ANÁLISIS DE EFECTIVAD DE LA AUTENTICACIÓN Y CONTROL DE ACCESO IMS-AKA COMO MECANISMO DE PROTECCIÓN DE INTEGRIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN EN LOS SERVICIOS BASADOS EN IP

ANDREA TATIANA ROMERO PEÑA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2022

ANÁLISIS DE EFECTIVAD DE LA AUTENTICACIÓN Y CONTROL DE ACCESO IMS-AKA COMO MECANISMO DE PROTECCIÓN DE INTEGRIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN EN LOS SERVICIOS BASADOS EN IP

ANDREA TATIANA ROMERO PEÑA

Monografía

Director:
YENNY STELLA NUÑEZ ALVAREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2022

Página de Aceptación

_____

Jurado I

_____

Jurado 2

Bogotá, mayo 2022

RESUMEN

Las redes de nueva generación (NGN) son consideradas en la actualidad como redes seguras y confiables con capacidad de integración y multiservicio. La arquitectura de las NGN se describe bajo un conjunto de especificaciones a través del protocolo de internet (IP) conocido como subsistema multimedia IP (IMS). No obstante, este protocolo ha tenido dificultades de seguridad lo que reduce la confiabilidad de las NGN; entre los protocolos más usados para reducir los problemas de seguridad se encuentra el acuerdo de autenticación y clave inicial (AKA) que se configura como un protocolo en constante evolución para reducir los problemas de seguridad emergente o inherentes en el IMS. La presente monografía realiza un análisis de la efectivad de la autenticación y control de acceso IMS-AKA como mecanismo de protección de integridad y confidencialidad de la información en los servicios basados en IP. Para cumplir con este fin, se identificó la arquitectura IMS-AKA y sus características de seguridad para el acceso seguro. En segundo lugar, se examinaron los diferentes mecanismos de seguridad utilizados por IMS-AKA para la autenticación y control de acceso en los servicios basados en IP, en tercer lugar, se establecieron los errores o fallos de autenticación y control de acceso relacionados con la configuración de seguridad IMS-AKA y, finalmente, se determinaron los procedimientos de configuración de la asociación de seguridad que influyen en la efectividad como mecanismo de protección de integridad y confidencialidad de la información en los servicios basados en IP. Se concluye que la mayoría de los aspectos dentro de la seguridad informática de las redes de nueva generación se encuentran en constante evolución y cambio y que estas son más vulnerables a ataques, se recomienda ejercer procedimientos de configuración que tenga en cuenta aspectos corporativos de prevención.

Palabras clave: autenticación y acuerdo de clave, subsistema multimedia IP, red de nueva generación, protocolos mejorados, seguridad.

ABSTRACT

New generation networks (NGN) are currently considered safe and reliable networks with integration and multi-service capacity. The NGN architecture is described under a set of specifications through the Internet Protocol (IP) known as IP Multimedia Subsystem (IMS). However, this protocol has had security difficulties, which reduces the reliability of the NGN; Among the most used protocols to reduce security problems is the initial key and authentication agreement (AKA), which is configured as a protocol in constant evolution to reduce emerging or inherent security problems in the IMS. This monograph aims to analyze the effectiveness of IMS-AKA authentication and access control as a protection mechanism for the integrity and confidentiality of information in IP-based services. To accomplish this, the IMS-AKA architecture and its security features for secure access were identified. Second, the different security mechanisms used by IMS-AKA for authentication and access control in IP-based services were examined, thirdly, the configuration-related authentication and access control errors or failures were established. IMS-AKA security system and, finally, the security association configuration procedures that influence the effectiveness as a mechanism for protecting the integrity and confidentiality of information in IP-based services were determined. It is concluded that most of the aspects within the computer security of the new generation networks are in constant evolution and change and that these are more vulnerable to attacks, it is recommended to exercise configuration procedures that take into account corporate aspects of prevention.

Keywords: authenticated and key agreement, IP multimedia subsystem, new-generation network, improved protocols, security

CONTENIDO

LISTA DE FIGURAS

pág

LISTA DE TABLAS

Pág

INTRODUCCIÓN

Las redes de nueva generación, en adelante NGN, por sus siglas en inglés, se han posicionado como redes seguras y confiables que permiten crear un entorno de red de telecomunicaciones a partir de la integración entre tecnologías inalámbricas, telefonía fija y servicios. Este tipo de redes están basadas en Protocolo de Internet (en adelante IP, por sus siglas en inglés) y pretenden ser multiservicios, multiprotocolo, multiacceso[1]. Según la recomendación UIT-T Y.2001 las NGN permiten el cumplimiento de ciertos objetivos importantes para el desarrollo de países como Colombia[2], por ejemplo, en esta recomendación se menciona el potencial de NGN para promover la competencia justa, alentar la inversión privada, ofrecer un acceso abierto a redes que favorezca la igualdad de oportunidades a ciudadanos, así como promueva la diversidad en contenidos y asegure la prestación[3].

Con esto en mente, la implementación y operación adecuada de NGN es de interés para países en desarrollo. No obstante, debido a la naturaleza abierta y colaborativa de este tipo de redes, se han evidenciado problemas de seguridad en las NGN asociados a ataques de redirección, ataques de hombre en el medio o man-in-the-middle attack (MITM) y ataques de denegación de servicio o denial-of-service attacks (DoS)[4]. Esto ha generado la creación de diversos protocolos de seguridad con el fin de reducir los ataques y garantizar la seguridad en el uso e implementación de NGN, entre los protocolos se encuentra el acuerdo de autenticación y clave inicial (AKA) que se configura como un protocolo en constante evolución para reducir los problemas de seguridad emergente o inherentes en el Subsistema Multimedia IP (IMS por sus siglas en ingles)[5].

Teniendo en cuenta lo anterior, la presente monografía procura reconocer cómo los esfuerzos de investigación relacionados con los acuerdos de autenticación y clave inicial (AKA) han evolucionado en el marco de las redes de nueva generación (NGN)

[1] APARICIO BAQUEN, Christian Camilo. Resiliencia en la plataforma MTC aplicada a smartcities [en línea]. Trabajo de Grado. Universidad de los Andes, Bogotá.: 2013.
[2] Unión internacional de telecomunicaciones. Serie Y: infraestructura mundial de la información, aspectos del protocolo internet y redes de la próxima generación Redes de la próxima generación – Marcos y modelos arquitecturales funcionales. Ginebra, 2004, p.3.
[3] DIAZ BOHÓRQUEZ, Anyel Carolina. Propuesta de política pública para la gestión de los residuos electrónicos generados por la transición hacia NGN en Colombia [en línea]. Trabajo de Grado Maestría. Universidad Nacional de Colombia, 2015.
[4] CHENGZHE, Lai, et al. SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks. Computer Networks [en línea]. 2013, enero. 5. 3492-3510. Disponible en: https://doi.org/10.1016/j.comnet.2013.08.003.
[5] Ibíd., p 23

basadas en el Subsistema Multimedia IP (IMS, por sus siglas en ingles) y su objetivo se basa en analizar los parámetros y esquemas de seguridad proporcionados por IMS-AKA para brindar efectividad en la autenticación y control de acceso en los servicios basados en IP De esta manera, se pretende comprender el estado actual de los protocolos AKA, así como reconocer las fortalezas y los retos de estos protocolos en la seguridad aplicada a NGN

1. PLANTEAMIENTO DEL PROBLEMA

A diferencia de las redes de segunda y tercera generación, que se caracterizan por tener una red central controlada por un único operador de red, las redes de nueva generación están controladas por múltiples operadores que coexisten y administran de manera conjunta la red central[6]. Esta característica conlleva a varios retos con respecto de seguridad informática en las NGN, artículos han encontrado que las tecnologías de la información y comunicación relacionadas con NGN son más propensos a ciberataques, dado a que existe una vulnerabilidad en las redes durante el procesamiento de gran cantidad de datos[7].

Debido a las preocupaciones de seguridad se han desarrollado diferentes protocolos desde los inicios de implementación de NGN a nivel mundial, dichos protocolos se han modificado en función de reducir los impactos de los ataques propios de NGN, y de responder a las nuevas formas de ataques que se han presentado durante la implementación de este tipo de redes. Uno de los protocolos más reconocidos es el protocolo basado en acuerdo de autenticación y clave inicial (AKA) el cual permite identificar y autorizar nodos móviles en diversas redes[8].

Actualmente, se evidencian diferentes protocolos tipo AKA, entre los que se encuentran EPS-AKA, UMTS-AKA de 3G, LTE AKA entre otros[9]. A la fecha, no se ha analizado la evolución de los protocolos AKA, por lo cual, no se conoce las debilidades, fortalezas y mejoras de los mismos que estos han presentado a lo largo de su desarrollo. Bajo esta diversidad de protocolos puede ser confuso comprender el estado actual de la seguridad en NGN y las limitaciones de los protocolos o los retos de seguridad que no se han logrado resolver. De manera que la presente monografía busca responder a la pregunta:

¿Cuáles son parámetros y esquemas de seguridad proporcionados por IMS-AKA para brindar efectividad en la autenticación y control de acceso en los servicios basados en IP?

[6] MAHDI, Glenford. A survey on authentication and key agreement protocols in heterogeneous networks. IJNSA: *International Journal of Network Security & Its Applications* [en línea]. 2012

[7] GANDOTRA, Ekta., BANSAL, Divya, y SOFAT, Sanjeev. Malware Analysis and Classification: A Survey. *Journal of Information Security* [en línea].

[8] CHENGZHE et al. Op. cit.

[9] NEETESH, Saxena, JAYA, Thomas, y NARENDRA, Chaudhari. ES-AKA: An Efficient and Secure Authentication and Key Agreement Protocol for UMTS Networks. *Wireless Personal Communications* [en línea]. 2015,

2. JUSTIFICACIÓN

El presente trabajo de investigación pretende analizar los parámetros y esquemas de seguridad proporcionados por IMS-AKA para brindar efectividad en la autenticación y control de acceso en los servicios basados en IP, esto a partir de la revisión de la evolución y las características propias de los protocolos, tales como sus fortalezas y debilidades al momento de solventar necesidades de seguridad. De esta manera, la utilidad de esta investigación radica en compilar información sobre el desarrollo de protocolos y, así mismo, reconocer los retos de seguridad resueltos, persistentes y nuevos en el campo de las redes de nueva generación y de los protocolos tipo AKA.

La información recopilada y analizada en este estudio, también podría permitir la detección de alternativas de mejoras a los protocolos AKA, y poner en evidencia puntos críticos de intervención, a partir de los cuales se podrían establecer nuevas investigaciones que aporten a la generación de conocimiento en beneficio del progreso de los sistemas de seguridad. Un ejemplo de la conveniencia de estudios de revisión como este es el trabajo hecho por Kouicem, Bouabdallah y Lakhlef, en el cual se analizaron las soluciones de seguridad y privacidad propuestas para el Internet de las cosas (IoT, por sus siglas en inglés), como conclusión de esta investigación se identificaron los principales problemas y/o campos de investigación que enfrenta la seguridad de IoT: la escalabilidad y el dinamismo[10].

Finalmente, este estudio pretende contribuir a la línea de investigación de Infraestructura tecnológica y seguridad en redes, específicamente en la temática de redes de nueva generación (NGN), de la Escuela de Ciencias Básicas, Tecnología e Ingeniería de la Universidad Nacional Abierta y a Distancia (UNAD). Esto a través del análisis de los parámetros y esquemas de seguridad proporcionados por IMS-AKA para brindar efectividad en la autenticación y control de acceso en los servicios basados en IP.

[10] KOUICEM, Djamel., BOUABDALLAH, Abdelmadjid y LAKHLEF, Hicham. Internet of things security: A top-down survey. Computer Networks [en línea]. 2018, 218.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Analizar los parámetros y esquemas de seguridad proporcionados por IMS-AKA para brindar efectividad en la autenticación y control de acceso en los servicios basados en IP

3.2 OBJETIVOS ESPECÍFICOS

- Identificar la arquitectura IMS-AKA y sus características de seguridad para el acceso seguro.

- Examinar los diferentes mecanismos de seguridad utilizados por IMS-AKA para la autenticación y control de acceso en los servicios basados en IP.

- Establecer los errores o fallos de autenticación y control de acceso relacionados con la configuración de seguridad IMS-AKA.

- Determinar los procedimientos de configuración de la asociación de seguridad que influyen en la efectividad como mecanismo de protección de integridad y confidencialidad de la información en los servicios basados en IP.

