

Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1252

(04/2010)

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

Sécurité du cyberspace – Gestion des identités

**Termes et définitions de base relatifs à la
gestion d'identité**

Recommandation UIT-T X.1252



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.1252

Termes et définitions de base relatifs à la gestion d'identité

Résumé

La Recommandation UIT-T X.1252 définit des termes clés utilisés dans le domaine de la gestion d'identité (IdM). Ces termes, qui proviennent de nombreuses sources, sont tous employés couramment dans les travaux relatifs à la gestion d'identité. L'objectif de la présente Recommandation n'est pas de proposer un énorme recueil de termes associés à la gestion d'identité. En effet, les termes définis ici sont limités à ceux qui sont considérés comme formant une liste de base des termes les plus importants et les plus couramment utilisés dans le domaine de la gestion d'identité. L'Annexe A de la présente Recommandation contient des explications relatives à certains de ces termes clés.

L'un des principaux objectifs de la présente Recommandation est de promouvoir une compréhension commune de ces termes parmi les groupes qui élaborent actuellement (ou qui ont l'intention d'élaborer) des normes relatives à la gestion d'identité. Les définitions sont formulées de manière à ce qu'elles soient, dans la mesure du possible, indépendantes des mises en œuvre ou des contextes particuliers et devraient par conséquent pouvoir servir de définitions de base pour tous les travaux menés dans le domaine de la gestion d'identité. Il est reconnu que, dans certains cas et certains contextes, des détails supplémentaires peuvent être nécessaires pour un terme donné, auquel cas il peut être envisagé de préciser la définition de base.

Historique

Edition	Recommandation	Approbation	Commission d'études
1.0	ITU-T X.1252	2010-04-16	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 2010

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
4	Abréviations et acronymes 2
5	Conventions 2
6	Termes et définitions 2
Annexe A – Terminologie de base IdM: éléments fondamentaux et explications	
A.1	Authentification et confiance 7
A.2	Déclaration/assertion 12
A.3	Inscription et enregistrement 12
A.4	Fournisseur d'identité et fournisseur de service d'identité..... 12
A.5	Profil d'identité 13
Bibliographie..... 15	

Introduction

Cette liste de termes et définitions dans le domaine de la gestion d'identité a commencé à être établie en 2007. Les étapes de son élaboration ont été nombreuses, elle a fait l'objet de contributions et de commentaires soumis par un grand nombre de personnes et elle a été revue à de nombreuses reprises. Ces termes et définitions proviennent de nombreuses sources, dont certaines – mais pas toutes – sont énumérées dans la bibliographie. Dans certains cas, la définition d'origine convenait et a été reprise, mais dans de nombreux cas, elle a été modifiée ou combinée avec d'autres pour être la meilleure possible pour un terme donné.

Des efforts considérables ont été faits pour que les définitions expriment la même signification que celles qui figurent dans les autres Recommandations | Normes internationales portant sur la gestion d'identité. Cela signifie que, dans certains cas, les mots peuvent être différents mais la signification devrait être la même.

Etant donné qu'un terme peut être utilisé dans un certain nombre de contextes différents, les définitions se limitent à une simple description de base, sans inclure les alternatives ou les variantes qui pourraient exister. Les éventuels détails ou précisions supplémentaires nécessaires peuvent être ajoutés en fonction des besoins.

Les éléments fondamentaux à partir desquels les définitions sont formulées sont examinés plus avant dans l'Annexe A.

Recommandation UIT-T X.1252

Termes et définitions de base relatifs à la gestion d'identité

1 Domaine d'application

La présente Recommandation contient un ensemble de base de définitions de termes couramment utilisés dans le domaine de la gestion d'identité (IdM). Les définitions donnent une définition de base de chaque terme, le but étant d'exprimer leur signification fondamentale, bien qu'une note puisse exceptionnellement être ajoutée afin de clarifier la définition. On trouvera à l'Annexe A l'explication de certains termes et définitions clés.

NOTE – Dans la présente Recommandation, l'emploi du terme "identité" relatif à la gestion d'identité (IdM) ne correspond pas à sa signification absolue et ne constitue pas en particulier la validation positive d'une personne.

2 Références

Les Recommandations UIT-T et autres références suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions de la présente Recommandation. Au moment de la publication, les éditions indiquées étaient en vigueur. Les Recommandations et autres références étant sujettes à révision, les utilisateurs de la présente Recommandation sont invités à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et autres références énumérées ci-dessous. Une liste des Recommandations UIT-T en vigueur est publiée périodiquement. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document en tant que tel le statut de Recommandation.

