(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 584 862**

(51) Int. CI.:

H04L 9/32 (2006.01)
H04K 1/00 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(96) Fecha de presentación y número de la solicitud europea: **21.12.2001 E 01985938 (8)**

(97) Fecha y número de publicación de la concesión europea: **22.06.2016 EP 1348280**

(54) Título: **Autenticación en comunicación de datos**

(30) Prioridad:

27.12.2000 FI 20002858
12.01.2001 FI 20010080

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
29.09.2016

(73) Titular/es:

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

(72) Inventor/es:

HAVERINEN, HENRY

(74) Agente/Representante:

VALLEJO LÓPEZ, Juan Pedro

DESCRIPCIÓN

Autenticación en comunicación de datos

Esta invención se refiere a la autenticación en la comunicación de datos. En particular, la invención se refiere a, pero no se limita a, la autenticación de estaciones móviles y servidores de red que se comunican entre sí a través de una red tal como Internet.

La Internet se usa para compartir información pública. Ya que es un sistema abierto, no debería usarse para compartir información confidencial a menos que se tomen precauciones para proteger la información mediante el uso de contraseñas, el cifrado y similares. Incluso así, si se usan contraseñas, pueden determinarse por los piratas informáticos. En Internet, hay clientes (normalmente ordenadores personales con programas de informáticos) y servidores (ordenadores servidores que ejecutan programas informáticos que les hace proporcionar servicios a los clientes). Normalmente los programas informáticos usados en los clientes y los servidores asumen que sus usuarios son honestos acerca de su identidad. Algunas aplicaciones cliente/servidor se basan en el cliente para limitar sus actividades a las que se les permite hacer, sin ninguna otra aplicación por el servidor. La autenticación fuerte es muy deseable para las transacciones que involucran dinero, datos confidenciales o ambos.

Una forma de mejorar la situación es el uso de los protocolos específicos de autenticación y, si es necesario, los protocolos de cifrado para verificar la autenticidad de un participante y para evitar que unos participantes no autorizados obtengan acceso. Además, estos protocolos pueden usarse normalmente para verificar la integridad de cualquier información intercambiada a través de un enlace de manera que un destinatario puede estar seguro de que los datos recibidos no se han manipulado.

Kerberos es un protocolo diseñado para proporcionar una autenticación fuerte para aplicaciones cliente/servidor usando la criptografía de clave secreta. Al menos se han descrito dos versiones de Kerberos, las versiones 4 y 5. La versión 5 de Kerberos se ha descrito por J. Kohl y C. Neuman en "The Kerberos Network Authentication Service (Version 5)", RFC 1510, septiembre de 1993. Las versiones 4 y 5 también se han descrito por W. Stallings, "Cryptography and Network Security, Principles and Practice", 2ª edición, p. 323-340. Estas dos versiones de Kerberos se describen brevemente en los siguientes párrafos.

La figura 1 muestra una vista general de un sistema Kerberos KS de acuerdo con la versión 4 de Kerberos. El sistema Kerberos KS comprende un cliente c que puede obtener acceso a Internet, un servidor de Kerberos KSS en Internet y un servidor de servicios V para proporcionar un servicio para el que se necesita autenticación. El servidor de Kerberos KSS comprende un servidor de autenticación AS, un servidor de concesión de tickets TGS, y una base de datos DB que comprende unas contraseñas (cifradas) de diferentes clientes. El cliente c contiene un ordenador personal (PC), que comprende un módulo de entrada/salida IO_C (tal como un módem o un adaptador de red) para conectar a Internet, una unidad central de procesamiento CPU_C para procesar los datos y una memoria MEM_C. La memoria tiene una parte no volátil para almacenar las aplicaciones para controlar la CPU_C y una parte de memoria de acceso aleatorio para su uso en el procesamiento de datos. Además, el cliente c tiene una interfaz de usuario UI para interactuar con un usuario. La UI puede solicitar a un usuario dar una contraseña y puede recibir la contraseña. En un sistema Kerberos, las aplicaciones, junto con el ordenador personal, forman el cliente c que puede usar los servicios de un host (ordenador) accesible a través de una red insegura.

La V es un servidor que proporciona el servicio al cliente c. Se autentica al cliente c usando una secuencia de autenticaciones, en la que el cliente c se autentica primero en el AS para obtener una concesión de ticket el ticket $ticket_{tgs}$. Usando el $ticket_{tgs}$ el cliente c puede obtener a continuación una concesión de servicio el ticket $ticket_V$. Este ticket puede usarse a continuación para el servicio. Este procedimiento se explicará en detalle con referencia a las figuras 1 y 2.

Con el fin de trabajar, el sistema Kerberos ya debería tener un primer secreto compartido (o primera clave de autenticación, K_c) conocido por el cliente c, el AS y el TGS. Un segundo secreto compartido (K_v) debería conocerse por el AS, el TGS y el servidor de servicio V, pero no por el cliente c. Estos secretos compartidos se presumen que existen.

Para cualquier secreto específico a conocerse por cualquier participante específico es suficiente con que el participante pueda, cuando sea necesario, obtener el secreto, por ejemplo, preguntando al usuario (siendo el participante un cliente) o solicitándolo a la base de datos (siendo el participante un AS o un TGS). Normalmente, el TGS y el AS están co-localizados, pero en algunos casos el servidor Kerberos KSS también puede distribuirse de manera que el TGS y el AS no están co-localizados.

El funcionamiento del sistema Kerberos KS como una secuencia de etapas se ilustra en la figura 2. En resumen, la figura 2 muestra la mensajería entre el usuario, el cliente c, el servidor de autenticación AS, el servidor de concesión de tickets TGS y el servidor de servicios V. Para mayor comodidad, la notación en el presente documento seguirá la usada en la publicación mencionada anteriormente de Stallings. Las etapas de la figura 2 se describirán a continuación.

Etapa 21: el usuario inicia sesión en el cliente c y solicita un servicio deseado en el servidor de servicios (host) enviando un inicio de sesión y una solicitud de servicio. Para iniciar la sesión, el usuario introduce la contraseña de un cliente K_c que es conocida por él y el servidor de autenticación. La contraseña del cliente es el primer secreto compartido. A partir de ahora, K_c se denomina como una primera clave de autenticación.

Etapa 22: el cliente c envía al AS una solicitud de un ticket de concesión el ticket $ticket_{tgs}$. La solicitud comprende el ID del cliente c (ID_C), el ID del TGS (ID_{tgs}), y una primera marca de tiempo TS_1 que corresponde al momento en que se ha enviado la solicitud.

Etapa 23: el AS forma un $ticket_{tgs}$ usando una segunda clave de autenticación K_{tgs} conocida por el AS y el TGS, pero no por el cliente c. El $ticket_{tgs} = E_{Ktgs} [K_{c,tgs} || ID_C || AD_C || ID_{tgs} || TS_2 || Tiempo\ de\ vida_2]$. E representa un algoritmo de cifrado que usa una segunda clave de autenticación K_{tgs} como su clave de cifrado. $K_{c,tgs}$ es una primera clave de sesión formada por el AS (por ejemplo, una clave aleatoria) para su uso entre el cliente c y el TGS. AD_C es la dirección del cliente c, ID_{tgs} es una identidad del TGS, TS_2 es la segunda marca de tiempo que muestra el momento de la emisión del $ticket_{tgs}$ y $Tiempo\ de\ vida_2$ es el momento de la expiración del $ticket_{tgs}$. Las barras " || " indican una concatenación. El $ticket_{tgs}$ es para usarse más adelante, para obtener los tickets de concesión de servicio ($ticket_V$) para el uso de los diversos servicios. A continuación, el AS cifra los datos usando la K_c de la siguiente manera: $E_{KC} [K_{c,TGS} || ID_{tgs} || TS_2 || Tiempo\ de\ vida_2]$ y envía el $ticket_{tgs}$ y los datos cifrados al cliente c.

Etapa 24: a continuación el cliente c, solicita la K_c de su usuario. El usuario debería conocer la K_c.

Etapa 25: el usuario proporciona al cliente c la K_c.

Etapa 26: mediante el uso de la K_c y la $K_{c,TGS}$, el cliente c descifra los datos cifrados recibidos desde el AS y forma un primer autenticador de cliente, $autenticador_{c1} = E_{Kc,tgs} [ID_C || AD_C || ID_V || TS_3]$. ID_V es el ID del V y TS_3 es el momento de formar el $autenticador_{c1}$. Como lector experto comprenderá que el cliente c solo es capaz de obtener la $K_{c,tgs}$ si conoce la K_c. El $autenticador_{c1}$ se usa posteriormente por el TGS para autenticar al cliente c. El cliente c a continuación, envía una solicitud para un servicio de concesión de ticket ($ticket_V$) al TGS. La solicitud contiene ID_V, $ticket_{tgs}$ y $autenticador_{c1}$.

Etapa 27: el TGS forma el $ticket_V$ y lo envía junto con una segunda clave de sesión cifrada $K_{c,V}$ al cliente c. La segunda clave de sesión se cifra con la primera clave de sesión $K_{c,tgs}$. El $ticket_V$ se forma por el TGS usando el conocimiento de un segundo secreto compartido K_V del V, de la siguiente manera: $ticket_V = E_{KV} [K_{c,V} || ID_C || AD_C || ID_V || TS_4 || Tiempo\ de\ vida_4]$, en el que:

$K_{c,V}$ es una segunda clave de sesión para su uso entre el cliente c y V,
TS_4 es una marca de tiempo que muestra el momento de formar el $ticket_V$, y
$Tiempo\ de\ vida_4$ establece el tiempo de vida del $ticket_V$ para evitar los ataques de repetición después de la expiración del tiempo de vida del $ticket_V$.

Etapa 28: el cliente c envía una solicitud de servicio al V. La solicitud contiene el $ticket_V$ y un segundo autenticador de cliente, $autenticador_{c2}$, en el que $autenticador_{c2} = EK_{C,V} [ID_C || AD_C || TS_5]$. TS_5 es una marca de tiempo que muestra el momento de formar el segundo autenticador de cliente.

Etapa 29: después de que el servidor de servicio V ha examinado el $autenticador_{c2}$, puede autenticarse él mismo al cliente c para una autenticación mutua. Esto se hace respondiendo con el TS_5, incrementado en 1 y cifrado con la $K_{c,V}$, de tal manera que el cliente c puede confiar en que V sea el servidor correcto ya que puede cifrar con la misma $K_{c,V}$. La respuesta es, por lo tanto $E_{Kc,v} [TS_5 + 1]$.

La etapas 22 y 23 se producen una vez por cada sesión de inicio de sesión de usuario. El $ticket_{tgs}$ es por lo tanto válido durante la duración de la sesión de inicio de sesión de usuario (o hasta que caduque). Las etapas 26 y 27 se producen una vez por cada tipo de servicio. En otras palabras, para cada tipo de servicio, se aplica y se concede un $ticket_V$ diferente. Las etapas 28 y 29 se producen una vez por cada sesión de servicio de un tipo de servicio concedido.

La descripción de la figura 2 ilustra cómo Kerberos puede proporcionar una autenticación centralizada a una pluralidad de diferentes servidores de servicios que confían en el servidor Kerberos KSS (la combinación del AS y el TGS). El KSS tiene un segundo secreto compartido diferente Kv con cada V y cada V está registrado en el KSS.

El sistema de la figura 1 representa un dominio: por ejemplo, un solo empleador en un país o una ciudad es propietario de todas las entidades.

Kerberos versión 5 proporciona algunas mejoras respecto a la versión 4, que incluyen permitir una pluralidad de dominios Kerberos a interoperar de manera que un servidor de autenticación AS puede conceder tickets de concesión de servicio $ticket_V$ a los servidores de servicio V de diferentes dominios de autenticación.

A continuación, se describirá con referencia a la figura 1 el funcionamiento de un sistema Kerberos de acuerdo con Kerberos versión 5. En Kerberos versión 5, la autenticación y la distribución de claves se inicia con un procedimiento de intercambio de servicio de autenticación, en el que el cliente c solicita un $ticket_{tgs}$ del AS y el AS forma y envía el $ticket_{tgs}$ y otros parámetros cifrados con la K_c en respuesta. El $ticket_{tgs}$ y la clave $K_{c,tgs}$ se usarán como credenciales para obtener los tickets de concesión de servicio ($ticket_V$) para usar los servicios. El intercambio de servicio de autenticación es el siguiente:

(1) desde c a AS, un mensaje KRB_AS_SOL = Opciones || ID_C || $Dominio_C$ || ID_{tgs} || tiempos || $Mensaje\ aleatorio_1$
(2) desde el AS al c, mensaje KRB_AS_RES = $Dominio_C$ || ID_C || $ticket_{tgs}$ || E_{Kc} [$K_{c,TGS}$ || tiempos || $mensaje\ aleatorio_1$ || $dominio_{tgs}$ || ID_{tgs}]

en la que

$$ticket_{tgs} = E_{Ktgs}[indicadores \,||\, K_{c,tgs} \,||\, dominio_C \,||\, ID_C \,||\, AD_C \,||\, tiempos]$$

y en la que

opciones	diversas opciones usadas para solicitar que determinados indicadores se establezcan en el ticket devuelto
indicadores	diversos indicadores de mensajes para su uso en el protocolo Kerberos versión 5
$dominio_c$	dominio del cliente
$dominio_{tgs}$	dominio del TGS
tiempos	tiempo de inicio, tiempo de caducidad y tiempo de renovación del $ticket_{tgs}$
$mensaje\ aleatorio_1$	un valor aleatorio generado por el cliente para garantizar que la respuesta es reciente (no una copia de una respuesta anterior)

Se debería tener en cuenta que los diferentes tipos de campos pueden cifrarse juntos, porque todos los diferentes tipos se representan en última instancia, por los códigos binarios (ceros y unos), que pueden aplicarse dentro de la misma función, independientemente de su origen.

