Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1252

(04/2021)

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 (1)	
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 (1)	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 (2)	
Comunicaciones de emergencia	X.1300–X.1309
Seguridad en las redes de sensores ubicuos	X.1310–X.1339
Seguridad de las redes eléctricas inteligentes	X.1330–X.1339
Recomendaciones relacionadas con la PKI	X.1340–X.1349
Seguridad en la Internet de las cosas (IoT)	X.1360–X.1369
Seguridad en los sistemas de transporte inteligente (ITS)	X.1370–X.1379
Seguridad de tecnología de libro mayor distribuido	X.1400–X.1429
Seguridad de tecnología de libro mayor distribuido	X.1430–X.1449
Protocolos de seguridad (2)	X.1450–X.1459
INTERCAMBIO DE INFORMACIÓN DE CIBERSEGURIDAD	
Aspectos generales de la ciberseguridad	X.1500–X.1519
Intercambio de estados/vulnerabilidad	X.1520–X.1539
Intercambio de eventos/incidentes/heurística	X.1540–X.1549
Intercambio de políticas	X.1550–X.1559
Petición de heurística e información	X.1560–X.1569
Identificación y descubrimiento	X.1570–X.1579
Intercambio asegurado	X.1580–X.1589
SEGURIDAD DE LA COMPUTACIÓN EN NUBE	
Visión general de la seguridad de la computación en nube	X.1600–X.1601
Diseño de la seguridad de la computación en nube	X.1602–X.1639
Prácticas óptimas y directrices en materia de seguridad de la computación en nube	X.1640–X.1659
Aplicación práctica de la seguridad de la computación en nube	X.1660–X.1679
Otras cuestiones de seguridad de la computación en nube	X.1680–X.1699
COMUNICACIÓN CUÁNTICA	
Terminologías	X.1700–X.1701
Generador de números aleatorio cuántico	X.1702–X.1709
Marco de seguridad QKDN	X.1710–X.1711
Diseño de seguridad para QKDN	X.1712–X.1719
Técnicas de seguridad para QKDN	X.1720–X.1729
SEGURIDAD DE LOS DATOS	
Seguridad de los macrodatos	X.1750–X.1759
SEGURIDAD DE LAS IMT-2020	X.1800–X.1819

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 la definición 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 Recomendación UIT-T X.1252 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. La Recomendación UIT-T X.1252 incluye un anexo en el que se explican las razones por las que algunos de estos términos son tan importantes.

Uno de los principales objetivos de la Recomendación UIT-T X.1252 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	Identificador exclusivo*
1.0	UIT-T X.1252	16-04-2010	17	11.1002/1000/10440
2.0	UIT-T X.1252	30-04-2021	17	11.1002/1000/14642

* Para acceder a la Recomendación, sírvase digitar el URL http://handle.itu.int/ en el campo de dirección del navegador, seguido por el identificador único de la Recomendación. Por ejemplo, http://handle.itu.int/11.1002/1000/11830-en.

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

ÍNDICE

Recomendación UIT-T X.1252

Términos y definiciones de referencia para la gestión de la identidad

1 Alcance

En la presente Recomendación se define un conjunto de términos que se utilizan normalmente para la gestión de la identidad (IdM). Se proporciona una definición básica de los términos, con objeto de transmitir el significado fundamental, aunque excepcionalmente se incluye una nota en los casos en los que contribuye a aclarar la definición. En el Anexo A se proporciona el fundamento de algunos términos y definiciones clave.

NOTA – En la presente Recomendación la utilización del término "identidad" en relación con la IdM no alude a su significado absoluto. En particular, no constituye 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 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 una Recomendación

Ninguna.

3 Definiciones

En la cláusula 6 se enumeran los términos y las definiciones pertinentes.

4 Abreviaturas y acrónimos

En esta Recomendación se utilizan las siguientes siglas y acrónimos:

CID	Identificador criptográfico (*cryptographic identifier*)
DDO	Descriptor de objeto DID (*DID object descriptor*)
DID	Identificador descentralizado (*decentralized identifier*)
DLT	Tecnología de libro mayor distribuido (*distributed ledger technology*)
ID	Identificador (*identifier*)
IdM	Gestión de identidad (*identity management*)
IdP	Proveedor de identidad (*identity provider*)
IdSP	Proveedor de servicio de identidad (*identity service provider*)
IH	Nodo de identidad (*identity hub*)
NGN	Red de la próxima generación (*next generation network*)
PII	Información de identificación personal (*personally identifiable information*)
PKI	Infraestructura de clave pública (*public key infrastructure*)
RA	Autoridad de registro *(registration authority*)

RE Entidad solicitante (*requesting entity*)

RP Parte retransmisora (*relying party*)

SIM Módulo de identificación del abonado (*subscriber identity module*)

SSI Identidad con soberanía propia (*self-sovereign identity*)

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

5 Convenios

Ninguno.

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 puede utilizarse para el encaminamiento hacia ese punto de terminación físico o lógico en una red pública o privada.

NOTA – Sobre la base de [b-UIT-T E.101].

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 determina cómo éstas deben relacionarse entre sí y llevar a cabo actividades conjuntas.

6.5 anónimo (*anonym*): Identificador utilizado exactamente en una ocasión.

6.6 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 y la frecuencia de utilización de un servicio.

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

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

6.8 garantía (*assurance*)

NOTA – Véase garantía de autentificación y garantía de identidad.

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

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

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

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

6.13 autentificación (*authentication*) [b-UIT-T X.501]: Proceso oficializado de verificación que, de ser satisfactoria, da lugar a una identidad autentificada para una entidad.

NOTA – En el contexto de la gestión de identidad se entiende que el término autentificación se refiere a la autentificación de una entidad.

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

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

6.15 autorización (*authorization*): Concesión de derechos y, sobre la base de esos derechos, concesión de acceso.

NOTA – Sobre la base de [b-UIT-T X.800].

6.16 vinculación (*binding*): Una asociación, un nexo o una relación que se establece explícitamente.

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

6.18 certificado (*certificate*): 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 autentificación de la integridad y el origen de los datos.

NOTA: Sobre la base de la definición de "certificado de seguridad" que figura en [b-UIT-T X.810].

6.19 declaración (*claim*) [b-OED]: Afirmación digital sobre atributos de identidad realizada por una entidad sobre sí misma u otra entidad. Declarar que es el caso, sin estar en condiciones de proporcionar pruebas.

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

6.20 declarante (*claimant*): Entidad que es la principal o la representa a los efectos de la autentificación.

NOTA 1 – Un declarante desempeña las funciones necesarias para participar en intercambios de autentificación en nombre de un principal.

NOTA 2 – Sobre la base de [b-UIT-T X.811].

6.21 definición de declaración (*claim definition*) [b-OED]: Definición legible de forma automatizada de la estructura semántica de una declaración.