4. MARCO REFERENCIAL

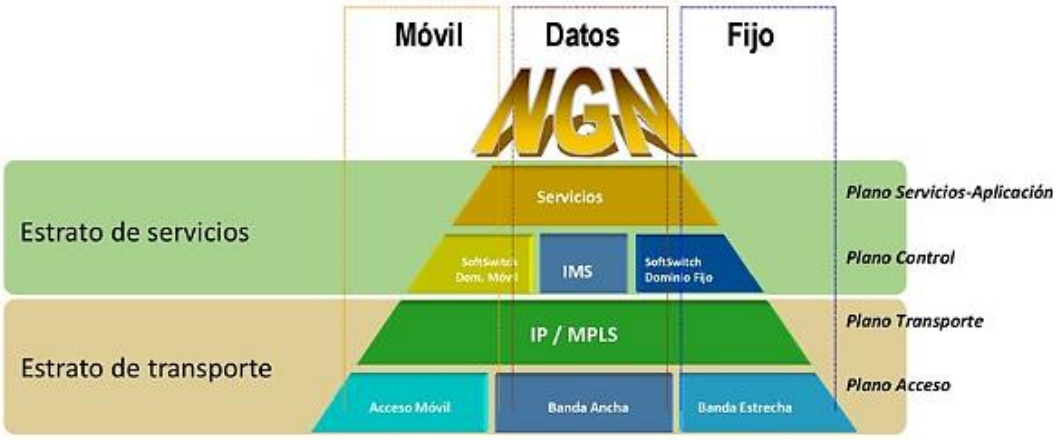
4.1 MARCO TEÓRICO

4.1.1 Redes de nueva generación (NGN)

Las redes de nueva generación (NGN) permiten la convergencia tecnológica de servicios multimedia como voz, datos, video, multimedia, entre otros. Este tipo de redes están fundamentadas en el protocolo IP (Internet Protocol) y requieren de calidad, seguridad y movilidad de datos, por lo cual, se reconocen como redes rápidas y competitivas[11]. En la Figura 1, se expone el modelo actual de NGN, subdivido en dos estratos, el de servicios y el de transporte, los cuales a su vez están divididos en planos de acceso, transporte, control y servicio. Por su parte, la Unión Internacional de Telecomunicaciones definió la NGN como una:

> Red basada en paquetes que permite prestar servicios de telecomunicación y en la que se pueden utilizar múltiples tecnologías de transporte de banda ancha propiciadas por la QoS, y en la que las funciones relacionadas con los servicios son independientes de las tecnologías subyacentes relacionadas con el transporte. Permite a los usuarios el acceso sin trabas a redes y a proveedores de servicios y/o servicios de su elección. Se soporta movilidad generalizada que permitirá la prestación coherente y ubicua de servicios a los usuarios[12].

Figura 1. Modelo actual de NGN



[11] BARRAGÁN DEL POZO, Edgar Edison. Análisis de la tecnología IMS (IP Multimedia Subsystem) y diseñar un servicio de transmisión multimedia de video mediante Open IMS core para evaluar el tráfico unicast y multicast [en línea]. Tesis de Maestría. Escuela Superior Politécnica de Chimborazo, 2019. p. 6.
[12] Unión Internacional de telecomunicaciones, Op. cit, p.2.

Fuente: MONTERO, Juan. Redes avanzadas y servicios. 2018. Disponible en https://slideplayer.es/slide/13809638/#.XdNKkjszyq4.gmail. Consultado el 17 de noviembre de 2019

4.1.2 Características de las redes de nueva generación.

Las NGN también pueden definirse en cuanto pueden trasmitir paquetes de servicios integrados aprovechando al máximo el ancho de banda[13]. Entre las principales características de las NGN se encuentran[14]:

- La transferencia o conmutación de datos está basada en paquetes IP/MPLS (Multiprotocol Label Switching).

- Aplica la movilidad generalizada, entendida como la capacidad de utilizar varias tecnologías de acceso con la posibilidad de que el usuario este en movimiento dentro de las fronteras de red existentes.

- Separa las funciones de llamada/sesión y aplicación/servicio, también separa la prestación del servicio y de transporte (Ver Figura 1).

- Facilita la convergencia entre servicios fijos y móviles.

- Permite el interfuncionamiento con redes tradicionales, a través de la migración de redes PSTD, ISDN y otras, a través de interfaces abiertas y protocolos SoftSwitch.

- Soporta múltiples tecnologías de red de telecomunicaciones que alcanzan las instalaciones del usuario final, también conocidas como tecnologías de última milla.

- Permite el acceso sin restricciones de usuarios asociados a diferentes proveedores de servicios.

- Las funciones de servicios son independientes de las tecnologías de transporte.

- Soporta una gama amplia de servicios como los servicios de tiempo real, flujo continuo en tiempo no real y multimedia.

- La arquitectura facilita la conexión basada en paquetes con y sin conexión y/o circuitos.

[13] Ibid., p.2-3
[14] BARRAGÁN, Edgar, Op. cit, p. 7

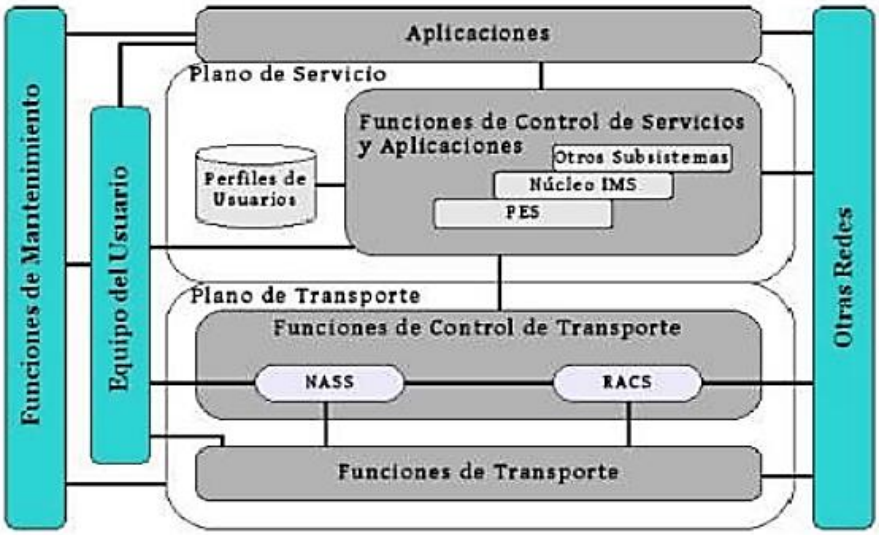
- Permite la distribución simultanea de servicios como telefonía, televisión, acceso a Internet, datos, entre otros.

4.2 MARCO CONCEPTUAL

4.2.1 Arquitectura de las redes de nueva generación.

La arquitectura funcional en las redes de nueva generación se diseñó con la finalidad de cumplir requisitos y de respaldar los servicios a prestar. Para lograr esto, las funciones de NGN se dividen en dos estratos o planos principales, el estrato de transporte y el estrato de servicio. Adicionalmente, se diferencian las redes de los usuarios de otro tipo de redes, así se establecen tres tipos de redes: User Network Interface (UNI), Network Network Interface (NNI) y Application Network Interface (ANI). A partir de estas redes la NGN diferencia en términos de capacidad, escalas, roles, y responsabilidades a las redes de usuarios tipo UNI de otras redes de tipo NNI[15] . En la Figura 2, se muestra de manera general la arquitectura de las NGN.

Figura 2. Arquitectura de redes de nueva generación (NGN)



Fuente: BARRAGÁN, Edgar. Análisis de la tecnología IMS (IP Multimedia Subsystem) y diseñar un servicio de transmisión multimedia de video mediante open ims core para evaluar el tráfico unicast y multicast. Escuela Superior Politecnica de Chimborazo, 2019, p. 6.

[15] MORITA, Naotaka y IMANAKA, Hideo. Introduction to the Functional Architecture of NGN. *IEICE TRANSACTIONS on Communications* [en línea]. 2007, p.1026.

4.2.2 Estrato de transporte.

Este estrato se dedica a la entrega de paquetes IP, que pueden incluir garantía de la calidad del servicio (QoS por sus siglas en inglés), movilidad a nivel de IP, y seguridad[16]. Por tanto, como expone Domínguez, el estrato de transporte "soporta las tareas de la transferencia de información de usuario, control y gestión, y las tareas de control y gestión de los recursos de transporte, para llevar los datos entre entidades terminales"[17].

El estrato de transporte se clasifica en dos subsistemas. El primero, corresponde a Network Attachment Subsystem (NASS), este se encarga de implantar órdenes entre el Equipo del Usuario (UE) y la red de acceso. Lo anterior, requiere de una autenticación y autorización basada en las configuraciones del UE y la reservación de recursos mediante IP. De esta manera, NASS conforma la red de acuerdo con las necesidades del UE. El segundo subsistema, corresponde a Resource and Andministration Control Subsystem (RACS), el cual se encarga de reservar, administrar y controlar recursos que requiere el UE. Por tanto, RACS administra la creación y destrucción de recursos entre planos de señalización, multimedia y gateways[18].

4.2.3 Estrato de servicios

El estrato de servicio provee el control relacionado con el servicio, que se requiere para la navegación web, el intercambio de correos electrónicos, la telefonía IP, videoconferencias, entre otros. Domínguez, expone que este estrato "permite a los usuarios el empleo de diferentes servicios a través de tareas de control y gestión de los recursos y servicios de la red, que facilitan la transferencia de los datos del servicio en cuestión"[19].

Los perfiles de usuarios y los subsistemas que ofrecen servicios, como el núcleo IMS y el Emulation and Simulation (PES) son los principales componentes en el estrato de servicio (Ver Figura 2). En este punto, es indispensable que se localicen los datos del usuario, pero no de los dispositivos asociados a este, así juega un papel importante el almacenamiento de la información del usuario, sus

[16] Ibíd., p.1024.
[17] DOMÍNGUEZ CANG, Nayibis. Arquitectura orientada al servicio de Redes de Nueva Generación (NGN) [en línea]. Trabajo de grado, electrónica y telecomunicaciones. Universidad Central Marta Abre U De las Villas, 2007. p. 11.
[18] BARRAGÁN, Edgar. Op. cit., p. 8.
[19] DOMÍNGUEZ, Nayibis. Op. cit., p. 11.

subscripciones y sus dinámicas de interacción con la red. De esta manera, cada usuario puede tener asociado un conjunto de equipos del usuario, una cantidad de servicios disponibles y unas preferencias específicas de entrega de servicios [20].

[20] BARRAGÁN, Edgar, Op. cit., p. 8-9.

5. ARQUITECTURA IMS-AKA Y SUS CARACTERÍSTICAS DE SEGURIDAD PARA EL ACCESO

5.1 SUBSISTEMA MULTIMEDIA IP (IMS)

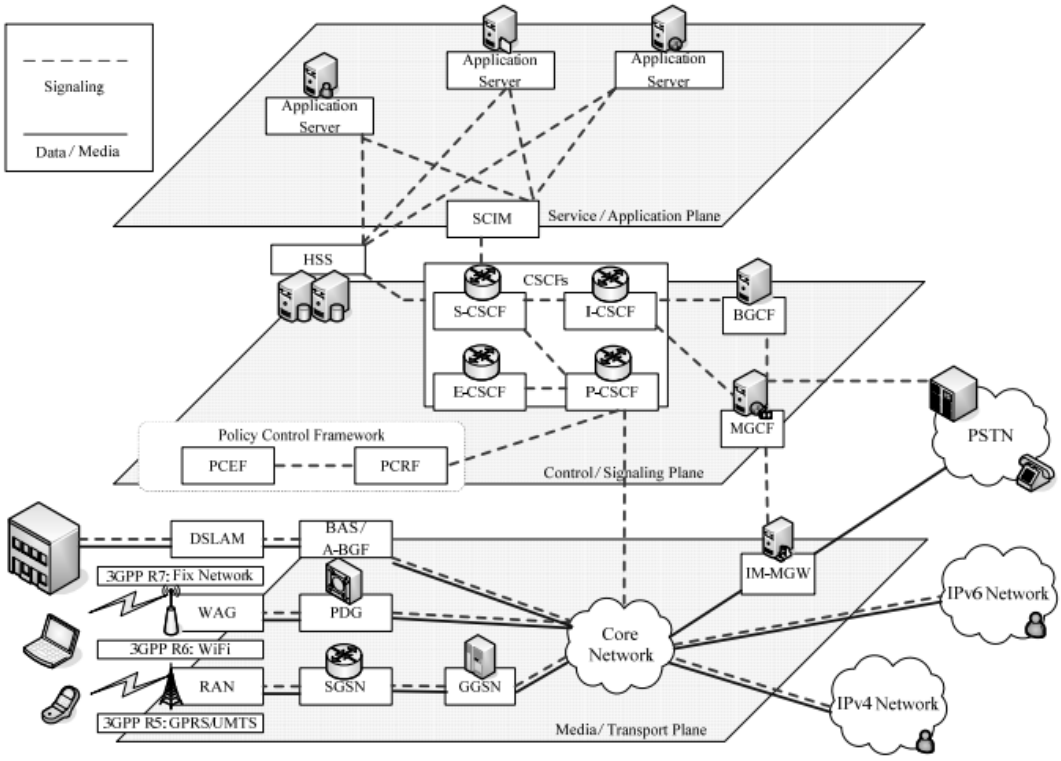
El Subsistema Multimedia IPS (IMS, por sus siglas en inglés) es un estándar internacional que determina la arquitectura general de servicios de voz basadas en IP y multimedia, y es un componente principal en la arquitectura NGN (Ver Figura 2)[21]. El IMS puede usarse para gestionar problemas asociados con el servicio, como la calidad del servicio (QoS), la carga, el control de acceso, la gestión de usuarios y servicios[22]. El conjunto de estándares esenciales para la implementación de IMS se lanzó en el 2004 y fue implementado, por primera vez, en la tecnología inalámbrica europea, no obstante, es con las NGN que se avanzado en la implementación de IMS a gran escala[23]. Como explican Saeed, Maryam y Mohammad “el NGN IMS, también conocido como "Core IMS" es un subconjunto de 3GPP IMS definido en TS 123 002 que está restringido a funcionalidades de control de sesión”[24].

