utiliza una identidad temporal para originar una demanda de autenticación, el intruso atacante es incapaz de atacar a la BSF de forma malintencionada, porque que el UE obtiene una nueva identidad temporal después de que el UE realice una autenticación satisfactoria y la BSF memoriza también un registro correlativamente memorizado con la nueva identidad temporal; por lo tanto, la BSF es incapaz de encontrar la identidad privada del usuario mediante la identidad temporal proporcionada por el intruso atacante y no se realizará la autenticación del intruso atacante.

Etapa 201: La BSF realiza la autenticación mutua con el UE mediante la información de autenticación reenviada por el servidor HSS.

Mientras que la BSF realiza la autenticación mutua (esto es, el denominado inicialización operativo) con el UE, el UE y la BSF realizan una autenticación mutua y generan una clave compartida "Ks". Mientras tanto, el usuario calcula la clave derivativa "clave específica de NAF" por intermedio de un algoritmo derivativo preestablecido en función de la

clave "Ks" generada. La etapa 201 se pone en práctica de la misma manera que en la técnica anterior y por ello no se describe de nuevo.

Etapa 202: Dos identidades temporales diferentes se generan para la autenticación mutua (una identidad temporal puede ser B-TID o TMPI). Una identidad temporal se utiliza por el UE para originar una demanda de re-autenticación para la BSF y la otra se utiliza por el UE para originar una demanda de servicio a la NAF.

En esta etapa, después de que se realice la autenticación mutua, la BSF memoriza las dos identidades temporales generadas correlativamente con la identidad privada (tal como IMPI) del usuario que origina la demanda de autenticación. Una identidad temporal se utiliza para identificar al usuario en la demanda de servicio en la interfaz Ua y la otra se utiliza para identificar al usuario en la re-autenticación que se produce en la interfaz Ub.

En esta forma de realización, B-TID1 y B-TID2 representan dos identidades temporales diferentes, que se generan en los métodos siguientes:

Método 1: B-TID1 y B-TID2 se generan por la BSF.

En general, el valor variable "RAND", transmitido en la autenticación mutua, puede utilizarse para generar una identidad B-TID mediante un parámetro de codificación Base64encode (valor variable "RAND") + nombre de dominio de BSF. Base64encode es un modo de codificación, que convierte un número en cadenas, estando constituida cada cadena por seis bits. Cada dos cadenas están vinculadas por un operador "+". Para impedir que los intrusos intercepten, en su ataque, el valor variable "RAND" en el proceso de autenticación mutua y su inferencia operativa adicional en el valor B-TID, esta forma de realización puede generar, además, dos valores de B-TID diferentes en la forma siguiente:

B-TID1 = Base64encode (hash (RAND + valor aleatorio "RANDx")) + nombre de dominio de BSF, en donde el valor aleatorio "RANDx" se genera por la BSF de forma aleatoria. Debe entenderse que un B-TID1 puede generarse mediante el valor aleatorio "RANDx" en numerosas maneras. En esta forma de realización, B-TID1 se obtiene a través del valor aleatorio "RANDx" aleatoriamente generado por la BSF en lugar de a través del valor variable "RAND" transmitido en la autenticación mutua. De este modo, los impulsos atacantes son incapaces de interceptar el valor variable "RAND" en el proceso de autenticación mutua e inferir, además, el valor B-TID.

B-TID2 = "ID_" + Base64encode (cadena *hash* (RAND + valor aleatorio RANDy)) + nombre de dominio de BSF. Debe entenderse que una B-TID2 puede generarse mediante el valor aleatorio "RANDy" en numerosas maneras. En esta forma de realización, la B-TID2 se obtiene por intermedio del valor aleatorio "RANDy" generado de forma aleatoria por la BSF en lugar de a través del valor variable "RAND" transmitido en la autenticación mutua. De este modo, los intrusos atacantes son incapaces de interceptar el valor variable "RAND" en el proceso de autenticación mutua e infieren, además, en el valor de B-TID.

El valor aleatorio "RANDy" se genera de forma aleatoria por la BSF. La B-TID2 puede ser Base64encode (valor preestablecido RANDz) + cadena característica preestablecida, a modo de ejemplo, B-TID2 = Base64encode (*hash* (RANDz + valor aleatorio RANDy)) + "ID" + nombre de dominio de BSF.

En la fórmula anterior, "*hash*" significa la operación *Hash* e "ID_" significa una cadena adicional preestablecida. Para reducir la probabilidad de generar la misma B-TID en dos procesos de inicialización operativo, se añade una cadena a una u otra B-TID, a modo de ejemplo, B-TID2, para diferenciar la B-TID1 de la B-TID2 de modo formal. A modo de ejemplo, si el valor obtenido de la cadena operativa *Hash* (RAND + otro valor aleatorio especificado por la BSF "RANDx") contiene 256 dígitos, la B-TID tiene 2256 valores. Dos valores de B-TIDs necesitan asignarse en un proceso de inicialización operativo. Si no se toman ningunas medidas para diferenciar la B-TID1 de la B-TID2 de modo formal, la misma B-TID se asignará más probablemente en dos procesos de inicialización operativa y el número de usuarios servidos por la BSF disminuirá en consecuencia. Por lo tanto, esta forma de realización añade una cadena a una B-TID para diferenciar entre B-TIDs, con lo que se evita la disminución de usuarios simultáneamente servibles por la BSF debido a una B-TID extra asignada a proceso de inicialización operativo.

Como alternativa, en la re-autenticación en la interfaz Ub, la propia B-TID es un valor de Base64encode (valor aleatorio "RANDy") exclusivo del nombre de dominio de BSF. Con la B-TID utilizada en la interfaz Ub, no es necesario encontrar la BSF en función del nombre de dominio de BSF incluido en la B-TID. Por lo tanto, no se requiere el nombre de dominio de BSF y las dos B-TIDs pueden diferenciarse sin el nombre de dominio de BSF.

Método 2: La identidad temporal (tal como TMPI, B-TID) se genera, al nivel local, por la BSF y el UE, respectivamente, a través de los mismos parámetros.