NOTA – Las definiciones de declaración facilitan la interoperabilidad de las declaraciones y pruebas entre varios expedidores, titulares y partes dependientes.

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

6.23 correlación (*correlation*): Combinación de varias partes de información que guardan relación con una entidad o pasan a estar relacionadas con una entidad al combinarse.

NOTA – La correlación está estrechamente relacionada con la identificación. La correlación puede facilitar la identificación y la inferencia de información sobre una entidad que no esté directamente facilitada por los datos proporcionados.

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

NOTA – [b-ISO/CEI 29115] es similar al texto de la [b-UIT-T X.1254] y contiene la misma definición de credenciales que fue elaborada por los grupos participantes.

6.25 *minimización de datos* (*data minimization*): Limitar la recopilación, el almacenamiento y la utilización de identificadores, atributos y otros datos relacionados con una entidad a sólo lo estrictamente necesario para llevar a cabo la autenticación, así como limitar todo intercambio y

divulgación de datos relativos a una entidad, comprendida la información contextual de una solicitud, a sólo lo necesario para responder a la solicitud y a la parte dependiente.

6.26 identificador descentralizado (*decentralized identifier, DID*): Identificador único global que no requiere una autoridad central de registro porque emplea la tecnología de libro mayor distribuido u otro tipo de red descentralizada. Un DID se asocia exactamente a un descriptor de objeto DID.

NOTA – Véase [b-W3C-DIDs].

6.27 descriptor de objeto DID (*DID object descriptor, DDO*): Conjunto de datos que describen al titular del identificador descentralizado, incluidos mecanismos como claves públicas criptográficas, que el titular o un delegado del DID puede utilizar para autentificarse y demostrar su asociación con el DID.

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

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

6.30 libro mayor distribuido (*distributed ledger*) [b-UIT-T X.1400]: Tipo de libro mayor que se comparte, replica y sincroniza de manera distribuida y descentralizada.

6.31 sistema de gestión de claves descentralizado (*decentralized key management system*): Norma para la gestión de claves criptográficas interoperables basadas en identificadores descentralizados.

6.32 *dominio* (*domain*): Entorno en el que una entidad puede utilizar un conjunto de atributos a los efectos de identificación, entre otros fines.

NOTA – Un dominio proporciona contexto.

6.33 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.

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

NOTA 1 – La entidad puede materializarse de manera física o lógica.

NOTA 2 – 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.

6.35 autentificación 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 autentificación se refiere a la autentificación de una entidad.

6.36 federación (*federation*) [b-UIT-T Y.2720]: Establecimiento de una relación entre dos o más entidades o una asociación de proveedores de servicios y proveedores de servicios de identidad.

6.37 titular (*holder*) [b-UIT-T Y.2720]: Entidad expedida por la declaración de un expedidor. Si la declaración admite prueba de conocimiento cero, el titular será asimismo el comprobador.

6.38 identificación (*identification*) [b-ISO/CEI 24760-1]: Proceso conducente a reconocer una entidad en un dominio específico por sus características específicas.

6.39 identificador (*identifier, ID*) [b-UIT-T E.101]: Serie de cifras, caracteres y símbolos utilizados para identificar inequívocamente a un abonado, un usuario, un elemento de red, una función, una entidad de red, un servicio o una aplicación. Los identificadores pueden utilizarse para el registro y la autorización. Pueden ser públicos para todas las redes o privados para una red específica (normalmente los identificadores privados no se revelan a terceros).

NOTA – Un identificador puede consistir en un atributo creado específicamente con un valor asignado que sea único dentro del dominio.

6.40 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.

6.41 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.

6.42 política de seguridad basada en la identidad (*identity-based security policy*) [b-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.

6.43 gestión de identidad (*identity management, IdM*): Conjunto de funciones y capacidades (por ejemplo, administración, gestión y mantenimiento, descubrimiento, intercambios de comunicación, correlación y vinculación, cumplimiento de una política, autentificación 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.

NOTA – Sobre la base de [b-UIT-T Y.2720].

6.44 titular de identidad (*identity owner*): Entidad que puede ser considerada responsable. El titular de la identidad debe ser una persona o una organización. Mutuamente excluyente con Cosa.

6.45 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.

6.46 demostración de identidad (*identity proofing*) [b-ISO/CEI 29115]: Proceso mediante el cual la autoridad de registro (RA) obtiene y comprueba información suficiente para identificar una entidad con respecto a un grado de garantía específico o entendido.

6.47 proveedor de identidad (*identity provider, IdP*)

NOTA – Véase proveedor de servicio de identidad (IdSP).

6.48 proveedor intermediario de servicio de identidad: Proveedor de servicio de identidad (IdSP) que actúa como intermediario fiable entre otros IdSP.

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

6.50 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.

6.51 independiente (*independent*): Persona que controla directamente las claves privadas y los secretos maestros necesarios para administrar una identidad descentralizada.

6.52 individuo (*individual*): Propietario de identidad que es una persona natural. Mutuamente excluyente con Organización.

6.53 expedidor (*issuer*): Entidad que expide una declaración.

6.54 clave de expedidor (*issuer key*): Tipo especial de clave criptográfica necesaria para que el expedidor expida una declaración que admite pruebas de conocimiento cero.

6.55 portaclaves (*key-chain*): Se refiere a la tarea de proteger el almacenamiento de claves privadas y datos en una unidad física fiable de un dispositivo.

6.56 identidad legal (*legal identity*): Conjunto de información suficiente para identificar al titular de una identidad a efectos de responsabilidad jurídica en al menos una jurisdicción. La identidad jurídica puede establecerse, a los efectos de la red provisional, por referencia a uno o más recursos de la web de acceso público, como sitios web, blogs, perfiles de redes sociales u otras páginas web que proporcionen información suficiente para pasar esa prueba.

6.57 vinculación (*linkability*): Capacidad de distinguir, dentro de un conjunto de información, si dos o más atributos, identificadores, identidades u otros datos están relacionados con un grado de probabilidad suficientemente alto para resultar útiles.

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

NOTA – Comparar con aseveración.

6.59 autentificación mutua (*mutual authentication*) [b-ISO/CEI 29115]: Autentificación de identidades de entidades de modo que cada una de ellas está seguro de la identidad de la otra.

6.60 nombre (*name*): Combinación de caracteres utilizada para identificar entidades (por ejemplo, un abonado o un elemento de red) a partir de la cual es posible determinar o convertir su dirección. Los caracteres posibles son cifras, letras y símbolos.

NOTA 1 – 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.

NOTA 2 – Sobre la base de [b-UIT-T E.101].

6.61 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.

6.62 pauta (*pattern*)

NOTA – Véase pauta de identidad.

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

6.64 información de identificación personal (*personally identifiable information, PII*): 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 .

