(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 687 238**

(51) Int. CI.:

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

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **25.02.2008 PCT/EP2008/001479**

(87) Fecha y número de publicación internacional: **03.09.2009 WO09106091**

(96) Fecha de presentación y número de la solicitud europea: **25.02.2008 E 08716023 (0)**

(97) Fecha y número de publicación de la concesión europea: **11.07.2018 EP 2248317**

(54) Título: **Método de arquitectura de arranque de seguro basado en autenticación de resumen basada en contraseña**

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
24.10.2018

(73) Titular/es:

NOKIA SOLUTIONS AND NETWORKS OY (100.0%)
Karaportti 3
02610 Espoo, FI

(72) Inventor/es:

BLOMMAERT, MARC y
HORN, GÜNTHER

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Método de arquitectura de arranque de seguro basado en autenticación de resumen basada en contraseña

Campo de la invención

La presente invención se refiere a un método y aparato para realizar autenticación entre un cliente y un servidor, y más específicamente a un mecanismo de arranque seguro basado en la autenticación de resumen del Protocolo de Transferencia de Hipertexto (HTTP) basado en contraseña.

Antecedentes de la invención

La seguridad de los terminales móviles, tales como los dispositivos de comunicación portátiles (por ejemplo, teléfonos celulares o equipos de usuario (UE)), asistentes digitales personales, ordenadores portátiles, o cualquier dispositivo adecuado que pueda comunicar con una red inalámbrica, es cada vez más importante para los usuarios de terminales móviles. Los algoritmos de seguridad pueden emplearse para conseguir seguridad entre un terminal móvil y otra entidad de red. Estos algoritmos de seguridad a menudo se basan en un secreto que se comparte entre el terminal móvil y la otra entidad de red que permite que se autentique el terminal móvil. Normalmente, este secreto compartido se incorpora en forma de una clave.

Una función de servidor de arranque (BSF) es un elemento intermediario en redes celulares que proporciona funciones independientes de aplicación para autenticación mutua de terminales móviles y servidores que son conocidos entre sí y para arrancar el intercambio de claves de sesión secretas posteriormente. Esto permite el uso de servicios adicionales que necesitan autenticación y comunicación segura. En este caso, el término “arranque” está relacionado con crear una relación de seguridad con un dispositivo previamente desconocido en primer lugar y permitir instalar elementos de seguridad (por ejemplo claves) en el dispositivo y la BSF posteriormente. La configuración y función para desplegar una relación de seguridad genérica a menudo se denomina arquitectura de arranque genérica (GBA) o arquitectura de autenticación genérica (GAA).

La GBA como se especifica en la especificación TS 33.220 del protocolo de asociación de la 3ª generación (3GPP) está actualmente basada en el hecho de que un usuario está en posesión de un módulo de identidad de usuario (por ejemplo una tarjeta de circuito integrado universal (UICC) o módulo de identidad de abonado (SIM)) en el que puede ejecutarse un mecanismo de autenticación y acuerdo de clave (AKA). La GBA ha definido un mecanismo genérico que permite, basándose en una ruta secreta almacenada en el módulo de identidad de usuario, generar y usar secretos derivados entre el UE y diferentes aplicaciones en una red. El mecanismo de GBA permite que diferentes aplicaciones en las redes y terminales eviten una gran diversidad de mecanismos de autenticación y permite tratar problemas de seguridad de una vez de manera consistente.

La autenticación para servidores de aplicación basados en HTTP de propiedad de operadores de redes fijas así como la misma red está principalmente basada en contraseña. Por lo tanto, los operadores de red que poseen únicamente acceso fijo pueden no desear introducir módulos de identidad de usuario para los clientes únicamente para el fin de GBA. Desarrollar una GBA basada en contraseña ayudaría a estos operadores. El mecanismo de GBA es útil, ya que puede restringir el número de contraseñas almacenadas en la red y para gestionarse por el usuario.

Un ejemplo de autenticación de cliente para el que la comunicación segura es altamente deseable es la autenticación de acceso de resumen de HTTP que verifica que tanto cliente como servidor conocen un secreto compartido (por ejemplo contraseña de HTTP). Después de la verificación, se comienzan las comunicaciones seguras entre el cliente y el servidor. El esquema de autenticación de acceso de resumen de HTTP está basado en un paradigma de desafío-respuesta sencillo. El esquema implica un desafío que se emite al cliente que usa un valor de número aleatorio utilizado sólo una vez. En ingeniería de seguridad, un “número aleatorio utilizado sólo una vez” (nonce) de este tipo significa “número usado una vez” y es a menudo un número aleatorio o pseudo-aleatorio emitido en un protocolo de autenticación para asegurar que las comunicaciones anteriores no pueden reusarse en ataques de reproducción. En la autenticación de acceso de resumen de HTTP, se usan números aleatorios utilizados sólo una vez para calcular un resumen al que se ha aplicado una función de troceo de una contraseña. La aplicación de función de troceo puede basarse en una aplicación de, por ejemplo, la función de troceo criptográfica MD-5. Los números aleatorios utilizados sólo una vez son diferentes cada vez que se presenta un código de respuesta de desafío de autenticación, y cada solicitud de cliente tiene un número de secuencia único, haciendo por lo tanto el ataque de reproducción virtualmente imposible. Una respuesta de HTTP válida al desafío verifica el conocimiento del secreto compartido.

De acuerdo con un mecanismo de autenticación conocido para usar la GBA basándose en el resumen de HTTP (también conocido como GBA_H), se requieren cambios a los exploradores convencionales que incluyen seguridad de capa de transacción (TLS), de modo que el UE y la BSF pueden acceder al secreto maestro de TLS para uso en la GBA. Adicionalmente, el mecanismo de GBA_H es vulnerable a un ataque de Hombre en el Medio (MITM) donde el atacante ejecuta una sesión de TLS con la BSF e interactúa con el UE mediante HTTP fuera del túnel de TLS. El MITM necesita engañar al UE en comunicación con el MITM usando el resumen de HTTP fuera de TLS. Para

conseguir esto, el MITM podría ser un servidor corrupto o un servidor instalado adicional, y el usuario podría ser engañado (por ejemplo por técnicas de correo electrónico y/o ingeniería social) para contactar con el servidor de MITM requiriendo que el usuario ejecute el resumen de HTTP. Adicionalmente, los usuarios no siempre tienen conocimiento de cuándo se requiere una conexión segura o activa en su explorador.

Adicionalmente, se describe una solución de GBA 2G en el anexo I de TS 33.220 y usa TLS entre el UE y la BSF. Esta solución asegura que la entropía de la clave arrancada es mayor que la entropía que puede alcanzarse usando un vector de autenticación 2G. Al mismo tiempo, esta solución no es vulnerable al ataque MITM. La clave arrancada se deriva desde tanto el resultado de autenticación como alguna información que se transmite dentro del túnel de TLS. Sin embargo, la GBA 2G usa la AKA de resumen de HTTP para autenticación y por lo tanto requiere que el secreto raíz se almacene de manera segura en un módulo de identidad de usuario.

