Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

Y.2720

(01/2009)

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

Redes de la próxima generación – Seguridad

Marco general para la gestión de identidades en las redes de la próxima generación

Recomendación UIT-T Y.2720

Unión Internacional de Telecomunicaciones

RECOMENDACIONES UIT-T DE LA SERIE Y

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

INFRAESTRUCTURA MUNDIAL DE LA INFORMACIÓN	
Generalidades	Y.100–Y.199
Servicios, aplicaciones y programas intermedios	Y.200–Y.299
Aspectos de red	Y.300–Y.399
Interfaces y protocolos	Y.400–Y.499
Numeración, direccionamiento y denominación	Y.500–Y.599
Operaciones, administración y mantenimiento	Y.600–Y.699
Seguridad	Y.700–Y.799
Características	Y.800–Y.899
ASPECTOS DEL PROTOCOLO INTERNET	
Generalidades	Y.1000–Y.1099
Servicios y aplicaciones	Y.1100–Y.1199
Arquitectura, acceso, capacidades de red y gestión de recursos	Y.1200–Y.1299
Transporte	Y.1300–Y.1399
Interfuncionamiento	Y.1400–Y.1499
Calidad de servicio y características de red	Y.1500–Y.1599
Señalización	Y.1600–Y.1699
Operaciones, administración y mantenimiento	Y.1700–Y.1799
Tasación	Y.1800–Y.1899
Televisión IP sobre redes de próxima generación	Y.1900–Y.1999
REDES DE LA PRÓXIMA GENERACIÓN	
Marcos y modelos arquitecturales funcionales	Y.2000–Y.2099
Calidad de servicio y calidad de funcionamiento	Y.2100–Y.2199
Aspectos relativos a los servicios: capacidades y arquitectura de servicios	Y.2200–Y.2249
Aspectos relativos a los servicios: interoperabilidad de servicios y redes en las redes de la próxima generación	Y.2250–Y.2299
Numeración, denominación y direccionamiento	Y.2300–Y.2399
Gestión de red	Y.2400–Y.2499
Arquitecturas y protocolos de control de red	Y.2500–Y.2599
Redes 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.2720

Marco general para la gestión de identidades en las redes de la próxima generación

Resumen

En la Recomendación UIT-T Y.2720 se proporciona un marco para la gestión de identidades (IdM) en las redes de la próxima generación (NGN). La finalidad principal de este marco es describir un enfoque estructurado para la concepción, definición y aplicación de soluciones de IdM y facilitar la compatibilidad en un entorno heterogéneo.

La gestión de la información en materia de identidad (por ejemplo, identificadores, credenciales y atributos) no es algo nuevo. Sin embargo, a medida que nos dirigimos hacia un entorno de redes convergentes en el que los servicios se basan en contextos y funciones y en el que se puede acceder a los mismos desde cualquier lugar y en cualquier momento, la protección, seguridad y gestión de la información acerca de la identidad se hacen cada vez más complejas. Además, pueden existir distintas soluciones independientes entre sí que explican la necesidad de la compatibilidad. Así pues, se necesitan nuevas capacidades mejoradas, automatizadas y compatibles por los siguientes motivos:

- los usuarios finales utilizan cada vez más identidades múltiples;
- dichas identidades pueden estar asociadas con distintos contextos y privilegios de servicio;
- es posible que las identidades sólo identifiquen parcialmente al usuario final;
- las identidades pueden utilizarse en cualquier momento y desde cualquier lugar;
- es posible que las identidades no sean compatibles entre los proveedeores.

La IdM aborda esta situación, y consiste en una serie de funciones y capacidades (por ejemplo, administración, gestión y mantenimiento; descubrimiento; intercambios de comunicaciones; correlación y vinculación; cumplimiento de la política; autenticación y asertos) que se utilizan para:

- la protección de la información sobre la identidad (por ejemplo, identificadores, credenciales y atributos);
- la protección de la identidad de una entidad (por ejemplo, usuarios, suscriptores, grupos, aparatos de usuario, organizaciones, redes y proveedores de servicios, elementos y objetos de red y objetos virtuales); y
- las aplicaciones habilitadoras de negocios y de seguridad.

Este marco está destinado a ser utilizado como base para el desarrollo y la especificación de aspectos concretos de la IdM tales como los requisitos, mecanismos y procedimientos que se requieran. También permite darse una idea general clara y coherente de la totalidad de la IdM en las NGN.

El marco que proporciona esta Recomendación está destinado a las NGN (es decir, redes de paquetes gestionados) según lo dispuesto en la Recomendación UIT-T Y.2001, Visión general de las redes de próxima generación. Sin embargo, podría aplicarse a otros tipos de red (por ejemplo, redes corporativas y de empresa).

NOTA – El contenido del término "identidad" en la presente Recomendación, tal como éste se utiliza en relación con el concepto de IdM, no es exhaustivo. En particular, no debe entenderse en modo alguno como una validación positiva de una persona.

Orígenes

La Recomendación UIT-T Y.2720 fue aprobada el 23 de enero de 2009 por la Comisión de Estudio 13 (2009-2012) del UIT-T por el procedimiento de la Resolución 1 de la AMNT.

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/.

© UIT 2010

Reservados todos los derechos. Ninguna parte de esta publicación puede reproducirse por ningún procedimiento sin previa autorización escrita por parte de la UIT.

ÍNDICE

Página

1 Alcance 1

2 Referencias 1

3 Definiciones 2

3.1 Términos definidos en otros textos 2

3.2 Términos definidos en normas publicadas por organismos distintos de la UIT 2

3.3 Términos definidos en esta Recomendación 2

4 Abreviaturas 4

5 Introducción 4

5.1 Panorama general de la gestión de identidad (IdM) 4

5.2 Motores e incentivos de negocios 6

5.3 Proveedor de identidad (IdP) 8

5.4 Arquitectura funcional de las NGN y utilización de identificadores 9

6 Panorama general del marco IdM 10

7 La IdM en el contexto de las arquitecturas y modelos de referencia NGN 11

7.1 Relación general entre arquitecturas y servicios NGN 11

7.2 Recomendación UIT-T Y.2011 (Principios generales y modelo de referencia general de las redes de próxima generación NGN) 12

8 Marco de la gestión de identidad 13

8.1 Gestión del ciclo de vida de la identidad 13

8.2 Funciones OAM&P de la gestión de identidad 14

8.3 Funciones de señalización y control de la gestión de identidad 17

8.4 Funciones de identidad federada de la gestión de identidad 22

8.5 Usuario y funciones de abonado de la gestión de identidad 22

8.6 Calidad de funcionamiento y fiabilidad 23

8.7 Seguridad IdM 24

Bibliografía 25

Recomendación UIT-T Y.2720

Marco general para la gestión de identidades en las redes de la próxima generación

1 Alcance

En la presente Recomendación se proporciona un marco para la IdM en las NGN y el propósito principal consiste en describir los conceptos fundamentales, los componentes funcionales y las capacidades de la IdM a las que cabe recurrir para organizar y orientar soluciones estructuradas para las NGN. En la presente Recomendación:

- se describen los motivos, beneficios y ventajas comerciales que aportan los servicios IdM, y las capacidades genéricas utilizadas para proporcionar garantía de identidad y definir conceptos IdM aplicables a las NGN, basándose en los requisitos y la arquitectura funcionales de las NGN, según se definen éstos en [b-ITU-T Y.2012], *Requisitos funcionales y arquitectura de la red de próxima generación, versión 1*;
- se identifican y describen las entidades, los papeles, los habilitadores y las comunicaciones funcionales que soportan servicios y capacidades IdM para las NGN;
- se identifican y describen las relaciones intrarred que se requieren para soportar servicios y capacidades IdM en una NGN; y
- se identifican y describen las relaciones necesarias para soportar servicios y capacidades IdM entre proveedores NGN (por ejemplo, dentro de una federación), así como entre proveedores NGN y otros proveedores (por ejemplo, entre federaciones).

El marco descrito en la presente Recomendación está destinado a las NGN (por ejemplo, redes de paquetes gestionados), según se definen en [b-ITU-T Y.2001], *Panorama general de las NGN*. Sin embargo, podría aplicarse, en su caso, a otros tipos de redes (redes de consorcios y redes de empresas del sector privado).

La idea es utilizar el marco mencionado como una base para diseñar y especificar determinados aspectos de la IdM para las NGN, por ejemplo, los requisitos, mecanismos y procedimientos detallados que se requieran. El marco proporciona asimismo un panorama preciso y coherente de la IdM considerada en su totalidad en las NGN.

NOTA – El contenido del término "identidad" en la presente Recomendación, tal como éste se utiliza en relación con el concepto de IdM, no es exhaustivo. En particular, no debe entenderse en modo alguno como una validación positiva de una persona.

2 Referencias

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

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

3 Definiciones

3.1 Términos definidos en otros textos

En la presente Recomendación se utilizan los siguientes términos, que se definen en otros textos.

3.1.1 anonimato [b-ITU-T X.1121]: Posibilidad que permite el acceso anónimo a servicios con el objeto de no descubrir la información personal y el comportamiento del usuario, tales como su localización y frecuencia de utilización de un servicio.

3.1.2 autenticación [b-ITU-T X.811]: Garantía de la identidad declarado por una entidad.

3.1.3 autorización [b-ITU-T X.800]: Atribución de derechos, que incluye la concesión de acceso basado en derechos de acceso.

3.1.4 declarante [b-ITU-T X.811]: Confirmación de la identidad declarada de una entidad. Un declarante incluye las funciones necesarias para intervenir en intercambios de autenticación en nombre de un principal.

3.1.5 delegación [b-ITU-T X.911]: Acción que asigna autoridad, responsabilidad o una función a otro objeto.

3.1.6 identificador [b-ITU-T Y.2091]: Un identificador es una serie de dígitos, caracteres y símbolos o cualquier otra forma de datos utilizados para identificar abonados, usuarios, elementos de red, funciones, entidades de red que proporcionan servicios/aplicaciones, u otras entidades (por ejemplo, objetos físicos o lógicos).

