

Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1250

(09/2009)

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

Seguridad en el ciberespacio – Gestión de identidades

**Capacidades básicas para una mejor gestión y
compatibilidad de identidades a escala mundial**

Recomendación UIT-T X.1250

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.1250

Capacidades básicas para una mejor gestión y compatibilidad de identidades a escala mundial

Resumen

En la Recomendación UIT-T X.1250 se describen las capacidades básicas para lograr la gestión de identidades (IdM) y su compatibilidad a escala mundial (es decir, para mejorar el intercambio y la confianza en los identificadores que utilizan las entidades en las redes y servicios de telecomunicaciones/IT). La necesidad de la IdM, y las definiciones en este marco, dependen en gran medida del contexto y suelen estar sujetas a políticas y prácticas muy divergentes de los distintos países. Las capacidades comprenden la protección y el control de la información de identificación personal (IIP).

Historia

Edición	Recomendación	Aprobación	Comisión de estudios
1.0	ITU-T X.1250	2009-09-25	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.....	2
	3.1 Términos definidos en otros textos.....	2
	3.2 Términos definidos en esta Recomendación	2
4	Abreviaturas.....	3
5	Convenios	4
6	Generalidades	4
7	Capacidades de gestión y compatibilidad de identidades a escala mundial	5
	7.1 Ejemplos de modelos de transacción de la gestión de identidad.....	5
	7.2 Conjunto compatible de capacidades de gestión de identidad (IdM).....	9
	7.3 Cuatro componentes de identidad básicos.....	10
	7.4 Descubrimiento de las capacidades de identidad	12
	7.5 Compatibilidad e intermediación	13
	7.6 Seguridad de gestión de identidad	14
	7.7 Protección, control y utilización de información de identificación personal (IIP)	15
	7.8 Auditoría y cumplimiento.....	17
	7.9 Calidad de funcionamiento, fiabilidad y disponibilidad.....	17
	7.10 Internacionalización	18
	Bibliografía	19

Recomendación UIT-T X.1250¹

Capacidades básicas para una mejor gestión y compatibilidad de identidades a escala mundial

1 Alcance

En esta Recomendación se describen algunas capacidades básicas para mejorar la gestión y compatibilidad de las identidades a escala mundial al utilizar las redes y los servicios de telecomunicaciones públicas. Estas capacidades básicas se clasifican en los siguientes grupos funcionales:

- Modelos de gestión de identidad comunes y estructurados.
- Configuración de atributos (incluidos identificadores), credenciales y capacidades.
- Descubrimiento de los recursos, capacidades y federaciones de proveedores de servicio de identidad.
- Compatibilidad entre las plataformas de gestión, proveedores de servicio de identidad y federaciones de proveedores, incluidos los proveedores de servicio de identidad intermediarios.
- Seguridad y otras medidas para contrarrestar las amenazas y riesgos de seguridad, incluida la protección de los recursos de identidad, de la información de identificación personal y de la privacidad.
- Auditoría y cumplimiento, incluida la aplicación de políticas y la protección de información de identificación personal.
- Calidad de funcionamiento, fiabilidad y disponibilidad de las capacidades de gestión de identidad.

Hoy en día existen muy diversas redes y servicios de telecomunicaciones/IT, muy distribuidas e interconectadas, aunque fundamentalmente autónomas en lo que respecta a la gestión de identidades (IdM). Si bien estas redes y capacidades están evolucionando, su tamaño y complejidad pueden menoscabar la compatibilidad entre las capacidades de IdM. Por este motivo, las capacidades de IdM de esta Recomendación se basan fundamentalmente en las capacidades de red y los modelos generales existentes, incluidos los que se consideran efectivamente prácticas idóneas. No obstante, para lograr la gestión y compatibilidad de identidades a escala mundial, en esta Recomendación se describe un trayecto evolutivo y se muestra cómo aprovechar las capacidades existentes cuando ello es posible. También se define una capacidad de identidad intermediaria que pueden emplear muchas arquitecturas de sistemas de IdM y de apoyo para integrar las capacidades de IdM existentes.

La aplicación de capacidades de IdM en cada país está sujeta a los requisitos específicos de la legislación nacional.

NOTA – La utilización en esta Recomendación del término "identidad" en relación con la IdM no ha de entenderse en su sentido absoluto. En particular, no constituye una validación positiva de una persona.

2 Referencias

Ninguna.

¹ Es posible que esta Recomendación no pueda aplicarse en algunos países debido a su legislación nacional.

3 Definiciones

3.1 Términos definidos en otros textos

En la presente Recomendación se utilizan los siguientes términos, definidos en otros textos:

3.1.1 declarante [b-UIT-T Y.2720] y [b-UIT-T X.811]: Entidad que es la principal a la representada a efectos de la autenticación. El declarante dispone de las funciones necesarias para intervenir en intercambios de autenticación en nombre de una entidad.

3.1.2 información de identificación personal (IIP) [b-UIT-T Y.2720]: La información que tiene que ver con una persona viva, y que hace posible identificarla (lo que incluye la información que permite identificar a una persona cuando se combina con otra información, incluso cuando por sí sola no permite identificar claramente a esa persona).

3.1.3 parte confiante [b-UIT-T Y.2720]: Entidad que confía en la representación o declaración de identidad de una entidad solicitante/aseverante en un contexto de petición.

3.2 Términos definidos en esta Recomendación

En esta Recomendación se definen los siguientes términos:

3.2.1 agente: Una entidad que actúa en nombre de otra entidad.

3.2.2 anonimato: Propiedad a tenor de la cual una entidad no puede ser identificada dentro de un conjunto de entidades.

NOTA – El anonimato evita el rastreo de entidades o de su comportamiento, tales como la ubicación del usuario, la frecuencia con la que se utiliza un servicio, etc.

3.2.3 atributo: Información relacionada con una entidad que especifica una característica de la entidad.

3.2.4 autenticación: Véase autenticación de entidad.

3.2.5 garantía de autenticación: 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.

3.2.6 vinculación: Asociación, unión o vínculo explícitamente establecido.

3.2.7 declaración. Afirmación por parte del declarante del valor o valores de uno o varios atributos de identidad de una entidad digital, afirmación que en general se cuestiona o se pone en duda.

3.2.8 entidad: 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.

3.2.9 autenticación de entidad: Proceso encaminado a lograr suficiente confianza en la vinculación entre la entidad y la identidad presentada.

3.2.10 federación: Una asociación de usuarios, proveedores de servicio y proveedores de identidad.

3.2.11 identificador: Uno o más de los atributos utilizados para identificar a una entidad dentro de un contexto.

3.2.12 identidad: Representación de una entidad bajo la forma de uno o más elementos de información que permiten distinguir suficientemente a la(s) entidad(es) dentro del contexto. A los

efectos de la IdM, se entiende que el término identidad es 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.

3.2.13 proveedor intermediario de servicio de identidad: Proveedor de servicio de identidad que actúa como intermediario entre otros proveedores de servicio de identidad.

