

Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1255

(09/2013)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION
ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Sécurité du cyberspace – Gestion des identités

Cadre pour la découverte des informations relatives à la gestion d'identité

Recommandation UIT-T X.1255

RECOMMANDATIONS UIT-T DE LA SÉRIE X
RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	X.1050–X.1069
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	X.1120–X.1139
Sécurité de la toile	X.1140–X.1149
Protocoles de sécurité	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	X.1200–X.1229
Lutte contre le pollupostage	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1339
ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Echange concernant les vulnérabilités/les états	X.1520–X.1539
Echange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Echange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Echange garanti	X.1580–X.1589

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Cadre pour la découverte des informations relatives à la gestion d'identité

Résumé

La Recommandation UIT-T X.1255 a pour objet de définir un cadre d'architecture ouverte dans lequel il est possible de découvrir des informations relatives à la gestion d'identité (IdM). Ces informations seront nécessairement représentées de différentes manières et seront prises en charge par divers cadres de confiance ou d'autres systèmes IdM utilisant différents schémas de métadonnées. Ce cadre permettra par exemple à des entités fonctionnant dans le contexte d'un système IdM de résoudre avec précision des identificateurs provenant d'autres systèmes IdM. Les utilisateurs ou les organisations (ou les programmes exploités pour leur compte) qui ne sont pas en mesure de découvrir ces informations n'ont d'autre choix que de déterminer la meilleure façon d'établir la crédibilité et de vérifier l'authenticité d'une identité adéquate, que ce soit pour un utilisateur, une ressource de système, une entité d'information, etc. A la lumière de ces informations, il revient à l'utilisateur ou à l'organisation de déterminer si, aux fins considérées, il peut ou non se fier à un cadre de confiance donné ou à un autre système IdM. Les éléments principaux du cadre présenté dans cette Recommandation sont notamment: 1) un modèle de données d'entité numérique; 2) un protocole d'interface d'entité numérique; 3) un ou plusieurs système(s) de résolution/d'identificateur; et 4) un ou plusieurs registres de métadonnées. Ces éléments constituent la base du cadre d'architecture ouverte.

Historique

Edition	Recommandation	Approbation	Commission d'études
1.0	ITU-T X.1255	2013-09-04	17

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous <http://www.itu.int/ITU-T/ipr/>.

© UIT 2013

Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, par quelque procédé que ce soit, sans l'accord écrit préalable de l'UIT.

TABLE DES MATIÈRES

	Page
1 Domaine d'application	1
2 Références.....	1
3 Définitions	1
3.1 Termes définis ailleurs	1
3.2 Termes définis dans la présente Recommandation	2
4 Abréviations et acronymes	3
5 Conventions	3
6 Recommandation	3
6.1 Notion de confiance.....	4
6.2 Informations de confiance	5
6.3 Registres fédérés pour la découverte	6
7 Architecture d'interopérabilité pour les registres fédérés	7
7.1 Modèle de données d'entité numérique	8
7.2 Protocole d'interface d'entité numérique	10
7.3 Interactions avec un registre	11
7.4 Systèmes de résolution	12
7.5 Requêtes réparties et métadonnées agrégées dans les registres fédérés	13
7.6 Schémas de métadonnées	16
7.7 Interopérabilité des métadonnées	17
8 Types et attributs de type.....	17
9 Fédération hiérarchique et fédération fondée sur des relations entre homologues.....	19
Appendice I – Scénarios d'utilisation.....	22
Appendice II – Notation BNF d'un enregistrement de type.....	26
Bibliographie.....	28

Cadre pour la découverte des informations relatives à la gestion d'identité

1 Domaine d'application

La découverte des informations relatives à la gestion d'identité a trait au fait que l'on doit avoir la possibilité d'obtenir des informations pertinentes sur les identificateurs, y compris sur ceux qui utilisent la syntaxe des adresses de courrier électronique, les URL et les identificateurs persistants. Cette découverte est essentielle pour assurer l'interopérabilité entre des systèmes d'information hétérogènes.

La présente Recommandation décrit un cadre qui:

- permet de découvrir des informations relatives à l'identité et leur provenance, notamment des informations relatives à des services, des processus et des entités;
- permet de découvrir des attributs des informations relatives à l'identité, notamment des logos visuels et des noms de site lisibles par l'homme;
- permet de découvrir des attributs et des fonctionnalités d'applications;
- décrit un modèle de données et un protocole permettant d'assurer l'interopérabilité de métaniveau pour la représentation et la découverte des informations précitées et l'accès à ces informations dans des environnements IdM hétérogènes.

2 Références

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

[ISO 8601] ISO 8601 (2004), *Eléments de données et formats d'échange – Echange d'information – Représentation de la date et de l'heure.*

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 entité [b-UIT-T Y.2720]: tout type d'élément qui a une existence séparée et distincte et peut être identifié de manière unique. Dans le contexte de la gestion IdM, il peut s'agir d'abonnés, d'utilisateurs, d'éléments de réseaux, de réseaux, d'applications logicielles, de services et de dispositifs. Une entité peut avoir plusieurs identificateurs.

3.1.2 fournisseur d'identité [b-UIT-T Y.2720]: entité qui crée, maintient et gère des informations d'identité sécurisées pour d'autres entités (par exemple, utilisateurs/abonnés, organisations et dispositifs) et propose des services fondés sur l'identité basés sur une relation de confiance, commerciale ou d'autres natures.

3.1.3 partie utilisatrice [b-UIT-T Y.2720]: entité qui est tributaire d'une représentation ou d'une déclaration d'identité soumise par une entité requérante/assertante.

3.1.4 confiance [b-UIT-T Y.2720]: degré de fiabilité du caractère, de l'aptitude, du pouvoir ou de la vérité de quelqu'un ou de quelque chose.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 association: relation, éventuelle, entre deux entités identifiées.

3.2.2 entité numérique: entité représentée comme ou convertie en structure de données indépendante de la machine, constituée d'un ou de plusieurs éléments sous forme numérique qui peuvent être analysés par différents systèmes d'information; cette structure contribue à assurer l'interopérabilité entre divers systèmes d'information dans l'Internet.

3.2.3 découverte: fait de rechercher ou de localiser des informations relatives à une cible, autrement dit d'obtenir des connaissances relatives à la cible.

3.2.4 élément: partie d'une entité numérique constituée d'une paire type-valeur, où le type est représenté par un identificateur persistant qui peut être résolu et la valeur est l'information numérique pertinente correspondant à ce type.

3.2.5 registres fédérés: ensemble de registres interopérables qui enregistrent les métadonnées et participent à un ensemble commun de méthodes permettant de partager les informations de manière fiable et dans un format largement accepté.

3.2.6 identificateur: séquence de bits utilisés pour obtenir des informations sur l'état de l'entité en cours d'identification; pour cela, on utilise généralement un système de résolution approprié.

3.2.7 gestion d'identité: moyen permettant de valider les informations de gestion d'identité, que ce soit pour un utilisateur, une ressource de système, des informations ou d'autres entités.

3.2.8 informations de gestion d'identité: informations relatives à l'identité comprenant tous les types de métadonnées associées à l'identité, à la provenance, à l'association et à la confiance.

3.2.9 métadonnées: informations structurées relatives à l'identité d'utilisateurs, de systèmes, de services, de processus, de ressources, d'informations ou d'autres entités.

3.2.10 identificateur persistant: identificateur unique dont la résolution donne des informations sur l'état d'une entité numérique et qui peut être résolu au moins aussi longtemps que l'entité numérique existe.

3.2.11 provenance: informations relatives à n'importe quelle source d'informations, y compris la ou les parties qui interviennent pour produire, introduire et/ou attester ces informations.

3.2.12 registre: mécanisme utilisé pour enregistrer les métadonnées relatives aux entités numériques et stocker les schémas de métadonnées, et qui permet de rechercher des identificateurs persistants grâce à l'utilisation des schémas de métadonnées.

3.2.13 répertoire: interface qui accepte les dépôts d'entités numériques, permet de les conserver et offre un accès sécurisé aux entités numériques via leurs identificateurs.

3.2.14 système de résolution: système qui accepte en entrée les identificateurs qu'il connaît et fournit des informations pertinentes sur l'état de l'entité en cours d'identification.

3.2.15 point de contact: registre qui, dans un système de registres fédérés, est choisi pour servir d'interface avec un registre désigné dans une autre fédération, généralement à des fins d'échange entre homologues.

3.2.16 cadre de confiance: système IdM dans le cadre duquel un ensemble d'engagements vérifiables est conclu par chacune des diverses parties à une transaction auprès des parties homologues; ces engagements comportent nécessairement: a) des contrôles afin de garantir le respect des engagements; et b) des solutions en cas de non-respect de ces engagements.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

API	interface de programmation d'application (<i>application program interface</i>)
Bits	chiffres binaires (<i>binary digits</i>)
BNF	formalisme de Backus-Naur (<i>backus-naur form</i>)
ADN	acide désoxyribonucléique
DE	entité numérique (<i>digital entity</i>)
DEIP	protocole d'interface d'entité numérique (<i>digital entity interface protocol</i>)
HTTP	protocole de transfert hypertexte (<i>hypertext transfer protocol</i>)
ID	identificateur
IdM	gestion d'identité (<i>identity management</i>)
IdP	fournisseur d'identité (<i>identity provider</i>)
MAC	contrôle d'accès au support (<i>media access control</i>)
P2P	relation entre homologues (<i>peer-to-peer</i>)
PKI	infrastructure de clé publique (<i>public key infrastructure</i>)
RP	partie utilisatrice (<i>relying party</i>)
TCP	protocole de commande de transmission (<i>transmission control protocol</i>)
TF	cadre de confiance (<i>trust framework</i>)
URL	localisateur uniforme de ressource (<i>uniform resource locator</i>)
XML	langage de balisage extensible (<i>extensible markup language</i>)

5 Conventions

Aucune.

6 Recommandation

La présente Recommandation décrit un cadre d'architecture ouverte permettant de découvrir des informations de gestion d'identité. Elle traite:

- a) de la notion de confiance, qui est un aspect important de la gestion d'identité;
- b) des informations de confiance, qui peuvent être utilisées pour déterminer dans quelle mesure on peut se fier à une information IdM donnée;
- c) des registres fédérés pour la découverte;
- d) d'une architecture d'interopérabilité pour la fédération; et
- e) des fédérations hiérarchiques et des fédérations fondées sur des relations entre homologues.

La découverte d'informations de gestion d'identité repose sur l'utilisation de métadonnées obtenues auprès d'un registre ou d'un système de registres fédérés. Le cadre inclut un moyen permettant de résoudre les identificateurs persistants. En général, les registres fédérés seront utilisés par plusieurs parties et devront prendre en charge le modèle de données d'entité numérique pour représenter les enregistrements de métadonnées et le protocole d'interface d'entité numérique pour assurer l'interopérabilité de ces registres. Plusieurs schémas étant censés être utilisés, chaque registre doit contenir des détails sur les schémas de métadonnées publics et/ou privés utilisés par les différents identificateurs persistants. Les identificateurs persistants utilisant un schéma privé peuvent être

rendus publics, si on le souhaite, ou ils peuvent être conservés de manière privée ainsi que les schémas de métadonnées associés en vue d'une utilisation limitée au sein de communautés restreintes.

