Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

Y.2703

(01/2009)

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

Redes de la próxima generación – Seguridad

Aplicación del servicio autentificación, autorización y contabilidad (AAA) en las NGN

Recomendación UIT-T Y.2703

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.2703

Aplicación del servicio autentificación, autorización y contabilidad (AAA) en las NGN

Resumen

En esta Recomendación se presenta una aplicación del servicio autentificación, autorización y contabilidad (AAA) para las NGN versión 1.

Historia

Edición	Recomendación	Aprobación	Comisión de estudios
1.0	ITU-T Y.2703	2009-01-23	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 [ha recibido/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
1	Alcance	1
2	Referencias	1
3	Definiciones	1
3.1	Términos definidos en otras Recomendaciones	1
3.2	Términos definidos en esta Recomendación	1
4	Abreviaturas y acrónimos	2
5	Convenios	2
6	Conceptos generales del servicio AAA	2
6.1	Generalidades	2
6.2	El proceso AAA	2
6.3	Procedimiento AAA	3
7	Modelo de aplicación de autentificación y autorización en las NGN	3
8	Arquitectura AAA en las NGN	5
8.1	Acceso del usuario a la red	5
8.2	Acceso del usuario al servicio de red	6
8.3	Autentificación y autorización para el acceso del usuario a servicios de terceros	6
9	Ingreso	6
10	Autentificación	7
10.1	Entidades de autentificación	7
10.2	Procedimiento de autentificación	7
11	Autorización	9
11.1	Autorización en las NGN	9
11.2	Entidades de autorización	9
11.3	Procedimiento de autorización	9
12	Contabilidad	10
12.1	Contabilidad de seguridad	10
12.2	Funciones de contabilidad de seguridad	10
Apéndice I – Protocolo de autentificación para AAA en las NGN		12
I.1	Protocolo EAP para el servicio AAA en las NGN	12
I.2	Protocolos AAA	13
Apéndice II – Certificados digitales X.509 como credenciales		14
Apéndice III – Casos de uso de la autentificación y la autorización		15
III.1	Autentificación y autorización del usuario para su acceso a la red	15
III.2	Autentificación y autorización de usuarios por el proveedor de servicio NGN para darles acceso a servicios/aplicaciones	17

Página

III.3 Autentificación y autorización de proveedores NGN por el usuario 19

III.4 Autentificación y autorización por el proveedor NGN de otros proveedores de servicios/aplicaciones..... 20

III.5 Utilización del servicio de autentificación y autorización de un tercero..... 21

Bibliografía 23

Recomendación UIT-T Y.2703

Aplicación del servicio autentificación, autorización y contabilidad (AAA) en las NGN

1 Alcance

En esta Recomendación se describe una aplicación del servicio autentificación, autorización y contabilidad (AAA) para las redes de la próxima generación (NGN) basada en [b-UIT-T Y.2201]: Requisitos de las redes de próxima generación, versión 1; [b-UIT-T Y.2012]: Requisitos funcionales y arquitectura de la red de próxima generación; [b-UIT-T Y.2701]: Requisitos de seguridad de la versión 1 de la red de próxima generación; y [b-UIT-T Y.2702]: Requisitos de autentificación y autorización en las redes de la próxima generación, versión 1. Esta Recomendación se aplica al proceso de autentificación, autorización y contabilidad en el acceso a las NGN empleando el cliente AAA y el servidor AAA. En concreto, esta Recomendación trata de la función de contabilidad sólo desde el punto de vista de su contribución a la contabilidad de seguridad.

El alcance de esta Recomendación comprende:

1) El proceso de ingreso.
2) Las funciones y procedimientos de autentificación.
3) Las funciones y procedimientos de autorización.
4) Las funciones y procedimientos de contabilidad de seguridad.

2 Referencias

Ninguna.

3 Definiciones

3.1 Términos definidos en otras Recomendaciones

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

3.1.1 autentificación [b-UIT-T X.811]: Confirmación de la identidad declarada de una entidad.

3.1.2 certificado de autentificación [b-UIT-T X.811]: Certificado de seguridad garantizado por una autoridad de autenticación, y que puede utilizarse para confirmar la identidad de una entidad.

3.1.3 información de autentificación [b-UIT-T X.811]: Información utilizada con fines de autenticación.

3.1.4 autorización [b-UIT-T X.800]: Atribución de derechos, que incluye la concesión de acceso basada en derechos de acceso.

3.1.5 declarante [b-UIT-T X.811]: Entidad que es o representa a un principal para fines de autenticación. Un declarante incluye las funciones necesarias para intervenir en intercambios de autenticación en nombre de un principal.

3.1.6 registro de auditoría de seguridad [b-UIT-T X.800]: Datos recogidos que pueden usarse para efectuar una auditoría de seguridad.

3.2 Términos definidos en esta Recomendación

En esta Recomendación se definen los siguientes términos:

3.2.1 contabilidad de seguridad: Función que efectúa un seguimiento de las acciones o eventos relacionados con la seguridad que pueden utilizarse como fuentes en la función de auditoría de seguridad.

4 Abreviaturas y acrónimos

En la presente Recomendación se emplean las siguientes abreviaturas.

AAA Autentificación, autorización, contabilidad (*authentication, authorization, accounting)*

AM-FE Entidad funcional de gestión de acceso (*access management functional entity)*

ANI Interfaz aplicación-red (*application to network interface)*

EAP Protocolo de autentificación extensible (*extensible authentication protocol)*

ID Identidad – definida por la red, el servicio o la entidad a que se accede (*identity – as defined by the network, service, or entity being accessed)*

NAS Servidor de acceso a red (*network access server)*

NGN Red de la próxima generación (*next generation network)*

NNI Interfaz red-red (*network to network interface)*

NP Proveedor de red (*network provider)*

OAMP Operaciones, administración, mantenimiento y configuración (*operations administration maintenance and provision)*

RACF Función de control de acceso a recursos (*resource access control function)*

SCTP Protocolo de transporte de control de tren (*stream control transport protocol)*

SR Recurso de servicio (*service resource)*

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

TE Equipo terminal (*terminal equipment)*

TUP-FE Entidad funcional de perfil de usuario de transporte (*transport user profile funcional entity)*

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

5 Convenios

Ninguno.

6 Conceptos generales del servicio AAA

En esta cláusula se presentan los conceptos básicos del servicio de autentificación, autorización y contabilidad.

6.1 Generalidades

El servicio autentificación, autorización y contabilidad contiene las funciones con que se verifica la identidad de un usuario (autentificación), se da acceso a los servicios (autorización) y se mide el consumo de recursos (contabilidad).

6.2 El proceso AAA

Dentro del AAA se realizan los siguientes procesos:

La autentificación valida la identidad del usuario extremo antes de permitir su acceso a la red. El usuario extremo presenta una serie de credenciales, como una combinación nombre de

usuario/contraseña, una clave de seguridad, un certificado o datos biométricos (por ejemplo, huellas digitales). Por norma general, estas credenciales se validan durante el proceso de ingreso. La verificación de las credenciales da paso al proceso de autorización.

La autorización define los privilegios y servicios que corresponden al usuario extremo una vez que se le concede el acceso a la red. Esto puede comprender la concesión de una dirección IP o la invocación de un filtro para determinar qué aplicaciones o protocolos se soportan. En un entorno gestionado por AAA, la autentificación y la autorización se realizan al mismo tiempo.

La contabilidad contiene el método de recopilación de información sobre el consumo de recursos por parte del usuario extremo, que a continuación puede procesarse para la facturación, la auditoría y la planificación. Algunos datos de contabilidad se emplean para efectuar un rastreo de auditoría de seguridad.

Estos tres procesos se centralizan en una serie de funciones que, en conjunto, ejercen el control de acceso.

6.3 Procedimiento AAA

El sistema de servicio AAA está compuesto por un servidor AAA y un cliente AAA.

El servidor AAA tiene acceso a una base de datos de perfiles de usuario y datos de configuración, y se comunica con los clientes AAA residentes en los componentes de red, como el servidor de acceso a red (NAS, *network access server*) y los encaminadores, para prestar servicios AAA distribuidos.

El servicio AAA puede resumirse en los siguientes pasos:

- El usuario extremo se conecta al dispositivo punto de entrada y solicita acceso a la red.
- El cliente AAA remite la identidad/credenciales de autentificación del usuario extremo al servidor AAA.
- El servidor AAA autentifica al usuario a partir de las credenciales. Si la autentificación se completa con éxito, el servidor determina el/los servicio(s) autorizados y devuelve una respuesta de aceptación rechazo, además de otros datos pertinentes, al cliente AAA.
- El cliente AAA notifica al usuario extremo que se le concede o deniega el acceso a los recursos especificados.

El cliente AAA envía un mensaje de contabilidad al servidor AAA durante el establecimiento y la terminación de la conexión para su registro y almacenamiento.

7 Modelo de aplicación de autentificación y autorización en las NGN

La presente Recomendación se basa en los requisitos de seguridad de las NGN definidos en [b-UIT-T Y.2701] y en el modelo de referencia de autentificación en las NGN de [b-UIT-T Y.2702]. El modelo de referencia de autentificación en las NGN (figura 7-1) muestra ocho puntos de referencia de autentificación, tres de los cuales se tienen en cuenta en esta Recomendación.