3.1.7 redes de la próxima generación (NGN) [b-ITU-T Y.2001]: Red basada en paquetes que permite prestar servicios de telecomunicación y en la que se pueden utilizar múltiples tecnologías de transporte de banda ancha propiciadas por la calidad de servicio, y en la que las funciones relacionadas con los servicios son independientes de las tecnologías subyacentes relacionadas con el transporte. Permite a los usuarios el acceso sin trabas a redes y a proveedores de servicios y/o servicio de su elección. Se soporta movilidad generalizada que permitirá la prestación coherente y ubicua de servicios a los usuarios.

3.1.8 principal [b-ITU-T X.811]: Entidad cuya identidad puede ser autenticada.

3.1.9 dominio de seguridad [b-ITU-T X.810]: Un conjunto de elementos, una política de seguridad, una autoridad de seguridad y un conjunto de actividades pertinentes a la seguridad, donde el conjunto de elementos está sujeto a la política de seguridad, para las actividades especificadas y la política de seguridad es administrada por la autoridad de seguridad para el dominio de seguridad.

3.1.10 verificador [b-ITU-T X.811]: Entidad que es o representa la entidad que requiere una identidad autenticada. Un verificador incluye las funciones necesarias para intervenir en intercambios de autenticación.

3.2 Términos definidos en normas publicadas por organismos distintos de la UIT

3.2.1 atributo [b-ETSI TS 102 042]: Información descriptiva vinculada a una entidad que especifica una característica de una entidad, por ejemplo, condición, calidad u otra información asociada con dicha entidad.

3.3 Términos definidos en esta Recomendación

En la presente Recomendación se definen los siguientes términos:

3.3.1 garantía: Medida de la confianza en que las características de seguridad y la arquitectura de las capacidades de gestión de identidad median con exactitud y garantizan el cumplimiento de las políticas de seguridad objeto de entendimiento entre la parte dependiente y el proveedor de identidad.

3.3.2 garantía de la autenticación: Véase "garantía".

3.3.3 nivel de garantía: Expresión cuantitativa de la garantía convenida por una parte dependiente y un proveedor de identidad.

3.3.4 credencial: Objeto identificable que puede utilizarse para autenticar que el declarante es quien declara serlo, así como para autorizar los derechos de acceso del declarante.

3.3.5 descubrimiento: El acto de localizar una descripción procesable mediante máquina de un recurso relacionado con una red que puede haberse desconocido previamente y que satisface ciertos criterios funcionales. Entraña la correspondencia de un conjunto de criterios funcional y de otro tipo con un conjunto de descripciones de recursos. La idea es encontrar un recurso idóneo relacionado con el servicio.

3.3.6 entidad: Todo lo que tiene existencia separada y distinta y puede identificarse unívocamente. Ejemplos de entidad en el contexto de la gestión de identidad, son los siguientes: abonados, usuarios, elementos de red, redes, aplicaciones de soporte lógico, servicios y dispositivos. Una entidad puede contar con múltiples identificadores.

3.3.7 federación: Establecimiento de una relación entre dos o más entidades o una asociación que abarca un número variable de proveedores de servicio y proveedores de identidad.

3.3.8 identidad federada: Identidad que puede utilizarse para acceder a un grupo de servicios o aplicaciones limitado por las políticas y condiciones de una federación.

3.3.9 identidad: Información acerca de una entidad que resulta suficiente para identificar a dicha entidad en un determinado contexto.

3.3.10 proveedor de identidad: Entidad que crea, mantiene y gestiona información digna de confianza sobre la identidad de otras entidades (por ejemplo, usuarios/abonados, organizaciones y dispositivos) y ofrece servicios basados en la identidad, así como en la confianza, el negocio de que se trate y otros tipos de relaciones.

3.3.11 gestión de identidad: Conjunto de funciones y capacidades (por ejemplo, administración, gestión y mantenimiento, descubrimiento, intercambios de comunicación, correlación y vinculación, cumplimiento de una política, autenticación y asertos) que se utilizan para:

- garantizar la información de identidad (por ejemplo, identificadores, credenciales, atributos);
- garantizar la identidad de una entidad (por ejemplo, usuarios/abonados, grupos, dispositivos de usuario, organizaciones, proveedores de red y servicios, elementos y objetos de red, y objetos virtuales);
- habilitar aplicaciones de negocios y de seguridad.

3.3.12 pauta: Expresión estructurada derivada del comportamiento asociado con una entidad y que describe a dicha identidad; lo que puede incluir la reputación de la misma. Las pautas pueden asociarse unívocamente a una entidad o a una clase a la cual la entidad se encuentra asociada.

3.3.13 información de identificación personal: La información que tiene que ver con una persona viva, y que hace posible identificarla (lo que incluye la información que permite identificar a una persona cuando se combina con otra información, incluso cuando por sí sola no permite identificar claramente a esa persona).

3.3.14 presencia: Conjunto de atributos que caracterizan una entidad en relación con la situación presente.

3.3.15 privacidad: Protección de la información de identidad personal.

3.3.16 parte dependiente: Entidad que depende de una representación o declaración de identidad de una entidad solicitante/asertante.

3.3.17 confianza: Medida de la dependencia con respecto al carácter, capacidad, solidez o verdad de alguien o algo.

4 Abreviaturas

En la presente Recomendación se utilizan las siguientes abreviaturas:

API Interfaz de programación de aplicaciones (*application programming interface*)

BSS Sistema de soporte de negocio (*business support system*)

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

FRA Requisitos y arquitectura funcionales (*functional requirements and architecture*)

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

IdM Gestión de identidad (*identity management*)

IdP Proveedor de identidad (*identity provider*)

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

OAM&P Operación, administración, mantenimiento y provisión (*operation, administration, maintenance and provisioning*)

OSS Sistema de soporte de operaciones (*operations support system*)

PII Información de identificación personal (*personally identifiable information*)

PSTN Red telefónica pública conmutada (*public switched telephone network*)

QoE Calidad de experiencia (*quality of experience*)

QoS Calidad percibida (*quality of service*)

RP Parte dependiente (*relying party*)

SAML Lenguaje de marcas de asertos de seguridad (*security assertion markup language*)

SBC Controlador limítrofe de sesión (*session border controller*)

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

SP Proveedor de servicios (*service provider*)

SS7 Sistema de señalización N.° 7 (*signaling system No. 7*)

URI Identificador uniforme de recursos (*uniform resource identifier*)

VoIP Voz con protocolo de Internet (*voice over Internet protocol*)

5 Introducción

5.1 Panorama general de la gestión de identidad (IdM)

La gestión de la información de identidad de una entidad (por ejemplo, identificadores, credenciales y atributos) no es una práctica novedosa. Con todo, a medida que se pasa un entorno de red convergente donde los servicios se basan en contextos y papeles, y es posible acceder a los mismos desde cualquier parte y en todo momento, se hacen más complejos la garantía, la seguridad y la gestión de la información de identidad. Por otra parte, el hecho de que la compatibilidad resulte necesaria puede dar lugar a soluciones diferentes e independientes. Así pues, es preciso contar con capacidades nuevas, mejoradas, automatizadas y compatibles. El propósito perseguido con el presente marco consiste en describir un enfoque estructural para diseñar, definir e implementar soluciones que faciliten la compatibilidad en un entorno heterogéneo.

La IdM, aborda esta situación y es un conjunto de funciones y capacidades (administración, gestión y mantenimiento, descubrimiento, intercambio de comunicación, correlación y vinculación, cumplimiento de política, autenticación, asertos, etc.) que se utilizan para:

- garantizar la información de identidad;
- garantizar la identidad de una entidad;
- habilitar aplicaciones de negocios y de seguridad.

En la figura 1 se traza un panorama general de la IdM.

Figura 1 – Panorama general de la IdM

La información de identidad asociada con una entidad puede dividirse en las siguientes categorías:

- identificadores (identidad de usuario, dirección de correo electrónico, números de teléfono, URI, direcciones IP, etc.);
- credenciales (certificados digitales, testigos, biométrica, etc.); y
- atributos (papeles, declaraciones, privilegios, pautas, ubicación, etc.).

Las funciones y capacidades de IdM se utilizan para garantizar la información de identidad, garantizar la identidad de una entidad, y soportar aplicaciones de negocios y de seguridad que incluyen servicios basados en la identidad.

Asimismo, los servicios y capacidades IdM permiten a las entidades usuarias/abonadas controlar la forma en que la información de identidad se utiliza y difunde. La IdM hace posible también que la información de identidad federada sea compartida y utilizada por los miembros de una federación (por ejemplo, asociados empresariales) para soportar servicios federados.

La IdM habilita el desarrollo de diferentes aplicaciones, entre las cuales cabe citar de manera no exhaustiva las siguientes:

- *aplicaciones de negocios*
  - inicio y término de sesión únicos (por ejemplo, acceso a múltiples aplicaciones y servicios, sin necesidad de autenticar individualmente cada plataforma de aplicaciones o servicios);
  - servicios federados (por ejemplo, acceso a servicios de un proveedor de servicio a otra o a través de diferentes proveedores de NGN);
- *servicios basados en la identidad*
  - servicios de identificador, credenciales y atributo;
  - servicio de vinculación (correspondencia e interfuncionamiento de la información de identidad en un entorno heterogéneo);
  - pauta de servicios de información;
- *aplicaciones de seguridad*
  - control de acceso en caso de servicios de red y aplicaciones (por ejemplo, VoIP, IPTV y datos);
  - control de acceso basado en papeles a información, recursos y activos;
  - gestión de autorización y privilegios;
  - servicios de protección de la seguridad (por ejemplo, características de seguridad destinadas a proteger recursos de infraestructura de red e información y activos de identidad de usuarios/abonados;
  - protección de la información personal identificable (PII).

En un entorno federado caracterizado por la existencia de varios de proveedores de servicios, los servicios y las capacidades IdM se utilizan para descubrir y comunicar información con el fin de propiciar confianza en la identidad o identidades de una entidad que forme parte de un grupo de diversas entidades de red, tales como abonados/declarantes, partes dependientes (por ejemplo, usuarios, proveedores de servicios y proveedores de red), proveedores de servicios de identidad (por ejemplo, proveedores de credenciales y proveedores de verificadores) de un dominio a otro de red o de seguridad. Así por ejemplo, un proveedor de identidad seleccionado (por ejemplo, un proveedor de autenticación/verificador, etc.) puede verificar identificadores, credenciales y atributos asociados con una identidad, que a su vez pueden comunicarse mediante asertos, a una parte dependiente (por ejemplo, un proveedor de servicio), para facilitar el control de acceso, las diferentes decisiones de negocios y el cumplimiento de las políticas aplicables (por ejemplo, privacidad y protección de información de identificación personal, etc.).