Por lo tanto, sería deseable un mecanismo de arranque seguro basado en autenticación de resumen de HTTP basada en contraseña, que alivie al menos una de las desventajas de susceptibilidad a vulnerabilidades de las soluciones basadas en resumen de HTTP conocidas, ausencia de renovación de clave para la clave arrancada, ausencia de confidencialidad directa debido a la divulgación de contraseña y su efecto en una clave arrancada generada antes del compromiso de contraseña, y el requisito del explorador adicional para interfaces de pila de seguridad de capa de transacción.

El documento US2008016230 (A1) desvela un equipo de usuario en un sistema de comunicaciones, comprendiendo el equipo de usuario: una memoria dispuesta para almacenar al menos un identificador asociado con el equipo de usuario; un transceptor dispuesto para comunicar con un nodo en el sistema de comunicación, en el que el transceptor está dispuesto para recibir el al menos un identificador desde el nodo en el sistema de comunicaciones, en el que el al menos un identificador se usa por el equipo de usuario para autenticar el equipo de usuario a al menos un nodo adicional en el sistema de comunicaciones.

Sumario

Es un objetivo de la presente invención proporcionar un mecanismo de arranque seguro basado en una autenticación de resumen basada en contraseña. El objetivo se consigue con la materia objeto de las reivindicaciones independientes.

Este objetivo se consigue mediante un método de arquitectura de arranque genérica, comprendiendo dicho método:

- autenticar un cliente a un servidor de arranque y establecer una clave compartida entre dicho cliente y dicho servidor de arranque;
- usar un procedimiento de autenticación de acceso de resumen basado en contraseña; generar una clave arrancada basándose en al menos un parámetro reciente no usado en una ejecución de protocolo anterior entre dicho cliente y dicho servidor, y asegurar dicho procedimiento de autenticación usando una función de derivación de clave que calcula un parámetro de respuesta de resumen modificado usando la contraseña del usuario y un parámetro de respuesta de resumen como valores de entrada.

Adicionalmente, el objetivo anterior se consigue por una arquitectura de arranque genérica adaptada para autenticar un cliente a un servidor de arranque, para establecer una clave compartida entre dicho cliente y dicho servidor de arranque, para usar un procedimiento de autenticación de acceso de resumen basado en contraseña para dicha autenticación, medios de arranque para asegurar dicho procedimiento de autenticación generando una clave arrancada basándose en al menos un parámetro reciente no usado en una ejecución de protocolo anterior entre dicho cliente y dicho servidor, y medios de generación de respuesta para asegurar dicho procedimiento de autenticación usando una función de derivación de clave que calcula un parámetro de respuesta de resumen modificado usando la contraseña del usuario y un parámetro de respuesta de resumen como valores de entrada.
Por consiguiente, la autenticación del usuario está basada en un parámetro de respuesta de resumen modificado y una elección apropiada de parámetros de entrada para derivación de la clave arrancada. Los ataques de MITM pueden eliminarse de esta manera debido al hecho de que se asegura la implicación del usuario, de modo que el MITM no conoce la contraseña. Además, no se requieren características especiales a partir de la pila de TLS, de modo que se elimina la dependencia de capas de protocolo inferiores y la arquitectura global se hace más limpia y por lo tanto más flexible.
Los dos conceptos de modificar el parámetro de respuesta de resumen y generar la clave arrancada basándose en al menos un parámetro reciente se enlazan por el concepto común de proporcionar la implicación del usuario para mejorar la seguridad durante el intercambio de señalización de autenticación.

De acuerdo con un primer aspecto, el parámetro de respuesta de resumen puede modificarse aplicando una función de troceo a un nombre de usuario, la contraseña de usuario, y un valor de número aleatorio utilizado sólo una vez.

De acuerdo con un segundo aspecto, el parámetro de respuesta de resumen puede modificarse aplicando una función de troceo al parámetro de respuesta de resumen y la contraseña de usuario.

De acuerdo con un tercer aspecto, la clave arrancada puede generarse basándose en una contraseña y un parámetro de respuesta de resumen.

De acuerdo con un cuarto aspecto, la clave arrancada puede generarse aplicando una función de troceo a el al menos un parámetro reciente y un parámetro de cadena arbitrario.

De acuerdo con un quinto aspecto, la clave arrancada puede generarse aplicando la función de autenticación a el al menos un parámetro reciente, al parámetro de cadena arbitraria, y una contraseña.

En un ejemplo específico, la función de autenticación puede ser una función de derivación de clave usada en una arquitectura de arranque genérica.

El al menos un parámetro reciente puede comprender valores de número aleatorio utilizado sólo una vez intercambiados entre el cliente y el servidor. Como alternativa, el al menos un parámetro reciente puede comprender un parámetro de respuesta de resumen. Como otra alternativa, el al menos un parámetro reciente puede comprender un número aleatorio específico de servidor.

El método de arquitectura de arranque genérica puede comprender adicionalmente modificar interfaces desde el servidor de arranque a un dispositivo terminal del cliente y a una base de datos de abonados, mientras se dejan las interfaces entre el servidor de arranque y una función de aplicación de red y entre la función de aplicación de red y el dispositivo terminal en conformidad con la especificación que subyace el procedimiento de autenticación de resumen basado en contraseña.

El cliente puede ser un dispositivo de terminal móvil y el servidor puede comprender una función de servidor de arranque.

Otras modificaciones ventajosas se definen en las reivindicaciones dependientes.

Breve descripción de los dibujos

La invención se describirá ahora en mayor detalle basándose en realizaciones con referencia a los dibujos adjuntos en las que:

La Figura 1 muestra una arquitectura esquemática de una infraestructura de autenticación en la que puede implementarse la presente invención;

La Figura 2 muestra un diagrama de bloques esquemático de una entidad de autenticación de acuerdo con las realizaciones;

La Figura 3 muestra un procesamiento esquemático y diagrama de señalización de un procedimiento de autenticación de acuerdo con una primera realización;

La Figura 4 muestra un procesamiento esquemático y diagrama de señalización de una arquitectura de autenticación de acuerdo con una segunda realización;

La Figura 5 muestra un procesamiento esquemático y diagrama de señalización de un procedimiento de autenticación de acuerdo con una tercera realización; y

La Figura 6 muestra un diagrama de bloques esquemático de una implementación basada en software de acuerdo con una cuarta realización de la presente invención.

Descripción de las realizaciones

A continuación, las realizaciones de la presente invención se describirán basándose en una infraestructura de autenticación de GBA que está basada en un mecanismo de resumen de HTTP para establecer credenciales, es decir, derivar la clave o claves de sesión entre un cliente y un servidor.

