

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1252

(04/2010)

SERIE X: REDES DE DATOS, COMUNICACIONES DE
SISTEMAS ABIERTOS Y SEGURIDAD

Seguridad en el ciberespacio – Gestión de identidades

**Términos y definiciones de referencia para la
gestión de la identidad**

Recomendación UIT-T X.1252

RECOMENDACIONES UIT-T DE LA SERIE X
REDES DE DATOS, COMUNICACIONES DE SISTEMAS ABIERTOS Y SEGURIDAD

REDES PÚBLICAS DE DATOS	X.1–X.199
INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.200–X.299
INTERFUNCIONAMIENTO ENTRE REDES	X.300–X.399
SISTEMAS DE TRATAMIENTO DE MENSAJES	X.400–X.499
DIRECTORIO	X.500–X.599
GESTIÓN DE REDES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS Y ASPECTOS DE SISTEMAS	X.600–X.699
GESTIÓN DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.700–X.799
SEGURIDAD	X.800–X.849
APLICACIONES DE INTERCONEXIÓN DE SISTEMAS ABIERTOS	X.850–X.899
PROCESAMIENTO DISTRIBUIDO ABIERTO	X.900–X.999
SEGURIDAD DE LA INFORMACIÓN Y DE LAS REDES	
Aspectos generales de la seguridad	X.1000–X.1029
Seguridad de las redes	X.1030–X.1049
Gestión de la seguridad	X.1050–X.1069
Telebiometría	X.1080–X.1099
APLICACIONES Y SERVICIOS CON SEGURIDAD	
Seguridad en la multidifusión	X.1100–X.1109
Seguridad en la red residencial	X.1110–X.1119
Seguridad en las redes móviles	X.1120–X.1139
Seguridad en la web	X.1140–X.1149
Protocolos de seguridad	X.1150–X.1159
Seguridad en las comunicaciones punto a punto	X.1160–X.1169
Seguridad de la identidad en las redes	X.1170–X.1179
Seguridad en la TVIP	X.1180–X.1199
SEGURIDAD EN EL CIBERESPACIO	
Ciberseguridad	X.1200–X.1229
Lucha contra el correo basura	X.1230–X.1249
Gestión de identidades	X.1250–X.1279
APLICACIONES Y SERVICIOS CON SEGURIDAD	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1339
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	
Intercambio de estados/vulnerabilidad	X.1520–X.1539
Intercambio de eventos/incidentes/eurística	X.1540–X.1549
Intercambio de políticas	X.1550–X.1559
Petición de eurística e información	X.1560–X.1569
Identificación y descubrimiento	X.1570–X.1579
Intercambio asegurado	X.1580–X.1589

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

Recomendación UIT-T X.1252

Términos y definiciones de referencia para la gestión de la identidad

Resumen

La Recomendación UIT-T X.1252 contiene las definiciones de los principales términos utilizados en la gestión de la identidad (IdM). Los términos proceden de muchas fuentes y se utilizan corrientemente en el contexto de IdM. La presente Recomendación no tiene por objeto constituir un compendio exhaustivo de los términos relacionados con la IdM, sino más bien recopilar una lista básica de los términos que se consideran más importantes y que se utilizan habitualmente en el contexto de la IdM. En el Anexo A a la presente Recomendación se explican las razones por las que algunos de estos términos son tan importantes.

Uno de los principales objetivos de la presente Recomendación es armonizar el significado de estos términos entre los grupos que se dedican al desarrollo de normas sobre IdM (o tienen previsto dedicarse a ello). Se ha tratado de que, en la medida de lo posible, las definiciones sean independientes de la realización o el contexto concretos y, por ende, puedan constituir un conjunto básico de definiciones para cualquier trabajo en el ámbito de la IdM. Se reconoce que, en algunos casos y contextos, puede requerirse una definición más detallada de un determinado término, en cuyo caso, se podría considerar la posibilidad de desarrollar la definición básica.

Historia

Edición	Recomendación	Aprobación	Comisión de estudios
1.0	ITU-T X.1252	2010-04-16	17

PREFACIO

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

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

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

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

NOTA

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

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

PROPIEDAD INTELECTUAL

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

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

© 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.....	1
4 Abreviaturas y acrónimos	2
5 Convenios	2
6 Términos y definiciones	2
Anexo A – Aspectos principales y razón de ser de la terminología básica IdM.....	7
A.1 Autenticación y confianza.....	7
A.2 Declaración/aseveración.....	12
A.3 Inscripción y registro	12
A.4 Proveedor de identidad y proveedor de servicio de identidad.....	13
A.5 Pauta de identidad.....	13
Bibliografía	15

Introducción

Esta lista de términos y definiciones IdM se comenzó a compilar en 2007. Desde entonces han habido varias versiones y se han recibido numerosos comentarios y contribuciones al respecto y la lista ha sido revisada varias veces. Los términos y definiciones proceden de muy diversas fuentes, algunas de las cuales, pero no todas, se enumeran en la Bibliografía. En algunos casos la definición original era la adecuada y se incluyó tal cual, pero en muchos otros fue necesario modificarla o fusionarla con otras para obtener la "más correcta" para cada término.

Se veló en particular por que las definiciones tengan idéntico significado en todas las demás Recomendaciones | Normas Internacionales sobre IdM. Aunque en algunos casos las palabras utilizadas no sean las mismas, el significado sí lo es.

Puesto que un término se utiliza en diferentes contextos, las definiciones se limitan a una descripción básica o sencilla del término, sin incluir las alternativas o variaciones que pudieran existir. En caso necesario se puede incluir alguna aclaración o información adicional.

Los aspectos fundamentales en los que se basan las definiciones se analizan detalladamente en el Anexo A.

Recomendación UIT-T X.1252

Términos y definiciones de referencia para la gestión de la identidad

1 Alcance

La presente Recomendación contiene una compilación de términos y definiciones que se utilizan normalmente para la gestión de la identidad (IdM). Las definiciones proporcionan una definición básica del término, es decir que están destinadas a transmitir el significado fundamental, aunque excepcionalmente se incluye una nota para aclarar la definición.

NOTA – En la presente Recomendación la utilización del término "identidad" en relación con la IdM no alude a su significado absoluto y no constituye, en particular, ninguna 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 alienta a los usuarios de esta Recomendación a que 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 la presente Recomendación, la referencia a un documento no confiere a este último, como documento autónomo, la categoría de una Recomendación.