- [UIT-T X.501] Recommandation UIT-T X.501 (2005) | ISO/CEI 9594-2:2005,
Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: les modèles.
- [UIT-T X.800] Recommandation UIT-T X.800 (1991), *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT.*
- [UIT-T X.810] Recommandation UIT-T X.810 (1995) | ISO/CEI 10181-1:1996,
Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: aperçu général.
- [UIT-T X.811] Recommandation UIT-T X.811 (1995) | ISO/CEI 10181-2:1996,
Technologies de l'information – Interconnexion des systèmes ouverts – Cadres de sécurité pour les systèmes ouverts: cadre d'authentification.
- [UIT-T Y.2701] Recommandation UIT-T Y.2701 (2007), *Prescriptions de sécurité des réseaux de prochaine génération de version 1.*
- [UIT-T Y.2702] Recommandation UIT-T Y.2702 (2008), *Spécifications d'authentification et d'autorisation pour les réseaux de prochaine génération de version 1.*
- [UIT-T Y.2720] Recommandation UIT-T Y.2720 (2009), *Cadre de gestion d'identité dans les réseaux NGN.*

3 Définitions

Ce paragraphe est délibérément laissé en blanc.

4 Abréviations et acronymes

Les abréviations suivantes sont utilisées dans la présente Recommandation:

IdM	gestion d'identité (<i>identity management</i>)
IdP	fournisseur d'identité (<i>identity provider</i>)
IdSP	fournisseur de service d'identité (<i>identity service provider</i>)
NGN	réseau de prochaine génération (<i>next generation network</i>)
PII	informations d'identification personnelle (<i>personally identifiable information</i>)
RP	partie utilisatrice (<i>relying party</i>)

5 Conventions

Ce paragraphe est délibérément laissé en blanc.

6 Termes et définitions

6.1 contrôle d'accès (*access control*): procédure utilisée pour déterminer si l'accès à des ressources, fonctionnalités, services ou informations devrait être accordé à une entité, compte tenu des règles préétablies et des droits spécifiques ou de l'autorité associés à l'entité requérante.

6.2 adresse (*address*) [UIT-T Y.2091]: identificateur d'un point de terminaison particulier qui est utilisé pour le routage.

6.3 agent (*agent*): entité qui agit au nom d'une autre entité.

6.4 alliance (*alliance*): accord entre deux entités indépendantes ou plus qui définit leurs relations et la manière dont elles effectuent conjointement des activités.

6.5 anonymat (*anonymity*): situation dans laquelle une entité 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.).

6.6 assertion (*assertion*): affirmation faite par une entité non accompagnée d'une preuve de validité¹.

6.7 garantie (*assurance*): voir garantie d'authentification et garantie d'identité.

6.8 niveau de garantie (*assurance level*): niveau de confiance dans le lien entre une entité et l'information d'identité présentée.

6.9 attribut (*attribute*): information liée à une entité qui en spécifie une caractéristique.

6.10 type d'attribut (*attribute type*) [UIT-T X.501]: composante d'un attribut qui indique la classe d'information donnée par cet attribut.

6.11 valeur d'attribut (*attribute value*) [UIT-T X.501]: instance particulière de la classe d'information indiquée par un type d'attribut.

6.12 authentification (d'entité) (*entity authentication*): processus utilisé pour obtenir une confiance suffisante dans le lien entre l'entité et l'identité présentée.

NOTE – Dans un contexte de gestion d'identité (IdM), le terme authentification désigne l'authentification d'entité.

¹ Il est convenu que les termes assertion et déclaration sont très proches.

6.13 garantie d'authentification (*authentication assurance*): degré de confiance obtenu 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.

NOTE – La confiance repose sur le degré de confiance dans le lien entre l'entité communicante et l'identité présentée.

6.14 autorisation (*authorization*) [UIT-T Y.2720] et [UIT-T X.800]: octroi de droits et octroi d'accès sur la base de ces droits.

6.15 lien (*binding*): association, rapport ou relation explicite établi.

6.16 reconnaissance biométrique (*biometric recognition*) [b-ISO/IEC CD 2382-37]: reconnaissance automatisée des personnes physiques fondée sur l'observation de leurs caractéristiques comportementales et biologiques.

6.17 certificat (*certificate*) [UIT-T X.810]: ensemble de données relatives à la sécurité délivré par une autorité de sécurité ou un tiers de confiance, qui, conjointement avec les informations de sécurité, sont utilisés pour fournir des services d'intégrité et d'authentification de l'origine des données.

6.18 déclaration (*claim*) [b-OED]: affirmer être le cas, sans pouvoir fournir de preuve¹.

6.19 déclarant (*claimant*) [UIT-T Y.2720] et [UIT-T X.811]: entité qui est ou représente une entité principale à des fins d'authentification.

NOTE – Un déclarant comporte les fonctions nécessaires pour engager des échanges pour authentification au nom d'une entité principale.

6.20 contexte (*context*): environnement avec des frontières définies dans lequel des entités existent et interagissent.

6.21 justificatif (*credential*): ensemble de données présentées comme preuve d'une identité déclarée et/ou de droits.

6.22 délégation (*delegation*): action d'attribuer une autorité, une responsabilité ou une fonction à une autre entité.