La BSF y el UE utilizan la información adquirida en el proceso de inicialización operativa, a modo de ejemplo, la clave compartida "Ks", o la clave derivativa "clave específica de NAF", para generar una identidad temporal. De forma similar, para impedir que los intrusos atacantes intercepten el valor variable "RAND" en el proceso de autenticación mutua e infieran, además, una identidad temporal, la BSF y la tarjeta de circuito integrado universal

(UICC) en una GBA_U pueden generar una identidad temporal, respectivamente, en la forma siguiente:

B-TID = base64encode (derivación(CK||IK))@nombre_dominio_servidores_BSF

En la fórmula anterior, CK e IK son claves generadas en la autenticación mutua y el nombre_dominio_servidores_BSF es el nombre del servidor BSF. Dos identidades temporales diferentes pueden obtenerse mediante dos funciones de derivación diferentes o dos parámetros diferentes de la misma función.

Además, para simplificar el cálculo de la identidad temporal generada por UICC, la derivación (CK||IK) puede reutilizar la función de derivación de claves (KDF). Si las dos identidades privadas se representan por B-TID1 y B-TID2, la B-TID1 y la B-TID2 se generan en la forma siguiente:

B-TID1 = base64encode (KDF (CK, IK, "utilización de Ua", RAND, nombre_BSF))@nombre_dominio_servidores_BSF, en donde RAND es un valor variable transmitido en la autenticación mutua y nombre_BSF es el nombre de la BSF.

B-TID2 = 'TD_"+base64encode (KDF (CK, IK, "utilización de Ub", RAND, nombre_BSF))@nombre_dominio_servidores_BSF, en donde la cadena "utilización de Ua" y la cadena "utilización de Ub" son cadenas especiales que preestablecidas para la finalidad de obtener dos valores de claves diferentes desde la KDF por intermedio de los mismos parámetros.

En este método de generación, el “ID_” puede añadirse también a base64encode (KDF (CK, IK, "utilización de Ub", RAND, nombre_BSF)).

Método 3: Una identidad temporal (tal como B-TID) se genera por la BSF y el UE al nivel local y la otra identidad temporal se genera por la BSF al nivel local y se envía al UE. La BSF y el UE generan una identidad temporal, al nivel local, en la misma manera que el segundo método anteriormente mencionado. La BSF genera la otra identidad temporal, al nivel local, en la misma manera que el primer método antes mencionado. A modo de ejemplo, la identidad temporal para identificar el usuario en la interfaz Ua se adquiere por la BSF en función del valor RAND utilizado en el proceso de autenticación mutua con el UE y enviado al UE; la identidad temporal para uso en la interfaz Ub se obtiene por la BSF y el UE mediante cálculo.

Debe entenderse que para el proceso de GBA_ME, el UE anterior se refiere al propio equipo móvil (ME). Para el proceso de GBA_U, el UE anterior se refiere a la tarjeta de circuito integrado universal (UICC) en el equipo ME. En el proceso de GBA_U, las claves "CK" y "IK" en el lado de UE y las claves que se derivan de dichas dos claves se generan por la tarjeta UICC y se memorizan en la UICC en lugar de enviarse a ME. Por lo tanto, para el proceso de GBA_U, el equipo UE genera la identidad temporal (tal como B-TID) en la tarjeta UICC.

En esta etapa, después de que se generen dos B-TIDs, se utiliza el primer método anterior para generar la B-TID (incluyendo B-TID1 y B-TID2), la BSF encripta, además, la B-TID y la envía al UE, indicando que la B-TID está encriptada. Debe entenderse que la B-TID puede encriptarse en numerosas maneras. El método de encriptación específico es independiente de esta forma de realización de la presente invención. La finalidad de la encriptación es garantizar la seguridad de la transmisión de B-TID. Además, para ser compatible con el UE de la versión R6, si el UE es incapaz de identificar la B-TID enviada desde la BSF, la BSF necesita enviar una B-TID de la versión R6, esto es, utilizar el valor aleatorio RAND generado en la autenticación mutua y el proceso de negociación de claves como una B-TID. Cuando la red y el UE adoptan el método dado a conocer en esta forma de realización de la presente invención, resulta innecesario enviar una B-TID de la versión R6 al UE.

Si los métodos segundos y terceros anteriores se utilizan para generar una B-TID (incluyendo B-TID1 y B-TID2), la BSF envía una indicación de generación de B-TID al UE, dando instrucciones al UE para generar la B-TID en la misma manera que la BSF. Además, para ser compatible con el UE de la versión R6, si el UE es incapaz de identificar la B-TID enviada desde la BSF, la BSF necesita enviar una B-TID de la versión R6, a saber, utilizar el valor aleatorio RAND generado en la autenticación mutua y el proceso de negociación de claves como una B-TID. Cuando la red y el UE adoptan ambos el método dado a conocer en esta forma de realización de la presente invención, resulta innecesario enviar una B-TID de la versión R6 al UE.

Posteriormente, el UE procesa las dos B-TIDs recibidas para asegurar que estarán disponibles en el momento de la demanda de re-autenticación o para acceder a NAF. Para proceso de GBA_ME, si el UE recibe una B-TID encriptada (incluyendo B-TID1 y B-TID2), el equipo UE desencripta la B-TID recibida (incluyendo B-TID1 y B-TID2) y memoriza las B-TID1 y B-TID2 desencriptadas; si el UE recibe una indicación de generación de B-TID, el UE genera una B-TID (incluyendo B-TID1 y B-TID2) al nivel local, en la misma manera que la BSF y la memoriza.

Para el proceso de GBA_U, (i) si el equipo ME recibe una B-TID encriptada (incluyendo B-TID1 y B-TID2), ME reenvía la B-TID encriptada a la UICC y la UICC desencripta la B-TID recibida (incluyendo B-TID1 y B-TID2) y memoriza las B-TID1 y B-TID2 desencriptadas; la UICC envía la B-TID desencriptada (incluyendo B-TID1 y B-TID2) a la ME y ME memoriza las B-TID1 y B-TID2 recibidas; (ii) si ME recibe una indicación de generación de B-TID, ME

genera una B-TID (incluyendo B-TID1 y B-TID2) localmente en la misma manera que la BSF; la UICC memoriza la B-TID generada (incluyendo B-TID1 y B-TID2) y envía la B-TID al ME; y ME memoriza las B-TID1 y B-TID2 recibidas.