- [UIT-T X.501] Recomendación UIT-T X.501 (2005) | ISO/CEI 9594-2:2005, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Modelos.*
- [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.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 autenticación.*
- [UIT-T Y.2701] Recomendación UIT-T Y.2701 (2007), *Requisitos de seguridad para las redes de la próxima generación, versión 1.*
- [UIT-T Y.2702] Recomendación UIT-T Y.2702 (2008), *Requisitos de autenticación y autorización en las redes de próxima generación versión 1.*
- [UIT-T Y.2720] Recomendación UIT-T Y.2720 (2009), *Marco general para la gestión de identidades en la red de la próxima generación.*

3 Definiciones

Este párrafo se deja deliberadamente en blanco.

4 Abreviaturas y acrónimos

En esta Recomendación se utilizan las siguientes siglas y acrónimos:

IdM	Gestión de identidad (<i>identity management</i>)
IdP	Proveedor de identidad (<i>identity provider</i>)
IdSP	Proveedor de servicio de identidad (<i>identity service provider</i>)
NGN	Red de la próxima generación (<i>next generation network</i>)
PII	Información de identificación personal (<i>personally identifiable information</i>)
RP	Parte retransmisora (<i>relying party</i>)

5 Convenios

Este párrafo se deja deliberadamente en blanco.

6 Términos y definiciones

6.1 control de acceso (*access control*): Procedimiento utilizado para determinar si se debe conceder a una entidad acceso a recursos, instalaciones, servicios o informaciones, sobre la base de normas preestablecidas, y la autoridad o los derechos específicos asociados a la parte solicitante.

6.2 dirección (*address*): Identificador de un punto de terminación específico (y se utiliza para el encaminamiento hacia ese punto de terminación).

6.3 agente (*agent*): Una entidad que actúa en nombre de otra entidad.

6.4 alianza (*alliance*): Un acuerdo entre dos o más entidades independientes a tenor del cual se define cómo éstas deben relacionarse entre sí y llevar a cabo actividades conjuntas.

6.5 anonimato (*anonymity*): Situación en la que una entidad no puede ser identificada dentro de un conjunto de entidades.

NOTA – El anonimato impide el rastreo de entidades o de su comportamiento, como por ejemplo la localización del usuario, la frecuencia de utilización de un servicio, y así sucesivamente.

6.6 aseveración (*assertion*): Declaración hecha (por una entidad) sin presentar evidencias de su validez¹.

6.7 garantía (*assurance*): Véase garantía de autenticación y garantía de identidad.

6.8 nivel de garantía (*assurance level*): Nivel de confianza en la vinculación entre una entidad y la información de identidad presentada.

6.9 atributo (*attribute*): Información relacionada con una entidad que especifica una característica de la entidad.

6.10 tipo de atributo (*attribute type*) [UIT-T X.501]: Aquel componente de un atributo que indica la clase de información que proporciona dicho atributo.

6.11 valor de atributo (*attribute value*) [UIT-T X.501]: Una instancia particular de la clase de información que indica un tipo de atributo.

6.12 autenticación (de entidad) (*entity authentication*): Proceso utilizado para obtener una confianza suficiente en la vinculación entre la entidad y la identidad presentada.

¹ Hay acuerdo en que los términos aseveración y declaración son muy similares.

NOTA – En el contexto de la gestión de identidad (IdM) se entiende que el término autenticación se refiere a la autenticación de una entidad.

6.13 garantía de autenticación (*authentication assurance*): Grado de confianza a la que se llega en el proceso de autenticación de que el asociado de la comunicación es la entidad que declara ser o se espera que sea.

NOTA – La confianza se basa en el grado de confianza de la relación entre la entidad que comunica y la entidad que está presente.

6.14 autorización (*authorization*) [UIT-T Y.2720] y [UIT-T X.800]: Concesión de derechos y, sobre la base de esos derechos, concesión de acceso.

6.15 vinculación (*binding*): Una asociación, atadura o lazo explícitamente establecido.

6.16 Reconocimiento biométrico (*biometric recognition*) [b-ISO/CEI CD 2382-37]: Reconocimiento automático de personas basado en la observación de sus características biológicas y conductuales.

6.17 certificado (*certificate*) [UIT-T X.810]: Conjunto de datos relacionados con la seguridad transmitidos por una autoridad responsable de la seguridad o una tercera parte facultada para ello, junto con la información sobre seguridad que se utiliza para proporcionar los servicios de autenticación de la integridad y el origen de los datos.

6.18 declaración (*claim*) [b-OED]: Declarar que es el caso, sin estar en condiciones de proporcionar pruebas¹.

6.19 declarante (*claimant*) [UIT-T Y.2720] y [UIT-T X.811]: Entidad que es la principal o la representa a los efectos de la autenticación.

NOTA – Un declarante desempeña las funciones necesarias para participar en intercambios de autenticación en nombre de un principal.

6.20 contexto (*context*): Entorno con fronteras definidas en el cual existen e interactúan las entidades.

6.21 credencial (*credential*): Conjunto de datos presentado como evidencia de una identidad y/o unos derechos declarados.

6.22 delegación (*delegation*): Acción mediante la cual se asigna una autoridad, responsabilidad o función a otra entidad.

6.23 identidad digital (*digital identity*): Representación digital de la información conocida acerca de un particular, un grupo o una organización concretos.

6.24 inscripción (*enrolment*): Proceso de inauguración de una entidad en un contexto.

NOTA 1 – La inscripción podría incluir la verificación de la identidad de la entidad y el establecimiento de una identidad contextual.

NOTA 2 – Asimismo, la inscripción es un prerrequisito para el registro. En muchos casos esta última expresión se utiliza para describir ambos procesos.

6.25 entidad (*entity*): Cualquier cosa que tenga una existencia autónoma y bien definida y pueda ser identificada en contexto.

NOTA – Una entidad puede ser una persona física, un animal, una persona jurídica, una organización, una cosa activa o pasiva, un dispositivo, una aplicación informática, un servicio, etc., o un grupo de estos elementos. En el contexto de las telecomunicaciones, como ejemplos de entidades cabe mencionar puntos de acceso, abonados, usuarios, elementos de red, redes, aplicaciones informáticas, servicios y dispositivos, interfaces, etc.

