(19) OFICINA ESPAÑOLA DE PATENTES Y MARCAS

ESPAÑA

(11) Número de publicación: **2 817 556**

(51) Int. CI.:

H04W 12/06 (2009.01)
H04L 9/32 (2006.01)

(12) TRADUCCIÓN DE PATENTE EUROPEA T3

(86) Fecha de presentación y número de la solicitud internacional: **27.07.2017 PCT/EP2017/069073**

(87) Fecha y número de publicación internacional: **22.02.2018 WO18033364**

(96) Fecha de presentación y número de la solicitud europea: **27.07.2017 E 17751049 (2)**

(97) Fecha y número de publicación de la concesión europea: **22.07.2020 EP 3501194**

(54) Título: **Servidor de autenticación de una red de telecomunicación celular y UICC correspondiente**

(30) Prioridad:

17.08.2016 EP 16306062

(45) Fecha de publicación y mención en BOPI de la traducción de la patente:
07.04.2021

(73) Titular/es:

THALES DIS FRANCE SA (100.0%)
6, rue de la Verrerie
92190 Meudon, FR

(72) Inventor/es:

PHAN, LY THANH

(74) Agente/Representante:

ELZABURU, S.L.P

DESCRIPCIÓN

Servidor de autenticación de una red de telecomunicación celular y UICC correspondiente

El campo de la invención es el de las telecomunicaciones en redes celulares (3G (UMTS), redes 4G (LTE) o redes futuras (5G)).

Un objetivo particular de estas redes es ayudar a establecer comunicaciones entre terminales que se comunican con elementos de seguridad (UICC, eUICC, USIM, ...).

Estos elementos de seguridad suelen estar en forma de tarjetas extraíbles de sus terminales, habitualmente formadas por teléfonos móviles, teléfonos inteligentes, PDA, ... También existen elementos de seguridad integrados en terminales o máquinas que forman parte de un módem (por tanto, no extraíbles), siendo estas máquinas vehículos, máquinas expendedoras de bebidas, etc. ...

Más precisamente, la invención se refiere a la autenticación en dichas redes. Una aplicación, llamada USIM y almacenada en una (e)UICC tiene el objetivo de autenticar el equipo del usuario cuando el usuario intenta conectarse a una red de UMTS o LTE. Una aplicación de este tipo identifica de manera única a un usuario y a su operador de telefonía móvil mediante la utilización de la IMSI almacenada en el elemento de seguridad. También es necesario en dichas redes que la red autentique los elementos de seguridad.

La autenticación permite verificar que la identidad (IMSI o TMSI) transmitida por el terminal que se comunica con la tarjeta SIM en la ruta de radio es la correcta, para proteger, por un lado, al operador de la utilización fraudulenta de sus recursos, y, por otro lado, a los abonados, mediante la prohibición a terceros no autorizados para utilizar sus cuentas. La autenticación del abonado puede ser requerida por la red móvil hasta la última actualización de ubicación, establecimiento de llamada (entrante o saliente) y antes de habilitar o deshabilitar algunos servicios. También se requiere durante la implementación de la clave de cifrado en algunos canales dedicados.

La autenticación de GSM se basa en un protocolo de pregunta de seguridad/respuesta y en algoritmos de cifrado de clave secreta. No obstante, en un esquema de GSM, la red autentica la tarjeta SIM, pero la tarjeta SIM no autentica la red. La tarjeta SIM del terminal no puede verificar la identidad y la validez de la red a la que está conectado el móvil.

El mecanismo de autenticación utilizado en una red 3G (UMTS) o red 4G (LTE) es una autenticación mutua (el terminal autentica la red y la red autentica el terminal).

La autenticación de 3G (AKA para autenticación y acuerdo de clave) se basa en una clave K compartida que solo está presente en un elemento de la red llamado HLR (Registro de ubicación de abonados locales – Home Location Register, en inglés) y el USIM. Como el HLR nunca se comunica directamente con el terminal, el VLR del servidor del MSC realiza el procedimiento de autenticación. Por tanto, el VLR representa un servidor de autenticación.

El servidor del MSC descarga de uno a cinco vectores de autenticación (AV, Vector de autenticación – Authentication Vector, en inglés) del HLR cuando el servidor del MSC recibe del terminal una solicitud de conexión.

Los parámetros en el AV son:

- RAND: la pregunta de seguridad que sirve como uno de los parámetros de entrada para generar las otras 4 configuraciones del AV. RAND está codificado en 128 bits;

- SRES: el resultado esperado, utilizado por la red para la autenticación del USIM (entre 32 y 128 bits);

- AUTN: el token de autenticación utilizado por el USIM para la autenticación de la red (128 bits);

- CK: la clave de sesión utilizada para el cifrado de comunicaciones (128 bits);

- IK: una clave de integridad (128 bits), para proteger la integridad de la señalización entre el terminal y el RNC (“Radio Network Controller”, en inglés), el elemento de la red de UMTS que controla las estaciones base de transmisión de radio básicas (el RNC gestiona la asignación de recursos de radio, cifrando los datos antes de enviarlos al terminal, así como parte de la ubicación de los abonados).

