Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1250

(09/2009)

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

Sécurité du cyberespace – Gestion des identités

Capacités de base pour l'amélioration de l'interopérabilité globale dans la gestion d'identité

Recommandation UIT-T X.1250

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	
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.

Recommandation UIT-T X.1250

Capacités de base pour l'amélioration de l'interopérabilité globale dans la gestion d'identité

Résumé

La Recommandation UIT-T X.1250 décrit les capacités de base pour l'interopérabilité globale dans la gestion d'identité (IdM) (c'est-à-dire les capacités permettant d'améliorer l'échange et la confiance concernant les identificateurs utilisés par les entités dans les réseaux et services de télécommunication/informatiques). Les définitions et les besoins concernant la gestion d'identité dépendent fortement du contexte et font souvent l'objet de politiques et de pratiques très différentes d'un pays à l'autre. Les capacités comprennent la protection et la gestion des informations d'identification personnelle (PII).

Historique

Edition	Recommandation	Approbation	Commission d'études
1.0	ITU-T X.1250	2009-09-25	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 [avait/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/.

TABLE DES MATIÈRES

Recommandation UIT-T X.1250

Capacités de base pour l'amélioration de l'interopérabilité globale dans la gestion d'identité

1 Domaine d'application

La présente Recommandation décrit les capacités de base qui sont destinées à améliorer l'interopérabilité globale dans la gestion d'identité (IdM) dans les réseaux et services publics de télécommunication. Ces capacités de base sont regroupées en domaines fonctionnels, comme suit:

- Modèles communs, structurés, de gestion d'identité.
- Fourniture d'attributs (identificateurs compris), de justificatifs d'identité et de capacités.
- Découverte des ressources, capacités et fédérations des fournisseurs de service d'identité.
- Interopérabilité entre plates-formes de gestion, fournisseurs de service d'identité et fédérations de fournisseurs, y compris les fournisseurs relais de service d'identité.
- Mesures de sécurité et autres mesures destinées à réduire les menaces et risques sur les identités, en particulier protection des ressources d'identité, des informations d'identification personnelle et de la confidentialité.
- Audit et conformité des informations d'identification personnelle, en particulier mise en œuvre des politiques et protection.
- Performance, fiabilité et disponibilité des capacités de gestion d'identité.

Les réseaux et services de télécommunication/informatiques d'aujourd'hui sont très divers, hautement répartis, hautement interconnectés, mais pour l'essentiel autonomes pour ce qui est de la gestion d'identité (IdM). Si ces réseaux et leurs capacités évoluent, leur taille et leur complexité peuvent empêcher l'interopérabilité des capacités IdM. C'est pourquoi, les capacités IdM évoquées dans la présente Recommandation sont pour l'essentiel tributaires des capacités et des modèles généraux des réseaux existants, y compris des pratiques qui sont effectivement "les meilleures". Toutefois, pour parvenir à l'interopérabilité globale dans la gestion d'identité, la présente Recommandation décrit un trajet d'évolution et indique comment tirer parti des capacités existantes, le cas échéant. Elle définit en outre une capacité de relais d'identité qui peut être utilisée dans de nombreux systèmes IdM ou architectures auxiliaires pour intégrer les capacités IdM existantes.

L'implémentation de capacités IdM dans certains pays est assujettie à des impératifs propres à la juridiction nationale.

NOTE – Le terme "identité" employé dans la présente Recommandation en relation avec la gestion d'identité n'est pas utilisé dans son acception absolue. En particulier, il ne renvoie pas à la validation positive d'une personne.

2 Références

Néant.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 déclarant [b-UIT-T Y.2720] et [b-UIT-T X.811]: entité qui est ou représente une entité principale à des fins d'authentification. Un déclarant comporte les fonctions nécessaires pour engager des échanges pour authentification au nom d'une entité principale.

3.1.2 informations d'identification personnelle (PII) [b-UIT-T Y.2720]: informations relatives à une personne physique, permettant de l'identifier (y compris les informations permettant d'identifier une personne lorsqu'elles sont combinées avec d'autres informations, même si elles n'identifient pas clairement la personne).

3.1.3 partie utilisatrice (*relying party*) [b-UIT-T Y.2720]: entité qui est tributaire d'une représentation ou d'une déclaration d'identité soumise par une entité requérante/assertante dans un contexte de demande donné.

3.2 Termes définis dans la présente Recommandation

Les termes suivants sont définis dans la présente Recommandation:

3.2.1 agent: entité qui agit au nom d'une autre entité.

3.2.2 anonymat: propriété d'une entité qui ne peut pas être identifiée parmi un ensemble d'entités.

NOTE – L'anonymat permet d'empêcher le traçage d'entités ou de leur comportement (emplacement de l'utilisateur, fréquence d'utilisation d'un service, etc.).

3.2.3 attribut: informations liées à une entité qui en spécifient une caractéristique.

3.2.4 authentification: voir authentification d'entité.

3.2.5 garantie d'authentification: confiance obtenue dans le processus d'authentification, dans le fait que le partenaire de communication est l'entité qu'il déclare être ou qu'il est censé être.

3.2.6 rattachement: association, rapport ou lien explicite établi.

3.2.7 déclaration: assertion faite par un déclarant relative à la valeur ou aux valeurs d'un ou de plusieurs attributs d'identité d'un sujet numérique, généralement une assertion qui est contestée ou mise en doute.

3.2.8 entité: tout élément qui a une existence séparée et distincte et peut être identifié dans un contexte.

NOTE – Une entité peut être une personne physique, un animal, une personne morale, une organisation, une chose active ou passive, un dispositif, une application logicielle, un service, etc., ou un groupe de ces éléments. Dans le contexte des télécommunications, il peut s'agir de points d'accès, d'abonnés, d'utilisateurs, d'éléments de réseau, de réseaux, d'applications logicielles, de services et de dispositifs, d'interfaces, etc.

3.2.9 authentification d'entité: processus permettant d'obtenir une confiance suffisante dans le lien entre l'entité et l'identité présentée.

3.2.10 fédération: association d'utilisateurs, de fournisseurs de services et de fournisseurs d'identité.

3.2.11 identificateur: un ou plusieurs attributs utilisés pour identifier une entité dans un contexte.

3.2.12 identité: représentation d'une entité sous la forme d'un ou de plusieurs éléments d'information qui sont suffisants pour pouvoir distinguer les entités dans un contexte. Aux fins de l'IdM, le terme identité désigne l'identité contextuelle (sous-ensemble d'attributs), c'est-à-dire que la diversité des attributs est limitée par un cadre avec des frontières définies (le contexte) dans lequel l'entité existe et interagit.

NOTE – Chaque entité est représentée par une identité holistique, qui comprend tous les éléments d'information possibles caractérisant cette entité (les attributs). Toutefois, l'identité holistique est théorique et échappe à toute description et utilisation pratique, car le nombre de tous les attributs possibles est indéfini.

3.2.13 fournisseur relais de service d'identité: fournisseur de service d'identité faisant office d'intermédiaire entre d'autres fournisseurs de service d'identité.

