Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

Y.2704

(01/2010)

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

Redes de la próxima generación – Seguridad

Mecanismos y procedimientos de seguridad para las NGN

Recomendación UIT-T Y.2704

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 futuras	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

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

Recomendación UIT-T Y.2704

Mecanismos y procedimientos de seguridad para las NGN

Resumen

En la Recomendación UIT-T Y.2701, *Requisitos de seguridad para las redes de la próxima generación, versión 1*, se proporcionan requisitos de seguridad en relación con las redes de la próxima generación (NGN) y sus interfaces (por ejemplo, UNI, NNI y ANI). En la Recomendación UIT-T Y.2704 se describen algunos de los mecanismos de seguridad que cabe utilizar para atender a los requisitos descritos en la Recomendación UIT-T Y.2701 y se especifica el conjunto de opciones correspondiente a cada mecanismo seleccionado. Concretamente, en la Recomendación se describe una serie de mecanismos de identificación, autentificación y autorización y, acto seguido, se pasa a examinar la seguridad de transporte para la señalización y OAMP, así como la seguridad de medios de comunicación. Ulteriormente, se exponen los mecanismos de registro de auditoría y, por último, el aprovisionamiento. Los mecanismos de seguridad descritos en esta Recomendación se basan en el modelo de confianza definido en la Recomendación UIT-T Y.2701.

La lista de mecanismos de seguridad expuestos en esta Recomendación no es exhaustiva, por lo cual se alienta a los proveedores a soportar las herramientas de seguridad, capacidades y medidas operacionales adicionales que se requieran, aparte de los mecanismos especificados en la presente Recomendación, con miras a la protección de la seguridad de las NGN.

Historia

Edición	Recomendación	Aprobación	Comisión de estudios
1.0	ITU-T Y.2704	2010-01-29	13

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.2704

Mecanismos y procedimientos de seguridad para las NGN

1 Alcance

En [UIT-T Y.2701], *Requisitos de seguridad para las redes de la próxima generación, versión 1*, se ofrecen requisitos de seguridad con respecto a las redes de la próxima generación (NGN) y sus interfaces (por ejemplo, UNI, NNI y ANI), lo que incluye un modelo de confianza. Aunque los mecanismos de seguridad seleccionados para atender a estos requisitos contendrán algunas opciones, las opciones discordantes no son deseables, ya que suelen aparejar factores de vulnerabilidad de la seguridad y dificultan el logro de la compatibilidad.

Así pues, en la Recomendación se destacan algunos importantes mecanismos de seguridad que cabe utilizar para atender a los requisitos señalados en [UIT-T Y.2701] y se especifica el conjunto de opciones que pueden utilizarse para cada mecanismo seleccionado con el fin de reducir los problemas de compatibilidad y discordancia. La lista de mecanismos descritos en esta Recomendación no es exhaustiva por lo cual se alienta a los proveedores a soportar las herramientas de seguridad, capacidades y medidas operacionales adicionales que se requieran, aparte de los mecanismos especificados en esta Recomendación con miras a la protección de la seguridad de las NGN.

El objetivo es que la presente Recomendación se utilice junto con [UIT-T Y.2701] para servir de base a la seguridad de las NGN. La Recomendación debería utilizarse junto con otras Recomendaciones relacionadas con la seguridad y, en su caso, otras especificaciones aplicables a aspectos de seguridad específicos.

NOTA – Los mecanismos de identificación y autentificación expuestos en la Recomendación forman parte de un tema más amplio, generalmente conocido con el nombre "gestión de identidad" (IdM).

1.1 Hipótesis

La Recomendación se basa en los siguientes supuestos:

1) La agregación de identidades funcionales, según se definen éstas en [UIT-T Y.2012], para constituir un solo elemento de red variará de un vendedor a otro.

2) A cada proveedor de NGN incumben responsabilidades específicas dentro de su dominio de seguridad. Así por ejemplo, la implementación de los servicios y prácticas de seguridad aplicables para garantizar: a) su propia protección, b) que la seguridad de extremo a extremo no quede comprometida dentro de su red, y c) elevada disponibilidad e integridad de las comunicaciones NGN.

3) Cada dominio de la red establecerá una serie de políticas relativas en relación con los acuerdos de nivel de servicio (SLA), y vigilará su obligado cumplimiento con el fin de garantizar la seguridad de dicho dominio y la seguridad de las interconexiones de la red. Está previsto que los SLA especifiquen los servicios, mecanismos y prácticas de seguridad que habrán de implementar para proteger las redes interconectadas y las comunicaciones (señalización/tráfico de control, tráfico de portadora y tráfico de gestión) a través de las UNI, las ANI y las NNI correspondientes.

4) En esta Recomendación se aborda la seguridad de la red, que es una arquitectura de varias capas y consiste en la seguridad de los perímetros de los dominios fiables, la seguridad física del equipo del proveedor y, posiblemente, la utilización de encriptado.

1.2 Resumen

La presente Recomendación se estructura como sigue:

- Cláusula 2 (Referencias) – En esta cláusula se presentan las referencias normativas.
- Cláusula 3 (Definiciones) – En esta cláusula se presentan las definiciones que se utilizan en esta Recomendación.
- Cláusula 4 (Abreviaturas y acrónimos) – En esta cláusula se presenta la lista de abreviaturas y acrónimos que se utilizan en esta Recomendación.
- Cláusula 5 (Convenios) – Esta cláusula se deja voluntariamente vacía.
- Cláusula 6 (Amenazas y riesgos contra la seguridad) – En esta cláusula se referencian los riesgos y amenazas contra la seguridad aplicables a las NGN.
- Cláusula 7 (Modelo de confianza en la seguridad) – En esta cláusula se proporciona un resumen del modelo de confianza definido en [UIT-T Y.2701].
- Cláusula 8 (Identificación, autentificación y autorización) – En esta cláusula se proporcionan mecanismos y medidas de seguridad de la identificación, la autentificación y la autorización.
- Cláusula 9 (Seguridad de transporte para la señalización y OAMP) – En esta cláusula se ofrecen mecanismos de encriptado de la señalización y OAMP, así como de protección de la integridad.
- Cláusula 10 (Seguridad de medios de comunicación) – En esta cláusula se proporcionan mecanismos para proteger los medios de comunicación (esto es, el tráfico de portadora).
- Cláusula 11 (OAMP) – Esta cláusula proporciona información y referencias en lo que respecta al registro de autoría, la interrogación y el registro cronológico.
- Cláusula 12 (Provisionamiento de equipo en zona no objeto de confianza) – En esta cláusula se proporciona información sobre la prestación de equipo de abonado en la zona no fiable de que se trate.
- Apéndice I – Ejemplos de garantía de la dirección de origen y de su aplicación al mecanismo de identificación y autentificación de abonado.
- Apéndice II – Seguridad de interconexión en el servicio de telecomunicaciones de emergencia (STE).
- Apéndice III – Prácticas óptimas en materia de seguridad.
- Bibliografía.

2 Referencias

Las siguientes Recomendaciones del UIT-T y otras referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de la presente Recomendación. Al efectuar esta publicación, estaban en vigor las ediciones indicadas. Todas las Recomendaciones y otras referencias son objeto de revisiones, por lo que se preconiza que los usuarios de esta Recomendación investiguen la posibilidad de aplicar las ediciones más recientes de las Recomendaciones y otras referencias citadas a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T actualmente vigentes. En esta Recomendación, la referencia a un documento, en tanto que autónomo, no otorga a éste el rango de Recomendación.

[UIT-T Y.2012] Recomendación UIT-T Y.2012 (2006), *Requisitos y arquitectura funcional de las redes de la próxima generación, versión 1*.

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

[UIT-T Y.2702] Recomendación UIT-T Y.2702 (2008), *Requisitos de autenticación y autorización de las redes de la próxima generación, versión 1*.

[UIT-T Y.2703] Recomendación UIT-T Y.2703 (2009), *Aplicación del servicio de autenticación, autorización y contabilidad a las redes de la próxima generación*.

[UIT-T Y.2720] Recomendación UIT-T Y.2720 (2009), *Marco general para la gestión de identidades en las redes de la próxima generación*.

[UIT-T X.509] Recomendación UIT-T X.509 (2008) | ISO/CEI 9594-8:2008, *Tecnología de la información – Interconexión de sistemas abiertos – El Directorio: Marcos para certificados de claves públicas y atributos*.

[UIT-T X.660] Recomendación UIT-T X.660 (2008) | ISO/CEI 9834-1:2008, *Tecnología de la información – Interconexión de sistemas abiertos – Procedimientos para la operación de autoridades de registro para interconexión y sistemas abiertos: Procedimientos generales y arcos superiores del árbol de identificadores de objeto de ASN.1*.

[UIT-T X.1035] Recomendación UIT-T X.1035 (2007), *Protocolo de intercambio de claves con autentificación mediante contraseña*.

[IETF RFC 4302] IETF RFC 4302 (2005), *IP Authentication Header*.

[IETF RFC 4303] IETF RFC 4303 (2005), *IP Encapsulating Security Payload (ESP)*.

[IETF RFC 5246] IETF RFC 5246 (2008), *The Transport Layer Security (TLS) Protocol Version 1.2*.

3 Definiciones

3.1 Términos definidos en otros documentos

En esta Recomendación se utilizan los siguientes términos definidos en otros documentos.

3.1.1 activo [UIT-T Y.2701]: Cualquier elemento de valor para la organización, sus actividades económicas, funcionamiento y continuidad.

3.1.2 elemento frontera [UIT-T Y.2701]: Elemento de red cuya función consiste en la conexión de diversos dominios de seguridad y administrativos.

3.1.3 red institucional [UIT-T Y.2701]: Red privada que admite numerosos usuarios y que puede estar situada en diversos lugares (por ejemplo, una empresa, una ciudad universitaria).

3.1.4 elemento frontera de dominio [UIT-T Y.2701]: Elemento frontera bajo el control exclusivo del proveedor que proporciona funciones de seguridad con otros dominios de red.

3.1.5 servicio de telecomunicaciones de emergencia [STE] [b-UIT-T E.107]: Servicio nacional que proporciona telecomunicaciones prioritarias a los usuarios del STE autorizados en situaciones de catástrofe y emergencia.

3.1.6 elemento frontera de red [UIT-T Y.2701]: Elemento frontera bajo el control exclusivo del proveedor de servicios que proporciona funciones de seguridad con equipos terminales.

3.1.7 dominio de seguridad [UIT-T Y.2701]: Conjunto de elementos, política de seguridad, autoridad de seguridad y conjunto de actividades relativas a la seguridad donde los elementos se gestionan de conformidad con la política de seguridad. La política estará administrada por la autoridad de seguridad. Un dominio de seguridad determinado puede abarcar múltiples zonas de seguridad.

3.1.8 testigo de seguridad [b-UIT-T X.810]: Conjunto de datos protegido por uno o más servicios de seguridad, junto con la información de seguridad utilizada para el aprovisionamiento de estos servicios de seguridad, que se transfiere entre entidades comunicantes.

3.1.9 zona de seguridad [UIT-T Y.2701]: En esta Recomendación se definen tres zonas de seguridad: 1) fiable; 2) fiable pero vulnerable; y 3) no fiable. Una zona de seguridad se define por el control operativo, la ubicación y la conectividad con otros elementos de red/dispositivos.

3.1.10 elemento frontera de equipo terminal [UIT-T Y.2701]: Elemento frontera que proporciona funciones de seguridad entre el equipo situado en los locales del cliente y la red del proveedor de servicios.

3.1.11 confianza [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.

3.1.12 zona fiable pero vulnerable [UIT-T Y.2701]: Desde el punto de vista de un proveedor de NGN, zona de seguridad donde el proveedor de las NGN explota los elementos/dispositivos de red (configuración y mantenimiento). El equipo puede estar bajo control del cliente/abonado o del proveedor de la NGN. Además, el equipo puede estar ubicado dentro o fuera del dominio del proveedor de la NGN. La comunicación se establece con elementos tanto de la zona fiable como con elementos de la zona no fiable, por lo que se considera "vulnerable". La principal función de seguridad consiste en proteger los elementos de red de la zona fiable de los ataques de seguridad cuyo origen se encuentra en la zona no fiable de manera infalible.

3.1.13 zona fiable [UIT-T Y.2701]: Desde el punto de vista de un proveedor de NGN, dominio de seguridad donde se encuentran los elementos y sistemas de la red del proveedor de la NGN que nunca comunican directamente con los equipos del cliente. Las características comunes de los elementos de la red NGN en este dominio que están bajo control del proveedor de las NGN correspondiente, están ubicadas en los locales de dicho proveedor (lo que proporciona seguridad física), y establecen comunicación únicamente con elementos del dominio "fiable" y con elementos del dominio "fiable pero vulnerable".

3.1.14 zona no fiable [UIT-T Y-2701]: Desde el punto de vista de un proveedor de NGN, zona que incluye todos los elementos de red de las redes de cliente o, posiblemente, redes pares u otras zonas del proveedor fuera del dominio original, conectados a los elementos frontera del proveedor de NGN.

3.1.15 usuario [b-UIT-T Y.2091]: Un usuario final, una persona, un abonado, un sistema, un equipo terminal (FAX, PC, etc.), una entidad (funcional), un proceso, una aplicación, un proveedor o una red de una institución.

3.1.16 red de usuario [UIT-T Y.2701]: Red privada constituida por un equipo terminal que pueden utilizar numerosos usuarios.

3.2 Términos definidos en esta Recomendación

En esta Recomendación se utilizan los siguientes términos:

3.2.1 autentificador: Se trata de un elemento de red que facilita la identificación y la autentificación de abonados, dispositivos o usuarios finales. Así por ejemplo, los elementos frontera con funcionalidad B2BUA o P-CSCF-FE pueden ser autentificadores de abonados para servicios basados en SIP.

4 Abreviaturas y acrónimos

En esta Recomendación se utilizan las siguientes abreviaturas y acrónimos.

3G	Tercera generación (*3rd generation*)
AGW	Pasarela de acceso (*access gateway*)
AH	Encabezador de autentificación (*authentication header*)
AKA	Acuerdo de autentificación y clave (*authentication and key agreement*)
ANI	Interfaz aplicación-red (*application-to-network interface*)
AS/WS	Servidor de aplicaciones/servidor de web (*application server/web server*)
AuC	Centro de autentificación (*authentication center*)
B2BUA	Agente de usuario de extremo a extremo (*back-to-back user agent*)
BE	Elemento frontera (*border element*)
BSR	Encaminador de la estación de base (*base station router*)
CA	Autoridad de certificación (*certificate authority*)
COPS	Servicio de política abierta común (*common open policy service*)
CRL	Lista de revocación de certificados (*certificate revocation list*)
CSC-FE	Entidad funcional de control de sesión de llamada (*call session control functional entity*)
DBE	Elemento frontera de dominio (*domain border element*)
DNS	Sistema de nombre de dominio (*domain name system*)
DoS	Denegación del servicio (*denial of service*)
DTMF	Multifrecuencia bitonal (*dual-tone multi-frequency*)
ECC	Criptografía de curva elíptica (*elliptic curve cryptography (ECC)*)
ESP	Protocolo de seguridad encapsulado (*encapsulating security protocol*)
FE	Entidad funcional (*functional entity*)
GBA	Arquitectura de inicialización genérica (*generic bootstrapping architecture*)
GW	Pasarela (*gateway*)
HMAC	Código de autentificación de mensajes mediante troceo con clave (*hash message authentication code*)
HTTP	Protocolo de transferencia de hipertextos (*hypertext transfer protocol*)
I-CSC-FE	Entidad funcional de control de sesión de llamada interrogante (*interrogating call session control functional entity*)
ID	Identidad (*identity*)
IdM	Gestión de identidad (*identity management*)
IDPS	Sistemas de detección y prevención de intrusiones (*intrusion detection and prevention systems*)
IDS	Sistema de detección de intrusiones (*intrusion detection systems*)
IKE	Intercambio de claves Internet (*internet key exchange*)
IMS	Subsistema de multimedios IP (*IP multimedia subsystem*)

IP	Protocolo Internet (*Internet Protocol*)
LAN	Red de área local (*local area network*)
MD5	Mensaje digest 5 (*message digest* 5)
MIB	Base de información de gestión (*management information base*)
MPLS	Conmutación para etiquetas multiprotocolo (*multi protocol label switching)*
MRP-FE	Entidad funcional de procesamiento de recurso de medios (*media resource processing functional entity*)
MS	Estación móvil (*mobile station*)
NAC-FE	Entidad funcional de control de acceso de red (*network access control functional entity*)
NAPT	Dirección de red y translación de puertos (*network address and port translation*)
NAT	Translación de direcciones de red (*network address translation*)
NBE	Elemento frontera de red (*network border element*)
NE	Elemento de red (*network element*)
NGN	Red de próxima generación (*next generation network*)
NNI	Interfaz red-red (*network-to-network interface*)
OAMP	Operaciones, administración, mantenimiento y configuración (*operations, administration, maintenance and provisioning*)
OID	Identificador de objeto (*object identifier*)
ONU	Unidades de red óptica (*optical network units*)
PAK	Clave autentificada de contraseña (*password authenticated key*)
P-CSC-FE	Entidad funcional de control de sesión de llamada intermediaria (*proxy call session control functional entity*)
POTS	Servicio telefónico tradicional (*plain old telephone service*)
QoS	Calidad de servicio (*quality of service*)
RAC-FE	Entidad funcional de control de recursos y admisión (*resource and admission control functional entity*)
RADIUS	Servicio de autentificación a distancia mediante marcación de usuario (*remote authentication dial in user service*)
RAN	Red de acceso radioeléctrico (*radio access network*)
RDSI	Red digital de servicios integrados
RTPC	Red telefónica pública conmutada (*public switch telephone network*)
RTSP	Protocolo de trenes en tiempo real (*real time streaming protocol*)
SAA-FE	Entidad funcional de autentificación y autorización de servicio (*service authentication and authorization functional entity*)
SASL	Capa de autentificación y seguridad simple (*simple authentication and security layer*)
S-CSC-FE	Entidad funcional de control de sesión de llamada servidora (*serving call session control functional entity*)

SDP Protocolo de descripción de sesión (*session description protocol*)

SIM Módulo de identidad de abonado (*subscriber identity module*)

SIP Protocolo de iniciación de sesión (*session initiation protocol*)

SLA Acuerdo de nivel de servicio (*service level agreement*)

SL-FE Entidad funcional de localizador de suscripción (*subscription locator functional entity*)

SNMP Protocolo de gestión de red simple (*simple network management protocol*)

SRTP Protocolo seguro en tiempo real (*secure real time protocol*)

STE Servicio de telecomunicaciones de emergencia

TAA-FE Entidad funcional de autentificación y autorización de transporte (*transport authentication and authorization functional entity*)

TCP Protocolo de control de transmisión (*transmission control protocol*)

TE Equipo terminal (*terminal equipment*)

TE-BE Elemento frontera de equipo terminal (*terminal equipment border element*)

TLS Seguridad de capa de transporte (*transport layer security*)

TMN Red de gestión de telecomunicaciones (*telecommunications management network*)

TRIP Encaminamiento de telefonía con IP (*telephony routing over IP*)

UA Agente de usuario (*user agent*)

UDP Protocolo de datagramas de usuario (*user datagram protocol*)

UE Equipo de usuario (*user equipment*)

UICC Tarjeta de circuito integrado universal (*universal integrated circuit card*)

UMTS Sistema universal de telecomunicaciones móviles (*universal mobile telecommunications system*)

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

URL Localizador de recursos uniforme (*uniform resource locator*)

USIM Módulo de identidad de abonado universal (*universal subscriber identity module*)

VLAN LAN virtual (*virtual LAN*)

VPN Red privada virtual (*virtual private network*)

WLAN LAN inalámbrica (*wireless LAN*)

xDSL Línea de abonado digital x (*x digital subscriber line*)

5 Convenios

Ninguno.

6 Riesgos y amenazas en materia de seguridad

Tratándose de los riesgos y amenazas contra la seguridad que se ha previsto puedan plantearse en un entorno NGN, véase la cláusula 4 en [UIT-T Y.2701].

7 Modelo de confianza en la seguridad

La elección de los mecanismos de seguridad por parte del proveedor NGN depende del modelo de confianza aplicable. En esta Recomendación se parte del supuesto de que se utilizará el modelo de confianza definido en [UIT-T Y.2701]. Esta cláusula constituye un resumen del modelo de confianza en la seguridad de las NGN definido en [UIT-T Y.2701].

La arquitectura de referencia funcional NGN define entidades funcionales (FE). Con todo, como los aspectos de seguridad de la red dependen en gran medida de la forma en que aúnen físicamente las FE, la arquitectura de seguridad de las NGN se basa en los elementos de red (NE) físicos, esto es, cajas tangibles que contienen una o más FE. La forma en que se agregan estas FE para constituir NE difiere de un vendedor a otro y de un proveedor NGN a otro.

7.1 Modelo único de confianza en la red

En esta cláusula se definen tres zonas de seguridad:

1) fiable;

2) fiable pero vulnerable;

3) no fiable,

que dependen del control operacional, la ubicación y la conectividad respecto de otros dispositivos/elementos de red. Estas tres zonas se ilustran en el modelo de confianza en la seguridad representado en la figura 1.