Los algoritmos F1 a f5 se utilizan para generar estos parámetros (véase la Figura 1). Se genera un MAC (64 bits) (para ayudar al terminal a autenticar la red, no necesariamente el VLR). AK es una clave de anonimato generada a partir del RAND y de K.

El AuC genera un vector de autenticación a partir de la clave K del terminal que comparte con el USIM y otros dos parámetros: un número de secuencia SQN (48 bits) y el número pseudoaleatorio RAND.

SQN es un contador dispuesto en el HLR/AuC, y es individual para cada USIM. Por su parte, el USIM realiza un seguimiento de una secuencia de contador denominado seguimiento SQuicc, que es el número de secuencia más grande que el USIM ha aceptado.

El vector de autenticación generó cinco partes: el valor aleatorio (RAND), el resultado (RES), que se requerirá en el proceso de pregunta de seguridad/respuesta con el USIM, el token de autenticación (AUTN) para la red de autenticación al USIM, la clave de sesión (CK), que se utilizará para el cifrado, y la clave de control de integridad (IK), que sirven para proteger la integridad de los mensajes de señalización.

El token de autenticación, AUTN, es igual a: AUTN = SQN $\oplus$ AK II AMF II MAC

siendo AK = f5 (RAND, K), AMF (16 bits) un campo de gestión de autenticación, II representa una concatenación y $\oplus$ la función XOR.

Después de la transmisión de la IMSI al HLR/AuC, el VLR, tras la recepción del quíntuplo (RAND, AUTN, XRES, CK, IK), transmite la pregunta de seguridad, RAND, y el token de autenticación, AUTN, que recibió del HLR, al USIM, y espera una respuesta, RES.

En el USIM, tal como se muestra en la Figura 2, MAC, AMF y SQN $\oplus$ AK son recuperadas del AUTN. A continuación, calcula f5 (RAND, K) = AK y deduce SQN.

Si SQuicc está demasiado lejos de SQN (no incluido en un cierto rango), el USIM realiza una fase de resincronización con la red.

Si SQuicc no está demasiado lejos de SQN (incluido en el rango anterior), calcula XMAC = f1 (K, RAND, SQN) y lo compara con el MAC. Si son iguales, la red es autenticada por el USIM.

El USIM también calcula la RES utilizando el RAND y la K para el algoritmo f2. La clave de sesión, CK, también se calcula utilizando el RAND y la clave K del USIM con el algoritmo f3.

La pregunta de seguridad/respuesta se puede resumir de la siguiente manera: El USIM es autenticado por el VLR si el resultado, RES, calculado por el USIM y transmitido al VLR es el mismo XRES recibido del HLR/AuC. Por lo tanto, el token de autenticación, AUTN, permite al USIM verificar si el AuC es auténtico y que no es un tipo de ataque de suplantación de identidad (“man in the middle”, en inglés) por la red de acceso. Además, si RES es igual a XRES, el VLR considera que la autenticación mutua ha tenido éxito. De esta forma se obtiene una autenticación mutua entre la red y el USIM.

Este mecanismo de autenticación se describe en el documento TS 33.102 del 3GPP (por ejemplo, en su versión 13.0.0 de enero de 2016).

Se ha solicitado a la organización 3GPP que proporcione cobertura de red para la organización Protección Civil en caso de desastre o durante operaciones de Protección Civil cuando no hay cobertura de radio 3GPP por parte de operadores nacionales. Por ejemplo, en el caso de un desastre natural, por ejemplo, un huracán, se pueden perder todas las conexiones a una infraestructura de red fija de evolución a largo plazo (LTE – Long Term Evolution, en inglés) existente. Este tipo de operaciones se denominan operaciones aisladas para Protección Civil (IOPS – Isolated Operation for Public Safety, en inglés), ya que el eNB local no tiene acceso a la red central (HLR/AUC) para autenticar al usuario móvil.

IOPS se especifica en el anexo K del documento TS 123 401 de ETSI, V13.6.1 de mayo de 2016 (LTE; mejoras del servicio general de radio por paquetes (GPRS – General Packet Radio Service, en inglés) para el acceso a la red de acceso de radio terrestre universal evolucionada (E-UTRAN – Evolved Universal Terrestrial Radio Access Network, en inglés).

Cuando se pierde la conectividad entre el eNB (estación base de LTE) y la infraestructura fija de la red de LTE, no se puede realizar la autenticación del equipo del usuario. Para proporcionar comunicaciones durante una emergencia, una infraestructura desplegable de LTE puede ser instalada y activada temporalmente para proporcionar cobertura temporal de LTE. Cuando se activa, la infraestructura desplegable de LTE no está conectada a la infraestructura fija de la red LTE y la infraestructura desplegable LTE puede permanecer activa durante un período de tiempo prolongado mientras la infraestructura fija de la red LTE se vuelve a poner en servicio.