6.23 identité numérique (*digital identity*): représentation numérique des informations connues à propos d'un individu, d'un groupe ou d'une organisation spécifique.

6.24 inscription (*enrolment*): processus d'inauguration d'une entité dans un contexte.

NOTE 1 – L'inscription peut comprendre la vérification de l'identité de l'entité et l'établissement d'une identité contextuelle.

NOTE 2 – De plus, l'inscription est un préalable nécessaire à l'enregistrement, qui, dans de nombreux cas, est utilisé pour décrire les deux processus.

6.25 entité (*entity*): 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 entités. 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.

6.26 authentification d'entité (*entity authentication*): processus permettant d'obtenir une confiance suffisante dans le lien entre l'entité et l'identité présentée.

NOTE – Dans un contexte de gestion d'identité (IdM), le terme authentification désigne l'authentification d'entité.

6.27 fédération (*federation*): association d'utilisateurs, de fournisseurs de service et de fournisseurs de service d'identité.

6.28 identification (*identification*): processus de reconnaissance d'une entité compte tenu de ses caractéristiques contextuelles.

6.29 identificateur (*identifier*): un ou plusieurs attributs utilisés pour identifier une entité dans un contexte.

6.30 identité (*identity*): représentation d'une entité sous la forme d'un ou de plusieurs attributs qui sont suffisants pour pouvoir distinguer les entités dans un contexte. Aux fins de la gestion d'identité (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.

6.31 garantie d'identité (*identity assurance*): degré de confiance dans le processus de validation et de vérification d'identité utilisé pour établir l'identité de l'entité à laquelle le justificatif a été délivré, et degré de confiance dans le fait que l'entité qui utilise le justificatif est cette entité ou l'entité à laquelle le justificatif a été délivré ou attribué.

6.32 politique de sécurité fondée sur l'identité (*identity based security policy*) [UIT-T X.800]: politique de sécurité fondée sur les identités et/ou les attributs d'utilisateurs, d'un groupe d'utilisateurs, ou d'entités agissant au nom des utilisateurs et des ressources/objets utilisés.

6.33 fournisseur relais de service d'identité (*identity service bridge provider*): fournisseur de service d'identité faisant office d'intermédiaire digne de confiance entre d'autres fournisseurs de service d'identité.

6.34 gestion d'identité (*identity management*) [UIT-T Y.2720]: ensemble de fonctions et de fonctionnalités (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, les attributs), pour garantir l'identité d'une entité et pour permettre des applications commerciales et de sécurité.

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

6.36 contrôle d'identité (*identity proofing*): processus permettant de valider et de vérifier suffisamment d'informations pour confirmer l'identité déclarée de l'entité.

6.37 fournisseur d'identité (IdP, *identity provider*): voir fournisseur de service d'identité (IdSP).

6.38 fournisseur de service d'identité (IdSP, *identity service provider*): entité qui vérifie, tient à jour, gère et peut créer et attribuer des informations d'identité d'autres entités.

6.39 vérification d'identité (*identity verification*): processus consistant à confirmer qu'une identité déclarée est correcte sur la base de la comparaison des déclarations d'identité offertes avec les informations précédemment contrôlées.

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

6.41 authentification mutuelle (*mutual authentication*): processus par lequel deux entités (par exemple un client et un serveur) s'authentifient mutuellement de telle sorte que chacun soit sûr de l'identité de l'autre.

6.42 nom (*name*): expression par laquelle une entité est connue, définie et désignée.

NOTE – Un nom est utilisé dans un contexte et il ne peut être supposé qu'il soit unique ou sans ambiguïté. Aux fins du routage, il peut être transformé ou converti en adresse.

6.43 non-répudiation (*non-repudiation*): capacité de protection contre le fait que l'une des entités impliquées dans une action nie avoir participé à la totalité ou à une partie de l'action.

6.44 profil (*pattern*): voir profil d'identité.

6.45 persistant (*persistent*): existant et en mesure d'être utilisé dans des services en dehors du contrôle direct de l'attribueur délivreur, sans limite de temps fixée.

6.46 information d'identification personnelle (PII, *personally identifiable information*): toute information: a) identifiant ou permettant d'identifier la personne à laquelle elle se rapporte, de se mettre en rapport avec elle ou de la localiser; b) permettant d'obtenir des informations d'identification ou les coordonnées d'une personne; ou c) étant ou pouvant être directement ou indirectement liée à une personne physique.

6.47 entité principale (*principal*) [UIT-T Y.2720], [UIT-T X.811] et [UIT-T Y.2702]: entité dont l'identité peut être authentifiée.

6.48 respect de la vie privée (*privacy*): droit des individus de contrôler ou d'agir sur des informations les concernant, qui peuvent être collectées, gérées, conservées, consultées et utilisées ou distribuées.