Les Appendices I et II contiennent respectivement un aperçu des scénarios d'utilisation et un exemple de description BNF d'un enregistrement de type (le formalisme BNF est une notation normalisée pour représenter les grammaires indépendantes du contexte).

6.1 Notion de confiance

Le terme 'confiance' est un terme qui comporte un certain nombre de connotations. Faire confiance à une personne ou à un procédé signifie généralement que l'on s'attend à ce que des événements aient un résultat donné, même si ces événements ne sont pas spécifiés précisément. Dans le cadre des systèmes de découverte, il faudra toutefois une spécification supplémentaire. Déclarer simplement que A fait confiance à B ne signifie pas que A fait confiance à B pour tous les résultats possibles d'un événement. Faire confiance à B pour offrir un service en retour d'un paiement donné est différent de faire confiance à B pour garder ce paiement secret ou pour ne pas publier les noms de ceux qui effectuent ces paiements.

Dans les cadres de confiance, l'élément le plus important est la gestion d'identité, afin d'être sûr que les parties à une transaction donnée sont bien celles qu'elles déclarent être. Mais la confiance dans le résultat d'une transaction donnée avec une partie donnée dépend non seulement de l'identité de cette partie mais aussi d'autres attributs des déclarations et assertions faites par cette partie. Pour pouvoir évaluer ces attributs de manière cohérente, il est nécessaire de disposer d'un vocabulaire ou d'un ensemble de mesures qui puisse être appliqué à ces attributs. Ces mesures et descriptions pourraient être appliquées par des tierces parties faisant office d'agences d'évaluation pour les cadres de confiance, ou une moyenne pourrait être faite sur des groupes d'évaluations émanant des utilisateurs, comme c'est le cas pour des systèmes faisant l'objet de Recommandations et d'autres applications 'faisant appel à la foule'. Les catégories recommandées pour ces mesures et descriptions sont décrites ci-après.

Force: niveau de fiabilité. Quelles sont les chances qu'une partie fera ce qu'elle dit qu'elle fera? Quelles sont les chances que l'assertion d'identité (par exemple je suis l'auteur de ce logiciel et les royalties me reviennent) est correcte? Ce niveau sera probablement exprimé par une valeur numérique ou littérale.

Classement: de quel type de fiabilité l'assertion relève-t-elle? Peut-on établir des catégories normalisées? L'identité est une catégorie en soi. Parmi les autres catégories, on pourrait citer la fiabilité financière (par exemple quelles sont les chances qu'une partie donnée procède comme promis dans une transaction financière), la confidentialité (quelles sont les chances qu'une partie donnée conserve de manière privée des informations pour lesquelles elle déclare qu'elles ne seront pas divulguées) et le fait de faire autorité (par exemple quelles sont les chances que les informations reçues en provenance d'une partie donnée soient exactes). D'autres catégories de haut niveau sont possibles et des sous-catégories sont possibles dans chaque catégorie.

Longueur de la chaîne de confiance: pour certaines transactions sécurisées, on utilise une chaîne de confiance, conçue fréquemment en termes de hiérarchie de certificats ou de couches logicielles signées numériquement. Le concept s'applique d'une manière générale à tous les domaines sécurisés: plus la chaîne d'assertions sécurisées par rapport à une ancre de confiance est longue, plus le niveau final de confiance est faible. Une mesure de la longueur de cette chaîne constituerait une mesure essentielle de la fiabilité de n'importe quelle identité ou autre assertion.

Chacun de ces attributs (et bien d'autres) pourrait être inclus dans les enregistrements de métadonnées décrivant les fournisseurs d'identité, les parties utilisatrices et tout autre élément impliqué dans des transactions sécurisées.

6.2 Informations de confiance

On examine ci-après trois aspects distincts relatifs aux informations de confiance en lien avec les fonctions et les actions exécutées dans une découverte fédérée et celles assurées par les entités constitutives participantes.

6.2.1 Informations de confiance dans une réponse de découverte

L'un des principaux objectifs de l'architecture ouverte décrite dans la présente Recommandation est de permettre de découvrir des informations de gestion d'identité; la détermination de la confiance est toutefois laissée au soin de l'utilisateur. D'autres fonctionnalités ou services peuvent être pris en charge dans l'architecture sous la forme de composants/modules facultatifs (logiciels et/ou matériels). A cet égard, l'architecture pourrait inclure facultativement un cadre de confiance et pourrait permettre d'enrichir une réponse de découverte en y incorporant des informations de confiance, voire pourrait prendre en charge la détermination de la confiance. Les entités externes pourraient déterminer si elles souhaitent recevoir ces informations de confiance directement. Elles pourraient choisir de désactiver la fonctionnalité et chercher à collecter elles-mêmes, ou à partir de leurs propres sources, des informations de confiance en vue de la détermination de la confiance.

6.2.2 Confiance dans le système de découverte

Il faut pouvoir faire confiance au système de découverte, afin que les parties externes aient confiance dans l'utilisation de ses capacités pour enregistrer des informations de gestion d'identité ou accéder à ces informations. Ce type de confiance peut être obtenu par divers moyens, y compris l'établissement de méthodes spécifiques, conjointement avec des politiques et des procédures associées à des fins de fiabilité. Parmi celles-ci, on peut citer l'évaluation des éléments mis en œuvre dans le contexte du cadre, les mesures prises à l'encontre des éléments ou des parties externes au comportement incorrect, et l'adaptation de cadres solides de sécurité et de confidentialité. Toutefois, la définition de la méthode exacte à utiliser pour parvenir à ce type de confiance n'entre pas dans le cadre de la présente Recommandation.

6.2.3 Parties externes fiables

L'architecture doit prendre en charge des politiques et des procédures qui encouragent les parties externes fiables à l'utiliser pour enregistrer des informations. Pour des raisons de sécurité, les entités constitutives qui sont directement impliquées dans l'enregistrement des informations de gestion d'identité doivent pouvoir contrôler les données insérées dans le système et détecter et/ou éviter les cas où des parties malveillantes essaient d'enregistrer de fausses informations.

Les demandes anonymes devraient être prises en charge, mais un grand nombre d'entre elles ne conduiront peut-être pas à des réponses utiles, sauf si l'identité des différents requérants est connue à l'avance grâce à d'autres moyens. En pareils cas, une capacité de gestion d'identité devrait pouvoir valider l'identité, quels que soient les éléments, y compris les utilisateurs/requérants. A l'intérieur du cadre, un fournisseur d'identité autorisé et reconnu attribue à chaque élément un identificateur persistant unique, dont la résolution donne des informations pertinentes sur l'élément. Comme indiqué ci-avant, aucune hypothèse n'est faite quant à la manière dont un élément d'une instance particulière déterminera s'il peut faire confiance à ces informations.

Pour de nombreuses demandes, l'identité du requérant (une partie externe qui a envoyé une demande de découverte) doit être validée avant qu'une réponse soit envoyée. Dans le cas général, tous les requérants seraient évalués avant que toute autre mesure soit prise. On suppose qu'aucune capacité de prise de décision n'est invoquée à l'intérieur de l'architecture; toutefois, avant d'élaborer la réponse finale à une demande de découverte, un mécanisme externe d'appui décisionnel peut être invoqué afin d'obtenir à l'avance une permission de la part des producteurs d'identité.

6.3 Registres fédérés pour la découverte

La présente Recommandation décrit un système de registres fédérés pour la découverte dont le but est de permettre de trouver et d'évaluer les métadonnées et autres informations relatives aux identificateurs, ainsi que les cadres de confiance et les autres systèmes IdM. Les registres fédérés peuvent fonctionner ensemble et partager leurs entités de métadonnées sous réserve de toute restriction éventuellement applicable. Les informations effectives qui correspondent à ces métadonnées peuvent être stockées dans les registres respectifs (si un tel stockage est autorisé), dans un ou plusieurs répertoires répartis; dans certains cas, les informations correspondant à ces métadonnées ne seront peut-être pas du tout accessibles dans l'Internet. Dans ce dernier cas, on surmonterait généralement cette limitation en procédant à une résolution de l'identificateur donnant des informations d'état pertinentes relatives à l'entité; toutefois, un registre pourrait également choisir de fournir ces informations.

A l'intérieur d'un système de registres fédérés, un registre donné peut fournir à un deuxième registre, pour une entité donnée, soit la copie complète de l'enregistrement de métadonnées d'origine correspondant à l'entité, soit un résumé de cet enregistrement. L'enregistrement d'origine, ou sa variante, serait décrit de manière à pouvoir déterminer d'où il a été obtenu, et à caractériser le type de communauté ou de domaine représenté par ce registre. Ce même registre initial pourrait donc faire office de point de collecte interdomaines pour de nombreux autres registres et offrir un service de recherche qui pourrait renvoyer les chercheurs vers d'autres registres pour rassembler d'autres informations. Ces points de collecte sont parfois appelés points de contact.

L'élément de l'architecture correspondant au registre est conçu selon plusieurs principes essentiels. Outre le fait qu'un identificateur doit être attribué à chaque entité numérique enregistrée, les enregistrements de métadonnées figurant dans le registre sont eux-mêmes structurés sous forme d'entités numériques, ayant chacune un identificateur associé. Ainsi, les enregistrements de métadonnées peuvent être référencés séparément; la résolution de leurs identificateurs donnera des informations d'état actuel relatives aux entités de métadonnées, même si les enregistrements passent d'un registre à un autre, ou sont disponibles auprès de plusieurs registres.

L'architecture ne limite aucunement le nombre d'entités de métadonnées qui peuvent être enregistrées pour une même entité numérique. Il peut être souhaitable de générer plusieurs entités de métadonnées pour les mêmes informations, en fonction de différentes perspectives, de différentes audiences, etc. La gestion de ces entités de métadonnées est grandement simplifiée par l'utilisation d'identificateurs uniques et persistants: on peut ainsi facilement déterminer si deux enregistrements de métadonnées font ou ne font pas référence aux mêmes informations sous-jacentes. D'autres entités peuvent également être créées afin de relier entre elles différentes entités de métadonnées et d'obtenir un résultat qui ne pourrait pas être obtenu à partir d'une recherche parmi ces différentes entités.

L'architecture permet d'établir des relations multipoint-multipoint, dans les deux sens, entre les répertoires et les registres. Un répertoire donné peut fournir des métadonnées relatives aux mêmes entités à plusieurs registres; et un registre donné peut accepter des métadonnées provenant de plusieurs répertoires. Le fait de collecter les métadonnées provenant de plusieurs répertoires et de les mettre dans un même registre permet de fédérer ces répertoires. Le fait de permettre à ces répertoires de fournir des métadonnées relatives aux mêmes entités à plusieurs registres permet à un même répertoire de faire partie de plusieurs fédérations, éventuellement distinctes les unes des autres par le fait qu'elles desservent des communautés différentes, qu'elles utilisent des schémas de métadonnées différents, des approches différentes en matière d'indexation et de recherche, et d'autres capacités.