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

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

3.2.15 proveedor de servicio de identidad: Entidad que verifica, mantiene, gestiona y puede crear y asignar información de identidad de otras entidades.

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

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

3.2.18 seudónimo: 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.

3.2.19 entidad solicitante: Entidad que hace una representación o declaración de identidad a una parte confiante en un contexto de petición.

3.2.20 objeto terminal: Objeto (como una tarjeta SIM) que puede estar relacionado con un dispositivo terminal de red (como un teléfono móvil).

3.2.21 confianza: Firme creencia en la fiabilidad y veracidad de la información, o en la competencia de una entidad para actuar adecuadamente dentro de un contexto especificado.

3.2.22 usuario: Entidad que utiliza un recurso, por ejemplo sistemas, equipos, terminales, procesos, aplicaciones o redes empresariales.

3.2.23 centrado en el usuario: Un sistema IdM que puede proporcionar al usuario (IdM) la capacidad de controlar y hacer cumplir diversas políticas de privacidad y seguridad que rigen el intercambio de información sobre identidad, con inclusión de IIP, entre entidades.

4 Abreviaturas

En esta Recomendación se utilizan las siguientes abreviaturas:

DHCP Protocolo dinámico de configuración de ordenador principal (*dynamic host configuration protocol*)

ID Identificador (*identifier*)

IdM Gestión de identidad (*identity management*)

IDRF	Identificación por radiofrecuencias
IdSP	Proveedor de servicio de identidad (<i>identity service provider</i>)
IIP	Información de identificación personal
IT	Tecnología de la información (<i>information technology</i>)
NGN	Redes de la próxima generación (<i>next generation network(s)</i>)
SIM	Módulo de identidad del abonado (<i>subscriber identity module</i>)
URL	Localizador de recurso uniforme (<i>uniform resource locator</i>)

5 Convenios

Ninguno.

6 Generalidades

El crecimiento y la evolución de las capacidades de comunicación han propiciado la proliferación de numerosos servicios de comercio electrónico, transacciones electrónicas y cibergobierno. Las comunicaciones no son únicamente un recurso y las tecnologías de comunicación basadas en el protocolo Internet, como las NGN, se han convertido en una pieza fundamental para la realización de transacciones electrónicas cotidianas.

Las capacidades descritas en esta Recomendación tienen por objeto apoyar el desarrollo e implantación de capacidades de gestión de identidad estructuradas y compatibles dentro de un marco común a todos los sistemas de redes y servicios de telecomunicaciones/IT, sujeto no obstante a las políticas nacionales y regionales en materia de información y privacidad de identificación personal.

Las capacidades que se presentan en esta Recomendación comprenden:

a) **Ejemplos de modelos de gestión de identidad estructurados comunes**

La gestión de identidad suele conllevar la aseveración por parte de una entidad de algún tipo de identidad a otra parte vinculada a ella en el marco de una red o servicio de telecomunicaciones/IT. A fin de lograr el nivel de garantía de autenticación deseado, las partes deciden o solicitan la comunicación de información adicional entre ellas o con un tercero. El intercambio de información inicial puede contener un proceso de autenticación preferida o una delegación. Una parte o las dos que intervienen en el intercambio pueden elegir continuar con el anonimato o la seudonimia. Estos tipos de interacciones pueden representarse mediante modelos comunes cuyas capacidades se describen más adelante en esta Recomendación. Estos modelos permiten la configuración multipartita de las capacidades de identidad, si se desean o necesitan. Los modelos también resultan importantes para conseguir las capacidades IdM compatibles que se describen y emplean en redes tales como las NGN.

b) **Configuración y protección de credenciales, identificadores, atributos y capacidades de identidad patrón con niveles de garantía conocidos**

Estas categorías de información y su configuración, mantenimiento, utilización, rechazo y/o protección para alcanzar los niveles de garantía deseados son comunes a las actividades de gestión de identidad.

c) **Descubrimiento de recursos, capacidades y federaciones de proveedores de servicio de identidad**

Uno de los más graves problemas a que se enfrenta la IdM en un mundo de capacidades y aplicaciones de red muy dinámicas y diversas es el descubrimiento de las fuentes actuales

de identidad y los servicios que éstas proporcionan. Las capacidades de descubrimiento suelen ser necesarias para alcanzar los niveles de garantía deseados.

d) **Compatibilidad entre plataformas, proveedores y federaciones de identidad, con inclusión de los proveedores intermediarios de servicio de identidad**

En una infraestructura de capacidades y red pública muy distribuida con un gran número de usuarios nómadas y de proveedores, la gestión de la identidad puede conllevar un gran número de preguntas y respuestas entre las diversas partes y federaciones de las que pueden ser parte. La compatibilidad mundial entre partes que se encargan de las capacidades de gestión de la identidad es fundamental, y consiste en protocolos comunes bien conocidos para formular preguntas ante capacidades de identidad.

e) **Seguridad y otras medidas para contrarrestar las amenazas y riesgos de identidad, incluida la protección y el control de los recursos de identidad y la información de identificación personal**

Dado que estos recursos e informaciones de identidad son valiosos, sensibles y constituyen un componente fundamental de las redes, especialmente las que se consideran infraestructura nacional esencial y conciernen a la privacidad de las personas, es indispensable proteger los recursos y la información sobre la identidad basándose en el análisis de riesgos en el entorno de la IdM.

f) **Auditoría y conformidad, incluido el cumplimiento de las políticas y la protección de información de identificación personal**

La configuración de la gestión de identidad suele estar sujeta a diversas disposiciones jurídicas, reglamentarias, gubernamentales y comerciales que exigen un cierto nivel de capacidades de auditoría y conformidad. Estas capacidades son muy variadas, en particular: auditoría de la conformidad con la reglamentación, medidas de protección de la información de identificación personal, avisos a consumidores y el mantenimiento de la adecuada exactitud y trazabilidad temporal.

g) **Posibilidad de utilización y adaptación: calidad de funcionamiento, fiabilidad, internacionalización y operaciones de socorro**

Las capacidades de gestión de identidad se pueden utilizar y adaptar para acomodarse a la constante y muy distribuida evolución de los sistemas de identidad. Dado que de la información y los recursos de identidad depende que las entidades se autentifiquen entre sí, esto es, se acepten como asociados de la comunicación, suelen ser componentes de la infraestructura crítica y es posible que hayan de cumplir determinados niveles de calidad de funcionamiento, fiabilidad, disponibilidad y capacidades.

7 Capacidades de gestión y compatibilidad de identidades a escala mundial

En esta cláusula figuran distintos ejemplos de modelos de transacción de la gestión de identidad y se elabora un conjunto compatible de capacidades de gestión de identidad (IdM) y componentes básicos de identidad. También se examina el descubrimiento de capacidades, compatibilidad e intermediación de identidad, la seguridad de la gestión de identidad, la protección, control y utilización de información de identificación personal (IIP) y la auditoría y cumplimiento. Asimismo en esta labor se tiene en cuenta la internacionalización y la calidad de funcionamiento, fiabilidad y disponibilidad.