Estos puntos son:

1) acceso del usuario a la red;

2) acceso del usuario al servicio proporcionado por la red;

4) acceso del proveedor de servicio al usuario receptor.

Los puntos de referencia 1) y 4) se refieren al transporte de tráfico de usuario y pueden considerarse dependientes del control de acceso "horizontal" en el nivel de control de transporte, mientras que los puntos de referencia 2) y 8) pueden considerarse dependientes de los datos de control entre las capas de transporte y control de servicio y, por tanto, "verticales". Esta relación se muestra en la figura 7-2.

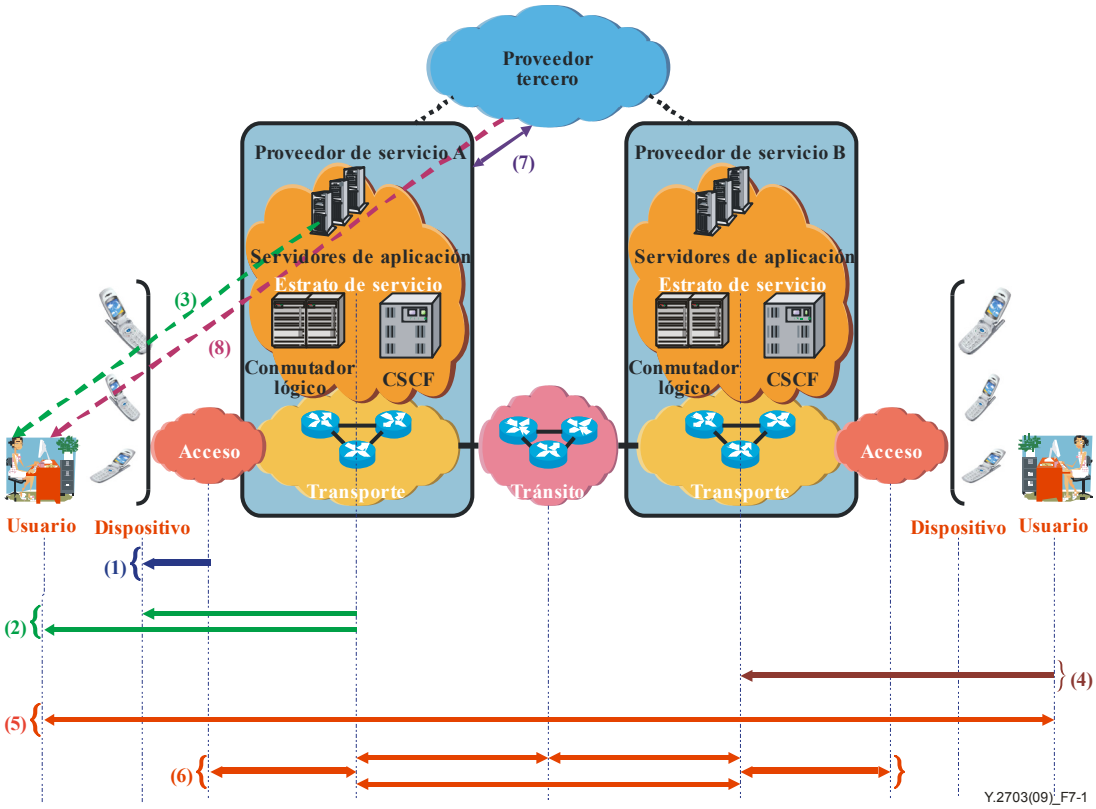

Figura 7-1 – Modelo de arquitectura de referencia de extremo a extremo (autentificación en las NGN – Y.2702)

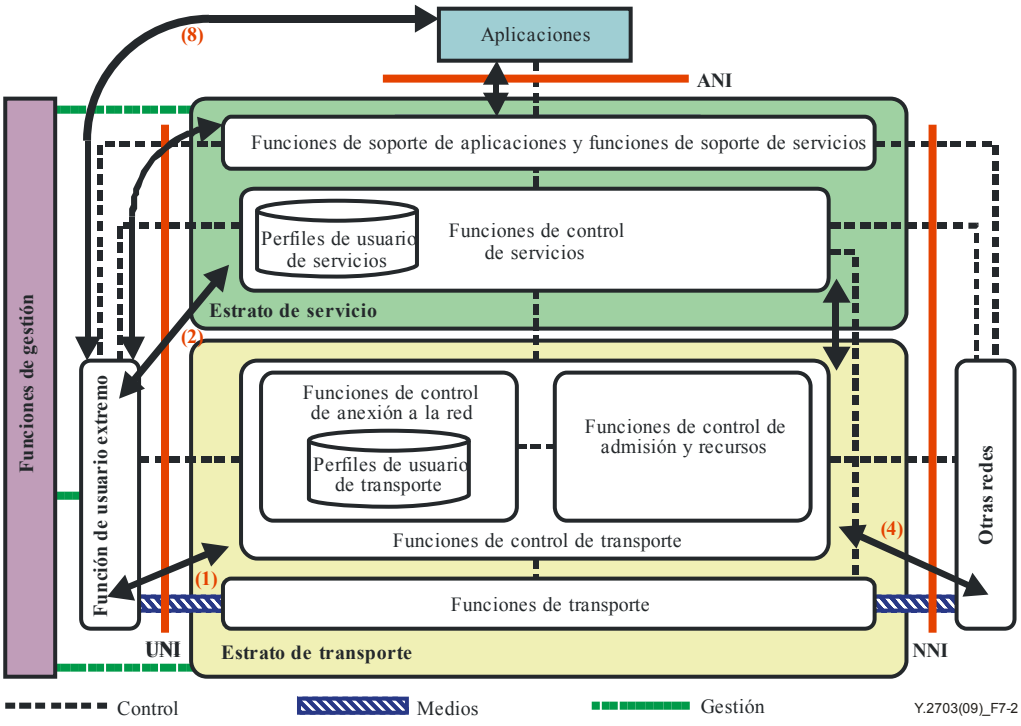

Figura 7-2 – Arquitectura de las NGN y dominios AAA conexos (autentificación en las NGN – Y.2702)

8 Arquitectura AAA en las NGN

En esta cláusula se describe la relación entre el modelo de referencia AAA y el modelo de arquitectura funcional descrito en [b-UIT-T Y.2012].

8.1 Acceso del usuario a la red

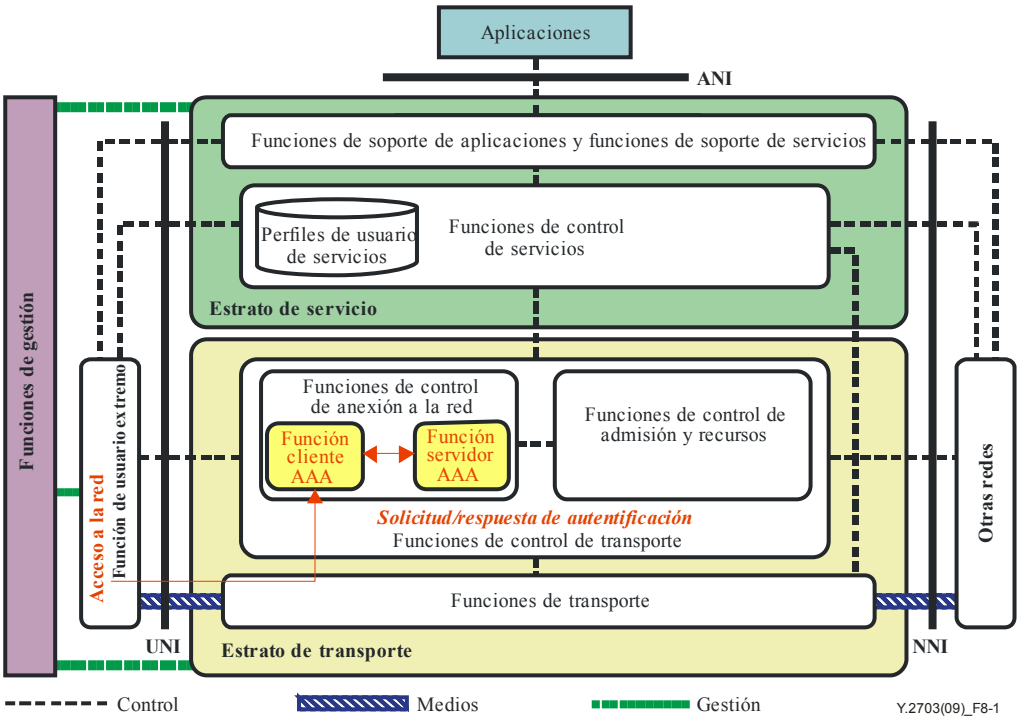

Figura 8-1 – Autentificación y autorización de un usuario para su acceso a la red

La figura 8-1 muestra la aplicación de AAA al acceso del usuario a la red (es decir, una aplicación de tipo 1 de la figura 7-1 anterior).