Enfin, une instance de registre peut être fédérée avec d'autres registres. Plusieurs registres peuvent se transmettre leurs entités de métadonnées, ou des entités qui sont fonction de ces enregistrements de métadonnées d'origine. Un registre donné, appelé Reg1, peut fournir à un deuxième registre, appelé Reg2, pour une entité donnée, soit la copie complète de l'enregistrement de métadonnées

d'origine correspondant à l'entité, soit un résumé de cet enregistrement. L'enregistrement d'origine, ou sa variante, serait incorporé dans une entité numérique de manière à pouvoir déterminer qu'il provient de Reg1, et à caractériser le type de communauté ou de domaine représenté par Reg1. Si Reg1 est toujours fédéré avec Reg2, alors Reg2 pourrait faire office de point de collecte interdomaines pour de nombreux autres registres comme Reg1 et offrir un service de recherche qui pourrait renvoyer les chercheurs vers d'autres registres ou directement vers les entités numériques proprement dites, suivant l'approche suivie pour combiner et indexer les enregistrements de métadonnées potentiellement hétérogènes.

La présente Recommandation porte sur la gestion d'identité, mais un tel système peut aussi servir à découvrir d'autres types d'informations dans des systèmes répartis complexes dans l'Internet tels que ceux qui font intervenir "l'informatique en nuage" ou "l'Internet des objets". Dans un système de registres fédérés, les informations de résolution sont obtenues auprès des différents systèmes IdM. Grâce au mécanisme de découverte de la fédération, l'interopérabilité des systèmes IdM sera assurée de manière plus générale et une entité pourra obtenir des informations appropriées relatives aux autres systèmes IdM, ce qui lui permettra de développer sa confiance dans l'utilisation d'identificateurs provenant de ces systèmes.

La technologie de base des registres est utilisée par de très nombreux groupes, certains ayant opté pour des versions à code source ouvert et d'autres ayant développé des solutions propriétaires sur la base de spécifications communément comprises. La fédération est obtenue via des protocoles de partage de l'information. Une partie importante des travaux futurs basés sur la présente Recommandation sera consacrée à la description puis à l'établissement de manière formelle de ces spécifications, à la définition de protocoles et de procédures appropriés ainsi que de schémas de métadonnées appropriés, et à la détermination d'une approche communément acceptable de préservation de la confidentialité, le cas échéant. On considère que la marche à suivre en vue de décider d'opter pour un système IdM donné n'entre pas dans le cadre de la présente Recommandation.

7 Architecture d'interopérabilité pour les registres fédérés

Le système de registres fédérés de la présente Recommandation repose sur une architecture ouverte qui assure l'interopérabilité de systèmes d'information arbitraires. Il permet d'authentifier les informations et d'accéder à des informations structurées sous la forme d'entités numériques et stockées dans la plupart des types de systèmes de stockage normalisés. Une entité numérique est une structure de données commune permettant d'assurer l'interopérabilité de systèmes dans l'Internet; elle contient des éléments numériques, à savoir des données typées, associées à un identificateur persistant unique.

Trois éléments architecturaux sont utilisés pour la gestion des entités numériques. Chacun de ces éléments peut être utilisé séparément, mais ils se complètent et les trois ensembles offrent une capacité répartie et modulable de gestion de l'information pour l'Internet. Ces éléments sont les suivants:

- a) un système d'identificateurs modulable et réparti pour l'identification des entités numériques et pour la résolution des identificateurs;
- b) des répertoires pour l'accès aux entités numériques et leur gestion; et
- c) des registres pour la recherche fédérée et la découverte. Ces éléments permettent de gérer le système réparti résultant sur la base de spécifications et de protocoles d'interface et d'éviter de devoir procéder à une maintenance permanente d'éléments particuliers.

Les entités numériques constituent l'élément central autour duquel tous les autres éléments et services sont créés et gérés. Elles ne remplacent pas les formats et structures de données existants, mais permettent au contraire de représenter de manière commune ces formats et structures. Elles peuvent ainsi faire l'objet d'une interprétation uniforme et être transférées entre divers systèmes

d'information hétérogènes, quels que soient les changements opérés sur les systèmes au fil du temps. La conception de ce modèle est simple, mais sa mise en oeuvre détaillée n'est pas évidente. Un protocole permet d'interagir avec les entités numériques par l'intermédiaire des répertoires. Dans la présente Recommandation, toutes les métadonnées seront conformes au modèle de données d'entité numérique dans un souci d'interopérabilité et pour plus de commodité.

L'architecture ouverte repose principalement sur le modèle de données d'entité numérique et le protocole d'interface d'entité numérique pour l'accès aux entités numériques, décrits ci-dessous, associés à un système d'identificateurs et/ou de résolution et à des registres/répertoires. Ensemble, ces éléments permettent de gérer à long terme les informations structurées sous la forme d'entités numériques grâce à une identification unique et persistante, à une méthode permettant d'obtenir des informations d'état actuel relatives aux objets, à un service permettant d'obtenir les entités ou d'en faire un certain usage, et à un moyen permettant de déterminer les identificateurs des entités numériques sur la base d'informations contenues dans les registres de métadonnées.

7.1 Modèle de données d'entité numérique

Le modèle de données d'entité numérique décrit ici permet de représenter de manière uniforme les enregistrements de métadonnées sous la forme d'entités numériques, et peut aussi être utilisé pour représenter d'autres types d'information sous la forme d'entités numériques. C'est un modèle logique à partir duquel plusieurs formes de codage et de stockage sont possibles, et qui définit un point de référence unique (à savoir l'identificateur) pour de nombreux types d'information accessibles dans l'Internet. Chaque entité numérique a un ensemble d'attributs intrinsèques, un ensemble d'attributs définis par l'utilisateur, mis dans un ou plusieurs éléments, et éventuellement un ou plusieurs éléments supplémentaires contenant des informations (texte, signaux vidéo, images, etc.) représentées sous forme numérique. Tous ces éléments pourront être accessibles grâce à la spécification d'un protocole d'interface d'entité numérique défini précisément (voir § 7.2), permettant une authentification sécurisée au moyen d'une clé publique, et incorporant éventuellement un autre moyen d'authentification utilisant des interfaces API de niveau supérieur, selon ce que les répertoires d'entités numériques pourraient mettre en oeuvre. L'accès aux entités numériques peut ainsi se faire en toute confidentialité et sécurité.

L'attribut fixe essentiel d'une entité numérique est son identificateur unique persistant associé, dont la résolution donne des informations d'état actuel relatives à l'entité numérique, notamment son ou ses emplacements, les contrôles d'accès, et la validation, lorsqu'une demande de résolution est soumise au système de résolution. Comme exemple d'autres attributs intrinsèques d'une entité numérique, on peut citer: la date de dernière modification, la date de création et la taille. D'autres attributs peuvent être définis par les utilisateurs moyennant des permissions appropriées.

Parmi les attributs qui ne sont pas spécifiquement pris en considération dans le modèle de données d'entité numérique de base, on peut citer la propriété, l'authentification et les modalités et conditions d'accès. Ces attributs seront importants dans la plupart des mises en oeuvre d'entités numériques; il semble toutefois peu probable de pouvoir définir une solution unique. Les informations de propriété et de contrôle d'accès figureront probablement dans des attributs d'entité numérique définis par les utilisateurs ou dans des éléments de données distincts. On dispose ainsi d'une méthode commune pour prendre en charge divers schémas relatifs à la propriété et à la gestion d'informations, ainsi que divers schémas d'authentification et d'autorisation, sans partir de l'hypothèse qu'une même approche sera utilisée dans tous les domaines et dans toutes les communautés d'utilisateurs.

L'association d'un modèle de données standard, d'un protocole défini pour les interactions avec ce modèle de données, et d'un système de résolution/d'identificateur, est essentielle pour la gestion cohérente à long terme des informations dans l'Internet. Le système de résolution devrait être un système réparti, sécurisé et hautement performant, conçu pour qu'il puisse être fait référence de manière persistante aux entités numériques sur de longues périodes de temps et indépendamment des changements d'emplacement, de méthodes d'accès, de propriété et d'autres attributs modifiables.

La capacité de base de découverte d'informations IdM résulte de l'utilisation de l'élément registre, qui inclut le répertoire. La fonction d'un registre donné est d'assurer une fédération entre les collections d'entités numériques, pour permettre aux utilisateurs finals et aux applications de faire des recherches et de naviguer dans l'univers des entités enregistrées. Les répertoires qui contiennent des collections d'entités numériques peuvent fournir à un ou plusieurs registres des métadonnées relatives aux entités numériques dont ils sont responsables. Un même registre peut collecter des métadonnées auprès de plusieurs répertoires, et un même répertoire peut envoyer des métadonnées à plusieurs registres. Les registres peuvent offrir des fonctions de recherche et d'établissement de rapport parmi les entités représentées et offrir un point d'accès au monde structuré des entités numériques et des répertoires.

Dans certaines situations, il se peut que les registres ne soient pas, à proprement parler, nécessaires, par exemple dans le cas où une référence directe à une entité numérique, sous la forme de son identificateur, est intégrée dans une autre entité numérique ou dans un message ou un autre document. Bien souvent toutefois, l'utilisateur final, ou le processus automatique agissant pour le compte d'un utilisateur, ne connaîtra pas l'identificateur de départ, et devra utiliser une sorte de processus de recherche ou de tri pour découvrir la référence nécessaire. Même si un utilisateur connaît l'identificateur, il est possible qu'il ne sache pas comment le résoudre, ou comment interpréter les résultats de la résolution. Le fait d'enregistrer l'existence des entités numériques dans des registres peut aider à résoudre ce problème de façon très générale.

La définition d'opérations qui interagissent avec un modèle de données spécifié permet de créer et d'utiliser des entités numériques pour représenter la plupart des types d'informations structurées. On trouvera plus de détails dans le paragraphe qui suit. Un modèle de données d'entité numérique type est illustré sur la Figure 1. La représentation des entités indépendamment des détails de la mise en oeuvre du système de stockage correspondant est essentielle pour l'interopérabilité, car elle permet d'utiliser un même modèle logique pour divers formats et méthodes de stockage.

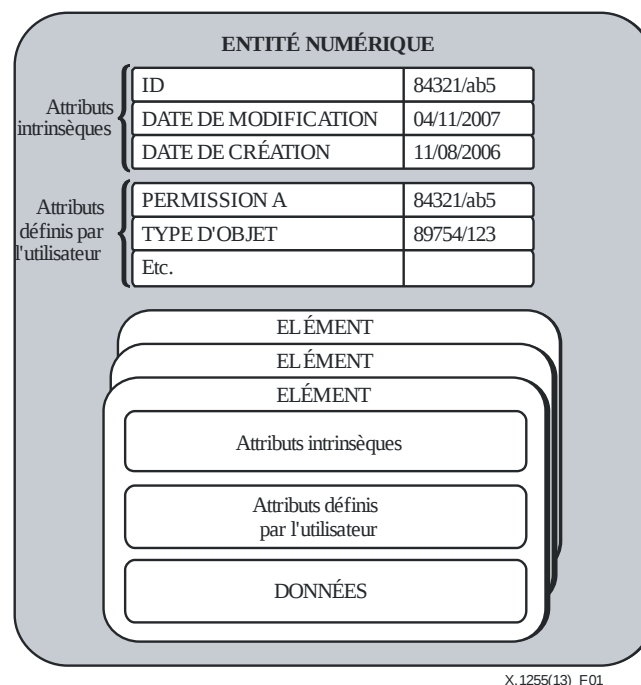


Figure 1 – Exemple de représentation d'une entité numérique

A l'exception de l'identificateur persistant en haut, toutes les données indiquées sur la Figure 1 sont conceptuelles. Chaque élément d'une entité numérique peut prendre différentes formes: références d'entité numérique selon l'identificateur, entité numérique réelle, données locales en clair correctement typées.