6.65 principal (***principal*)**: Una entidad cuya identidad puede ser autentificada.

NOTA – Esta información figura en [b-UIT-T X.811], [b-UIT-T Y.2702] y [b-UIT-T Y.2720].

6.66 política de privacidad (*privacy policy*): Política que establece los requisitos para proteger el acceso a la información de identificación personal 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.

6.67 clave privada (*private key*): (En un criptosistema de claves públicas) clave de un par de claves de entidad que sólo es conocida por esa entidad.

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

6.69 prueba (*proof*): Verificación criptográfica de una declaración. Una forma sencilla de prueba es la firma digital. Un hash criptográfico es también una forma de prueba. Las pruebas son de dos tipos: transparentes o de conocimiento cero. Las pruebas transparentes revelan toda la información de una declaración. Las pruebas de conocimiento cero facilitan la revelación selectiva de la información en una declaración.

6.70 comprobador (*prover*): Entidad que expide una prueba a partir de una declaración. El comprobador también es el titular de la declaración.

6.71 seudónimo (*pseudonym*) [b-ISO/CEI 24760-1]: Identificador que contiene la mínima información de identidad suficiente para permitir al verificador establecer un vínculo con una identidad conocida.

NOTA 1 – El pseudónimo puede ser un identificador con un valor escogido por la persona o asignado de manera aleatoria.

NOTA 2 – 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.

6.72 datos públicos (*public data*) [b-UIT-T L.1410]: Datos que están disponibles para el público sin que su acceso se restrinja por requisitos de afiliación, acuerdos de no divulgación o restricciones análogas.

6.73 clave pública (*public key*) [b-UIT-T X.509]: La clave del par de claves de la entidad que es de dominio público.

6.74 perfil público (*public profile*): Información que describe un proveedor de servicios, que comprende su identidad legal, sus logotipos u otras marcas registradas, sus ubicaciones, información de comercialización, enlaces web y cualquier otra información requerida por el marco de confianza para garantizar la plena transparencia acerca de la identidad jurídica y las cualificaciones del proveedor.

6.75 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.

6.76 parte dependiente (*relying party, RP*): Entidad que se basa en la representación o declaración de identidad de una entidad solicitante/declarante en un contexto de petición.

NOTA – Sobre la base de [b-UIT-T Y.2720].

6.77 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.

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

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

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

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

6.81 auditoría de seguridad (*security audit*): 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 procedimiento.

6.82 dominio de seguridad (*security domain*): 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.

NOTA – Sobre la base de [b-UIT-T X.810]. En [b-UIT-T Y.2701] y [b-UIT-T Y.2720] se proporcionan definiciones análogas.

6.83 zona de seguridad (*security zone*): Zona protegida caracterizada mediante control operacional, ubicación y conectividad a otros dispositivos/elementos de red.

NOTA – Sobre la base de [b-UIT-T Y.2701].

6.84 autoridad de dominio de seguridad (*security domain authority*) [b-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.

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

6.86 cosa (*thing*): Entidad que no puede ser considerada legalmente responsable. Puede tratarse de un animal (por ejemplo, una mascota, un ganado), un objeto físico (por ejemplo, una casa, un coche, un teléfono) o un objeto digital (por ejemplo, un programa de software, un servicio de red, una estructura de datos). Mutuamente excluyente con el titular de la identidad.

6.87 confianza (*trust*): Confianza de una parte o entidad en que otra parte o entidad se comportará de una manera bien definida que no infrinja las normas, políticas o cláusulas jurídicas acordadas del sistema de gestión de la identidad.

6.88 custodio de confianza (*trust anchor*): Titular de la identidad que puede servir como punto de partida en la red descentralizada de confianza. El custodio de confianza tiene dos privilegios únicos:

- añadir nuevos titulares de identidad a la red; y
- expedir invitaciones del custodio de confianza.

El custodio de confianza debe cumplir los criterios pertinentes y estar de acuerdo con las obligaciones del custodio de confianza definidas en el marco de confianza. Todos los garantes y administradores son automáticamente custodios de confianza.

6.89 marco de confianza (*trust framework*): Conjunto de especificaciones, normas y acuerdos jurídicamente vinculantes que rigen un sistema de identidades.

NOTA – Sobre la base de [b-OIX-TFIS].

6.90 tercero fiable (*trusted third party*): 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.

NOTA 1 – Sobre la base de [b-UIT-T X.810] y [b-UIT-T Y.2702].

NOTA 2 – Véase [b-UIT-T X.800].

6.91 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.

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

6.93 centrado en el usuario (*user-centric*): Sistema de gestión de identidad que puede proporcionar al usuario la capacidad de controlar y hacer cumplir diversas políticas que rigen los datos, en particular la información de identificación personal del usuario.

6.94 nodo validador (*validator node*): Nodo que valida nuevas transacciones de los registros de identidad y escribe activamente las transacciones válidas en el libro mayor utilizando el protocolo de consenso del libro mayor.

6.95 declaración verificable (*verifiable claim*): Declaración que incluye una prueba del expedidor. Por regla general, esta prueba consiste en una firma digital. La declaración verificable se puede verificar mediante una clave pública asociada al identificador descentralizado del expedidor.

NOTA – Sobre la base de [b-W3C-VC].

6.96 verificación (*verification*): [b-ISO/CEI 24760-1]: Proceso que determina que la información de identidad correspondiente con una determinada entidad es correcta.

NOTA 1 – El proceso de identificación se aplica a la verificación de los atributos declarados u observados.

NOTA 2 – 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..

NOTA 3 – La información es correcta en el momento de la verificación.

6.97 verificador (*verifier*) [b-ISO/CEI 24760-1]: entidad que verifica.

6.98 cartera (cartera de identidad) (*wallet (identity wallet)*): Aplicación que permite principalmente al usuario ser titular de identificadores y credenciales mediante el almacenamiento de las correspondientes claves privadas en el dispositivo de usuario.

6.99 prueba de conocimiento cero (zero knowledge proof, *ZKP*): Prueba que utiliza una criptografía especial y un secreto maestro para permitir la divulgación selectiva de información en un conjunto de declaraciones. La ZKP demuestra la veracidad de algunos o todos los datos de un conjunto de declaraciones sin revelar ninguna información adicional, incluida la identidad del verificador.

NOTA 1 – El concepto de "divulgación selectiva" significa una amplia gama de opciones para la divulgación. Por ejemplo, las ZKP pueden utilizarse para comprobar diversas declaraciones sobre datos confidenciales, en particular: 1) la mayoría de edad, sin revelar la fecha de nacimiento; 2) la solvencia (no estar en quiebra), sin mostrar la composición de la cartera; 3) la propiedad de un activo, sin revelar ni establecer vínculos con transacciones anteriores.