La K_c se usa para cifrar la $K_{c,tgs}$ y otros parámetros en el mensaje KRB_AS_RES. Debería observarse que en Kerberos, cualquiera puede solicitar un $ticket_{tgs}$ pero solo el cliente válido es capaz de usarlo. Debido a que solo el cliente válido conoce la K_c, otros no son capaces de descifrar la $K_{c,tgs}$ que se requiere cuando se usa el $ticket_{tgs}$. En Kerberos, la K_c solo se usa en el mensaje de KRB_AS_RES para cifrar la $K_{c,tgs}$ y otros parámetros. Se usan diferentes claves de sesión en lugar de la K_c en todos los demás mensajes de Kerberos.

Con los $ticket_{tgs}$ y la $K_{c,tgs}$, el cliente c es capaz de obtener nuevas versiones del $ticket_V$ y la $K_{c,V}$ del TGS. Las nuevas versiones pueden usarse además para obtener un servicio de los V.

La autenticación también puede necesitarse en las redes de comunicaciones móviles. En la actualidad, existen diversos tipos de redes de comunicaciones móviles, con diferentes tipos de procedimientos de autenticación. Normalmente, las redes de comunicaciones móviles digitales, tales como GSM, proporcionan la autenticación digital de un abonado con el fin de soportar la facturación del operador de red que explota la red. En GSM, la autenticación se basa en el uso de tripletes GSM, que se generan por los módulos de identidad de suscriptor dedicado (SIM) en un extremo del abonado y en un centro de autenticación (AuC) del operador de red. El AuC es normalmente una funcionalidad proporcionada por un registro de localización base (HLR) de una red GSM. En GSM, los tripletes GSM pueden usarse de una manera bastante relajada, de tal manera que su orden no es estrictamente fijo. En el próximo sistema de telecomunicaciones móviles universal (UMTS) la autenticación se diferencia de la de GSM. Una visión general de la autenticación en UMTS se proporciona en la especificación técnica (TS) del proyecto de asociación de 3ª generación (3GPP) 33.102 V3.6.0 (2000-10), párrafo 6.3, y abstraído a continuación:

En UMTS, los módulos de autenticación de usuario se denominan como módulos de identidad de abonado UMTS (USIM) y el AuC genera unos vectores de autenticación, o quintetos, que comprenden los siguientes componentes: un número aleatorio RAND, una respuesta esperada XRES, una clave de cifrado CK, una clave de integridad IK y un testigo de autenticación AUTN. Cada vector de autenticación es bueno para una autenticación. RAND, XRES y CK corresponden aproximadamente a RAND, SRES y K_c de GSM, pero específicamente AUTN y su uso forman una diferencia significativa sobre GSM. El AUTN se basa, entre otros, en un número de secuencia SQN correspondiente a un vector de autentificación específico.

El documento US 5 535 276 desvela como se describe en su resumen que en un sistema, tal como un sistema que usa un protocolo de Kerberos, los usuarios del sistema tienen cada uno una clave de cifrado asimétrico asociada. La seguridad de las comunicaciones a través del sistema se aumenta por un primer usuario que genera una clave de cifrado asimétrico temporal que tiene una primera parte de clave temporal y una segunda parte de clave temporal asociada. La segunda parte de clave temporal se cifra por el primer usuario con la primera parte de clave privada de la primera clave de cifrado de usuario para formar un primer mensaje cifrado.

Otro usuario, preferentemente un servidor de autenticación, aplica la segunda parte de clave privada y la parte de clave pública de la criptografía de la primera clave de cifrado de usuario al primer mensaje cifrado para descifrar la segunda parte de clave temporal y por lo tanto autenticar al primer usuario en el servidor de seguridad. A continuación, el servidor de autenticación cifra el primer mensaje cifrado con la segunda parte de clave privada de la primera clave de cifrado de usuario para formar un segundo mensaje cifrado. El primer usuario aplica a continuación la parte de clave pública de la primera clave de cifrado de usuario para descifrar el segundo mensaje cifrado y obtener la segunda parte de clave temporal, autenticando de este modo al servidor de seguridad para el primer usuario.

El documento WO00/02406 proporciona un método, que permite a los clientes en una red IP móvil (IP, protocolo de Internet) generar una K_c usando un módulo de identidad de abonado (SIM) de un operador de GSM. Los operadores GSM tienen unas bases de datos que contienen las identidades de los abonados y sus datos secretos. En GSM, el secreto almacenado en un SIM se denomina como Ki. El SIM tiene la capacidad de generar una clave de sesión GSM K_{gsm}, una respuesta firmada de forma cifrada unidireccional SRES de un desafío RAND basado en el secreto Ki. Este procedimiento del documento WO00/02406 se muestra como una serie de etapas 31 a 37 en la figura 3.

Un servidor de seguridad SS (correspondiente a un KSS) envía (etapa 31) una solicitud de ID de autenticación a un terminal TE1 (correspondiente a un cliente c). El cliente c responde (etapa 32) mediante su identidad de abonado móvil internacional (IMSI). El servidor de seguridad envía (etapa 33) una solicitud de información de seguridad a un servidor proxy. El servidor proxy adquiere (etapa 34) la información de seguridad a partir de un registro de localización base de un operador GSM cuyo SIM está usándose, que contiene un triplete GSM (K_{gsm}, RAND y desafío). El servidor proxy envía (etapa 35) el triplete GSM al servidor de seguridad. El servidor de seguridad envía (etapa 36) el desafío RAND al cliente c.

Etapa 37: El cliente c forma su propia versión de la clave de sesión GSM K_{gsm} y el SRES correspondiente a su Ki y el RAND recibidos. A continuación, el cliente c envía de vuelta la SRES de manera que el servidor de seguridad puede compararla con la SRES recibida en el triplete GSM desde el servidor proxy. Si la SRES proporcionada por el servidor proxy y la SRES generada por el cliente c coinciden, se realiza una autenticación positiva y el servidor de seguridad pueden empezar a usar la clave de sesión GSM K_{gsm} como la K_c entre cliente c y el servidor de seguridad (es decir, un servidor Kerberos).

El documento WO00/02406 combina la tecnología GSM con la tecnología Kerberos. En lugar de la autenticación de un teléfono móvil inalámbrico por una red GSM usando los tripletes GSM y comparando las diferentes respuestas de uno contra el otro, el SIM se usa para generar una respuesta a un desafío recibido desde una red IP móvil. La respuesta se envía a continuación a la red IP móvil para su comparación con la respuesta correcta para la Ki y el RAND para detectar que el cliente c es genuino y que no está intentando acceder ilegítimamente a los servicios usando una IMSI de otro cliente.

La autenticación SIM GSM y la generación de claves para IP móvil de H. Haverinen (draft-haverinen-mobileip-gsmsim-01.txt) es un proyecto de Internet que especifica, de acuerdo con su resumen, un mecanismo para la autenticación de acceso a la red IP móvil y la distribución de claves usando el módulo de identidad de suscriptor GSM (SIM). El mecanismo usa nuevos subtipos de las extensiones de distribución de claves generalizadas para la solicitud de registro ip móvil y la respuesta de registro.

El modo de autenticación SIM GSM para IKE por J. Rinnemaa es un proyecto de Internet (rinnemaa-ipsra-gsmsimmode-00.txt) que presenta, de acuerdo con su resumen, un método de autenticación de desafío-respuesta basado en el módulo de identidad de suscriptor GSM (SIM). El método se usa para autenticar un usuario IPSec remoto en una pasarela de seguridad. Los ejemplos en el documento se basan en el modo principal IKE modificado. En la fase de autenticación, se genera un secreto compartido utilizando el SIM GSM y a continuación se usa también para autenticar el intercambio IKE.

De acuerdo con un primer aspecto de la invención, se proporciona un método de autenticación de un cliente, que comprende las etapas de:

enviar la información de identidad de cliente a un bloque de autenticación, siendo la información de identidad de cliente una identidad de abonado móvil internacional;
obtener al menos un desafío y al menos un primer secreto para el bloque de autenticación basado en un secreto del cliente específico para el cliente;
formar las primeras credenciales;
formar una primera clave de autenticación usando el al menos un primer secreto;
cifrar las primeras credenciales usando la primera clave de autenticación;
enviar el al menos un desafío y las primeras credenciales cifradas al cliente;
formar la primera clave de autenticación en el cliente;
descifrar las primeras credenciales cifradas en el cliente usando la primera clave de autenticación; caracterizado por que
el cifrado de las primeras credenciales es independiente del bloque de autenticación que recibe cualquier

respuesta basada en el secreto del cliente.

El método del primer aspecto puede entenderse como un cliente que envía un mensaje de solicitud a un bloque de autenticación y responde directamente al mensaje de solicitud, el cliente recibe las primeras credenciales cifradas que contienen un ticket de autenticación y descifra las primeras credenciales usando el secreto específico para el cliente. Esto permite al cliente obtener la primera credencial sin una etapa intermedia de enviar de vuelta al bloque de autenticación cualquier respuesta basada en el secreto del cliente.

Preferentemente, el bloque de autenticación se localiza en una red de comunicación de datos. Incluso más preferentemente, un servidor de red proporciona el bloque de autenticación.

Preferentemente, las primeras credenciales se cifran antes de que el bloque de autenticación reciba cualquier respuesta basada en el secreto del cliente desde el cliente.

Preferentemente, las primeras credenciales cifradas se envían junto con el al menos un desafío al cliente.

Incluso más preferentemente, no se envía una respuesta basada en el secreto del cliente desde el cliente al bloque de autenticación. No enviar ninguna respuesta de este tipo hace que sea mucho más posible el uso de la totalidad del primer secreto en formar la primera clave de autenticación, lo que refuerza criptográficamente a la misma.

Preferentemente, el desafío es un código aleatorio.

Preferentemente, la formación de la primera clave de autenticación se basa en dos o más primeros secretos. Esto refuerza criptográficamente aún más la primera clave de autenticación.

El método de la invención se basa en un nuevo enfoque para un problema de crear un primer secreto compartido entre un bloque de autenticación y el cliente. En la invención, se han dado cuenta de que es posible formar las primeras credenciales, la primera clave de autenticación y cifrar las primeras credenciales con la primera clave de autenticación cuando el bloque de autenticación obtiene el desafío y el primer secreto. La criptografía se usa tanto para la autentificación indirecta como para la entrega de las primeras credenciales. Solo si el cliente ha resuelto la primera clave de autenticación correctamente, puede descifrar las primeras credenciales. El cliente puede formar a continuación un mensaje de solicitud de servicio usando criptográficamente las primeras credenciales descifradas y de este modo puede llegar a autentificarse como un subproducto de la formación del mensaje de solicitud de servicio. Esto proporciona unas ventajas significativas. El método permite una autenticación segura y rápida, en la que se forman las primeras credenciales y a continuación se envían con el al menos un desafío sin necesidad de autenticar primero por separado al cliente. Esto hace que el método pueda usarse con diversos métodos de autenticación conocidos, incluyendo las versiones 4 y 5 de Kerberos y también reduce la cantidad de señales de comunicaciones que necesitan enviarse y recibirse. El método hace además innecesario un bloque de autenticación para almacenar el primer secreto después de formar la primera clave de autenticación y las primeras credenciales. Esto reduce la complejidad del proceso de autenticación y hace que sea más rápido, debido a que algunos mensajes se vuelven redundantes. La autenticación es también más fuerte, si todos los datos contenidos por el primer secreto se usan en la formación de la primera clave de autenticación. Esto no era posible en la técnica anterior, en la que se transmitía una respuesta firmada (SRES) desde el cliente al bloque de autenticación como texto legible de tal manera que cualquier tercera parte la podría haber obtenido fácilmente.

Preferentemente, la etapa de obtención de al menos un desafío y al menos un primer secreto para el bloque de autenticación basado en un secreto del cliente específico para el cliente se produce antes de la necesidad de autenticar al cliente. Incluso más preferentemente, se obtiene una colección de desafíos y primeros secretos suficientes para la formación de al menos dos primeras credenciales para el cliente en un lote. Más preferentemente, se obtiene una colección de este tipo para un grupo de clientes, de tal manera que el bloque de autenticación tiene los datos ya disponibles para autenticar a cualquiera de los clientes del grupo sin necesidad de obtenerlos primero. Esto permite una autenticación más rápida de un grupo de clientes que pertenecen a la misma organización o grupo como los datos relativos a sus secretos del cliente que ya están disponibles para el bloque de autenticación y no necesitan obtenerse por separado en cada autenticación de un cliente.

Preferentemente, la información de identidad de cliente es la identidad de abonado. Incluso más preferentemente, el bloque de autenticación forma una identificación para su uso en unos mensajes de autenticación adicionales para el cliente de tal manera que el identificador de abonado no necesita incluirse en los mismos.

Preferentemente, la primera clave de autenticación se forma usando una función hash de al menos un primer secreto. Incluso más preferentemente, la primera clave de autenticación se forma usando una función hash de al menos el primer secreto y el protector de ataque de repetición. El uso del protector de ataque de repetición en la formación de la primera clave de autenticación y el uso de una función hash hace posible que el bloque de autenticación autentique al cliente.

En una realización alternativa, la formación de la primera clave de autenticación se basa en una parte de un primer

secreto.

Preferentemente, la formación de las primeras credenciales comprende las subetapas de:

cifrar la primera información correspondiente al cliente con una segunda clave de autenticación no conocida por el cliente; y
verificar que la primera información se ha cifrado usando la segunda clave de autenticación.

Preferentemente, el método comprende además la etapa de generar un mensaje de solicitud de servicio usando criptográficamente las primeras credenciales descifradas.

