Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

Y.2760

(05/2011)

SERIE Y: INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN, ASPECTOS DEL PROTOCOLO INTERNET Y REDES DE LA PRÓXIMA GENERACIÓN

Redes de la próxima generación – Seguridad

Marco de seguridad para la movilidad en las NGN

Recomendación UIT-T Y.2760

Unión Internacional de Telecomunicaciones

RECOMENDACIONES UIT-T DE LA SERIE Y

INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN, ASPECTOS DEL PROTOCOLO INTERNET Y REDES DE LA PRÓXIMA GENERACIÓN

INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN	
Generalidades	Y.100–Y.199
Servicios, aplicaciones y programas intermedios	Y.200–Y.299
Aspectos de red	Y.300–Y.399
Interfaces y protocolos	Y.400–Y.499
Numeración, direccionamiento y denominación	Y.500–Y.599
Operaciones, administración y mantenimiento	Y.600–Y.699
Seguridad	Y.700–Y.799
Características	Y.800–Y.899
ASPECTOS DEL PROTOCOLO INTERNET	
Generalidades	Y.1000–Y.1099
Servicios y aplicaciones	Y.1100–Y.1199
Arquitectura, acceso, capacidades de red y gestión de recursos	Y.1200–Y.1299
Transporte	Y.1300–Y.1399
Interfuncionamiento	Y.1400–Y.1499
Calidad de servicio y características de red	Y.1500–Y.1599
Señalización	Y.1600–Y.1699
Operaciones, administración y mantenimiento	Y.1700–Y.1799
Tasación	Y.1800–Y.1899
Televisión IP sobre redes de próxima generación	Y.1900–Y.1999
REDES DE LA PRÓXIMA GENERACIÓN	
Marcos y modelos arquitecturales funcionales	Y.2000–Y.2099
Calidad de servicio y calidad de funcionamiento	Y.2100–Y.2199
Aspectos relativos a los servicios: capacidades y arquitectura de servicios	Y.2200–Y.2249
Aspectos relativos a los servicios: interoperabilidad de servicios y redes en las redes de la próxima generación	Y.2250–Y.2299
Numeración, denominación y direccionamiento	Y.2300–Y.2399
Gestión de red	Y.2400–Y.2499
Arquitecturas y protocolos de control de red	Y.2500–Y.2599
Redes basadas en paquetes	Y.2600–Y.2699
Seguridad	**Y.2700–Y.2799**
Movilidad generalizada	Y.2800–Y.2899
Entorno abierto con calidad de operador	Y.2900–Y.2999
REDES FUTURAS	Y.3000–Y.3499
COMPUTACIÓN EN LA NUBE	Y.3500–Y.3999

Para más información, véase la Lista de Recomendaciones del UIT-T.

Recomendación UIT-T Y.2760

Marco de seguridad para la movilidad en las NGN

Resumen

En la presente Recomendación se especifica el marco de seguridad para la movilidad en el estrato de transporte de las NGN. Se abordan los requisitos de seguridad, los mecanismos de seguridad y los procedimientos de gestión y control de la movilidad en las NGN.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio
1.0	ITU-T Y.2760	2011-05-20	13

Palabras clave

NGN, seguridad de la movilidad.

PREFACIO

La Unión Internacional de Telecomunicaciones (UIT) es el organismo especializado de las Naciones Unidas en el campo de las telecomunicaciones y de las tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es un órgano permanente de la UIT. Este órgano estudia los aspectos técnicos, de explotación y tarifarios y publica Recomendaciones sobre los mismos, con miras a la normalización de las telecomunicaciones en el plano mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), que se celebra cada cuatro años, establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen Recomendaciones sobre dichos temas.

La aprobación de Recomendaciones por los Miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 de la AMNT.

En ciertos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, se preparan las normas necesarias en colaboración con la ISO y la CEI.

NOTA

En esta Recomendación, la expresión "Administración" se utiliza para designar, en forma abreviada, tanto una administración de telecomunicaciones como una empresa de explotación reconocida de telecomunicaciones.

La observancia de esta Recomendación es voluntaria. Ahora bien, la Recomendación puede contener ciertas disposiciones obligatorias (para asegurar, por ejemplo, la aplicabilidad o la interoperabilidad), por lo que la observancia se consigue con el cumplimiento exacto y puntual de todas las disposiciones obligatorias. La obligatoriedad de un elemento preceptivo o requisito se expresa mediante las frases "tener que, haber de, hay que + infinitivo" o el verbo principal en tiempo futuro simple de mandato, en modo afirmativo o negativo. El hecho de que se utilice esta formulación no entraña que la observancia se imponga a ninguna de las partes.

PROPIEDAD INTELECTUAL

La UIT señala a la atención la posibilidad de que la utilización o aplicación de la presente Recomendación suponga el empleo de un derecho de propiedad intelectual reivindicado. La UIT no adopta ninguna posición en cuanto a la demostración, validez o aplicabilidad de los derechos de propiedad intelectual reivindicados, ya sea por los miembros de la UIT o por terceros ajenos al proceso de elaboración de Recomendaciones.

En la fecha de aprobación de la presente Recomendación, la UIT no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Página

Recomendación UIT-T Y.2760

Marco de seguridad para la movilidad en las NGN

1 Alcance

En esta Recomendación se describe el marco de seguridad para la movilidad en el estrato de transporte de las redes de la próxima generación (NGN). Se tienen en cuenta los requisitos de seguridad de [UIT-T Y.2018]. En la presente Recomendación se abordan la autentificación y la gestión de claves, el establecimiento del contexto de seguridad, la seguridad de la movilidad IP, y la seguridad de la gestión, el control y el transporte de movilidad en el estrato de transporte. Además, se presentan casos de movilidad entre distintas tecnologías y entre tecnologías idénticas, y dentro de un mismo dominio o entre dominios distintos.

2 Referencias

Las siguientes Recomendaciones UIT-T y demás referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de esta Recomendación. A la fecha de esta publicación, las ediciones citadas están en vigor. Todas las Recomendaciones y demás referencias están sujetas a revisión, por lo que se alienta a los usuarios a que estudien la posibilidad de utilizar la edición más reciente de las Recomendaciones y demás referencias que se indican a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente en vigor. En la presente Recomendación, la referencia a un documento no confiere a este último, como documento autónomo, la categoría de una Recomendación.

[UIT-T Q.1706] Recomendación ITU-T Q.1706/Y.2801 (2006), *Requisitos de gestión de movilidad para las redes de próxima generación*.

[ITU-T X.805] Recomendación UIT-T X.805 (2003), *Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo*.

[ITU-T Y.2011] Recomendación UIT-T Y.2011 (2004), *Principios generales y modelo de referencia general de las redes de próxima generación*.

[UIT-T Y.2012] Recomendación UIT-T Y.2012 (2010), *Requisitos y arquitectura funcional de las redes de la próxima generación*.

[UIT-T Y.2014] Recomendación UIT-T Y.2014 (2010), *Funciones de control de conexión de red en las redes de próxima generación*.

[UIT-T Y.2018] Recomendación UIT-T Y.2018 (2009), *Marco y arquitectura de gestión y de control de la movilidad en la capa de transporte de las redes NGN*.

[UIT-T Y.2701] Recomendación UIT-T Y.2701 (2007), *Requisitos de seguridad para las redes de la próxima generación, versión 1*.

[UIT-T Y.2704] Recomendación UIT-T Y.2704 (2010), *Mecanismos y procedimientos de seguridad en las redes de próxima generación*.

[UIT-T Y-Sup.7] Recomendaciones de la Serie Y del UIT-T– *Suplemento 7 (2008), Serie Y.2000 del UIT-T – Suplemento sobre el alcance de las NGN versión 2*.

[UIT-R M.1645] Recomendación UIT-R M.1645 (2003), *Marco y objetivos generales del desarrollo futuro de las IMT-2000 y de los sistemas posteriores*.

3 Definiciones

3.1 Términos definidos en otras Recomendaciones

En la presente Recomendación se utilizan los siguientes términos ya definidos en otras Recomendaciones:

3.1.1 traspaso (cláusula 6.2.2 de [UIT-T Q.1706)]: La capacidad de ofrecer los servicios con alguna repercusión en los acuerdos de nivel de servicio para un objeto en movimiento y que se ha desplazado.

3.1.2 movilidad horizontal (cláusula 6.2.3 de [UIT-T Q.1706]): Movilidad sobre la misma capa, conforme a la definición de [UIT-R M.1645]. En general se trata de la movilidad dentro de la misma tecnología de acceso.

3.13 movilidad (cláusula 3.2 de [UIT-T Q.1706]): La posibilidad que tiene el usuario u otra entidad del servicio móvil de comunicar y acceder a los servicios independientemente de la posición y del entorno técnico.

3.1.4 estrato de transporte NGN [(cláusula 3.10 de [UIT-T Y.2011]): Parte de la NGN que proporciona las funciones de usuario que transfieren datos y las funciones que controlan y gestionan los recursos de transporte que transportan dichos datos entre entidades terminales.

3.1.5 confianza (cláusula 3.2.9 de [UIT-T Y.2701)]: Se dice que la entidad X confía en la entidad Y para la realización de un conjunto de actividades única y exclusivamente si la entidad X confía en que la entidad Y se va a comportar de una manera concreta con respecto a dichas actividades.

3.1.6 movilidad vertical (cláusula 6.2.3 de [UIT-T Q.1706]): Movilidad entre dos capas diferentes, conforme a la definición de [UIT-R M.1645]. En general se trata de la movilidad entre distintas tecnologías de acceso.

3.2 Términos definidos en esta Recomendación

En la presente Recomendación se definen los siguientes términos:

3.2.1 movilidad intertecnológica: Véase "Movilidad vertical" en la cláusula 3.1.

3.2.2 movilidad intratecnológica: Véase "Movilidad horizontal" en la cláusula 3.1.

3.2.3 contexto de seguridad: Conjunto de parámetros de seguridad, incluidos los identificadores, las claves, los algoritmos de clave, etc.

4 Abreviaturas y acrónimos

En esta Recomendación se utilizan las abreviaturas y acrónimos siguientes:

3G	3ª generación (*3rd generation*)
ABG-FE	Entidad funcional de pasarela de frontera de acceso (*access border gateway functional entity*)
AE	Extensión de autentificación (*authentication extension*)
AKA	Acuerdo de autentificación y claves (*authentication and key agreement*)
AM-FE	Entidad funcional de gestión de acceso (*access management functional entity*)
AN-FE	Entidad funcional de nodo de acceso (*access node functional entity*)
ANI	Interfaz aplicación-red (*application to network interface*)
AR-FE	Entidad funcional de retransmisión de acceso (*access relay functional entity*)

DDoS	Denegación de servicio distribuida (*distributed deny of service*)
EAP	Protocolo de autentificación extensible (*extensible authentication protocol*)
EN-FE	Entidad funcional de nodo extremo (*edge node functional entity*)
FA	Agente visitado (*foreign agent*)
HA	Agente propio (*home agent*)
HDC-FE	Entidad funcional de control de decisión de traspaso (*handover decision control functional entity*)
IP	Protocolo Internet (*Internet protocol*)
L3HEF	Función de ejecución de traspaso de capa 3 (*layer 3 handover execution function)*
MIP	IP móvil (*mobile IP*)
MIPv4	IP móvil para IP versión 4. Véase [b-IETF RFC 3220]
MIPv6	IP móvil para IP versión 6. Véase [b-IETF RFC 3775]
MLM-FE	Entidad funcional de gestión de ubicación móvil (*mobile location management functional entity*)
MMCF	Funciones de control de gestión de movilidad (*mobility management control functions*)
MN	Nodo móvil (*mobile node*)
MOBIKE	Protocolo de multidireccionamiento y movilidad IKEv2 (*IKEv2 mobility and multihoming protocol*). Véase [b-IETF RFC 4555]
NACF	Funciones de control de anexión a la red (*network attachment control functions*)
NGN	Red de la próxima generación (*next generation network*)
NID-FE	Entidad funcional de distribución de información en la red (*network information distribution functional entity*)
NNI	Interfaz red-red (*network to network interface*)
PKI	Infraestructura de clave pública (*public key infrastructure*)
PMIPv6	Intermediario móvil IPv6 (*proxy mobile IPv6*). Véase [b-IETF RFC 5213]
RAN	Red de acceso radioeléctrico (*radio access network*)
RRP	Respuesta de registro (*registration reply*)
RRQ	Petición de registro (*registration request*)
TAA-FE	Entidad funcional de autorización y autentificación de transporte (*transport authentication and authorization functional entity*)
TLM-FE	Entidad funcional de gestión de ubicación de transporte (*transport location management functional entity*)
TLS	Seguridad de capa de transporte (*transport layer security*)
TTLS	Seguridad de capa de transporte tunelizada (*tunnelled transport layer security)*
TUP-FE	Entidad funcional de perfil de usuario de transporte (*transport user profile functional entity*)
UE	Equipo de usuario (*user equipment*)

UNI Interfaz usuario-red (*user to network interface*)

WiMax Interoperabilidad mundial para acceso por microondas (*worldwide interoperability for microwave access*)

WLAN LAN inalámbrica (*wireless LAN*)

5 Requisitos de seguridad para la movilidad en las NGN

Las NGN soportan múltiples tecnologías de acceso, como WLAN, WiMax, y 3G RAN, etc. [UIT-T Y.2012]. El soporte de la movilidad es una de las características de las NGN, que comprende el nomadismo y el traspaso. En las NGN versión 2, el traspaso puede darse entre redes de acceso o dentro de una misma red de acceso [UIT-T Y-Sup.7].