Las redes LTE incluyen, entre otros componentes, bases de datos, tales como un servidor de abonados locales (HSS), que almacena información relacionada con el usuario y con la suscripción. Por ejemplo, el HSS fijo está configurado para almacenar la IMSI (Identidad de abonado móvil internacional – International Mobile Subscriber Identity, en inglés) y una clave de autenticación (K) relacionada utilizada para identificar y autenticar a un abonado en un dispositivo de comunicación (tal como un teléfono móvil o un ordenador).

El sistema desplegable puede estar dispuesto en un entorno móvil, por ejemplo, en un camión. Para que el sistema implementable complete con éxito la autenticación de acceso a la red de los dispositivos de comunicación, el sistema implementable debe mantener su propio HSS cuando no hay conectividad a la infraestructura fija de la red

de LTE. El HSS desplegable también está configurado para almacenar información relacionada con el usuario y con la suscripción.

No obstante, la solución actual propuesta por el 3GPP a las organizaciones de Protección Civil (Ministerio del Interior del Reino Unido, Departamento de Comercio de EE. UU., Ministerio del Interior, Francia) no cumple completamente los requisitos. En la actualidad, la solución solo permite que entre 50 y 60 redes locales diferentes de IOPS operen en un país/estado, donde una estimación aproximada requeriría de 10 a 15 veces más. En un país tal como Francia, por ejemplo, hay aproximadamente 100 departamentos que pueden tener policías locales, bomberos, primera fuerza de rescate, gendarmería, etc. y cada una de estas entidades necesita un FSS/AUC, por ejemplo, en cada departamento.

La solución actual se basa en una diversificación de una clave de IOPS a largo plazo Ki (Ki1 para la policía local, Ki2 para los bomberos, ...) en 50 a 60 claves locales K de IOPS (una para cada red local de IOPS). La indexación y diversificación de claves está basada en el campo de la gestión de la autenticación (AMF – Authentication Management Field, en inglés) en el paquete de AUTN del vector de autenticación (véase el documento TS 33.102 del 3GPP). Cada clave local K de IOPS se comparte (almacena) previamente en el HSS/AUC de IOPS local y en el USIM que tiene permiso para acceder a la red local de IOPS correspondiente.

La limitación proviene de los bits disponibles en el AMF en el mecanismo de autenticación del 3GPP para proporcionar al USIM el identificador de red local IOPS: el AMF puede contener 16 bits, pero 10 están reservados para los MNO y, por lo tanto, solo 6 bits están disponibles en el AMF para identificación de redes locales IOPS.

El número máximo de redes locales IOPS que pueden funcionar (idealmente $2^6 = 64$), por lo tanto, en muchos casos, no es suficiente.

La presente invención propone una solución a este problema.

La invención propone un servidor de autenticación de una red de telecomunicaciones celular, estando el servidor de autenticación dispuesto para generar un token de autenticación para ser transmitido a un terminal de telecomunicaciones, comprendiendo el token de autenticación un código de autenticación de mensaje y un número de secuencia, en donde el código de autenticación de mensaje es igual a:

$$MACx = KIdx \text{ XOR } f1(AMF,SQNx,RAND,K)$$

siendo KIdx una información de índice de clave en forma de una desviación de un MAC igual a:

$$MAC = f1(K,AMF,SQNx,RAND)$$

siendo f1 una función, K una clave, RAND un número aleatorio y SQNx un contador de secuencia relativo a una clave Kx correspondiente obtenida a partir de la clave K, y KIdx, y AMF el contenido de un campo de gestión de autenticación tal como el definido en el documento TS 33.102 del 3GPP.

Preferiblemente, el servidor de autenticación también calcula un vector de autenticación que se transmitirá al terminal de telecomunicaciones, siendo el vector de autenticación igual a:

$$AVx = RAND||XRESx||CKx||IKx||AUTNx$$

Siendo:

$$XRESx = f2(RAND,Kx)$$

$$CKx = f3(RAND,Kx)$$

$$AUTNx = SQNx \text{ XOR } AK \,||\, AMF \,||\, MACx$$

$$AK = f5(RAND,K)$$

Ventajosamente, el servidor de autenticación es un servidor de autenticación IOPS.