NOTA 2 – Sobre la base de [b-UIT-T X.1403].

Anexo A

Aspectos principales y razón de ser de la terminología básica sobre gestión de la identidad

(Este anexo forma parte de la presente Recomendación)

Antecedentes

En el curso de los debates sobre IdM se han descrito las diferentes maneras de comprender los objetivos al respecto, los procedimientos básicos utilizados 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 IdM.

Introducción

Identidad es el término alrededor del cual giran todos los otros términos IdM. En el mundo real, más que en el 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 y el comportamiento. En otros se puede aludir a la fecha de nacimiento, el lugar de nacimiento, la dirección de su casa y el número de teléfono. Normalmente en un proceso de comunicación ambas partes necesitan suficiente confianza para saber que se están comunicando con la parte correcta. En ese proceso de búsqueda de confianza normalmente participan dos o más particulares, o "entidades": la entidad cuya identidad debe confirmarse – la entidad solicitante (RE), y la entidad que confiará en una identidad confirmada – la RP. En este proceso puede intervenir una tercera entidad que gestiona las identidades, el IdSP.

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 (ID) 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 Autentificación y confianza

El proceso de autentificación es una parte importante de la IdM. En el presente apartado se ayuda a explicar el proceso de autentificación y su pertinencia para la confianza.

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

El proceso de autentificación 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 autentificación 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, por la cual se entiende algo que tenga una existencia separada y bien definida y pueda identificarse en contexto.

NOTA 1 – Entidad que puede tener una incorporación física o lógica.

NOTA 2 – 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 e interfaces.

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 en un dominio específico difiere del de otras entidades.

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.

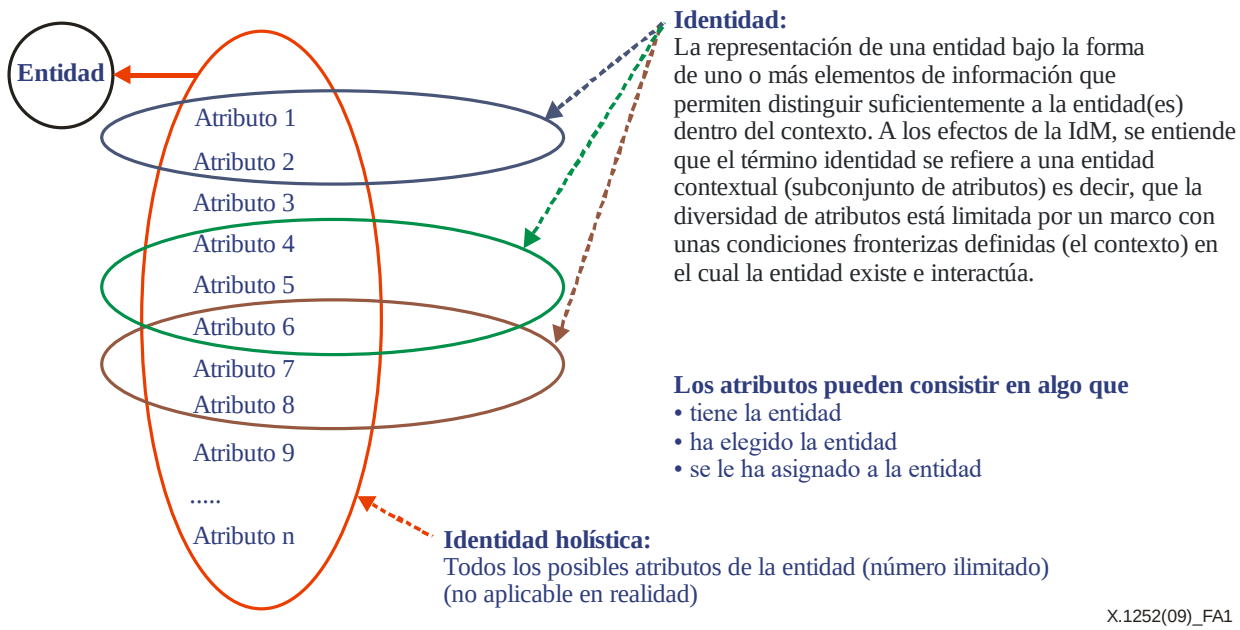


Figura A.1 – Relaciones entre entidad, identidades y atributos

Como ya se indicó, la autentificación es pertinente para la IdM. 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 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, en particular:

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

En general este proceso de adquirir confianza, es decir el proceso de autentificación, se realiza mutualmente. Esto significa que el proceso de autentificación 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:

Autentificación de Y: La entidad Y actúa como RE, la entidad X actúa como RP.

Autentificación de X: La entidad X actúa como RE, y la entidad Y como RP.

Con miras a simplificar el proceso y facilitar su comprensión, el proceso de autentificación 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 RP,
- suficiente confianza en que la RP 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).