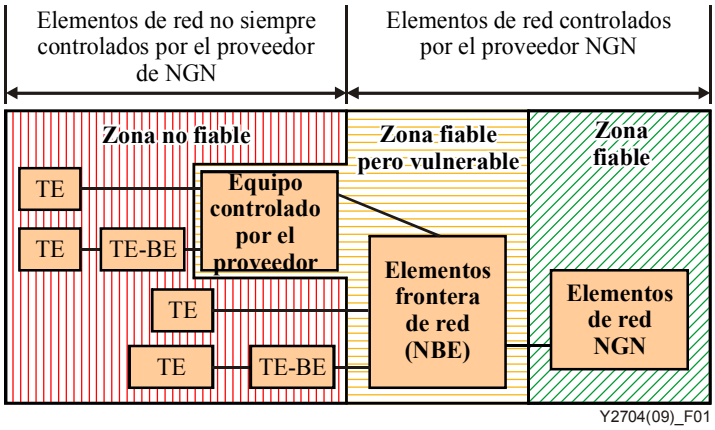


Figura 1 – Modelo de confianza en la seguridad [UIT-T Y.2701]

Una "zona de seguridad de la red fiable" o, en forma resumida, "zona fiable", es una zona donde los elementos de red y sistemas de un proveedor NGN residen y no comunican en ningún caso directamente con el equipo de cliente u otros dominios. Las características comunes de los elementos de red NGN situados en esta zona son las siguientes:

1) estos elementos son controlados íntegramente por el proveedor de NGN (para la configuración, el mantenimiento y el control operativo);

2) están situados en el dominio de este proveedor; y

3) comunican únicamente con otros elementos de la zona "fiable" y con elementos de la zona "fiable pero vulnerable".

No ha de asumirse que un elemento de red es intrínsecamente seguro por encontrarse en una zona fiable.

Los elementos de red en la "zona fiable" estarán protegidos por un conjunto de métodos. En este sentido, cabe dar algunos ejemplos: la seguridad física de los elementos de la red NGN, el fortalecimiento general de los sistemas, la utilización de señalización segura, y la seguridad de mensajes de gestión y la utilización de diversas VPN dentro de la red (MPLS/)IP. Se supone que se utilizará el mismo conjunto de métodos para la comunicación en la zona "fiable" y entre los elementos de red NGN en la zona "fiable" y los de la "fiable pero vulnerable".

Una "zona de seguridad fiable pero vulnerable" o, resumiendo, "zona fiable pero vulnerable", es una zona donde los elementos/dispositivos de red comunican con los elementos de la "zona no fiable", razón por la cual son "vulnerables". Además, se comunican con los elementos de la zona "fiable". Al igual que los elementos de red de la zona "fiable", el equipo puede encontrarse bajo el control del proveedor NGN, aunque puede estar situado dentro o fuera de los locales del proveedor NGN. La principal función de seguridad es proteger a los NE en la zona fiable frente a los ataques contra la seguridad que se originan en la zona no fiable. La combinación de métodos aplicados para asegurar la comunicación entre elementos de red NGN en la zona "fiable pero vulnerable" y la zona "no fiable" pueden diferir de los utilizados para la zona "fiable".

Se llama "elementos frontera de red" (NBE) a los elementos localizados en el dominio del proveedor NGN dotados de conectividad con los elementos fuera de la zona fiable. A este respecto, cabe dar algunos ejemplos:

- Elementos frontera de red (NBE) en la UNI que sirven de interfaz a los elementos de control de servicio o transporte del proveedor NGN en la zona fiable para proporcionar al usuario/abonado acceso a la red del proveedor NGN con propósitos de servicio y/o transporte.
- Elemento frontera de dominio (DBE), que es el mismo tipo de equipo que el elemento frontera de red, salvo que reside en la frontera entre dos dominios.
- Dispositivo de configuración y de arranque del NBE (DCB-NBE) que sirve de interfaz con el sistema de configuración de dispositivos del proveedor NGN en la zona fiable para configurar el dispositivo de usuario/abonado y el equipo de proveedor NGN situado en la planta externa.
- Interfaces OAMP-NBE con los sistemas OAMP del proveedor NGN en la zona fiable, para configurar y mantener el dispositivo de usuario/abonado y el equipo del proveedor NGN situado en la planta externa.
- Servidor de aplicaciones/servidor web NBE (AS/WS-NBE) que hace las veces de interfaz con AS/WS-NBE en la zona fiable, para proporcionar acceso de usuario/abonado basado en servicios a la web.

En la figura 1 pueden verse las relaciones existentes entre estos NBE y los NE que deben protegerse.

Entre los ejemplos de dispositivos/elementos explotados por un operador NGN pero no situados en los locales del proveedor NGN, y que pueden o no encontrarse bajo el control del proveedor NGN se consignan aquí los siguientes:

- equipo de planta externa en la red/tecnología de acceso;
- encaminador de estación de base (BSR, *base station router*), elemento de red que integra la estación de base, el controlador de la red radioeléctrica y las funcionalidades de encaminador para el acceso inalámbrico;
- unidades de red ópticas (ONU, *optical network units*) situadas en la residencia del usuario/abonado.

La zona "fiable pero vulnerable", que abarca los NBE, quedará protegida por una serie de diferentes métodos. En ese sentido, cabe citar la seguridad física de los elementos de red NGN, el fortalecimiento general de los sistemas, la utilización de señalización segura para todos los mensajes de señalización enviados a elementos de red NGN en la zona "fiable" y la seguridad de mensajes OAMP y filtros de paquetes y cortafuegos. Una "zona no fiable" incluye todos los elementos de red de las redes del cliente o, posiblemente, de las redes entre pares u otros dominios del proveedor NGN, que se conectan a los elementos frontera de la red del proveedor de NGN. Puede darse el caso de que en la "zona no fiable", que abarca el equipo terminal el equipo no se encuentre bajo el control de los proveedores de NGN y de que resulte imposible imponer al usuario la política de seguridad del proveedor NGN. Ahora bien, convendría procurar aplicar algunas medidas de seguridad y, a dicho efecto, se recomienda garantizar la seguridad de la señalización, los medios y OAMP, y fortalecer el TE-BE situado en la "zona no fiable". Sin embargo, debido a la comunicación con elementos de red de la zona "no fiable", la seguridad es inferior a la de la zona "fiable".

7.2 Modelo de confianza en redes entre pares

Cuando el NGN se conecta a otra red, la presencia o ausencia de confianza dependerá de:

- la interconexión física, en cuyo marco la interconexión puede ir de una conexión directa en un edificio seguro a una conexión entre distintos edificios (posiblemente sin seguridad) mediante instalaciones compartidas;
- modelo entre pares, en cuyo marco el tráfico puede intercambiarse directamente entre dos operadores de servicio NGN o a través de uno o más proveedores de transporte NGN;
- relaciones de negocio entre redes, en cuyo marco pueden especificarse cláusulas de penalidad en los SLA, y/o definir el grado de confianza en que se garantice la política de seguridad de otros proveedores NGN; en general, los proveedores NGN deberían considerar no fiables a otros proveedores,

En la figura 2 puede verse un ejemplo según el cual se estima no fiable una red conectada.

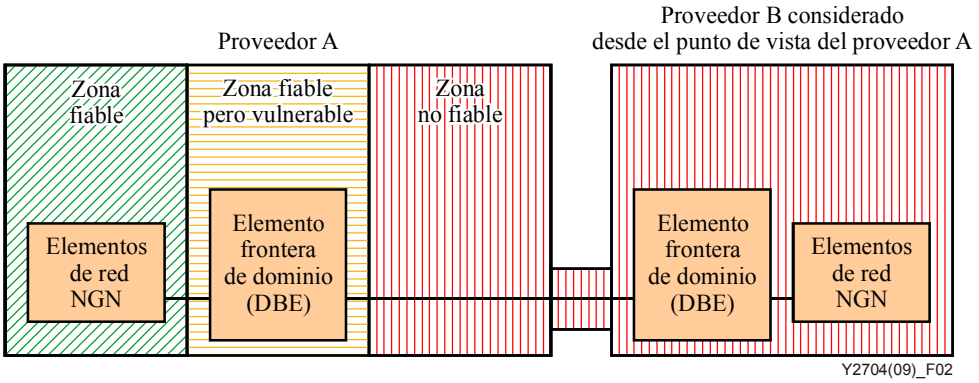


Figura 2 – Modelo de confianza entre pares [UIT-T Y.2701]

8 Identificación, autentificación y autorización

Se remite aquí a [UIT-T Y.2701], [UIT-T Y.2702], [UIT-T Y.2703] y [UIT-T Y.2720], con propósitos de información sobre la identificación, autentificación, autorización y gestión de identidad (IdM).

En esta cláusula se describen los mecanismos de identificación, autentificación y autorización, en particular, aquellos que interesan a los servicios basados en el SIP. Los mecanismos que conciernen a otros servicios quedan para ulterior estudio.

8.1 Abonados

Toda petición de servicio NGN es formulada por un abonado, debido a lo cual sirve para identificar a éste. Dependiendo del SLA existente entre el proveedor NGN y el abonado, puede ser necesario proceder a una mayor identificación (y a la autentificación conexa) del usuario final.

Esto puede lograrse utilizando un elemento funcional que facilita la identificación y autentificación de abonados, dispositivos y usuarios finales (denominado autentificador). Así por ejemplo, los elementos frontera de red (NBE) con funcionalidad de agente usuario de extremo a extremo (B2BUA) o P-CSC-FE pueden ser autentificadores de abonados, tratándose de servicios basados en el SIP. La identificación y autentificación se lleva a cabo mediante el intercambio y la validación de credenciales entre el autentificador y el TE.

8.2 Elemento de red

En [UIT-T Y.2701] se recomienda identificar y autentificar elementos de red para las comunicaciones.

Si el elemento frontera recibe una petición de un elemento de red NGN en la zona fiable, la identificación contenida en la petición puede considerarse exacta y no verificarse ulteriormente, a reserva de la política de seguridad del proveedor NGN.

Si el elemento frontera recibe peticiones de elementos de red en la zona no fiable o en la zona fiable pero vulnerable, se recomienda que los elementos de red se identifiquen y autentifiquen y que se verifiquen los privilegios de comunicación. La identificación y la autentificación se efectúan intercambiando y validando credenciales entre el autentificador y el NE.

8.3 Utilización de credenciales en el marco de la seguridad de las NGN

En el ámbito de la seguridad NGN se utilizan credenciales para identificar y autentificar dispositivos, abonados y/o usuarios finales. Las credenciales destinadas a identificar y autentificar un dispositivo, un abonado y/o un usuario extremo se describen en la cláusula 8.3.1. Estas credenciales pueden adoptar una de dos formas distintas, sea certificados de clave pública X.509 (descritos en la cláusula 8.3.2) o una clave compartida, que se analiza en la cláusula 8.3.3. El certificado de clave pública X.509 puede utilizarse para establecer un transporte seguro entre el TE y el autentificador (según se describe en la cláusula 8.3.1), basándose en la política del proveedor NGN. La clave compartida puede utilizarse sea para establecer un transporte seguro, o al generar/verificar la respuesta a una puesta a prueba iniciada por el autentificador (descrita en la cláusula 8.3.1), basándose en la política del proveedor de NGN.

8.3.1 Credenciales de dispositivo, abonado y usuario final

En las NGN se utilizan tres distintos tipos de credenciales:

1) credenciales de dispositivo;
2) credenciales de abonado;
3) credenciales de usuario final.

El fabricante de un dispositivo puede acompañar éste con las credenciales del caso. Así por ejemplo, durante la fabricación del dispositivo, el fabricante puede acreditar el dispositivo con credenciales "codificadas", credenciales que incluyen información sobre asuntos tales como el número de serie del dispositivo o el fabricante. Las credenciales de un dispositivo identifican a éste. Un proveedor NGN puede asociar credenciales de un dispositivo con un determinado servicio de abonado para obviar la necesidad de presentar credenciales de abonado. En tales casos, las peticiones del dispositivo pueden asociarse con una determinada cuenta basada en la política del proveedor de NGN.

Las credenciales de abonado se utilizan para asociar el originador de una petición NGN con una determinada cuenta. Las credenciales de abonado se registran (por ejemplo, mediante descarga y SIM) en los dispositivos capaces de aceptar tales credenciales. Las credenciales de abonado instaladas en un dispositivo asocian al abonado con dicho dispositivo. Todas las llamadas efectuadas a partir del dispositivo se asociarán con el abonado y las credenciales que se hayan instalado en el dispositivo. Es posible instalar varios conjuntos de credenciales en un solo dispositivo, en cuyo caso el dispositivo sirve para distinguir entre las peticiones asociadas con cada abonado.

NOTA – Los clientes de una NGN pueden contar o no con uno o más abonos a la NGN asociados con varios o ningún dispositivo. Asimismo, el abono a la NGN puede asociarse con uno o más usuarios finales (lo que quiere decir que el usuario final no es necesariamente el abonado), que pueden utilizar diferentes dispositivos o compartir el mismo, basándose en la política del proveedor de NGN.

Las credenciales de usuario final se utilizan para identificar y autentificar a usuarios finales específicos de la red. Así por ejemplo, una tarjeta SIM puede identificar al usuario final; en efecto cuando el usuario final mete en el teléfono su tarjeta SIM, se asocia dicha tarjeta con el usuario final (y todas las llamadas se identifican como llamadas procedentes de dicho usuario). En este contexto, otro ejemplo que cabe dar también son los testigos de seguridad y los testigos de equipo (dispositivos físicos) o de soporte lógico (programas instalados en dispositivos universales, por ejemplo, computadores personales). Este tipo de testigos se proporcionan a un usuario autorizado para ampliar el proceso de autentificación. Un testigo de seguridad puede almacenar claves criptográficas, por ejemplo, una firma digital o datos biométricos, tales como huellas digitales. Una petición que tiene origen en un dispositivo NGN se identificará y autentificará para cerciorarse de que procede del usuario final asociado con ese testigo de seguridad. En ciertos casos (por ejemplo, en el caso de la tarjeta SIM anterior), cabe la posibilidad de que varios usuarios finales utilicen el servicio asociado con un solo abonado (esto es, una cuenta de abonado), y las llamadas originadas por el usuario final se cargan a la cuenta del abonado. El abonado y el usuario final pueden ser la misma entidad, pero también puede haber un gran número de usuarios finales por abonado. Los usuarios finales pueden identificarse y autentificarse por sí mismos en relación con la red, para aprovechar servicios personales. Es posible establecer asociaciones de seguridad en la capa de transporte individual, utilizando credenciales de usuario final entre el TE y la red NGN (autentificadores). El proveedor NGN asocia las credenciales de usuario final con el servicio de abonado de que se trate con propósitos de facturación.

8.3.2 Utilización como credenciales de certificados de clave pública X.509

Un certificado de clave pública X.509 es un documento digital que incluye un identificador de identidad, sus atributos, una clave pública que pertenece a dicha entidad e información de autentificación de otro tipo (por ejemplo, información sobre el expedidor del certificado, la lista de revocación de certificado (CRL), y los plazos de la validez del certificado). En el cuadro 1 se describen algunos de los campos básicos y los campos de extensión de un certificado de clave pública X.509. La descripción detallada de los campos del certificado de clave pública X.509 puede consultarse en [UIT-T X.509]. Los certificados de clave pública son firmados digitalmente por terceras partes fiables, partes que por regla general se denominan autoridades de certificación CA) de los certificados de clave pública. Una CA computa el resultado de troceo (por ejemplo, utilizando SHA-1) de todos los campos, excepto del *campo de valor de la firma*, lo encripta con su propia clave privada y, acto seguido, agrega la firma junto con el algoritmo de firma aplicado al certificado (en el *campo de valor de la firma*).

Cuadro 1 – Algunos campos básicos de un certificado de clave pública X.509

Nombre del campo	Descripción
Asunto	Identifica la entidad asociada con el certificado de clave pública (el nombre de directorio distinguido del titular del certificado)
Número de serie	Identificador único del certificado
Entidad de expedición	Identifica la entidad que firma y expide el certificado (el nombre de directorio distinguido de la CA)
Válido a partir de	Fecha y hora de inicio de la validez del certificado
Válido hasta	Fecha y hora del término de la validez del certificado
Clave pública	Clave pública del titular del certificado
Versión	Versión del certificado de clave pública X.509 codificado
Nombre alternativo del asunto	Otro identificador del titular del certificado
Puntos de distribución de CRL	Nombre o dirección del punto de distribución de CRL
Autoridad de acceso a la información	Nombre o dirección para acceder a la información acerca de la CA
Utilización de clave ampliada	Descripción de los propósitos para los cuales puede utilizarse el certificado (lista de identificadores de objetos definidos (OID) de UIT-T | ISO/CEI) [UIT-T X.660]
Políticas de aplicación	Aplicación y servicios que puede utilizar el certificado (especificados por el identificador de objetos)
Políticas de certificación	Políticas y mecanismos utilizados por la CA para la recepción de peticiones de tramitación, autorización, expedición y gestión de certificados
Algoritmo de la firma	Algoritmo identificador del algoritmo y la función de troceado utilizados por la CA para firmar el certificado (por ejemplo, SHA-1 con RSA)
Valor de la firma	La firma del certificado

Los elementos de red NGN pueden utilizar los certificados de clave pública especificados en [UIT-T X509] para establecer asociaciones de seguridad con otros elementos de red, y proporcionar así la base de una mutua identificación y autentificación. El TE y el autentificador pueden utilizar estos certificados entre sí con idéntica finalidad.

Tratándose de un certificado de abonado o de usuario final, el <identificador de cuenta de abonado> (véase la cláusula 8.4.2), el identificador que sirve para extraer información de la cuenta del abonado, es utilizado por el autentificador con el fin de obtener mayor información acerca de las credenciales a través de las SAA/TAA-FE. En el caso de un certificado de dispositivo, el autentificador utiliza el nombre del fabricante del dispositivo y del número de serie de dicho dispositivo para determinar el <identificador de cuenta de abonados asociado> (que será únicamente válido si el dispositivo se encuentra asociado con un abonado) y, acto seguido, se emplea el <identificador de cuenta de abonado> como se ha visto antes a fin de obtener información sobre las credenciales a través de las SAA/TAA-FE.

Los certificados de usuario final, de servicio y de dispositivo pueden utilizarse para crear conexiones TLS entre el dispositivo y el autentificador (cláusula 9.1.2), o para crear conexiones IPsec mediante autentificación IKE (cláusula 9.2.4.3).

8.3.3 Claves compartidas como credenciales

Una clave compartida puede emplearse para mejorar la seguridad del acceso a la NGN. En tal caso, se proporciona al abonado o usuario final copia de la clave compartida, y se almacena otra copia en las correspondientes entidades funcionales, por ejemplo, las entidades funcionales de perfil de usuario de servicio (SUP-FE) o las entidades funcionales de perfil de usuario de transporte (TUP-FE). Todas las claves deben contar con un solo nombre y el autentificador se sirve de ese nombre para obtener más información acerca de las credenciales.

Cuando se utilizan claves precompartidas, el grado de inmunidad del sistema depende del que tenga el secreto compartido. La idea es garantizar que el secreto compartido no sea el eslabón débil de la cadena de seguridad. Esto hace necesario que el secreto compartido contenga tanta entropía (aleatoriedad) como la cifra utilizada. Dicho de otro modo, se recomienda que el secreto compartido tenga al menos una entropía de 128-160 bits.

Cabe señalar que el método de claves simétricas difiere en ciertos aspectos del método de claves asimétricas descrito en la cláusula 8.3.2, y que se ha de tener en cuenta lo siguiente:

– una entidad ha de disponer de un conjunto de claves simétricas distinto para cada parte comunicante;
– las claves se han de configurar, crear y almacenar de manera segura;
– una entidad debe confiar en que su comunicante mantendrá en secreto la clave compartida.

8.3.4 Información suministrada en las SUP/TUP-FE para cada conjunto de credenciales

Las SUP/TUP-FE son los depósitos de todas las credenciales de dispositivo, abonado y usuario final que cabe utilizar para acceder a la infraestructura NGN. Estas FE se implementan normalmente como parte integral del autentificador para optimizar el tratamiento de las peticiones de autentificación. Con todo, para soportar movilidad, puede resultar necesario que el autentificador consulte a un servidor distante SAA/TAA-FE para obtener información acerca de las credenciales. El identificador de cuenta de abonado o el nombre de clave se utilizan para extraer información por conducto de las SAA/TAA-FE.

Es preciso prestar en las FE, por ejemplo las SUP/TUP-FE que almacenan las credenciales, la siguiente información de seguridad sobre cada conjunto de credencial:

1) el identificador de cuenta de abonado o el nombre de clave;
2) si se requiere identificación y autentificación de usuario final para este abonado;
3) si dichas credenciales describen a un abonado o a un usuario final; y
4) los valores permisibles del encabezador "De" de las peticiones.

A continuación, se ofrecen algunos ejemplos acerca de la información almacenada en los depósitos de credenciales; entre otros, las SUP/TUP-FE.