Las NGN tienen las siguientes características:

1) Modelo de confianza: el modelo de confianza de seguridad de las NGN define tres zonas de seguridad: fiable, fiable pero vulnerable y no fiable [UIT-T Y.2701]. Según este modelo la red de acceso ha de pasar por una pasarela de seguridad antes de acceder a la red dorsal.

2) Las NGN soportan múltiples tecnologías de acceso.

3) Las NGN soportan diversos protocolos de movilidad, como MIPv4, MIPv6, DSMIPv6, PMIPv6 y MOBIKE.

4) Las NGN soportan equipos de usuario con múltiples tecnologías radioeléctricas, como WLAN, WiMax, 3G RAN etc.

5) Las NGN soportan la continuidad del servicio cuando se realiza un traspaso entre sistemas de acceso heterogéneos.

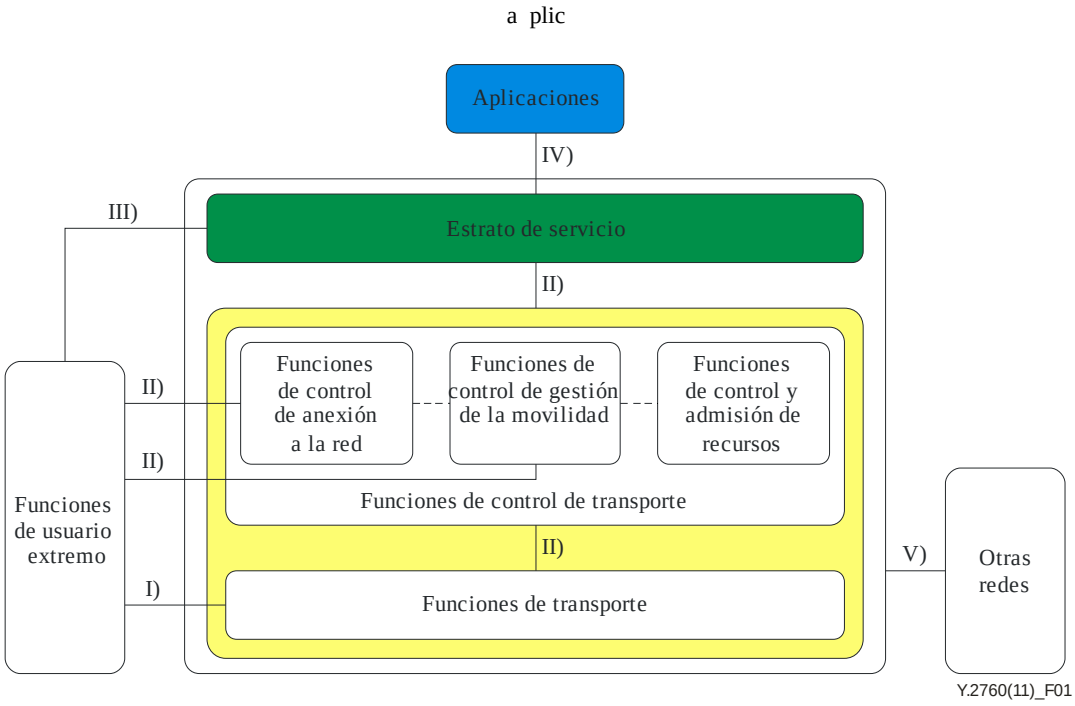

Figura 1 – Arquitectura de seguridad de la movilidad en las NGN

Se definen cinco ámbitos de seguridad para:

I) centrarse en la seguridad en la capa de transporte entre las funciones de usuario extremo y las funciones de transporte, como la seguridad de acceso, que pueden estar física o lógicamente protegidas entre las funciones de usuario extremo y la entidad de red de acceso en las funciones de transporte. I) también atañe a la seguridad de la UNI entre las funciones de usuario extremo y las funciones de transporte.

II) centrarse en la seguridad en la capa de control entre funciones de usuario extremo y la entidad funcional de control de transporte. II) también se centra en la seguridad en la interfaz de mensaje de control entre la entidad funcional de transporte y la entidad funcional de control de transporte. II) atañe a la seguridad de la UNI entre las funciones de usuario extremo y las funciones de control de transporte.

III) centrarse en la seguridad de la interfaz entre funciones de usuario extremo y el estrato de servicio. III) también se centra en la seguridad de la interfaz de mensaje de control entre la entidad funcional de control de transporte y el estrato de servicio. III) atañe a la seguridad de la UNI entre las funciones de usuario extremo y el estrato de servicio.

IV) Está centrado en la seguridad de la interfaz entre el estrado de servicio y la entidad de aplicación. IV) atañe a la seguridad de la ANI entre las funciones de usuario extremo y las funciones de transporte.

V) Está centrado en la seguridad de la interfaz entre las NGN y otras redes, lo que incluye tanto la capa de transporte como la capa de control. V) atañe a la seguridad de la NNI entre la red NGN y otras redes.

Los principios definidos en [UIT-T X.805] son aplicables a las amenazas y requisitos de seguridad identificados en esta Recomendación.

5.1 Amenazas de seguridad

En [UIT-T Y.2018] se identifican las siguientes amenazas de seguridad:

T1 El UE puede no estar autorizado a iniciar la señalización de movilidad con la MLM-FE.

T2 Intrusos pueden manipular la señalización de movilidad.

T3 Puede usurparse la MLM-FE para facilitar información falsa al UE.

T4 Intrusos pueden tener conocimiento de la ubicación del UE.

T5 Puede haber un ataque de redireccionamiento del tráfico.

T6 Puede haber un ataque en el trayecto o un ataque por intermediario.

T7 Un ataque DDoS puede consumir una gran cantidad de recursos de red.

T8 El UE puede no estar autorizado a obtener información de la HDC-FE o la NID-FE.

T9 Se pueden usurpar la HDC-FE o la NID-FE para introducir información falsa en el UE.

T10 Puede modificarse o espiarse la señalización entre el UE y la HDC-FE o la NID-FE.

T11 Se pueden modificar o espiar los datos del plano de usuario.

5.2 Requisitos de seguridad

En [UIT-T Y.2018] se identifican los siguientes requisitos de seguridad:

R1 El UE y la NID-FE han de estar mutuamente autentificados.

R2 La señalización entre el UE y la MLM-FE ha de tener protección de integridad y confidencialidad.

R3 La señalización entre el UE y la MLM-FE ha de estar protegida contra los ataques de reproducción.

R4 Se ha de garantizar la privacidad de la ubicación del UE.

R5 El UE y la HDC-FE han de estar mutuamente autentificados.

R6 La señalización entre el UE y la HDC-FE ha de tener protección de integridad y confidencialidad.

R7 La señalización entre el UE y la HDC-FE ha de estar protegida contra los ataques de reproducción.

R8 Se ha de facilitar autentificación de baja latencia y protección de la señalización.

R9 Se ha de optimizar la transferencia del contexto de seguridad.

R10 La solución de seguridad de la movilidad ha de ser independiente del medio.

R11 Se ha de disponer de mecanismos para proteger el tráfico en el plano de usuario entre el UE y la EN-FE cuando así lo indique el perfil de usuario.

Además de los requisitos de seguridad identificados en [UIT-T Y.2018], también se aplica el siguiente requisito:

R12 Se ha de soportar la seguridad de múltiples conexiones.

6 Capacidades de seguridad soportadas por las entidades funcionales correspondientes

Las entidades funcionales relacionadas con la seguridad de la movilidad en las NGN son las siguientes:

- Entidad funcional de perfil de usuario de transporte (TUP-FE)
- Entidad funcional de autentificación y autorización de transporte (TAA-FE)
- Entidad funcional de gestión de ubicación móvil (MLM-FE)
- Entidad funcional de control y decisión de traspaso (HDC-FE)
- Entidad funcional de distribución de información de red (NID-FE)
- Entidad funcional de gestión de acceso (AM-FE)
- Función de ejecución de traspaso en capa 3 (L3HEF)
- Entidad funcional de nodo de acceso (AN-FE)

6.1 Entidad funcional de perfil de usuario de transporte (TUP-FE)

La TUP–FE almacena datos de autentificación de abono, como las claves, los métodos de autentificación y el perfil de usuario de transporte. Puede encontrarse la descripción funcional detallada de la TUP-FE en [UIT-T Y.2014].

6.2 Entidad funcional de autentificación y autorización de transporte (TAA-FE)

La TAA-FE extrae datos de autentificación e información de autorización de accesos de la TUP-FE. La TAA-FE también puede ejercer de intermediario.

Puede encontrarse la descripción funcional detallada en [UIT-T Y.2014].

6.3 Entidad funcional de gestión de ubicación móvil (MLM-FE)

La MLM-FE obtiene la información de autentificación, autorización y contabilidad de la NACF, realiza la autentificación mutua con el UE y crea una asociación de seguridad entre el UE y la MLM-FE. Puede encontrarse la descripción funcional detallada en [UIT-T Y.2018].

6.4 Entidad funcional de control y decisión de traspaso (HDC-FE)

La HDC-FE ha de establecer una asociación de seguridad con el UE y obtiene la clave de seguridad utilizada para la asociación de la TAA-FE a través de la TLM-FE. Puede encontrarse la descripción funcional detallada en [UIT-T Y.2018].

6.5 Entidad funcional de distribución de información de red (NID-FE)

La NID-FE ha de establecer una asociación de seguridad con el UE para proteger la información, como la información de selección de red. La NID-FE puede obtener la información de seguridad de la TAA-FE a través de la TLM-FE. Puede encontrarse la descripción funcional detallada en [UIT-T Y.2018].

6.6 Entidad funcional de gestión de acceso (AM-FE)

La AM-FE remite las peticiones de acceso a la red a la TAA-FE para autentificar al usuario, autorizar o denegar el acceso a la red y extraer los parámetros de configuración de acceso propios del usuario. La AM-FE puede reutilizar los datos de registro/autentificación de la red para una recuperación rápida sin tener que realizar todo el procedimiento de registro/autentificación/configuración repetidamente. Puede encontrarse la descripción funcional detallada en [UIT-T Y.2014].

6.7 Función de ejecución de traspaso en capa 3 (L3HEF)

La L3HEF ha de establecer una asociación de seguridad con el UE para proteger el tráfico entre ellos. Puede encontrarse la descripción funcional detallada en [UIT-T Y.2018].

NOTA – La seguridad de la L3HEF cumple el requisito de seguridad de protección del tráfico en el plano de usuario entre el UE y la EN-FE.

6.8 Entidad funcional de nodo de acceso (AN-FE)

La AN-FE ha de establecer una asociación de seguridad con el UE, y obtiene las claves de la TAA-FE a través de la AM-FE. Puede encontrarse la descripción funcional detallada en [UIT-T Y.2018].

7 Autentificación y gestión de claves

7.1 Marco de gestión de claves

Para la seguridad de la movilidad en las NGN se utiliza el mecanismo de derivación jerárquica de claves. Hay diversos tipos de claves en las NGN, por ejemplo, clave raíz, clave de sesión, etc. La clave raíz es un tipo de credencial a largo plazo almacenada de manera segura (por ejemplo clave de secreto compartido o contraseña). La clave de sesión es una clave a corto plazo que se genera a partir de la clave raíz. Tanto el UE como la entidad de autentificación de las NGN (por ejemplo, TAA-FE/TUP-FE) almacenan la clave raíz compartida.

Normalmente las claves de sesión se generan a partir de la clave raíz y de otros parámetros de generación de claves, como la información de negociación durante el procedimiento de autentificación. La clave de sesión se utiliza para proteger el tráfico de señalización y el tráfico de usuario. La clave de sesión puede seguir derivándose. El mecanismo de derivación de claves depende del algoritmo criptográfico o el protocolo específicos.

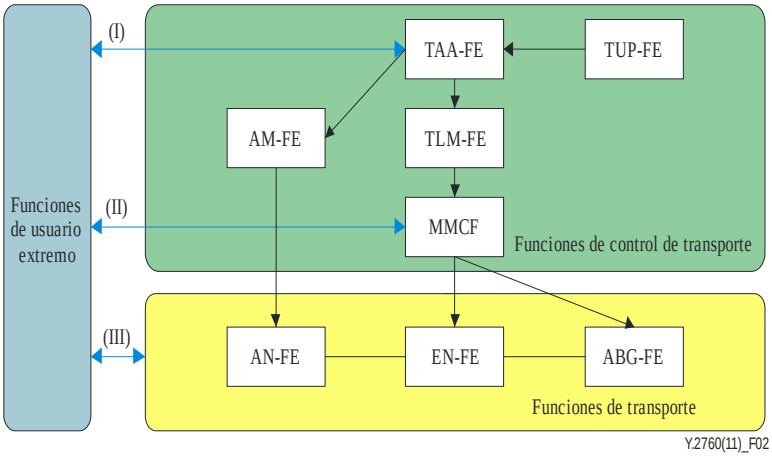

Figura 2 – Marco genérico de claves para la seguridad de la movilidad en las NGN

El marco genérico de claves para la seguridad de la movilidad en las NGN se describe de la siguiente manera:

I) El UE ejecuta el procedimiento de autentificación mutua con las entidades funcionales de la NGN. En el marco de este procedimiento, la TUP-FE genera vectores de autentificación basados en la clave raíz y envía estos vectores de autentificación a la TAA-FE. Una vez finalizado satisfactoriamente el procedimiento de autentificación mutua, tanto la TAA-FE como el UE generan claves de sesión. Las claves de sesión pueden emplearse para generar claves de subsesión. La clave de sesión se transfiere a las entidades funcionales como la AM-FE y la MMCF. Tanto la AM-FE como la MMCF pueden generar claves de subsesión basadas en la clave de sesión recibida.