5.2 Motores e incentivos de negocios

Aparte de ser un habilitador de la seguridad de las NGN, la IdM habilita y facilita nuevas e incipientes aplicaciones y servicios de negocios (por ejemplo, aplicaciones convergentes fijas y móviles y aplicaciones basadas en la web) en las NGN. Concretamente, como puede verse en la figura 2, los servicios, capacidades y funciones IdM soportan una amplia gama de aplicaciones y servicios de usuarios finales/abonados, empresas privadas (por ejemplo, redes, proveedores de servicios, consorcios) y empresas públicas.

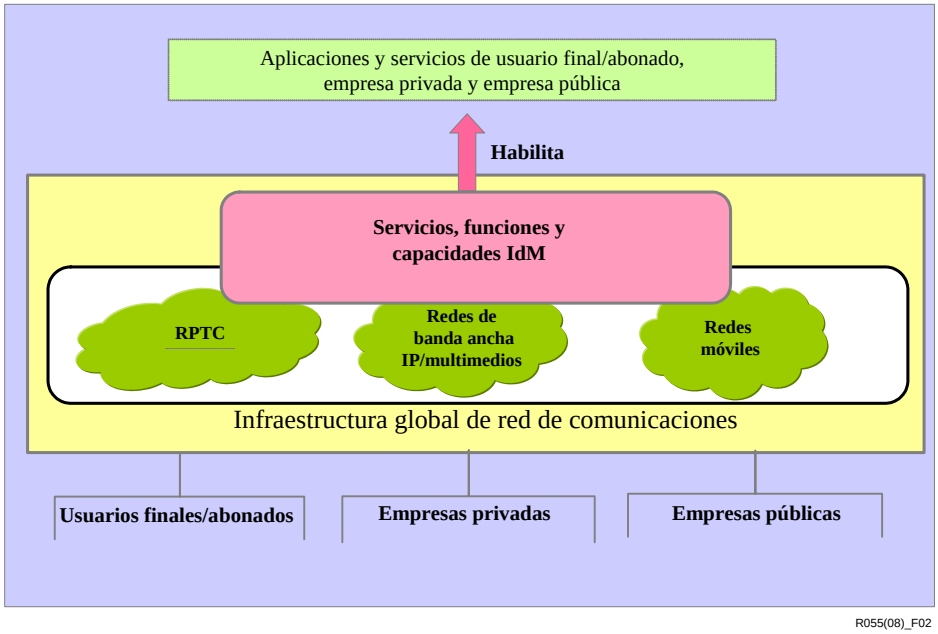


Figura 2 – Utilización de servicio IdM

La IdM es un componente esencial de la gestión de la seguridad de las NGN, así como de la habilitación del acceso nómada a petición a servicios y aplicaciones NGN, que caracteriza a las expectativas de los usuarios finales en la era de la información. Junto con otros mecanismos defensivos (por ejemplo cortafuegos, sistemas de detección de intrusiones y protección contra virus), la IdM desempeña un cometido importante en lo que respecta a la protección de la infraestructura y los servicios y aplicaciones NGN contra ciberdelitos tales como el fraude y el robo de identidad. Asimismo, como los usuarios confiarán en la seguridad y fiabilidad de las transacciones NGN, la IdM habilitará nuevas ofertas de servicios basados en la identidad. Así pues, el recurso a la IdM mejorará significativamente los servicios y las capacidades de red existentes. En el cuadro 1 se resumen los motores e incentivos de la IdM.

Cuadro 1 – Motores e incentivos de la IdM

Punto de vista	Motores e incentivos de la IdM
Usuarios finales/abonados	• Control de la información personal y protección de la información de identificación personal por parte del usuario. Proporciona la capacidad de controlar a quién se permite acceder (esto es, dar consentimiento) a información personal y la forma en que se utiliza. • Inicio de sesión/el término de sesión únicos – Proporciona acceso uniforme a múltiples aplicaciones y servicios, a través de múltiples proveedores de servicios/federaciones. • Control de acceso flexible a redes y servicios de aplicación (por ejemplo, VoIP, IPTV y datos). • Establecimiento de contactos sociales – Proporciona capacidades de identidad dinámicas y flexibles para acceder con confianza a servicios de establecimientos de contactos sociales. • Seguridad – Proporciona confianza en las transacciones, al incluir protección contra el robo de identidad.

Punto de vista	Motores e incentivos de la IdM
Empresas privadas (por ejemplo, proveedores NGN)	• Habilitación del acceso a servicios basados en abono a partir de cualquier lugar, en todo momento y utilizando todo tipo de dispositivo. • Prestación de funciones y capacidades de garantía de identidad para soportar múltiples aplicaciones y servicios. • Habilitación de la conectividad dinámica/automática entre múltiples asociados (por ejemplo, usuarios finales, redes visitadas y redes propias), en comparación con la concertación de arreglos entre pares con miras a establecer acuerdos de servicio, intercambiar información de identidad y garantizar el cumplimiento de políticas. • Habilitación de la prestación de nuevas aplicaciones y servicios (por ejemplo, convergencia fija y móvil), incluidos servicios basados en la identidad tales como servicios de identificador, credencial y atributo a abonados y otros proveedores de servicio. • Habilitación de un plan normalizado API y de datos para el diseño de aplicaciones de una plataforma a otra de multivendedores y de entrega de servicios. • Habilitación de identidad y servicios federados. • Suministro de protección a servicios de aplicación, infraestructura de red y recursos. • Habilitación de una observancia más fácil de los requisitos de reglamentación.
Empresas públicas	• Habilitación de servicios y capacidades de garantía de identidad y mejoramiento del nivel de confianza en las identidades para soportar: – servicios de gobierno electrónico (cibergobierno) (por ejemplo, transacciones basadas en la web); – servicios de seguridad pública (por ejemplo, servicios de emergencia llamando al 911); – servicio de cumplimiento de la ley (por ejemplo, intercepciones autorizadas por la ley); – servicio de telecomunicaciones de emergencia; – servicios de pronta alerta; – servicios de seguridad nacional. • Se habilitan servicios públicos federados. • Se proporciona protección en favor de la infraestructura de comunicaciones (por ejemplo, contra amenazas a la ciberseguridad).

5.3 Proveedor de identidad (IdP)

En la presente Recomendación no se impone restricción alguna a quienes proporcionan servicios de proveedor de identidad (IdP).

Un IdP es una entidad que crea, mantiene y gestiona información de identidad digna de confianza de otras entidades (por ejemplo, usuarios/abonados, organizaciones y dispositivos) y ofrece servicios de identidad basados en la confianza, transacciones de negocio y otros tipos de relaciones.

En un entorno garantizado por múltiples proveedores de servicios, puede suceder que un proveedor NGN sea un proveedor de identidad. Resulta también posible que un proveedor de red NGN ofrezca servicios IdP (por ejemplo, servicios basados en la identidad) a otros proveedores. Asimismo, cabe la posibilidad de utilizar servicios IdP ofrecidos por una tercera parte.

5.4 Arquitectura funcional de las NGN y utilización de identificadores

Según se describe en [b-ITU-T Y.2012], *Requisitos funcionales y arquitectura de la red de próxima generación, versión 1*, las NGN consisten en una serie de elementos funcionales que utilizan identificadores de identidades para realizar sus funciones, con el fin de soportar y facilitar servicios y aplicaciones. En la figura 3 se dan varios ejemplos de identidades que se hacen corresponder a un diagrama funcional NGN, esto es, la arquitectura NGN descrita en [b-ITU-T Y.2012].