6.26 autenticación de entidad (*entity authentication*): Proceso encaminado a lograr suficiente confianza en la vinculación entre la entidad y la identidad presentada.

NOTA – En un contexto la gestión de identidad (IdM) se entiende que el término autenticación se refiere a la autenticación de una entidad.

6.27 federación (*federation*): Una asociación de usuarios, proveedores de servicios y proveedores de servicios de identidad.

6.28 identificación (*identification*): Proceso conducente a reconocer a una entidad por sus características contextuales.

6.29 identificador (*identifier*): Uno o más de los atributos utilizados para identificar a una entidad dentro de un contexto.

6.30 identidad (*identity*): Representación de una entidad bajo la forma de uno o varios atributos que permiten distinguir suficientemente a la entidad o entidades dentro del contexto. A los efectos de la gestión de identidad (IdM), se entiende que este término constituye una identidad contextual (subconjunto de atributos), es decir que la diversidad de atributos está limitada por un marco con fronteras definidas (el contexto) en el cual existe e interactúa la entidad.

NOTA – Cada entidad está representada por una identidad holística, que comprende todos los posibles elementos de información que caracterizan a dicha entidad (los atributos). Sin embargo, la identidad holística es una cuestión teórica y elude cualquier descripción y utilización práctica, dado que el número de todos los atributos posibles es indefinido.

6.31 garantía de identidad (*identity assurance*): El grado de confianza en el proceso de validación y verificación de la identidad utilizado para determinar la identidad de la entidad para la cual se expide la credencial, y el grado de confianza en que la entidad que utiliza la credencial es dicha entidad o la entidad a la cual se le expidió o asignó la credencial.

6.32 política de seguridad basada en la identidad (*identity-based security policy*) [UIT-T X.800]: Una política de seguridad basada en las identidades y/o los atributos de los usuarios, grupos de usuarios o entidades que actúan en nombre de los usuarios y los recursos/objetos a los que se tiene acceso.

6.33 proveedor intermediario de servicio de identidad (*identity service bridge provider*): Proveedor de servicio de identidad que actúa como intermediario fiable entre otros proveedores de identidad.

6.34 gestión de identidad (IdM) (*identity management*) [UIT-T Y.2720]: 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 que interviene en aplicaciones comerciales y de seguridad.

6.35 pauta de identidad (*identity pattern*): Una expresión estructurada de atributos de una entidad (por ejemplo, el comportamiento de una entidad) que podría utilizarse en algunos procesos de identificación.

6.36 demostración de identidad (*identity proofing*): Proceso mediante el cual se valida y verifica información suficiente como para confirmar la identidad alegada por la entidad.

6.37 proveedor de identidad (IdP) (*identity provider*): Véase proveedor de servicio de identidad (IdSP).

6.38 proveedor de servicio de identidad (IdSP) (*identity service provider*): Entidad que verifica, mantiene, gestiona y puede crear y asignar información de identidad de otras entidades.

6.39 verificación de identidad (*identity verification*): Proceso a tenor del cual se confirma que la identidad declarada es correcta mediante la comparación de las declaraciones de identidad ofrecidas con información previamente demostrada.

6.40 manifestación (*manifestation*): Una representación observada o descubierta (es decir, no autoaseverada) de una entidad. (Comparar con aseveración.)

6.41 autenticación mutua (*mutual authentication*): Proceso a tenor del cual dos entidades (como por ejemplo un cliente y un servidor) se autentican entre sí de modo que cada uno de ellos está seguro de la identidad del otro.

6.42 nombre (*name*) [UIT-T Y.2091]: Expresión por la que se conoce o se hace referencia a una entidad.

NOTA – El nombre se utiliza en un determinado contexto y no puede suponerse que sea singular o no ambiguo. A los efectos de encaminamiento, puede ser resuelto o traducido en una dirección.

6.43 no repudio (*non-repudiation*): Capacidad para conferir protección contra la denegación por parte de una de las entidades que intervienen en una acción o han participado en la totalidad o parte de la acción.

6.44 pauta (*pattern*): Véase pauta de identidad.

6.45 persistente (*persistent*): Existente y apto para ser utilizado en servicios fuera del control directo del asignador que expide, sin un límite de tiempo estatuido.

6.46 información de identificación personal (PII) (*personally identifiable information*): Toda información a) que identifica a una persona y que puede utilizarse para identificar, contactar o localizar a la misma; b) que puede utilizarse para obtener información de identificación o de contacto sobre una determinada persona; c) que puede relacionarse directa o directamente con una persona .

6.47 principal (*principal*) [UIT-T Y.2720], [UIT-T X.811] y [UIT-T Y.2702]: Una entidad cuya identidad puede ser autenticada.

6.48 privacidad (*privacy*): Derecho de los particulares de controlar la información personal relacionada con ellos que se puede compilar, gestionar, retener y utilizar o distribuir, o de influir en dicha información.

6.49 política de privacidad (*privacy policy*): Política que define los requisitos para proteger el acceso a la información de identificación personal (PII) y la divulgación de la misma, así como los derechos de los particulares con respecto a la forma en la que se utiliza su información personal.

6.50 privilegio (*privilege*): Derecho que, una vez concedido a una entidad, le permite llevar a cabo un acto.

6.51 demostración (*proofing*): Verificación y validación de la información cuando se inscriben nuevas entidades en los sistemas de identidad.

6.52 seudónimo (*pseudonym*): Un identificador cuya vinculación con una entidad no se conoce o sólo se conoce hasta cierto grado dentro del contexto en el cual se utiliza.

NOTA – Los seudónimos pueden utilizarse para evitar o reducir los riesgos relativos a la privacidad que entraña la utilización de relaciones de identificador que pueden revelar la identidad de la entidad.

6.53 registro (*registration*): Proceso a tenor del cual una entidad solicita un privilegio para utilizar un servicio o un recurso y se le asigna dicho privilegio.

NOTA – La inscripción es un prerrequisito para el registro. Las funciones de inscripción y registro pueden estar combinadas o separadas.

6.54 parte confiante (RP) (*relying party*) [UIT-T Y.2720]: Entidad que confía en la representación o declaración de identidad de una entidad solicitante/aseverante en un contexto de petición.

6.55 repudio (*repudiation*): Denegación de haber participado en la totalidad o parte de una acción por parte de una de las entidades que intervienen en la misma.

