Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

Y.2702

(09/2008)

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

Redes de la próxima generación – Seguridad

Requisitos de autentificación y autorización para las NGN, versión 1

Recomendación UIT-T Y.2702

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.2702

Requisitos de autentificación y autorización para las NGN, versión 1

Resumen

En la Recomendación UIT-T Y.2702 se especifican los requisitos de autentificación y autorización para las redes de la nueva generación (NGN).

Orígenes

La Recomendación UIT-T Y.2702 fue aprobada el 12 de septiembre de 2008 por la Comisión de Estudio 13 del UIT-T (2005-2008) conforme al procedimiento consignado en la Resolución 1 de la AMNT.

Palabras clave

Red de la próxima generación (NGN), autentificación, autorización, seguridad, gestión de identidades (IdM), privilegios, atributos e identificadores.

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

1 Alcance 1

2 Referencias 2

3 Definiciones 2

3.1 Definiciones que figuran en [UIT-T X.800] 2

3.2 Definiciones que figuran en [UIT-T X.810] 2

3.3 Definiciones que figuran en [UIT-T X.811] 3

3.4 Definiciones que figuran en [UIT-T Y.2701] 3

3.5 Términos definidos en la presente Recomendación 4

4 Siglas y acrónimos 4

5 Modelos de referencia 6

5.1 Marco de autentificación UIT-T X.811 6

5.2 Amenazas a la autentificación 11

5.3 Garantía de autentificación 13

5.4 Autorización y gestión de privilegios 14

5.5 Modelo arquitectónico de referencia de extremo a extremo 15

5.6 Relación con la arquitectura de la NGN especificada en [UIT-T Y.2012] 16

6 Requisitos generales 18

7 Autentificación y autorización del usuario para el acceso a la red 18

7.1 Descripción 18

7.2 Modelo general de referencia 19

7.3 Requisitos 22

8 Autentificación y autorización del usuario por parte del proveedor NGN de servicio para el acceso al servicio/la aplicación 25

8.1 Descripción 25

8.2 Requisitos 26

9 Autentificación y autorización de los proveedores NGN por parte del usuario 29

9.1 Descripción 30

9.2 Objetivos y requisitos 30

10 Autentificación y autorización entre usuarios homólogos con el apoyo del proveedor NGN 30

11 Autentificación y autorización mutua de red 31

11.1 Descripción 31

11.2 Requisitos para la autentificación mutua de red 32

12 Autentificación y autorización de un tercer proveedor de servicio/aplicación por parte del proveedor NGN 33

12.1 Descripción 33

12.2 Requisitos 33

Página

13 Utilización del servicio de autentificación y autorización por terceros proveedores ... 34
13.1 Descripción ... 34
13.2 Requisitos ... 34
14 Autentificación y autorización de objetos ... 34
14.1 Descripción ... 34
14.2 Requisitos ... 35
Apéndice I – Caso de utilización de SAML ... 36
I.1 Utilización de la Recomendación [b-UIT-T X.1141], Lenguaje de marcas de asertos de seguridad (SAML 2.0) ... 36
I.2 Procedimientos de autentificación de servicio/aplicación ... 36
I.3 Autentificación de servicio/aplicación – Ejemplos de flujo de llamada ... 36
I.4 Seguridad de los procedimientos y mecanismos de autentificación de servicio/aplicación ... 37
Apéndice II – Autentificación y autorización ETS ... 38
II.1 Panorama general ... 38
II.2 Autentificación y autorización del usuario ETS ... 38
II.3 Autentificación y autorización del proveedor NGN para el ETS ... 39
II.4 Ejemplos de casos de autentificación y autorización ETS ... 39
Apéndice III – 3GPP Arquitectura de inicialización genérica ... 45
Apéndice IV – Ejemplos de flujo de llamada para la gestión de identidades (IdM) ... 47
IV.1 Descripción general ... 47
IV.2 Ejemplos de flujos de llamada ... 47
Bibliografía ... 59

Recomendación UIT-T Y.2702

Requisitos de autentificación y autorización para las NGN, versión 1

1 Alcance

En la presente Recomendación se especifican los requisitos de autentificación y autorización para las redes de la próxima generación (NGN) basados en la Recomendación [UIT-T Y.2012]. Se especifican los requisitos para la autentificación y autorización a través de la interfaz usuario-red (UNI), la interfaz red-red (NNI) y la interfaz aplicación-red (ANI), así como de cualquier entidad interna de la red que pueda exigir la autentificación y la autorización. En la presente Recomendación se tratan, entre otros, los siguientes temas:

1) La autentificación y autorización del usuario para acceder a la red (por ejemplo, la autentificación y autorización de un dispositivo de usuario, una pasarela de red residencial o una pasarela empresarial para acoplarse u obtener acceso a la red).
2) La autentificación y autorización del usuario por parte del proveedor de servicios para acceder a un servicio/aplicación (por ejemplo, la autentificación y autorización de un usuario, un dispositivo o una combinación de usuario/dispositivo cuando resulten necesarias para acceder a un servicio/aplicación NGN).
3) Autentificación y autorización de la red por parte del usuario (por ejemplo, el usuario autentifica la identidad de la red NGN conectada o del proveedor de servicios).
4) Autentificación y autorización entre usuarios homólogos (por ejemplo, la autentificación y autorización del usuario llamado (o entidad que termina la llamada), la autentificación y autorización de la entidad que origina la llamada o la autentificación del origen de los datos durante el funcionamiento de la red).
5) Autentificación y autorización mutua entre redes (por ejemplo, la autentificación y autorización a través de la interfaz NNI a nivel de transporte o de servicio/aplicación).
6) Autentificación y autorización del proveedor de servicios/aplicaciones.
7) Utilización del servicio de autentificación y autorización de un tercero.
8) Autentificación de objetos (por ejemplo, proceso de aplicación, contenido de mensajes e identificadores del contenido de datos).

Los elementos anteriores constan de la autentificación de los flujos del tráfico de señalización, de portador y de gestión, si procede.

Además, en esta Recomendación también se proporcionan modelos de referencia para la autentificación y la autorización NGN.

NOTA 1 – Se considera que la autentificación y autorización NGN forman parte de una disciplina más general denominada gestión de identidades (IdM) en las NGN. Las funciones y capacidades de autentificación y autorización que se describen en la presente Recomendación, deben utilizarse para las capacidades de garantía de identidad de la IdM en las NGN.

NOTA 2 – En la presente Recomendación, el término "usuario" no se refiere únicamente a una persona; un usuario puede ser una persona, grupos, empresas o entidades jurídicas.

NOTA 3 – La autentificación de una entidad no representa una validación positiva de una persona.

2 Referencias

Las siguientes Recomendaciones UIT-T y demás referencias contienen disposiciones que, mediante su referencia en este texto, constituyen disposiciones de esta Recomendación. A la fecha de esta publicación, las ediciones citadas están en vigor. Todas las Recomendaciones y otras referencias son objeto de revisión, por lo que se alienta a los usuarios de esta Recomendación a que utilicen la edición más reciente de las Recomendaciones y demás referencias que se indican a continuación. Se publica periódicamente una lista de las Recomendaciones UIT-T vigentes. La referencia a un documento en esta Recomendación no le confiere, como documento autónomo, la categoría de Recomendación.

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

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

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

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

[UIT-T Y.2012] Recomendación UIT-T Y.2012 (2006), *Requisitos funcionales y arquitectura de la versión 1 de la NGN*

[UIT-T Y.2201] Recomendación UIT-T Y.2201 (2007), *Requisitos de la versión 1 de las NGN*

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

3 Definiciones

3.1 Definiciones que figuran en [UIT-T X.800]

En la presente Recomendación se utilizan los siguientes términos definidos en [UIT-T X.800]:

3.1.1 información de autentificación: Información utilizada para establecer la validez de una identidad alegada.

3.1.2 autorización: Atribución de derechos, que incluye la concesión de acceso basada en derechos de acceso.

3.1.3 credencial: Datos que se transfieren para determinar la supuesta identidad de una entidad.

3.1.4 autentificación del origen de los datos: Confirmación de que la fuente de los datos recibidos es la alegada.

3.1.5 autentificación de entidad par: Corroboración de que una entidad par en una asociación es la pretendida.

3.2 Definiciones que figuran en [UIT-T X.810]

En la presente Recomendación se utilizan los siguientes términos definidos en [UIT-T X.810]:

3.2.1 confianza: Se dice que la entidad X confía en la entidad Y para un conjunto de actividades solamente si la entidad X puede confiar en que la entidad Y se comporta de una manera particular con respecto a las actividades.

3.2.2 tercero fiable: Autoridad de seguridad o su agente en la que se confía en lo que respecta a ciertas actividades pertinentes a la seguridad (en el contexto de una política de seguridad).

3.3 Definiciones que figuran en [UIT-T X.811]

En la presente Recomendación se utilizan los siguientes términos definidos en [UIT-T X.811]:

3.3.1 método de autentificación asimétrico: Método de autentificación en el que no toda la información de autentificación es compartida por ambas entidades.

3.3.2 identidad autentificada: Identificador distintivo de un principal que ha sido confirmado por autentificación.

3.3.3 autentificación: Confirmación de la identidad declarada de una entidad.

3.3.4 certificado de autentificación: Certificado de seguridad garantizado por una autoridad de autentificación, y que puede utilizarse para confirmar la identidad de una entidad.

3.3.5 intercambio de autentificación: Secuencia de una o más transferencias de intercambio de información de autentificación (AI) destinadas a efectuar una autentificación.

3.3.6 información de autentificación (AI): Información utilizada con fines de autentificación.

3.3.7 iniciador de autentificación: Entidad que comienza un intercambio de autentificación.

3.3.8 declarante: Entidad que es o representa a un principal a los efectos de la autentificación. Un declarante incluye las funciones necesarias para intervenir en intercambios de autentificación en nombre de un principal.

3.3.9 información de autentificación de declaración (AI de declaración): Información utilizada por un declarante para generar la información de autentificación de intercambio necesaria para autentificar un principal.

3.3.10 información de autentificación de intercambio (AI de intercambio): Información intercambiada entre un declarante y un verificador durante el proceso de autentificación de un principal.

3.3.11 principal: Entidad cuya identidad puede ser autentificada.

3.3.12 método de autentificación simétrico: Método de autentificación en el que ambas entidades comparten la misma información de autentificación.

3.3.13 información de autentificación de verificación (AI de verificación): Información utilizada por un verificador para confirmar una identidad declarada mediante AI de intercambio.

3.3.14 verificador: Entidad que es o representa a la entidad que requiere una identidad autentificada. Un verificador incluye las funciones necesarias para intervenir en intercambios de autentificación.

3.4 Definiciones que figuran en [UIT-T Y.2701]

En la presente Recomendación se utilizan los siguientes términos definidos en [UIT-T Y.2701]:

3.4.1 elemento limítrofe: Elemento de red que desempeña funciones de conexión de diferentes dominios de seguridad y administrativos.

3.4.2 red corporativa: Red privada que conecta diversos usuarios y puede estar en varios emplazamientos (por ejemplo, una empresa, un campus).

3.4.3 dominio de seguridad: Formado por un conjunto de elementos, una política de seguridad, una autoridad de seguridad y un conjunto de actividades relacionadas con la seguridad en el que los elementos se gestionan con arreglo a la política de seguridad. La autoridad de seguridad se encarga de gestionar la política. Un determinado dominio de seguridad puede constar de varias zonas de seguridad.

3.4.4 elemento limítrofe del equipo terminal: Elemento limítrofe que desempeña funciones de seguridad entre el equipo del cliente y la red del proveedor de servicios.

3.5 Términos definidos en la presente Recomendación

En la presente Recomendación se define el siguiente término:

3.5.1 acuerdo de nivel de servicio (*service level agreement,* SLA): Acuerdo oficial entre dos o más partes, al que se llega tras una actividad de negociación, con alcance para definir las características del servicio, las responsabilidades y prioridades de cada una de las partes. Un SLA puede incluir declaraciones sobre seguridad, calidad de funcionamiento, tarificación y facturación, prestación del servicio y compensaciones.

4 Siglas y acrónimos

En la presente Recomendación se utilizan las siguientes siglas y acrónimos.

ACL Lisa de control de acceso *(access control list)*

AI Información de autentificación *(authentication information)*

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

AS Servidor de aplicaciones *(application server)*

BE Elemento limítrofe *(border element)*

BSF Función de servidor de inicialización *(bootstrapping server function)*

B-TID Identificador de la transacción de inicialización *(bootstrapping transaction identifier)*

CSCF Función de control de la sesión de llamada *(call session control function)*

DSL Bucle digital de abonado *(digital subscriber loop)*

ENI Implementación nacional del ETS *(ETS national implementation)*

ETS Servicio de telecomunicaciones de emergencia *(emergency telecommunication service)*

FE Entidades funcionales *(functional entities)*

GAA Arquitectura de autentificación genérica *(generic authentication architecture)*

GBA Arquitectura de inicialización genérica *(generic bootstrapping architecture)*

GUSS Ajustes de seguridad del usuario de la GBA *(GBA user security settings)*

HSS Sistema de abonado residencial *(home subscriber system)*

HTTP Protocolo de transferencia de hipertexto *(hypertext transfer protocol)*

HTTPS Seguridad HTTP *(HTTP security)*

IAD Dispositivo de acceso integrado *(integrated access device)*

I-CSCF Función de control de la sesión de llamada de interrogación *(interrogating call session control function)*

ID-FF Marco de federación de identidades *(identity federation framework)*

IdM	Gestión de identidades *(identity management)*
IdP	Proveedor de identidad *(identity provider)*
ID-WSF	Marco de servicios web de identidad *(identity web services framework)*
IMS	Servicio de multimedios IP *(IP multimedia service)*
IP	Protocolo Internet *(Internet protocol)*
IWF	Función de interfuncionamiento *(interworking function)*
LUAD	Dispositivo o agente de usuario con capacidad liberty *(liberty enabled user agent or device)*
MAC	Control de acceso a los medios *(media access control)*
MS	Servidor de medios *(media server)*
NACF	Función de control de acoplamiento a la red *(network attachment control function)*
NAF	Función de aplicación de red *(network application function)*
NAP	Punto de acceso a la red *(network access point)*
NGN	Red de la próxima generación *(next generation network)*
NNI	Interfaz red-red *(network-to-network interface)*
OAM&P	Operaciones, administración, mantenimiento y configuración *(operations, administration, maintenance and provisioning)*
OSI	Interconexión de sistemas abiertos *(open system interconnection)*
P-CSCF	Función de control de la sesión de llamada de intermediario *(proxy call session control function)*
PES	Servicio de transición RTPC/RDSI *(PSTN/ISDN evolution service)*
PIN	Número de identificación personal *(personal identification number)*
PKI	Infraestructura de claves públicas *(public key infrastructure)*
PII	Información identificable personalmente *(personally identifiable information)*
PSK	Claves precompartidas *(pre-shared keys)*
RACF	Función de control de recursos y admisión *(resource and admission control function)*
RBAC	Control de acceso según la función *(role based access control)*
RDSI	Red digital de servicios integrados *(integrated services digital network)*
RP	Parte que confía *(relying party)*
RPH	Encabezamiento de prioridad de recursos *(resource-priority header)*
RSVP	Protocolo de reserva de recursos *(resource reservation protocol)*
SAML	Lenguaje de marcas de asertos de seguridad *(security assertion markup language)*
SASL	Capa de seguridad y autentificación sencilla *(simple authentication and security layer)*
SBC	Controlador limítrofe de la sesión *(session border controller)*
S-CSCF	Función de control de la sesión de llamada de servicio *(serving call session control function)*
SDP	Protocolo de descripción de la sesión *(session description protocol)*

SIM Módulo de identificación de abonado *(subscriber identification module)*

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

SLF Función de localizador de abonado *(subscriber locator function)*

SOAP Protocolo sencillo de acceso a objetos *(simple object access protocol)*

SP Proveedor de servicios *(service provider)*

SSOS Servicio de inicio de sesión unificado *(single-sign-on service)*

TDR Telecomunicaciones para operaciones de socorro *(telecommunication for disaster relief)*

TE Equipo terminal *(terminal equipment)*

TE-BE Equipo terminal – Elemento limítrofe *(terminal equipment – border element)*

TLS Seguridad en la capa de trasporte *(transport layer security)*

UAI Interfaz usuario-autentificación *(user authentication interface)*

UE Equipo de usuario *(user equipment)*

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

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

WS Servidor web *(web server)*

XML Lenguaje de marcas extensible *(eXtensible markup language)*

5 Modelos de referencia

5.1 Marco de autentificación UIT-T X.811

En la presente Recomendación se utilizan los conceptos básicos de autentificación descritos en [UIT-T X.811], que se resumen a continuación.

5.1.1 Conceptos básicos de autentificación

La autentificación permite corroborar la identidad alegada de una entidad. Sólo tiene sentido en el contexto de una relación entre un principal y un verificador. Pueden distinguirse dos casos importantes:

- el principal está representado por un declarante que dispone de una relación de comunicación específica con el verificador (autentificación de entidad); y
- el principal es el origen de los datos que tiene el verificador (autentificación del origen de los datos).

La autentificación de entidad sirve para corroborar la identidad de una entidad principal, en el contexto de una relación de comunicaciones. La identidad autentificada de un principal sólo puede garantizarse cuando se recurre a un servicio de autentificación.

NOTA 1 – Al utilizar la autentificación del origen de los datos es necesario también asegurarse de que los datos no hayan sido modificados. Para ello puede utilizarse un servicio de integridad, por ejemplo:

- utilizar entornos en los que no pueden alterarse los datos;
- verificar que la huella digital de los datos recibidos corresponda con la de los datos enviados;
- emplear un mecanismo de firma digital; o
- utilizar un algoritmo de cifrado simétrico.

NOTA 2 – El término "relación de comunicaciones" empleado en la definición de autentificación de entidad puede interpretarse de manera muy general y podría referirse, por ejemplo, a una conexión OSI, a la comunicación entre procesos o a la interacción entre un usuario y un terminal.

5.1.2 Identificadores

Un principal es una entidad cuya identidad puede autentificarse. Cada principal dispone de uno o varios identificadores distintos. Las entidades utilizan los servicios de autentificación para verificar las identidades que alegan los principales. La identidad del principal verificada de este modo se denomina la identidad autentificada. Análogamente, un principal cuya identidad se ha verificado se denomina entidad autentificada.

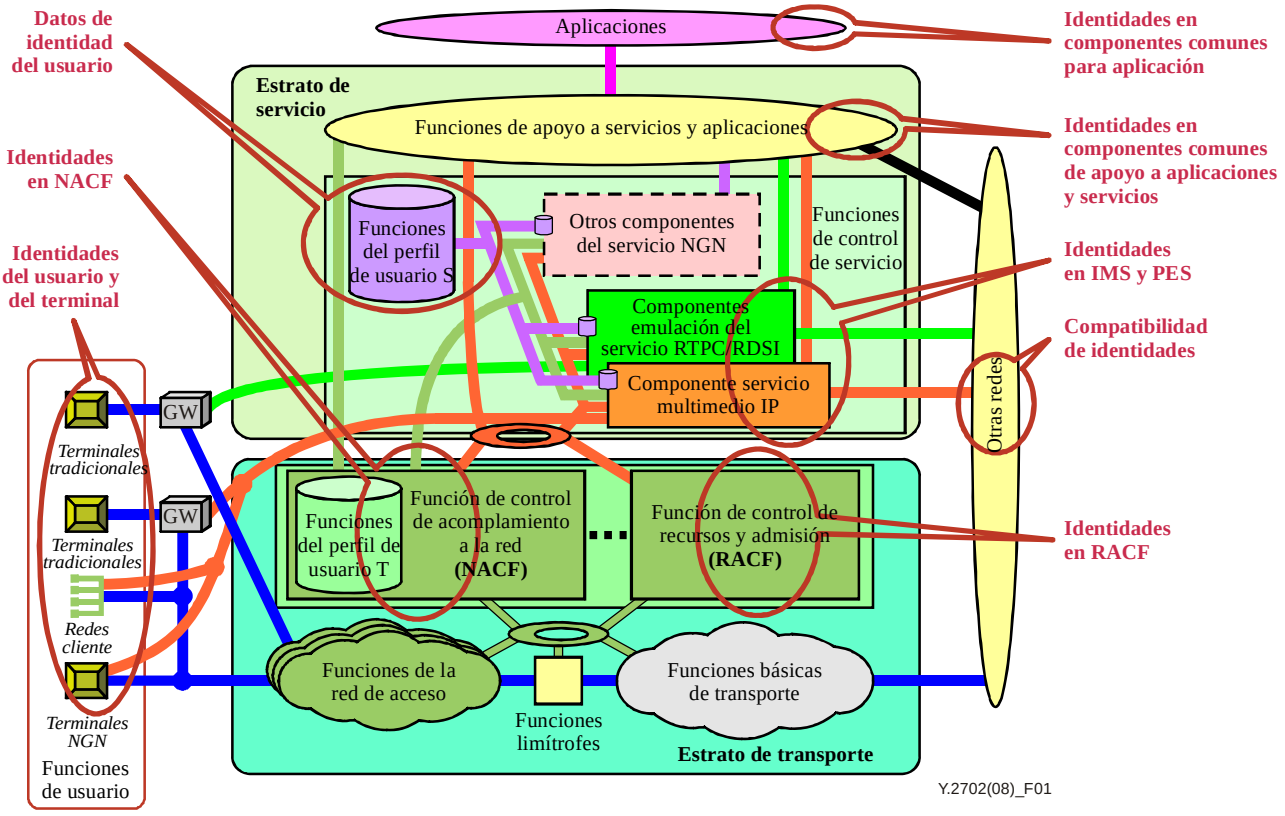
Como ejemplos de principales que pueden identificarse y por consiguiente autentificar se pueden citar los siguientes:

- usuarios humanos (personas);
- proveedores NGN;
- procesos;
- sistemas abiertos en tiempo real;
- entidades de la capa OSI;
- empresas, y
- flujos en el portador, señalización y tráfico de gestión.

Los identificadores distintivos se utilizan para alegar la identidad de manera inequívoca dentro de un determinado dominio de seguridad. Estos identificadores sirven para distinguir a los principales entre sí dentro de un mismo dominio, en una de las dos maneras siguientes:

1) mediante la pertenencia del miembro a un grupo de entidades consideradas equivalentes a los efectos de la autentificación (en este caso, el grupo en su conjunto se considera un solo principal y tiene un solo identificador distintivo); o
2) mediante la identificación de una y sólo una entidad.

Cuando la autentificación se efectúa entre diferentes dominios de seguridad, un solo identificador distintivo quizá no resulte suficiente para identificar inequívocamente una entidad, por cuanto varias autoridades de diferentes dominios de seguridad puede utilizar los mismos identificadores distintivos. En tal caso, resulta indispensable utilizar los identificadores distintivos junto con el identificador del dominio de seguridad para obtener así un identificador inequívoco para la unidad.



NOTA – La pasarela (GW) puede existir en el estrato de transporte o en las funciones de usuario.

Figura 1 – Ejemplo de identificadores NGN

Los componentes y elementos funcionales en los diferentes estratos y capas de la NGN pueden recurrir a los identificadores utilizados para identificar un principal o una entidad. En la Figura 1 se muestra un ejemplo de identificadores para las NGN basado en la Figura 8 (Componentes de la NGN) de la [UIT-T Y.2012].

Ejemplos de identificadores distintivos característicos son los siguientes:

- nombres de directorio;
- direcciones de red;
- títulos AP y títulos AE;
- identificadores de objeto;
- nombres de personas (inequívocos dentro del contexto del dominio);
- quíntuples que constan de:
  - dirección IP de origen,
  - dirección IP de destino,
  - número del puerto de origen,
  - número del puerto de destino, y
  - número del protocolo.

5.1.3 Entidades de autentificación

El término "declarante" se utiliza para describir la entidad que es o representa un principal a los efectos de la autentificación. El declarante dispone de las funciones necesarias para llevar a cabo un intercambio de autentificación de parte de un principal.

El término "verificador" se utiliza para describir la entidad que es o representa la entidad solicitante de una identidad autentificada. El verificador dispone de las funciones necesarias para llevar a cabo un intercambio de autentificación destinado a solicitar la verificación de una identidad alegada.

Toda identidad que participe en una autentificación mutua desempeñará las funciones de declarante y verificador.

El término "tercero fiable" se utiliza para describir una autoridad de seguridad, o su agente, en el que confían otras entidades en lo relativo a las actividades de seguridad. En el contexto de la presente Recomendación, el declarante y/o verificador confía en el tercero fiable a los efectos de la autentificación.

NOTA – El componente o verificador puede constar de múltiples componentes funcionales que se hallen en diferentes sistemas abiertos.

5.1.4 Información de autentificación

Los tipos de información de autentificación que se describen en la presente norma son los siguientes:

- información de autentificación de intercambio (AI de intercambio);
- información de autentificación de declaración (AI de declaración);
- información de autentificación de verificación (AI de verificación).

El terminó "intercambio de autentificación" se emplea para describir una secuencia de una o varias transferencias de AI de intercambio a los efectos de la autentificación.

En la Figura 2 se ilustra la relación entre el declarante, el verificador y el tercero fiable. También se muestran los tres tipos de información de autentificación que constituyen un intercambio de autentificación

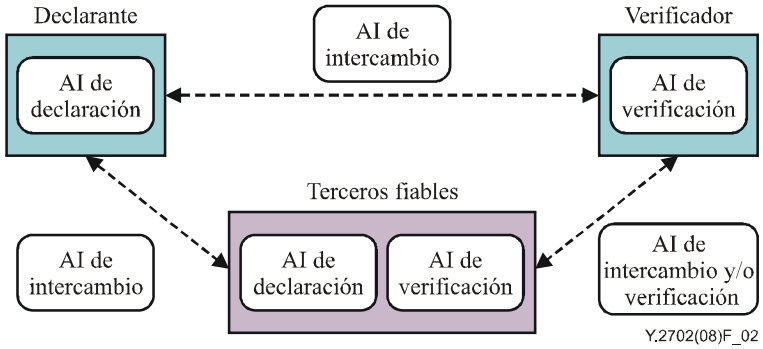


Figura 2 – Relaciones entre el declarante, el verificador y el tercero fiable

En ciertos casos, para generar la AI de intercambio puede resulta necesario interactuar con un tercero fiable. Análogamente, para verificar la AI de intercambio, es posible que el verificador tenga que interactuar con un tercero fiable. En estos casos, el tercero fiable puede poseer la AI de verificación relacionada con un principal.

También es posible que se utilice un tercero fiable en la transferencia de AI de intercambio. Dependiendo del tipo de intercambio, el tercero puede desempeñar la función de declarante respecto al verificador.

Por otra parte, las entidades pueden requerir información de autentificación para autentificar al tercero fiable.

5.1.5 Autentificación basada en múltiples factores

Consiste en verificar varios identificadores y atributos relacionados con el principal para corroborar la autenticidad de la identidad de dicho principal. Por regla general, la autentificación multifactor puede realizarse a partir de los siguientes grupos de atributos de autentificación:

1) algo que eres (por ejemplo, las características físicas o de comportamiento del usuario, o las características o atributos del cliente que se comparan, tales como el análisis mecanográfico o el reconocimiento vocal);
2) algo que posees (por ejemplo, el permiso de conducir o un testigo de seguridad);
3) algo que sabes (por ejemplo, una contraseña, un número de identificación personal o una imagen de seguridad).

El ejemplo más común de clave de autentificación basada en un sólo factor es una contraseña (algo que se sabe). A veces para verificar la identidad de una entidad no basta con una contraseña y se requerirá una autentificación más robusta mediante otras claves de autentificación para acceder a ciertos recursos, aplicaciones y servicios NGN. Ello dependerá de los riesgos y la probabilidad de que entidades no autorizadas obtengan acceso a los recursos, aplicaciones y servicios NGN.

Los factores de autentificación y las claves deben seleccionarse en función de los riesgos. Así pues, para determinar la autentificación necesaria se habrán de evaluar las repercusiones que tendría el acceso a recursos, aplicaciones y servicios NGN por parte de entidades no autorizadas. Ejemplos de claves de autentificación electrónica son los siguientes:

- contraseñas,
- testigos físicos,
- testigos lógicos,
- testigos basados en dispositivos de contraseña volátil.

La autentificación mediante contraseñas está muy extendida. La "contraseña" es un secreto que el declarante memoriza y utiliza para autentificar su identidad. Normalmente son cadenas de caracteres o imágenes memorizadas que el abonado debe identificar cuando se le presentan junto a otras imágenes similares. Ahora bien, los sistemas basados en contraseña son susceptibles a muchos ataques. Aunque para proteger la contraseña puede recurrirse a protecciones adicionales en el canal de comunicaciones, con ello tampoco se impiden todos los tipos de ataques.

Los testigos físicos son dispositivos físicos especializados que protegen los secretos (en general, claves criptográficas) y realizan operaciones criptográficas. Para la autentificación se ha de poseer el dispositivo y conocer la clave. Se utilizan operaciones criptográficas para la autentificación de las dos partes y la protección del canal de comunicaciones empleado en el intercambio de autentificación.

Los testigos lógicos consisten fundamentalmente en un código lógico que simula un testigo físico y tiene muchas de las ventajas de éste (por ejemplo, la clave criptográfica se suele almacenar en disco o en otro soporte). La clave del testigo lógico puede cifrase utilizando una clave obtenida a partir de ciertos datos de activación. Los datos de activación suelen consistir en una contraseña que sólo conoce el usuario y que resulta indispensable para activar el testigo. Así pues, la autentificación consiste en facilitar la clave y su verificación. Al igual que en los testigos físicos, los testigos lógicos se utilizan para autentificar las dos partes y para proteger el canal de comunicaciones utilizado en el intercambio de autentificación.

El testigo basado en dispositivo generador de contraseñas volátiles es un dispositivo físico personal que genera contraseñas "volátiles" para la autentificación. Estos sistemas de contraseñas volátiles se basan en una serie de contraseñas generadas mediante algoritmos especiales. Cada contraseña de la serie se denomina contraseña volátil por cuanto es distinta de las otras generadas y sólo puede

utilizarse una vez. Existen sistemas de contraseñas volátiles muy diversos que ofrecen distintos grados de protección contra ataques.

5.2 Amenazas a la autentificación

Los factores y las claves de autentificación pueden ser objeto de ataques dirigidos a:

1) "Algo que eres" – consiste en duplicar las características o atributos del cliente con el que se compara (por ejemplo, las huellas digitales, los patrones mecanográficos).
2) "Algo que posees" – consiste en conseguir o copiar lo que posee el cliente.
3) "Algo que sabes" – consiste en adivinar o descubrir cierta información que memoriza el cliente.

En general, las amenazas a la autentificación pueden clasificarse en ataques dirigidos contra el protocolo de autentificación y otros ataques que puedan revelar información confidencial o el valor de los testigos.

La utilización de múltiples factores de autentificación mejora la seguridad, por cuanto se habrán de socavar varios métodos. La utilización de un dispositivo físico (que se posee) que no sea fácil de duplicar también reduce la posibilidad de un ataque, ya que normalmente el propietario reparará en que ha extraviado el dispositivo. Utilizando claves de autentificación basadas en testigos físicos o lógicos junto con datos de activación (por ejemplo una contraseña) se obtiene una doble autentificación, que ya no se basa inequívocamente en la mera posesión de un testigo.

El cliente puede socavar el sistema de autentificación si divulga deliberadamente su clave de autentificación basada en un solo factor a un cómplice y luego desmiente este hecho con el propósito de rechazar las subsiguientes autentificaciones. Estas artimañas resultan menos creíbles si se utiliza una autentificación basada en múltiples factores, lo que puede disuadir este tipo de ataques.

5.2.1 Amenazas al protocolo de autentificación

Ejemplos de amenazas contra el protocolo de autentificación son los siguientes:

1) Intervenir la comunicación:
   - se observa el intercambio de mensajes del protocolo de autentificación para analizarlos después;
   - se trata en general de sonsacar testigos para luego hacerse pasar por declarantes.
2) Impostores:
   - el declarante impostor se hace pasar por un abonado ante el verificador para tratar de adivinar testigos y obtener otra información sobre un determinado abonado;
   - el verificador impostor se hace pasar por un verificador que da legitimidad a los declarantes abonados con el fin de obtener testigos que luego puede utilizar para hacerse pasar por un abonado con el fin de legitimar verificadores;
   - el tercero fiable impostor se hace pasar por un sistema tercero fiable ante los verificadores para obtener información confidencial del usuario.
3) Apropiadores:
   - se apropian de una sesión autentificada y luego se hacen pasar por abonados ante los terceros fiables con el fin de obtener información confidencial o introducir información falsa;
   - se apropian de la sesión autentificada y luego se hacen pasar por un tercero fiable ante los verificadores con el fin de obtener información confidencial o facilitar información falsa.

Estos ataques pueden mitigarse de los siguientes modos:

- Exigir que en cada autentificación varíe un elemento para contrarrestar los ataques por repetición.
- Los ataques por intervención y por apropiación de la sesión pueden contrastarse mediante técnicas criptográficas que protejan el canal de señalización (cifrado del canal) utilizado para el intercambio de autentificación (por ejemplo, TLS en modo anónimo).
- Los ataques por intromisión y por suplantación de la identidad del verificador pueden contrarrestarse, hasta cierto punto, utilizando protecciones similares a los ataques por intervención o apropiación de la sesión. Combinando el cifrado con otras técnicas criptográficas se mejora la protección contra estos ataques (por ejemplo, utilizando un intercambio mutuo de paso de testigo además de la criptografía -como es el caso de TLS en modo autentificado- de tal modo que las claves criptográficas obren en poder del cliente y el verificador efectúe una autentificación mutua "fuerte").
- La resistencia que ofrece el cifrado contra los ataques por intromisión y por suplantación de la identidad del verificador es tan sólo limitada, ya que es posible poner en peligro la seguridad de intercambio sin burlar el cifrado. Por ejemplo, es posible engañar a un cliente para que acepte un intercambio autentificación que supuestamente procede el verificador pero que en realidad no es el caso. Entre el cliente y el verificador pueden utilizarse técnicas criptográficas de autentificación mutua.

5.2.2 Amenazas a los testigos de autentificación

Si un atacante se hace con el control de un testigo podrá hacerse pasar por el propietario de dicho testigo. Las amenazas contra los testigos pueden clasificarse según el tipo de ataque contra las claves de autentificación como se indica a continuación:

- El atacante puede robar o clonar algo que posees. Por ejemplo si el atacante consigue acceso al computador de un usuario puede copiar el testigo lógico. Los testigos físicos pueden robarse o duplicarse.
- El atacante puede enterarse de algo que sabes. Puede adivinar una contraseña o un PIN. Cuando el testigo consiste en un secreto compartido, el atacante puede obtener acceso al verificador y conseguir el valor del secreto. Por otra parte, el atacante puede instalar código malicioso (por ejemplo, un programa que registre las teclas pulsadas) con el fin de capturar esta información. El atacante, además, puede determinar el secreto mediante ataques fuera de línea dirigidos al tráfico de la red correspondiente a un intento de autentificación.
- El atacante puede duplicar algo que eres. El atacante puede obtener una copia del testigo de identificación del usuario y construir un duplicado.

Para mitigar estas amenazas existen diversas estrategias:

- Reducir las posibilidades de ataques utilizando múltiples factores. Si el atacante necesita robar un testigo criptográfico y adivinar una contraseña, el esfuerzo quizá resulte demasiado grande.
- Emplear mecanismos de seguridad físicos para impedir la duplicación de testigos robados. Estos mecanismos pueden utilizarse para comprobar, detectar y reaccionar en caso de alteración.
- Utilizar contraseñas complejas, lo que reduce la probabilidad de que el atacante las adivine. Al exigir que se utilicen contraseñas largas que no figuren en diccionarios, se obliga a los atacantes a tener que probar todas las combinaciones posibles.
- Recurrir a controles de seguridad de red y de sistema para impedir que el atacante obtenga acceso al sistema o instale código malicioso.

5.2.3 Otras amenazas a la autentificación

Los ataques no se dirigen inequívocamente al protocolo de autentificación. También pueden consistir en:

- ataques mediante código malicioso que pueden poner en peligro los testigos de autentificación;
- ataques por intrusión, que obtienen credenciales o testigos al entrar al sistema del abonado/declarante, de la autoridad de certificación o del verificador;
- amenazas desde el interior que pueden poner en peligro los testigos de autentificación;
- ataques por otros medios, con los que se consiguen de alguna otra manera los testigos, por ejemplo mediante ingeniería social para inducir al abonado a revelar su contraseña al atacante o "fisgonear";
- ataques que consisten en engañar a los declarantes para que utilicen un protocolo inseguro, haciéndoles creer que es seguro, o utilizar un ardid para burlar los controles de seguridad (por ejemplo, aceptar certificados de servidor que no pueden validarse);
- rechazo intencionado por parte del abonado que ha puesto deliberadamente en peligro sus testigos.

Una forma de luchar contra los ataques de código malicioso y de ingeniería social consiste en educar y asesorar al cliente. Para contrarrestar los ataques que tratan de defraudar al cliente se recurre normalmente a la auditoría y la detección de anomalías. Un mecanismo de disuasión contra este tipo de ataques es utilizar la autentificación basada en múltiples claves. Los ataques desde el interior pueden contrarrestarse investigando al personal, efectuando auditorías y (en su caso) la separación de funciones y el doble control.

5.3 Garantía de autentificación

Para proteger los recursos, aplicaciones y servicios de una NGN, el proveedor NGN debe determinar el nivel de garantía de la autentificación necesario para el acceso a la red y las transacciones de aplicación/servicio.

Cada proveedor NGN debe establecer y aplicar un proceso que ofrezca garantía de autentificación. Este proceso consistirá en un método para establecer categorías de confianza (es decir, confianza en la información sobre la identidad presentada por medios electrónicos al proveedor de servicios) en los mecanismos de autentificación y la información facilitada para tal fin.

Este proceso servirá para establecer y utilizar niveles de garantía relativos y discretos con el fin de cuantificar la confianza en el proceso de autentificación. Por ejemplo, podrían utilizarse "n" niveles de garantía de autentificación, de tal modo que nivel cero corresponda al nivel de menor garantía y el nivel "n" al más alto. Estos niveles podían utilizarse para definir el nivel de garantía en función de las posibles consecuencias (por ejemplo, la naturaleza de las posibles repercusiones) en caso de que se produzca un error de autentificación, partiéndose del supuesto de que todos los identificadores utilizados en la autentificación no son equivalentes o no tienen necesariamente el mismo valor para la autentificación.

A continuación se muestra un ejemplo del método de garantía de autentificación:

Ejemplo de método de autentificación	
Nivel de garantía	**Confianza relativa**
Nivel 0	Sin confianza en la validez de la identidad alegada (por ejemplo, la utilización de controles de lista de acceso)
Nivel 1	Confianza moderada en la validez de la identidad alegada
Nivel 2	Confianza elevada en la validez de la identidad alegada
--	--
Nivel n	Mayor grado de confianza en la validez de la identidad alegada

El proveedor NGN debe evaluar los posibles riesgos que entrañan los errores de autentificación o determinar el nivel correspondiente de garantía en una entidad (por ejemplo, la identidad del usuario). Los errores de autentificación que tengan las consecuencias más adversas requerirán mayores niveles de garantía.

El riesgo que conllevan los errores de autentificación depende de dos factores:

a) daños o repercusiones potenciales;

b) la probabilidad de tales daños o repercusiones.

Las categorías de daños y repercusiones son, entre otras, las siguientes:

- molestias, dificultades o daños al prestigio o la reputación,
- pérdidas financieras,
- responsabilidad del cliente o del proveedor NGN,
- daños a la infraestructura, recursos, aplicaciones, servicios o intereses públicos del proveedor NGN,
- perjuicio a los intereses públicos o del gobierno (por ejemplo, comunicaciones esenciales tales como ETS y TDR),
- revelación no autorizada de información confidencial,
- daño a los servicios de seguridad personal,
- violación del código civil o criminal.

5.4 Autorización y gestión de privilegios

La autentificación por sí misma no basta para determinar el margen de maniobra de una entidad autentificada una vez que se le ha otorgado acceso. Así pues, la autentificación debe combinarse con mecanismos de gestión de autorizaciones y privilegios y con métodos para controlar el acceso a servicios y recursos NGN. Por ejemplo, la asignación de funciones y privilegios a usuarios/abonados para controlar el acceso a servicios, aplicaciones e interfaces de gestión para gestionar su suscripción y perfil del usuario. Otra posibilidad es el control de acceso basado en la función (RBAC) para controlar el acceso OAM&P.

Las autorizaciones o privilegios pueden considerarse un atributo de la identidad de la entidad. Dependiendo de la política de seguridad, los privilegios de autorización de una entidad pueden validarse al efectuar la autentificación.

5.5 Modelo arquitectónico de referencia de extremo a extremo

En esta cláusula se describe el modelo de referencia de extremo a extremo utilizado para organizar y agrupar las prescripciones de autentificación en la presente Recomendación. El modelo de referencia consiste en lo siguiente:

1) Autentificación y autorización de usuario para acceder a la red (por ejemplo, la autentificación y autorización de un dispositivo usuario, una pasarela de red residencial o una pasarela empresarial para obtener acceso o acoplarse a la red).

2) Autentificación del proveedor de servicios y autorización del usuario para acceder al servicio/aplicación (por ejemplo, autentificación y autorización del usuario, un dispositivo o una combinación de usuario/dispositivo para acceder al servicio/aplicación NGN).

3) Autentificación y autorización del usuario por parte del proveedor de servicios para acceder a un determinado servicio/aplicación (por ejemplo, la autentificación y autorización específicas de ETS y TDR[1]).

4) Autentificación y autorización de la red por parte del usuario (por ejemplo, el usuario autentifica la identidad de la red NGN conectada o del proveedor de servicios).

5) Autentificación y autorización entre usuarios homólogos (por ejemplo, la autentificación y autorización del usuario llamado (o entidad terminal), la autentificación y autorización de la entidad de origen o la autentificación del origen de los datos durante el funcionamiento de la red).

6) Autentificación y autorización mutua entre redes (por ejemplo, la autentificación y autorización a través de la interfaz NNI a nivel de transporte o a nivel de servicio/aplicación).

7) Autentificación y autorización del proveedor de servicios/aplicaciones.

8) Utilización del servicio de autentificación de un tercero.

En la Figura 3 se ilustra los puntos de referencia de autentificación mencionados en los párrafos precedentes.

En la presente Recomendación el término "usuario" no se refiere estrictamente a una persona; un usuario puede ser una persona, grupos, empresas o entidades jurídicas

[1] La autentificación ETS puede requerir otras capacidades además de las básicas.

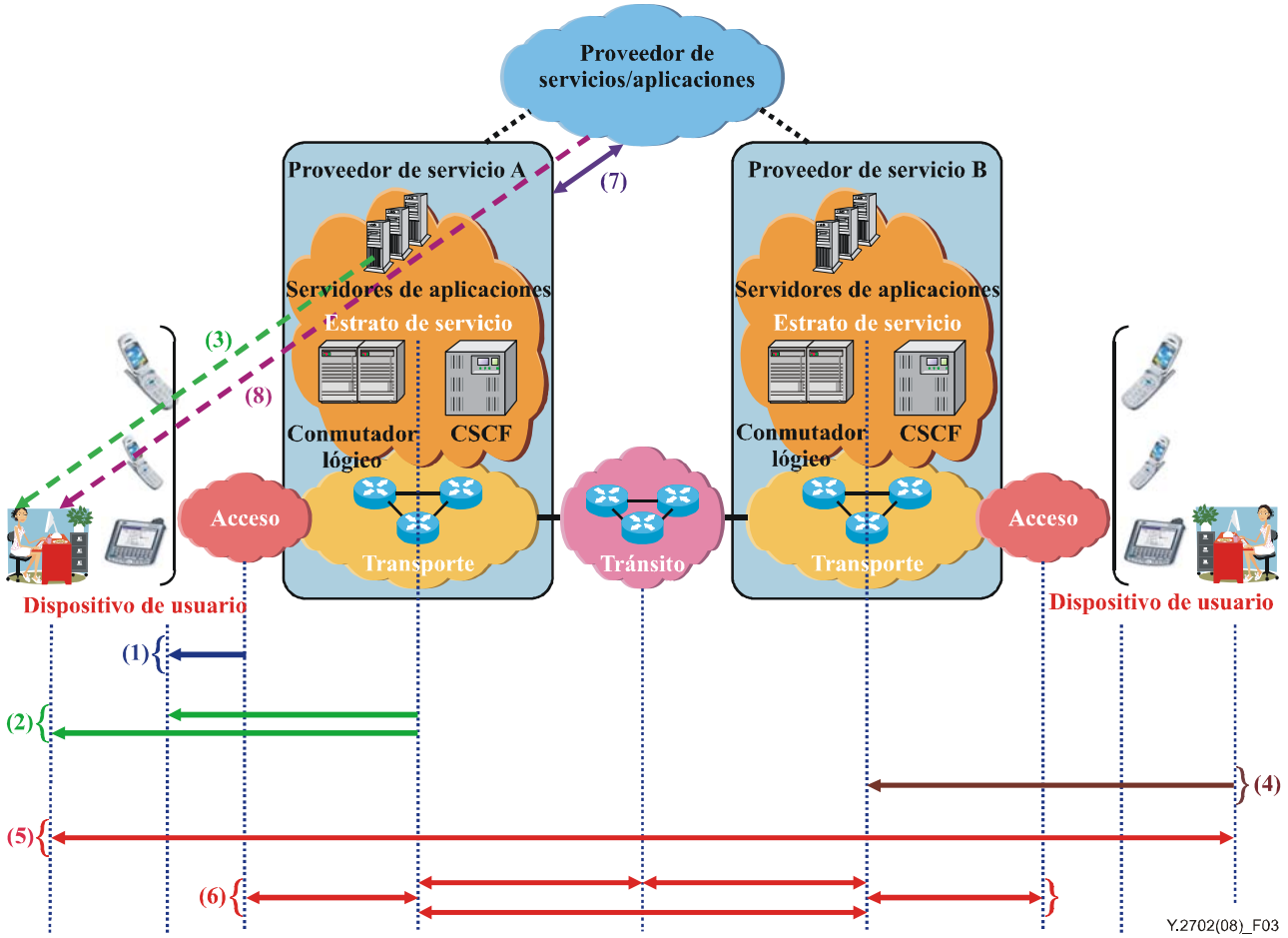


Figura 3 – Modelo arquitectónico de referencia de extremo a extremo

Cómo se observa en la Figura 3, la autentificación y autorización se efectúa a nivel de transporte y a nivel de servicio/aplicación. Además, puede efectuarse una autentificación vinculada o agregada, por ejemplo, cuando el proveedor de servicio vincula/agrupa la autentificación del usuario y del dispositivo del usuario para lograr un mayor nivel de garantía de autentificación. En la mayoría de los casos, la autentificación horizontal se efectúa en cada tramo. La principal excepción es la autentificación entre usuarios, que se efectúa de extremo a extremo. Salvo el caso de autentificación de usuario y autorización de la red, las relaciones requieren la autentificación mutua.

5.6 Relación con la arquitectura de la NGN especificada en [UIT-T Y.2012]

En esta cláusula se describe la relación entre modelo de referencia descrito en la presente Recomendación y el modelo arquitectónico funcional descrito en [UIT-T Y.2012]. Concretamente, se destaca lo siguiente:

- La relación de autentificación entre homólogos en la Figura 1 de la [UIT-T Y.2012], "descripción general de la arquitectura de las NGN".
- Los elementos funcionales de la Figura 1 de la [UIT-T Y.2012] para efectuar la autentificación.
- Los elementos funcionales de la Figura 1 de la [UIT-T Y.2012] para la vinculación, correlación y gestión de identidades.
- Los elementos funcionales de la Figura 1 de la [UIT-T Y.2012] para obligar a aplicar el control de acceso basado en el rechazo de la autentificación.

La Figura 4 se basa en la Figura 1 de la [UIT-T Y.2012] para ilustrar las relaciones de autentificación indicadas en la cláusula 5.5 de la presente Recomendación. Las relaciones de autentificación entre homólogos se muestran mediante flechas sólidas bidireccionales. En cambio, no se muestra el punto 5), es decir la autentificación y autorización entre usuarios homólogos. Obsérvese que aun cuando sea el proveedor NGN (en lugar de la ANI) quien suministre las aplicaciones al usuario, sigue habiendo una relación de autentificación entre el usuario y la aplicación, y el estrato de servicio y la aplicación.

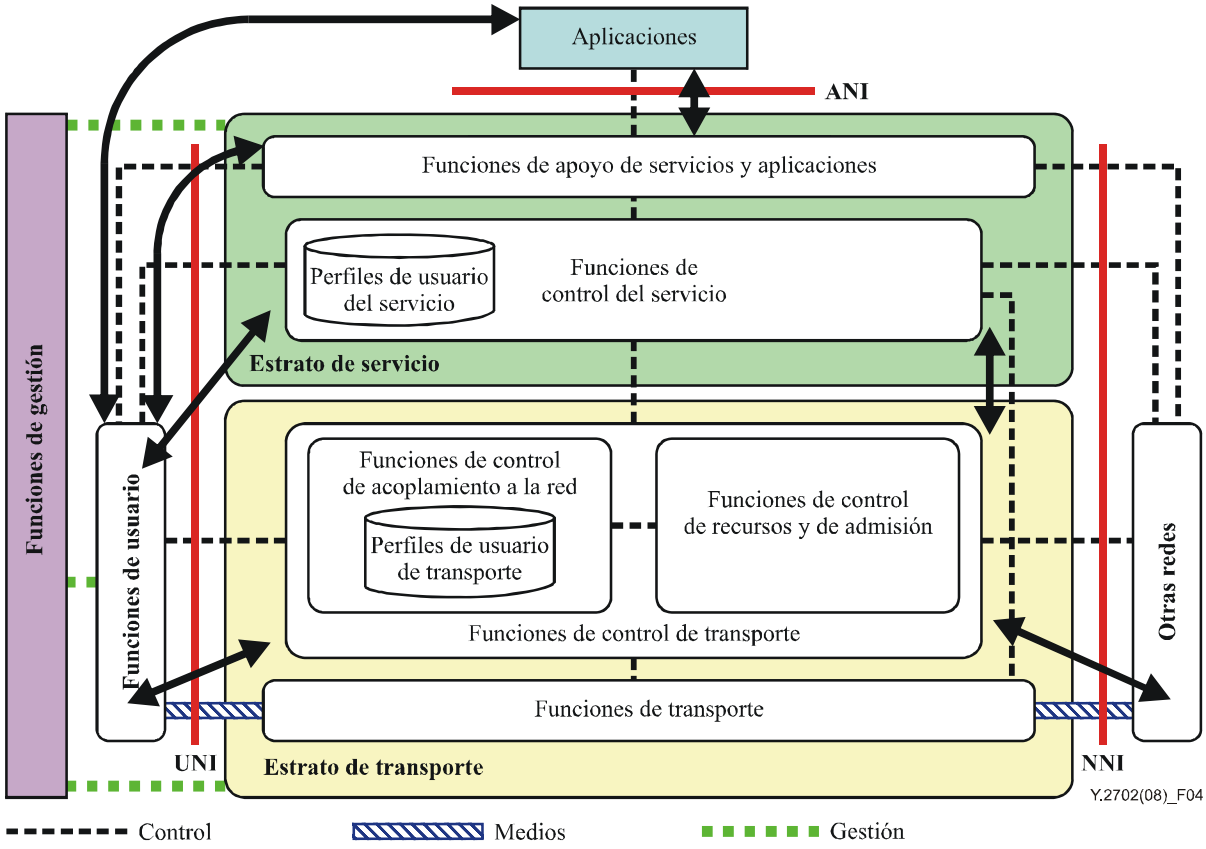


Figura 4 – Relaciones de autentificación entre homólogos

En la Figura 5 se ilustran las entidades funcionales (FE) del modelo de referencia descrito en la [UIT-T Y.2012] que desempeñan o pueden desempeñar las funciones de autentificación y autorización.

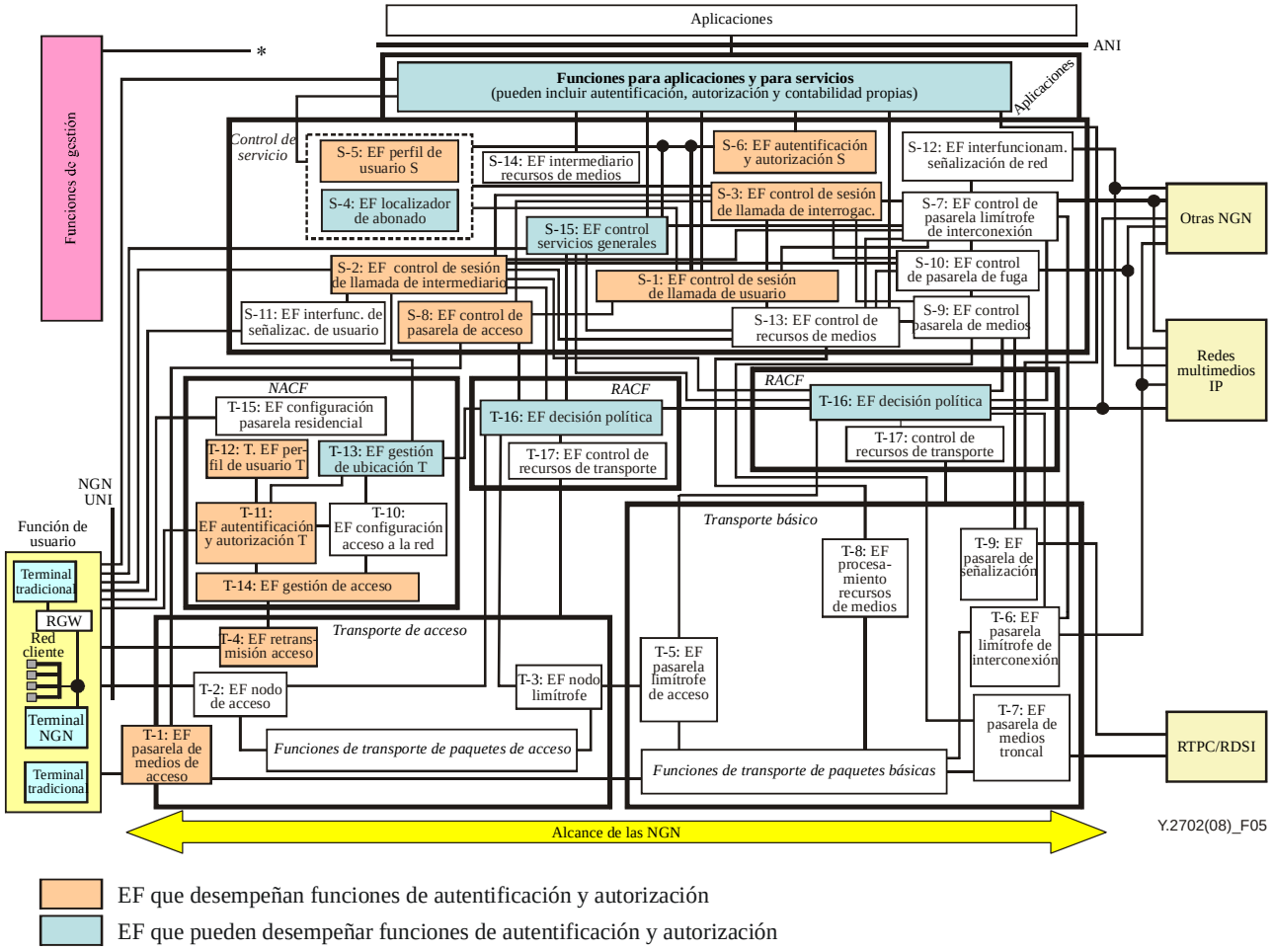


Figura 5 – Entidades funcionales de autentificación y autorización de [UIT-T Y.2012]

6 Requisitos generales

Esta Recomendación exige el apoyo de los requisitos generales de identificación, autentificación y autorización definidos en [UIT-T Y.2701] y [UIT-T Y.2201], a saber:

(R-1) – Se soportarán los requisitos definidos en el § 7.3.2 (Autentificación) de [UIT-T Y.2701].

(R-2) – Se soportarán los requisitos definidos en el § 6.12 (Identificación, autentificación y autorización) de [UIT-T Y.2201].

7 Autentificación y autorización del usuario para el acceso a la red

7.1 Descripción

Se necesitan servicios y capacidades de autentificación y autorización para el acceso a la red con miras a atenuar los riesgos inherentes a un acceso no autorizado. Asimismo, se necesitan servicios de autentificación y autorización para el acceso a la red con el fin de verificar las identidades y determinar si se debe conceder o no acceso al equipo del usuario final (es decir, equipo terminal (TE) y equipo terminal-elemento limítrofe (TE-BE)) que solicita conectividad a la NGN.

Suposiciones generales

a) El término usuario final no se refiere estrictamente a una persona; los usuarios finales pueden ser personas, grupos, empresas o entidades jurídicas.

b) De conformidad con [UIT-T Y.2012], no se hace suposición alguna en relación con las diversas interfaces y redes de usuario final que se podrían conectar a la red de acceso NGN. En la NGN se admiten todas las categorías de equipos del usuario final, es decir desde teléfonos tradicionales de una sola línea hasta complejas redes empresariales. Los equipos de usuario final pueden ser móviles o fijos.

c) La determinación de los elementos de red que implementan los servicios de acceso y autorización no cae dentro del alcance de esta Recomendación.

d) Las funciones de autorización y acceso a red pueden proporcionarse como parte de la función general del acoplamiento a red (NACF) definida en [UIT-T Y.2012].

7.2 Modelo general de referencia

En la Figura 6 se ilustra el modelo de referencia para la autorización y autentificación del acceso/el acoplamiento a la red, que consta de los siguientes dominios de seguridad:

1) Dominio del cliente – Dominio no confiable que contiene el equipo de usuario que utiliza el cliente y a quién le pertenece, por ejemplo:

   a) TE y TE-BE tradicionales

      - El TE tradicional representa los dispositivos de usuario tradicionales que se conectan mediante el acceso en banda estrecha (por ejemplo, líneas analógicas y RDSI). Estos TE obtienen acceso a la red IP mediante una pasarela del proveedor NGN (por ejemplo, una pasarela de medios o de acceso).
      - El TE-BE tradicional representa los equipos de usuario que actúan como un conjunto de puntos de extremo (por ejemplo, pasarelas de red empresarial y residencial) que se conectan mediante el acceso en banda estrecha (por ejemplo, líneas analógicas y RDSI). Estos TE-BE obtienen acceso a la red IP mediante una pasarela del proveedor NGN (por ejemplo, pasarela de medios o de acceso).

   b) TE y TE-BE tradicionales con un dispositivo de acceso integrado (IAD)

      - El TE tradicional con el IAD representa los dispositivos de usuario tradicionales que se conectan mediante acceso en banda ancha (por ejemplo, xDSL o Cable). Estos TE obtienen el acceso a la red IP por medio del IAD en el dominio del cliente.
      - El TE-BE tradicional representa los equipos de usuario que actúan como un conjunto de puntos de extremo (por ejemplo, pasarelas de red empresarial y residencial) que se conectan por acceso en banda ancha (por ejemplo, xDSL y Cable). Este equipo de usuario obtiene el acceso a la red IP por medio del IAD en el dominio del cliente.

   c) TE y TE-BE NGN

      - TE NGN representa los dispositivos de usuario en el dominio del cliente con capacidades IP para la conectividad directa a la red IP (por ejemplo, utilizando acceso en banda ancha de cable y xDSL).
      - TE-BE NGN representa los equipos de usuario que actúan como conjuntos de puntos de extremo (por ejemplo, pasarelas de red empresarial y residencial) con capacidades IP para la conectividad directa a la red IP.

2) Dominio del proveedor NGN de acceso: Red de acceso acogida por un proveedor NGN (por ejemplo, banda estrecha, xDSL y Cable). El proveedor NGN de acceso puede o no ser el mismo que el proveedor NGN de servicio. Las relaciones de confianza entre los proveedores NGN están regidas por los acuerdos sobre el nivel de servicio (SLA).

3) Dominio del proveedor NGN de servicio: El proveedor NGN de servicio ofrece un servicio/aplicación NGN a sus abonados. Las relaciones de confianza entre los proveedores NGN están regidas por los SLA.

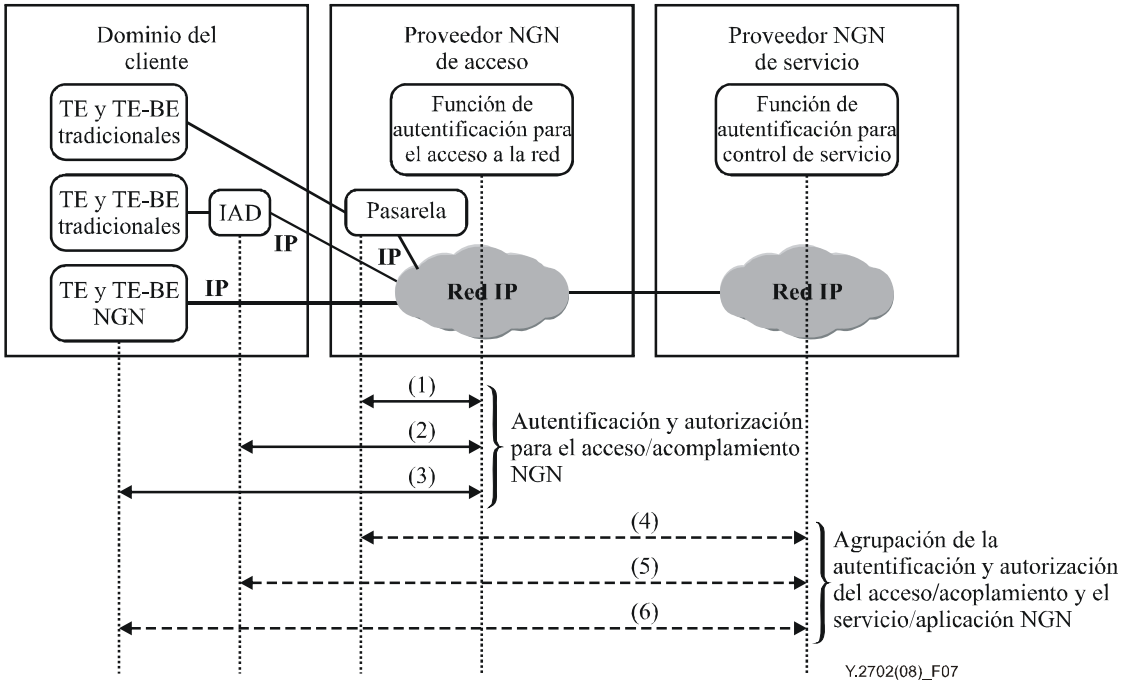


Figura 6 – Modelo de referencia de autentificación y autorización para el acceso/acoplamiento a la red

En la Figura 6 se ilustran las relaciones correspondientes a la identificación, autentificación y autorización para el acceso/acoplamiento a la red:

a) Autentificación y autorización del acceso/acoplamiento NGN a dispositivos – Servicios y capacidades para identificar, autentificar y autorizar el acceso o el acoplamiento a dispositivos de usuario para acceder a la red IP.

   1) Este flujo de información representa a los servicios y capacidades destinados a identificar, autentificar y autorizar TE y TE-BE tradicionales para el acceso/el acoplamiento a la red IP. El flujo de información tiene lugar entre la cabecera (declarante) en el dominio NGN de acceso que termina los TE y el TE-BE tradicionales en el dominio del cliente y un elemento de red (por ejemplo, el punto de acceso a la red) en el dominio NGN de acceso que proporciona las funciones de autentificación y de autorización para el acceso/acoplamiento NGN. Las funciones de autorización y autentificación del acceso/acoplamiento NGN (verificador) pueden formar parte de la NADF general definida en [UIT-T Y.2012]. No obstante, el lugar donde se implementa esta función depende del tipo de implementación.

2) Este flujo de información representa servicios y capacidades para identificar, autentificar y autorizar TE y TE-BE tradicionales con IAD en el dominio del cliente para el acceso/acoplamiento a la red IP de acceso. El flujo de información tiene lugar entre el IAD (declarante) en el dominio del cliente y el elemento de red (por ejemplo, el punto de acceso a la red) en el dominio NGN de acceso que proporciona la autentificación y autorización del acceso/acoplamiento NGN. La función de autentificación y autorización del acceso/acoplamiento NGN (verificador) puede formar parte de la NACF general definida en [UIT-T Y.2012]. No obstante, el lugar donde dicha función se implementa depende del tipo de implementación.

3) Este flujo de información representa servicios y capacidades para identificar, autentificar y autorizar TE y los TE-BE NGN con capacidades IP en el dominio del cliente para el acceso/acoplamiento a la red IP. El flujo de información tiene lugar entre los TE o TE-BE NGN (declarantes) en el dominio del cliente y un elemento de red (por ejemplo, el punto de acceso a la red) en el dominio NGN de acceso que proporciona la autentificación y la autorización para el acceso/acoplamiento NGN. La función de autentificación y autorización del acceso/acoplamiento NGN (verificador) puede formar parte de la NACF general definida en [UIT-T Y.2012]. No obstante, el lugar donde dicha función se implementa depende del tipo de implementación.

b) Agrupación de la autentificación y autorización del acceso/acoplamiento a dispositivos y de la aplicación/el servicio NGN – Servicios y capacidades para agrupar la autentificación del dispositivo de usuario por parte del proveedor NGN de acceso con la autentificación y autorización del usuario por parte del proveedor NGN de servicio:

4) Este flujo de información representa servicios y capacidades para que el proveedor NGN de servicio identifique y autorice implícitamente los TE y TE-BE tradicionales. El flujo de información circula entre una pasarela (declarante) en el dominio de la red de acceso y el dominio del proveedor NGN (verificador).

5) Este flujo de información representa servicios y capacidades para que el proveedor NGN de servicio identifique y autorice implícitamente los TE y el TE-BE tradicionales con IAD. El flujo de información circula entre el IAD (declarante) en el dominio del cliente y el dominio del proveedor NGN de servicio (verificador).

6) Este flujo de información representa servicios y capacidades para que el proveedor NGN de servicio identifique, autentifique y autorice directamente los TE y TE-BE NGN en el dominio del cliente. El flujo de información circula entre el TE NGN y el TE-BE NGN (declarante) en el dominio del cliente y el dominio del proveedor NGN de servicio (verificador).

Modelo de referencia para el nomadismo

En la Figura 7 se ilustra el modelo de referencia para el nomadismo. Este modelo de referencia es similar al modelo de referencia general, salvo porque conforme a esta hipótesis se debe tomar en consideración una NGN visitada y una NGN contratada.

1) Dominio de la NGN visitada: NGN acogida por un proveedor NGN visitado. Proporciona funciones de red visitada a otros proveedores NGN (por ejemplo, el proveedor de la red contratada). Las relaciones de confianza están regidas por los SLA. La red visitada puede ofrecer servicios NGN y puede tener sus propios abonados.

2) Dominio de la NGN contratada: NGN acogida por el proveedor de la NGN contratada. El proveedor de la NGN contratada ofrece servicios NGN a sus abonados. Las relaciones de confianza están regidas por los SLA.

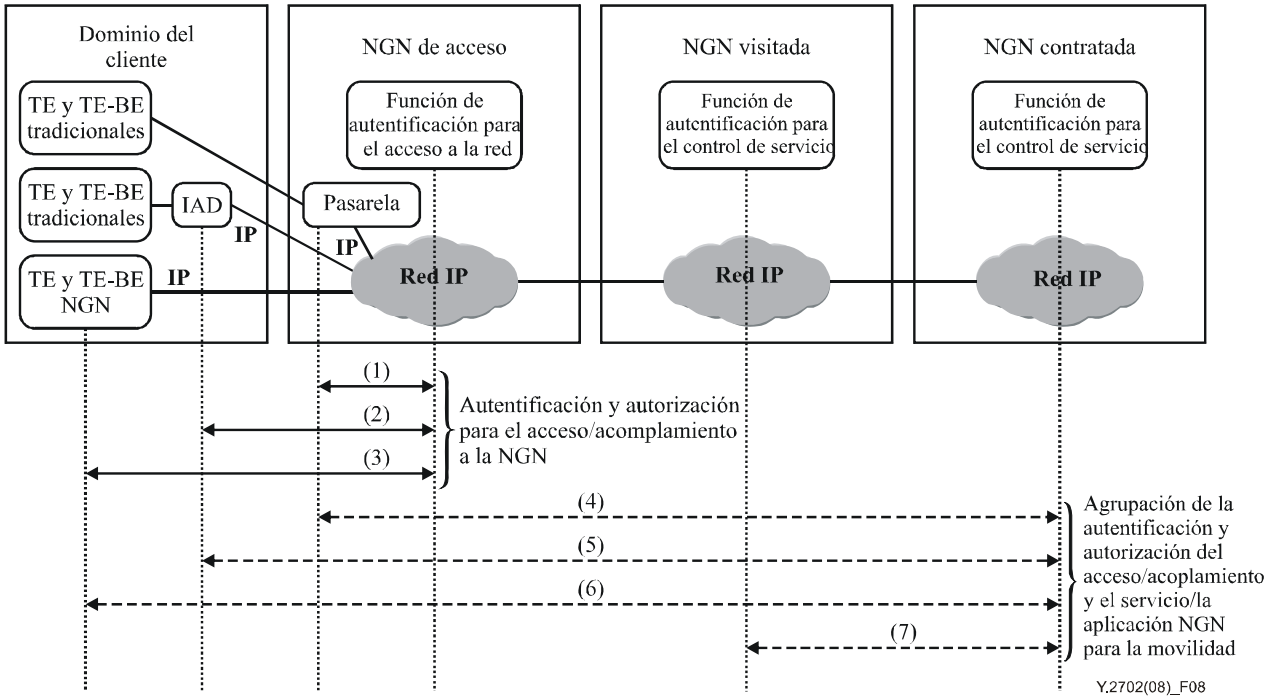


Figura 7 – Modelo de referencia para el nomadismo

El modelo de referencia muestra los flujos de información entre los diferentes dominios con el fin de agrupar la autentificación y la autorización del dispositivo de usuario y la autentificación y la autorización del usuario para facilitar el nomadismo. Los flujos de información representan servicios y capacidades para agrupar la autentificación y autorización del dispositivo de usuario, por parte del proveedor NGN visitado, con la autentificación y la autorización del usuario, por parte del proveedor NGN contratado, para facilitar el nomadismo.

(1) – (6) – Estos flujos de información son los mismos flujos que los descritos en la Figura 6 para la hipótesis de un único proveedor de servicio.

(7) Este flujo de información representa servicios y capacidades para que un proveedor NGN visitado y un proveedor NGN contratado intercambien información de identificación, autentificación y autorización para favorecer el nomadismo.

7.3 Requisitos

7.3.1 Requisitos generales

A continuación figuran los requisitos generales de la identificación, autentificación y autorización para el acceso/acoplamiento NGN a dispositivos:

(R-3) – Es preciso que la NGN sea capaz de identificar los dispositivos de abonado/usuario final (por ejemplo, TE y TE-BE), a tenor de la política del proveedor NGN.

(R-4) – Es preciso que la NGN sea capaz de identificar, autentificar y autorizar el acoplamiento del TE y el TE-BE en los puntos de acceso a la red (NAP).

(R-5) – Es preciso que se conceda inequívocamente acceso a la red a los TE y TE-BE autorizados.

(R-6) – Cuando se trata de múltiples redes, es preciso que cada uno de los dominios administrativos (por ejemplo, el proveedor NGN de acceso, el proveedor NGN visitado y el proveedor NGN contratado) haga cumplir las políticas pertinentes (por ejemplo, las relaciones de confianza) relativas a la identificación, autentificación y autorización del acceso/acoplamiento a la red del TE y el TE-BE (por ejemplo, recurriendo a los SLA).

(R-7) – Es preciso que la NGN tenga capacidades para proteger la información de autentificación y de autorización (por ejemplo, el perfil del usuario, la información sobre el abono, las pautas de identidad) contra el acceso no autorizado, la manipulación y la corrupción.

(R-8) – Es preciso que la NGN tenga capacidades para ofrecer confidencialidad y protección de la integridad de los intercambios de mensajes e información utilizados para la autentificación y la autorización.

(R-9) – Es preciso que la NGN tenga capacidades para proteger contra ataques (por ejemplo, retransmisión de mensajes y denegación de servicio) a las funciones y capacidades de autentificación y autorización.

(R-10) – Es preciso que la NGN sea capaz de detectar y registrar intentos de acceso no autorizado (por ejemplo, se podría fijar un margen configurable para el número de intentos de acceso no autorizado más allá del cual se generará una alarma que se registrará y señalará al sistema de gestión).

7.3.2 TE y TE-BE tradicionales

Los NAP que soportan el acceso a la red de los TE y TE-BE tradicionales deben tener capacidades para identificar, autentificar y autorizar dicho acceso.

(R-11) – Es preciso que los puntos de acceso a la red (NAP) que soportan a los TE y TE-BE tradicionales tengan capacidades para identificar inequívocamente la línea fija para el acoplamiento o la conectividad a la NGN. Se puede utilizar una dirección de capa 2 para identificar una línea fija (por ejemplo, MAC o dirección de capa de enlace). Esta función podría proporcionarse como parte de la NACF general definida en [UIT-T Y.2012].

(R-12) – Es preciso que los NAP que soportan a los TE y TE-BE tradicionales tengan capacidades para autentificar y autorizar la línea fija con miras al acoplamiento o la conectividad a la NGN. Se puede utilizar la información sobre el perfil del usuario/el abono al estrato de transporte y las listas de control de acceso (ACL) para autorizar el acceso de la línea fija a la NGN. Estas funciones se pueden proporcionar como parte de la NACF general definida en [UIT-T Y.2012].

(R-13) – Es preciso que los NAP que soportan a los TE y TE-BE tradicionales tengan capacidades para enlazar y vincular la identidad de una línea fija con la dirección IP utilizada para la conectividad de acceso NGN. Esta función se puede proporcionar como parte de la NACF general definida en [UIT-T Y.2012].

7.3.3 TE y TE-BE tradicionales con IAD

Los NAP que soportan el acceso a la red de los TE y TE-BE tradicionales con IAD en el dominio del cliente deben tener capacidades para identificar, autentificar y autorizar dicho acceso.

(R-14) – Es preciso que los NAP que soportan los TE y TE-BE tradicionales con IAD en el dominio del cliente tengan capacidades para identificar inequívocamente la línea fija y el IAD para el acoplamiento y la conectividad a la NGN. Se puede utilizar una dirección de capa 2 para identificar una línea fija (por ejemplo, dirección de capa de enlace o MAC) y una dirección IP para el IAD. Esta función se podría proporcionar como parte de la NACF general definida en [UIT-T Y.2012].

(R-15) – Es preciso que los NAP que soportan los TE y TE-BE tradicionales con IAD en el dominio del cliente tengan capacidades para autentificar y autorizar el IAD con miras al acoplamiento y la conectividad a la NGN. Inequívocamente los IAD autorizados pueden obtener el acoplamiento y la conectividad a la NGN. Se puede utilizar la información sobre el perfil del usuario/el abono al estrato de transporte y las listas de control de acceso (ACL) para autorizar el acceso de la línea fija y el IAD a la NGN.

Estas funciones se pueden proporcionar como parte de la NACF general definida en [UIT-T Y.2012].

(R-16) – Es preciso que los NAP que soportan los TE y TE-BE tradicionales con IAD tengan capacidades para enlazar y vincular la identidad de una línea fija con la identidad del IAD. Esta función podría proporcionarse como parte de la NACF general definida en [UIT-T Y.2012].

7.3.4 TE y TE-BE NGN

Los NAP que soportan el acceso a la red de los TE y TE-BE NGN deben tener capacidades para identificar, autentificar y autorizar dicho acceso a la NGN.

(R-17) – Es preciso que los NAP que soportan los TE y TE-BE NGN (es decir, la conectividad IP directa) tengan capacidades para identificar inequívocamente los dispositivos de usuario dentro de su dominio para el acoplamiento y la conectividad a la NGN. Los TE y TE-BE NGN pueden ser identificados inequívocamente por las direcciones de red y las identidades de dispositivos (por ejemplo, identidades de equipo, tarjetas SIM, testigos de seguridad, direcciones IP, etc.).

(R-18) – Es preciso que los NAP que soportan a los TE y TE-BE NGN (es decir, la conectividad IP directa) tengan capacidades para autentificar y autorizar dispositivos de usuario dentro de su dominio para el acoplamiento y la conectividad NGN. La autenticación y la autorización podría basarse en la información sobre el perfil del usuario/el abono al estrato de transporte. Inequívocamente los TE y TE-BE NGN autorizados pueden obtener el acoplamiento o la conectividad de red para la NGN. Estas funciones podrían proporcionarse como parte de la NACF general definida en [UIT-T Y.2012].

7.3.5 Autentificación y autorización de una combinación de dispositivo de usuario y usuario

Sobre la base de una evaluación de riesgos, podría ser necesario proceder a la autentificación y autorización combinada del usuario y del dispositivo del usuario para ofrecer una garantía de identidad superior. La NGN puede tener capacidades para agrupar las funciones de autentificación del acoplamiento/acceso NGN y el acceso a servicios/aplicaciones basados en información sobre el estrato de transporte (por ejemplo, información sobre acceso a la red y dispositivos de usuario) y el estrato de servicio (por ejemplo, perfil del usuario/abono).

(R-19) – Se necesitan capacidades para identificar y vincular inequívocamente una combinación del usuario y el dispositivo del usuario, a tenor de la política del proveedor NGN.

(R-20) – Se necesitan capacidades para autentificar y autorizar una combinación del usuario y el dispositivo del usuario a tenor de la política del proveedor NGN. Sólo los usuarios y dispositivos de usuario autorizados pueden obtener el acoplamiento/acceso a la red y el acceso a servicios/aplicaciones.

7.3.6 Autentificación y autorización de una combinación de dispositivos de usuario y de usuario para el nomadismo

Se puede proceder a la autentificación y autorización de una combinación del dispositivo del usuario y del usuario con el fin de ofrecer una garantía de identidad superior para el nomadismo. Se podrían utilizar capacidades para intercambiar y compartir información sobre identificación, autentificación y autorización (por ejemplo, información sobre perfiles de usuario) entre los diferentes dominios administrativos (es decir, proveedor NGN de acceso, proveedor NGN visitado y proveedor NGN contratado) para la IdM (véase el § 8.2.2).

(R-21) – Es preciso disponer de capacidades para identificar inequívocamente una combinación de dispositivos de usuario y de usuario para el nomadismo, a tenor de la política del proveedor NGN.

(R-22) – Se necesitan capacidades para autentificar y autorizar una combinación de dispositivos de usuario y de usuarios para el nomadismo, a tenor de la política del proveedor NGN. En los casos en los cuales el servicio es independiente del dispositivo de usuario, la autentificación de la información de acceso tal como la línea fija, el emplazamiento o la dirección de acceso podría combinarse con la autentificación del usuario para ofrecer una seguridad superior.

8 Autentificación y autorización del usuario por parte del proveedor NGN de servicio para el acceso al servicio/la aplicación

8.1 Descripción

Se necesitan capacidades para atenuar los riesgos inherentes al acceso no autorizado a los servicios y prestaciones proporcionados por un proveedor NGN. Se necesitan servicios y capacidades de autentificación y autorización para determinar si un usuario está autorizado para recibir un servicio o para realizar una acción conforme a sus privilegios. Se considera que la autentificación y autorización para servicios/aplicaciones es una autentificación de un usuario por parte del proveedor NGN y una autorización para que dicho usuario reciba servicios NGN o realice una acción conforme a sus privilegios. La autentificación y autorización de servicio/aplicación puede entrañar la verificación de las entidades y la autorización de los privilegios de:

- el usuario
- el dispositivo de usuario
- una combinación de dispositivo de usuario y usuario.

Según la arquitectura NGN definida en [UIT-T Y.2012], en el estrato de servicio se prestarán las funciones de autentificación y autorización de servicio/aplicación utilizando la información sobre el perfil del usuario y el abono.

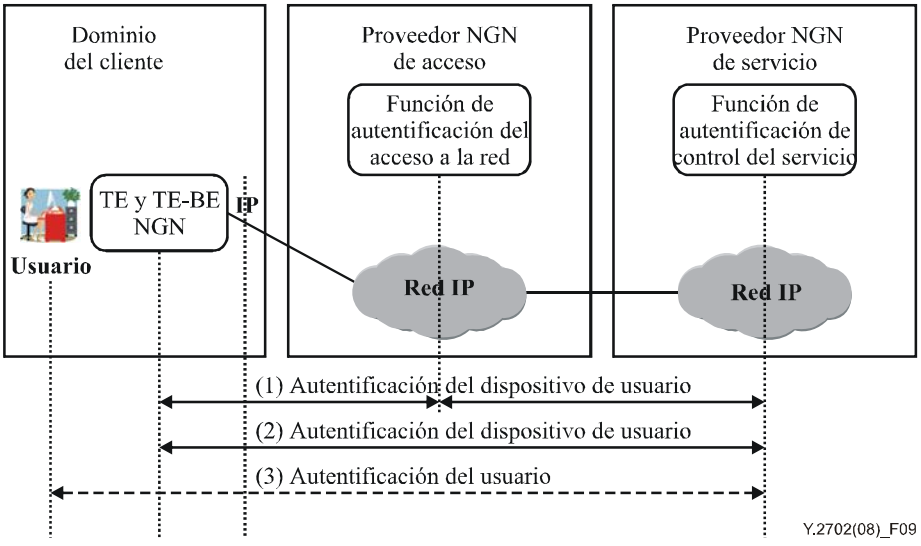


Figura 8 – Modelo de referencia para la autentificación y autorización de servicio/aplicación

La Figura 8 contiene ejemplos de relaciones para la autentificación/autorización de servicio/aplicación en un entorno hipotético de proveedor de múltiples redes:

1) Este flujo de información representa al proveedor NGN de servicio dependiendo del proveedor NGN de acceso para la autentificación de un dispositivo de usuario mediante relaciones de confianza.

2) Este flujo de información representa la autentificación y la autorización de un dispositivo de usuario por parte del proveedor NGN de servicio. Este caso exigiría que el dispositivo del usuario tuviese capacidades especiales de identificación (por ejemplo, SIM).

3) Este flujo de información representa la autentificación del usuario por el proveedor NGN de servicio (por ejemplo, el usuario se registra e indica una palabra clave o PIN).

8.2 Requisitos

8.2.1 Requisitos generales

A continuación se indican los requisitos generales respecto de la autentificación y la autorización del usuario por el proveedor NGN:

(R-23) – La NGN debe tener capacidades para identificar a un usuario, un dispositivo de usuario y una combinación de dispositivo de usuario y usuario a partir de la información sobre el perfil del usuario y el abono.

(R-24) – La NGN debe tener capacidades para autentificar y autorizar a un usuario, un dispositivo de usuario o una combinación de dispositivo de usuario y usuario a partir de la información sobre el perfil del usuario y el abono.

(R-25) – Los servicios de la NGN sólo se deben conceder a un usuario, un dispositivo de usuario o una combinación de dispositivo de usuario y usuario autorizados.

(R-26) – La NGN debe tener capacidades para verificar y autorizar los privilegios de un usuario (por ejemplo, permitiendo que el usuario realice ciertas acciones inequívocamente si su función o privilegio está autorizado).

(R-27) – En una configuración de múltiples redes, cada uno de los dominios administrativos (por ejemplo, proveedor NGN de acceso, proveedor NGN visitado y proveedor NGN contratado) debe observar las políticas (por ejemplo, los SLA) inherentes a la identificación, la autentificación y la autorización de un usuario, un dispositivo de usuario o una combinación de dispositivo de usuario y usuario.

(R-28) – La NGN debe tener capacidades para ofrecer confidencialidad y protección de la integridad durante los intercambios de mensajes e información utilizados para la autentificación y autorización de un usuario, un dispositivo de usuario y una combinación de dispositivo de usuario y usuario.

(R-29) – La NGN debe tener capacidades para proteger la información sobre autentificación y autorización contra el acceso no autorizado, la manipulación o la corrupción del servicio (por ejemplo, información sobre el perfil del usuario y el abono).

(R-30) – La NGN debe tener capacidades para proteger las funciones y capacidades de autentificación y autorización contra ataques al servicio (por ejemplo, la retransmisión de mensajes y la denegación de servicio).

(R-31) – Es preciso tener capacidades para agrupar la autentificación del dispositivo de usuario dependiente de la tecnología de la red de acceso con la autentificación del usuario a tenor de la política del proveedor NGN.

(R-32) – La NGN debe ser capaz de detectar y registrar los intentos de acceso no autorizado a los servicios o recursos NGN (por ejemplo, se puede fijar un umbral configurable para un número de intentos no autorizado por encima del cual se generará una alarma, que se registrará y señalará al sistema de gestión).

(R-33) – La NGN debe ser capaz de detectar y registrar intentos de acceso no autorizados (por ejemplo, acciones de usuario no autorizadas).

8.2.2 Compartición de los resultados de la autentificación para la IdM

El proveedor NGN puede necesitar intercambiar resultados de la autentificación entre diferentes servicios y/o aplicaciones dentro de su red y a nivel externo con otros proveedores NGN para facilitar los servicios de gestión de identidades (IdM). Esto podría incluir asertos y demás información pertinente para la IdM, entre las que cabe citar las siguientes:

a) política de confianza;

b) método de autentificación e información utilizados para la autentificación (por ejemplo, claves de autentificación);

c) niveles de garantía;

d) información sobre gestión de privilegios (por ejemplo, privilegios asignados o validados).

Las capacidades para un intercambio seguro de información sobre los resultados de la autentificación (por ejemplo, asertos) y demás información conexa, según se indicó *supra*, permitirá a los proveedores NGN diseñar plataformas de servicio/aplicación con características de autentificación y autorización eficaces y de fácil utilización para el usuario. Por ejemplo, la información sobre los resultados de la autentificación puede compartirse entre los sistemas (por ejemplo, servidores de aplicación) que ofrecen diferentes servicios y/o aplicaciones para que el proveedor NGN pueda ofrecer prestaciones y capacidades "de inicio de sesión unificado" para comodidad del usuario. En el intercambio y la compartición de los resultados de la autentificación dentro de la red de un proveedor NGN deben cumplirse los siguientes requisitos:

(R-34) – La NGN debe tener capacidades para permitir que los sistemas y los elementos de red (por ejemplo, servidores de aplicación) ofrezcan diferentes servicios y/o aplicaciones para el intercambio y la compartición de la información sobre los resultados de la autentificación (por ejemplo, asertos, información sobre gestión de privilegios, política de confianza y niveles de garantía) a tenor de la política de seguridad y el diseño específico de la plataforma de servicio/aplicación del proveedor NGN.

(R-35) – La comunicación entre los diferentes sistemas o elementos de red (por ejemplo, servidores de aplicación) para el intercambio o la compartición de información sobre los resultados de la autentificación debe protegerse contra el acceso no autorizado, la observación, la manipulación o la corrupción (por ejemplo, protección de confidencialidad y la integridad). Esto incluye la protección de cualesquiera informaciones almacenadas.

En un entorno de múltiples redes, los proveedores NGN podrían tener que intercambiar y compartir de una manera segura la información sobre los resultados de la autentificación con sujeción a los SLA. Para el intercambio y la compartición de los resultados de la autentificación entre diferentes proveedores NGN deben cumplirse con los siguientes requisitos:

(R-36) – Es preciso tener capacidades para que los proveedores NGN puedan intercambiar y compartir los resultados de la autentificación de una manera segura (es decir, a través de las interfaces NNI y ANI), de conformidad con las relaciones de confianza, las políticas y los SLA entre los proveedores NGN.

(R-37) – La comunicación entre los proveedores NGN para el intercambio y la compartición de información sobre los resultados de la autentificación (es decir, a través de las interfaces NNI y ANI) debe protegerse contra el acceso no autorizado, la observación, la manipulación o la corrupción (por ejemplo, protección de la confidencialidad y la integridad). Esto incluye la protección de cualesquiera informaciones almacenadas. Las prácticas y mecanismos de seguridad específicos estarán basados en las relaciones de confianza, las políticas y los SLA entre los proveedores NGN.

(R-38) – Se necesitan capacidades para comprobar el método de autentificación y divulgar información sobre el o los métodos que se utilizaron para autentificar entidades ante los terceros fiables, a saber:

- Método de verificación de la identidad del usuario.
- Método de autentificación (uso de certificados digitales, firmas, testigos de seguridad, datos biométricos, SIM, etc.).
- Política de confianza.
- Niveles de garantía de autentificación.

La compartición de la información y los resultados de la autentificación está sujeta a la observancia de las políticas pertinentes, tales como las legislaciones y reglamentaciones nacionales y regionales para la protección de Información Personalmente Identificable (Personally Identifiable Information, PII).

(R-39) – Es preciso que el proveedor NGN garantice la observancia de las políticas pertinentes, tales como las legislaciones y reglamentaciones nacionales y regionales para la protección de información personalmente identificable (PII). Ello incluye las políticas elaboradas sobre la base de los siguientes principios encaminados a la protección de datos básicos:

- Vinculación de los datos a una finalidad específica.
- No intercambiar datos entre aplicaciones para diferentes finalidades.
- Limitación de los datos al mínimo necesario para una finalidad específica.
- Derecho de las personas a ejercer control sobre su PII.

8.2.3 Autentificación y autorización del usuario por parte del proveedor NGN de servicio para el acceso a servicios/aplicaciones específicos

Los proveedores NGN tendrán que administrar los privilegios del usuario para su acceso (con inclusión de los privilegios y las funciones del usuario para realizar acciones) a servicios y aplicaciones específicos tales como:

- Servicios de transmisión vocal.
- Servicios de emisión de secuencias.
- Servicios de datos y mensajería.
- Servicio de telecomunicaciones de emergencia (ETS) y telecomunicaciones de socorro en casos de catástrofe (TDR).

Cada servicio puede tener sus propios requisitos en cuanto al nivel de garantías para validar la identidad y los privilegios de un usuario, el dispositivo de usuario o una combinación de dispositivo de usuario y usuario, en función de los riesgos inherentes a la probabilidad de que entidades no autorizadas obtengan acceso al recurso del servicio. El nivel de garantía necesario para la autentificación y validación de los privilegios de un usuario, un dispositivo de usuario o una combinación de dispositivo de usuario y usuario debe establecerse e implementarse para un servicio concreto, a tenor de la política de seguridad NGN. Ello entrañaría la admisión y utilización de diversos métodos de autentificación que varían desde los métodos de autentificación básicos, en los que se utilizan palabras claves y números de identificación personal (PIN), hasta métodos más rigurosos para los que se recurre a claves de autentificación, como por ejemplo:

a) Certificados digitales (por ejemplo, X.509 PKI).

b) Testigos de seguridad (testigos físicos y lógicos) y tarjetas inteligentes.

c) Datos sobre las características de comportamiento (por ejemplo, análisis mecanográfico).

d) Datos de identificación biométrica (por ejemplo, reconocimiento de la voz, identificación de huellas dactilares, iris o retina).

NOTA – La autentificación de una entidad no es una indicación de validación positiva de una persona.

Para la autentificación y la autorización también es preciso tener en cuenta la facilidad de utilización por parte del usuario. Este aspecto es muy pertinente en determinados tipos de servicios tales como ETS y TDR. Es conveniente que el procedimiento de autentificación resulte fácil de utilizar para el usuario. Para mayor información sobre ejemplos de autentificación y autorización ETS véase el apéndice II.

Al considerar la autentificación y autorización para un servicio específico se han de tener en cuenta los siguientes requisitos, además de los consignados en los párrafos 8.2.1 y 8.2.2:

(R-40) – Se debe disponer de métodos para la autentificación de credenciales, a tenor de la política del proveedor NGN. Es preciso admitir y utilizar métodos de autentificación de múltiples factores, según proceda, a tenor de la política del proveedor NGN en lo tocante a garantías de privilegios e identidad.

(R-41) – Debe ser posible identificar inequívocamente a todos los usuarios abonados a un servicio/aplicación, a tenor de la política del proveedor NGN. Esto incluye la identificación de un conjunto de usuarios finales cuyas identidades de usuario podrían no ser proporcionadas por el proveedor NGN[2].

(R-42) – A tenor de la política del proveedor NGN, debe ser posible vincular a cierto número de usuarios particulares al mismo abono.

(R-43) – Debe ser posible dirigirse a cada uno de los usuarios/abonados relacionados con un abono a un servicio/aplicación inequívoca con fines de comunicación.

(R-44) – A tenor de la política del proveedor NGN, el usuario final debe poder acceder a un servicio varias veces simultáneamente y/o desde múltiples dispositivos.

(R-45) – Debe ser posible admitir múltiples perfiles de abono para un usuario final en particular. Es preciso que dichos perfiles de abono múltiples sean identificables de manera exclusiva.

A tenor de la política del proveedor NGN, podría ser necesaria la autentificación periódica de un usuario para mayor garantía y seguridad.

(R-46) – A tenor de la política del proveedor NGN, debe ser posible volver a autentificar al usuario periódicamente (por ejemplo, usuario final, objeto o elemento de red) a lo largo de una transacción o sesión de comunicación establecida.

9 Autentificación y autorización de los proveedores NGN por parte del usuario

En este párrafo se estipulan los requisitos para que el usuario autentifique y autorice a la red (por ejemplo, la autentificación por el usuario de la identidad de la red NGN conectada o del proveedor de servicio).

[2] Un punto extremo incorporado tendrá dos o más usuarios incorporados, cuya identidad podría conocer inequívocamente el punto extremo y no el proveedor NGN.

9.1 Descripción

La arquitectura NGN permite a los usuarios finales obtener servicios de múltiples proveedores NGN. Además, el proveedor NGN de transporte (por ejemplo, el proveedor NGN de acceso) puede ser diferente del proveedor NGN de servicio. Como resultado de ello, los usuarios finales podrían tener que verificar las identidades de los proveedores NGN (por ejemplo, proveedores de acceso, de transporte y de servicio). Concretamente, se necesitan:

- Capacidades para que un usuario final pueda identificar, autentificar y autorizar al proveedor NGN de acceso para la conectividad a la red (por ejemplo, el acceso a la red).
- Capacidades para que un usuario final pueda identificar, autentificar y autorizar a un proveedor NGN de servicio.

9.2 Objetivos y requisitos

9.2.1 Autentificación del proveedor NGN por parte del usuario para el acoplamiento a la red

Los puntos de acceso a la red en los que están conectados los TE y TE-BE NGN deben tener capacidades para que el usuario pueda identificar, autentificar y autorizar el acoplamiento a la red.

(R-47) – Los puntos de acceso a la red (NAP) en los que están conectados los TE y TE-BE NGN (es decir, la conectividad IP directa) tendrán capacidades para que el usuario final pueda identificar al proveedor NGN para el acoplamiento y la conectividad, si así lo exige la política de seguridad.

(R-48) – Los puntos de acceso a la red (NAP) en los que están conectados los TE y TE-BE NGN (es decir, la conectividad IP directa) tendrán capacidades para que el usuario pueda autentificar y autorizar al proveedor NGN para el acoplamiento y la conectividad, si así lo exige la política de seguridad. Estas funciones pueden ofrecerse como parte de la función general de control del acoplamiento a la red (NACF) definida en [UIT-T Y.2012].

(R-49) – En un entorno de redes múltiples, cada uno de los dominios administrativos (es decir, proveedor de acceso a la red, proveedor NGN visitado y proveedor NGN contratado) debe hacer cumplir las políticas (por ejemplo, relaciones de confianza) relativas a la identificación, la autentificación y la autorización del acoplamiento a la red (por ejemplo, recurriendo a los SLA).

9.2.2 Autenticación del proveedor NGN por parte del usuario para la obtención del servicio

Se pueden ofrecer capacidades para que el usuario final pueda autentificar y autorizar a un proveedor NGN con el fin de obtener servicios NGN.

(R-50) – La NGN tendrá capacidades para permitir que el usuario final identifique inequívocamente al proveedor NGN que ofrece un servicio o un conjunto de servicios, si así lo exige la política de seguridad.

(R-51) – La NGN tendrá capacidades para permitir que el usuario final autentifique y autorice al proveedor NGN que ofrece un servicio o un conjunto de servicios, si así lo exige la política de seguridad.

10 Autentificación y autorización entre usuarios homólogos con el apoyo del proveedor NGN

Este párrafo tiene carácter informativo y se incluye en aras de la integridad.

Las comunicaciones entre homólogos son transparentes para el proveedor NGN, ya que el tráfico atraviesa su red inequívocamente a nivel de la capa de transporte. Cabe señalar que un proveedor NGN podría desempeñar la función de un IdP que ofrece servicios IdM (por ejemplo, capacidades de autentificación entre homólogos) para estas situaciones hipotéticas de comunicación.

11 Autentificación y autorización mutua de red

11.1 Descripción

Para atenuar los riesgos de un acceso no autorizado se necesita autentificación y autorización mutua. Se necesitan asimismo servicios de autentificación y autorización del acceso a red para verificar las identidades y determinar si se debe conceder acceso a la capa de transporte de la red y/o acceso a servicios y capacidades. El acceso a la red puede tener lugar en las interfaces NNI o ANI.

En la Figura 9 se ilustra el modelo de referencia para una autentificación y autorización mutua de red con los siguientes dominios de seguridad:

1) Dominio de red de acceso: Red de acceso acogida por un proveedor de red de acceso (por ejemplo, banda estrecha, xDSL y cable). El proveedor de red de acceso puede o no ser el mismo que el proveedor NGN. Las relaciones de confianza entre el proveedor de red de acceso y el proveedor NGN están regidas por los acuerdos sobre nivel de servicio (SLA).
2) Dominio NGN visitado: NGN acogida por un proveedor de red visitada. Ofrece funciones de red visitada a otro proveedor de red NGN (es decir, al proveedor de red contratada). Las relaciones de confianza están regidas por los acuerdos sobre nivel de servicio (SLA). La red visitada puede ofrecer servicios NGN y tener sus propios abonados. Además, la red visitada puede haber concertado acuerdos con un tercer proveedor de servicio/aplicación. Además, la red visitada puede establecer una interfaz con la red contratada a través de una red de tránsito, y sus relaciones de confianza estarán regidas por los SLA.
3) Dominio de red contratada: NGN acogida por un proveedor de red contratada. La red contratada ofrece servicios NGN a sus abonados. Además, la red contratada puede haber concertado un acuerdo con un tercer proveedor de servicio/aplicación a través de una ANI. Las relaciones de confianza entre los proveedores de red visitada y de red contratada, con inclusión de cualquier otro tercer proveedor, están regidas por los acuerdos sobre nivel de servicio (SLA). Además, la red contratada puede establecer una interfaz con una red visitada u otra red por medio de una red de tránsito, y las relaciones de confianza estarán gobernadas por los SLA.
4) Dominio de red de tránsito: La NGN proporciona inequívocamente servicios de transporte. Las relaciones de confianza entre la red de transporte y las redes adyacentes, con inclusión de cualquier tercer proveedor, están regidas por los acuerdos sobre nivel de servicio (SLA).
5) Otros dominios de red: Puede tratarse de un proveedor NGN o de un proveedor no NGN. Las relaciones de confianza están regidas por los acuerdos sobre nivel de servicio (SLA).

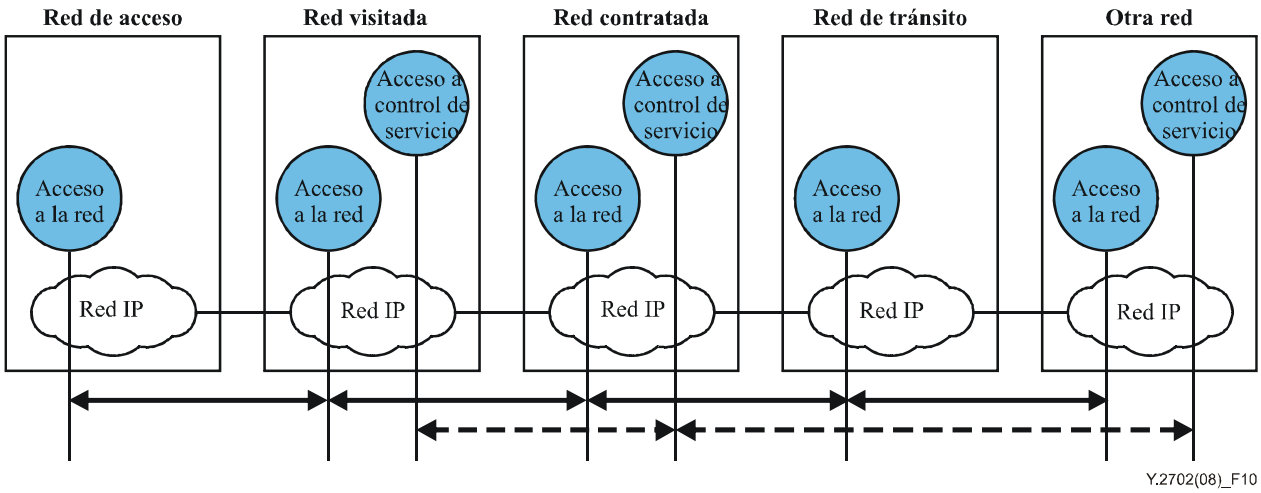


Figura 9 – Autentificación mutua de red

11.1.1 Autentificación de nivel de transporte

Según se ilustra en la Figura 9, la autentificación del nivel de transporte se efectúa en cada tramo, de modo que la autentificación siempre tiene lugar con la red adyacente en la capa de transporte. Ello significa que la red contratada no tiene por qué haber concertado forzosamente un acuerdo SLA con la otra red que se indica en la figura, sino más bien que la relación a nivel de transporte tiene lugar entre la red contratada y la red de tránsito y luego entre la red de tránsito y la otra red.

11.1.2 Autentificación a nivel de servicio/aplicación

Según se ilustra en la Figura 9, la autentificación a nivel de servicio/aplicación tiene lugar directamente entre los estratos de control de servicio de la red visitada, la red contratada y otras redes, a un nivel de servicio/aplicación de par a par. Esta relación de par a par no es física sino lógica. El trayecto físico es vertical desde el control de servicio hasta el acceso a la red en una red, luego se transporta directamente o por conducto de una red de tránsito, y después verticalmente desde la red hasta el acceso al control del servicio en la red homóloga de servicio/aplicación.

11.2 Requisitos para la autentificación mutua de red

(R-52) – La NGN debe tener capacidades para identificar las redes adyacentes en el estrato de transporte.

(R-53) – La NGN debe tener capacidades para autentificar y autorizar el acceso desde las redes adyacentes en el estrato de transporte.

(R-54) – La NGN debe tener capacidades para identificar las redes adyacentes en el estrato de servicio/aplicación.

(R-55) – La NGN debe tener capacidades para autentificar y autorizar el acceso desde redes adyacentes en el estrato de servicio/aplicación.

(R-56) – Cada uno de los proveedores NGN debe hacer cumplir las políticas relativas a la identificación, autentificación y autorización mutua de red (por ejemplo, recurriendo a los SLA y a las relaciones de confianza).

(R-57) – Para la comunicación entre redes debe ser posible identificar a los elementos de red involucrados, mediante la correlación de los identificadores de elementos de red con los identificadores relacionados con el proveedor NGN interconectado.

(R-58) – La NGN debe tener capacidades para proteger la información sobre autentificación y autorización mutua de red contra el acceso no autorizado, la manipulación y la corrupción.

(R-59) – La NGN debe tener capacidades para proteger las funciones y capacidades de autentificación y autorización mutua de red contra ataques (por ejemplo, retransmisión de mensajes y denegación de servicio).

(R-60) – La NGN debe poder detectar y registrar los intentos de acceso no autorizado desde otras redes (por ejemplo, se podría fijar un umbral configurable para el número de intentos de acceso no autorizado por encima del cual se activa una alarma, se procede al registro y se da cuenta de ello al sistema de gestión).

A tenor de la política del proveedor NGN, para mayor garantía y seguridad podría ser necesario proceder a la autentificación periódica de un proveedor NGN adyacente.

(R-61) – A tenor de la política del proveedor NGN, debe ser posible volver a autentificar periódicamente al proveedor NGN de interconexión mientras dura la transacción o sesión de comunicación establecida.

12 Autentificación y autorización de un tercer proveedor de servicio/aplicación por parte del proveedor NGN

12.1 Descripción

Podría darse el caso de que el proveedor de una aplicación o servicio sea diferente del proveedor NGN (es decir, un tercer proveedor de servicio/aplicación). En tal caso hipotético, el proveedor NGN tendría que autentificar y autorizar al tercer proveedor de servicio/aplicación, según se ilustra en la Figura 10.

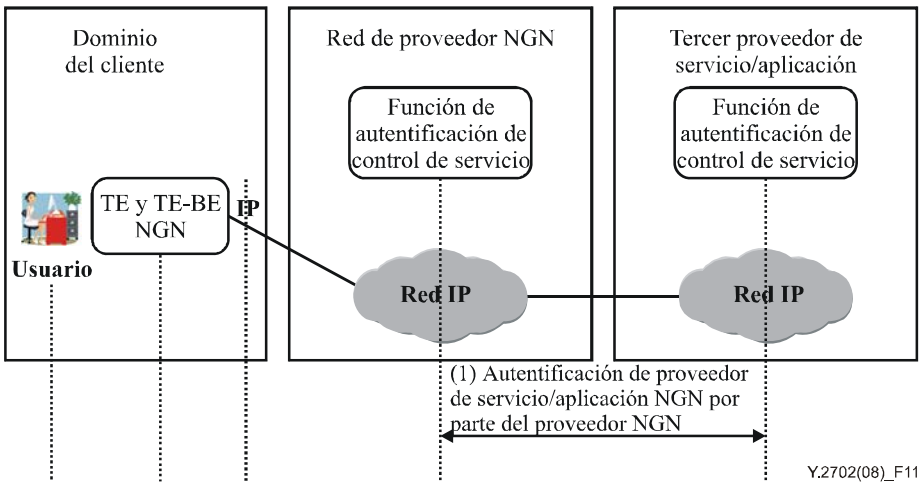


Figura 10 – Autentificación y autorización del tercer proveedor de servicio/aplicación

Cabe señalar que las autentificaciones de red y de usuario descritas en los párrafos anteriores tienen lugar aunque no se indiquen en la Figura 10 y en el texto que figura a continuación.

12.2 Requisitos

(R-62) – Un tercer proveedor de servicio/aplicación debe tener capacidades para identificarse a sí mismo ante un proveedor de servicio NGN.

(R-63) – Un tercer proveedor de servicio/aplicación debe tener capacidades para identificarse a sí mismo ante un usuario.

(R-64) – La NGN debe tener capacidades para identificar inequívocamente a terceros proveedores de servicio/aplicación.

(R-65) – La NGN debe tener capacidades para autentificar y autorizar a terceros proveedores de servicio/aplicación.

(R-66) – El proveedor NGN y los terceros proveedores de servicio/aplicación deben hacer cumplir las políticas relativas a la identificación, autentificación y autorización (por ejemplo, recurriendo a los SLA y a las relaciones de confianza).

(R-67) – La NGN y los terceros proveedores de servicio/aplicación deben tener capacidades para proteger la información sobre autentificación y autorización contra el acceso no autorizado, la manipulación y la corrupción.

(R-68) – La NGN y el tercer proveedor de servicio/aplicación deben tener capacidades para proteger las funciones y capacidades de autentificación y de autorización contra ataques (por ejemplo, retransmisión de mensajes y denegación de servicio).

(R-69) – La NGN debe ser capaz de detectar y registrar los intentos de acceso no autorizado por parte de terceros proveedores de servicio/aplicación (por ejemplo, se podría fijar un umbral configurable para el número máximo de intentos de acceso no autorizado por encima del cual se activará una alarma, se procederá al registro y se dará cuenta al sistema de gestión).

A tenor de la política del proveedor NGN, para mayor garantía y seguridad podría ser necesario proceder a una autentificación periódica del tercer proveedor de servicio/aplicación.

(R-70) – A tenor de la política del proveedor NGN, se debe poder volver a autentificar periódicamente al tercer proveedor de servicio/aplicación mientras dura la transacción o sesión de comunicación establecida.

13 Utilización del servicio de autentificación y autorización por terceros proveedores

13.1 Descripción

Los terceros proveedores del servicio de autentificación y autorización pueden ofrecer:

- la autentificación del usuario a un proveedor de servicio;
- la autentificación del proveedor de servicio a un usuario;
- la autentificación entre proveedores de servicio; y
- la autentificación de un proveedor de servicio/aplicación por un usuario o un proveedor de servicio.

A este respecto, cuando se recurra a un tercer proveedor de servicio de autentificación participarán por lo menos tres entidades. Además del tercer proveedor del servicio de autentificación que desempeña funciones de servicio de autentificación en respuesta a una solicitud, éste debe autentificarse a sí mismo ante el solicitante y el solicitado.

13.2 Requisitos

Se deben cumplir los requisitos estipulados en el párrafo 12.2.

14 Autentificación y autorización de objetos

14.1 Descripción

Además de autentificar y autorizar usuarios, dispositivos de usuario y proveedores de servicio, es necesario autentificar objetos en general, lo que incluye objetos físicos tales como sistemas o elementos de red, y objetos virtuales tales como:

- aplicaciones;
- procesos de aplicación;

- programas informáticos;
- contenidos de datos y mensajes de señalización, gestión y portadores.

14.2 Requisitos

(R-71) – La NGN debe tener capacidades para identificar inequívocamente objetos, a tenor de la política del proveedor NGN.

(R-72) – La NGN debe tener capacidades para autentificar y autorizar objetos, a tenor de la política del proveedor NGN.

(R-73) – La NGN debe tener capacidades para verificar y autorizar los privilegios de un objeto (por ejemplo, autorizar al objeto a realizar una acción o participar en un proceso inequívocamente si su función o privilegio está autorizado).

(R-74) – El proveedor NGN debe hacer cumplir las políticas inherentes a la identificación, autentificación y autorización de objetos.

(R-75) – La NGN debe tener capacidades para proteger la confidencialidad y la integridad de los mensajes y la información intercambiados con fines de autentificación y autorización de objetos.

(R-76) – La NGN debe tener capacidades para proteger la información sobre autentificación y autorización de objetos contra el acceso no autorizado, la manipulación y la corrupción.

(R-77) – La NGN debe tener capacidades para proteger las funciones y capacidades de autentificación y autorización de objetos contra ataques (por ejemplo, retransmisión de mensajes y denegación de servicio).

(R-78) – La NGN debe ser capaz de detectar y registrar los intentos de acceso no autorizado de objetos (por ejemplo, se podría fijar un umbral configurable para el número máximo de intentos de acceso no autorizado por encima del cual se generará una alarma, se procederá al registro y se dará cuenta de ello al sistema de gestión).

(R-79) – La NGN debe ser capaz de detectar y registrar los intentos de usar privilegios que no estén autorizados (por ejemplo, acciones de usuario no autorizado).

A tenor de la política del proveedor NGN, para mayor seguridad y garantía podría ser necesario proceder a la autentificación periódica de un proveedor NGN adyacente.

(R-80) – A tenor de la política del proveedor NGN, debe ser posible volver a autentificar periódicamente al objeto asociado mientras dura la transacción o sesión de comunicación establecida.

Apéndice I

Caso de utilización de SAML

(Este apéndice no es una parte integrante de la presente Recomendación)

I.1 Utilización de la Recomendación [b-UIT-T X.1141], Lenguaje de marcas de asertos de seguridad (SAML 2.0)

Este apéndice contiene ejemplos de transmisión de los resultados de la autentificación y promueve al mismo tiempo la privacidad en cuanto a la utilización de SAML para la autentificación de un servicio/aplicación.

I.2 Procedimientos de autentificación de servicio/aplicación

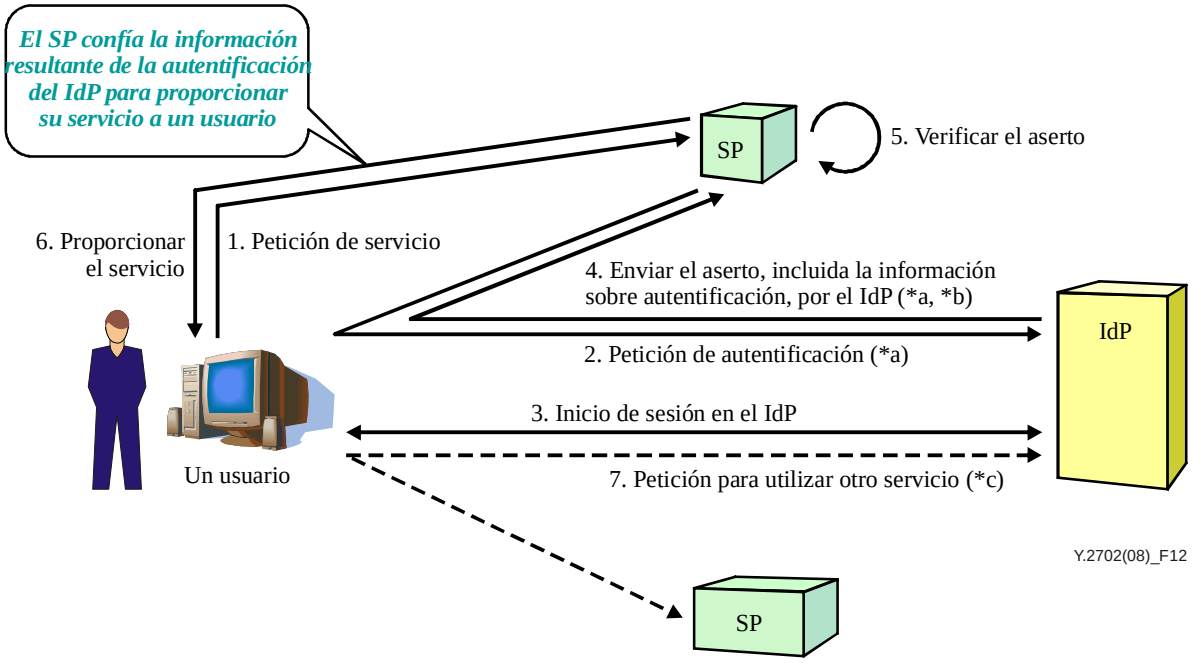
Cuando es preciso intercambiar los resultados de la autentificación entre los servicios y/o aplicaciones fiables que pueden ser de un tercer proveedor, se puede utilizar el lenguaje de marcas de asertos de seguridad (SAML 2.0). El SAML 2.0 es una especificación abierta normalizada por la Organización para el Progreso de las Normas sobre la Información Estructurada (OASIS). El SAML se puede utilizar concretamente para los siguientes casos:

– Inicio de sesión unificado: cuando diferentes servicios y aplicaciones permiten que sus usuarios procedan al inicio de sesión unificado para su propia conveniencia, sin intercambiar entre ellos toda la información de usuario.

– Federación de cuentas: cuando diferentes servicios y aplicaciones vinculan sus cuentas para el mismo usuario.

I.3 Autentificación de servicio/aplicación – Ejemplos de flujo de llamada

La Figura I.1 contiene un ejemplo típico de inicio de sesión unificado con federación utilizando SAML 2.0.



(*a) 2 y 4 son comunicaciones efectuadas (por ejemplo, HTTP-redirect) por medio de un agente del usuario (por ejemplo, el navegador web).

(*b) Según las necesidades, el aserto puede contener información sobre atributos y una decisión relativa a la autorización.

(*c) El mismo flujo que de 1. a 6., con exclusión del registro ante el IdP. (En otras palabras, el usuario sólo debe iniciar la sesión en el IdP una sola vez para ser autentificado.)

Figura I.1 – Ejemplo de flujo de llamada SSO utilizando SAML 2.0

En [b-UIT-T X.1141] se definen los términos indicados en la Figura I.1 como sigue:

- Proveedor de identidad (IdP)

  Un tipo de proveedor de identidad que crea, mantiene y administra información de identidad para los principales y proporciona la autentificación del principal a otros proveedores de servicio dentro de una federación, como con los perfiles del navegador web.

- Proveedor de servicio

  Función asumida por una entidad del sistema cuando dicha entidad proporciona servicios a los principales o a otras entidades del sistema.

- Aserto

  Una pieza de datos producida por una autoridad SAML en relación ya sea con un acto de autentificación realizado en un sujeto, la información de atributos respecto del sujeto, o datos sobre autorización aplicables al sujeto con respecto a un recurso dado.

I.4 Seguridad de los procedimientos y mecanismos de autentificación de servicio/aplicación

El propio SAML 2.0 posee características tales como una federación anónima y seudónimos para proteger la seguridad, así como la privacidad. La federación anónima proporciona un nameID transitorio al proveedor de servicio. Los seudónimos permiten identificar a los usuarios ante un proveedor de servicio durante el inicio de sesión unificado utilizando seudónimos de tipo par que preservan la privacidad y permiten mantener al mismo tiempo una relación persistente con el usuario. SAML 2.0 también permite encriptar declaraciones de atributos, identificadores de nombres o asertos completos. Esta característica permite asegurarse de que se protege la confidencialidad de estos elementos de extremo a extremo, según las necesidades.

Apéndice II

Autentificación y autorización ETS

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

II.1 Panorama general

Numerosos países disponen de un servicio de telecomunicaciones de emergencia (*emergency telecommunications service*, ETS) o lo están desarrollando. La implementación del ETS es, por definición, un asunto de carácter nacional. No obstante, las catástrofes/emergencias pueden trascender las fronteras geográficas y por consiguiente existe la posibilidad de que los países/administraciones concierten acuerdos bilaterales y/o multilaterales para conectar sus respectivos sistemas ETS. [b-UIT-T E.107] contiene orientación para permitir las telecomunicaciones entre una implementación nacional del ETS (ENI) y otra u otras ENI.

Los proveedores NGN deben autorizar el acceso inequívocamente a los usuarios del ETS autorizados. Se debe evitar el acceso no autorizado, como por ejemplo el de intrusos haciéndose pasar por usuarios autorizados. Por lo tanto, en aras de la seguridad del ETS, es importante disponer de mecanismos y capacidades para autentificar y autorizar el acceso del usuario, el dispositivo de usuario o una combinación de usuario y dispositivo de usuario ETS, según proceda, en cumplimiento de la política pertinente[3] y con el nivel de seguridad correspondiente al servicio específico (por ejemplo, transmisión de voz, datos, vídeo).

En la interconexión entre implementaciones nacionales ETS, los proveedores NGN tendrán que confiar entre sí para la autentificación y autorización de los usuarios ETS en el marco de acuerdos sobre nivel de servicio. Hay múltiples métodos para la autentificación y la autorización ETS. En este apéndice se proporciona información sobre algunos métodos para la autentificación y autorización ETS, con inclusión de algunos ejemplos de flujos de llamadas.

II.2 Autentificación y autorización del usuario ETS

La manera de autentificar y autorizar a los usuarios ETS es un asunto de carácter nacional. Por lo general, un proveedor NGN autentifica y autoriza una petición de llamada/sesión ETS de un usuario aplicando el método de inscripción/registro y según la manera de invocar al servicio. La autentificación puede efectuarse por llamada/sesión, puede ser una autentificación de una sola vez (por tiempo limitado) aplicable al acceso actual del usuario ETS, o bien se puede realizar mediante abono. Los proveedores NGN deben acelerar la autentificación de usuarios de telecomunicaciones de emergencia autorizados en una fase temprana del proceso de establecimiento de la llamada/sesión. Se utilizarán métodos y mecanismos específicos para la autentificación y autorización a tenor de la política aplicable (por ejemplo, uso de un número de identificación personal (PIN) y el perfil de usuario/abono). Una vez que se autentifica y autoriza al usuario, al dispositivo del usuario o a una combinación de usuario y dispositivo del usuario a tenor de la política aplicable, la llamada/sesión ETS se marca e indica en el sentido hacia adelante a las redes subsiguientes, y facultativamente se indica también el nivel de prioridad del usuario ETS. Además, una vez autentificada y autorizada, se le asigna prioridad a todos los aspectos de la llamada/sesión ETS, la señalización/el control, el tráfico portador y cualquier tipo de gestión aplicable.

---

[3] NOTA – En este contexto la política incluye todas las políticas aplicables, tales como las normas y reglamentos del gobierno y el organismo regulador y la política del proveedor NGN.

Entre los métodos para la autentificación y autorización del ETS cabe citar los siguientes:

a) Utilización de un número de identificación personal (PIN): Conforme a este método se usa un PIN para autentificar y autorizar al usuario. Con este método identificamos al usuario pero no al dispositivo del usuario, y por lo tanto se utiliza normalmente en los casos en los que el usuario está autorizado para invocar el servicio ETS desde cualquier dispositivo.

b) Utilización del perfil del servicio/abono: De conformidad con este método, se proporciona el perfil de servicio terminal del usuario para indicar el abono ETS. Se autentifica el terminal del usuario y se identifica el perfil de servicio del usuario como parte del procedimiento de registro normal del proveedor NGN (es decir, el proveedor ETS). Cuando el usuario inicia una petición, al cotejarlo con el perfil del servicio del usuario se determina si éste está autorizado o no para el ETS. Si el abono ETS se valida para el terminal del usuario, entonces se accede a la petición ETS.

c) Uso de una combinación de PIN y perfil del usuario: También se pueden utilizar métodos que combinan el empleo de PIN y el perfil del servicio para autentificar tanto al usuario como al dispositivo del usuario con el fin de ofrecer un mayor nivel de seguridad.

d) Utilización de testigos de seguridad especiales y biométrica: Además de los métodos antes descritos, existen otros métodos más complejos que utilizan testigos de seguridad especiales y capacidades de biométrica para autentificar y autorizar a los usuarios ETS y ofrecer un nivel más alto de seguridad respecto de la identidad.

II.3 Autentificación y autorización del proveedor NGN para el ETS

También es preciso considerar la autentificación y autorización para la transmisión y recepción del tráfico ETS entre proveedores NGN, tomando en consideración un entorno de múltiples proveedores y una separación entre el transporte y el control del servicio. La autentificación y autorización de los proveedores NGN para la transmisión y recepción de tráfico y las llamadas/sesiones ETS en el marco de los SLA y a tenor de la política aplicable también es importante con fines de seguridad ETS.

II.4 Ejemplos de casos de autentificación y autorización ETS

II.4.1 Ejemplo de un caso de autentificación y autorización básicas utilizando PIN

En la Figura II.1 se ilustra un caso de autentificación y autorización básica ETS utilizando un número de identificación personal (PIN).

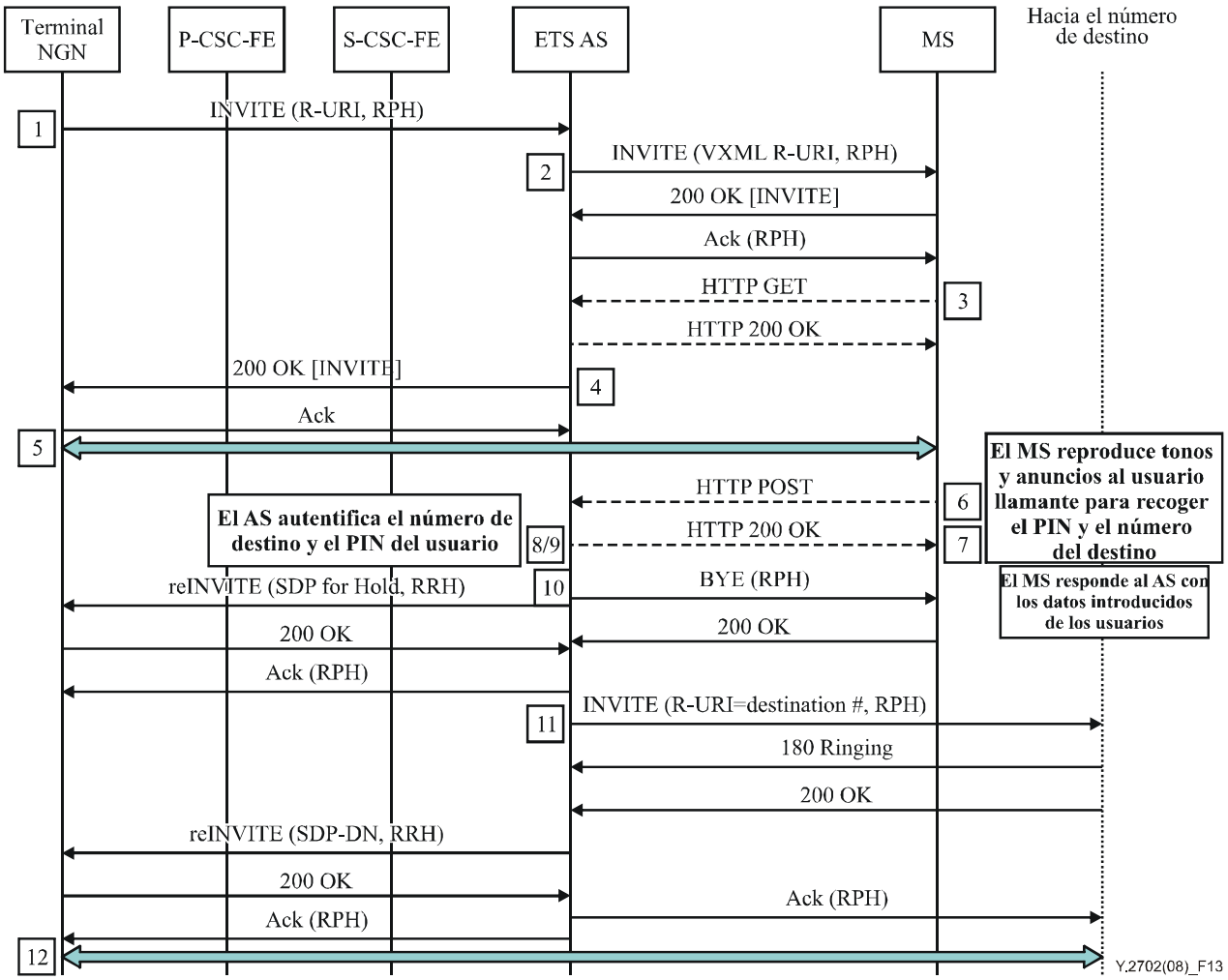


Figura II.1 – Autentificación y autorización con PIN

En este ejemplo se supone que el usuario ETS solicita/invoca la llamada/sesión ETS haciendo una solicitud de llamada/sesión a un número ETS. Además, todas las solicitudes SIP contienen un encabezamiento de prioridad de recursos (RPH) [b-IETF RFC 4412] para indicar que es preciso conferir un trato prioritario.

1) La llamada/sesión se encamina a un servidor de aplicaciones (AS) ETS en donde se inicia el proceso de autentificación.

2) El AS ETS envía un mensaje INVITE al servidor de medios (MS) seleccionado, con una oferta SDP relacionada con el llamante. El mensaje INVITE contiene el URL de un guión VoiceXML, almacenado en el AS ETS. En el guión se describe cómo debería interactuar el MS con el llamante (qué anuncios mostrar, cómo recoger los dígitos, cuántos dígitos recoger, temporizadores entre dígitos, etc.).

3) Al recibir el mensaje INVITE, el MS:

- puede enviar un 100 Trying al AS ETS;
- recupera el guión VoiceXML directamente del AS ETS utilizando el HTTP y el URL en el mensaje INVITE. (El MS envía un HTTP GET al AS y el guión VoiceXML se devuelve del AS ETS en un HTTP 200 OK);
- valida el guión;
- formula y envía un mensaje 200 OK que contiene su propio SDP al AS ETS.

4) El AS ETS envía un mensaje 200 OK a la parte llamante (terminal NGN), incluyendo en dicho mensaje la información sobre sesión que recibió del MS.

5) A esta altura la conexión de medios está disponible entre el MS y la parte llamante.

6) Al recibir el mensaje ACK y el guión VXML en el HTTP 200 OK, el MS ejecuta el guión VoiceXML. Éste reproduce un tono y recoge los dígitos (PIN) ingresados por la parte llamante.

7) Luego el MS envía los dígitos recogidos directamente al AS ETS utilizando un mensaje HTTP POST.

8) Al recibir los dígitos compilados, el AS ETS verifica si los dígitos recibidos (PIN) son válidos.

- Si los dígitos recibidos no son válidos (número de dígitos recibidos o número erróneo), el AS ETS determina que es necesario proseguir la interacción con el llamante. El AS ETS devuelve un mensaje HTTP 200 OK al MS con un nuevo guión VoiceXML. El AS ETS emitirá instrucciones para el tratamiento final.
- Si los dígitos recibidos son válidos, el AS ETS encomendará al MS que reproduzca el anuncio para recoger los dígitos (número de destino).

9) El AS ETS determina que los dígitos de destino ingresados por la parte llamante son válidos.

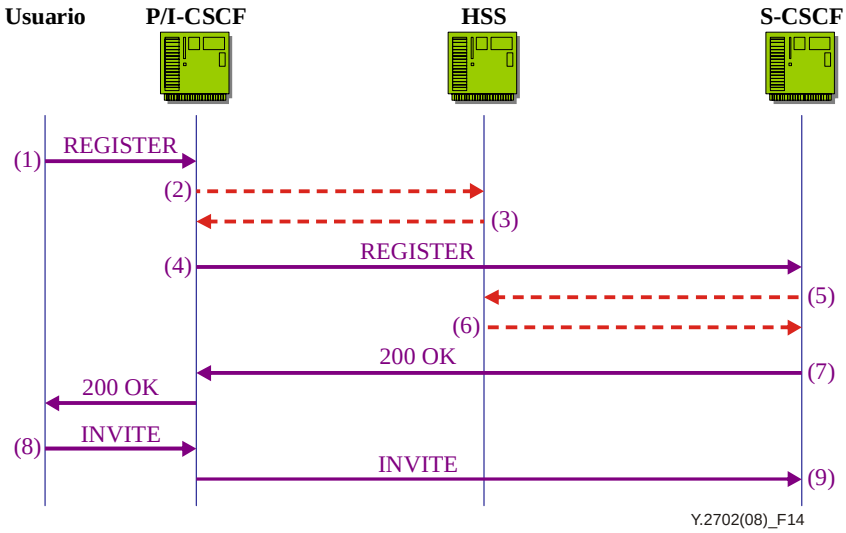
10) El AS ETS libera el MS de la llamada/sesión con un SIP BYE, y envía un mensaje reINVITE a la parte llamante, con un SDP para poner los medios en espera.

11) El AS ETS envía un mensaje INVITE hacia la parte de destino. Al recibir el mensaje 200 OK (respuesta), el AS ETS envía un reINVITE con el SDP correspondiente al destino hacia la parte llamante.

12) Se establece un trayecto de medios entre la parte llamante y el número de destino, con el AS ETS de autentificación incluido en el trayecto de control de llamada.

II.4.2 Ejemplo de caso de autentificación y autorización utilizando el perfil de servicio/abono

En la Figura II.2 se ilustra un caso en el cual se utiliza el perfil de servicio/abono para la autentificación y autorización ETS.



NOTA – Para mayor simplicidad, no se indican todos los intercambios de mensajes.

Figura II.2 – Ejemplo utilizando el abono

En este ejemplo se utiliza el perfil de servicio/abono relacionado con el dispositivo de usuario. La red efectúa el procedimiento habitual de registro y autentificación del dispositivo de usuario. Cuando el usuario invoca una llamada/sesión ETS, el perfil de servicio/abono se verifica para determinar si el dispositivo de usuario está autorizado o no para la llamada/sesión ETS. Los flujos de llamada son los siguientes:

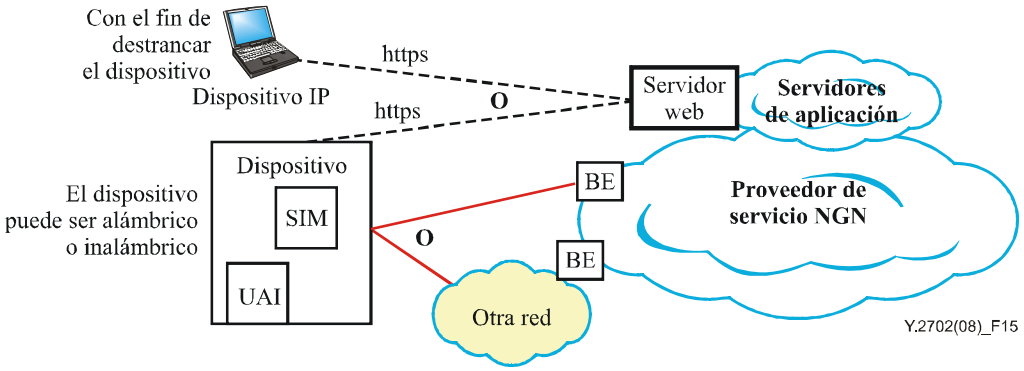
1) Inicio del registro
2) P/I-CSCF consulta al HSS
3) El HSS verifica el abono de usuario y proporciona la identidad de S-CSCF
4) P/I-CSCF envía el mensaje de registro a S-CSCF
5) S-CSCF consulta HSS
6) HSS proporciona información sobre el perfil de servicio del usuario (esto podría entrañar la interacción con AS)
7) S-CSCF envía 200 OK
8) El usuario inicia la sesión ETS
9) S-CSCF verifica el perfil de servicio para determinar si la sesión ETS está o no autorizada.

II.4.3 Ejemplo de autentificación y autorización de una combinación de usuario y dispositivo de usuario

En la Figura II.3 se muestra un ejemplo en el que se utiliza un dispositivo de usuario con una tarjeta SIM que se acopla a la red con autentificación de inicialización genérica (GBA) normalizada 3GPP.

En este ejemplo, el dispositivo tiene una interfaz de autentificación de usuario (UAI), que permite al usuario proporcionar información de autentificación por medio del dispositivo a la capa de aplicación en la red de proveedores de servicio. La UAI puede ser tan simple como un teclado o tan complicada como las capacidades biométricas.

Se supone que existen comunicaciones seguras para la señalización y los medios



AS – Servidor de aplicación (*application server*)
CSCF – Función de control de la sesión de llamada (*call session control function*)
HSS – Sistema de abonado residencial (*home subscriber server*)
IBCF – Función de control limítrofe de interconexión (*interconnect border control function*)
I-BGF – Función de pasarela limítrofe de interconexión (*interconnect border gateway function*)
I-CSCF – CSCF de interrogación (*interrogating CSCF*)
IMS – Subsistema de multimedios IP (*IP multimedia subsystem*)
MGCF – Función de control de pasarela de medios (*media gateway control function*)
MGCP – Protocolo de control de pasarela de medios (*media gateway control protocol*)
MRFC – Controlador de función de recursos de medios (*media resource function controller*)
MS – Servidor de medios (*media server*)
NAT – Traducción de dirección de red (*network address translation*)
P-CSCF – CSCF de intermediario (*proxy CSCF*)
S/BC – Controlador limítrofe de sesión (*session border controller*)
S-CSCF – Función de control de la sesión de llamada de servicio (*serving call session control function*)
SGBE – Elemento limítrofe de pasarela de señalización (*signaling gateway border element*)
SIM – Módulo de identificación de abonado (*subscriber identification module*)
UAI – Interfaz usuario-autentificación (user authentication interface)
USIM – SIM universal (*universal SIM*)

Figura II.3 – Autentificación y autorización del usuario ETS

Flujo de llamada/sesión:

1) El dispositivo del usuario está encendido.

2) El dispositivo se acopla de una manera segura a la red utilizando 3GPP GBA.

3) El usuario ETS inicia la autentificación local con el SIM en el dispositivo utilizando la UAI. La UAI puede ser un teclado, en el cual se introduce el PIN, o algún tipo de capacidad biométrica.

   a) El SIM autentifica al usuario ETS y proporciona un indicador de éxito. El SIM informa al servidor de aplicación ETS que el usuario ETS ha sido autentificado.

   b) De otro modo, la información podría retransmitirse de una manera segura a la capa de aplicación en la red del proveedor de servicio.

4) En este momento se autentifican en la red el dispositivo de usuario y el usuario "normales". El usuario que desempeña la función de usuario ETS ha sido autentificado por el AS del ETS.

Si después de *x* intentos el usuario no obtiene la autentificación local, entonces dicho usuario debe bloquearse en el dispositivo. Un método posible para desbloquear el dispositivo es que el usuario acceda a GUI a través de la interfaz AS/WS e ingrese un PIN para la validación. Si se valida la identidad del usuario, la AS/WS enviará un mensaje al dispositivo ordenándole que se desbloquee.

II.4.4 Ejemplo de utilización en los locales de una empresa

Las llamadas ETS pueden tener su origen o terminar en los locales de una empresa pública, en cuyo caso por lo general:

- Se trata de instalaciones especializadas de los locales del gobierno y el proveedor de servicio.
- El usuario se registra con el local de la empresa y no con el proveedor de servicio.

- El local de la empresa se registra con un comodín o una IWF (por ejemplo, SBC) en el borde de la red del proveedor de servicio, de modo que efectúa un registro sustituto en nombre de la empresa.

Así pues, si se desea obtener una autentificación más completa que la autentificación basada en el PIN, habrá que realizar funciones adicionales, de las que cabe citar, entre otras, las siguientes:

- La empresa divulga la presencia del usuario al proveedor de servicio. Estos datos aumentarán la garantía de la autentificación.
- Se recurre a un testigo seguro de la empresa al proveedor de servicio para identificar esto como una posible llamada/sesión ETS en la capa 2/3 (por ejemplo, extensión del testigo seguro en RSVP).

Según el usuario, se necesitará garantía de autentificación con datos procedentes de múltiples fuentes.

Apéndice III

3GPP Arquitectura de inicialización genérica

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

La arquitectura de inicialización genérica (GBA) especifica un procedimiento de inicialización independiente del acceso. Constituye un marco para la autentificación mutua entre los usuarios finales y la función de aplicación de red (NAF).

La GBA es un sistema de autentificación que consta de tres partes:

- El usuario final que trata de obtener servicios de red a través del equipo de usuario (UE).
- El servidor de aplicaciones (denominado función de aplicaciones de red o NAF).
- Una entidad fiable (denominada función de servidor de inicialización o BSF), que participa en la autentificación y el intercambio de claves entre las dos entidades.

Los fundamentos del proceso de autentificación GBA se ilustran en el modelo de referencia y se describen a continuación.

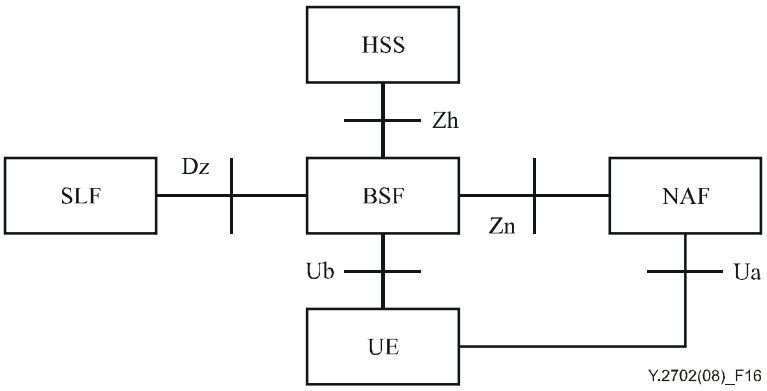


Figura III.1 – Modelo sencillo de red para la inicialización con arreglo a la norma [b-ETSI TS 133 220]

El procedimiento GBA consiste en tres etapas básicas:

1) La NAF solicita la autentificación y negocia que se utilice la GBA a través del punto de referencia Ua.

2) El cliente BSF que se ejecuta en el UE inicia el procedimiento de inicialización a través del punto de referencia Ub. La BSF busca información de autentificación y la configuración de seguridad del usuario GBA que figura en el HSS a través de Zh. El UE y BSF se autentifican mutuamente mediante HTTP Digest AKA. Como resultado de este procedimiento, el UE recibe el identificador de transacción de inicialización (B-TID) de la BSF y crea una clave compartida (Ks) entre el UE y la BSF.

3) El UE calcula Ks_NAF a partir de Ks y envía B-TID (junto con los datos específicos de la aplicación) a la NAF.

4) La NAF envía B-TID a la BSF a través del punto de referencia Zn.

5) Basándose en B-TID, la BSF determina el Ks que debe utilizar, calcula Ks_NAF a partir de éste y envía Ks_NAF a la NAF.

6) Por último, el UE y la NAF pueden autentificarse entre sí mediante la clave compartida Ks_NAF. El procedimiento de autentificación exacto depende del protocolo entre el UE y la NAF. Por ejemplo, la GBA especifica que las aplicaciones basadas en HTTP pueden utilizar la autentificación HTTP Digest]b-IETF RFC 2617] o el juego de claves precompartidas TLS [b-IETF RFC 4279].

NOTA – La BSF consulta a la SLF a través del punto de referencia Dz con el fin de obtener el nombre del HSS en el que figuran los datos específicos del abonado. La SLF no es necesaria cuando la BSF está configurada para utilizar un HSS predefinido.

La correspondencia de las entidades GBA con las entidades NGN especificada en la [UIT-T Y.2012]:

- NAF – corresponde a la entidad *aplicaciones* de la Figura 3 de la [UIT-T Y.2012].
- BSF – puede incluirse en la FE de autentificación y autorización T-11. Es decir, T-11 puede aumentarse y activarse con las capacidades del servidor BSF.
- HSS corresponde a la FE del perfil de usuario del servicio S-5.
- SLF corresponde a la FE de localizador de abonado S-4.
- UE corresponde a la función de usuario final.

Apéndice IV

Ejemplos de flujo de llamada para la gestión de identidades (IdM)

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

IV.1 Descripción general

Los ejemplos de flujos que se muestran en el presente apéndice proceden de [b-TR 33.980]

Estos flujos muestran en detalle los posibles métodos de interfuncionamiento entre el lenguaje de marcas de asertos de seguridad v2.0, SAML v2.0 (o bien el marco de federación de identidades de Liberty Alliance, ID-FF), el marco de servicios web de identidades (ID-WSF), el lenguaje de marcas de asertos de seguridad (SAML) y un componente de GAA denominado arquitectura de inicialización genérica (GBA). El presente apéndice tiene carácter informativo y sólo se aplica en caso de que se utilicen conjuntamente ID-WSF y GBA o SAML v2.0 y GBA.

IV.2 Ejemplos de flujos de llamada

Estos flujos sólo se aplican en caso de que se utilicen en conjunto Liberty Alliance y GBA o SAML v2.0 y GBA.

IV.2.1 Caso SSO: ID-FF con transferencia <lib:AuthnResponse>

IV.2.1.1 HTTPS con TLS convencional

En este caso el UE no conoce el protocolo de acceso al enlace (LAP). Todos los elementos del protocolo se toman del marco de federación de [b-ID-FF] y se complementan con información específica de GAA indicada en [b-TS 33.222]. En primer lugar se describen los pasos necesarios cuando se utiliza HTTPS con TLS convencional [b-IETF RFC 2246] con arreglo a la cláusula 5.3 de [b-TS 33.222]:

1) El UE envía una petición HTTP al proveedor de servicios (SP) para obtener acceso a un servicio de éste. Esta petición contiene la indicación de que admite autentificación basada en GBA (véase paso 3), lo cual resulta necesario para el redireccionamiento de la petición con arreglo al paso 3.

2) Después de recibir la petición HTTP procedente del UE, el SP determina el proveedor de identidad y envía una respuesta HTTP "redirect" (redireccionamiento) con <lib:AuthnRequest> al UE. El mecanismo mediante el cual se obtiene la dirección del proveedor de identidad depende de la implementación y del proveedor de servicio.

3) El UE, por su parte, se pone en contacto con el IdP mediante el URL que figura en el campo Location del encabezamiento y el UE debe aceptar el URL de NAF/IdP con una petición HTTP que contiene la información <lib:AuthnRequest> [b-ID-FF bindings].

   El UE indica a NAF/IdP que admite la autentificación GBA, para lo cual añade una cadena constante en el encabezamiento HTTP "User-Agent" como un testigo producto conforme a lo especificado en la [b-IETF RFC 2616]. Esta cadena constante se configura con arreglo al paso 2 de la cláusula 5.3 de [b-TS 33.222].

   En caso de que exista una relación de seguridad inicializada entre el UE y el IdP, el UE y el IdP/NAF comparten las claves para proteger el punto de referencia Ua y el UE dispone de todos los datos necesarios para efectuar la autentificación HTTP Digest a partir de mensajes anteriores. En tal caso, el paso 3 se combina con la petición referida en el paso 5, y se omite el paso 4.

4) Como el IdP está coubicado con la NAF, la autentificación HTTP Digest se realiza conforme a [b-TS 33.222] y se envía al UE una respuesta HTTP con el campo de encabezamiento WWW-Authenticate y el estado Unauthorized. El método y la descripción de esta autentificación se definen en [b-TS 33.222] y no en [b-ID-FF].

   Si el UE no contiene una sesión de inicialización válida o la vigencia del material de clave no está lo suficientemente actualizado para el IdP, el UE ejecutará un nuevo procedimiento de inicialización con la BSF, lo cual es transparente para el SP.

5) El UE devuelve al IdP los datos de autorización, utilizando como nombre de usuario el B-TID y como contraseña Ks_(ext/int)_NAF. El UE puede incluir otros datos de usuario relativos al LAP.

   Si el IdP se encuentra coubicado con la NAF, el procedimiento es el descrito en [b-TS 33.222]. El USS puede contener información específica de Liberty.

6) Se procesa el <lib:AuthnRequest>. El IdP responde con <lib:AuthnResponse> en el campo URL de la respuesta HTTP redirect [b-ID-FF bindings]. El IdP puede añadir otros datos relativos a LAP.

7) El UE se pone de nuevo en contacto con el SP utilizando este URL y la petición HTTP con <lib:AuthnResponse>.

8) El SP responde con una respuesta HTTP.

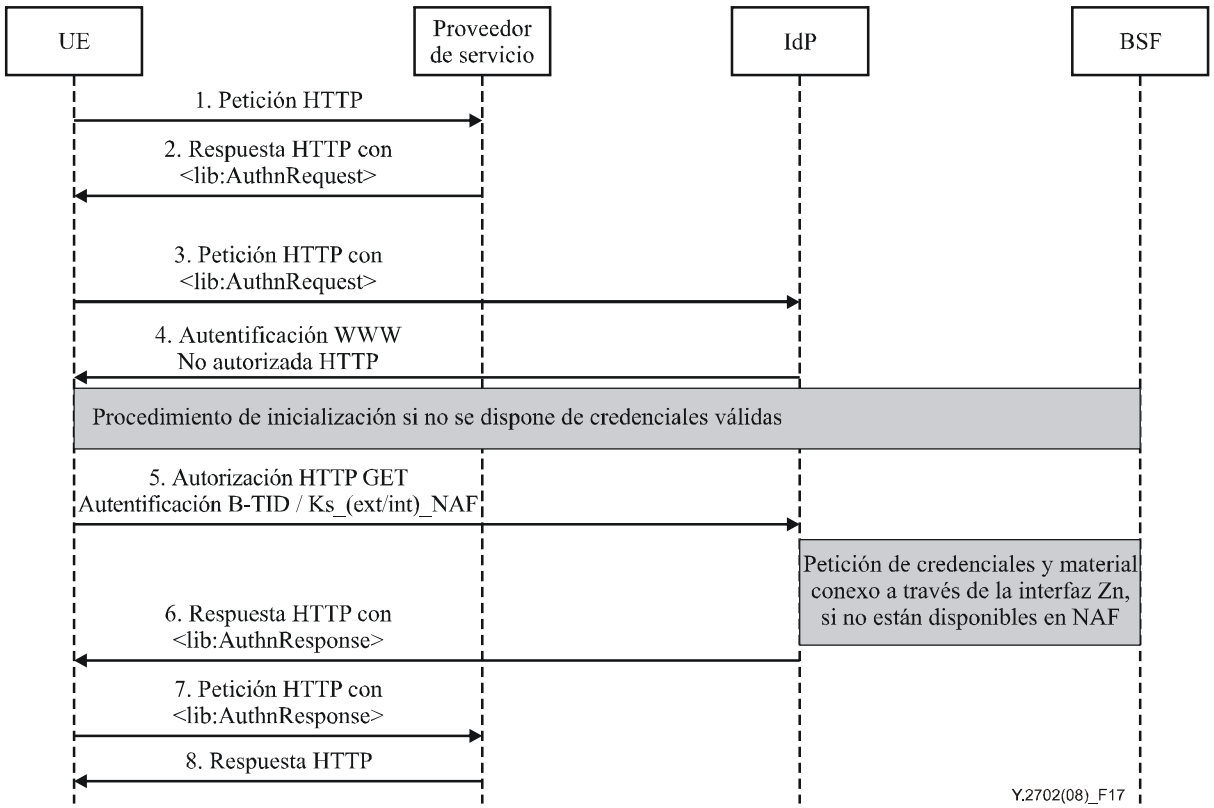


Figura IV.1 – Flujo de mensajes para SSO con <lib:AuthnResponse> y TLS convencional con GBA

NOTA 1 – Como el IdP está coubicado con la NAF, es decir, el Ua se selecciona para la autentificación según se describe en [b TS 33.222], cada petición a través del Ua se autoautentifica, dado que cada una transporta todo el encabezamiento de autorización. No hay diferencia entre la primera petición y las siguientes.

NOTA 2 – La especificación LAP ID-FF [b-ID-FF] define también una comunicación basada en POST entre el UE y el IdP aparte de la petición basada en GET con una cadena de consulta. Esto es conforme con [b TS 33.222], por cuanto especifica una petición HTTP sin indicar explícitamente un método para ello.

NOTA 3 – Para seleccionar la dirección adecuada del proveedor de identidad, el SP puede recurrir a la indicación recibida en el paso 1 de que admite a la autentificación GBA.

IV.2.1.2 HTTPS con PSK TLS

Al utilizar HTTPS con claves precompartidas (PSK) TLS conforme a la cláusula 5.4 de [b TS 33.222], se siguen los siguientes pasos:

1) El UE envía una petición HTTP al SP para obtener acceso a un servicio de éste. Esta petición contiene la indicación de que admite autentificación GBA (véase el paso 3 de la cláusula IV.2.1.1), dado que el IdP/NAF podría forzar al UE a utilizar TLS convencional aun cuando el UE invite a utilizar el PSK TLS.

2) Tras recibir la petición HTTP procedente del UE, el SP determina el proveedor de identidad y envía al UE una respuesta HTTP redirect con < lib:AuthnRequest> en el URL. El mecanismo mediante el cual se obtiene la dirección del proveedor de identidad depende de la implementación y del proveedor de servicio.

3) El UE comienza a establecer un túnel PSK TLS hacia el IdP/NAF, como se especifica en la cláusula 5.4 de [b TS 33.222], con el fin de prepararse para enviar la petición de redireccionamiento a IdP/NAF (véase paso 4). Al establecer el túnel TLS, el UE indica la posibilidad de utilizar PSK TLS, y el IdP/NAF puede seleccionar emplear PSK TLS con GBA.

   A partir del juego de cifras TLS seleccionado por IdP/NAF, el UE reconoce si IdP/NAF utilizará PSK TLS.

   En caso de que exista una relación de seguridad inicializada entre el UE y el IdP/NAF, el UE y el IdP/NAF comparten las claves para proteger el punto de referencia Ua. Así pues, el UE posee todos los datos necesarios para establecer el túnel PSK TLS de conformidad con [b TS 33.222] y el siguiente paso podrá darse inmediatamente sin ejecutar procedimiento de inicialización alguno.

   En caso de que no exista una relación de seguridad inicializada entre el UE y el IdP/NAF, pero el UE contenga una clave de inicialización válida Ks, el UE establece un túnel PSK TLS con el IdP/NAF basado en la correspondiente Ks_(ext)_NAF.

   Si el UE no contiene una sesión de inicialización válida o el material de claves no está lo suficientemente actualizado para IdP/NAF, el UE ejecutará un nuevo procedimiento de inicialización con la BSF, lo cual es transparente para el SP.

4) El UE accede al URL de IdP/NAF con la petición HTTP GET y con la información <lib:AuthnRequest> [b-ID-FF bindings] por el túnel PSK TLS establecido.

5) El IdP extrae la <lib:AuthnRequest>, la procesa, utiliza la autentificación del UE obtenida durante el establecimiento del túnel PSK TLS y envía al UE una respuesta HTTP redirect, mediante la cual se vuelve a redireccionar el UE hacia el SP. El URL puede contener un artefacto SAML o una <lib:AuthnResponse>.

6) El SP extrae y procesa el artefacto SAML o la <lib:AuthnResponse> y contesta con una respuesta HTTP.

7) El SP contesta con una respuesta HTTP.

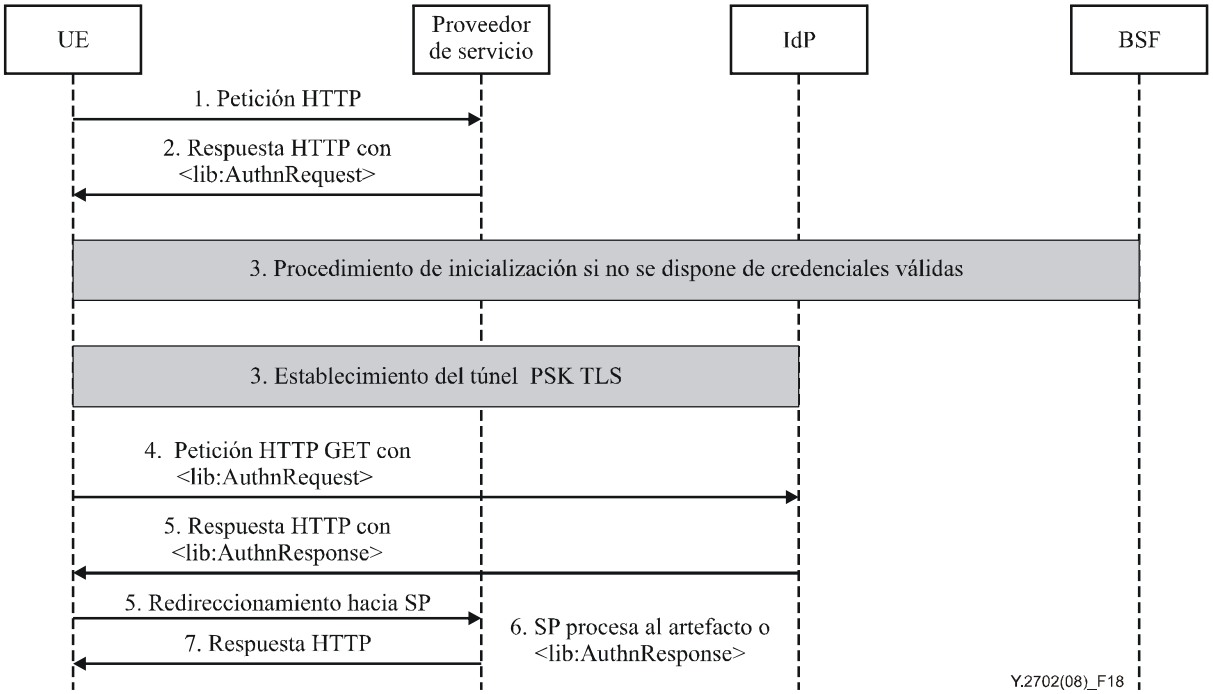


Figura IV.2 – Flujo de mensajes para SSO con <lib:AuthnResponse> y utilización de PSK TLS con GBA

NOTA – Las notas que figuran en la cláusula IV.2.1.1 son también aplicables a la utilización de PSK TLS descrita en la presente subcláusula.

IV.2.2 El caso de SSO: ID-FF con transferencia de artefactos

Este caso es similar al descrito en la cláusula IV.2.1, con la salvedad de que el proveedor de servicios puede ponerse en contacto directamente con el IdP.

NOTA – Dado que el flujo de mensajes es idéntico para la utilización de artefactos y <lib:AuthnResponse>, se aplican a la presente cláusula las mismas diferencias entre la utilización de TLS convencional y PSK TLS indicadas en la cláusula IV.2.1. Los flujos de mensaje que figuran en la presente cláusula corresponden al TLS convencional, aunque también es posible utilizar PSK TLS.

El IdP debe disponer de una interfaz adicional con el SP, que le permita a este SP recuperar el aserto de autentificación. Esta interfaz no es totalmente independiente de la GBA, ya que la información de autentificación puede incluir información relacionada con la GBA, por ejemplo la identidad de usuario, un seudónimo y otra información procedente de GUSS, restricciones basadas en la GBA, etc.

1) El UE envía una petición HTTP al SP para obtener acceso a un servicio de éste. Esta petición contiene la indicación de que admite autentificación basada en GBA (véase paso 3), lo cual es necesario para el redireccionamiento de la petición con arreglo al paso 3.

2) Tras recibir la petición HTTP procedente del UE, el SP determina el proveedor de identidad y envía al UE una respuesta HTTP redirect con < lib:AuthnRequest>. El mecanismo mediante el cual se obtiene la dirección del proveedor de identidad depende de la implementación y del proveedor de servicio.

3) El UE, por su parte, se pone en contacto con el IdP mediante el URL que figura en el campo Location del encabezamiento y el UE debe aceptar URL de NAF/IdP con una petición HTTP que contiene información <lib:AuthnRequest> [b-ID-FF bindings].

El UE indica a NAF/IdP que admite la autentificación GBA, para lo cual añade una cadena constante en el encabezamiento HTTP "User-Agent" como un testigo producto conforme a lo especificado en la [b-IETF RFC 2616]. Esta cadena constante se configura con arreglo al paso 2 de la cláusula 5.3 de [b-TS 33.222].

En caso de que exista una relación de seguridad inicializada entre el UE y el IdP/NAF, el UE y el IdP/NAF comparten las claves para proteger el punto de referencia Ua y el UE dispone de todos los datos necesarios para efectuar la autentificación HTTP Digest a partir de mensajes anteriores. En tal caso, el paso 3 se combina con la petición referida en el paso 5, y se omite el paso 4.

4) Si el UE aún no se ha autentificado ante el IdP, la autentificación ha de efectuarse en este momento, tal y como se define en [b-TS 33.222]. Liberty Alliance no define en [b-ID-FF] el método y la información necesaria para esta autentificación. El IdP envía una respuesta al UE HTTP con el estado Unauthorized (no autorizado), según se define en [b-TS 33.222].

   Si la NAF no dispone de material de claves válido y específico de NAF, o dicho material no está lo suficientemente actualizado para satisfacer a la NAF o el IdP, se habrá de realizar el procedimiento de inicialización definido en [b-TS 33.220], lo cual es transparente para el SP.

5) El UE responde con una petición HTTP GET cuyo campo de encabezamiento de autorización contiene como nombre de usuario el B-TID y como contraseña Ks_(ext/int)_NAF. El UE puede incluir otros datos de usuario relacionados con LAP.

   El IdP/NAF puede solicitar las credenciales y material conexo, en caso de que no las tenga almacenadas. El USS puede contener otra información específica de Liberty.

6) El IdP responde con un artefacto SAML en el campo URL de la respuesta HTTP redirect [b-ID-FF bindings]. El IdP puede incluir otros datos relacionados con LAP.

7) El UE se pone nuevamente en contacto con el SP a través de esta URL y envía una petición HTTP con el mismo artefacto SAML.

8) El SP envía una petición HTTP con el mismo artefacto SAML al IdP. La petición contiene un mensaje de petición SOAP <samlp:Request> destinado al punto extremo SOAP del proveedor de identidad, solicitándole el aserto, para lo cual le proporciona el artefacto de aserto SAML en el campo <samlp:AssertionArtefact> tal y como se especifica en [b-ID-FF bindings].

9) El IdP puede ahora construir o encontrar el aserto solicitado y responde con un mensaje de respuesta SOAP <samlp:Response> con el aserto <saml:Assertion> solicitado o un código de estado, según lo definido en [b-OASIS]. El IdP envía el aserto de autentificación que corresponde al artefacto.

10) El SP procesa el mensaje SOAP con el aserto <saml:Assertion> incluido en la respuesta <samlp:Response>, verifica la signatura del <saml:Assertion> y procesa el mensaje con arreglo a lo definido en [b-ID-FF bindings], y por último envía una respuesta HTTP.

La vida útil del aserto de autentificación SAML debe ser igual o inferior a la del B-TID.

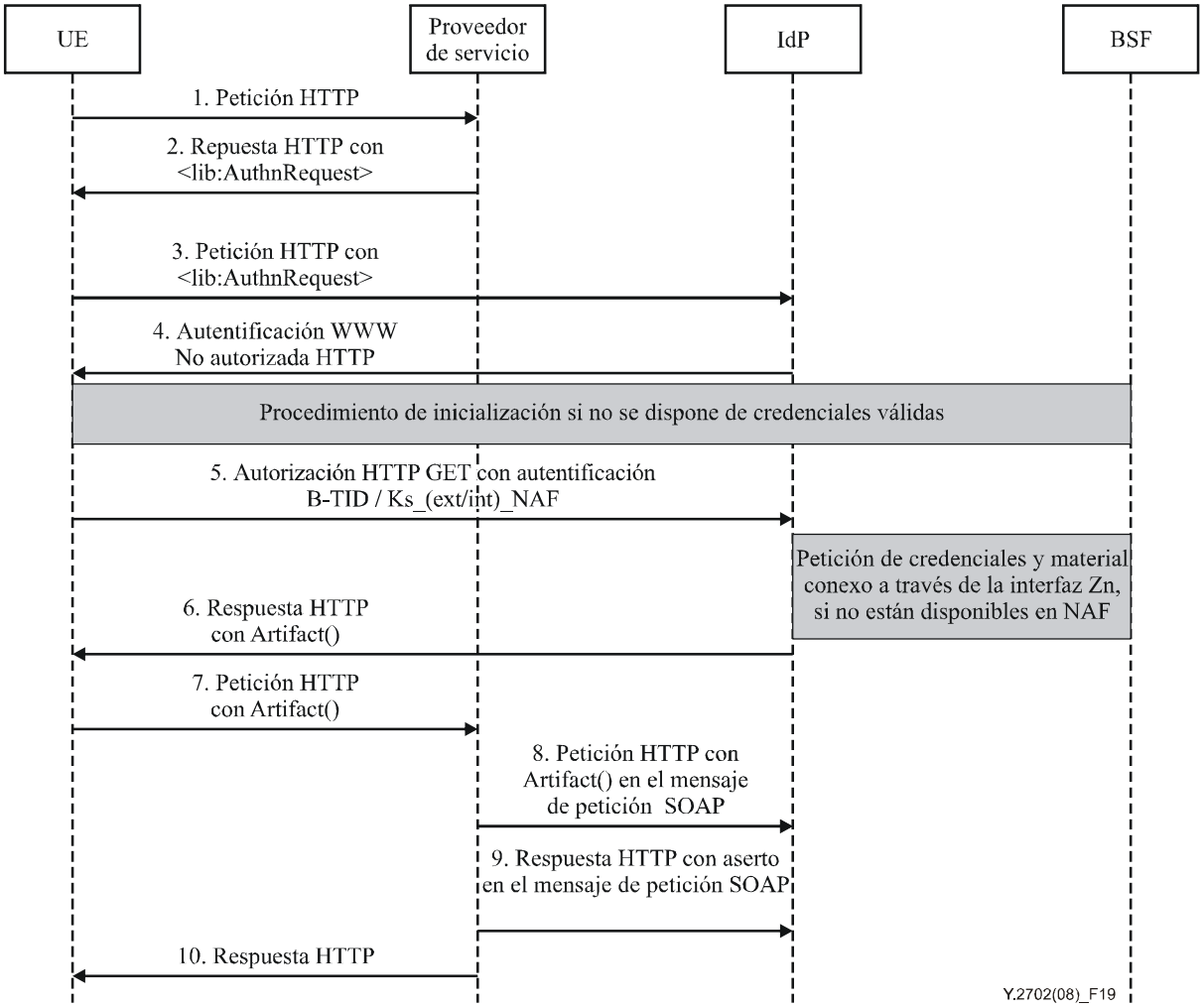


Figura IV.3 – Flujo de mensajes para SSO con transferencia de artefacto y utilización de GBA

IV.2.3 Caso SSO: servicio de autentificación ID-WSF

En este caso el UE tiene activado el LAP, es decir un LUAD (dispositivo o agente de usuario con capacidad Liberty, como se define en los perfiles ID-WSF de Liberty de la especificación de dispositivos y agentes de usuario con capacidad Liberty [b-ID-WSF profiles]). Los elementos del protocolo utilizados proceden del servicio de autentificación ID–WSF [b-ID-WSF service], y la interacción del UE con IdP consta de dos ejecuciones consecutivas del protocolo. El cliente LUAD activo se pone en contacto con el NAF/IdP antes de acceder al servicio que ofrece el SP.

1) El UE se autentifica ante el servicio de autentificación (AS) del IdP y obtiene un testigo de seguridad que le permite invocar ciertos servicios.

2) El UE llama al servicio de inicio de sesión unificado (SSOS) del IdP utilizando para ello el testigo de seguridad. En este paso el UE recibe el aserto de autentificación (información relativa a la autentificación y autorización) que tendrá que utilizar en el SP.

3) El UE presenta el aserto de autentificación al SP que se comporta como un WSP para el acceso al servicio web.

Si el WSP que ofrece el servicio web al usuario forma parte del dominio del operador IdP, el cliente LUAD también podrá contactar directamente al WSP gracias al testigo de seguridad. En este caso puede omitirse el contacto con el SSOS.

La integración de estos tres pasos con la GBA se realiza del modo siguiente:

– El primer paso se integra en la comunicación entre el usuario (LUAD) y el AS, conforme a lo especificado en el LAP [b-ID-WSF service]. El protocolo de autentificación está incorporado en el protocolo SASL. Si procede, el UE debe ejecutar el protocolo en Ub. Esto no se basa en los protocolos LAP [b-ID-WSF security], [b-ID-FF] o [b-ID-WSF service], sino en los protocolos GBA inequívocamente [b-TS 33.220].

– El segundo y tercer pasos son totalmente idénticos a lo definido en el LAP (sin conexión a la GBA). La única dependencia respecto al GBA es el contenido del aserto de autentificación SAML que depende, en parte, de los resultados del GBA (los parámetros del protocolo, por ejemplo, el tiempo de ejecución, y los parámetros específicos del usuario, por ejemplo los procedentes de USS).

A continuación figura el flujo de mensajes para el caso de SSO del servicio de autentificación ID-WSF con transferencia de respuesta. Este flujo también puede aplicarse cuando el SSOS ofrece además un servicio de autentificación ID-WSF, en cuyo caso el SSOS está coubicado en el AS.

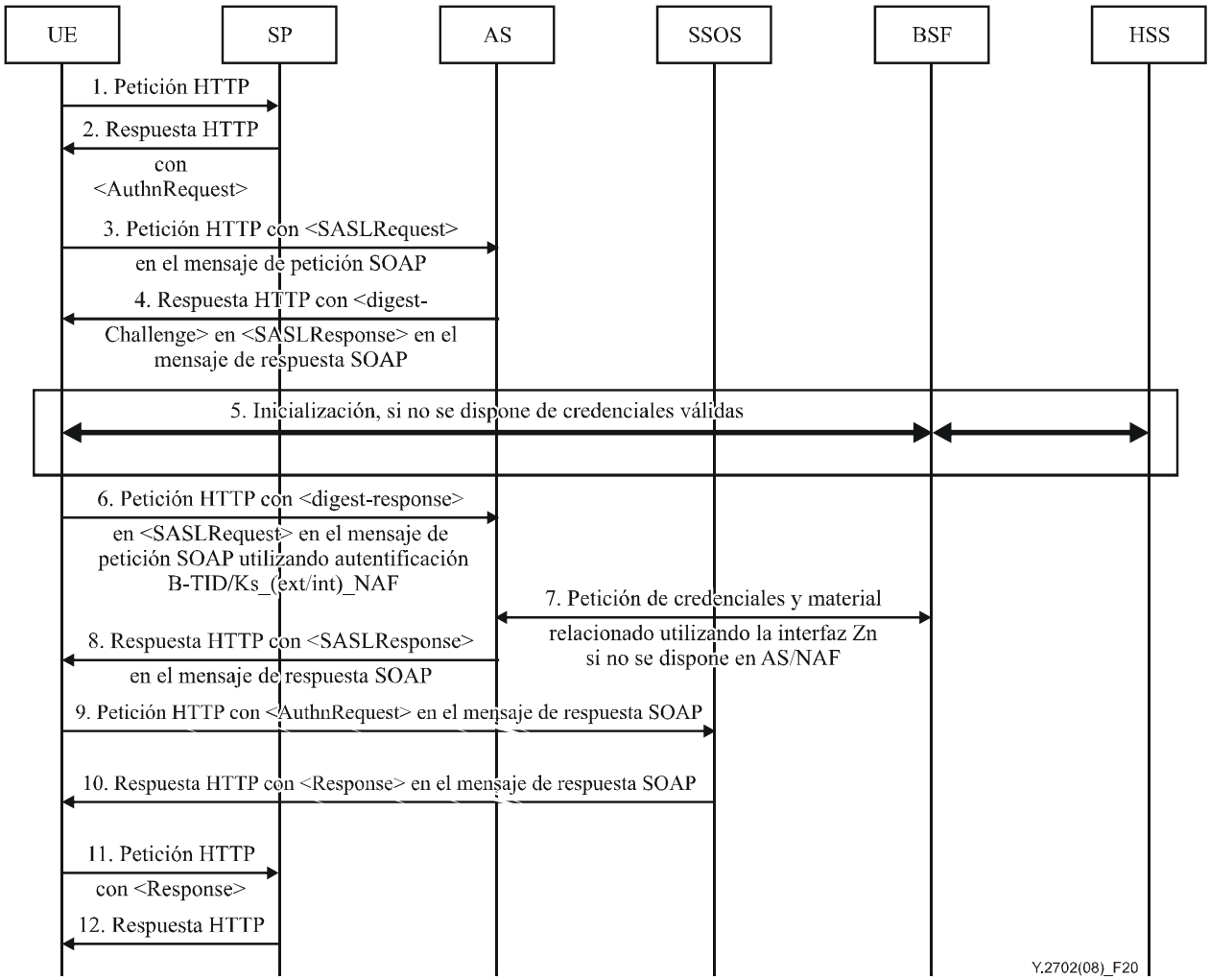


Figura IV.4 – Flujo de mensajes para ID-WSF AS y SSO con transferencia de respuesta y utilización de GBA

1) El UE envía una petición HTTP al SP para obtener acceso a un servicio de éste.

2) Tras recibir la petición HTTP procedente del UE, el SP obtiene la dirección del AS y envía al UE una respuesta HTTP redirect al UE. La respuesta HTTP puede contener o no un encabezamiento <lib:AuthnRequest> en función de la aplicación o el modelo de despliegue. El mecanismo mediante el cual se obtiene la dirección del AS depende de la implementación.

3) El UE (LUAD-WSC) envía una petición HTTP al AS, con un encabezamiento <SASLRequest> delimitado con arreglo a SOAP, cuyo parámetro "mechanism" contiene una lista de uno o varios nombres de los mecanismos que admite el cliente.

   El UE indicará al NAF/AS que puede utilizarse la autentificación GBA para lo cual añade una cadena constante en el encabezamiento HTTP "User-Agent" como un testigo producto conforme a lo especificado en la [b-IETF RFC 2616]. Esta cadena constante se configura con arreglo al paso 2 de la cláusula 5.3 de [b-TS 33.222].

   En caso de que exista una relación de seguridad inicializada entre el UE y NAF/AS, el UE y NAF/AS comparten las claves para proteger el punto de referencia Ua y el UE podrán proceder a la subsiguiente autentificación si el perfil SASL lo permite. En tal caso, el paso 3 se combina con la petición referida en el paso 6, y se omiten los pasos 4 y 5.

4) El AS envía una respuesta HTTP al UE, con un encabezamiento <SASLResponse> delimitado con arreglo a SOAP, cuyo parámetro "serverMechanism" contiene el nombre del mecanismo SASL seleccionado (por ejemplo, autentificación DIGEST) de la lista de mecanismos SASL que admite el cliente y, en este caso, el encabezamiento <SASLResponse> contiene además un parámetro <digest-challenge>. El método y la información de este parámetro son conformes a la [b-IETF RFC 2831].

5) Si el UE no contiene una sesión de inicialización válida o el material de claves no está lo suficientemente actualizado para el AS, el UE ejecutará un nuevo procedimiento de inicialización con la BSF y obtendrá una clave compartida Ks_(ext/int)_NAF, lo cual es transparente para el SP.

6) El UE vuelve a enviar una petición HTTP al AS, con un encabezamiento <SASLRequest> delimitado con arreglo a SOAP, cuyo parámetro "mechanism" contiene el mecanismo SASL que se le ha devuelto en el paso 4 y, en este caso, el encabezamiento <SASLRequest> contiene además un parámetro <digest-response>, en el que los datos de autorización se calculan utilizando el B-TID como nombre de usuario y la Ks_(ext/int)_NAF como contraseña. El método y la información de este parámetro son conformes a la [b-IETF RFC 2831]. El UE puede incluir otros datos de usuario relativos al LAP.

7) Como el AS se encuentra coubicado con la NAF, el AS solicita Ks_(ext/int)_NAF y otro material de claves a la BSF por medio de la interfaz Zn, si aún no dispone de esta información.

8) El AS procesa el parámetro <digest-response> del encabezamiento <SASLRequest> y luego envía una respuesta HTTP con un encabezamiento <SASLResponse> delimitado con arreglo a SOAP. El encabezamiento <SASLResponse> contiene un parámetro ID-WSF EPR (EndpointReference) que remite a la instancia SSOS y el tipo de servicio URI se configura con arreglo a [b-ID-WSF service] para determinar ID-WSF SSOS. El encabezamiento <SASLResponse> contiene además las credenciales necesarias para que el UE invoque al SSOS. El AS puede incluir otros datos relativos al LAP.

9) El UE envía una respuesta HTTP al SSOS, con un encabezamiento <samlp2:AuthnRequest> delimitado con arreglo a SOAP, cuyo atributo ProtocolBinding se configura de conformidad con [b-ID-WSF service] para determinar la vinculación del protocolo SAML que habrá de utilizarse. Esta petición incluye además un encabezamiento <wsse:security> con las credenciales que se han devuelto en el paso 8. El UE quizá tenga que construir él mismo el encabezamiento <samlp2:AuthnRequest> si no lo ha recibido en el paso 2, dependiendo del modelo de despliegue o la aplicación.

10) Se tramita la <samlp2:AuthnRequest>. El SSOS responde con un encabezamiento <samlp2: Response> en el URL de la respuesta HTTP redirect [b-ID-FF bindings]. El encabezamiento <samlp2: Response> contiene el parámetro <saml2:Assertion>. El SSOS puede incluir otros datos relativos al LAP.

11) El UE se pone nuevamente en contacto con el SP utilizando este URL y la petición HTTP con <samlp2: Response >.

12) El SP responde con una respuesta HTTP.

NOTA – Si el IdP está coubicado con el BSF, el primer paso puede integrarse en el punto de referencia Ub de la GBA [b-TS 24.109]. El segundo paso puede integrarse en la interfaz Ua del GBA.

Pese a que los dos protocolos presentan esta analogía de forma en lo que respecta a la ejecución de dos protocolos consecutivos, al parecer no es posible una simple correspondencia. La sintaxis y la semántica de los elementos de información que se transfieren en los protocolos GBA y LAP difieren considerablemente.

IV.2.4 Caso SSO: SAML v2.0 con transferencia de <samlp:Response>

IV.2.4.1 HTTPS con TLS

Este caso es similar al descrito en la cláusula IV.2.1.1 con la diferencia de que todos los elementos del protocolo se toman del [b-SAML v2.0] que integra el perfil SSO del navegador web [b-OASIS]. Por consiguiente, todos los pasos descritos en dicha cláusula son igualmente aplicables a ésta, sustituyendo <lib:AuthnRequest> por <samlp:AuthnRequest> y <lib:AuthnResponse> por <samlp:Response>. No se reproducen dichos pasos en esta cláusula, pero se incluye una versión adaptada de la Figura IV.1.

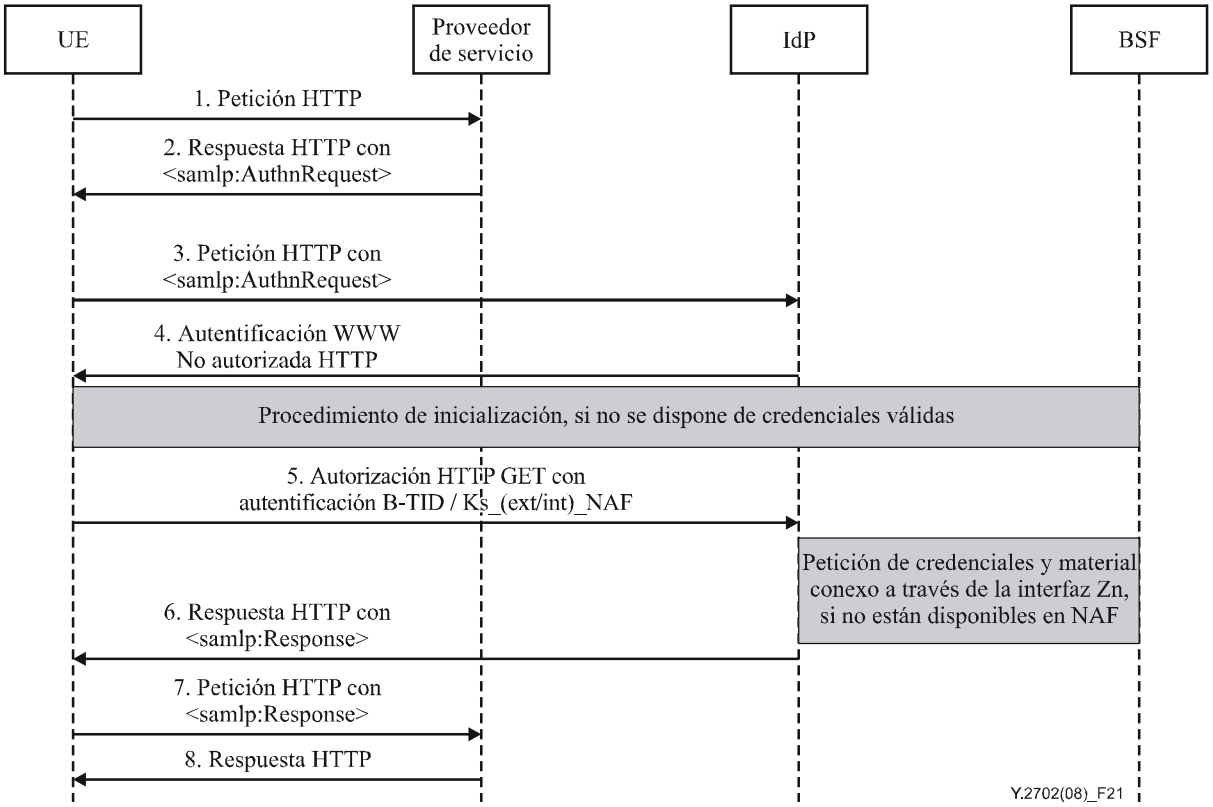


Figura IV.5 – Flujo de mensajes de SSO con <samlp:Response> y TLS con GBA

IV.2.4.2 HTTPS con PSK TLS

Este caso es similar al descrito en la cláusula IV.2.1.2 con la diferencia de que todos los elementos del protocolo se toman del SAML v2.0 [b-SAML v2.0] que integra el perfil SSO del navegador web [b-OASIS]. Por consiguiente, todos los pasos descritos en dicha cláusula son igualmente aplicables a ésta, sustituyendo <lib:AuthnRequest> por <samlp:AuthnRequest> y <lib:AuthnResponse> por <samlp:Response>. No se reproducen dichos pasos en esta cláusula, pero se incluye una versión adaptada de la Figura IV.2.

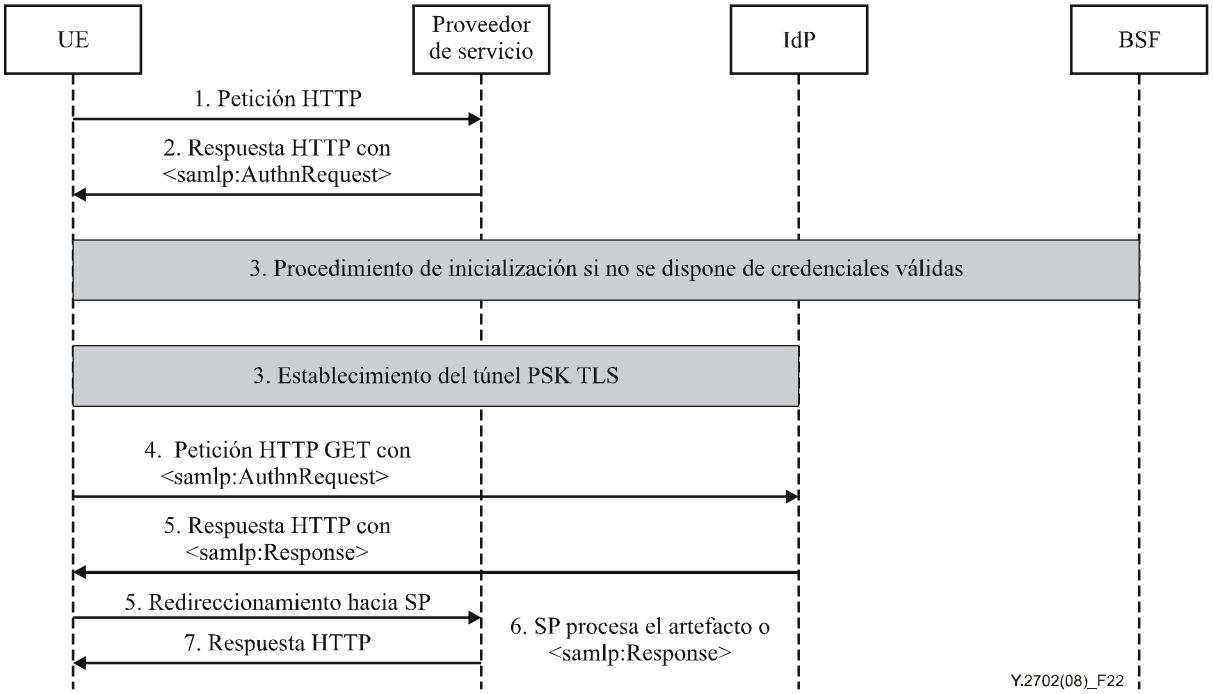


Figura IV.6 – Flujo de mensajes para SSO con <samlp:Response> y PSK TLS con GBA

IV.2.5 Caso SSO: SAML v2.0 con transferencia de artefactos (resolución)

Este caso es similar al descrito en la cláusula IV.2.2 con la diferencia de que todos los elementos del protocolo se toman del v2.0 [b-SAML v2.0] que integra el perfil SSO del navegador web [b-OASIS]. Por consiguiente, todos los pasos descritos en dicha cláusula son igualmente aplicables a ésta, sustituyendo <lib:AuthnRequest> por <samlp:AuthnRequest>. No se reproducen dichos pasos en esta cláusula, pero se incluye una versión adaptada de la Figura IV.3.

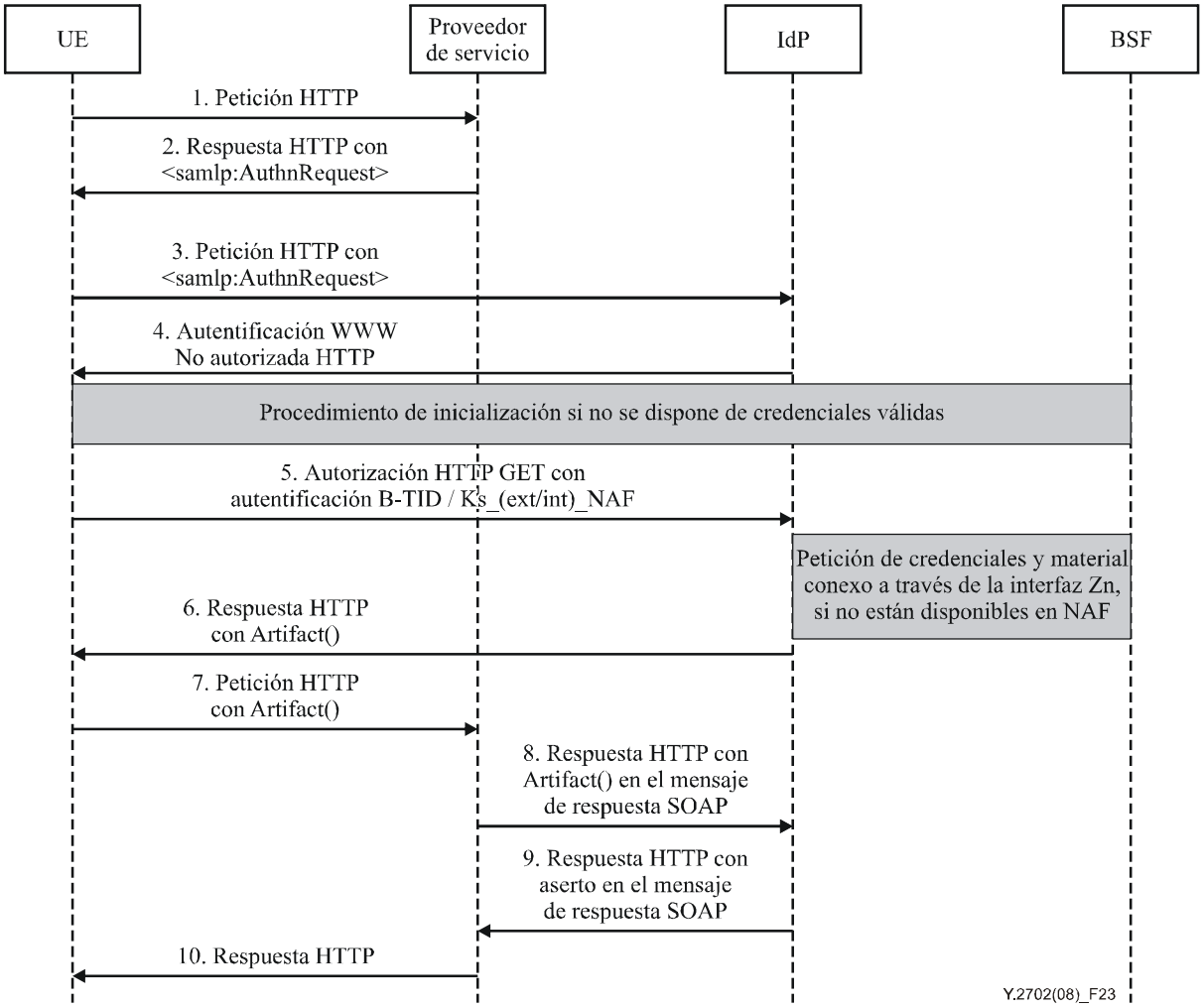


Figura IV.7 – Flujo de mensajes para SSO con resolución de artefactos (SAML v2.0) y utilización de GBA

Bibliografía

[b-UIT-T E.107] Recomendación UIT-T E.107 (2007), *Servicio de telecomunicaciones de emergencia (ETS) y marco de interconexión para implementaciones nacionales del ETS*.

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

[b-UIT-T X.1141] Recomendación UIT-T X.1141 (2006), *Lenguaje de etiquetas de aserción de seguridad (SAML 2.0)*.

[b-Alliance] Liberty Alliance Project, ID-SIS: *Liberty Alliance ID-SIS 1.0 Specifications*.
<http://www.projectliberty.org/liberty/specifications__1>

[b-ID-FF] Liberty Alliance Project, ID-FF v1.2: *Liberty ID-FF Architecture Overview*.
<http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_ff_1_2_specifications>

[b-ID-FF bindings] Liberty Alliance Project, *ID-FF v1.2: Liberty ID-FF Bindings and Profiles Specification*.
<http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_ff_1_2_specifications>

[b-ID-FF protocols] Liberty Alliance Project, ID-FF v1.2: *Liberty ID-FF Protocols and Schema Specification*.
<http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_ff_1_2_specifications>

[b-ID-WSF binding] Liberty Alliance Project, ID-WSF v2.0: *Liberty ID-WSF SOAP Binding Specification*.
<http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_wsf_2_0_specifications_including_errata_v1_0_updates>

[b-ID WSF discovery] Liberty Alliance Project, ID-WSF v2.0: *Liberty ID-WSF Discovery Service Specification*.
<http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_wsf_2_0_specifications_including_errata_v1_0_updates>

[b-ID-WSF profiles] Liberty Alliance Project, ID-WSF: *Profiles for Liberty enabled User Agents and Devices*.
<http://projectliberty.org/liberty/content/download/3447/22967/file/liberty-idwsf-client-profiles-v2.0-original.pdf>

[b-ID-WSF security] Liberty Alliance Project, ID-WSF v2.0: *Liberty ID-WSF Security Mechanisms*.
<http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_wsf_2_0_specifications_including_errata_v1_0_updates>

[b-ID-WSF service] Liberty Alliance Project, ID-WSF v2.0: *Liberty ID-WSF Authentication Service Specification and Single Sign-On Service*.
<http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_wsf_2_0_specifications_including_errata_v1_0_updates>

[b-ID-WSF v1.2] Liberty Alliance Project, ID-WSF v1.2: *Security Mechanisms*.
<http://www.projectliberty.org/resource_center/specifications/liberty_alliance_id_wsf_1_1_specifications>

[b-LAP] Liberty Alliance Project Support Documents: *Authentication Context Specification v2.0*.
<http://www.projectliberty.org/resource_center/specifications/liberty_alliance_specifications_support_documents_and_utility_schema_files>

[b-M-04-04] M-04-04: *E-Authentication Guidance for Federal Agencies*.
<http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf >

[b-NIST 800-63] NIST Special Publication 800-63 (2006), *Electronic Authentication Guidelines*.
<http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf >

[b-OASIS] OASIS, *Profiles for the OASIS Security Assertion Markup Language (SAML) v2.0*.
<http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf>

[b-OASIS auth] OASIS, *Authentication Contexts for the OASIS Security Assertion Markup Language (SAML) V2.0*.
<http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf>

[b-Reverse] Liberty Alliance Project Support Documents: *Liberty Reverse HTTP Binding for SOAP Specification v1.1*.
<http://www.projectliberty.org/resource_center/specifications/liberty_alliance_specifications_support_documents_and_utility_schema_files>

[b-SAML assertions] OASIS, SAML v2 Core, *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*.
<http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>

[b-SAML v2.0] OASIS, SAML v2 Core, *Conformance Requirements for the OASIS Security Assertion Markup Language (SAML) V2.0*.
<http://docs.oasis-open.org/security/saml/v2.0/saml-conformance-2.0-os.pdf>

[b-TR 21.905] 3GPP TR 21.905 (in force), *Vocabulary for 3GPP Specifications*.
<http://www.3gpp.org/ftp/Specs/html-info/21905.htm>

[b-TR 33.980] 3GPP TR 33.980 (in force), *Liberty Alliance and 3GPP security interworking; Interworking of Liberty Alliance Identity Federation Framework (ID-FF), Identity Web Services Framework (ID-WSF) and Generic Authentication Architecture (GAA) (Release 7)*.
<http://www.3gpp.org/ftp/Specs/html-info/33980.htm>

[b-TS 24.109] 3GPP TS 24.109 (in force), *Bootstrapping interface (Ub) and network application function interface (Ua); Protocol details.*
<http://www.3gpp.org/ftp/Specs/html-info/24109.htm>

[b-TS 29.109] 3GPP TS 29.109 (in force), *Generic Authentication Architecture (GAA); Zh and Zn Interfaces based on the Diameter protocol; Stage 3*.
<http://www.3gpp.org/ftp/Specs/html-info/29109.htm>

[b-TS 33.220] 3GPP TS 33.220 (in force), *Generic Authentication Architecture (GAA); Generic bootstrapping architecture*.
<http://www.3gpp.org/ftp/Specs/html-info/33220.htm>

[b-TS 33.221] 3GPP TS 33.221 (in force), *Generic Authentication Architecture (GAA); Support for subscriber certificates*.
<http://www.3gpp.org/ftp/Specs/html-info/33221.htm>

[b-TS 33.222] 3GPP TS 33.222 (in force), *Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)*.
<http://www.3gpp.org/ftp/Specs/html-info/33222.htm>

[b-IETF RFC 2222] IETF RFC 2222 (1997), *Simple Authentication and Security Layer (SASL)*.
<http://www.ietf.org/rfc/rfc2222.txt?number=2222>

[b-IETF RFC 2246] IETF RFC 2246 (1999), *The TLS Protocol Version 1.0*.
<http://www.ietf.org/rfc/rfc2246.txt?number=2246>

[b-IETF RFC 2616] IETF RFC 2616 (1999), *Hypertext Transfer Protocol-HTTP/1.1*.
<http://www.ietf.org/rfc/rfc2616.txt?number=2616>

[b-IETF RFC 2617] IETF RFC 2617 (1999), *HTTP Authentication: Basic and Digest Access Authentication*.
<http://www.ietf.org/rfc/rfc2617.txt?number=2617>

[b-IETF RFC 2831] IETF RFC 2831 (2000), *Using Digest Authentication as a SASL Mechanism*.
<http://www.ietf.org/rfc/rfc2831.txt?number=2831>

[b-IETF RFC 3546] IETF RFC 3546 (2003), *Transport Layer Security (TLS) Extensions*.
<http://www.ietf.org/rfc/rfc3546.txt?number=3546>

[b-IETF RFC 4279] IETF RFC 4279 (2005), *Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)*.
<http://www.ietf.org/rfc/rfc4279.txt?number=4279>

[b-IETF RFC 4412] IETF RFC 4412 (2006), *Communication Resource Priority for the Session Initiation Protocol*.
<http://www.ietf.org/rfc/rfc4412.txt?number=4412>

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, 2009