5.1.1 Arquitectura IMS.

La arquitectura IMS se suele dividir en tres niveles o planos, el plano de medio/ transporte, el plano de control/señalización y el plano servicio/aplicación como se muestra en la siguiente figura.

Figura 3. Arquitectura de IMS por capas

[21] Ibíd., p. 9.
[22] CHANG, Kai-Di, et al. Challenges to Next Generation Services in IP Multimedia Subsystem. *Journal of Information Processing System [en línea]. 2010 p.129.*
[23] SAEED Mahdavi, MARYAM, Sabet y MOHAMM, Doostu. New Infrastructure of NGN and IMS Networks. *International Journal of Future Computer and Communication* [en línea]. 2016 p.134.
[24] Ibíd., p.134.



Fuente: CHANG, Kai -Di et al., Challenges to Next Generation Services in IP Multimedia Subsystem, *Journal of Information Processing System*, 2010, p. 130.

El primer plano, medios/transporte, hace uso de diversas tecnologías de acceso, en la cual los usuarios pasan por LAN inalámbrica, UMTS (Universal Telecommunication Systems) o GPRS (Servicio general de radio por paquetes) para obtener conectividad de red. En cuanto se logra la conexión se pasa al plano de control/señalización en el cual hay diversos componentes de IMS como Proxy-CSCF (P-CSCF), Interrogating-CSCF (I-CSCF) y Servir-CSCF (S-CSCF). La señalización trabaja bajo el protocolo de Session Initation Protocol (SIP) y se procesa y enruta al destino a través de este plano. Una vez se conecte y señalice a IMS, los usuarios podrían acceder a servicios multimedia a través del plano servicio/aplicación, en el cual se encuentran los servidores de aplicaciones generados y/o usados por los operadores [25].

5.2 ACUERDO DE AUTENTICACIÓN Y CLAVE INICIAL (AKA)

[25] CHANG, Kai -Di et al., Op. cit., p. 130.

La autenticación es una de las dimensiones de seguridad asociadas a IMS y a NGN. Así pues, con el fin de acceder a los servicios alojados en la capa IMS de la arquitectura de NGN, el Equipo del Usuario debe someterse a un procedimiento de autenticación de red y de capa IMS. A partir, de la autenticación en varias capas se puede aumentar la seguridad en el acceso a la red, y, por ende, reducir el riesgo de UE malintencionados[26].

A estos procedimientos se les conoce como protocolos de acuerdos de autenticación y clave inicial (AKA). Los AKA son uno de los protocolos de seguridad estándar para evitar los ataques a clientes de NGN[27], fue diseñado por el 3GPP (Proyecto Asociación de Tercera Generación) a finales del siglo XX, y tiene como objetivo autenticar un teléfono equipado con tarjeta USIM con redes y establecer claves para proteger posteriores comunicaciones[28].En este protocolo el termino autenticación implica la confirmación de la identidad del usuario y el acuerdo de clave corresponde a una serie de pasos en los que dos o más partes acuerdan una clave bajo un sistema de criptografía[29].

5.3 SEGURIDAD IMS

Con el IMS se abrió la posibilidad de hacer una incorporación de servicios de voz, datos o multimedia a través del protocolo IP. Entre las amenazas de seguridad para el sistema IMS se encuentra: “Acceso no autorizado a servicios. Molestar o hacer un mal uso de los servicios de red (lo que lleva a denegación de servicio o disponibilidad reducida). Acceso no autorizado a datos sensibles (violación de confidencialidad). Manipulación no autorizada de datos sensibles (violación de la integridad)[30]. Ante esto, la IMS tiene áreas de seguridad en: el acceso, el dominio de la red, en la operación y en el mantenimiento de la red. De esta manera se presentan cuatro asociantes de seguridad: con la primera se proporciona una autenticación mutua entre el usuario o equipo (UE) y la red principal de IMS en el subsistema (IM CN SS). El suscriptor del hogar (HSS) es el responsable de generar claves y desafíos mientras se realiza la autenticación fuera por la función de control de sesión de llamada de servicio (S-CSCF). Segundo, hay vínculo seguro mediante

[26] SHARMA, Madhu y LEUNG, Victor, IP Multimedia subsystem authentication protocol in LTE-heterogeneous networks, *Human-centric Computing and Information Sciences* [en línea]. 2012, p. 2.
[27] FOUQUE, Pierre, ONETE, Cristina, y RICHARD, Benjamin, Achieving Better Privacy for the 3GPP AKA Protocol, *Proceedings on Privacy Enhancing Technologies* [en línea]. 2016, p. 255-57.
[28] BORGAONKAR,Ravishankar et al., New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols., *Proceedings on Privacy Enhancing Technologies* [en línea]. 2019, p. 108.
[29] ZHANG, Fangguo, LIU, Shengli, y KIM, Kwangjo, ID-Based One Round Authenticated Tripartite Key Agreement Protocol with Pairings, *International Research center for Information Security* [en línea]. 2002, p. 1-2.
[30] PRISELAC, Dubravko y MIKUC, Miljenko. Security risks of pre-IMS AKA access security solutions. [En línea]. p.4

la intervención del el Proxy CSCF (P-CSCF)[31]. Tercero, proporciona seguridad dentro del dominio de la red internamente para la interfaz *Customer experience* (Cx)[32] Continuando, la cuarta asociación de seguridad hace referencia a al protocolo de inicio de sesiones (SIP) que actúa a la hora de crear. Modificar o cerrar sesiones entre uno o varios participantes.[33]

5.4 SEGURIDAD AKA

A diferencia del protocolo bipartita denominado Intercambio de claves autenticado (AKE, por sus siglas en inglés), el protocolo AKA, requiere de tres participantes para llevar a cabo la autenticación. Dichos participantes son los clientes móviles, el servidor y el operados. El cliente móvil puede subscribirse a servicios dispuestos por operadores, no obstante, el canal por el cual se proporciona el servicio es de una red local intermedia conocida como servidor. Para algunos tipos de servicios, en su mayoría de alcance doméstico, el servidor y el operados están asociados, y las claves de autenticación pueden ser conocidas por ambos (Tabla 1). Por su parte, en servicios en los cuales el servidor está asociado a un operador diferente los valores secretos de largo plazo están a disposición exclusivamente del cliente y del operador[34].

Con esto en mente, el esquema general del protocolo AKA se fundamenta en claves simétricas de largo plazo. En esta, los clientes están asociados con una clave única y una clave del operador, además, para evitar la duplicidad de claves se almacena un valor derivado de ambas claves denotado como *Top c*[35]. Entre los requerimientos del protocolo AKA se encuentran garantizar la entrega de servicios, garantizar la privacidad del cliente, entendida como la confidencialidad de identidad del usuario, la no rastreabilidad y la confidencialidad de ubicación del usuario[36]. Con estos requerimientos se pretende que el protocolo AKA asegure un mínimo de privacidad del cliente.

---

[31] OSORIO MOLINA, Luis Alonso y SUÁREZ DE AQUIZ, Luisa Edmme. Estado del Arte de IP multimedia subsystem (IMS). [En línea]. Trabajo de grado de especialización en ingeniería en telecomunicaciones. Universidad Pontificia Bolivariana. 2009. P.78.

[32] RODRIGUEZ QUIÑONES, Viviana. Mecanismo de seguridad para la arquitectura IMS basado en un modelo transversal usando técnicas de clave pública. Trabajo de Grado de maestría en ingeniería de Sistemas y Computación. [en línea]. Universidad de los Andes, 2010. [Consultado el 15 de diciembre de 2021]. Disponible en: https://repositorio.uniandes.edu.co/bitstream/handle/1992/11174/u402515.pdf?sequence=1

[33] RUIDIAZ VERA, Deider Enrique y BLANCO VIDAL, Cristian. Análisis del protocolo SIP para desarrollo de redes de nueva generación con aplicaciones de sistemas IP multimedia [en línea]. Tesis de Grado. Universidad Tecnológica de Bolívar. 2006. 96, p.

[34] FOUQUE, Pierre, ONETE, Cristina, y RICHARD, Benjamin, Achieving Better Privacy for the 3GPP AKA Protocol. *Proceedings on Privacy Enhancing Technologies* [en línea]. p. 255.

[35] Ibíd., p. 255.

[36] Ibíd., p. 256.

Otro requerimiento importante de este protocolo, por lo cual fue diseñado, es la garantía de seguridad ante usuarios, servidores o proveedores corruptos o malignos. Para el caso de servidores no afiliados con el proveedor este requerimiento es de gran importancia debido a que garantiza la seguridad en la transacción del servicio por medio del tercero. De esta manera, existen posibles problemas de seguridad asociados al servidor y, por ende, propiedades fundamentales del protocolo AKA, las cuales se pueden clasificar en dos, la primero, relacionado con la confidencialidad de estado, esto quiere decir que los servidores no pueden acceder a la clave secreta del cliente o del operador, ni acceder al estado del cliente. El segundo problema está relacionado con la solidez, de esta manera el servidor no puede ejecutar con éxito un protocolo de intercambio de claves con el cliente sin la intermediación del operador[37]. En la tabla descrita a continuación las siglas hacen referencia a Estación Móvil (MS), Estación Base del Controlador 1 (BSc1), Servidor Controlador de Red de Radio 1 (SRNC1), Registro de ubicación de visitantes (SGSN), Registro de Ubicación de Inicio (HLR) y servidor de autenticación (AuC) por sus siglas en inglés.

Tabla 1. Pasos generales de protocolo AKA (redes 3G)

Pasos	**Acciones**	**Descripción**
1	MS Inicio de sesión ↓ BSc1/ SRNC1	Etapa inicial, el mensaje incluye la estación móvil (MS), las preferencias de seguridad se envían a la Estación Base del Controlador (BSC) / Servidor Controlador de Red de Radio (SRNC)
2	BSc1 / SRNC1 ↓ SGSN 1 / VLR1	BSc1 consulta en el Nodo de Soporte GPRS el Registro de ubicación de visitantes (SGSN / VLR) y define si permite que MS se una o no.
3	SGSN 1/VLR1 ↓ HLR	VLR1 solicita al Registro de Ubicación de Inicio (HLR) un conjunto de parámetros de seguridad adjuntos a MS.
4	Ki HLR ↔ AuC *SV que se genera utilizando las funciones F1-F5	HLR obtiene la clave Ki del servidor de autenticación (AuC) y la usa junto con otros parámetros, para generar un vector de seguridad (SV) utilizando las funciones F1-F2
5	HLR SV ↓ VLR1/SGSN1	HLR envía SV al VLR1

[37] Ibíd., p. 257.