Cuando una entidad de la función de control de transporte (normalmente, T-14 AM-FE) detecta una solicitud de conexión de un usuario terminal, esta entidad asume el papel de cliente AAA y solicita a las entidades de la función de control de transporte que ejercen de servidor AAA (como T-11 TAA-FE y T-12 TUP-FE) que autentifiquen al usuario y autoricen su utilización de los recursos de la NGN. Para este procedimiento de solicitud y respuesta pueden emplearse protocolos como RADIUS o Diameter. A partir de la solicitud de un cliente AAA, el servidor AAA autentifica al usuario mediante procedimientos explícitos (por ejemplo, EAP) o implícitos (por ejemplo, autentificación de línea de acceso). Una vez debidamente autorizado el usuario de acuerdo con el perfil de usuario (generalmente gestionado por la TUP-FE), el servidor AAA solicita la RACF para la reserva y atribución de recursos NGN para ese usuario. Cuando se le conceden, el servidor AAA notifica al cliente AAA el permiso para conectar ese equipo de usuario.

8.2 Acceso del usuario al servicio de red

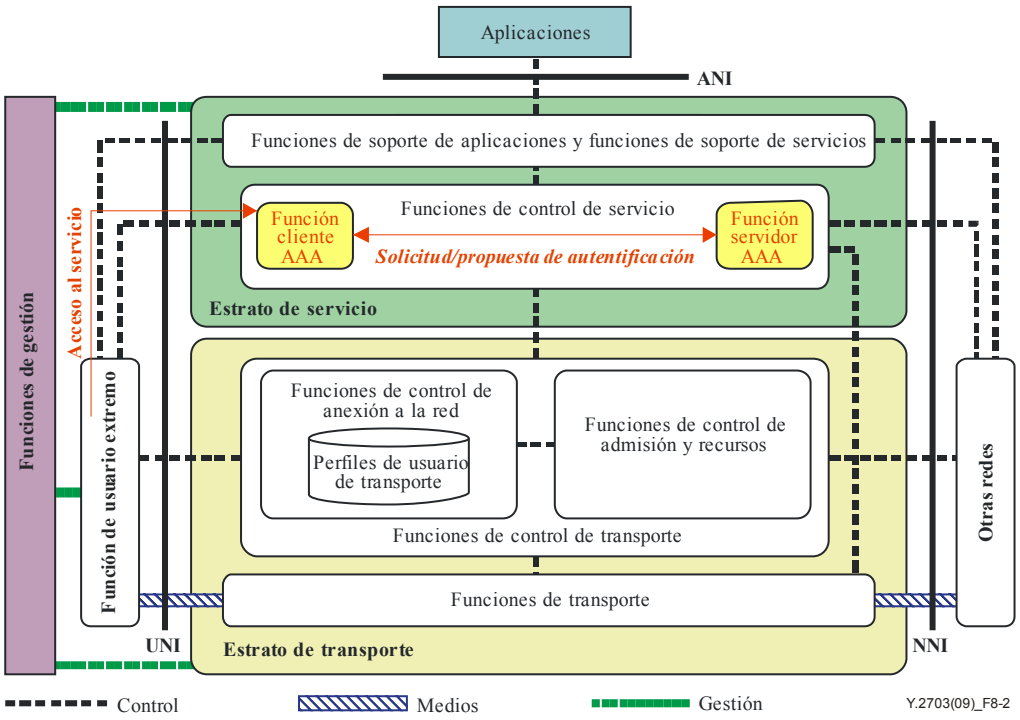

Figura 8-2 – Autentificación y autorización de un usuario para acceso al servicio

En la figura 8-2 se muestra la aplicación de AAA para el acceso del usuario al servicio (es decir, una aplicación de tipo 2 de la figura 7-1 anterior).

Igual que en el caso anterior, figura 8-1, un cliente AAA de las funciones de control de servicio (generalmente, S-1 S-CES-FE) detecta la solicitud de conexión de un usuario terminal y solicita a un servidor AAA (como S-5 SUP-FE o S-6 SAA-FE) la autentificación y autorización para el servicio solicitado. En función del resultado de la autentificación y la autorización se otorga o deniega el acceso al servicio solicitado.

Una vez que el usuario está conectado a la red o al servicio, cada cliente AAA notifica a su servidor AAA la información sobre los recursos de NGN consumidos por el usuario para que pueda recopilar la información de contabilidad asociada con el usuario.

8.3 Autentificación y autorización para el acceso del usuario a servicios de terceros

La versión 1 de la NGN no prevé el acceso a servicios de terceros a través de una ANI. Por consiguiente, la autentificación y autorización para el acceso del usuario a servicios de terceros queda fuera del alcance de la presente Recomendación. Esta Recomendación no muestra el modelo de referencia para los servicios de terceros, aunque en el apéndice III se muestra un ejemplo que ilustra la autentificación y autorización de un servicio de terceros.

9 Ingreso

La aplicación de AAA exige la autentificación de la identificación de la entidad, por ejemplo, del usuario o el dispositivo. Las credenciales que identifican a la entidad se establecen mediante un proceso de ingreso que otorga una identidad exclusiva al usuario/dispositivo. Las credenciales se utilizan en el proceso de autentificación siempre que se quiere acceder al/a los servicios(s). El proceso de ingreso puede comprender la aceptación de términos y condiciones, así como acuerdos financieros, aunque la verificación inicial de la identidad y las credenciales se denomina ingreso, el

posterior acceso a los servicios y las verificaciones de credenciales se conocen como registro. Las modalidades de ingreso dependerán de la política del proveedor, la naturaleza del servicio, etc.

10 Autentificación

En esta Recomendación se emplean los conceptos básicos de autentificación de [b-UIT-T X.811]. Los servicios y capacidades de autentificación para el acceso a la red y el servicio se necesitan para contrarrestar las amenazas que suponen los intentos de acceso no autorizado. En el apéndice II puede encontrarse más información sobre los certificados digitales.

10.1 Entidades de autentificación

El término "declarante" se utiliza para designar a la entidad que solicita la autentificación. Un declarante comprende las funciones necesarias para iniciar los intercambios de autentificación.

El cliente AAA ejerce una función especializada que forma parte del trayecto de acceso entre el declarante y la entidad verificadora en cada solicitud de acceso y que aplica la decisión adoptada por el verificador.

En un entorno gestionado por AAA, el servidor AAA es la entidad verificadora y expide un certificado de autentificación al declarante, una vez que se ha autentificado con éxito.

10.2 Procedimiento de autentificación

En un entorno gestionado por AAA, el servidor AAA ofrece al usuario el servicio de autentificación. Identifica la entidad que solicita el acceso en medida suficiente para determinar los servicios a que está autorizado y que se le facturarán. El servidor AAA puede expedir un certificado de autentificación.

10.2.1 Autentificación satisfactoria

Los siguientes pasos y la figura 10-1 son un ejemplo del flujo de mensajes para una autentificación satisfactoria.

Paso 1: Una entidad solicita acceso al cliente AAA.

Paso 2: El cliente AAA solicita al servidor AAA la autentificación de la entidad.

Paso 3: El servidor AAA solicita al cliente AAA las credenciales de la entidad para iniciar la autentificación.

Paso 4: El cliente AAA solicita a la entidad las credenciales necesarias para la autentificación.

Paso 5: La entidad, ahora declarante, envía las credenciales requeridas al cliente AAA.

Paso 6: El cliente AAA remite las credenciales requeridas al servidor AAA para la autentificación.

Paso 7: El servidor AAA coteja las credenciales recibidas con el perfil de usuario del declarante.

Paso 8: Si se verifican las credenciales, el servidor AAA procede al proceso de autorización sin notificarlo al cliente AAA o al declarante.

Paso 9: Después del proceso de autorización, el servidor AAA envía un mensaje de acceso permitido al cliente AAA.

Paso 10: El cliente AAA remite el mensaje de acceso permitido al declarante.

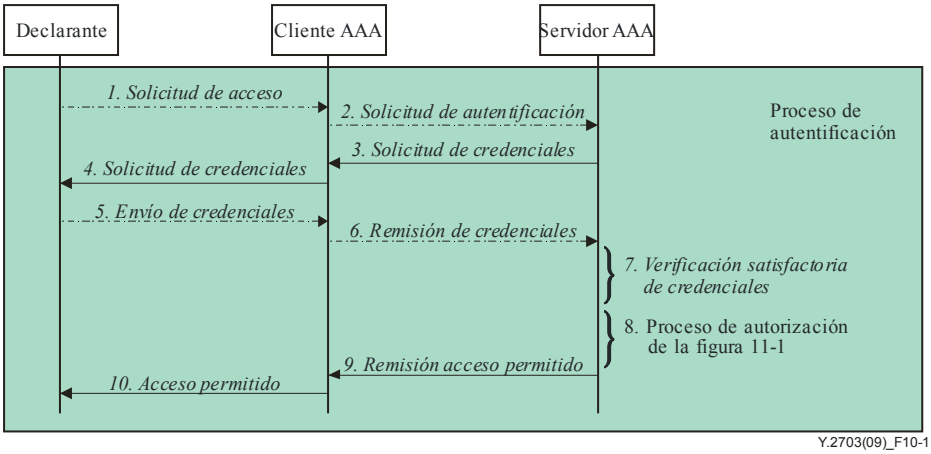

Figura 10-1 – Flujo de mensajes para una autentificación satisfactoria

10.2.2 Autentificaciones no satisfactorias

Los siguientes pasos y la figura 10-2 son un ejemplo del flujo de mensajes para una autentificación no satisfactoria.