7.1 Ejemplos de modelos de transacción de la gestión de identidad

Una de las transacciones básicas de la gestión de identidad es el proceso de pregunta-respuesta comúnmente utilizado en el intercambio de información estructurada que se muestran en la figura 1. La forma más básica de intercambio de mensajes involucra a dos partes que utilizan un protocolo y un modelo de información acordados.

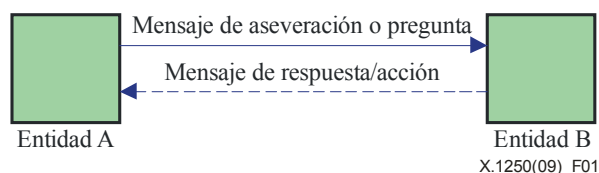


Figura 1 – Proceso básico de pregunta y respuesta para el intercambio de información

Las partes que participan en este proceso pueden ser cualquier tipo de entidad. 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. Puede tratarse de una persona, organización o institución, pero en términos más generales, puede ser cualquier objeto físico o virtual, como el equipo de red, el software, el dispositivo terminal, el sensor, el objeto físico activamente etiquetado (por ejemplo mediante identificación por radiofrecuencia (IDRF) o códigos ópticos) o el objeto pasivamente etiquetado. Los dispositivos de red, por ejemplo, pueden considerarse entidades sujetas a capacidades de IdM especiales en nombre de usuarios extremos, proveedores y autoridades gubernamentales. En el contexto de la gestión de derechos digitales, una entidad puede ser material protegido por la propiedad intelectual o el derecho de autor, como los multimedia o el contenido TVIP. Un tipo especial de identidad es el grupo. La identidad del grupo es la intersección de las identidades (atributos comunes) de los miembros del grupo.

En la mayoría de los casos, la gestión de identidad utiliza modelos complejos. Por ejemplo, cuando la parte confiante que recibe en primer lugar la declaración no es el proveedor de servicio de identidad, como se muestra en la figura 2a o 2b, la función del proveedor de servicio de identidad está separada y diferenciada de la parte confiante; la parte confiante evalúa las respuestas del proveedor o proveedores de servicio de identidad y decide si el nivel de garantía de autenticación de la identidad es suficiente. La principal función del proveedor de servicio de identidad es gestionar la creación, actualización, verificación, suspensión y supresión de información acerca de la identidad.

Existen muchos modelos posibles para el intercambio de información sobre la identidad. Uno de los más utilizados es el modelo de pregunta-respuesta que ilustra la figura 2a. Algunos de los nuevos protocolos IdM abiertos se basan en este modelo.

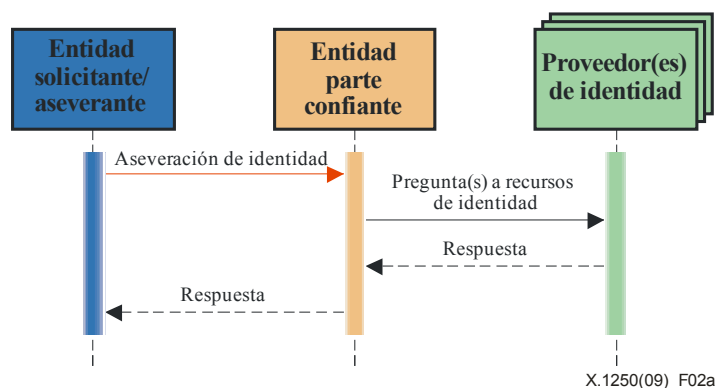


Figura 2a – Ejemplo de modelo tripartito de gestión de identidad

Otro modelo de gestión de identidad que ofrece mayor control a la parte solicitante de las relaciones de identidad es el de la figura 2b.

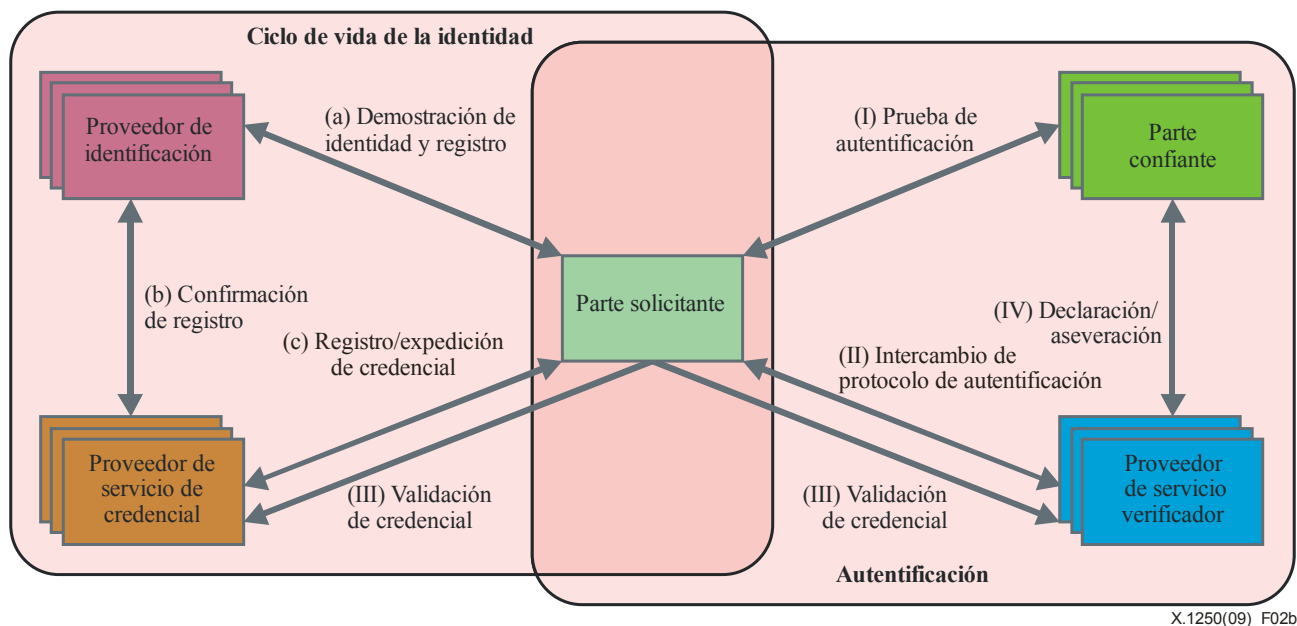


Figura 2b – Ejemplo de modelo pentapartito de gestión de identidad centrado en el usuario

Los modelos "centrados en el usuario" (es decir, modelos que requieren la activación del control pleno por la parte solicitante para la utilización de sus identidades) están recibiendo una atención considerable y pueden llegar a ser obligatorios en las legislaciones nacionales y regionales. En la figura 2b se muestra un ejemplo en que las funciones y capacidades especializadas de gestión de identidad proceden de distintos proveedores de servicio. Todas las preguntas/respuestas se formulan a través de la parte solicitante. A los efectos de este tipo de modelos se definen las siguientes entidades:

- **Proveedor de identidad:** Entidad que mantiene y gestiona y puede crear información de identidad fiable de otras entidades (por ejemplo, usuarios, organizaciones y dispositivos) y que ofrece servicios de identidad basados en la confianza. Esta entidad, que es responsable de la asignación y expedición también se denomina inscripción de atributos (por ejemplo relacionados con la identidad (como un abonado para un proveedor de credenciales) para un contexto específico), es asimismo responsable de la gestión del ciclo de vida de la identidad, que comprende la demostración, registro y mantenimiento de la identidad, incluida su revocación.
- **Proveedor de servicios de credencial:** Entidad que ofrece las capacidades relacionadas con la expedición de credenciales y testigos (por ejemplo, credenciales que vinculan testigos identificadores y atributos verificables).
- **Proveedor de servicios de verificación:** Entidad que ofrece las capacidades de evaluación de la información de identificación (por ejemplo declaraciones y credenciales) y de clasificación de su validez.
- **Parte confiante** [b-UIT-T Y.2720]: Entidad que confía en la representación o declaración de identidad de una entidad solicitante/aseverante en un contexto de petición.

En general, las actividades de pregunta-respuesta pueden clasificarse en dos categorías:

a) Ciclo de vida de la identidad

- **Registro y demostración de identidad (es decir, inscripción):** Este flujo de información representa la inauguración de una entidad dentro de un contexto específico, es decir, los procesos de registro y demostración asociados con la asignación de atributos relacionados con la identidad de esa entidad en ese contexto. Por ejemplo, puede conllevar la verificación y pruebas documentales de que una persona real está asociada con un nombre de abonado o un pseudónimo.
- **Confirmación de registro:** Este flujo de información representa las interacciones entre un proveedor de servicio de identidad y un proveedor de servicios de credencial para confirmar las identidades registradas.
- **Registro/expedición de credenciales:** Este flujo de información representa el intercambio de información entre el proveedor de servicios de credencial y la parte solicitante para registrar una identidad y obtener las credenciales que vinculan testigos a un nombre o pseudónimo y otros atributos asociados con la entidad.

b) Autenticación y aseveración

- **Aseveración:** Este flujo de información representa el intercambio de información entre la parte confiante y el proveedor de servicio de verificación para obtener una clasificación de la declaración.
- **Prueba de autenticación:** Este flujo de información representa a una parte confiante poniendo a prueba a una parte solicitante para su autenticación, o instándola a autenticarse. Por ejemplo, la parte confiante puede redirigir a la parte solicitante hacia un proveedor de servicio de verificación específico, o la parte solicitante puede escoger un proveedor de servicio de verificación específico.
- **Intercambio de protocolo de autenticación:** Este flujo de información representa el intercambio de mensajes de protocolo para la autenticación de la parte solicitante por parte del proveedor de servicio de verificación.
- **Validación de credenciales:** Este flujo de información representa el intercambio de información entre el proveedor de servicio de verificación y el proveedor de servicio de credenciales para validar las credenciales, si es necesario.

Los modelos descritos en la presente Recomendación no son exhaustivos. El objetivo es que sean flexibles, y pueden incluir contextos en que haya muchos proveedores de servicio de identidad y en que las partes solicitante o confiante también sean proveedores de servicio de identidad.

c) Variación de las aseveraciones

- **Delegación:** Una aseveración puede contener también una expresión de una validación preferida o una "delegación". Una expresión de una validación preferida informa a la parte confiante del proveedor de servicio de identidad al que debe preguntar, siempre y cuando la parte confiante pueda establecer una cadena de confianza con el proveedor de servicio de identidad preferido. Las delegaciones son un medio de acomodarse a situaciones en que una entidad actúa en nombre de otra entidad. Estas delegaciones son comunes, por ejemplo, cuando un padre actúa en nombre de su hijo, un adulto actúa en nombre de otro adulto incapacitado, un empleado actúa en nombre de una empresa o un abogado actúa en nombre de un cliente, o el Estado en nombre de un ciudadano o viceversa.
- Las delegaciones pueden emplearse para dar a la entidad delegada parte de las capacidades o derechos autorizados asignados a la entidad a la cual corresponde la identidad. En estos casos, la pregunta de la parte confiante al proveedor de servicio de identidad puede incluir peticiones adicionales para verificar que el delegante ha

registrado al delegado como agente autorizado. Esta petición se realiza además de la autenticación del agente. Es posible que existan relaciones de identidad compartida o delegada entre muchas entidades en estos modelos. El alcance de la cadena de delegación (es decir, la delegación de una delegación) depende de la tecnología disponible así como de las leyes, reglamentos o régimen empresarial, federativo y jurídico.

- **Anonimato y seudonimia:** Las entidades también pueden aseverar una identidad anónima o seudónima. En estos casos, el nivel de garantía de la identidad depende de factores externos que la parte confiante habrá de tomar en consideración, por cuanto no puede alcanzarse el nivel de garantía de la entidad. La anonimidad y la seudonimia pueden utilizarse cuando la actividad que se lleva a cabo no requiere una verificación real de la identidad (por ejemplo, cuando la actividad es tan banal que no se necesita gestionar la identidad). Por otra parte, algunas leyes, reglamentos o políticas de protección de datos pueden requerir la utilización de seudónimos o el anonimato.

7.2 Conjunto compatible de capacidades de gestión de identidad (IdM)

La gestión de identidad ha surgido como una capacidad común a todas las capas de los modelos de red básicos, por ejemplo las NGN [b-UIT-T Y.2012], [b-UIT-T Y.2720]. Las capacidades IdM se utilizan en la parte de aplicaciones para el control de servicio de red, como parte de la función de transporte subyacente y en las capacidades de gestión empleadas para administrar estas capas.

Existe con frecuencia una falta de coordinación entre estas capas en lo que respecta a la gestión de identidad. En la medida en que lo permitan las políticas regionales o nacionales a este respecto, deben preverse capacidades IdM compatibles en cada capa de la red.

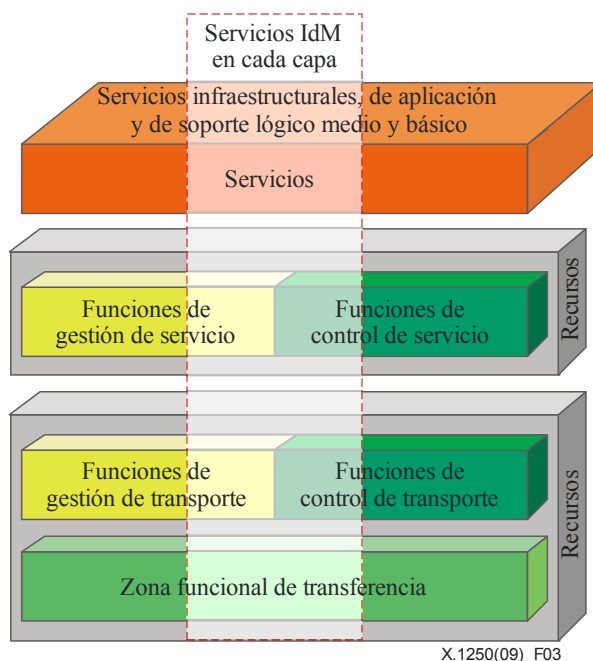


Figura 3 – Alcance de la compatibilidad en las capas de red para la gestión de identidad

La figura 3 ilustra que pueden existir capacidades IdM en todas las capas verticales de la arquitectura de red, y que son necesarias la sincronización y la armonización.

7.3 Cuatro componentes de identidad básicos

A fin de facilitar la compatibilidad de las capacidades de IdM, en la presente Recomendación se clasifica la información sobre la identidad en las siguientes cuatro categorías básicas:

- capacidades de identificadores;
- capacidades de credenciales;
- capacidades de atributos;
- capacidades de pautas.

Pueden utilizarse combinaciones de estas cuatro categorías de información de identidad para ofrecer mayor nivel de granularidad en la garantía de identidad; y pueden proporcionarse como capacidades de identidad individuales o en combinación con distintas entidades, como se muestra en la figura 4. Esta figura puede interpretarse como una ampliación de la figura 2. Por regla general se utiliza el modelo de pregunta-respuesta. No es necesario utilizar todas estas capacidades de identidad en una sola aplicación de IdM. Su utilización y existencia en tanto que capacidades, depende del contexto IdM, particularmente el nivel de garantía de autenticación de la entidad deseado o exigido.

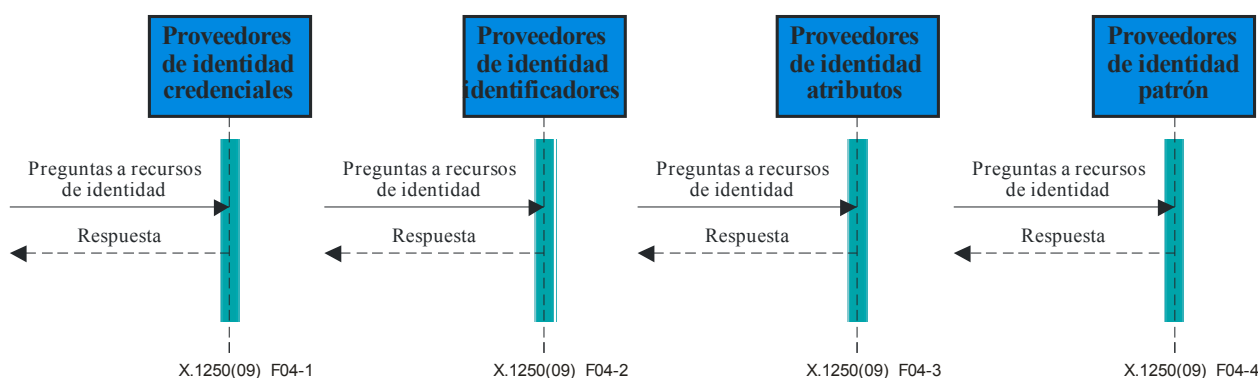


Figura 4 – Ejemplo de las cuatro capacidades básicas de pregunta-respuesta acerca de la identidad

La distinción entre estas capacidades de identidad en la práctica puede ser difusa. Por ejemplo, las credenciales tienen sus propios identificadores y los proveedores mantienen alguna información de atributo relativa a la identidad asociada a que pertenecen las credenciales, y el proveedor puede mantener un registro cronológico de la utilización de las credenciales que a su vez utiliza para realizar un análisis patrón a fin de minimizar el robo de identidad y el fraude.

Los proveedores de IdM, al igual que los proveedores de servicios de telecomunicaciones/IT o financieros, o cualquier institución u organización con una relación especial con el usuario extremo o el cliente, pueden ofrecer todas estas capacidades como un todo indivisible. El grado de "apertura de IdM" y de compatibilidad con los proveedores IdM se basará en la confianza o la afinidad de necesidades, las relaciones comerciales y los requisitos reglamentarios o jurídicos.

7.3.1 Capacidades de identificadores

Los identificadores son atributos (por ejemplo nombres) generalmente asignados a una entidad a los efectos de gestión de los sistemas de información o comunicaciones. Normalmente su aplicación es especializada. Por ejemplo, los números de teléfono, los URL o las direcciones de correo electrónico se utilizan tanto para acceder al servicio/dispositivo como para el encaminamiento por redes de comunicaciones.

7.3.2 Capacidades de credenciales

Las credenciales se emplean como apoyo a la autenticación de entidades, ya sea una o ambas partes que intervienen en una transacción o intercambio de información. Una de las primeras y aún más utilizadas formas de credencial certificada es la que se basa en la norma de certificado digital UIT-T X.509 [b-UIT-T X.509]. Otros tipos de credencial son las credenciales expedidas por el Estado, tarjetas de identificación laboral, tarjetas SIM móviles inalámbricas y tarjetas de crédito de instituciones financieras o para cajeros automáticos.

A veces, las credenciales incluyen representaciones biométricas. Algunas aplicaciones requieren la capacidad de verificar rápidamente que las credenciales son válidas y no se han revocado. Sin embargo, hay que tener en cuenta que las comprobaciones de credenciales pueden dar lugar a mucha información de rastreo por los IdSP, lo que puede representar un riesgo de privacidad. Por consiguiente, son importantes las credenciales fuertes, que no requieran comprobaciones.

La complejidad de utilización y gestión de credenciales digitales por parte del público en general a gran escala puede reducirse mediante la adopción de métodos de IdM centrados en el usuario, junto con las capacidades de gestión de credenciales, tales como carteras electrónicas [b-UIT-T X.1251]. Dependiendo del contexto, la credencial de usuario puede incluir la capacidad de utilizar diversas credenciales para adaptarse a distintos niveles de garantía de autenticación de entidades requeridos.

7.3.3 Capacidades de atributos

Los atributos son características de las entidades que se suelen obtener de manera relativamente estática como parte en el proceso de asignación de credenciales o identificadores (por ejemplo, nombres, dirección física, información de contacto, etc.). En otros casos, como el de la ubicación geoespacial de la entidad, los atributos pueden ser muy dinámicos.

Las capacidades de descubrimiento y consulta de atributos pueden requerir protocolos compatibles especializados, que generalmente efectúan algún tipo de verificación, en especial cuando concierne a la IIP, para la protección y el control de información de identificación personal. Los protocolos y plataformas compatibles centrados en el usuario pueden ofrecer un medio para que el usuario extremo designe el modo en que ha de tratarse la información de atributo.

7.3.4 Capacidades de pautas

Las pautas de identidad son una expresión estructurada de los atributos de una entidad que podrían utilizarse en algunos procesos de identificación.

Las pautas pueden comprender la identidad observada o descubierta (es decir, no declarada o aseverada), por ejemplo información sobre la reputación o las transacciones habituales de una entidad. Esta información es particularmente importante para detectar el robo de identidad. Las capacidades de identidad de pauta especializadas también se emplean para soportar capacidades de ciberseguridad, como la firma de pauta de un virus o ataque a la infraestructura.

Al igual que las capacidades de identidad atributo, cuando el patrón se refiere a una persona real, la configuración tiene un alto potencial de ampliación y, en ocasiones, de conflicto entre federaciones y posibles requisitos jurídicos y reglamentarios, en especial para la protección de información de identificación personal. En algunos países, cuando la IIP resulta afectada, las capacidades de retención y análisis de datos relativos a pautas están sometidas a fuertes políticas de protección de datos y privacidad, incluyendo la prohibición de recopilación de datos y mecanismos de supresión de datos.

7.3.5 Capacidades generales de gestión de datos de IdM

Algunas capacidades de IdM se aplican a la gestión de sistemas de IdM y a la gestión de los datos de IdM para todas las capacidades de identidad. Las capacidades han de soportar:

- la capacidad de que la parte solicitante pueda acceder/suprimir/modificar/supervisar/controlar su propia información de identidad, de acuerdo con las leyes, reglamentos y/o políticas aplicables;
- la capacidad de que las entidades autorizadas (por ejemplo administradores de sistema, padres, fuerzas de la seguridad, órganos de imposición legislativa y otros terceros autorizados) puedan acceder/modificar/supervisar su información de identidad, de acuerdo con las leyes, reglamentos y/o políticas aplicables;
- la importación/exportación de información de identidad, de acuerdo con las leyes, reglamentos y/o políticas aplicables;
- un mecanismo para indicar alguna clase de información sobre el nivel de calidad de la información que proporcionan a las partes confiantes. Esto exige llegar a un acuerdo entre las partes acerca del valor informativo;
- la capacidad de que una parte solicitante delegue la gestión de su información de identidad en otra entidad;
- la gestión del ciclo de vida de todas las identidades, incluido un medio para verificar rápidamente la situación actual de la información, de acuerdo con las leyes, reglamentos y/o políticas aplicables;
- un mecanismo común de identificar y controlar la divulgación de todas las identidades, de acuerdo con las leyes, reglamentos y/o políticas aplicables.

7.3.6 Niveles de garantía de las entidades

Los recursos y la configuración tienen asociados niveles de garantía muy variables, en función de un gran número de factores técnicos y administrativos, que son conformes con las políticas y normativas adecuadas al contexto.

Las capacidades comprenden:

- la indicación de niveles de garantía de la información de identificador pública, en especial a las autoridades de registro para las comunicaciones públicas, incluidos los identificadores subatribuidos en sistemas de denominación y numeración jerárquicos;
- un protocolo mutuo que indique el nivel de garantía asociado con la información proporcionada. Se recomiendan mecanismos abiertos y comunes a escala mundial;
- un mecanismo para que la parte solicitante, la parte confiante o, por ejemplo, el proveedor de servicio de identidad especifique la garantía y las condiciones de validez de un servicio de identidad, y especifique qué medida se ha de tomar en caso de incumplimiento de las condiciones.

7.4 Descubrimiento de las capacidades de identidad

Uno de los principales problemas de la IdM en el muy dinámico y diverso mundo de las capacidades y aplicaciones de red es el descubrimiento de fuentes para cada una de las cuatro capacidades de IdM fundamentales. Se dispone de una gran cantidad de fuentes autónomas y distribuidas. No basta con que simplemente existan capacidades de IdM. Las partes confiantes necesitan medios normalizados de conocer su existencia y saber cómo llegar a ellos, como se muestra en la figura 5 siguiente. El proceso de descubrimiento puede implicar el soporte de un nuevo protocolo de descubrimiento, semejante al protocolo dinámico de control de anfitrión, donde el cliente puede descubrir un servidor DHCP y adquirir una dirección IP e información de pasarela.

Por tanto, el proceso de descubrimiento puede ser tan simple como que un detentor de identidad facilite una URI u OID válida a una parte confiante.

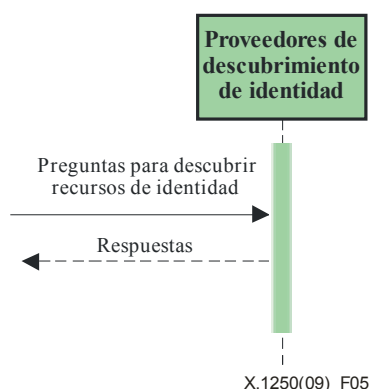


Figura 5 – Ejemplo de capacidades de pregunta-respuesta para el descubrimiento de identidad desde cualquier entidad

Además, el descubrimiento de las capacidades de identidad debe comprender el descubrimiento de las capacidades disponibles a través de federaciones. Algunas federaciones y comunidades que utilizan protocolos específicos han elaborado soluciones parciales para ajustarse a las necesidades de descubrimiento dentro de los límites de sus comunidades de usuarios. No obstante, en la actualidad no se dispone de medios de descubrimiento mundiales o interfederaciones. Sería conveniente contar con un sistema que soporte el descubrimiento y disponer de las siguientes capacidades de descubrimiento:

- políticas de acuerdo de actividad entre proveedores de servicio de identidad en federaciones u otros dominios;
- un único registro cronológico de entrada/salida y la publicación de esta capacidad de manera normalizada, de forma que pueda descubrirse.

7.5 Compatibilidad e intermediación

La compatibilidad a escala mundial entre las partes que facilitan los recursos de gestión de la identidad forma parte fundamental de los requisitos de configuración. En esta cláusula se describen las capacidades para entablar preguntas en una federación o a través del proveedor intermediario.

Las federaciones se basan en el principio de aceptación mutua de los resultados de autenticación entre los dominios participantes, y no en el de intercambio de la información de identidad entre esos dominios.

7.5.1 Capacidades relativas a la federación

Las capacidades relativas a la federación incluyen:

- la capacidad de una parte confiante para establecer un dominio de autenticación (es decir, seguridad) mediante alianzas y la participación en federaciones;
- la obtención de autorización de la parte solicitante para federar las identidades de las partes solicitantes, de acuerdo con las leyes, reglamentos y/o políticas aplicables;
- la capacidad de que una parte solicitante delegue la autoridad para federar su identidad, de acuerdo con las leyes, reglamentos y/o políticas aplicables.

7.5.2 Capacidades relativas al proveedor intermediario de identidad

Las capacidades relativas al proveedor intermediario de identidad incluyen:

- la capacidad de que una parte solicitante pueda establecer permisos y prohibiciones sobre capacidades de intermediación de identidad;
- un mecanismo para descubrir al proveedor de servicio de identidad de las partes solicitantes conexas;
- un mecanismo de intermediación de identidad para:
 - a) permitir la federación de cuentas de partes solicitantes en un proveedor de servicio de identidad y una parte confiante en distintos dominios de autenticación, siempre y cuando ambos tengan los correspondientes permisos de la parte solicitante y del proveedor intermediario de servicio de identidad, y
 - b) el transporte de la dirección de un proveedor de servicio de identidad en respuesta a un mensaje a una parte confiante;
- un mecanismo para lograr la compatibilidad de la información de la parte solicitante obtenida de un proveedor de servicio de identidad y que pueda ser reconocida y utilizada por el proveedor de servicio de identidad y las partes confiantes conexas en distintos dominios (por ejemplo, dos redes);
- en caso de que se cree una federación a través de un proveedor intermediario de servicio de identidad, un medio para notificar a la parte confiante o al proveedor de servicio de identidad los cambios acaecidos en las políticas del proveedor intermediario de servicio de identidad. Este mecanismo permite a la parte confiante o al proveedor de servicio de identidad dar por terminada su participación en la federación;
- en caso de que se cree una federación a través de un proveedor intermediario de servicio de identidad, un medio para notificar a la parte solicitante los cambios acaecidos en las políticas del proveedor intermediario de servicio de identidad. Este mecanismo permite a la parte solicitante dar por terminada la aceptación y la participación en la federación.

7.6 Seguridad de gestión de identidad

Dado que la información de identidad y los recursos de red que proporcionan las capacidades de identidad son componentes valiosos, sensibles y fundamentales de la red, especialmente los que se consideran parte de la infraestructura nacional crítica, es necesario que estén protegidos. La seguridad de una infraestructura de IdM conlleva políticas administrativas, prácticas operativas, tecnologías y técnicas para evitar que los sistemas y datos de IdM corran peligro alguno, estén estáticos o en tránsito.

Esta cláusula suplementa las prácticas idóneas de seguridad expuestas en [b-UIT-T X.1205] con otras capacidades de seguridad de las infraestructuras de IdM, que comprenden:

- transacciones seguras (por ejemplo, con confidencialidad, integridad, protección antirreproducción) entre todas las partes (partes solicitantes, partes confiantes, proveedores de servicio de identidad);
- mecanismos contra el repudio de las transacciones de IdM;
- protección del descubrimiento de capacidades de identidad contra, por ejemplo, la usurpación de identidad del proveedor de servicio de identidad;
- información de seguridad para la auditoría de las transacciones de IdM;
- la aplicación de capacidades para detectar intrusiones y responder a las mismas, basadas en el análisis de transacciones de IdM, y posiblemente alertar a los propietarios de la identidad sobre presuntos ataques a su información de identidad;

- la facilitación de medios para que las partes confiantes puedan informar rápidamente a los proveedores de servicio de identidad sobre la puesta en peligro de la identidad; y asegurar esta capacidad de informe contra la explotación.

Las políticas y directivas de utilización, en ocasiones denominadas "gobernanza de identidad", también son medidas importantes en un entorno de múltiples proveedores de servicio de identidad para mitigar las amenazas y riesgos, además de proteger la información de identificación personal. Cuando atañen a federaciones, alianzas o proveedores intermediarios, estas medidas pueden ser promulgadas por todas las partes confiantes y proveedores de servicio de identidad participantes. El creciente uso de aplicaciones de IdM centradas en el usuario también puede exigir que los usuarios extremos especifiquen políticas vinculadas con sus atributos de identidad, como se describe y recomienda en la cláusula 7.7. La aplicación de capacidades de seguridad comunes entre los participantes en una federación tiene beneficios importantes y las federaciones deben disponer de especificaciones de seguridad muy desarrolladas.

Conviene disponer de las siguientes capacidades de política y seguridad de las IdM:

- capacidades de garantía de autenticación de entidades en conformidad con las directrices aplicables;
- un mecanismo de no repudio de las transacciones de IdM;
- el establecimiento dinámico de mecanismos limitados en el tiempo para relaciones transitorias y cambiantes. Para ello puede ser necesario un proveedor intermediario mutuamente fiable que pertenezca a una o más federaciones;
- la seguridad entre federaciones, incluidos mecanismos de negociación para la comunicación segura entre federaciones y el intercambio de información entre las mismas en respuesta a amenazas de ciberseguridad;
- la capacidad de que las aplicaciones en objetos terminales tengan medios para autorizar el acceso a la información de identidad de usuario del objeto terminal, de acuerdo con las leyes, los reglamentos y la política aplicable;
- un mecanismo para que el proveedor de servicio de identidad notifique a todas las partes afectadas que una identidad está en peligro o se ha revocado;
- un método seguro de aprendizaje de las capacidades de identidad;
- registro de la información de seguridad para las transacciones de IdM con un nivel de detalle suficiente para determinar la responsabilidad y permitir la realización de análisis forenses;
- capacidades de detección de intrusión y respuesta para las transacciones de IdM;
- mecanismos para que las partes confiantes puedan informar de la situación de peligro de una identidad.

7.7 Protección, control y utilización de información de identificación personal (IIP)

La protección de la información de identificación personal tiene varias facetas. Dos de ellas incluyen la utilización de capacidades de seguridad en la infraestructura de IdM y la utilización de capacidades que aportan transparencia y notifican a las entidades la utilización de su información de identidad, además de la capacidad de vincular sus preferencias con respecto a tal información. En este contexto, la "vinculación" consiste en algún tipo de mecanismo permanente que permita a terceros adueñarse de la información de identidad para descubrir las capacidades de política IIP de la entidad asociadas. Las plataformas de productos centradas en el usuario y las capacidades de los proveedores intermediarios de servicio de identidad permiten con cada vez más frecuencia la utilización de estas preferencias.

De acuerdo con algunas legislaciones nacionales y regionales, la IIP ha de obtenerse de manera justa y de conformidad con un objetivo legítimo y explícito. La información conexas intercambiada entre partes comunicantes debe limitarse exclusivamente a los datos necesarios para que la "parte confiante" pueda prestar un servicio o un recurso a una parte solicitante.

Desde el punto de vista de la privacidad, algunas legislaciones nacionales contienen una serie de principios que han de tenerse en cuenta:

- la IIP vinculante debe recabarse para fines específicos, explícitos y legítimos y no debe procesarse de manera incompatible con dichos fines;
- la IIP debe ser adecuada, pertinente y no excesiva respecto de los fines para los que se ha recabado y/o procesado;
- la IIP debe ser precisa y mantenerse actualizada; deben tomarse las medidas necesarias para garantizar que los datos inexactos o incompletos se suprimen o corrigen, habida cuenta de los fines para los que se ha recabado y/o procesado;
- la IIP debe mantenerse en un formato que permita la identificación de objetos de datos durante no más tiempo del estrictamente necesario para los fines para los cuales se recabaron y/o procesaron;
- la IIP no debe intercambiarse entre aplicaciones para fines distintos;
- la IIP debe limitarse al mínimo necesario para un objetivo específico;
- la IIP debe protegerse. Deben adoptarse las medidas técnicas y organizativas adecuadas para proteger la IIP contra la destrucción accidental o ilícita, la pérdida, la alteración, la revelación o el acceso no autorizados, en particular cuando el procesamiento implica la transmisión de datos por una red, y contra toda forma ilícita de procesamiento;
- las personas tienen el derecho de acceder, modificar y suprimir su IIP;
- la IIP no debe guardarse durante más tiempo del necesario para los fines definidos.

Otras jurisdicciones requieren mecanismos de protección que incluyen la utilización de notificaciones cuando se accede a la cuenta o se modifica la información. La utilización de la IIP en las redes y servicios de telecomunicaciones/TIC ha de realizarse de acuerdo con un objetivo final explícito. Es con respecto a tal objetivo final que se puede apreciar la pertinencia, adecuación y cantidad precisa de los datos registrados, las categorías de personas u organizaciones que pueden recibirlos y la duración durante la cual se pueden almacenar los datos recogidos.

Las capacidades comprenden:

- la recopilación, procesamiento y protección de la IIP de conformidad con los principios y la legislación en materia de protección de datos y privacidad. Como mínimo, la protección ha de comprender la especificada por la OCDE en las directrices mundiales de privacidad. Las reglamentaciones regionales/nacionales aplicables pueden imponer requisitos obligatorios adicionales (por ejemplo, la Directiva Europea sobre Protección de Datos 95/46/CE);
- protección de los límites reconocidos para minimizar la recopilación de información de identificación personal. La IIP ha de obtenerse para fines específicos, explícitos y legítimos únicamente con el consentimiento del sujeto en cuestión;
- funciones tales como cuando un proveedor de servicio de identidad ha federado por su cuenta la identidad de una parte solicitante con dos o más partes confiantes, estas últimas no han de poder utilizar dicha información para determinar que las identidades se refieren a la misma parte solicitante;
- un servicio de notificación cuando se modifiquen los atributos de identidad de la parte solicitante;
- un servicio de notificación cuando se modifiquen las declaraciones de consentimiento de la parte solicitante;

- envío de una alerta a los propietarios de la identidad sobre transacciones de IdM interpretadas por el proveedor de servicio de identidad como una amenaza a sus identidades;
- envío de una notificación a los propietarios de la identidad de las amenazas a los sistemas y capacidades de los proveedores de servicio de identidad;
- la posibilidad de imponer una duración máxima al almacenamiento de la IIP, para que no se guarde durante más tiempo del estrictamente necesario para los fines definidos;
- la capacidad de que las entidades relacionadas puedan comprobar, corregir y suprimir la IIP conexas de acuerdo con las leyes, reglamentos y políticas.

7.8 Auditoría y cumplimiento

La IdM está sujeta a diversos requisitos jurídicos, reglamentarios e industriales que pueden necesitar un determinado nivel de auditoría y cumplimiento. Como ejemplos de medidas de auditoría y cumplimiento se pueden contar el mantenimiento de registros cronológicos de seguridad, la protección y utilización adecuada de la información personal y la notificación a las entidades a que pertenece la información. La auditoría ha de conformarse a las capacidades de protección de la IIP descritas en la cláusula 7.7 *supra*, especialmente debido al hecho de que otra nueva parte puede estar implicada y producirse un conflicto con las leyes, reglamentos y políticas en materia de privacidad.

Las capacidades incluyen:

- mecanismos para permitir la realización de análisis forenses;
- mecanismos mutuos y seguros para intercambiar información de auditoría de gestión de identidad;
- sellos de tiempo;
- la marcación de sellos de tiempo en función del contexto, con arreglo a la importancia de la información auditada y del valor temporal;
- la adopción de las medidas necesarias para garantizar que la auditoría de la gestión de identidad cumple los requisitos aplicables en materia de privacidad.

7.8.1 Capacidades de exactitud de sello de tiempo

Los sellos de tiempo exactos son muy importantes para gestionar el ciclo de vida de la identidad y mantener la seguridad en los sistemas de IdM, dado que toda la información de identidad existe dentro de unos límites temporales. La auditoría describe los eventos ocurridos dentro de esos límites. Para los fines de la auditoría los sellos de tiempo son esenciales, y la calidad, si no la posibilidad de utilización, de los datos auditados se determina por la exactitud de los sellos de tiempo en las ubicaciones correspondientes para poder auditar capacidades de red y aplicaciones distribuidas muy asíncronas. Convendría disponer, entre otras, de las capacidades de exactitud de sellos de tiempo suficientes para la auditoría en ubicaciones de referencia comunes acordadas, de conformidad con un nivel de garantía mutuamente acordado.

7.9 Calidad de funcionamiento, fiabilidad y disponibilidad

La IdM es una importante capacidad de red que ha de diseñarse y aplicarse para lograr objetivos de calidad de funcionamiento, fiabilidad y disponibilidad. Se recomienda que los objetivos de fiabilidad y disponibilidad de la IdM sean comparables a los de otras funciones de red críticas, pues las IdM forman el núcleo de la autenticación y autorización de acceso y de todas las transacciones en la red. Esto implica, por ejemplo, garantizar que la alimentación, soporte medioambiental y los objetivos conectividad de la IdM sean suficientes. La calidad de funcionamiento de la IdM (por ejemplo, tiempo de pregunta-respuesta) debe soportar la carga prevista de preguntas de la IdM.

La disponibilidad de un sistema de IdM no es homogénea en todos los componentes (elementos de expedición, elementos de búsqueda, elementos de revocación) y en último término ha de estar vinculada al nivel de garantía de la credencial. Los siguientes requisitos de disponibilidad son los más convenientes, pero diferirán de un componente de bloque de construcción a otro (depósito, sistema de inscripción, capacidad de revocación):

- habilidad y disponibilidad a niveles comparables a los de otros elementos, sistemas y capacidades de red críticos;
- incorporación de capacidades de IdM en los planes de recuperación de los proveedores en caso de catástrofe;
- aplicaciones de IdM con tiempos de respuesta razonables para las transacciones de IdM.

7.10 Internacionalización

La compatibilidad a escala mundial necesita que se puedan utilizar diversos juegos de caracteres e idiomas. Los objetivos de internacionalización se reconocen como un elemento importante del diseño y el soporte de todas las aplicaciones de red públicas, incluidas las capacidades de IdM.

Bibliografía

- [b-UIT-T X.509] Recomendación UIT-T X.509 (2005) | ISO/CEI 9594-8:2005, *Tecnología de la información – Interconexión de sistemas abiertos – El directorio: Marcos para certificados de claves públicas y atributos.*
- [b-UIT-T X.805] Recomendación UIT-T X.805 (2003), *Arquitectura de seguridad para sistemas de comunicaciones extremo a extremo.*
- [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 autenticación.*
- [b-UIT-T X.1205] Recomendación UIT-T X.1205 (2008), *Aspectos generales de la ciberseguridad.*
- [b-UIT-T X.1251] Recomendación UIT-T X.1251 (2009), *A framework for user control of digital identity.*
- [b-UIT-T Y.110] Recomendación UIT-T Y.110 (1998), *Principios y marco de la infraestructura mundial de la información.*
- [b-UIT-T Y.2012] Recomendación UIT-T Y.2012 (2006), *Requisitos y arquitectura funcional de las redes de la próxima generación, versión 1.*
- [b-UIT-T Y.2702] Recomendación UIT-T Y.2702 (2008), *Requisitos de autenticación 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 la red de la próxima generación.*
- [b-IETF RFC 2560] IETF RFC 2560 (1999), *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.*

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