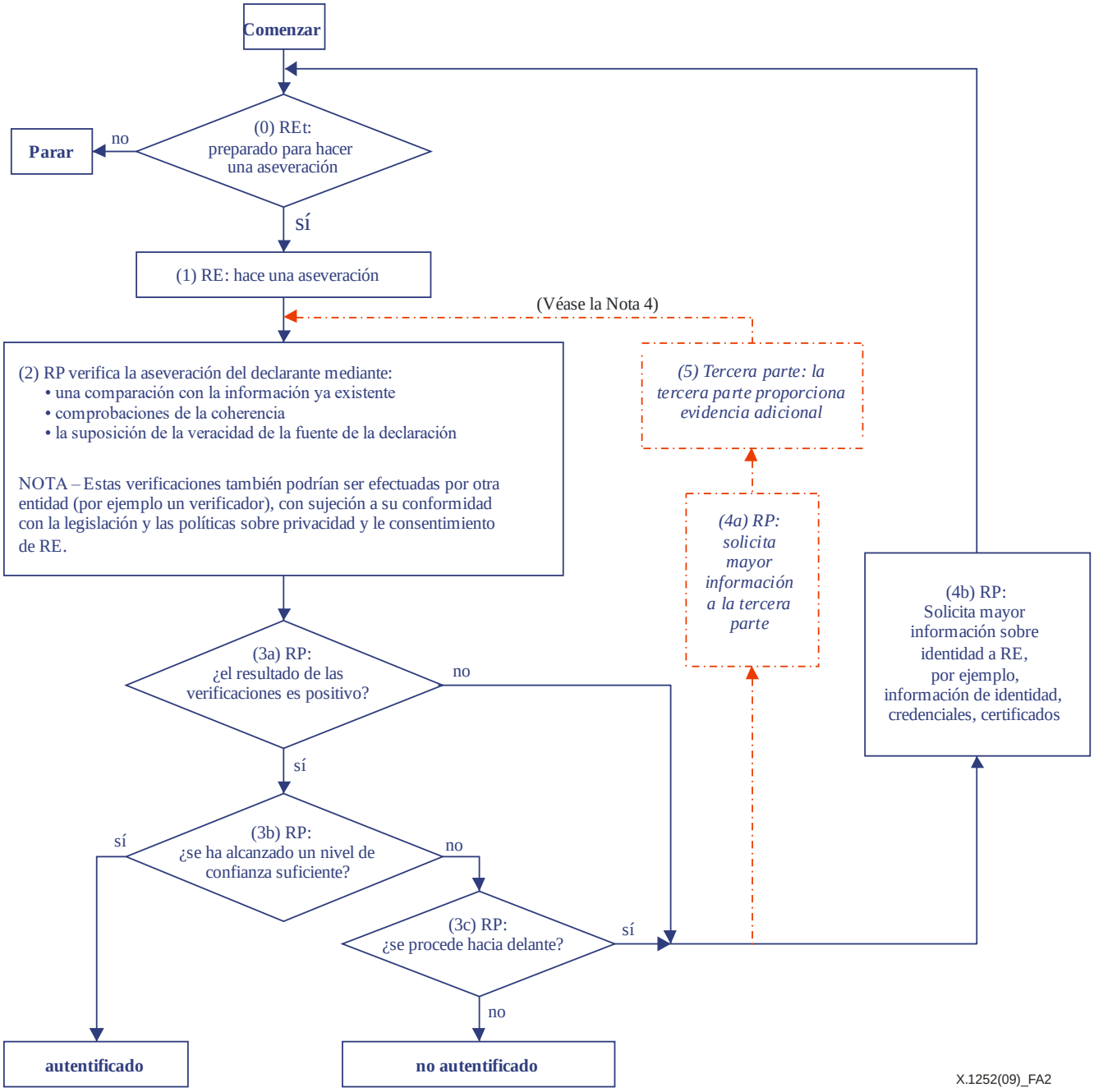
En algunos casos (pero no en los sistemas centrados en el usuario) puede participar directamente una tercera parte para proporcionar información adicional, a título de evidencia, a la RP, para aumentar la confianza en los atributos de la RE.

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, un cifrado específico);
- corresponde a 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.



NOTA 1 – En esta figura se ilustra el proceso de autentificación 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 saltear 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 autentificación unidireccional

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 ejemplo de diagrama de la Figura A.2, siempre corresponde a la RP decidir si acepta o no a la RE sobre la base del proceso de autentificación. 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 autentificación. Por lo tanto, es necesario que las implementaciones técnicas de los mecanismos de autentificación 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 IdM, 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 autentificación 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 de módulo de identificación del abonado (SIM) de previo pago, no se necesita autentificación alguna.

Durante el proceso de autentificación 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 autentificación (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;
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 autentificación distintos.

A.2 Declaración o 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, puede definirse 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, los adjetivos "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 RP decidir si acepta la declaración o aseveración basada en la verificación por la RP (o por un verificador que actúa en respuesta a la solicitud de la RP).

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 (IdP) e IdSP. Aunque el término IdP se utiliza en algunas Recomendaciones UIT-T, cabe inferir que se refiere a una entidad que proporciona identidades, y no a una entidad que las gestiona. 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 y proveedor de servicio financiero.

Por consiguiente, el término IdSP se considera un poco más descriptivo que el de IdP 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 IdP para IdSP y retener el término IdP, pero en vez de definir este último término, incluir sencillamente un puntero de referencia a 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, cabe proporcionar dos definiciones de pauta: "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 asimismo imaginar situaciones en las que se utilizan una sola vez, por ejemplo en códigos de un solo uso.

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 autentificación 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 autentificación 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, con respecto al consumo de ciertos medicamentos.

Anexo B

Aspectos principales y fundamentos de la terminología básica de la gestión descentralizada de la identidad

(Este anexo forma parte de la presente Recomendación)

B.1 Identidad descentralizada

Los modelos de identidad presentados en el Anexo A se centran en el IdP. El modelo supone que los usuarios confían en los IdP para establecer, mantener y proporcionarles identidades que puedan utilizar en sus interacciones en línea. Este planteamiento centrado en el IdP requiere que los usuarios confíen sus identidades a los IdP. En el enfoque centrado en el IdP, los IdP ofrecen servicios de federación para la reutilización de la identidad. La capacidad de reutilizar la identidad del usuario se limita a los miembros de la federación. En la federación de identidad, los proveedores constituyen el núcleo de la confianza y se dedican a proteger su modelo comercial, a diferencia de implantar un auténtico sistema descentralizado de eco de identidad que permita a los usuarios hacerse cargo de su identidad y sus relaciones. El modelo de identidad centrado en el IdP requiere que exista una confianza implícita en los IdP centralizados. El modelo propiamente dicho no es flexible ni dinámico.

Por otra parte, en el modelo de identidad descentralizado el sistema permite a los usuarios controlar su propia identidad. En el enfoque descentralizado, los proveedores se centran en hacer valer las declaraciones sobre identidades específicas. Los modelos de identidad descentralizados se nutren del desarrollo actual de las tecnologías de libro mayor distribuido (DLT).

A fin de permitir la prestación de servicios en todos los dominios participantes, los modelos de identidad centralizados se centran en la prestación de servicios de autenticación en un dominio para permitir el acceso a otro a través de puentes federados de identidades. En las interacciones en línea, la presión de confirmar la identidad declarada de la entidad recae en los sistemas basados en la identidad, en lugar de proporcionar control de acceso. Por ello, una de las principales funciones de los sistemas de identidad descentralizados es proporcionar un modelo que permita formular afirmaciones sobre la identidad de un usuario que puedan utilizarse fácilmente entre los proveedores.

El modelo de identidad centrado en el usuario consiste en el control individual o administrativo en múltiples dominios de identidad sin necesidad de una federación que actúe como círculo de confianza. La identidad centrada en el usuario tiene por objeto crear una identidad en línea persistente para una entidad cuyo objetivo es mejorar la experiencia en línea y, al mismo tiempo, proporcionar a los usuarios un mayor control sobre sus identidades mediante la utilización de modelos de confianza descentralizados. Sin embargo, debido a la falta de simplicidad y a la carencia de tecnologías como las DLT, el modelo centrado en el usuario no tuvo éxito.

El concepto de identidad centrada en el usuario se ha ido afianzando desde que surgieron las DLT. Se está desarrollando una pila de protocolos basada en DLT para permitir una verdadera infraestructura de identidad descentralizada. Estos sistemas pueden funcionar con DLT públicas, privadas, sin permiso o con permiso para permitir la gestión de identidades digitales. El objetivo es devolver a los usuarios el control de las afirmaciones de identidad, manteniendo al mismo tiempo la seguridad, la integridad y la privacidad del sistema.