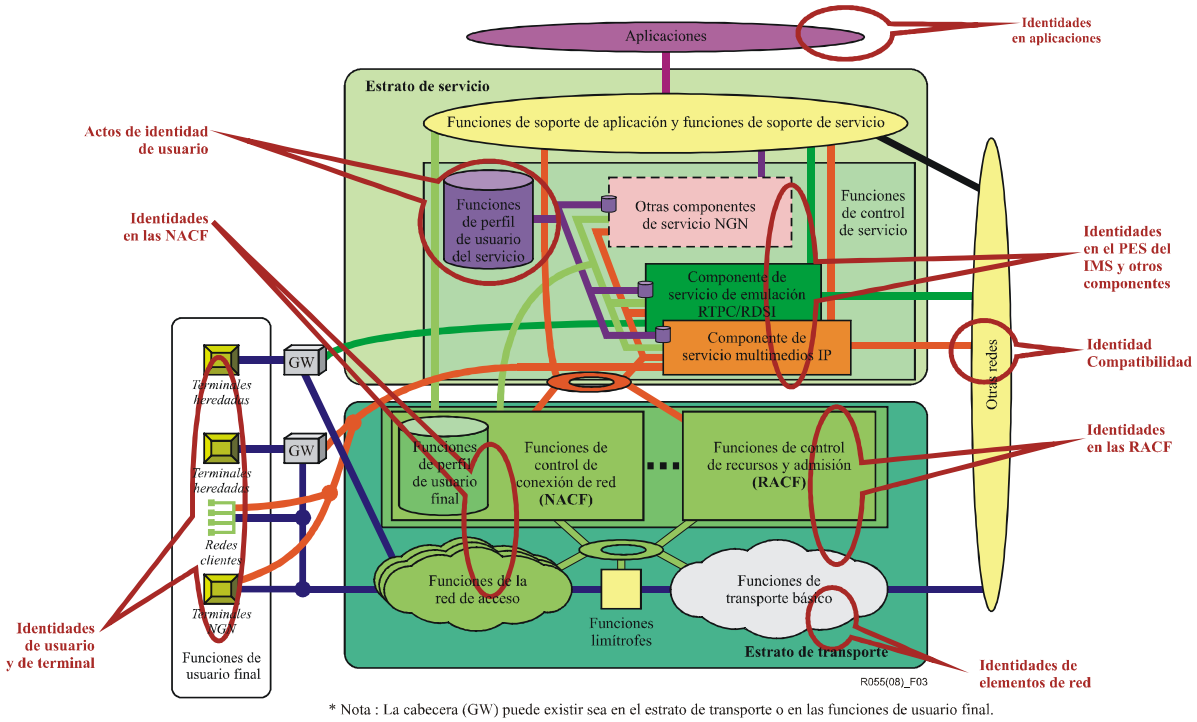


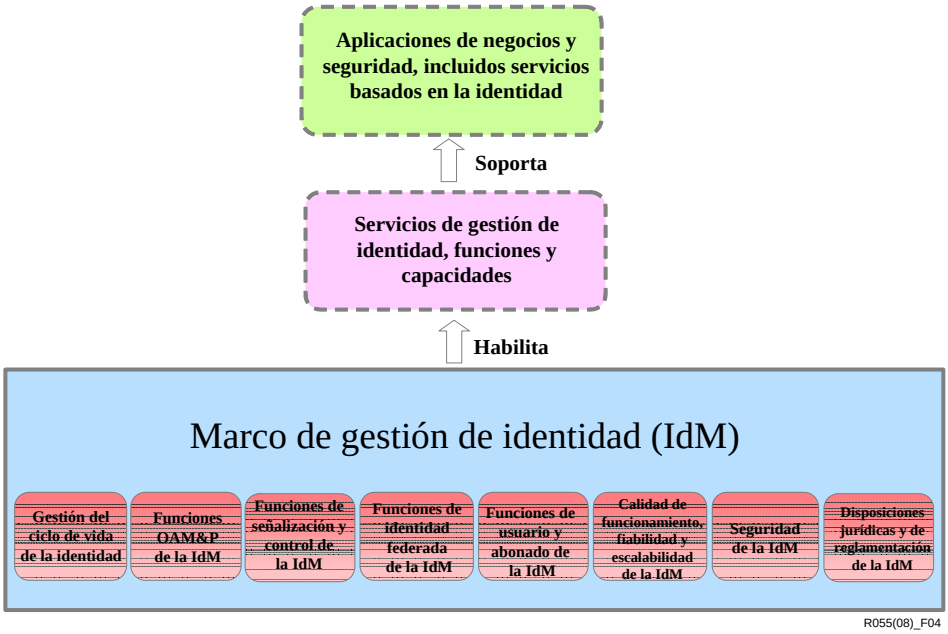
Figura 3 – Ejemplos de identidades NGN

Como para todas las operaciones NGN se utilizan estas diferentes identidades, importa mantener la integridad de dichas identidades. La IdM proporciona servicios de garantía, capacidades y funciones para mantener la integridad y la utilización de identidades NGN.

En el entorno de la red NGN una sola entidad puede contar con múltiples atributos de identidad, atributos que pueden ser utilizados por diferentes elementos de red (por ejemplo, en distintos dominios de proveedor NGN o en diversos estratos de la NGN (es decir, el estrato de servicio o el estrato de transporte), y por distintas entidades en diferentes lugares. Así pues, resulta necesario que la IdM proporcione capacidades que permitan un intercambio de información seguro entre entidades (y/o lugares), tales como partes dependientes (por ejemplo, aplicación, servicio o sus proveedores) y proveedores de identidad (IdP). Hay que señalar que el proveedor NGN puede ser también un IdP. El intercambio de información IdM se basa en políticas fijadas y en la confianza establecida entre las entidades mencionadas en un entorno caracterizado por múltiples proveedores de servicios. Esta confianza se basa en el aserto y la validación de identidades de una NGN distribuida a otra. La IdM proporciona, igualmente, capacidades para proteger la privacidad de la información sobre las identidades (por ejemplo, atributos de identidad específicos), así como para garantizar que sólo se difunda información autorizada de una NGN a otra.

6 Panorama general del marco IdM

Este marco se organiza como puede verse en la figura 4.



* NOTA – Las disposiciones jurídicas y de reglamentación quedan fuera de este marco, pero se indican aquí con propósitos de integridad.

Figura 4 – Descripción general del marco IdM

El marco consiste en las siguientes funciones y capacidades IdM:

1) Gestión del ciclo vital de la identidad:

   Esto incluye los procesos de funciones de gestión del ciclo de vida en lo que concierne a las identidades y la información de identidad (por ejemplo, identificadores, credenciales y atributos). La gestión del ciclo de vida de la identidad entraña los procesos y procedimientos asociados con la contratación y expedición de identidad, o datos e información asociados con una identidad de una entidad.

2) Funciones de operación, administración, mantenimiento y provisión de la gestión de identidad IdM:

   Esto incluye funciones y capacidades de gestión de operación, administración, mantenimiento y provisión (OAM&P) relacionadas concretamente con el soporte de la IdM. OAM&P es un grupo de funciones de gestión que proporcionan indicación sobre fallos del sistema o la red, supervisión de la calidad de funcionamiento, gestión de seguridad, funciones de diagnóstico, configuración y provisión de usuario. Concretamente, en este contexto se incluyen funciones y capacidades soportadas por sistemas de gestión de red, normalmente denominadas OSS (sistemas de soporte de operaciones) y BSS (sistemas de soporte de negocios).

3) Funciones de señalización y control de la IdM:

   Esto incluye las funciones y capacidades de señalización y control utilizadas para soportar servicios, capacidades y funciones de la IdM. Abarca también señalización y control para las comunicaciones en tiempo real y en tiempo casi real.

4) Funciones de identidad federada de la IdM:

Esto incluye funciones y capacidades para la federación de identidad y el soporte de servicios federados.

5) Funciones de usuario y abonado de la IdM:

Esto incluye las funciones y procesos relacionados con el control ejercido por los usuarios finales y los abonados de su información relacionada con la identidad (PII, preferencias personales, ubicación, etc.). Abarca, igualmente, funciones de control, delegación y autorización del uso y difusión de información relacionada con la identidad.

6) Calidad de funcionamiento, fiabilidad y escalabilidad de la IdM:

Esto incluye funciones y procedimientos para abordar sistemas y soluciones de calidad de funcionamiento, fiabilidad y escalabilidad de la IdM.

7) Seguridad de la IdM:

Esto incluye funciones y procedimientos para abordar la protección de la seguridad en los sistemas, servicios y capacidades de IdM.

8) Disposiciones jurídicas y de reglamentación aplicables a la IdM:

La normativa de reglamentación no queda contemplada en la presente Recomendación.

NOTA – Este punto se indica únicamente con propósitos de integridad.

En la cláusula 8 puede verse una descripción detallada de estos temas.

7 La IdM en el contexto de las arquitecturas y modelos de referencia NGN

7.1 Relación general entre arquitecturas y servicios NGN

La figura 5 ilustra la relación existente entre el marco general de la IdM y el contexto más amplio de las redes NGN.

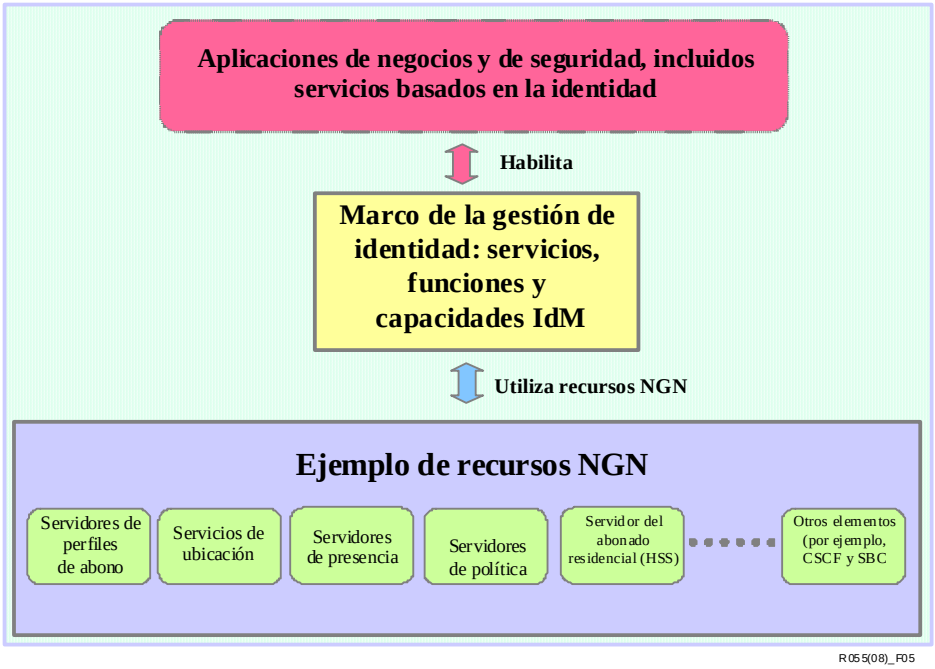


Figura 5 – Relación con las arquitecturas y servicios NGN

Como se indica en el diagrama, este marco utiliza los recursos de la red NGN (por ejemplo, información de suscripción, servidores de ubicación, política, presencia y abonado residencial, y otros elementos de la red tales como función de control de sesión de llamada (CSCF, *call session control function*), y controlador limítrofe de sesión (SBC, *session border controller*). Los servicios, funciones y capacidades IdM proporcionados por el marco IdM se utilizan para soportar y mejorar aplicaciones de negocios y de seguridad, lo que incluye servicios basados en la identidad.

7.2 Recomendación UIT-T Y.2011 (Principios generales y modelo de referencia general de las redes de próxima generación NGN)

En esta cláusula se describen los servicios, funciones y capacidades IdM en el contexto de los modelos y referencias arquitecturales de las NGN definidos en [UIT-T Y.2011], *Principios generales y modelo de referencia general de las redes de próxima generación.*

En la figura 6 se describe el ámbito de la IdM en el contexto del modelo arquitectónico de referencia definido en la figura 2 de [UIT-T Y.2011], así como el hecho de que las funciones relacionadas con la IdM pueden encontrarse en los planos de usuario, control y gestión.

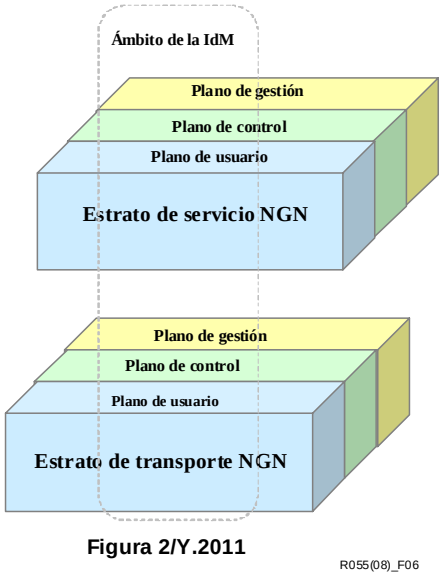


Figura 6 – Ámbito de la IdM en el contexto de la figura 2 de [UIT-T Y.2011]

En la figura 7 puede verse el ámbito de la IdM en el contexto del modelo arquitectural de referencia NGN definido en la figura 3 de [UIT-T Y.2011], así como el hecho de que las funciones relacionadas con IdM pueden incluirse en todas las capas verticales de la arquitectura NGN.

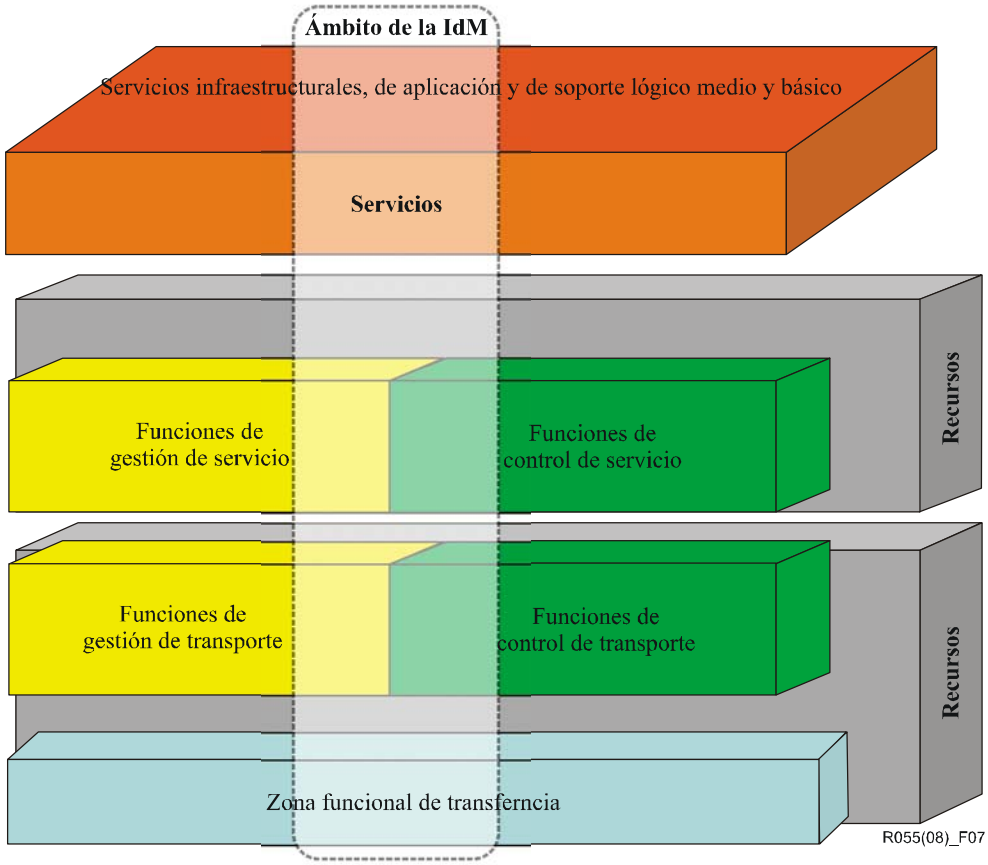


Figura 3/Y.2011

Figura 7 – IdM en el contexto de la figura 3 de [UIT Y.2011]

8 Marco de la gestión de identidad

En esta cláusula se describen detalladamente los grupos funcionales mencionados en la cláusula 6.

8.1 Gestión del ciclo de vida de la identidad

8.1.1 Prueba y registro

El primer paso de la creación de una identidad para una entidad (abonado, dispositivo, organización, proveedor NGN de objeto, etc.) comienza con el proceso de prueba y registro de la identidad o credencial correspondiente. Este proceso sirve para adoptar una entidad o credencial asociada con una determinada entidad que puede basarse en un determinado contexto (por ejemplo, papeles).

En el caso de que los abonados sean usuarios finales, se trata del proceso en virtud del cual un solicitante pide convertirse en abonado de un IdP o un proveedor NGN.

Tratándose de abonados que sean usuarios finales, el nombre del abonado podría ser un nombre verificado. Un nombre verificado se asocia con la identidad de una entidad y antes de que un solicitante pueda recibir credenciales o registrar un testigo asociado con un nombre verificado, debe demostrar que la entidad es una identidad real y que es la entidad que está autorizada a utilizar dicha identidad. Este proceso se denomina prueba de identidad. Una vez que se verifica el nombre, éste podrá asociarse con pseudónimos para permitir el anonimato.

El proceso de prueba incluye la verificación de atributos y declaraciones asociados con una identidad. Asimismo, entraña procesos y procedimientos encaminados a verificar y validar información al inscribir una entidad en un sistema de identidad.

La eficacia global de la IdM depende inicialmente del proceso de prueba y registro. Es necesario contar con requisitos de garantía, adecuadamente definidos, así como establecer procedimientos adecuados de política y gestión, para garantizar que el proceso global de inscripción se diseñe e implemente de manera apropiada.

Las directrices que habrá que considerar versan, entre otras cosas, sobre lo siguiente:

- Capacitación del personal que participa en el proceso de inscripción.
- Calidad de los documentos y otras pruebas que apoyan la inscripción de una entidad.
- Procesos necesarios para evitar disfraces durante la inscripción.
- Procesos necesarios para evitar inscripciones múltiples o dobles de la misma entidad.

8.1.2 Concesión y revocación

La conclusión exitosa del proceso de inscripción da lugar a la concesión de un medio (por ejemplo, una credencial) con la cual la entidad puede autenticarse en el futuro. Así por ejemplo, la concesión de una o varias credenciales, por un IdP (o proveedor NGN) que vincule la entidad o atributo afín (por ejemplo, un privilegio o una declaración) a la identidad asociada con una entidad.

La revocación de identidad es el proceso encaminado a rescindir una identidad y las credenciales asociadas. La parte o sistema (por ejemplo, IdP o proveedor NGN) que expida una identidad o credencial es responsable del mantenimiento y protección de la información asociada con la identidad. Esta revocación resulta necesaria para impedir el uso permanente de una identidad o credencial que no sea ya válida o haya experimentado un problema de seguridad.

Las directrices que hay que considerar versan, entre otras cosas, sobre lo siguiente:

- establecimiento de criterios de concesión y revocación;
- establecimiento de criterios para realizar actualizaciones y modificaciones;
- sincronización de la información de identidad;
- establecimiento de procesos y procedimientos en materia de expedición y revocación;
- auditoría y revisión de procesos de concesión y revocación;
- procedimientos y procesos de notificación, de expedición, actualizaciones y revocación de identidad o credenciales (lo que quiere decir que todos los sistemas y procesos mediante los cuales se ha establecido una identidad deben estar en condiciones de determinar que se han expedido, actualizado y revocado la identidad o las credenciales);
- procedimientos y procesos adecuadamente definidos para la expedición y revocación de una identidad o credencial y la política del caso. Es también necesario contar con procedimientos de gestión para garantizar que el proceso global se diseñe e implemente de manera idónea;
- mecanismos para proteger los procesos y procedimientos de revocación ante amenazas contra la seguridad.

8.2 Funciones OAM&P de la gestión de identidad

8.2.1 Modelo y plan de datos

Los diferentes proveedores NGN, federaciones o empresas pueden contar con sus propios formatos, planes, definiciones o semánticas para representar e intercambiar datos e información relacionados con la identidad. Así por ejemplo, una determinada información, tal como una fecha de nacimiento, puede ser representada de manera distinta por dos diferentes sistemas (por ejemplo, mes/día/año o día/mes/año). La semántica, planes y protocolos utilizados para solicitar e intercambiar información relacionada con la identidad pueden diferir también y generar así problemas de compatibilidad. Por ejemplo, en la red telefónica pública conmutada (RTPC) hay información de identidad como el número de la parte llamante o la identidad del llamante que se representa utilizando una semántica

específica y se recupera recurriendo a protocolos específicos (por ejemplo, SS7), distintos del sistema VoIP basado en el protocolo de iniciación de sesión.

Reviste importancia disponer de las soluciones que permitan garantizar la compatibilidad entre sistemas IdM heterogéneos que utilizan diferentes modelos, estructuras y planes de datos.

Las directrices que deben considerarse versan, entre otras cosas, sobre lo siguiente:

- modelos y esquemas de datos para facilitar la compatibilidad entre sistemas IdM heterogéneos (por ejemplo, fuentes de datos de identidad) dentro de un dominio de proveedor NGN (es decir, diferentes productos de proveedor);
- modelos y planes de datos para facilitar la compatibilidad entre diferentes proveedores NGN (interfuncionamiento);
- modelos y planes de datos para facilitar la compatibilidad entre diferentes federaciones (por ejemplo, un proveedor NGN y proveedores de servicios web).

8.2.2 Gestión de identidad

La identidad o identidades de una identidad (usuario/abonado, organización federación, empresa, proveedor de servicio, dispositivo, objetos, etc.) pueden estar asociadas con uno o más identificadores que habrá que gestionar y mantener.

Un identificador es una designación que se utiliza para representar la identidad de una entidad, por ejemplo, un usuario ID, una red ID, una dirección de correo electrónico, un seudónimo o un nombre de grupo. Así por ejemplo, cabe asociar los siguientes identificadores con la identidad de un usuario/abonado:

- Identidad de usuario.
- Dirección de correo-e.
- Número de teléfono.
- URI.
- Dirección IP.

La eficacia global de la IdM depende de que se garantice que los diferentes identificadores pueden correlacionarse y vincularse para garantizar la identidad de una entidad. Así pues, será necesario contar con requisitos y procedimientos adecuadamente definidos para la gestión de los identificadores.

En lo que concierne a los diseños e implementaciones IdM habrá que tener en cuenta, entre otras cosas, lo siguiente:

- Hay diferentes tipos de identificadores con varias características que habría que gestionar. Así por ejemplo, algunos identificadores pueden ser (esto es, únicos para diferentes federaciones), seudónimos globales que revisten significación únicamente dentro de un sistema, o un identificador puntual con un determinado periodo de validez.
- Los identificadores pueden tener diferentes características con efectos para la privacidad en lo que respecta a protegerse contra la correlación inadecuada de las acciones de un usuario.

8.2.3 Gestión de atributos

Los atributos de identidad son descriptores de una entidad: tipo de entidad, dirección IP preferida, dominio, información sobre la dirección, número de teléfono, etc. Por otra parte, los atributos pueden contener declaraciones, derechos, privilegios, listas de delegados y restricciones especiales. Otros tipos de atributos incluyen la información supervisada para detectar intrusiones: intentos de afirmación de identidad fracasados, manipulación de contadores, etc.

La eficacia de la IdM dependerá de que se garantice que los atributos pueden correlacionarse y vincularse para garantizar la identidad de una entidad. Esto incluye el almacenamiento y la provisión de atributos. En consecuencia, resulta necesario establecer requisitos y procedimientos adecuadamente definidos para la gestión de atributos.

La pauta es un tipo especial de atributo y consiste en cualquier característica que se pueda asociar con la conducta de una entidad. Los sistemas IdM pueden asignar la información sobre pautas, basándose en la reputación de la entidad consideradas y las interacciones anteriores, en lugar de ser establecida por la propia entidad. Entre los ejemplos de información sobre pautas que puede utilizarse para evaluar la garantía de entidad, cabe citar direcciones IP, puntos de acceso, información de ubicación, tiempo de utilización y sistemas a los cuales se accede. Las características inteligentes pueden tomar en consideración además eventos actuales para predecir pautas de utilización futura.

Las directrices que cabe considerar en relación con la gestión de atributos versan, entre otras cosas, sobre lo siguiente:

- información sobre pautas que puede considerarse como PII;
- requisitos y procedimientos estrictos en cuanto a la gestión de información sobre pautas;
- recurso a la información sobre pautas para reducir a un mínimo el robo de identidad;
- cumplimiento de la política PII.

8.2.4 Gestión de credenciales

Las credenciales se utilizan para autenticar una identidad declarada e incluyen:

- nombres de usuario/contraseñas;
- certificados digitales;
- testigos y tarjetas inteligentes;
- consejos de seguridad;
- información relacionada con infraestructura pública fundamental, por ejemplo, claves, certificados, autoridades signatarias de certificados e información criptográfica;
- biométrica.

La gestión de credenciales de identidad abarca las actividades operacionales que se requieren con el fin de crear, publicar y gestionar la información utilizada para autenticar declaraciones de identidad. La eficacia de la IdM depende de los procesos, procedimientos y capacidades de la gestión de credenciales. Así pues, se requieren requisitos y procedimientos adecuadamente definidos en lo que respecta a la gestión de credenciales.

Las directrices para la gestión de credenciales versan, entre otras cosas, sobre lo siguiente:

- establecimiento y mantenimiento de políticas de credenciales;
- procesos y procedimientos de gestión del ciclo de vida de las credenciales (un subconjunto de la gestión del ciclo de vida de la identidad examinado en la cláusula 8.1); y
- acuerdos de política y servicios en múltiples entornos de proveedores de servicios/red (negociación de políticas de credenciales, cumplimiento de los requisitos de federación, publicación de información sobre credenciales, tales como claves públicas).

8.2.5 Registro y auditoría

Las funciones y capacidades de registro y auditoría revisten importancia para garantizar la eficacia de las soluciones IdM. Entre las medidas de auditoría y cumplimiento, cabe citar el mantenimiento de registros históricos de seguridad para satisfacer los requisitos de responsabilidad, la protección y la utilización adecuada de la información personal y la prestación de notificaciones a los sistemas o entidades idóneos (por ejemplo, propietarios de identidad).

Las directrices para el registro y la auditoría versan, entre otras cosas, sobre lo siguiente:

- el registro y la auditoría de eventos relacionados con la IdM (acceso a información de identidad, intentos de acceso no autorizados, actualización de indicaciones de tiempo, etc.) para realizar análisis forenses;
- mecanismos y procedimientos para habilitar el seguimiento;
- detección de falta de cumplimiento de las políticas aplicables;
- garantía del cumplimiento de los requisitos de la reglamentación nacional.

8.3 Funciones de señalización y control de la gestión de identidad

8.3.1 Introducción

Las funciones de señalización y control se utilizan para descubrir y comunicar información de identidad digna de confianza (identificadores, atributos, declaraciones, etc.) asociados con una entidad (usuario/abonado, grupo, organización, elemento de red, proveedor de servicio, etc.) para soportar servicios, funciones y capacidades IdM.

En esta cláusula se describen las funciones de señalización y control relacionadas con la IdM.

8.3.2 Descubrimiento de información de identidad

En un entorno distribuido como el de la información de identidad de las NGN puede haber diferentes elementos de red (servidor de abono, servidor de ubicación, servidor de presencia, servidor de abono en el hogar, etc.). Hay medios estructurados para descubrir las fuentes de información de identidad que forman parte integral de la IdM. La idea es que una aplicación haga uso de la información de identidad, dicha aplicación debe saber que esa información existe. En un entorno NGN dinámico y en evolución se espera que sean también dinámicas la información de identidad y las fuentes de información de identidad. En consecuencia, las partes e identidades dependientes (por ejemplo, aplicaciones) requerirían medios estructurados para quedar enteradas de la existencia y el descubrimiento de información de identidad. Hay que añadir también el descubrimiento de servicios y capacidades de función IdM.

Las directrices que deben considerarse en cuanto a la especificación e implementación de las capacidades de descubrimiento versan, entre otras cosas, sobre lo siguiente:

- descubrimiento dentro de un dominio de proveedor NGN (intrarred);
- descubrimiento entre diferentes dominios de proveedor NGN (interred);
- descubrimiento entre miembros de una federación. Véase la cláusula 8.4.2, descubrimiento de federación.

El descubrimiento incluye, por otra parte, capacidades para encontrar o localizar IdP. En el marco IdM NGN el descubrimiento es algo necesario, ya que existen múltiples IdP. En casos en que haya un solo IdP (por ejemplo, una empresa) no hay necesidad de recurrir a la operación de descubrimiento, puesto que se sabrá dónde obtener atributos de identidad. Asimismo, dentro de la red de un sólo proveedor NGN puede haber múltiples sistemas que proporcionan diferentes funciones relacionadas con la gestión de identidad y funciones de descubrimiento adecuadas.

El descubrimiento resulta similar a una búsqueda de una identidad en la web. La información que requiere el motor de búsqueda consiste en las características de identidad y el resultado de la búsqueda es una lista de identificadores e IdP que corresponde a los requisitos. Este escenario de interrogación y respuesta hacen necesario por regla general que los IdP se registren como proveedores de un determinado servicio de identidad para un usuario/dispositivo dados.

Los métodos disponibles que pueden utilizarse para soportar las necesidades asociadas en lo que concierne al descubrimiento y el acceso fidedignos pueden dividirse aproximadamente en dos categorías: 1) enfoques de superposición raíz de raíces y/o 2) descubrimiento inferencial. Para aplicar el primero de estos dos enfoques es necesario que cierta entidad asuma el papel de registrador principal de espacios de nombres con un servidor de soporte, mientras que el segundo requiere disponer de reglas adecuadamente conocidas, en virtud de las cuales pueda obtenerse recursivamente la dirección de un servidor de apoyo.

8.3.3 Comunicaciones IdM

Se trata, entre otras cosas, de capacidades y funciones que permiten descubrir e intercambiar información de identidad (identificadores, credenciales, atributos, etc.) asociada con la identidad de una entidad que está ubicada en diferentes sistemas de la red (en un servidor de abono, servidor de ubicación, servidor de presencia, etc.) dentro de una red de proveedor NGN y que pueda correlacionarse y verificarse (esto es, mediante un servidor de aplicaciones IdM que ofrezca funciones de autenticación y correlación), con el fin de proporcionar capacidades de garantía de identidad. Cabe la posibilidad de comunicar asertos de identidad y atributos asociados (declaraciones, privilegios, etc.) asertos sobre sistemas subyacentes (por ejemplo, servicios de aplicación) para tomar decisiones de control de acceso. Esto permitiría a distintos servicios de aplicación (por ejemplo, diferentes plataformas de vendedor) hacer uso de una infraestructura común en cuanto a la IdM, en lugar de recurrir a soluciones independientes y autónomas. Entre las relaciones de comunicación que habría que considerar aquí figuran las siguientes:

- intrarred: comunicaciones con un dominio de proveedor NGN (por ejemplo, entre elementos de una red);
- interred: comunicaciones entre dos proveedores NGN;
- federación: comunicaciones entre miembros de una federación.

8.3.3.1 Comunicaciones en tiempo real y en tiempo casi real

En la solución que se utilice para descubrir e intercambiar información de identidad debe tomarse en consideración si se requieren comunicaciones en tiempo real o en tiempo casi real. Esto dependerá de que se soporten las correspondientes aplicaciones.

8.3.3.2 Señalización y protocolos e interfaces de control

En la figura 8 se indican las interfaces externas que resultan aplicables para soportar comunicaciones IdM. Así por ejemplo, interfaces que se utilizan para intercambiar información de identidad, controlar servicios, funciones y capacidades IdM.