Les registres peuvent utiliser ou incorporer des répertoires pour stocker les enregistrements de métadonnées; les répertoires sont des systèmes de gestion de l'information qui donnent accès aux collections d'entités numériques via le protocole d'interface d'entité numérique. Les répertoires peuvent généralement être considérés comme incorporant les entités numériques auxquelles ils donnent accès. Dans une représentation plus détaillée, ils apparaîtraient toutefois comme des portails d'entrée dans diverses mémoires et divers systèmes d'information, mappant les données brutes dans des entités numériques qui peuvent être stockées localement ou à distance. Il pourrait s'agir simplement d'un système de fichiers conservant les données relatives à une entité numérique donnée dans un ou plusieurs fichiers qui sont inconnus ou invisibles pour les utilisateurs. Une autre solution, en particulier pour les entités complexes, consiste à répartir les données en plusieurs endroits et dans plusieurs systèmes et à les rassembler sous forme d'entité numérique uniquement sur demande, les informations de mappage de l'entité étant conservées dans une mémoire et les données proprement dites étant conservées dans d'autres systèmes. Cette technique d'interaction avec les systèmes existants est essentielle pour la fédération, étant donné que les informations contenues dans un système d'information arbitrairement complexe peuvent être subdivisées logiquement en entités numériques, et que ces entités numériques peuvent être mises à disposition de manière normalisée, le protocole DEIP étant utilisé dans les applications centrées sur l'utilisateur.

Un client d'entité numérique peut localiser un ou plusieurs répertoires pour une entité numérique donnée grâce à la résolution de son identificateur. La demande de résolution renverra l'emplacement d'un ou de plusieurs répertoires pertinents avec lesquels le client peut lancer une transaction relative à l'entité numérique.

Le logiciel des répertoires d'entités numériques dispose en principe de plusieurs interfaces de réseau pour la réalisation d'opérations sur les entités numériques, à savoir le protocole d'interface d'entité numérique pour l'interaction avec l'entité numérique proprement dite, ainsi que des interfaces souhaitables localement en fonction des options technologiques actuelles. Les diverses interfaces présentent chacune leurs propres avantages en termes de sécurité, de compatibilité avec les serveurs proxy, et d'utilisation de logiciels client ubiquitaires. Le protocole d'interface d'entité numérique intègre une certaine redondance, ainsi qu'une authentification forte – individuelle et de groupe. La redondance est prise en charge par un système de duplication miroir dans lequel chaque répertoire d'entités numériques communique avec les autres afin de conserver la synchronisation des entités dupliquées. L'authentification repose sur des clés secrètes ou des clés publique/privée ou sur d'autres mécanismes.

Parmi les autres fonctionnalités importantes, figurent la duplication, facilitant la duplication miroir parmi les répertoires, et l'extensibilité grâce à des modules d'extension. Des modules d'extension pourraient être créés pour gérer à la fois les activités propres au type d'entité (par exemple l'analyse d'un format vidéo et la fourniture d'une section demandée) et les activités orientées vers les services de réseau (par exemple la fourniture de métadonnées à un registre d'entités numériques).

7.2 Protocole d'interface d'entité numérique

Chaque interaction avec une entité numérique consiste en l'invocation ou l'application par une entité identifiée d'une opération sur une entité numérique. Les informations de gestion d'identité concernant l'entité, chaque opération et la cible de l'opération sont toutes identifiées de manière univoque et persistante. En outre, les entités identifiées sont des ressources de diverses sortes; les informations d'état pertinentes relatives à une ressource peuvent inclure, entre autres, sa clé publique.

Les opérations sont appliquées aux entités par des répertoires, qui sont eux-mêmes des entités numériques, et qui donnent accès aux entités qu'ils contiennent. Le protocole d'interface d'entité numérique définit la méthode par laquelle l'entité communique avec un répertoire afin d'invoquer des opérations sur les entités numériques auxquelles le répertoire donne accès. Ces opérations peuvent notamment être utilisées pour accéder à des enregistrements de métadonnées spécifiques au

moyen de leurs identificateurs; mais il est également possible d'accéder à ces enregistrements de manière sémantique par d'autres moyens (applications dédiées de registre, navigateurs web, etc.).

Une opération sur une entité numérique fait intervenir les éléments suivants:

- EntityID: identificateur de l'entité demandant l'invocation de l'opération;
- TargetObjectID: identificateur de l'entité à laquelle l'opération s'applique;
- OperationID: identificateur qui spécifie l'opération à effectuer;
- Input: séquence de bits contenant les données d'entrée de l'opération (paramètres, contenu ou autres informations); et
- Output: séquence de bits contenant les données de sortie de l'opération (contenu ou autres informations).

Les informations de gestion d'identité peuvent être accompagnées d'un certificat contenant une assertion de confiance explicite ou implicite au sujet des informations ou peuvent être communiquées dans le cadre d'un tel certificat. Toutefois, le destinataire n'acceptera pas nécessairement le certificat si celui-ci n'a pas été créé par une autorité de confiance acceptable. Au lieu des certificats, on peut aussi utiliser des jetons pour fournir un résultat de confiance analogue. Ces certificats ou jetons augmentent la probabilité que les informations d'identité acheminées soient exactes; toutefois, les mécanismes de sécurité intrinsèques susceptibles d'être mis en oeuvre dans le cadre de cette architecture ouverte peuvent valider de manière indépendante le fait que l'entité utilisant les informations de gestion d'identité possède la clé privée appropriée qui peut être utilisée pour valider l'entité identifiée. L'une ou l'autre partie à une demande de transaction faisant intervenir des entités identifiées peut demander à l'autre partie de chiffrer une chaîne avec sa clé privée et de la retourner à la partie requérante pour validation. Les parties à n'importe quelle transaction au sein du système peuvent invoquer d'autres moyens d'authentification, mais il n'existe aucune obligation a priori de négociation de ces autres moyens. Le mécanisme par défaut indiqué ci-après consiste à utiliser des paires de clés publique/privée, ce que permet intrinsèquement le protocole DEIP. Toutefois, d'autres mécanismes d'authentification peuvent être utilisés d'un commun accord entre les parties si elles le souhaitent. L'invocation du protocole DEIP entraîne, au minimum, les étapes ci-après qui ne sont pas facultatives:

- a) une association est établie entre la partie A et la partie B, à savoir les deux parties à la transaction, à moins qu'il existe déjà une association qu'elles peuvent utiliser à cette fin;
- b) la partie A peut facultativement demander à la partie B de se valider auprès de la partie A, par exemple en utilisant une méthode PKI;
- c) la partie A adresse alors une demande spécifique à la partie B, selon qu'il convient;
- d) la partie B peut facultativement demander à la partie A de se valider auprès de la partie B, par exemple en utilisant une méthode PKI;
- e) la partie B accepte ou rejette la demande, selon qu'il convient; et
- f) la transaction est terminée et soit une nouvelle demande est générée soit il est mis fin à l'association, s'il y a lieu.

Un exemple possible de spécification du protocole d'interface d'entité numérique est décrit dans la publication [b-DOIP] (voir également [b-DO Repo]), mais ne fait pas partie intégrante de la présente Recommandation.

7.3 Interactions avec un registre

Chaque interaction avec un registre fait intervenir une entité identifiée qui peut être une personne ou une ressource de système; chaque entité a un identificateur persistant qui peut être utilisé pour l'authentifier. Lors de l'établissement, un registre peut être préconfiguré pour faire confiance aux clients identifiés d'une certaine manière via leurs identificateurs. Les clients peuvent également

choisir d'authentifier les registres selon la même procédure. En outre, certains clients peuvent être configurés de manière à fonctionner selon les exigences particulières d'un processus de fédération. Ainsi, une opération particulière serait possible au niveau du registre en plus de celles qui sont communément mises à la disposition de tous les clients fiables. Lorsque des clients interagissent avec un registre, le registre lance une demande-réponse pour vérifier que le client possède la clé privée correspondante. Une fois cette vérification faite, le registre vérifie que l'identificateur appartient à l'entité.

Les opérations suivantes sont assurées à l'interface du registre:

- **Enregistrer une entité numérique:** Les informations d'enregistrement peuvent être uniquement des métadonnées, mais elles peuvent aussi être des métadonnées associées à une entité numérique à laquelle les métadonnées s'appliquent. Le registre gère l'entité numérique enregistrée en utilisant son répertoire interne. En outre, il indexe les informations structurées sous la forme d'une entité numérique en utilisant des règles préconfigurées qui déterminent comment analyser, mettre sous forme de jetons, et indexer les informations contenues. Si nécessaire, le registre crée un identificateur pour l'entité numérique et fait en sorte qu'il soit inséré dans le système de résolution.
- **Annuler l'enregistrement d'une entité numérique précédemment enregistrée:** Le registre supprime l'entité numérique de son répertoire interne, annule son indexation et met à jour le système de résolution afin que l'entité ait le statut supprimé.
- **Récupérer une entité numérique précédemment enregistrée via son identificateur:** Le registre sérialise l'entité numérique gérée dans son répertoire interne et la transmet au client.
- **Faire une recherche:** Le registre analyse l'expression de recherche concernant des mots clés, des correspondances exactes ou des requêtes sur un intervalle afin de trouver les entités numériques indexées correspondantes, et retourne les identificateurs de ces entités. Des techniques de recherche plus évoluées, telles que les requêtes en langage naturel, peuvent être facilement intégrées, si les résultats des travaux de recherche le permettent.
- **Obtenir le numéro de la transaction la plus récente:** Le registre, qui attribue des numéros de série à chaque opération d'enregistrement ou d'annulation d'enregistrement effectuée le concernant, retourne le dernier de ces numéros à un client qui est configuré pour participer à un processus de fédération avec le registre. Ainsi, les clients potentiels (les autres registres participant au processus de fédération) peuvent déterminer l'état du registre afin de distribuer des entités enregistrées en fonction de la topologie de fédération configurée et du niveau d'agrégation choisi.

L'authentification peut être désactivée, mais il est recommandé que le registre authentifie le client et vice versa. Le codage des messages échangés peut varier et dépend de la mise en oeuvre. Les messages peuvent être codés sous forme d'opérations de répertoire d'entités numériques, auquel cas une transaction de registre sera une série d'opérations de répertoire, par exemple créer une entité numérique, ajouter un élément. Une autre solution consiste à coder les messages au moyen de bibliothèques de codage de données tierces, sous réserve que la source et le destinataire s'entendent (probablement à l'avance) sur l'utilisation de la même bibliothèque.