II) Las asociaciones de seguridad para los puntos de referencia entre el UE y la MMCF se basan en la clave de sesión que se obtiene de la TAA-FE a través de la TLM-FE. La clave de sesión utilizada en II) se genera o deriva en función de la clave de sesión de la TAA-FE.

III) Las asociaciones de seguridad entre el UE y la capa funcional de transporte de la NGN se establecen basándose en claves compartidas, que se generan a partir de la anterior clave de sesión en la TAA-FE, la AM-FE o la MMCF. La AN-FE recibe la clave de sesión de la TAA-FE a través de la AM-FE. Si la AM-FE tiene la capacidad de derivar la clave de sesión, la AN-FE puede obtener la clave de sesión directamente de la AM-FE. Tanto la EN-FE como la ABG-FE reciben las claves generadas de la TAA-FE a través de la TLM-FE y la MMCF. Si la MMCF tiene la capacidad de derivar claves de sesión, tanto la EN-FE como la ABG-FE pueden obtener las claves de la MMCF.

El procedimiento de autentificación se basa en un protocolo pregunta-respuesta, por ejemplo, AKA [b-3GPP TS 33.102].

7.2 Autentificación

7.2.1 Procedimiento de autentificación genérico

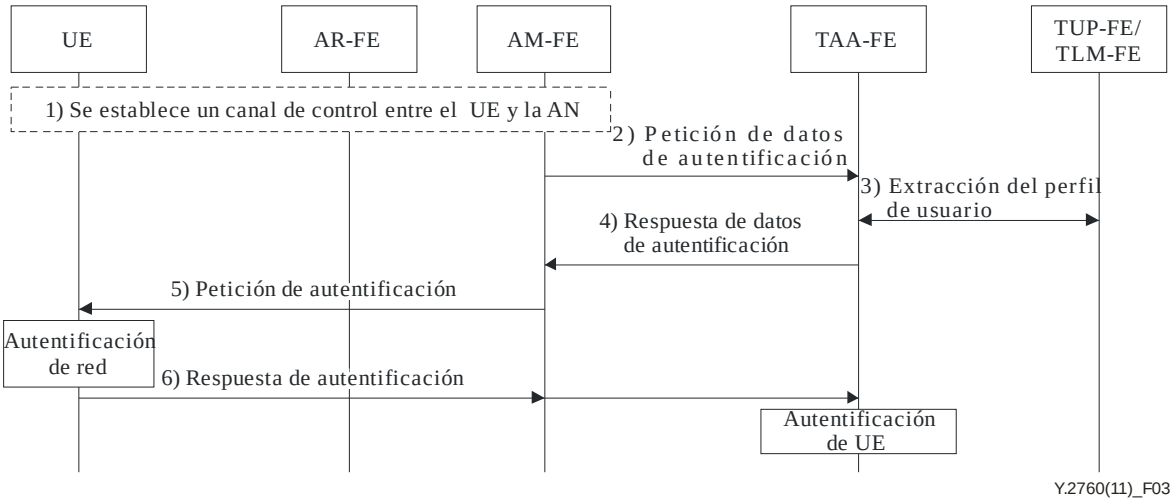

Figura 3 – Procedimiento de autentificación genérico

1) Se establece el canal de control entre el UE y las funciones de la red de acceso (este procedimiento queda fuera del alcance de la presente Recomendación).
2) La AM-FE envía la información del UE a la TAA-FE para pedir los datos de autentificación.
3) La TAA-FE obtiene la información de autentificación de la petición de autentificación, que comprende el ID de abonado del usuario e información de la red de acceso, interactúa con la TUP-FE/TLM-FE para obtener el perfil del usuario y los vectores de autentificación, incluido el testigo de autentificación y la clave de sesión.
4) La TAA-FE envía la respuesta de datos de autentificación, incluido el testigo de autentificación, a la AM-FE.
5) La AM-FE envía la petición de autentificación al UE. El UE extrae el testigo de autentificación de la petición de autentificación, genera vectores de autentificación locales, incluida la clave de sesión a partir del testigo de autentificación y de la clave raíz. El UE autentifica la red validando el testigo de autentificación recibido.
6) El UE envía la respuesta de autentificación a la AM-FE, incluido el testigo de autentificación generado por el UE. La AM-FE remite la información a la TAA-FE. La TAA-FE extrae el testigo de autentificación y verifica la validación del testigo de autentificación recibido para autentificar al UE.

7.2.2 Procedimiento de reautentificación rápida genérico

La reautentificación rápida se utiliza para reducir la latencia del traspaso. La TUP-FE/TLM-FE no participa en el procedimiento de reautentificación rápida, que agiliza el procedimiento de autentificación y reduce la carga de la TUP-FE/TLM-FE. Se recomienda que tanto el UE como las entidades de autentificación de las NGN soporten la reautentificación rápida genérica.

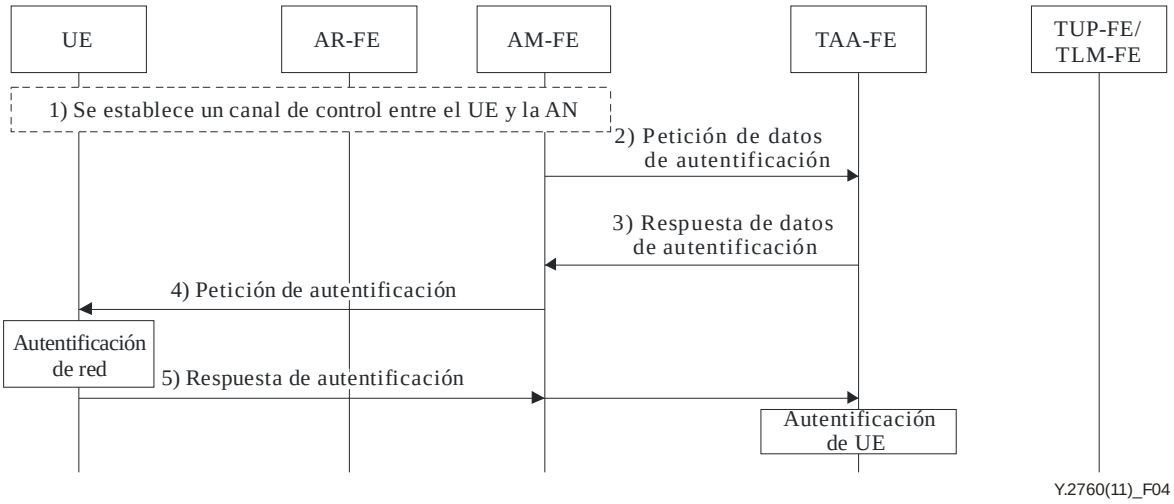

Figura 4 – Procedimiento de reautentificación rápida genérico

Se ejecutan los siguientes pasos, siempre y cuando el UE y la TAA-FE tengan la capacidad de reautentificación rápida.

1) Se establece el canal de control entre el UE y las funciones de la red de acceso (este procedimiento queda fuera del alcance de la presente Recomendación).
2) La AM-FE envía la información del UE a la TAA-FE para pedir los datos de autentificación.
3) La TAA-FE envía la respuesta de datos de autentificación, incluido el testigo de autentificación, a la AM-FE.
4) La AM-FE envía la petición de autentificación al UE. El UE extrae el testigo de autentificación de la petición de autentificación, genera vectores de autentificación locales, incluida la clave de sesión, a partir del testigo de autentificación y de la clave raíz. El UE autentifica la red validando el testigo de autentificación recibido.
5) El UE envía la respuesta de autentificación a la AM-FE, incluido el testigo de autentificación generado por el UE. La AM-FE remite la información a la TAA-FE. La TAA-FE extrae el testigo de autentificación y verifica la validación del testigo de autentificación recibido para autentificar al UE.

Cuando el UE reutiliza la clave de sesión, la información de reautentificación rápida sólo se utiliza para la autentificación mutua. Cuando el UE no reutiliza la clave de sesión, tanto el UE como la entidad de autentificación (por ejemplo, TAA-FE /TUP-FE) generan una nueva clave de sesión basada en la clave de sesión y en la información de reautentificación rápida.

7.2.2.1 Reautentificación rápida optimizada

En el procedimiento de reautentificación rápida optimizado, el UE que ha sido previamente autentificado por la NGN genera información de autentificación. Este procedimiento es diferente del de reautentificación genérico por cuanto el UE autentifica primero a la NGN y luego la red NGN genera el testigo autentificado.

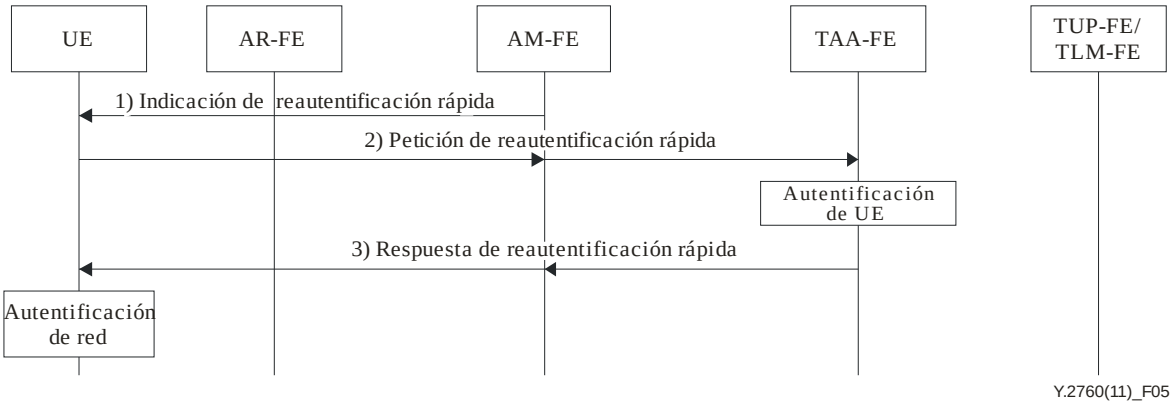

Figura 5 – Procedimiento de reautentificación rápida optimizado

1) Se establece el canal de control entre el UE y las funciones de la red de acceso (este procedimiento queda fuera del alcance de la presente Recomendación). La AM-FE envía la indicación de reautentificación optimizada al UE, que indica que la TAA-FE soporta la reautentificación rápida optimizada.

2) El UE genera el vector de autentificación y envía la petición de reautentificación optimizada a la TAA-FE a través de la AM-FE. La petición de reautentificación optimizada comprende el testigo de autentificación y la información de reautentificación. La TAA-FE genera el vector de autentificación local y una nueva clave de sesión a partir de la información de reautentificación y de la clave de sesión. La TAA-FE autentifica al UE validando el testigo de autentificación recibido.

3) La TAA-FE envía la respuesta de reautentificación, incluido el vector de autentificación, al UE a través de la AM-FE. El UE autentifica la red mediante su propio vector de autentificación. Una vez realizada la autentificación satisfactoriamente, el UE puede generar una clave de subsesión.

7.2.3 Autentificación intradominio

7.2.3.1 Autentificación en una conexión de red única

La conexión de red única implica que el UE puede detectar una red distinta, pero acceder sólo a una red cada vez. Por preautentificación se entiende que el UE realiza la autentificación mutua con la red objetivo a través de la red de servicio antes de que el UE efectúe el traspaso a la red objetivo. Cuando el UE sólo soporta la conexión de red única, el UE utiliza la preautentificación para mantener la continuidad del servicio y una latencia más baja. El procedimiento de preautentificación es semejante al de autentificación genérico. De ser necesario, participan en el procedimiento de preautentificación la AM-FE de servicio y la AM-FE objetivo.