La Figura 1 muestra un diagrama de bloques esquemático de la arquitectura de autenticación con las entidades implicadas en un enfoque de arranque sugerido. Esta arquitectura implica que un equipo de usuario (UE) 10, por ejemplo un teléfono celular móvil o similares, necesita acceso a un servicio específico, un servidor de aplicación 30 (por ejemplo una función de aplicación de red (NAF)), que proporciona el servicio, una BSF genérica 20 que dispone una relación de seguridad entre el UE y el servidor de aplicación, y una base de datos de abonados del operador de la red móvil 50 (por ejemplo un servidor de abonado doméstico (HSS)), que aloja perfiles de usuario.

De acuerdo con la Figura 1, la BSF 20 y el UE 10 se autentican mutuamente y acuerdan claves de sesión que pueden aplicarse posteriormente entre el UE 10 y la NAF 30. La BSF 20 puede restringir la aplicabilidad del material

de clave a una NAF específica usando un procedimiento de derivación de clave que puede usarse con múltiples NAF durante el tiempo de vida del material de clave. Este tiempo de vida del material de clave se establece de acuerdo con una política local de la BSF 20. La BSF 20 puede obtener ajustes de seguridad de usuario de GBA desde el HSS 50.

Después de que se haya completado el arranque, el UE 10 y la NAF 30 puede ejecutar algún protocolo específico de aplicación donde la autenticación de mensajes estará basada en aquellas claves de sesión generadas durante la autenticación mutua entre el UE 10 y la BSF 20. El conjunto de todos los ajustes de seguridad de usuario se almacena en el HSS 50. En casos donde el abonado tenga múltiples suscripciones, el HSS 50 puede contener uno o más ajustes de seguridad que pueden mapearse a una o más identidades privadas.

Adicionalmente, puede proporcionarse una función de localizador de abonado (SLF) 40, que se consulta por la BSF 20 en conjunto con una operación de interfaz Zh para obtener el nombre del HSS 50 que contiene datos específicos de abonado requeridos. La SLF 40 se accede mediante una interfaz Dz. La SLF 40 no se requiere en un único entorno de HSS o cuando la BSF 20 está configurada para usar un HSS predefinido.

El punto de referencia Ub entre el UE 10 y la BSF 20 proporciona autenticación mutua entre el UE 10 y la BSF 20. Permite que el UE 10 arranque las claves de sesión. Adicionalmente, el punto de referencia Ua entre el UE 10 y la NAF 30 lleva el protocolo de aplicación, que se asegura usando el material de clave acordado entre el UE 10 y la BSF 20 como resultado de la autenticación de resumen de HTTP a través del punto de referencia Ub. Adicionalmente, el punto de referencia Zh usado entre la BSF 20 y el HSS 50 permite que la BSF 20 extraiga la información de autenticación requerida y todos los ajustes de seguridad de usuario de GBA desde el HSS 50. Finalmente, el punto de referencia Zn puede usarse por la NAF 30 para extraer el material de clave acordado durante un protocolo de autenticación de resumen de HTTP anterior ejecutado a través del punto de referencia Ub desde el UE 10 a la BSF 20. Puede usarse también para extraer ajustes de seguridad de usuario específicos de aplicación desde la BSF 20, si se solicita por la NAF 30.

La Figura 2 muestra un diagrama de bloques esquemático de una entidad de autenticación que puede proporcionarse en el UE 10 o en la BSF 20 en la Figura 1. La entidad de autenticación comprende un módulo de generación de respuesta (RGM) 43, un módulo de aprovisionamiento de contraseña (PPM) 42, y un módulo de generación de contraseña de HTTP que puede emplear, por ejemplo, una GBA 41. LA GBA 41 es una arquitectura de estructura que permite el arranque (o cambio) de una clave de seguridad entre el UE 10 y la BSF 20, que puede usarse a continuación para derivar adicionalmente claves de seguridad para su uso entre el UE 10 y la NAF 30. Más específicamente, la GBA 41 genera la contraseña de HTTP y envía la contraseña de HTTP al PPM 42. El PPM 42 almacena la contraseña de HTTP para todas las aplicaciones de HTTP.

En la operación, cuando una aplicación de cliente de HTTP 45 requiere una respuesta de HTTP para establecer comunicaciones seguras con un elemento de procesamiento (no mostrado) en el otro extremo de conexión, la aplicación de cliente de HTTP 45 envía una solicitud al RGM 43. La solicitud comprende información que incluye una identidad de aplicación, un nombre de usuario, opcionalmente una función de troceo de una carga útil de HTTP si se requiere protección de integridad de carga útil, y un valor de número aleatorio utilizado sólo una vez, todos los cuales se reciben desde el elemento de procesamiento que pueden incluir un servidor de HTTP. Siguiendo la recepción de la solicitud, el RGM 43 solicita la contraseña de HTTP desde el PPM 42. El PPM 42 envía la contraseña de HTTP al RGM 43 que a continuación envía una respuesta de HTTP a la aplicación de cliente de HTTP 45 para permitir el establecimiento de comunicaciones seguras con el elemento de procesamiento.

En una operación para verificación de una respuesta de resumen de servidor, se proporciona un módulo de verificación de respuesta 44. Si se recibe una respuesta de resumen de servidor por la aplicación de cliente de HTTP 45, se envía una solicitud de verificación al RVM 44. La solicitud de verificación comprende información que incluye la respuesta de resumen de servidor y opcionalmente un cuerpo de entidad al que se ha aplicado una función de troceo y un valor de número aleatorio utilizado sólo una vez de cliente (valor de número aleatorio utilizado sólo una vez de cliente (cnonce)), etc. El RVM 44 a continuación solicita la contraseña de HTTP desde el PPM 42. El PPM 42 envía la contraseña de HTTP al RVM 44 que a continuación genera una respuesta de resumen de servidor calculada de acuerdo con un algoritmo de seguridad o función de seguridad. El RVM 44 a continuación comprueba la validez de la respuesta de resumen de servidor en comparación con la respuesta de resumen de servidor calculado y envía los resultados de verificación a la aplicación de cliente de HTTP 45 para verificar la respuesta de resumen de servidor.

La entidad de autenticación de la Figura 2 puede implementarse por circuitos de hardware discretos en un único chip o un conjunto de chips o un módulo, o puede implementarse basándose en rutinas de software que proporcionan las funciones de los bloques 41 a 45.

De acuerdo con las siguientes realizaciones, un mecanismo de arranque seguro basado en el resumen de HTTP basado en contraseña se proporciona por al menos una de una autenticación de un usuario basada en al menos una respuesta de resumen modificada y una elección apropiada de parámetros de entrada para la derivación de clave. Adicionalmente, el protocolo Ub puede ejecutarse a través de TLS con autenticación de la BSF 20 basándose en

certificados de servidor.

De acuerdo con una primera realización, el protocolo en la interfaz Ub se modifica de modo que - en lugar de devolver un parámetro resumen-respuesta = H(nombre de usuario, contraseña, valor de número aleatorio utilizado sólo una vez, ...), como se especifica en el resumen de HTTP convencional (donde H es una función de troceo, por ejemplo MD-5) - el UE 10 devuelve un parámetro resumen-GBA-respuesta = H*(resumen-respuesta, contraseña, ...) a la BSF 20, donde el resumen-respuesta es el resumen-respuesta de HTTP convencional y H* es otra función de troceo (por ejemplo la función de derivación de clave (KDF) usada en GBA). De esta manera se asegura la implicación del usuario apropiada, de modo que el MITM no tiene conocimiento de la contraseña.

La Figura 3 muestra un procesamiento a modo de ejemplo y esquemático y diagrama de señalización de la primera realización.

En una etapa inicial 0 el UE 10 inicia el procedimiento de arranque iniciando una sesión de TLS con la BSF 20. El UE 10 y la BSF 20 negocian un TLS autenticado únicamente del lado de servidor. El UE 10 autentica la BSF 20 por un certificado presentado por la BSF 20. La BSF 20 no requiere autenticación desde el UE 10 en este punto. Después de la negociación de TLS, el UE 10 envía un mensaje de solicitud de HTTP a la BSF 20, que contiene una entidad de usuario privada en un encabezamiento de autenticación de la misma (etapa 1). En respuesta a lo mismo, se realiza recuperación de datos desde el HSS 50 en la etapa 2. Más específicamente, la BSF 20 envía una consulta al HSS 50 para recuperar una contraseña, una contraseña resumida, o un vector de autenticación de resumen (D-AV) para el usuario. El D-AV consiste en el valor “qop” (calidad de protección), el algoritmo de autenticación, dominio, y una función de troceo, denominada H(A1), de la IMPI (Identidad Privada Multimedia de IP, es decir una entidad de usuario privada), dominio y contraseña. Se hace referencia a RFC 2617 para información adicional sobre los valores en el vector de autenticación para autenticación basada en resumen de SIP.

El HSS 50 responde con el vector de autenticación apropiado para el usuario y un algoritmo. Los contenidos del vector de autenticación permiten que la BSF 20 calcule un desafío para el UE 10.

En la etapa 3, la BSF 20 responde a la solicitud del UE con un mensaje 401 No autorizado que comprende un encabezamiento de WWW-autenticar para forzar al UE 10 a autenticarse a sí mismo. El encabezamiento de WWW-autenticar incluye diversos parámetros de autenticación, tales como un parámetro de resumen-respuesta. A continuación, en la etapa 4, el cliente en el UE 10 genera un parámetro de resumen-GBA-respuesta modificado para la respuesta de autenticación. De esta manera, puede mejorarse la autenticación de usuario para contrarrestar un ataque de MITM. El parámetro de resumen-GBA-respuesta modificado ya no puede calcularse simplemente desde el conocimiento del resumen-respuesta de parámetro incluido en el encabezamiento de WWW-autenticar. En la etapa 5, el cliente envía el parámetro de resumen-GBA-respuesta modificado a través del túnel de TLS a la BSF 20. La BSF 20 comprueba la respuesta para la corrección en la etapa 6. Posteriormente, en la etapa 7, la BSF 20 deriva una clave arrancada (o clave de GBA) Ks y envía un mensaje 200 OK que incluye el tiempo de vida de la clave y un identificador de transacción de arranque (B-TID) al UE 10 para indicar autenticación satisfactoria. Finalmente, en la etapa 9, el cliente en el UE 10 también deriva la clave arrancada Ks.

El parámetro de resumen-GBA-respuesta puede calcularse en la etapa 4 basándose en la ecuación:

resumen-GBA-respuesta = KDF (para1, para2, ...),

en el que *para1*, *para2*, ... son parámetros y *KDF* indica una función de derivación de clave. Uno de estos parámetros puede ser la contraseña, y otro parámetro puede ser una función del parámetro de número aleatorio utilizado sólo una vez, como se define por ejemplo en la especificación del IETF RFC 2617. La inclusión de la contraseña en la función de troceo anterior (por ejemplo función de KDF) se usa para comprobar la implicación del usuario y evitar de esta manera la suplantación de cliente, y la inclusión del parámetro de número aleatorio utilizado sólo una vez o una función del mismo evita la reproducción de mensajes de respuesta en la interfaz Ub.

De acuerdo con una primera implementación de ejemplo de la primera realización, el parámetro de resumen-GBA-respuesta puede calcularse basándose en la siguiente ecuación:

resumen-GBA-respuesta = KDF (*contraseña*, *resumen-respuesta*, *“gba-resumen-autenticación de 3GPP”*),

en el que la contraseña y el parámetro de resumen-respuesta pueden corresponder a RFC 2617, y el parámetro “*gba-resumen-autenticación de 3GPP* “ puede ser una cadena de texto.

En otro ejemplo de implementación, el parámetro resumen-GBA-respuesta puede calcularse como sigue:

resumen-GBA-respuesta = KDF (*nombre de usuario*, *contraseña*, *valor de número aleatorio utilizado sólo una vez*),

en el que *KDF* puede ser diferente de la función de derivación de clave MD-5 usada en RFC 2617.

Por supuesto, pueden usarse otras combinaciones de parámetros también en la primera realización preferida.

La generación o cálculo del parámetro resumen-GBA-respuesta puede realizarse en el RGM 43 de la entidad de autenticación mostrada en la Figura 2.

La Figura 4 muestra un procesamiento esquemático y diagrama de señalización de acuerdo con una segunda realización y de acuerdo con la invención, donde la clave arrancada o GBA Ks se deriva desde valores de número aleatorio utilizado sólo una vez intercambiados a través de la conexión de TLS segura. Las etapas del procedimiento mostrado en la Figura 4 corresponden principalmente a aquellas en la Figura 3, de modo que únicamente se explican las etapas diferentes a continuación.

La clave GBA Ks puede calcularse como sigue:

*Ks = H** ("*gba-ks-resumen de 3gpp*", *valor de número aleatorio utilizado sólo una vez*, *valor de número aleatorio utilizado sólo una vez de cliente*, ...).

en el que la primera cadena "*gba-ks-resumen de 3gpp*" tiene un valor elegido arbitrariamente para distinguir esta forma particular de derivación de clave de otros tipos de derivaciones de clave.

En las etapas 4 y 5, el parámetro de resumen-respuesta modificado se calcula y reenvía para evitar el ataque MITM. De esta manera, la segunda realización se crea sobre la primera realización y la mejora no derivando Ks desde el secreto maestro de TLS y eliminando por lo tanto la necesidad de tener una interfaz a la pila de TLS. Sin embargo, al contrario del procedimiento de la primera realización preferida, se derivan las claves arrancadas o GBA en las etapas 7 y 9 basándose en valores de número aleatorio utilizado sólo una vez intercambiados. Esta manera modificada de derivar la clave GBA Ks permite evitar el explorador adicional a interfaces de pila de TLS. Por supuesto, la autenticación de usuario mejorada basada en el parámetro de resumen-GBA-respuesta modificado puede usarse también en la segunda realización. Sin embargo, también puede prescindirse de esto.

De acuerdo con la segunda realización, se asegura que la clave GBA Ks es una función de un parámetro reciente, es decir un parámetro no usado en una ejecución de protocolo anterior, intercambiado a través de la conexión de TLS encriptada entre el usuario y la BSF 20.

De acuerdo con un ejemplo de la primera implementación de la segunda realización, la renovación puede conseguirse a través de una combinación de los dos parámetros valor de número aleatorio utilizado sólo una vez y valor de número aleatorio utilizado sólo una vez de cliente. El uso del parámetro de número aleatorio utilizado sólo una vez (un valor generado de manera única por el servidor y usado como un desafío por el cliente) garantiza la renovación de la clave GBA Ks a la BSF 20. Adicionalmente, el uso del parámetro valor de número aleatorio utilizado sólo una vez de cliente (un valor generado de manera única por el cliente que en este punto añade la renovación a la clave GBA Ks) garantiza la renovación de la clave GBA Ks al usuario (cliente). Como un ejemplo de implementación, la clave GBA Ks podría derivarse basándose en la siguiente ecuación:

Ks = KDF ("gba-ks-resumen de 3gpp", número aleatorio utilizado sólo una vez, número aleatorio utilizado sólo una vez de cliente, ...)

De acuerdo con un segundo ejemplo de implementación, la contraseña y el resumen-respuesta de parámetro puede usarse en lugar de los parámetros número aleatorio utilizado sólo una vez y número aleatorio utilizado sólo una vez de cliente para derivar la clave GBA Ks. Se observa que el parámetro de resumen-respuesta se deriva desde tanto el parámetro número aleatorio utilizado sólo una vez como el número aleatorio utilizado sólo una vez de cliente.

En este caso, la clave GBA Ks se deriva basándose en la siguiente ecuación:

Ks = KDF ("gba-ks-resumen de 3gpp", contraseña, resumen-respuesta, ...).

En un tercer ejemplo de implementación, un valor "Ks-entrada" como se especifica en el anexo 1 de TS 33.220 y enviado por la BSF 20 junto con el parámetro de número aleatorio utilizado sólo una vez podría usarse como entrada a la derivación de la clave de GBA Ks. En este caso, Ks podría incluso establecerse igual a este valor "Ks-entrada".

La Figura 5 muestra un diagrama de señalización y procesamiento esquemático de acuerdo con una tercera realización, en la que el uso de TLS puede descartarse para hacer de esta manera la solución muy sencilla. Sin embargo, una brecha de la contraseña puede hacer conocidas todas las claves GBA Ks anteriores si los arranques en la interfaz Ub se grabaran por un atacante.

Se supone que la BSF 20 se autentica por medio de la autenticación mutua, es decir usando el parámetro respuesta-resumen en el encabezamiento de información de autenticación, por ejemplo como se especifica en RFC 2617. Por lo tanto, la mayoría de las etapas de la Figura 5 corresponden a aquellas de la Figura 4 con la excepción

de que la etapa 0 de TLS se ha omitido. Sin embargo, la derivación de la clave GBA Ks en las etapas 7 y 9 se mejora adicionalmente asegurando que se implica un secreto compartido, es decir la contraseña. Por lo tanto, la clave GBA Ks puede calcularse usando la siguiente ecuación:

Ks = H ("gba-ks-resumen de 3gpp", contraseña, valor de número aleatorio utilizado sólo una vez, valor de número aleatorio utilizado sólo una vez de cliente, ...).*

Más específicamente, cuando la función de troceo es la KDF y no se ven implicados parámetros adicionales, la ecuación se vuelve:

Ks = KDF ("gba-ks-resumen de 3gpp", contraseña, valor de número aleatorio utilizado sólo una vez, valor de número aleatorio utilizado sólo una vez de cliente)

con un uso directo de los parámetros valor de número aleatorio utilizado sólo una vez, valor de número aleatorio utilizado sólo una vez de cliente.

De acuerdo con otro ejemplo de implementación, la contraseña podría combinarse con el parámetro de resumen-respuesta, de modo que el cálculo de la clave GBA Ks está basado en la siguiente ecuación:

Ks = KDF ("gba-ks-resumen de 3gpp", contraseña, resumen-respuesta).

Por consiguiente, la contraseña proporciona el secreto requerido y por lo tanto evita que un MITM o un tercero pueda calcular la clave de GBA Ks, puesto que tanto el valor de número aleatorio utilizado sólo una vez y número aleatorio utilizado sólo una vez de cliente pueden estar disponibles para una tercera parte. El parámetro resumen-respuesta o los parámetros número aleatorio utilizado sólo una vez y número aleatorio utilizado sólo una vez de cliente proporcionan la renovación requerida.

Las etapas de derivación de clave 7 y 9 en las Figuras 3 a 5 pueden realizarse en la GBA 41 de la Figura 2 basándose en los parámetros requeridos que pueden entregarse por el RVM 44.

La Figura 6 muestra un diagrama de bloques esquemático de una implementación basada en software alternativa de acuerdo con una cuarta realización. Las funcionalidades descritas pueden implementarse en cualquier entidad de autenticación (que puede proporcionarse en el UE 10 o la BSF 20) con una unidad de procesamiento 410, que puede ser cualquier procesador o dispositivo informático con una unidad de control que realiza control basándose en rutinas de software de un programa de control almacenado en una memoria 412. El programa de control puede almacenarse también de manera separada en un medio legible por ordenador. Las instrucciones de código de programa se extraen desde la memoria 412 y se cargan en la unidad de control de la unidad de procesamiento 410 para realizar las etapas de procesamiento de las funcionalidades anteriores de las Figuras 2 a 5, que pueden implementarse como las rutinas de software anteriormente mencionadas. Las etapas de procesamiento pueden realizarse basándose en datos de entrada Dl y pueden generar datos de salida DO. Los datos de entrada Dl pueden corresponder a los parámetros de autenticación mencionados en las ecuaciones anteriores para calcular la clave de GBA Ks o el parámetro de resumen-GBA-respuesta, y los datos de salida DO pueden corresponder a la clave de GBA Ks o el parámetro de resumen-GBA-respuesta.

En consecuencia, las realizaciones anteriores pueden implementarse como un producto de programa informático que comprende medios de código para generar cada etapa individual de los procedimientos de señalización de las Figuras 3 a 5 para la respectiva entidad de autenticación cuando se ejecutan en un dispositivo informático o procesador de datos de la respectiva entidad de autenticación en el UE 10 o la BSF 20 o cualquier dispositivo terminal correspondiente o entidad de red.

En resumen, se ha descrito un método, aparatos, y producto de programa informático, en el que se usa un procedimiento de autenticación de acceso de resumen basado en contraseña para realizar autenticación entre un cliente y un servidor, en el que el procedimiento de autenticación se asegura por al menos uno de modificación de un parámetro de resumen-respuesta con una contraseña de usuario y generación de una clave arrancada basándose en la contraseña de usuario y al menos un parámetro reciente no usado en una ejecución de protocolo anterior entre el cliente y el servidor.

Es evidente que la invención puede aplicarse fácilmente a cualquier servicio y entorno de red (fijo e inalámbrico), donde se use un procedimiento de autenticación de acceso de resumen basado en contraseña. Puede usarse en relación con cualquier autenticación entre un cliente y un servidor. Más específicamente, la BSF 20 puede ser también cualquier servidor de autenticación, autorización y contabilidad (AAA) o cualquier otro nodo de conexión con una BSF o funcionalidad AAA. Las realizaciones pueden por lo tanto variar dentro del alcance de las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un método de arquitectura de arranque genérica (41), comprendiendo dicho método:

autenticar un cliente (44) a un servidor de arranque y establecer una clave compartida entre dicho cliente (44) y dicho servidor de arranque;
usar un procedimiento de autenticación de acceso de resumen basado en contraseña para dicha autenticación;
generar una clave arrancada basándose en al menos un parámetro reciente no usado en una ejecución de protocolo anterior entre dicho cliente y dicho servidor, **caracterizado** por que el método comprende
asegurar dicho procedimiento de autenticación usando una función de derivación de clave que calcula un parámetro de respuesta de resumen modificado usando la contraseña del usuario y un parámetro de respuesta de resumen como valores de entrada.

2. El método de acuerdo con la reivindicación 1, que comprende adicionalmente modificar interfaces desde dicho servidor de arranque a un dispositivo terminal de dicho cliente (44) y a una base de datos de abonados (50), mientras se dejan interfaces entre dicho servidor de arranque y una función de aplicación de red y entre dicha función de aplicación de red y dicho dispositivo de terminal en conformidad con la especificación que subyace a dicho procedimiento de autenticación de resumen basado en contraseña.

3. El método de acuerdo con las reivindicaciones 1 o 2, que comprende adicionalmente modificar dicho parámetro de respuesta de resumen

a.) aplicando una función de troceo a un nombre de usuario, dicha contraseña de usuario, y un valor de número aleatorio utilizado sólo una vez, o,
b.) aplicando una función de troceo a dicho parámetro de respuesta de resumen y dicha contraseña de usuario.

4. El método de acuerdo con las reivindicaciones 1 o 2, que comprende adicionalmente generar dicha clave arrancada aplicando una función de troceo a dicho al menos un parámetro reciente y un parámetro de cadena arbitrario.

5. El método de acuerdo con una cualquiera de las reivindicaciones anteriores, en el que dicho al menos un parámetro reciente comprende uno de valores de número aleatorio utilizado sólo una vez intercambiados entre dicho cliente (44) y dicho servidor, un parámetro de respuesta de resumen o un número aleatorio específico de servidor.

6. El método de acuerdo con una cualquiera de las reivindicaciones 2 a 5, en el que dicha función de troceo es una función de derivación de clave usada en una arquitectura de arranque genérica.

7. El método de acuerdo con una cualquiera de las reivindicaciones anteriores, en el que dicho cliente (44) es un dispositivo de terminal móvil (10) y dicho servidor comprende una función de servidor de arranque (20).

8. Un aparato de arquitectura de arranque genérica (41) adaptado para autenticar un cliente (44) a un servidor de arranque, para establecer una clave compartida entre dicho cliente (44) y dicho servidor de arranque, para usar un procedimiento de autenticación de acceso de resumen basado en contraseña para dicha autenticación, medios de arranque para asegurar dicho procedimiento de autenticación generando una clave arrancada basándose en al menos un parámetro reciente no usado en una ejecución de protocolo anterior entre dicho cliente (44) y dicho servidor, **caracterizado** por que el aparato comprende medios de generación de respuesta (43) para asegurar dicho procedimiento de autenticación usando una función de derivación de clave que calcula un parámetro de respuesta de resumen modificado usando la contraseña del usuario y un parámetro de respuesta de resumen como valores de entrada.

9. El aparato de acuerdo con la reivindicación 8, en el que dichos medios de generación de respuesta (43) están adaptados para modificar dicho parámetro de respuesta de resumen

a.) aplicando una función de troceo a un nombre de usuario, dicha contraseña de usuario y un valor de número aleatorio utilizado sólo una vez, o,
b.) aplicando una función de troceo a dicho parámetro de respuesta de resumen y dicha contraseña de usuario.

10. El aparato de acuerdo con una cualquiera de las reivindicaciones 8 a 9, en el que dichos medios de arranque (41) están adaptados para generar dicha clave arrancada aplicando una función de troceo a dicho al menos un parámetro reciente y un parámetro de cadena arbitrario.

11. El aparato de acuerdo con una cualquiera de las reivindicaciones 8 a 10, en el que dicho al menos un parámetro reciente comprende uno de valores de número aleatorio utilizado sólo una vez intercambiados entre dicho cliente (44) y dicho servidor, un parámetro de respuesta de resumen o un número aleatorio específico de servidor.

12. El aparato de acuerdo con una cualquiera de las reivindicaciones 8 a 11, en el que dicha función de troceo es una función de derivación de clave usada en una arquitectura de arranque genérica.

13. El aparato de acuerdo con una cualquiera de las reivindicaciones 8 a 12, en el que dicho cliente es un dispositivo de terminal móvil (10) y dicho servidor comprende una función de servidor de arranque.

14. Un dispositivo terminal, un dispositivo servidor o un módulo de chip **caracterizados** por comprender un aparato de acuerdo con la reivindicación 8.

15. Un producto de programa informático **caracterizado** por comprender medios de código para producir las etapas de cualquiera de las reivindicaciones de método 1-7 cuando se ejecuta en un dispositivo informático.

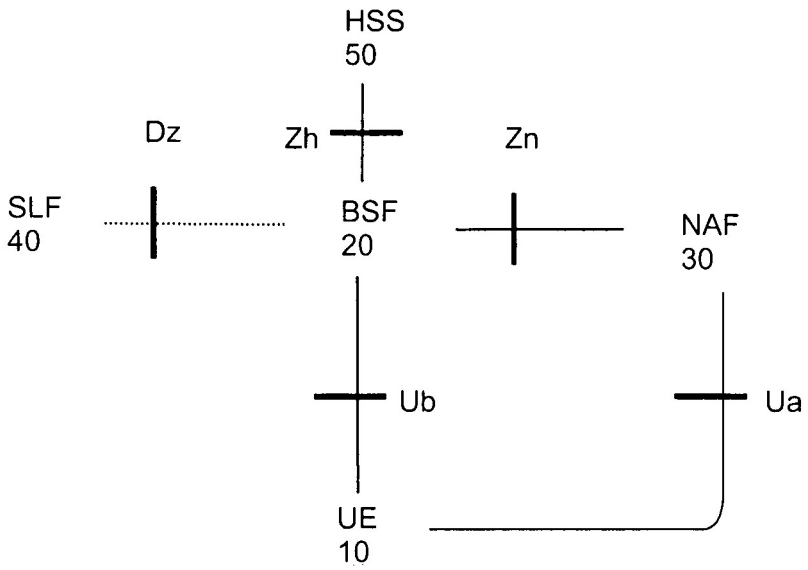
HSS
50
Dz
Zh
Zn
SLF
40
BSF
20
NAF
30
Ub
Ua
UE
10

Fig. 1

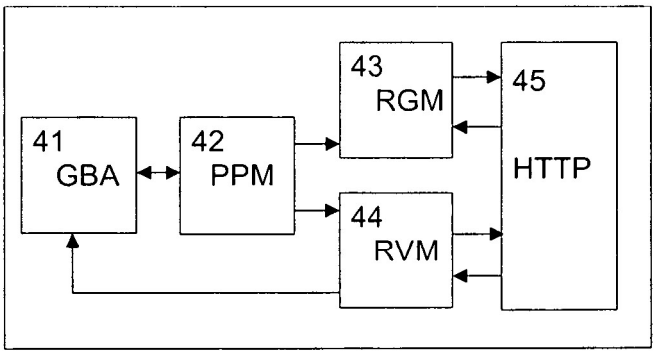
43
RGM
45
41
GBA
42
PPM
HTTP
44
RVM

Fig. 2

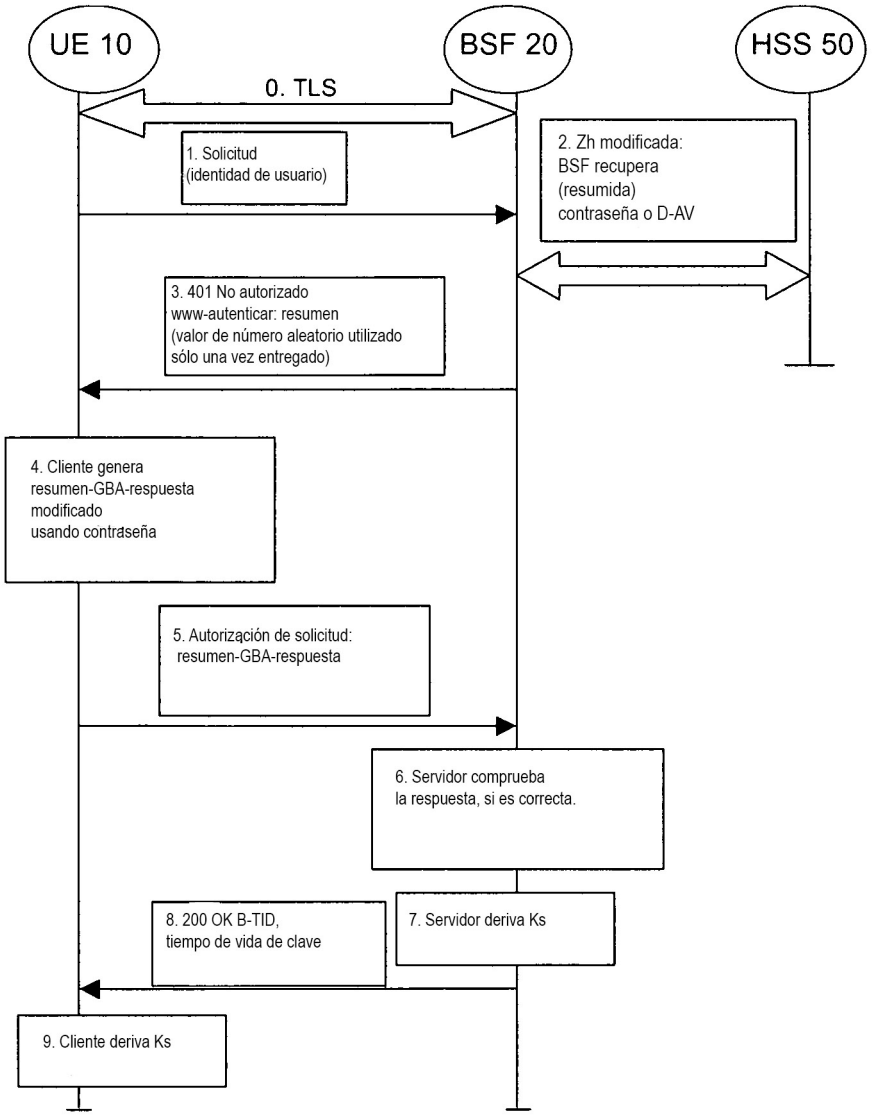
UE 10
BSF 20
HSS 50
0. TLS
1. Solicitud
(identidad de usuario)
2. Zh modificada:
BSF recupera
(resumida)
contraseña o D-AV
3. 401 No autorizado
www-autenticar: resumen
(valor de número aleatorio utilizado
sólo una vez entregado)
4. Cliente genera
resumen-GBA-respuesta
modificado
usando contraseña
5. Autorización de solicitud:
resumen-GBA-respuesta
6. Servidor comprueba
la respuesta, si es correcta.
7. Servidor deriva Ks
8. 200 OK B-TID,
tiempo de vida de clave
9. Cliente deriva Ks

Fig. 3

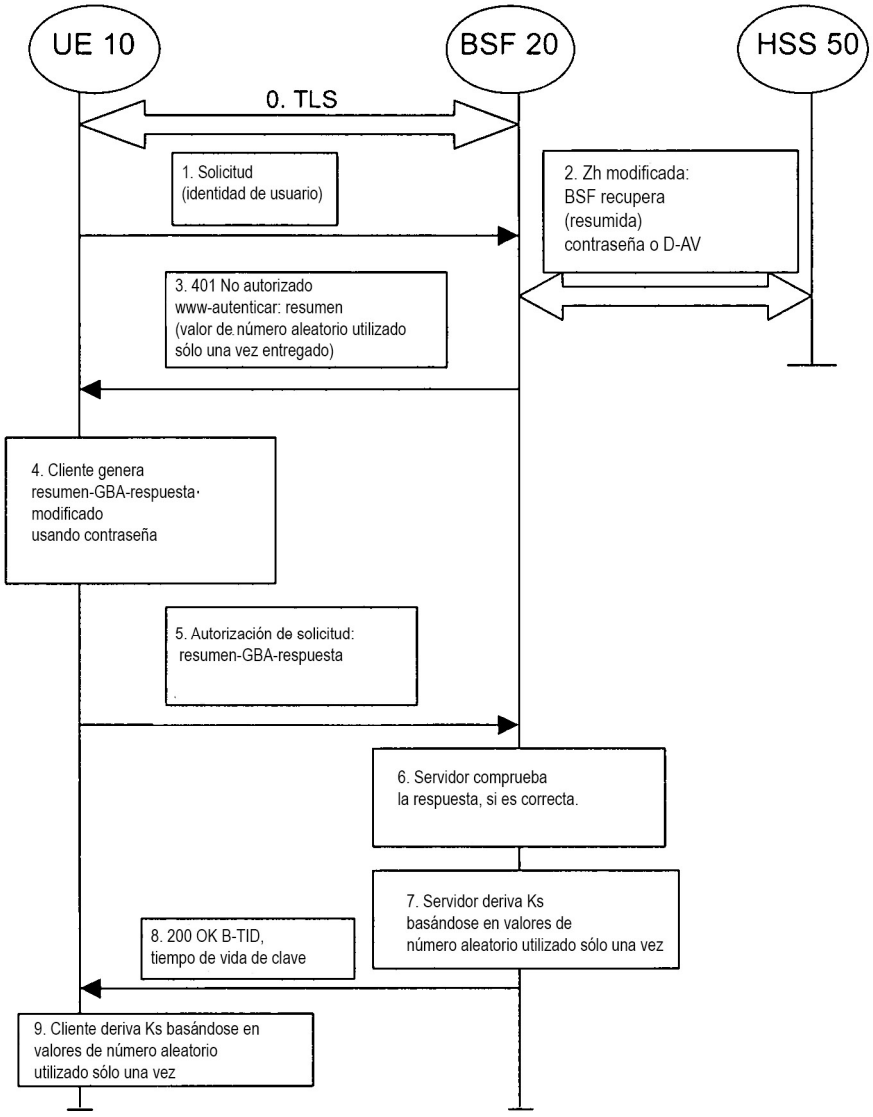
UE 10
BSF 20
HSS 50
0. TLS
1. Solicitud
(identidad de usuario)
2. Zh modificada:
BSF recupera
(resumida)
contraseña o D-AV
3. 401 No autorizado
www-autenticar: resumen
(valor de número aleatorio utilizado
sólo una vez entregado)
4. Cliente genera
resumen-GBA-respuesta·
modificado
usando contraseña
5. Autorización de solicitud:
resumen-GBA-respuesta
6. Servidor comprueba
la respuesta, si es correcta.
7. Servidor deriva Ks
basándose en valores de
número aleatorio utilizado sólo una vez
8. 200 OK B-TID,
tiempo de vida de clave
9. Cliente deriva Ks basándose en
valores de número aleatorio
utilizado sólo una vez

Fig. 4

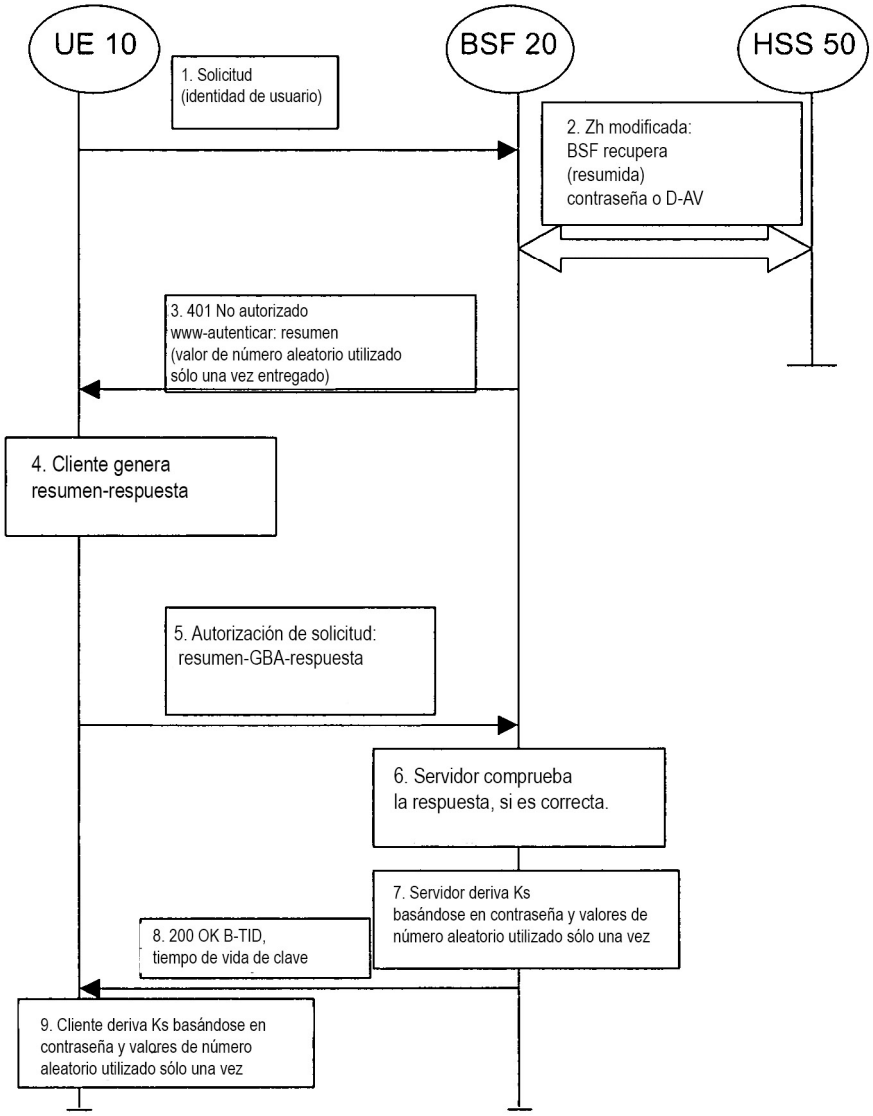
UE 10
BSF 20
HSS 50
1. Solicitud
(identidad de usuario)
2. Zh modificada:
BSF recupera
(resumida)
contraseña o D-AV
3. 401 No autorizado
www-autenticar: resumen
(valor de número aleatorio utilizado
sólo una vez entregado)
4. Cliente genera
resumen-respuesta
5. Autorización de solicitud:
resumen-GBA-respuesta
6. Servidor comprueba
la respuesta, si es correcta.
7. Servidor deriva Ks
basándose en contraseña y valores de
número aleatorio utilizado sólo una vez
8. 200 OK B-TID,
tiempo de vida de clave
9. Cliente deriva Ks basándose en
contraseña y valores de número
aleatorio utilizado sólo una vez

Fig. 5

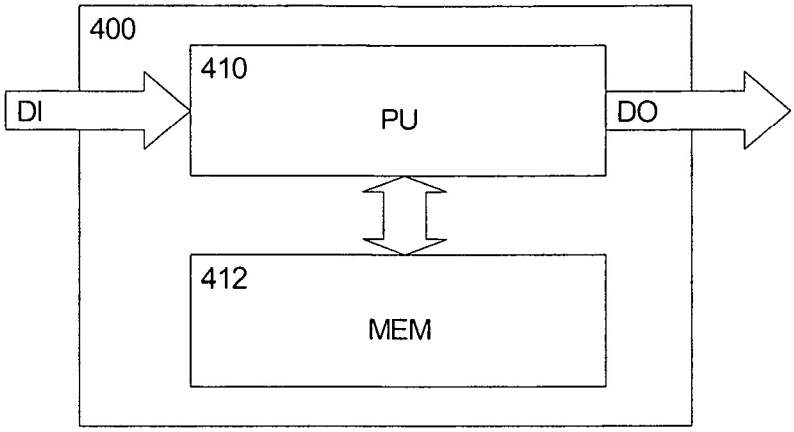

Fig. 6