B.2 Modelo de identidad descentralizada

La identidad descentralizada es un modelo que promueve el control individual (con capacidad para delegar el control) a través de cualquier número de autoridades (incluidos los IdP). Uno de los modelos específicos de identidad descentralizada es el denominado identidad autosoberana (SSI), que se basa en los supuestos enumerados en el Cuadro B.1.

Cuadro B.1 – Supuestos en materia de identidad autosoberana

Existencia	Los usuarios deben tener una existencia independiente
Control	Los usuarios deben controlar sus identidades
Acceso	Los usuarios deben tener acceso a sus propios datos
Transparencia	Los sistemas y algoritmos deben ser transparentes
Persistencia	Las identidades deben ser duraderas
Portabilidad	La información y los servicios acerca de la identidad deben ser transferibles
Interoperabilidad	Las identidades han de ser tan ampliamente utilizables como sea posible
Consentimiento	Los usuarios deben aceptar la utilización de su identidad
Minimización	La divulgación de declaraciones debe reducirse al mínimo
Protección	Deben protegerse los derechos del usuario

Los aspectos deseados coinciden en gran medida con lo que la DLT puede ofrecer. Las implementaciones descentralizadas de identidad se basan generalmente en declaraciones y atestados en los que a menudo los actores desempeñan diversos papeles.

Los sistemas de identidad descentralizados pueden utilizarse para facilitar transacciones en línea fiables. Los sistemas de identidad descentralizados permiten a los usuarios demostrar atributos sobre sí mismos al proveedor de servicios (o viceversa) utilizando para ello declaraciones verificables (atestados). Todo el proceso puede realizarse de manera interoperable y fiable mediante una pila tecnológica que permita la difusión de declaraciones de confianza sin necesidad de que los participantes en la transacción interactúen directamente.

En un sistema de identidad descentralizado, el proveedor de servicios actúa como una RP, mientras que las declaraciones las formula el expedidor de atestados, que expide los atestados necesarios que faltan. El atestado es un conjunto de afirmaciones sobre la exactitud de otro conjunto de afirmaciones. El conjunto original de afirmaciones también puede denominarse declaración. El receptor de un atestado debe ser capaz de validar el compromiso de quien atestigua las reclamaciones. El compromiso debe, por lo tanto, adoptar la forma de una firma digital o de un puntero a los datos en un libro distribuido.

La identificación de los nodos en la red se realiza mediante identificadores descentralizados (DID). El DID es imprescindible para participar en la red y realizar transacciones. Se trata del número, nombre o cadena con el que se identifica a alguien. El identificador criptográfico (CID) es un DID vinculado criptográficamente a una determinada clave privada.

En la actualidad, la mayoría de las soluciones basadas en la identidad admiten un limitado control de la identidad, la transparencia y la portabilidad, por cuanto esas soluciones las ofrecen proveedores de identidades con sistemas patentados en calidad de terceros. Es posible que en un futuro próximo no exista un sistema de gestión de identidades plenamente conforme, pero ello no es óbice para excluir la necesidad de establecer el principio de soberanía fundamental.

Para permitir la SSI, se está normalizando una nueva generación de protocolos y soluciones de gestión de la identidad descentralizada, como se explica en las siguientes cláusulas.

B.2.1 Identificadores descentralizados

Los identificadores descentralizados (DID) son ID destinados a sistemas de identidad verificables y descentralizados, en particular la identidad digital "autosoberana". En general, los DID los genera el propio usuario y son de su propiedad. Los DID poseen características únicas, que aportan mayores garantías de inmutabilidad y son a prueba de manipulación. El DID está completamente bajo el control del titular del DID, con independencia de cualquier registro centralizado, IdP o autoridad de

certificación. Los DID son localizadores uniformes de recursos (URL) que establecen la relación entre el titular del DID y medios con los que dicho titular puede efectuar interacciones fiables.

En general, hay dos tipos de DID: DID públicos y DID por pares (considérese semiprivados):

1) Los DID públicos son ID utilizados por aquellos usuarios que deciden vincularse con datos accesibles públicamente. Algunos ejemplos son perfiles públicos en las redes sociales o la verificación de una profesión, como la de médico. Los DID públicos permiten al usuario avalar las actividades que juzga oportuno compartir con los demás y que los demás pueden verificar. Por ejemplo, es posible verificar que mi médico de cabecera es el titular del DID. Los DID públicos son rastreables y vinculables a través de Internet.

2) Los DID por pares se generan en el marco de una relación o conjunto de interacciones en las que los usuarios desean realizar transacciones mutuas. Los DID por pares aíslan a los usuarios y evitan la correlación. Para la mayoría de los usuarios, los DID por pares serán el principal mecanismo para realizar interacciones basadas en la identidad.

La resolución de DID da lugar a documentos DID, que son documentos sencillos en los que se describe cómo utilizar DID específicos. Cada documento DID contiene por lo menos tres elementos: material criptográfico, conjuntos de autenticación y extremos de servicio. El material criptográfico combinado con los conjuntos de autenticación proporciona una serie de mecanismos para autentificar al titular DID (por ejemplo, claves públicas y protocolos biométricos pseudónimos). Los extremos de servicio permiten la comunicación fiable con el titular del DID.

Para utilizar el DID con un libro mayor distribuido o red en concreto es preciso definir un método DID en una especificación independiente. El método DID especifica un conjunto de reglas que rigen la forma de registrar, resolver, actualizar y revocar un DID en un libro mayor o red en concreto.

Este diseño elimina la dependencia de los registros centralizados para los ID, así como de las autoridades de certificación centralizadas para la gestión de las claves, que es la norma en la infraestructura de clave pública (PKI). Como los DID residen en un libro mayor distribuido, cada entidad puede ejercer su propia autoridad.

Obsérvese que también se pueden desarrollar métodos DID para ID registrados en sistemas IdM federados o centralizados. Por su parte, todos los tipos de sistemas de ID pueden incorporar soporte para DID. De esta manera se crea un puente de interoperabilidad entre los mundos de identificadores centralizados, federados y descentralizados.

B.2.2 Nodos de identidad

Los nodos de identidad (IH) son componentes responsables de almacenar las aseveraciones de identidad sobre los sujetos. Los IH se basan en un modelo descentralizado para almacenar representaciones semánticas de cualquier objeto y exponerlas como URL específicas. La arquitectura de un IH puede reunir identidades almacenadas en diferentes proveedores, desde directorios en la nube hasta dispositivos.

B.2.3 Mecanismo resolutivo universal de identificadores descentralizados

El mecanismo resolutivo universal de DID actúa como un sistema distribuido que puede resolver DID en múltiples DLT o cadenas de bloques. El mecanismo resolutivo universal de DID tiene una finalidad similar a la del mecanismo vinculante de los sistemas de nombre de dominio. En lugar de trabajar con nombres de dominio, los mecanismos resolutivos universales de DID se concentran en SSI que pueden crear y registrar directamente las entidades a las que remiten. El concepto se ilustra en la Figura B.1.