6.56 entidad solicitante (*requesting entity*): Entidad que hace una representación o declaración de identidad a una parte confiante dentro de algún contexto de petición.

6.57 revocación (*revocation*): La anulación por alguien con la autoridad necesaria de algo efectuado previamente.

6.58 función (*role*): Serie de propiedades o atributos que describen las capacidades o las funciones que puede desempeñar una entidad.

NOTA – Cada entidad puede tener/desempeñar varias funciones. Las capacidades pueden ser inherentes o asignadas.

6.59 auditoría de seguridad (*security audit*) [UIT-T X.800]: Análisis y examen independiente de las actividades y registros del sistema con miras a ensayar el buen funcionamiento de sus controles para garantizar la observancia de los procedimientos de explotación y política establecidos, detectar fallos en la seguridad y recomendar cualesquiera cambios pertinentes en materia de control, política y procedimientos.

6.60 dominio de seguridad (*security domain*) [UIT-T Y.2720], [UIT-T Y.2701] y [UIT-T X.810]: Un conjunto de elementos, una política de seguridad, una autoridad responsable de la seguridad y un conjunto de actividades relacionadas con la seguridad cuyos elementos se gestionan de conformidad con la política de seguridad.

6.61 zona de seguridad (*security zone*) [UIT-T Y.2701]: Una zona protegida definida mediante control operacional, ubicación y conectividad a otros dispositivos/elementos de red.

6.62 autoridad de dominio de seguridad (*security domain authority*) [UIT-T X.810]: Una autoridad encargada de la seguridad que también es responsable de la implementación de una política de seguridad en un dominio de seguridad.

6.63 identidad autoaseverada (*self-asserted identity*): La entidad que asevera la propia entidad.

6.64 confianza (*trust*): Firme creencia en la fiabilidad y veracidad de la información, o en la habilidad y disposición de una entidad para actuar adecuadamente dentro de un contexto especificado.

6.65 nivel de confianza (*trust level*): Un grado coherente y cuantificable de fiabilidad en el carácter, la aptitud, la solidez o veracidad de alguien o algo.

6.66 tercera parte fiable (*trusted third party*) [UIT-T Y.2702], [UIT-T X.800] y [UIT-T X.810]: En el contexto de una política de seguridad, la autoridad responsable de la seguridad o su agente, que es fiable con respecto a algunas actividades relacionadas con la seguridad.

6.67 usuario (*user*): Entidad que utiliza un recurso, por ejemplo sistemas, equipos, terminales, procesos, aplicaciones o redes empresariales.

6.68 centrado en el usuario (*user-centric*): Un sistema de gestión de identidad (IdM) que puede proporcionar al usuario la capacidad de controlar y hacer cumplir diversas políticas de privacidad y seguridad que rigen el intercambio de información sobre identidad, en particular la información de identificación personal del usuario.

6.69 verificación (*verification*): Proceso o instancia que determina la autenticidad de algo.

NOTA – La verificación de la información (de identidad) puede implicar un análisis en lo que respecta a la validez, la fiabilidad de la fuente, lo original (inalterado), la corrección, la relación con la entidad, etc.

6.70 verificador (*verifier*): Entidad que verifica y valida la información sobre identidad.

Anexo A

Aspectos principales y razón de ser de la terminología básica IdM

(Este anexo forma parte integrante de la presente Recomendación)

Antecedentes

En el curso de los debates sobre gestión de identidad (IdM) se han descrito las diferentes maneras de comprender la intención de la IdM, los procedimientos básicos utilizados, la terminología y las definiciones de términos. Estas diferencias han dado lugar a equívocos y a prolongadas deliberaciones durante el proceso de normalización IdM.

Para evitar que esos malentendidos se reiteren en el futuro, en el presente anexo se consideran algunos de los acuerdos a los que se llegó durante los debates entablados en el UIT-T sobre esa terminología y esos conceptos básicos y se explican las reflexiones que llevaron a acuñar (o en algunos casos a adoptar) los términos incluidos en esta Recomendación. Tenga a bien tomar nota de que este anexo no abarca ni explica la visión holística de la gestión de identidades.

Introducción

Identidad es el término alrededor del cual giran todos los otros términos IdM. En el mundo real, más que en el mundo digital, por ejemplo, la identidad en la persona natural se acepta sin ambages y se fundamenta en toda una serie de características o atributos. En algunos casos se trata de rasgos físicos como la altura, el color del cabello, la apariencia general, los modales, el comportamiento, etc. En otros se puede aludir a la fecha de nacimiento, el lugar de nacimiento, la dirección de su casa o el número de teléfono. Normalmente en un proceso de comunicación ambas partes deben tener suficiente confianza en que se están comunicando con la parte correcta. En este proceso de buscar ese grado de confianza normalmente participan dos o más particulares o "entidades": la entidad cuya identidad debe confirmarse – la *entidad solicitante* – y la entidad que se fiará en una identidad confirmada – la *parte confiante*. En este proceso puede intervenir una tercera entidad que gestiona las identidades: el *proveedor del servicio de identidad*.

En el mundo digital o "en línea", una "identidad" también está formada de atributos, al igual que en el mundo real. Sin embargo, en este caso la "identidad" puede limitarse a una única característica o puede tener muchas; eso dependerá del contexto en el que aparece. Esto se aplica tanto a los objetos inanimados como a las personas naturales, de modo que a menudo se hace referencia a los usuarios como si fuesen entidades.

Por lo general los identificadores y/o atributos caracterizarán únicamente a una entidad dentro de un contexto particular. A causa de ello, una entidad podría tener cierto número de identidades diferentes, algunas de las cuales serían un subconjunto de otras identidades.

A.1 Autenticación y confianza

El proceso de autenticación es una parte importante de la IdM. Las consideraciones que figuran a continuación ayudan a explicar el proceso de autenticación y su pertinencia para la confianza.

Cabe señalar que, al aplicar este modelo a los procedimientos y aplicaciones reales, hay que tener muy en claro cuáles son los correspondientes asociados en la comunicación y las cadenas de confianza aplicables.

El proceso de autenticación podría describirse como sigue:

La mayoría de los procesos de comunicación exigen que los asociados en la comunicación tengan un grado de confianza suficiente en que se están realmente comunicando con el asociado previsto. Por lo tanto, al comienzo de la comunicación, los asociados tratan de llegar a un grado adecuado de confianza sobre la base de la información sobre identidad disponible del asociado, es decir, confianza en la vinculación entre la entidad y la identidad presentada.