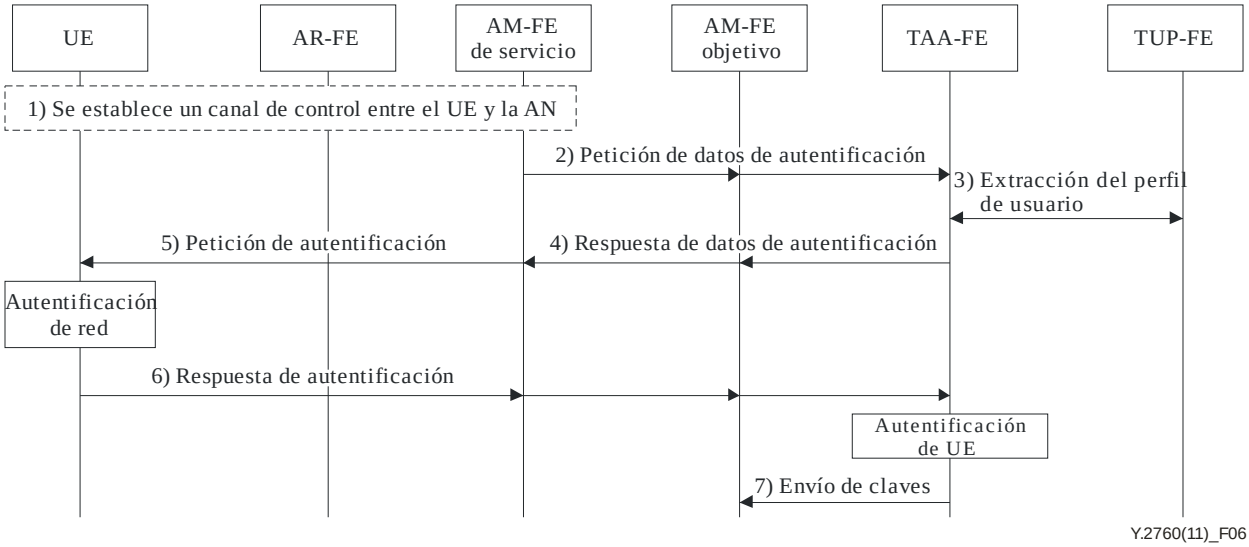

Figura 6 – Procedimiento de preautentificación en conexión de red única

1) Se establece el canal de control entre el UE y las funciones de la red de acceso (este procedimiento queda fuera del alcance de la presente Recomendación).
2) La AM-FE envía la petición de datos de autentificación a la TAA-FE, que comprende la información de abonado. La AM-FE de servicio y la AM-FE objetivo remiten la petición de datos de autentificación.
3) La TAA-FE extrae el perfil del usuario interactuando con la TUP-FE.
4) La TAA-FE envía la respuesta de datos de autentificación a la AM-FE objetivo y la AM-FE de servicio, incluido el testigo de autentificación.
5) La AM-FE de servicio envía la petición de autentificación al UE. El UE extrae el testigo de autentificación y autentifica a la red utilizando su propia información de autentificación. Una vez realizada la autentificación satisfactoriamente, el UE genera la clave de sesión.
6) El UE envía la respuesta de autentificación a la AM-FE de servicio. La AM-FE de servicio remite la información a la AM-FE objetivo y la TAA-FE, incluido el testigo de autentificación. La TAA-FE extrae el testigo de autentificación y autentifica al UE. Una vez realizada la autentificación satisfactoriamente, la TAA-FE genera la clave de sesión, de la que se puede derivar una clave de subsesión, de ser necesario.
7) La TAA-FE envía la clave a la AM-FE objetivo, que se utilizará una vez que el UE efectúe el traspaso a la red objetivo para proteger la comunicación entre el UE y la red objetivo.

7.2.4 Autentificación entre dominios

Un dominio administrativo distinto supone la existencia de un proveedor NGN diferente. A continuación se describe un procedimiento de autentificación para el traspaso del UE entre distintos dominios administrativos.

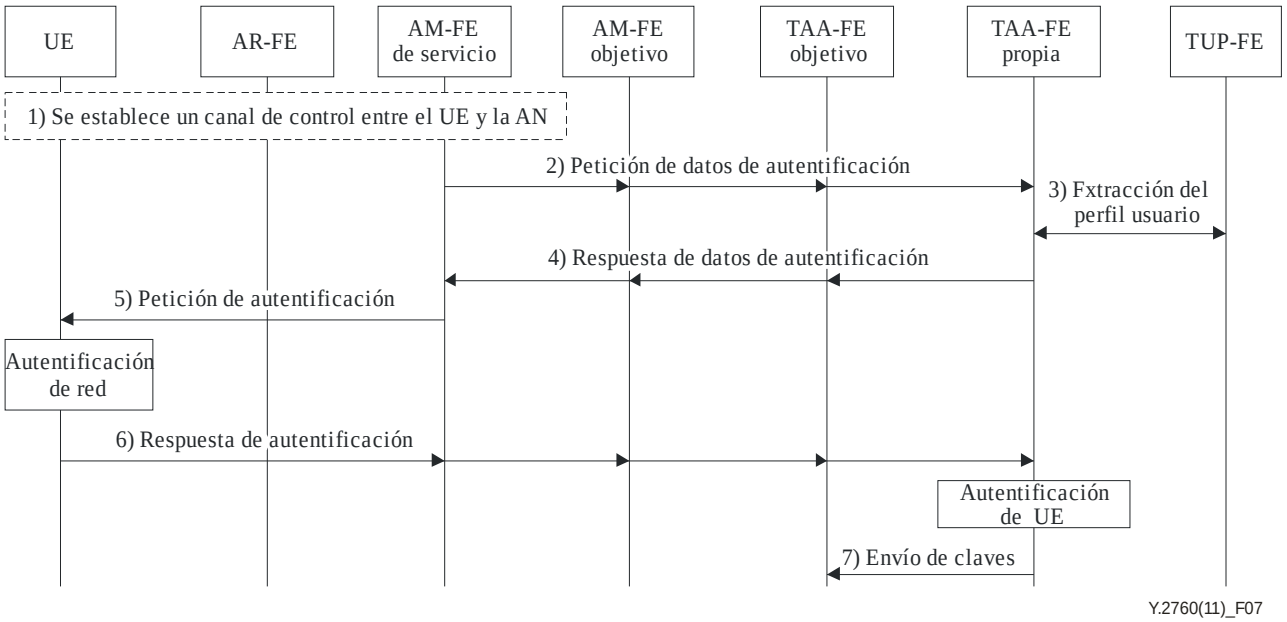

Figura 7 – Procedimiento de autentificación entre distintos dominios

1) Se establece el canal de control entre el UE y las funciones de la red de acceso (este procedimiento queda fuera del alcance de la presente Recomendación).
2) La AM-FE de servicio envía la petición de datos de autentificación a la TAA-FE propia, incluida la información de abonado. La AM-FE objetivo y la TAA-FE objetivo reenvían la petición de datos de autentificación. La TAA-FE propia extrae el perfil del usuario interactuando con la TUP-FE.
3) La TAA-FE extrae el perfil del usuario interactuando con la TUP-FE.
4) La TAA-FE propia envía la respuesta de datos de autentificación a la AM-FE de servicio, incluido el testigo de autentificación. La TAA-FE objetivo y la AM-FE objetivo reenvían la petición de datos de autentificación.
5) La AM-FE de servicio envía la petición de autentificación al UE. El UE extrae el testigo de autentificación y la red de autentificación de su propia información de autentificación, una vez efectuada satisfactoriamente la autentificación, el UE genera la clave de sesión.
6) El UE envía la respuesta de autentificación a la TAA-FE propia, incluido el testigo de autentificación. La TAA-FE propia extrae el testigo de autentificación y autentifica al UE. Una vez efectuada satisfactoriamente la autentificación, la TAA-FE propia genera la clave de sesión que se puede utilizar para generar claves de subsesión, de ser necesario.
7) Una vez efectuada satisfactoriamente la autentificación, la TAA-FE propia envía las claves a la TAA-FE objetivo, que se utilizarán después de que el UE realice el traspaso de la red de servicio a la red objetivo a fin de proteger la comunicación entre el UE y la red objetivo.

7.2.5 Mecanismo de correspondencia de claves en la autentificación

Cuando un UE va de una red de servicio a una red objetivo, se ejecuta la autentificación mutua y se genera la clave de sesión. Las NGN soportan diversos mecanismos de derivación de claves y la correspondencia de claves se emplea para coordinar las claves utilizadas en los distintos mecanismos de derivación de claves.

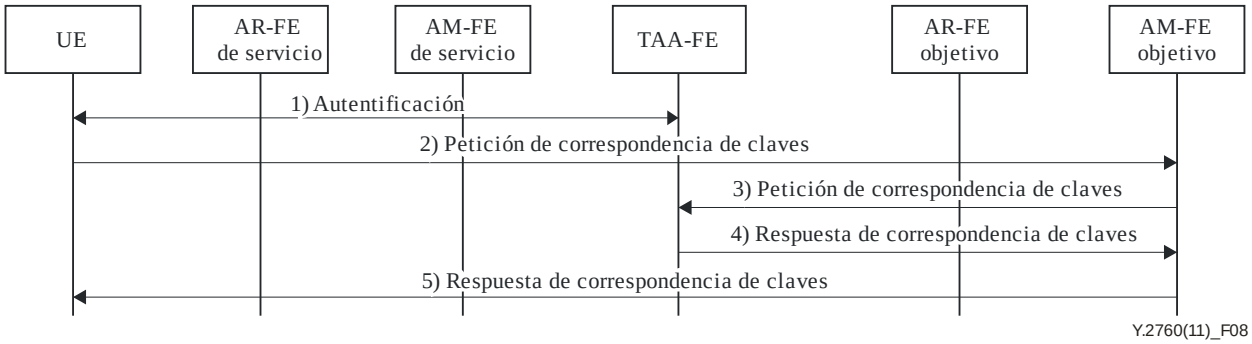

Figura 8 – Procedimiento de correspondencia de claves

1) Se establece una conexión entre el UE y la TAA-FE, se ejecuta el procedimiento de autentificación y se genera la clave de sesión.
2) El UE detecta la red objetivo y prepara el traspaso a la red objetivo. El UE envía una petición de correspondencia de claves a la AM-FE objetivo. La petición de correspondencia de claves comprende información como el mecanismo de derivación de claves utilizado y el mecanismo de derivación de claves soportado.
3) La AM-FE objetivo envía la petición de correspondencia de claves a la TAA-FE.
4) La TAA-FE recibe la petición de correspondencia de claves y establece la correspondencia entre las claves de la red de servicio y las claves de la red objetivo, y envía la respuesta de correspondencia de claves a la AM-FE objetivo.
5) La AM-FE objetivo envía la respuesta de correspondencia al UE. El UE establece la correspondencia entre las claves de la red de servicio y las claves de la red objetivo. Tanto el UE como la TAA-FE comparten las claves objetivo de la red objetivo, que se utilizan para proteger el tráfico entre el UE y la red objetivo.

7.2.6 Autentificación en conexiones de red múltiples

Autentificación en conexiones de red múltiples significa que el UE tiene la capacidad de comunicar con múltiples redes de acceso simultáneamente. Cuando el UE tiene la capacidades de conectarse con múltiples redes de acceso, el UE conecta con la red objetivo y ejecuta el procedimiento de autentificación mutua antes de desconectarse de la red de servicio. La autentificación mutua es la autentificación genérica de la figura 3. Una vez realizada la autentificación mutua satisfactoriamente, tanto el UE como la TAA-FE generan la clave de sesión compartida y la TAA-FE envía la clave de sesión a la AM-FE objetivo. Cuando el UE pasa a la red objetivo, el tráfico entre el UE y la red objetivo está protegido por la clave de sesión o de subsesión.

7.2.7 Autentificación multiconexión

Por multiconexión se entiende que el UE mantiene más de una conexión de red simultáneamente. Los distintos tipos de conexión de red pueden ofrecer al usuario conexiones con diferentes características, como la anchura de banda, el bajo retardo y la alta seguridad. La multiplicidad de conexiones con diversos dominios administrativos queda fuera del alcance de la presente Recomendación.

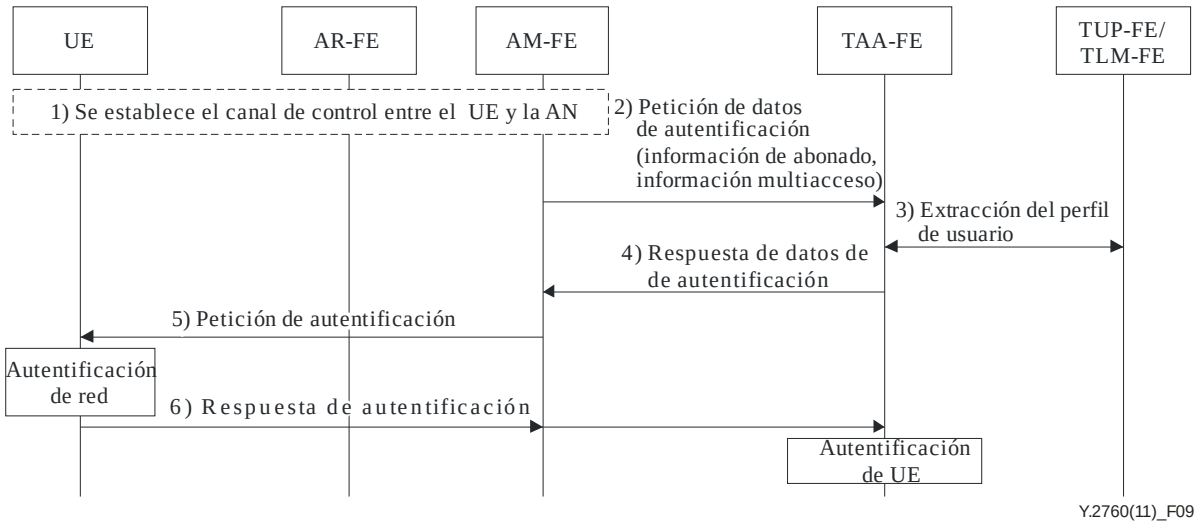

Figura 9 – Autentificación multiconexión

1) Se establece el canal de control entre el UE y las funciones de la red de acceso (este procedimiento queda fuera del alcance de la presente Recomendación). El UE obtiene de la red de acceso información y una indicación del soporte de la autentificación multiacceso.
2) La AM-FE envía la petición de datos de autentificación a la TAA-FE. La petición de datos de autentificación comprende información del UE como la información de abonado (por ejemplo, ID de abonado del usuario); información multiacceso (por ejemplo, indicación multiacceso e ID de interfaz de acceso múltiple).
3) La TAA-FE obtiene la información de autentificación e interactúa con la TUP-FE/TLM-FE para obtener el perfil del usuario y el vector de autentificación. La TUP-FE/TLM-FE genera un vector de autentificación. En el vector de autentificación se incluye el testigo de autentificación.
4) La TAA-FE envía la respuesta de datos de autentificación, incluido el testigo de autentificación, a la AM-FE.
5) La AM-FE envía la petición de autentificación al UE. El UE genera testigos de autentificación locales a partir de la información de autentificación del mensaje de petición de autentificación. El UE autentifica la red verificando la validación del testigo de autentificación recibido de acuerdo con los testigos de autentificación locales. Una vez realizada satisfactoriamente la autentificación, el UE genera la clave de sesión a partir de la información de autentificación. Si está activada la indicación multiacceso, el UE genera múltiples claves de sesión de acuerdo con la información multiacceso.
6) El UE envía un mensaje de respuesta de autentificación a la AM-FE. La AM-FE remite la información a la TAA-FE, incluido el testigo de autentificación generado por el UE. La TAA-FE extrae el testigo de autentificación del mensaje de respuesta de autentificación y autentifica el UE de acuerdo con el vector de autentificación de la TAA-FE. Una vez realizada satisfactoriamente la autentificación, la TAA-FE genera la clave de sesión de

acuerdo con el testigo de autentificación. Si está activada la indicación multiacceso, la TAA-FE genera múltiples claves de sesión de acuerdo con la información multiacceso.