Paso 1: Una entidad solicita acceso al cliente AAA.

Paso 2: El cliente AAA solicita al servidor AAA la autentificación de la entidad.

Paso 3: El servidor AAA solicita al cliente AAA las credenciales de la entidad para iniciar la autentificación.

Paso 4: El cliente AAA solicita a la entidad las credenciales necesarias para la autentificación.

Paso 5: La entidad, ahora declarante, envía las credenciales requeridas al cliente AAA.

Paso 6: El cliente AAA remite las credenciales requeridas al servidor AAA para la autentificación.

Paso 7: El servidor AAA coteja las credenciales recibidas con el perfil de usuario del declarante.

Paso 8: De no poder verificarse las credenciales, el servidor AAA envía al cliente AAA un mensaje de denegación de acceso.

Paso 9: El cliente AAA remite al declarante el mensaje de denegación de acceso.

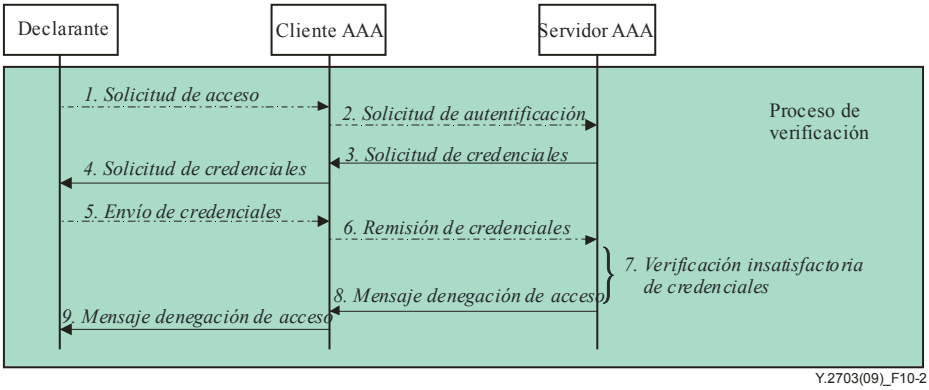

Figura 10-2 – Flujo de mensajes para una autentificación no satisfactoria

11 Autorización

La autorización se define como el acto de determinar si se puede conceder un privilegio concreto a quien presenta una determinada credencial. Tal privilegio puede ser el derecho de acceder a un recurso de servicio (SR, *service resource*) y puede comprender la lectura, escritura o modificación de recursos, en función de la política aplicada. El proceso de autorización sigue al de autentificación y aprueba o deniega el acceso al servicio NGN de acuerdo con el resultado de los pasos de autentificación anteriores y de la política.

11.1 Autorización en las NGN

El objetivo de la autorización es dar y controlar el acceso de usuarios autentificados a los servicios autorizados. En las NGN, el servidor AAA se comunica con los elementos de red que contienen los privilegios de acceso de las entidades que han efectuado el ingreso.

En esta Recomendación la autentificación y la autorización se tratan como procesos asociados, generalmente efectuados de manera secuencial para las entidades que han efectuado el ingreso cada vez que solicitan acceso. No obstante, la política del proveedor puede permitir que una entidad solicite acceso/derechos de utilización inmediatos sin llevar a cabo los procesos de reautentificación o ingreso. Este caso no se aborda en este Recomendación.

La autorización del usuario para un servicio se lleva a cabo cuando el servidor AAA se comunica con los elementos de red apropiados y recibe de ellos la información de autorización. Una vez completado el proceso de autorización por parte del servidor AAA, se remite al usuario que solicita el servicio un acuse de recibo.

La recepción del acuse de recibo supone que se ha completado con éxito el proceso de autentificación y autorización y la entidad que solicita el acceso se conecta a la red o el SR autorizado.

11.2 Entidades de autorización

El servidor AAA realiza automáticamente el proceso de autorización, una vez terminada la autentificación, sin que en ello participe la entidad que solicita el acceso. El servidor AAA dispone de una función especial que toma decisiones de autorización aplicando la política de control de acceso.

11.3 Procedimiento de autorización

El procedimiento de autorización que se muestra en la figura 11-1 es el siguiente:

Paso A: Una vez debidamente autentificada la entidad, el servidor AAA identifica los servicios y recursos disponibles y a que puede acceder el declarante.

Paso B: Una vez completado el Paso A, el servidor AAA indica a las funciones de control de transporte y servicio que asigne/atribuya servicios y recursos para su utilización por parte del declarante.

Paso C: El servidor AAA envía un mensaje de acceso permitido al cliente AAA.

Paso D: El cliente AAA remite el mensaje de acceso permitido al declarante.

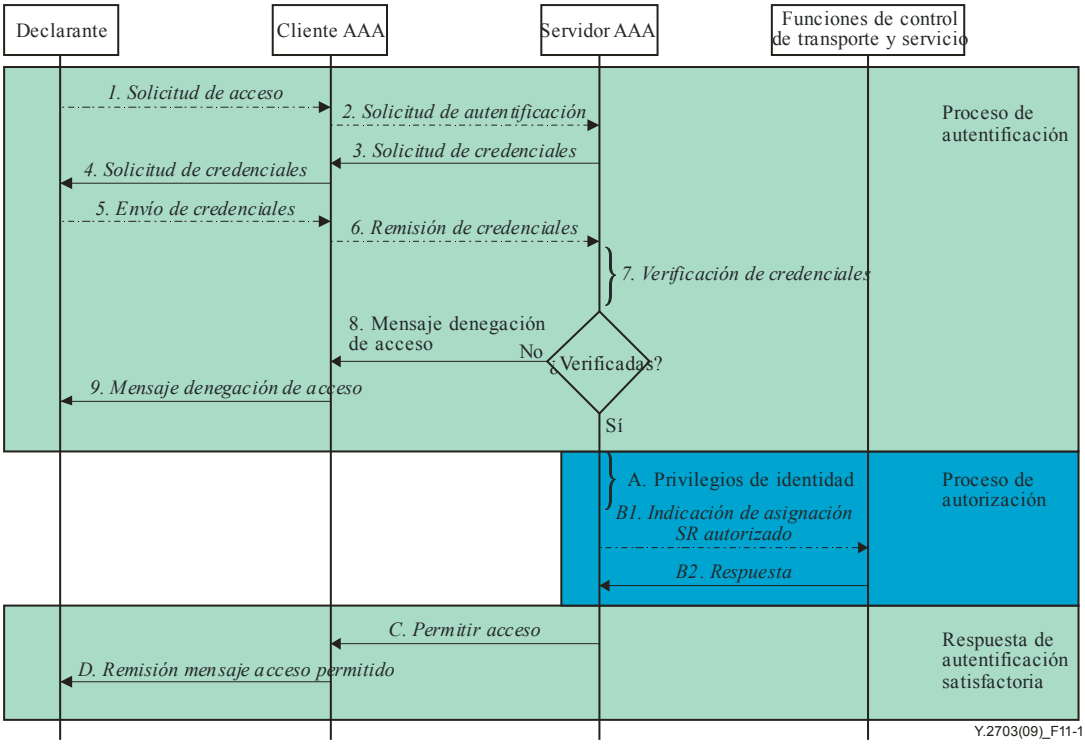

Figura 11-1 – Flujo de mensajes del proceso de autorización

12 Contabilidad

La última "A" de la abreviatura "AAA" significa Contabilidad ("accounting" en inglés). La contabilidad en el contexto AAA comprende un elemento de seguridad que puede utilizarse asociado con otros datos de eventos de seguridad para el soporte de una función de contabilidad.

12.1 Contabilidad de seguridad

La contabilidad de eventos de seguridad emplea el subconjunto de funciones de contabilidad mencionado, que proporciona datos de contabilidad que, a continuación, se utilizan para realizar un rastreo de auditoría de seguridad que utilizará la función de auditoría de seguridad. El alcance del rastreo de auditoría de seguridad depende de las necesidades y políticas de auditoría de seguridad determinadas por el proveedor de NGN para cada contexto concreto, por ejemplo, tiempos de inicio y final de acceso satisfactorio o insatisfactorio a la red o el servicio, el servicio a que se accede y la información de identidad de la entidad que accede (en el caso de autentificación satisfactoria). La función de auditoría real queda fuera del alcance de esta Recomendación. En la figura 12-1 puede verse el procedimiento de contabilidad de seguridad.