Preferentemente, la primera información contiene al menos uno de los elementos seleccionados de un grupo que consiste en: la identidad del cliente, la identidad del servidor de concesión de tickets, el dominio del cliente, y una marca de tiempo.

Preferentemente, el cliente es un terminal móvil multifuncional que tiene al menos una funcionalidad de telecomunicaciones móviles y una funcionalidad de comunicaciones de redes de paquetes de datos. Aún más preferentemente, la funcionalidad de telecomunicaciones móviles soporta el sistema global para comunicaciones móviles. Esto proporciona una gran base de módulos de identidad de abonado ya existentes (SIM) durante el funcionamiento para autenticar a los clientes en diferentes redes de comunicación de datos distintas de las redes de telecomunicaciones.

Preferentemente, la funcionalidad de telecomunicaciones móviles soporta un sistema de telecomunicaciones en el que se usan vectores de autenticación ordenados.

Preferentemente, el al menos un desafío y el al menos un primer secreto corresponden al menos a un número de secuencia específico y transmitir el al menos un número de secuencia, y el método comprende además las etapas de:

mantener un contador de número de secuencia en el cliente;
obtener en el cliente el número de secuencia usando al menos uno de entre el al menos un desafío y el al menos un primer secreto; y
comprobar en el cliente si el número de secuencia está en un intervalo correcto acerca del contador de número de secuencia.

Preferentemente, el método comprende además la etapa de iniciar la sincronización del número de secuencia en el caso de que el número de secuencia no esté en el intervalo correcto acerca del contador de número de secuencia.

Preferentemente, el inicio de la sincronización del número de secuencia comprende una etapa de formar un mensaje de solicitud de sincronización que contiene al menos un desafío fuera del al menos un desafío.

Preferentemente, el inicio de la sincronización del número de secuencia comprende una etapa de formar un mensaje de solicitud de sincronización contenido en el contador de número de secuencia.

Preferentemente, el mensaje de solicitud de sincronización comprende además un código de autenticación de mensaje.

Preferentemente, la comprobación de las primeras credenciales se basa en el número de secuencia y comprende las etapas de mantener un contador de número de secuencia por el cliente; y determinar si se ha calculado al menos un parámetro de las primeras credenciales usando el número de secuencia. Preferentemente, la determinación de si se ha calculado al menos un parámetro de las primeras credenciales usando el número de secuencia se basa en el número de secuencia y una operación or exclusiva.

De acuerdo con un segundo aspecto de la invención, se proporciona un método de autenticación de un cliente, que comprende las etapas de:

enviar una información de identidad de cliente a un bloque de autenticación, siendo la información de identidad de cliente una identidad de abonado móvil internacional;
recibir por el cliente, al menos, uno de los desafíos y las primeras credenciales cifradas desde el bloque de autenticación;
formar en el cliente un primer secreto basándose en un secreto del cliente y el desafío;
formar una primera clave de autenticación en el cliente usando el primer secreto; y
descifrar la primera clave de autenticación en el cliente usando las primeras credenciales cifradas;

caracterizado por que

el descifrado de las primeras credenciales cifradas es independiente de enviar cualquier respuesta basada en secreto del cliente desde el cliente al bloque de autenticación.

De acuerdo con un tercer aspecto de la invención, se proporciona un método de autenticación de un cliente, que comprende las etapas de:

recibir por un bloque de autenticación una información de identidad de cliente desde un cliente, siendo la información de identidad de cliente una identidad de abonado móvil internacional;
obtener para el bloque de autenticación al menos un desafío y al menos un primer secreto basado en un secreto del cliente específico para el cliente;
formar las primeras credenciales;
formar una primera clave de autenticación usando el al menos un primer secreto;
cifrar las primeras credenciales usando la primera clave de autenticación;
enviar el al menos un desafío y las primeras credenciales cifradas al cliente;
recibir desde el cliente un mensaje que contiene una primera información; y
comprobar si se han usado las primeras credenciales para procesar criptográficamente la primera información;

caracterizado por que

el cifrado de las primeras credenciales es independiente del bloque de autenticación que recibe cualquier respuesta basándose en el secreto del cliente desde el cliente.

De acuerdo con un cuarto aspecto de la invención, se proporciona un método de autenticación de un cliente, que comprende las etapas de:

enviar la información de identidad de cliente a un bloque de autenticación, siendo la información de identidad de cliente una identidad de abonado móvil internacional;
obtener al menos un desafío y al menos un primer secreto por el bloque de autenticación basado en un secreto del cliente específico para el cliente;
formar las primeras credenciales;
formar una primera clave de autenticación usando el al menos un primer secreto;
cifrar las primeras credenciales usando la primera clave de autenticación por el bloque de autenticación;
enviar el al menos un desafío y las primeras credenciales cifradas al cliente por el bloque de autenticación;
formar la primera clave de autenticación en el cliente;
descifrar las primeras credenciales cifradas en el cliente usando la primera clave de autenticación; y
autenticar al cliente usando las primeras credenciales.

De acuerdo con un quinto aspecto de la invención, se proporciona un sistema de autenticación, que comprende un bloque de autenticación y un cliente; y:

una primera entrada en el bloque de autenticación para recibir una información de identidad de cliente, siendo la información de identidad de cliente una identidad de abonado móvil internacional;
una segunda entrada en el bloque de autenticación para recibir al menos un desafío y al menos un primer secreto basado en un secreto específico para el cliente;
un primer procesador en el bloque de autenticación

para formar las primeras credenciales;
para formar una primera clave de autenticación usando el al menos un primer secreto; y
para cifrar las primeras credenciales usando la primera clave de autenticación;

una salida en el bloque de autenticación para proporcionar el al menos un desafío y las primeras credenciales cifradas al cliente; y
un primer procesador en el cliente para formar la primera clave de autenticación y para descifrar las primeras credenciales cifradas usando la primera clave de autenticación;

caracterizado por que

el cifrado de las primeras credenciales es independiente del bloque de autenticación que recibe cualquier respuesta basada en el secreto del cliente desde el cliente

De acuerdo con un sexto aspecto de la invención, se proporciona un cliente a un sistema de autenticación que comprende un bloque de autenticación; comprendiendo el cliente:

una primera salida para proporcionar al bloque de autenticación una información de identidad de cliente, siendo la información de identidad de cliente una identidad de abonado móvil internacional;
una primera entrada para recibir al menos un desafío y las primeras credenciales cifradas;

un primer procesador

para formar un primer secreto basándose en un secreto del cliente y el desafío;
para formar una primera clave de autenticación usando el primer secreto; y
para descifrar las primeras credenciales cifradas usando la primera clave de autenticación;

caracterizado por que

el descifrado de las primeras credenciales cifradas es independiente de enviar cualquier respuesta basada en el secreto del cliente desde el cliente al bloque de autenticación.

De acuerdo con un séptimo aspecto de la invención, se proporciona un bloque de autenticación para un sistema de autenticación que comprende un cliente; comprendiendo el bloque de autenticación:

una primera entrada para recibir una información de identidad de cliente, siendo la información de identidad de cliente una identidad de abonado móvil internacional;
una segunda entrada para recibir al menos un desafío y al menos un primer secreto basado en un secreto específico para el cliente;
un primer procesador

para formar las primeras credenciales;
para formar una primera clave de autenticación usando el al menos un primer secreto; y
para cifrar las primeras credenciales usando la primera clave de autenticación;

una salida para proporcionar al cliente el al menos un desafío y las primeras credenciales cifradas;
la primera entrada que está adaptada además para recibir desde el cliente un mensaje que contiene una primera información;
y el primer procesador que está adaptado además para comprobar si se han usado las primeras credenciales para procesar criptográficamente la primera información;

caracterizado por que

el cifrado de las primeras credenciales es independiente del bloque de autenticación que recibe cualquier respuesta basada en el secreto del cliente desde el cliente.

De acuerdo con un octavo aspecto de la invención, se proporciona un producto de programa informático para controlar un cliente; comprendiendo el producto de programa informático:

un código ejecutable por ordenador para permitir al cliente enviar una información de identidad de cliente a un bloque de autenticación, siendo la información de identidad de cliente una identidad de abonado móvil internacional;
un código ejecutable por ordenador para permitir al cliente recibir desde el bloque de autenticación al menos un desafío y las primeras credenciales cifradas;
un código ejecutable por ordenador para permitir al cliente formar un primer secreto basándose en un secreto del cliente y el desafío;
un código ejecutable por ordenador para permitir al cliente formar una primera clave de autenticación usando el primer secreto; y
un código ejecutable por ordenador para permitir al cliente descifrar las primeras credenciales cifradas usando la primera clave de autenticación;

caracterizado por que

el descifrado de las primeras credenciales cifradas es independientes de enviar cualquier respuesta basada en el secreto del cliente desde el cliente al bloque de autenticación.

De acuerdo con un noveno aspecto de la invención, se proporciona un producto de programa informático para controlar un bloque de autenticación con el fin de permitir que el bloque de autenticación autentique un cliente, comprendiendo el producto de programa informático:

un código ejecutable por ordenador para permitir que el bloque de autenticación reciba una información de identidad de cliente desde un cliente, siendo la información de identidad de cliente una identidad de abonado móvil internacional;
un código ejecutable por ordenador para permitir que el bloque de autenticación obtenga al menos un desafío y al menos un primer secreto basado en un secreto específico para el cliente;
un código ejecutable por ordenador para permitir que el bloque de autenticación forme las primeras credenciales;
un código ejecutable por ordenador para permitir que el bloque de autenticación forme una primera clave de

autenticación usando el al menos un primer secreto;
un código ejecutable por ordenador para permitir que el bloque de autenticación cifre las primeras credenciales usando la primera clave de autenticación;
un código ejecutable por ordenador para permitir que el bloque de autenticación envíe el al menos un desafío y las primeras credenciales cifradas al cliente;
un código ejecutable por ordenador para permitir que el bloque de autenticación reciba desde el cliente un mensaje que contenga la primera información; y
un código ejecutable por ordenador para permitir que el bloque de autenticación compruebe si se han usado las primeras credenciales para procesar criptográficamente la primera información; caracterizado por que el cifrado de las primeras credenciales es independiente de recibir cualquier respuesta basada en el secreto específico para el cliente desde el cliente.

Las realizaciones de un aspecto se aplican también a otros diversos aspectos de la invención. En aras de la brevedad, las realizaciones no se han repetido en relación con cada aspecto de la invención. Un lector experto apreciará las ventajas de los diversos aspectos basándose en las ventajas del primer aspecto de la invención.

A continuación se describirá la invención, solo a modo de ejemplo, con referencia a los dibujos adjuntos, en los que:

la figura 1 muestra una visión general de un sistema Kerberos de acuerdo con Kerberos versión 4;
la figura 2 muestra el funcionamiento del sistema Kerberos de la figura 1;
la figura 3 muestra un procedimiento de autenticación del documento WO 0002406;
la figura 4 es un diagrama de bloques que muestra un cliente de acuerdo con una realización preferida de la invención;
la figura 5 es un diagrama de bloques que muestra un servidor de autenticación de acuerdo con la realización preferida de la invención;
la figura 6 muestra el funcionamiento de un sistema Kerberos modificado de acuerdo con una realización preferida de la invención;
la figura 7 muestra un diagrama de bloques de un sistema de autenticación de red de área local inalámbrica de acuerdo con una realización de la invención;
la figura 8 muestra un procedimiento de autenticación del sistema de autenticación de la figura 7;
la figura 9 muestra un procedimiento de autenticación en el cliente de acuerdo con otra realización más de la invención; y
la figura 10 muestra la construcción de los parámetros AUTS.

Las figuras 1 a 3 se han descrito anteriormente.

La figura 4 es un diagrama de bloques que muestra un cliente c de acuerdo con una realización preferida de la invención. El cliente c comprende un bloque de funcionalidad de telefonía Tel, un bloque de funcionalidad de terminal IP, una IP para conectarse a una red IP, una memoria ROM no volátil, una memoria de acceso aleatorio RAM_C, una interfaz de usuario UI_C, un lector de SIM con un SIM en el mismo, un software SW_C almacenado en la ROM_C, y una unidad de procesamiento central CPU_C para ejecutar el $software_C$ y controlar el funcionamiento del cliente c en consecuencia. El bloque de funcionalidad de telefonía Tel proporciona la funcionalidad de telefonía convencional, tal como hacer llamadas telefónicas y una funcionalidades de comunicación moderna, tales como hacer llamadas de datos, enviar o recibir faxes, e-mails. Normalmente, el Tel es compatible con el GSM fase 2+. Puede soportar además el servicio general de radiocomunicaciones por paquetes (GPRS), que es un servicio de comunicaciones basado en paquetes construido sobre GSM. En ese caso, el cliente c soporta dos tipos diferentes de redes de paquetes de datos. El funcionamiento del cliente c se describirá en detalle con referencia a la figura 6.

La figura 5 muestra un diagrama de bloques de un servidor de autenticación AS de acuerdo con la realización preferida de la invención. El servidor de autenticación AS comprende un bloque de entrada/salida IO_{AS}, una base de datos de claves (posiblemente distribuida geográficamente) DB para almacenar las claves aprobadas como tales o de forma cifrada, una memoria no volátil ROM_{AS}, una memoria de acceso aleatorio RAM_{AS}, un software SW_{AS} almacenado en la ROM_{AS}, un acceso a un centro de autenticación AuC de una red de telecomunicaciones (normalmente de una red GSM), y una unidad central de procesamiento CPU_{AS} para ejecutar el $software_{AS}$ y controlar el funcionamiento del AS en consecuencia. El funcionamiento del servidor de autenticación se describirá en detalle con referencia a la figura 6.