6.49 politique de respect de la vie privée (*privacy policy*): politique qui définit les conditions applicables à la protection de l'accès aux informations d'identification personnelle (PII) et de leur diffusion, ainsi que les droits des individus en ce qui concerne la manière dont leurs informations personnelles sont utilisées.

6.50 privilège (*privilege*): droit permettant à l'entité à laquelle il est octroyé d'effectuer une action particulière.

6.51 contrôle (*proofing*): vérification et validation des informations lors de l'inscription de nouvelles entités dans des systèmes d'identité.

6.52 pseudonyme (*pseudonym*): 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.

NOTE – Un pseudonyme peut permettre d'éviter ou de réduire les risques en matière de confidentialité associés à l'utilisation de liens d'identification susceptibles de divulguer l'identité de l'entité.

6.53 enregistrement (*registration*): processus par lequel une entité demande et se voit attribuer des privilèges pour utiliser un service ou une ressource.

NOTE – L'inscription est un préalable nécessaire à l'enregistrement. Les fonctions d'inscription et d'enregistrement peuvent être combinées ou séparées.

6.54 partie utilisatrice (RP, *relying party*) [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.

6.55 répudiation (*repudiation*): fait de nier, pour l'une des entités impliquées, avoir participé à la totalité ou à une partie d'une action.

6.56 entité requérante (*requesting entity*): entité soumettant une représentation ou une déclaration d'identité à une partie utilisatrice dans un contexte de demande donné.

6.57 révocation (*revocation*): annulation par quelqu'un ayant l'autorité nécessaire de quelque chose qui s'est fait précédemment.

6.58 rôle (*role*): ensemble de propriétés ou d'attributs qui décrivent les capacités ou les fonctions d'une entité.

NOTE – Chaque entité peut avoir de nombreux rôles. Ses capacités peuvent lui être propres ou lui être attribuées.

6.59 audit de sécurité (*security audit*) [UIT-T X.800]: analyse et examen indépendants des enregistrements et activités du système afin de s'assurer de l'adéquation des commandes du système, pour garantir le respect de la politique et des procédures opérationnelles établies, détecter les failles dans la sécurité et recommander des modifications appropriées concernant le contrôle, la politique et les procédures.

6.60 domaine de sécurité (*security domain*) [UIT-T Y.2720], [UIT-T Y.2701] et [UIT-T X.810]: ensemble d'éléments, politique de sécurité, autorité de sécurité et ensemble d'activités liées à la sécurité dont les éléments sont gérés conformément à la politique de sécurité.

6.61 zone de sécurité (*security zone*) [UIT-T Y.2701]: Zone protégée définie par son contrôle opérationnel, son emplacement et sa connectivité aux autres dispositifs/éléments de réseau.

6.62 autorité de domaine de sécurité (*security domain authority*) [UIT-T X.810]: autorité de sécurité qui est responsable de la mise en œuvre d'une politique de sécurité pour un domaine de sécurité.

6.63 identité auto-assertée (*self-asserted identity*): identité qu'une entité déclare comme étant la sienne.

6.64 confiance (*trust*): conviction que des informations sont fiables et vraies ou qu'une entité est apte et disposée à agir de façon appropriée dans un contexte spécifié.

6.65 niveau de confiance (*trust level*): degré cohérent et quantifiable de fiabilité du caractère, de l'aptitude, du pouvoir ou de la réalité de quelqu'un ou de quelque chose.

6.66 tiers de confiance (*trusted third party*) [UIT-T Y.2702], [UIT-T X.800] et [UIT-T X.810]: dans le contexte d'une politique de sécurité, autorité de sécurité ou son agent auquel il est fait confiance au regard de certaines activités liées à la sécurité.

6.67 utilisateur (*user*): toute entité qui utilise une ressource, par exemple un système, un équipement, un terminal, un processus, une application ou un réseau d'entreprise.

6.68 centré sur l'utilisateur (*user-centric*): système de gestion d'identité (IdM) qui confère 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, y compris des informations d'identification personnelle des utilisateurs, entre entités.

6.69 vérification (*verification*): processus ou instance d'établissement de l'authenticité de quelque chose.

NOTE – La vérification des informations d'identité peut comprendre un examen de leur validité, de l'exactitude de leur source, de l'original (sans modification), de leur exactitude, de leur lien à l'entité, etc.

6.70 vérificateur (*verifier*): entité qui vérifie et valide des informations d'identité.

Annexe A

Terminologie de base IdM: éléments fondamentaux et explications

(Cette annexe fait partie intégrante de la présente Recommandation)

Contexte

Les discussions sur la gestion d'identité (IdM) ont fait apparaître des différences de compréhension suivant les personnes quant à l'objet de l'IdM, aux procédures de base utilisées ainsi qu'à la terminologie et aux définitions des termes. Ces différences ont donné lieu à des malentendus et à des discussions prolongées pendant le processus de normalisation de l'IdM.

