Unión Internacional de Telecomunicaciones

UIT-T

SECTOR DE NORMALIZACIÓN
DE LAS TELECOMUNICACIONES
DE LA UIT

X.1255

(09/2013)

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

Seguridad en el ciberespacio – Gestión de identidades

Marco para la indagación de información de gestión de identidades

Recomendación UIT-T X.1255

Unión Internacional de Telecomunicaciones

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	
Aspectos generales de la ciberseguridad	X.1500–X.1519
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 heurística 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.1255

Marco para la indagación de información de gestión de identidades

Resumen

La finalidad de la Recomendación UIT-T X.1255 es describir una arquitectura marco abierta que permita la indagación de información de gestión de identidades (IdM). Esta información IdM se representará necesariamente de diferentes maneras y contará con el soporte de diversos marcos de confianza u otros sistemas IdM que utilizan estructuras de metadatos diferentes. Este marco, por ejemplo, permitirá a las entidades que funcionan en el contexto de un sistema IdM resolver con exactitud identificadores procedentes de otros sistemas IdM. Sin la capacidad de indagar este tipo de información, se deja a criterio de los usuarios y organizaciones (o los programas que actúan en su nombre) la forma más idónea de determinar la credibilidad y autenticidad de la identidad correspondiente, ya sea un usuario, un recursos del sistema, información u otras entidades. A partir de esta información, el usuario o la organización determina si confía o no en un determinado marco de confianza u otros sistema IdM a tal efecto. Los componentes fundamentales del marco descrito en la presente Recomendación son: 1) un modelo de datos de entidades digitales, 2) un protocolo interfaz de entidades digitales, 3) uno o varios identificadores/sistemas de resolución y 4) uno o varios registros de metadatos. Estos son los componentes básicos de la arquitectura marco abierta.

Historia

Edición	Recomendación	Aprobación	Comisión de Estudio
1.0	ITU-T X.1255	2013-09-04	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 no ha recibido notificación de propiedad intelectual, protegida por patente, que puede ser necesaria para aplicar esta Recomendación. Sin embargo, debe señalarse a los usuarios que puede que esta información no se encuentre totalmente actualizada al respecto, por lo que se les insta encarecidamente a consultar la base de datos sobre patentes de la TSB en la dirección http://www.itu.int/ITU-T/ipr/.

ÍNDICE

Recomendación UIT-T X.1255

Marco para la indagación de información de gestión de identidades

1 Alcance

La indagación de información de gestión de identidades consiste en la capacidad de obtener información pertinente acerca de identificadores, comprendidos los que utilizan la sintaxis de direcciones de correo electrónico y de URL, así como los identificadores invariables. La indagación es fundamental para lograr la compatibilidad entre sistemas de información heterogéneos.

El alcance de esta Recomendación corresponde a un marco que:

- permite indagar información relativa a la identidad y su procedencia, en particular la información que se dese identificar, como servicios, procesos y entidades;
- permite indagar atributos de la información relativa a la identidad, tales como logotipos visuales y nombres de sitios legibles;
- permite indagar atributos y la funcionalidad de aplicaciones;
- describe un modelo de datos y un protocolo a los efectos de permitir la compatibilidad a nivel de metadatos para la representación, el acceso y la indagación de información en entornos IdM heterogéneos.

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.

[ISO 8601] ISO 8601:2004, *Data elements and interchange formats – Information interchange – Representation of dates and times*.

3 Definiciones

3.1 Términos definidos en otros documentos

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

3.1.1 entidad [b-UIT-T Y.2720]: Todo lo que tiene existencia separada y distinta y puede identificarse unívocamente. Ejemplos de entidad en el contexto de la gestión de identidad, son los siguientes: abonados, usuarios, elementos de red, redes, aplicaciones de soporte lógico, servicios y dispositivos. Una entidad puede contar con múltiples identificadores.

3.1.2 proveedor de identidad [b-UIT-T Y.2720]: Entidad que crea, mantiene y gestiona información digna de confianza sobre la identidad de otras entidades (por ejemplo, usuarios/abonados, organizaciones y dispositivos) y ofrece servicios de identidad basados en relaciones de confianza, negocio y otros tipos de relaciones.

3.1.3 parte dependiente [b-UIT-T Y.2720]: Entidad que depende de una representación o declaración de identidad de una entidad solicitante/asertante.

3.1.4 confianza [b-UIT-T Y.2720]: Medida de la dependencia con respecto al carácter, capacidad, solidez o verdad de alguien o algo.

3.2 Términos definidos en esta Recomendación

En la presente Recomendación se definen los siguientes términos:

3.2.1 asociación: Relación, en su caso, entre dos entidades identificadas.

3.2.2 entidad digital: Entidad representada o convertida en una estructura de datos independiente de la máquina formada por uno o varios elementos en formato digital que pueden analizarse sintácticamente por diferentes sistemas de información; la estructura contribuye a la compatibilidad entre diversos sistemas de información en Internet.

3.2.3 indagación: El acto o proceso de buscar o localizar determinada información, es decir, de obtener datos acerca de lo buscado.

3.2.4 elemento: Parte de una entidad digital formada por un par tipo-valor, donde el tipo representa el identificador invariable y resoluble y el valor la información digital correspondiente a dicho tipo.

3.2.5 registros federados: Colección de registros de metadatos compatibles y que tienen en común un conjunto de métodos para compartir información fiable y en un formato comprensible por todos ellos.

3.2.6 identificador: Secuencia de bits utilizada para obtener información acerca de la entidad digital que se desea identificar; por lo general, se efectúa a través de un sistema de resolución adecuado.

3.2.7 gestión de identidades: Mecanismo mediante el cual se verifica la información de gestión de identidades, ya sea para un usuario, un recurso de sistema, información u otras entidades.

3.2.8 información de gestión de identidades: Información relativa a la identidad que comprende todos los tipos de metadatos relacionados con la identidad, procedencia, asociación y confianza.

3.2.9 metadatos: Información estructurada que pertenece a la identidad de usuarios, sistemas, servicios, procesos, recursos, información u otras entidades.

3.2.10 identificador invariable: Identificador exclusivo que permite obtener información de estado acerca de la entidad digital y que es resoluble al menos mientras exista dicha entidad digital.

3.2.11 procedencia: Información relativa a cualquier fuente de información, comprendida la parte o partes que participan en su generación, introducción o que la avalan.

3.2.12 registro: Mecanismo para registrar metadatos sobre entidades digitales y almacena estructuras de metadatos, y que permite buscar identificadores invariables en el registro a partir de la utilización de estructuras de metadatos.

3.2.13 repositorio: Interfaz que acepta depósitos de entidades digitales, permite su almacenamiento y ofrece acceso seguro a los entidades digitales por medio de sus identificadores.

3.2.14 sistema de resolución: Sistema que acepta identificadores conocidos por el sistema y suministra información pertinente sobre el estado de la entidad identificada.

3.2.15 punto de contacto: Registro dentro de un sistema de registros federados que se selecciona para actuar de interfaz con un registro designado de otra federación, generalmente a efectos de reciprocidad.

3.2.16 marco de confianza: Sistema IdM en el que cada una de las diversas partes en una transacción adquiere un conjunto de compromisos verificables con sus contraparte; estos compromisos comprenden necesariamente: a) controles para ayudar a cumplir dichos compromisos; y b) soluciones en caso de que no se cumplan.

4 Abreviaturas y acrónimos

En la presente Recomendación se utilizan las siguientes abreviaturas:

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

Bits dígitos binarios (*binary digits*)

BNF Forma Backus normal (*backus normal form*)

DEIP Protocolo interfaz de entidades digitales (*digital entity interface protocol*)

DNA Ácido desoxirribonucleico (*deoxyribonucleic acid*)

ED Entidad digital

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

ID Identificador (*identifier*)

IdM Gestión de identidad (*identity management*)

IdP Proveedor de identidad (*identity provider*)

MAC Control de acceso al medio (*media access control*)

P2P entre pares (*peer-to-peer*)

PKI Infraestructura de clave pública (*public key infrastructure*)

RP Parte dependiente (*relying party*)

TCP Protocolo de control de transmisión (*transmission control protocol*)

TF Marco de confianza (*trust framework*)

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

XML Lenguaje de marcado extensible (*extensible markup language*)

5 Convenios

Ninguno.

6 Recomendaciones

En esta Recomendación se describe una arquitectura marco abierta para la indagación de información de gestión de identidades. Se abordan los siguientes temas:

a) concepto de confianza, aspecto importante en la gestión de identidades;

b) información relativa a la confianza, que puede utilizarse para determinar qué grado de fiabilidad depositar en una determinada parte de información IdM;

c) registros federados para la indagación;

d) arquitectura compatible para la federación; y

e) análisis de federaciones jerárquicas y punto a punto.

La indagación de información de gestión de identidades se basa en metadatos que se obtienen de un registro o sistema de registros federados. El marco comprende mecanismos para resolver identificadores invariables. Por lo general, los registros federados estarán administrados por múltiples partes y se basarán en el modelo de datos de entidades digitales para representar metadatos y en el protocolo de interfaz de entidades digitales para que tales registros sean compatibles. Se parte del supuesto de que se utilizarán múltiples estructuras y que cada registro proporcionará información acerca de sus estructuras de metadatos públicas y/o privadas mediante sus respectivos identificadores invariables. Los identificadores invariables de estructura privada podrán conocerse de manera pública, si así se desea, o mantenerse privado junto con las estructuras de metadatos correspondientes con el fin de limitar su utilización a determinadas comunidades.

En los Apéndices I y II figura, respectivamente, una descripción general de casos de utilización y un ejemplo de descripción BNF de un registro de tipo (BNF es una notación normalizada para representar gramáticas sin contexto).

6.1 Concepto de confianza

El término 'confianza' es un tecnicismo que tiene varias connotaciones. Confiar en una persona o un proceso significa generalmente tener cierto grado de confianza en el resultado de determinados eventos, aun cuando éstos no se especifiquen con exactitud. Ahora bien, al crear sistemas de indagación será necesario ser más específico. Afirmar sencillamente que A puede confiar en B no implica que A puedan confiar en B para todos los posibles resultados de un evento. Confiar en que B prestará un servicio por el que se ha pagado una determinada suma no significa lo mismo que confiar en que B mantendrá en secreto dicho pago o que no publicará los nombres de quienes han efectuado dicho pagos.

El aspecto más importante en los marcos de confianza es la gestión de identidades, es decir, saber si las partes en una determinada transacción son realmente quienes dicen ser. Sin embargo, la confianza en el resultado de una determinada transacción con una parte dada depende no solamente de la identidad de esa parte sino también de otros atributos de las afirmaciones y asertos formulados por dicha parte. Para evaluar coherentemente esos atributos es necesario disponer de un vocabulario o un conjunto de métricas que puedan aplicarse a dichos atributos. Estas medidas y descripciones podría aplicarlas un tercero que ejerza de agencia de calificación del marco de confianza, o se podrían promediar entre grupos de calificación de usuarios, como se hace en los sistemas de recomendación y otras aplicaciones de 'colaboración pública'. A continuación se describen las categorías recomendadas para estas mediciones y descripciones.

Solidez: Nivel de credibilidad. Probabilidad de que esta parte sea quien dice ser. Probabilidad de que lo que afirma la identidad sea cierto (por ejemplo, soy el autor de ese software y las regalías me pertenecen). Probablemente se expresa mediante un valor numérico o una letra.

Clasificación: Tipo de credibilidad que se afirma. Posibilidad de establecer categorías. La identidad es una categoría propiamente dicha. Otras categorías serían credibilidad financiera (por ejemplo, probabilidad de que una determinada parte actúa según lo previsto en una transacción financiera), privacidad (probabilidad de que una determinada parte mantenga en secreto la información que se compromete a no revelar) y grado de autoridad (por ejemplo, probabilidad de que la información recibida de una determinada parte sea exacta). Son igualmente posibles otras categorías más generales y también clasificaciones más detalladas dentro de cada categoría.

Longitud de la cadena de confianza: La fiabilidad de algunas transacciones depende de la cadena de confianza, considerada a menudo como una jerarquía de certificación o capas de software firmado por medios digitales. El concepto se aplica generalmente a todos los ámbitos de confianza: cuanto mayor sea la cadena respecto de un determinado punto, más débil será el nivel de confianza final. La longitud de esta cadena es un índice fundamental de la credibilidad de toda identidad u otra afirmación.

Todos estos (y muchos otros) son los atributos que podrían incluirse en los registros de metadatos que describen a proveedores de servicios, partes fiables y otros componentes que intervienen en las transacciones fiables.

6.2 Información relativa a la confianza

A continuación se examinan tres aspectos distintos de la información relativa a la confianza en lo que respecta a las funciones y actuaciones que intervienen en la indagación federada y los relativos a las entidades constituyentes que participan.

6.2.1 Información relativa a la confianza que figura en la respuesta a una indagación

El principal objetivo de la arquitectura abierta que se describe en la presente Recomendación es permitir la indagación de la información de gestión de identidades; ahora bien, la forma de determinar la confianza se deja al criterio del usuario. La arquitectura admite componentes/módulos opciones (software y hardware) que ofrezcan una funcionalidad o servicios adicionales. En este sentido, la arquitectura podría incluir facultativamente un marco de confianza, así como una respuesta a la indagación más completa/detallada con información relativa a la confianza e incluso la posibilidad de determinar la confianza. Las entidades externas podrán determinar si desean recibir directamente esta información de confianza. Además, tendrán la opción de desactivar esta función y recabar la información de confianza por cuenta propia o a partir de sus propias fuentes.

6.2.2 Confianza en el sistema de indagación

El sistema de indagación debe ser fiable, de modo que las partes externas tengan confianza al utilizar sus funciones para registrar información de gestión de identidades o acceder a la misma. Este tipo de confianza puede obtenerse por diversos medios, en particular mediante el establecimiento de métodos específicos y sus correspondientes políticas y procedimientos a efectos de fiabilidad. Puede consistir en la evaluación de los distintos componentes del marco, las acciones (medidas) adoptadas en caso de que los componentes o partes externas actúen indebidamente, y la adaptación de marcos de seguridad y privacidad sólidos. Sin embargo, la definición de la metodología exacta para obtener este tipo de confianza queda fuera del alcance de la presente Recomendación.

6.2.3 Partes externas que confían

La arquitectura debe admitir la utilización de procedimientos y políticas que incentiven a las partes externas dependientes a hacer uso de éstos para registrar información. Por motivos de seguridad, las entidades que intervienen directamente en la consignación de información de gestión de identidades deben poder controlar los datos introducidos en el sistema y detectar y/o evitar que se registre información falsa.

Debería permitirse solicitudes anónimas, pero muchas quizá no den lugar a respuestas útiles a no ser que la identidad del solicitante se conozca de antemano por otros medios. En tales casos, la validación de la identidad estará a cargo de una capacidad de gestión de identidades que se aplique a todos los componentes, usuarios/solicitantes inclusive. En este marco, un proveedor de identidad autorizado y reconocido asigna a cada componente un identificador invariable exclusivo que puede utilizarse para hallar la información correspondiente a dicho componente. Como se mencionó más arriba, no se hace hipótesis alguna acerca de la forma en que cualquier componente de una determinada instancia determina si confía o no en esta información.

En muchas solicitudes debe validarse la identidad del solicitante (la parte externa que solicita la indagación) antes de enviar una respuesta. En general, todos los solicitantes se evalúan antes de tomar cualquier medida. La arquitectura no presume que se haya de recurrir a una capacidad decisoria interna; ahora bien, antes de construir la respuesta definitiva a una solicitud de indagación, puede apelar a un mecanismo de decisión externa para obtener previamente el permiso de los proveedores de identidad.

6.3 Registros federados para la indagación

En la presente Recomendación se describe un sistema de registros federados con el fin de obtener metadatos y otra información relacionada con los identificadores, así como para encontrar y evaluar marcos de confianza y otros sistemas IdM. Los registros federados pueden colaborar para compartir sus entidades de metadatos, a reserva de las restricciones del caso. La información real que corresponde a estos metadatos puede almacenarse en sus respectivos registros (si dicho almacenamiento está autorizado), en uno o varios repositorios distribuidos; en algunos casos la información que corresponde a estos metadatos quizá no sea accesible por Internet. En este último caso, esta limitación se suele obtener al resolver la información relativa al estado de la entidad a partir del identificador; otra posibilidad sería dedicar un registro a consignar dicha información.

En un sistema de registros federados, un determinado registro puede consignar una entrada de metadatos correspondiente a una determinada entidad a un segundo registro, entrada que puede ser una copia íntegra de los metadatos originales registrados o bien un resumen de la entrada del registro original. La comunicación constará del registro original, o una variante del mismo, descrito de tal manera que pueda identificarse su procedencia y que sea característica del tipo de comunidad o domino representado por dicho registro. Así, el mismo registro inicial podría servir de punto de recopilación entre dominios para muchos otros registros y proporcionar un servicio de búsqueda que pueda remitir búsquedas a otros registros para recabar información adicional. Estos puntos de recopilación se denominan a veces puntos de contacto.

El diseño del componente registro de la arquitectura se basa en varios conceptos fundamentales. Además de exigir que cada entidad registrada tenga asignada un identificador, los metadatos consignados en el registro obedecen a una estructura de entidades digitales, cada uno con su correspondiente identificador, lo que permite referenciar por separado estos registros de metadatos; y sus identificadores permitirán obtener información actualizada sobre las entidades de metadatos, aun cuando los registros se trasladen de un registro a otro o estén disponibles en varios registros.

La arquitectura no limita en modo alguno el número de entidades de metadatos que pueden registrarse para una misma entidad digital. Pudiera ser conveniente generar múltiples entidades de metadatos para la misma información cuando ésta se considere desde diferentes perspectivas, para audiencias distintas, etc. La gestión de estos metadatos se simplifica mucho si se utilizan identificadores exclusivos e invariables: por ejemplo, puede determinarse fácilmente si dos registros de metadatos hacen o no referencia a la misma información subyacente. También pueden crearse entidades adicionales para relacionar entre sí varias entidades de metadatos de un modo tal que no se obtendrían los mismos resultados si se buscaran las entidades por separado.

La arquitectura permite relaciones muchos a muchos, en ambos sentidos, entre los repositorios y los registros. Un determinado registro puede consignar metadatos de las mismas entidades en múltiples registros; y un determinado registro puede aceptar metadatos procedente de múltiples repositorios. La recopilación de metadatos de múltiples repositorios en un mismo registro permite crear una federación de tales repositorios. Al permitir que dichos repositorios consignen metadatos sobre las mismas entidades en múltiples registros se logra que un mismo repositorio forme parte de múltiples federaciones, diferenciadas quizá por las diferentes comunidades a las que dan servicio, por las diferentes estructuras de metadatos que utilizan, por las distintas formas de indexación y búsqueda, y por otras capacidades.

Por último, una instancia de un registro puede federarse con otros registros. Múltiples registros pueden enviarse entre sí sus entidades de metadatos, o entidades que son una función de dichos registros de metadatos originales. Un determinado registro, Reg1, puede consignar una entrada de metadatos para un determinado objeto en un segundo registro, Reg2, que puede ser una copia íntegra de la entrada de metadatos original o un resumen del mismo. La comunicación constará de la entrada original, o una variante de la misma, integrada en una entidad digital de forma que indique su procedencia de Reg1 y que sea característico del tipo de comunidad o dominio representado por Reg1. Si Reg1 siempre está federado con Reg2, éste último podrá servir de punto

de recopilación entre dominios para muchos otros registros como el Reg1 y ofrecer un servicio de búsqueda que pueda remitir búsquedas a otros registros o directamente a las ED del caso, dependiendo del método utilizado para combinar e indexar los posibles registros de metadatos heterogéneos.

Si bien la presente Recomendación se concentra en la gestión de identidades, este tipo de sistemas también puede servir para indagar otros tipos de información en sistemas distribuidos complejos en Internet, como los de "Computación en Nube" o "Internet de las Cosas". La información necesaria para la resolución en los sistemas de registros federados se obtiene de sistemas IdM individuales. La utilización del mecanismo de indagación de la federación favorece la compatibilidad de sistemas IdM en general, permite a la entidad obtener información adecuada acerca de otros sistemas y ayuda a la generación de confianza en la utilización de identificadores de dichos sistemas.

Muchos grupos utilizan la tecnología de registro básica, algunos las versiones de código fuente abierto (*open source*) mientras que otros han desarrollado sus propias versiones patentadas basadas en especificaciones comunes. La federación se consigue mediante protocolos de compartición de información. Una parte importante para los futuros trabajos basados en la presente Recomendación será describir y formalizar estas especificaciones, con el fin de definir protocolos y procedimientos adecuados, junto con las correspondientes estructuras de metadatos, y determinar un enfoque comúnmente aceptable para mantener, en su caso, la privacidad. La forma de seleccionar o confiar en un determinado sistema IdM queda fuera del alcance de la presente Recomendación.

7 Arquitectura para la compatibilidad de registros federados

El sistema de registros federados que se describe en la presente Recomendación se basa en una arquitectura abierta que permite la compatibilidad entre cualesquiera sistemas de información (en el Apéndice I se describe una arquitectura representativa). Este sistema ofrece un mecanismo de autentificación de información y de acceso a información estructurada en la forma de entidades digitales y almacenada en sistemas de almacenamiento convencionales. Una entidad digital es una estructura de datos común que permite la compatibilidad entre sistemas en Internet; los elementos de una ED son material digital, a saber datos escritos, incluido un identificador invariable exclusivo de dicho material.

Para gestionar las entidades digitales se utilizan tres componentes arquitectónicos. Cada uno de estos componentes puede utilizarse por separado, pero son complementarios entre sí y juntos constituyen un sistema distribuido y ampliable para la gestión de información en Internet. Estos componentes son:

a) sistema identificador ampliable y distribuido para la identificación de ED y para la resolución de identificadores;

b) repositorios para acceder y gestionar entidades digitales; y

c) registros para la búsqueda e indagación federadas. El sistema distribuido integrado por estos tres componentes puede gestionarse por medio de protocolos y especificaciones de interfaz, en lugar de efectuar el mantenimiento continuo de componentes específicos.

Las entidades digitales constituyen el núcleo entorno al cual se construyen y gestionan todos los demás componentes y servicios. Estas entidades no sustituyen los formatos y las estructuras de datos existentes, sino que ofrecen una forma de representar estos formatos y estructuras que permite su interpretación uniforme y que, por ende, pueden transferirse de un sistema de información heterogéneo a otro, e incluso en los sistemas que evolucionan con el tiempo. Aunque parezca sencillo, la realización práctica de este modelo no es trivial y comprende un protocolo para interacción entre ED a través de repositorios. A los efectos de compatibilidad y para facilitar su referencia, todos los metadatos en la presente Recomendación son conformes con el modelo de datos ED.

El modelo de datos ED y el protocolo interfaz de entidades digitales para acceder a las ED, que se describe a continuación, junto con el identificador y/o el sistema de resolución, así como el método de registro/repositorio para acceder a las ED, constituyen el núcleo de la arquitectura abierta. Todos estos componentes permiten gestionar a largo plazo la información estructurada en entidades digitales gracias a la identificación inequívoca e invariable de los mismos, lo que ofrece un método para obtener información sobre el estado actual de los objetos, un servicio para obtener o bien utilizar las entidades, y un mecanismo para determinar los identificadores de ED basado en la información contenida en los registros de metadatos.

7.1 Modelo de datos de entidades digitales

El modelo de datos de ED que se describe a continuación facilita un mecanismo uniforme para representar entradas de metadatos en la forma de entidades digitales, y puede utilizarse además para representar otros tipos de información como ED. Se trata de un modelo lógico que permite múltiples formas de codificación y almacenamiento, así como un punto de referencia único (es decir, el identificador) para muchos tipos de información que pudieran estar disponibles en Internet. Cada ED consta de un conjunto intrínseco de atributos, una serie de atributos definidos por el usuario e integrados en uno o varios elementos, así como otros posibles elementos adicionales que contienen información, por ejemplo texto, vídeo o imágenes en formato digital. Todos estos elementos pueden ponerse a disposición a través de una especificación DEIP bien definida (véase la cláusula 7.2), que integre la capacidad de autentificación utilizando seguridad de clave pública y quizá otros mecanismos de autentificación que emplean API de niveles más altos y que pudieran aplicar los repositorios de ED. De esta forma se ofrece acceso a los ED con privacidad y seguridad.

El atributo fijo esencial de una ED es su correspondiente identificador invariable exclusivo, que puede resolverse para obtener información sobre el estado actual de la ED, en particular su ubicación, controles de acceso y validación, para lo cual se ha de presentar una solicitud de resolución al sistema de resolución. Ejemplos de otros atributos intrínsecos de ED son: fecha de la última modificación, fecha de creación y tamaño. Los usuarios tienen la opción de crear atributos definidos por ellos mismos con sus correspondientes permisos.

Los atributos que no forman parte específica del modelo de datos ED básico son el titular, la autentificación y las condiciones de acceso. Estos atributos serán una parte muy importante de la mayoría de las realizaciones prácticas de ED; no obstante, es poco probable que exista una solución única. La información acerca del titular y del control de acceso figurará probablemente en atributos ED ampliables o en elementos de datos separados. De este modo se obtiene una forma común de gestionar diversas estructuras de gestión de información y titularidad, así como múltiples tipos de autentificación y autorización, sin tener que suponer que todos los dominios y comunidades de usuarios utilizan el mismo mecanismo.

La combinación de un modelo de datos normalizado, un protocolo definido para la interacción con dicho modelo de datos y un sistema identificador/de resolución, es fundamental para la gestión coherente de información a largo plazo por Internet. El sistema de resolución debería ser un sistema distribuido, seguro y de alto rendimiento, concebido para permitir la referencia invariable a entidades digitales durante largos periodos de tiempo con independencia de la ubicación, el método de acceso, el título y de otros atributos variables.

La capacidad esencial de detectar información IdM es consecuencia de la utilización del componente registro, que comprende el repositorio. La función de un determinado registro es la federación de varias colecciones de ED, lo que permite a los usuarios y las aplicaciones realizar búsquedas y navegar por el universo de entidades registradas. Los repositorios que contienen colecciones de ED pueden consignar metadatos sobre las ED que son de su responsabilidad en uno o varios registros. Un mismo registro puede recabar metadatos de múltiples repositorios y un mismo repositorio puede enviar metadatos a múltiples registros. Estos registros pueden disponer de

funciones de búsqueda y notificación acerca de las entidades representadas y servir de punto de entrada al mundo estructurado de ED y repositorios.

Puede darse la situación en la que los registros no sean estrictamente necesarios, por ejemplo cuando se incluye una referencia directa a una ED, a saber, su identificador, en otra ED, en un mensaje o en otro documento. No obstante, en muchos casos el usuario final, o el proceso automático que actúa en su nombre, no conocerá el identificador con el que comenzar, y tendrá que recurrir a otras formas de búsqueda o clasificación para indagar la referencia del caso. Aun cuando el usuario conozca el identificador, quizá no sepa cómo resolverlo o interpretar los resultados obtenidos. Consignar la existencia de ED en registros puede ayudar a soluciones este problema de una manera muy general.

Al definir las operaciones que interactúan con un determinado modelo de datos, es posible construir entidades digitales y utilizarlos para representar la mayoría de los tipos de información estructurada. Este tema se aborda en la cláusula siguiente. En la Figura 1 se ilustra el modelo estándar de datos de entidades digitales. La representación de entidades en un formato independiente de las características particulares del sistema de almacenamiento correspondiente es fundamental para la compatibilidad, por cuanto permite emplear diversos formatos de almacenamiento y normalizar los distintos enfoques en un mismo modelo lógico.

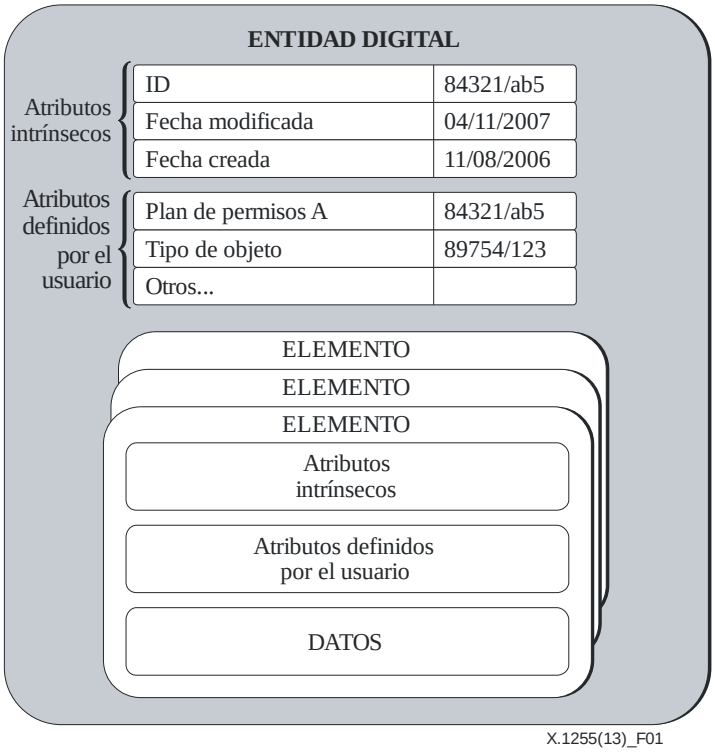

Figura 1 – Ejemplo ilustrativo de entidad digital

Excepto en el caso del identificador invariable de arriba, todos los datos de la Figura 1 son exclusivamente conceptuales. Cada elemento de una entidad digital puede adoptar formas diferentes, por ejemplo, referencias a entidades digitales mediante el identificador, una entidad digital real, datos locales debidamente introducidos.

Los registros pueden utilizar o incorporar repositorios para almacenar entradas de metadatos; estos repositorios son sistemas de gestión de información que dan acceso a colecciones de ED a través del protocolo interfaz de entidades digitales. Los repositorios suelen estar concebido para incorporar las entidades digitales a los que dan acceso. Ahora bien, desde un punto de vista más detallado pueden considerarse como portales de diversos sistemas de almacenamiento e información, que hacen la correspondencia de datos en bruto con entidades digitales almacenadas localmente o a distancia.

Puede tratarse sencillamente de un sistema de ficheros que almacena los datos para una determinada ED en uno o varios ficheros que el usuario desconoce o que no están visibles para el mismo. Otra posibilidad, especialmente para entidades complejas, es que los datos estén distribuidos en diversas ubicaciones y sistemas y que la ED se cree sólo por solicitud previa, de modo que un componente almacenamiento guarde el 'mapa' de la entidad, mientras que los datos se almacenan en otros sistemas. Esta técnica de interacción con sistemas existentes es característica de las federaciones, donde la información contenida en cualquier sistema de información complejo puede dividirse lógicamente en ED, y estas ED pueden ponerse a disposición en un formato normalizado, utilizando una instancia del DEIP en aplicaciones centradas en el usuario.

El cliente ED puede localizar uno o varios repositorios para una determinada ED resolviendo su identificador. La solicitud de resolución obtendrá como respuesta uno o varios repositorios pertinentes con los que el cliente puede iniciar una transacción ED.

El software de repositorio ED suele ofrecer múltiples interfaces de red para efectuar operaciones con entidades digitales, a saber, el protocolo interfaz de entidades digitales para interactuar con el ED propiamente dicho, así como las interfaces locales correspondientes que dependen de la opción tecnológica del caso. Cada una de las interfaces tiene sus ventajas en cuanto a seguridad, compatibilidad con los servidores intermediarios y utilización de software cliente ubicuo. La redundancia se consigue mediante el protocolo interfaz de entidades digitales, junto con una autentificación robusta individual y en grupo. La redundancia se obtiene mediante un sistema de duplicación en el que cada repositorio de ED se comunica con los demás donde las entidades duplicadas se mantienen sincronizadas. La autentificación se basa en un secreto o claves públicas/privadas, aunque también son posibles otros mecanismos de autentificación.

Otras características notables son la duplicación, que permite crear fácilmente imágenes especulares en repositorios y la capacidad de ampliación mediante un mecanismo de conexión. Estos mecanismos puede crearse para gestionar actividades específicas del tipo de entidad, por ejemplo, realizar un análisis sintáctico de un formato de vídeo y expedir una sección solicitada, o para actividades relacionadas con servicios de red, por ejemplo, contribuir con metadatos al registro de una ED.

7.2 Protocolo interfaz de entidades digitales

Cada interacción con una ED consta de una entidad identificada que solicita o aplica una operación sobre la ED. La información de gestión de identidades acerca de dicha entidad, cada operación y la entidad a la que se aplica la operación están identificadas de manera exclusiva e invariable. Asimismo, los distintos tipos de recursos también son entidades identificadas y la información sobre el estado del recurso correspondiente puede contener, entre otras cosas, su clave pública.

Los repositorios son los que aplican las operaciones a las entidades digitales. Estos repositorios son a su vez entidades digitales que dan acceso a las entidades que contienen. El protocolo interfaz de entidades digitales define el método mediante el cual la entidad se comunica con el repositorio con el fin solicitar operaciones que se aplican a las entidades digitales accesibles a través de dicho repositorio. Estas operaciones pueden utilizarse, por ejemplo, para acceder a entradas de metadatos específicas mediante sus identificadores; pero también se puede acceder a estas entradas del registro por otros mecanismos semánticos, como "aplicaciones" de registro especializadas y navegadores web.

Las operaciones sobre una entidad digital constan de los siguientes elementos:

- EntityID: El identificador de la entidad que solicita la operación;
- TargetEntityID: El identificador de la entidad al que se aplica la operación;
- OperationID: El identificador que especifica la operación a realizar;
- Entrada: Secuencia de bits que contiene las entradas de la operación, en particular los parámetros, el contenido u otra información; y

- Salida: Secuencia de bits que contiene el resultado de la operación, ya sea contenido u otra información.

La información de gestión de identidades puede acompañarse de un certificado, o comunicarse en una parte del mismo, en el que se afirme explícita o implícitamente la veracidad de la información. Ahora bien, el destinatario puede aceptar o no el certificado si no fue creado por una autoridad de confianza aceptable. También pueden utilizarse credenciales en lugar de certificados para obtener un resultado de confianza similar. Estos certificados o credenciales aumenta la probabilidad de que la información acerca de la identidad comunicada sea exacta; no obstante, puede recurrirse a mecanismos de seguridad intrínsecos, que pueden formar parte de esta arquitectura abierta, para validad de manera independiente que la entidad digital que utiliza la información de gestión de identidades posee la clave privada correspondiente que puede utilizarse para validad la entidad digital identificada. Toda parte en un transacción en la que intervienen entidades identificadas puede solicitar a la otra parte que encripte una cadena con su clave privada y la devuelva a la parte solicitante para su validación. Las partes en una transacción dentro del sistema pueden recurrir a otros mecanismos de autentificación, pero en principio no hay necesidad de negociar esos otros mecanismos. El mecanismo por defecto que se indica a continuación consiste en utilizar pares de claves pública/privada, que forma parte integrante de la instancia del DEIP. No obstante, puede recurrirse a otros mecanismos de autentificación, si las parte así lo acuerdan de antemano. Para recurrir al DEIP se habrán de seguir, como mínimo, los siguientes pasos obligatorios:

a) Establecer una relación entre las partes A y B, es decir, las dos partes en la transacción, salvo cuando ya exista una que pueda utilizarse a tal efecto.

b) Otra opción es que la parte A pida a la parte B que se autovalide mediante, por ejemplo, un método basado en KPI.

c) A continuación la parte A envía una solicitud específica a la parte B, según proceda.

d) Otra opción es que la parte B pida a la parte A que se autovalide mediante, por ejemplo, un método basado en KPI.

e) La parte B accede o no a la solicitud, según el caso; y

f) La transacción termina y bien se envía una nueva solicitud o bien se corta la relación, según proceda.

En la bibliografía [b-DOIP] se puede encontrar un ejemplo de especificación detallada de DEIP (véase asimismo [b-DO Repo]), pero éste no forma parte integrante de la presente Recomendación.

7.3 Interacciones con un registro

En toda interacción con un registro interviene una entidad digital identificada, ya sea un individuo o un recurso del sistema; cada interacción dispone de un identificador invariable que puede emplearse para autentificar la entidad digital. Durante la configuración, el registro puede configurarse de antemano para confiar en cualquier cliente identificado siguiendo un procedimiento específico por medio de sus identificadores. Los clientes también pueden optar por autentificar registros utilizando el mismo procedimiento. Por otra parte, pueden configurarse determinados clientes para funcionar conforme lo exija concretamente el proceso de federación, lo que permitiría realizar una operación específica sobre el registro, además de las ya disponibles para todos los clientes de confianza. Cuando los clientes interactúan con un registro, éste genera una respuesta-pregunta para verificar que el cliente dispone de la clave privada correspondiente. Una vez verificado, el registro comprueba que el identificador pertenezca a la entidad digital.

La interfaz del registro efectúa las siguientes operaciones:

- **Registrar una entidad digital**: La información necesaria para registrar una entidad puede consistir exclusivamente de metadatos, aunque también puede consistir de metadatos combinados con la ED correspondiente. El registro gestiona la entidad digital registrada utilizando su repositorio interno. Además, indexa la información estructurada como entidad

digital utilizando las reglas preconfiguradas que determinan cómo realizar un análisis sintáctico, crear credenciales e indexar la información que contiene. En caso necesario, el registro crea un identificador de la entidad digital y hace que se introduzca en el sistema de resolución.

- **Dar de baja una entidad digital previamente registrada**: El registro elimina el entidad digital de su repositorio interno, la desindexa y actualiza el sistema de resolución para registrar que la entidad ha sido suprimido.
- **Recuperar una entidad digital previamente registrada mediante su identificador**: El registro efectúa una serialización de la entidad digital gestionada en su repositorio interno y lo reenvía al cliente.
- **Buscar**: El registro realiza un análisis sintáctico de la expresión con el fin de buscar palabras clave, concordancias exactas o una serie de consultas para encontrar la concordancia con entidades digitales indexadas, y devuelve los identificadores de las entidades digitales encontradas. Es posible integrar fácilmente técnicas de búsqueda más avanzadas, tales como consultas en lenguaje corriente, si los resultados de la búsqueda lo permiten.
- **Obtener el número de la última transacción**: El registro, que asigna números secuenciales a cada operación registrar o dar de baja, devuelve dicho número al cliente que está configurado para participar en un proceso de federación con el registro. Los posibles clientes (u otros registros que participan en la federación) puede utilizar este número para determinar el estado del registro con el fin de enviar entidades registradas en función de la topología de la federación configurada y el nivel de agregación seleccionado.

Aunque la autentificación puede desactivarse, conviene que el registro autentifique al cliente y viceversa. La codificación de mensajes intercambiados varía en función del sistema en concreto. Los mensajes pueden codificarse como operaciones del repositorio de entidades digitales, de modo que una transacción del registro consistirá en una serie de operaciones del repositorio, por ejemplo, crear entidad o añadir elemento. Otra posibilidad sería codificar los mensajes utilizando bibliotecas de codificación de terceros, siempre y cuando el remitente y destinatario se hayan puesto de acuerdo (probablemente de antemano) para utilizar la misma biblioteca.

7.4 Sistemas de resolución

El sistema de resolución es otro componente del marco (aunque puede haber varios de estos sistemas) que hace corresponder los identificadores con información sobre el estado de la entidad digital que se desea identificar, por ejemplo su ubicación en Internet, información sobre la autentificación de dicha entidad digital, o la clave pública relacionada con el identificador. La naturaleza abierta de esta arquitectura marco permite la compatibilidad entre sistemas de resolución, que es el objeto de la presente Recomendación. La información de estado puede modificarse según las necesidades para que responda al estado actual de la entidad digital identificada sin cambiar su identificador, de modo que éste no varía al cambiar la ubicación u otros parámetros de estado.

Si se conoce el identificador del recurso deseado, el sistema de resolución y el conjunto de repositorios proporcionan todo lo necesario para que el usuario final o el proceso autorizado pueda ver o acceder a la entidad digital. En cambio, cuando se desconoce la identidad del recurso deseado, ésta se tendrá que indagar. En la ciencia de la información y en biblioteconomía, el primer caso se denomina búsqueda de un "elemento conocido" (es decir, se sabe lo que se desea obtener pero no cómo). El segundo caso exige normalmente una búsqueda por materia; el objetivo de las herramientas utilizadas en este tipo de búsqueda es reducir ésta a una búsqueda de un elemento conocido. El registro de entidades digitales permite realizar esta función.

Si bien una instancia de un registro puede operar de manera independiente, sólo puede satisfacer las solicitudes de indagación sobre las que tiene conocimiento. La federación de múltiples registros le permite tener conocimiento de otras entidades digitales registradas en otro lugar y, por ende,

realizar búsquedas más amplias en toda la colección de entidades digitales. Un aspecto importante de la indagación de información de gestión de identidades es la capacidad para determinar qué registros pueden contener información pertinente sobre la identidad. Es posible que un sistema necesite indagar información disponible en otro sistema, que posiblemente tenga un diseño diferente. Suponiendo que alguna entidad haya definido una forma de relacionar estos dos sistemas y la información en ellos contenida, el marco de indagación debería permitir indagar tales relaciones. Ahora bien, en la presente Recomendación no se analiza quién o qué es responsable de tales relaciones, qué tipo de información puede relacionarse ni cómo se crea la relación o se accede a la misma. Estas cuestiones varían generalmente según el contexto y, por lo tanto, en la presente Recomendación no se propone ningún tipo de práctica en materia de relaciones. A fin de aclarar este punto, el término "relación" se ha añadido a las definiciones y el concepto se ha incluido en la definición de información de gestión de identidades.

En muchos casos, la privacidad resulta esencial; ésta se gestiona mediante técnicas IdM basadas en identificadores para individuos, grupos, funciones y recursos, así como las condiciones que se obtienen de los metadatos almacenados.

7.5 Consultas distribuidas y metadatos agregados a registros federados

El sistema de registros federados descrito en la presente Recomendación debería ser ampliamente accesible y servir de base para el sistema de indagación de la arquitectura abierta. El sistema ofrece una forma uniforme de indagar información de gestión de identidades. Los sistemas de registros federados permiten a múltiples IdM participar en la configuración de registros compatibles y determinar qué información están dispuestos a compartir con otros registros.

La tecnología de registros ofrece un mecanismo mediante el cual las partes responsables de crear entidades digitales en Internet, tales como servicios y otras entidades, pueden registrar la existencia de un determinado conjunto de entidades, adjuntando metadatos descriptivos y estructurales sobre las entidades, incluida la información sobre la procedencia, y así mejorar la capacidad de indagar entidades por el público en general o una comunidad en particular. Un elemento esencial de los metadatos que debe registrarse junto con la entidad digital es su identificador invariable, el cual debe ser resoluble en Internet. En el caso de entidades digital que aún no están identificadas, el registro puede configurarse para crear identificadores durante el proceso de registro y proporcionar las herramientas necesarias a los administradores de entidades digitales para mantener actualizada la información necesaria para la resolución.

El sistema de registros federados permite alcanzar los cuatro objetivos principales de la indagación. En primer lugar, permite la selección uniforme de políticas que han de aplicarse a todos los marcos de confianza participantes y a otros sistemas IdM. En segundo lugar, permite al usuario acceder a la información del registro para la que dispone de autorización sin tener que tratar directamente con múltiples registros. En tercer lugar, ofrece infraestructura para la privacidad y otras restricciones de acceso establecidas por cada sistema IdM. En cuarto y último lugar, permite el acceso semántico a registros en favor del plurilingüismo.

El concepto de registros federados se basa en la arquitectura abierta descrita en el presente documento, la cual presenta las siguientes ventajas:

- Políticas de selección unificadas: Para efectuar consultas basadas en propiedades de la información que supuestamente contienen, es posible seleccionar registros y sus marcos de confianza afines u otros sistemas IdM más generales. Normalmente se selecciona un sistema IdM que efectúa cierto nivel de investigación para fundamentar su información. Otra posibilidad es seleccionar un marco de confianza mínimo u otros sistemas IdM que sólo verifique información sobre la tarjeta de crédito o el permiso de conducir. El otro extremo consiste en seleccionar un sistema IdM que haga pruebas de ADN. Puede seleccionarse una organización que aplique políticas destinadas a garantizar la integridad de

los sistemas. De esta forma, puede aplicarse un método de selección uniforme a todo el universo de registros y sus correspondientes sistemas IdM.

- Metadatos compartidos: La información disponible en un sistema de registros federados se denomina metadatos compartidos. Se asocia una plantilla genérica a los metadatos compartidos, que identifica cómo se representan los metadatos y, por ende, cómo se accede a los mismos para su ulterior procesamiento. La plantilla no contiene entradas específicas.
- Acceso federado: Si uno de los registros no contiene la información deseada, puede ser accesible desde otro u otros registros. De hecho, en una operación normal, el sistema funciona de un modo tal que esta información esté disponible para el usuario con independencia del registro que la contenga. Este acceso puede conseguirse de diversas manera, tales como la federación jerárquica y mediante sistemas punto a punto.
- Acceso privado: Algunos registros estarán restringidos para ciertos grupos de usuarios, tipos de aplicación o funciones conexas que utilizan el sistema, mientras que otros estarán abiertos a todos. La forma de restringir el acceso a la información de indagación basada en criterios para tales restricciones es inherente al sistema. Para mantener la privacidad dentro del sistema se recurrirá a uno o varios mecanismos, convenidos por los registros participantes.
- Acceso semántico: Se utiliza un sistema de creación de tipos para insertar "tipos". Los IdP pueden designar tipos propios de acuerdo con las directrices de la especificación. Esto permite el acceso semántico a la información pertinente con independencia de dónde esté almacenada en el sistema y puede ayudar a cumplir los requisitos en materia de plurilingüismo.

Los metadatos en este tipo de sistemas están disponibles en la forma de datos estructurados, con el correspondiente identificador exclusivo invariable que existe mientras exista el entidad digital. Los metadatos de varios registros pueden diferir en el campo temático y/o en la estructura de metadatos, lo que dificulta efectuar una búsqueda coherente y sencilla por el conjunto de todos los registros. Si los metadatos de diferente estructura o campo temático se reducen a su mínimo común denominador, que es una solución para combinar este tipo de datos, entonces una estrategia de búsqueda óptima podría consistir en identificar los registros más idóneos para realizar una búsqueda más detallada. La trasformación al mínimo común denominador pueden realizarla los registros fuente o el registro recopilador. Otra posibilidad es que la búsqueda propiamente dicha se haga corresponder de algún modo con la consulta a diversas estructuras de metadatos, lo que genera un conjunto de consultas que se diversifican a partir del original.

Una posibilidad es agregar entidades de metadatos para la indagación de información procedente de múltiples dominios, pero también existe la alternativa de realizar consultas distribuidas a varios registros que gestionan las entidades de metadatos de su dominio. El panorama de federación de registros permite otras posibilidades, como se ilustra en el espacio tridimensional de la Figura 2.

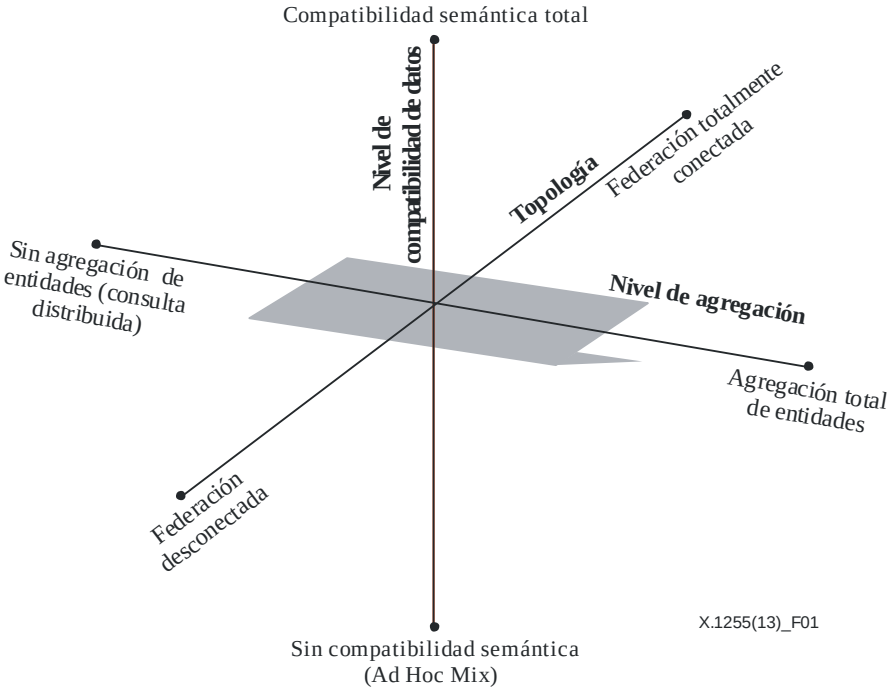

Figura 2 – Consultas distribuidas por múltiples registros

En esta Figura se muestran tres ejes. El primer eje representa el nivel de agregación de los metadatos del registro, que varía desde ninguna agregación a una agregación total. El segundo eje indica el grado de conectividad topológica entre los registros. El tercer eje tiene que ver con la compatibilidad de la información procedente de registros diferentes. A continuación se describe en detalle cada uno de estos ejes.

El eje de agregación indica el grado de compromiso alcanzado previamente entre los registros para la agregación de entidades de metadatos. En el extremo izquierdo del eje figuran las entidades que no se agregan entre registros antes de cualquier consulta, mientras que el extremo derecho del eje indica que todas las entidades se agregan antes de cualquier consulta. Los puntos del eje representan otras posibilidades, en particular la agregación del mínimo denominador común de la información de metadatos, la agregación de índices de búsqueda, etc. La vigencia de la información agregada se reduce al desplazarse de izquierda a derecha; las consultas distribuidas producen resultados más actualizados, mientras que la vigencia de las entidades de metadatos agregadas depende de cuándo se agregaron.

El eje topología indica el grado de conexión entre los registros. En un extremo del eje, los registros no tienen conectividad de red entre sí, por lo que no comparten información; en el otro extremo, los registros están totalmente conectados entre sí. Obsérvese que "la forma" en que están conectados sigue dependiendo del nivel de agregación, ya que la topología sólo determina los posibles vínculos.

El eje de compatibilidad de datos indica el grado en que las entidades de metadatos de un registro dado que aporta determinada información son compatibles con las entidades de metadatos de otro registro que aporta información a un dominio diferente. Es decir, la estructura de metadatos de un determinado registro puede ser o no compatible con la estructura adoptada por otro registro. Algunas veces es preciso transformar las entidades de metadatos para lograr cierto nivel de compatibilidad, si no compatibilidad total. En otros casos, cuando las estructuras semánticas son demasiado diferentes, ninguna transformación será suficiente para obtener un nivel útil de compatibilidad.

Obsérvese que no todos los puntos en el espacio tridimensional de la Figura 2 son válidos. Por ejemplo, una consulta distribuida en nodos desconectados no implica una distribución de consultas a todos esos nodos. Análogamente, la agregación total de entidades incompatibles implica un

sistema de entidades incoherentes. El diseño básico del registro debería permitir todas las configuraciones posibles con arreglo a los puntos válidos del espacio tridimensional ilustrado. Por otra parte, dependerá de cada implementación en concreto si la correspondencia se hace en la transformación de las entradas de metadatos o en la búsqueda, o si la transformación de estas entradas se efectúa en los registros de contribución o de recopilación. Si bien las consecuencias para el rendimiento pueden ser considerables, el diseño básico debería permitir estas variaciones en la implementación.

El método adoptado en la presente Recomendación no soluciona por sí mismo el problema de la búsqueda y recuperación en sistemas de información heterogéneos, pero sí ofrece un marco común en el que pueden emplearse métodos diferentes. De hecho, es probable que no haya una solución única al problema y que el método óptimo varía en función de las prácticas del grupo y del campo temático.

7.6 Estructuras de metadatos

Uno de los principales objetivos de la presente Recomendación es sentar las bases para definir un conjunto de estructuras de metadatos de alto nivel que sirvan para indagar información sobre: a) identificadores utilizados en diversos sistemas IdM; b) proveedores de identidad; c) partes dependientes; y d) marcos de confianza y otros sistemas IdM a todos los niveles, en particular, de política, procedimiento e infraestructura técnica subyacente. Los elementos necesarios de estas estructuras de metadatos dependerá de los casos de utilización específicos, pero tendrán que poderse extender a nivel de elemento y de estructura con el fin de permitir el crecimiento y el cambio en ámbitos dinámicos.

Las diversas entidades que intervienen en la gestión de identidades pueden definir las estructuras específicas propias que requieran, hacerlas corresponder con las estructuras generales de metadatos normalizadas de alto nivel con el fin de describir sus servicios, políticas y procedimientos, así como registrar tales descripciones en uno o varios conjuntos de registros federados. Estos registros permitirán utilizar servicios de indagación en las entidades registradas.

Si bien es posible crear una sola estructura de metadatos que integre todos los aspectos de las tecnologías IdM, las organizaciones pertinentes y las políticas y procedimientos correspondientes, se propone empezar con una estructura para cada tipo de entidad participante. El proceso para llegar a un acuerdo sobre las estructuras de metadatos será un proceso de colaboración en la que cada parte interesada contribuirá con sus conocimientos acerca de los atributos que deben contener dichas estructuras; las estructuras evolutivas pueden verificarse para diversos casos de utilización, con el fin de comprobar si ofrecen la información necesaria para los procesos de indagación y, de ser necesario, pueden mejorarse posteriormente.

7.7 Compatibilidad de metadatos

Los identificadores son uno de los factores más importantes para lograr la compatibilidad de metadatos. Ahora bien, otros aspectos de la compatibilidad de metadatos, en particular los que implican la definición humana y el contexto de descripciones, quedan fuera del alcance de la presente Recomendación. Otros atributos especificados en metadatos, como los que describen o permiten una determinada configuración, por ejemplo un modo de conexión específico y un método de agregación, pertenecen al ámbito de las operaciones con registros. A fin de gestionar entidades de metadatos en diversos registros, la compatibilidad de metadatos resultará más fácil si las partes se ponen de acuerdo en una estructura de metadatos común. Así, los metadatos se gestionarán como entidades homogéneas, que los registros interpretarán y procesarán de manera coherente. En la cláusula 9 se ilustran dos casos concretos de federación en el contexto de nivel de agregación y topología, dimensiones éstas que son normalmente aplicables a este marco.

8 Tipos y atributos tipo

Los registros contienen entradas de metadatos en la forma de entidades digitales que se pretende intercambiar con otros registros federados. Cada entrada consta de un conjunto de elementos, cada uno de los cuales contiene un campo "tipo" y un campo "valor". Es fundamental comprender el significado de cada tipo para manifestar los valores correspondientes en una forma distinta de una secuencia de bits opaca, o una serie de secuencias binarias.

A fin de comprender su significado, los tipos se representan mediante identificadores invariables que pueden resolverse para obtener información útil acerca del tipo. Si bien la descripción de tipos se ha concebido para que las creen personas, es necesario disponer de un mecanismo estándar para describir y representar tipos.

Aunque es previsible que los aspectos y atributos específicos de lo que en última instancia constituirá un tipo evolucionen con el tiempo, los siguientes cuatro aspectos se consideran esenciales:

- La primera categoría de atributos es la más sencilla y consiste en descripciones en lenguaje común de la finalidad del tipo. Su finalidad es describir el tipo, los recursos y concepto, así como su utilización. Estos atributos se podrán describir en varios idiomas.
- La segunda categoría de atributos de la descripción de un tipo consiste en la información sobre su procedencia. Toda definición de un tipo debería incluir la fecha de creación, la fecha de la última modificación, sus contribuyentes, su estado y los alias u otros identificadores que pudiera tener.
- La tercera categoría de atributos consiste en la descripción de las categorías de tipos y la posibilidad de que los tipos utilicen otros tipos.
- La cuarta categoría de atributos ofrece la posibilidad de que diversos sistemas actúen dinámicamente sobre un recurso de un determinado tipo.

Las tres últimas categorías se describen a continuación con mayor detalle.

Por lo general, los tipos se utilizan para describir una determinada categoría de recursos y/o conceptos con arreglo a un conjunto específico de características. Esta categoría representa el domino de aplicabilidad del tipo y se denomina género del tipo. Por ejemplo, el tipo de codificación de caracteres utilizado para especificar cómo se debe representar un carácter en formato binario sería del género codificación. Un tipo de formato de datos utilizado para especificar cómo representar una estructura como un conjunto de bits sería del género formato.

Cada descripción de tipo incluirá un atributo que especifica su género. El atributo descripción del género del tipo constituye una estructura de clasificación sencilla que permite normalizar el desarrollo de nuevos tipos y ayuda a los usuarios del tipo a indagar los tipos existentes. El género de tipo es propiamente dicho un tipo y pueden añadirse tantos nuevos géneros de tipo como hagan falta para ampliar la clasificación del tipo.

Para aprovechar al máximo la reutilización de tipos y minimizar la creación de duplicados, cada tipo será capaz de describirse a sí mismo mediante los tipos existentes. Si, por ejemplo, un nuevo tipo necesita especificar que su recurso está serializado en XML, incluirá para ello una referencia al tipo de serialización XML existente. Los tipos pueden utilizar otros tipos mediante la ampliación o creación de instancias.

Cada tipo debería incluir todos y cada uno de los tipos que utiliza y cómo los utiliza. La capacidad de los tipos de autodefinirse utilizando otros tipos no sólo reducirá la duplicación de tipos, sino que además permitirá a los usuarios comprender un determinado tipo con más detalle.

Por último, una descripción de tipo debería permitir que diversos sistemas pudieran adquirir dinámicamente la capacidad de actuar sobre cualquier recurso tipificado. La descripción de tipo debería incluir atributos que especifiquen la ubicación de vinculaciones del servicio de red y/o los

módulos específicos, sus plataformas y sus interfaces correspondientes. Esto permite vincular de manera segura y dinámica una biblioteca genérica de tratamiento de tipos a ese servicio, o adquirir, cargar y ejecutar el módulo de aplicación correspondiente al tipo y procesar el recurso.

Los tipos, como se indicó más arriba, se identifican de manera inequívoca. Al resolver esos identificadores de tipo en algunos sistemas de resolución se obtendrá la entrada del tipo. En el Apéndice II figura un ejemplo de notación BNF para una entrada de tipo que conceptualmente define el grupo de entidades que forman parte de la entrada del tipo.

Se requieren como mínimo cuatro secciones para definir de manera coherente y sin ambigüedad un tipo, a saber, descripción, procedencia, género y procesamiento.

La descripción es una secuencia de una o varias descripciones en lenguaje común que definen, entre otras cosas, la finalidad y la utilización del tipo. El lenguaje en el cual se escriben esas descripciones, que puede guardar conformidad con [b-IETF RFC 1766], deberá estar representado inequívocamente por su tipo y figurar antes que las descripciones.

La procedencia comprende la fecha de creación, la fecha de la última modificación, los contribuyentes, los alias (u otros identificadores) y el estado. La fecha debe estar en consonancia con la norma [ISO 8601]. Los contribuyentes consisten en los nombres del personal o las organizaciones que han contribuido a la creación o consignación de un tipo en el registro designado. Los alias se obtienen de referencias a consignaciones efectuadas anteriormente en otros registros de tipo locales que se declaran a los efectos de establecer el contexto del tipo definido. El estado indica si el tipo se sigue utilizando o ha quedado desfasado u obsoleto.

El género se refiere a la esencia del tipo. La definición de nuevos tipos a partir de los existentes es un concepto muy eficaz y fundamental para definir tipos complejos. Un último concepto en relación con el género es especificar si la información del género es un componente para definir otros tipos o si se define para una manifestación particular de un tipo. Por ejemplo, un tipo de codificación binaria es en sí un componente que permite definir otros tipos.

La información puede transferirse a un servicio que sabe cómo analizar y procesar la información del tipo. Los clientes recurren a un servicio para sintetizar la información suministrada. La definición del servicio debería identificar cómo acceder al mismo, cómo solicitarlo y qué resultados cabe esperar de dicho servicio. No se recomienda ninguna notación en particular para definir este tipo de servicios.

9 Federación jerárquica y federación de reciprocidad

En una federación jerárquica, el registro central se utiliza para facilitar la búsqueda de la información contenida en múltiples registros, de modo que sólo es necesario consultar un registro. Puede haber varios registros centrales, pero es necesario conocerlos y consultarlos todos para completar la búsqueda.

En una federación de reciprocidad (o entre pares), ciertos registros optan por asociarse con otros registros seleccionados. Las razones por las que se seleccionan acuerdos de reciprocidad son variables. Algunas de las razones en las que se basa un determinado registro a la hora de seleccionar los registros con los que concertar acuerdos de reciprocidad son las políticas de la organización relacionadas con la gestión de registros, las políticas de confianza que prohíben o proporcionan puntos de contacto entre registros y la disponibilidad/fiabilidad de los registros que participan en una red P2P.

Ahora bien, tanto las federaciones jerárquicas como las de reciprocidad se refieren a la topología de la federación, y no determinan en modo alguno el nivel de agregación seleccionado en cada caso. Si bien es posible aplicar diversos niveles de agregación, a continuación se dan dos ejemplos concretos a título ilustrativo. En el Cuadro 1 se indican las ventajas (con un signo +) y los inconvenientes (signo –) de los dos tipos de sistemas federados para los casos en que se ha acordado de antemano

la agregación de todas las entidades de metadatos y en que las consultas se propagan en tiempo real por los registros en respuesta a una consulta al sistema IdM.

Cuadro 1

	Federación jerárquica	**Federación de reciprocidad**
Agregación total de entidades de metadatos en el registro de recopilación	+ La indagación total en el dominio se consigue mediante el proceso de agregación definitivo. + Se garantiza la pertinencia de la información en todo el dominio mediante la normalización de las entidades de metadatos durante la agregación. + Eficiencia gracias a la búsqueda y recuperación localizadas. – Forma rígida. Requiere una configuración minuciosa que puede interferir con las políticas de la organización. – Falla por un solo elemento, ya sea en el recopilador central o en los recopiladores intermediarios. – Posibilidad de introducir información obsoleta debido a la reducida frecuencia de agregación. – Posibles problemas de ampliación del nivel superior de la jerarquía.	+ Permite agrupaciones flexibles, no rígidas, consagradas a ámbitos de interés específicos. + No se producen fallas por un solo elemento, dado que es posible activar múltiples rutas para la federación. + Se garantiza la pertinencia de la información en todo el dominio mediante la normalización de las entidades de metadatos durante la agregación. + Eficiencia gracias a la búsqueda y recuperación localizadas. – No se garantiza la integridad de la indagación entre dominios, a no ser que la estructura esté totalmente conectada. – Elevado coste para eliminar duplicaciones cuando los registros pueden federarse a través de múltiples rutas. – Problemas de seguridad a no ser que todos los puntos de contacto sean de confianza.

Cuadro 1

	Federación jerárquica	Federación de reciprocidad
Propagación de consultas por los registros	+ Vigencia de las entidades de metadatos y de la información que contienen. + Sistema ampliable. – No se garantiza la integridad de la indagación entre dominios debido a una probable falta de disponibilidad de nodos de registro en el momento de propagar la consulta. – La pertinencia de los resultados puede verse comprometida debido a la fusión de resultados en tiempo de ejecución. – Forma rígida. Requiere una configuración minuciosa que puede interferir con las políticas de la organización. – Falla por un solo elemento, ya sea en el nodo de registro central o en los nodos de registro intermediarios que distribuyen las consultas o devuelven los resultados. – Problemas de rendimiento debido a que el hardware utilizado para implantar el registro no es robusto.	+ Vigencia de las entidades de metadatos y de la información que contienen. + Sistema ampliable. – No se garantiza la integridad de la indagación entre dominios debido a una probable falta de disponibilidad de nodos de registro en el momento de propagar la consulta, incluso con rutas de federación redundantes. – La pertinencia de los resultados puede verse comprometida debido a la fusión de resultados en tiempo de ejecución. – Elevado coste para eliminar duplicaciones cuando los registros pueden federarse a través de múltiples rutas. – Problemas de rendimiento debido a que el hardware utilizado para crear el registro no es robusto.

El software de registro admite y permite distintas combinaciones de la matriz que figura en el Cuadro 1. Algunas combinaciones son más difíciles de construir que otras. Los problemas de ampliación se resuelven utilizando una tecnología de repositorio que crea abstracciones de los sistemas de almacenamiento reales y que permite emplear simultáneamente varios sistemas de almacenamiento. También se ofrece la duplicación y distribución de carga entre los registros, lo que mitiga el problema de ampliación. La detección de duplicados, que podría ser un problema en los registros con relaciones muchos a muchos, puede reducirse considerablemente utilizando identificadores invariables.

La agregación de datos, a diferencia de la consulta distribuida, parte del supuesto de que el registro que inicia el movimiento de registros de metadatos los envía a discreción, en lugar de como respuesta a una solicitud recibida. Por otra parte, el registro que suministra los registros se denomina remitente y el que los recibe destinatario. En una federación, el destinatario será el punto de contacto del sistema de registros federados. El registro remitente envía debidamente a los destinatarios los cambios efectuados en los metadatos, por ejemplo los registros de metadatos creados o los editados. Estas transacciones abarcan cambios de estado de una entidad digital, a saber, creación, modificación, alias y supresión, así como relaciones de adición/eliminación/sustitución. Cada registro que se envía al registro se traduce en acciones de registrar y dar de baja en el núcleo del registro. Cada una de estas acciones es una transacción, que tiene su correspondiente identificador, un número que normalmente se va incrementando comenzando por el cero. Este método también es aplicable a los casos en que los registros obedecen a una jerarquía de reciprocidad o jerárquica.

La propagación de consultas se consigue configurando cada registro para propagar las consultas a determinados registros, con independencia de que la jerarquía sea jerárquica o P2P. Además de las interfaces específicas de la comunidad, los registros de entidades digitales también pueden utilizar por defecto el protocolo interfaz de entidades digitales. Es posible propagar las consultas a otros registros recurriendo a este protocolo.

Apéndice I

Casos de utilización

(Este apéndice no forma parte integral de la presente Recomendación.)

A continuación se describen algunos ejemplos para ilustrar la utilización de un sistema de registros federados, así como posibles atributos que se han de registrar para que los procesos de indagación funcionen de manera aceptable.

- Un cliente, ya sea humano o máquina, desea obtener un servicio de un proveedor de servicios en Internet. El proveedor de servicios exige una prueba de identidad y acepta las credenciales de identidad de cualquiera de los proveedores de identidad de un conjunto. El cliente (por lo general, software) debe ser capaz de determinar qué IdP son aceptables, si el cliente posee o no las credenciales pertinentes de uno o varios IdP aceptados, y, en caso negativo, cómo obtenerlas.

  El proveedor de servicio debe anunciar qué IdP acepta para el servicio o servicios del caso. Puede indicarlo directamente, de manera normalizada, o remitir a un registro, también de manera normalizada. En cualquier caso, los IdP deben identificarse con exactitud y de manera inequívoca. A continuación el cliente puede ajustarse a la participación actual en una organización de IdP o bien saber cómo cumplir los requisitos del IdP y presentarle las credenciales correspondientes. En caso de que el proveedor del servicio indique directamente los IdP con exactitud y de manera inequívoca, y el cliente pueda aportar las credenciales específicas del IdP, no será necesario recurrir a un registro. Sin embargo, en todos los demás casos será preciso indagar cierto nivel de información sobre los IdP aceptables. Para un determinado identificador exclusivo e invariable, esta información se puede buscar directamente en el registro de los IdP particulares. Para cumplir los requisitos de este caso en concreto, los metadatos que describen a un determinado IdP tendrán que ofrecer a los clientes la información necesaria para determinar si un determinado IdP ha sido una buena opción para el servicio del caso. Los atributos pertinentes serán el identificador exclusivo invariable del IdP, para una posible referencia cruzada, por ejemplo, para examinar sitios, marcos de confianza en los que participa el IdP, políticas y procedimientos, requisitos legales, software requerido, política de tasas, etc. Alguna de esta información se proporcionará de manera indirecta, por ejemplo, muchos de los detalles técnicos y políticos de un determinado IdP quedarán definidos por la participación de este IdP en uno o varios marcos de confianza particulares.
- Los mismos detalles que permitirían a un cliente indagar si un determinado IdP es adecuado también servirían al proveedor de servicio para indagar acerca de uno o varios IdP cuyas credenciales aceptarían y que, por tanto, podría añadir a su lista de IdP aceptables. Los metadatos de los IdP abarcarían estos dos casos de utilización.
- En la situación inversa al primer caso, un cliente accede a un servicio y presenta una credencial de identidad que el servicio no ha visto nunca antes. Suponiendo que dicha credencial consiste en, como mínimo, un identificador del IdP, el servicio debe decidir si aceptar o no dicha credencial, con el fin de investigar con mayor detalle la posibilidad de utilizarla, o simplemente rechazarla sin investigar más. En este caso, el registro tendrá que indagar información general acerca del tipo de identificador y del IdP al cual representa. Para ello quizá tenga que efectuar otras búsquedas en el registro sobre tecnologías específicas que utiliza el IdP, en particular los marcos de confianza pertinentes.
- Por lo general, las diversas entidades que intervienen en la gestión de identidad serán, explícita o tácitamente, miembros de uno o varios marcos de confianza o de otros sistemas IdM. Será necesario especificar los atributos de cada sistema IdM para crear una estructura de metadatos que describa ese marco de confianza. Cabe plantearse varias preguntas

importantes, a saber, si el sistema IdM descrito por la organización que lo ofrece es un conjunto de normas que lo constituyen, una forma de medir el cumplimiento de estas normas, y así sucesivamente. Con independencia de la respuesta a estas preguntas, es evidente que sería útil que algunos IdP e incluso algunas RP estuviesen conectadas a descripciones de un nivel más general, como las organizaciones InCommon, Kantara, Safe-BioPharma y OIX, que permitiera su indagación dentro de un registro o una federación de registros.

En la Figura I.1 se ilustra la forma en la que podría utilizarse un sistema de registros federados (el "sistema") en un caso específico de utilización.

Paso 1: En este ejemplo, el usuario final solicita un servicio a una parte dependiente.

Paso 2: La parte dependiente responde con la identidad de uno o varios marcos de confianza con los que confía, en este caso un solo marco (TF1).

Paso 3: El usuario final contacta al sistema con el identificador de TF1.

Paso 4: El sistema responde con la entrada del registro correspondiente a TF1. La información de TF1 incluye los mínimos atributos que serán necesarios para confiar dentro de ese marco.

Paso 5: El usuario final evalúa esos requisitos mínimos para determinar si es posible ganar la confianza de la RP. En este paso supondremos que la evaluación del usuario final es positiva y queda demostrado que el usuario puede satisfacer los atributos mínimos, por ejemplo, con un permiso de conducir.

Paso 6: El usuario final puede dirigirse de nuevo al sistema para solicitar los IdP que corresponden con TF1 y que admiten los protocolos que utiliza el usuario final, por ejemplo, HTTP y correo electrónico, que para simplificar denominaremos protocolo X.

Paso 7: El sistema determina que los proveedores de identidad (IdP) que emplean el protocolo X pertenecen al TF1.

Paso 8: El sistema indica al usuario final el conjunto de IdP que cumplen los requisitos de la parte dependiente y los del usuario final.

Paso 9: El usuario final examina el conjunto de IdP que le ha indicado el sistema y selecciona uno de ellos (IdP1).

Paso 10: El usuario final, que dispone de los atributos exigidos por IdP1 y emplea un protocolo que entiende IdP1, inicia una interacción pregunta/respuesta con IdP1.

Paso 11: Tras una interacción pregunta/respuesta satisfactoria, el IdP1 entrega a la RP una credencial de autentificación.

Paso 12: La parte dependiente, que ahora confía en el usuario final, le presta el servicio solicitado.

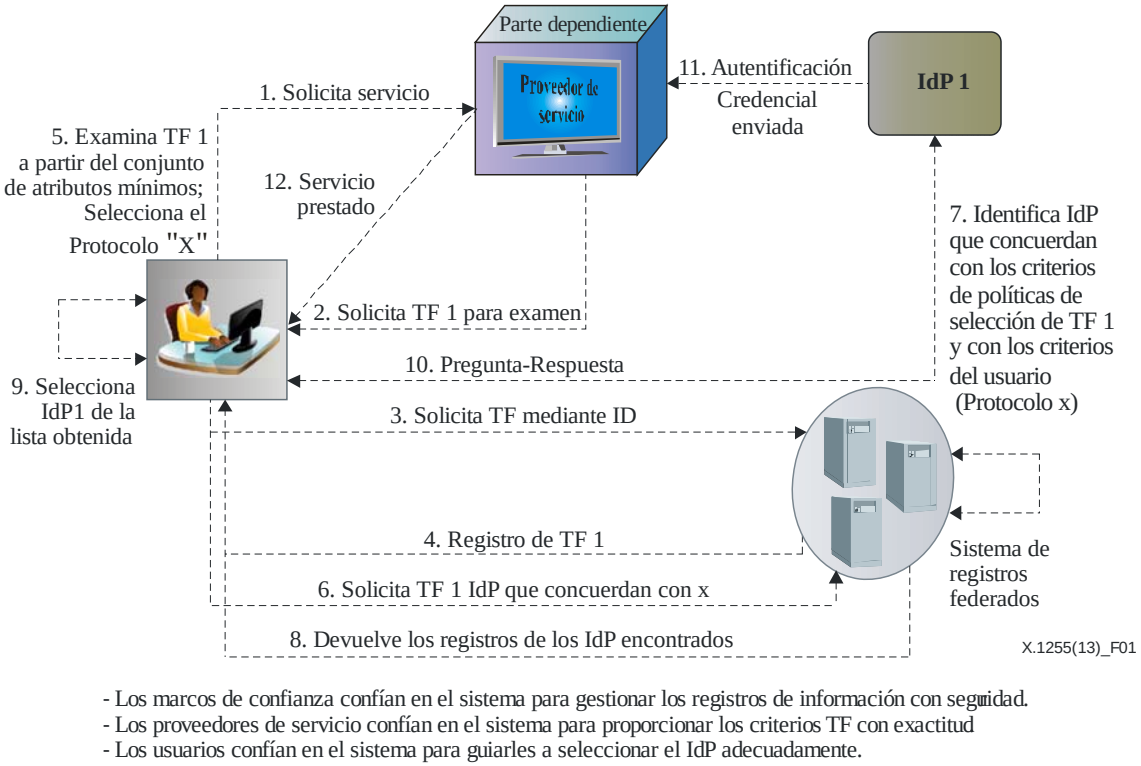

Figura I.1 – Autentificación basada en marcos de confianza

En la Figura I.2 se muestra la estructura de alto nivel de las entradas del registro almacenada en el sistema de registros federados que permite la transacción descrita en la Figura I.1 así como los otros casos de utilización descritos en los párrafos precedentes. El sistema almacena estas entradas en el registro en la forma de entidades digitales, cada uno con su identificador invariable. Cada entidad tiene que construirse con arreglo a esquemas específicos para que se puedan crear los prototipos necesarios.

Todo marco de confianza constará de un identificador, una descripción general del marco, el conjunto de atributos utilizados en la autentificación y punteros a una o varias políticas de selección de IdP, que son en sí entidades digitales independientes almacenadas en el sistema. Estos punteros constituyen un nivel adicional de referencia indirecta, de modo tal que todos los IdP que pertenecen a un mismo TF pueden agruparse por criterios en vez de en una lista numerada. Cada entidad de política de selección de IdP constará de un identificador, una descripción general, una lista de las tecnologías aceptables (por ejemplo, protocolos admisibles), una lista de organismos de acreditación de la organización (por ejemplo, una organización gubernamental) y cualquier restricción operativa especial. La relación entre los TF y las políticas de selección del IdP será de muchos a muchos en los dos sentidos, es decir, un TF dado podrá disponer de múltiples políticas de selección IdP y una determinada política de selección de IdP podrá ser utilizada por varios múltiples TF.

Los otros dos tipos de entidades propuestas que almacena el sistema son los IdP y sus partes dependientes. Cada IdP dispondrá de un identificador invariable, una descripción general, los atributos de usuario necesarios, una política de evaluación de dichos atributos, protocolos específicos y acreditaciones aceptadas, y puntos extremo específicos, por ejemplo, la ubicación del IdP en la forma de protocolos aceptados. Cada parte dependiente constará de un identificador invariable, una descripción general, el conjunto de TF con los que confía y toda restricción operativa específica.

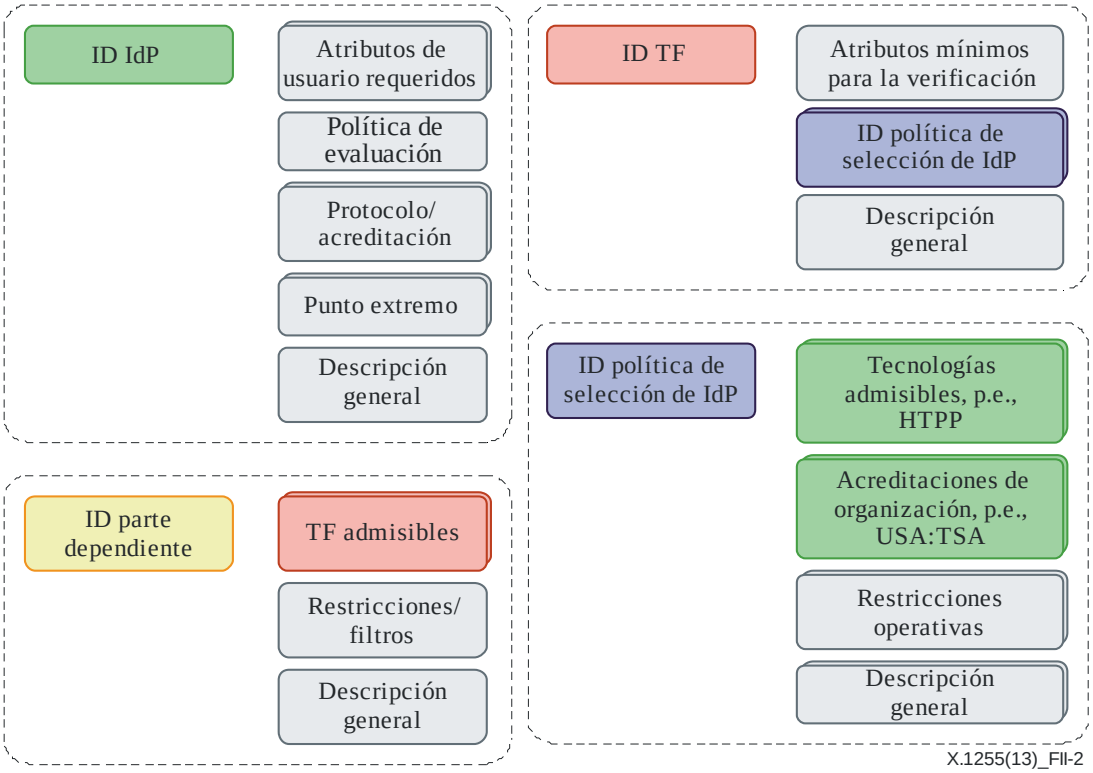

Figura I.2 – Estructura de alto nivel

Apéndice II

Notación BNF de un registro tipo

(Este apéndice no forma parte integral de la presente Recomendación.)

BNF de un registro tipo:

```
<type identifier> := <unicode string>
<type> := <description section> <section delimiter>
    <provenance section> <section delimiter>
    <genre section> <section delimiter>
    <processing section>
```

```
<description section> := <language> '=' <human readable description>
    [<repetition delimiter> <description section>]
<language> := Any item from RFC 1766
<human readable description> := <unicode string>
```

```
<provenance section> := <creation date> <list delimiter>
    <last modified date> <list delimiter>
    <contributors> <list delimiter>
    <aliases> <list delimiter>
    <status>
<creation date> := Conforms to ISO 8601
<last modified date> := Conforms to ISO 8601
<contributors> := <unicode string>
    [<repetition delimiter> <contributors>]
<aliases> := <unicode string>
    [<repetition delimiter> <aliases>]
<status> := 'in use' | 'deprecated' | 'obsolete'
```

```
<genre section> := <genre> '=' <genre details>
    [<repetition delimiter> <genre section>]
<genre> := 'data structure' | 'encoding' | 'format'
<genre details> := <human readable description>
    [<list delimiter> <genre subsection>]
<genre subsection> := 'form='<form> <list delimiter>
    'relationship=' <relationship> <list delimiter>
    'related to=' <type identifier>
    [<repetition delimiter> <genre subsection>]
<form> := 'expression' | 'manifestation'
<relationship> := 'is equivalent to' | 'is derived from' |
    'is informed from'
```

```
<processing section> := <processor type> '=' <processor>
    [<repetition delimiter> <processing section>]
<processor type> := 'network service' | 'downloadable program' |
    'parsing function'
<processor> := <network service type> '=' <network service binding> |
   <compatible platform> <list delimiter>
   <program network location> <list delimiter>
   <program arguments> |
   <pseudo code>
<compatible platform> := 'Linux' | 'Windows' | 'Mac OS'
<program arguments> := <type>
     {<list delimiter> <unicode string>}
<pseudo code> := <unicode string>
```

```
<unicode string> := <visible character> [<unicode string>] |
    <whitespace character> <[unicode string>]
<visible character> = Any visible character in Unicode presumably encoded in
UTF-8
<whitespace character> := Any whitespace character in Unicode presumably encoded
in UTF-8
```

Notas:

1. <type identifier> expedido por el sistema de resolución global genera como resultado un registro <type>.
2. Todos los delimitadores, a saber <section delimiter>, <repetition delimiter> y <list delimiter>, depende del sistema en concreto y no se definen expresamente en este apéndice.
3. <network service type> tampoco se define en este apéndice, pero debería abarcar los servicios de red populares que el organismo considere oportunos.
4. <network service binding> tampoco se define, aunque debería basarse en el tipo servicio de red. Las definiciones reales que guardan conformidad con cada uno de los tipos de servicio deberían declararse aquí.
5. <program network location> tampoco se define en este apéndice, pero debería indicar el protocolo de red que el cliente debe utilizar para descargar el programa de la red.
6. <compatible platform> puede ampliarse o especificarse con más detalle que aquí.

Bibliografía

[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-IETF RFC 1766] IETF RFC 1766 (1995), *Tags for the Identification of Languages*. <http://www.ietf.org/rfc/rfc1766.txt>

[b-DO Repo] Reilly, S. and Tupelo-Schneck, R. (2010), *Digital Object Repository Server: A Component of the Digital Object Architecture D-Lib Magazine*, Vol. 16, No. 1/2. <http://dx.doi.org/10.1045/january2010-reilly>

[b-DOIP] Reilly, S. (2009), *Digital Object Protocol Specification, Version 1.0*, Corporation for National Research Initiatives. <http://hdl.handle.net/4263537/5045>

SERIES DE RECOMENDACIONES DEL UIT-T

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

Impreso en Suiza
Ginebra, 2013