6	VLR1/SGSN1 RAND & ↓ AuTN MS	VLR1 / SGSN1 envía un valor aleatorio (RAND) y valor de autenticación (AuTN) a MS como prueba de verificación
7	Autenticación mutua entre la red y MS	MS compara los parámetros de SV regenerados para tener autenticación mutua
8	BSc1/ SRNC1 ↓ MS	BSC / SRNC devuelve una lista de integridad protegida de las preferencias de seguridad de MS

Fuente: Adaptado de RANA, Priya, Securing 4G networks with y-communication using AKA protocol, *International Journal of Computing and Business Research (IJCBR)*, 2011, p. 6-7

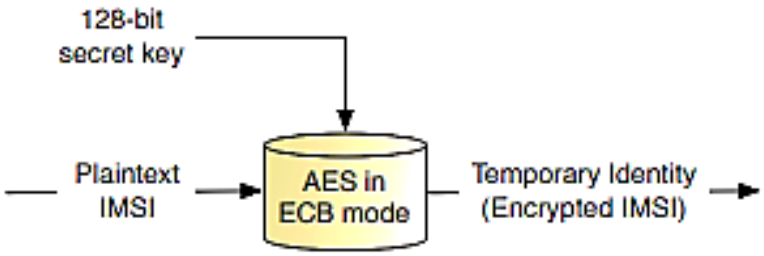
5.5 FORTALEZAS GENERALES DEL PROTOCOLO AKA

En la literatura se han reportado diversas fortalezas del protocolo AKA con respecto al protocolo AKE y otros protocolos de autenticación como el protocolo de identificación por radiofrecuencia (RFDI, por sus siglas en inglés) o el protocolo de identidad de host (HIP, por sus siglas en inglés). Entre las principales está la característica tripartita de este protocolo, lo que permite el uso de redes locales existentes para la prestación de un servicio[38].

Otra fortaleza es la seguridad de los algoritmos usados para el intercambio de claves y encriptación por claves de 128 bits en la cual se genera una identidad temporal que mantiene el anonimato del cliente[39], esta característica facilita el cumplimiento del requerimiento de confidencialidad, puesto que permite que las claves a largo plazo, tanto públicas como privadas, no se vean comprometidas si una de las claves es conocida.[40]

Figura 4. Generación de identidad temporal

[38] Ibíd., 255.
[39] HAN, Kyusuk y KIM, Kwangjo. 3G-WLAN interworking: Security analysis and new authentication and key agreement based on EAPAKA. *Conference: Wireless Telecommunications Symposium* [en línea] 2009, p.4.
[40] BIKOS, Anastasios y SKLAVOS, Nicolas, LTE/SAE Security Issues on 4G Wireless Networks, *Copublished by the IEEE Computer and Reliability Societies*, [en línea] 2013, p. 56.



Fuente: HAN, Kyusuk y KIM, Kwangjo, 3G-WLAN interworking: Security analysis and new authentication and key agreement based on EAPAKA, Wireless Telecommunications Symposium, Washington: WTS, 2009, p.4.

6. DIFERENTES MECANISMOS DE SEGURIDAD UTILIZADOS POR IMS-AKA PARA LA AUTENTICACIÓN Y CONTROL DE ACCESO EN LOS SERVICIOS BASADOS EN IP

Para el año 2009 se evidencia una tendencia hacia la implementación y las mejoras en el método de protocolo de autenticación extensible para la autenticación y acuerdo clave (EAP-AKA). Este método fue definido en el año 2006 en la RFC 4178, el documento expone que "EAP-AKA incluye soporte opcional de privacidad de identidad, resultado opcional indicaciones y un procedimiento opcional de autenticación rápida" [41]. Así pues, para el año 2009 se presenta una mejora al EAP-AKA denominada EAP-AKA', esto a través de la RFC 5448, en este documento se describe un cambio a la función de derivación de claves, con esto se facilita el uso de EAP de manera interoperable. La nueva función enlaza claves que derivan del método de red de acceso por nombre, para esto se define una encapsulación de EAP para AKA a través de radio 3GPP y otras bandas usadas en EAP-AKA[42].

En este documento también se encuentra soporte para evitar ataques a EAP-AKA y explica las diferencias en seguridad entre el EPA-AKA de la RFC 4178 y el EAP-AKA con las modificaciones de la RFC 5448. Entre las diferencias se mencionan un nuevo mecanismo para evitar la inseguridad en la negociación de métodos de EAP, Arkko et al. explican que para un ataque man-in-the-middle se pueden forzar los *endpoints* para reducir el método de seguridad, en el EAP-AKA' los puntos finales *endpoints* se comunican y manifiestan que desean usar EAP-AKA' sobre EAP-AKA fortaleciendo la seguridad de los mensajes, esta característica fortalece la negociación de cifrado para seleccionar la derivación de claves, esto permite que el cliente y el operador puedan negarse a cambios en *endpoints* que no solicitaron o iniciaron [43].

Durante el 2009 y 2010 se desarrolló un estudio en el que se evaluó el uso de criptografía de curva elíptica (ECC, por sus siglas en inglés) como alternativa de para reducir la sobrecarga computacional[44]. Dicho estudio pretendió mejorar la criptografía del protocolo AKA y aumentar la eficiencia y seguridad, esto teniendo en cuenta tres mejoras al protocolo AKA propuestas con anterioridad. La primera mejora fue propuesta por Sui, Ai-fen et al. en 2005, y consistía hacer uso del algoritmo simple de acuerdo de clave autenticada (SAKA) de Seo y Sweeney, que proporcionara autenticación de identidad, validación y secreto de clave. Este

[41] ERICSSON, Arkko y NOKIA, Haverinen, RFC 4187 - EAP-AKA Authentication», Request for Comments, *The Internet Society,* [en línea] 2006, p. 1.
[42] ARKKO, J, LEHTOVIRTA, V, ERICSSON, et al., RFC 5448 Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA'), *Network Working Group* [en línea], 2009, p. 1-3; p. 24, https://www.rfc-editor.org/rfc/pdfrfc/rfc5448.txt.pdf.
[43] ARKKO, J, LEHTOVIRTA, V, ERICSSON, et al., Op. cit., p. 15-17.
[44] LO, Jung et al., A SECURE AND EFFICIENT ECC-BASED AKA PROTOCOL FOR WIRELESS MOBILE COMMUNICATIONS, *International Journal of Innovative Computing, Information and Control*, [en línea] 2010, p. 1-2.

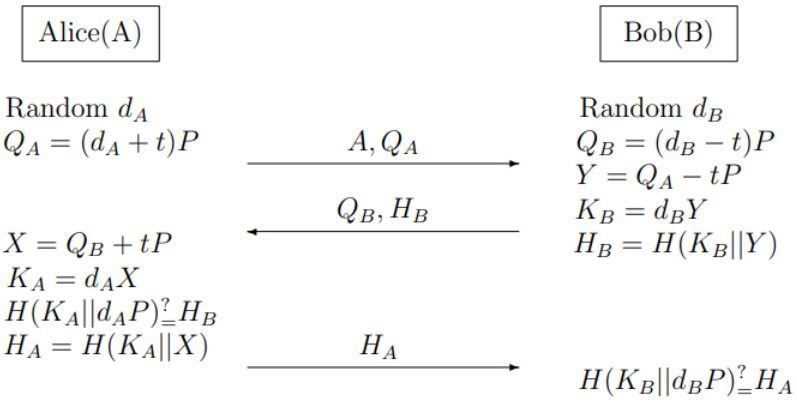
protocolo podía frustrar ataques tipo MITM y mejorar la distribución de la clave A (clave de autenticación), que es la clave maestra en las redes móviles IS-95 y cdma2000. Este protocolo redujo sobrecarga y almacenamiento, a la vez que aumento la seguridad del protocolo AKA propuesto en las especificaciones 3GPP2 [45], no obstante, este protocolo no resistió el ataque de adivinación de contraseña fuera de línea[46]. La segunda mejora fue propuesta por Lu, Cao, y Zhu, en el 2007 ellos reconocieron la limitación del protocolo de Sui, Ai-fen et al. y lo mejoraron a partir de la modificación en de la función hash en un solo sentido [47.] La tercera mejora fue propuesta por Chang, Chin-Chen y Chang, Shih-Chand en el 2008, buscaba responder a las fallas de los protocolos de Sui, Ai-fen et al y de Lu, Cao, y Zhu. Para esto, incluyeron una autenticación basada en la curva elíptica para redes móviles inalámbricas lo que presentó mejoras la seguridad del protocolo de distribución A-Key en 3GPP2[48].

Con esto en mente, Lo, Jung et al. modificaron criptografía de curva elíptica usada por Chang, Chin-Chen y Chang, Shih-Chand, con este esquema se logró resistir el ataque de adivinación de contraseña fuera de línea. La carga computacional es menor que la del esquema de Lu, Cao, y Zhu, porque ambos participantes calculan de manera individual una razón entre Q_A y Q_B. De manera similar, Lo, Jung et al. explican que este esquema no genera ninguna relación entre los mensajes transmitidos a través de la red, por lo cual el ataque de adivinanzas paralelas no tendría éxito. Además, solo se necesita un valor por parte del servidor, por lo que el almacenamiento utilizado también es menor que en los esquemas de Lu, Cao, y Zhu al. y el de Chang y Chang. Así pues, con este trabajo se consolida un protocolo más simple y con mejor seguridad y rendimiento para para entornos inalámbricos [49]. En la Figura 5, se muestra el diagrama del protocolo propuesto, donde Alice y Bob son dos usuarios intercambiando claves y se evidencian los pasos de verificación, intercambio, finalización o cancelación de protocolo. El proceso se da en 4 pasos a saber. “En el primer paso, Alice (A) selecciona un número aleatorio dA $\in$ [1, n−1] y calcula QA = (dA + t) P, donde t es un número entero predeterminado por la contraseña correspondiente y P es un punto en la curva elíptica. Entonces A envía su identidad A y QA a Bob (B). En el segundo paso, se repite la operación para Bob (B), quien también elige un número aleatorio dB $\in$ [1, n - 1] y luego calcula QB = (dB - t) P, Y = QA - tP, KB = dBY y HB = H (KB || Y). A continuación, B envía

[45] SUI, Ai-fen. et al., An improved authenticated key agreement protocol with perfect forward secrecy for wireless mobile communication, *2005 IEEE Wireless Communications and Networking Conference* [en línea], 2005, p. 2086.
[46] CHANG, Chin-Chen y CHANG, Shih-Chand, An improved authentication key agreement protocol based on elliptic curve for wireless mobile networks, *2008 International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, 2008, p. 1375; LU, Rongxing, CAO, Zhenfu, y ZHU, Haojin, An enhanced authenticated key agreement protocol for wireless mobile communication, *Computer Standards & Interfaces* [en línea], 2007, p. 647-48.
[47] LU, Rongxing, CAO, Zhenfu, y ZHU, Haojin, An enhanced authenticated key agreement protocol for wireless mobile communication, *Computer Standards & Interfaces* [en línea], 2007.
[48] Ibíd., p. 1376-78.
[49] LO, Jung et al., Op. cit, p. 7-9.

el QB y HB a A. En el cuarto y último paso, cuando B recibe el mensaje, comprueba la igualdad de H (KB || dBP) y HA. Solo si se mantiene la igualdad, B acepta la clave de sesión KB. De lo contrario, B termina el protocolo". [50]

Figura 5. Mejora en el protocolo AKA basado en trabajos previos e implementación de ECC



Fuente: LO, Jung et al., A secure and efficient ecc-based aka protocol for wireless mobile communications, International Journal of Innovative Computing, Information and Control, 2010, p. 4.

Para el 2011 se empezó a explorar la implementación de protocolos AKA en redes 4G, por ejemplo, en el trabajo de Rana se examina la posibilidad de utilizar mecanismos de seguridad 3G como AKA para sistemas 4G como Y-Comm. Así pues, se implementó un protocolo AKA y se evaluó el rendimiento del protocolo según los estándares X.805[51]. El estudio permitió concluir que los protocolos AKA para 3G no respondían a los restos de seguridad de las redes 4G, las cuales tenían exigencias mayores en seguridad. Consecuentemente, se concluyó que se requerían módulos integrados de seguridad y protocolos que protegieran a los diversos actores: usuarios, servidores y red [52].

En el mismo orden de ideas, Gu, Lili presenta en el 2011 un trabajo de investigación en el que realiza un protocolo AKA mejorado (IAKA) que vincula procedimientos de autenticación de dos capas a través de una identidad IP multimedia de usuario privado (IMPI)[53]. El proceso de autenticación por dos capas integra diversos sistemas IMS, de esta manera, cada suscriptor tiene dos identidades. La primera identidad está asociada a la capa de acceso, por ejemplo, un IMSI para red móvil

[50] Ibíd., p. 4
[51] RANA, Priya. Securing 4G networks with y-communication using aka protocol. IJCBR: *International Journal of Computing and Business Research* [en línea]. 2011. p. 4-8.
[52] Ibíd., p. 15.
[53] GU, Lili. Improved Internet Protocol Multimedia Subsystem Authentication for Long Term Evolution. [en línea]. Tesis de Grado de Maestría en Ingeniería. RMIT University, Australia. 2011., p. 3.

4G. La segunda identidad, es la capa de paquetes IP, por ejemplo, un número IMPI. El trabajo de Gu, Lili analiza el caso de las redes 4G LTE, el primer paso de autenticación se da en la capa LTE que permite al usuario acceder a la red al verificar el número IMSI, el segundo paso de autenticación verifica al usuario IMPI le permite acceder a la capa de servicios multimedia[54].

Teniendo en cuenta lo anterior, la mejora al protocolo AKA pretendía proporcionar un enlace seguro de la red y la autenticación de las capas de servicio mediante el uso del número IMPI que evita la doble ejecución de la autenticación protocolo AKA, Para esto, Gu, Lili propuso una jerarquía de claves de 4 capas que aumentaron el rendimiento del sistema, su seguridad y su ahorro de energía del terminal de consumo[55]. Como resultado de este trabajo se obtuvo un protocolo mejorado de un solo paso para redes 4G, por lo que se consideró en el año 2011 como una propuesta simplifica de los procedimientos de autenticación 4G LTE / IMS durante. En la Tabla 2, se evidencia la diferencia en los procesos y la reducción de pasos y de actores involucrados en el protocolo IAKA. En este caso, como se evidencia en la tabla con (IAKA) no es necesario: 1. La Solicitud de autenticación (S-CSCF-> HSS), 2. La respuesta de autenticación (HSS-> S-CSCF), 3. La verificación de AUTN y cálculo del número RES por UE, ni 5. La comparación de RES y XRES por S-CSCF.

Tabla 2. Comparación de entre procesos de autenticación en protocolo de una capa (IAKA) y protocolo de dos capas (3GPP).

IAKA	**3GPP**
Registro SIP (UE->P-CSCF)	Registro SIP (UE->P-CSCF, P-CSCF ->I-CSCF, I-CSCF->SCSCF)
-	Solicitud de autenticación (S-CSCF-> HSS)
Obtiene AV de MME (P-CSCF->MME, MME->P-CSCF)	Cálculo de AV por HSS
-	Respuesta de autenticación (HSS-> S-CSCF)
-	Almacenamiento de AV por S-CSCF
Respuesta SIP 401 NO AUTORIZADO (P-CSCF-> UE)	Respuesta SIP 401 NO AUTORIZADO (S-CSCF-> I-CSCF, I-CSCF-> PCSCF, P-CSCF-> UE)
-	Verificación de AUTN y cálculo del número RES por UE
Creación de IPSec SAs	Creación de IPSec SAs
-	Comparación de RES y XRES por S-CSCF

[54] Ibíd., p. 38.
[55] Ibíd., p. 50.

Solicitud de asignación de servidor / Respuesta (S-CSCF-> HSS, HSS-> SCSCF)	Solicitud de asignación de servidor / Respuesta (S-CSCF-> HSS, HSS-> SCSCF)
Respuesta de registro SIP 2000K (S-CSCF->I-CSCF, I-CSCF->PCSCF, P-CSCF->UE)	Respuesta de registro SIP 2000K (S-CSCF->I-CSCF, I-CSCF->PCSCF, P-CSCF->UE)

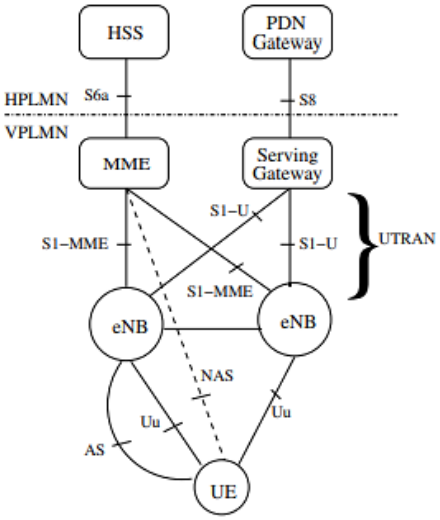
Fuente: Adaptado de Gu, Lili, Improved Internet Protocol Multimedia Subsystem Authentication for Long Term Evolution, RMIT UNIVERSITY, 2011, p. 54-55.

En el 2012 se introdujo un nuevo modelo para garantizar la interoperabilidad y privacidad en el protocolo AKA, este modelo se basó en el hecho de que el UE confiaría solo en la red doméstica (HN) con la que está registrado. La identidad internacional del suscriptor móvil (IMSI) no se compartiría con terceros y en ninguna situación la IMSI abandonaría el UE o HN. Este nuevo modelo remplaza el anterior, el cual contemplaba un intercambio entre el UE y la red de servicio (SN), donde la HN confía plenamente en la SN para presentar el servicio al UE suscrito, así pues, el IMSI se intercambia de manera constante entre la HN y la SN, lo anterior, generaba una relación de confianza resultado de dos relaciones de confianza anteriores, en la cual el UE debía confía completamente en la SN y transmitir su IMSI inmediatamente después de recibir una solicitud del SN[56].

De esta manera, con las mejoras propuestas por Choudhury, Roychoudhury, y Saikia, se evidencia la implementación del estándar avanzado de evolución a largo plazo (LTE-Advanced) propuesto por 3GPPen el año 2011. El LTE, todos los usuarios están registrados a una red móvil terrestre o HN del usuario, por lo cual, la información del perfil del usuario se almacena en un *Home Subscriber Server* (HSS). Con esto, un UE visitante se conecta a un nodo de control para la red de acceso LTE que debe ser autenticado por el HSS (Ver Figura 6) en la que se explica la nueva relación de confianza entre el equipo del usuario (UE) y la Red doméstica (HN) que al mismo tiempo es un resultado transitivo de la dos relaciones de confianza anteriores; por lo cual, la UE completamente confía al SN con su IMSI y transmite su IMSI inmediatamente después de recibir una solicitud del SN [57].

Figura 6. Arquitectura de seguridad de LTE

[56] CHOUDHURY, Hiten, ROYCHOUDHURY, Basav, y SAIKIA, Dilip, A New Trust Model for Improved Identity Privacy in Cellular Networks, *International Journal of Computer Applications*, [en línea], 2012, p. 1-3.
[57] Ibíd., p.3



Fuente: CHOUDHURY, Hiten, ROYCHOUDHURY, Basav, y SAIKIA, Dilip, A New Trust Model for Improved Identity Privacy in Cellular Networks, *International Journal of Computer Applications*, 2012, p. 2.

Durante el 2013 se evidenció, de manera explícita, el aporte y uso del protocolo AKA para garantizar la seguridad en la nube y en las transacciones de comercio electrónico. Como exponen Leu, Lin, y Castiglione los principales desafíos para estas aplicaciones correspondían a la verificación de integridad, autenticación, control de acceso, prevención de ataques, entre otros [58]. De esta manera, ellos consideraron que los enfoques de seguridad se debían centrar, principalmente, en técnicas de cifrado durante el intercambio de información entre dos entidades comunicadas. Los autores retoman elementos de trabajos anteriores como la autenticación rápida iterativa localizada o, Autenticación FIL, la cual reemplazó la autenticación rápida del protocolo EAP-AKA[59]. La autenticación FIL hace uso de un proceso iterativo y un proceso de autenticación localizado, lo que permite que se aceleren los tiempos de autenticación y se disminuyan los tiempos de autenticación durante la transferencia. Otro elemento recuperado en este trabajo es la arquitectura *firewall,* esta posee características adaptativas y escalables que generó reglas y políticas para la detección de actividad de tráfico inusual[60]. En resumen, la arquitectura *firewall* está compuesta por una estructura modular de múltiples capas e incluye al menos un módulo IO encargado de la funcionalidad del *firewall*, un módulo de procesamiento encargado de la seguridad y un controlador de *firewall* que administra los módulos anteriores; para el procesamiento de información, el modulo IO recibe un paquete de datos el cual se identifica en el módulo de seguridad con el fin de verificar si la sesión está asociada al paquete de datos, luego esto se

[58] LEU, Fang-Yie., LIN, Chu-Hsing, y CASTIGLIONE, Aniello, Special issue on cloud, wireless and e-commerce security, *Journal of Ambient Intelligence and Humanized Computing*, [en línea].2013, p. 207-208.
[59] Ibíd., p. 207.
[60] Ibíd., p. 207.

transmite e identifica para prestar el servicio al UE [61]. Así pues, se logra aplicar esto a entornos de información distribuida como la nube y no se requiere de paquetes específicos de hardware y/o software[62].

Como tercer elemento, Leu, Lin, y Castiglione proponen el uso de *Machine Learning* (ML) y *Soft Computing* (SC) para garantizar seguridad en tecnologías de información y comunicación (TIC). Las principales aplicaciones corresponden a la contraseña para el control de acceso, la detección de intrusos y el filtrado de spam. El ML y SC permiten que un sistema cambie sus respuestas de seguridad ante entradas dinámicas y reales[63], por lo cual, permite dar respuesta a nuevas formas de ataques y aprende de estos lo que aumenta la eficacia de los protocolos AKA. Con respecto a este tema, se exploró la modificación de protocolos para que trabajen en condiciones adversas y, así, se mejoren los algoritmos de seguridad y de aprendizaje. Por último, Leu, Lin, y Castiglion abordan el esquema de firma proxy parcialmente ciego, el cual resuelve algunos problemas de la autenticación FIL, por ejemplo, disminuye la posibilidad de revocación de privilegios proxy y la autenticación de firmas anteriores que podría generar un rastreo de las firmas y UE. También, el esquema de firma proxy parcialmente ciego cumple con los requisitos de seguridad de las firmas proxy ciegas, como imposibilidad de ser olvidadas[64].

Entre el 2013 y 2014, también se desarrollaron mejoras al protocolo AKA enfocados en los estándares y protocolos UMTS. Caragata et al., proponen dos modificaciones al protocolo AKA. La primera modificación consiste en cambiar la clave TK, de tal manera que esta sea diferente para cada conjunto AV generado por un HE determinado, así, "[este] valor se establecerá durante el protocolo CIP utilizando una función de seguridad ya implementada en USIM, con la función 3 (F3). TK tendrá una longitud de 128 bits y se usará exactamente como la clave K se usa actualmente en el procedimiento AKA" [65]. Por su parte, la segunda modificación se relaciona con la protección de los mensajes durante la ejecución del protocolo AKA, así, se cambia el orden del paso de verificación con las claves de cifrado e integridad, CK e IK. El protocolo AKA tradicional efectúa este paso al principio del intercambio del mensaje, por lo que Caragata et al, proponen hacer este paso al final y con esto se esperaría que se redujeran la cantidad de mensajes desprotegidos[66]. En conclusión, trabajos como el de Caragata, buscaron realizar modificaciones teniendo en cuenta las limitaciones y fortalezas de los protocolos UMTS-AKA para esos años, en la **¡Error! No se encuentra el origen de la referencia.**, se evidencian los protocolos existentes para UMTS en el año 2014, y

[61] CHOUNG-YAW, Michael, Distributed firewall architecture using virtual machines, United States Patent Shieh US 8,612,744 B2, Palo Alto, enviado el 16 de agosto de 2012, y aprobado el 17 de diciembre de 2013, p. 1-3.
[62] LEU, Fang-Yie, LIN, Chu-Hsing, y CASTIGLIONE, Aniello, Op. cit., p. 207.
[63] Ibíd., p. 207-208.
[64] Ibíd., p. 208.
[65] CARAGATA, Daniel *et al.,* Confidential initial identification and other improvements for UMTS security, *Security Comm. Networks*, [en línea].2014,p. 562.
[66] Ibíd., 562.

las características en cuanto a seguridad. Donde, EAKAP es Autenticación Extendida y Protocolo de Acuerdo Clave, AKA, Autenticación y Acuerdo clave; AP - AKA, Protocolo Adaptativo - AKA; S - AKA, protocolo seguro AKA; X - AKA, extensión de AKA.

En el 2016 el grupo 3GPP eligió el EPS-AKA como el procedimiento de autenticación para usuarios de redes móviles. El estándar EPS (Evolved Packet System), es el resultado de la combinación entre la evolución a largo plazo red (LTE) y red de System Architecture Evolution (SAE) en la que el LTE desempeña el papel del acceso red y el SAE el papel de red central. [67] Para el 2017, 3GPP presentó un informe con la evolución del EPS donde especifica las características de seguridad y los mecanismos de seguridad de este estándar, en este incluye la descripción de dos versiones mejoradas: *Evolved Packet Core* (EPC) y el *Evolved-UTRAN* (E-UTRAN)[68].

En estudios previos, el mecanismo de autenticación EPS-AKA fue vulnerable a varios tipos de ataques pasivos y activos de manera que, Abdeljebbar y Kouch, buscaron mejoras en el proceso de protección en la comunicación entre el UE y los otros elementos de la red. De su estudio se encontraron las sugerencias que se listan a continuación[69]:

1. Proteger la comunicación entre entidades involucradas en el procedimiento de autenticación con criptografía asimétrica.
2. Mantener oculta la identidad del UE (IMSI) al servidor.
3. Usar un parámetro secreto denominado parámetro de validación del usuario (UVP), para la autenticación de UE por el HSS. Con esto, se protegería al UE de suplantación.
4. Implementar dos nuevos parámetros secretos, llamados parámetro de validación de red de servicio (SVP) y parámetro de validación de red doméstica (HVP). El SVP se utiliza para autenticar el Mobility Management Entity (MME) por el HSS local mientras que el HVP es utilizado para autenticar el HSS por el MME del servidor, con esto, los nuevos parámetros vinculan la red doméstica con la red de servicios.