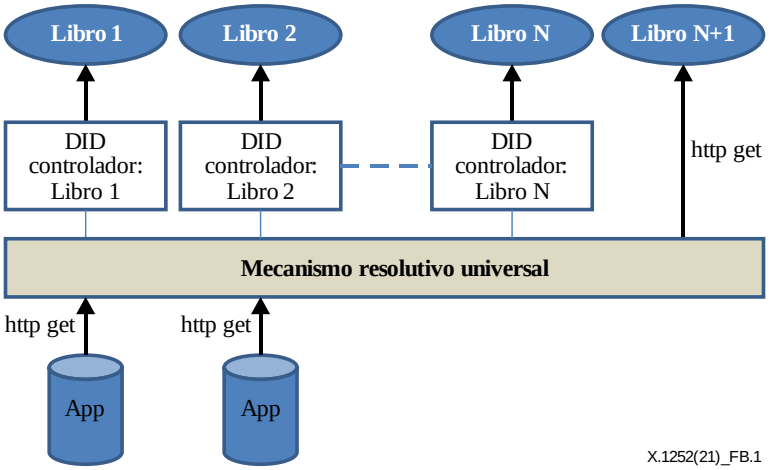


Figura B.1 – Mecanismo resolutivo universal de DID

B.2.4 Credenciales verificables

Las credenciales verificables son útiles cuando una entidad necesita probar, por ejemplo que:

- tiene más de una cierta edad;
- es capaz de conducir un vehículo motorizado particular;
- requiere un medicamento en particular;
- está formado y certificado como electricista;
- dispone de licencia profesional para ejercer la medicina;
- tiene autorización para viajar al extranjero.

El ecosistema de credenciales verificables está compuesto por cuatro funciones primarias:

1) El expedidor, que expide las credenciales verificables sobre un tema específico.
2) El portador, quien guarda las credenciales en nombre del titular. El portador suele ser también el titular de la credencial.
3) El verificador, que solicita un perfil del sujeto. El perfil contiene el conjunto específico de credenciales. El verificador confirma que las credenciales proporcionadas en el perfil son adecuadas para el fin previsto.
4) El registro de ID, que es el mecanismo utilizado para expedir ID para los titulares.

En la Figura B.2 se representa gráficamente el ecosistema:

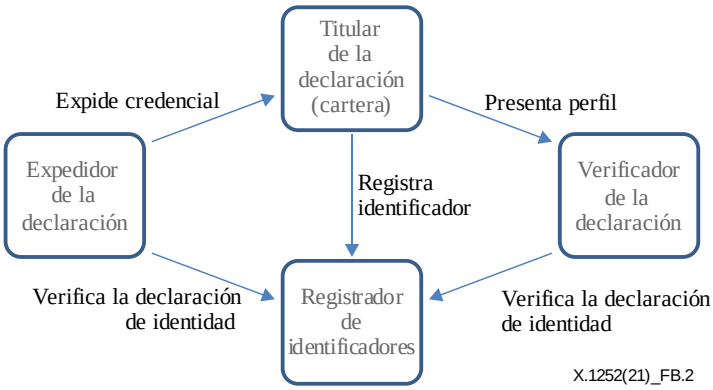


Figura B.2 – Ecosistema

B.2.5 Cartera descentralizada

En este modelo, el usuario puede acceder a un servicio presentando su ID a un proveedor de servicios (RP) en la forma de un testigo. El RP verifica la identidad comparando los valores generadores (*hash*) de los ID con sus correspondientes registros generadores que se almacenan en la DLT. El RP concede o rechaza el acceso en función del resultado de la verificación. En casos más avanzados, el usuario puede deducir pares de claves separados a partir de una clave privada maestra para generar ID separados para las diferentes relaciones, con el fin de permitir interacciones que respeten la privacidad.

La Figura B.3 ilustra las interacciones generales de identidad en el ámbito del servicio basado en identidades. La figura muestra las siguientes etapas en las transacciones de identidad descentralizadas:

- El usuario decide interactuar utilizando los servicios de identidad descentralizados de una estructura fiable de identidades. Como se ilustra en el recuadro del libro mayor descentralizado de la Figura B.3, la DLT presta servicios para que el usuario final pueda establecer un DID y una relación con el libro mayor. La tarea de establecer el DID para el usuario culmina guardando la dirección de libro mayor para ese usuario y creando pares de claves públicas y privadas para interactuar con el usuario. El libro también mantiene el documento DID y establece los correspondientes enlaces de datos de notación de objeto JavaScript necesarios, conforme a lo especificado por el usuario. El libro mayor proporciona servicios básicos de identidad que permiten a los servicios descubrir cómo interactuar con la cartera del usuario a fin de consultar sobre las declaraciones disponibles bajo el control del usuario.
- El establecimiento de un DID en el libro mayor conduce a la creación de la cartera que utilizará el usuario para presentar declaraciones verificadas a la RP. La cartera contiene las claves privadas, las claves públicas y otros perfiles de identidad del usuario que requiera el DID. Recurriendo a técnicas de conocimiento cero se garantiza que las declaraciones puedan verificarse preservando la privacidad y en consonancia con la actual utilización de las credenciales y documentos tradicionales en papel. Por ejemplo, un usuario puede demostrar su edad con un permiso de conducir en un restaurante sin necesidad de que el expedidor participe en la transacción. A continuación se indican los pasos necesarios. La cartera puede ser virtual, en la que una parte de la misma se encuentra en el dispositivo móvil del usuario y otra parte en la nube. Esta configuración permite crear agentes que actúen en nombre del usuario y presten servicios sin necesidad de que éste participe directamente.
    1) Registro DID: el usuario descarga la cartera asociada al proveedor de servicios DLT y registra su DID en el libro mayor. La DLT genera los pares de claves privadas y públicas para la cartera de identidad. Además, se crea una ubicación o dirección y se almacena en la DLT durante el proceso de registro.
    2) Inicialización de la identidad: para que una DLT se utilice en sistemas descentralizados de gestión de identidades, se supone que el marco de confianza especifica el conjunto de servicios de identidad disponibles para los participantes. A este respecto, el usuario puede confiar en la disponibilidad de un expedidor (parte fiable) que pueda validar la identidad de los servicios. El usuario puede basarse en las declaraciones iniciales de su cartera para reunir declaraciones de múltiples proveedores a fin de incluirlas en su cartera y mejorar la validez de su identidad dentro del sistema. De la Figura B.3 se desprende que toda relación está protegida por un DID mutuo entre el expedidor, el titular (usuario) y el verificador.
    3) Verificación: si un titular (usuario) desea acceder a un servicio ofrecido por una RP, ésta (el verificador) preguntará al usuario sobre las declaraciones disponibles. El verificador consultará entonces el libro mayor para validar las declaraciones firmadas utilizando las claves públicas correspondientes al DID y que guardan relación con la transacción. Esta

etapa incluye otras capas de autentificación. En particular, por la manera en que el sistema funciona, éste supone que la cartera es fidedigna en cuanto a que conoce las claves privadas del titular. Supone además que se ha producido una autentificación adecuada para garantizar que el propietario legítimo de la cartera es realmente la entidad que está efectuando la transacción.