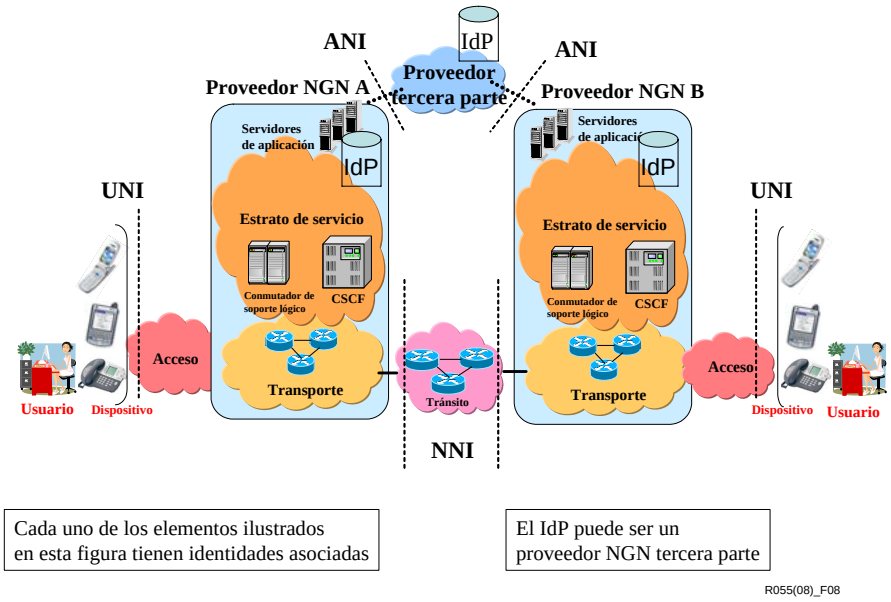


Figura 8 – Interfaces externas

Las interfaces externas incluyen:

- interfaz usuario-red (UNI);
- interfaz aplicación-red (ANI);
- interfaz red-red (NNI).

Los requisitos y protocolos que habrá que utilizar dependen concretamente de la interfaz de que se trate, la información que haya que comunicar o las funciones de control que deban desempeñarse. Para facilitar la compatibilidad, habrá que identificar y especificar los requisitos específicos, las opciones de protocolo y los perfiles que deban utilizarse. Las soluciones de interfaz dependerán de factores tales como la aplicación de que se trate y las necesidades de servicio (por ejemplo, tiempo real en comparación con tiempo casi real), las soluciones de protocolo escogidas (por ejemplo, SAML, Diameter, RADIUS) y los mecanismos y enfoques empleados (por ejemplo, arquitectura de inicialización genérica [b-ITU-T X.509] (GBA)).

No sólo las interfaces externas sino también las internas revisten importancia en lo que concierne a las soluciones globales. Dentro de una red NGN la información de identidad debe estar ubicada en diferentes elementos de red y servicios de aplicaciones (por ejemplo, servidores de abono, ubicación y presencia y otros elementos de red, tales como CSCF y SBC). Las interfaces internas y los protocolos que deban utilizarse para descubrir e intercambiar información de identidad son factores importantes en lo que respecta a la compatibilidad entre vendedores.

8.3.3.3 Mecanismos y procedimientos

Habrá que identificar y especificar los mecanismos y procedimientos que se utilizan para implementar una función o capacidad determinadas de la IdM. Así por ejemplo, será necesario identificar y especificar los mecanismos o protocolos de que se trate, así como el lugar y la forma en que deban utilizarse. Entre los ejemplos de mecanismos y protocolos que cabe citar figuran los siguientes:

- SAML
- X.509

- GBA
- E.115

8.3.4 Correlación y vinculación

La información de identidad (identificadores, credenciales, atributos, etc.) puede correlacionarse para establecer un vínculo que garantice la identidad de una entidad. Así por ejemplo, la información de identidad asociada con un abonado (por ejemplo, identidad de usuario), un dispositivo de abonado (por ejemplo, identidad de dispositivo), y la información de ubicación pueden correlacionarse para establecer un vínculo que proporcione una mayor garantía en cuanto al abonado.

Las directrices que habrá que considerar en lo que respecta a la especificación e implementación de la correlación y la vinculación, versan, entre otras cosas, sobre lo siguiente:

- el cumplimiento de la política aplicable (por ejemplo, políticas de anonimato o privacidad).

8.3.5 Autenticación

La autenticación es el proceso que lleva a establecer confianza en la identidad de una entidad. Una forma de lograr la garantía de autenticación es describir los objetivos y directrices necesarios para cuantificar la probabilidad de que una entidad sea quién o lo qué declara ser. En este contexto habrá que considerar la necesidad de determinar qué identificadores de entidad son más importantes que otros en el proceso de identificación y por qué razón ciertos identificadores utilizados en la autenticación no deben tener el mismo valor de autenticación.

Habitualmente la confianza se establece asignando pares de identidad de usuario y contraseña a cada sistema. Sin embargo, en las NGN no conviene adoptar este enfoque, por ser ineficaz desde el punto de vista operacional y dar lugar a prácticas inseguras. Las directrices que habrá que considerar a la hora de especificar e implementar autenticación versan, entre otras cosas, sobre lo siguiente:

- la confidencialidad e integridad de los mecanismos de autenticación;
- la solidez de las credenciales para ser dignas de confianza de un sistema a otro.

8.3.6 Garantía de autenticación

La garantía de autenticación es el proceso que lleva a establecer confianza en las identidades y declaraciones que se presentan a un sistema de información. No toda la información utilizada con propósitos de autenticación debería considerarse en igualdad de condiciones o tener necesariamente el mismo valor de garantía. Así, la confianza en una autenticación que utilice biométrica es muy diferente a la que inspira una autenticación que utilice identidad de usuarios/contraseñas. Habrá que asignar a cada identificador un valor relativo basado en los principios fundamentales para cuantificar la confianza en que una entidad autenticada sea la entidad válida.

El propósito de la garantía de autenticación es cuantificar la probabilidad de que una entidad sea quién o lo qué declara ser. No todos los identificadores utilizados en un proceso de decisiones de autenticación se consideran iguales o tienen necesariamente el mismo valor en términos de autenticación. Por otra parte, si aumentase la gravedad de un error de autenticación, habría que aumentar la garantía del nivel de autenticación requerido.

Disponer de un mecanismo para cuantificar y comunicar la garantía de autenticación permite que las partes dependientes tomen decisiones en cuanto a su confianza en el proceso de autenticación utilizado para validar la identidad o las declaraciones de una entidad.

Entre los beneficios primarios de la garantía de autenticación figura la capacidad para determinar el nivel de confianza en que una entidad sea lo que se declara que es a lo largo del ciclo de vida de la identidad. Los criterios normalizados para asignar y comunicar la garantía relativa del valor del proceso, y los mecanismos y los datos de autenticación (por ejemplo, contraseñas, credenciales y

biométricas) de una federación a otra resultan esenciales para soportar servicios federados y protección de la ciberseguridad.

En un proceso de garantía de la autenticación se tiene en cuenta, entre otras cosas, lo siguiente:

- El mecanismo de autenticación: las contraseñas estáticas son menos robustas que las contraseñas puntuales y un testigo de equipo con un PIN es por regla general mejor que un testigo de soporte lógico.
- El protocolo de autenticación: un protocolo del que se conoce su seguridad contra ataques "de hombre en medio" o un protocolo basado en operaciones criptográficas que se considera generalmente robusto.
- Las características del dispositivo utilizado para autenticar: la confianza en materia de autenticación se basa parcialmente en las características del dispositivo que utiliza el usuario, lo que quiere decir que un computador comprado en una tienda y que sea propiedad y esté bajo el control de una organización o un dispositivo especializado resistente contra alteraciones resultan mejores que un programa adquirido en una tienda accesible públicamente.
- La ubicación de la entidad en curso de autenticación: habrá que considerar la ubicación del usuario, por ejemplo, si se encuentra dentro del perímetro de una organización o en un quiosco público, café Internet, etc. La confianza en materia de autenticación será mayor si resulta difícil que un terminal público situado en un quiosco convenza al servidor de autenticación de que se encuentra situado dentro del perímetro físico de una organización.
- La pauta de comunicaciones: la autenticación entraña normalmente una pauta de comunicaciones (redes inalámbricas, líneas comerciales arrendadas, etc.) entre la entidad en curso de autenticación y el servidor que proporciona autenticación y/o decisiones de acceso. Es necesario que la información que se utilice para realizar la autenticación se envíe de manera fiable al servidor de autenticación y no pueda ser falsificada por un atacante.
- La facilidad relativa de manipulación de la autenticación por causa de conducta maliciosa: importa evaluar el riesgo asociado con el hecho de que se comprometan claves criptográficas.

8.3.7 Delegación

La delegación entraña acciones y procesos de transferencia de privilegios para realizar ciertas acciones en nombre del principal de una entidad que tenga privilegios con respecto a otra entidad que no los posea.

Así, la delegación de autoridad empieza con la capacidad para definir qué cuentas tienen la capacidad para desempeñar ciertas acciones de gestión (por ejemplo, la creación de nuevas cuentas) o gestionar funciones específicas (tales como el cambio de contraseña de una cuenta). Por consiguiente, una vez supuesta la capacidad de delegar acciones o esfuerzos de administración, a continuación el objetivo sería proporcionar un entorno en el cual las tareas se emprendan de manera segura y responsable.

8.3.8 Cumplimiento de las políticas

En el diseño e implementación de soluciones IdM habrá que tomar en consideración el hecho de que se cumplan las políticas aplicables. En este sentido, cabe citar que el cumplimiento de las políticas guarda normalmente relación con:

- el anonimato y la privacidad;
- la creación y acopio de información de identidad;
- la utilización y difusión de información de identidad.

8.3.9 Soporte de servicios que requieren tratamiento prioritario

En el diseño e implementación de soluciones IdM habrá que tener en cuenta el soporte de servicios de aplicación y de sesiones de comunicación que requieran tratamiento prioritario, por ejemplo, servicios de telecomunicaciones de emergencia (ETS). Así, cualquier interacción con sistemas IdM que se emprenda para establecer y mantener sesiones de comunicación ETS debe ser objeto de tratamiento prioritario. Se remite al lector a [b-ITU-T E.107] y [b-ITU-T Y.2205] con propósitos de información sobre los servicios y capacidades que requieren tratamiento prioritario.

8.4 Funciones de identidad federada de la gestión de identidad

8.4.1 Identidad federada

La finalidad general de la federación es permitir que cada miembro de una federación siga siendo independiente, al paso que se facilita el intercambio de información de identidad específica para permitir la prestación de servicios federados. Así, cabe la posibilidad de federar, esto es poner a disposición de los miembros de una federación, cierta información de identidad de un usuario/abonado (por ejemplo, un subconjunto de un perfil de abonado).