7.4 Systèmes de résolution

L'un des éléments du cadre est le système de résolution (il peut y en avoir plusieurs) qui convertit les identificateurs en informations d'état utiles relatives à l'entité numérique en cours d'identification, par exemple son emplacement dans l'Internet, ou des informations d'authentification relatives à cette entité, ou une clé publique associée à l'identificateur. L'architecture ouverte du cadre permet d'assurer l'interopérabilité des systèmes de résolution, ce qui est un objectif souhaitable de la présente Recommandation. Les informations d'état peuvent être modifiées si nécessaire pour refléter l'état actuel de l'entité identifiée sans modifier son

identificateur, ce qui permet d'avoir un identificateur persistant au fil des modifications d'emplacement et autres modifications d'état connexes.

Si l'identificateur d'une ressource nécessaire est connu, le système de résolution et l'ensemble de répertoires fournissent à un processus ou à un utilisateur final autorisé ce dont il a besoin pour visualiser l'entité ou l'accéder. Mais lorsque l'identité de la ressource nécessaire est inconnue, elle devra être découverte. Dans le domaine des sciences de l'information et des bibliothèques, on parle dans le premier cas de recherche d'un "élément connu" (autrement dit la personne sait ce qu'elle souhaite et a besoin de savoir comment y accéder). Dans le deuxième cas, il faut généralement procéder à une recherche par sujet, les outils utilisés dans une telle recherche ayant pour but de la ramener à la recherche d'un élément connu. Le registre d'entités numériques permet de remplir cette fonction.

Une instance de registre peut fonctionner de manière autonome, mais elle peut uniquement répondre aux demandes de découverte d'informations dont elle a connaissance. La fédération de plusieurs registres lui permet d'avoir connaissance d'entités numériques enregistrées ailleurs, de sorte qu'une recherche plus large est possible dans toute la collection des entités numériques. L'aptitude à déterminer quels registres peuvent contenir des informations relatives à l'identité concernée est un aspect important de la découverte des informations de gestion d'identité. Il se peut qu'un système donné soit amené à découvrir des informations disponibles dans un autre système, éventuellement de conception différente. Dans l'hypothèse où une entité a défini un moyen d'associer de tels systèmes différents et les informations qu'ils contiennent, le cadre de découverte devrait alors permettre de découvrir ces associations. Toutefois, la présente Recommandation n'aborde pas la question de savoir qui est chargé d'établir ces associations, quels types d'informations peuvent être associés, ou comment l'association est établie et comment on y accède, ce qui, en général, dépendra du contexte. La présente Recommandation ne propose donc aucune pratique en matière d'association, quelle qu'elle soit. Dans un souci de clarté, le terme "association" figure dans la liste des termes définis et le concept est utilisé dans la définition des informations de gestion d'identité.

Dans de nombreux cas, la confidentialité est essentielle et, pour la gérer, on utilise des techniques de gestion d'identité basées sur les identificateurs des personnes, groupes, rôles et ressources, ainsi que les termes et conditions qui sont obtenus à partir des métadonnées stockées.

7.5 Requête réparties et métadonnées agrégées dans les registres fédérés

Le système de registres fédérés décrit dans la présente Recommandation devrait être largement accessible. Formant la base d'un système de découverte à architecture ouverte, il offre un moyen uniforme de découverte des informations de gestion d'identité. Un système de registres fédérés permet à plusieurs fournisseurs IdM de participer à la fourniture de registres interopérables et de déterminer quelles informations ils souhaitent partager avec les autres registres.

La technologie des registres permet aux parties chargées de créer des entités numériques dans l'Internet, y compris des services et d'autres entités, d'enregistrer l'existence d'un ensemble donné de ces entités, d'accompagner cet enregistrement de métadonnées descriptives et structurelles relatives aux entités, y compris des informations de provenance, et d'améliorer ainsi la découvrabilité des entités soit pour le grand public soit pour une communauté particulière. Une métadonnée essentielle qui doit être enregistrée avec l'entité numérique est son identificateur persistant; celui-ci doit pouvoir être résolu dans l'Internet. Pour les entités qui ne sont pas déjà identifiées, le registre peut être configuré pour créer des identificateurs dans le cadre du processus d'enregistrement et offrir les outils dont les administrateurs des entités numériques ont besoin pour tenir à jour les informations de résolution.

Le système de registres fédérés permettra de réaliser quatre grands objectifs en matière de découverte. Premièrement, il permettra d'appliquer des politiques de sélection uniformes à travers les cadres de confiance et autres systèmes IdM participants. Deuxièmement, il permettra à un utilisateur d'accéder aux informations de registre auxquelles il est autorisé à accéder sans avoir à

s'adresser directement à plusieurs registres. Troisièmement, il fournit une infrastructure d'appui en ce qui concerne la confidentialité et les autres restrictions d'accès établies par les différents systèmes IdM. Et quatrièmement, il permettra de prendre en charge le multilinguisme en assurant un accès sémantique aux registres.

Le concept de registres fédérés, basé sur l'architecture ouverte décrite dans la présente Recommandation, offre les avantages suivants:

- **Politiques de sélection unifiées:** Les registres et les cadres de confiance ou autres systèmes IdM de façon plus générale qui leur sont associés peuvent être sélectionnés pour les requêtes sur la base des propriétés des informations qu'ils sont censés contenir. Un système IdM dont les informations sont confirmées par une vérification effectuée à un certain niveau serait en principe sélectionné. Un cadre de confiance minimal ou un autre système IdM qui ne fait que vérifier les informations de carte de crédit ou les permis de conduire peut aussi être sélectionné. A l'autre extrême, un système IdM qui soumet les personnes à des tests ADN peut être sélectionné. Une organisation qui met en oeuvre des politiques visant à garantir l'intégrité des systèmes peut être sélectionnée. Ainsi, une méthode uniforme de sélection peut être appliquée à travers l'ensemble des registres et de leurs systèmes IdM associés.
- **Métadonnées partagées:** Les informations rendues accessibles dans un système de registres fédérés sont appelées métadonnées partagées. Un gabarit générique est associé aux métadonnées partagées, qui définit la manière dont les métadonnées sont représentées et donc la manière dont on peut y accéder en vue d'un traitement ultérieur. Le gabarit ne contient pas d'éléments spécifiques.
- **Accès fédéré:** Si un registre donné ne possède pas les informations voulues, celles-ci pourront être accessibles auprès d'un ou de plusieurs autres registres. En réalité, en mode normal, le système fonctionnera de manière telle que ces informations seront directement accessibles à l'utilisateur, indépendamment du registre qui a pu les contenir. Un tel accès peut être rendu possible par divers moyens (fédération hiérarchique, systèmes d'échange entre homologues, etc.).
- **Accès privé:** Certains registres seront restreints à certains groupes d'utilisateurs, types d'application ou rôles associés à l'utilisation du système, tandis que d'autres seront peut-être ouverts à tous. Le moyen de restreindre l'accès selon certains critères fait partie intégrante du système. Un ou plusieurs mécanismes, convenus par les registres participants, seront utilisés pour préserver la confidentialité à l'intérieur du système.
- **Accès sémantique:** Un système de typage est utilisé pour interpréter les "types" insérés. Les fournisseurs IdP peuvent choisir leurs propres types conformément aux lignes directrices relatives à la spécification. Ainsi, un accès sémantique aux informations pertinentes sera possible indépendamment de l'endroit où elles sont susceptibles d'être stockées dans le système, ce qui sera utile pour la prise en charge du multilinguisme.

Dans un tel système, les métadonnées sont disponibles sous forme de données structurées et comportent un identificateur persistant unique associé dont l'existence est aussi longue que celle de l'entité numérique. Le domaine et/ou le schéma des métadonnées peuvent varier d'un registre à l'autre, d'où des difficultés pour effectuer une recherche simple mais cohérente à travers l'agrégation de tous les enregistrements. Si, pour les différents schémas ou domaines, les métadonnées sont réduites à un schéma correspondant au plus petit dénominateur commun, ce qui constitue une solution pour agréger ce type de données, une stratégie de recherche optimale peut consister à identifier les meilleurs registres possibles pour une recherche plus détaillée. La transformation en schéma correspondant au plus petit dénominateur commun pourrait être effectuée par les registres sources ou par le registre collecteur. Une autre solution pourrait consister à effectuer un certain mappage de la recherche proprement dite afin de mener des requêtes appropriées – basées sur la requête d'origine – sur les divers schémas de métadonnées.

Tandis qu'agrérer les entités de métadonnées pour découvrir des informations provenant de plusieurs domaines est une possibilité, effectuer des requêtes réparties à travers plusieurs registres gérant chacun les entités de métadonnées de son domaine en est une autre. Il existe diverses autres possibilités dans le contexte de la fédération des registres, comme illustré par l'espace à trois dimensions représenté sur la Figure 2.

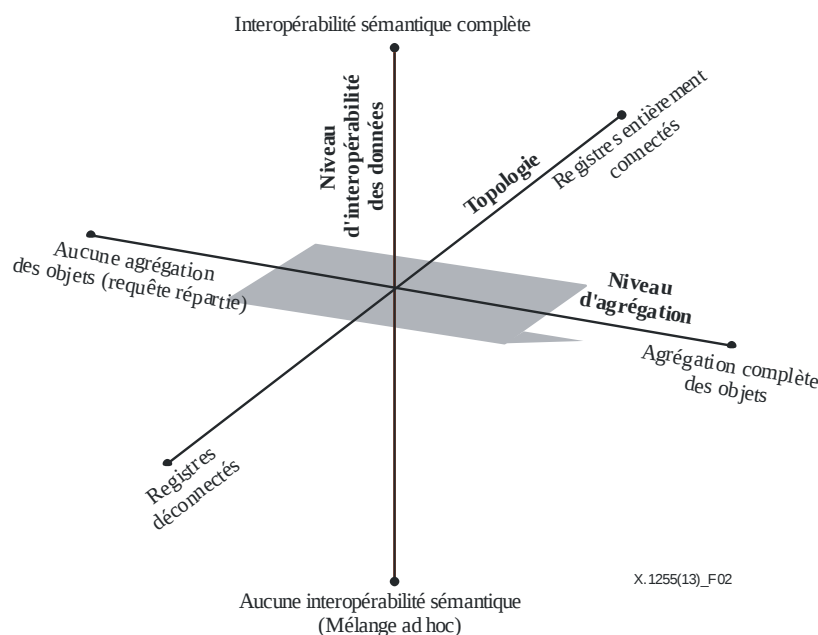


Figure 2 – Requêtes réparties à travers plusieurs registres

Sur cette Figure 2, trois axes sont représentés. Le premier axe indique le niveau d'agrégation des métadonnées des registres et va d'aucune agrégation à l'agrégation complète. Le deuxième axe indique le degré de connectivité topologique entre les registres. Le troisième axe se rapporte à l'interopérabilité des informations des différents registres. Chacun de ces axes est décrit plus en détail ci-après.

L'axe de niveau d'agrégation indique dans quelle mesure il est procédé au préalable à l'agrégation des entités de métadonnées à travers les registres. Le point à l'extrémité gauche de l'axe correspond à des entités qui ne sont pas agrégées à travers les registres avant toute requête, tandis que le point à l'extrémité droite de l'axe correspond au fait que tous les entités sont agrégées avant toute requête. Les points le long de l'axe représentent d'autres possibilités, y compris l'agrégation des informations de métadonnées correspondant au plus petit dénominateur commun, l'agrégation des indices de recherche, etc. A mesure que l'on se déplace de gauche à droite, l'actualité des informations agrégées diminue; la requête répartie produit davantage de résultats récents, tandis que l'actualité des entités de métadonnées agrégées dépend de la question de savoir à quand remonte la dernière agrégation.