La figura 6 muestra el funcionamiento de un sistema Kerberos modificado de acuerdo con la realización preferida de la invención. El sistema comprende el cliente c de la figura 4 y el servidor de autenticación AS de la figura 5. Los números de referencia correspondientes se han aplicado a los mensajes y a las etapas correspondientes descritas en relación con las figuras 1 y 2. A continuación, se describirán las etapas.

Etapa 61: El SIM proporciona la identidad de abonado móvil internacional (IMSI) de un abonado de la red de telecomunicaciones (cuyo SIM es este) a un cliente c (nodo móvil, el ID del TGS (ID_{tgs}), y una primera marca de tiempo o un número al azar (como un protector de ataque de repetición, o un $mensaje\ aleatorio_1$) correspondiente al momento en que se envía la solicitud.

Etapa 62: El cliente c envía un mensaje KRB_AS_SOL, es decir, una solicitud $ticket_{tgs}$, que comprende el IMSI, el ID_{tgs} y el mensaje aleatorio$_1$ al AS.

Etapa 63: El AS solicita n (uno o más) tripletes GSM de un AuC de la red de telecomunicaciones móviles que está identificado por la IMSI. Estos tripletes se forman usando una función criptográfica y un secreto de abonado conocido tanto por el SIM como por el AuC.

Etapa 64: El AUC responde con uno o más conjuntos de desafíos (RAND) y unas claves de sesión GSM (K_{gsm}) y, normalmente, también unas respuestas firmadas correspondientes (SRES). El AS forma una primera clave de autenticación K_c usando las n claves de sesión GSM K_{gsm} y/o las respuestas firmadas SRES de los tripletes GSM de la siguiente manera: $K_c = hash_1$ [n x K_{gsm}, n x SRES, mensaje aleatorio$_1$], en la que $hash_1$ es una primera función hash, que es una función hash unidireccional conocida tanto por el cliente c como por el AS. x es una notación de los n parámetros K_{gsm}, no de una multiplicación. De acuerdo con la realización preferida de la invención, las respuestas firmadas no se comparan en absoluto (y por lo tanto no se transmiten en texto legible) de tal manera que las SRES recibidas también puede usarse en la formación de la K_c. El uso de los datos más secretos en la formación de la K_c aumenta su resistencia criptográfica. Como alternativa, solo pueden usarse las claves de sesión GSM K_{gsm} o las respuestas firmadas SRES. Además, en la generación de la primera clave de autenticación K_c el número de claves de sesión GSM K_{gsm} usado puede diferir del número de SRES usadas. Solo es necesario para el cliente c conocer cómo se genera la K_c. La K_c servirá en la autenticación entre el AS y el cliente c. Además, una primera clave de sesión $K_{c,tgs}$ se forma por el AS. El $K_{c,tgs}$ puede ser, por ejemplo, una clave aleatoria generada por el AS.

Etapa 23': El AS forma un ticket de concesión de tickets $ticket_{tgs}$ como se ha descrito anteriormente en relación con la sección de la técnica anterior. La etapa 23' difiere de la etapa 23 descrita en la sección de la técnica anterior de manera que el AS envía también los n RAND que se han usado en la generación de la K_c además del $ticket_{tgs}$ y la $K_{c,tgs}$ cifrada con la K_c. El mensaje enviado desde el AS al c en la etapa 23' puede denominarse como un mensaje KRB_AS_RES.

Etapa 65: El cliente c proporciona los n RAND al SIM, que forma los n pares correspondiente de valores SRES y K_{gsm}.

Etapa 66: El SIM proporciona los n pares de valores SRES y K_{gsm} formados en el etapa anterior al cliente c. A continuación, el cliente c forma una versión propia de la K_c usando el SRES y los valores de K_{gsm} de una manera similar a la que se había hecho anteriormente. Después de tener su propia versión de la K_c, a continuación el funcionamiento del sistema sigue en las etapas 26 al 29 del protocolo convencional Kerberos versión 5 explicado anteriormente con referencia a la figura 2.

Las etapas 24 y 25 se sustituyen por las etapas 65 y 66, debido a que la autenticación puede realizarse de manera automática si el usuario ha aceptado el acceso a su SIM.

Como se ha mencionado anteriormente, la IMSI se envía desde el cliente c al AS y a continuación los RAND se envían desde el AS al cliente c. Esta mensajería puede implementarse de diversas maneras, entre las que se describe a continuación la implementación de acuerdo con la realización preferida.

El intercambio de servicio de autenticación de Kerberos versión 5 comprende una transmisión inicial de los datos de autenticación previa opcionales (PA_DATOS) desde el cliente c al AS. La presencia de los datos de autenticación previa se muestra en un indicador PREAUTHENT. El uso de PA_DATOS no se ha normalizado pero, de acuerdo con Stallings, "la implementación MIT de la versión 5 ha cifrado el bloque de autenticación previa de marca de tiempo que contiene un factor de confusión al azar, un número de versión, y una marca de tiempo, cifrados en la clave basada en la contraseña del cliente". A continuación, el "bloque de autenticación previa", o datos, se descifra por el AS. A continuación, el AS puede verificar la verdadera autenticidad del cliente c y enviar tickets solo si se confirma la autenticación previa. Stallings continúa describiendo otra posibilidad que utiliza una tarjeta inteligente que genera una serie de contraseñas teniendo cada una su propio período de validez limitado. Las contraseñas pueden estar basadas en la contraseña del usuario, pero a medida que cambian, las contraseñas transmitidas son, en efecto, arbitrarias y son difíciles de determinar. El uso de un lector de tarjetas inteligentes puede estar indicado por un indicador HW_AUTHENT, que identifica los protocolos que requieren el uso del hardware que se espera que esté solo en posesión del cliente c correcto.

En la realización preferida de la invención, los indicadores PA_DATOS y HW_AUTHENT se utilizan en la presente invención de manera que la IMSI puede transmitirse en el campo PA_DATOS y el indicador HW_AUTHENT puede usarse para indicar el uso de un SIM para la autenticación. En lugar de usar el PA_DATOS para cualquier autenticación previa, las solicitudes de AS, responden a un valor específico del indicador HW_AUTHENT, los tripletes GSM del AuC del abonado. El AUC correcto se encuentra usando la IMSI.

El AS envía los n RAND al cliente c en un mensaje Kerberos versión 5 convencional KRB_AS_RES, en un campo de datos de autenticación previa (PA_DATOS). Después de recibir los RAND, el cliente c puede formar su propia versión de la K_c y descifrar la $K_{c,tgs}$.

En la realización preferida, el campo PA_DATOS se usa para enviar la IMSI desde el cliente c al AS. Aunque la ID del cliente ID_C, una ID_C falsa que no es la verdadera ID del cliente (por ejemplo, un valor aleatorio o una constante tal como cero), se usa como la ID_C. La ID_C (falsa) se integra en todos los siguientes mensajes de autenticación en los que se solicitan o se conceden tickets. Como una ventaja de enviar la IMSI en el campo PA_DATOS, la IMSI no se convierte en parte de una serie de mensajes adicionales. Esto es bueno ya que la IMSI identifica al abonado. Por razones de seguridad, es deseable limitar su disponibilidad general. El uso de una indicación de autenticación previa y los campos de datos también es ventajoso, con el fin de proporcionar una manera normalizada para indicar al AS que se está usando un método de utilización de una autenticación por SIM de acuerdo con la invención. Puede usarse la versión 5 convencional de Kerberos con pequeños cambios y no es necesario ejecutar primero unos protocolos propietarios con el fin de obtener la primera clave de sesión $K_{c,tgs}$ para su uso en el protocolo Kerberos versión 5.

También se ha mencionado en el párrafo anterior que se puede dar a la ID del cliente ID_C un valor arbitrario. Por otra parte, la ID_C puede elegirse más tarde por el AS. La ID_C se envía de vuelta desde el AS como un texto legible de manera que no importa si la ID_C cambia después de que el cliente c haya enviado el primer mensaje con una ID_C inicial arbitraria. Es ventajoso para el AS elegir la ID_C, ya que proporciona una oportunidad para la asignación centralizada de identidades de manera que cada identidad puede ser única durante su tiempo de vida.

La figura 7 muestra un diagrama de bloques de un sistema de autenticación de red de área local inalámbrica 70 de acuerdo con una realización de la invención. El sistema 70 comprende un cliente c, un punto de acceso AP, un centro de distribución de claves Kerberos KSS que contiene tanto un servidor de autenticación Kerberos (AS, no mostrado en la figura 7) como un servidor de concesión de tickets (TGS, no mostrado en la figura 7). Las funciones de AP como un servidor proxy entre el cliente c y el KSS, se ilustrarán a continuación con referencia a la figura 8. Además, el AP contiene una funcionalidad de servidor de servicios Kerberos (V, no mostrado en la figura 7).

La figura 8 muestra un procedimiento de autenticación del sistema de autenticación 70 de la figura 7. El procedimiento se inicia a partir de las etapas 810 y 812, en las que el AP envía anuncios que informan al cliente c sobre sí mismo y el cliente c asocia al AP. A continuación, se envía un mensaje de solicitud de identidad de protocolo de autenticación extensible (EAP) mediante el AP (etapa 814) al cliente c. El cliente c responde con una respuesta de identidad EAP (etapa 816). A continuación, el AP envía una solicitud EAP-GSS (etapa 818) al cliente c. Todas estas etapas 810 a 816 son familiares para un experto en la materia, por ejemplo, a partir de la publicación "TGe Security Baseline", noviembre de 2000, por D. Halasz, S. Norman, G. Zorn, B. Aboba, T. Moore, J. Walker, B. Beach, B. O'Hara, diapositiva 18, (IEEE 802,11 a 00/419).

A continuación, el cliente c forma (etapa 820) un mensaje AS_SOL, lo que corresponde al KRB_AS_SOL explicado anteriormente y a continuación, el cliente c envía el mensaje al AP encapsulado por IAKERB y los protocolos EAP-GSS adicionales. Ambos protocolos IAKERB y EAP-GSS se conocen por un experto en la materia, véase por ejemplo "Generic Security Service Application Program Interface, Version 2, Update 1" (RFC 2743), enero de 2000, por J. Linn y "Initial Authentication and Pass Through Authentication Using Kerberos V5 and the GSS-API (IAKERB)", noviembre de 2000, por M. Swift, J. Trostle, B. Aboba y G. Zorn (draft-ietf-cat-iakerb-05.txt).

El AP reenvía (etapa 822) el mensaje AS_SOL al KSS, que responde (etapa 824) con un mensaje AS_RES al AP. El AP reenvía (etapa 826) el AS_RES encapsulado por los protocolos IAKERB y EAP-GSS al cliente c. El AS_RES corresponde a la KRB_AS_RES explicado anteriormente.

En las etapas 828 a 834 se solicita y se concede un ticket de concesión de servicio de tickets al cliente c.

Como se ha mencionado en la descripción de la figura 7, el AP tiene dos funciones. El AP funciona como un proxy IAKERB cuando se reenvían a los clientes los mensajes AS_SOL/AS_RES y TGS_SOL/TGS_RES (etapas 820 a 834). Además, el AP contiene un servidor de servicios Kerberos (V), por ejemplo, para proporcionar acceso a una red, tal como Internet. En las etapas 828 a 834, el cliente c obtiene un $ticket_V$ para el AP del KSS. En las etapas 840 y 842 (AP_SOL y AP_RES), el cliente usa el $ticket_V$ para obtener un servicio de un servidor de servicios, por ejemplo, un acceso a Internet a través del AP.

Normalmente, se usará una clave de sesión individual entre el cliente y el punto de acceso (distribuido en las etapas 840 a 842) y la clave generada SIM solo se utilizará en el intercambio de servicios de autenticación.

En otra realización alternativa más, la IMSI puede transmitirse desde el cliente c al AP en el mensaje de respuesta de identidad EAP (etapa 816), en cuyo caso no será necesario transmitir el mensaje AS_SOL.

La figura 9 muestra un sub-procedimiento de autenticación en el cliente de acuerdo con otra realización más de la invención. En esta realización, el cliente tiene un USIM SIM UMTS en lugar de un SIM GSM. En la descripción del proceso en el cliente, el proceso en el extremo de red se hace claro también para un experto en la materia. El sub-procedimiento corresponde al procedimiento de autenticación y de concordancia de claves (AKA) UMTS y se usa para obtener el quinteto UMTS. El quinteto UMTS comprende 5 elementos de datos: un desafío RAND, una respuesta esperada XRES que debería coincidir con una respuesta RES que el USIM genera, una clave de cifrado

CK, una clave de integridad IK y un testigo de autenticación de red AUTN. El quinteto UMTS se recibe normalmente en el campo PA_DATOS, como se ha descrito anteriormente con referencia a la figura 6.

El sub-procedimiento ejemplifica cómo un número de secuencia SQN puede integrarse en la autenticación y cómo puede comprobarse y re-sincronizarse adicionalmente en el caso de que esté fuera de sincronización.

El quinteto UMTS se ha generado normalmente por un AuC de un operador UMTS del abonado (USIM) usando un secreto compartido K (que corresponde a K_i, un secreto compartido en GSM). El quinteto se forma de tal manera que solo dos elementos de datos necesitan transmitirse al USIM para permitirle obtener todo el quinteto, es decir, el RAND y el AUTN. El cliente recibe estos dos elementos de datos. A continuación, el USIM obtiene el quinteto usando el AUTN, el RAND y la K. Normalmente, el USIM genera una RES, una CK y una IK usando solo la K y el RAND, con las tres diferentes funciones de autenticación respectivas f2 a f4 conocidas tanto por el USIM como por el AuC.