El proceso de establecer confianza reviste particular importancia cuando los asociados en la comunicación se encuentran lejos uno del otro y están conectados únicamente por un enlace de telecomunicaciones. El proceso de autenticación se ejecuta con miras a determinar, con un suficiente grado de confianza, que la identidad presentada por un asociado en la comunicación realmente le pertenece al mismo.

Una comunicación siempre implica que dos o más asociados distintos intercambian información. A causa de la amplia diversidad de asociados posibles (por ejemplo, humanos y cosas), es preciso definir un término general. El término elegido es *entidad*, la cual se define como: algo que tenga una existencia separada y bien definida y pueda identificarse en contexto.

NOTA:

- Una entidad puede ser una persona física, un animal, una persona jurídica, una organización, una cosa activa o pasiva, un dispositivo, una aplicación informática, un servicio, etc., o un grupo de estos elementos.
- En el contexto de las telecomunicaciones, cabe citar como ejemplos de entidades puntos de acceso, abonados, usuarios, elementos de red, redes, aplicaciones informáticas, servicios y dispositivos, interfaces, etc.

La información que puede utilizarse para la identificación de una entidad está basada en los atributos de dicha entidad. Se define un *atributo* como: la información inherente a una entidad que especifica una característica de esa entidad. En términos prácticos, la identificación de una entidad normalmente se basa en un subconjunto de sus atributos, puesto que la identificación se ve limitada por lo que se llama contexto, dentro del cual la entidad existe e interactúa. Cuanto más reducido sea el contexto y más clara sean las condiciones fronterizas, menor será el número de atributos necesarios para la identificación. El *contexto* se define como: entorno con unas condiciones fronterizas definidas en el cual la entidad existe e interactúa.

Dado que la definición de una entidad está basada en la capacidad de ser identificada, es necesario disponer de una definición clara de *identificación*: el proceso a tenor del cual se reconoce a una entidad tal como está caracterizada dentro del contexto.

Para hacer una distinción entre las entidades, basta con utilizar un subconjunto de los atributos que sea adecuado para el contexto. Esto se conoce como la *identidad*, que está definida de la siguiente manera: la representación de una entidad bajo la forma de uno o varios atributos que permiten distinguir suficientemente a las entidades dentro del contexto. A los efectos de la IdM, se entiende que el término identidad se refiere a una identidad contextual (subconjunto de atributos), es decir que la diversidad de atributos está limitada por un marco con unas condiciones de frontera definidas (el contexto) en el cual la entidad existe e interactúa.

Una identidad puede ser un subconjunto de otra identidad. También puede haber intersecciones de identidades. Sin embargo, por diversas razones (tales como las consideraciones relativas a la privacidad), se puede evitar explícitamente o incluso excluir la intersección de identidades, utilizada con diferentes finalidades o en diferentes contextos.

En la figura A.1 se muestran las relaciones entre entidad, identidades y atributos.