L'axe de topologie indique dans quelle mesure les registres sont connectés. A l'une des extrémités de l'axe, les registres ne sont pas du tout connectés en réseau, d'où l'absence de partage d'informations; à l'autre extrémité, les registres sont entièrement connectés entre eux. Il est à noter que le degré de connexion dépend du niveau d'agrégation et que la topologie détermine uniquement les liens possibles.

L'axe de niveau d'interopérabilité des données indique dans quelle mesure les entités de métadonnées d'un registre concernant un certain domaine d'information sont interopérables avec les entités de métadonnées d'un autre registre concernant un domaine d'information différent. En d'autres termes, les schémas de métadonnées adoptés par un registre donné ne sont pas nécessairement interopérables avec les schémas adoptés par l'autre registre. Parfois, il est nécessaire de transformer les entités de métadonnées pour parvenir à un certain niveau d'interopérabilité, voire à une interopérabilité totale. Dans d'autres cas, lorsque les schémas sont trop éloignés l'un de l'autre du point de vue sémantique, aucune transformation, quelle qu'elle soit, ne permettra d'atteindre un niveau utile d'interopérabilité.

Il est à noter que les points de l'espace à trois dimensions représenté sur la Figure 2 ne sont pas tous valables. Par exemple, une requête répartie sur des noeuds déconnectés implique que l'on a pas de répartition de requêtes du tout. De même, l'agrégation complète d'entités non interopérables implique que l'on a un système d'entités incohérents. Dans la mesure où les points de l'espace à trois dimensions illustré sont valables, il convient de prévoir ces possibilités de configuration dans la conception de base des registres. Par ailleurs, la question de savoir si le mappage a lieu au niveau de la transformation des enregistrements de métadonnées ou au niveau de la recherche et la question de savoir si les enregistrements de métadonnées sont transformés par les registres sources ou par le registre collecteur dépendent de la mise en oeuvre. Les conséquences sur le plan des performances peuvent être importantes, mais la conception de base devrait rendre possibles différentes variantes de mise en oeuvre.

L'approche retenue dans la présente Recommandation ne résout pas le problème de la recherche et de la récupération à travers des systèmes d'information hétérogènes, mais elle permet de disposer d'un cadre commun dans lequel différentes approches peuvent être utilisées. De fait, il est probable qu'il n'y ait pas de solution unique au problème et que les approches optimisées varient suivant la communauté de pratique et le domaine.

7.6 Schémas de métadonnées

L'un des principaux objectifs de la présente Recommandation est de jeter les bases de la définition d'un ensemble de schémas de métadonnées de "haut niveau" pour assurer la découverte d'informations concernant: a) les identificateurs utilisés dans divers systèmes IdM; b) les fournisseurs d'identité; c) les parties utilisatrices; et d) les cadres de confiance et autres systèmes IdM à tous les niveaux, ainsi que les politiques, les procédures et l'infrastructure technique sous-jacente. Les éléments nécessaires de ces schémas de métadonnées dépendront des différents scénarios d'utilisation, mais devront être extensibles à la fois au niveau des éléments et au niveau des schémas pour s'adapter à la croissance et à l'évolution dans un domaine dynamique.

Les diverses entités intervenant dans la gestion d'identité peuvent définir chacune leurs propres schémas particuliers et, si nécessaire, les mapper dans ces schémas de métadonnées normalisés de haut niveau pour décrire leurs services, politiques et procédures, et enregistrer ces descriptions dans un ou plusieurs registres d'un ensemble de registres fédérés. Ces registres prendraient en charge des services de découverte à travers les entités enregistrées.

Il est possible qu'on puisse créer un seul schéma de métadonnées tenant compte de tous les aspects des technologies IdM, des organisations concernées et des politiques et procédures associées, mais il est proposé de commencer par un schéma différent pour chaque type d'entité concernée. Le processus engagé pour parvenir à un ensemble convenu de schémas de métadonnées deviendra un processus collaboratif dans lequel les parties intéressées partageront leurs connaissances relatives aux attributs qui doivent être pris en charge par les schémas; les schémas en évolution pourront alors être testés dans divers scénarios d'utilisation afin de déterminer s'ils fournissent bien les informations nécessaires pour les processus de découverte, et pourront être complétés si nécessaire.

7.7 Interopérabilité des métadonnées

Les identificateurs sont importants pour parvenir à l'interopérabilité des métadonnées. Toutefois, certains autres aspects de l'interopérabilité des métadonnées, en particulier ceux nécessitant une définition humaine et un contexte de descriptions, n'entrent pas dans le cadre de la présente Recommandation. D'autres attributs spécifiés dans les métadonnées, tels que ceux décrivant ou permettant une configuration particulière, par exemple un mode de connexion et une approche d'agrégation spécifiques, relèvent du fonctionnement des registres. Aux fins de la gestion des entités de métadonnées à travers divers registres, l'interopérabilité des métadonnées sera facilitée si les parties qui travaillent en collaboration arrêtent des schémas de métadonnées communs. Les métadonnées seront alors gérées comme étant des entités homogènes, et les registres les interpréteront et les traiteront de manière cohérente. Le paragraphe 9 ci-après illustre deux cas particuliers de fédération dans le contexte du niveau d'agrégation et de la topologie, deux dimensions qui s'appliquent d'une manière générale à ce cadre.

8 Types et attributs de type

Les registres contiennent des enregistrements de métadonnées sous la forme d'entités numériques qui sont destinés à être échangés avec d'autres registres fédérés. Chacun de ces enregistrements est constitué d'un ensemble d'éléments, contenant chacun un champ "type" et un champ "valeur". Il est essentiel de bien comprendre la signification de chaque type afin que les valeurs associées se présentent sous une forme autre qu'une séquence opaque de bits, ou qu'un ensemble opaque de séquence de bits.

Pour bien comprendre ce qu'un type signifie, les types sont représentés par des identificateurs persistants dont la résolution donne des informations utiles relatives au type. La description des types est destinée à être créée par des personnes, mais il est nécessaire de disposer d'un moyen standard pour décrire et représenter les types.

Les aspects et attributs spécifiques qui seront finalement pris en compte dans la définition d'un type devraient évoluer au fil du temps, mais les quatre aspects suivants sont considérés comme essentiels:

- la première catégorie d'attributs est la plus simple et est constituée de descriptions de l'entité du type qui sont lisibles par l'homme. Ces descriptions sont destinées à décrire l'entité du type, les ressources et concepts associés, et son utilisation. Ces attributs prendront en charge des descriptions dans plusieurs langues;
- la deuxième catégorie d'attributs de la description du type est constituée des informations de provenance. Pour chaque type, sa définition devrait inclure la date de sa création, la date de sa dernière mise à jour, ses contributeurs, son statut, et tout identificateur d'alias qu'il est susceptible avoir;
- la troisième catégorie d'attributs est liée à la description de la catégorisation des types et à la capacité de types de tirer parti d'autres types;
- la quatrième catégorie d'attributs permet à divers systèmes d'agir dynamiquement sur une ressource d'un type particulier.

Les trois dernières catégories sont décrites plus en détail ci-après.

Un type est généralement utilisé pour décrire une catégorie particulière de ressources et/ou de concepts conformément à un ensemble donné de caractéristiques. Cette catégorie représente le domaine d'applicabilité du type et correspond à ce que l'on appelle le genre du type. Par exemple, pour un type de codage de caractères utilisé pour spécifier comment un caractère doit être représenté dans un format binaire, son genre serait le codage. Pour un type de formatage de données utilisé pour spécifier comment représenter une structure sous la forme d'un ensemble de bits, son genre serait le formatage.

Pour chaque type, sa description comporte un attribut qui spécifie son genre. L'attribut de description de genre du type offre un mécanisme simple de classement qui permettra de normaliser le développement des nouveaux types et d'aider les utilisateurs des types à découvrir les types existants. Le genre d'un type est lui-même un type et de nouveaux genres de type pourront être ajoutés si nécessaire pour étoffer le classement des types.

Pour pouvoir réutiliser le plus possible les types et éviter la création de doubles, chaque type sera décrit en fonction des types existants. Si, par exemple, un nouveau type doit spécifier que sa ressource est sérialisée en XML, il devrait le faire en incluant une référence au type de sérialisation XML existant. Les types peuvent tirer parti d'autres types par extension ou par instanciation.

Chaque type devrait indiquer tous les types dont il tire parti et par quel moyen. La définition des types en fonction d'autres types permettra non seulement de réduire la duplication des types mais permettra aussi aux utilisateurs des types de comprendre plus en détail un type particulier.

Enfin, la description d'un type devrait permettre à divers systèmes d'acquérir dynamiquement la capacité d'agir sur n'importe quelle ressource associée à un type. Elle devrait inclure des attributs qui spécifient l'emplacement des rattachements au service de réseau et/ou des mises en oeuvre particulières de module, leurs plates-formes, et leurs interfaces associées. Ainsi, une bibliothèque générique de traitement de type pourra se rattacher dynamiquement et en toute sécurité à ce service, ou acquérir, charger et exécuter le module de mise en oeuvre correspondant au type et traiter la ressource.

Comme examiné ci-dessus, les types ont un identificateur unique. La résolution de ces identificateurs de type dans un système de résolution prédéfini donnera un enregistrement de type. L'Appendice II présente un exemple de notation BNF d'un enregistrement de type, qui définit sur le plan conceptuel le groupe des entités qui constituent cet enregistrement.

Au moins quatre sections sont nécessaires pour définir sans ambiguïté et de manière cohérente un type, à savoir la description, la provenance, le genre et le traitement.

La section de description est une séquence d'une ou plusieurs descriptions lisibles par l'homme qui définissent, entre autres, l'objet et l'utilisation du type. La langue, éventuellement conforme à la norme [b-IETF RFC 1766], dans laquelle ces descriptions sont faites, doit être représentée de manière univoque par son type et précéder les descriptions.

La section de provenance contient la date de création, la date de la dernière modification, les contributeurs, les alias (ou identificateurs de remplacement) et le statut. Les dates devraient être conformes à la norme [ISO 8601]. Les contributeurs sont les noms des personnes ou des organisations qui ont contribué à la création ou à l'enregistrement du type dans un registre de types désigné. Les alias font référence à l'enregistrement précédent dans d'autres registres de types locaux et sont déclarés ici afin d'établir le contexte du type défini. Le statut indique si le type est utilisé, déconseillé ou obsolète.

La section de genre indique l'essence du type. Définir de nouveaux types en fonction des types existants est un mécanisme puissant qui est essentiel pour la définition de types complexes. Un autre mécanisme concernant les genres consiste à spécifier si les informations de genre constituent un module pour la définition d'autres types ou si elles définissent une manifestation particulière d'un type. Par exemple, un type de codage binaire est un module qui permet de définir d'autres types.