Tratándose de un certificado de dispositivo TE NGN que tramita cuatro líneas de telefonía tradicional, con números 212-555-1111-1113 y 1151:

Cuenta de abonado:	123-456789
A partir de los encabezadores::	sip:212-555-111[1-3]@NGN .ngn.com
	| sip:212-555-1151@NGN .ngn.com
Cadena de identidad:	sip:212-555-1111@NGN .ngn.com
Tipo de credenciales:	abonado
Identidad de usuario final requerida:	no

Tratándose de un certificado de abonado asignado a la familia de John Doe:

Cuenta de abonado:	Familia Doe
De los encabezadores:	sip:*Doe@NGN .ngn.com
Cadena de identidad:	sip:Doe@NGN .ngn.com
Tipo de credenciales:	abonado
ID de usuario final requerida:	no

Tratándose de una clave precompartida asignada a la familia de John Doe:

Nombre de la clave:	JohnDoe
Clave:	dfe56131d1958046689d83306477ecc
De los encabezadores:	sip:*Doe@NGN .ngn.com
Cadena de identidad:	sip: Doe@NGN .ngn.com
Tipo de credenciales:	abonado
ID de usuario final requerida:	no

Tratándose de un TE-BE que presta servicio a la empresa Acme Widget:

Cuenta de abonado:	Empresa Acme Widget
De los encabezadores:	sip:*@acme.com
Cadena de identidad:	sip:acme.com
Tipo de credenciales:	abonado
ID de usuario final requerida:	no

Tratándose de un usuario final situado en la empresa Acme Widget:

Cuenta de abonado:	Empresa Acme Widget
De los encabezadores:	sip:bob@acme.com
Cadena de identidad:	sip:bob@acme.com
Tipo de credenciales:	usuario final

8.4 Identificación y autentificación de abonado

8.4.1 Estrategia general

La identidad del originador en el SIP está contenida normalmente en el encabezador "De". Con todo, la identificación del abonado gracias a la utilización del encabezador "De" en una petición SIP puede ser objeto de ataques de usurpación de identidad (*spoofing*), por lo cual no se utiliza cuando se requiere un mayor nivel de garantía de la identidad del abonado. Se procede pues, de otro modo, esto es, comparando el valor del encabezador "De" con la identidad del abonado obtenida por otros medios.

Para reducir al mínimo los efectos sobre el retardo del establecimiento de la llamada, la identificación y autentificación del abonado se obtiene a partir de la dirección de origen de red (dirección de origen que figura en el encabezador del paquete IP) o de la asociación de seguridad de transporte (asociación que establece, por ejemplo, entre otros, IPsec o TLS, entre el dispositivo de originación y el autentificador), siempre que ello es posible. Cuando estas técnicas no permiten obtener una identificación que sea coherente con el encabezador "De" que figura en la petición SIP, se expide al originador una puesta a prueba y si la correspondiente respuesta contiene las

credenciales adecuadas, se seguirá adelante con la petición. En las siguientes cláusulas se proporciona información más detallada sobre estos procedimientos.

Los procedimientos consignados en la cláusula 8.4.2 describen, basándose en la dirección de origen de red, la forma en que el autentificador determina si:

1) este método no sirve para determinar la identidad del abonado;
2) se determina la identidad del abonado y éste corresponde al encabezador "De" incluido en la petición; o
3) el abonado queda determinado pero no corresponde con el encabezador "De" que figura en la petición.

Los procedimientos consignados en la cláusula 8.4.3 describen, basándose en la asociación de seguridad de transporte, la forma en que el autentificador determina si:

1) este método no sirve para determinar la identidad del abonado;
2) se determina la identidad del abonado determinado y éste corresponde con el encabezador "De" incluido en la petición; o
3) el abonado queda determinado pero no corresponde con el encabezador "De" que figura en la petición.

Las medidas adoptadas por el autentificador se consignan en el cuadro 2.

Cuadro 2 – Acciones del autentificador para cada resultado de la autentificación

Determinación de dirección de origen del abonado	Seguridad del transporte determinación del abonado	Acciones del autentificador
No disponible	No disponible	Utilización de una puesta a prueba/respuesta
No disponible	Corresponde	De acuerdo
No disponible	Diferente	Utilización de una puesta a prueba/respuesta
Corresponde	No disponible	De acuerdo
Corresponde	Corresponde	De acuerdo
Corresponde	Diferente	Utilización de la identidad de abonado derivada de la dirección de origen de red
Diferente	No disponible	Utilización de una puesta a prueba/respuesta
Diferente	Corresponde	Utilización de la identidad de abonado derivada de la asociación de seguridad de transporte
Diferente	Diferente	Utilización de una puesta a prueba/respuesta

Si la acción resultante consiste en utilizar una puesta a prueba/respuesta, se siguen los procedimientos expuestos en la cláusula 8.4.4.

Para identificar y autentificar abonados puede utilizarse no sólo la estrategia expuesta en las cláusulas 8.4.2 a 8.4.4, sino también la arquitectura genérica de inicialización (GBA), que se describe en la cláusula 8.4.5.

Las estrategias de autentificación descritas en la presente Recomendación son ejemplos típicos y cada proveedor NGN puede seleccionar, entre estas estrategias, cuáles desea utilizar (por ejemplo, seguir sólo uno de los procedimientos expuestos en las siguientes cláusulas).

8.4.2 Identificación del abonado mediante la dirección de origen de red

Ésta es la forma más simple de identificar al abonado, ya que se basa únicamente en la dirección de origen proporcionada junto con los paquetes IP. El autentificador consulta una correspondencia preaprovisionada de gamas de direcciones IP con <identificador de cuenta de abonado> y, si la dirección de origen de la petición se encuentra en una de estas gamas, el autentificador considera que la petición ha sido originada por el abonado. El <identificador de cuenta de abonado> se utiliza, acto seguido, para obtener las credenciales del abonado por conducto de las SAA/TAA-FE y verificar que sean conformes con el valor del encabezador "De".

Si el valor del encabezador "De" es conforme con el abonado, se considera un "corresponde"; si el valor del encabezador "De" no es conforme con el abonado, se considera "diferente"; si la dirección de origen IP no contiene ninguna de las gamas de direcciones preaprovisionadas, se considera "no disponible".

La eficacia de este método de identificación de abonados depende de que se garantice la dirección de origen. La garantía de la dirección de origen significa que la dirección IP sólo puede ser utilizada por el abonado legítimo a quien se ha asignado la dirección. Para ello, es necesario realizar las dos siguientes acciones en cuanto a las FE de procesamiento de transporte y control de transporte, acciones que, además, deben coordinarse adecuadamente: 1) gestionar estrictamente las correspondencias entre el abonado y su dirección asignada; y 2) impedir que se usurpe la dirección basándose en esta información gestionada. En el apéndice I se ofrece una serie de ejemplos en relación con dichas acciones y su coordinación.

8.4.3 Identificación del abonado mediante asociación de seguridad TLS/IPsec

Cuando se establece un transporte TLS seguro para la señalización del tráfico entre el dispositivo originador y el autentificador, y dicho transporte seguro se autentifica con un certificado TE-BE X.509 (véase la cláusula 8.3.2), el autentificador verifica que el encabezamiento "De" sea conforme con los valores autorizados para el abonado identificado en el <identificador de cuenta de abonado>.

Cuando se establece un transporte seguro (sea IPsec o TLS) para el tráfico de señalización entre el dispositivo originador y el autentificador, y dicho transporte seguro se autentifica con un certificado de dispositivo TE NGN X.509 (véanse las cláusulas 8.3.1 y 8.3.2), el autentificador utiliza el nombre del fabricante del dispositivo y el número de serie del dispositivo para determinar el <identificador de cuenta del abonado> conexo (válido únicamente si el dispositivo se ha asociado con un abonado). El <identificador de cuenta del abonado> se utiliza para obtener las credenciales del abonado y se verifica que dichas credenciales sean conformes con el valor contenido en el encabezador "De".

Cuando se establece un transporte seguro (sea IPsec o TLS) para el tráfico de señalización entre el dispositivo originador y el autentificador, y dicho transporte seguro se autentifica con un certificado de abonado TE NGN X.509 (véanse las cláusulas 8.3.1 y 8.3.2), el autentificador utiliza el <identificador de cuenta del abonado> para obtener las credenciales del abonado por conducto de las SAA/TAA-FE. A continuación, el autentificador verifica la conformidad de las credenciales del abonado y el valor contenido en el encabezador "De".

Cuando se establece un transporte seguro (sea IPsec o TLS) para el tráfico de señalización entre el dispositivo originador y el autentificador, y dicho transporte seguro se autentifica con un certificado de usuario final TE NGN X.509 (véanse las cláusulas 8.3.1 y 8.3.2), el autentificador utiliza el <identificador de cuenta del abonado> para obtener las credenciales del abonado por conducto de las SA/TAA-FE. A continuación, el autentificador verifica la conformidad de las credenciales del abonado y el valor contenido en el encabezamiento "De".

Si se establece un transporte seguro (sea IPsec o TLS) para el tráfico de señalización entre el dispositivo de origen y el autentificador, y dicho transporte seguro se autentifica con una clave precompartida (véase la cláusula 9.2.4.3.1), el autentificador utiliza el nombre de la clave para obtener las credenciales del abonado por conducto de las SA/TAA-FE. Acto seguido, el autentificador verifica la conformidad de las credenciales del abonado y el valor contenido en el encabezador "De".

Si no se utiliza un transporte seguro entre el dispositivo originador y el autentificador, y se recurre a una conexión TLS "cliente anónimo", este método es "no disponible".

8.4.4 Identificación del abonado mediante puesta a prueba/respuesta

La puesta a prueba/respuesta es una versión más segura del mecanismo identidad del usuario/contraseña (consistente en enviar la identificación y contraseña de un usuario como parte de una petición de servicio, lo que planteaba el problema de que ambas pueden volver a emplearse fácilmente para obtener ulteriormente el servicio de manera fraudulenta). En un mecanismo de puesta a prueba/respuesta, el servidor envía una puesta a prueba al cliente, pidiéndole que desempeñe una determinada tarea de encriptado sirviéndose de una clave compartida. El resultado de este cálculo se incluye en la respuesta y es verificado por el servidor. En caso de que dicho intercambio sea interceptado por terceros, éste no podrá emplearse una vez más, ya que el servidor no vuelve a utilizar en ningún caso una puesta a prueba anterior.

Existe un importante tipo de métodos de puesta a prueba-respuesta en los que se dan cita la conveniencia de los métodos de autentificación basados en contraseñas y la seguridad de los métodos basados en el mecanismo de puesta a prueba-respuesta. El protocolo de intercambio de claves autentificadas mediante contraseña (PAK) pertenece a esa categoría de métodos. El protocolo PAK garantiza la mutua autentificación de ambas partes en el acto de establecer una clave criptográfica simétrica a través del intercambio Diffie-Hellman. La utilización del intercambio Diffie-Hellman garantiza la *perfecta seguridad en el futuro*, que es una propiedad de los protocolos de establecimiento de claves, la cual garantiza que el pirateo de una clave de sesión o de una clave privada a largo plazo después de una determinada sesión no comprometa ninguna sesión anterior. Por otra parte, el método de autentificación PAK protege el intercambio contra ataques de *intermediario*. La autentificación se basa en un secreto precompartido, que se protege (esto es, sigue sin ser revelado) contra cualquier escucha clandestina, para impedir un ataque de diccionario fuera de línea. Así pues, el protocolo puede utilizarse en una gran variedad de aplicaciones que entrañan secretos precompartidos basados en la posibilidad de que existan contraseñas débiles. El protocolo PAK se especifica en [UIT-T X.1035] y [b-TIA 683-D].

Una puesta a prueba/respuesta entraña un intercambio de mensajes adicional entre el autentificador y el punto de extremo originador, así como un cálculo a cargo del punto de extremo originador, por lo cual podría contribuir al retardo percibido por el usuario. El objetivo de la seguridad de las NGN consiste en utilizar una puesta a prueba/respuesta únicamente cuando es absolutamente necesario lograr el nivel necesario de identificación y autentificación.

Cuando se establece una conexión de transporte segura (sea IPsec o TLS) para el tráfico de señalización entre el dispositivo originador y el autentificador, y éste último autenticó una petición previamente cursada dentro de un periodo configurable con los mismos contenidos del encabezador "De", la autentificación se considera lograda y se acepta la petición. Tratándose de la señalización del establecimiento de llamada, dado que la primera petición típica que se cursa a través de una nueva conexión es un "Registro", esta puesta a prueba/respuesta se hará en un momento en que no contribuya a retardar el establecimiento de la llamada.

Como las peticiones de autentificación requieren un gran número de cálculos, resulta esencial que el autentificador limite la frecuencia de las consultas formuladas a las SAA/TAA-FE. Los límites definidos en el presente párrafo pueden aceptarse con independencia de que las SAA/TAA-FE sean parte integral del autentificador o un elemento separado. Para un punto de extremo un ataque simple

de denegación de servicio se reduce a inundar al autentificador con peticiones incorrectas -si cada una de estas peticiones exige realizar un cálculo criptográfico en las SAA/TAA-FE, la prestación del servicio para atender a todas las peticiones (válidas o inválidas) se retrasará o quedará prácticamente detenida. Para contrarrestar dichos ataques, el autentificador puede rechazar localmente una petición de autorización cursada por un punto de extremo, cuando se encuentre pendiente otra petición de este tipo procedente del mismo punto de extremo. Una variante ligeramente más compleja que el proceso descrito consiste en que el autentificador rechace localmente una petición, cuando se hayan formulado al menos en total XXX peticiones dentro de los últimos YYY segundos (valores XXX e YYY que habrán de ser configurables en el autentificador). Asimismo, el autentificador puede esperar deliberadamente durante un periodo configurable antes de responder a una petición de autorización abortada. Esto impide, igualmente, la realización de varios tipos de ataque mediante "desciframiento de contraseñas".

8.4.4.1 Puesta a prueba/respuesta con señalización SIP a partir del dispositivo originador

Cuando el dispositivo originador utiliza el protocolo de señalización SIP, cabe utilizar opcionalmente los mecanismos de autentificación sustitutivos definidos en [b-IETF RFC 3261] para implementar una puesta a prueba/respuesta. Véanse la cláusula 22.2 de [b-IETF RFC 3261], así como las cláusulas 3 de [b-IETF RFC 2617], y 3 de [b-IETF RFC 3310].

El autentificador responde a la petición SIP con una respuesta 407 (sustituto de autentificación requerido), respuesta en la que incluye un encabezador de autentificación sustitutivo con: plan de autentificación "Digest", dominio de "NGN .ngn.net", calidad de protección (qop "auth"), número de uso único de un valor criptográficamente aleatorio de 16 octetos (en hex), opcionalmente, un valor del parámetro "Opaque" idéntico al que figura en la respuesta 407 y un algoritmo de "MD5" o "AKAv1-MD5", dependiendo del acuerdo de servicio concertado con el cliente.

Un ejemplo de un encabezador de autentificación sustitutivo en una respuesta 407 es el siguiente:

```
Proxy-Authenticate: Digest realm="NGN .ngn.com", qop="auth",
nonce="ea9c8e88df84f1cec4341ae6cbe5a359", opaque="", stale=FALSE, algorithm=MD5
```

El dispositivo originador responde a la respuesta 407 con una petición regenerada, que contiene un encabezador de autentificación sustitutivo. Este encabezador se verifica para cerciorarse de que contenga la siguiente información: plan de autentificación de "Digest", dominio idéntico al que figura en la respuesta 407, número de uso único idéntico al consignado en la respuesta 407, un "Opaque" idéntico al incluido en la respuesta 407. Asimismo, el encabezador de autentificación sustitutiva incluye un parámetro "Username" que proporciona el nombre de la clave, un parámetro "Uri" que corresponde a la petición URI de la petición y un parámetro "Response", que se especifica en [b-IETF RFC 2617] o [b-IETF RFC 3310].

Un ejemplo de encabezamiento de autorización sustitutiva en una petición reexpedida es el siguiente:

```
Proxy-Authorization: Digest username="bob", realm="NGN .ngn.com",
nonce="ea9c8e88df84f1cec4341ae6cbe5a359", opaque="", uri="sip:5551212@ngn.com",
response="dfe56131d1958046689d83306477ecc"
```

Los mecanismos de autentificación de usuario a usuario definidos en [b-EITF RFC 3261] pueden utilizarse también para implementar una puesta a prueba/respuesta. Para mayor información, véase la cláusula 22.2 de [b-IETF RFC 3261], así como las cláusulas 3 de [b-IETF RFC 2617], y 3 de [b-IETF RFC 3310].

Si una petición se bifurca, cabe la posibilidad de que algunos NE de la NGN (por ejemplo, MGC-FE) y/o TE de esa red deseen poner a prueba el dispositivo originador. El NE bifurcador (por ejemplo, S-CSC-FE) agrega estas puestas a prueba y las consigna en una sola respuesta que dicho NE envía al dispositivo originador. Al recibir la respuesta, que contiene múltiples puestas a prueba, el dispositivo originador cursa una nueva petición en la cual incluye múltiples credenciales.

8.4.4.2 Puesta a prueba/respuesta para el dispositivo originador con señalización distinta de la especificada en el SIP

Si se prevé que el dispositivo originador utilice SIP, pero éste expide su petición utilizando un protocolo de señalización distinto del SIP, se considera que ha fallado la puesta a prueba/respuesta. Se rechaza la petición.

8.4.5 Arquitectura genérica de inicialización (GBA)

La arquitectura genérica de inicialización (GBA) especifica un procedimiento de arranque independiente del acceso y constituye un marco para la mutua autentificación de los usuarios finales y la función de aplicación de la red (NAF, *network application function*), procedimiento que cabe utilizar para identificar y autentificar abonados en la NGN. Para mayor información sobre la GBA, véase [b-ETSI TS133 220].

8.5 Identificación y autentificación de usuarios finales

8.5.1 Estrategia general

Aunque la identificación del abonado es indispensable en el caso de la infraestructura NGN, la identificación del usuario final es un servicio opcional que puede solicitar el abonado o el servicio. Normalmente, esto se hace para proporcionar servicios adicionales, por ejemplo, movilidad y presencia personales, en cuyo caso se requerirá la identidad del usuario solicitante si éste tiene la intención de utilizar el servicio. Si un abonado desea contar con este nivel adicional de identificación, todos los correspondientes dispositivos de extremo deberían soportar la capacidad necesaria para introducir credenciales adicionales de usuario final o utilizar un certificado de usuario final en lugar de un certificado de abonado.

El autentificador puede aplicar dos métodos para identificar y autentificar al usuario final. El primero de ellos, se implementa mediante la asociación de seguridad en el plano del transporte utilizada para el intercambio de señalización. En caso de que dicha asociación de seguridad sea establecida con un certificado de usuario final (o una clave precompartida asociada con un solo usuario final), la identificación de usuario final es total. El segundo método consiste en proceder mediante puesta a prueba/respuesta, en cuyo caso el nombre de clave dado en la respuesta se asocia con un solo usuario final. Estos dos métodos se describen más detalladamente en las siguientes cláusulas.

Los dispositivos NGN avanzados pueden contar con múltiples identidades, por ejemplo, un certificado de abonado y también uno o más certificados de usuario final, en relación con la persona o personas que utilicen los dispositivos de que se trate. Un dispositivo de este tipo crearía múltiples conexiones TLS con el autentificador, cada uno de ellas para cada uno de los certificados. Acto seguido, el dispositivo enviaría al autentificador peticiones a través de la correspondiente conexión de señalización, basándose en la identidad deseada para la llamada del caso.

Preocupa el hecho de que las credenciales destinadas a un solo usuario siguen siendo válidas mucho después de que el usuario haya "partido". Si la asociación de seguridad de transporte se ha basado en un certificado de usuario final, el abonado puede exigir una actividad continua para mantener la validez de la autentificación. De no ser así, el autentificador procede a cerrar la conexión de transporte seguro y exige al dispositivo originador que la restablezca con el certificado vigente del usuario final (o en su defecto el certificado del abonado o el certificado del dispositivo). En las cláusulas 9.1.2 y 9.2.4.3.1 se ofrece información detallada acerca de los requisitos que gobiernan esta conducta del autentificador, requisitos que se basan en dos temporizadores: uno que limita el tiempo absoluto durante el cual pueden ser válidas las credenciales de usuario final para una asociación de seguridad determinada, y el segundo, que limita el tiempo muerto entre dos peticiones sucesivas. Cabe la posibilidad de que el abonado o el usuario final suministren los valores de temporización, pero en ambos casos estos valores deben quedar limitados por los máximos fijados por el proveedor NGN.

8.5.2 Identificación del usuario final mediante asociación de seguridad TLS/IPsec

Si se ha establecido un transporte TLS seguro para el tráfico de señalización entre el dispositivo originador y el autentificador, y dicho transporte seguro ha sido autentificado mediante un certificado TE-BE X.509 (véase la cláusula 8.6), el autentificador verifica que el encabezador "De" sea conforme con los valores permitidos para el abonado identificado en el <identificador de cuenta de abonado> contenido en el certificado.

Si se ha establecido un transporte seguro (sea IPsec o TLS) para el tráfico de señalización entre el dispositivo originador y el autentificador, y el transporte seguro ha sido autentificado mediante un certificado de usuario final TE NGN X.509 (véase la cláusula 8.6), el autentificador utiliza el <identificador de cuenta de abonado> para obtener las credenciales del abonado por conducto de las SAA/TAA-FE. Acto seguido, el autentificador verifica la conformidad entre las credenciales del abonado y el valor del encabezador "De". Si se ha establecido un transporte seguro IPsec para el tráfico de señalización entre el dispositivo originador y el autentificador (véase la cláusula 8.4.4) y el transporte seguro ha sido autentificado con una clave precompartida (véase la cláusula 9.2.4.3.1), el autentificador utiliza el nombre de clave para obtener las credenciales del abonado por conducto de las SAA/TAA-FE. A continuación, el autentificador verifica la conformidad entre las credenciales del abonado y el valor contenido en el encabezador "De".

8.5.3 Identificación del usuario final mediante puesta a punto/respuesta

Los procedimientos de puesta a punto/respuesta para la identificación del usuario final son idénticos a los utilizados para identificar al abonado, como puede verse en la cláusula 8.4.4.

En este caso, la única extensión consiste en que el autentificador verifica la información recuperada por conducto de las SAA/TAA-FE en relación con el nombre de la clave, en busca de una indicación de que la clave se encuentra asociada con un usuario final. De ser así, concluye con éxito la identificación del usuario final.

Si el autentificador ha realizado ya una puesta a prueba/respuesta para identificar al abonado, y la clave nombrada devuelta en la respuesta no identifica a un usuario final, la identificación del usuario final fracasa. En tal caso, se procede a expedir una puesta a prueba, aunque no se haya necesitado puesta a prueba/respuesta para identificar al abonado.

8.6 Identificador y autentificación mediante TE-BE

Los procedimientos de identificación y autentificación efectuados por un TE-BE son prácticamente idénticos a los realizados por un autentificador. Existen, sin embargo, dos diferencias:

1) Cabe aprovisionar al TE-BE con todas las credenciales necesarias para identificar y autentificar al abonado o abonados y a los usuarios finales a los que atiende ese elemento, ya que este último no tiene acceso a la función distribuida SAA/TAA-FE, que está disponible para un autentificador.
2) La petición reexpedida en respuesta a una puesta a prueba del autentificador, que contiene el encabezador "Autorización sustitutiva", se transmite al autentificador, en lugar de ser procesada en el TE-BE.

8.6.1 Utilización de certificados X.509

Existe una asociación de seguridad entre cada TE-BE y al menos un NBE, asociación que se establece con el certificado X.509 expedido por el TE-BE de que se trate. Las peticiones recibidas en el NBE siguen los procedimientos de identificación y autentificación señalados en la cláusula 8.4.3, lo que redunda en una verificación mínima de la identificación por parte del TE-BE. Cuando se requiere una puesta a prueba/respuesta (por ejemplo, en el caso de un usuario "itinerante"), el intercambio tendrá lugar entre el punto de extremo originante y el NBE, y se transmitirá de manera transparente a través del TE-BE.

Un transporte seguro entre el punto de extremo y el TE-BE es una opción. Está previsto que la dirección de origen de red identifique adecuadamente la mayoría de las peticiones.

Los puntos de extremo registran al NBE a través del TE-BE.

8.7 Autentificador-interfaz SAA/TAA-FE

8.7.1 Utilización de RADIUS y sus ampliaciones

Las SAA/TAA-FE contienen el punto de decisión y las SUP/TUP-FE constituyen depósitos para almacenar credenciales de usuario final y de dispositivo en la infraestructura NGN. Algunas funciones SAA/TAA-FE, como la autentificación, pueden distribuirse para optimizar la calidad de funcionamiento de las peticiones de autentificación.

Normalmente, existen dos opciones en lo que respecta a la utilización del protocolo de comunicación entre el autentificador y el SAA/TAA-FE; a saber RADIUS [b-IETF RFC 2865] (muy conocido y soportado) y Diameter [b-IETF RFC 3588] (que se ha definido para rectificar varias deficiencias de RADIUS). Aunque la idea es que con el tiempo la infraestructura NGN migre a Diameter; se reconoce que las actuales implementaciones de los servidores se basan en RADIUS, y que se han desarrollado un gran número de extensiones ad doc del protocolo RADIUS básico para atender a las necesidades de esta función de autentificación. Aunque esta versión de la presente Recomendación se basa en RADIUS con la extensión descrita en [b-IETF RFC 5090], es probable que en una futura versión de la Recomendación se modifique esta interfaz, para que se base en Diameter con la extensión descrita en [b-IETF RFC 4740].

El autentificador se convierte en un cliente de RADIUS, y el servidor SAA/TAA-FE pasa a ser un servidor RADIUS, según se define en [b-IETF RFC 2865]. Ambos podrán implementar las extensiones necesarias para la autentificación SIP Digest, según se indica en [b-IETF RFC 5090]. La conexión entre el autentificador y el servidor SAA/TAA-FE puede quedar asegurada mediante IPsec con autentificación recíproca.

Recurriendo a las extensiones [b-IETF RFC 4590], el autentificador formula una petición RADIUS con los parámetros del encabezador "autentificación sustitutiva" y el servidor RADIUS calcula la respuesta esperada y devuelve ésta al autentificador. Acto seguido, el autentificador valida la petición, comparando la respuesta realmente procedente del punto de extremo con la respuesta esperada.

Un ejemplo del mensaje enviado al servidor SAA/TAA-FE a partir del autentificador es el siguiente:

```
Code = 1 (Access-Request)
    Identifier = 1
    Length = 164
    Authenticator = 56 7b e6 9a 8e 43 cf b6 fb a6 c0 f0 9a 92 6f 0e
    Attributes:
    NAS-IP-Address = d5 89 45 26 (213.137.69.38)
    NAS-Port-Type = 5 (Virtual)
    User-Name = "bob"
    Digest-Response (206) = "2ae133421cda65d67dc50d13ba0eb9bc"
    Digest-Attributes (207) = [Realm (1) = "NGN .ngn.com"]
    Digest-Attributes (207) = [Nonce (2) = " ea9c8e88df84f1cec4341ae6cbe5a359 "]
    Digest-Attributes (207) = [Method (3) = "INVITE"]
    Digest-Attributes (207) = [URI (4) = " sip:5551212@ngn.com "]
    Digest-Attributes (207) = [Algorithm (5) = "md5"]
    Digest-Attributes (207) = [User-Name (10) = "bob"]
```

```
Un ejemplo de la respuesta enviada al autentificador a partir del servidor
SAA/TAA-FE es la siguiente:

Code = 2 (Access-Accept)
      Identifier = 1
      Length = 20
      Authenticator = 6d 76 53 ce aa 07 9a f7 ac b4 b0 e2 96 2f c4 0d
      Attributes:
      Digest-Response (206) = "dfe56131d1958046689d83306477ecc"
```

8.7.2 Asociación de seguridad de señalización de transporte

Cuando se recurre a un certificado X.509 para establecer la asociación de seguridad de señalización de transporte, los SUP/TUP-FE almacenan el conjunto aceptable (indicado por el <identificador de cuenta de abonado>) de encabezadores "De" que puede aparecer en peticiones cursadas a partir de dicho origen, conjunto que se hará corresponder al encabezador "De" proporcionado en la petición de que se trate.

Si se utiliza una clave precompartida para establecer la asociación de seguridad de señalización de transporte (por ejemplo, el proveedor de servicio entre pares), los SUP/TUP-FE almacenan el conjunto aceptable (indicado por el nombre de clave) de encabezadores "De", que puede aparecer en peticiones cursadas a partir de dicho origen, conjunto que se hará corresponder con el encabezamiento "De" proporcionado en la petición de que se trate.

8.8 Identificación y autentificación del tráfico de portadora

En ocasiones convendría identificar cada flujo de tráfico de portadora para mejorar la seguridad, entre otras cosas, con el fin de contrarrestar ataques fraudulentos tales como la usurpación de identidad o la inyección de RTP. En las NGN el tráfico de portadora puede identificarse mediante un quíntuplo que contiene:

- la dirección IP de origen;
- la dirección IP de destino;
- el puerto de origen;
- el puerto de destino;
- el número de protocolo.

El mecanismo de identificación descrito en la presente cláusula utiliza este identificador para autentificar todos los paquetes. El mecanismo se basa en un secreto compartido y la utilización de la función de troceo criptográfica, código de autentificación de mensajes mediante troceo con clave (HMAC). Véase [b-NIST FIPS 198-1] con propósitos de información.

Las entidades que participan en el proceso de autentificación – la función de usuario final y el nodo de acceso FE – se describen en [UIT-T Y.2701] y se representan en la figura 3, en la que se ofrece como ejemplo la UNI.

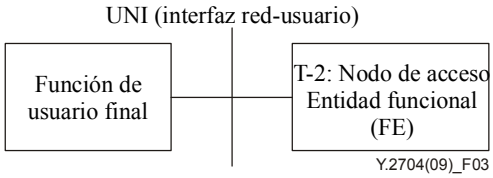


Figura 3 – Entidades NGN que participan en el procedimiento de autentificación – Ejemplo, la UNI

Para describir el mecanismo se utilizan las siguientes convenciones:

- *F* es un identificador (quíntuple) del tráfico de portadora.
- *K* es un secreto compartido que poseen la función de usuario final y el nodo de acceso FE.
- *P* es un paquete que la función de usuario final se propone enviar al nodo de acceso FE.
- *i* es un número de secuencia de un paquete que se encuentra incrementando las dos partes que comunican entre sí. Dicho número tiene un valor de 64 bits.
- *t* es una indicación de tiempo con un valor de 64 bit que indica el tiempo en segundos. Puede ser también un número de uso único.
- (*P*', *Q*) es un paquete que ha recibido el nodo de acceso FE.

Cuando la función de usuario final pretende enviar un paquete *P* al nodo de acceso FE, computa un valor de la función *H(F, t+i, K)*, que es una función de troceo de una concatenación de *F*, *t+i,* y *K*, y a continuación adjunta este valor al paquete *P*. En consecuencia, el paquete íntegro enviado al nodo de acceso FE a partir de la función de usuario final es *[P, H(F, t+i, K)]*. Cuando el nodo de acceso FE recibe un paquete (*P', Q*), computa el valor de *H(F, t+i, K)*. Si se utiliza una indicación de tiempo, el nodo de acceso FE computa los diferentes resultados del troceo de todos los valores de *t* que contiene la gama convenida para determinar la diferencia entre los tiempos correspondientes a la función de usuario final y al nodo de acceso FE (esto debe hacerse una sola vez al iniciarse una sesión). De ser así, el nodo de acceso FE busca una correspondencia entre *Q* y cualquiera de los valores computados en relación con los resultados del troceo. El paquete se autentifica, cuando se descubre una correspondencia. El correspondiente valor de *t* se utilizará para los paquetes del flujo.

Si se utiliza un número de uso único, el nodo de acceso FE se limitará a verificar si el valor calculado en relación con los resultados del troceo es igual *Q*. En ese caso, se autentificará el paquete.

En un entorno que puedan sobrevenir pérdidas de paquetes, puede no bastar limitarse a incrementar *i* de paquete a paquete. De ser así el nodo de acceso de la FE puede buscar de *i* hasta *i+d* (donde *d* es un pequeño número) para volver a sincronizar *i*.

La utilización de este mecanismo de autentificación contribuye a contrarrestar ataques fraudulentos tales como usurpación de identidad o inyecciones de RTP.

El mecanismo mencionado permite, por otra parte, autentificar el tráfico generado por el usuario, sin por ello revelar su identidad.

Por lo que hace a esta implementación, se propone que la función de usuario final y la función de nodo de acceso FE convengan en el formato del identificador *F*, el secreto compartido *K*, la función de troceo *H*, la hora sincronizada exacta para iniciar la indicación de tiempo *t*, cuándo y cómo pueden añadirse la cantidad troceada al paquete *P*, el valor de *d* y qué inicios habrá que seleccionar para sincronizar una vez más *i*.

La utilización de este mecanismo es objeto de una política de seguridad del operador de red. Existen otros mecanismos a los que cabe recurrir para autentificar los flujos; por ejemplo, IPsec. La ventaja del mecanismo mencionado en comparación con el IPsec es que, mientras que el IPsec exige encriptar el paquete IP considerado en su totalidad (en el modo túnel) o la cabida útil (en el modo transporte), este mecanismo hace necesario calcular únicamente el valor de la función de troceo *H(F, t+i, K),* lo que puede hacerse más rápidamente y requiere menos recursos de cálculo.

9 Seguridad de transporte para la señalización y OAMP

La seguridad de transporte se utiliza en una infraestructura NGN para ofrecer garantías de confidencialidad e integridad de los datos de señalización y los mensajes OAMP. En la presente cláusula se especifican los perfiles de TLS e IPsec que deben emplear los elementos de red de la infraestructura NGN, ya que son importantes mecanismos de seguridad. La lista de mecanismos no

es exhaustiva y cabe la posibilidad de adoptar otras implementaciones, dependiendo de las políticas del proveedor NGN.

Dentro de la zona fiable y de la zona fiable pero vulnerable, el túnel VPN (por ejemplo, IPsec o TLS) resulta necesario para garantizar los mensajes OAMP. En la cláusula 9.1 se proporciona el perfil correspondiente a los casos de utilización de TLS y en la cláusula 9.2 el perfil relativo a los casos de utilización de IPsec. Entre el TE-BE y la OAMP-NBE (esto es, entre la zona no fiable y la zona fiable pero vulnerable), se recurre a IPsec para crear un túnel VPN. En la cláusula 9.3 se especifica el perfil de IPsec aplicable.

Aunque no es preciso contar con seguridad de medios en la infraestructura NGN, algunos elementos frontera implementan este tipo de seguridad para dar servicio a determinados puntos de extremo. Por lo que hace a estos elementos, en la cláusula 10 se consigna un perfil de protocolos de seguridad de medios.

9.1 TLS

En la infraestructura NGN suele utilizarse TLS para garantizar la seguridad de diferentes tipos de tráfico de señalización (por ejemplo, SIP, COPS, TRIP, HTTP) entre los elementos de red situados en la zona fiable. Se apoya también TLS en los elementos frontera, que pueden recibir señalización encriptada a partir de puntos de extremo de cliente, y por el TE-BE para comunicar con un NBE. En [UIT-T Y.2701] se señalan requisitos específicos para cada tipo de elemento de red.

El protocolo TLS se define en [b-IETF RFC 5246] y proporciona privacidad e integridad de datos con un protocolo de capa de transporte fiable, tal como TCP o SCTP.

A menos de que se especifique otra cosa en esta cláusula, convendría que los elementos de red de la infraestructura NGN exijan la concordancia del TLS con la especificación del TLS [b-IETF RFC 5246] y todos los requisitos especificados en [b-IETF RFC 3261] en relación con su utilización en el SIP. Aunque TLS soporta la negociación y la utilización de métodos de compresión, cabe la posibilidad de que en la infraestructura NGN no se utilice compresión, para evitar que se degrade la calidad de funcionamiento.

9.1.1 Series de cifras

Las series de cifras entrañan la utilización del método de acuerdo sobre claves autentificadas empleado en la toma de contacto TLS, así como cifras de encriptado y autentificación que sirven para garantizar la seguridad de la capa de registro. Las series de cifras son negociadas con los clientes TLS, presentando una lista de series de cifras soportada en el mensaje "Hola cliente", que el servidor responderá con la serie de cifras seleccionada en el mensaje "Hola servidor".

Un gran número de factores ejercen influencia en la elección del algoritmo de encriptado. En este sentido, pueden señalarse ejemplos tales como:

1) Seguridad requerida
   - Valor de los datos (para la organización y/o otras entidades – mientras más valioso sean los datos, más robusta será el encriptado requerido).
   - Valor temporal de los datos (si los datos son valiosos, pero únicamente para un periodo breve (por ejemplo, días y así años), podría utilizarse un algoritmo de encriptado más débil).
   - Amenaza contra los datos (cuanto más elevado sea el nivel de amenaza, más robusto será el encriptado requerido).
   - Otras medidas de protección establecidas que pueden reducir la necesidad de encriptado robusto – por ejemplo, utilizar métodos para proteger comunicaciones, tales como circuitos especializados, en lugar de recurrir a la Internet pública.

2) Calidad del servicio requerida (la exigencia de requisitos de calidad más estrictos puede exigir el aprovisionamiento de recursos de sistema adicionales, tales como un acelerador criptográfico de equipo, o requerir un encriptado más débil).

3) Recursos de sistema (un número menor de recursos [por ejemplo, procesamiento y memoria], puede requerir un encriptado más débil).

4) Restricciones de importación, exportación o utilización.

5) Planes de encriptado soportados por elementos de red.

6) Planes de encriptado soportados por dispositivos de usuario.

En el cuadro 3 aparece una lista de series de cifras propuestas que se adecuan a las NGN, aunque este cuadro no es exhaustivo.

Cuadro 3 – Series de cifras propuestas para las NGN

Nombre del conjunto de cifras	Referencia	Intercambio de clave	Cifra	Troceo
TLS_RSA_WITH_AES_128_CBC_SHA	b-IETF RFC 5246	RSA	AES-128 en modo CBC	SHA-1
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	b-IETF RFC 5246	Diffie-Hellman en modo efímero con firmas RSA	AES-128 en modo CBC	SHA-1
TLS_RSA_WITH_3DES_EDE_CBC_SHA	b-IETF RFC 2246	RSA	3DES en modo CBC	SHA-1
TLS_DHE_WITH_3DES_EDE_CBC_SHA	b-IETF RFC 5246	Diffie-Hellman en modo efímero con firmas RSA	3DES en modo CBC	SHA-1
TLS_RSA_WITH_CAMELLIA_128_CBC_SHA	b-IETF RFC 4132	RSA	Camellia-128 en modo CBC	SHA-1
TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA	b-IETF RFC 4132	Diffie-Hellman en modo efímero con firmas RSA	Camellia-128 en modo CBC	SHA-1

El conjunto de cifras que se indica en el cuadro 4 extraído de [b-IETF RFC 5246], [b-IETF RFC4132] y [b-IETF RFC 4492] puede ser utilizado también opcionalmente por cualquier NE.

Cuadro 4 – Series de cifras de posible utilización (opcional) en relación con las NGN

Nombre de la serie de cifras	Referencia	Intercambio de claves	Cifra	Troceo
TLS_DH_DSS_WITH_AES_128_CBC_SHA	b-IETF RFC 5246	Diffie-Hellman con firma DSS	AES-128 en modo CBC	SHA-1
TLS_DH_RSA_WITH_AES_128_CBC_SHA	b-IETF RFC 5246	Diffie-Hellman con firma RSA	AES-128 en modo CBC	SHA-1
TLS_DHE_DSS_WITH_AES_128_CBC_SHA	b-IETF RFC 5246	Diffie-Hellman en modo efímero con firma DSS	AES-128 en modo CBC	SHA-1
TLS_DHE_RSA_WITH_AES_128_CBC_SHA	b-IETF RFC 5246	Diffie-Hellman en modo efímero con firma RSA	AES-128 en modo CBC	SHA-1
TLS_RSA_WITH_AES_256_CBC_SHA	b-IETF RFC 5246	RSA	AES-256 en modo CBC	SHA-1
TLS_DH_DSS_WITH_AES_256_CBC_SHA	b-IETF RFC 5246	Diffie-Hellman con firma DSS	AES-256 en modo CBC	SHA-1
TLS_DH_RSA_WITH_AES_256_CBC_SHA	b-IETF RFC 5246	Diffie-Hellman con firma RSA	AES-256 en modo CBC	SHA-1
TLS_DHE_DSS_WITH_AES_256_CBC_SHA	b-IETF RFC 5246	Diffie-Hellman en modo efímero con firma DSS	AES-256 en modo CBC	SHA-1
TLS_DHE_RSA_WITH_AES_256_CBC_SHA	b-IETF RFC 4132	Diffie-Hellman en modo efímero con firma RSA	AES-256 en modo CBC	SHA-1
TLS_DH_DSS_WITH_CAMELLIA_128_CBC_SHA	b-IETF RFC 4132	Diffie-Hellman con firma DSS	Camellia-128 en modo CBC	SHA-1
TLS_DH_RSA_WITH_CAMELLIA_128_CBC_SHA	b-IETF RFC 4132	Diffie-Hellman con firma RSA	Camellia-128 en modo CBC	SHA-1
TLS_DHE_DSS_WITH_CAMELLIA_128_CBC_SHA	b-IETF RFC 4132	Diffie-Hellman en modo efímero con firma DSS	Camellia-128 en modo CBC	SHA-1
TLS_RSA_WITH_CAMELLIA_256_CBC_SHA	b-IETF RFC 4132	RSA	Camellia-256 en modo CBC	SHA-1
TLS_DH_DSS_WITH_CAMELLIA_256_CBC_SHA	b-IETF RFC 4132	Diffie-Hellman con firma DSS	Camellia-256 en modo CBC	SHA-1
TLS_DH_RSA_WITH_CAMELLIA_256_CBC_SHA	b-IETF RFC 4132	Diffie-Hellman con firma RSA	Camellia-256 en modo CBC	SHA-1
TLS_DHE_DSS_WITH_CAMELLIA_256_CBC_SHA	b-IETF RFC 4132	Diffie-Hellman en modo efímero con firma DSS	Camellia-256 en modo CBC	SHA-1
TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA	b-IETF RFC 4132	Diffie-Hellman en modo efímero con firma RSA	Camellia-256 en modo CBC	SHA-1
TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA	b-IETF RFC 4492	EC-Diffie-Hellman con firma ECDSA	3DES en modo CBC	SHA-1

Cuadro 4 – Series de cifras de posible utilización (opcional) en relación con las NGN

Nombre de la serie de cifras	Referencia	Intercambio de claves	Cifra	Troceo
TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA	b-IETF RFC 4492	EC-Diffie-Hellman con firma ECDSA	AES-128 en modo CBC	SHA-1
TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA	b-IETF RFC 4492	EC-Diffie-Hellman con firma ECDSA	AES-256 en modo CBC	SHA-1
TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA	b-IETF RFC 4492	EC-Diffie-Hellman en modo efímero con firma ECDSA	3DES en modo CBC	SHA-1
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA	b-IETF RFC 4492	EC-Diffie-Hellman en modo efímero con firma ECDSA	AES-128 en modo CBC	SHA-1
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA	b-IETF RFC 4492	EC-Diffie-Hellman en modo efímero con firma ECDSA	AES-256 en modo CBC	SHA-1
TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA	b-IETF RFC 4492	EC-Diffie-Hellman con firma RSA	3DES en modo CBC	SHA-1
TLS_ECDH_RSA_WITH_AES_128_CBC_SHA	b-IETF RFC 4492	EC-Diffie-Hellman con firma RSA	AES-128 en modo CBC	SHA-1
TLS_ECDH_RSA_WITH_AES_256_CBC_SHA	b-IETF RFC 4492	EC-Diffie-Hellman con firma RSA	AES-256 en modo CBC	SHA-1
TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA	b-IETF RFC 4492	EC-Diffie-Hellman en modo efímero con firma RSA	3DES en modo CBC	SHA-1
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	b-IETF RFC 4492	EC-Diffie-Hellman en modo efímero con firma RSA	AES-128 en modo CBC	SHA-1
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	b-IETF RFC 4492	EC-Diffie-Hellman en modo efímero con firma RSA	AES-256 en modo CBC	SHA-1

NOTA 1 – RC-4 es una cifra popular y de gran utilización. Con todo, no se incluye en la lista anterior, ya que no corresponde a una norma abierta.