En consecuencia, la B-TID usada para enviar una demanda de servicio a la NAF, a través de la interfaz Ua es diferente de la B-TID utilizada para enviar una demanda de re-autenticación a la BSF por intermedio de la interfaz Ub. De esta manera se protege efectivamente a la BSF contra ataques, evita una carga innecesaria sobre la BSF y ahorra recursos.

Además, esta forma de realización añade una cadena a una B-TID para diferenciar entre B-TIDs, con lo que se evita la disminución de usuarios simultáneamente servibles por la BSF debido a una B-TID extra asignada en cada proceso de inicialización.

La Figura 3 es un diagrama de flujo de protección de la BSF contra posibles ataques en una forma de realización de la presente invención. Tomando a modo de ejemplo el proceso de GBA_U, esta forma de realización se elabora sobre el método de la presente invención. Según se ilustra en la Figura 3, se supone que la demanda de autenticación enviada por ME es una demanda de re-autenticación y ME memoriza una identidad temporal válida (tal como B-TID) y la BSF memoriza la IMPI de ME correspondiente a la B-TID. El método incluye las etapas siguientes:

Etapa 300: ME envía una demanda de autenticación a la BSF, que incluye a B-TID.

Etapa 301: En función de la B-TID recibida, la BSF detecta que la propia BSF memoriza una IMPI de ME correspondiente a B-TID, lo que indica que ME es un usuario válido.

Etapa 302a: La BSF incluye la IMPI correspondiente a la B-TID en la demanda de información de autenticación y envía la demanda al servidor HSS para adquirir información de autenticación tal como vectores de autenticación.

Si BSF deja de encontrar a la IMPI correspondiente a B-TID en la BSF en función de la B-TID recibida, la BSF prosigue con la etapa 302b. Es decir, la BSF reenvía una indicación de error a ME y termina el proceso de autenticación.

Etapas 303-304: El servidor HSS reenvía vectores de autenticación a la BSF y la BSF utiliza la información de autenticación para realizar la autenticación mutua y la negociación de claves con ME.

La puesta en práctica específica de esta etapa es la misma que para la etapa 201 y por ello no se describe de nuevo.

Etapa 305: La BSF genera dos B-TIDs y las encripta.

Esta forma de realización supone que el primer método en la etapa 202 se utiliza para generar la B-TID y por ello no se describe, de nuevo el método de generación específico.

Etapa 306: La BSF introduce las dos B-TIDs encriptadas en un mensaje de indicación de éxito operativo y envía el mensaje a ME.

Etapa 307: ME introduce las dos B-TIDs encriptadas en una orden de APDU y reenvía la orden a UICC.

Etapa 308: La UICC desencripta las dos B-TIDs recibida y memoriza las dos B-TIDs desencriptadas.

Etapa 309: La UICC reenvía las dos B-TIDs desencriptadas a ME y ME memoriza las dos B-TIDs recibidas.

Etapa 310: ME utiliza una de las B-TIDs para originar una demanda de re-autenticación y utiliza la otra B-TID para originar una demanda de servicio a la NAF.

Según se deduce de la forma de realización anterior de la presente invención, para impedir que los intrusos atacantes intercepten la IMPI, la B-TID puede incluirse en la demanda de re-autenticación; para impedir que los intrusos atacantes intercepten la B-TID en la interfaz Ua y utilizar la B-TID para originar demandas de re-autenticación en la interfaz Ub, la BSF genera dos B-TIDs diferentes en la autenticación del UE, una para la autenticación del UE en la interfaz Ua y otra para la autenticación del UE en la interfaz Ub. De esta manera, la B-TID utilizada para demandar servicios en la interfaz Ua es diferente de la B-TID utilizada para demandar la re-autenticación en la interfaz Ub. Esto protege a la BSF efectivamente contra los ataques, evita una carga innecesaria sobre la BSF y ahorra recursos.

Además, en el proceso de generar una B-TID, para evitar que sea interceptada la B-TID, se pueden aplicar dos métodos: (1) Ambas B-TID1 y B-TID2 se generan por la BSF, desencriptada y enviada al UE; (2) dos B-TIDs diferentes se generan por la BSF y el UE, respectivamente, en la misma forma después de la terminación del proceso de inicialización; o bien, una B-TID se genera por la BSF y el UE, respectivamente, en la misma manera, y

la otra B-TID se genera por la BSF, encriptada y enviada al UE. Esto protege a la BSF efectivamente contra posibles ataques, evita una carga innecesaria sobre la BSF, ahorra recursos e impide el ataque de la denegación de servicio (DoS).

Un sistema para proteger una entidad BSF contra ataques se da a conocer en una forma de realización de la presente invención que incluye una entidad BSF, un equipo UE y una entidad NAF.

En este sistema, la entidad BSF genera dos identidades temporales diferentes, las encripta y las envía al UE; el UE desencripta identidades temporales recibidas, utiliza una identidad temporal para originar una demanda de re-autenticación a la BSF a través de la interfaz Ub y utiliza la otra para originar una demanda de servicio para la entidad NAF mediante la interfaz Ua; después de recibir la demanda de servicio desde el equipo UE, la entidad NAF envía su propia identidad junto con la identidad temporal recibida a BSF para buscar la identidad temporal si la entidad NAF falla en encontrar la identidad temporal al nivel local.

La entidad BSF memoriza la identidad temporal y la identidad privada del usuario correlativamente. Después de recibir la identidad temporal incluida en la demanda de re-autenticación desde el UE, la entidad BSF comprueba si la identidad temporal se memoriza al nivel local. Si es así, la BSF utiliza la identidad privada del usuario memorizada correlativamente con la B-TID para demandar al servidor HSS información de autenticación y para realizar la autenticación del UE.

Otro sistema para proteger a una entidad BSF contra posibles ataques, dada a conocer en una forma de realización de la presente invención, incluye una entidad BSF, un equipo UE y una entidad NAF.

En este sistema, la entidad BSF genera una identidad temporal, encripta la identidad temporal y la envía al UE; la entidad BSF envía una indicación de generación de identidad temporal al UE, dando instrucciones al UE para generar la otra identidad temporal por intermedio de los parámetros obtenidos en la autenticación mutua; mientras tanto, la entidad BSF genera la otra identidad temporal en la misma manera. El equipo UE recibe la identidad temporal enviada desde la entidad BSF y la desencripta. Después de recibir la indicación de generación de identidad temporal, el equipo UE genera la otra identidad temporal. A continuación, el UE origina una demanda de re-autenticación a la BSF por intermedio de la interfaz Ub utilizando una identidad temporal y origina una demanda de servicio a la entidad NAF por intermedio de la interfaz Ua utilizando la otra identidad temporal. Después de recibir la demanda de servicio desde el UE, la entidad NAF envía su propia identidad y la identidad temporal recibida a la BSF para buscar la identidad temporal si la entidad NAF falla en encontrar la identidad temporal al nivel local.

La entidad BSF memoriza la identidad temporal y la identidad privada del usuario de forma correlativa. Después de recibir la identidad temporal incluida en la demanda de re-autenticación, desde el equipo UE, la entidad BSF comprueba si la identidad temporal está memorizada al nivel local. Si es así, la BSF utiliza la identidad privada del usuario memorizada correlativamente con la identidad temporal para demandar al servidor HSS la información de autenticación y para realizar la autenticación del UE.

Un tercer sistema para proteger una entidad BSF contra posibles ataques, dado a conocer en una forma de realización de la presente invención, incluye una entidad BSF, un equipo UE y una entidad NAF.

En este sistema, la entidad BSF genera dos identidades temporales diferentes y envía una indicación de generación de identidad temporal, dando instrucciones al UE para generar dos identidades temporales diferentes en la misma manera; después de recibir la indicación, el equipo UE genera dos identidades temporales diferentes en la misma manera que la entidad BSF, utiliza una identidad temporal para originar una demanda de re-autenticación a la BSF por intermedio de la interfaz Ub y utiliza la otra para originar una demanda de servicio a la entidad NAF por intermedio de la interfaz Ua; después de recibir la demanda de servicio desde el UE, la entidad NAF envía su propia identidad junto con esta identidad temporal a la BSF para buscar la identidad temporal si la entidad NAF falla en encontrar la identidad temporal, al nivel local.

La entidad BSF memoriza la identidad temporal y la identidad privada del usuario de forma correlativa. Después de recibir la identidad temporal incluida en la demanda de re-autenticación desde el UE, la entidad BSF comprueba si la identidad temporal está memorizada al nivel local. Si es así, la BSF utiliza la identidad privada del usuario memorizada correlativamente con la identidad temporal para demandar al servidor HSS información de autenticación y para realizar la autenticación el UE.

Un aparato para la protección de una entidad BSF contra posibles ataques, dada a conocer en una forma de realización de la presente invención, incluye:

un primer módulo, adaptado para adquirir dos identidades temporales diferentes; y un segundo módulo, adaptado para originar una demanda de re-autenticación para una entidad BSF mediante la primera identidad temporal adquirida por el primer módulo y para originar una demanda de servicio para una entidad NAF por intermedio de la segunda identidad temporal.

El primer módulo puede adquirir dos identidades temporales diferentes en tres maneras: (1) el primer módulo recibe dos identidades temporales diferentes desde la entidad BSF; (2) el primer submódulo, en el primer módulo, recibe la primera identidad temporal desde la entidad BSF y recibe la indicación de generación de identidad temporal desde la entidad BSF; y el segundo submódulo genera la otra identidad temporal en función de la indicación de generación de identidad temporal obtenida por el primer submódulo; (3) el primer submódulo en el primer módulo recibe la indicación de generación de identidad temporal desde la entidad BSF; el segundo submódulo genera dos identidades temporales diferentes en función de la indicación de generación de identidad temporal obtenida por el primer submódulo.
Según una forma de realización de la presente invención, el aparato para proteger a una entidad BSF contra posibles ataques puede ser un equipo móvil (ME) o una tarjeta de circuito integrado universal (UICC) en el equipo móvil.

Una entidad BSF dada a conocer en una forma de realización de la presente invención, incluye un primer módulo, adaptado para generar una primera identidad temporal que se utiliza por el equipo UE para originar una demanda de re-autenticación y una segunda identidad temporal que se utiliza por el UE para originar una demanda de servicio.

El primer módulo en la entidad BSF está adaptado, además, para encriptar las dos identidades temporales generadas diferentes y para enviarlas al UE; o bien, enviar una indicación de generación de identidad temporal al UE, dando instrucciones al equipo UE para generar dos identidades temporales diferentes en la misma manera; o bien, encriptar una identidad temporal y enviarla al UE y enviar una indicación de generación de identidad temporal al UE, dando instrucciones al UE para generar la otra identidad temporal.

La entidad BSF incluye, además, un segundo módulo, adaptado para demandar al servidor HSS información de autenticación si el segundo módulo encuentra que la identidad temporal está memorizada localmente después de recibir una demanda de re-autenticación desde el UE; de no ser así, terminar el proceso de autenticación, o reenviar una indicación de error al UE y terminar el proceso de autenticación.

Los componentes del sistema para proteger a la entidad BSF contra posibles ataques, los componentes del aparato para proteger la entidad BSF contra posibles ataques y las funciones que la entidad BSF han sido descritas anteriormente en los procedimientos de las formas de realización anteriores y por ello no se describirán de nuevo.

Aunque la presente invención ha sido descrita mediante algunas formas de realización a modo de ejemplo, la presente invención no está limitada a dichas formas de realización. Es evidente para los expertos en esta técnica que se pueden realizar varias modificaciones y variaciones a la presente invención sin desviarse por ello de su alcance de protección. La presente invención está prevista para cubrir las modificaciones y variaciones aportadas a condición de que caigan dentro del alcance de protección definido por las reivindicaciones siguientes.