8 Establecimiento del contexto de seguridad

8.1 Transferencia del contexto de seguridad entre la AM-FE de servicio y la AM-FE objetivo

Se ha de proteger el tráfico de transferencia del contexto de seguridad entre la AM-FE de servicio y la AM-FE objetivo. La seguridad entre la AM-FE de servicio y la AM-FE objetivo se logra estableciendo una asociación de seguridad. Si dos AM-FE están en la misma zona, no se necesita la asociación de seguridad. Si dos AM-FE se encuentran en zonas distintas, como dominios de distintos operadores, el mecanismo de seguridad y la política o el acuerdo del operador crean la asociación de seguridad.

8.2 Transferencia del contexto de seguridad entre la AR-FE de servicio y la AR-FE objetivo

Cuando el UE realiza el traspaso entre la AR-FE de servicio y la AR-FE objetivo, el tráfico de transferencia del contexto de seguridad entre la AR-FE objetivo y la AR-FE de servicio ha de estar protegido. La seguridad de la transferencia del contexto de seguridad entre la AR-FE de servicio y la AR-FE objetivo se logra estableciendo una asociación de seguridad.

8.3 Transferencia del contexto de seguridad entre el UE y la HDC-FE

8.3.1 Transferencia del contexto de seguridad iniciada por el anfitrión

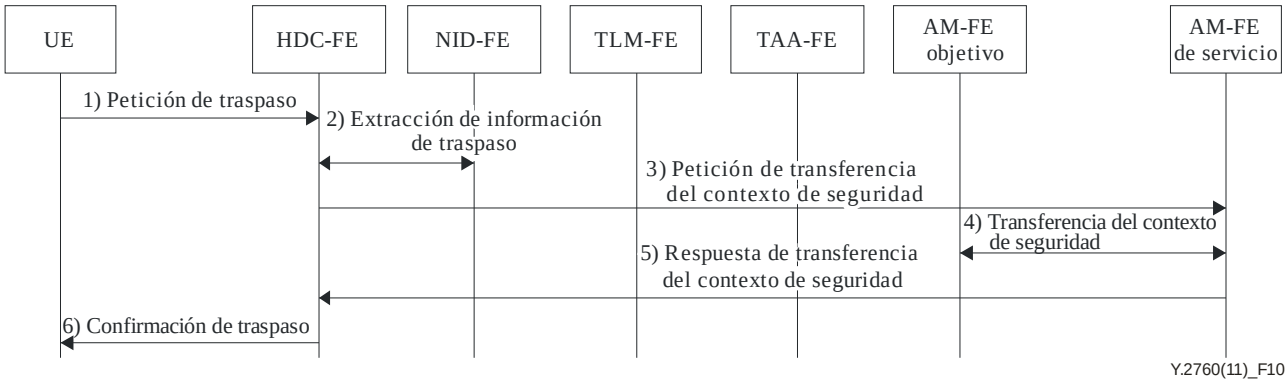

Figura 10 – Procedimiento de transferencia del contexto de seguridad iniciada por el anfitrión

Cuando el UE decide realizar un traspaso desde la red de servicio a la red objetivo, el UE envía una petición de traspaso a la HDC-FE, que desencadena la transferencia del contexto de seguridad. Una vez terminada la transferencia del contexto de seguridad, la AM-FE objetivo utiliza el contexto de seguridad para proteger el tráfico entre el UE y la red objetivo. Se siguen los siguientes pasos:

1) El UE envía una petición de traspaso a la HDC-FE.
2) La HDC-FE recibe la petición de traspaso, interactúa con la NID-FE para obtener la información relacionada con el traspaso
3) La HDC-FE remite la petición de traspaso, incluida la información conexa, a la AM-FE de servicio.
4) La AM-FE de servicio interactúa con la AM-FE objetivo para transferir el contexto de seguridad.

5) Cuando se ha finalizado la transferencia del contexto de seguridad, la AM-FE de servicio envía la respuesta de transferencia del contexto de seguridad a la HDC-FE.

6) La HDC-FE recibe la respuesta de transferencia del contexto de seguridad. Si se realiza con éxito la transferencia del contexto de seguridad, la HDC-FE envía al UE la confirmación del traspaso.

8.3.2 Transferencia del contexto de seguridad iniciada por la red

Cuando la HDC-FE decide activar el UE para realizar el traspaso de la red de servicio a la red objetivo, la HDC-FE envía un mensaje de inicialización de traspaso para proceder a la transferencia del contexto de seguridad. Una vez finalizada la transferencia del contexto de seguridad, la AM-FE objetivo utiliza el contexto de seguridad para proteger el tráfico entre el UE y la red objetivo.

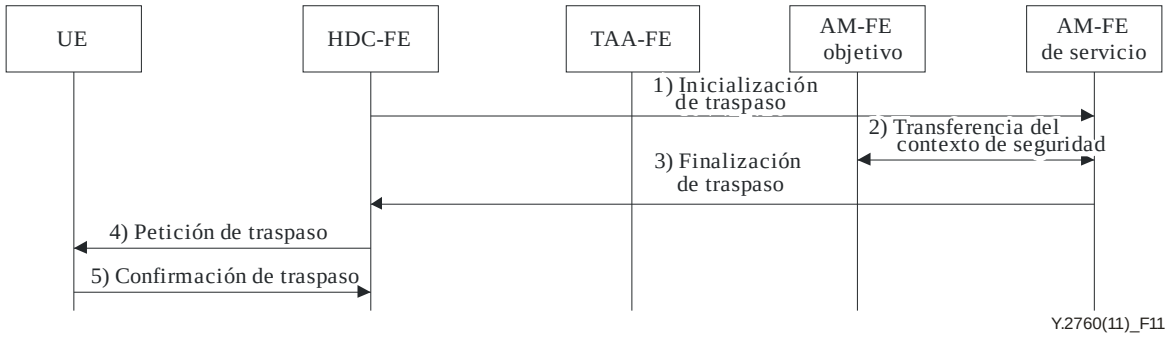

Figura 11 – Procedimiento de transferencia del contexto de seguridad iniciada por la red

1) La HDC-FE prepara el procedimiento de traspaso y envía un mensaje de inicialización de traspaso a la AM-FE de servicio para proceder a la transferencia del contexto de seguridad.

2) La AM-FE de servicio interactúa con la AM-FE objetivo para transferir el contexto de seguridad.

3) Cuando se ha finalizado la transferencia del contexto de seguridad, la AM-FE de servicio envía un mensaje de finalización de traspaso a la HDC-FE.

4) Cuando la HDC-FE recibe el mensaje de finalización de traspaso, inicia el procedimiento de traspaso enviando una petición de traspaso al UE.

5) El UE envía el mensaje de confirmación de traspaso cuando se ha completado el traspaso.

9 Seguridad de la movilidad IP

9.1 Seguridad de la movilidad basada en el anfitrión

Es necesario proteger el tráfico de control de la movilidad del anfitrión entre el UE y la MLM-FE (C). Se ha de crear una asociación de seguridad (SA) entre el UE y la MLM-FE(C). La SA entre el UE y el MLM-FE (P) es optativa.

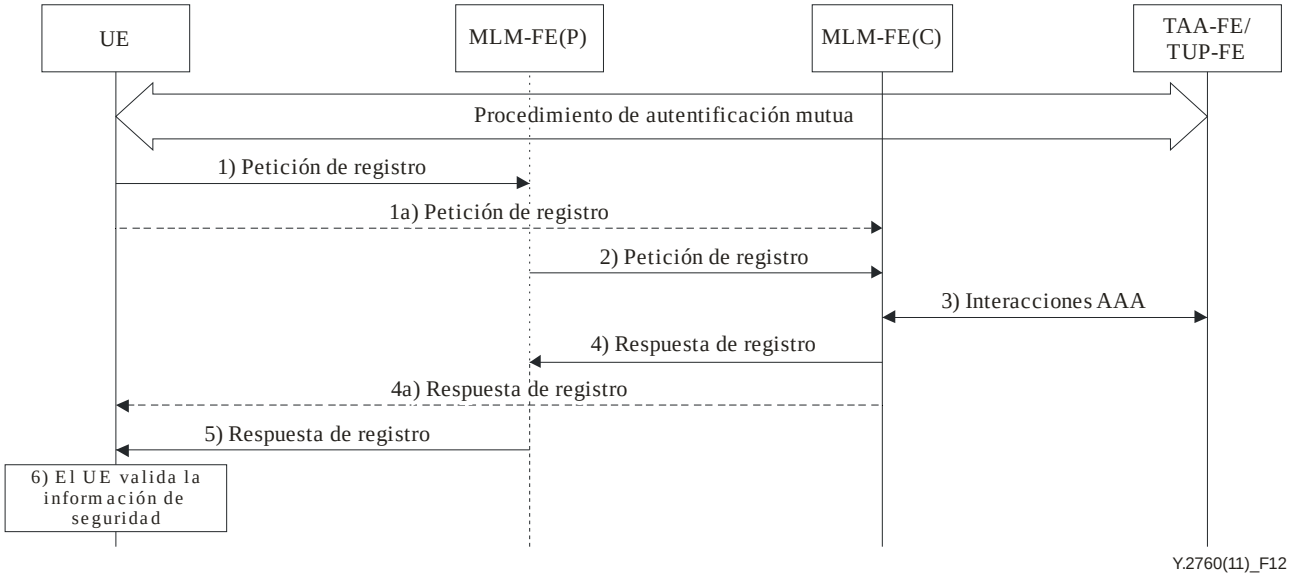

Figura 12 – Procedimiento de movilidad basada en el anfitrión

Se ejecutan los siguientes pasos, suponiendo que el UE y la TAA-FE han finalizado el procedimiento de autentificación genérico.

1) El UE envía una petición de registro a la MLM-FE(P). La petición de registro incluye información de seguridad entre el UE y la MLM-FE(C), e información de seguridad entre el UE y la MLM-FE(P).
   - 1a) Si no hay MLM-FE(P), el UE envía una petición de registro a la MLM-FE(C) directamente.
2) La MLM-FE(P) valida la información de seguridad entre el UE y la MLM-FE(P) y remite la petición de registro a la MLM-FE(C). La MLM-FE(P) puede añadir información de seguridad entre la MLM-FE(P) y la MLM-FE(C) al mensaje de petición de registro antes de remitirlo.
3) La MLM-FE(C) interactúa con la TAA-FE/TUP-FE para obtener información de autentificación e información de autorización.
4) La MLM-FE(C) valida la información de seguridad entre el UE y la MLM-FE(C) de la petición de registro. La MLM-FE(C) envía una respuesta de registro e información de seguridad a la MLM-FE(P). La respuesta de registro puede comprender información de seguridad entre el UE y la MLM-FE(C), así como información de seguridad entre la MLM-FE(P) y la MLM-FE(C).
   - 4a) Si no hay MLM-FE (P), la MLM-FE(C) envía la respuesta de registro directamente al UE. La respuesta de registro puede comprender información de seguridad entre el UE y la MLM-FE(C).
5) La MLM-FE(P) valida la información de seguridad entre la MLM-FE(P) y la MLM-FE(C) y envía la respuesta de registro al UE. La MLM-FE(P) puede añadir información de seguridad entre el UE y la MLM-FE(P) al mensaje de respuesta de registro antes de remitirlo.
6) La MLM-FE(C) valida la información de seguridad entre el UE y la MLM-FE(C), y crea una SA entre el UE y la MLM-FE(C). Si hay MLM-FE(P), el UE valida la información de seguridad entre el UE y la MLM-FE(P) y crea una SA entre el UE y la MLM-FE(P).

9.2 Seguridad de la movilidad basada en la red

La protección del tráfico de control de movilidad basada en la red entre dos entidades de red en una zona fiable, o fiable pero vulnerable, es optativa y depende de la política del operador. Los mecanismos de seguridad del tráfico de control de la movilidad basada se basan en los definidos en [UIT-T Y.2704].

10 Seguridad entre el UE y la HDC-FE

El flujo de información entre el UE y la HDC-FE se utiliza para transmitir información para la decisión del traspaso. El UE y la HDC-FE deben establecer una asociación de seguridad para proteger el flujo de información entre el UE y la HDC-FE.

10.1 Establecimiento de la asociación de seguridad entre el UE y la HDC-FE a instancias del anfitrión

El procedimiento de establecimiento de asociación de seguridad a instancias del anfitrión implica que el UE inicia el procedimiento de creación de una asociación de seguridad entre el UE y la HDC-FE que se muestra en la figura 13. El establecimiento de la asociación de seguridad entre el UE y la HDC-FE a instancias del anfitrión está sometido a dos condiciones. En primer lugar, el UE y la TAA-FE ya comparten las claves. Se consigue que compartan las claves con el procedimiento de autentificación mutua. En segundo lugar, el UE conoce la información de la HDC-FE, como la dirección por la cual el UE envía la petición de asociación de seguridad a la HDC-FE. La manera en que el UE obtiene la información de la HDC-FE queda fuera del alcance de la presente Recomendación. Se utiliza la TLM-FE para transmitir información de claves desde/hacia la TAA-FE, pero se omite en las siguientes figuras.ppp

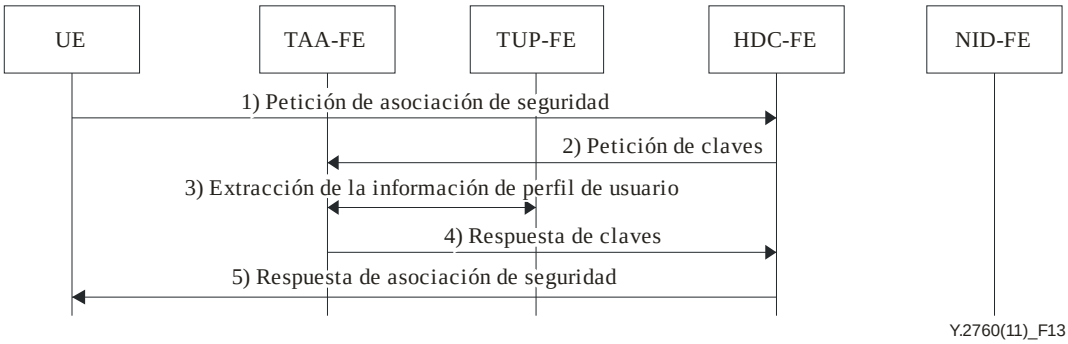

Figura 13 – Procedimiento de establecimiento de una asociación de seguridad a instancias del anfitrión

1) El UE genera claves compartidas para crear una asociación con la HDC-FE. En función de la información de autentificación, el UE envía una petición de asociación de seguridad a la HDC-FE, incluida la información de autentificación y la información del UE.
2) La HDC-FE envía la petición de claves a la TAA-FE, incluida la información de la HDC-FE, la información de autentificación y la información del UE.
3) La TAA-FE extrae la información del perfil de usuario interactuando con la TUP-FE y verifica que la HDC-FE está autorizada a crear una asociación de seguridad con el UE.
4) La TAA-FE genera claves para la HDC-FE de conformidad con la información de autentificación, la información de la HDC-FE y la información del UE, cuando la HDC-FE está autorizada a crear una asociación de seguridad con el UE. La TAA-FE envía la respuesta de claves a la HDC-FE incluyendo información tal como las claves, para la HDC-FE y el periodo de validez de las claves.

5) La HDC-FE envía la respuesta de asociación de seguridad para indicar que se ha establecido una asociación de seguridad entre el UE y la HDC-FE.

10.2 Establecimiento de la asociación de seguridad entre el UE y la HDC-FE a instancias de la red

El procedimiento de establecimiento de una asociación de seguridad a instancias de la red implica que la red inicia el procedimiento de creación de una asociación de seguridad entre el UE y la HDC-FE, como se muestra en la figura 14. El establecimiento de una asociación de seguridad entre el UE y la HDC-FE a instancias de la red está sometido a dos condiciones. En primer lugar, el UE y la TAA-FE comparten las claves. Se pueden generar las claves compartidas una vez efectuado el procedimiento de autentificación mutua. En segundo lugar, la HDC-FE conoce la información del UE, como la información de abonado o la información de ubicación mediante la cual la HDC-FE envía la información de asociación de seguridad al UE. La manera en que la HDC-FE obtiene la información del UE queda fuera del alcance de la presente Recomendación.

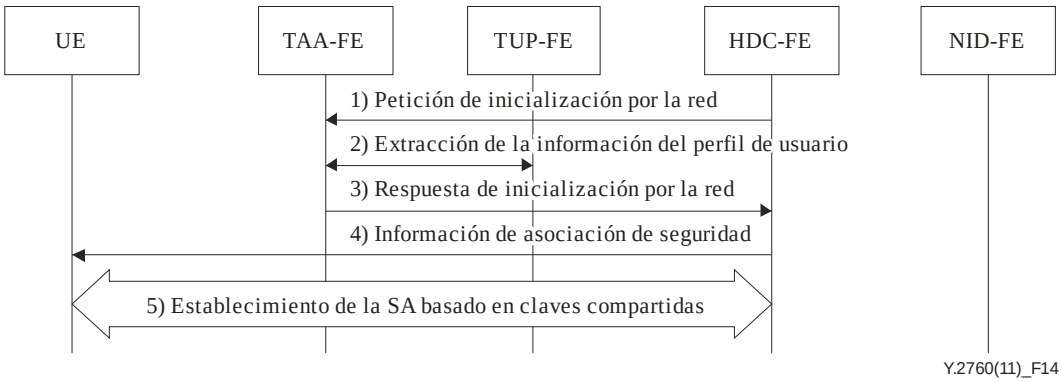

Figura 14 – Procedimiento de establecimiento de una asociación de seguridad a instancias de la red

1) La HDC-FE envía la petición de inicialización por la red a la TAA-FE, incluida la información de la HDC-FE y la información del UE.
2) La TAA-FE extrae la información del perfil de usuario interactuando con la TUP-FE y verifica que la HDC-FE está autorizada a iniciar la creación de una asociación de seguridad con el UE.
3) La TAA-FE genera claves para la HDC-FE de acuerdo con la información de la HDC-FE y la información del UE cuando la HDC-FE está autorizada a iniciar la creación de una asociación de seguridad con el UE. La TAA-FE envía la respuesta de inicialización por la red a la HDC-FE, incluida la información de autentificación tal que las claves para la HDC-FE y su periodo de validez.
4) La HDC-FE envía la información de asociación de seguridad, incluida la información de autentificación, al UE para crear una asociación de seguridad.
5) El UE genera claves para la HDC-FE de conformidad con la información de autentificación en la información de asociación de seguridad, y valida la información de asociación de seguridad. Se crea una asociación de seguridad entre la HDC-FE y el UE.

10.3 Preestablecimiento de la asociación de seguridad entre el UE y la HDC-FE basado en PKI

El procedimiento de establecimiento de la asociación de seguridad entre el UE y la HDC-FE basado en PKI se muestra en la figura 15. La condición para el establecimiento de una asociación de seguridad entre el UE y la HDC-FE es que el UE conozca la información de la HDC-FE, como la dirección por la que el UE envía la petición de asociación de seguridad a la HDC-FE. La manera en que el UE obtiene la información de la HDC-FE queda fuera del alcance de la presente Recomendación.

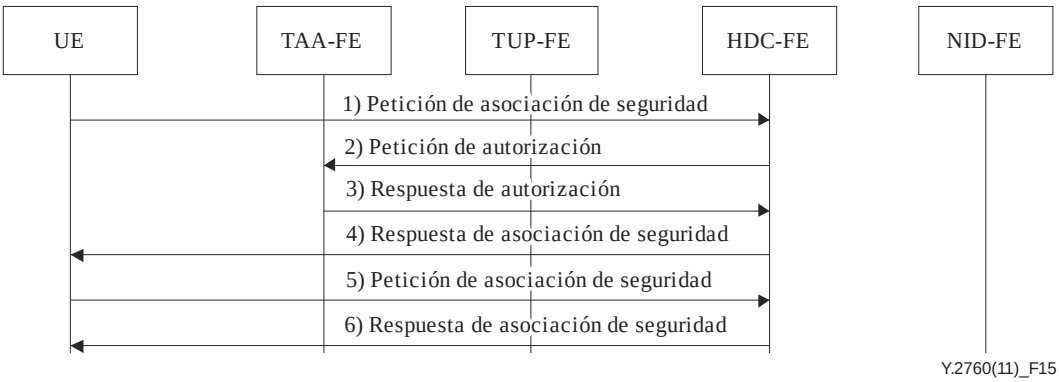

Figura 15 – Procedimiento de establecimiento de una asociación de seguridad basado en PKI

1) El UE envía una petición de asociación de seguridad a la HDC-FE, incluidos el certificado del UE y la información de la UE.
2) La HDC-FE valida el certificado del UE y envía la petición de autorización, incluida la información del UE y la información de la HDC-FE a la TAA-FE.
3) La TAA-FE verifica la autorización de acuerdo con la información del UE y la información de la HDC-FE. Si el UE está autorizado a utilizar la HDC-FE, la TAA-FE envía la respuesta de autorización a la HDC-FE, incluidos la información de autorización y el certificado del servidor.
4) La HDC-FE recibe la información de autorización y envía la respuesta de asociación de seguridad al UE, incluido el certificado del servidor.
5) Si se necesitan claves compartidas entre el UE y la TAA-FE, la TAA-FE envía la información de generación de claves al UE en el paso 4. El UE genera claves compartidas a partir de la información de generación de claves recibida y de la información de generación de claves local. El UE envía la información de generación de claves local a la HDC-FE.
6) La HDC-FE genera claves a partir de la información de generación de claves recibida y de la información de generación de claves local. La HDC-FE envía la respuesta de asociación de seguridad al UE. Se establece una asociación de seguridad entre el UE y la HDC-FE.

11 Seguridad entre el UE y la NID-FE

11.1 Establecimiento de la asociación de seguridad entre el UE y la NID-FE a instancias del anfitrión

El procedimiento de establecimiento de la asociación de seguridad entre el UE y la NID-FE a instancias del anfitrión se muestra en la figura 16. El procedimiento de establecimiento de la asociación de seguridad entre el UE y la NID-FE está sometido a las siguientes condiciones: 1) El UE y la TAA-FE comparten claves. Las claves compartidas pueden generarse después del

procedimiento de autentificación mutua. 2) El UE conoce la información de la NID-FE, como la dirección por la que el UE envía la petición de asociación de seguridad a la NID-FE. La manera en que el UE obtiene la información de la NID-FE queda fuera del alcance de esta Recomendación.

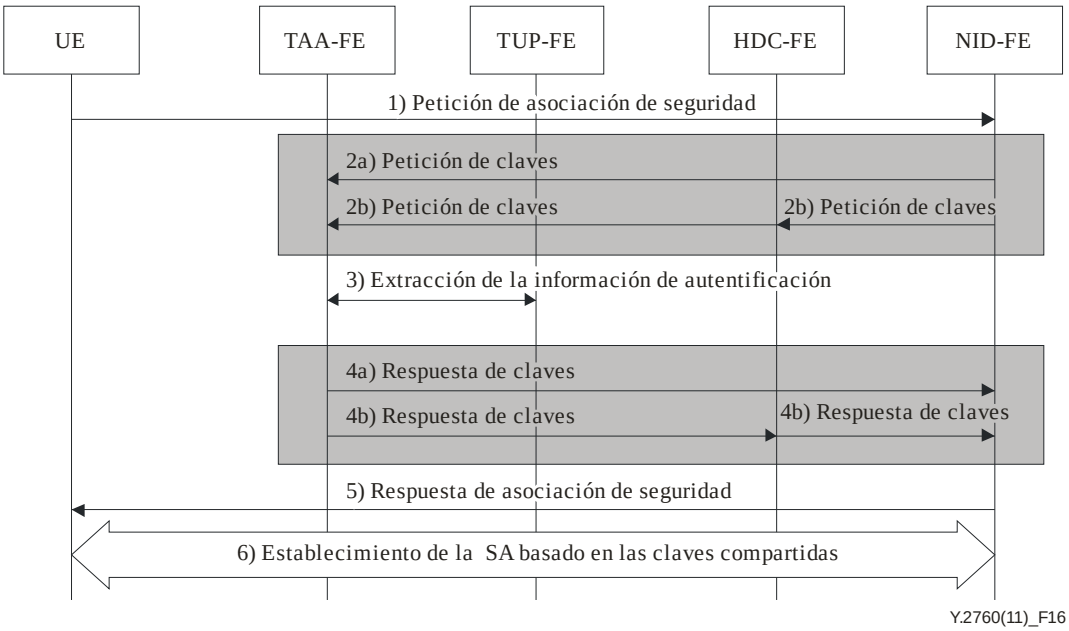

Figura 16 – Establecimiento de una asociación de seguridad a instancias del anfitrión

1) El UE envía la petición de asociación de seguridad a la NID-FE.
2) La NID-FE envía la petición de claves a la TAA-FE, incluida la información de la NID-FE y la información del UE. Cuando la NID-FE no puede enviar la petición de autentificación directamente a la TAA-FE, la NID-FE envía la petición de autentificación a la TAA-FE a través de la HDC-FE.
3) La TAA-FE interactúa con la TUP-FE y genera claves para la NID-FE.
4) La TAA-FE envía la respuesta de claves a la HDC-FE, incluida la información de autentificación. La información de autentificación comprende las claves compartidas y su periodo de validez. Cuando la TAA-FE no puede enviar la petición de autentificación directamente a la NID-FE, la TAA-FE envía la petición de autentificación a la NID-FE a través de la HDC-FE.
5) La NID-FE envía la respuesta de asociación de seguridad, incluida la información de autentificación, al UE protegido por las claves compartidas.
6) El UE genera claves compartidas y valida la respuesta de asociación de seguridad. Se crea una asociación de seguridad entre la NID-FE y el UE basada en las claves compartidas.

11.2 Establecimiento de la asociación de seguridad entre el UE y la NID-FE a instancias de la red

El procedimiento de establecimiento de la asociación de seguridad entre el UE y la NID-FE a instancias de la red se muestra en la figura 17. El procedimiento de establecimiento de la asociación de seguridad entre el UE y la NID-FE está sometido a las siguientes condiciones: 1) El UE y la TAA-FE comparten claves. Las claves de sesión compartidas pueden generarse después del procedimiento de autentificación mutua. 2) El UE conoce la información de la NID-FE, como la dirección por la que el UE envía la petición de asociación de seguridad a la NID-FE. La manera en que el UE obtiene la información de la NID-FE queda fuera del alcance de esta Recomendación.

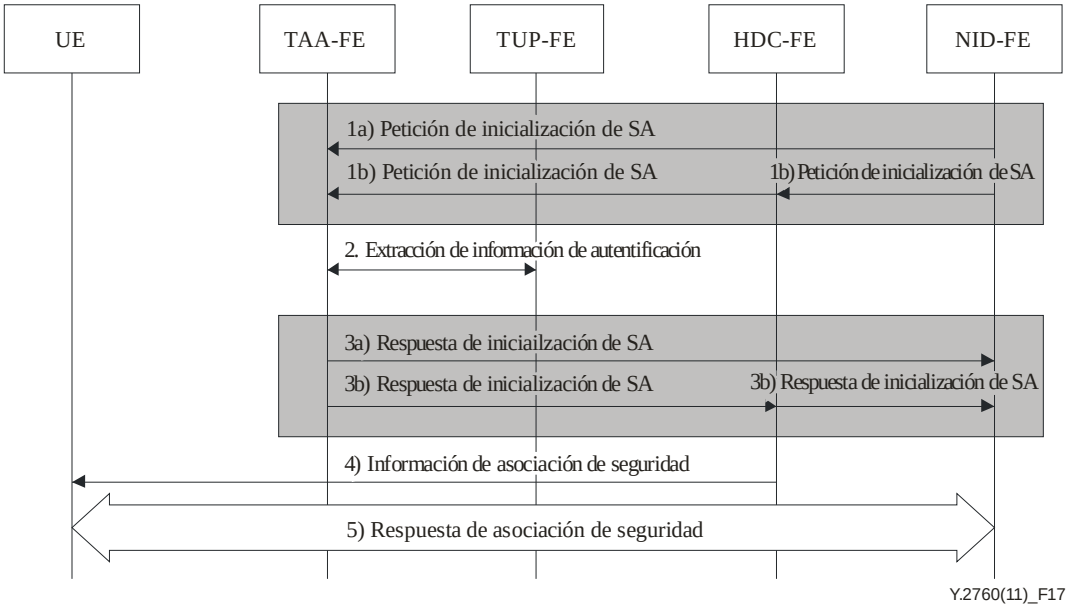

Figura 17 – Establecimiento de una asociación de seguridad a instancias de la red

1) La NID-FE envía la petición de inicialización de SA a la TAA-FE, incluida la información de la NID-FE. Cuando la NID-FE no puede enviar la petición de inicialización de SA directamente a la TAA-FE, la NID-FE envía la petición de inicialización de SA a la TAA-FE a través de la HDC-FE.

2) La TAA-FE interactúa con la TUP-FE y genera claves para la NID-FE.

3) La TAA-FE envía la respuesta de inicialización de SA a la NID-FE, incluida la información de autentificación. La información de autentificación comprende las claves y su periodo de validez. Cuando la TAA-FE no puede enviar la respuesta de inicialización de SA directamente a la NID-FE, la TAA-FE envía la respuesta de inicialización de SA a la NID-FE a través de la HDC-FE.

4) La NID-FE envía la información de asociación de seguridad, incluida la información de autentificación, al UE protegido por las claves.

5) El UE genera claves compartidas y valida la información de asociación de seguridad. Se crea una asociación de seguridad entre la NID-FE y el UE basada en las claves.

11.3 Establecimiento de la asociación de seguridad entre el UE y la NID-FE basada en PKI

El procedimiento de establecimiento de la asociación de seguridad entre el UE y la NID-FE basada en PKI se muestra en la figura 18. El procedimiento de establecimiento de la asociación de seguridad entre el UE y la NID-FE tiene como condiciones previas que el UE conozca la información de la NID-FE tal como la dirección por la que el UE envía la petición de asociación de seguridad a la NID-FE. La manera en que el UE obtiene la información de la NID-FE queda fuera del alcance de la presente Recomendación.

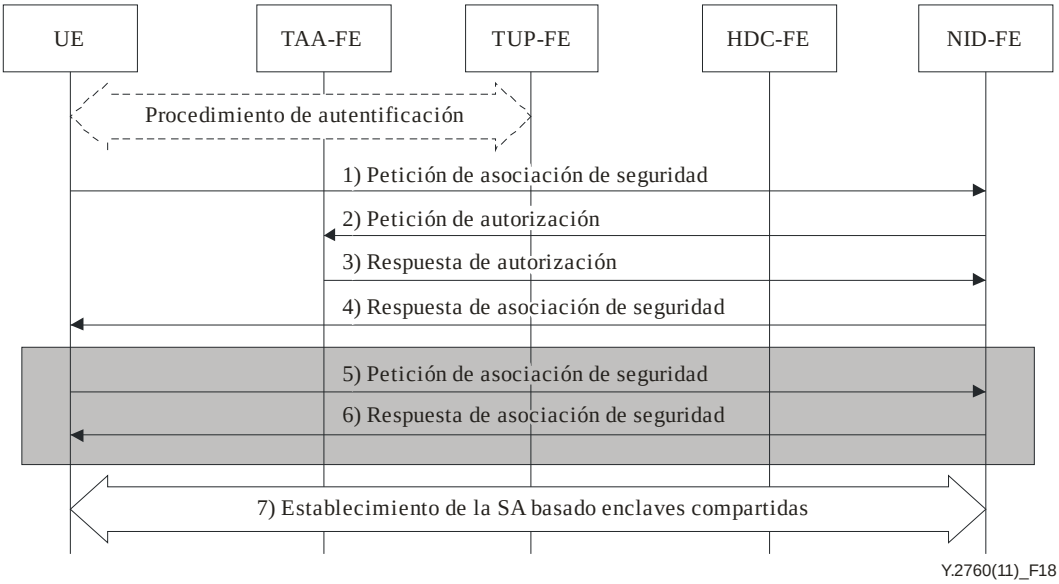

Figura 18 – Procedimiento de establecimiento de una asociación de seguridad basada en PKI

Una vez finalizado el procedimiento de autentificación entre la TUP-FE y la TAA-FE, se ejecutan los siguientes pasos.

1) El UE envía la petición de asociación de seguridad a la NID-FE, incluido el certificado del UE y la información del UE.
2) La NID-FE valida el certificado del UE y envía le petición de autorización, incluida la información del UE y la información de la NID-FE, a la TAA-FE.
3) La TAA-FE verifica la autorización de acuerdo con la información del UE y la información de la NID-FE. Si el UE está autorizado para utilizar la NID-FE, la TAA-FE envía la respuesta de autorización a la NID-FE, incluida la información de autorización y el certificado del servidor.
4) La NID-FE recibe la información de autorización y envía la respuesta de asociación de seguridad al UE, incluido el certificado del servidor.
5) Si se necesitan claves compartidas entre el UE y la TAA-FE, la TAA-FE envía la información de generación de claves al UE en el paso 4. El UE genera claves compartidas a partir de la información de generación de claves recibida y de la información de generación de claves local. El UE envía la información de generación de claves local a la NID-FE como parte de la petición de asociación de seguridad.
6) La NID-FE genera claves a partir de la información de generación de claves recibida y de la información de generación de claves local. La NID-FE envía la respuesta de asociación de seguridad al UE.
7) Se establece la asociación de seguridad entre el UE y la NID-FE.

12 Seguridad de las funciones de transporte

12.1 Seguridad entre el UE y la entidad funcional de nodo de acceso

El tráfico entre el UE y la AN-FE ha de estar protegido. La asociación de seguridad entre el UE y la AN-FE se basa en claves compartidas. Una vez finalizado con éxito el procedimiento de autentificación entre el UE y la TAA-FE, tanto el UE como la TAA-FE generan claves, como la clave de sesión, para proteger el tráfico entre el UE y la AN-FE. La TAA-FE envía claves a la AN-FE a través de la AM-FE y la AR-FE.

12.2 Seguridad entre el UE y la L3HEF (Función de ejecución de traspaso en capa 3)

El tráfico entre el UE y la L3HEF ha de estar protegido. La asociación de seguridad entre el UE y la L3HEF se basa en claves precompartidas. Una vez finalizada con éxito la autentificación, tanto el UE como la TAA-FE generan claves, como la clave de sesión, para proteger el tráfico entre el UE y la L3HEF. La L3HEF obtiene las claves directamente de la TAA-FE. Asimismo, la L3HEF obtiene claves de la TAA-FE a través de la AM-FE o la HDC-FE.

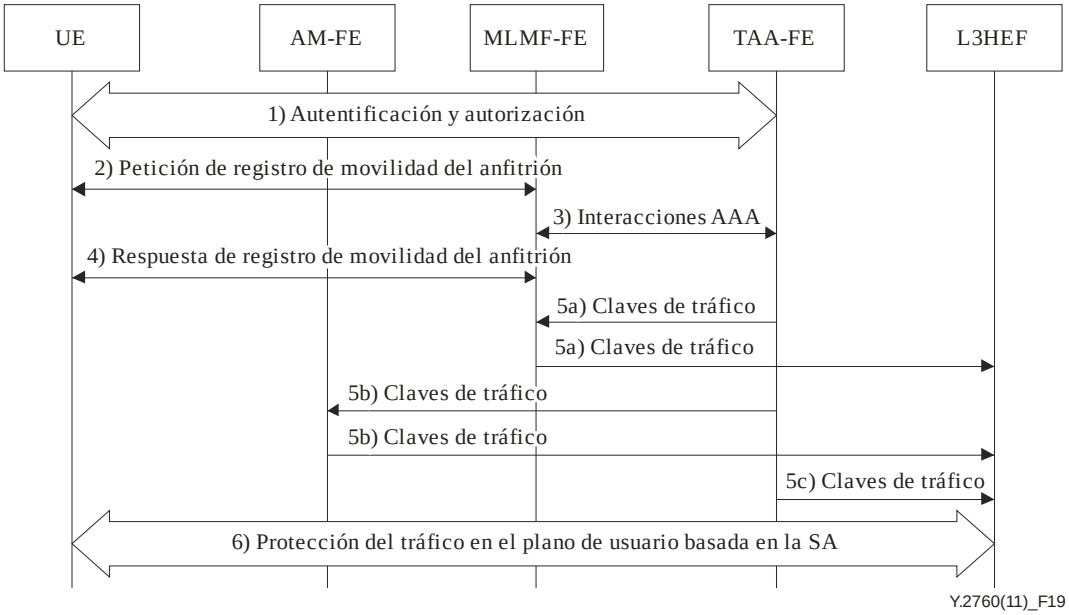

Figura 19 – Procedimiento de seguridad del tráfico entre el UE y la L3HEF en el plano de usuario

1) Se establece una conexión entre el UE y la TAA-FE. Una vez finalizada la autentificación mutua, tanto el UE como la TAA-FE comparten claves, como las claves transitorias y la clave de sesión.
2) El UE envía la petición de registro de movilidad del anfitrión a la MLM-FE para crear una asociación de seguridad de la movilidad basada en el anfitrión.
3) La MLM-FE obtiene las claves interactuando con la TAA-FE. La MLM-FE autentifica al UE a partir de las claves. Una vez finalizada con éxito la autentificación, la MLM-FE crea una asociación de seguridad con el UE basada en las claves.
4) La MLM-FE envía la respuesta de registro de movilidad del anfitrión al UE. El UE valida el mensaje de respuesta de registro de movilidad del anfitrión y crea una asociación de seguridad con la MLM-FE.
5) Una vez creadas las asociaciones de seguridad entre el UE y la MLM-FE, pueden darse tres casos:
   - 5a) La TAA-FE genera claves de tráfico y envía las claves de tráfico a la L3HEF a través de la MLM-FE.
   - 5b) La TAA-FE genera claves de tráfico y envía las claves de tráfico a la L3HEF a través de la MLM-FE y la AM-FE.
   - 5c) La TAA-FE envía las claves de tráfico directamente a la L3HEF.
6) La L3HEF utiliza las claves de tráfico para proteger el tráfico en el plano de usuario entre el UE y la L3HEF.

Apéndice I

(Este apéndice es una parte integrante de la presente Recomendación)

I.1 Ejemplo de procedimiento de autentificación completa

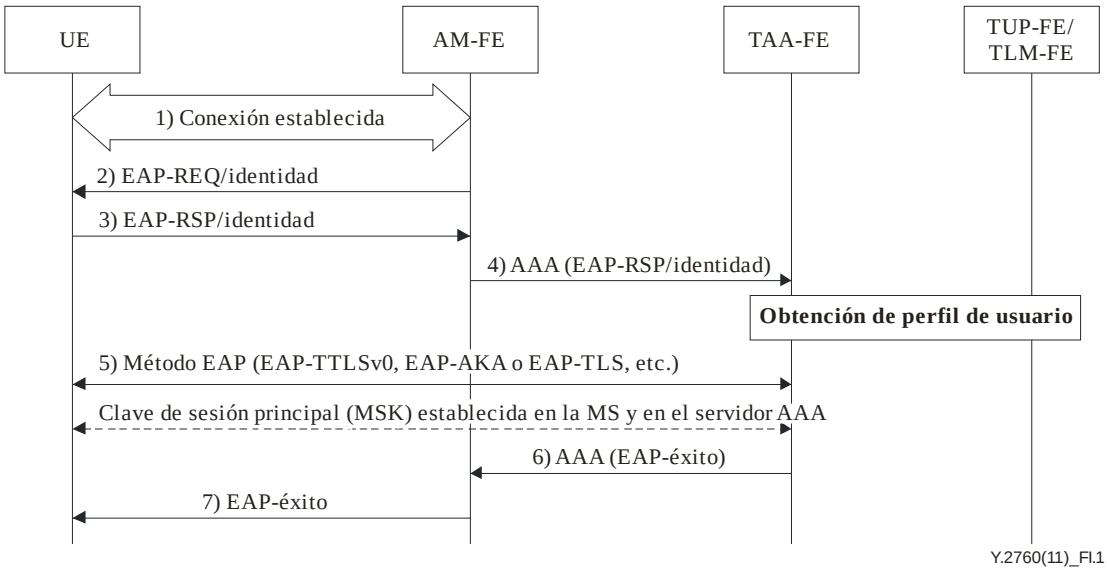

Figura I.1 – Procedimiento de autentificación completa

NOTA – Por "identidad" en los pasos 2-4 se entiende la Identidad del UE.

En la figura I.1 se muestra la inicialización de la autentificación.

1) Se establece la conexión entre el UE y la AM-FE
2) La AM-FE envía una petición EAP (EAP-REQ)/identidad al UE [b-IETF RFC 3748].
3) El UE envía una respuesta EAP (EAP-RSP)/identidad.
4) La AM-FE remite la EAP-RSP/Identidad a la TAA-FE; posteriormente, la TAA-FE intercambia información con la TUP-FE/TLM-FE, y la TUP-FE/TLM-FE envía información del usuario, incluido el perfil, a la TAA-FE.
5) Se ejecuta el proceso de derivación y distribución de claves en la TAA-FE y el UE. Pueden considerarse varios métodos, como EAP-TTLS, EAP-AKA, EAP-TLS etc.
6) La TAA-FE envía el mensaje EAP-éxito a la AM-FE.
7) La AM-FE informa al UE del éxito de la autentificación con el mensaje EAP-éxito. Una vez completado con éxito el proceso de intercambio de claves basado en EAP, el UE y la AM-FE comparten las claves derivadas durante el intercambio.

I.2 Ejemplo de procedimiento de reautentificación rápida

Cuando se realiza un traspaso, la reautentificación rápida puede mantener la continuidad del servicio con una baja latencia. Para la reautentificación rápida se ha de utilizar el identificador de reautentificación rápida, y no es necesario realizar el intercambio de información de autentificación entre la TAA-FE y la TUP-FE/TLM-FE.

El procedimiento general de reautentificación rápida es como se muestra a continuación.

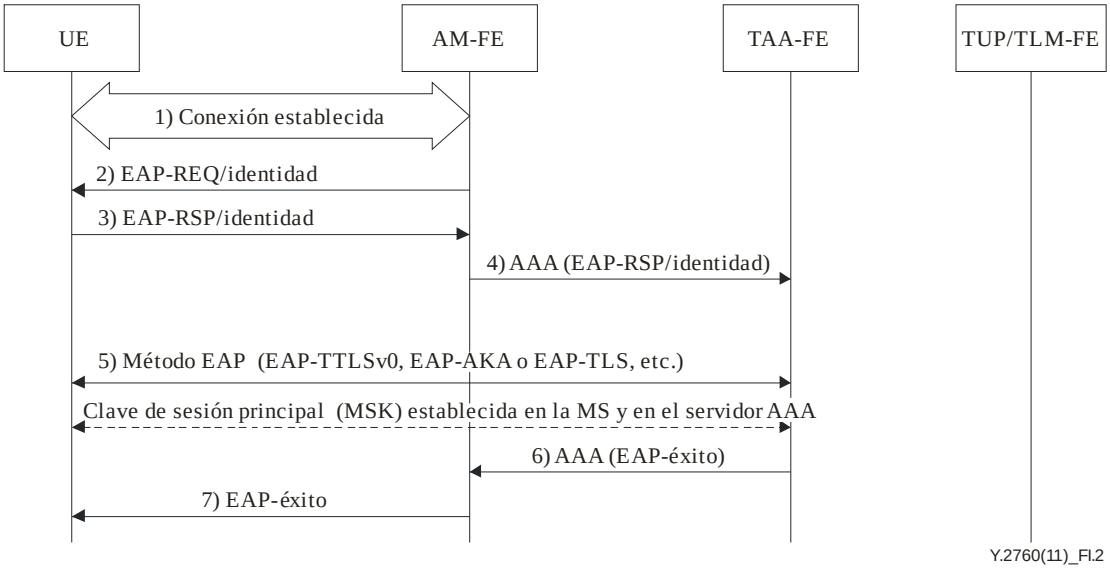

Figura I.2 – Procedimiento de reautentificación rápida

1) Se establece una conexión entre el UE y la AM-FE.
2) La AM-FE envía la EAP-REQ/Identidad al UE, que lleva el id de reautentificación.
3) El UE envía un mensaje EAP-RSP/Identidad.
4) La AM-FE remite la EAP-RSP/Identidad a la TAA-FE.
5) Se ejecuta el proceso de derivación y distribución de claves. Se pueden considerar diversos métodos, como EAP-AKA, EAP-TLS, etc.
6) La TAA-FE envía el mensaje EAP-éxito a la AM-FE.
7) La AM-FE informa al UE del éxito de la autentificación con el mensaje EAP-éxito. Una vez completado satisfactoriamente el proceso de intercambio de claves basado en EAP, el UE y la AM-FE comparten las claves derivadas durante el intercambio.

I.3 Ejemplo de movilidad del anfitrión

Para MIPv4, la seguridad de la movilidad IP se basa en las extensiones de autentificación MIP definidas en [b-IETF RFC 3344]. Se han de proteger los mensajes de señalización de movilidad IP entre el UE y el nodo que actúa como HA (es decir, la MLM-FE) utilizando extensiones de autentificación MIP y, optativamente, entre el UE y el nodo que actúa como FA (es decir, la MLM-FE).

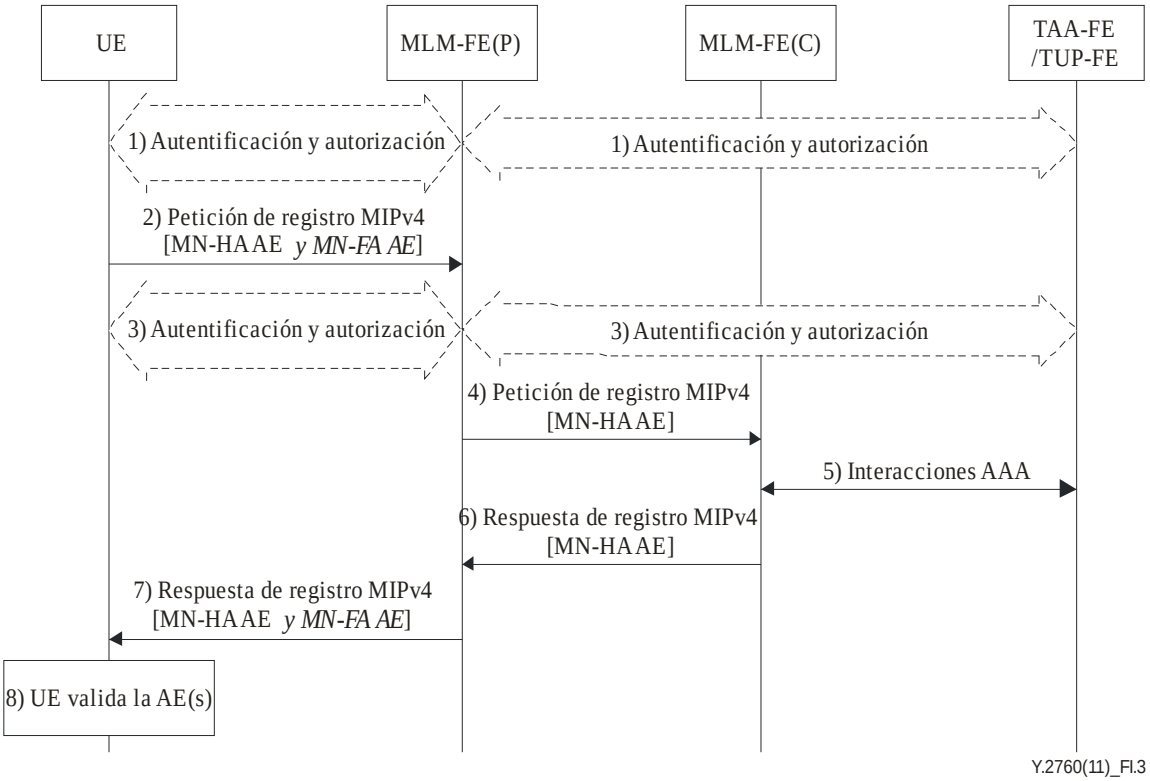

Figura I.3 – Procedimiento de inicialización MIPv4

El procedimiento de inicialización MIPv4 que se muestra en la figura I.3 es el siguiente:

1) Se realizan la autentificación y la autorización entre el UE y la MLM-FE con la ayuda de la TAA-FE /TUP-FE.

2) El UE envía una petición de registro (RRQ) a la FA (MLM-FE). El UE incluye la extensión de autentificación MN-HA (AE) y, optativamente, la extensión de autentificación MN-FA (AE), como se especifica en [b-IETF RFC 3344].

3) La RRQ desencadena el procedimiento de autentificación de acceso.

4) La FA procesa el mensaje de conformidad con [b-IETF RFC 3344] y valida la extensión de autentificación MN-FA, de haberla. La FA remite a continuación el mensaje RRQ a la HA(MLM-FE).

5) La MLM-FE seleccionada obtiene la información de autentificación y autorización de la TAA-FE /TUP-FE.

6) La MLM-FE valida la extensión de autentificación MN-HA. Una vez validada la extensión de autentificación, la MLM-FE envía una respuesta de registro (RRP) al UE a través de la FA.

7) La FA procesa la RRP de conformidad con [b-IETF RFC 3344]. A continuación, la FA remite el mensaje RRP al UE. La FA incluye la extensión de autentificación MN-FA, si la FA ha recibido la extensión de autentificación MN-FA en el mensaje RRQ.

8) El UE valida la extensión de autentificación MN-HA y la extensión de autentificación MN-FA, de haberla.

Bibliografía

[b-IETF RFC 3220] IETF RFC 3220 (2002), *IP Mobility Support for IPv4.*

[b-IETF RFC 3344] IETF RFC 3344 (2002), *IP Mobility Support for IPv4.*

[b-IETF RFC 3748] IETF RFC 3748 (2004), *Extensible Authentication Protocol (EAP).*

[b-IETF RFC 3775] IETF RFC 3775 (2004), *Mobility Support in IPv6*.

[b-IETF RFC 4555] IETF RFC 4555 (2006), *IKEv2 Mobility and Multihoming Protocol (MOBIKE).*

[b-IETF RFC 5213] IETF RFC 5213 (2008), *Proxy Mobile IPv6.*

[b-3GPP TS 33.102] 3GPP TS 33.102 V7.1.0 (2007), *3G Security: Security Architecture.*

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios generales de tarificación
Serie E	Explotación general de la red, servicio telefónico, explotación del servicio y factores humanos
Serie F	Servicios de telecomunicación no telefónicos
Serie G	Sistemas y medios de transmisión, sistemas y redes digitales
Serie H	Sistemas audiovisuales y multimedia
Serie I	Red digital de servicios integrados
Serie J	Redes de cable y transmisión de programas radiofónicos y televisivos, y de otras señales multimedia
Serie K	Protección contra las interferencias
Serie L	Construcción, instalación y protección de los cables y otros elementos de planta exterior
Serie M	Gestión de las telecomunicaciones, incluida la RGT y el mantenimiento de redes
Serie N	Mantenimiento: circuitos internacionales para transmisiones radiofónicas y de televisión
Serie O	Especificaciones de los aparatos de medida
Serie P	Terminales y métodos de evaluación subjetivos y objetivos
Serie Q	Conmutación y señalización
Serie R	Transmisión telegráfica
Serie S	Equipos terminales para servicios de telegrafía
Serie T	Terminales para servicios de telemática
Serie U	Conmutación telegráfica
Serie V	Comunicación de datos por la red telefónica
Serie X	Redes de datos, comunicaciones de sistemas abiertos y seguridad
Serie Y	**Infraestructura mundial de la información, aspectos del protocolo Internet y redes de la próxima generación**
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2012