NOTA 2 – La criptografía curva elíptica (ECC) es un criptosistema de claves públicas que puede convenir para ciertas aplicaciones en las NGN. Concretamente, la ECC puede resultar interesante para implementar ciertas aplicaciones, debido a sus ventajas en términos de eficiencia. En comparación con otros criptosistemas prevalecientes, tales como RSA, la ECC ofrece seguridad equivalente, pero con dimensiones de clave significativamente más reducidas. Asimismo, la ECC se caracteriza por su eficiencia y brinda más ventajas que otras técnicas de claves públicas y, por otra parte, brinda el mismo nivel de protección.

9.1.2 Utilización de certificados con el TLS

TLS es un protocolo basado en servidor-cliente con autentificación opcional de cliente. Sin embargo, dentro de la zona fiable de la infraestructura NGN y entre la zona fiable y la zona fiable pero vulnerable una autentificación mutua puede lograrse recurriendo al TLS. En tal caso, el servidor TLS envía una petición de certificado al cliente. Si un cliente situado en la zona fiable o la zona fiable pero vulnerable no proporciona un certificado de cliente, el servidor puede rechazar su petición de conexión. El cliente TLS y los certificados de servidor deberían ser conformes con las especificaciones de la certificación de infraestructura NGN indicadas en la cláusula 8.3. Los

certificados pueden verificarse, según se especifica en la cláusula 8.3. Antes de proceder con la conexión TLS, el servidor TLS o el cliente puede verificar si el sistema distante corresponde a su certificado.

Entre la zona fiable pero vulnerable y la zona no fiable, el servidor TLS puede enviar una petición de certificado al cliente. Si el cliente no tiene un certificado, responderá con un mensaje de certificado cliente vacío y la sesión procederá como si se tratase de un cliente anónimo.

Cuando un NBE acepta una conexión autentificada con un punto de extremo basado en un certificado de usuario final NGN (véase la cláusula 8.5.2), el NBE puede implementar dos temporizadores en la conexión. El primer temporizador, T1, se inicia cuando la conexión queda establecida. El segundo temporizador, T2, se inicia cuando la conexión queda establecida y es puesta a cero cada vez que se recibe una petición en el NBE de la conexión. Siempre que cada uno de ambos temporizadores alcanza su valor límite (lo que puede depender de los valores contenidos en el certificado), el NBE pone a cero la conexión y el punto extremo la restablecerá para reactualizar el certificado de usuario final NGN.

9.1.3 Gestión de claves de sesión

Se espera que las sesiones TLS entre elementos de red de infraestructura NGN sean duraderas. Así pues, resulta importante cambiar periódicamente las claves de sesión. Las claves de sesión para las sesiones TLS pueden modificarse después de un periodo configurable.

9.2 IPsec en zonas viables y fiables pero vulnerables

En la infraestructura NGN IPsec puede utilizarse para dar seguridad a varios tipos de tráfico (por ejemplo, SNMP, RADIUS) entre los elementos de red dentro de la zona fiable. En [UIT-T Y.2701] se señalan los requisitos específicos correspondientes a cada tipo de elemento de red.

Según se describe de manera general en [b-IETF RFC 4301], IPsec está integrado por una serie de distintos componentes, que pueden utilizarse para proporcionar confidencialidad, integridad y protección de reproducción. Algunos de estos componentes pueden configurarse manualmente, pero normalmente se utiliza para ello un componente de gestión de claves. Por otra parte, típicamente, la decisión sobre la utilización de IPsec es controlada por una base de datos de política. En esta cláusula se describe el subconjunto de obligada implementación de los componentes de IPsec.

En los elementos de red que utilizan IPsec se recomienda cerciorarse de que las conexiones seguras TLS no se ejecuten con IPsec.

NOTA – Los elementos de red que utilizan IPsec deberían garantizar que los trenes de medios asegurados con SRTP o RC4 no se ejecuten con IPsec, para garantizar que no se realice doble encriptado alguno, ya que esto constituiría un despilfarro de los recursos NGN. Hay que señalar, igualmente, que el paso en túnel del encriptado pueda realizarse a partir del usuario final.

9.2.1 AH y ESP

El encabezador de autentificación (AH), descrito en [b-IETF RFC 4302] y [b-IETF RFC 4835], y el protocolo de seguridad de encapsulado (ESP), descrito en [IETF RFC 4303], son los más adecuados para su utilización con protocolos de seguridad alámbricos. Ambos proporcionan opcionalmente protección de reproducción. El ESP se utiliza típicamente para proporcionar confidencialidad, integridad y autentificación del tráfico. Asimismo, puede proporcionar integridad y autentificación sin confidencialidad. Por otra parte, ESP puede utilizarse para proporcionar únicamente confidencialidad. AH protege partes del encabezador IP precedente, lo que incluye las direcciones de origen y de destino. Aunque AH puede proteger también las opciones IP que deben ser vistas por encaminadores intermedios, es necesario que dicho encabezador esté intacto y sea auténtico cuando se proporcione al sistema receptor, pese a lo cual la utilización de tales opciones IP es sumamente infrecuente.

Los elementos de red de la infraestructura NGN pueden soportar el protocolo de seguridad de encapsulado (ESP) definido en [IETF RFC 4303]. ESP_DES (con 40 y 56 bits), ESP_3DES, ESP_AES [b-IETF RFC 3602] y ESP_CAMELLIA [b-IETF RFC 4312] pueden ser soportados en modo de encadenamiento de bloques de cifras (CBC, *cipher block chaining*). Cabe la posibilidad de que los elementos de red que soportan ESP_NULL NO empleen ESP_NULL al comunicar con otros elementos de red de la infraestructura NGN. El algoritmo de encriptado realmente utilizado en el marco del ESP se negocia durante la gestión de claves.

[b-IETF RFC 4301] exige todas las implementaciones del ESP para soportar el concepto de asociaciones de seguridad (SA, *security associations*) y [b-IETF RFC 4301] proporciona un modelo general para procesar el tráfico IP relativo a las AS. Aunque existen determinadas implementaciones IPsec que no es necesario ajustar a los detalles de este modelo general, el comportamiento externo de cualquier implementación IPsec puede corresponder al comportamiento externo del modelo general. Esto garantiza que los componentes no acepten tráfico procedente de direcciones desconocidas y no envíen o acepten tráfico sin seguridad (cuando ésta se requiera). Los elementos de red de la infraestructura NGN que implementan IPsec pueden comportarse de modo tal que sean conformes con el modelo general descrito en [b-IETF RFC 4301].

9.2.2 Modo transporte y túnel

Cabe la posibilidad de utilizar tanto AH como ESP en modo transporte o modo túnel. En modo túnel, el encabezador IPsec es seguido por un encabezador IP interno. En esto consiste la utilización normal de las redes privadas virtuales (VPN), y se requiere en general cuando el extremo del trayecto protegido IPsec no es el último destino, por ejemplo, cuando IPsec se implementa en un cortafuegos o un encaminador. Entre el modo transporte y la comunicación punto a punto, se prefiere ese modo.

Los elementos de red de la infraestructura NGN pueden soportar IPsec en modo transporte.

9.2.3 Protección de reproducción

Los elementos de red de la infraestructura NGN pueden utilizar el servicio de protección contra reproducción opcional IPsec (servicio antirreproducción). En los elementos de red de la infraestructura NGN, el servicio de antirreproducción IPsec puede activarse en todo momento. El número de secuencia IPsec fuera de la ventana antirreproducción activada se valida como una reproducción y el paquete se rechaza. Cuando se activa el servicio antirreproducción, un número de secuencia IPsec no puede desbordar y pasar a 0. Antes de que eso suceda, debería crearse una nueva asociación de seguridad, según se especifica en [IETF RFC 4303].

9.2.4 Gestión de claves

Todos los sistemas criptográficos exigen una gestión de claves. Aunque IPsec entraña una utilización de planes de gestión de claves tanto manuales como automáticos, los planes manuales no pueden escalarse tan adecuadamente como los planes automáticos y no ofrecen protección contra reproducción. Todos los planes de gestión proporcionan autentificación. Los elementos de red de la infraestructura NGN deberían implementar uno de los mecanismos de intercambio automatizado de claves descritos en esta cláusula.

Cuando IKE no se utiliza para la gestión de claves, un protocolo de gestión de claves alternativo requiere una interfaz con la capa IPsec para crear/actualizar/suprimir asociaciones de seguridad de IPsec. Las asociaciones de seguridad IPsec pueden establecerse o restablecerse automáticamente, si así se requiere. Esto hace que la capa IPsec necesite, igualmente, una forma de señalizar una aplicación de gestión de claves, cuando sea necesario establecer una nueva asociación de seguridad (por ejemplo, cuando la antigua SA esté a punto de expirar o cuando no exista una SA en una determinada interfaz). Asimismo, puede ser necesario disponer de algunos elementos frontera para ejecutar múltiples protocolos de gestión de claves (por ejemplo, IKE, para garantizar la seguridad

de las conexiones para OAMP, y PKINIT). En estos casos se recomienda recurrir a la interfaz PF_KEY [b-IETF RFC 2367].

9.2.4.1 Identificadores de transformación

Los procedimientos de gestión de claves utilizan los identificadores de transformación IPsec para negociar algoritmos de encriptado que emplean ESP en IPsec. Estos identificadores de transformación son utilizados también por el IKE para garantizar la seguridad de sus mensajes de fase 1 y fase 2. En [b-IETF RFC 5282] se proporciona una lista de los identificadores de transformación IPsec disponibles. En la infraestructura de las NGN pueden soportarse los identificadores de transformación ESP_3DES (valor 0x03, con clave de 192 bits, modo CBC) y ESP_CAMELLIA (valor 0x16, con clave de 128 bits, modo CBC) [b-IETF RFC 4312]. Se recomienda soportar el identificador de transformación ESP_AES (valor 0x0C, con clave de 128 bits, modo CBC). El IKE permite negociar la magnitud de la clave de encriptado, por lo cual, si en el futuro se desea incrementar el tamaño de la clave para alguno de los algoritmos antes mencionados, el IKE utilizará esta función incorporada.

Tratándose de todos los identificadores de transformación precitados, el vector de inicialización (IV, *initialization vector*) CBC se transporta en el espacio libre de cada carga útil de paquete ESP [b-IETF RFC 2451]. AES-128, definido en [b-NIST FIPS 197] y [b-IETF RFC 3602], puede emplearse en modo CBC con un tamaño de bloque de 128 bits y un vector de inicialización generado aleatoriamente. AES-128 exige 10 rondas de operaciones critográficas [b-IETF RFC 3602]. Cabe la posibilidad de utilizar Camellia-128, definido en [b-IETF RFC3713] y [b-IETF RFC 4312], en modo CBC, con un tamaño de bloque de 128 bits y un vector de inicialización generado aleatoriamente. Camellia-128 requiere 18 rondas de operaciones criptográficas [b-IETF RFC 3713].

9.2.4.2 Algoritmos de autentificación

Los procedimientos de gestión de claves utilizan algoritmos de autentificación IPsec para negociar el algoritmo de autentificación de paquetes que se esté utilizando. En [b-IETF RFC 5282] se proporciona una lista de algoritmos de autentificación IPsec disponibles. Entre la infraestructura NGN cabe soportar los algoritmos de autentificación HMAC-MD5-96 (valor 0x01, con clave de 128 bits, definido en [b-IETF RFC 2403]) y HMAC-SHA-1-96 (valor 0x02, con clave de 160 bits, definido en [b-IETF RFC 4835]).

9.2.4.3 Intercambio de claves Internet (IKE)

En [b-IETF RFC 2409] se describe un mecanismo automatizado de intercambio de claves conocido con el nombre de IKE. La gestión de claves IKE es íntegramente asíncrona con respecto a los mensajes de datos y no contribuye a generar ningún retardo durante el establecimiento de una comunicación. La única excepción a este respecto sería que se produjera un error imprevisto, cuando uno de los puntos de extremo perdiera inesperadamente la asociación de seguridad.

El IKE es un protocolo de gestión de claves entre pares, que consiste en dos fases. En la primera de ellas, se negocia un secreto compartido mediante un intercambio de claves Diffie-Hellman. Dicho secreto se utiliza, acto seguido, para autentificar la segunda fase del IKE, fase en la que se negocia otro secreto al que se recurre con el fin de derivar claves para el protocolo IPsec ESP.

9.2.4.3.1 Primera fase del IKE

Se definen tres distintos modos de autentificación durante la primera fase del IKE. La autentificación IKE con encriptado de clave pública NO DEBE utilizarse en la infraestructura NGN, ya que esto exige que el iniciador busque rápidamente la clave pública del respondedor. Puede soportarse la autentificación IKE con firmas y la autentificación IKE con llaves precompartidas.

El IKE define conjuntos específicos de parámetros Diffie-Hellman (primo y generador) que pueden utilizarse para la fase de intercambio IKE 1. El primer grupo puede ser soportado en elementos de red de la infraestructura NGN, y se recomienda que se soporten también los grupos restantes.

Si se recurre a la autentificación IKE con firmas, el cliente y el servidor pueden intercambiar certificados X.509 (véase la cláusula 8.3.2). Los certificados pueden verificarse, como se señala en la cláusula 8.3.

Cuando un elemento frontera de red acepta una conexión autentificada con un punto de extremo basándose en un certificado de usuario final NGN, el NBE puede implementar dos temporizadores en la conexión. El primer temporizador, T1, se inicia cuando se establece la conexión, mientras que el segundo, T2, lo hace cuando la conexión se establece, y se vuelve a poner a cero cada vez que durante la conexión se recibe una petición en el NBE. Cuando cada temporizador llega a su valor límite (lo que puede depender de los valores contenidos en el certificado), el NBE vuelve a poner a cero la conexión, que será restablecida por el punto de extremo para renovar el certificado de usuario final NGN.

Si se utiliza la autentificación IKE con claves precompartidas, se utilizará una clave derivada por algún mecanismo fuera de banda (esto es, manual) para autentificar el intercambio. Existen implementaciones que pueden permitir utilizar claves precompartidas de al menos 128 octetos. En los elementos de red no es necesario verificar los requisitos relativos a las claves precompartidas. Hay implementaciones que pueden soportar el modo agresivo definido en la cláusula 5.4 de [b-IETF RFC 2409] y utilizar el nombre de clave como identidad del iniciador/respondedor. Se sabe que el modo agresivo de IKE v1 [b-IETF RFC 2409] en combinación con una clave precompartida no es seguro. Con este modo, el troceo del secreto se transmite sin encriptar por la red, por lo que si un atacante intercepta el tráfico IP, puede extraer la clave con un ataque de fuerza bruta fuera de línea. Para evitar el cálculo de fuerza bruta de la clave precompartida a partir de su troceo, se recomienda utilizar una clave precompartida de 128 bits como mínimo.

Cuando se recurre a claves precompartidas, la solidez del sistema dependerá de la solidez del secreto compartido, pues se trata de evitar que el secreto compartido sea el eslabón débil de la cadena de seguridad. Esto hace necesario que el secreto compartido cuente con el mismo nivel de entropía (aleatoriedad) que la cifra que se esté empleando. Dicho de otro modo, se recomienda que el secreto compartido tenga al menos una entropía comprendida entre 128 y 160 bits.

9.2.4.3.2 Segunda fase del IKE

En la segunda fase del IKE se establece una asociación de seguridad ESP IPsec, lo que incluye las claves ESP y las series de cifras. Primeramente, se establece un secreto de segunda fase compartido y, a continuación, de dicho secreto se deriva todo el material de clave, recurriendo a la función unívoca especificada en [b-IETF RFC 2409]. El secreto de la segunda fase se forma a partir de números encriptados de una única utilización que se intercambian las dos partes. Aparte del encriptado de nombres de una única utilización, [b-IETF RFC 2409] permite otro intercambio Diffie-Hellman, aunque puede ocurrir que éste no se utilice en elementos de red de la infraestructura NGN. Esto se hace para evitar la penalidad de calidad de funcionamiento.

9.3 Protocolo de acuerdo de claves entre una zona no fiable y una zona fiable pero vulnerable

El protocolo de acuerdo de claves (AKA) especificado para redes IMS puede utilizarse también, si así se juzga viable. El protocolo de acuerdo de claves (AKA) y autentificación del sistema universal de telecomunicaciones móviles (UMTS) soporta una mutua autentificación de la estación móvil y de la red. UMTS AKA es un protocolo de puesta a prueba-respuesta que utiliza una clave *K* a largo plazo compartida por el módulo de identidad de abonado universal (USIM) y el centro de autentificación (AuC). Estas entidades residen, respectivamente, en la tarjeta de circuitos integrados

universal (UICC) de la estación móvil y en la red de base de la estación móvil. El protocolo AKA se especifica en [b-3GPP.33.102], Arquitectura de Seguridad.

Aunque el mecanismo AKA se emplea típicamente para autentificar dispositivos inalámbricos equipados con tarjetas inteligentes (por ejemplo, UICC), no hay nada en las especificaciones del AKA que impida utilizar dicho mecanismo para autentificar los dispositivos fijos capaces de ejecutar la aplicación USIM.

9.4 IPsec entre una zona no fiable y una zona fiable pero vulnerable

El TE-BE es un elemento de red NGN que reside en la zona no fiable. Con todo, sigue siendo gestionado por la portadora NGN y necesita acceso al sistema OAMP situado dentro de la zona fiable. Por consiguiente, existe un OAMP-SE que reside en la zona fiable pero vulnerable y actúa como punto de transmisión para los mensajes OAMP.

El TE-BE puede garantizar que las conexiones aseguradas por TLS no se ejecuten a lo largo del túnel VPN IPsec. El TE-BE puede garantizar que los trenes de medios asegurados con seguridad de medios SRTP no sean ejecutados a lo largo del túnel VPN IPsec.

El túnel VPN IPsec puede utilizar IPsec ESP [IETF RFC 4303] en modo túnel [b-IETF RFC 4301].

El servicio antitransmisión IPsec puede habilitarse en todo momento.

El túnel VPN IPsec puede soportar identificadores de transformación ESP_3DES (con un tamaño de clave de 192 bits y modo CBC) y ESP_CAMELLIA (con una clave de 128 bits y modo CBC) [b-IETF RFC 4312]. Se recomienda que el túnel VPN IPsec soporte el identificador de transformación ESP_AES (con una clave de 128 bits y modo CBC).

El túnel VPN IPsec puede soportar algoritmos de autentificación HMAC-MD5-96 (con clave de 128 bits), y HMAC-SHA-1-96 (con clave de 160 bits).

La generación de gestión de claves en relación con el túnel VPN IPsec puede hacerse con IKE [b-IETF RFC 2409], utilizando autentificación IKE con firmas digitales, o autentificación IKE con una clave precompartida. Si se recurre a la autentificación IKE con firmas digitales, el cliente y el servidor pueden intercambiar certificados X.509, certificados que pueden ser objeto de verificación.