Otras modificaciones de interés para el protocolo AKA se han desarrollado en el marco de la comunicación máquina a máquina (M2M) y del Internet de las cosas (IoT), estas aplicaciones han generado un ecosistema en el cual gran variedad de

[67] ABDELJEBBAR, Mourad y KOUCH, Rachid, Security Improvements of EPS-AKA Protocol, *International Journal of Network Security*, [en línea].2018, p. 636.
[68] FOUQUE, Pierre., ONETE, Cristina y RICHARD, Benjamin. Op.cit., p.9
[69] ABDELJEBBAR, Mourad y KOUCH, Rachid, Security Improvements of EPS-AKA Protocol, Op. cit,. p. 638.

objetos puede comunicarse entre sí. Bajo este panorama existen diferentes desafíos de seguridad entre los que se encuentran la seguridad en la comunicación y la privacidad de los usuarios. Los protocolos AKA han jugado un papel importante en la resolución de estos desafíos. Así pues, ellos proponen un nuevo nivel de seguridad del protocolo de autenticación que satisface los requisitos de seguridad al proporcionar protección contra varios ataques, reduciendo el consumo de ancho de banda mediante la optimización de los mensajes de autenticación y asegurando una comunicación eficiente entre varios dispositivos IoT [70].

[70] OUAISSA, Mariya., RHATTOY, Abdallah, y CHANA, Idriss. New Security Level of Authentication and Key Agreement Protocol for the IoT on LTE Mobile Networks. WINCOM: *International Conference on Wireless Networks and Mobile Communications* [en línea], 2019.

7. ERRORES O FALLOS DE AUTENTICACIÓN Y CONTROL DE ACCESO RELACIONADOS CON LA CONFIGURACIÓN DE SEGURIDAD IMS-AKA

Entre las debilidades de los protocolos AKA, OU et al. exponen "el consumo de ancho de banda, la sobrecarga de espacio y la sincronización del número de secuencia" [71]. Bikos y Sklavos argumentan que la dimensión de integridad solo se presenta para canales de señalización dejando propenso el estrato de servicios a la modificación, eliminación, creación y/o replicación de los datos [72].

También se han evidenciado vulnerabilidades a la seguridad del cliente, esto por medio de ataques IMSI-catcher, ataques de paginación IMSI y suplantación por corrupción de servidor [73.] Este tipo de ataques se relacionan al hecho de que los clientes deben enviar su identificador permanente IMSI para llevar a cabo la ejecución del protocolo, así facilita el rastreo de ubicaciones por parte de servidores no confiables. Otros problemas de vulnerabilidad reportados en la literatura son los ataques DoS, por ejemplo, se puede presentar la inundación de frecuencias de radio con solicitudes falsas de conexión inalámbrica [74.]

El uso de criptografía de curva elíptica (ECC, por sus siglas en inglés) y del algoritmo simple de acuerdo de clave autenticada (SAKA) de Seo y Sweeney, que proporcionara autenticación de identidad, validación y secreto de clave no resistió el ataque de adivinación de contraseña fuera de línea[75]. La modificación en de la función hash en un solo sentido que proponen Lu, Cao, y Zhu, no pudo resistir los ataques de adivinanzas paralelas de claves[76]. La inclusión de una autenticación basada en la curva elíptica para redes móviles inalámbricas que propuso Chang, Chin-Chen y Chang, Shih-Chand no resolvió a cabalidad los problemas de seguridad presentes en los protocolos anteriores[77].

Con la implementación de los protocolos AKA en 4G se evaluaron mediante los estándares X.805. se hallaron ocho vulnerabilidades de seguridad entre las que se encontraban el control de acceso, la seguridad en la comunicación, autenticación, la integridad de los datos, el no rechazo, la disponibilidad del servicio, la privacidad y la confidencialidad [78].

De manera que, hasta este punto se puede hacer una comparación de los protocolos de seguridad para UMTS y, en estos, establecer los errores o fallos de

---

[71] OU, Hsia et al., TK-AKA: using temporary key on Authentication and Key Agreement protocol on UMTS, *International Journal of Network Management* [en línea], 2008, p.1.
[72] BIKOS, Anastasios y SKLAVOS, Nicolas, Op. cit., p. 59.
[73] CRAMER, Ronald y SHOUP, Victor. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. Lecture Notes in Computer Science [en línea]. Springer (Berlin), 2006, p. 2.
[74] BIKOS, Anastasios y SKLAVOS, Nicolas, Op. cit., p. 58.
[75] CHANG, Chin-Chen y CHANG, Shih-Chand, Op. cit., p. 48.
[76] Ibíd., p.78.
[77] LU, Rongxing, CAO, Zhenfu, y ZHU, Haojin, Op. cit., p. 1376-78.
[78] RANA, Priya, Op. cit, p. 7-9.

autenticación y control de acceso relacionados con la configuración de seguridad IMS-AKA que, como se puede observar en la tabla 3 presentan fallos en Protección de identidad, Integridad del mensaje y Debilidad ante ataques específicos.

Tabla 3. Comparación de protocolos de seguridad para UMTS

Protocolo	**Protección de identidad**	**Integridad del mensaje**	**Aumento de la sobrecarga computacional en MS**	**Aumento de la sobrecarga computacional en SN**	**Aumento de la sobrecarga computacional en HE**	**Debilidad ante ataques específicos**
Caragata el al.	Sí	Sí	Sí	No	Sí	No
UMTS	No	No	-	-	-	Sí
EAKAP	No	Sí	Sí	Sí	Sí	No
AP-AKA	No	No	No	Sí	No	Sí
S-AKA	No	Sí	No	No	No	Sí
Coctel AKA	No	No	Sí	Sí	No	Sí
X-AKA	No	Sí	No	Sí	No	Sí

Fuente: Adaptado de CARAGATA, Daniel et al., Confidential initial identification and other improvements for UMTS security, *Security Comm. Networks*, 2014, p. 564.[79]

También se puede afirmar que EPS-AKA fue vulnerable a varios tipos de ataques pasivos y activos, como avance de la privacidad, ataques de denegación de servicio y algunos ataques de IP [80]. También en el marco de la comunicación máquina a máquina (M2M) y del Internet de las cosas (IoT) los protocolos AKA como explican Ouaissa, Rhattoy, y Chana, el protocolo estándar de EP-AKA no admite elementos IoT y genera algunos problemas, incluyendo vulnerabilidades de ataque de seguridad y sobrecarga de tráfico debido al mensaje de control. [81].

[79] CARAGATA, Daniel, ASSAD, Safwan, SHONIREGUN, Charles, y AKMAYEVA, Galyna. Confidential initial identification and other improvements for UMTS security, *Security Comm. Networks* [en línea], 2014. p. 564

[80] ABDELJEBBAR, Mourad y KOUCH, Rachid, Op. cit, p. 638.

[81] OUAISSA, Mariya, RHATTOY, Abdallah, y CHANA, Idriss, op. cit, p.1.

8. PROCEDIMIENTOS DE CONFIGURACIÓN DE LA ASOCIACIÓN DE SEGURIDAD QUE INFLUYEN EN LA EFECTIVIDAD COMO MECANISMO DE PROTECCIÓN DE INTEGRIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN EN LOS SERVICIOS BASADOS EN IP

Como se ha mencionado en los anteriores capítulos, la apertura de la arquitectura de IMS con el fin de facilitar el acceso a la red y el uso del protocolo de inicio de sesión (SIP) aumenta la vulnerabilidad a los ataques por inundación de SIP, este se presenta como uno de los problemas de seguridad en las NGN[82]. Otras amenazas a la seguridad de IMS son la denegación del servicio, el spam, acceso no autorizado a la red, ataques a la red de núcleo, entre otros. Esta vulnerabilidad inherente al proceso de apertura implica retos en seguridad informática en el momento de implementar y ampliar la cobertura de NGN[83].

Ahora bien, como se observa (ver figura 7) en la arquitectura IMS hay cuatro capas, la primera va desde la capa de servicio hasta el servidor de las aplicaciones, la segunda, hace referencia a una capa de control que en cuatro pasos verifica el núcleo del IMS, en la tercera capa se verifica el trasporte en IPV4 o IPV6 y, en la cuarta y última capa se abre la capa de acceso desde alguna línea inalámbrica. Estas cuatro capas en conjunto buscan proporcionar una mayor confiabilidad en el servicio.

Figura 7 IMS Arquitectura en Capas.

[82] DOUST, Noorallah y JAHROMI, Mansour, Detecting Flooding Attacks on IMS Networks Using Kullback-Leibler Divergence and Triple EWMA., *Journal of Electrical Engineering Science* [en línea], 2017, p. 29-31.
[83] MOHAPATRA, Sumant, SWAIN, Biswa, y DAS, Pravanjan, Comprehensive survey of possible security issues on 4G networks, *International Journal of Network Security & Its Applications (IJNSA)* [en línea], 2015, p. 66.

Fuente: OMAR, Mohammed, KIPRUTO, Cheruiyot, y KIMWELE, Michael, Securing The IP Multimedia Subsystem with IPsec and HTTP Digest, *International Journal of Computer,* 2017, p.118.

Ahora bien, una definición tradicional la seguridad de la red comprende la integridad, la confidencialidad y la disponibilidad. La integridad del mensaje asegura que si una parte no autorizada modifica un mensaje entre el remitente y el receptor, el receptor puede detectar esta modificación. Además de la integridad del mensaje, los mecanismos de integridad siempre proporcionar algún tipo de prueba del origen de los datos.[84]

Sumado a esta definición tradicional, Shuang et al. exponen que hay seis dimensiones asociadas a la seguridad en IMS. Primero, se encuentra la **autenticación** en esta la IMS proporciona autenticación bidireccional entre usuarios y operadores. Así, la IMS previene obtención de permisos por usuarios ilegales y verificación o posibilidad de autenticación desde el usuario. La segunda dimensión corresponde a la **integridad** de los datos, en este caso los datos se protegen de cualquier modificación, eliminación, creación y/o replicación de los datos por parte de usuarios no autorizados. En tercer lugar, está el **no rechazo**, esta dimensión permite a operadores prevenir que un individuo o entidad niegue una acción realizada, esta característica, es de utilidad en servicios como la facturación electrónica, en los cuales se puede saber los pasos realizados por un usuario garantizando la confiabilidad y precisión de las acciones. [85].

Continuando, la cuarta dimensión corresponde a la **confidencialidad** que hace referencia a divulgar información de manera exclusiva a los usuarios autorizados e impedir que usuarios no autorizados accedan a dicha información. En quinto lugar, se encuentra la **disponibilidad**, la cual garantiza el acceso a los elementos de la red para los usuarios autorizados, esto implica que haya un correcto almacenaje, flujo y recuperación de datos. Por último, está la **autorización** que permite estimar si las solicitudes de los usuarios son acordes al perfil del usuario y la política del operador [86]

Por lo general, la confidencialidad se logra mediante el cifrado. Los ataques de denegación de servicio (DoS) comprometen la disponibilidad del sistema al impedir que los usuarios autorizados accedan a un servicio en particular. El DoS más común consiste en mantener ocupados a los servidores realizando una operación o

[84] OMAR, Mohammed, KIPRUTO, Cheruiyot, y KIMWELE, Michael, Securing the IP Multimedia Subsystem with IPsec and HTTP Digest, *International Journal of Computer* [en línea]*,* 2017, p.118.
[85] SHUANG, Kai, et al. IMS Security Analysis using Multi-attribute Model. *Journal of netw*orks [en línea]. 2011, p. 265.
[86] Ibíd., p.266.

enviando a los servidores más tráfico del que puede manejar[87]. IMS define una arquitectura y un marco completos que permiten la convergencia de tecnologías de voz, video, datos y redes móviles a través de una infraestructura basada en IP llenando el vacío entre dos paradigmas exitosos de comunicación, tecnología celular e internet. Sin embargo, las soluciones actuales, como firewalls, software anti-espía y los sistemas antivirus no han podido del todo contrarrestar las amenazas emergentes porque solo apuntan a tipos específicos de amenazas. [88]

Las principales amenazas que afectan la integridad y la confidencialidad de la información en mayor mediada son: escuchas a escondidas, secuestro de registros, suplantación de identidad del servidor, manipulación del cuerpo del mensaje, eliminación de sesiones, negación de servicio y amplificación. Desde este panorama de riesgo, entre los procedimientos de configuración de la asociación de seguridad que influyen en la efectividad como mecanismo de protección de integridad y confidencialidad de la información en los servicios basados en IP está el de modelar la arquitectura de red IMS con: Puerta de enlace de seguridad (SEG), El Traductor de direcciones de red (y puerto) (NA (P) T-PT), trabajo de interconexión de IPv4 / IPv6. Actualmente, los mecanismos de seguridad de IMS utilizan TLS7 o IPsec8 para proporcionar autenticación, integridad y confidencialidad. El TLS proporciona privacidad en las comunicaciones a través de la red IP y permite que las aplicaciones cliente / servidor comunicarse de forma segura contra ataques de escuchas clandestinas, manipulación o falsificación de mensajes.[89]

Con lo anterior en mente se puede decir que AKA tiene, entre otras, una protección de trafico con IPsec, el protocolo UDP y el protocolo TCP. Para esto se requiere que todo el tráfico entre el equipo de usuario (EU por sus sigas en inglés) y un P-CSCF durante una sesión se envíe a canales específicos protegidos por IPsec. En este procedimiento AKA utiliza la interfaz IMS (protocolo SIP) para la comunicación entre un UE y un P-CSCF. Ambos lados tienen un puerto de cliente y un puerto de servidor. Las configuraciones de seguridad (claves, etc.) se almacenan en asociaciones de seguridad (SA) y se identifican mediante índices de parámetros de seguridad (SPI). La interfaz IMS admite dos protocolos de transporte alternativos TCP y UDP. Los canales protegidos por IPsec se utilizan de forma diferente según el protocolo de transporte utilizado. De manera que AKA proporciona autenticación mutua de UE y el sistema IMS de servicio.

[87] CAMARILLO, Gonzalo, y GARCIA, Miguel. The 3G IP Multimedia Subsystem (IMS) Merging the Internet and the cellular worlds. *Chichester, England: John Wiley & Sons* [en línea]*,* 2006, p. 215.
[88] OMAR, Mohammed, KIPRUTO, Cheruiyot, y KIMWELE, Michael op. cit, p.119.
[89] Ibíd., p.124.

9. CONCLUSIONES

El objetivo que se cumple con esta monografía consistió en hacer un análisis de la efectividad de la autenticación y control de acceso IMS-AKA como mecanismo de protección de integridad y confidencialidad de la información en los servicios basados en IP. Lo anterior se cumplió debido a que se desarrolló una revisión detallada del tema en bases de datos, plataformas y repositorios institucionales donde se almacenan revistas y periódicos especializados en el área como la *Computer and Reliability Societies*, el *Journal of Information Processing System, el Journal of Electrical Engineering Science, el Journal of Information Security, International Journal of Network Security & Its Applications.* Como se puede observar la mayoría de las bases y plataformas consultadas son el idioma inglés, sin embargo, también se consultaron repositorios universitarios como el de la Universidad de los Andes, la Universidad, Universidad Pontificia Bolivariana, entre otras.

Ahora bien, para cumplir con este objetivo general, en primer lugar, hizo un recorrido teórico y conceptual sobre definiciones relacionadas con Redes de nueva generación (NGN), sus características y su arquitectura en la que se identificó principalmente que estas se dividen en dos planos o estratos principales relacionados con el trasporte y el servicio. Se encontró que hay tres tipos de redes: *User Network Interface* (UNI), *Network Network Interface* (NNI) y *Application Network Interface* (ANI). Durante esta primera revisión de conceptos también se describieron conceptos relacionados con el Subsistema Multimedia IP (IMS) y como este puede usarse para gestionar problemas asociados con el servicio, como la calidad del servicio (QoS), la carga, el control de acceso, la gestión de usuarios y servicios, se describió la Arquitectura IMS y sus tres niveles o planos, y la definición del Acuerdo de Autenticación y Clave Inicial (AKA) que es conocida como un protocolo que busca evitar ataques y, en general, los problemas de seguridad emergentes en el IMS.

Con relación al cumplimiento de los cuatro objetivos específicos que se proponían desarrollar, en un primer momento, se identificó y se describió la arquitectura IMS-AKA y sus características de seguridad para el acceso seguro. De esta manera se identificó que el protocolo AKA requiere de los clientes móviles, el servidor y el operados para llevar a cabo su autenticación. El esquema general del protocolo AKA se fundamenta en claves simétricas de largo plazo que garantizan la confidencialidad de identidad del usuario, la no rastreabilidad y la confidencialidad de ubicación.

En un segundo momento se describieron los diferentes mecanismos de seguridad utilizados por IMS-AKA para la autenticación y control de acceso en los servicios basados en IP. Lo anterior se hace a través de una revisión histórica del protocolo que abarcó una revisión desde el año 2010 hasta el año 2019. En un tercer momento se listaron los errores o fallos de autenticación y control de acceso relacionados con la configuración de seguridad IMS-AKA donde de evidencio que EPS-AKA fue vulnerable a varios tipos de ataques pasivos y activos, como avance de la privacidad, ataques de denegación de servicio y algunos ataques de IP.

Por último, el cuarto objetivo específico se cumple en la medida en que se describieron las seis dimensiones asociadas a la seguridad en IMS, asimismo las principales amenazas que afectan la integridad y la confidencialidad de la información y los procedimientos de configuración de la asociación de seguridad que influyen en la efectividad como mecanismo de protección de integridad y confidencialidad de la información en los servicios basados en IP.

Con esta monografía se logró identificar que hay aspectos de seguridad informática cuyo tratamiento se encuentra en constante evolución. Lo anterior, sobre todo cuando se habla de redes de nueva generación debido a su característica de estar bajo la manipulación de múltiples operadores que coexisten y administran de manera conjunta la red central, situación que hace que sean más vulnerables y que lleva a que se abran cada día nuevos retos en materia de seguridad.

Finalmente, a modo de recomendación, se espera a futuro describir los procedimientos de configuración más en detalle teniendo en cuenta aspectos comparativos entre estos.

BIBLIOGRAFÍA

ABDELJEBBAR, Mourad y KOUCH, Rachid. Security Improvements of EPS-AKA Protocol. IJNS: *International Journal of Network Security* [en línea]. 2018, julio, 20(4).636-644. [Consultado el 15 de diciembre de 2021]. Disponible en: 10.6633/IJNS.201807 20(4).05)

ALASH, Mahdi., MAPP, Glenford y LASEBAE. A survey on authentication and key agreement protocols in heterogeneous networks. IJNSA: *International Journal of Network Security & Its Applications* [en línea]. 2012, agosto. (4)4. 199-214. [Consultado el 15 de diciembre de 2021]. Disponible en: https://www.researchgate.net/publication/230577649_A_Survey_on_Authentication_and_Key_Agreement_Protocols_in_Heterogeneous_Networks

APARICIO BAQUEN, Christian Camilo. Resiliencia en la plataforma MTC aplicada a smartcities [en línea]. Trabajo de Pregrado. Universidad de los Andes, Bogotá, 2013. [Consultado el 22 de noviembre, 2021]. Disponible en: https://repositorio.uniandes.edu.co/handle/1992/19804

ARKKO, Jari., LEHTOVIRTA, Vesa y ERICSSON, Pasi. RFC 5448 Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA'). *Network Working Group* [en línea]. 2009, mayo. [Consultado el 15 de diciembre de 2021]. Disponible en: https://datatracker.ietf.org/doc/rfc5448/

BARRAGÁN DEL POZO, Edgar Edison. Análisis de la tecnología IMS (IP Multimedia Subsystem) y diseñar un servicio de transmisión multimedia de video mediante Open IMS core para evaluar el tráfico unicast y multicast [en línea]. Tesis de Maestría. Escuela Superior Politécnica de Chimborazo, 2019. [Consultado el 15 de diciembre de 2021]. Disponible en: http://dspace.espoch.edu.ec/handle/123456789/12991

BIKOS, Anastasios, y SKLAVOS, Nicolas. LTE/SAE Security Issues on 4G Wireless Networks. *Copublished by the IEEE Computer and Reliability Societies* [en línea]. Patras (Grecia) 2013, marzo - abril. [Consultado el 15 de diciembre de 2021]. ISSN 1540-7993/55-62. 1540-7993/13. Disponible en: https://www.academia.edu/55175454/LTE_SAE_Security_Issues_on_4G_Wireless_Networks

BORGAONKAR, Ravishankar, *et al.* New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols. *Proceedings on Privacy Enhancing Technologies* [en línea]. Berlín (Alemania), 2019. [Consultado el 15 de diciembre de 2021]. Disponible en: https://eprint.iacr.org/2018/1175.pdf

CARAGATA, Daniel, *et al.* Confidential initial identification and other improvements for UMTS security. *Security Comm. Networks* [en línea]. 2014, marzo, 7(3).636-644. [Consultado el 15 de diciembre de 2021]. ISSN 1939-0122. Disponible en: https://www.researchgate.net/publication/260409399_Confidential_initial_identification_and_other_improvements_for_UMTS_security

CASTILLO, Carlos., SALCEDO, Octavio y FORERO, Felipe. New Generation Networks: a Networking Trend. *Journal of Technology* [en línea]. 2014, abril, 13(1). 45-54. [Consultado el 15 de diciembre de 2021]. Disponible en: https://dialnet.unirioja.es/descarga/articulo/6041576.pdf

CHANG, Chin-Chen, y CHANG, Shih-Chand. An improved authentication key agreement protocol based on elliptic curve for wireless mobile networks. *International Conference on Intelligent Information Hiding and Multimedia Signal Processing* [en línea]. 2008, agosto 18(6). 1433–1440. [Consultado el 15 de diciembre de 2021]. Disponible en: 10.1016/j.cnsns.2012.09.032

CHANG, Kai-Di, *et al.* Challenges to Next Generation Services in IP Multimedia Subsystem. *Journal of Information Processing System* [en línea]. 2010, junio.6(2). 129-146. [Consultado el 15 de diciembre de 2021]. Disponible en: http://bbcr.uwaterloo.ca/~xshen/paper/2013/saasae.pdf

CHENGZHE, Lai, *et al*. SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks. *Computer Networks* [en línea]. 2013, enero. 5. 3492-3510. [Consultado el 15 de diciembre de 2021]. Disponible en: https://doi.org/10.1016/j.comnet.2013.08.003.

CHOUDHURY, Hiten., ROYCHOUDHURY, Basav, y SAIKIA, Dilip. A New Trust Model for Improved Identity Privacy in Cellular Networks. *International Journal of Computer Applications* [en línea]. 2012, octubre. 56.(14).1-8. [Consultado el 15 de diciembre de 2021]. Disponible en: https://www.researchgate.net/publication/258652782_A_New_Trust_Model_for_Improved_Identity_Privacy_in_Cellular_Networks

CHOUNG-YAW, Michael. CHOUNG-YAW, Michael, Distributed firewall architecture using virtual machines, United States Patent Shieh US 8,612,744 B2, Palo Alto, enviado el 16 de agosto de 2012, y aprobado el 17 de diciembre de 2013 [en línea] 2013, agosto. [Consultado el 15 de diciembre de 2021]. Disponible en: https://scienceon.kisti.re.kr/srch/selectPORSrchPatent.do?cn=USP2013128612744

CRAMER, Ronald y SHOUP, Victor. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack. *Lecture Notes in Computer Science* [en línea]. Springer (Berlin), 2006 mayo. 1462. 13-25. [Consultado el 15 de

diciembre de 2021]. Disponible en: https://link.springer.com/chapter/10.1007%2FBFb0055717#citeas

CAMARILLO, Gonzalo y GARCIA, Miguel. The 3G IP Multimedia Subsystem (IMS). Merging the Internet and the cellular worlds. Chichester, England: John Wiley & Sons, 2006. (Edición Kindle). ISBN-13: 978-0470516621

DEVI, Sri, y MOHANKUMAR, M. An Empirical Study on Cyber Security Threats and Attacks. *International Journal of Scientific Research and Review* [en línea]. 2019. [Consultado el 15 de diciembre de 2021]. Disponible en: https://www.semanticscholar.org/paper/AN-EMPIRICAL-STUDY-ON-CYBER-SECURITY-THREATS-AND-Devi Mohankumar/3f197fcc0bd775fc2e970a71139736e606e1ec5b

DIAZ BOHÓRQUEZ, Anyel Carolina. Propuesta de política pública para la gestión de los residuos electrónicos generados por la transición hacia NGN en Colombia [en línea]. Trabajo de Grado Maestría. Universidad Nacional de Colombia, 2015. [Consultado el 15 de diciembre de 2021]. Disponible en: https://repositorio.unal.edu.co/handle/unal/54798