12.2 Funciones de contabilidad de seguridad

La contabilidad de seguridad es un servicio que efectúa las siguientes funciones:

1) Captura: es responsable de adquirir datos detectables de un evento y presentar información pertinente en cuanto a seguridad. Los datos capturados pueden incluir:
   - el resultado de la autentificación;
   - información relacionada con la revocación de autentificaciones y/o certificados;
   - información sobre garantía de autentificación;
   - otra información relativa al proceso de autentificación.

2) Almacenamiento: conserva los resultados de la función de captura.

3) Examen: intenta describir precisamente el evento mediante. Una verificación de la exactitud de los datos capturados, una distinción de los hechos previo examen de los datos capturados.

4) Informe: toma la información de la función de examen y la entrega a la función de auditoría.

5) Auditoría: verifica la exactitud del informe de contabilidad de seguridad o su adaptación a la política de utilización y las directrices de seguridad. La función de auditoría puede necesitar una capacidad de alerta inmediata.

Cabe señalar que sólo la captura es una función AAA, pues el almacenamiento, el examen, el informe y la auditoría son funciones de gestión, que quedan fuera del alcance de la presente Recomendación.

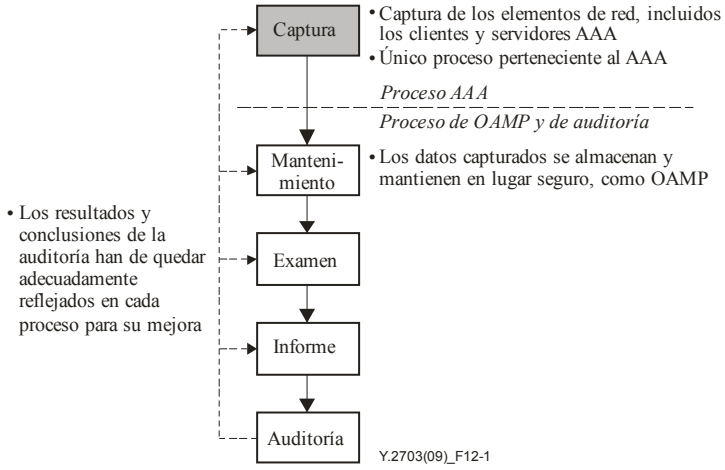

Figura 12-1 – Ejemplo del proceso de contabilidad de seguridad

Apéndice I

Protocolo de autentificación para AAA en las NGN

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

En este apéndice se describe el protocolo EAP que se transporta en las capas de enlace de datos y los protocolos AAA que establecen el marco AAA en las distintas aplicaciones.

I.1 Protocolo EAP para el servicio AAA en las NGN

El protocolo EAP define un marco de autentificación que soporta varios métodos de autentificación. El EAP se ejecuta en el servidor par y de autentificación a través del autentificador. El EAP se transporta directamente en las capas de enlace de datos, como IEEE 802 y PPP (protocolo punto a punto).

No obstante, a causa de la dependencia del enlace, el protocolo EAP necesita una capa inferior, como EAPoL, IEEE 802.1X y IEEE 802.11i. En la figura I.1 se muestra el modelo de multiplexación EAP. La capa de método EAP comprende un algoritmo de autentificación. El par EAP y el autentificador funcionan respectivamente como cliente de autentificación y autentificador. La capa EAP se encarga de la entrega de mensajes EAP. La capa inferior transmite o recibe las tramas EAP entre el par y el autentificador. Dado que la capa de enlace está formada por varios protocolos de enlace, el EAP requiere varias capas inferiores para cada protocolo de enlace.

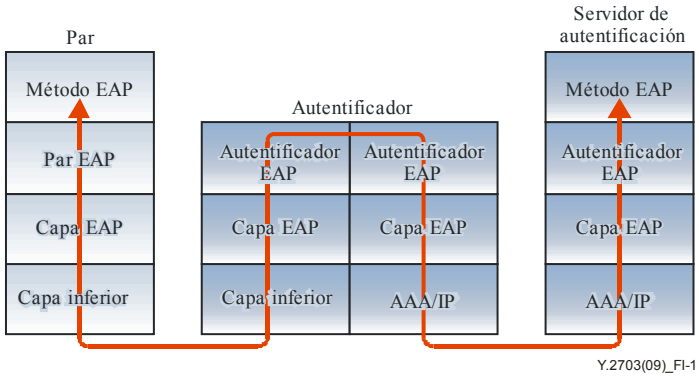

Figura I.1 – Modelo de reenvío EAP

El EAP necesita la capa inferior para entregar mensajes de manera fiable, detector errores y ordenar los mensajes, de la siguiente manera:

- Dado que el EAP no conoce el par que recibe el mensaje del autentificador, necesita un canal fiable entre el par y el autentificador.
- El EAP no garantiza que los mensajes EAP se entrega al destino sin errores. El EAP necesita una función de detección de errores de la capa inferior.
- Los mensajes EAP puede cambiarse de orden o duplicarse por cualquier motivo. Por ende, el EAP necesita las funciones de detección de duplicación y ordenamiento para garantizar un funcionamiento correcto.
- La capa inferior no sabe si la capa superior incluye o no un protocolo de autentificación. El EAP necesita una indicación del protocolo de autentificación.

I.2 Protocolos AAA

Los protocolos AAA, como RADIUS, se implantaron en un primer momento para proporcionar acceso de marcación PPP y al servidor terminal. El protocolo Diameter se creó con el crecimiento de Internet y la introducción de nuevas tecnologías de acceso. En el cuadro I.1 se presenta una comparación entre los protocolos AAA.

Cuadro I.1 – Comparación entre protocolos AAA

	RADIUS	**DIAMETER**
Tamaño de red	Pequeño	Grande
Transporte	UDP	SCTP/TCP
Criptación	Sólo contraseña	Paquete entero
Autentificación/Autorización	Combinación	Combinación
Norma	IETF	IETF
Arquitectura de protocolo	C/S	P2P
Adaptabilidad	Baja	Alta

En el caso del protocolo RADIUS, la gestión de grupos de líneas en serie y módems para un gran número de usuarios puede necesitar una gran cantidad de apoyo administrativo. Dado que los grupos de módems son, por definición, un enlace con el mundo exterior, necesitan que se preste mucha atención a la seguridad, la autorización y la contabilidad. La mejor manera de hacerlo es gestionando una única "base de datos" de usuarios, lo que permite la autentificación (verificación de nombre de usuario y contraseña), así como la información de configuración que detalle el tipo de servicio que se entrega al usuario.

El protocolo Diameter básico puede utilizarse sólo en las aplicaciones de contabilidad, pero para la autentificación y la autorización siempre de extiende para una aplicación particular.

Apéndice II

Certificados digitales X.509 como credenciales

(Este apéndice no forma parte integrante de esta Recomendación)

Un método común para garantizar la autentificación es el empleo de certificados digitales descritos en [b-UIT-T X.509] y [b-UIT-T X.811]. El certificado definido en [b-UIT-T X.509], ampliamente utilizado, contiene los siguientes tipos de datos.

- ***version*** es la versión del certificado codificado. Si está presente el componente extensions en el certificado, la versión será v3. Si el componente issuerUniqueIdentifier o *subjectUniqueIdentifier* estará presente la versión será v2 o v3.
- ***serialNumbe*r** es un número entero asignado por la CA. El valor de serialNumber tendrá que ser único para cada certificado expedido por una determinada CA (es decir, el nombre del expedidor y el número de serie identifican a un único certificado).
- ***signature*** contiene el identificador de algoritmo para el algoritmo y la función de troceo utilizados por la CA para firmar el certificado (por ejemplo, md5WithRSAEncryption, sha-1WithRSAEncryption, id-dsa-with-sha1, etc.).
- ***issuer*** identifica la entidad que ha firmado y expedido el certificado.
- ***validity*** es el intervalo del tiempo durante el cual la CA garantiza que mantendrá información sobre el estado del certificado.
- ***subject*** identifica la entidad asociada con la clave pública que se encuentra en el campo de clave pública del sujeto.
- ***subjectPublicKeyInfo*** se utiliza para encaminar la clave pública que se está certificando y para identificar el algoritmo del cual esta clave pública es un ejemplar de (por ejemplo, rsaEncryption, dhpublicnumber, id-dsa, etc.).
- ***issuerUniqueIdentifier*** se utiliza para identificar unívocamente a un expedidor en el caso de reutilizar un nombre.
- ***subjectUniqueIdentifier*** se utiliza para identificar unívocamente un sujeto en el caso de reutilizar un nombre.
- El ***extensions field*** permite la adición de nuevos campos a la estructura.

Apéndice III

Casos de uso de la autentificación y la autorización

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

El ejemplo de utilización del servicio AAA que figura en este apéndice se basa en el modelo de referencia de [b-UIT-T Y.2702].

III.1 Autentificación y autorización del usuario para su acceso a la red

Los servicios de autentificación y autorización para acceso a la red son necesarios a fin de verificar las identidades y determinar si se puede otorgar el acceso al equipo de usuario extremo.