La invención también se refiere a una UICC que comprende una aplicación de USIM, estando configurada la aplicación de USIM para recibir, desde un terminal de telecomunicaciones con el que coopera, un mensaje.

$$AUTNx \,||\, RAND$$

siendo RAND un número aleatorio y AUTNx igual a:

$$AUTNx = SQNx \text{ XOR } AK \,||\, AMF \,||\, MACx$$

siendo AK = f5 (RAND, K)

y siendo MACx igual a:

$$MACx = KIdx \text{ XOR } f1(AMF,SQNx,RAND,K)$$

siendo KIdx una información de índice de clave en forma de desviación de un MAC igual a:

$$MAC = f1(K,AMF,SQNx,RAND)$$

siendo f1 y f5 funciones, K una clave, SQNx un contador de secuencia relativo a una clave Kx correspondiente obtenida a partir de la clave K, y KIdx, y AMF el contenido de un campo de gestión de autenticación tal como el definido en el documento TS 33.102 del 3GPP,

calculando la aplicación un valor

$$XMAC = f1(AMF,SQNx,RAND,K)$$

y un índice de clave

$$KId = XMAC \text{ XOR } MACx$$

verificando la aplicación que el KId calculado coincide con uno de los KIds en una lista blanca almacenada y, si la coincidencia es positiva, calcula la clave Kx correspondiente en base al KIdx, y calcula la clave AK, SQNx y

$$RESx = f2(Kx,RAND)$$

$$CKx = f3(Kx,RAND)$$

$$IKx = f4(Kx,RAND)$$

y enviando RESx, CKx e IKx al terminal de telecomunicaciones.

Otras particularidades y ventajas de la invención resultarán evidentes con la lectura de una realización ventajosa de la invención, que se da a título ilustrativo y no limitativo, y haciendo referencia a los dibujos adjuntos, en los que:

- la Figura 1 representa la generación de AUTN y vectores de autenticación AV a nivel de HSS/AUC;

- la Figura 2 representa la autenticación por un USIM del HSS/AUC de un operador de red;

- la Figura 3 representa una realización preferida de la presente invención, obtenida al nivel de un HSS/AUC;

- la Figura 4 representa el método de autenticación mutua según la invención.

Las Figuras 1 y 2 se han descrito previamente con respecto al estado de la técnica.

La Figura 3 representa una realización preferida de la presente invención, obtenida al nivel de un HSS/AUC.

Respecto a esta figura en comparación con la Figura 1, las diferencias son las siguientes:

Se utiliza una nueva clave Kx para generar SQNx (en lugar de SQN), XRESx (en lugar de XRES), CKx (en lugar de CK), IKx (en lugar de IK) y otro índice de clave KIdx se utiliza para diversificar el MAC para obtener un valor MACx.

La invención consiste en que el Servidor de Autenticación (HSS/AUC) inyecte una información adicional de índice de Clave (KIdx – K Index, en inglés) en forma de desviación en la parte de MAC (MACx) del AUTN que se envía al USIM. La información adicional del índice de claves permite generar e indexar claves adicionales sin cambiar el protocolo de autenticación existente.

El algoritmo de inyección de índice de clave se describe mediante las siguientes ecuaciones para un KIdx determinado:

K se calcula en base al AMF, tal como se propone en el documento TS 33.102 del 3GPP. Es una clave diversificada de la clave a largo plazo definida para IOPS.

Kx = Deriv (KIdx, K). Por ejemplo, Kx = HMAC-SHA-256 (K, KIdx).

SQNx = Generado en relación con la clave Kx correspondiente. Por ejemplo, SQNx es un número de secuencia que se incrementa en 1 cada vez que se genera un vector de autenticación en base a la clave Kx.

$$MACx = KIdx \text{ XOR } f1(AMF,SQNx,RAND,K)$$

$$AK = f5(RAND,K)$$

$$AUTNx = SQNx \text{ XOR } AK \,||\, AMF \,||\, MACx$$

$$XRESx = f2(RAND,Kx)$$

$$CKx = f3(RAND,Kx)$$

$$IKx = f4(RAND,Kx)$$

$$AVx = RAND||XRESx||CKx||IKx||AUTNx$$

A continuación, se muestran algunos ejemplos que muestran cómo un MAC se transforma en un MACx:

Para MAC (64 bits) = 0x1122334455667788 y Kldx = 0x2222222222222222, MACx (64 bits) = 0x33001166774455AA.

Para MAC (64 bits) = 0x1122334455667788 y Kidx = 0x5151515151515151, MACx (64 bits) = 0x40736215043726D9.

Kx está, por ejemplo, diversificado, o es, por ejemplo, un número aleatorio.

Kldx es una información de índice de clave correspondiente a Kx.

Una vez que los vectores de Autenticación son generados por el HSS/AUC (tras el procedimiento de autenticación del USIM), son enviados a la Entidad de Gestión de la Movilidad (MME – Mobility Management Entity, en inglés), que gestiona localmente la autenticación y autorización del USIM/Mobile.

La Figura 4 representa el método de autenticación mutua según la invención.

Aquí están representadas cuatro entidades: el HSS/AUC, la MME, el terminal de telecomunicaciones ME y el USIM.

Con el propósito de autenticación, el USIM envía primero su IMSI al HSS/AUC a través de la ME y la MME. El HSS/AUC genera localmente los vectores de autenticación AVx y envía estos vectores a la MME. La MME almacena localmente el AVx y envía el par (RAND, AUTNx) al USIM.