REIVINDICACIONES

1. Un método para proteger una entidad de función de servicio de inicialización (BSF) contra un posible ataque, caracterizado por cuanto que comprende:

realizar, por una entidad BSF, de una autenticación mutua con un equipo de usuario (UE) utilizando una identidad temporal o una identidad privada de usuario enviada desde el UE;

generar, por la entidad BSF, una primera identidad temporal y una segunda identidad temporal después de que la entidad BSF realice la autenticación mutua con el UE, en donde la primera identidad temporal es diferente de la segunda identidad temporal y en donde las primera y segunda identidades temporales son diferentes de la identidad temporal o de la identidad privada del usuario;

enviar, por la entidad BSF, la primera identidad temporal y la segunda identidad temporal al UE; y

recibir, por la entidad BSF, una demanda de re-autenticación que incluye la primera identidad temporal desde el UE;

en donde, el UE envía una demanda de servicio que incluye la segunda identidad temporal a una entidad de función de aplicación de red (NAF).

2. El método según la reivindicación 1, en donde la realización, por la entidad BSF, de la autenticación mutua con el UE utilizando la identidad temporal enviada desde el UE comprende en particular:

recibir, por la entidad BSF, una demanda de autenticación desde el UE, en donde la demanda de autenticación que incluye la identidad temporal;

determinar, por la entidad BSF, si la entidad BSF memoriza una identidad privada de usuario correlativamente con la identidad temporal; y

demandar, por la entidad BSF, un servidor de abonado residencial (HSS) para información de autenticación por intermedio de la identidad privada del usuario si la entidad BSF memoriza la identidad privada del usuario y realizar, por la entidad BSF, la autenticación mutua con el UE utilizando la información de autenticación enviada desde el servidor HSS; o,

acabar, por la entidad BSF, un proceso de autenticación en curso si la entidad BSF no memoriza la identidad privada del usuario; o enviar, por la entidad BSF, una indicación de error al UE y acabar un proceso de autenticación en curso si la entidad BSF no memoriza la identidad privada del usuario.

3. El método según la reivindicación 1, en donde:

la entidad BSF genera la primera identidad temporal y la segunda identidad temporal utilizando dos valores aleatorios (RAND) generados de forma aleatoria.

4. El método según la reivindicación 1, en donde la primera identidad temporal es una identidad temporal (TMPI) y la segunda identidad temporal es un Identificador de Transacción de Inicialización (B-TID).

5. Una entidad de función de servicio de inicialización (BSF), caracterizada por cuanto que comprende:

un procesador, configurado para realizar una autenticación mutua con un equipo de usuario (UE) utilizando una identidad temporal o una identidad privada de un usuario enviada desde el UE y para generar una primera identidad temporal y una segunda identidad temporal después de que la entidad BSF realice la autenticación mutua con el UE, en donde la primera identidad temporal es diferente de la segunda identidad temporal y en donde las primera y segunda identidades temporales son diferentes de la identidad temporal o de la identidad privada del usuario;

un transmisor, configurado para enviar la primera identidad temporal y la segunda identidad temporal al UE; y

un receptor, configurado para recibir una demanda de re-autenticación que incluye la primera identidad temporal desde el UE;

en donde el UE está configurado para enviar una demanda de servicio que incluye la segunda identidad temporal a entidad de función de aplicación de red (NAF).

6. La función BSF según la reivindicación 5, en donde si el procesador realiza la autenticación mutua con el UE utilizando la identidad temporal,

el receptor está configurado, además, para recibir una demanda de autenticación desde el UE, en donde la

demanda de autenticación incluye la identidad temporal;

el procesador está configurado, además, para determinar si la entidad BSF memoriza una identidad privada del usuario correlativamente con la identidad temporal; y

el procesador está configurado, además, para demandar un servidor de abonado residencial (HSS) para información de autenticación a través de la identidad privada del usuario si la entidad BSF memoriza la identidad privada del usuario; o,

el procesador está configurado, además, para acabar un proceso de autenticación en curso si la entidad BSF no memoriza la identidad privada del usuario; o para enviar una indicación de error al UE y acabar un proceso de autenticación en curso si la entidad BSF no memoriza la identidad privada del usuario.

7. La función BSF según la reivindicación 5, en donde:

el procesador está configurado, además, para generar la primera identidad temporal y la segunda identidad temporal utilizando dos valores aleatorios (RAND) generados de forma aleatoria.

8. La función BSF según la reivindicación 5, en donde la primera identidad temporal es una identidad temporal (TMPI) y la segunda identidad temporal es un Identificador de Transacción de Inicialización (B-TID).

9. Un método para proteger a entidad de función de servicio de inicialización (BSF) contra un ataque, caracterizado por cuanto que comprende:

realizar, por una entidad BSF, una autenticación mutua con un equipo de usuario (UE) utilizando una identidad temporal o una identidad privada del usuario enviada desde el UE;

generar, por la entidad BSF, una primera identidad temporal y una segunda identidad temporal, en donde la primera identidad temporal es diferente de la segunda identidad temporal y las primera y segunda identidades temporales son diferentes de la identidad temporal o de la identidad privada del usuario;

enviar, por la entidad BSF, una indicación de generación de identidad temporal al UE, en donde la indicación de generación de identidad temporal se utiliza para dar instrucciones al equipo de usuario UE respecto a la generación de la primera identidad temporal y de la segunda identidad temporal utilizando una misma forma como la entidad BSF; y

recibir, por la entidad BSF, una demanda de re-autenticación que incluye la primera identidad temporal procedente del UE;

en donde, el UE envía una demanda de servicio que incluye la segunda identidad temporal a una entidad de función de aplicación de red (NAF).

10. El método según la reivindicación 9, en donde la primera identidad temporal y la segunda identidad temporal se generan por la entidad BSF y el UE utilizando una clave obtenida en la autenticación mutua.