III.1.1 Autentificación y autorización para el acceso/anexión del dispositivo a la NGN

En este caso, hay tres tipos de autentificación y autorización para el acceso/anexión del dispositivo a la NGN. Estos servicios y capacidades permiten identificar, autentificar y autorizar el acceso o la anexión de los dispositivos de usuario a la red IP:

– identificar, autentificar y autorizar TE y TE-BE heredados para el acceso/anexión a la red IP ((1) de la figura III.1);

– identificar, autentificar y autorizar TE y TE-BE con IAD en el dominio del cliente para el acceso/anexión a la red IP ((2) de la figura III.1);

– identificar, autentificar y autorizar NGN TE y TE-BE con capacidades IP en el dominio del cliente para el acceso/anexión a la red IP ((3) de la figura III.1).

El cliente AAA presta el servicio de autentificación al dispositivo y al proveedor de red, y permite automáticamente al dispositivo acceder al proveedor de red, cuando procede.

El procedimiento de identificación del caso (1) de la figura III.1 es el siguiente.

Paso 1: La pasarela (declarante) solicita acceso/anexión a la red desde al cliente AAA.

Paso 2: El cliente AAA solicita la identificación de la pasarela al servidor AAA (verificador), que identifica la pasarela.

Paso 3: El servidor AAA envía los resultados de la identificación al cliente AAA.

Paso 4: El cliente AAA remite los resultados a la pasarela, donde el cliente AAA almacena la lista de acceso de la pasarela.

En los casos (2) y (3), el declarante es respectivamente el IAD y el NGN TE. El resto del proceso es idéntico al del caso (1).

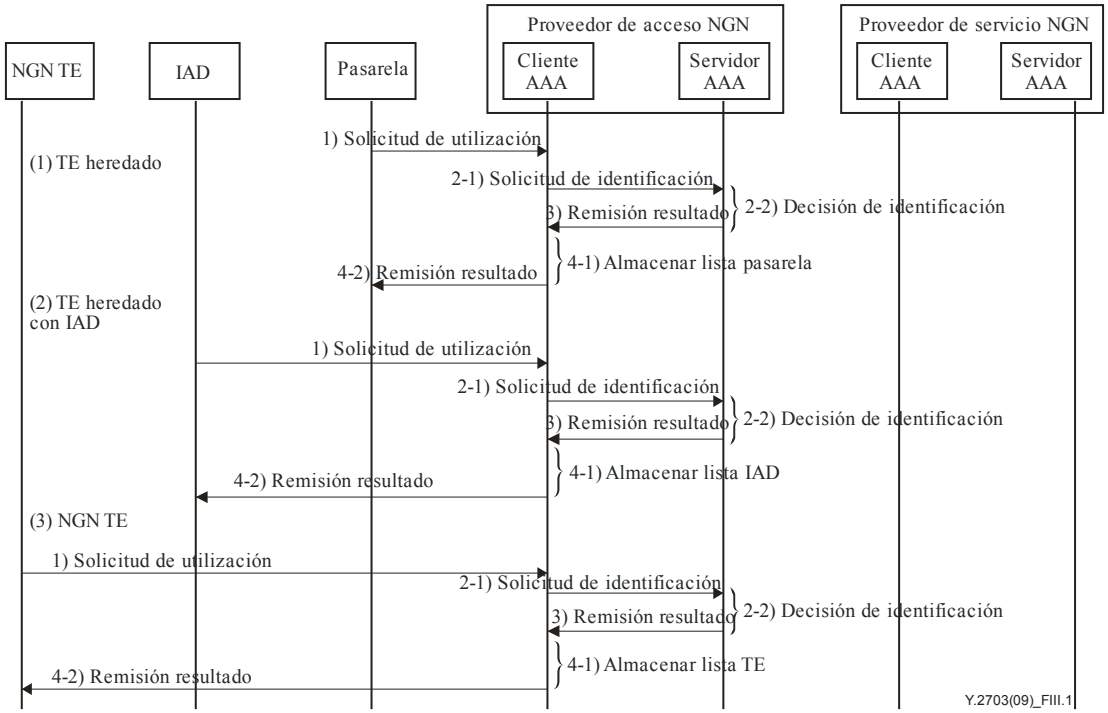

Figura III.1 – Procedimiento de identificación del dispositivo para su acceso a la red NGN

III.1.2 Autentificación y autorización combinada para el acceso/anexión del dispositivo a la NGN y para servicios/aplicaciones

En este caso, hay tres tipos de autentificación y autorización del dispositivo para el acceso/anexión a la NGN. Estos servicios y capacidades permiten combinar la autentificación del dispositivo de usuario por parte del proveedor de acceso NGN con la autentificación y autorización del proveedor de servicios NGN:

– Servicios y capacidades para que el proveedor de servicio NGN identifique y autorice implícitamente el TE y el TE-BE heredados ((1) de la figura III.2).

– Servicios y capacidades para que el proveedor de servicio NGN identifique y autorice implícitamente el TE y el TE-BE con IAD heredados ((2) de la figura III.2).

– Servicios y capacidades para que el proveedor de servicio NGN identifique, autentifique y autorice directamente el NGN TE y el TE-BE en el dominio del cliente ((3) de la figura III.2).

El cliente AAA presta el servicio de autentificación al dispositivo y al proveedor de servicios/aplicaciones y permite automáticamente al dispositivo acceder al proveedor de servicios/aplicaciones, cuando procede.

El procedimiento de identificación del caso (1) de la figura III.2 es el siguiente.

Paso 1: La pasarela (declarante) solicita al cliente AAA la utilización del servicio/aplicación.

Paso 2: El cliente AAA solicita la identificación de la pasarela al servidor AAA (verificador) en el dominio de red de acceso, donde el servidor AAA identifica la pasarela.

Paso 3: El servidor AAA envía los resultados de la identificación simultáneamente al cliente AAA y al servidor AAA del dominio de proveedor de servicio NGN.

Paso 4: El cliente AAA remite los resultados a la pasarela, donde el cliente AAA almacena la lista de acceso de la pasarela.

El procedimiento de identificación del caso (2) de la figura III.2 es el siguiente.

Paso 1: El IAD (declarante) solicita al cliente AAA la utilización del servicio/aplicación.

Paso 2: El cliente AAA solicita la identificación del IAD al cliente AAA en el dominio de proveedor de servicio NGN, donde el servidor AAA (verificador) del dominio de proveedor de servicio NGN identifica el IAD.

Paso 3: El servidor AAA envía los resultados de la identificación al cliente AAA.

Paso 4: El cliente AAA remite los resultados al IAD, donde el cliente AAA almacena la lista de acceso del IAD.

En el caso (3), el NGN TE es el declarante. El resto del proceso es idéntico al del caso (2).

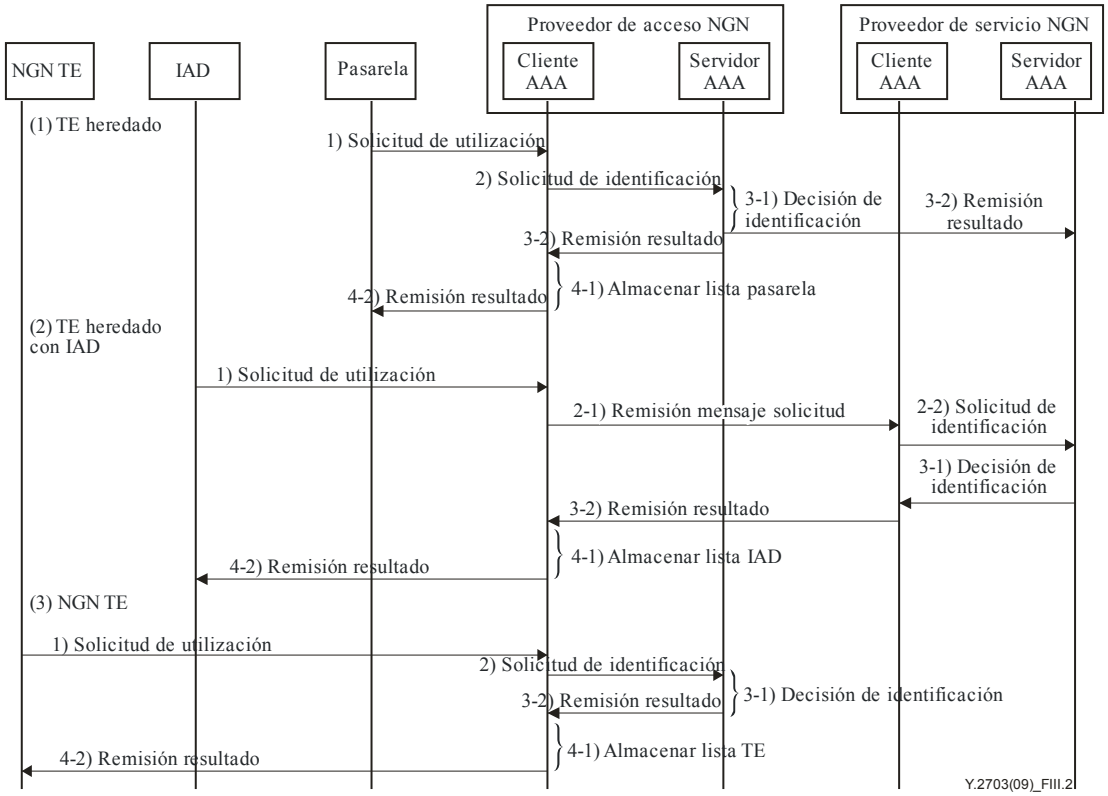

Figura III.2 – Procedimiento de identificación del dispositivo para la utilización del proveedor de servicio/aplicación

III.2 Autentificación y autorización de usuarios por el proveedor de servicio NGN para darles acceso a servicios/aplicaciones

En este caso, hay tres tipos de autentificación y autorización del servicio/aplicación en múltiples redes:

– Autentificación indirecta de un dispositivo de usuario por el proveedor de servicio NGN mediante relaciones de confianza con el proveedor de acceso NGN ((1) de la figura III.3).