Afin d'éviter que ces malentendus se reproduisent à l'avenir, cette annexe présente certains des accords conclus pendant les discussions qui ont eu lieu au sein de l'UIT-T sur cette terminologie et ces concepts de base et tente d'expliquer le cheminement jusqu'à l'établissement (ou, dans certains cas, l'adoption) des termes figurant dans la présente Recommandation. Il convient de noter que cette annexe ne présente ni n'explique le point de vue holistique de la gestion d'identité.

Introduction

Identité est le terme autour duquel tous les autres termes IdM s'articulent. Dans le monde réel, et non dans le monde numérique, par exemple, l'identité d'une personne physique est acceptée sans ambages et est fondée sur tout un ensemble de caractéristiques ou d'attributs. Dans cet ensemble figurent des caractéristiques physiques comme la taille, la couleur des cheveux, l'apparence générale, les habitudes, le comportement, etc. On peut aussi utiliser la date de naissance, le lieu de naissance, l'adresse du domicile ou le numéro de téléphone. Normalement, dans un processus de communication, les deux parties doivent avoir suffisamment confiance dans le fait qu'elles communiquent avec le partenaire correct. Le processus permettant d'obtenir cette confiance fait en principe intervenir deux individus ou "entités" ou plus: l'entité dont l'identité doit être confirmée (*entité requérante*) et l'entité qui utilisera une identité confirmée (*partie utilisatrice*), une troisième entité qui gère les identités (*fournisseur de service d'identité*) pouvant intervenir.

Dans le monde numérique ou "en ligne", une "identité" est également constituée d'attributs, tout comme dans le monde réel. Toutefois, dans ce cas, l'"identité" peut reposer sur une seule caractéristique ou sur un grand nombre, suivant le contexte dans lequel elle apparaît. Ceci s'applique aux objets inanimés comme aux personnes physiques, de sorte que les utilisateurs sont souvent désignés comme étant des entités.

D'une manière générale, les identificateurs et/ou les attributs caractériseront de manière univoque une entité dans un contexte particulier. C'est pourquoi une entité peut avoir un certain nombre d'identités différentes, dont certaines seront un sous-ensemble d'autres identités.

A.1 Authentification et confiance

Le processus d'authentification est une partie importante de l'IdM. Dans ce qui suit, on tente d'expliquer le processus d'authentification et son importance pour la confiance.

Il est à noter que, lors de l'application de ce modèle à des procédures et applications réelles, il faut avoir une idée très claire des partenaires de communication et des chaînes de confiance applicables.

Le processus d'authentification peut être décrit comme suit:

Dans la plupart des processus de communication, il faut que les partenaires de communication aient suffisamment confiance dans le fait qu'ils communiquent réellement avec le partenaire voulu. Par conséquent, au début d'une communication, les partenaires essaient d'obtenir un niveau de confiance approprié sur la base des informations d'identité disponibles concernant le partenaire, c'est-à-dire d'avoir une confiance suffisante dans le lien entre l'entité et l'identité présentée.

Le processus d'établissement de la confiance est particulièrement important lorsque les partenaires de communication sont distants l'un de l'autre et ne sont reliés que par une liaison de télécommunication. Le processus d'authentification est exécuté afin de déterminer, avec un degré de confiance suffisant, que l'identité présentée par un partenaire de communication lui appartient réellement.

Une communication fait toujours intervenir deux partenaires distincts ou plus qui échangent des informations. En raison de la grande variété de partenaires possibles (par exemple des êtres humains et des choses), il faut définir un terme général. Le terme choisi est *entité*, laquelle est définie comme suit: 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 entités.
- 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.

Les informations qui peuvent être utilisées pour l'identification d'une entité sont fondées sur les attributs de l'entité. Un *attribut* est défini comme suit: information liée à une entité qui en spécifie une caractéristique. Dans la pratique, l'identification d'une entité est généralement fondée sur un sous-ensemble de ses attributs car elle est limitée par ce qu'on appelle le contexte, dans lequel l'entité existe et interagit. Plus le contexte est étroit et plus les frontières sont claires, moins nombreux seront les attributs nécessaires pour l'identification. Le *contexte* est défini comme suit: environnement avec des frontières définies dans lequel des entités existent et interagissent.

Etant donné que la définition de l'entité est fondée sur la capacité d'être identifiée, il faut définir clairement l'*identification*: processus de reconnaissance d'une entité telle qu'elle est caractérisée dans un contexte.

Pour distinguer les entités, il suffit d'utiliser un sous-ensemble des attributs qui soit adapté au contexte, à savoir l'*identité*, qui est définie comme suit: représentation d'une entité sous la forme d'un ou de plusieurs attributs qui sont suffisants pour pouvoir distinguer les entités dans un contexte. Aux fins de la gestion d'identité (IdM), le terme identité désigne une 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.

Une identité peut être un sous-ensemble d'une autre identité. Il peut aussi y avoir des intersections d'identités. Toutefois, pour diverses raisons (par exemple dans un souci de respect de la vie privée), on peut éviter explicitement, voire exclure, les intersections d'identités utilisées à des fins différentes ou dans des contextes différents.

La Figure A.1 montre les relations entre entité, identités et attributs.

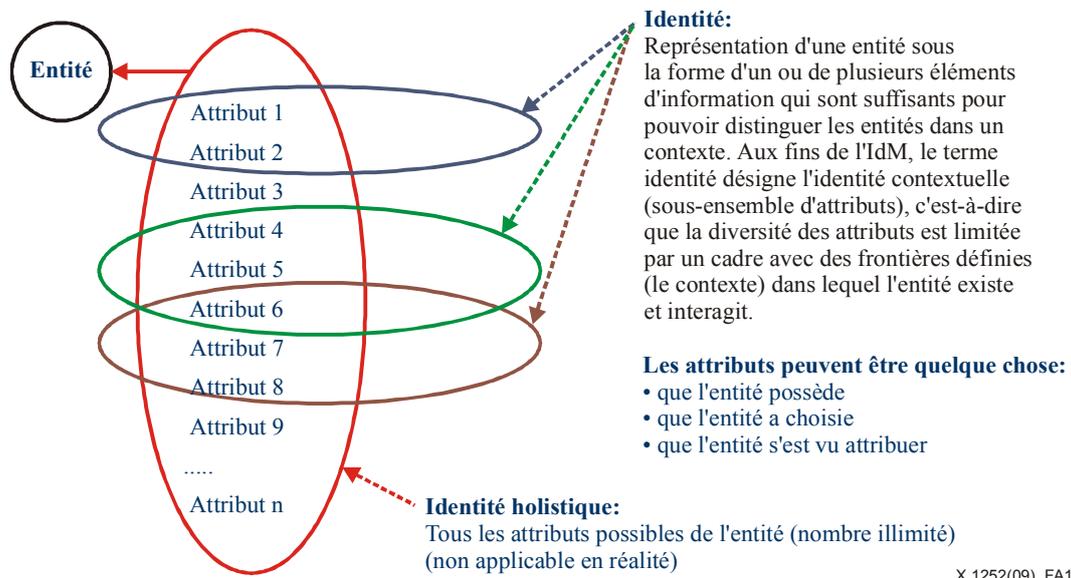


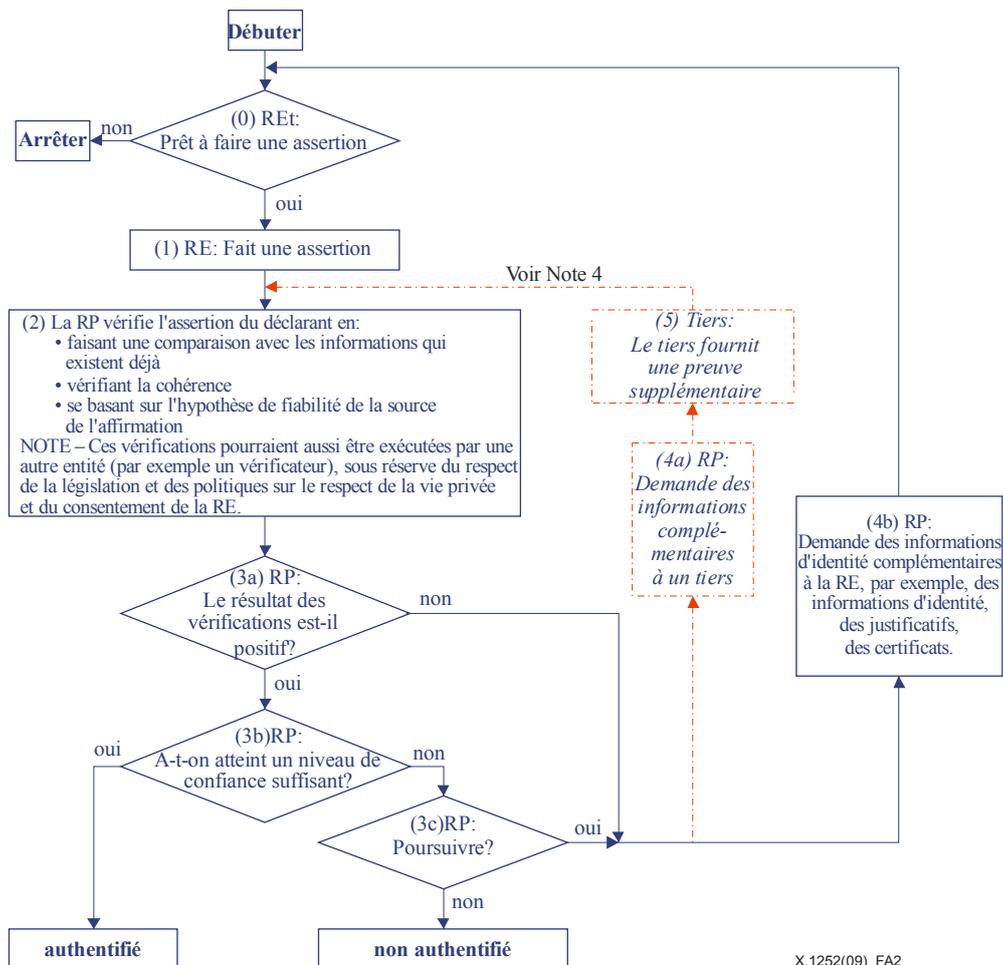
Figure A.1 – Relations entre entité, identités et attributs

Comme nous l'avons déjà indiqué, l'authentification est importante dans le cadre de la gestion d'identité. Il s'agit du processus nécessaire pour obtenir une confiance suffisante dans le fait que la communication a lieu avec le partenaire voulu. Le niveau de confiance réel nécessaire dépendra de la sensibilité de l'application et/ou des risques encourus si la communication a lieu avec un partenaire autre que le partenaire voulu.

Des droits ou des privilèges peuvent être attribués avec diverses finalités, par exemple:

- échanger ou fournir des informations qui ne sont pas destinées à être mises à la disposition de tous;
- accorder un accès à:
 - des informations;
 - des espaces/zones/domaines;
 - des services;
 - des ressources;
- conclure des contrats.

Pour pouvoir obtenir le niveau de confiance nécessaire, il faut que le partenaire de communication puisse être clairement distingué des autres partenaires de communication possibles et que cette distinction puisse être réévaluée périodiquement en fonction des besoins.



X.1252(09)_FA2

NOTE 1 – Cette Figure montre le processus d'authentification unidirectionnel de base. En général, ce processus est exécuté mutuellement de manière parallèle ou entrelacée.
 NOTE 2 – Si aucun niveau de confiance n'est requis, l'étape 2 peut être sautée.
 NOTE 3 – Ce flux peut être exécuté plusieurs fois, à des instants et/ou en des endroits différents.
 NOTE 4 – L'intervention d'un tiers est subordonnée à la législation et aux politiques sur le respect de la vie privée et au consentement de la RE. (---)

Figure A.2 – Processus d'authentification unidirectionnel

En général, ce processus visant à obtenir la confiance (processus d'authentification) est réalisé mutuellement. Autrement dit, le processus d'authentification illustré sur la Figure A.2 est réalisé deux fois, chacune des entités remplissant chacun des rôles, à savoir:

Authentification de Y: l'entité Y est l'entité requérante (RE) et l'entité X la partie utilisatrice (RP)

Authentification de X: l'entité X est l'entité requérante et l'entité Y la partie utilisatrice.

Dans un souci de simplicité et de clarté, le processus d'authentification illustré sur la Figure A.2 est décrit dans un seul sens. Toutefois, les flux des deux processus sont entrelacés.

L'exécution entrelacée permet aux parties de vérifier les conditions préalables avant de présenter des attributs potentiellement confidentiels. Ces conditions peuvent être les suivantes:

- savoir comment s'adresser à la partie utilisatrice,
- avoir une confiance suffisante dans le fait que la partie utilisatrice est la bonne (les utilisateurs devraient par exemple être suffisamment sûrs d'être sur la bonne page web avant de saisir des informations d'identité telles que leur nom d'utilisateur et leur mot de passe).

Dans certains cas (mais pas dans les systèmes centrés sur l'utilisateur), un tiers pourrait intervenir directement pour fournir des informations complémentaires de preuve à la partie utilisatrice afin d'améliorer la confiance dans les attributs de l'entité requérante.

Les identités sont constituées d'attributs. Ceux-ci peuvent être quelque chose:

- que l'entité possède (par exemple une carte codée)
- que l'entité connaît (par exemple un mot de passe)
- qui caractérise l'entité (par exemple la couleur, la taille)
- que l'entité est capable de faire (par exemple chiffrement particulier)
- qui indique l'emplacement de l'entité
- qui est une combinaison des attributs précédents.

Pour contrôler les identités, on peut:

- vérifier la cohérence des informations proprement dites
- vérifier la cohérence avec d'autres informations justificatives
- faire une comparaison avec des informations déjà connues.

Les attributs peuvent aussi être spécifiés sous la forme d'un *profil d'identité*, qui est une expression structurée d'attributs d'une entité (par exemple le comportement d'une entité) qui pourrait être utilisée dans certains processus d'identification.

Il convient tout particulièrement de noter que, comme indiqué sur le diagramme de la Figure A.2, il appartient toujours à la partie utilisatrice de décider d'accepter ou non l'entité requérante sur la base du processus d'authentification. Personne d'autre ne peut prendre cette décision.