11. El método según la reivindicación 9, en donde la realización, por la entidad BSF, de la autenticación mutua con el UE utilizando la identidad temporal enviada desde el UE comprende, en particular:

recibir, por la entidad BSF, una demanda de autenticación desde el UE, en donde la demanda de autenticación incluye la identidad temporal;

determinar, por la entidad BSF, si la entidad BSF memoriza una identidad privada del usuario correlativamente con la identidad temporal; y

demandar, por la entidad BSF, a un servidor de abonado residencial (HSS) información de autenticación a través de la identidad privada del usuario si la entidad BSF memoriza la identidad privada del usuario y realizar, por la entidad BSF, la autenticación mutua con el equipo UE utilizando la información de autenticación enviada desde el HSS; o,

acabar, por la entidad BSF, un proceso de autenticación en curso si la entidad BSF no memoriza la identidad privada del usuario; o enviar, por la entidad BSF, una indicación de error al equipo UE y acabar un proceso de autenticación en curso si la entidad BSF no memoriza la identidad privada del usuario.

12. El método según la reivindicación 9, en donde la primera identidad temporal es una identidad temporal (TMPI) y la segunda identidad temporal es un Identificador de Transacción de Inicialización (B-TID).

13. Una entidad de función de servicio de inicialización (BSF), caracterizada por cuanto que comprende:

un procesador, configurado para realizar una autenticación mutua con un equipo de usuario (UE) utilizando una identidad temporal o una identidad privada del usuario enviada desde el UE y generar una primera identidad temporal y una segunda identidad temporal, en donde la primera identidad temporal es diferente de la segunda identidad temporal y las primera y segunda identidades temporales son diferentes de la identidad temporal o de la identidad privada del usuario;

un transmisor configurado para enviar una indicación de generación de identidad temporal al UE, en donde la indicación de generación de identidad temporal se utiliza para dar instrucciones al equipo UE respecto a la generación de la primera identidad temporal y de la segunda identidad temporal utilizando la clave obtenida en la autenticación mutua; y

un receptor, configurado para recibir una demanda de re-autenticación que incluye la primera identidad temporal desde el UE;

en donde el UE está configurado para enviar una demanda de servicio que incluye la segunda identidad temporal a una entidad de función de aplicación de red (NAF).

14. La función BSF según la reivindicación 13, en donde

el procesador está configurado, además, para generar la primera identidad temporal y la segunda identidad temporal utilizando una clave obtenida en la autenticación mutua; y

el UE está configurado, además, para generar la primera identidad temporal y la segunda identidad temporal utilizando la clave.

15. La función BSF según la reivindicación 13, en donde:

el receptor está configurado, además, para recibir una demanda de autenticación desde el UE, en donde la demanda de autenticación incluye la identidad temporal;

el procesador está configurado, además, para determinar si la entidad BSF memoriza una identidad privada del usuario correlativamente con la identidad temporal; y

el procesador está configurado, además, para demandar a un servidor de abonado residencial (HSS) información de autenticación mediante la identidad privada del usuario si la entidad BSF memoriza la identidad privada del usuario; o,

el procesador está configurado, además, para acabar un proceso de autenticación en curso si la entidad BSF no memoriza la identidad privada del usuario; o para enviar una indicación de error al equipo UE y terminar un proceso de autenticación en curso si la entidad BSF no memoriza la identidad privada del usuario.

16. La función BSF según la reivindicación 13, en donde la primera identidad temporal es una identidad temporal (TMPI), la segunda identidad temporal es un Identificador de Transacción de Inicialización (B-TID).

17. Un método para proteger una entidad de función de servicio de inicialización (BSF) contra un ataque, caracterizado por cuanto que comprende:

realizar, por una entidad BSF, una autenticación mutua con un equipo de usuario (UE) utilizando una identidad temporal o una identidad privada del usuario enviada desde el UE;

generar, por la entidad BSF, una primera identidad temporal y una segunda identidad temporal, en donde la primera identidad temporal es diferente de la segunda identidad temporal y las primera y segunda identidades temporales son diferentes de la identidad temporal o de la identidad privada del usuario;

enviar, por la entidad BSF, la primera identidad temporal y la segunda identidad temporal al UE;

enviar, por la entidad BSF, una indicación de generación de identidad temporal al UE, en donde la indicación de generación de identidad temporal se utiliza para dar instrucciones al UE en cuanto a la generación de otra de la primera identidad temporal y de la segunda identidad temporal utilizando una misma forma que la entidad BSF; y

recibir, por la entidad BSF, una demanda de re-autenticación que incluye la primera identidad temporal desde el UE;

en donde, el UE envía una demanda de servicio que incluye la segunda identidad temporal a una entidad de función de aplicación de red (NAF).

18. El método según la reivindicación 17, que comprende, además:

generar, por la entidad BSF, la primera identidad temporal y la segunda identidad temporal utilizando un valor aleatorio RAND generado de forma aleatoria y la otra de entre la primera identidad temporal y la segunda identidad temporal utilizando una clave obtenida en la autenticación mutua;

en donde el equipo UE genera la otra de entre la primera identidad temporal y la segunda identidad temporal utilizando la clave obtenida en la autenticación mutua.

19. El método según la reivindicación 17, en donde la realización, por la entidad BSF, de la autenticación mutua con el UE utilizando la identidad temporal enviada desde el UE comprende, en particular:

recibir, por la entidad BSF, una demanda de autenticación desde el UE, en donde la demanda de autenticación incluye la identidad temporal;

determinar, por la entidad BSF, si la entidad BSF memoriza una identidad privada del usuario correlativamente con la identidad temporal y

demandar, por la entidad BSF, a un servidor de abonado residencial (HSS) para información de autenticación mediante la identidad privada del usuario si la entidad BSF memoriza la identidad privada del usuario y realizar, por la entidad BSF, la autenticación mutua con el UE utilizando la información de autenticación enviada desde el servidor HSS o,

terminar, por la entidad BSF, un proceso de autenticación en curso si la entidad BSF no memoriza la identidad privada del usuario; o enviar, por la entidad BSF, una indicación de error al UE y acabar un proceso de autenticación en curso si la entidad BSF no memoriza la identidad privada del usuario.