Tras la recepción, el USIM recupera la información del AMF de AUTNx (siendo AUTNx = SQNx XOR AK || AMF || MACx).

En base a la información del AMF, el USIM verifica si la clave de largo plazo debe ser obtenida en una clave K de IOPS. Si es así, calcula la clave K de IOPS.

El USIM calcula el XMAC esperado con f1: XMAC = f1 (AMF, SQNx, RAND, K)

y el índice de claves Kld = XMAC XOR MACx. MACx es extraído de AUTNx.

El USIM verifica que el Kld calculado sea un valor aceptable. Por ejemplo, el Kld calculado coincide con uno de los Klds en una lista blanca almacenada de Klds. Si esta coincidencia es positiva, el Kld emparejado es el Kldx inyectado. La lista blanca de Klds es una lista de Kldx que son aceptables por el USIM. Esta lista puede ser dispuesta en el USIM durante la fabricación del USIM, o ser descargada al USIM de manera inalámbrica durante el funcionamiento. En otras realizaciones, los Klds aceptables pueden ser Klds que cumplan algunas condiciones dadas, por ejemplo, Klds cuyo número de bits configurados en 1 es igual a 6.

El USIM calcula/recupera la clave Kx correspondiente en base al Kldx y calcula la clave AK = f5 (RAND, K), descifra el SQNx de AUTNx y verifica que SQNx sea coherente con Kx para evitar ataques de repetición.

A continuación, el USIM calcula RESx, CKx, IKx en base al RAND y a la Kx.

El USIM devuelve RESx, CKx e IKx a la ME.

La ME almacena CKx e IKx (ya que no conoce la clave a largo plazo) y envía RESx como respuesta a la pregunta de seguridad, a la MME.

A continuación, la MME compara el RESx recibido con su valor esperado XRESx.

El proceso de autenticación tiene éxito si XRESx y RESx son iguales. De lo contrario, la autenticación del USIM se considera fallida.

La invención permite indexar claves adicionales en el caso de utilización de Operación aislada para Protección Civil.

La indexación adicional reutiliza el mismo protocolo de autenticación, por lo que el intercambio de mensajes entre las distintas entidades: HSS/AUC, MME, ME, USIM no se modifica.

Puesto que el índice de clave es inyectado como una desviación al MAC, el proceso de recuperación consiste en realizar una búsqueda de la desviación recuperada en una lista blanca. Esto no requiere volver a calcular el MAC o las claves.

La invención eleva las limitaciones en el mecanismo de autenticación del 3GPP a más redes locales IOPS para ser implementadas sin colisiones de claves. Se puede utilizar para casos de utilización de operaciones aisladas de Protección Civil, pero también se puede utilizar en casos de utilización comercial/del consumidor.

REIVINDICACIONES

1. Un servidor de autenticación de una red de telecomunicaciones celular, estando dispuesto dicho servidor de autenticación para generar un token de autenticación para ser transmitido a un terminal de telecomunicaciones, comprendiendo dicho token de autenticación un código de autenticación de mensaje y un número de secuencia, en donde dicho código de autenticación de mensaje es igual a:

$$MACx = KIdx \text{ XOR } f1(AMF,SQNx,RAND,K)$$

siendo Kldx una información de índice de clave en forma de desviación de un MAC igual a:

$$MAC = f1(K,AMF,SQNx,RAND)$$

siendo f1 una función, K una clave, RAND un número aleatorio y SQNx un contador de secuencia relativo a una clave Kx correspondiente obtenida a partir de la clave K, y Kldx, y AMF el contenido de un campo de gestión de autenticación tal como el definido en el documento TS 33.102 del 3GPP.

2. Un servidor de autenticación según la reivindicación 1, en el que también calcula un vector de autenticación a transmitir a dicho terminal de telecomunicaciones, siendo dicho vector de autenticación igual a:

$$AVx = RAND||XRESx||CKx||IKx||AUTNx$$

Siendo:

$$XRESx = f2(RAND,Kx)$$

$$CKx = f3(RAND,Kx)$$

$$AUTNx = SQNx \text{ XOR } AK \,||\, AMF \,||\, MACx$$

$$AK = f5(RAND,K)$$

3. Un servidor de autenticación según la reivindicación 1 o 2, en el que es un servidor de autenticación IOPS.

4. UICC que comprende una aplicación de USIM, estando configurada dicha aplicación de USIM para recibir desde un terminal de telecomunicaciones con el que coopera, un mensaje

$$AUTNx \text{ II } RAND$$

siendo RAND un número aleatorio y AUTNx igual a:

$$AUTNx = SQNx \text{ XOR } AK \,||\, AMF \,||\, MACx$$

siendo AK = f5 (RAND, K)

y siendo MACx igual a:

$$MACx = KIdx \text{ XOR } f1(AMF,SQNx,RAND,K)$$

siendo Kldx una información de índice de clave en forma de desviación de un MAC igual a:

$$MAC = f1(K,AMF,SQNx,RAND)$$

siendo f1 y f5 funciones, K una clave, SQNx un contador de secuencia relativo a una clave Kx correspondiente obtenida a partir de la clave K, y Kldx, y AMF el contenido de un campo de gestión de autenticación tal como el definido en el documento TS 33.102 del 3GPP,

calculando dicha aplicación un valor

$$XMAC = f1(AMF,SQNx,RAND,K)$$

y un índice de clave

$$KId = XMAC \text{ XOR } MACx$$

verificando dicha aplicación que el Kld calculado coincide con uno de los KIds en una lista blanca almacenada y, si la coincidencia es positiva, calcula la clave Kx correspondiente en base a la Kldx, y calcula dicha clave AK, SQNx y

$$RESx = f2(Kx,RAND)$$

$$CKx = f3(Kx,RAND)$$

$$IKx = f4(Kx,RAND)$$

y enviando RESx, CKx e IKx a dicho terminal de telecomunicaciones.

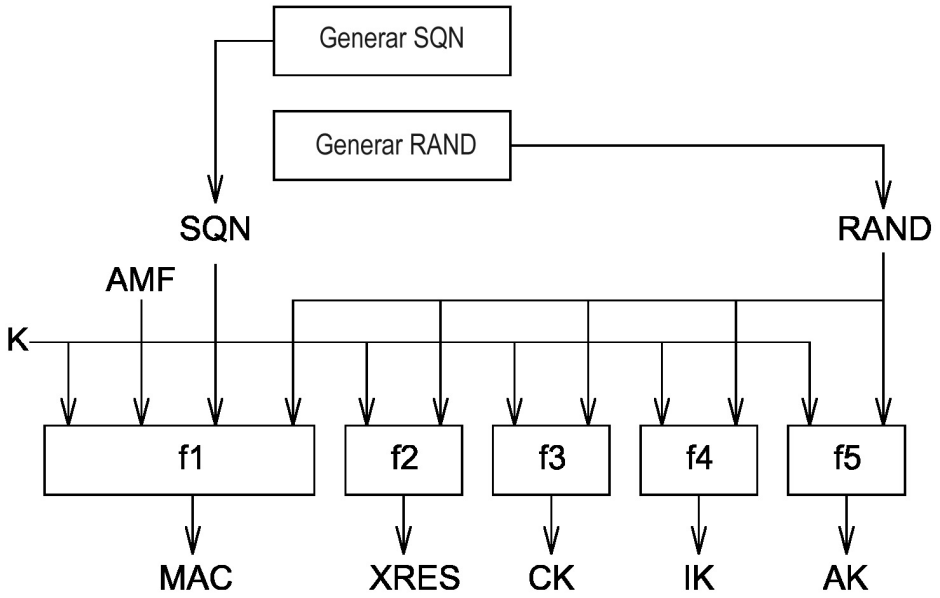

Fig. 1

AUTN := SQN⊕AK || AMF || MAC

AV := RAND || XRES || CK || IK || AUTN

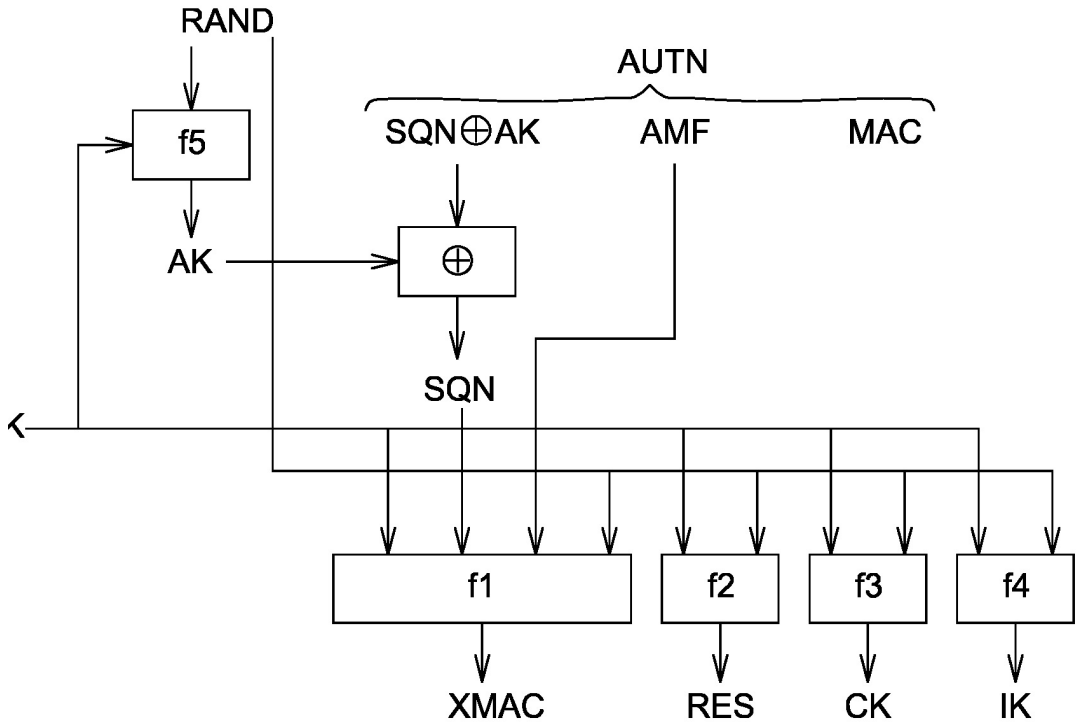

Fig. 2

Verificar MAC = XMAC

Verificar que SQN está en el intervalo correcto

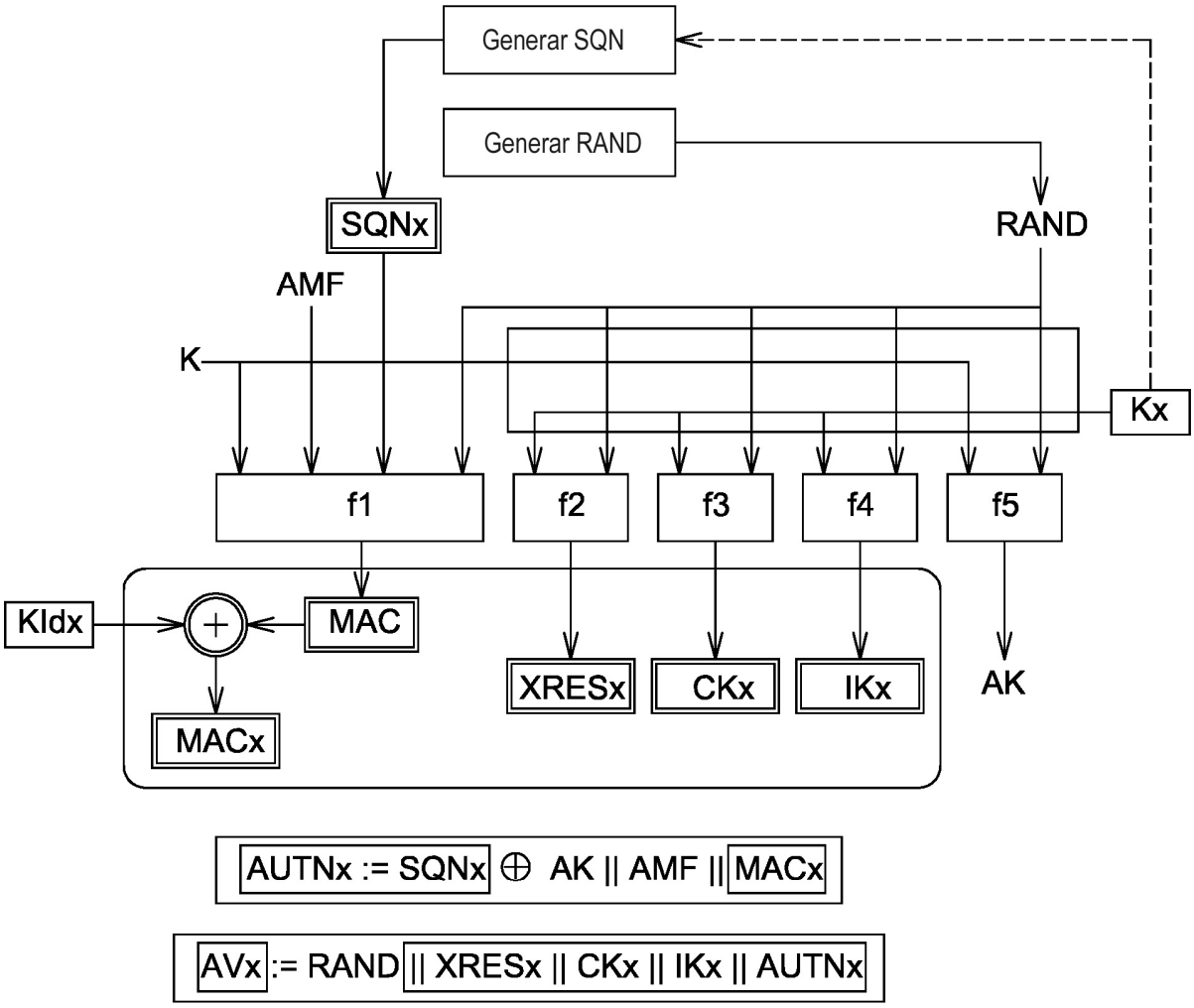
Generar SQN
Generar RAND
SQNx
RAND
AMF
K
Kx
f1
f2
f3
f4
f5
KIdx
MAC
MACx
XRESx
CKx
IKx
AK
AUTNx := SQNx ⊕ AK || AMF || MACx
AVx := RAND || XRESx || CKx || IKx || AUTNx