4) Validación de la declaración: la RP utiliza las declaraciones proporcionadas por la cartera para verificar la identidad y el atributo del usuario mediante la firma PKI, así como las técnicas de validación basadas en valores generadores.

5) Autorización: la RP determina los servicios a los que se puede acceder en función de los resultados de las verificaciones de identidad.

- El diseño de los DID exige la existencia de un mecanismo resolutivo universal para cualquier DID. Este sigue siendo un tema de trabajo en curso de la comunidad DLT. En los modelos de identidad descentralizados, es necesario establecer una capa de autenticación de DID interoperable. Este asunto se sigue estudiando.
- La autentificación del DID permite al titular de la identidad tomar control del DID cuando interactúa con una RP. Para ello, ésta ha de ejecutar las siguientes etapas:

  1) la RP resuelve el DID del titular de la entidad a un documento DID;

  2) la RP trata de autentificar al titular de la identidad utilizando objetos de autentificación contenidos en el documento DID;

  3) los objetos de autentificación pueden incluir o remitir a objetos de clave pública, si la prueba del titular de la identidad se establece mediante una firma criptográfica.
- La autenticación de DID debe entenderse como ampliable en cuanto a la forma en que el titular de la identidad puede demostrar que tiene el control sobre el DID.

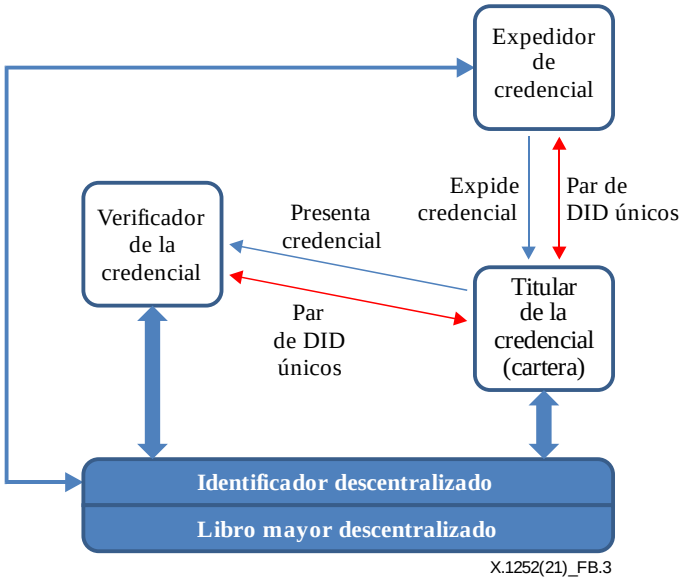


Figura B.3 – Cartera de identidad descentralizada con declaraciones verificables

Bibliografía

[b-UIT-T E.101] Recomendación UIT-T E.101 (2009), *Definición de los términos utilizados para los identificadores (nombres, números, direcciones y otros identificadores) para los servicios y redes públicos de telecomunicación en las Recomendaciones de la serie E*.

[b-UIT-T L.1410] Recomendación UIT-T L.1410 (2014), *Metodología para la evaluación de los efectos medioambientales del ciclo de vida de los bienes, redes y servicios de tecnologías de la información y la comunicación*.

[b-UIT-T X.501] Recomendación UIT-T X.501 (2019) | ISO/CEI 9594-2:2020, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Modelos*.

[b-UIT-T X.509] Recomendación UIT-T X.509 (2019) | ISO/IEC 9594-8:2020, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Marcos para certificados de claves públicas y atributos.*

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

[b-UIT-T X.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*.

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

[b-UIT-T X.1254] UIT-T X.1254 (2020), *Marco de garantía de autentificación de entidad.*

[b-UIT-T X.1400] Recomendación UIT-T X.1400 (2020), *Términos y definiciones sobre tecnología de libro mayor distribuido*.

[b-UIT-T X.1403] Recomendación UIT-T X.1403 (2020), *Directrices de seguridad para la utilización de la tecnología de libro mayor distribuido en la gestión descentralizada de identidades*.

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

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

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

[b-ISO/CEI 2382-37] ISO/CEI 2382-37:2017, *Tecnología de la información – Vocabulario – Parte 37: Biometría*.

[b-ISO/CEI 24760-1] ISO/CEI 24760-1:2019, *Seguridad y privacidad en las TI – Marco para la gestión de identidades – Parte 1: Terminología y conceptos*.

[b-ISO/CEI 29115] ISO/CEI 29115:2013, *Tecnología de la información – Técnicas de seguridad – Marco de garantía de autentificación de entidad*.

[b-OIX-TFIS] Makaay, E., Smedinghoff, T., Thibeau, D. (2017). *Trust frameworks for identity systems*, Serie de estudios sobre marcos de confianza. *London: Open Identity Exchange. 18 pp*. Disponible [estado al 2021-05-17] en: https://connectis.com/wp-content/uploads/2018/05/OIX-White-Paper_Trust-Frameworks-for-Identity-Systems_Final.pdf

[b-W3C-DIDs] W3C (Internet), [sin título], Identificadores descentralizados (DID) … Cambridge, MA: World Wide Web Consortium. Disponible [estado al 2021-05-15] en: https://w3c.github.io/did-core/

[b-W3C-VC] W3C Working Group Note (2019), *Verifiable credentials use cases.* Cambridge, MA: World Wide Web Consortium. Disponible [estado al 2021-05-17] en: http://www.w3.org/TR/vc-use-cases/

SERIES DE RECOMENDACIONES DEL UIT-T

Serie A	Organización del trabajo del UIT-T
Serie D	Principios de tarificación y contabilidad y cuestiones económicas y políticas de las telecomunicaciones/TIC internacionales
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	Medio ambiente y TIC, cambio climático, ciberdesechos, eficiencia energética, construcción, instalación y protección de los cables y demás 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	Calidad de la transmisión telefónica, instalaciones telefónicas y redes de líneas locales
Serie Q	Conmutación y señalización, y mediciones y pruebas asociadas
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, redes de próxima generación, Internet de las cosas y ciudades inteligentes
Serie Z	Lenguajes y aspectos generales de soporte lógico para sistemas de telecomunicación

Impreso en Suiza
Ginebra, 2021