El USIM también genera un código de autenticación de mensaje esperado XMAC usando el RAND, el AUTN y la K. El AUTN contiene un campo SQN $\oplus$ AK, en el que AK es una clave de anonimato, un campo de gestión de autenticación AMF, y un código de autenticación de mensaje MAC. El primer campo mencionado permite al USIM obtener el XMAC, que se compara con el MAC. El primer USIM genera la AK usando el RAND y la K con una función de autenticación f5. A continuación, el USIM calcula (SQN $\oplus$ AK) $\oplus$ AK y obtiene el SQN (nota: el término de la fórmula que está entre paréntesis es el campo del AUTN y el AK en el extremo de la fórmula se obtiene por el USIM). A continuación, el USIM puede calcular el XMAC con la K, el SQN, el AMF y el RAND, usando una primera función de autenticación f1.

El USIM compara el XMAC con el MAC que se ha incluido en el AUTN. Si son diferentes, el cliente envía un mensaje de rechazo de autenticación de usuario de vuelta al AuC con una indicación de la causa y el cliente abandona el procedimiento de autenticación en curso. En este caso, el AuC puede iniciar un nuevo procedimiento de identificación y autenticación hacia el cliente.

El USIM también verifica que el número de secuencia recibido SQN está en el intervalo correcto. El SQN puede no diferir más que por una cantidad predeterminada del SQN mantenido por el USIM. Si el USIM considera que el número de secuencia no está en el intervalo correcto, envía un mensaje de fallo de sincronización de vuelta al AuC incluyendo un parámetro apropiado, y abandona el procedimiento en curso.

El sub-procedimiento descrito anteriormente se ajusta en el marco del intercambio de servicio de autenticación Kerberos. Se explica con más detalle a continuación en el marco del intercambio de servicio de autenticación basado en Kerberos.

El cliente c solicita un $ticket_{tgs}$ enviando un mensaje KRB_AS_SOL al AS. El mensaje tiene el siguiente formato básico:

$$\text{Opciones} \,||\, ID_C \,||\, \text{IMSI} \,||\, \text{Dominio}_c \,||\, ID_{tgs} \,||\, \text{tiempos} \,||\, \text{Mensaje aleatorio1}$$

El mensaje KRB_AS_SOL es como en el Kerberos convencional, excepto que contiene la IMSI del cliente. La IMSI puede transmitirse en el campo de identidad del cliente (ID_C), por ejemplo, usando el tipo de nombre de Kerberos PRINCIPAL, o un nuevo tipo de nombre reservado para UMTS. Kerberos soporta diversos mecanismos de autenticación con el campo de datos de autenticación previa (padatos) de los mensajes KRB_AS_SOL y KRB_AS_RES.

En una realización alternativa, la IMSI se transmite usando el campo padatos de Kerberos. Esto tiene la ventaja de que el cliente usa una identidad distinta de la IMSI como la ID_C en todos los mensajes de Kerberos, y la IMSI tiene que transmitirse solo una vez.

En otra realización alternativa más, para evitar el envío de la IMSI en los mensajes de Kerberos siguientes, el AS elige una identidad para el cliente c, genera el ticket para esta nueva identidad y transmite la identidad con el $ticket_{tgs}$ del mensaje KRB_AS_RES.

El AS responde con un mensaje KRB_AS_RES al cliente c. El mensaje KRB_AS_RES tiene el siguiente formato básico:

$$\text{Dominio}_c \,||\, ID_C \,||\, \text{Ticket}_{tgs} \,||\, \text{n RAND} \,||\, \text{n AUTN} \,||\, E_{Kc}\,[K_{c,tgs} \,||\, \text{tiempos} \,||\, \text{Mensaje aleatorio}_1 \,||\, \text{Dominio}_{tgs} \,|\, ID_{tgs}]$$

en la que n es un número entero (al menos 1), K_c = h (n CK, n Ik, Mensaje aleatorio1) y la función h () es una función hash unidireccional. En una realización alternativa, K_c = h (n CK, n IK, n RES, Mensaje aleatorio1)

El mensaje KRB_AS_RES es similar al Kerberos de la técnica anterior correspondiente, excepto que contiene n RAND y AUTN. Los RAND y AUTN pueden estar contenidos en el campo padatos del mensaje KRB_AS_RES.

Tras la recepción de un KRB_AS_RES, el cliente verifica primero los n AUTN como en el AKA UMTS convencional. Si los n parámetros AUTN se comprueban correctamente, el cliente ejecuta los algoritmos AKA UMTS en el USIM y obtiene la K_c a partir de los n quintetos y el mensaje aleatorio$_1$. A continuación, el cliente es capaz de descifrar la parte cifrada del KRB_AS_RES y comprobarla, al igual que en la autenticación Kerberos normal. Si las comprobaciones tienen éxito, el cliente ha obtenido un ticket de concesión de ticket y una clave de sesión de servidor de concesión de ticket. Desde este punto en adelante, el cliente funciona como cualquier otro cliente Kerberos. El cliente no necesita el USIM hasta que el ticket$_{tgs}$ expira y el cliente tiene que solicitar un nuevo ticket$_{tgs}$ ejecutando el intercambio de servicio de autenticación de nuevo (a menos que se necesite el USIM para otros fines, tal como la colocación de una llamada de teléfono UMTS ordinaria).

Como en el Kerberos convencional, en el caso de AKA UMTS, el AS es incapaz de verificar que el KRB_AS_SOL proviene de un cliente c legítimo. Tras la recepción del mensaje KRB_AS_SOL, el AS recupera los quintetos UMTS para el cliente, genera la clave K_c y envía el mensaje KRB_AS_RES. El AS no necesita guardar la clave K_c o cualquier otra información de estado para el cliente.

Si el ticket se ha solicitado por un cliente legítimo (es decir, el cliente c que posee la USIM que tiene la IMSI usada), el cliente puede obtener la clave K_c y descifrar la parte cifrada del mensaje KRB_AS_RES y obtener el ticket$_{tgs}$. Como en el Kerberos convencional, solo los clientes c legítimos son capaces de usar el ticket$_{tgs}$ recibido en el mensaje KRB_AS_RES.

A continuación, el cliente c obtiene el SQN fuera al menos de un RAND y un AUTN (normalmente los primeros de los n RAND y AUTN) y comprueba si está en el intervalo correcto.

Si el SQN está en el intervalo correcto (no demasiado lejos del SQN_{MS}), el cliente c aprueba el ticket$_{tgs}$ y puede usarlo. De lo contrario, el cliente c envía un nuevo KRB_AS_SOL como un mensaje de solicitud de re-sincronización (en la etapa (3)) que contiene un AUTS correspondiente al primer RAND y AUTN. El AUTS es un parámetro usado para re-sincronizar el SQN. La construcción del parámetro AUTS se muestra en la figura 10. Hay un MAC-S (código de autenticación de mensaje para la re-sincronización) formado para ser una parte del AUTS. El mensaje KRB_AS_SOL usado ahora tiene el siguiente formato básico:

opciones || ID_C || IMSI || RAND || AUTS || Dominio$_c$ || ID$_{tgs}$ || tiempos || Mensaje aleatorio$_1$

En respuesta al mensaje de solicitud de resincronización, el AS hace que el AuC sincronice su SQN con el USIM (a SQN_{MS}), recupere un nuevo conjunto de quintetos UMTS y los envía al cliente c en un nuevo mensaje KRB_AS_RES que ahora se forma usando el SQN sincronizado (es decir, en el que los RAND y AUTN se basan en los SQN en sincronización con el SQN_{MS} del USIM). El KRB_AS_RES tiene ahora el siguiente formato básico:

Dominio$_c$ || ID_C || Ticket$_{tgsi}$ || n RAND || n AUTN || E_{Kc} [$K_{c,tgs}$ || tiempos || Mensaje aleatorio$_1$ || Dominio$_{tgs}$ || ID$_{tgs}$]

Es una ventaja remarcable de esta realización que la autenticación UMTS pueda extenderse a Kerberos compatible con el servidor de concesión de tickets y los servidores de servicio Kerberos (también conocidos como servidores de aplicación) sin ninguna modificación de los mismos. Basta con que el cliente Kerberos y el AS sean conscientes AKA UMTS. Los servidores TGS y de servicios Kerberos V no necesitan ser conscientes AKA UMTS. El AS puede tener una interfaz con la red de autorización UMTS, de manera similar al AS de la LAN inalámbrica de operador de red (OWLAN) para la red GSM. El servidor de autenticación Nokia es un ejemplo de un AS OWLAN.

Las diferentes realizaciones de la invención permiten el uso de diversos módulos de identificación de red de telecomunicaciones, que incluyen los SIM y USIM, para autenticar clientes para varias otras redes de datos o de sus servicios usando tickets que conceden el acceso a los mismos o a sus servicios. Por ejemplo, puede usarse un dispositivo de telecomunicaciones móviles UMTS tanto por los servicios de telecomunicaciones UMTS proporcionados por su operador de telecomunicaciones (sobre una interfaz de radio) como por los servicios de LAN inalámbricos (y/o cableados). El dispositivo puede obtener una primera clave de autenticación o clave de sesión K_c fuerte y relativamente fiable basándose en el módulo de identificación de usuario del dispositivo, y usar esa clave de sesión sin necesidad de enviar devuelta ninguna "respuesta firmada" tal como una RES o una SRES y por lo tanto esos datos pueden usarse además en la creación de la clave de sesión.

Por otra parte, la generación de la clave de sesión basándose en las credenciales de la red de telecomunicaciones móviles (datos de tripletes GSM o datos de quintetos UMTS) permite unas transferencias rápidas de la itinerancia del punto de acceso.

Se han descrito las implementaciones y las realizaciones específicas de la invención. Es evidente para un experto en la materia que la invención no está limitada a los detalles de las realizaciones presentadas anteriormente, sino que pueden implementarse en otras realizaciones usando unos medios equivalentes sin desviarse de las características de la invención. El alcance de la invención está limitado solamente por las reivindicaciones de patente adjuntas.

REIVINDICACIONES

1. Un método del lado del cliente de autenticación de un cliente (c), que comprende las etapas de:

enviar la información de identidad de cliente (IMSI) a un servidor de autenticación (AS), siendo la información de identidad de cliente una identidad de abonado móvil internacional;
recibir por el cliente las primeras credenciales cifradas ($K_{c,tgs}$) y n desafíos (RAND) desde el servidor de autenticación (AS), siendo el número n de los desafíos (RAND) al menos uno de, cifrándose las primeras credenciales ($K_{c,tgs}$) con una primera clave de autenticación (K_c), basándose la primera clave de autenticación en los n primeros secretos (K_{gsm}, SRES; CK, IK, RES) y asociándose el n primer secreto (K_{gsm}, SRES; CK, IK, RES) a la información de identidad de cliente;
formar en el cliente los n primeros secretos (K_{gsm}, SRES) basándose en un secreto del cliente (Ki) y los n desafíos (RAND);
formar en el cliente (c) usando los n primeros secretos (K_{gsm}, SRES) la primera clave de autenticación (K_c); y
descifrar las primeras credenciales cifradas ($K_{c,tgs}$) usando la primera clave de autenticación (K_c) en el cliente; **caracterizado por que**
el descifrado de las primeras credenciales cifradas ($K_{c,tgs}$) es independiente del envío de cualquier respuesta basada en el secreto del cliente (Ki) desde el cliente (c) al servidor de autenticación (AS).

2. Un método de acuerdo con la reivindicación 1, **caracterizado por que** los n desafíos y las primeras credenciales cifradas se reciben en un mensaje común.

3. Un método de acuerdo con las reivindicaciones 1 o 2, **caracterizado por** los n desafíos (RAND) y los n primeros secretos correspondientes a los n números de secuencia específicos (SQN) y la transmisión de los n números de secuencia (SQN), y comprendiendo además el método las etapas de:

mantener un contador de número de secuencia (SQN_{MS}) en el cliente (c);
obtener en el cliente (c) un número de secuencia (SQN) usando uno de los n desafíos (RAND) y uno de los n primeros secretos (K_{gsm}, SRES; CK, IK, RES); y
comprobar en el cliente (c) si el número de secuencia (SQN) está dentro de un intervalo predeterminado.

4. Un método de acuerdo con la reivindicación 3, **caracterizado por que** el método comprende además la etapa de iniciar una sincronización del número de secuencia en el caso de que el número de secuencia (SQN) no esté dentro del intervalo predeterminado.

5. Un método de acuerdo con cualquiera de las reivindicaciones 1 a 4, **caracterizado por que** una respuesta (SRES) formada en el cliente (c) por medio del secreto del cliente (Ki) y el al menos un desafío (RAND) se usan exclusivamente en el cliente (c).

6. Un método de acuerdo con cualquiera de las reivindicaciones 1 a 5, **caracterizado por que** la primera clave de autenticación (K_c) está basada en dos o más primeros secretos.

7. Un método de acuerdo con cualquiera de las reivindicaciones 1 a 6, **caracterizado por que**

el método comprende además la etapa de enviar un mensaje aleatorio que es un protector de ataque de repetición desde el cliente al servidor de autenticación; y
la formación de la primera clave de autenticación que comprende una sub-etapa de usar una función hash de al menos el primer secreto y el protector de ataque de repetición.

8. Un método de acuerdo con cualquiera de las reivindicaciones 1 a 7, **caracterizado por que** el método comprende además la etapa de generar un mensaje de solicitud de servicio usando criptográficamente las primeras credenciales descifradas.