Fig. 3

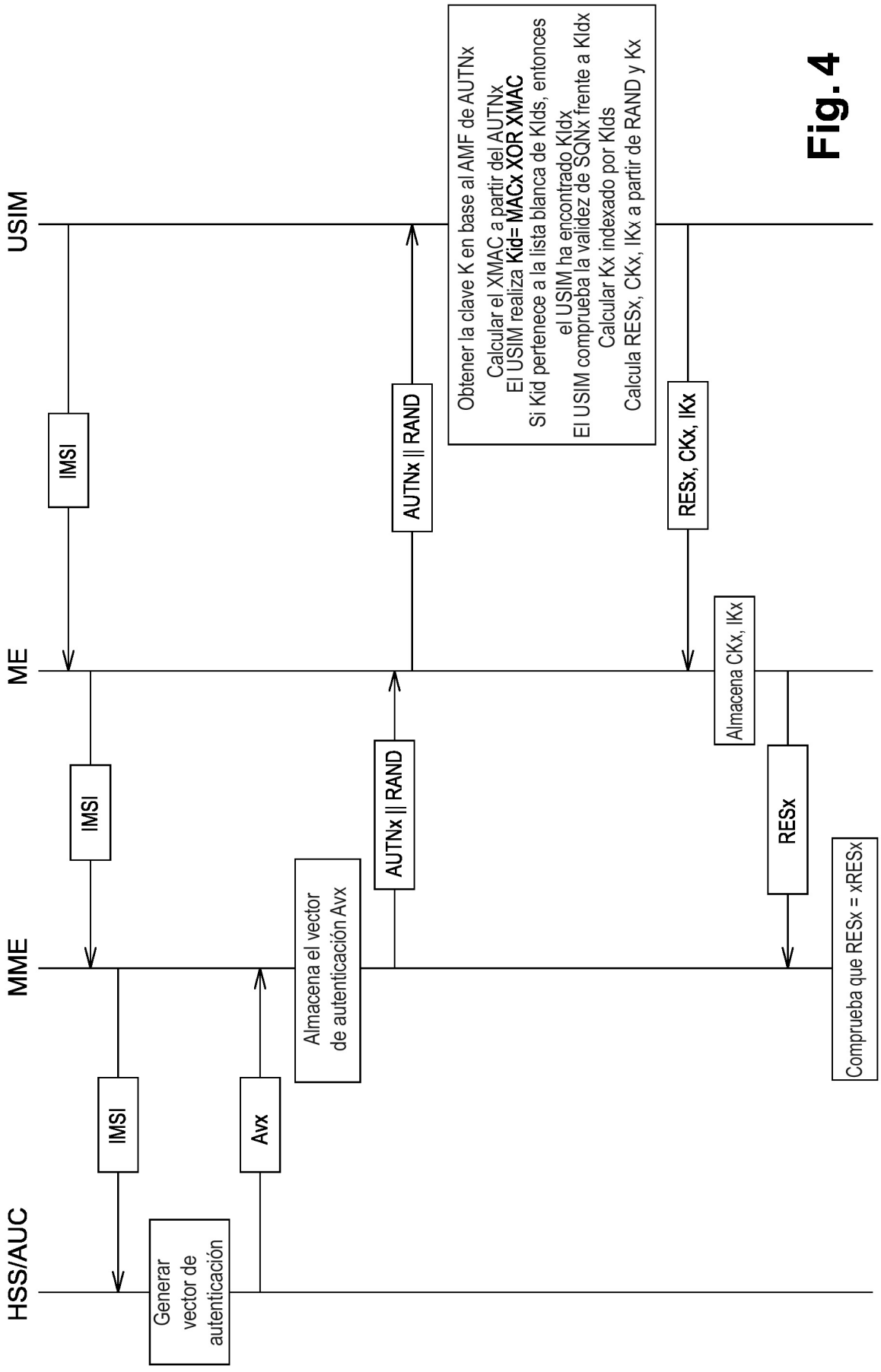
USIM
ME
MME
HSS/AUC
IMSI
IMSI
IMSI
Generar vector de autenticación
Avx
Almacena el vector de autenticación Avx
AUTNx || RAND
AUTNx || RAND
Obtener la clave K en base al AMF de AUTNx
Calcular el XMAC a partir del AUTNx
El USIM realiza Kid= MACx XOR XMAC
Si Kid pertenece a la lista blanca de KIds, entonces el USIM ha encontrado KIdx
El USIM comprueba la validez de SQNx frente a KIdx
Calcular Kx indexado por KIds
Calcula RESx, CKx, IKx a partir de RAND y Kx
RESx, CKx, IKx
Almacena CKx, IKx
RESx
Comprueba que RESx = xRESx

Fig. 4