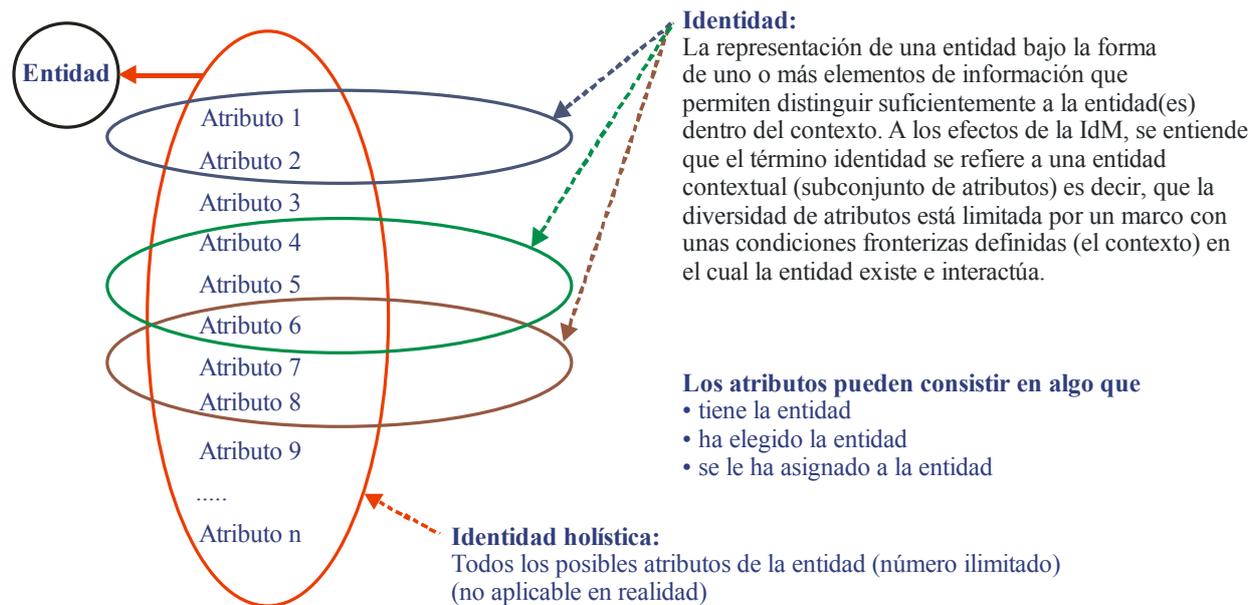


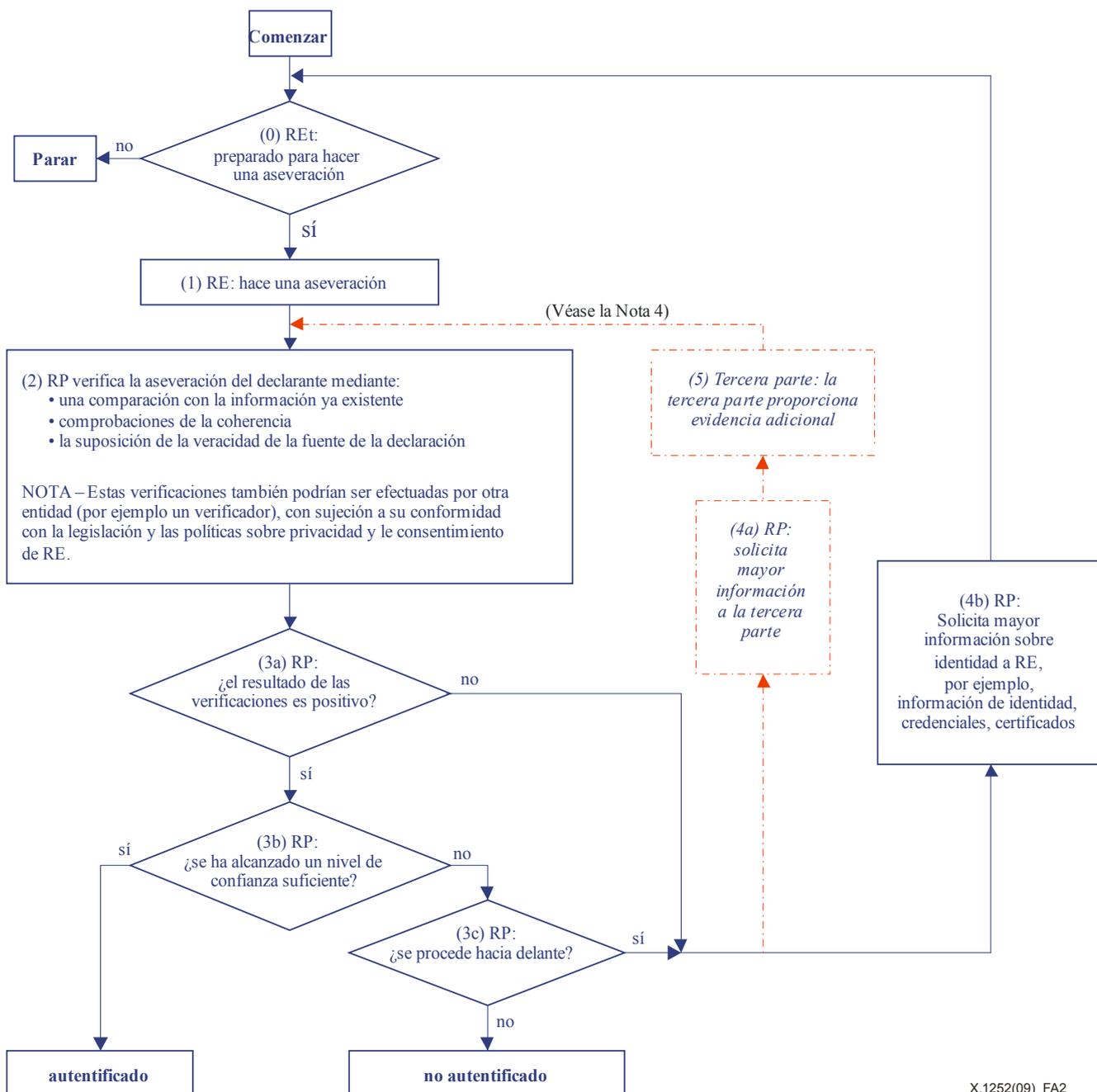
Figura A.1 – Relaciones entre entidad, identidades y atributos

Como ya se indicó, la autenticación es pertinente para la gestión de identidades. Se trata del proceso necesario para lograr un grado de confianza suficiente en que la comunicación se está efectuando con el asociado previsto. El nivel real de confianza necesaria dependerá de la sensibilidad de la aplicación y/o el riesgo de consiguientes daños por el hecho de entrar en comunicación con un asociado erróneo.

Se pueden asignar derechos o privilegios con diversas finalidades, como por ejemplo las siguientes:

- compartir o proporcionar información que no se desea poner a disposición de todo el mundo;
- conceder acceso a:
 - información;
 - salas/zonas/dominios;
 - servicios;
 - recursos;
- concertar contratos.

Para obtener ese grado de confianza es necesario que el asociado en la comunicación pueda distinguirse claramente de otros posibles asociados y que esa distinción pueda volver a hacerse periódicamente según las necesidades.



X.1252(09)_FA2

NOTA 1 – En esta figura se ilustra el proceso de autenticación unidireccional básico. Por lo general este proceso se ejecuta mutuamente de manera paralela y/o entrelazada.
 NOTA 2 – Si no se exige ningún nivel de confianza, se puede saltar el paso 2.
 NOTA 3 – Este flujo puede realizarse múltiples veces y esas reiteraciones también pueden estar separadas en el tiempo y/o en el espacio.
 NOTA 4 – La intervención de una tercera parte está sujeta a la conformidad con las políticas y la legislación sobre privacidad y el consentimiento de R. (- - - - -)

Figura A.2 – Proceso de autenticación unidireccional

En general este proceso de adquirir confianza, es decir el proceso de autenticación, se realiza mutuamente. Esto significa que el proceso de autenticación que se ilustra en la figura A.2 se realiza dos veces con cada una de las entidades que actúan en cada función, es decir:

Autenticación de Y: La entidad Y actúa como entidad solicitante (RE) y la entidad X actúa como parte confiante (RP).

Autenticación de X: La entidad X actúa como entidad solicitante y la entidad Y como parte confiante.

Con miras a simplificar el proceso y facilitar su comprensión, el proceso de autenticación que se ilustra en la figura A.2 está descrito únicamente en una dirección. No obstante, los flujos de estos dos procesos están entrelazados.

La ejecución entrelazada permite a las partes verificar las condiciones previas antes de presentar atributos posiblemente confidenciales. Esas condiciones pueden ser las siguientes:

- conocimiento de cómo dirigirse a la parte confiante,
- suficiente confianza en que la parte confiante es la correcta (por ejemplo, los usuarios deben tener cierta confianza de que se encuentran en la página web adecuada antes de proporcionar información de identidad tal como el nombre de usuario y la contraseña).

En algunos casos (pero no en los sistemas centrados en el usuario) puede participar directamente una tercera parte para proporcionar información adicional, a título de evidencia, a la parte confiante, para aumentar la confianza en los atributos de la entidad solicitante.

Las identidades están compuestas de atributos, los cuales pueden ser algo que:

- la entidad tiene (por ejemplo, tarjeta codificada);
- la entidad conoce (por ejemplo, contraseña);
- la entidad es (por ejemplo, color, tamaño);
- la entidad es capaz de hacer (por ejemplo, una encriptación específica) ;
- indica la ubicación de la entidad;
- es una combinación de los anteriores atributos.