9. Un método del lado del servidor de autenticación de un cliente (c), que comprende las etapas de:

recibir por un servidor de autenticación (AS) una información de identidad de cliente (IMSI) desde un cliente (c), siendo la información de identidad de cliente una identidad de abonado móvil internacional;
obtener para el servidor de autenticación (AS) n desafíos (RAND) y n primeros secretos (K_{gsm}, SRES), basándose los n primeros secretos en un secreto del cliente (Ki) específico para el cliente (c) y en los n desafíos (RAND), en donde n es al menos uno y el secreto del cliente (Ki) está asociado a la información de identidad de cliente (IMSI);
formar las primeras credenciales ($K_{c,tgs}$);
formar una primera clave de autenticación (K_c) usando los n primeros secretos (K_{gsm}, SRES);
cifrar las primeras credenciales ($K_{c,tgs}$) usando la primera clave de autenticación (K_c);
enviar los n desafíos (RAND) y las primeras credenciales cifradas ($K_{c,tgs}$) al cliente (c);
recibir del cliente (c) un mensaje que contiene una primera información; y

comprobar si las primeras credenciales se han usado para procesar criptográficamente la primera información; **caracterizado por que**
el cifrado de las primeras credenciales ($K_{c,tgs}$) es independiente de la recepción de cualquier respuesta basada en el secreto del cliente (Ki) desde el cliente (c) al servidor de autenticación (AS).

10. Un método de acuerdo con la reivindicación 9, **caracterizado por que** el servidor de autenticación está configurado para proporcionar al cliente las primeras credenciales cifradas y los n desafíos en un mensaje común.

11. Un método de acuerdo con las reivindicaciones 9 o 10, **caracterizado por que** el servidor de autenticación obtiene los n desafíos (RAND) y al menos un primer secreto (K_{gsm}, SRES) basado en un secreto del cliente (Ki) específico para el cliente (c) se produce antes de una necesidad de autenticar al cliente.

12. Un método de acuerdo con cualquiera de las reivindicaciones 9 a 11**, caracterizado por** el servidor de autenticación que forma además una identificación para su uso en un mensaje de autenticación siguiente para el cliente.

13. Cliente (c) para un sistema de autenticación que comprende un servidor de autenticación (AS); comprendiendo el cliente:

una primera salida (IO_C) para proporcionar al servidor de autenticación (AS) una información de identidad de cliente (IMSI), siendo la información de identidad de cliente una identidad de abonado móvil internacional;
una primera entrada (IO_C) para recibir unas primeras credenciales cifradas ($K_{c,tgs}$) y n desafíos (RAND), en donde n es al menos uno, cifrándose las primeras credenciales ($K_{c,tgs}$) con una primera clave de autenticación (K_c), basándose la primera clave de autenticación (K_c) en los n primeros secretos (K_{gsm}, SRES; CK, IK, RES), y asociándose los n primeros secretos (K_{gsm}, SRES; CK, IK, RES) a la información de identidad de cliente (IMSI); y
un primer procesador (CPU_C)

para formar los n primeros secretos (K_{gsm}, SRES) basándose en un secreto del cliente (Ki) y en los n desafíos (RAND);
para formar la primera clave de autenticación (K_c) usando los n primeros secretos (K_{gsm}, SRES); y
para descifrar las primeras credenciales cifradas ($K_{c,tgs}$) usando la primera clave de autenticación (K_c);

caracterizado por que

el cifrado de las primeras credenciales ($K_{c,tgs}$) es independiente de la recepción de cualquier respuesta basada en el secreto del cliente (Ki) desde el cliente (c) al servidor de autenticación (AS).

14. Un cliente de acuerdo con la reivindicación 13, **caracterizado por que** las primeras credenciales cifradas y los n desafíos se reciben en un mensaje común.

15. Un cliente de acuerdo con las reivindicaciones 13 o 14, **caracterizado por** los n desafíos (RAND) y los n primeros secretos correspondientes a los n números de secuencia específicos (SQN) y la transmisión de los n números de secuencia (SQN), y comprendiendo además el cliente:

medios para mantener un contador de número de secuencia (SQN_{MS}) en el cliente (c);
medios para obtener en el cliente (c) un número de secuencia (SQN) usando uno de los n desafíos (RAND) y los n primeros secretos (K_{gsm}, SRES; CK, IK, RES); y
medios para comprobar en el cliente (c) si el número de secuencia (SQN) está dentro de un intervalo predeterminado.

16. Un cliente de acuerdo con la reivindicación 15, **caracterizado por que** el cliente comprende además los medios para iniciar una sincronización del número de secuencia en el caso de que el número de secuencia (SQN) no esté dentro del intervalo predeterminado.

17. Un cliente de acuerdo con cualquiera de las reivindicaciones 13 a 16, **caracterizado por que** el cliente está configurado para no enviar ninguna respuesta basada en el secreto del cliente (Ki) al servidor de autenticación (AS).

18. Un cliente de acuerdo con cualquiera de las reivindicaciones 13 a 17, **caracterizado por que** la primera clave de autenticación (K_c) está basada en dos o más primeros secretos.

19. Un cliente de acuerdo con cualquiera de las reivindicaciones 13 a 18, **caracterizado por que**:

el cliente comprende además unos medios para enviar un mensaje aleatorio que es un protector de ataque de repetición desde el cliente al servidor de autenticación; y
la formación de la primera clave de autenticación que comprende una sub-etapa de usar una función hash de al menos el primer secreto y el protector de ataque de repetición.

20. Un cliente de acuerdo con cualquiera de las reivindicaciones 13 a 19, **caracterizado por** los medios adicionales de cliente para generar un mensaje de solicitud de servicio usando criptográficamente las primeras credenciales descifradas.

21. Un servidor de autenticación (AS) para un sistema de autenticación que comprende un cliente (c); comprendiendo el servidor de autenticación:

una primera entrada (IO_{AS}) para recibir una información de identidad de cliente (IMSI), siendo la información de identidad de cliente una identidad de abonado móvil internacional;
una segunda entrada (IO_{AS}) para recibir n desafíos (RAND) y n primeros secretos (K_{gsm}, SRES), siendo n al menos uno y basándose los n primeros secretos en un secreto del cliente (Ki) específico para el cliente (c) y en los n desafíos (RAND), en donde el secreto del cliente (Ki) está asociado a la información de identidad de cliente;
un primer procesador (CPU_{AS})

para formar primeras credenciales ($K_{c,tgs}$);
para formar una primera clave de autenticación (K_c) usando los n primeros secretos (K_{gsm}, SRES); y
para cifrar las primeras credenciales ($K_{c,tgs}$) usando la primera clave de autenticación (K_c);

una salida (IO_{AS}) para proporcionar al cliente las primeras credenciales cifradas ($K_{c,tgs}$) y los n desafíos (RAND);
estando la primera entrada (IO_{AS}) adaptada además para recibir del cliente (c) un mensaje que contiene una primera información; y
estando el primer procesador (CPU_{AS}) adaptado además para comprobar si se han usado las primeras credenciales para procesar criptográficamente la primera información; **caracterizado por que**
el cifrado de las primeras credenciales ($K_{c,tgs}$) es independiente de la recepción cualquier respuesta basada en el secreto del cliente (Ki) desde el cliente (c) al servidor de autenticación (AS).

22. Un servidor de autenticación (AS) de acuerdo con la reivindicación 21, **caracterizado por que** la salida está configurada para proporcionar al cliente las primeras credenciales cifradas y los n desafíos en un mensaje común.

23. Un servidor de autenticación (AS) de acuerdo con la reivindicación 21, **caracterizado por que** el servidor de autenticación comprende además unos medios para obtener los n desafíos (RAND) y los n primeros secretos (K_{gsm}, SRES) basándose en un secreto del cliente (Ki) específico para el cliente (c) antes de una necesidad de autenticar al cliente.

24. Un servidor de autenticación (AS) de acuerdo con la reivindicación 21, **caracterizado por que** el servidor de autenticación comprende además unos medios para formar una identificación para su uso en un mensaje de autenticación siguiente para el cliente.

25. Sistema de autenticación, que comprende un servidor de autenticación (AS) de acuerdo con la reivindicación 21 y un cliente (c) de acuerdo con la reivindicación 13.

26. Producto de programa informático para controlar un cliente; comprendiendo el producto de programa informático:

un código ejecutable por ordenador para permitir que el cliente envíe una información de identidad de cliente (IMSI) a un servidor de autenticación (AS), siendo la información de identidad de cliente una identidad de abonado móvil internacional;
un código ejecutable por ordenador para permitir que el cliente reciba desde el servidor de autenticación (AS) las primeras credenciales cifradas ($K_{c,tgs}$) y los n desafíos (RAND), siendo n al menos uno y estando las primeras credenciales ($K_{c,tgs}$) cifradas con una primera clave de autenticación (K_c), basándose la primera clave de autenticación (K_c) en los n primeros secretos (K_{gsm}, SRES; CK, IK, RES), y estando los n primeros secretos (K_{gsm}, SRES; CK, IK, RES) asociados a la información de identidad de cliente (IMSI);
un código ejecutable por ordenador para permitir que el cliente forme los n primeros secretos (K_{gsm}, SRES) basándose en un secreto del cliente (Ki) y los n desafíos (RAND);
un código ejecutable por ordenador para permitir que el cliente forme la primera clave de autenticación (K_c) usando los n primeros secretos (n K_{gsm}, SRES); y
un código ejecutable por ordenador para permitir que el cliente descifre las primeras credenciales cifradas ($K_{c,tgs}$) usando la primera clave de autenticación (K_c); **caracterizado por que**
el descifrado de las primeras credenciales cifradas ($K_{c,tgs}$) es independiente del envío de cualquier respuesta basada en el secreto del cliente (Ki) desde el cliente (c) al servidor de autenticación (AS).

27. Producto de programa informático para controlar un ordenador, para hacer que el ordenador autentique un cliente (c), comprendiendo el producto de programa informático:

un código ejecutable por ordenador para permitir que el ordenador reciba una información de identidad de cliente (IMSI) desde un cliente (c) a un servidor de autenticación (AS), siendo la información de identidad de cliente una

identidad de abonado móvil internacional;
un código ejecutable por ordenador para permitir que el ordenador obtenga n desafíos (RAND) y n primeros secretos (K_{gsm}, SRES) para el servidor de autenticación (AS), basándose los n primeros secretos en un secreto del cliente (Ki) específico para el cliente (c) y en los n desafíos (RAND), en donde n es al menos uno y el secreto del cliente (Ki) está asociado a la información de identidad de cliente;
un código ejecutable por ordenador para permitir que el ordenador forme las primeras credenciales ($K_{c,tgs}$);
un código ejecutable por ordenador para permitir que el ordenador forme una primera clave de autenticación (K_c) usando los n primeros secretos (K_{gsm}, SRES);
un código ejecutable por ordenador para permitir que el ordenador cifre las primeras credenciales ($K_{c,tgs}$) usando la primera clave de autenticación (K_c);
un código ejecutable por ordenador para permitir que el ordenador envíe al cliente (c) los n desafíos (RAND) y las primeras credenciales cifradas ($K_{c,tgs}$);
un código ejecutable por ordenador para permitir que el ordenador reciba desde el cliente (c) un mensaje que contiene una primera información; y
un código ejecutable por ordenador para permitir que el ordenador compruebe si se han usado las primeras credenciales para procesar criptográficamente la primera información;

caracterizado por que

el cifrado de las primeras credenciales ($K_{c,tgs}$) es independiente de la recepción de cualquier respuesta basada en el secreto del cliente (Ki) desde el cliente (c) al servidor de autenticación (AS).

28. Producto de programa informático para controlar una entidad de red de comunicaciones de datos; comprendiendo el producto de programa informático:

un código ejecutable por ordenador para permitir que la entidad de red de comunicaciones de datos implemente el método de acuerdo con una cualquiera de las reivindicaciones 2 a 12.