3.2.14 gestion d'identité: ensemble de fonctions et de capacités (par exemple, l'administration, la gestion et la tenue à jour, la découverte, les échanges de communication, la corrélation et les liens, l'application des politiques, l'authentification et les assertions) utilisées pour:

- garantir les informations d'identité (par exemple, les identificateurs, les justificatifs d'identité, les attributs);
- garantir l'identité d'une entité (par exemple les utilisateurs/abonnés, les groupes, les dispositifs d'utilisateur, les organisations, les fournisseurs de réseau et de service, les éléments et objets de réseau et les objets virtuels); et
- permettre des applications commerciales et liées à la sécurité.

3.2.15 fournisseur de service d'identité: entité qui vérifie, maintient, gère et peut créer et attribuer des informations d'identité pour d'autres entités.

3.2.16 profil d'identité: expression structurée d'attributs d'une entité (par exemple le comportement d'une entité) qui pourrait être utilisée dans certains processus d'identification.

3.2.17 manifestation: représentation observée ou découverte (c'est-à-dire non auto assertée) d'une entité. (Comparer avec assertion.)

3.2.18 pseudonyme: identificateur dont le lien avec une entité est inconnu ou n'est connu que dans une certaine mesure, dans le contexte dans lequel il est utilisé.

3.2.19 entité requérante: entité soumettant une représentation ou une déclaration d'identité à une partie utilisatrice dans un contexte de demande donné.

3.2.20 objet terminal: objet (comme une carte SIM) qui peut avoir une relation à un dispositif terminal de réseau (comme par exemple un téléphone mobile).

3.2.21 confiance: conviction que des informations sont fiables et vraies, ou qu'une entité est compétente pour agir de façon appropriée dans un contexte spécifié.

3.2.22 utilisateur: toute entité qui utilise une ressource, par exemple un système, un équipement, un terminal, un processus, une application ou un réseau d'entreprise.

3.2.23 centré sur l'utilisateur: système IdM qui peut conférer à l'utilisateur (IdM) la capacité de contrôler et d'appliquer diverses politiques de respect de la vie privée et de sécurité régissant l'échange d'informations d'identité, en particulier des informations PII, entre entités.

4 Abréviations

La présente Recommandation utilise les abréviations ci-dessous:

DHCP	protocole de configuration de serveur dynamique (*dynamic host configuration protocol*)
ID	identificateur (*identifier*)
IdM	gestion d'identité (*identity management*)
IdSP	fournisseur de services d'identité (*identity service provider*)
IT	technologies de l'information (*information technology*)
NGN	réseau(x) de prochaine génération (*next generation network(s)*)
PII	informations d'identification personnelle (*personally identifiable information*)
RFID	identification par radiofréquence (*radio frequency identification*)
SIM	module d'identification de l'abonné (*subscriber identity module*)
URL	identificateur uniforme de ressources (*uniform resource locator*)

5 Conventions

Néant.

6 Généralités

La croissance et l'évolution des capacités de communication ont favorisé la prolifération de nombreux cyberservices aux consommateurs, entreprises et pouvoirs publics. Les communications ne sont plus seulement une ressource pour naviguer à la recherche d'informations, les technologies de communication basées sur le protocole Internet, telles que les NGN, deviennent un facilitateur indispensable pour effectuer les cybertransactions au quotidien.

Les capacités décrites dans la présente Recommandation visent à soutenir le développement et le déploiement de capacités de gestion d'identité structurées et interopérables à l'intérieur d'un cadre commun pour tous les systèmes de réseaux et services de télécommunication/informatiques, sous réserve de l'observation des politiques régionales et nationales concernant les informations d'identification personnelle et la confidentialité.

Les capacités décrites dans la présente Recommandation sont les suivantes:

a) **Exemples de modèles communs, structurés, de gestion d'identité**

La gestion d'identité suppose normalement un échange entre entités d'une ou de plusieurs identités au moyen d'un réseau ou d'un service de télécommunication/informatique. Pour atteindre un niveau de garantie d'authentification souhaité, les parties peuvent décider ou être tenues de communiquer d'autres informations entre elles ou à une tierce partie. L'échange de communication initial peut comprendre l'expression d'un processus d'authentification préféré ou une délégation. L'une des parties à l'échange ou les deux peuvent aussi choisir de rester anonymes ou d'utiliser des pseudonymes. Ces types d'interaction peuvent être représentés par des modèles communs (dont les capacités sont exposées ci-après). Ces modèles permettent la fourniture de capacités d'identité entre de multiples parties, si souhaité ou requis; ils sont par ailleurs importants pour l'implémentation des capacités IdM interopérables décrites et prises en charge sur des réseaux tels que des NGN.

b) **Fourniture et protection de capacités d'identité (justificatifs d'identité, identificateurs, attributs et profils) avec des niveaux de garantie connus**

Ces catégories d'informations d'identité et leur fourniture, tenue à jour, utilisation, révocation et/ou protection suivant des niveaux de garantie souhaités sont communes aux activités de gestion d'identité.

c) **Découverte des ressources, capacités et fédérations des fournisseurs de service d'identité**

Dans le monde très dynamique et divers des capacités et applications de réseau, un important problème de gestion d'identité est la découverte des sources d'identité et des services qu'elles fournissent. Les capacités de découverte sont souvent nécessaires pour atteindre les niveaux de garantie souhaités.

d) **Interopérabilité entre plates-formes d'identité, fournisseurs et fédérations d'identité, y compris les fournisseurs relais de service d'identité**

Dans une infrastructure de réseau public et de capacités hautement répartie, et comptant un nombre élevé de fournisseurs et d'utilisateurs nomades, la gestion d'identité peut impliquer un nombre élevé de questions et de réponses entre les diverses parties et les fédérations au sein desquelles elles peuvent agir. L'interopérabilité globale entre parties fournissant des capacités de gestion d'identité est essentielle, et suppose le recours à des protocoles communs pour élaborer des demandes de capacités d'identité.

e) **Mesures de sécurité et autres mesures destinées à réduire les menaces et risques sur les identités, en particulier protection et gestion des ressources d'identité et des informations d'identification personnelle**

Etant donné que les informations et les ressources d'identité sont des éléments de grande valeur, sensibles et vitaux des réseaux – surtout lorsque ces informations et ressources sont considérées comme faisant partie d'une infrastructure nationale critique – et qu'elles ont une incidence sur le respect de la vie privée des personnes, il faut prévoir une protection de leur sécurité basée sur une analyse des risques dans l'environnement IdM.

f) **Audit et conformité des informations d'identification personnelle, en particulier mise en œuvre des politiques et protection**

La gestion d'identité fait normalement l'objet de diverses législations, réglementations et spécifications des secteurs public et privé qui nécessitent un certain niveau de capacités d'audit et de conformité. La gamme de ces capacités est large, notamment: audit pour la conformité aux réglementations, mesures destinées à la protection des informations d'identification personnelle, communiqués à l'intention des usagers et maintien de la précision et de la traçabilité appropriées des horodates.

g) **Utilisabilité et variabilité: performance, fiabilité, disponibilité, internationalisation et reprise après sinistre**

Les capacités de gestion d'identité sont utilisables et variables pour s'adapter à la constante évolution des systèmes d'identité qui sont très répartis. Etant donné que les informations et ressources d'identité constituent la base suivant laquelle les entités s'authentifient mutuellement, c'est-à-dire s'acceptent mutuellement comme partenaires de communication, ce sont souvent des éléments de l'infrastructure critique, pour lesquels des niveaux spécifiques de performance, de fiabilité, de disponibilité et de capacités doivent éventuellement être respectés.