Las identidades pueden verificarse mediante:

- la coherencia de la propia información;
- la coherencia con otra información justificativa;
- una comparación con informaciones ya conocidas.

Los atributos también pueden especificarse en términos de una *pauta de identidad*, que es una expresión estructurada de los atributos de una entidad (por ejemplo, el comportamiento de una entidad) que puede utilizarse en algunos procesos de identificación.

Cabe destacar en particular que, según se ilustra en el diagrama de la figura A.2, siempre corresponde a la RP decidir si acepta o no a la entidad solicitante sobre la base del proceso de autenticación. Ninguna otra parte puede tomar esa decisión.

En general, todo asociado en una comunicación debe estar en condiciones de fijar el nivel de confianza necesario para permitir la ejecución de privilegios. Sin embargo, ese derecho puede verse limitado – y en algunos casos debe estar limitado – por la legislación.

Cuando existe una asimetría apreciable entre los asociados en la comunicación se corre el peligro particular de que el asociado más poderoso aproveche equívocamente esa situación y exija un nivel insuficientemente elevado de confianza o rechace su propia autenticación. Por lo tanto, es necesario que las implementaciones técnicas de los mecanismos de autenticación estén basadas en mecanismos simétricos para evitar la asimetría. Además, podría ser necesario formular reglamentaciones para impedir que una parte aproveche indebidamente su situación de dominancia en condiciones asimétricas.

Por lo general cuando se solicita la gestión de identidad, es necesario ser muy claro respecto de las entidades involucradas y su finalidad, de modo que el contexto y las identidades (conjunto de atributos) puedan limitarse a esa finalidad específica.

Para alcanzar el nivel de confianza necesario con fines exclusivamente de telecomunicación, por lo general basta con que el cliente tenga suficiente confianza en estar conectado con el proveedor de servicio o transporte previsto y que los proveedores tengan confianza en que la utilización de los

servicios está autorizada, puede facturarse y debe ser pagada. Esto último puede lograrse mediante la autenticación o, por ejemplo, una cuenta de abonado o un punto de acceso, los cuales no tienen por qué ser forzosamente idénticos al usuario real del servicio o una referencia al mismo. En algunos casos, como ocurre con las tarjetas telefónicas de previo pago o las tarjetas SIM de previo pago, no se necesita autenticación alguna.

Durante el proceso de autenticación se puede presentar una credencial como evidencia de algunos o la totalidad de los atributos de una identidad contextual presentada. Se define como *credencial* un conjunto de datos presentados como evidencia de una identidad y/o derechos/declarados. Sin embargo, es necesario hacer una clara distinción entre dos tipos de credencial:

- 1) un conjunto de datos presentados como evidencia de una identidad declarada, que es pertinente a los efectos de la autenticación (por ejemplo, un pasaporte). Este tipo de credencial se utiliza para aumentar el grado de confianza en los atributos mediante la confirmación por la parte que expide la credencial; y
- 2) un conjunto de datos presentados como evidencia de derechos, que es pertinente únicamente con fines de autorización (por ejemplo, el billete para un concierto o un partido de fútbol). Éste permite ejercer un privilegio (como ser admitido a un evento por el hecho de tener un billete de entrada) sin revelar necesariamente la identidad de la entidad que presenta la credencial.

Algunas credenciales pueden incluir ambas funciones y ambos tipos de credencial podrían estar sujetos a procesos de autenticación distintos.

A.2 Declaración/aseveración

Por lo general se conviene en que el significado de los términos declaración y aseveración es bastante similar, pero con una connotación ligeramente distinta. En algunos casos, se considera que una aseveración es más "fuerte" que una declaración. Por ejemplo, en el Diccionario de Inglés de Oxford se define una declaración como:

- a) afirmar que ése es el caso, sin poder proporcionar una prueba de ello;
- b) afirmar que algo es el caso,

y aseveración como: una afirmación segura y vigorosa. Sin embargo, en un contexto digital, las expresiones "segura" y "vigorosa" no tienen una verdadera significación.

En las redes abiertas, la parte que hace una afirmación (es decir, que presenta información sobre identidad) y la parte que confía en la misma mantendrán una relación más compleja y ambivalente. Por lo tanto, se supone que toda declaración es dudosa y, como tal, está sujeta a verificación o a la solicitud de evidencias adicionales. No se puede partir de la base de que las declaraciones o aseveraciones se formulan con alguna autoridad. Siempre corresponderá a la parte confiante decidir si acepta o no la declaración o aseveración basada en la verificación por la parte confiante (o por un verificador que actúa en respuesta a la solicitud de la parte confiante).

A.3 Inscripción y registro

La inscripción y el registro son dos procesos que están estrechamente relacionados y existe cierta superposición entre ambos. A veces ambos términos se utilizan indistintamente y, aunque pueden estar combinados en un mismo paso, en realidad son dos procesos distintos.

La inscripción es el proceso de inauguración (o establecimiento) de una entidad en un contexto. La inscripción puede incluir la verificación de la identidad de la entidad y el establecimiento de una identidad contextual. El registro es el proceso a tenor del cual una entidad solicita privilegios para utilizar un servicio o recurso y esos privilegios le son asignados. La inscripción es un requisito previo para el registro.

En el mundo real, por ejemplo, un usuario podría en algún momento inscribirse para utilizar servicios de banca genéricos, y en un momento posterior registrarse para recibir servicios de banca en línea. De otro modo, al abrir una nueva cuenta el usuario podría cumplir con las formalidades (es decir, inscribirse) de identificación (y conexas) y registrarse para recibir servicios de banca en línea al mismo tiempo.

A.4 Proveedor de identidad y proveedor de servicio de identidad

Un examen de las prácticas en vigor demuestra que en la actualidad se utilizan comúnmente los términos *proveedor de identidad* y *proveedor de servicio de identidad*. Aunque el término *proveedor de identidad* se utiliza en algunas Recomendaciones UIT-T, cabe inferir que se refiere a una entidad que *proporciona* identidades, y no a una entidad que *gestiona* identidades. Además, este término puede inducir a error, dado que las identidades no pueden proporcionarse, sino que existen o evolucionan cuando se asignan atributos. Además, el término *proveedor de servicio* se utiliza de manera generalizada en contextos tales como el de proveedor de servicio de verificación, proveedor de servicio de credencial, proveedor de servicio financiero, etc.