20. El método según la reivindicación 17, en donde la primera identidad temporal es una identidad temporal (TMPI) y la segunda identidad temporal es un Identificador de Transacción de Inicialización (B-TID).

21. Una entidad de función de servicio de inicialización (BSF), caracterizada por cuanto que comprende:

un procesador, configurado para realizar una autenticación mutua con un equipo de usuario (UE) utilizando una identidad temporal o una identidad privada del usuario enviada desde el UE y para generar una primera identidad temporal y una segunda identidad temporal, en donde la primera identidad temporal es diferente de la segunda identidad temporal y las primera y segunda identidades temporales son diferentes de la identidad temporal o de la identidad privada del usuario;

un transmisor, configurado para enviar una de entre la primera identidad temporal y la segunda identidad temporal al UE y para enviar una indicación de generación de identidad temporal al UE, en donde la indicación de generación de identidad temporal se utiliza para dar instrucciones al UE para generar otra de entre primera identidad temporal y la segunda identidad temporal utilizando una misma manera que la entidad BSF y

un receptor, configurado para recibir una demanda de re-autenticación que incluye la primera identidad temporal desde el UE;

en donde el UE está configurado, además, para enviar una demanda de servicio que incluye la segunda identidad temporal a una entidad de función de aplicación de red (NAF).

22. La función BSF según la reivindicación 21, en donde:

el procesador está configurado, además, para generar una de entre la primera identidad temporal y la segunda identidad temporal utilizando un valor aleatorio RAND, de forma aleatoria y la otra de entre la primera identidad temporal y la segunda identidad temporal utilizando una clave obtenida en la autenticación mutua;

en donde el equipo UE está configurado, además, para generar la otra de entre la primera identidad temporal y la segunda identidad temporal usando la clave obtenida en la autenticación mutua.

23. La función BSF según la reivindicación 21, que comprende, además:

el receptor que está configurado, además, para recibir una demanda de autenticación desde el UE, en donde la demanda de autenticación incluye la identidad temporal;

el procesador que está configurado, además, para determinar si la entidad BSF memoriza una identidad privada del usuario correlativamente con la identidad temporal y

el procesador que está configurado, además, para demandar a un servidor de abonado residencial (HSS) información de autenticación por intermedio de la identidad privada del usuario si la entidad BSF memoriza la identidad privada del usuario o

el procesador que está configurado, además, para terminar un proceso de autenticación en curso si la entidad BSF no memoriza la identidad privada del usuario; o para enviar una indicación de error al equipo UE y terminar un proceso de autenticación en curso si la entidad BSF no memoriza la identidad privada del usuario.

24. La función BSF según la reivindicación 21, en donde la primera identidad temporal es una identidad temporal (TMPI) y la segunda identidad temporal es un Identificador de Transacción de Inicialización (B-TID).

25. Un medio de soporte legible por ordenador que comprende un programa informático, memorizado en un soporte no transitorio, que se caracteriza por cuanto que se ejecuta por una unidad de ordenador, lo que hará que la unidad de ordenador realice las etapas de una entidad de Función de Servicio de Inicialización (BSF) según cualquiera de las reivindicaciones 1 a 4, 9 a 12, 17 a 20.