10 Seguridad de medios

Encriptar medios no es necesario en la infraestructura NGN, pero puede exigirse que se soporte dicho encriptado si hay clientes que desean su utilización. Dicho soporte puede incluir el soporte de protocolos de encriptado de medios, SRTP [b-IETF RFC 3711]. En el resto de la presente cláusula se supone que los elementos frontera de red (es decir, el límite del dominio del proveedor de red) implementan encriptado/desencriptado, aunque es posible proceder de esta forma en una plataforma separada que compartan los NBE. En cada uno de ambos casos, es preciso que el encriptado/desencriptado se encuentre coubicado con otras capacidades de procesamiento de medios, tales como la detección y transcodificación multifrecuencia bitonal (DTMF).

Por lo que hace a la necesidad de conectar a los abonados que desean encriptado de medios en su enlace de acceso con aquellos que no lo desean (o no lo soportan), se plantean cuatro casos separados, como se indica en la figura 4.

El primero y más simple de dichos casos es aquel en el que ningún punto de extremo desea encriptado. Los medios fluirán del origen al destino, a través de elementos frontera, sin encriptado o enlace alguno. El elemento frontera de red (NBE) 1 (que sirve de originador) o el elemento frontera de red (NBE) 2 (que sirve de destino) no realizan encriptado alguno.

El segundo caso se produce cuando el originador, pero no así el destino, desea un tren de medios encriptado. En ese caso el NBE 1 actúa como un punto de retransmisión de encriptado/ desencriptado. El NBE 1 recibe la corriente de encriptado procedente del originador, la decripta y la transmite a través de la infraestructura NGN al NBE 2, que, a su vez, la transmite (sin encriptar aún) al destino. En el sentido opuesto, el NBE 1 recibe los medios sin encriptar a través de la infraestructura NGN y los encripta antes de enviarlos al originador. Después, los medios transmitidos a través del tramo 1 (del originador al NBE 1) se encriptan, mientras que los medios transmitidos a través del tramo 2 (entre el NBE 1 y el NBE 2) y del tramo 3 (entre el NBE 2 y el destino) no se encriptan.

El tercer caso tiene lugar cuando el destino, pero no así el originador, desea un tren de medios encriptado. El NBE 2 actúa como punto de retransmisión de encriptado/desencriptado. El NBE 1 recibe los medios sin encriptar del originador y los transmite (sin encriptar aún) a través de la infraestructura NGN al NBE 2, que encripta estos medios y los transmite al destino. En sentido opuesto, el NBE 2 recibe el flujo de medios encriptado del punto extremo de destino y lo decripta antes de transmitirlo a través de la infraestructura NGN. El NBE 1 transmite los medios no encriptados al originador. Así pues, los medios transmitidos a través de los tramos 1 y 2 no se encuentran encriptados, a diferencia de lo que sucede con los medios transmitidos a través del tramo 3.

El cuarto caso es aquel en el que el originador y el destino desean medios encriptados, pero ninguno de los dos soporta planes de encriptado compatibles o existe algún servicio mejorado que es proporcionado por la infraestructura NGN (por ejemplo, detección por multifrecuencia bitonal (DTMF) para aplicaciones de tarjeta de llamada). Tanto el NBE 1 como el NBE 2 actúan como puntos de retransmisión de encriptado/desencriptado. El NBE 1 recibe el tren encriptado del originador, lo desencripta y transmite a través de la infraestructura NGN al NBE 2. El NBE 2 lo encripta y transmite a su destino. En sentido opuesto, el NBE 2 recibe los medios encriptados del punto de extremo de destino y los desencripta antes de transmitirlos hacia adelante a la infraestructura NGN. El NBE 1 recibe los medios encriptados y los encripta antes de enviarlos al originador. De este modo, los medios transmitidos a través de los tramos 1 y 3 están encriptados, pero no así los medios que se transmiten a través de la infraestructura NGN (tramo 2).

El quinto caso es aquel en el que el originador y el destino desean medios encriptados, soportan planes de encriptado compatibles, y la infraestructura NGN no proporciona ningún servicio mejorado. El NBE 1 recibe los medios encriptados del originador y los transmite sin modificación alguna a través de la infraestructura NGN al NBE 2, que los transmite sin modificación al destino. En sentido opuesto, el NBE 2 recibe los medios encriptados o del destino y los transmite sin modificación a través de la infraestructura NGN al NBE 1, que los transmite sin alterarlos al originador. Así pues, los medios transmitidos a través de los tres tramos están encriptados. La señalización necesaria queda más allá del alcance de la presente Recomendación.

El encriptado de medios descrito en esta cláusula proporciona autentificación, confidencialidad e integridad de los mensajes.

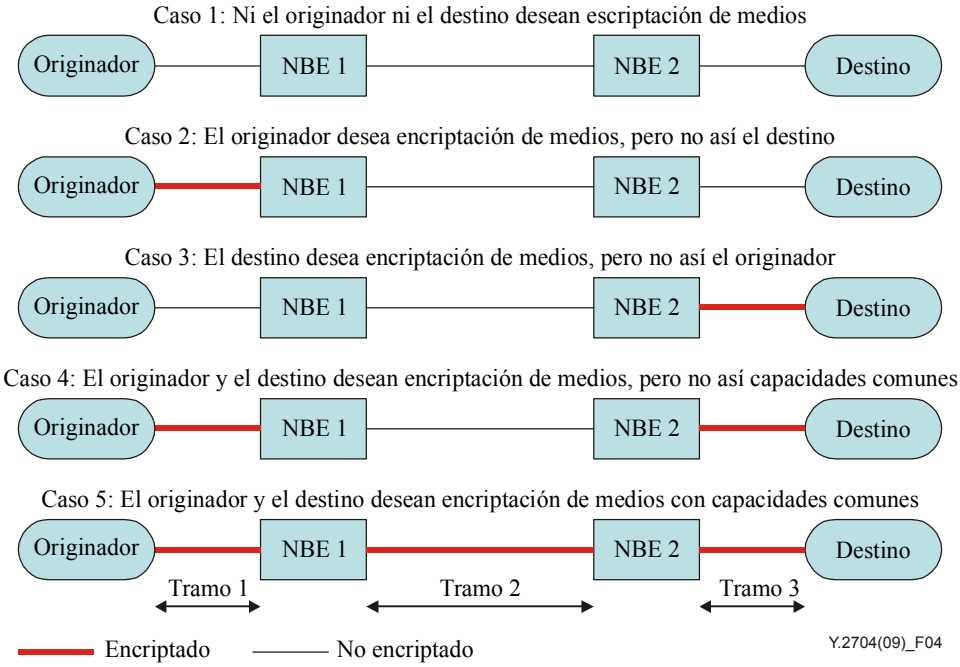


Figura 4 – Relación entre el encriptado de medios, las capacidades de los BE y los deseos del originador/destino

10.1 SRTP

El RTP seguro se describe en [b-IETF RFC 3711] y se define como un perfil de RTP [b-IETF RFC 3550]. La idea es implementarlo entre la aplicación RTP y la capa de transporte situada en la pila de protocolos – interceptando un paquete RTP y transmitiendo hacia delante un paquete SRTP equivalente en el lado de transmisión, e interceptando un paquete SRTP y transmitiendo el paquete RTP equivalente hasta la pila situada en el lado receptor. En esencia, el RTP seguro encripta la cabida útil del paquete RTP, añade una etiqueta de autentificación en el extremo del paquete en el lado de transmisión, verifica dicha etiqueta y descripta la cabida útil en el lado de recepción.

10.1.1 Algoritmos de encriptado y autentificación

Un NBE que apoye el SRTP puede soportar AES en modo opuesto [b-IETF RFC 3711]. Véase también [b-NIST FIPS SP 800-38a] para mayor información. El NBE puede soportar HMAC-SHA1 para generar verificaciones de integridad de mensaje, con una longitud de etiqueta de 80 bits.

10.1.2 Negociación de series de cifras y generación de claves

La generación de claves para el SRTP puede realizarse de diferentes modos:

1) mediante aprovisionamiento (sirviéndose de un elemento de aprovisionamiento TE);

2) utilizando el material de claves generado por el dispositivo situado en el punto de extremo e incluido en el protocolo de descripción de sesión (SDP) [b-IETF RFC 4566] en las peticiones INVITA;

3) el material de claves se intercambia utilizando un protocolo de gestión de claves separado y se transporta con SDP.

Para cada abonado, el NBE puede obtener de las SAA/TAA-FE la clave original SRTP y a partir de la misma derivar claves preliminares de encriptado y sesión de autentificación. Cabe la posibilidad de soportar una clave original SRTP con una longitud de 128 bits. Es posible soportar también el algoritmo de derivación de claves descrito en [b-IETF RFC 3711]. Las longitudes respectivas de la clave preliminar de encriptado, de la clave preliminar complementaria de sesión de la clave

preliminar de autentificación pueden ser 128, 112 y 160 bits. Cuando una nueva clave original SRTP se expide a un abonado, el NBE puede estar en condiciones de utilizarla inmediatamente.

Si el SDP contenido en la petición INVITA cuenta con "RTP/SAVP" en cuanto valor del protocolo de medios en la línea "m=", pero no así un valor de clave en la línea "k=", ni tampoco un atributo "a=crypto", el NBE puede utilizar las claves preliminares generadas a partir del sistema de aprovisionamiento como claves reales para la sesión. La serie de cifras en este caso, no es negociable.

Si el SDP contenido en la petición INVITA cuenta con "RTP/SAVP" como valor del protocolo de medios en la línea "m=" y no así el atributo "a=crypto" ni tampoco un valor de clave en una línea "k=", el NBE puede utilizar la clave contenida en la línea "k=" como clave original SRTP y generar a partir de ésta claves de sesión y autentificación. En este caso, la serie de cifras no es negociable.

Si el SDP contenido en la petición INVITA cuenta con "RTP/SAVP" en cuanto valor del protocolo de medios en la línea "m=" y un atributo "a=crypto", el NBE puede atender a los requisitos de [b-IETF RFC 4568] para generar las claves de sesión y autentificación. Así por ejemplo, la entrada SDP "a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:PS1uQCVeeCFCanVmcjkpPywjNWhcYD0mXXtxaVBR|2^20|1:4" indica que la serie de AES_CM_128_HMAC_SHA1_80, y el key_param se define en el texto, comenzando con "inline:". Dentro del key_param el primer campo está constituido por la clave original adjuntada junto con la clave complementaria original, concatenada y codificada en base 64. La lista de series de cifras válidas se consigna en la cláusula 5.2 de [b-IETF RFC 4568], y de estas series se escoge una como parte del intercambio oferta/respuesta SDP.

Si el SDP contenido en la petición INVITA cuenta con "RTP/SAVP" en cuanto valor del protocolo de medios en la línea "m=" y un atributo "a= key-mgmt", el NBE puede atender a los requisitos de [b-IETF RFC 4567] para generar parámetros de claves y seguridad. Así por ejemplo, "a=key-mgmt:mikey AQAFgM0XflABAAAAAAAAAAAA..." indica que el protocolo de gestión de claves es mikey [b-IETF RFC 3830], y que el texto restante está integrado por los datos de gestión de claves, que se codifican en base 64 [b-IETF RFC 4648].

10.1.3 Interfaz de autentificación entre el elemento de red NGN y el servidor de testigo seguro

Los elementos de red NGN pueden implementar SASL [b-IETF RFC 4422], que protege sus funciones OAMP. La capa SASL puede incluir una verificación de autentificación basada en el testigo de seguridad, según se define en [b-IETF RFC 2808]. Dicho testigo se identifica con la clave SASL "Testigo Seguro". El usuario que desee acceder a OAMP proporciona:

1) una identidad de autorización que permita a los administradores del sistema iniciar la sesión con una identidad de usuario distinta (si dicha identidad está vacía el sistema recurre por defecto a la identidad de autentificación);
2) una identidad de autentificación (una identidad cuya contraseña se utilizará); y
3) el valor del NIP del usuario y una contraseña de 6 dígitos en el testigo seguro.

El elemento de red puede actuar como un cliente conforme con SAA/TAA-FE como parte de la utilización del testigo seguro por parte de SASL. El elemento de red NGN recoge las credenciales del usuario presentadas y las envía al servidor de testigo seguro. Los campos recogidos incluyen el nombre del usuario, el código NIP y el valor del testigo seguro visualizado en ese momento. El elemento de red recibe un mensaje de estado aceptar/denegar/volver a intentar. Si el proceso prospera, el SASL habilita al usuario para acceder a las funciones OAMP, basándose en el nivel de acceso asociado con dicho nombre de usuario.

11 OAMP

Habrá que realizar un registro de auditoría de todos los intentos de acceso a OAMP (con independencia de su éxito), así como efectuar todos los cambios OAMP y ratificaciones OAMP. Por otra parte, se registran los eventos que se consideran significativos atendiendo a la política del proveedor NGN.

En esta cláusula se describen algunos mecanismos basados en importantes características. La lista de estos mecanismos no es exhaustiva y podrían adoptarse otras implementaciones, dependiendo de las políticas del proveedor NGN.

NOTA – El evento de registro exige seguridad. Para mayor información véase [UIT-T Y.2701] y [b-UIT-T M.3016.0].

11.1 Interfaz de los elementos de red con los sistemas de registro

Se recomienda que los elementos de red envíen la información sobre el registro al servidor distante encargado del registro. Estos elementos, que utilizan el protocolo Syslog [b-IETF RFC 5424] para llevar a cabo la función mencionada pueden atender a los requisitos señalados en esta cláusula.

Los elementos de red que utilizan el protocolo Syslog pueden incluir una indicación de tiempo, basándose en el valor recibido, a través de SNTP/NTP, de una fuente de tiempo fiable y el protocolo puede dar la indicación de tiempo en UTC. Los elementos pueden incluir el nombre de su servidor (si se ha aprovisionado este dispositivo) o su dirección IP en el encabezador del mensaje syslog.

11.2 Utilización del protocolo SNMP por parte de los elementos de red

Resulta indispensable que los elementos de red NGN puedan gestionarse a partir de una plataforma distante. El protocolo SNMP es el mecanismo normalizado de la industria idóneo para realizar dicha tarea. El SNMPv3 [b-IETF RFC 3413], [b-IETF RFC 3414], y [b-IETF RFC 3415] resuelve muchos de los fallos de seguridad que presenta SNMPv2, y es cada vez más fácil disponer del mismo en todas partes.

Se recomienda que los elementos de red envíen su información de registro al servidor distante encargado de iniciar la sesión. Dichos elementos pueden utilizar el protocolo SNMP para realizar esta tarea, con las reservas que se exponen en otras partes de la presente Recomendación en relación con el protocolo SNMPv3.

SNMP se caracteriza por una arquitectura global [b-IETF RFC 3411], el mecanismo requerido para nombrar objetos y eventos (MIBs) [b-IETF RFC 1155], [b-IETF RFC 1212], [b-IETF RFC 1215], [b-IETF RFC 2578], [b-IETF RFC 2579] y [b-IETF RFC 2580], y varias operaciones de protocolo [b-IETF RFC 3416] y [b-IETF RFC 3417]. Para una descripción más detallada de los documentos que describen el actual marco de gestión normalizada de Internet, véase la cláusula 7 de [b-IETF RFC 3410].

Todos los elementos de red NGN pueden actuar como un cliente SNMP. Si se emplea el SNMP v1 o el SNMP v2, y así lo requiere la política de seguridad del proveedor, estos elementos deben utilizar UDP o IPSec como medio de transporte. Cada instancia de un mensaje puede codificarse utilizando las reglas de codificación básicas ASN.1 [b-UIT-T X.690] en un único datagrama UDP. El cliente puede escuchar en los puertos 161 y 162 las instrucciones relativas, respectivamente, a las aplicaciones de respuesta de mandos y a las aplicaciones de recepción de notificación.

Es preciso que los elementos de red NGN realicen todos los MBI necesarios para informar acerca de los eventos de seguridad y los registros de auditoría.

11.3 Gestión de parches de seguridad

La instalación regular de parches de mantenimiento y seguridad en elementos y servidores de la red NGN reduce a un mínimo su vulnerabilidad ante ataques y fallos no intencionales. Es preciso desplegar una estrategia detallada de gestión de parches, que incluya procesos y plataformas de verificación e instalación.

11.4 Gestión de versiones

Es preciso realizar copias de seguridad de las configuraciones de los elementos de red y de los cambios introducidos en los mismos. El objetivo principal de la realización de copias de seguridad del sistema es permitir que éste se recupere en caso de que se produzcan problemas con el equipo o el soporte lógico que redunden en la corrupción de una carga para probar la solidez de los programas y/o los datos conexos del sistema. Cabe la posibilidad de incluir los siguientes tipos de información en una carga para probar la solidez del sistema:

- Datos y lógica de cliente.
- Conectividad del tráfico de la red; por ejemplo facilidades y enlaces.
- Soporte lógico de aplicación proporcionado por el operador de la NGN y el vendedor.
- El sistema operativo.
- La configuración del equipo.

Es necesario mantener un registro en curso de las actividades de aprovisionamiento, con el fin de que todos los elementos de red (NE) puedan actualizarse con las acciones de aprovisionamiento que se hayan efectuado desde la realización de una imagen de copia de seguridad.

La plataforma de prestación puede proporcionar las siguientes capacidades.

- Un diario de las actividades de aprovisionamiento para cada uno de los elementos de la red que se aprovisione directamente.
- Al menos una semana de actividades de aprovisionamiento para cada NE.

La plataforma de aprovisionamiento puede permitir a los usuarios examinar manualmente las actividades de aprovisionamiento almacenadas para cada NE. Es preciso que en la descripción de las actividades proporcionadas al usuario se resuman la magnitud, el número y el tipo de las diferentes transacciones en un periodo dado.

La plataforma de aprovisionamiento puede proporcionar una utilidad que permita el reaprovisionamiento de un NE designado, volviendo a introducir los datos en un NE especificado. En este dispositivo debería ser posible la selección de datos y tiempo de inicio y término en relación con los datos que deban volver a aprovisionarse. Basándose en las fechas/tiempos de inicio y término especificados, la plataforma de aprovisionamiento debería reintroducir automáticamente todos los datos que se hayan obtenido entre esos dos puntos temporales en el NE que se especifique.

11.5 Registro de auditoría, arranque e inicio de sesión en los TE-BE

Todos los requisitos referentes al registro de auditoría, el arranque y la realización de copias de seguridad aplicables a los elementos de la red NGN se aplican también a los TE-BE.

Los TE-BE están conectados a los sistemas OAMP a través de un túnel VPN. En consecuencia, los TE-BE envían sus mensajes de realización de copias de seguridad, reciben peticiones SNMP y envían respuestas SNMP a través del túnel VPN. Se recomienda que los TE-BE no acepten petición alguna OAMP en cualquier otra interfaz.

Los requisitos de los túneles VPN se consignan en la cláusula 9.4.

12 Aprovisionamiento de equipos en zonas no fiables

El elemento de aprovisionamiento TE configura todos los equipos situados en los locales del cliente. Este elemento reside en la zona fiable y sólo puede comunicar con los TE a través del elemento frontera de red (NBE), como se indica en la figura 2. Un TE o TE-BE puede autentificar y establecer una asociación de seguridad con el NBE antes de que éste pueda obtener un fichero de configuración del elemento de aprovisionamiento TE. El NBE puede soportar TLS e IPsec para establecer SA con los TE (incluidos los TE-BE). Para mayor detalle, véanse las cláusulas 9.1 y 9.2.

En este contexto el equipo controlado por el proveedor puede considerarse como parte del NBE.

El elemento de prestación TE incluye la dirección de un NBE que figure en los datos de configuración descargados al dispositivo autentificado. El elemento de prestación TE puede incluir también un certificado que se utilizará para autentificar el abonado con el NBE descrito en la cláusula 8.4.

Un dispositivo TE solicitará aprovisionamiento por parte del proveedor de servicio NGN. El NBE recibirá esta petición y autentificará el TE con las SAA/TAA-FE. Cuando el dispositivo se haya autentificado, el elemento frontera transmitirá hacia adelante al elemento de aprovisionamiento TE la petición de aprovisionamiento. A continuación, este elemento de aprovisionamiento procede a descargar la configuración y/o el programa intermedio (*firmware*) al TE. Si el TE no puede ser autentificado, se registra dicho fracaso.