Por consiguiente, el término *proveedor de servicio de identidad* se considera un poco más descriptivo que el de *proveedor de identidad* y debería ser el término preferido. Es posible aceptar esa prioridad introduciendo sólo ligeros cambios en los documentos existentes y utilizar la definición actual de *proveedor de identidad* para *proveedor de servicio de identidad* y retener el término *proveedor de identidad*, pero en vez de definir este último término, incluir sencillamente un puntero de referencia a *proveedor de servicio de identidad*. El acrónimo debería ser IdSP.

A.5 Pauta de identidad

En general, las pautas se consideran información observada o reconocida y cuya estructura puede detectarse o corresponde a una estructura conocida. Es decir, una pauta de identidad puede considerarse información observable y reconocible que caracteriza una entidad y cuya estructura puede detectarse o corresponde a una estructura conocida.

Por ejemplo, la definición de *pauta* en dos diccionarios pertinentes son: "forma, orden o disposición regular o repetitiva"; y "un ejemplo fiable de rasgos, actos, tendencias u otras características observables de una persona, grupo o institución".

La interpretación general y las definiciones anteriores de pauta implica que ésta consiste en más de un elemento pero la repetición de un mismo atributo a lo largo del tiempo también constituye una pauta. Que se produzca una sola vez un mismo atributo no constituye una pauta pero la manera en que se produce uno o varios atributos puede representar una pauta. Asimismo, una pauta de identidad puede basarse en más de una actividad o conducta y no limitarse a la información observable o reconocible. En cambio, puede basarse en otros atributos. Por ejemplo, el dibujo de un neumático tiene una estructura clara y detectable, por lo que en este caso el atributo propiamente dicho puede considerarse una pauta de identidad. Tampoco es necesariamente cierto que una pauta debe ser observada más de una vez para resultar útil. Por ejemplo, cuando dos personas hablan sobre un automóvil que está expuesto en un concesionario pueden identificarlo y referirse al mismo como: "el que está al fondo en la esquina izquierda".

Las pautas pueden reutilizarse, pero es posible imaginar situaciones en las que se utilizan una sola vez, por ejemplo en códigos.

Si bien puede aducirse que todos los atributos tienen cierta estructura, una diferencia evidente entre atributos y pautas de identidad es que el observador detecta y obtiene la estructura pero ésta no la conocen necesariamente otras entidades, incluso las entidades observadas.

Además de emplearse para la identificación, las pautas de identidad también pueden utilizarse en algunos casos para la autenticación o la simple clasificación de entidades. Un ejemplo de esto último es el análisis de la conducta del consumidor para determinar los tipos de productos que le interesan y la frecuencia con la que los compran. En el contexto de "comercialización", las pautas se utilizan para clasificar entidades en ciertos grupos, de tal manera que combinando algunas de estas pautas se pueda identificar a entidades concretas.

Los elementos utilizados para identificar una entidad deben permitir que esta sea lo suficientemente distinguible dentro del contexto. Si se desea utilizar una pauta de identidad para la identificación o autenticación de entidades concretas (a diferencia de grupos), es indispensable que la pauta de identidad sea singular y no ambigua. Ahora bien, en algunos casos, por ejemplo cuando se emplea para la autorización, la pauta de identidad no tiene por qué ser única o no ambigua. Considérese como ejemplo cuando es necesario limitar el número de usuarios de un determinado servicio, por ejemplo para la participación en un campeonato deportivo. Es posible que sea necesario aplicar restricciones basadas, por ejemplo, en el consumo de ciertos medicamentos.

Bibliografía

Al elaborar la lista de términos y definiciones IdM se ha hecho referencia a un gran número de publicaciones, trabajos y glosarios IdM ya existentes. La lista dista mucho de ser exhaustiva, pero incluye:

- [b-ISO/IEC CD 2382-37] ISO/IEC CD 2382-37, *Information technology – Vocabulary – Part 37: Harmonized biometric vocabulary.*
- [b-ANSI] American National Standards Institute <http://www.ansi.org/>
- [b-AusCert] AusCert Conference 2005
- [b-Carnegie] Carnegie Mellon® Computing Services
www.cmu.edu/acs/documents/idm/
- [b-NSS] Committee on National Security Systems Glossary Working Group
- [b-Edentity] Edentity <http://www.edentity.co.uk/>
- [b-ETSI] ETSI Terms and Definitions Database Interactive
<http://webapp.etsi.org/Teddi/>
- [b-EU] EU Commission eGovernment Unit DG Information Society and Media
- [b-ICANN] ICANN <http://www.icann.org/en/general/glossary.htm>
- [b-Identity] Identity Commons http://wiki.idcommons.net/Main_Page
- [b-IETF] IETF Trust (2007) Network Working Group
- [b-ISO/IEC] ISO/IEC JTC 1/SC 27/WG5
- [b-ITU-T Id Mgmt] Grupo Temático de gestión de identidad del UIT-T
- [b-ITU-T Terms] Base de datos de términos y definiciones del UIT-T
<http://www.itu.int/ITU-T/dbase>
- [b-Cameron] Kim Cameron's Laws of Identity
<http://www.identityblog.com/?p=354>
- [b-Liberty] Liberty Alliance Technical Glossary
- [b-Modinis] Modinis <https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/WebHome>
- [b-NetMesh] NetMesh® Inc. <http://www.netmesh.us/>
- [b-NIST] National Institute of Standards and Technology
<http://www.nist.gov/index.html>
- [b-OASIS] OASIS <http://www.oasis-open.org/committees/security/ipr.php>
- [b-OED] Oxford English Dictionary
- [b-OECD] OECD Recommendation on Electronic Authentication
- [b-Mobile] Open Mobile Alliance™
<http://www.openmobilealliance.org/UseAgreement.html>
- [b-STORK] STORK-eID Consortium http://www.eid-stork.eu/index.php?option=com_frontpage&Itemid=1

[b-Trusted]

Trusted Computing Group <http://www.trustedcomputinggroup.org/>

[b-IAAC]

UK Information Advisory Council
<http://www.iaac.org.uk/Default.aspx?tabid=1>

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