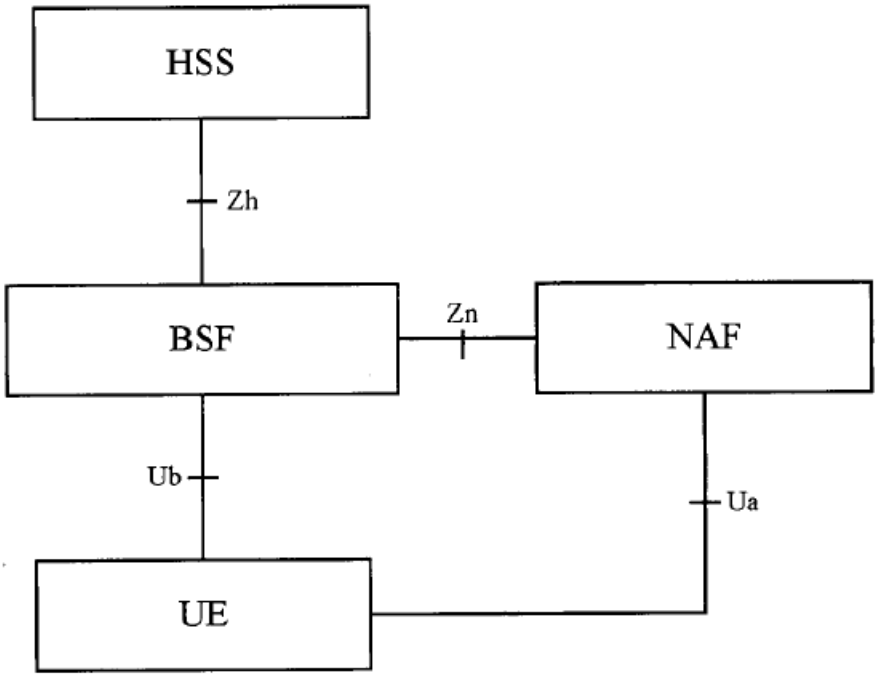

Figura 1

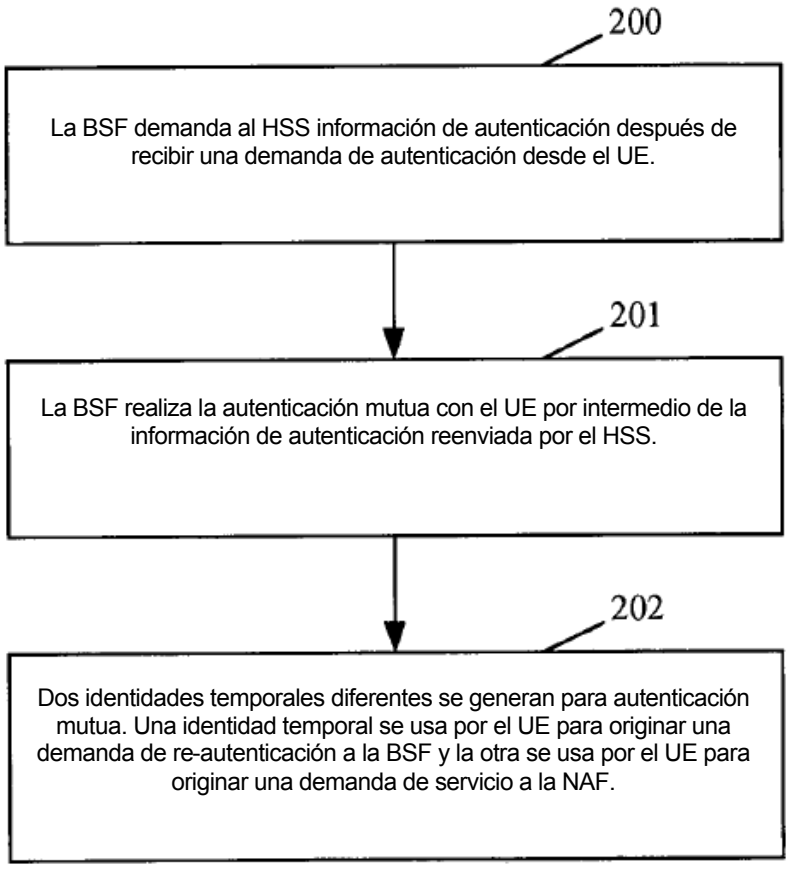

Figura 2

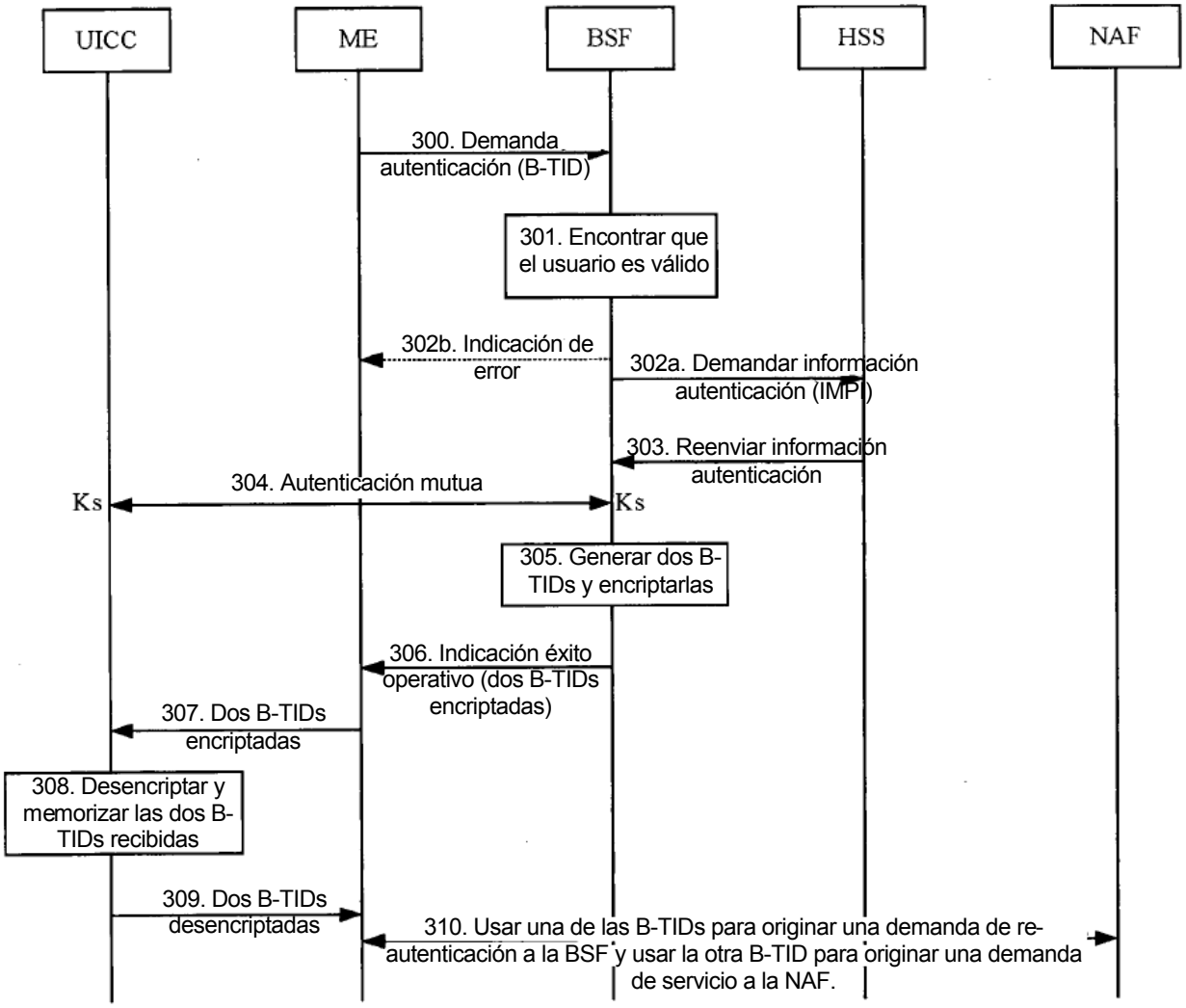
UICC
ME
BSF
HSS
NAF
300. Demanda autenticación (B-TID)
301. Encontrar que el usuario es válido
302b. Indicación de error
302a. Demandar información autenticación (IMPI)
303. Reenviar información autenticación
304. Autenticación mutua
Ks
Ks
305. Generar dos B-TIDs y encriptarlas
306. Indicación éxito operativo (dos B-TIDs encriptadas)
307. Dos B-TIDs encriptadas
308. Desencriptar y memorizar las dos B-TIDs recibidas
309. Dos B-TIDs desencriptadas
310. Usar una de las B-TIDs para originar una demanda de re-autenticación a la BSF y usar la otra B-TID para originar una demanda de servicio a la NAF.

Figura 3