Apéndice I

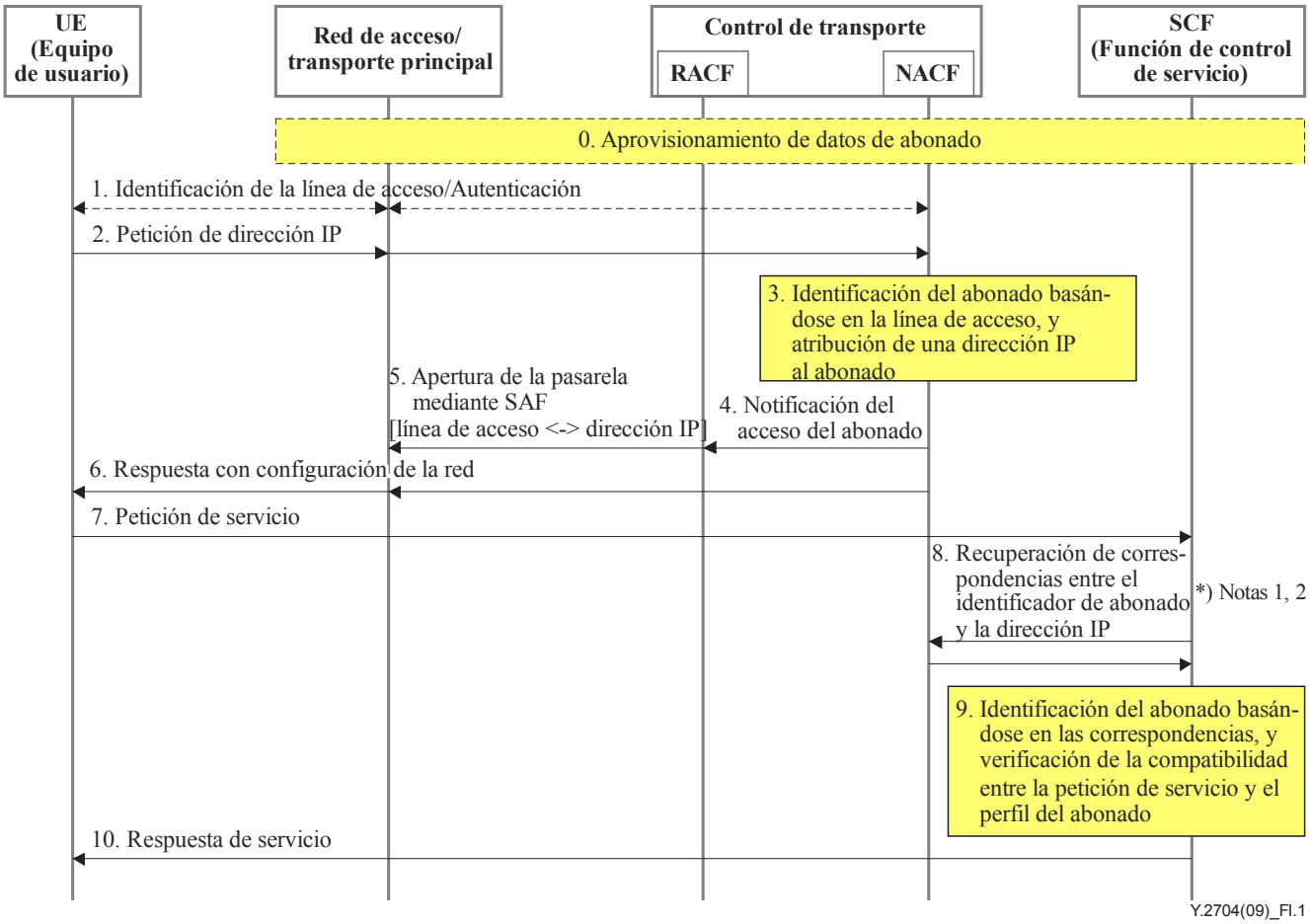
Ejemplos de garantía de dirección de origen y su aplicación al mecanismo de identificación autentificación de abonado

(Este apéndice no forma parte integrante de la presente Recomendación)

En este apéndice se dan una serie de ejemplos concretos en relación con los mecanismos de garantía de la dirección de origen y de su aplicación a la identificación y autentificación de abonado mediante la dirección de origen de red descrita en la cláusula 8.4.2.

I.1 Identificación y autentificación de abonado relacionada con la autentificación de la línea de acceso

En la presente cláusula se ofrece un ejemplo de la identificación y autentificación del abonado, en el cual puede verse que se asigna una dirección IP como resultado de la autentificación de la línea de acceso. Asimismo, todos los abonados se asocian estáticamente con su línea de acceso. Así pues, el mecanismo descrito resulta aplicable únicamente a los servicios no nómadas (esto es, fijos).



NOTA 1 – La información de correspondencia entre la dirección IP y el identificador de abonado puede proporcionarse a partir de la NACF a la SCF en el momento en que la NACF atribuya la dirección.

NOTA 2 – La NACF puede proporcionar las correspondencias existentes entre la dirección de IP y la información de ubicación (por ejemplo, identificador de línea) en lugar de proceder a determinar las correspondencias entre la dirección IP y le identificador de abonado. De ser así, es necesario que la SCF mantenga las correspondencias entre los identificadores de abonado y las respectivas ubicaciones y derive la identidad del abonado basándose en la información de ubicación enviada a partir de la NACF.

Figura I.1 – Flujos de mensaje de alto nivel del ejemplo 1

Descripción

0. Los perfiles de abonado se preconfiguran atendiendo a las FE correspondientes (por ejemplo, TUP-FE, SUP-FE), en la NACF o en la SCF.

   Los aspectos más importantes en materia de establecimiento en este escenario son los siguientes:

   1) La NACF (típicamente una TUP-FE) mantiene las correspondencias entre las identidades de los abonados (identificadores de cuentas de abonados) y las identidades de las líneas de acceso lógicas/físicas (por ejemplo, ID VLAN o puerto de acceso).

   2) La SCF (típicamente una SUP-FE), mantiene las correspondencias entre las identidades de los abonados y los atributos o perfiles de los correspondientes abonados (por ejemplo, valores del encabezador "a partir de" en el caso de servicios basados en el SIP). Cuando el espacio de nombres de las identidades de los abonados en la SCF difiera de los correspondientes en la NACF, se recomienda que la CSF mantenga igualmente las correspondencias entre dichas identidades.

      Por otra parte, no hay razón por la que la NACF deba mantener las correspondencias entre las identidades de los abonados y las entidades de las líneas de acceso. En estos casos, se recomienda que la SCF mantenga las correspondencias entre las identidades de los abonados y las entidades de las señales de acceso, para que la SCF pueda recuperar la identidad del abonado correspondiente a partir de la identidad de una línea de acceso.

      En las pasarelas en el transporte de acceso/núcleo, todas las puertas de las líneas de acceso de abonado se configuran inicialmente de manera tal que se cierren, con el fin de que cualquier paquete IP entrante, excepto por el hecho de que se descartan los paquetes necesarios para que el UE alcance la red (por ejemplo, enviando peticiones de dirección o peticiones de autentificación).

1. Un UE alcanza la red de acceso mediante su línea de acceso para conseguir conectividad IP con la NGN. En este caso, se supone que la autentificación de acceso realizada por la NACF es implícita y se ejecuta en la etapa 3. Con todo, opcionalmente, la NACF puede utilizar un método de autentificación de acceso explícita (por ejemplo, IEEE 802.1X). En este caso, la autentificación de acceso a la red se ejecuta en esta etapa, esto es, antes de asignar direcciones IP.

2. El UE pide que se atribuya una dirección IP, tarea que se realiza típicamente enviando Discover and Request DHCP, las pasarelas retransmiten estos mensajes a la NACF.

3. En este ejemplo, el acceso a la red autentifica la línea de acceso que corresponda y proporciona identidad de línea de acceso autentificada (por ejemplo, VLAN ID o puerto de acceso) a la NACF. Así pues, este último puede identificar la identidad de abonado del UE, basándose en la identidad de la línea de acceso, a través de la cual se envía la petición de dirección IP. A continuación, la NACF atribuye una dirección IP en el UE solicitante y almacena la correspondencia entre la ID de abonado y la dirección IP atribuida.

   Esta información de correspondencia puede ser enviada a partir de la NACF a la SCF y almacenarse (ocultarse) en la SCF. De ser así, puede soslayarse la etapa 8 indicada más abajo.

4. La NACF notifica a la RACF que sea conectada al abonado. Esta notificación incluye la identidad del abonado, la identidad de la línea de acceso (física/lógica), la dirección IP atribuida y los perfiles de calidad del servicio.

5. La RACF adopta una decisión de políticas sobre la atribución de recursos de red al abonado y ordena a las cabeceras que abran la puerta para la línea de acceso con una serie de reglas de filtrado de paquetes, que se definen para aceptar y encaminar hacia adelante los paquetes IP entrantes cuya dirección de fuente coincide con la dirección IP asignada al abonado, y que descarten otros paquetes entrantes.

   La ejecución obligatoria del filtrado de direcciones IP de fuente, junto con la coordinación de éste con la autentificación de la línea de acceso por parte de la NACF, que se ha descrito ya, garantiza que una dirección IP sólo pueda ser utilizada por el abonado al que se asigna la dirección.

6. La NACF devuelve la dirección IP atribuida al UE con otros parámetros de configuración de red (por ejemplo, las direcciones de los servidores DNS y las P-CSC-FE). Esto se realiza típicamente enviando Oferta DHCP y mensajes de respuesta.

7. Tras conseguir la conectividad IP, el UE envía a la SCF una petición de servicio (por ejemplo, señal REGISTRO, tratándose de los servicios basados en la SIP). Las pasarelas (cortafuegos con el filtrado de direcciones de origen) dejan pasar la petición de servicio hacia la SCF, únicamente si la dirección de origen de la petición corresponde a una de las asignadas por la NACF.

8. La SCF recupera de la NACF la información de correspondencias (esto es, la identidad del abonado y la dirección IP asignada) relativa a la dirección de origen de la petición de servicio.

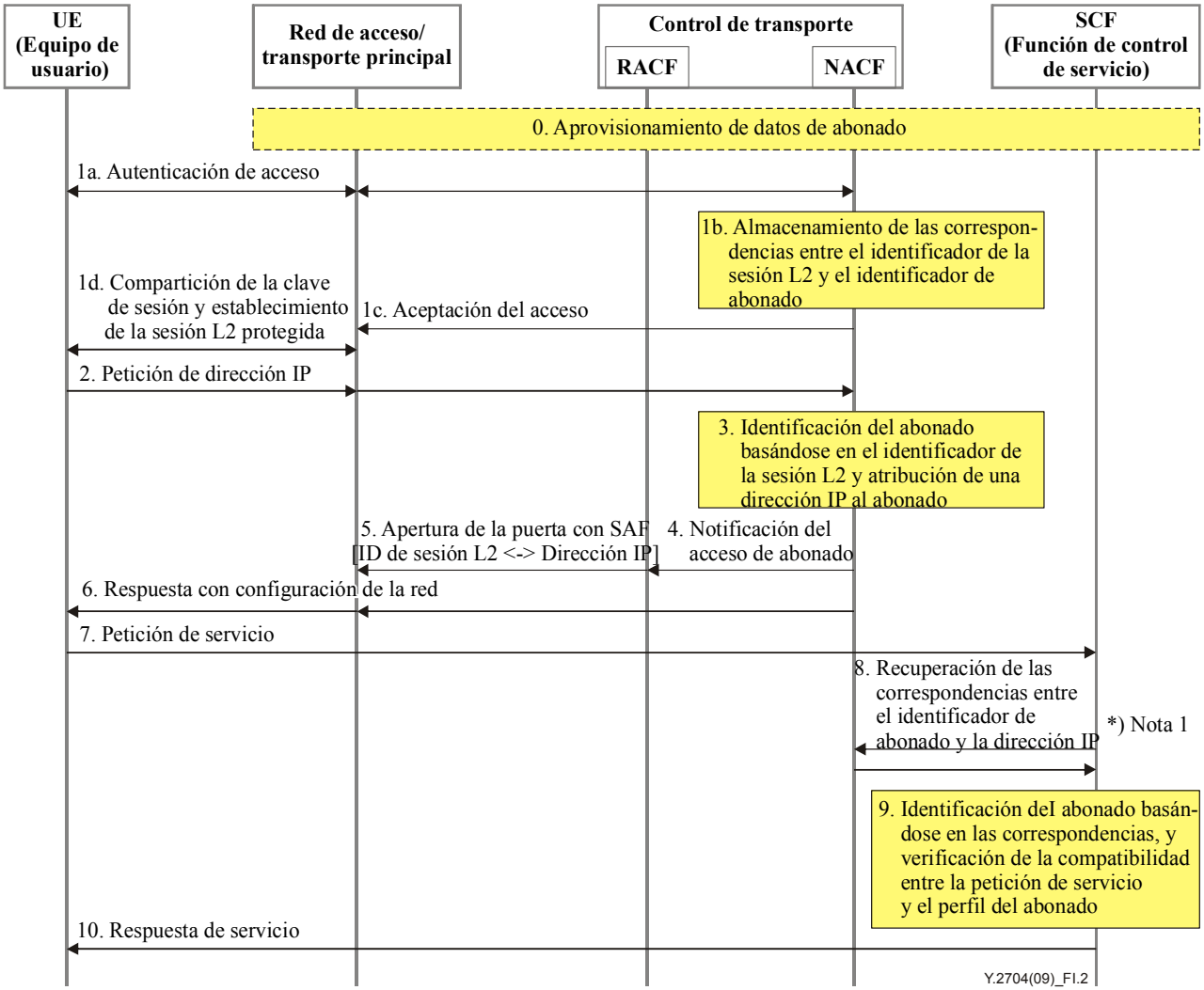
9. La SCF examina la petición de servicio que habrá de originarse a partir del abonado que asignó la identidad de abonado contenida en la información sobre correspondencias recuperada. Cuando el espacio de nombres de los identificadores de abonado en la SCF difiera del que figura en la NACF, la identidad de abonado recuperada habrá de traducirse a la identidad de abonado que figura en el espacio de nombres utilizado por la SCF, basándose en las correspondencias existentes entre dichos identificadores.

   La SCF extrae de la petición de servicio el valor de los atributos relativos a la identidad del abonado (por ejemplo, el valor del encabezador "De", tratándose de servicios basados en el SIP) y verifica la coherencia entre ambos valores y el correspondiente perfil del abonado.

10. Si la autentificación y la autorización se realizan con éxito, el SCF devuelve la respuesta normal para ofrecer el servicio solicitado (por ejemplo, "200 OK", en el caso de los servicios basados en el SIP).

I.2 Identificación y autentificación de abonado vinculadas a las autentificaciones explícitas de acceso en el establecimiento de la conectividad IP

En esta cláusula se ofrece un ejemplo de identidad y autentificación del abonado, en el cual puede verse que se asigna una dirección IP como resultado de una autentificación de acceso explícita durante el establecimiento de la conectividad IP. En este ejemplo se asocia dinámicamente a cada abonado o una sesión L2, que se establece en el momento en que se realiza la autentificación de acceso. Así pues, el mecanismo descrito en este ejemplo resulta aplicable tanto a los servicios nómadas como a los que no lo son.



NOTA 1 – Puede proporcionarse a la SCF a partir de la NACF la información de correspondencia entre la dirección IP y el identificador de abonado, en el momento en que la NACF atribuya la correspondiente dirección.

Figura I.2 – Flujos de mensaje de alto nivel del ejemplo 2

Descripciones

0. Los perfiles de abonado se preconfiguran en la NACF o la SCF atendiendo a la correspondiente FE (por ejemplo, TUP-FE, SUP-FE). A diferencia de lo que ocurría en el ejemplo anterior, la NACF no necesita mantener las correspondencias entre los identificadores de abonado y los identificadores de línea de acceso.

   En las pasarelas situadas en la red de acceso/transporte principal, se descartan todas las puertas destinadas a las sesiones de acceso L2 con UE, que se configuran inicialmente de manera tal que se cierren para impedir la entrada de cualquier paquete IP entrante, con la excepción de los paquetes necesarios para que los UE se adjunten a la red (por ejemplo, enviando peticiones de dirección o peticiones de autentificación).

1a. Cuando un UE solicita conectividad a la NGN, la red de acceso crea dinámicamente una sesión L2 con el UE, y un procedimiento de autentificación de acceso se realiza entre el UE y la NACF, sobre la base de la credencial del abonado (aplicando típicamente un método de autentificación explícito, por ejemplo IEEE 802.1X y RADIUS/Diameter). Las pasarelas envían hacia adelante mensajes de señalización para que se realice la autentificación.

1b. Durante el procedimiento de autentificación, el identificador de la sesión L2 (por ejemplo, VLAN-ID, dirección L2 del UE, etc.) asignado al UE se envía a la NACF. Cuando la autentificación se efectúa con éxito, la NACF almacena el identificador de la sesión L2 con el identificador de abonado autentificado.

1c. La NACF notifica la red de acceso que el UE se ha autentificado con éxito y que se ha autorizado el acceso a la red (por ejemplo un mensaje ACEPTAR ACCESO, tratándose del protocolo RADIUS).

1d. Tras recibir la notificación de la NACF sobre el éxito de la autentificación del abonado, la red de acceso establece una asociación de seguridad (SA) con el UE para proteger la integridad y confidencialidad de la sesión L2. Típicamente, esto se consigue recurriendo a los mecanismos de derivación de claves de sesión definidos en IEEE 802.1X y al procedimiento de protección definido para cada tecnología L2 (por ejemplo, TKIP/CCMP definido en IEEE 802.11i para LAN inalámbrica 802.11).

Los mecanismos de seguridad antes expuestos protegen la sesión L2 contra su utilización por otros proveedores y sienta las bases necesarias para impedir la usurpación de direcciones IP.

2. El UE solicita que se atribuya dirección IP, lo que se realiza típicamente, enviando DHCP Discover y Request, y las pasarelas retransmiten estos mensajes a la NACF.

3. La NACF identifica la entidad de abonado del UE, basándose en el identificador de la sesión L2, cuya solicitud se envía. Acto seguido, la NACF atribuye una dirección IP al UE solicitante y almacena las correspondencias entre el identificador de abonado y la dirección IP atribuida.

Esta información sobre correspondencias puede transmitirse a partir del NACF a la SCF y almacenarse (ocultarse) en la SCF. En este caso, puede saltarse el paso 8.

4. La NACF notifica a la RACF que el abonado ha sido conectado. Esta notificación incluye el identificador de abonado, el identificador de la sesión L2 (física/lógica), la dirección IP atribuida y los perfiles de calidad de servicio.

5. La RACF adopta una decisión de política en lo que respecta a la atribución de recursos de red al abonado y ordena a las pasarelas que abran la puerta a la sesión L2 con una serie de reglas de filtrado de paquetes, que se definen para aceptar transmitir hacia adelante los paquetes IP entrantes cuya dirección de origen es la dirección IP asignada al abonado, y que descarte otros paquetes entrantes.

La obligada ejecución del filtrado de direcciones IP de origen, coordinada con la autentificación de acceso por parte de la NACF, antes descrita, garantiza que una dirección de IP sólo pueda ser utilizada por el abonado al que se asignó la dirección.

Los pasos 6-10 son idénticos a los del ejemplo de la cláusula I.1 anterior.

Apéndice II

Seguridad de la interconexión en el servicio de telecomunicaciones de emergencia (STE)

(Este apéndice no forma parte integrante de la presente Recomendación)

II.1 Antecedentes

El servicio de telecomunicaciones de emergencia (STE) es un servicio nacional en cuyo marco se prestan servicios prioritarios a usuarios autorizados en situaciones de catástrofe y emergencias. La implementación del STE es un asunto de la incumbencia de los diferentes países. Con todo, las catástrofes y las emergencias pueden trascender las fronteras geográficas, por lo cual cabe la posibilidad de que los países/administraciones concierten acuerdos bilaterales y/o multilaterales para conectar sus respectivos sistemas STE. Esto permitiría prestar en momentos de catástrofe y emergencia servicios de telecomunicaciones (por ejemplo, voz, mensajería, vídeo y datos) prioritarios en el marco del STE, servicios que soportarían las redes nacionales, gracias a la concertación de acuerdos bilaterales y/o multilaterales. La garantía y disponibilidad de las comunicaciones STE dependerá de las capacidades y medidas de seguridad de obligado cumplimiento establecidas en cada red nacional que participe en una comunicación de extremo a extremo.

II.2 Alcance/objetivo

En el presente apéndice se proporciona orientación para permitir el soporte de la seguridad de red proporcionada para las comunicaciones STE en las implementaciones STE de las diferentes redes nacionales (esto es, países/administraciones).

La función de seguridad de usuario final entre pares que utiliza funciones especiales de seguridad de equipo de usuario final no se examina en el presente apéndice, que se limita a la seguridad de red proporcionada salto a salto para las comunicaciones STE a lo largo de múltiples redes. Se recomienda que la NGN sea capaz de soportar sin interfaces dichas funciones entre pares.

Este apéndice no tiene por objeto imponer condiciones sobre las implementaciones nacionales del STE y su objetivo principal es permitir la prestación de seguridad por una red para las comunicaciones prioritarias (de voz, vídeo, datos, y mensajería) a través de distintas redes nacionales (esto es, países/administraciones).

II.3 Objetivo de seguridad y directrices para la interconexión en el STE

Para informarse sobre los objetivos de seguridad y las directrices de interconexión en el STE, véase el apéndice I [UIT-T Y.2701].

II.4 Autentificación y autorización

Se recomienda que las redes nacionales soporten e implementen mecanismos y capacidades para autentificar y autorizar a un usuario, dispositivo o combinación de usuario y dispositivo del STE, basándose en el nivel de garantía necesario para acceder a un servicio específico (por ejemplo, voz, datos, vídeo) y la política del caso.

Se recomienda que los mecanismos de seguridad descritos en el cuerpo de la presente Recomendación, con miras a la identificación y autentificación de usuarios y dispositivos de usuario se utilicen, en su caso, para soportar implementaciones del STE en las redes nacionales:

- Asociaciones IPsec/TLS.
- Puesta a prueba/respuesta SIP y certificados X.509.
- Arquitectura genérica de arranque y asignación.