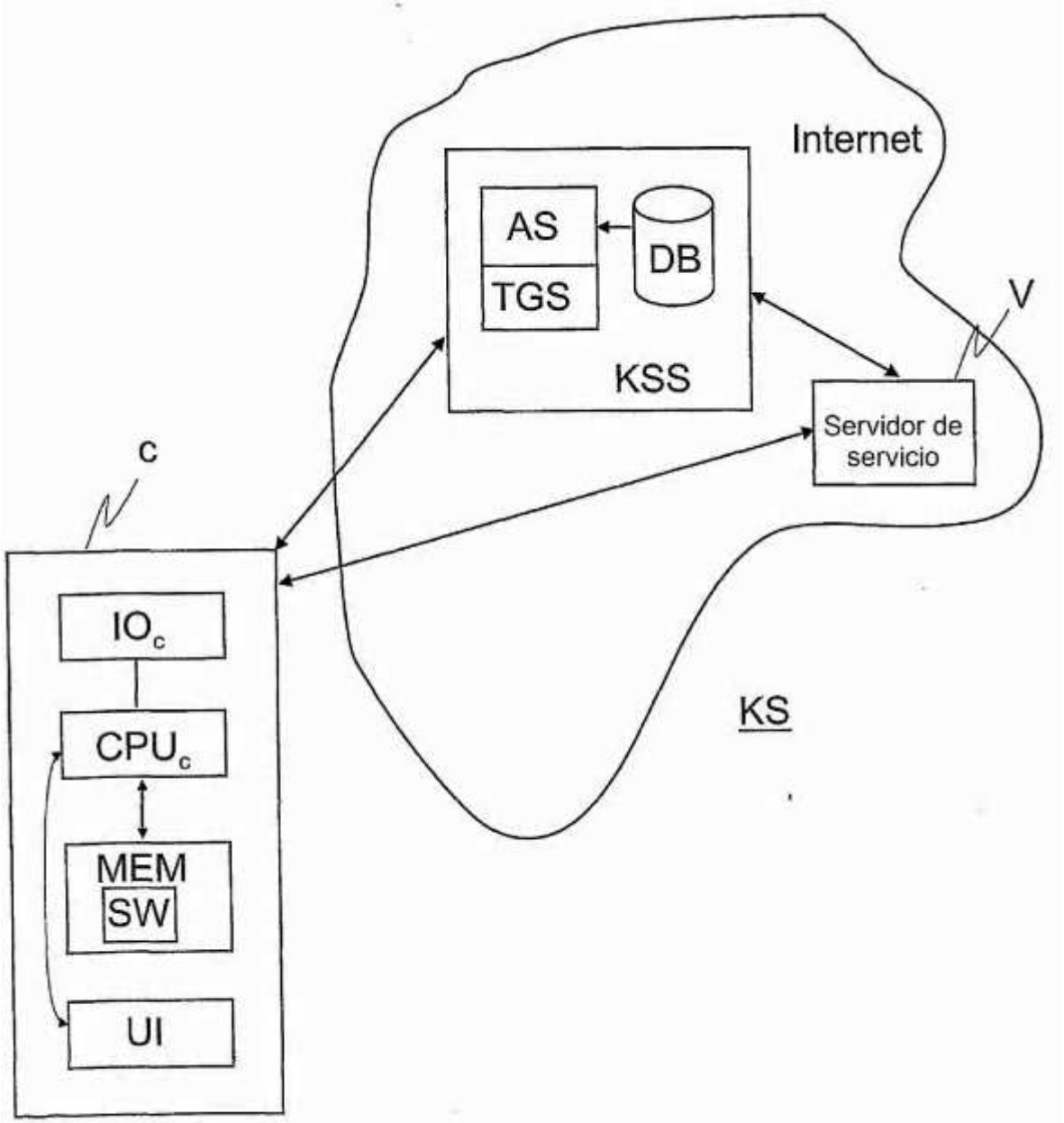

Internet
AS
DB
TGS
KSS
V
Servidor de servicio
C
IO$_C$
CPU$_C$
MEM
SW
UI
KS

Fig. 1

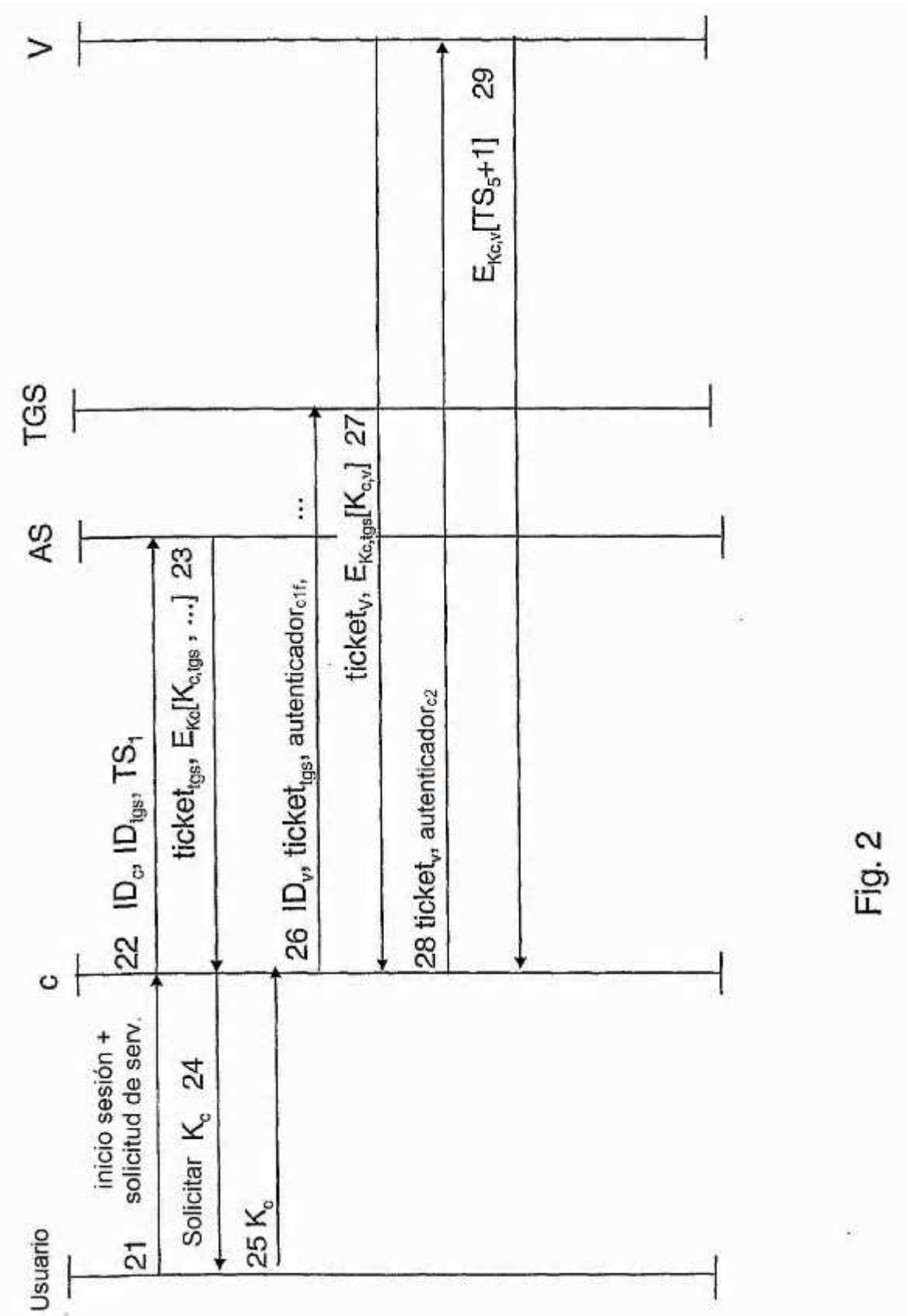

Usuario
c
AS
TGS
V
21 inicio sesión + solicitud de serv.
22 ID_c, ID_{tgs}, TS_1
Solicitar K_c 24
$ticket_{tgs}$, $E_{Kc}[K_{c,tgs}$, ...] 23
25 K_c
26 ID_v, $ticket_{tgs}$, autenticador$_{c1f}$,
...
$ticket_v$, $E_{Kc,tgs}[K_{c,v}]$ 27
28 $ticket_v$, autenticador$_{c2}$
$E_{Kc,v}[TS_5+1]$ 29

Fig. 2

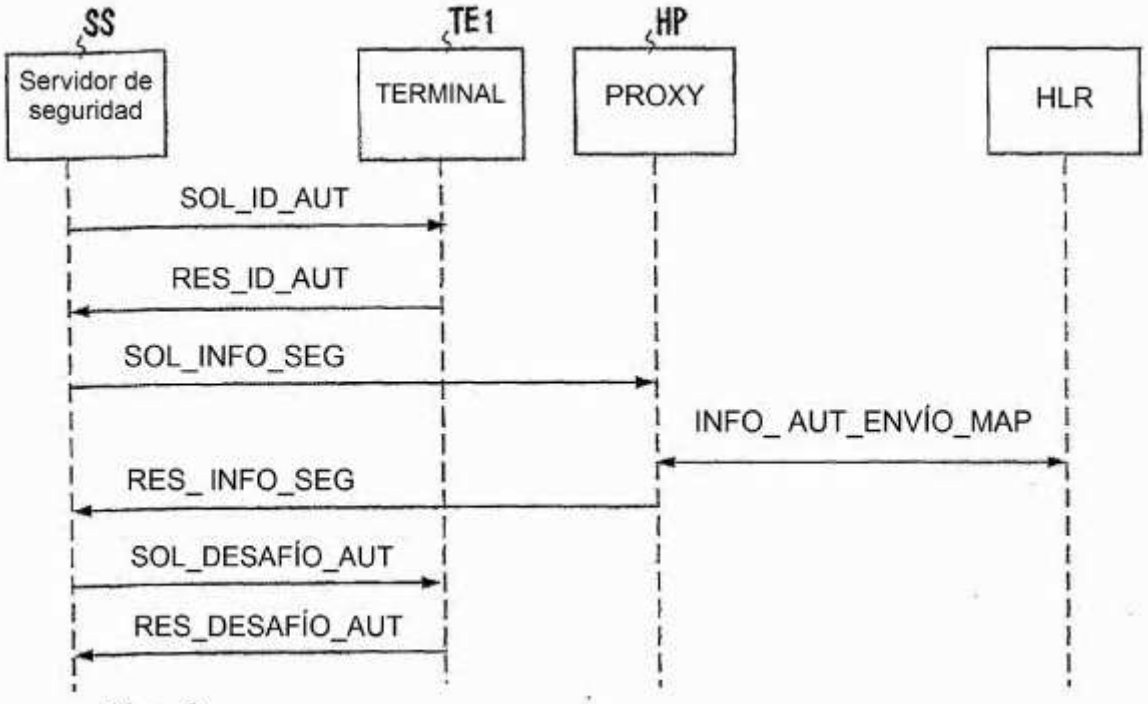

SS
Servidor de seguridad
TE1
TERMINAL
HP
PROXY
HLR
SOL_ID_AUT
RES_ID_AUT
SOL_INFO_SEG
INFO_ AUT_ENVÍO_MAP
RES_ INFO_SEG
SOL_DESAFÍO_AUT
RES_DESAFÍO_AUT

Fig. 3

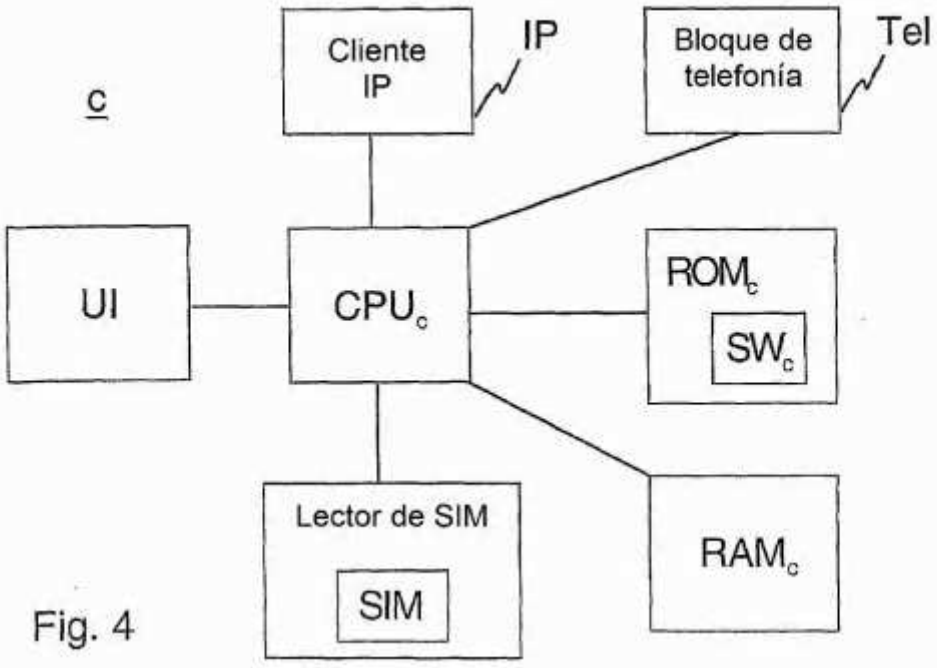

C
Cliente IP
IP
Bloque de telefonía
Tel
UI
CPU$_c$
ROM$_c$
SW$_c$
Lector de SIM
SIM
RAM$_c$

Fig. 4

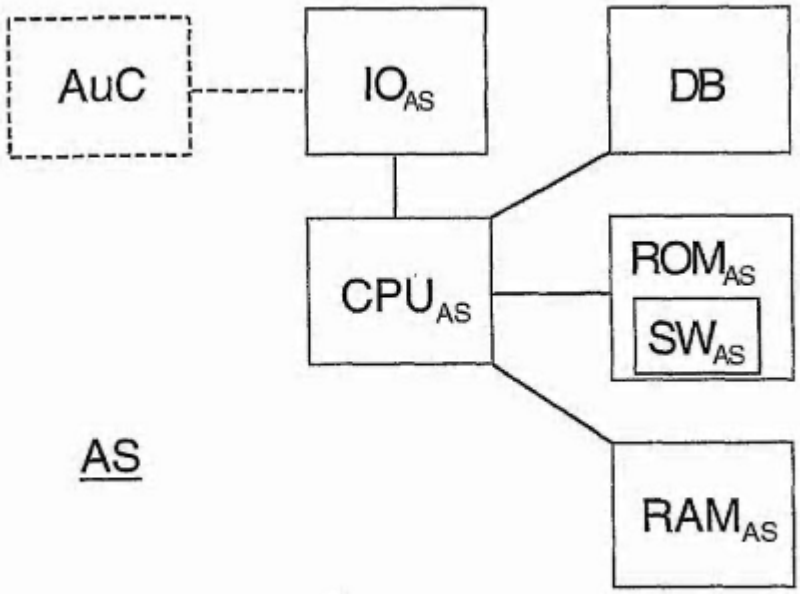


Fig. 5

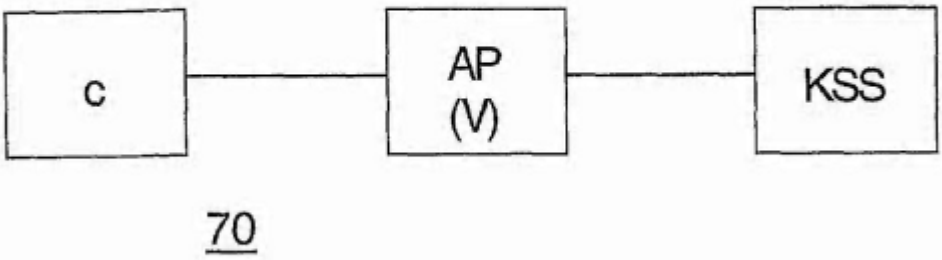


Fig. 7

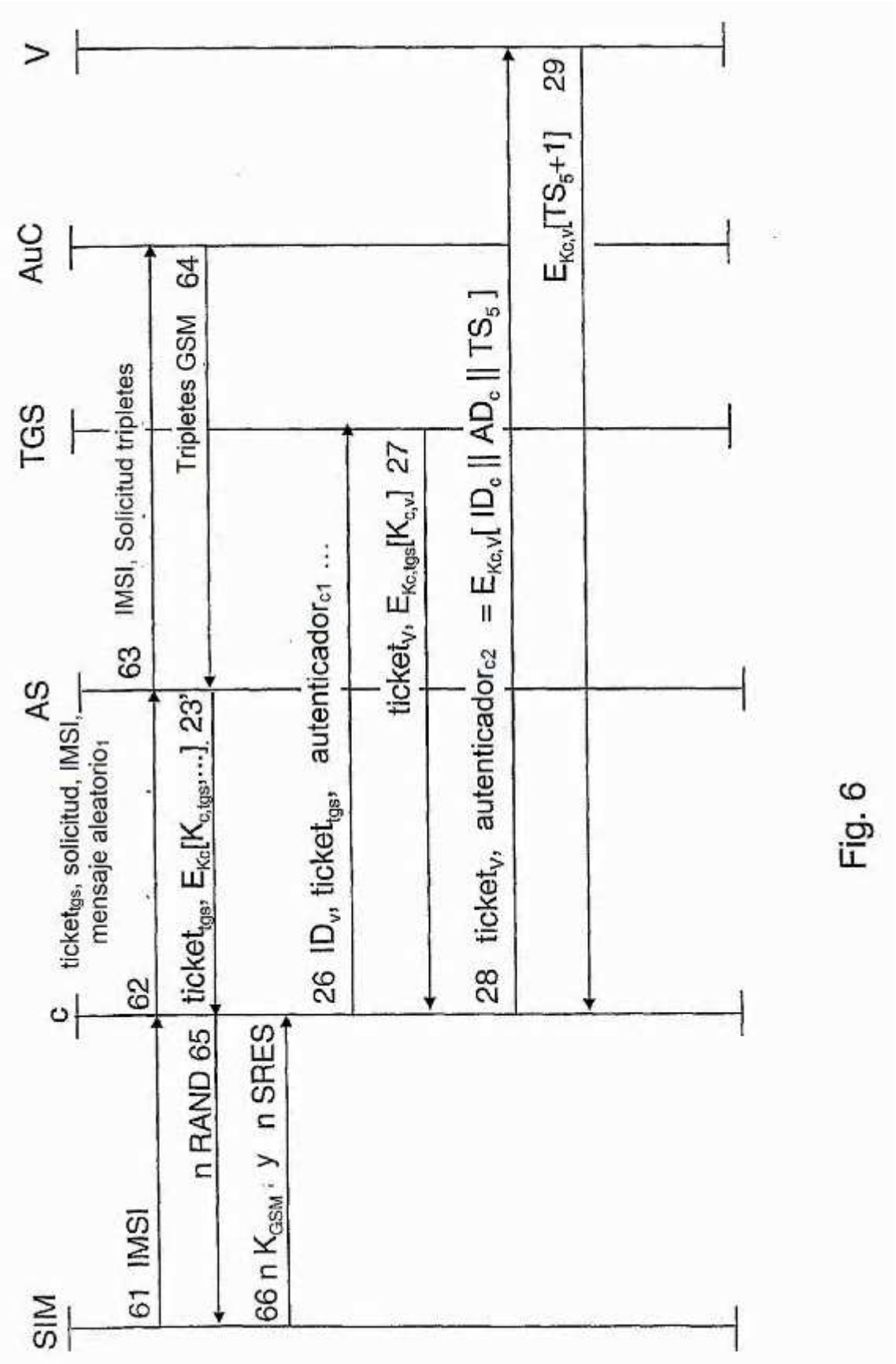

SIM
AS
TGS
AuC
V
c
61 IMSI
62
ticket$_{tgs}$, solicitud, IMSI, mensaje aleatorio$_1$
63 IMSI, Solicitud tripletes
Tripletes GSM 64
n RAND 65
ticket$_{tgs}$, E_{Kc}[$K_{c,tgs}$,...] 23'
n K_{GSM} y n SRES 66
26 ID_v, ticket$_{tgs}$, autenticador$_{c1}$ ...
ticket$_v$, $E_{Kc,tgs}$[$K_{c,v}$] 27
28 ticket$_v$, autenticador$_{c2}$ = $E_{Kc,v}$[ID_c || AD_c || TS_5]
$E_{Kc,v}$[TS_5+1] 29

Fig. 6

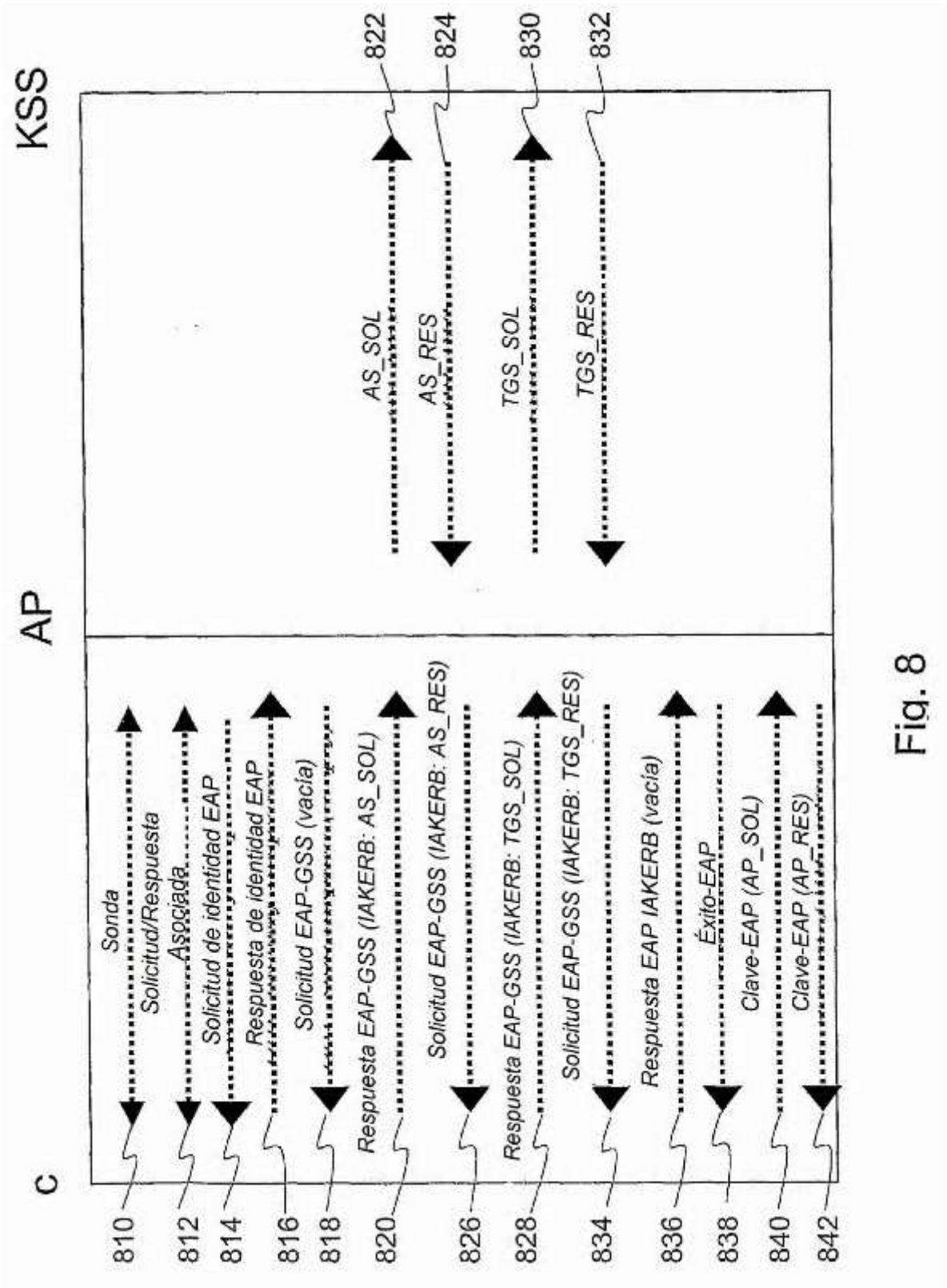
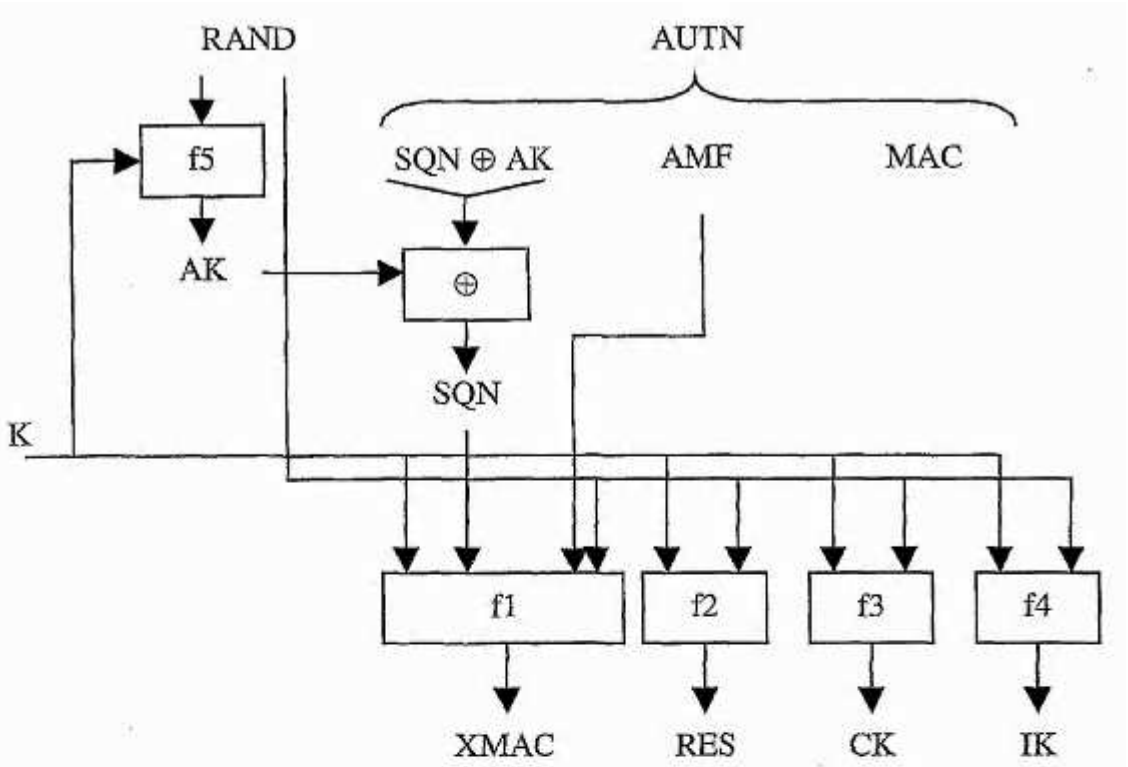

C
AP
KSS
Sonda
Solicitud/Respuesta Asociada
Solicitud de identidad EAP
Respuesta de identidad EAP
Solicitud EAP-GSS (vacía)
Respuesta EAP-GSS (IAKERB: AS_SOL)
Solicitud EAP-GSS (IAKERB: AS_RES)
Respuesta EAP-GSS (IAKERB: TGS_SOL)
Solicitud EAP-GSS (IAKERB: TGS_RES)
Respuesta EAP IAKERB (vacía)
Éxito-EAP
Clave-EAP (AP_SOL)
Clave-EAP (AP_RES)
AS_SOL
AS_RES
TGS_SOL
TGS_RES
810
812
814
816
818
820
822
824
826
828
830
832
834
836
838
840
842

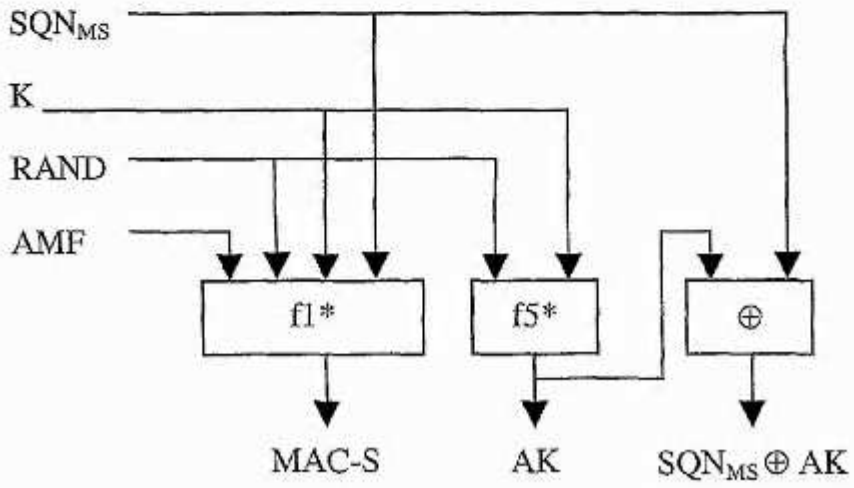
Fig. 8



Verificar MAC = XMAC

Verificar que SQN está en el intervalo correcto

Fig. 9



AUTS = $SQN_{MS} \oplus AK \parallel MAC\text{-}S$

Fig. 10