7 Capacités pour l'interopérabilité globale dans la gestion d'identité

Le présent paragraphe fournit des exemples de modèles possibles de transactions en gestion d'identité et présente un ensemble interopérable de capacités de gestion d'identité (IdM) et les éléments d'identité de base. Le présent paragraphe traite aussi de la découverte des capacités d'identité, de l'interopérabilité et des relais, de la sécurité IdM, de la protection, de la gestion et de l'utilisation des informations d'identification personnelle (PII) ainsi que de l'audit et de la conformité. Sont également couverts l'internationalisation et la performance, la fiabilité et la disponibilité.

7.1 Exemples de modèles possibles de transactions en gestion d'identité

L'une des principales transactions en gestion d'identité correspond au processus de base question/réponse commun à la plupart des échanges d'information structurés illustré sur la Figure 1. La forme la plus basique d'échange de messages fait intervenir deux parties utilisant un protocole et un modèle informationnel convenus.

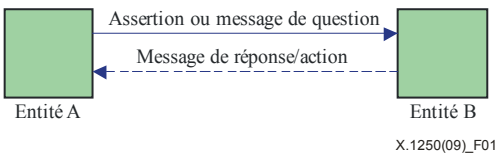

Figure 1 – Processus de base de question/réponse pour l'échange d'informations

Les parties participant à ce processus peuvent être n'importe quel type d'entité. Une entité peut être une personne physique, un animal, une personne morale, une organisation, une chose active ou passive, un dispositif, une application logicielle, un service, etc., ou un groupe de ces éléments. Dans le contexte des télécommunications, il peut s'agir de points d'accès, d'abonnés, d'utilisateurs, d'éléments de réseau, de réseaux, d'applications logicielles, de services et de dispositifs, d'interfaces, etc. Il peut s'agir de n'importe quel objet physique ou virtuel, tel qu'un équipement de réseau, un logiciel, des dispositifs terminaux, des capteurs, des objets physiques activement étiquetés (par exemple, utilisant des RFID ou des codes optiques) ou des objets passivement étiquetés. Des dispositifs réseaux peuvent, par exemple, être traités comme des entités sous réserve de capacités IdM spéciales pour le compte d'utilisateurs finals, de fournisseurs et d'autorités publiques. Dans le contexte de la gestion des droits numériques, l'entité peut être un élément protégé par les droits de la propriété intellectuelle ou les droits d'auteur, tel qu'un contenu multimédia ou de TVIP. Un type d'entité spéciale est le groupe. L'identité du groupe correspond à l'intersection des identités (attributs communs) de ses membres.

La plupart des cas d'utilisation de la gestion d'identité font appel à des modèles complexes. Par exemple, lorsque la partie utilisatrice qui reçoit à l'origine la déclaration n'est pas le fournisseur de service d'identité (voir la Figure 2a ou 2b), la fonction de fournisseur de service d'identité est séparée et distincte de celle de la partie utilisatrice; la partie utilisatrice évalue les réponses données par le ou les fournisseurs de service d'identité et décide s'il existe un degré suffisant de garantie d'authentification d'entité. La principale fonction d'un fournisseur de service d'identité est de gérer la création, la mise à jour, la vérification, la suspension et la suppression d'informations d'identité.

Il existe de nombreux modèles possibles d'échange d'informations d'identité. Un modèle couramment utilisé est le modèle tripartite avec question/réponse illustré sur la Figure 2a ci-dessous. Certains des nouveaux protocoles IdM "ouverts" sont fondés sur ce modèle.

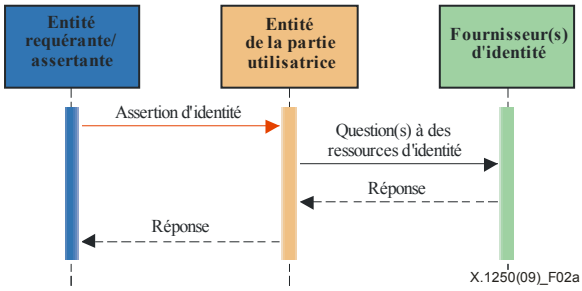

Figure 2a – Exemple d'un modèle tripartite de gestion d'identité

Un autre modèle de gestion d'identité, qui donne à l'entité requérante plus de pouvoir dans les relations d'identité, est illustré sur la Figure 2b.

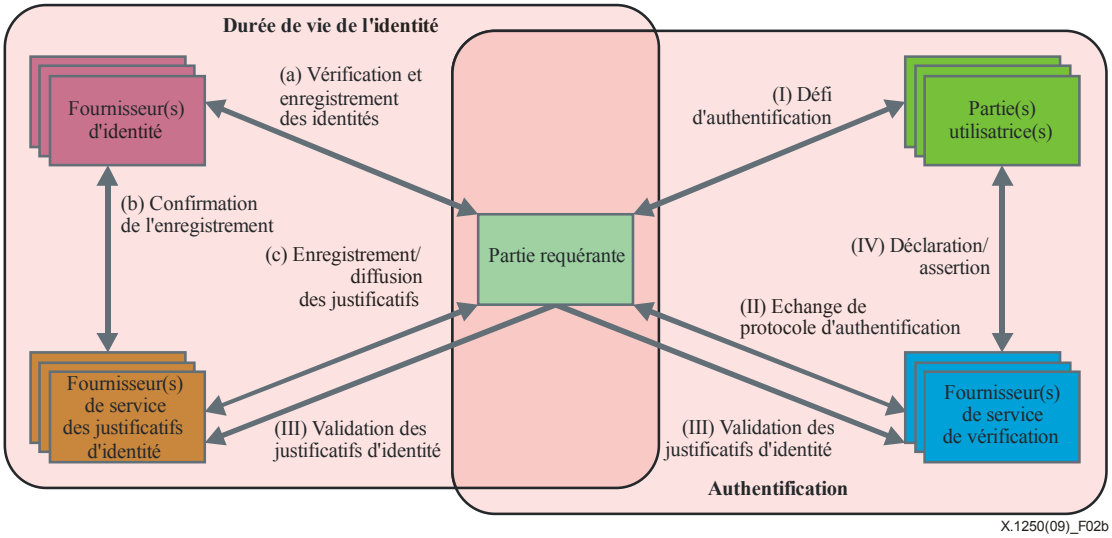

Figure 2b – Exemple d'un modèle de gestion d'identité à cinq parties centré sur l'utilisateur

Les modèles "centrés sur l'utilisateur" (c'est-à-dire dans lesquels les parties requérantes doivent pouvoir exercer un contrôle total sur l'utilisation de leurs identités) font l'objet d'une importante attention et peuvent en outre être rendus obligatoires dans des juridictions nationales et régionales. La Figure 2b montre un exemple où les rôles spécialisés et capacités de gestion d'identité sont fournis par différents fournisseurs de service. Toutes les questions /réponses passent par la partie requérante. Dans ces types de modèle, les entités sont définies de la façon suivante:

- **Fournisseur d'identité**: entité qui maintient, gère et peut créer des informations d'identités fiables concernant d'autres entités (par exemple, utilisateurs finals, organisations et dispositifs) et offre des services fondés sur l'identité. Cette entité, chargée de l'attribution et de la diffusion d'attributs (par exemple, pour un abonné à un fournisseur de justificatifs d'identité), lesquels constituent l'identité dans un contexte spécifique – on parle aussi d'inscription – est responsable de la gestion de l'identité, pendant toute sa durée de vie, ce qui comprend les activités de vérification, enregistrement et maintenance de l'identité, mais également sa révocation.
- **Fournisseur de service des justificatifs d'identité**: entité fournissant les capacités relatives à la diffusion des justificatifs d'identité et des jetons (par exemple, justificatifs liant des jetons à des identificateurs et attributs vérifiables).
- **Fournisseur de service de vérification**: entité fournissant des capacités d'évaluation des informations d'identité (par exemple, déclarations et justificatifs d'identité) et de classification de leur validité.
- **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 dans un contexte de demande donné.

En général, les activités de question/réponse peuvent être regroupées dans deux grandes catégories:

a) Durée de vie de l'identité

- **Enregistrement de l'identité et vérification (c'est-à-dire inscription)**: ce flux d'informations représente l'établissement d'une entité dans un contexte spécifique, c'est-à-dire les processus d'enregistrement et de vérification associés à l'attribution d'attributs constituant l'identité de l'entité en question dans ce contexte. Par exemple, ces processus peuvent inclure la vérification et la documentation des preuves qu'une personne réelle est associée à un nom d'abonné ou à un pseudonyme.

- **Confirmation de l'enregistrement**: ce flux d'informations représente les interactions entre un fournisseur de service d'identités et un fournisseur de service des justificatifs d'identité destinées à confirmer les identités enregistrées.
- **Enregistrement/diffusion des justificatifs d'identité**: ce flux d'informations représente l'échange d'informations entre le fournisseur de service des justificatifs d'identité et la partie requérante destiné à l'enregistrement d'une identité et à l'obtention de justificatifs liant des jetons à un nom ou à un pseudonyme et autres attributs associés à l'entité.

b) Authentification et assertion

- **Assertion**: ce flux d'informations représente un échange d'informations entre la partie utilisatrice et le fournisseur de service de vérification permettant d'obtenir une classification de la déclaration.
- **Défi d'authentification**: ce flux d'informations correspond à la situation où la partie utilisatrice présente un défi ou une invite d'authentification à la partie requérante. Par exemple, la partie utilisatrice peut renvoyer la partie requérante à un fournisseur de service de vérification spécifique, ou bien la partie requérante peut choisir un fournisseur de service de vérification spécifique.
- **Echange de protocole d'authentification**: ce flux d'informations représente un échange de messages de protocole en vue de l'authentification de la partie requérante par le fournisseur de service de vérification.
- **Validation des justificatifs d'identité**: ce flux d'informations représente un échange d'informations entre le fournisseur de service de vérification et le fournisseur de service des justificatifs d'identité pour valider, éventuellement, un justificatif d'identité.

Les modèles contenus dans la présente Recommandation ne sont pas exhaustifs. Conçus pour être flexibles, ils peuvent inclure des contextes où interviennent de nombreux fournisseurs de service d'identité, mais aussi où les parties requérantes ou utilisatrices sont aussi des fournisseurs de service d'identité.

c) Variantes concernant les assertions

- **Délégation**: une assertion peut contenir également une expression de validation préférée, ou une "délégation". Une expression de validation préférée informe la partie utilisatrice sur le service du fournisseur de service d'identité à contacter, pour autant que la partie utilisatrice puisse établir une chaîne de confiance à destination du fournisseur de service d'identité préféré. Une délégation permet de faire face à une situation où une entité agit pour le compte d'une autre entité. Les délégations ne sont pas rares; exemple: un parent peut agir au nom d'un enfant, un adulte au nom d'un autre adulte frappé d'incapacité, un employé au nom d'une entreprise, un mandataire au nom d'un client, ou l'Etat au nom d'un citoyen ou inversement.
- Une délégation peut servir à octroyer à une entité délégataire une partie des capacités ou des droits autorisés qui s'attachent à l'entité à laquelle l'identité est associée. Dans ces circonstances, lorsqu'elle consulte le fournisseur de service d'identité, la partie utilisatrice peut inclure des demandes additionnelles pour vérifier que le délégant a bien enregistré le délégataire en tant qu'agent autorisé. Cette demande s'ajoute à l'authentification de l'agent. Dans ces modèles peuvent exister entre de nombreuses entités des relations d'identité partagée ou déléguée; l'étendue de la chaîne de délégation (c'est-à-dire la délégation d'une délégation) dépend de la technologie disponible ainsi que des lois, des règlements et des politiques commerciales, juridiques et afférentes aux fédérations.

- **Anonymat et pseudonymat**: une entité peut aussi envoyer une assertion d'identité anonyme ou pseudonyme. Dans pareil cas, le niveau de garantie de l'identité dépend de facteurs extérieurs dont devrait tenir compte la partie utilisatrice, car aucun niveau de garantie de l'entité ne peut être obtenu. Anonymat et pseudonymat peuvent être utilisés lorsque le type d'activité en cause n'exige pas de vérification effective (par exemple, lorsque l'activité est si banale que toute opération de gestion d'identité devient inutile). Par ailleurs, certaines lois, réglementations et politiques de protection des données peuvent exiger l'utilisation de l'anonymat ou du pseudonymat.

7.2 Ensemble interopérable de capacités de gestion d'identité (IdM)

La gestion d'identité s'est imposée comme une capacité commune pour toutes les couches des modèles de réseau de base, par exemple dans les modèles applicables aux NGN [b-UIT-T Y.2012], [b-UIT-T Y.2720]. Les capacités IdM sont utilisées dans la partie application, pour la commande des services de réseau, dans le cadre de la fonction de transport sous-jacente et dans les capacités de gestion qui sont utilisées pour administrer ces couches.

Il existe fréquemment un manque de coordination parmi ces couches pour la gestion d'identité. Dans la mesure où les politiques régionales ou nationales le permettent, des capacités IdM interopérables devraient être prises en charge dans chacune des strates de réseau.

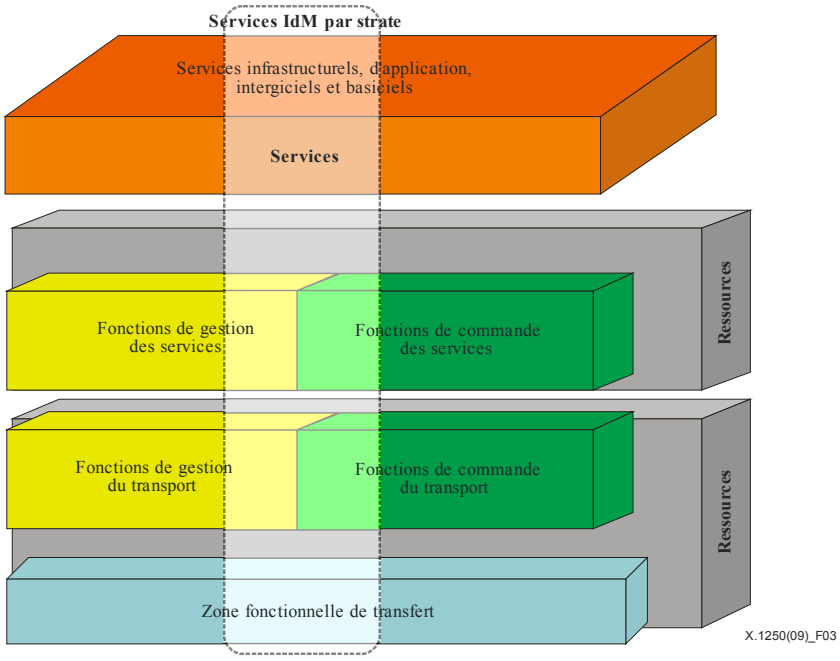

Figure 3 – Interopérabilité de la gestion d'identité au travers des strates de réseau

D'après la Figure 3, des capacités IdM peuvent exister dans la totalité des couches verticales de l'architecture de réseau et il faut à la fois une synchronisation et une harmonisation.

7.3 Quatre éléments d'identité de base

Pour faciliter l'établissement de capacités IdM interopérables, la présente Recommandation classe les informations d'identité dans les quatre catégories de base suivantes:

- Capacités d'identificateur.
- Capacités de justificatif d'identité.
- Capacités d'attribut.
- capacités de profil.

Des agrégations de chacune des quatre catégories d'informations d'identité peuvent être utilisées pour prendre en charge une plus grande granularité des niveaux de garantie d'identité et peuvent être fournies sous forme de capacités d'identité, soit individuellement, soit dans une certaine combinaison, par différentes entités (voir la Figure 4). L'illustration peut être considérée comme une extension des illustrations de la Figure 2. Le modèle de question/réponse est généralement utilisé. Il n'est pas nécessaire que toutes ces capacités d'identité soient utilisées dans une implémentation IdM; leur utilisation, et donc leur existence en tant que capacités, dépend du contexte IdM, notamment du niveau de la garantie d'authentification d'entité souhaitée ou exigée.

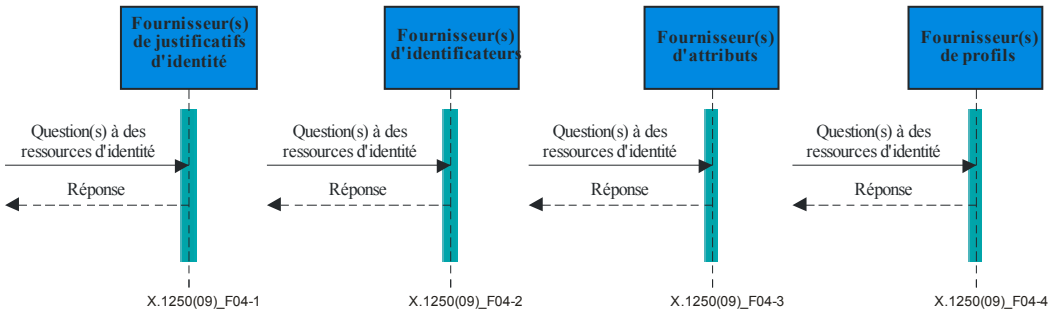

Figure 4 – Exemple de quatre capacités d'identité de base avec question/réponse

Les distinctions établies entre ces capacités d'identité peuvent être vagues d'un point de vue fonctionnel. Par exemple, les justificatifs d'identité ont leurs propres identificateurs, et les fournisseurs gèrent certaines informations d'attributs à propos de l'identité associée dont relève le justificatif, mais ils peuvent également tenir un fichier-journal concernant l'utilisation du justificatif, qui sert à une analyse de profil destinée à réduire au minimum les vols et utilisations frauduleuses d'identité.

Les fournisseurs IdM dans bon nombre d'implémentations telles que les télécommunications/l'informatique, ou les fournisseurs de services financiers (institutions ou organisations) entretenant une relation spéciale avec un utilisateur final ou client peuvent eux aussi fournir toutes ces capacités sous forme d'un tout. L'étendue de l'"ouverture IdM" et de l'interopérabilité avec des fournisseurs IdM relève d'une décision fondée sur la confiance et sur une communauté de besoins, d'activités, de relations et de dispositions réglementaires ou juridiques.

7.3.1 Capacités d'identificateur

Les identificateurs sont des attributs (par exemple, des noms) attribués généralement à une entité pour la gestion des systèmes d'information ou l'adressage des communications. En tant que tels, ils ont généralement une utilisation spécialisée. Par exemple, les numéros de téléphone, adresses URL et adresses e-mail sont utilisés aussi bien pour l'accès au service/dispositif que pour le routage sur les réseaux de télécommunication.

7.3.2 Capacités de justificatif d'identité

Les justificatifs d'identité sont utilisés pour aider à l'authentification des entités, soit une des deux parties à un échange d'informations ou à une transaction, soit les deux. Une des formes les plus anciennes, mais encore la plus généralisée, de justificatif d'identité par certificat est basée sur la norme d'un certificat numérique UIT-T X.509 [b-UIT-T X.509]. Parmi les autres formes de justificatifs d'identité, on retiendra les justificatifs délivrés par les services officiels, tels que badges professionnels, cartes SIM sans fil mobiles et cartes de crédit d'institutions financières ou cartes de guichet automatique bancaire (GAB).

Parfois, les justificatifs d'identité prennent également la forme de représentations biométriques. Certaines applications exigent de pouvoir vérifier rapidement que les justificatifs d'identité sont bien valables et n'ont pas été révoqués. Toutefois, il faut tenir compte du fait que les contrôles des justificatifs d'identité peuvent entraîner l'existence d'un grand nombre d'informations de traçage chez les IdSP, ce qui peut menacer la confidentialité. Par conséquent, il est important de disposer de justificatifs d'identité solides, qu'il n'est pas nécessaire de vérifier.

La complexité d'utilisation et de gestion des justificatifs d'identité numériques par le grand public sur une grande échelle peut être réduite en adoptant des approches IdM centrées sur l'utilisateur, combinées à des capacités de gestion des justificatifs d'identité (portefeuilles numériques, par exemple) [b-UIT-T X.1251]. Suivant le contexte, la prise en charge des justificatifs d'identité peut inclure la possibilité d'utiliser une variété de justificatifs d'identité pour atteindre différents niveaux de garantie d'authentification d'entité exigée.

7.3.3 Capacités d'attribut

En tant que caractéristiques d'entités, les attributs sont souvent relativement statiques – saisis dans le cadre du processus d'attribution des justificatifs d'identité ou des identificateurs (par exemple, noms, adresse physique, coordonnées de la personne à contacter, etc.). Dans d'autres cas (par exemple, emplacement géospatial), les attributs peuvent être fortement dynamiques.

Les capacités de découverte et de consultation des attributs peuvent nécessiter des protocoles interopérables spécialisés. Ces protocoles prennent généralement en charge un certain degré de vérification, notamment lorsque des informations PII sont en cause, pour la protection et la gestion des informations personnellement identifiables. Des plates-formes et des protocoles interopérables centrés sur l'utilisateur peuvent aussi permettre à l'utilisateur final de désigner comment les informations d'attribut doivent être traitées.

7.3.4 Capacités de profil

Un profil d'identité est une expression structurée d'attributs d'une entité qui pourrait être utilisée dans certains processus d'identification.

Il peut s'agir d'une identité observée ou découverte (c'est-à-dire ni déclarée ni assertée), par exemple des informations relatives à la réputation et aux transactions associées à une entité. Il est souvent particulièrement important pour détecter les vols d'identité. Des capacités d'identité de profil spécialisées sont également utilisées pour permettre la prise en charge de capacités de cybersécurité, telles que la signature par le profil d'un virus ou d'une attaque d'infrastructure.

Comme pour les capacités d'identité d'attribut, lorsque les profils correspondent à des personnes réelles, le système suppose également l'existence de tout un arsenal potentiel de spécifications fédératives et éventuellement juridiques et réglementaires, en augmentation et parfois conflictuelles, notamment pour la protection des informations d'identification personnelle. Dans certaines juridictions, si des informations PII sont en cause, les capacités de rétention et d'analyse des données de profil sont assujetties à d'importants impératifs de protection des données et de confidentialité, comprenant l'interdiction de la collecte de données et des mécanismes pour la suppression des données.

7.3.5 Capacités générales de gestion des données IdM

Un certain nombre de capacités IdM s'appliquent à la gestion du système IdM et à la gestion des données IdM pour toutes les capacités d'identité; les capacités assurent la prise en charge de:

- l'aptitude d'une partie requérante à accéder/supprimer/modifier/contrôler/gérer ses propres informations d'identité, sous réserve des lois, des règlements et/ou des politiques applicables;

- l'aptitude d'entités autorisées (par exemple, administrateurs système, parents, organes de sécurité publique, forces de police et autres tiers autorisés) à accéder/modifier/contrôler leurs informations d'identité, sous réserve des lois, des règlements et/ou des politiques applicables;
- l'importation/exportation d'informations d'identité, sous réserve des lois, des règlements et/ou des politiques applicables;
- un mécanisme pour indiquer un certain type d'informations sur le niveau de qualité des informations fournies aux parties utilisatrices. A cet effet, ces dernières doivent se mettre d'accord sur la valeur informative;
- l'aptitude pour une partie requérante à déléguer la gestion de ses informations d'identité à une autre entité;
- la gestion pendant toute la durée de vie de toutes les identités, ainsi qu'un moyen permettant de vérifier rapidement le statut des informations, sous réserve des lois, des règlements et/ou des politiques applicables;
- un mécanisme commun pour déterminer toutes les identités et en gérer la diffusion, sous réserve des lois, des règlements et/ou des politiques applicables.

7.3.6 Niveaux de garantie d'entité

Les ressources et leur détermination sont associées à des niveaux de garantie qui varient considérablement suivant un grand nombre de facteurs techniques et administratifs, qui sont conformes aux dispositions et normes adaptées au contexte.

Les capacités comprennent la prise en charge de:

- l'indication des niveaux de garantie des informations sur les identificateurs publics, en particulier pour les autorités d'enregistrement chargées des télécommunications publiques, y compris les attributaires qui sous-attribuent des identificateurs dans des systèmes de noms hiérarchiques et de numérotage;
- un protocole mutuel indiquant les niveaux de garantie associés aux informations fournies. On recommande des mécanismes globaux, communs, qui soient ouverts;
- un mécanisme permettant à une partie requérante, à une partie utilisatrice ou, par exemple, à un fournisseur de service d'identité de préciser les conditions de garantie et de validité pour un service d'identité, et d'indiquer les mesures qui seront prises si les conditions ne sont pas satisfaites.

7.4 Découverte des capacités d'identité

Dans le monde très dynamique et divers des capacités et des applications de réseau, un important problème IdM est la découverte des sources pour chacune des quatre capacités IdM essentielles. De nombreuses sources réparties et autonomes sont disponibles. La simple existence de capacités IdM ne suffit pas. Les parties utilisatrices doivent disposer de moyens standard pour être au courant de leur existence et savoir comment les atteindre (voir la Figure 5 ci-dessous). Le processus de découverte peut exiger la prise en charge d'un nouveau protocole de découverte, semblable en nature au protocole de pilotage de serveur dynamique grâce auquel un client peut découvrir un serveur DHCP et acquérir une adresse IP ainsi que des informations sur les passerelles. Le processus de découverte peut donc être aussi simple que celui où le détenteur d'identité fournit à une partie utilisatrice un URI ou un OID valable.

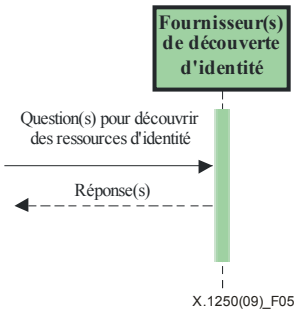

Figure 5 – Exemple de capacités de découverte d'identité d'une entité avec question/réponse

La découverte de capacités d'identité devrait en outre comprendre la découverte des capacités disponibles par l'intermédiaire de fédérations; certaines fédérations et communautés utilisant certains protocoles ont mis au point des solutions partielles pour satisfaire les besoins de découverte dans les limites de leurs communautés d'utilisateurs; toutefois, il n'existe pour l'heure aucun moyen pour une découverte globale ou une découverte entre fédérations. Un système prenant en charge la découverte est souhaitable. Les capacités de découverte souhaitables comprennent la prise en charge:

- des politiques d'accord d'activités des fournisseurs de service d'identité pour l'ensemble de la fédération ou des domaines;
- d'une seule et unique ouverture/fermeture de session, avec publication de cette capacité de manière normalisée, pour qu'elle puisse devenir "découvrable".

7.5 Interopérabilité et relais

L'interopérabilité globale entre parties fournissant des ressources de gestion d'identité est une nécessité impérieuse. Le présent paragraphe décrit des capacités pour instituer des consultations au sein d'une fédération ou par le biais d'un fournisseur relais.

Les fédérations sont fondées sur le principe de l'acceptation mutuelle des résultats d'authentification par les domaines participants et non sur le partage des informations d'identité entre ces domaines.

7.5.1 Capacités liées à une fédération

Les capacités liées à une fédération comprennent:

- la possibilité pour une partie utilisatrice d'établir un domaine d'authentification (c'est-à-dire de sécurité) par des alliances et une participation à des fédérations;
- l'obtention d'une autorisation de la partie requérante de fédérer les identités de partie requérante, sous réserve des lois, des règlements et des politiques applicables;
- la possibilité pour une partie requérante de déléguer un pouvoir de fédérer son identité, sous réserve des lois, des règlements et des politiques applicables.

7.5.2 Capacités liées à un relais d'identité

Les capacités liées à un relais d'identité comprennent:

- la possibilité pour une partie requérante d'établir des permissions et des interdictions en ce qui concerne les capacités de relais d'identité;
- un mécanisme pour découvrir le fournisseur de service d'identité des parties requérantes correspondantes;
- un mécanisme destiné au relais d'identité pour:

a) permettre la fédération des comptes des parties requérantes auprès d'un fournisseur de service d'identité et d'une partie utilisatrice dans différents domaines d'authentification à condition que chacun ait une permission appropriée de la partie requérante et du fournisseur relais de service d'identité; et

b) acheminer l'adresse d'un fournisseur de service d'identité dans un message de réponse adressé à une partie utilisatrice;

- un mécanisme pour assurer l'interopérabilité des informations de la partie requérante obtenues d'un fournisseur de service d'identité et leur permettre d'être reconnues et utilisées par le fournisseur de service d'identité correspondant ainsi que par les parties utilisatrices dans différents domaines (par exemple, deux réseaux);
- lorsqu'est créée une fédération via un fournisseur relais de service d'identité, un moyen pour notifier à la partie utilisatrice ou à un fournisseur de service d'identité l'occurrence de tout changement dans les politiques du fournisseur relais de service d'identité; ce mécanisme permet à la partie utilisatrice, ou à un fournisseur de service d'identité, de mettre fin à sa participation dans la fédération;
- lorsqu'est créée une fédération via un fournisseur relais de service d'identité, un moyen pour notifier à la partie requérante l'occurrence de tout changement dans les politiques du fournisseur relais de service d'identité; ce mécanisme permet à la partie requérante de ne plus accepter la fédération et de mettre fin à sa participation dans la fédération.

7.6 Sécurité IdM

Etant donné que les informations d'identité et les ressources de réseau qui fournissent les capacités d'identité sont des éléments de grande valeur, sensibles et vitaux des réseaux, en particulier celles qui sont considérées comme faisant partie d'une infrastructure nationale critique, elles doivent être protégées. La mise en sécurité d'une infrastructure IdM fait intervenir des politiques administratives, des pratiques opérationnelles, des technologies ainsi que des techniques destinées à prévenir tout risque pour les systèmes IdM et les données associées, qu'elles soient stationnaires ou en transit.

Le présent paragraphe complète les bonnes pratiques en matière de sécurité décrites dans la Recommandation [b-UIT-T X.1205] de plusieurs capacités pour aider à sécuriser les infrastructures IdM, à savoir:

- sécurisation des transactions (par exemple via une protection de la confidentialité, de l'intégrité et de l'antiréinsertion) entre toutes les parties (partie requérante, partie utilisatrice, fournisseur de service d'identité);
- mécanismes pour la non-répudiation des transactions IdM;
- sécurisation de la découverte des capacités d'identité, par exemple, pour assurer une protection contre une usurpation de nom du fournisseur de service d'identité;
- informations de sécurité pour l'audit des transactions IdM;
- implémentation de capacités pour détecter toute activité d'intrusion et y faire face en fonction d'une analyse des transactions IdM, et éventuellement pour alerter les détenteurs d'identité à propos des attaques soupçonnées visant leurs informations d'identité;
- implémentation de moyens permettant aux parties utilisatrices d'informer rapidement les fournisseurs de service d'identité de toute menace et sécurisation de cette capacité d'information contre toute exploitation.

Les politiques et directives d'utilisation (dénommées aussi parfois "gouvernance d'identité") sont également des mesures importantes, dans un environnement à plusieurs fournisseurs de service d'identité, pour réduire les menaces et les risques, mais aussi pour protéger les informations d'identification personnelle. Lorsque des fédérations, des alliances ou des fournisseurs relais

interviennent, ces mesures peuvent être promulguées par toutes les parties utilisatrices et tous les fournisseurs de service d'identité participants. L'utilisation accrue d'applications IdM centrées sur les utilisateurs peut aussi permettre aux utilisateurs finals requérants de spécifier des politiques qui aient un lien avec leurs attributs d'identité (voir l'exposé et la recommandation du § 7.7). La mise en œuvre de capacités de sécurité communes entre les membres d'une fédération présente d'importants avantages, et les fédérations devraient disposer de spécifications de sécurité bien adaptées.

Les capacités de sécurité et de politique IdM souhaitables comprennent:

- des capacités de garantie d'authentification d'identité, conformes aux directives applicables;
- un mécanisme de non-répudiation pour les transactions IdM;
- l'établissement dynamique de mécanismes, limités dans le temps, applicables aux relations transitoires et changeantes; un fournisseur relais mutuellement reconnu appartenant à une ou plusieurs fédérations peut avoir à intervenir;
- garantir la sécurité entre les fédérations, en particulier par des mécanismes de négociations pour des communications interfédérations sécurisées et l'échange d'informations entre fédérations en réponse à des menaces de cybersécurité;
- permettre à des applications sur des objets terminaux de pouvoir autoriser l'accès aux informations d'identité d'utilisateurs finals de l'objet terminal, sous réserve des lois, des règlements et des politiques applicables;
- un mécanisme permettant au fournisseur de service d'identité concerné d'envoyer une notification à toutes les parties affectées, au cas où l'attaque ou la révocation d'une identité serait signalée;
- une méthode sûre pour apprendre à reconnaître les capacités d'identité;
- la journalisation des informations de sécurité pour les transactions IdM avec suffisamment de détails pour établir la comptabilité et permettre une analyse scientifique;
- des capacités de détection des intrusions et de réaction pour les transactions IdM;
- des mécanismes pour permettre à des parties utilisatrices de rendre compte de toute attaque d'identité.

7.7 Protection, gestion et utilisation des informations d'identification personnelle

La préservation des informations d'identification personnelle (PII) revêt plusieurs facettes, dont deux sont l'utilisation de capacités de sécurité dans l'infrastructure IdM et l'utilisation de capacités pour informer en toute transparence les entités concernant l'utilisation de leurs informations d'identité, avec la possibilité de rattacher à cette information leurs préférences; dans ce contexte, on entend par "rattachement" un mécanisme permanent qui permet à un tiers possédant les informations d'identité de découvrir des capacités de politique pour les informations PII de l'entité associée. De plus en plus, des plates-formes produits centrées sur l'utilisateur ainsi que des capacités de fournisseurs relais de service d'identité permettent de mettre en œuvre ces types de préférence.

Dans certaines juridictions nationales et régionales, les informations PII doivent être collectées à bon escient, et à des fins explicites et légitimes. Les informations correspondantes échangées entre des parties communicantes devraient se limiter aux données nécessaires pour permettre à la partie utilisatrice de fournir un service ou une ressource à une partie requérante.

Du point de vue de la confidentialité, il existe dans certaines juridictions nationales un certain nombre de principes qui doivent être pris en compte, à savoir:

- les informations PII de rattachement doivent être collectées pour des finalités particulières, explicites et légitimes, et ne doivent pas faire l'objet d'un traitement supplémentaire incompatible avec ces finalités;

- les informations PII doivent être pertinentes et satisfaisantes et ne pas être excessives par rapport aux finalités pour lesquelles elles sont collectées et/ou font l'objet d'un traitement supplémentaire;
- les informations PII doivent être exactes et tenues à jour; il faut prendre toutes les mesures raisonnables pour faire en sorte que les données qui sont inexactes ou incomplètes, par rapport aux finalités pour lesquelles elles ont été collectées ou pour lesquelles elles font l'objet d'un traitement supplémentaire, soient effacées ou modifiées;
- les informations PII doivent être conservées sous une forme qui permet d'identifier les sujets des données pendant une durée ne dépassant pas la durée nécessaire pour les finalités pour lesquelles les données ont été collectés ou pour lesquelles elles font l'objet d'un traitement supplémentaire;
- les informations PII ne devraient pas être partagées entre applications pour des finalités différentes;
- les informations PII doivent être limitées au minimum nécessaire pour une finalité donnée;
- les informations PII doivent être sécurisées. Des mesures techniques et organisationnelles appropriées doivent être prises pour protéger les informations PII contre les destructions accidentelles ou illicites, pertes accidentelles, altérations, divulgations ou accès non autorisés, en particulier lorsque le traitement fait intervenir la transmission de données sur un réseau, ainsi que contre toutes les autres formes de traitement illicites;
- les personnes ont le droit d'accéder aux informations PII les concernant, de les modifier ou de les effacer;
- les informations PII ne doivent pas être conservées plus longtemps que nécessaire pour les finalités définies.

D'autres juridictions exigent des mécanismes de protection, dont l'utilisation de notifications pour chaque accès à un compte ou pour chaque modification d'informations. L'utilisation d'informations PII dans les réseaux et services de télécommunication/TIC devrait correspondre à une finalité explicite, par rapport à laquelle on peut estimer la nature pertinente, satisfaisante et non excessive des données enregistrées, les catégories de personnes et d'organisations pouvant recevoir ces données et la durée pendant laquelle les données collectées peuvent être stockées.

Les capacités comprennent:

- la collecte, le traitement et la protection des informations PII conformément aux principes et à la législation concernant la confidentialité et la protection des données. Au minimum, les protections devraient comprendre celles qui ont été spécifiées par l'OCDE dans le cadre de lignes directrices régissant la protection de la vie privée à l'échelle mondiale. Les réglementations régionales/nationales applicables peuvent imposer l'observation d'obligations supplémentaires (par exemple Directive européenne sur la protection des données 95/46/CE);
- la sécurisation et la protection de limites reconnues pour minimaliser la collecte des informations PII. Les informations PII devraient être obtenues pour des finalités spécifiées, explicites et légitimes, uniquement avec le consentement du sujet des données;
- des fonctionnalités telles que, lorsqu'un fournisseur de service d'identité a fédéré séparément l'identité d'une partie requérante avec deux ou plus de deux parties utilisatrices, il ne devrait pas être possible pour les parties utilisatrices d'utiliser les informations que leur a fournies le fournisseur de service d'identité pour déterminer que les identités renvoient à la même partie requérante;
- un service de notification lorsque des attributs d'une partie requérante sont modifiés;
- un service de notification lorsque les déclarations de consentement d'une partie requérante sont modifiées;

- une disposition pour alerter les titulaires d'identité en cas d'activité de transaction IdM interprétée par le fournisseur de service d'identité comme une tentative d'abuser de leur identité;
- une disposition pour informer les titulaires d'identité en cas d'attaque des systèmes et capacités du fournisseur de service d'identité;
- la possibilité d'appliquer des limites de durée pour le stockage des informations PII, pour que ces informations ne soient pas conservées plus longtemps que nécessaire pour les finalités définies;
- la possibilité pour les entités de vérifier, corriger et supprimer les informations PII correspondantes conformément aux lois, règlements et politiques applicables.

7.8 Audit et conformité

La gestion d'identité IdM est assujettie à divers impératifs, juridiques, réglementaires et commerciaux, qui peuvent exiger un certain niveau d'audit et de conformité. Exemples de mesures d'audit et de conformité: tenir des journaux de sécurité, protéger les informations personnelles et les utiliser à bon escient et informer les entités auxquelles s'appliquent les informations. Les procédures d'audit devraient être conformes aux capacités de protection des informations PII décrites au § 7.7 ci-dessus, en particulier parce qu'une autre nouvelle partie peut être concernée et qu'un conflit avec les lois, règlements et politiques en matière de confidentialité peut en résulter.

Les capacités comprennent:

- des mécanismes permettant une analyse scientifique;
- des mécanismes sécurisés et réciproques pour échanger des informations sur les procédures d'audit de la gestion d'identité;
- l'horodatage;
- l'horodatage des archives en fonction du contexte, selon l'importance des informations auditées et le facteur temps;
- il faut veiller à ce que les implémentations des procédures d'audit de la gestion d'identité respectent les impératifs applicables de confidentialité.

7.8.1 Capacités d'exactitude des horodates

Il est très important de disposer d'horodates exactes pour gérer les durées de vie des identités et maintenir la sécurité au sein des systèmes IdM, toutes les informations d'identité étant limitées dans le temps. La procédure d'audit décrit la survenance d'événements à l'intérieur de ces délais. Aux fins d'audit, les horodates sont essentielles, et la qualité, voire l'utilisabilité des données d'audit, est déterminée par l'exactitude des horodates aux endroits correspondant aux événements, ce qui permet d'assurer un audit satisfaisant des capacités de réseau et d'application hautement asynchrones et hautement réparties. Parmi les capacités souhaitables figurent des capacités d'exactitude des horodates qui soient suffisantes pour l'audit en des endroits de référence communs agréés, choisis de sorte qu'on ait un niveau de garantie mutuellement accepté.

7.9 Performance, fiabilité et disponibilité

La gestion d'identité IdM est une capacité de réseau importante qui doit être conçue et mise en œuvre de manière à permettre la réalisation d'objectifs de performance, de fiabilité et de disponibilité. Il est recommandé que les objectifs de fiabilité et de disponibilité IdM soient comparables aux autres fonctions de réseau critiques étant donné qu'ils constituent le cœur des procédures d'authentification et d'autorisation des accès ainsi que de toutes les transactions dans le réseau, d'où la nécessité, par exemple, de faire en sorte que les objectifs de puissance IdM, de support environnemental et de connectivité soient suffisants. La performance IdM (par exemple, le temps de réponse à une question) devrait être conforme aux charges escomptées de questions IdM.

La disponibilité d'un système IdM n'est pas homogène au travers de toutes les composantes (éléments de diffusion, de consultation, de révocation) et doit en fin de compte être liée au niveau de garantie du justificatif d'identité. Les impératifs de disponibilité suivants sont souhaitables, mais varieront entre les différents blocs constitutifs (organe d'archivage, système d'inscription, capacité de révocation):

- fiabilité et disponibilité à des niveaux comparables aux autres éléments, systèmes et capacités de réseau critiques;
- incorporation de capacités IdM dans les plans de reprise après sinistre du fournisseur;
- implémentations IdM assurant des temps de réponse raisonnables pour des transactions IdM.

7.10 Internationalisation

Pour une interopérabilité globale, il faut qu'on puisse utiliser des jeux de caractères et des langages différents. Les objectifs d'internationalisation sont reconnus comme étant un prérequis important au niveau de la conception et du support pour toutes les applications basées sur des réseaux publics, en particulier pour les capacités IdM.

Bibliographie

[b-UIT-T X.509] Recommandation UIT-T X.509 (2005) | ISO/IEC 9594-8:2005, *Technologies de l'information – Interconnexion des systèmes ouverts – L'Annuaire: Cadre général des certificats de clé publique et d'attributs*.

[b-UIT-T X.805] Recommandation UIT-T X.805 (2003), *Architecture de sécurité pour les systèmes assurant des communications de bout en bout*.

[b-UIT-T X.811] Recommandation UIT-T X.811 (1995) | ISO/IEC 10181-2:1996, *Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: Cadre d'authentification*.

[b-UIT-T X.1205] Recommandation UIT-T X.1205 (2008), *Présentation générale de la cybersécurité*.

[b-UIT-T X.1251] Recommandation UIT-T X.1251 (2009), *Cadre régissant le contrôle par l'utilisateur des identités numériques*.

[b-UIT-T Y.110] Recommandation UIT-T Y.110 (1998), *Infrastructure mondiale de l'information: principes et architecture générale*.

[b-UIT-T Y.2012] Recommandation UIT-T Y.2012 (2006), *Prescriptions fonctionnelles et architecture du réseau de prochaine génération version 1*.

[b-UIT-T Y.2702] Recommandation UIT-T Y.2702 (2008), *Spécifications d'authentification et d'autorisation dans les réseaux de prochaine génération de version 1*.

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

[b-IETF RFC 2560] IETF RFC 2560 (1999), *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP*.

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

Imprimé en Suisse
Genève, 2010