Asimismo, se recomienda adoptar medidas de seguridad para supervisar el acceso a los recursos STE, con el fin de detectar e impedir los diferentes tipos de ataques de denegación del servicio.

Asimismo, remitimos al apéndice I [UIT-T Y.2702] con propósitos de información sobre ejemplos de enfoques de autentificación y autorización STE.

II.5 Seguridad de transporte para la señalización y OAMP

Se recomienda que los mecanismos de seguridad, IPsec y TLS, descritos en el cuerpo de la presente Recomendación se utilicen, en su caso, para proteger el tráfico de señalización y OAMP del STE en las redes nacionales.

II.6 Tráfico de medios

Se recomienda que los mecanismos de seguridad destinados a identificar y proteger el tráfico de medios, descritos en el cuerpo de esta Recomendación, se utilicen, en su caso, para proteger el tráfico de medios STE en las redes nacionales.

II.7 Características restrictivas del soporte de la identidad de número llamante y de la identidad de nombre de llamante

La identidad de número llamante y la identidad de nombre de llamante son dos características de la RTPC heredadas que permiten a los usuarios determinar quién los llama. Las llamadas STE pueden atender a diferentes comunidades nacionales de usuarios con distintas sensibilidades ante la comunicación de dicha información a la parte llamada. En consecuencia, se recomienda soportar el correspondiente mecanismo para velar por el obligado cumplimiento de la política relativa al despliegue y comunicación de información de usuario STE.

II.8 Ausencia de rastro

Para ciertas comunicaciones STE resulta importante hacer todo por lo posible por que la información de ubicación relacionada con la parte llamante y la parte llamada no quede a disposición de todas las partes. En particular, se recomienda suprimir la información referente a la ubicación o, si así se estima necesario, sustituirla por una información poco importante, basándose en la política aplicable. La información relacionada con la ubicación incluye, entre otras cosas:

1) NPA-NXX o URI de las partes llamante y llamada.
2) Dirección geográfica de las partes llamante y llamada.
3) Coordenadas bidimensionales de las partes llamante y llamada.
4) Información celular de las partes llamante y llamada que pueda utilizarse para circunscribir la ubicación en una célula.
5) Dirección IP de las partes llamante y llamada.
6) Oficina de extremo de las partes llamante y llamada, o cualquier otra información sobre facilidades que permita determinar la proximidad geográfica de la parte llamante.

II.9 Encriptado entre pares de extremo a extremo

Una serie de usuarios puede solicitar llamadas/sesiones STE encriptadas con equipo de usuario (UE). Tratándose de dichas llamadas/sesiones, se aplicarían procedimientos normales de establecimiento de llamada/sesión STE y el UE proporcionaría el encriptado de extremo a extremo para la información de portadora (por ejemplo, voz) destinada al UE de terminación. El proceso de encriptado no tiene interfaz con respecto a la NGN. Sin embargo, se recomienda que la NGN sea capaz de soportar sin interfaces dichas funciones entre pares.

Apéndice III

Prácticas óptimas en materia de seguridad

(Este apéndice no forma parte integrante de la presente Recomendación)

III.1 Introducción

Para atender a los requisitos especificados en [UIT-T Y.2701] puede ser necesario contar con mecanismos de seguridad adicionales, aparte de los especificados en la presente Recomendación. Pueden emplearse mecanismos de seguridad de práctica óptima, tales como el fortalecimiento del sistema operativo, el análisis de la vulnerabilidad, y el establecimiento de sistemas de detección de intrusiones (IDS), para garantizar la seguridad en la infraestructura NGN. En [b-NIST SP 800-94] se proporciona orientación sobre los sistemas de detección y prevención de intrusiones (IDPS) y en [b-NIST SP 800-83] sobre NIST para la prevención y tratamiento de incidentes ocasionados por programas maliciosos.

En este apéndice se ofrece un resumen de algunos ejemplos de mecanismos de seguridad correspondientes a prácticas óptimas que deberían emplearse.

III.2 Cortafuegos

Los cortafuegos son bloques fundamentales en la constitución de la seguridad que permiten aislar redes en las fronteras comprendidas entre los segmentos de una red o entre diferentes redes. Los cortafuegos realizan el aislamiento basándose en reglas específicas de filtrado de tráfico configuradas en los cortafuegos. Los cortafuegos pueden utilizarse junto con otros mecanismos de seguridad para obtener una capa adicional de seguridad. La adición de cortafuegos contribuye a proporcionar una seguridad "radicalmente defensiva", debido al hecho de que se sobreimponen múltiples mecanismos de seguridad para lograr una mayor seguridad.

Un cortafuegos examina el tráfico entrante y el saliente, y debería configurarse para denegar todo tráfico, salvo el permitido específicamente por las reglas de cortafuego. Asimismo, un cortafuego puede proporcionar registro de tráfico y activar alarmas cuando se detectan paquetes no autorizados. Los cortafuegos pueden proporcionarse físicamente como dispositivos separados u ofrecerse como programas informáticos incorporados a los propios servidores. Entre los diferentes tipos de cortafuegos, cabe citar los que incorporan filtrado estático de paquetes o capa de aplicación, así como los cortafuegos de filtrado de paquetes conscientes de estados, por lo cual la elección de uno de ellos dependerá de las necesidades y preferencias del cliente.

Los cortafuegos de filtrado estático de paquetes examinan los paquetes entrantes y salientes y aplican un conjunto de reglas para determinar cuáles serán los paquetes que podrán atravesar el cortafuegos o cuáles serán descartados. Dicha determinación se basa típicamente en el origen de los paquetes y la dirección IP de destino, el tipo de protocolo y el origen y los puertos de destino TCP. Dependiendo de los paquetes y los criterios adoptados, el cortafuegos descartará o transmitirá hacia adelante dichos paquetes, y, posiblemente, creará una entrada de registro y/o activará una alarma. Algunos cortafuegos estáticos de filtrado de paquetes pueden proporcionar, igualmente, una inspección detallada de los paquetes, posiblemente, hasta la capa de aplicación.

Los paquetes de capa de aplicación ejecutan aplicaciones en nombre de las máquinas situadas en la red que protegen, y con frecuencia se califican como "sustitutivos" a estos cortafuegos. Al implementar las aplicaciones, los cortafuegos de capa de aplicación detectarán cualquier actividad anómala y, de ser así, no dejarán pasar los datos a las máquinas que protegen. Los cortafuegos de capa de aplicación pueden habilitarse con todas las aplicaciones necesarias y deben ejecutar dichas aplicaciones en nombre de todas las máquinas protegidas. Por esta razón, los cortafuegos de capa de aplicación ejercen gran influencia en la calidad de funcionamiento de la red.

Los cortafuegos conscientes de estados desempeñan funciones de filtrado de paquetes análogas a las que realizan los cortafuegos de filtrado estático de paquetes, y, además, mantienen la información correspondiente al estado de las conexiones de tráfico. La información de estado permite a un cortafuegos adoptar decisiones más adecuadas sobre el hecho de si debe autorizar o denegar un determinado tráfico. Así por ejemplo, un cortafuegos consciente de estados puede configurarse de manera tal que sólo autorice el tráfico procedente de máquinas situadas en un lado de la red para iniciar comunicaciones. Esto reviste particular importancia cuando las redes privadas se encuentran conectadas con redes públicas.

Para utilizar cortafuegos en calidad de señalización y seguridad de plano de control adicionales, los cortafuegos deberían configurarse para utilizar únicamente la señalización y la comunicación de control deseadas entre un conjunto de máquinas. Todo tráfico de la red distinto de las comunicaciones deseadas debería denegarse, proporcionando así una capa de protección a estas máquinas.

Hay que señalar que el aprovisionamiento de cortafuegos puede repercutir en la ingeniería de sistemas, y hacer que algunas aplicaciones deban fabricarse de forma tal que sean conscientes de cortafuegos. Hay que señalar también que los cortafuegos no protegerán contra ataques de seguridad tales como los que se realizan para usurpar información legítima de paquetes de señalización.

III.3 Fortalecimiento de los sistemas operativos

Los servidores y los elementos de la red que utilizan funciones de señalización y de plano de control son vulnerables ante varios ataques, entre los cuales cabe mencionar los siguientes:

- Programas que abren puertas traseras.
- Programas de rastreo.
- Herramientas de pirateo y desciframiento de claves.
- Explotación de defectos en los servicios del sistema operativo.
- Denegación del servicio (DoS).

Alguno de estos ataques se basan en técnicas muy conocidas, las cuales se utilizan junto con guiones y otras herramientas disponibles, que permiten a los piratas menos hábiles aplicar a los sistemas programas de aprovechamiento. Una vez que el sistema ha sido pirateado, un intruso puede optar, entre otras cosas, por lo siguiente:

- Modificar o destruir información.
- Divulgar información sensible.
- Instalar códigos maliciosos para reunir información.
- Utilizar el servidor pirateado para atacar otros sistemas.

Los procedimientos destinados a fortalecer los sistemas operativos pueden utilizarse para mejorar la resistencia contra ataques de estos sistemas. Los procedimientos mencionados consisten esencialmente en prácticas adecuadas, que se implementan durante la instalación o configuración de un sistema operativo. Aunque ninguno de estos sistemas es absolutamente seguro, los siguientes procedimientos para fortalecer los sistemas operativos hacen que éstos sean más difíciles de piratear.

El fortalecimiento de un sistema operativo entraña esencialmente restringir la utilización de servicios, puertos y accesos a aplicaciones y ficheros, así como ejecutar aplicaciones sólo a partir de cuentas restringidas de acceso privilegiado y únicamente con los puertos y servicios activados necesarios. Debería consultarse a los fabricantes de sistemas operativos con el fin de obtener los procedimientos más recientes para fortalecer sistemas operativos y parches de seguridad.

III.4 Evaluación de la vulnerabilidad

Realizar una evaluación de la vulnerabilidad de los elementos de una red tiene por objeto descubrir factores de vulnerabilidad y debilidad, así como zonas de riesgo en materia de seguridad. Los problemas de vulnerabilidad se diseñan con el fin de hacer que los sistemas fallen deliberadamente, interrumpiendo servicios, soslayando los controles de seguridad previstos, capturando datos confidenciales, obteniendo acceso no autorizado al sistema, o hurtando o denegando servicios. Asimismo, puede evaluarse la vulnerabilidad de los elementos de la red NGN para garantizar un nivel aún mayor de seguridad.

La evaluación de la vulnerabilidad de los elementos de red puede efectuarse durante la fase de verificación de los productos y, ulteriormente, como parte del mantenimiento de la red. Resulta conveniente realizar pruebas de vulnerabilidad en materia de seguridad durante la fase de verificación de los productos puesto que existe ya un procedimiento preestablecido para registrar y someter peticiones de cambio. Realizar evaluaciones de vulnerabilidad rutinarias es útil si se desea identificar nuevas amenazas y factores de vulnerabilidad, e iniciar acciones para mitigar los problemas identificados.

III.5 Sistemas de detección de intrusiones

Los sistemas de detección de intrusiones pueden utilizarse para proporcionar protección contra intrusiones y acciones no autorizadas. Así por ejemplo, cabe utilizar sistemas de detección de intrusiones para alertar a los administradores de la red acerca de la posibilidad de que se produzca un incidente de seguridad, por ejemplo el pirateo de un servidor SIP o un ataque de denegación del servicio.

Los sistemas de detección de intrusiones (IDS) pueden clasificarse en general con arreglo a los siguientes criterios:

- Detección de incidentes en tiempo real o fuera de línea: Un sistema IDS analiza el tráfico de la red en tiempo real y registra los eventos que se producen. Un sistema IDS fuera-línea analiza intrusiones en modo de pila una vez que los incidentes se hayan producido.
- Instalación basada en la red o en el servidor: Un IDS basado en la red entraña típicamente la instalación de varios monitores en puntos de estrangulamiento de la red donde el tráfico entre dos puntos puede ser supervisado. Un IDS basado en el servidor hace necesario instalar directamente los correspondientes programas informáticos en los servidores que habrá que proteger, y supervisa las conexiones de la red y la actividad de usuario en dichos servidores.
- Reactivo o pasivo: Un IDS reactivo interviene activamente para contrarrestar ataques, modificando reglas de cortafuego o filtros de encaminador o adoptando otras medidas. Un sistema IDS pasivo sólo notifica a los administradores o a otros sistemas de la red acerca del problema que se ha producido.

La mayoría de los productos IDS comerciales proporcionan una combinación de capacidades de supervisión basadas en la red o en servidores, con un dispositivo de gestión central destinado a recibir los informes de los diferentes monitores y alertar a los administradores de la red.

Bibliografía

[b-UIT-T E.107] Recomendación UIT-T E.107 (2007), *Servicio de Telecomunicaciones en caso de Emergencia (STE) y marco de interconexión para la implantación nacional de STE*.

[b-UIT-T M.3016.0] Recomendación UIT-T M.3016.0 (2005), *Seguridad en el plano de gestión: Visión general*.

[b-UIT-T X.690] Recomendación UIT-T X.690 (2008) | ISO/IEC 8825-1:2008, *Tecnología de la información – Reglas de codificación de notación de sintaxis abstracta uno: Especificación de las reglas de codificación básica, de las reglas de codificación canónica y de las reglas de codificación distinguida*.

[b-UIT-T X.810] Recomendación UIT-T X.810 (1995) | ISO/IEC 10181-1:1996, *Tecnología de la información – Interconexión de sistemas abiertos - Marcos de seguridad para sistemas abiertos: Visión general*.

[b-UIT-T Y.2091] Recomendación ITU-T Y.2091 (2008), *Términos y definiciones aplicables a las redes de la próxima generación*.

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

[b-3GPP TS 33.328] 3GPP TS 33.328, *IP Multimedia System (IMS) media plane security*.

[b-ETSI TS 133 220] ETSI TS 133 220 V9.2.0 (2010), *Generic Authentication Architecture (GAA); Generic bootstrapping architecture*.

[b-IETF RFC 1155] IETF RFC 1155 (1990), *Structure and Identification of Management Information for TCP/IP-based Internets*.

[b-IETF RFC 1212] IETF RFC 1212 (1991), *Concise MIB definitions*.

[b-IETF RFC 1215] IETF RFC 1215 (1991), *A Convention for Defining Traps for use with the SNMP*.

[b-IETF RFC 2246] IETF RFC 2246 (1999), *The TLS Protocol Version 1.0*.

[b-IETF RFC 2367] IETF RFC 2367 (1998), *PF_KEY Key Management API, Version 2*.

[b-IETF RFC 2403] IETF RFC 2403 (1998), *The Use of HMAC-MD5-96 within ESP and AH*.

[b-IETF RFC 2409] IETF RFC 2409 (1998), *The Internet Key Exchange (IKE)*.

[b-IETF RFC 2451] IETF RFC 2451 (1998), *The ESP CBC-Mode Cipher Algorithms*.

[b-IETF RFC 2578] IETF RFC 2578 (1999), *Structure of Management Information Version 2 (SMIv2)*.

[b-IETF RFC 2579] IETF RFC 2579 (1999), *Textual Conventions for SMIv2*.

[b-IETF RFC 2580] IETF RFC 2580 (1999), *Conformance Statements for SMIv2*.

[b-IETF RFC 2617] IETF RFC 2617 (1999), *HTTP Authentication: Basic and Digest Access Authentication*.

[b-IETF RFC 2808] IETF RFC 2808 (2000), *The SecurID®SASL Mechanism*.

[b-IETF RFC 2865] IETF RFC 2865 (2000), *Remote Authentication Dial In User Service (RADIUS)*.

[b-IETF RFC 3261] IETF RFC 3261 (2002), *SIP: Session Initiation Protocol*.

[b-IETF RFC 3310] IETF RFC 3310 (2002), *Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA)*.

[b-IETF RFC 3410] IETF RFC 3410 (2002), *Introduction and Applicability Statements for Internet Standard Management Framework*.

[b-IETF RFC 3411] IETF RFC 3411 (2002), *An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks*.

[b-IETF RFC 3413] IETF RFC 3413 (2002), *Simple Network Management Protocol (SNMP) Applications*.

[b-IETF RFC 3414] IETF RFC 3414 (2002), *User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)*.

[b-IETF RFC 3415] IETF RFC 3415 (2002), *View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)*.

[b-IETF RFC 3416] IETF RFC 3416 (2002), *Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)*.

[b-IETF RFC 3417] IETF RFC 3417 (2002), *Transport Mappings for the Simple Network Management Protocol (SNMP)*.

[b-IETF RFC 3550] IETF RFC 3550 (2003), *RTP: A Transport Protocol for Real-Time Applications*.

[b-IETF RFC 3588] IETF RFC 3588 (2003), *Diameter Base Protocol*.

[b-IETF RFC 3602] IETF RFC 3602 (2003), *The AES-CBC Cipher Algorithm and Its Use with IPsec*.

[b-IETF RFC 3711] IETF RFC 3711 (2004), *The Secure Real-time Transport Protocol (SRTP)*.

[b-IETF RFC 3713] IETF RFC 3713 (2004), *A Description of the Camellia Encryption Algorithm*.

[b-IETF RFC 3830] IETF RFC 3830 (2004), *MIKEY: Multimedia Internet KEYing*.

[b-IETF RFC 4132] IETF RFC 4132 (2005), *Addition of Camellia Cipher Suites to Transport Layer Security (TLS)*.

[b-IETF RFC 4279] IETF RFC 4279 (2005), *Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)*.

[b-IETF RFC 4301] IETF RFC 4301 (2005), *Security Architecture for the Internet Protocol*.

[b-IETF RFC 4306] IETF RFC 4306 (2005), *Internet Key Exchange (IKEv2) Protocol*.

[b-IETF RFC 4312] IETF RFC 4312 (2005), *The Camellia Cipher Algorithm and Its Use with IPsec*.

[b-IETF RFC 4422] IETF RFC 4422 (2006), *Simple Authentication and Security Layer (SASL)*.

[b-IETF RFC 4492] IETF RFC 4492 (2006), *Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS)*.

[b-IETF RFC 4566] IETF RFC 4566 (2006), *SDP: Session Description Protocol*.

[b-IETF RFC 4567] IETF RFC 4567 (2006), *Key Management Extensions for Session Description Protocol (SDP) and Real Time Streaming Protocol (RTSP)*.

[b-IETF RFC 4568] IETF RFC 4568 (2006), *Session Description Protocol (SDP) Security Descriptions for Media Streams*.

[b-IETF RFC 4590] IETF RFC 4590 (2006), *RADIUS Extension for Digest Authentication*.

[b-IETF RFC 4648] IETF RFC 4648 (2006), *The Base16, Base32, and Base64 Data Encodings*.

[b-IETF RFC 4740] IETF RFC 4740 (2006), *Diameter Session Initiation Protocol (SIP) Application*.

[b-IETF RFC 4835] IETF RFC 4835 (2007), *Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH)*.

[b-IETF RFC 5077] IETF RFC 5077 (2008), *Transport Layer Security (TLS) Session Resumption without Server-Side State*.

[b-IETF RFC 5090] IETF RFC 5090 (2008), *Radius Extension for Digest Authentication*.

[b-IETF RFC 5246] IETF RFC 5246 (2008), *The Transport Layer Security (TLS) Protocol Version 1.2*.

[b-IETF RFC 5282] IETF RFC 5282 (2008), *Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol*.

[b-IETF RFC 5424] IETF RFC 5424 (2009), *The Syslog Protocol*.

[b-ISO/IEC 15946-1] ISO/IEC 15946-1:2008, *Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 1: General*.

[b-ISO/IEC 15946-2] ISO/IEC 15946-2:2002, *Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital signatures*.

[b-ISO/IEC 15946-3] ISO/IEC 15946-3:2002, *Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 3: Key establishment*.

[b-ISO/IEC 15946-4] ISO/IEC 15946-4:2004: *Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 4: Digital signatures giving message recovery*.

[b-ISO/IEC 15946-5] ISO/IEC 15946-5:2008, *Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 5: Elliptic curve generation*.

[b-ISO/IEC 18033-3] ISO/IEC 18033-3:2005, *Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers*.

[b-NIST FIPS 197] NIST Federal Information Processing Standards (FIPS) 197 (2001): *Advanced Encryption Standard*.

[b-NIST FIPS 198-1] NIST Federal Information Processing Standards (FIPS) 198-1 (2008), *The Keyed-Hash Message Authentication Code (HMAC)*.

[b-NIST FIPS SP 800-38a] NIST Federal Information Processing Standards (FIPS), *Special Publication 800-38: Recommendation for Block Cipher Modes of Operations*. *Methods and Techniques, December 2001*.

[b-NIST SP 800-44 v2] NIST Special Publication 800-44 Version 2, *Guidelines on Securing Public Web Servers*.

[b-NIST SP 800-57] NIST Special Publication 800-57, *Recommendation on Key Management – Part 1: General (Revised)*.

[b-NIST SP 800-83] NIST Special Publication 800-83 (2005), *Guide to Malware Incident Prevention and Handling*.

[b-NIST SP 800-94] NIST Special Publication 800-94, *Guide to Intrusion Detection and Prevention Systems (IDPS)*.

[b-TIA 683-D] TIA Standard TIA-683-D (2006), *Over the Air Service Provisioning of Mobile Stations in Spread Spectrum Systems*.

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, 2010