Les informations peuvent être transmises à un service qui sait comment analyser et traiter les informations de type. Les clients invoquent un service pour synthétiser les informations données. La définition du service devrait préciser l'endroit où le service peut être atteint, la manière dont il peut être invoqué, et les résultats qui peuvent être attendus de ce service. Aucune notation particulière n'est recommandée pour la définition d'un tel service.

9 Fédération hiérarchique et fédération fondée sur des relations entre homologues

Dans une approche hiérarchique, on utilise un registre principal pour suivre les informations contenues dans plusieurs registres dans un souci de commodité afin de n'avoir à s'adresser qu'à un seul registre. Il pourrait y avoir plusieurs registres principaux, mais tous devraient être connus et consultés afin que la recherche soit complète.

Dans une approche fondée sur des relations entre homologues (P2P), certains registres choisissent d'établir une relation entre homologues avec certains autres registres. Les raisons d'un tel choix seront variables. Les politiques organisationnelles encadrant la gestion des registres, les politiques de confiance qui interdisent ou soutiennent les points de contact de fédération entre les registres, et la disponibilité/fiabilité des registres participant à un réseau P2P sont quelques-unes des raisons qui pousseront un registre donné à choisir une relation entre homologues avec tel ou tel registre.

Toutefois, les deux systèmes – hiérarchique et P2P – concernent uniquement la topologie de la fédération et ne déterminent pas le niveau d'agrégation choisi pour l'un ou l'autre scénario. Il existe divers niveaux d'agrégation applicables, mais deux exemples spécifiques sont donnés ci-après à titre d'illustration. Le Tableau 1 fait ressortir les avantages (indiqués par le signe +) et les inconvénients (indiqués par le signe –) des deux systèmes de fédération lorsque soit les entités de métadonnées sont complètement agrégées à l'avance soit des requêtes sont propagées en temps réel à travers les registres en réponse à une requête adressée à un système IdM.

Tableau 1

	Fédération hiérarchique	Fédération P2P
Agrégation complète des entités de métadonnées au niveau du registre collecteur	+ Découverte complète à travers les domaines grâce au processus d'agrégation définitive + Pertinence garantie des informations à travers les domaines grâce à la normalisation des entités de métadonnées pendant l'agrégation + Efficacité liée à la recherche et à la récupération localisées – Système rigide. Nécessite des processus de mise au point rigoureux qui sont susceptibles d'interférer avec les politiques organisationnelles – Points de défaillance isolés, soit au niveau du collecteur principal, soit au niveau de collecteurs intermédiaires – Possibilités d'informations obsolètes dues à un rafraîchissement lent de l'agrégation – Eventuels problèmes d'évolutivité au niveau le plus élevé de la hiérarchie	+ Possibilité de groupements souples, non rigides, concernant des domaines d'intérêt particuliers + Pas de points de défaillance isolés, du fait de la possibilité d'activer plusieurs routes pour la fédération + Pertinence garantie des informations à travers les domaines grâce à la normalisation des entités de métadonnées pendant l'agrégation + Efficacité liée à la recherche et à la récupération localisées – Aucune garantie d'exhaustivité de la découverte à travers les domaines, sauf en cas de connexion complète – De nombreux efforts de dédoublement sont nécessaires lorsque plusieurs routes sont possibles pour la fédération des registres – Problèmes de sécurité sauf si tous les points de contact sont fiables

Tableau 1

	Fédération hiérarchique	Fédération P2P
Propagation de la requête à travers les registres	+ Actualité des entités de métadonnées et des informations contenues dans ces entités + Système évolutif – Aucune garantie de découverte complète à travers les domaines en raison de la probabilité que des noeuds de registre ne soient pas disponibles au moment de la propagation de la requête – Le classement des résultats en fonction de leur pertinence est compromis en raison de la durée de fusion des résultats – Système rigide. Nécessite des processus de mise au point rigoureux qui sont susceptibles d'interférer avec les politiques organisationnelles – Points de défaillance isolés, soit au niveau du noeud collecteur principal, soit au niveau des noeuds collecteurs intermédiaires qui propagent les requêtes vers l'aval et distribuent les résultats vers l'amont – Problèmes de qualité de fonctionnement dus aux matériels non robustes utilisés pour le déploiement des registres	+ Actualité des entités de métadonnées et des informations contenues dans ces entités + Système évolutif – Aucune garantie de découverte complète à travers les domaines en raison de la probabilité que des noeuds de registre ne soient pas disponibles au moment de la propagation de la requête, même avec des routes redondantes dans la fédération – Le classement des résultats en fonction de leur pertinence est compromis en raison de la durée de fusion des résultats – De nombreux efforts de dédoublement sont nécessaires lorsque plusieurs routes sont possibles pour la fédération des registres – Problèmes de qualité de fonctionnement dus aux matériels non robustes utilisés pour le déploiement des registres

Les logiciels des registres prennent en charge et autorisent différentes combinaisons à partir de la matrice indiquée dans le Tableau 1. Certaines combinaisons sont plus difficiles à mettre en oeuvre que d'autres. Pour résoudre les problèmes d'évolutivité, on fait appel à une technologie de répertoire qui utilise une représentation abstraite des systèmes de stockage réels, et qui permet d'utiliser simultanément plusieurs systèmes de stockage. La duplication et l'équilibrage de charge des registres sont également assurés, ce qui permet d'atténuer le problème d'évolutivité. La détection des doubles, qui pourrait poser problème dans les relations multipoint-multipoint entre les registres, est grandement facilitée par l'utilisation d'identificateurs persistants.

Pour l'agrégation de données, le registre à l'origine du transfert d'enregistrements de métadonnées distribue ces enregistrements, tandis que pour la requête répartie, il répond aux demandes reçues. Le registre fournissant les enregistrements est désigné comme étant la source, et le destinataire est désigné comme étant le destinataire. Dans une fédération, le destinataire serait le point de contact pour le système de registres fédérés. Le registre source transmet aux destinataires les modifications exécutées avec succès relatives aux métadonnées, par exemple les créations ou les modifications des enregistrements de métadonnées. Ces transactions portent sur les changements de l'état d'une entité – création, modification, définition d'alias, suppression – ainsi que sur les relations d'ajout/de suppression/de remplacement. Chaque enregistrement d'une opération d'enregistrement qui est soumis à un registre est converti en actions d'enregistrement et d'annulation d'enregistrement à

l'intérieur du registre. Chacune de ces actions est une transaction, qui a un identificateur de transaction – un nombre qui en principe est incrémenté à partir de zéro. Cette approche s'applique de la même façon aux scénarios dans lesquels les registres sont organisés en mode P2P et ceux dans lesquels ils sont organisés en mode hiérarchique.

Configurer les différents registres afin de cibler les requêtes sur certains registres et de les propager vers ces registres, en mode hiérarchique ou P2P, permet d'assurer la propagation des requêtes. Les registres d'entités numériques, en plus de prendre en charge des interfaces propres à la communauté, prennent également en charge le protocole d'interface d'entité numérique comme interface par défaut. Les requêtes peuvent être propagées vers d'autres registres sur la base de l'utilisation de ce protocole.

Appendice I

Scénarios d'utilisation

(Le présent appendice ne fait pas partie intégrante de la Recommandation.)

Pour illustrer l'utilisation d'un système de registres fédérés, quelques scénarios seraient utiles. Plusieurs scénarios sont décrits ci-dessous conjointement avec les éventuels attributs qu'il faudrait enregistrer pour permettre au(x) processus de découverte de fonctionner de manière acceptable.

- Un client – soit un homme soit une machine – aimerait obtenir un service auprès d'un fournisseur de services dans l'Internet. Le fournisseur de services a besoin d'une preuve d'identité et accepte les justificatifs d'identité provenant de l'un quelconque des fournisseurs d'identité (IdP) parmi un ensemble donné. Le client (généralement logiciel) doit pouvoir déterminer quels sont les fournisseurs IdP acceptables, établir s'il possède déjà les justificatifs pertinents provenant d'un ou de plusieurs des fournisseurs IdP acceptés et, dans la négative, déterminer comment les obtenir.

Le fournisseur de services doit annoncer quels fournisseurs IdP sont acceptés pour le ou les services concernés, soit directement, de manière normalisée, soit par référence à un registre, également de manière normalisée. Dans l'un ou l'autre cas, les fournisseurs IdP doivent être identifiés de manière univoque et précise. Le client peut alors utiliser la participation actuelle à une organisation IdP ou avoir connaissance de la manière de répondre aux exigences IdP, et présenter les justificatifs pertinents au fournisseur de services. Dans le cas où une annonce directe est fournie par le fournisseur de services, où le ou les fournisseurs IdP concernés sont identifiés de manière univoque et précise et où le client peut fournir les justificatifs propres à un fournisseur IdP, aucun registre ne serait nécessaire. Mais dans tous les autres cas, il faut pouvoir découvrir un certain niveau d'informations concernant les fournisseurs IdP acceptés. Avec un identificateur unique et persistant, la découverte peut se faire par la consultation directe d'un registre de renseignements relatifs aux fournisseurs IdP. Pour répondre aux exigences de ce scénario d'utilisation, il faudrait que les métadonnées décrivant un fournisseur IdP donné fournissent aux clients les informations dont ils ont besoin pour déterminer si le choix d'un fournisseur IdP donné est raisonnable pour l'utilisation du service donné. Les attributs pertinents comporteraient l'identificateur persistant unique du fournisseur IdP proprement dit, pour d'éventuelles références croisées, par exemple pour examiner les sites, les cadres de confiance auxquels le fournisseur IdP participe, les politiques et procédures, les dispositions juridiques, les logiciels nécessaires, les éventuels barèmes de redevances, etc. Certaines de ces informations se présenteraient sous la forme d'un deuxième niveau d'accès, par exemple un grand nombre des détails techniques et politiques relatifs à un fournisseur IdP donné seraient définis par la participation dudit fournisseur à un ou plusieurs cadres de confiance définis.

- Les détails qui permettraient à un client de découvrir si un fournisseur IdP donné convient permettraient également à un fournisseur de services de découvrir un ou plusieurs fournisseurs IdP dont les justificatifs seraient acceptables et qui pourraient donc être ajoutés à la liste des fournisseurs IdP acceptables. Les métadonnées relatives aux fournisseurs IdP couvriraient ces deux cas d'utilisation.
- Dans le scénario inverse du premier scénario, un client accède à un service et présente un justificatif d'identité que le service n'a jamais rencontré avant. Dans l'hypothèse où le justificatif présenté est constitué d'un identificateur du fournisseur IdP ou commence par un tel identificateur, le service doit décider d'accepter le justificatif, ou d'examiner plus avant la possibilité d'accepter un tel justificatif, ou simplement de le rejeter sans examen complémentaire. Dans ce scénario, le registre aurait à découvrir des informations générales concernant le type d'identificateur et le fournisseur IdP qu'il représente. D'autres

consultations du registre pourraient alors être nécessaires concernant les technologies spécifiques utilisées par le fournisseur IdP, y compris les cadres de confiance pertinents.