– Autentificación y autorización directa de un dispositivo de usuario por el proveedor de servicio NGN. ((2) de la figura III.3).

– Autentificación directa del usuario por el proveedor de servicio NGN ((3) de la figura III.3).

El cliente AAA presta el servicio de autentificación del usuario y el proveedor de servicio/aplicación y permite automáticamente al usuario acceder al proveedor de servicio/aplicación, cuando proceda.

El procedimiento de identificación del caso (1) de la figura III.3 es el siguiente.

Paso 1: El TE (declarante) solicita al cliente AAA la utilización del servicio/aplicación.

Paso 2: El cliente AAA solicita la identificación del dispositivo al servidor AAA (verificador) en el dominio de red de acceso, donde el servidor AAA identifica el dispositivo.

Paso 3: El servidor AAA envía los resultados de la identificación simultáneamente al cliente AAA y al servidor AAA del dominio de proveedor de servicio NGN.

Paso 4: El cliente AAA remite los resultados a la pasarela, donde el cliente AAA almacena la lista de acceso del dispositivo.

El procedimiento de identificación del caso (2) de la figura III.3 es el siguiente.

Paso 1: El TE (declarante) solicita al cliente AAA del dominio de proveedor de servicio NGN la utilización del servicio/aplicación.

Paso 2: El cliente AAA solicita la identificación del dispositivo al servidor AAA (verificador) del dominio de proveedor de servicio NGN, donde el servidor AAA identifica el dispositivo.

Paso 3: El servidor AAA envía los resultados de la identificación al cliente AAA.

Paso 4: El cliente AAA remite los resultados al dispositivo, donde el cliente AAA almacena la lista de acceso del dispositivo.

El procedimiento de autentificación del caso (3) de la figura III.3 es el siguiente.

Paso 1: El usuario (declarante) solicita al cliente AAA del dominio de proveedor de servicio NGN la utilización del servicio/aplicación.

Paso 2: El cliente AAA solicita la autentificación del usuario al servidor AAA (verificador) en el dominio de proveedor de servicio NGN.

Paso 3: El servidor AAA envía los resultados de la autentificación al cliente AAA.

Paso 4: El cliente AAA remite los resultados al usuario, donde el cliente AAA almacena la lista de acceso del usuario.

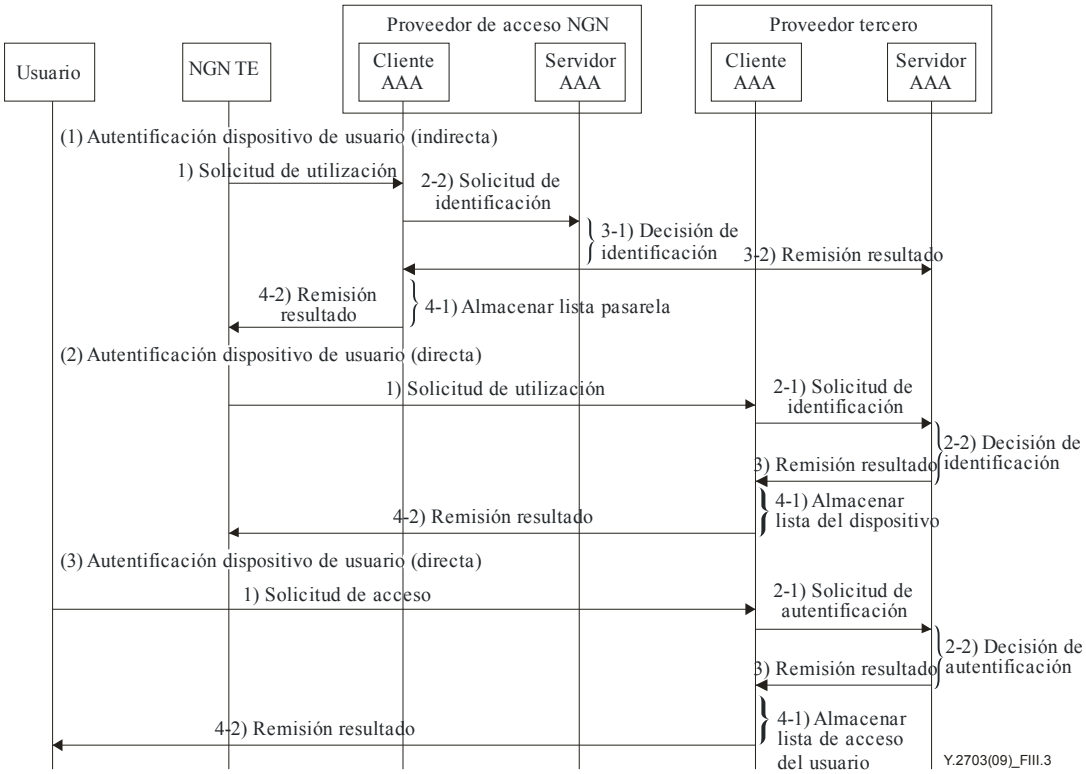

Figura III.3 – Procedimiento de autentificación y autorización del usuario por el proveedor de servicio NGN

III.3 Autentificación y autorización de proveedores NGN por el usuario

En este caso, hay dos tipos de autentificación y autorización por el usuario de la red:

– Autentificación del proveedor NGN por el usuario para anexión a la red ((1) de la figura III.4).

– Autentificación del proveedor NGN por el usuario para la obtención del servicio ((2) de la figura III.4).

El cliente AAA presta el servicio de autentificación para autentificar y autorizar la red y permite automáticamente al usuario acceder al proveedor de red, cuando procede.

El procedimiento de identificación del caso (1) de la figura III.4 es el siguiente.

Paso 1: El usuario (declarante) solicita la autentificación de NAP (puntos de acceso a la red) a un verificador tercero.

Paso 2: El verificador tercero remite la AI (información de autentificación) al NAP.

Paso 3: Intercambio de AI entre el verificador tercero y el NAP.

Paso 4: El verificador tercero remite los resultados al usuario, donde el verificador tercero verifica.

El procedimiento de identificación del caso (2) de la figura III.4 es el siguiente.

Paso 1: El usuario (declarante) solicita la autentificación de la red al verificador tercero.

Paso 2: El verificador tercero remite la solicitud del usuario al cliente AAA, donde el cliente AAA solicita la AI al servidor AAA.

Paso 3: El servidor AAA envía la AI al cliente AAA y hay intercambio de AI entre el verificador tercero y el cliente AAA.

Paso 4: El verificador tercero remite los resultados al usuario, donde el verificador tercero verifica.

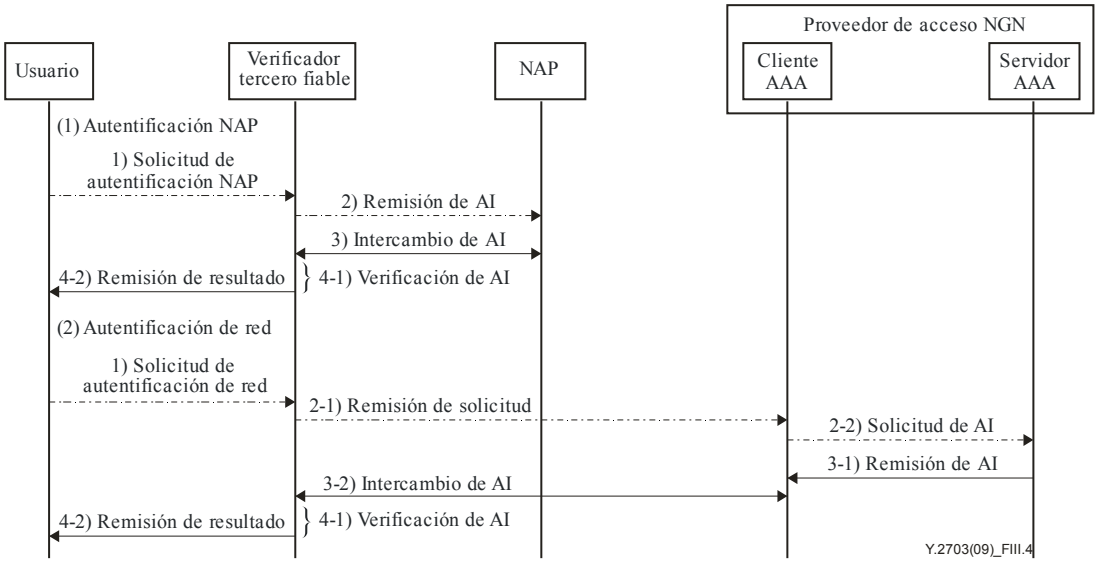

Figura III.4 – Procedimiento de autentificación y autorización de proveedores NGN

III.4 Autentificación y autorización por el proveedor NGN de otros proveedores de servicios/aplicaciones

En algunos casos, el proveedor de un servicio o aplicación es distintos del proveedor NGN (es decir, es un tercero el que actúa de proveedor de servicio/aplicación). El proveedor NGN habrá de autentificar y autorizar al otro proveedor de servicio/aplicación.