8.4.2 Descubrimiento de federación

El descubrimiento de federación consiste en una serie de funciones y mecanismos encaminados a descubrir e intercambiar información de identidad federada. Así, cierta información de identidad acerca de un usuario/abonado puede federarse (por ejemplo, un subconjunto de la información sobre el perfil de un abonado).

El principal aspecto del descubrimiento de federación consiste en identificar o descubrir a un IdP candidato o al IdP que sea la fuente fidedigna de una determinada información de identidad asociada con una entidad (por ejemplo, información de ubicación).

El descubrimiento es necesario en cualquier arquitectura en que existan múltiples IdP, o respecto de la cual la ubicación de los IdP sea potencialmente dinámica. Cuando sólo exista un único proveedor de identidad (por ejemplo, una empresa) no habrá necesidad de realizar una operación de descubrimiento, ya que cualquier RP/SP sabría implícitamente dónde obtener la información de identidad de la entidad considerada.

8.4.3 Puenteo e interfuncionamiento

En general, cada proveedor, NGN empresa o miembro de una federación puede poseer sus propios formatos, planes, definiciones o semánticas, para representar datos e información relacionados con la identidad. Así, es posible representar de manera distinta utilizando dos sistemas diferentes la misma información, por ejemplo una fecha de nacimiento. Por otra parte, la semántica, los planes y los mecanismos utilizados para solicitar e intercambiar información relacionada con la identidad pueden ser diferentes, lo que da lugar a problemas de compatibilidad. En consecuencia, habrá necesidad de contar con las capacidades adecuadas para hacer posible el puenteo y el interfuncionamiento entre diversas federaciones.

8.5 Usuario y funciones de abonado de la gestión de identidad

Es necesario disponer de funciones que permitan a un usuario final/abonado proporcionar información sobre el control de su información de identidad, para ofrecer soluciones IdM eficaces. Esto incluye funciones y capacidades que habilitan a una entidad tal como un usuario final/abonado para proporcionar a proveedores de servicios e IdP, información sobre condiciones, restricciones, consentimiento y autorización referentes a la creación, acopio, utilización y difusión de su información de identidad.

Estas funciones tienen que ver con el cumplimiento de políticas aplicables tales como las que atañen a la protección de la PII y la información de identidad anónima o seudoanónima.

Las directrices que deben considerarse, versan, entre otras cosas, sobre lo siguiente:

- medios para que los usuarios/abonados envíen al proveedor NGN información acerca del control de su información de identidad;
- cumplimiento de las políticas aplicables en materia de protección de la PII;
- facilidad de utilización en favor del usuario final/abonado.

8.6 Calidad de funcionamiento y fiabilidad

8.6.1 Calidad de funcionamiento

Las capacidades y funciones IdM se utilizarán para soportar y mejorar una amplia gama de aplicaciones de negocios y seguridad. Así, cabe la posibilidad de recurrir a funciones IdM para garantizar la identidad de entidades de comunicación antes de permitir una sesión de comunicación (por ejemplo, sesiones VoIP, IPTV o de datos). Por consiguiente, las repercusiones en materia de calidad de funcionamiento que trae implícitas la IdM para los servicios de aplicación de nivel superior a los que se presta soporte (VoIP, IPTV, datos), resultan importantes si se desea garantizar la eficacia global de la solución de que se trate. Así, por ejemplo, la IdM no debe afectar negativamente los servicios de aplicaciones de alto nivel a los que se presta soporte, ya que de este modo quedarían afectadas ante todo la calidad de servicio (QoS) globales y la calidad percibida (QoE) de los usuarios finales/abonados.

Las consideraciones en cuanto a la gestión de la calidad de funcionamiento revisten importancia en los diseños de soluciones IdM. La gestión de la calidad de funcionamiento requiere, entre otras cosas, el acopio y el análisis de datos estadísticos. La supervisión de la calidad de funcionamiento es la evaluación sistemática de la capacidad de un sistema de red para llevar a cabo la función que se le haya asignado, mediante el acopio y el análisis continuos de datos idóneos sobre la calidad de funcionamiento. Los procedimientos de supervisión de la calidad de funcionamiento tienen por objeto capturar condiciones de error y perturbaciones intermitentes producidas por el deterioro gradual del equipo de red. Técnicas proactivas de mantenimiento tales como la supervisión de la calidad de funcionamiento habilitan la pronta detección de perturbaciones antes de que éstas se agudicen.

8.6.2 Exactitud de la indicación de tiempo

La exactitud de la indicación de tiempo es un factor que hay que tener presente en la IdM y la auditoría describe la forma en que se han producido los correspondientes eventos en estas tramas temporales. Las indicaciones de tiempo resultan esenciales, con propósitos de auditoría, y la calidad, si no la usabilidad, de los datos de auditoría, viene determinada por la exactitud de la indicación de tiempo.

La exactitud de las indicaciones de tiempo depende de tres factores, a saber: la precisión con la que se lea el reloj de indicación de tiempo, la sincronización del reloj local con un reloj de referencia y la incertidumbre matemática del reloj local medida sobre la base de una referencia.

8.6.3 Fiabilidad y disponibilidad

La fiabilidad y resistencia de los elementos y sistemas de una red que proporciona funciones y capacidades IdM constituyen un aspecto importante del diseño e implementación de soluciones, ya que la IdM se utilizará para soportar y mejorar una amplia gama de aplicaciones de negocios y de seguridad que pueden poseer requisitos de disponibilidad específicos. En consecuencia, habrá que considerar requisitos y directrices tales como los siguientes con respecto a los factores de fiabilidad:

- diseños de sistemas (por ejemplo, redundancia) en lo que concierne a la robustez y resistencia;
- diversidad (por ejemplo, diversidad geográfica) en materia de disponibilidad.

Aparte del diseño e implementación de soluciones IdM, debe considerarse también la adopción de medidas en relación con los límites de la seguridad. Por ejemplo, la aplicación dependiente puede permitir ciertos privilegios limitados, cuando falle o deje de estar disponible el sistema IdM considerado en su totalidad.

8.7 Seguridad IdM

8.7.1 Protección de seguridad para los elementos de red que proporcionan IdM

Dado que la información y recursos de identidad representan aplicaciones y servicios valiosos, sensibles y utilizados para soportar aplicaciones y servicios de negocios, los elementos de red que proporcionan servicios, funciones y capacidades IdM serán blanco de ataques contra la seguridad, motivo por el que requerirán protección de seguridad.

Es necesario establecer requisitos y medidas adecuadas para garantizar y proteger los elementos y sistemas de red que proporcionan funciones, servicios y capacidades IdM. Entre las consideraciones de seguridad que cabe citar figuran las siguientes:

- protección de seguridad de los servicios, funciones y capacidades IdM;
- protección de seguridad de las interfaces de señalización y comunicación;
- protección de seguridad de las interfaces de gestión de sistemas IdM (es decir, interfaces utilizadas para configurar y gestionar la información de identidad).

8.7.2 Protección de información de identificación personal (PII)

La protección de esta información es un aspecto de la IdM que reviste gran importancia. Deben definirse e implementarse capacidades específicas para proteger la PII. Esto guarda relación con el cumplimiento de la política aplicable en materia de protección de la PII, con sujeción a los reglamentos nacionales y regionales. Entre las funciones y capacidades que habrá que tener en cuenta pueden citarse las siguientes:

- capacidades para que los usuarios/abonados comuniquen sus preferencias en relación con la PII;
- capacidades para proporcionar transparencia (es decir, capacidades que garanticen que sólo las entidades autorizadas tengan acceso a la PII o puedan observar la PII);
- capacidades para proporcionar notificaciones sobre la difusión y utilización y el empleo de información de identidad.

Bibliografía

[b-ITU-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-ITU-T E.115] Recomendación UIT-T E.115 ITU-T E.115 (2008), *Asistencia informatizada sobre directorios*.

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

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

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

[b-ITU-T X.811] Recomendación UIT-T X.811 (1995) | ISO/IEC 1081-2:1996, *Tecnología de la información – Interconexión de sistemas abiertos – Marcos de seguridad para sistemas abiertos: marco de autenticación*.

[b-ITU-T X.911] Recomendación UIT-T X.911 (2005) | ISO/IEC 15414:2006, *Tecnología de la información – Procesamiento distribuido abierto – Modelo de referencia – Lenguaje de empresa*.

[b-ITU-T X.1121] Recomendación UIT-T X.1121 (2004), *Marco general de tecnologías de seguridad para las comunicaciones móviles de datos de extremo a extremo*.

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

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

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

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

[b-ITU-T Y.2205] Recomendación UIT-T Y.2205 (2008), *Redes de la próxima generación – Telecomunicaciones de emergencia – Consideraciones técnicas*.

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

[b-ITU-T Y.2702] Recomendación UIT-T Y.2702 (2008), *Requisitos de autentificación y autorización para las NGN, versión 1*.

[b-ETSI EG 202 072] ETSI EG 202 072, V1.1.1 (2002), *Universal Communications identifier (UCI); Placing UCI in context; Review and analysis of existing identification schemes*.
<http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=14108>

[b-ETSI EG 202 236] ETSI EG 202 236, V1.1.1 (2003), *Telecommunications and Internet Protocol Harmonization Over Networks (TIPHON)*; *Design guide; Use of non-numeric names*.
<http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=17732>

[b-ETSI EG 284 004] ETSI EG 284 004, V1.1.2 (2007), *Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Incorporating Universal Communications Identifier (UCI) support into the specification of Next Generation Networks*.
<http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=21139>

[b-ETSI TS 102 042] ETSI TS 102 042, V1.3.4 (2007), *Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates*.
<http://webapp.etsi.org/workprogram/Report_WorkItem.asp?WKI_ID=27736>

[b-RFC 3650] IETF RFC 3650 (2003), *Handle System Overview*.
<http://www.ietf.org/rfc/rfc3650.txt?number=3650>

[b-NIST] NIST SP800-63, v6.3.3, *Electronic Authentication Guidelines.*
<http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf>

[b-OGIM] The Open Group, *Identity Management White Paper* (03/2004).
<http://www.opengroup.org/bookstore/catalog/w041.htm>

SERIES DE RECOMENDACIONES DEL UIT-T

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

Impreso en Suiza
Ginebra, 2010