- Les diverses entités participant à la gestion d'identité seraient généralement membres d'un ou de plusieurs cadres de confiance ou d'un autre système IdM, soit explicitement soit implicitement. La spécification des attributs de chaque système IdM serait nécessaire pour la création d'un schéma de métadonnées décrivant ce cadre de confiance. Plusieurs questions importantes se posent alors. Est-ce qu'un système IdM est décrit par l'organisation qui le fournit, un ensemble de normes qui le met en oeuvre, un moyen de mesurer la conformité aux normes, etc.? Indépendamment de la réponse à ces questions, il est clair qu'il serait utile que certains fournisseurs IdP voire certaines parties utilisatrices soient connectés à des descriptions de plus haut niveau, par exemple des organisations InCommon, Kantara, Safe-BioPharma et OIX qu'il serait possible de découvrir dans un registre ou dans une fédération de registres.

La Figure I.1 illustre la manière dont un système de registres fédérés (le "système") pourrait être utilisé avec un scénario d'utilisation particulier.

Etape 1: Dans cet exemple, l'utilisateur final demande un service auprès d'une partie utilisatrice.

Etape 2: La partie utilisatrice retourne l'identité d'un ou de plusieurs cadres de confiance auxquels elle fait confiance, dans ce cas un seul cadre (TF1).

Etape 3: L'utilisateur final s'adresse au système avec l'identificateur du cadre TF1.

Etape 4: Le système retourne l'enregistrement pertinent concernant le cadre TF1. Les informations relatives au cadre TF1 comportent les attributs minimaux nécessaires pour la confiance dans le contexte de ce cadre.

Etape 5: L'utilisateur final évalue ces exigences minimales pour déterminer s'il sera possible d'obtenir la confiance de la partie utilisatrice. Nous supposons ici que l'évaluation de l'utilisateur final est positive et montre que l'utilisateur final dispose des attributs minimaux, par exemple un permis de conduire.

Etape 6: L'utilisateur final s'adresse alors de nouveau au système pour lui demander quels sont les fournisseurs IdP du cadre TF1 qui prennent en charge le ou les protocoles que cet utilisateur final prend en charge, par exemple HTTP et courrier électronique, que nous représentons ici simplement sous la forme du protocole X.

Etape 7: Le système trouve les fournisseurs d'identité (IdP) du cadre TF1 qui prennent en charge le protocole X.

Etape 8: Le système retourne à l'utilisateur final l'ensemble des fournisseurs IdP qui correspondent aux exigences à la fois de la partie utilisatrice et de l'utilisateur final.

Etape 9: L'utilisateur final évalue l'ensemble des fournisseurs IdP retourné par le système et fait une sélection (IdP1).

Etape 10: L'utilisateur final, qui dispose des attributs exigés par le fournisseur IdP1 et qui prend en charge un protocole pris en charge par le fournisseur IdP1, lance une interaction demande/réponse avec le fournisseur IdP1.

Etape 11: L'interaction demande/réponse aboutit: le fournisseur IdP1 fournit un justificatif d'authentification à la partie utilisatrice.

Etape 12: La partie utilisatrice, qui fait maintenant confiance à l'utilisateur final, fournit le service demandé.

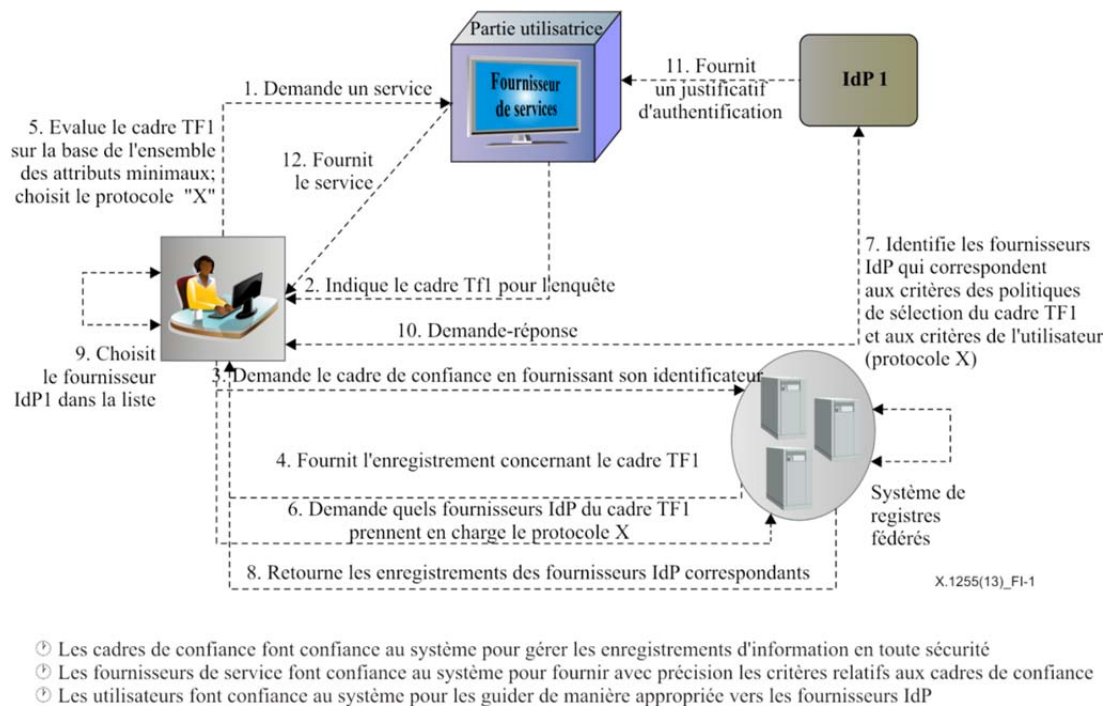


Figure I.1 – Authentification reposant sur des cadres de confiance

La Figure I.2 présente les schémas de haut niveau des enregistrements contenus dans le système de registres fédérés qui rendraient possible la transaction décrite sur la Figure I.1 ainsi que les autres scénarios d'utilisation décrits ci-avant. Ces enregistrements seraient conservés par le système sous forme d'entités numériques, chacune avec un identificateur persistant. Chacune devrait en outre être intégrée dans des schémas spécifiques en vue de la réalisation de prototypes.

Chaque cadre de confiance aurait un identificateur, une description générale du cadre, l'ensemble des attributs utilisés pour l'authentification, et des pointeurs vers une ou plusieurs politiques de sélection de fournisseur IdP, qui prennent la forme d'entités numériques distinctes conservées dans le système. Celles-ci forment un niveau supplémentaire d'accès tel que tous les fournisseurs IdP entrant dans un même cadre de confiance peuvent être regroupés par critères et non sous la forme d'une énumération. Chaque entité de politique de sélection de fournisseur IdP aurait un identificateur, une description générale, une liste de technologies acceptables (par exemple les protocoles pris en charge), une liste d'organismes d'accréditation organisationnels (par exemple une organisation gouvernementale) et des éventuelles contraintes opérationnelles particulières. La relation entre les cadres de confiance et les politiques de sélection des fournisseurs IdP serait multipoint-multipoint dans les deux sens, autrement dit un cadre de confiance donné pourrait prendre en charge plusieurs politiques de sélection de fournisseur IdP et une même politique de sélection de fournisseur IdP pourrait être utilisée par plusieurs cadres de confiance.

Les deux autres types d'entité qu'il est proposé de conserver dans le système sont les fournisseurs IdP et les parties utilisatrices. Chaque fournisseur IdP aurait un identificateur persistant, une description générale, les attributs d'utilisateur nécessaires, une politique d'évaluation pour ces attributs, les protocoles et accréditations spécifiques acceptés, et des points d'extrémité particuliers, par exemple l'emplacement du fournisseur IdP sous la forme des protocoles acceptés. Chaque partie utilisatrice aurait un identificateur persistant, une description générale, l'ensemble des cadres de confiance auxquels elle fait confiance, et les éventuelles restrictions opérationnelles particulières.

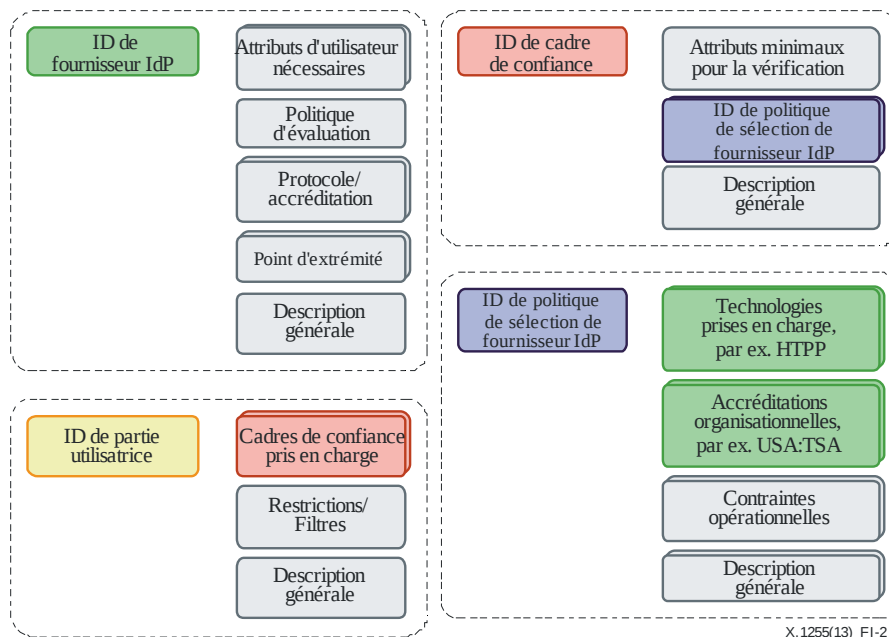


Figure I.2 – Schémas de haut niveau

Appendice II

Notation BNF d'un enregistrement de type

(Le présent appendice ne fait pas partie intégrante de la Recommandation.)

Notation BNF d'un enregistrement de type:

```
<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
```

Notes:

1. La résolution, dans le système de résolution global, de <type identifier> donne un enregistrement de <type>.
2. Tous les délimiteurs, à savoir <section delimiter>, <repetition delimiter> et <list delimiter>, sont propres à la mise en oeuvre et ne sont donc pas définis ici.
3. <network service type> n'est pas non plus défini ici, mais devrait couvrir les services de réseau courants jugés appropriés par l'organisme de mise en oeuvre.
4. <network service binding> n'est pas non plus défini ici, mais devrait être fondé sur le type de service de réseau. Il convient de faire figurer ici les définitions effectives conformes à chacun des types de service.
5. <program network location> n'est pas non plus défini ici, mais devrait identifier le protocole de réseau que le client devrait utiliser pour télécharger le programme depuis le réseau.
6. <compatible platform> peut faire l'objet d'une extension ou d'une spécification plus détaillée que la définition donnée ici.

Bibliographie

- [b-UIT-T Y.2720] Recommandation UIT-T Y.2720 (2009), *Cadre de gestion d'identité dans les NGN*.
- [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>>

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes généraux de tarification
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Terminaux et méthodes d'évaluation subjectives et objectives
Série Q	Commutation et signalisation
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	Réseaux de données, communication entre systèmes ouverts et sécurité
Série Y	Infrastructure mondiale de l'information, protocole Internet et réseaux de prochaine génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication