(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 706 540**

(51) Int. CI.:

H04W 12/06 (2009.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **25.06.2007 PCT/IB2007/001904**

(87) Fecha y número de publicación internacional: **10.01.2008 WO08004106**

(96) Fecha de presentación y número de la solicitud europea: **25.06.2007 E 07734965 (2)**

(97) Fecha y número de publicación de la concesión europea: **31.10.2018 EP 2039199**

(54) Título: **Sistema de credenciales de equipos de usuario**

(30) Prioridad:

06.07.2006 US 818517 P

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
29.03.2019

(73) Titular/es:

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

(72) Inventor/es:

HOLTMANNS, SILKE y
LAITINEN, PEKKA

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Sistema de credenciales de equipos de usuario

Campo técnico

La presente descripción se refiere a la seguridad en un sistema de comunicaciones, y más particularmente, pero no exclusivamente, a la gestión y la creación de los datos relacionados con la seguridad del usuario y credenciales para el equipo de usuario.

Descripción de la técnica relacionada

Un sistema de comunicación puede ser visto como una instalación que permite a las sesiones de comunicación o sesiones de datos entre entidades tales como un equipo de usuario y/u otros nodos asociados al sistema de comunicación. La comunicación puede comprender, por ejemplo, comunicación de voz, datos, multimedia, etc. Un equipo de usuario conectado a un sistema de comunicación puede, por ejemplo, estar provisto de una llamada telefónica bidireccional o una llamada de conferencia multidireccional o con una conexión de datos. Además, los servicios de llamadas de voz, varios otros servicios, por ejemplo, servicios de contenido mejorado tales como servicios multimedia u otros servicios de datos, pueden proporcionarse servicios de seguridad para un usuario. Un equipo de usuario puede comunicar datos hacia y desde una entidad del servidor, o entre dos o más equipos de usuario.

Un sistema de comunicación opera normalmente de acuerdo con un estándar o especificación dados, que establece lo que se permite hacer a las diferentes entidades asociadas al sistema y cómo que deben alcanzarse. Los protocolos de comunicación, los parámetros, las funciones, los puntos de referencia y las interfaces que se utilizarán para una conexión se definen normalmente por las normas o especificaciones.

Se conocen sistemas de comunicación que proporcionan comunicación inalámbrica para un equipo de usuario. Estos sistemas se conocen comúnmente como sistemas móviles, aunque en ciertos sistemas la movilidad puede estar restringida a áreas sustancialmente pequeñas. Un ejemplo de los sistemas móviles es la red móvil terrestre pública (PLMN). Otro ejemplo es un sistema móvil que se basa, al menos parcialmente, en el uso de satélites de comunicación. Las comunicaciones móviles también pueden proporcionarse por medio de otros tipos de sistemas, tales como por medio de redes de área local inalámbricas (WLAN), redes de área personal (PAN), redes de área amplia (WAN) o alguna otra forma de red que proporciona acceso de protocolo de Internet (IP).

En un sistema inalámbrico un nodo de acceso proporciona al equipo de usuario con acceso al sistema de comunicación. Un equipo de usuario puede estar en comunicación inalámbrica con dos o más nodos de acceso al mismo tiempo. La comunicación en la interfaz inalámbrica entre el equipo del usuario y los nodos de acceso se puede basar en un protocolo de comunicación adecuado. Los ejemplos de los diversos sistemas de acceso inalámbrico incluyen CDMA (código de acceso múltiple por división), WCDMA (CDMA de banda ancha), TDMA (acceso múltiple por división de tiempo), FDMA (acceso múltiple por división de frecuencia), o SDMA (acceso múltiple por división de espacio), instituto de Ingenieros Eléctricos y Electrónicos (IEEE) 802.11, DECT (Comunicación Inalámbrica Digital Mejorada), WLAN, WAN o conexión de cable y otros desarrollos e híbridos de estos.

El funcionamiento del aparato de la red es controlado por un dispositivo de control apropiado comúnmente incluyendo un número de diversas entidades de control. También se pueden proporcionar una o más puertas de enlace o servidores intermedios para conectar una red a otras redes u ocultar detalles internos de la red de nodos externos. Por ejemplo, una red PLMN puede estar conectada a otras redes de comunicación de línea fija o móvil o redes de comunicación de datos tales como una IP (Protocolo de Internet) y/u otras redes de paquetes de datos.

Un usuario o puede necesitar ser autenticado antes de que a él/ella se le permita acceder o utilizar diversas aplicaciones y utilizar de otra forma el equipo de usuario. Esto puede ser necesario por razones de seguridad y privacidad, pero también para permitir la facturación correcta del uso del servicio. Por ejemplo, puede ser necesario verificar que el usuario es quien dice ser, que tiene el derecho de usar un determinado servicio, que se le puede proporcionar acceso a información confidencial, etc. En un proceso de autenticación, un usuario puede ser identificado sobre la base de varios valores asociados al usuario conocido por un tercero.

Varios mecanismos de autenticación ya están en su lugar, o se han propuesto. Un ejemplo no limitativo es un mecanismo de autenticación propuesto por el proyecto de asociación de tercera generación (3GPP) denominado 'Arquitectura de autenticación genérica' (GAA) o la versión de la GAA definida por el Proyecto de asociación de tercera generación 2 (3GPP2). La GAA está diseñada para ser utilizado como un procedimiento de seguridad para diversas aplicaciones y servicios para usuarios de equipos de usuarios móviles, como estaciones móviles para sistemas celulares. Las credenciales de seguridad basadas en la GAA se pueden usar para la autenticación, pero también para otros fines de seguridad, como la integridad y la protección de confidencialidad de los mensajes. El objetivo de la GAA se basa en secretos compartidos que se almacenan en entidades de almacenamiento seguro específicas proporcionadas en asociación con el equipo de usuario y las bases de datos de suscriptores. El almacenamiento seguro y la entidad de generación de credenciales de un equipo de usuario puede proporcionarse mediante una

función de seguridad apropiada, por ejemplo, un módulo de seguridad, un módulo de identificación u otro entorno seguro en el equipo de usuario. Además, el almacenamiento y la generación de credenciales pueden realizarse por dos entidades diferentes. La base de datos de suscriptores puede ser proporcionada por una entidad de red apropiada, por ejemplo, un servidor de registro de ubicación local (HLR), servidor de abonado local (HSS), autorización de autenticación y contabilidad (AAA) o servidor de servicio de nombres de dominio (DNS) como base de datos.

Además, en el 3GPP se ha propuesto (3GPP TS 33.220) una infraestructura de autenticación. Esta infraestructura puede utilizarse para asegurar el interfuncionamiento con las funciones de la aplicación en el lado de la red y en el lado del usuario para comunicarse en situaciones en las que de otro modo no podrían hacerlo. Esta funcionalidad se conoce como "secuencia de instrucciones iniciales de aplicación de seguridad", o más generalmente simplemente como "secuencia de instrucciones iniciales", que se lleva a cabo en la arquitectura genérica de secuencia de instrucciones iniciales (GBA).

Los principios generales de la secuencia de instrucciones iniciales son que una función de servidor de secuencia genérica (BSF) permite que el equipo de usuario (UE) para autenticar con la misma, y ponerse de acuerdo sobre las claves de sesión, que luego se utilizan para una interacción segura entre una función de aplicación de red (NAF) y el UE. Dicha autenticación se basa preferentemente en la autenticación y el acuerdo de clave (AKA). Al ejecutar algoritmos AKA, el terminal móvil y la red se autentican mutuamente y acuerdan las claves de sesión específicas del servicio. Después de esta autenticación, el UE y una función de aplicación de red (NAF), a la que también se puede hacer referencia como proveedor de servicios, pueden ejecutar algún protocolo específico de la aplicación donde la seguridad de los mensajes se basa en las claves de sesión específicas del servicio acordadas entre el UE y la BSF.

El procedimiento de función secuencia de instrucciones iniciales no está destinado a ser dependiente de cualquier función de aplicación de red particular. El operador local debe confiar en el servidor que implementa la función de secuencia de instrucciones iniciales (secuencia de instrucciones iniciales) para manejar los vectores de autenticación. Las funciones de aplicación de red en la red doméstica del operador deben ser admitidas, pero también es posible el soporte de las funciones de aplicación de red en una red visitada, o incluso en una tercera red.

En las propuestas de aplicación de las técnicas de secuencia de instrucciones iniciales, se propone que el UE envía una petición de servicio a una NAF. La NAF debe comunicarse con la BSF para recuperar las claves de sesión específicas del servicio necesarias para la autenticación con el UE.

Normalmente, como se describe por encima de la entidad segura de almacenamiento de un equipo de usuario es proporcionada por una función de seguridad apropiada, por ejemplo, un módulo de seguridad, o un módulo de identificación tal como una tarjeta universal de circuito integrado (UICC) o un entorno de confianza en el terminal.

Este enfoque tiene limitaciones. En primer lugar, cuando el dispositivo no está diseñado para ser utilizado como un teléfono convencional y, por lo tanto, no contiene una tarjeta UICC o módulo de información de suscriptor (SIM) equivalente. Por ejemplo, un usuario que intenta acceder a una función de red con un dispositivo de mano como el Sony PlayStation Portable (PSP) no podría autenticar al usuario debido a la falta de una UICC. Además, un usuario que utilice una PC de tableta, un asistente personal digital (PDA) o un ordenador portátil que se conecte a través de un enlace inalámbrico o fijo no podrá acceder a la función de red y acceder al servicio al que el usuario puede acceder desde su suscripción de teléfono móvil. Además, actualmente no es posible tener un proceso de inicio de sesión único genérico para servicios basados en NAF a través de diferentes redes de acceso con una autenticación que esté vinculada a la presencia de una UICC o una tarjeta inteligente similar. Por lo tanto, los usuarios deben recordar una gran variedad de contraseñas y números de identificación personal (PIN), por ejemplo, para soluciones de voz sobre IP, acceso a su teléfono móvil, acceso a servicios web, etc.

En segundo lugar, donde el dispositivo es para ser utilizado por más de una persona, la conmutación entre los usuarios requiere que el equipo de usuario sea apagado, eliminar la UICC actual, insertar la nueva UICC para el siguiente usuario y volver a encender el equipo de usuario, lo que consume mucho tiempo, es hostil para el usuario, consume batería y es potencialmente capaz de dañar la UICC. Aunque un módulo de seguridad integrado supera el problema de cambiar la UICC, también evita la supervisión independiente de cada usuario. Por ejemplo, el dispositivo con un solo módulo con una sola identificación requeriría más entidades de control para evitar que los niños puedan acceder al material para adultos.

El documento WO00/72506 describe un método y un sistema para establecer comunicaciones seguras entre dispositivos móviles en una red de radio. Un método comprende el uso de criptografía de clave pública e identificadores de hardware únicos para permitir las autorizaciones de acceso a redes inalámbricas. Un método implica una combinación de certificados asociados a usuarios y dispositivos.

GEMPLUS: "Establecimiento clave entre una UICC y un terminal: propuesta de solución", PROYECTO DE 3GPP; S3-060024, PROYECTO DE ASOCIACIÓN DE 3ª GENERACIÓN (3GPP, CENTRO DE COMPETENCIA MÓVIL; 650, ROUTE DES LUCIOLES; F-06921 SOPHIA ANTIPOLIS CEDEX; FRANCE, vol. SA WG3 n.º Bangalore, 20060130, 30 de enero de 2006) describe una solución basada en TLS como una solución para el establecimiento clave entre una UICC y un terminal.

Sumario de la invención

Las realizaciones de la presente invención pretenden abordar uno o varios de los problemas anteriores.

La invención se presenta en el conjunto de reivindicaciones adjuntas. Las realizaciones y/o ejemplos de la siguiente descripción que no están cubiertos por las reivindicaciones adjuntas se consideran como no siendo parte de la presente invención.

Se proporciona según la invención un equipo de usuario según la reivindicación 1.

El al menos un identificador comprende preferentemente un primer identificador, en el que el primer identificador es preferentemente un identificador conocido públicamente.

El primer identificador es preferentemente al menos uno de: un nombre de usuario; una clave criptográfica pública; una dirección IP; y un valor de identificación de la línea que llama.

El segundo identificador es preferentemente al menos uno de: un valor de contraseña; y una clave criptográfica privada.

El transceptor está dispuesto preferentemente para recibir un mensaje de autenticación desde el nodo adicional.

El procesador está dispuesto preferentemente para generar una clave criptográfica para cifrar las comunicaciones entre el equipo de usuario y nodo adicional en función del mensaje de autenticación procesado y un resultado de una función unidireccional del segundo identificador.

Según un segundo aspecto de la invención, se proporciona un sistema como se especifica en la reivindicación 5.

El al menos un identificador comprende preferentemente un primer identificador, en el que el primer identificador es preferentemente un identificador conocido públicamente.

El primer identificador es preferentemente al menos uno de: un nombre de usuario; una clave criptográfica pública; una dirección IP; y un valor de identificación de la línea que llama.

El segundo identificador es preferentemente al menos uno de: un valor de contraseña; y una clave criptográfica privada.

El método para la autenticación de un equipo de usuario preferentemente comprende además la etapa de recibir en el equipo de usuario un mensaje de autenticación desde el nodo adicional.

El método para la autenticación de un equipo de usuario preferentemente comprende además la etapa de generar una clave criptográfica para cifrar las comunicaciones entre el equipo de usuario y nodo adicional en función del mensaje de autenticación procesado y un resultado de una función unidireccional del segundo identificador.

Según un aspecto de la invención, se proporciona un programa de ordenador según la reivindicación 8.

Según una realización, se puede proporcionar una red que comprende: al menos un equipo de usuario, un nodo y al menos un nodo adicional, el equipo de usuario que comprende: una memoria dispuesta para almacenar al menos un identificador asociado al equipo de usuario; un transceptor dispuesto para comunicarse con el nodo en el que el transceptor está dispuesto para recibir el al menos un identificador desde el nodo, en el que el equipo de usuario usa el al menos un identificador para autenticar el equipo del usuario en el al menos un nodo más en la red.

El al menos un identificador comprende preferentemente un identificador conocido públicamente.

El al menos un identificador comprende preferentemente un identificador privado conocido al equipo de usuario, solo el nodo y el nodo adicional.

El al menos un identificador es preferentemente al menos uno de: un nombre de usuario; una clave criptográfica pública; una dirección IP; un valor de identificación de la línea que llama; un valor de contraseña; y una clave criptográfica privada.

El nodo comprende preferentemente un servidor de credenciales.

El nodo comprende además preferentemente al menos uno de un nodo de función de aplicación de red y un nodo de función de secuencia de instrucciones iniciales.

Según un cuarto aspecto de la invención, se proporciona un nodo según la reivindicación 8.

El al menos un identificador comprende preferentemente un identificador conocido públicamente.
El al menos un identificador es preferentemente al menos uno de: un nombre de usuario; una clave criptográfica pública; una dirección IP; un valor de identificación de la línea que llama; un valor de contraseña; y una clave criptográfica privada.

El nodo es preferentemente un servidor de credenciales.

El nodo adicional es preferentemente al menos uno de un servidor de secuencia inicial y un servidor de aplicaciones de red.

Según una realización, se puede proporcionar un nodo en un sistema de comunicaciones, para proporcionar un equipo de usuario de una función de secuencia inicial que comprende: una memoria dispuesta para almacenar al menos un identificador asociado al equipo de usuario; un transceptor dispuesto para comunicarse con el equipo de usuario en el que el transceptor está dispuesto para recibir el al menos un identificador del equipo de usuario y en el que el equipo de usuario utiliza el al menos un identificador para autenticar el equipo de usuario.

El al menos un identificador comprende preferentemente al menos uno de un identificador conocido públicamente.

El al menos un identificador es preferentemente al menos uno de: un nombre de usuario; una clave criptográfica pública; una dirección IP; un valor de identificación de la línea que llama; un valor de contraseña; y una clave criptográfica privada.

El transceptor está dispuesto preferentemente para recibir el al menos un identificador desde el UE, y en el que el nodo está dispuesto para iniciar la autenticación del equipo de usuario a la recepción de la al menos un identificador.

El transceptor está dispuesto preferentemente para transmitir un mensaje de autenticación al equipo de usuario.

El nodo comprende preferentemente además un procesador, en el que el procesador está dispuesto para generar una clave criptográfica.

El transceptor preferentemente está dispuesto para transmitir la clave criptográfica a un servidor de función de aplicación en función de un mensaje de autenticación procesado.

La clave criptográfica se dispone preferentemente para proteger las comunicaciones entre el equipo de usuario y el servidor de función de aplicación.

El nodo comprende preferentemente un servidor de función de secuencia de instrucciones iniciales.

Según una realización, se puede proporcionar un nodo en un sistema de comunicaciones, para proporcionar a un equipo de usuario una función de aplicación que comprende: una memoria dispuesta para almacenar al menos un identificador asociado al equipo de usuario; un transceptor dispuesto para comunicarse con un nodo adicional para recibir el al menos un identificador de un nodo adicional, en el que el al menos un identificador se usa para autenticar el equipo del usuario.

El al menos un identificador comprende preferentemente al menos un identificador conocido públicamente.

El al menos un identificador preferentemente es al menos uno de: un nombre de usuario; una clave criptográfica pública; una dirección IP; un valor de identificación de la línea que llama; un valor de contraseña; y una clave criptográfica privada.

El transceptor está preferentemente dispuesto además para comunicarse con el equipo de usuario para recibir al menos un identificador adicional desde el UE, y en el que el nodo está dispuesto para iniciar la autenticación del equipo de usuario a la recepción del al menos otro identificador.

El transceptor está preferentemente dispuesto además para transmitir un mensaje de autenticación al equipo de usuario.

El identificador de al menos una se utiliza para autenticar el equipo de usuario.

El al menos un identificador comprende preferentemente al menos un identificador conocido públicamente.

El al menos un identificador preferentemente es al menos uno de: un nombre de usuario; una clave criptográfica pública; una dirección IP; un valor de identificación de la línea que llama; un valor de contraseña; y una clave criptográfica privada.

El transceptor está preferentemente dispuesto además para comunicarse con el equipo de usuario para recibir al menos un identificador adicional desde el UE, y en el que el nodo está dispuesto para iniciar la autenticación del equipo de usuario a la recepción de la al menos otro identificador.

El transceptor está preferentemente dispuesto además para transmitir un mensaje de autenticación al equipo de usuario.

El transceptor está preferentemente dispuesto además para recibir desde el nodo adicional, una clave criptográfica.

La clave criptográfica se dispone preferentemente para proteger las comunicaciones entre el equipo de usuario y el nodo.

El nodo comprende preferentemente un servidor de aplicaciones de red.

Breve descripción de los dibujos

Para una mejor comprensión de la presente invención, se hará referencia ahora a modo de ejemplo a los dibujos adjuntos, en los que:

La figura 1 muestra un sistema de comunicación en el que la presente invención puede realizarse;
La figura 2 muestra la vista esquemática de una arquitectura de comunicaciones en la que puede realizarse la presente invención;
La figura 3 muestra un diagrama de flujo del procedimiento de secuencia de instrucciones iniciales como se lleva a cabo en una realización de la presente invención; y
La figura 4 muestra un diagrama de flujo de un procedimiento de autenticación de una aplicación de red como se lleva a cabo en una realización de la presente invención.

Descripción detallada de las realizaciones preferidas

Algunas realizaciones de ejemplo y no limitativas de la invención se discuten a continuación con referencia a una red de comunicación móvil tal como una red móvil terrestre pública (PLMN), por ejemplo, utilizado para una conexión de línea de abonado digital (DSL). Antes de explicar esto con más detalle, un sistema de comunicación que comprende al menos una PLMN se explica brevemente con referencia a la figura 1.

En una PLMN 10 un número de estaciones base 12 están dispuestas para transmitir señales de forma inalámbrica a y recibir señales desde una pluralidad de equipos de usuarios móviles 14 (de los cuales se muestra uno en la figura 1). Del mismo modo, el equipo móvil de usuario 14 puede transmitir señales inalámbricas y recibir señales de las estaciones base 12. El funcionamiento de la red 10 se controla normalmente por medio de entidades controladoras apropiadas. Los datos requeridos para la operación de la PLMN se almacenan normalmente en entidades y servidores de almacenamiento de datos apropiados.

La figura 1 muestra un almacenamiento de datos 16 configurado para almacenar datos relacionados con la autenticidad del usuario. Este almacenamiento de datos también se conoce como servidor de credenciales. El servidor de credenciales está dispuesto para almacenar datos conocidos como credenciales secretas o secretos compartidos, que se seleccionan o generan, y que solo el servidor de credenciales y el usuario los conocen. Una credencial puede ser una clave criptográfica, una contraseña u otra forma de testigo de seguridad.

Este secreto compartido en una primera realización de la invención es una credencial generada cuando el usuario se registra en el servidor de credenciales por primera vez. Por ejemplo, cuando un usuario se registra en un servicio de voz sobre IP, se le puede pedir que proporcione o genere una contraseña en combinación con un nombre de usuario. Esta combinación es normalmente utilizada por el usuario para conectarse al servicio. Aunque el nombre de usuario es conocido por otras partes, la contraseña se mantiene en secreto de todas las demás, excepto el usuario y el servidor de credenciales. A veces, incluso el nombre de usuario se considera secreto.

En otras realizaciones de la presente invención la credencial se pasa desde el servidor de credenciales 16 al equipo de usuario 14. En algunas realizaciones de la invención, el equipo de usuario y el servidor de credenciales almacenan cada uno un valor de la credencial secreta asociada al UE y solo se conoce el uno al otro De este valor de la credencia secreta se puede derivar un certificado, un par de nombre de usuario/contraseña o una o dos credenciales secretas secundarias. Estos valores de credenciales secundarios son conocidos por la red y una entidad proveedora de servicios (la entidad proveedora de servicios puede ser, en algunas realizaciones de la invención, un tercero).

En otras realizaciones de la presente invención una credencial es un par de clave de cifrado pública/privada compartida entre el servidor de credenciales 16 y el equipo de usuario 14. En otras realizaciones, se pueden usar otros datos en asociación con la credencial para identificar al usuario, tal como el valor del identificador de línea del que llama.

El equipo de usuario (UE) 14 puede ser proporcionado por cualquier terminal de usuario correspondiente. El equipo del usuario puede contener o tener acceso a uno o más entornos seguros. En un sistema de comunicaciones móviles, el equipo del usuario constituye un terminal móvil, por ejemplo, un teléfono móvil, un asistente digital personal (PDA) o una PC móvil (ordenador personal), o similares.

Para el uso en un sistema de comunicaciones inalámbricas, el equipo de usuario comprende recibir y transmitir circuitos y medios para recibir y transmitir señales inalámbricas para la aplicación de las llamadas y otros canales de señalización de modo que está habilitado para comunicarse con las estaciones base 12, por ejemplo, para hacer llamadas de voz y enviar y recibir datos. El usuario también puede conectar su dispositivo directamente a una red basada en cable y, por lo tanto, acceder a los servicios que residen en el sistema de comunicación inalámbrica a través del protocolo IP. El equipo de usuario también puede estar habilitado para procesar las instrucciones de control que puede recibir de la red y enviar información de control a la red.

Un usuario puede acceder a diversas aplicaciones, por ejemplo, aplicaciones de servicios a través de la red a la que él o ella tiene acceso. Una entidad proveedora puede proporcionar una aplicación, por ejemplo, cualquiera de los servidores de aplicaciones 18 del proveedor de servicios. Se observa que los servidores de aplicaciones (AS) solo necesitan estar conectados a la red móvil, pero no son necesariamente parte de la red móvil. El servidor de aplicaciones puede ser algún tipo de servidor de difusión. Esto significa que el operador de la red 10 puede no tener necesariamente alguno o solo puede tener un control limitado sobre la operación de un proveedor de aplicaciones. Además, un sistema de comunicación puede ser proporcionado por una pluralidad de diferentes redes de comunicación. Por lo tanto, la entidad proveedora de la aplicación puede estar conectada a otra red que la red a la que se suscribe el usuario. Además, la red a la que se ha suscrito un usuario puede constar de varios tipos de red, por ejemplo, UMTS, línea fija, WLAN o similar, todos ejecutados por el mismo operador.

Un usuario o el equipo de usuario necesita normalmente para ser autenticado antes de que él/ella se le permite acceder o utilizar de otro modo diversas aplicaciones y servicios a través de la red. También puede requerirse que la comunicación sea asegurada. La figura 1 muestra un servidor de administración de seguridad 17 adaptado para la autenticación del usuario. El servidor de gestión de seguridad es capaz de generar claves. Por ejemplo, el servidor 17 proporciona una función de secuencia de instrucciones iniciales basada en valores de credenciales secretas almacenados en una base de datos de credenciales que puede ser parte del servidor de administración de seguridad o estar conectado a ella.

Un usuario puede ser identificado por el servidor de gestión de la seguridad basado en 17 diferentes credenciales. Se pueden dividir en credenciales de clave criptográfica pública y privada o credenciales secretas. Las credenciales secretas y las claves privadas de los pares de claves públicas/privadas son, como se describió anteriormente, generalmente solo conocidas por el operador, mientras que las credenciales de la clave pública pueden hacerse públicas. A veces también se usan credenciales semipúblicas, por ejemplo, direcciones IP. Los ejemplos no limitativos de credenciales de usuario secretas incluyen la Identidad de Abonado Móvil Internacional (IMSI) y la Identidad Privada Multimedia del Protocolo de Internet (IMPI). Entre los ejemplos no limitativos de credenciales públicas se incluyen el Número Digital del Sistema Integrado de Abonado Móvil (MSISDN, por sus siglas en inglés), el identificador de línea de llamada (CLF) y la Identidad Pública Multimedia de IP (IMPU).

Para mantener la información de identidad, el equipo de usuario 14 puede estar provisto de una memoria 15 dispuesta para almacenar información de autenticación. La memoria puede organizarse para almacenar una credencial segura que está organizada para permitir que las redes se aseguren de que el usuario sea quien dice ser o para asegurar un enlace de comunicación. La memoria puede contener una serie de aplicaciones de seguridad y otras. Un usuario puede tener varios tipos de identidades de usuario, credenciales de sesión e identificadores de servicio que se almacenan en la memoria. La memoria 15 en realizaciones de la invención almacena los secretos compartidos (con el almacenamiento de datos del abonado) y almacena las claves de seguridad generadas a partir del secreto compartido. El secreto compartido generado también se puede almacenar en una memoria secundaria que está conectada a la memoria primaria que guarda los secretos compartidos con el almacenamiento de datos del suscriptor. Los valores de credenciales secretas (claves compartidas con el almacenamiento de datos del suscriptor) se pueden usar para crear y recibir conexiones confiables entre el equipo del usuario y una aplicación, como la protección de contenido de transmisión.

La figura 2 muestra un ejemplo de la arquitectura del servidor dentro del cual operan las realizaciones de la presente invención. Más particularmente, la figura 2 es un diagrama de bloques esquemático de una disposición mejorada, que en su forma no mejorada se conoce como una arquitectura de autenticación genérica (GAA) de acuerdo con el sistema 3GPP.

La arquitectura de autenticación genérica mejorada (GAA) comprende un equipo de usuario 14 que se puede comunicar a un servidor de función de aplicación de red (NAF) 25 sobre una interfaz adecuada 4, por ejemplo, una

interfaz Ua. El servidor de aplicaciones de red 25 también se conoce como el servidor de aplicaciones, como se muestra en la figura 1. El equipo de usuario (UE) 14 también puede comunicarse con un servidor de administración de seguridad (servidor de la función de secuencia de instrucciones iniciales (BSF)) 17 a través de una interfaz adecuada 3, por ejemplo, una interfaz Ub. Pero los datos necesarios para la generación de credenciales también pueden enviarse desde la NAF a través de la interfaz Ua 4 al UE o directamente desde la BSF al UE. El servidor de administración de seguridad (el servidor BSF) 17 puede comunicarse con el servidor NAF 25 a través de una interfaz apropiada 1, por ejemplo, una interfaz Zn. El servidor de gestión de seguridad (servidor BSF) 17 puede comunicarse con el almacenamiento de datos 16 configurado para almacenar información de abonado (que en una primera realización de la invención es un servidor de credenciales) a través de la interfaz 2, por ejemplo, una interfaz Zh. El BSF también puede contener el almacenamiento de datos de seguridad, por ejemplo, en forma de una funcionalidad de servidor AAA de funcionalidad de servidor DNS extendido. El servidor NAF 25 se puede conectar en formas de realización adicionales de la invención directamente al almacenamiento de datos 16 configurado para almacenar información de abonado a través de una interfaz apropiada 7 (representada en la figura 2 como una línea discontinua), por ejemplo, una interfaz Sh o Zh. Aunque no se muestra en la figura 2, en algunas realizaciones, el equipo de usuario 14 está conectado al servidor de credenciales 16, para que el UE 14 y el servidor de credenciales intercambien el secreto compartido (por ejemplo, nombre de usuario, contraseña), identificador de línea de llamada, dirección IP o claves criptográficas (pares de claves públicas/privadas). Aunque esto se ha descrito anteriormente en relación con una realización mediante el paso de datos mediante un proceso de autenticación en conjunto del subsistema de conexión de red (NASS), una red de cable, se pueden utilizar otras formas de intercambiar esta información. Por ejemplo, la información se puede pasar al usuario fuera de línea, en forma de una carta, o como un archivo o parte de un archivo en forma de medios portátiles (por ejemplo, en un CD, DVD o unidad de memoria flash extraíble). Una función de un solo sentido puede cortar partes de un valor que fue la entrada de la función, pero también puede realizar un algoritmo criptográfico sofisticado.

En la siguiente sección se describen tres combinaciones de credenciales diferentes como ejemplos no exhaustivos del tipo de credencial que se puede crear como una etapa inicial por parte del usuario para autenticar a sí mismo en ausencia de la utilización de los identificadores convencionales como proporcionado por la UICC.

GBA-PKI (Arquitectura de secuencia de instrucciones iniciales genérica - Infraestructura de clave pública)

En una primera realización de la presente invención, la credencial secreta Ks compartida por el UE 14 y el servidor de credenciales 16 es el resultado de una función unidireccional que tiene como entrada una clave criptográfica privada asociada al usuario. La clave criptográfica se genera como parte de un par de claves privada/pública. El resultado de una función unidireccional de la clave privada se genera en una realización en el UE 14 y se pasa al servidor de credenciales 16 de manera segura. En una realización alternativa, el par de claves y el resultado de un valor de función unidireccional se generan en el servidor de credenciales 16 y se pasan al UE de forma segura. En algunas realizaciones, la clave pública se distribuye al mismo tiempo y de la misma manera. En algunas realizaciones, el par de claves se genera en un servidor generador de claves (no mostrado en la figura 1) y se distribuye de manera segura tanto al UE 14 como al servidor de credenciales 16. En algunas realizaciones de la invención, el resultado de una credencial de función unidireccional también incluye los datos de clave pública o podría contener el certificado completo.

El resultado de una función unidireccional de la clave privada se ha descrito anteriormente (que puede contener también la clave pública y/o todo el certificado) está asociado al usuario en el servidor de credenciales por los medios de credencial pública o semi pública. La credencial pública o semi pública asociada a la credencial compartida, por ejemplo, es el campo de datos "nombre de usuario" que se usa para registrarse en el servidor de credenciales. En un ejemplo adicional, la credencial pública es el valor de identidad de la línea que llama, un número que indica de qué conexión PSTN proviene la conexión a la red. Esto, aunque solo especifica que el usuario está conectado desde una localidad física específica.

GBA-LA (Arquitectura de secuencia de instrucciones iniciales genérica - Autenticación de línea)

En una realización adicional de la presente invención la credencial secreta Ks compartida entre el UE 14 y el servidor de credenciales 16 es el campo de datos de la contraseña utilizada cuando se registra inicialmente al usuario en el servidor de credenciales. En algunas realizaciones de la invención, la credencial secreta compartida entre el UE 14 y el servidor de credenciales 16 es una función unidireccional del campo de datos de contraseña (la función unidireccional recibe un primer valor y devuelve una salida o un valor en función de una asignación conocida o función unidireccional). El usuario proporcionaría su contraseña completa para la autenticación, pero el valor almacenado sería la función unidireccional aplicada a la contraseña. En algunas realizaciones, este valor también puede incluir algunos datos adicionales (llamados sal) para que sea más difícil para un atacante derivar un valor análogo como resultado de la función unidireccional. En una realización adicional, los valores adicionales generados por el UE 14 o el servidor de credenciales 16 o ambos se agregan a la función unidireccional para producir la credencial Ks. Después de aplicar la función unidireccional, es posible que deba reducirse el valor resultante, debido a restricciones de longitud. El valor adicional puede ser, por ejemplo, un valor aleatorio o una marca de tiempo actual. En una realización adicional de este tipo, la credencial privada o secreta es un valor de la credencia que es generado por una pasarela de red entre el UE 14 y el servidor de credenciales 16. El valor de la credencial se distribuye de forma segura al UE 14 y al servidor

de credenciales 16.

La credencial pública o semi pública se describe anteriormente se asocia al equipo de usuario en el servidor de credenciales. La credencial pública o semi pública asociada al usuario es el valor de identidad de la línea que llama, un número que indica a la red a través de la cual se conecta la conexión PSTN a través de la cual se encuentra el UE 14. El operador también puede asignar el identificador de línea que llama a una dirección IP y usar la dirección IP como credencial semi pública y, en su lugar, o adicionalmente, al identificador de línea que llama.

GBA-PW (Arquitectura de secuencia de instrucciones iniciales genérica - Autenticación de contraseña)

En una realización adicional de la presente invención la credencial secreta Ks compartida entre el UE 14 y el servidor de credenciales 16 es el campo de datos de la contraseña utilizada cuando se registra inicialmente al usuario en el servidor de credenciales 16. En algunas realizaciones de la invención, la credencial secreta compartida entre el UE 14 y el servidor de credenciales 16 es un resultado de la función unidireccional del campo de datos de contraseña (la función unidireccional recibe un primer valor, el valor de contraseña y devuelve un valor de salida en función de una asignación conocida o función unidireccional). En una realización adicional, los valores adicionales generados por el UE 14 o el servidor de credenciales 16 o ambos se agregan a la función unidireccional para producir el identificador secreto Ks. El valor o valores adicionales pueden ser, por ejemplo, valores aleatorios o marcas de tiempo actuales.

La credencial pública o semipública está asociada al usuario en el servidor de credenciales. El identificador único asociado a la credencial pública, por ejemplo, es el campo de datos de "nombre de usuario" utilizado inicialmente para registrarse en el servidor de credenciales.

Las realizaciones a modo de ejemplo de la presente invención se describirán con referencia a la arquitectura mejorada GAA (GBA) como se discute en más detalle a continuación con respecto a la autorización de un equipo de usuario 14 para acceder a una aplicación específica de un servidor de función de aplicación de red 25. Varios posibles componentes de estos se describirán brevemente, ya que el funcionamiento de estos no es esencial para realizar la invención.

El equipo de usuario 14 se comunica con una entidad de aplicación, por ejemplo, un servidor de función de aplicación de red (NAF) 25. El servidor NAF 25 proporciona un servicio al equipo de usuario 14, pero antes de que el servidor de función de aplicación de red 25 pueda entregar sus servicios al equipo de usuario 14 de manera segura, se necesita un procedimiento de autenticación específico del servicio y/o una comunicación segura en la que se basa nuestra invención en uno de los tres ejemplos anteriores.

Si el equipo de usuario 14 desea acceder a una aplicación desde el servidor NAF 25 pero no se ha sometido a una autenticación que ha hecho que la BSF recupere el material de la clave de autenticación o que el material recuperado ya no sea válido, el equipo de usuario 14 se somete a un procedimiento de autenticación inicial también conocido como secuencia de instrucciones iniciales. Esto puede ocurrir, por ejemplo, cuando un nuevo usuario opera el equipo del usuario o si un usuario no ha usado el equipo del usuario durante un tiempo predeterminado o si se había desconectado previamente del equipo del usuario. En los tres ejemplos anteriores, el usuario que utiliza el UE debe estar autenticado.

La figura 3 muestra los pasos llevados a cabo dentro de las realizaciones de la presente invención para llevar a cabo el procedimiento de autenticación de secuencia de instrucciones iniciales. En otra realización, la NAF puede empujar los datos relevantes de seguridad necesarios para crear una asociación de seguridad entre el UE y la NAF al UE, después de haberse comunicado con la BSF. En otra realización, la BSF puede empujar los datos relevantes de seguridad necesarios para crear la asociación de seguridad entre el UE y la NAF al UE.

En la primera etapa 301 el equipo de usuario transmite una petición de autorización que contiene algún tipo de identificación de usuario a la función de servidor de secuencia inicial (BSF) 17. Este ID de usuario en las realizaciones GBA-PKI y GBA-PW es el nombre de usuario. La ID de usuario en la realización de GBA-LA utilizada es el valor de identificación de la línea que llama y/o la dirección IP.

En la siguiente etapa 303, la BSF 17, al recibir el valor de identificación de usuario se comunica con el servidor de credenciales 16 para recuperar el perfil de usuario (Prof) juntos cualquier vector de autenticación requerida. El vector de autenticación incluye un valor de número aleatorio (RAND), un testigo de autenticación (AUTN), una respuesta de autenticación esperada (XRES) y el valor de identificación compartido. En el entorno de comunicaciones inalámbricas de la técnica anterior, el valor de identificación compartido (Ks) se almacena en la UICC o tarjeta inteligente similar. En la realización de GBA-PKI, el valor de identificación compartido es la clave privada o cualquier combinación descrita anteriormente que comprende la clave privada. En las realizaciones GBA-PW y GBA-LA, el valor de identificación compartido es el valor de la contraseña (o, en algunas realizaciones, el resultado de una función unidireccional del valor de la contraseña).

En la siguiente etapa 305, la BSF 17 transmite un mensaje al UE 14 para exigir el UE se autentifica a sí mismo a la BSF 17. El mensaje contiene el valor de número aleatorio (RAND) y el testigo de autenticación (AUTN) recibido del servidor de credenciales.

En la siguiente etapa 307, el UE 14 ejecuta algoritmos AKA como se conoce en la técnica para verificar el testigo de autentificación es correcto. El UE 14 también genera un valor de mensaje de respuesta (RES). En algunas realizaciones de la presente invención, el UE no utiliza el algoritmo AKA para autenticar el servidor, sino otros medios para autenticar en el servidor, por ejemplo, nombre de usuario/contraseña, certificados, pares de clave pública/privada, identificador de línea o medios similares. En esta realización, tanto el BSF como el UE son de confianza y es posible que no sea necesario autenticar el BSF.

En la siguiente etapa 309, el UE 14 transmite un mensaje de solicitud de autorización al BSF 17. El mensaje de solicitud contiene un valor de respuesta (RES) que se utiliza para verificar que el usuario es el mismo que solicita el procedimiento de autorización.

En la siguiente etapa 311, el BSF, a la recepción del mensaje de petición transmitida en la etapa 309, comprueba si el valor RES recibido coincide con el valor de respuesta esperado (XRES) ya almacenado en el BSF 17. Si los valores coinciden, el proceso avanza a la etapa 313.

En la etapa 313, la BSF 17 genera un valor de identificación de transacción secuencia de instrucciones iniciales (B-TID) que define de forma única la secuencia de instrucciones iniciales.

En la siguiente etapa 315, la BSF 17 transmite al UE 14 un mensaje de OK que contiene el valor B-TID y el valor de clave de por vida. El valor de la vida útil de la clave define la vida útil de este programa de secuencia de instrucciones iniciales actual para reducir la probabilidad de acceso no autorizado al sistema.

Al recibir el mensaje ok de la BSF 17, el equipo de usuario 14 ahora deriva material de clave criptográfica (Ks_NAF) que el UE puede usar para cifrar cualquier información que se envíe a una función de aplicación de red siguiendo este procedimiento de secuencia de instrucciones iniciales y antes La vida útil de la secuencia de instrucciones iniciales expira. El UE 14 utiliza el valor secreto compartido para derivar el material clave (Ks_NAF).

El procedimiento para generar el material de claves (Ks_NAF) utilizando datos UICC se conoce en la técnica y se especifica en 3GPP TS 33 220 V7.3.0 publicado en marzo de 2006. En este el material clave es generado por la función

$$Ks\_NAF = KDF(Ks, \text{“gba-me”}, RAND, IMPI, NAF\_ID)$$

donde KDF es la función de distribución de clave conocida, una función matemática que genera material de clave criptográfica que depende de los parámetros entre paréntesis y se describe en el Apéndice B de 3GPP TS 33 220. Los parámetros de derivación utilizados actualmente como se muestra arriba son: la credencial secreta o el valor clave Ks, la cadena de tipo GBA "gba-me", el valor de número aleatorio recibido de la BSF 17 (RAND), la identidad privada multimedia del protocolo de Internet del usuario (IMPI), y el valor de identificación NAF (NAF_ID).

En realizaciones de la presente invención, la función de derivación de claves tal como se especifica en el documento 3GPP se utiliza, aunque los parámetros difieran.

En las realizaciones GBA-PKI de la presente invención, los parámetros utilizados para generar el material clave son:

$$Ks\_PKI\_NAF = KDF(Ks, \text{“gba-pki”}, RAND, \text{Credencial pública}, NAF\_ID)$$

La cadena de tipo GBA proporciona una indicación de la base de la secuencia de instrucciones iniciales, es decir, "GBA-pki". El valor de la credencial secreta Ks en esta realización de la presente invención es el resultado de una función unidireccional que al menos contiene la clave privada del usuario (y puede contener además la clave pública y el certificado completo). La credencial pública (semipública) en algunas realizaciones de PKI es el valor del nombre de usuario asociado a la clave privada y en otras realizaciones el valor de identificación de la línea que llama.

En las realizaciones GBA-LA de la presente invención los parámetros utilizados para generar el material clave son:

$$Ks\_LA\_NAF = KDF(Ks, \text{“gba-la”}, RAND, \text{Credencial pública}, NAF\_ID)$$

La cadena de tipo GBA proporciona una indicación de la base de la secuencia de instrucciones iniciales, es decir, "gba-la". El valor de la credencia secreta Ks en esta realización de la presente invención es la contraseña o el resultado de la función unidireccional del valor de contraseña como se describe anteriormente. La credencial pública asociada (semipública) en las realizaciones de autenticación de línea es el valor de identificación de línea del que llama como también se describió anteriormente.

En las realizaciones GBA-PW de la presente invención los parámetros utilizados para generar el material clave son:

Ks_PW_NAF = KDF(Ks, “gba-pw”, RAND, Credencial pública, NAF_ID)

La cadena de tipo GBA proporciona una indicación de la base de la secuencia de instrucciones iniciales, es decir, "gba-pw". El valor de la credencia secreto Ks en esta realización de la presente invención es la contraseña o el resultado de una función unidireccional del valor de contraseña como se describe anteriormente. La credencial pública asociada (semi pública) es el valor del nombre de usuario asociado a la contraseña.

En algunas realizaciones de la presente invención, el valor del número aleatorio no se utiliza para derivar el material clave. En realizaciones adicionales de la presente invención, el valor de número aleatorio se reemplaza por un testigo tal como una marca de tiempo recibida desde el servidor de aplicaciones. En algunas realizaciones de las realizaciones GBA-PKI, la contraseña del usuario también se incluye como un parámetro adicional o se usa para reemplazar el valor RAND.

La figura 4 muestra las etapas del método empleado en realizaciones de la presente invención una vez que se ha llevado a cabo la secuencia de instrucciones iniciales inicial para que el UE con claves de autenticación "en vivo" se autentique con una función de aplicación de red 25.

Las etapas 401, 403 y 405 muestran en resumen el resultado de las etapas realizadas por la operación de secuencia de instrucciones iniciales como se muestra en la figura 3.

La etapa 401 muestra que el UE ha almacenado un valor de identificación de transacción de secuencia de instrucciones iniciales (B-TID) y el valor de identificación compartido (Ks).

La etapa 403 muestra que la función de servicio de secuencia de instrucciones iniciales (BSF) 17 tiene una copia del valor de ID de transacción de secuencia de instrucciones iniciales (B-TID), el valor de identificación compartido (Ks) y una parte específica de la aplicación del perfil de usuario (PROF) - detallar instrucciones especiales sobre a qué partes de la aplicación está autorizado el usuario para acceder, por ejemplo, un certificado de edad que permite a la función de la aplicación bloquear material adulto a menores.

La etapa 405 muestra la generación en el UE 14 del material de la clave Ks_NAF (el equivalente a la etapa 317 de la figura 3) a partir de los valores de identificación compartidos PKI/LA/PW como se describió anteriormente y utilizando la función de derivación de clave convencional (KDF) y algoritmos AKA.

En la etapa 407, el UE 14 realiza una petición de aplicación a la NAF 25 para el acceso para una aplicación específica. La solicitud de solicitud contiene el valor de identificación de la transacción de secuencia de instrucciones iniciales (B-TID). La solicitud también contiene datos específicos de la aplicación (msg), como la solicitud de un elemento específico del servicio requerido.

En la etapa 409, tras la recepción de la recepción de la solicitud en la NAF 25, la NAF 25 transmite una solicitud de autorización a la BSF 17. La solicitud de autorización contiene la ID de transacción de secuencia de instrucciones iniciales (B-TID) recibida del UE 14 junto con el valor de ID de NAF (ID de NAF).

En la etapa 411, a la recepción de la solicitud de autenticación desde la NAF 25, la BSF 17 genera el material de claves requerida por la NAF 25 para permitir que los datos a ser cifrados entre el UE 14 y la NAF 25. Este material clave Ks_NAF se genera de acuerdo con la función de derivación de clave conocida como se describió anteriormente.

La BSF 17 también transmite una respuesta de autorización a la NAF 25. La respuesta de autorización contiene el material clave generado Ks_NAF, y también puede contener la parte específica de la aplicación del perfil de usuario (PROF), el tiempo de secuencia de instrucciones iniciales (tiempo BOOTSTRAP) que define el momento en que se llevó a cabo el último proceso de secuencia de instrucciones iniciales y la vida útil de la clave (clave vida útil) que define el tiempo dentro del cual la clave generada es válida, y si la clave generada tiene una vida útil.

En la etapa 413, la NAF 25 a la recepción de la respuesta de autorización, almacena el material de clave específica de la aplicación que se derivó de la NAF, la parte específica de la aplicación del perfil de usuario (PROF), el tiempo de secuencia de instrucciones iniciales y la duración de la clave.

En la etapa 415, la NAF 25, después de haber almacenado la información, transmite una respuesta de aplicación 415 al equipo de usuario 14 en respuesta a la petición de la aplicación de la etapa 407.

Una vez que se ha completado este proceso, tanto el UE como la NAF ahora contienen material de clave de cifrado dentro del cual los datos pueden cifrarse antes de la transmisión entre ellos o pueden usarse para la autenticación del UE a la NAF.

La ventaja con las realizaciones de la presente invención como se ha descrito anteriormente puede describirse, por ejemplo, cuando la función de aplicación de red es el de la transmisión de información de vídeo digital que contiene gestión de derechos digitales. Esta transmisión solo se puede realizar cuando el usuario está correctamente autorizado para acceder al material. Por ejemplo, la NAF debe determinar si el usuario ha comprado correctamente el material y también si es adecuado para ver el material (por ejemplo, para evitar que los menores accedan a material temático para adultos). Al utilizar el servidor de credenciales que puede tener un nombre de usuario, un par de identificador de contraseña u otra información almacenada en el servidor de credenciales, no se requiere tener datos de identidad almacenados permanentemente (en el caso del módulo de seguridad fijo) o almacenados de manera semipermanente (en el caso del módulo de seguridad UICC) dentro del equipo del usuario.

Además, este proceso se puede utilizar para acceder a las funciones de la aplicación de red desde recursos de red fijos, así como recursos de red móvil. Sería posible usar formas de realización de la presente invención para acceder a los servidores de aplicaciones y secuencia de instrucciones iniciales y autenticar al usuario que usa el recurso de red fijo para conectarse a la función de la aplicación usando las mismas etapas descritas anteriormente.

Una ventaja adicional es que el identificador de clave privada en las realizaciones PKI se utiliza solo una vez durante secuencia de instrucciones iniciales, y no se utiliza entre otros servidores. Por lo tanto, esto tiene seguridad adicional ya que menos partes tienen acceso a la propia clave privada.

Una ventaja adicional es que el identificador compartido Ks se puede utilizar directamente sin ningún requisito para generar instantáneas identificadores de clave privada (por ejemplo, en la clave previamente compartida - seguridad de capa de transporte (PSK TLS) y por lo tanto no se requiere llevar a cabo operaciones computacionalmente complicadas de clave privada para el cliente (exceptuando cualquier recálculo de claves privadas después de un período de tiempo específico, por ejemplo, un día) y para el servidor.

Además, no hay ningún requisito para que el UE pueda manejar la revocación del certificado del cliente en comparación con el sistema de infraestructura de clave pública (PKI). Aunque existe un requisito de que el servidor BSF debe comunicarse con el servidor de credenciales para obtener el secreto, esto puede llevarse a cabo antes de la demanda cuando haya tiempo de procesamiento libre para que el usuario no experimente demoras significativas en la operación.

Las operaciones descritas anteriormente pueden requerir procesamiento de datos en las diferentes entidades. El procesamiento de datos se puede proporcionar por medio de uno o más procesadores de datos. El producto de código de programa informático adaptado apropiadamente se puede usar para implementar las realizaciones, cuando se carga en un ordenador. El producto de código de programa para proporcionar la operación puede almacenarse y proporcionarse por medio de un medio portador tal como un disco, tarjeta o cinta portadora. Una posibilidad es descargar el producto de código de programa a través de una red de datos. La implementación puede proporcionarse con el software adecuado en un servidor de ubicación.

En algunas realizaciones de la presente invención, la BSF y la funcionalidad de servidor de credenciales están alojadas dentro de una única entidad del servidor.

Se hace notar que mientras que en las realizaciones anteriores se describen en relación con el equipo de usuario tales como estaciones móviles, las realizaciones de la presente invención son aplicables a cualquier otro tipo adecuado de equipo de usuario.

Además, aunque hemos descrito el equipo de usuario que se conecta a una red, la aplicación funciona a través de una interfaz Ub. Credenciales secretas iguales o similares y valores de credenciales públicas o semipúblicas asociadas podrían comunicarse a través de varias interfaces de comunicación. Por ejemplo, las realizaciones que incorporan la realización GBA-PW como se describió anteriormente se podrían usar para la autenticación en la función de la aplicación en las conexiones HTTP Digest normales. Además, las realizaciones que incorporan las realizaciones GBA-PKI se pueden usar para la autenticación y la seguridad a través de las interfaces de intercambio TLS. En las realizaciones del protocolo de enlace de seguridad (TLS) de transporte, los valores de vida útil y B-TID se pueden enviar como uno de los parámetros del protocolo de enlace TLS como se describe en 3GPP TS33.222. Además, la credencial secreta en esta realización (Ks) puede ser la clave maestra TLS acordada. Esta clave maestra podría utilizarse para cualquier tipo de servicio, independientemente de la plataforma de dispositivo utilizada.

También se observa que aunque el sistema de comunicación a modo de ejemplo mostrado y descrito con más detalle en esta descripción utiliza la terminología de redes de la 3ª generación (3G) WCDMA (División de Código de Banda Ancha de Acceso Múltiple), tales como UMTS (Universal Mobile Sistema de Telecomunicaciones) o redes móviles terrestres públicas (PLMN) CDMA2000, las realizaciones de la solución propuesta se pueden usar en cualquier sistema de comunicación en el que la ventaja se pueda obtener por medio de las realizaciones de la invención. La invención tampoco se limita a entornos tales como los sistemas móviles celulares o WLAN. La invención podría implementarse, por ejemplo, como parte de la red de ordenadores conocida como "Internet" y/o como una "Intranet". Además, el equipo de usuario 14 en algunas realizaciones de la presente invención puede comunicarse con la red a través de una conexión fija, como una línea de abonado digital (DSL) (ya sea asíncrona o síncrona) o una línea de red

telefónica pública conmutada (PSTN) a través de una pasarela adecuada.

También se observa que mientras que lo anterior describe formas de realización a modo de ejemplo de la invención, hay varias variaciones y modificaciones que pueden realizarse a la solución dada a conocer sin apartarse del alcance de la presente invención como se define en las reivindicaciones adjuntas.

REIVINDICACIONES

1. Un equipo de usuario (14) de que comprende:

medios configurados para recibir, desde un primer nodo (16), al menos un primer identificador asociado al equipo de usuario, comprendiendo el al menos un primer identificador al menos un identificador privado, en donde el identificador privado es conocido solamente por el equipo de usuario (14), el primer nodo (16) y el segundo nodo (17);
una memoria (15) configurada para almacenar al menos un primer identificador y un identificador de usuario asociado al equipo de usuario (14);
un transceptor configurado para transmitir una solicitud de autorización (301) que comprende el identificador de usuario, la ID de usuario, al segundo nodo (17) para iniciar la autenticación del equipo de usuario (14) en el segundo nodo (17) y recibir un mensaje (315) desde el segundo nodo (17); en donde el mensaje (315) comprende al menos un identificador adicional, B-TID, utilizado por el equipo de usuario (14) para autenticar el equipo de usuario (14) a un tercer nodo (25); y
un procesador, configurado para procesar el mensaje (315) y generar una clave criptográfica, Ks_NAF, para cifrar las comunicaciones entre el equipo del usuario (14) y el tercer nodo (25) en función del mensaje procesado y el identificador privado.

2. Un equipo de usuario (14) según la reivindicación 1, en el que el identificador de usuario es al menos uno de:

un nombre de usuario;
una clave criptográfica pública;
una dirección IP; y
un valor de identificación de la línea que llama.

3. Un equipo de usuario (14) según la reivindicación 1, en el que el identificador privado es al menos uno de:

un valor de contraseña; y
una clave criptográfica privada.

4. Un método ejecutado por un equipo de usuario (14) que comprende:

recibir, por un equipo de usuario (14) desde un primer nodo (16), al menos un primer identificador asociado al equipo de usuario, al menos un primer identificador que comprende al menos un identificador privado, en donde el identificador privado es conocido solamente por el equipo de usuario (14), el primer nodo (16) y un segundo nodo (17);
almacenar en el equipo de usuario (14) el al menos un primer identificador y un identificador de usuario asociado al equipo de usuario;
transmitir una solicitud de autorización (301), que comprende el identificador de usuario, desde el equipo de usuario (14) al segundo nodo (17) para iniciar la autenticación del equipo de usuario (14) en el segundo nodo (17);
recibir en el equipo de usuario (14) un mensaje (315) del segundo nodo (17) en donde el mensaje (315) comprende al menos un identificador adicional, B-TID, usado por el equipo de usuario (17) para autenticar el equipo de usuario (14) a un tercer nodo (25);
procesar el mensaje (315) recibido en el equipo de usuario (14); y
generar una clave criptográfica, ks_NAF, para cifrar las comunicaciones entre el equipo del usuario (14) y el tercer nodo (25) en función del mensaje procesado y el identificador privado.

5. Un programa informático que, cuando se ejecuta en un equipo de usuario (14), realiza todas las etapas del método de la reivindicación 4.

6. Un nodo (17), que comprende:

un transceptor adaptado para comunicarse con un equipo de usuario (14), en donde el transceptor está adaptado para recibir una solicitud de autorización (301) que comprende un identificador de usuario, la ID de usuario, asociada al equipo de usuario (14) desde el equipo de usuario (14), en donde el transceptor está adaptado para transmitir un mensaje (315) al equipo de usuario (14), en donde el mensaje (315) comprende al menos un identificador adicional, B-TID, utilizado por el equipo de usuario (14) para autenticar el equipo de usuario (14) a otro nodo (25);
un procesador adaptado para generar una clave criptográfica, ks_NAF, para cifrar las comunicaciones entre el equipo del usuario (14) y el otro nodo (25) en función del mensaje procesado y un identificador privado, en donde además el nodo (17), al recibir la solicitud de autorización (301) que comprende el identificador de usuario, ID de usuario, asociado al equipo de usuario (14) desde equipo de usuario (14) está adaptado para comunicarse con un primer nodo (16) para recuperar un perfil de usuario del equipo de usuario (14) junto con cualquier vector de autenticación requerido, incluyendo dicho vector de autenticación el identificador privado, en donde el identificador privado es conocido solamente por el equipo de usuario (14), el nodo (17) y el primer nodo (16); y

en donde el transceptor está adaptado para transmitir la clave criptográfica al otro nodo (25) en función de un mensaje de autenticación (409) recibido desde el otro nodo (25).

7. Un nodo (17) según la reivindicación 6, en el que el primer identificador es al menos uno de:

un nombre de usuario;
una clave criptográfica pública;
una dirección IP; y
un valor de identificación de la línea que llama.

8. Un nodo (17) según la reivindicación 6, en el que el identificador privado es al menos uno de:

un valor de contraseña; y
una clave criptográfica privada.

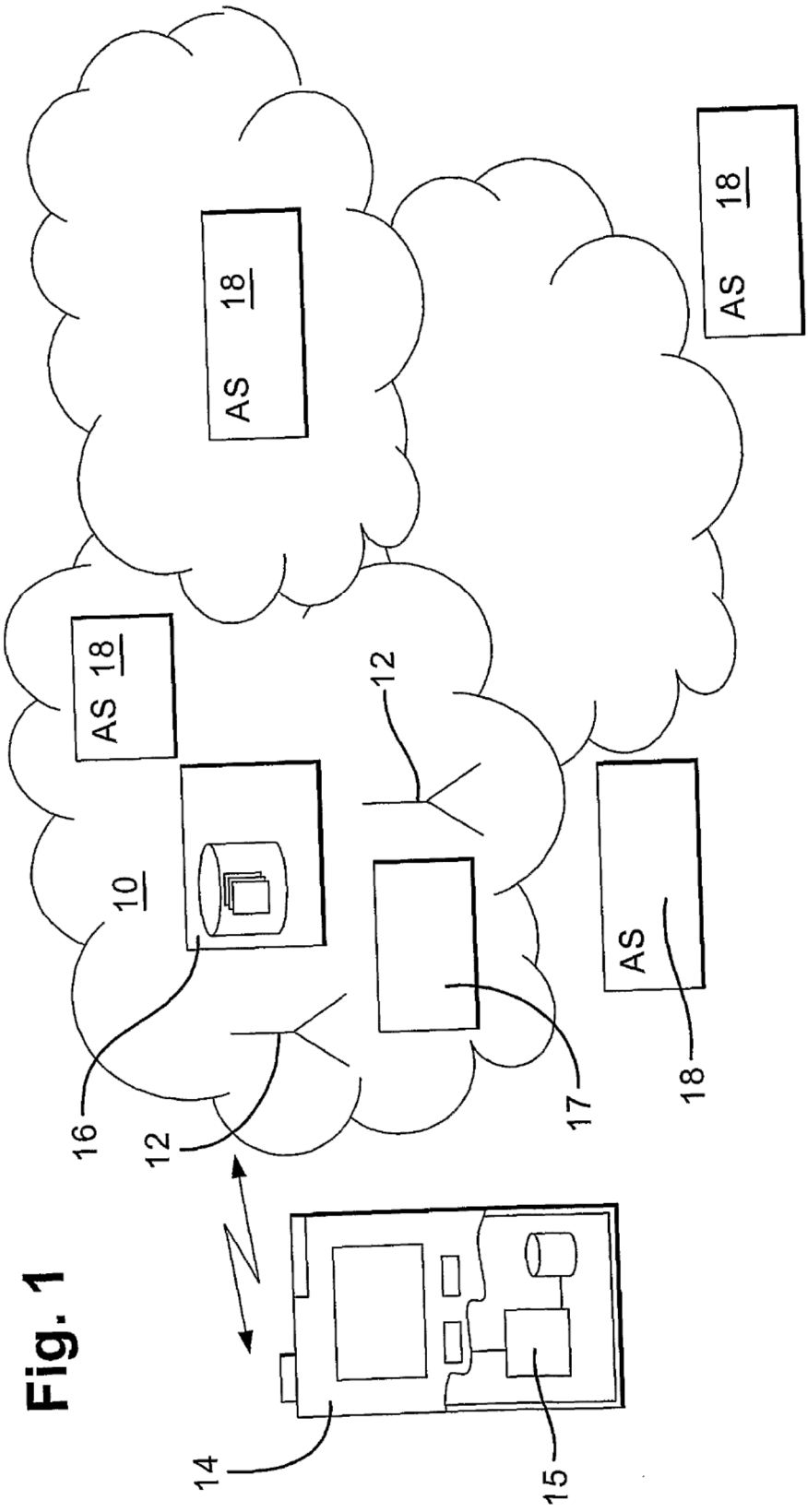

Fig. 1

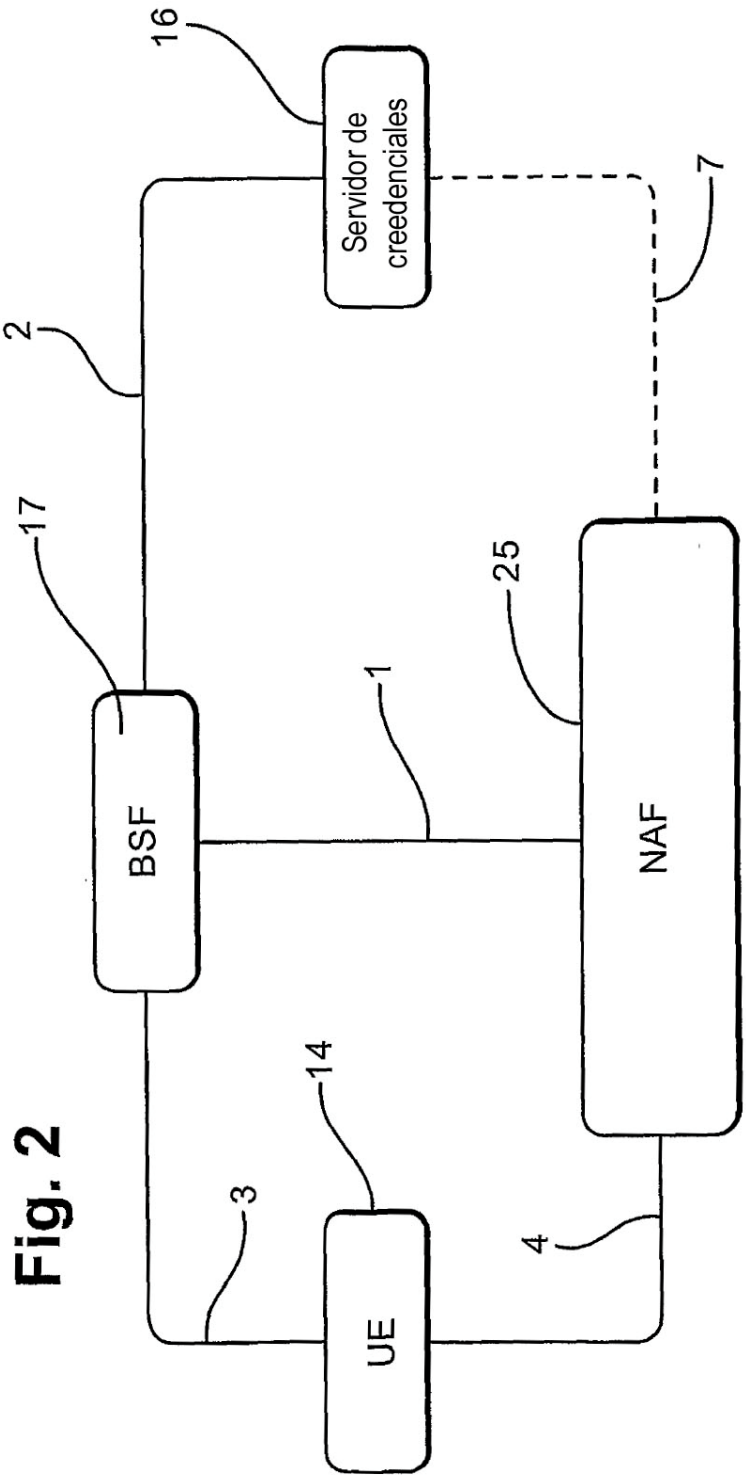

Fig. 2

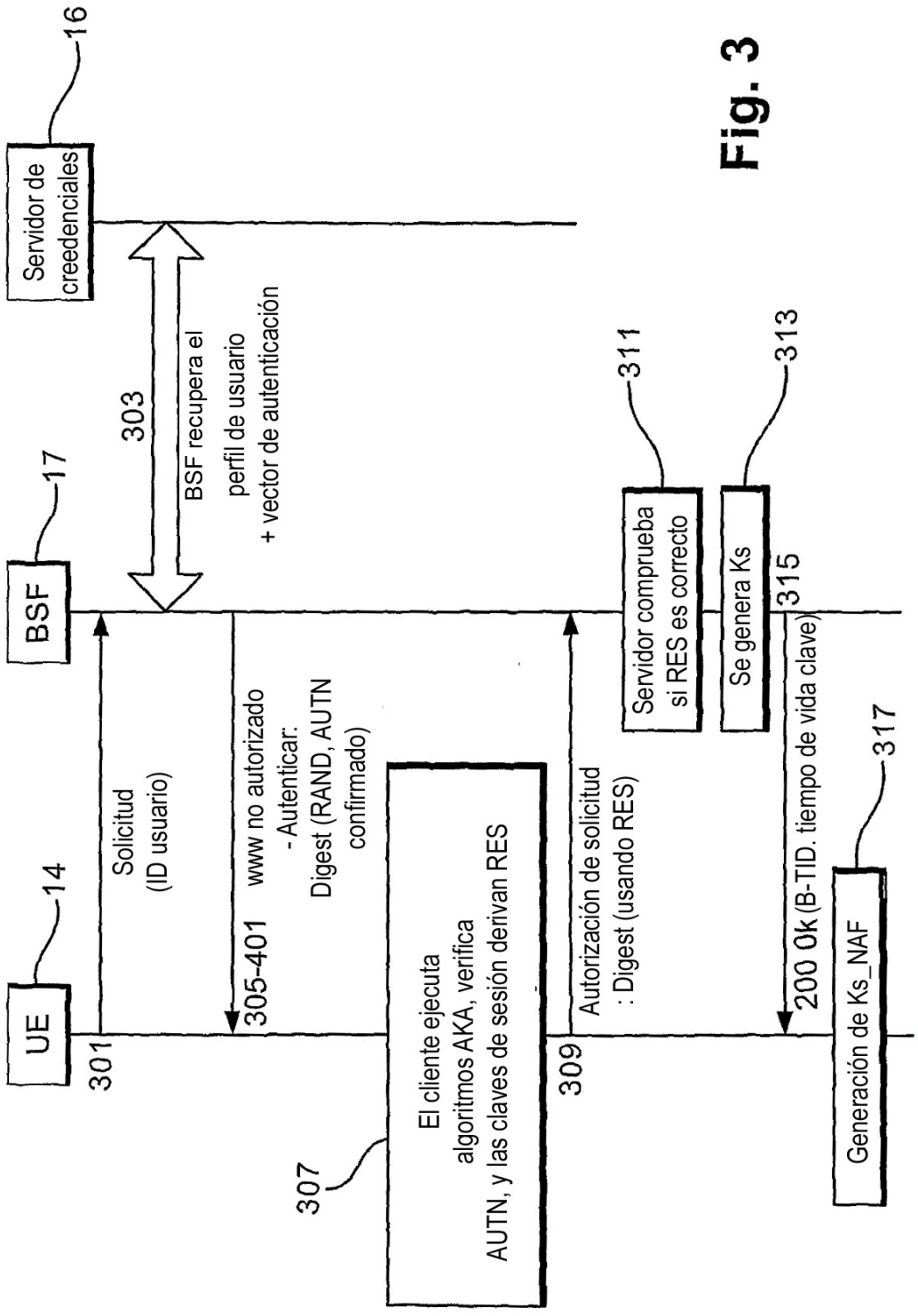
UE
14
BSF
17
Servidor de creedenciales
16
301
Solicitud
(ID usuario)
303
BSF recupera el
perfil de usuario
+ vector de autenticación
305-401
www no autorizado
- Autenticar:
Digest (RAND, AUTN
confirmado)
307
El cliente ejecuta
algoritmos AKA, verifica
AUTN, y las claves de sesión derivan RES
309
Autorización de solicitud
: Digest (usando RES)
311
Servidor comprueba
si RES es correcto
313
Se genera Ks
315
200 Ok (B-TID. tiempo de vida clave)
317
Generación de Ks_NAF

Fig. 3

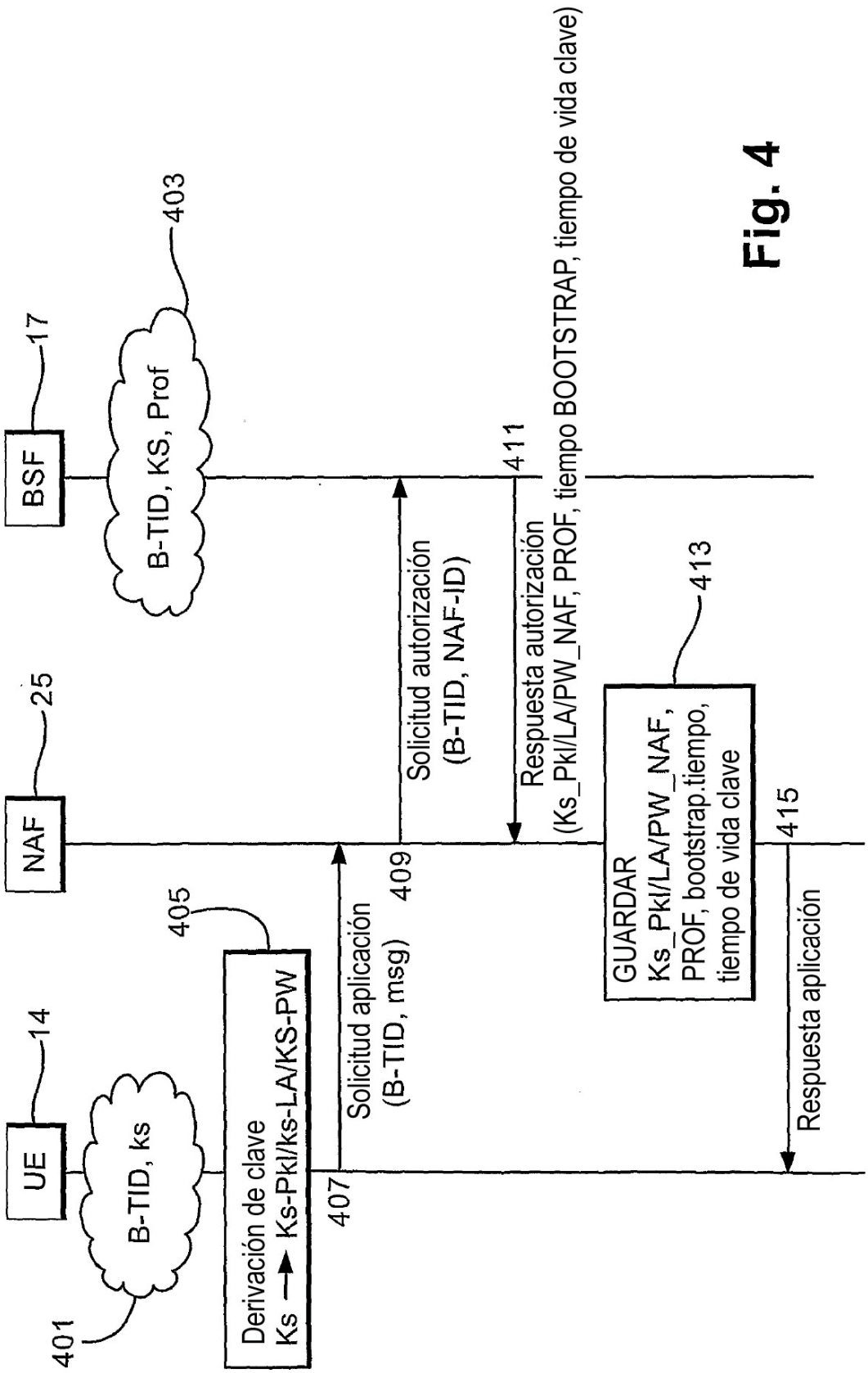
UE
14
NAF
25
BSF
17
B-TID, ks
401
B-TID, KS, Prof
403
Derivación de clave
Ks → Ks-PkI/ks-LA/KS-PW
405
Solicitud aplicación
(B-TID, msg)
407
Solicitud autorización
(B-TID, NAF-ID)
409
Respuesta autorización
(Ks_PkI/LA/PW_NAF, PROF, tiempo BOOTSTRAP, tiempo de vida clave)
411
GUARDAR
Ks_PkI/LA/PW_NAF,
PROF, bootstrap.tiempo,
tiempo de vida clave
413
Respuesta aplicación
415

Fig. 4