DOMÍNGUEZ CANG, Nayibis. Arquitectura orientada al servicio de Redes de Nueva Generación (NGN) [en línea]. Trabajo de grado, electrónica y telecomunicaciones. Universidad Central Marta Abre U De las Villas, 2007. [Consultado el 15 de diciembre de 2021]. Disponible en: http://dspace.uclv.edu.cu:8089/handle/123456789/5458

DOUST, Noorallah y JAHROMI, Mansour. Detecting Flooding Attacks on IMS Networks Using Kullback-Leibler Divergence and Triple EWMA. *Journal of Electrical Engineering Science* [en línea]. 2017, diciembre. 1. 29-41. [Consultado el 15 de diciembre de 2021]. ISSN:2008-9864. Disponible en: https://www.researchgate.net/publication/322420191_Detecting_Flooding_Attacks_on_IMS_Networks_Using_Kullback-Leibler_Divergence_and_Triple_EWMA

ERICSSON, Arkko, y NOKIA, Haverinen. RFC 4187 - EAP-AKA Authentication». Request for Comments. *The Internet Society* [en línea]. 2006, enero. [Consultado el 15 de diciembre de 2021]. Disponible en: https://datatracker.ietf.org/doc/html/rfc4187

FORERO, Felipe., CASTILLO, Carlos y SALCEDO, Octavio. New Generation Networks: a Networking Trend. *Journal of Technology* [en línea]. 2014, abril, 13(1). 45-54. [Consultado el 15 de diciembre de 2021]. Disponible en: https://dialnet.unirioja.es/descarga/articulo/6041576.pdf

FOUQUE, Pierre., ONETE, Cristina y RICHARD, Benjamin. Achieving Better Privacy for the 3GPP AKA Protocol. *Proceedings on Privacy Enhancing Technologies* [en línea]. 2016, enero.4.1-43. [Consultado el 15 de diciembre de 2021]. Disponible en: https://eprint.iacr.org/2016/480.pdf

GANDOTRA, Ekta., BANSAL, Divya, y SOFAT, Sanjeev. Malware Analysis and Classification: A Survey. *Journal of Information Security* [en línea]. 2014, enero. 05(02). 56-64. [Consultado el 15 de diciembre de 2021]. Disponible en: https://www.researchgate.net/publication/276495476_Malware_Analysis_and_Classification_A_Survey

GU, Lili. Improved Internet Protocol Multimedia Subsystem Authentication for Long Term Evolution. [en línea]. Tesis de Grado de Maestría en Ingeniería. RMIT University, Australia. 2011. [Consultado el 15 de diciembre de 2021]. Disponible en: https://core.ac.uk/download/pdf/15624505.pdf

HAN, Kyusuk y KIM, Kwangjo. 3G-WLAN interworking: Security analysis and new authentication and key agreement based on EAPAKA. *Conference: Wireless Telecommunications Symposium* [en línea] 1-9. 2009, mayo. [Consultado el 15 de diciembre de 2021]. Disponible en: https://www.researchgate.net/publication/224503036_3G-WLAN_interworking_Security_analysis_and_new_authentication_and_key_agreement_based_on_EAPAKA

HUI, Lucas *et al*. An improved authenticated key agreement protocol with perfect forward secrecy for wireless mobile communication. *IEEE Wireless Communications and Networking Conference,* [en línea], 2005, marzo. 4.2088-2093. [Consultado el 15 de diciembre de 2021]. Disponible en: 10.1109/WCNC.2005.1424840.

KHAN, Mohammed, y MITCHELL, Chris. Another Look at Privacy Threats in 3G Mobile Telephony. *Proceedings of ACISP* [en línea] 2014, julio. vol. 8544. [Consultado el 15 de diciembre de 2021]. Disponible en: https://www.researchgate.net/publication/224503036_3G-WLAN_interworking_Security_analysis_and_new_authentication_and_key_agreement_based_on_EAPAKA

KOUICEM, Djamel., BOUABDALLAH, Abdelmadjid y LAKHLEF, Hicham. Internet of things security: A top-down survey. *Computer Networks* [en línea]. 2018, marzo. 141. [Consultado el 15 de diciembre de 2021]. Disponible en: 10.1016/j.comnet.2018.03.012

LEU, Fang-Yie., LIN, Chu-Hsing, y CASTIGLIONE, Aniello. Special issue on cloud, wireless and e-commerce security. *Journal of Ambient Intelligence and Humanized*

Computing [en línea]. 2013. 4(2). [Consultado el 15 de diciembre de 2021]. Disponible en: https://dblp.uni-trier.de/db/journals/jaihc/jaihc4.html#LeuLC13

LO, Jung, LEE, Cheng-chi, HWANG, Min-shiang, y Chu, yen-ping. A secure and efficient ecc-based AKA protocol for wireless mobile communications. *International Journal of Innovative Computing, Information and Control* [en línea]. 2010, noviembre. 6.(11). 5249-5258. [Consultado el 15 de diciembre de 2021]. Disponible en: https://www.researchgate.net/publication/288138383_A_secure_and_efficient_ecc-based_AKA_protocol_for_wireless_mobile_communications

LU, Rongxing., CAO, Zhenfu, y ZHU, Haojin. An enhanced authenticated key agreement protocol for wireless mobile communication. *Computer Standards y Interfaces* [en línea]. 2007. Vol.29. 647-652. [Consultado el 15 de diciembre de 2021]. Disponible en: https://www.sciencedirect.com/science/article/abs/pii/S0920548907000311

MAHDI, Glenford. A survey on authentication and key agreement protocols in heterogeneous networks. IJNSA: *International Journal of Network Security & Its Applications* [en línea]. 2012, agosto. (4)4. 199-214. [Consultado el 15 de diciembre de 2021]. Disponible en: https://www.researchgate.net/publiction/230577649_A_Survey_on_Authentication_and_Key_Agreement_Protocols_in_Heterogeneous_Net

MOHAPATRA, Sumant., SWAIN, Biswa, y DAS, Pravanjan. Comprehensive survey of possible security issues on 4G networks. IJNSA: *International Journal of Network Security & Its Applications* [en línea]. 2015, marzo. 7(2):61-69. [Consultado el 15 de diciembre de 2021]. Disponible en: https://www.researchgate.net/publication/275224084_Comprehensive_Survey_of_Possible_Security_Issues_on_4G_Networks#:~:text=Worms%2C%20viruses%2C%20calls%20and%20spam,%5B3%5D%20.%20...

MORITA, Naotaka y IMANAKA, Hideo. Introduction to the Functional Architecture of NGN. *IEICE TRANSACTIONS on Communications* [en línea]. 2007, mayo. [Consultado el 15 de diciembre de 2021]. ISSN: 1745-1345. Disponible en: https://search.ieice.org/bin/summary.php?id=e90-b_5_1022

NEETESH, Saxena, JAYA, Thomas, y NARENDRA, Chaudhari. ES-AKA: An Efficient and Secure Authentication and Key Agreement Protocol for UMTS Networks. *Wireless Personal Communications* [en línea]. 2015, abril. 84(3):1981-2012. [Consultado el 15 de diciembre de 2021]. Disponible en: https://www.researchgate.net/publication/275214535_ES-AKA_An_Efficient_and_Secure_Authentication_and_Key_Agreement_Protocol_for_UMTS_Networks

OMAR, Mohammed., KIPRUTO, Cheruiyot, y KIMWELE, Michael. Securing the IP Multimedia Subsystem with IPsec and HTTP Digest. *International Journal of Computer* [en línea]. 2017, julio. 26(1), 117-128. [Consultado el 15 de diciembre de 2021]. Disponible en: https://ijcjournal.org/index.php/InternationalJournalOfComputer/article/view/1025

OU, Hsia., LIN, Ioun, HWANG, Min, y JAN, Jinn. TK-AKA: using temporary key on Authentication and Key Agreement protocol on UMTS. *International Journal of Network Management* [en línea]. 2009, julio. 19(4):291-303. [Consultado el 15 de diciembre de 2021]. Disponible en: https://www.researchgate.net/publication/220675963_TK-AKA_using_temporary_key_on_Authentication_and_Key_Agreement_protocol_on_UMTS

OUAISSA, Mariya., RHATTOY, Abdallah, y CHANA, Idriss. New Security Level of Authentication and Key Agreement Protocol for the IoT on LTE Mobile Networks. WINCOM: *International Conference on Wireless Networks and Mobile Communications* [en línea], 2019, octubre. [Consultado el 15 de diciembre de 2021]. Disponible en: https://ieeexplore.ieee.org/document/8629767

OSORIO MOLINA, Luis Alonso y SUÁREZ DE AQUIZ, Luisa Edmme. Estado del Arte de IP multimedia subsystem (IMS). [En línea]. Trabajo de grado de especialización en ingeniería en telecomunicaciones. Universidad Pontificia Bolivariana. 2009. [Consultado el 15 de diciembre de 2021]. Disponible en: https://repository.upb.edu.co/bitstream/handle/20.500.11912/696/digital_17333.pdf?sequence=1

PRISELAC, Dubravko y MIKUC, Miljenko. Security risks of pre-IMS AKA access security solutions. *Faculty of Electrical Engineering and Computing* [en línea]. 1-4 [Consultado el 15 de diciembre de 2021]. Disponible en: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.518.7914&rep=rep1&type=pdf

RANA, Priya. Securing 4G networks with y-communication using aka protocol. IJCBR: *International Journal of Computing and Business Research* [en línea]. 2011.Vol. 2. ISSN: 2229-6166. [Consultado el 15 de diciembre de 2021]. Disponible en: http://www.researchmanuscripts.com/PapersVol2N1Jan2011/8.pdf

RODRIGUEZ QUIÑONES, Viviana. Mecanismo de seguridad para la arquitectura IMS basado en un modelo transversal usando técnicas de clave pública. Trabajo de Grado de maestría en ingeniería de Sistemas y Computación. [en línea]. Universidad de los Andes, 2010. [Consultado el 15 de diciembre de 2021]. Disponible en:

https://repositorio.uniandes.edu.co/bitstream/handle/1992/11174/u402515.pdf?sequence=1

RUIDIAZ VERA, Deider Enrique y BLANCO VIDAL, Cristian. Análisis del protocolo SIP para desarrollo de redes de nueva generación con aplicaciones de sistemas IP multimedia [en línea]. Tesis de Grado. Universidad Tecnológica de Bolívar. 2006. [Consultado el 15 de diciembre de 2021]. Disponible en: https://biblioteca.utb.edu.co/notas/tesis/0036603.pdf

SAEED Mahdavi, MARYAM, Sabet y MOHAMM, Doostu. New Infrastructure of NGN and IMS Networks. *International Journal of Future Computer and Communication* [en línea]. 2016, enero. 5(3):134-141 [Consultado el 15 de diciembre de 2021]. Disponible en: https://www.researchgate.net/publication/304338631_New_Infrastructure_of_NGN_and_IMS_Networks

SHARMA, Madhu y LEUNG, Victor. IP Multimedia subsystem authentication protocol in LTE-heterogeneous networks. *Human-centric Computing and Information Sciences* [en línea]. 2012, octubre. 1(16). [Consultado el 15 de diciembre de 2021]. Disponible en: https://hcis-journal.springeropen.com/articles/10.1186/2192-1962-2-16

SHUANG, Kai, *et al.* IMS Security Analysis using Multi-attribute Model. *Journal of networks* [en línea]. 2011, enero. Vol. 6. 263-271. [Consultado el 15 de diciembre de 2021]. Disponible en:https://www.semanticscholar.org/paper/IMS-Security-Analysis-using-Multi-attribute-Model-Shuang-Wang/35d4afcdfbe2c8788e30e0e2f42be1e9381cc9a9

SUI, Ai-fen, *et al*. An improved authenticated key agreement protocol with perfect forward secrecy for wireless mobile communication. *IEEE Wireless Communications and Networking Conference* [en línea], 2005, marzo. 4.2088-2093. [Consultado el 15 de diciembre de 2021]. Disponible en: 10.1109/WCNC.2005.1424840.

UNIÓN INTERNACIONAL DE TELECOMUNICACIONES. [Sitio web]. Ginebra: UIT-T. Serie y: infraestructura mundial de la información, aspectos del protocolo internet y redes de la próxima generación Redes de la próxima generación – Marcos y modelos arquitecturales funcionales. [Consultado el 15 de diciembre de 2021]. Disponible en: Disponible en: https://www.itu.int/rec/T-REC-Y/es

ZHANG, Fangguo., LIU, Shengli, y KIM, Kwangjo. ID-Based One Round Authenticated Tripartite Key Agreement Protocol with Pairings. *International Research center for Information Security* [en línea], 2002, enero. 1-13. [Consultado el 15 de diciembre de 2021]. Disponible en: https://www.researchgate.net/publication/220336035_ID-

Based_One_Round_Authenticated_Tripartite_Key_Agreement_Protocol_with_Pairings