El cliente AAA presta el servicio de autentificación para que el proveedor NGN autentifique y autorice al otro proveedor de servicio/aplicación.

El procedimiento de identificación de la figura III.5 es el siguiente.

Paso 1: El cliente AAA (declarante) del proveedor NGN solicita la autentificación del proveedor de servicio/aplicación tercero a un verificador tercero.

Paso 2: El verificador tercero remite la solicitud del usuario al cliente AAA del proveedor de servicio/aplicación tercero y el cliente AAA solicita la AI al servidor AAA.

Paso 3: El servidor AAA remite la AI al cliente AAA y hay intercambio de AI entre el verificador tercero y el cliente AAA.

Paso 4: El verificador tercero remite los resultados al cliente AAA del proveedor NGN, donde el verificador tercero verifica y el servidor AAA almacena el resultado.

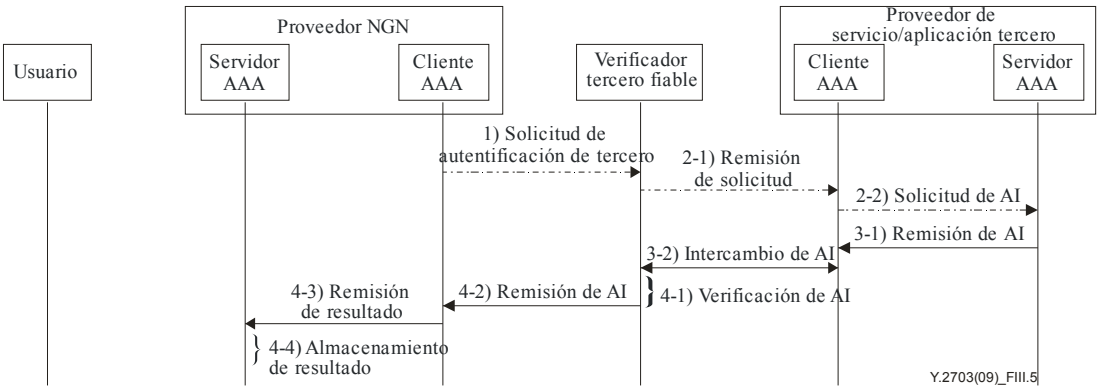

Figura III.5 – Procedimiento de autentificación y autorización del proveedor NGN de un proveedor de servicio/aplicación tercero

Bibliografía

[b-UIT-T M.3410] Recomendación UIT-T M.3410 (2008), *Directrices y requisitos para el soporte de la gestión de telecomunicaciones en sistemas de gestión de la seguridad.*

[b-UIT-T Q.3201] Recomendación UIT-T Q.3201 (2007), *Arquitectura del protocolo de señalización de seguridad basada en el protocolo de autentificación extensible para las conexiones de red.*

[b-UIT-T Q.3202.1] Recomendación UIT-T Q.3202 (2008), *Protocolos de autentificación basados en el protocolo de autentificación extendido-autentificación y acuerdo de clave (EAP-AKA) para el interfuncionamiento entre 3GPP, WiMax y WLAN en las NGN.*

[b-UIT-T X.509] Recomendación UIT-T X.509 (2005) | ISO/IEC 9594-8:2005, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Marcos para certificados de claves públicas y atributos*.

[b-UIT-T X.800] Recomendación UIT-T X.800 (1991), *Arquitectura de seguridad de la interconexión de sistemas abiertos para aplicaciones del CCITT.*

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

[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 X.811] Recomendación UIT-T X.811 (1995) | ISO/IEC 10181-2:1996, *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: Marco de autentificación*.

[b-UIT-T X.812] Recomendación UIT-T X.812 (1995) | ISO/IEC 10181-3:1996, *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: Marco de control de acceso*.

[b-UIT-T X.816] Recomendación UIT-T X.816 (1995) | ISO/IEC 10181-7:1996, *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: Marco de auditoría y alarmas de seguridad*.

[b-UIT-T Y.2001] Recomendación UIT-T Y.2001 (2004), *Visión general de las redes de próxima generación*.

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

[b-UIT-T Y 2012] Recomendación UIT-T Y.2012 (2006), *Requisitos funcionales y arquitectura de la red de próxima generación*.

[b-UIT-T Y.2201] Recomendación UIT-T Y.2201 (2007), *Requisitos de las redes de próxima generación, versión 1*.

[b-UIT-T Y.2233] Recomendación UIT-T Y.2233 (2008), *Requisitos y marco de referencia que admiten capacidades de contabilidad y tasación en las redes de la próxima generación*.

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

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

III.5 Utilización del servicio de autentificación y autorización de un tercero

Los proveedores de servicios pueden actuar como tercero para prestar servicios de autentificación y autorización. En este caso, los servicios de autentificación y autorización de terceros pueden ser de dos tipos:

– Autentificación del usuario para un proveedor de servicios ((1) de la figura III.6).

– Autentificación del proveedor de servicios para un usuario ((2) de la figura III.6).

III.5.1 Autentificación del usuario para un proveedor de servicios

El cliente AAA presta el servicio de autentificación a un proveedor de servicios para autentificar y autorizar un usuario y permite automáticamente al usuario acceder al proveedor de servicios/aplicaciones tercero, cuando procede.

El procedimiento de identificación de la figura III.6 es el siguiente.

Paso 1: El usuario (declarante) solicita al cliente AAA el acceso a la red.

Paso 2: El cliente AAA solicita la calificación del usuario al servidor AAA del proveedor de servicios/aplicaciones tercero, donde el servidor AAA (verificador) autentifica al usuario.

Paso 3: El servidor AAA envía los resultados de la autentificación al cliente AAA.

Paso 4: El cliente AAA remite los resultados al usuario, donde el cliente AAA almacena la lista de acceso del usuario.

Paso 5: Si se le concede, el usuario puede acceder al recurso especificado de la red.

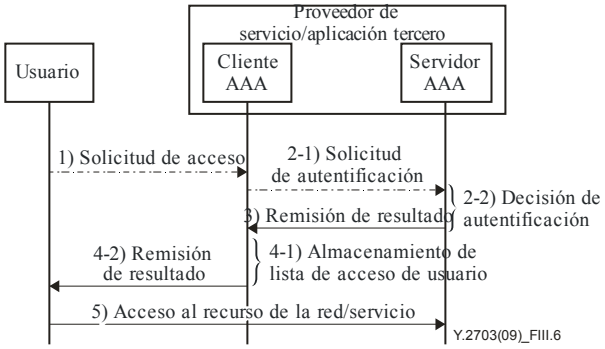

Figura III.6 – Procedimiento de utilización del servicio de autentificación y autorización de terceros

III.5.2 Autentificación del proveedor de servicios para un usuario

El cliente AAA presta el servicio de autentificación al usuario para autentificar un proveedor de servicios. El procedimiento de identificación de la figura III.7 es el siguiente.

Paso 1: El usuario (declarante) del dominio personalizado solicita al verificador tercero la autentificación del proveedor de servicios/aplicaciones tercero.

Paso 2: El verificador tercero remite la solicitud del usuario al cliente AAA del proveedor de servicios/aplicaciones tercero y el cliente AAA solicita la AI al servidor AAA.

Paso 3: El servidor AAA remite la AI al cliente AAA y hay intercambio de AI entre el verificador tercero y el cliente AAA.

Paso 4: El verificador tercero remite los resultados al cliente AAA del proveedor NGN, donde el verificador tercero verifica y almacena el resultado.

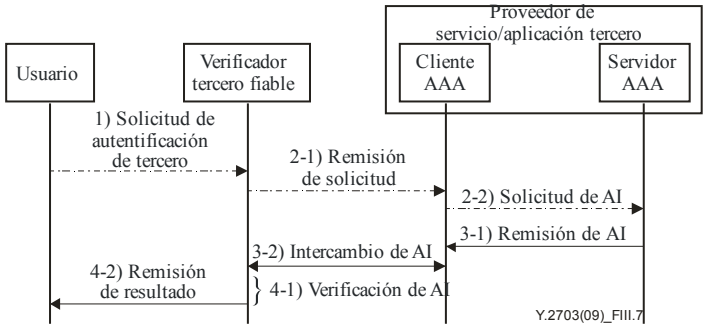

Figura III.7 – Procedimiento de utilización del servicio de auentificación y autorización de terceros

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