En général, chaque partenaire de communication devrait pouvoir fixer le niveau de confiance nécessaire pour permettre l'exécution des privilèges. Toutefois, ce droit peut être limité et, dans certains cas, doit être limité par la législation.

Lorsqu'il existe une asymétrie importante entre les partenaires de communication, le risque est que le partenaire le plus puissant abuse de la situation et demande un niveau de confiance insuffisamment élevé ou refuse sa propre authentification. Il est donc nécessaire que les mises en œuvre techniques des mécanismes d'authentification soient fondées sur des mécanismes symétriques pour éviter toute asymétrie. De plus, des réglementations pourraient être nécessaires pour éviter qu'une partie se trouve en position dominante et abuse de cette position dans les situations asymétriques.

En général, lors de l'application de la gestion d'identité, il faut avoir une idée très claire des entités impliquées et de leur finalité de manière à pouvoir limiter le contexte et les identités (ensemble d'attributs) à la finalité particulière.

En ce qui concerne le niveau de confiance aux seules fins de télécommunication, il suffit généralement que le client soit suffisamment sûr d'être raccordé au fournisseur de service ou de transport voulu et que les fournisseurs aient confiance dans le fait que l'utilisation des services est permise, peut être facturée et devrait être payée. La confiance dans le paiement peut par exemple être obtenue grâce à l'authentification d'un point d'accès ou d'un compte d'abonné, qui ne correspond pas nécessairement à l'utilisateur réel du service. Dans certains cas (cartes téléphoniques prépayées ou cartes SIM prépayées), aucune authentification ne sera nécessaire.

Pendant le processus d'authentification, un justificatif peut être présenté en tant que preuve d'une partie ou de la totalité des attributs d'une identité contextuelle présentée. Un *justificatif* est défini comme suit: ensemble de données présentées comme preuve d'une identité déclarée et/ou de droits. Toutefois, il est nécessaire de faire clairement la distinction entre deux types de justificatif:

- 1) un ensemble de données présentées comme preuve d'une identité déclarée, valable pour l'authentification (par exemple un passeport). Ce type de justificatif est utilisé pour accroître la confiance dans les attributs grâce à la confirmation par la partie qui délivre le justificatif; et
- 2) un ensemble de données présentées comme preuve de droits, valable uniquement pour l'autorisation (par exemple un billet pour assister à un concert ou à un match de football). Il permet l'exercice d'un privilège (par exemple être admis à une manifestation sur présentation d'un billet d'entrée) sans que l'identité de l'entité présentant le justificatif ne soit nécessairement révélée.

Certains justificatifs peuvent inclure les deux fonctions et les deux types de justificatif pourraient faire l'objet d'un processus d'authentification distinct.

A.2 Déclaration/assertion

Il est généralement convenu que les termes déclaration et assertion ont une signification relativement proche mais légèrement différente. Dans certains cas, on considère qu'une assertion est "plus forte" qu'une déclaration. Par exemple, le dictionnaire d'anglais d'Oxford définit une déclaration comme suit:

- a) affirmer être le cas, sans pouvoir fournir de preuve,
- b) affirmation que quelque chose est le cas,

et une assertion comme suit: affirmation certaine et vigoureuse. Toutefois, dans un contexte numérique, les termes "certaine" et "vigoureuse" n'ont pas vraiment de sens.

Dans les réseaux ouverts, la relation entre la partie qui fait une affirmation (c'est-à-dire qui présente des informations d'identité) et la partie qui se fie à cette affirmation sera plus complexe et ambivalente. Par conséquent, toute affirmation est supposée être douteuse et, en tant que telle, doit faire l'objet d'une vérification ou d'une demande de preuves supplémentaires. On ne peut pas partir de l'hypothèse que les déclarations et les assertions sont formulées avec quelque autorité que ce soit. Il appartiendra toujours à la partie utilisatrice de décider d'accepter ou non la déclaration ou l'assertion sur vérification par elle-même (ou par un vérificateur agissant à sa demande).

A.3 Inscription et enregistrement

L'inscription et l'enregistrement sont deux processus qui sont étroitement liés et qui se chevauchent. Les termes sont parfois utilisés de façon interchangeable et, même si une combinaison en une seule étape est possible, il s'agit en fait de deux processus distincts.

L'inscription est: le processus d'inauguration (d'établissement) d'une entité dans un contexte. L'inscription peut comprendre la vérification de l'identité de l'entité et l'établissement d'une identité contextuelle. L'enregistrement est: le processus par lequel une entité demande et se voit attribuer des privilèges pour utiliser un service ou une ressource. L'inscription est un préalable nécessaire à l'enregistrement.

Dans le monde réel, un utilisateur peut par exemple s'inscrire à un moment donné pour utiliser des services bancaires génériques puis s'enregistrer ultérieurement pour recevoir des services bancaires en ligne. Autre possibilité: à l'ouverture d'un nouveau compte, l'utilisateur peut remplir les formalités d'identification (et connexes) (c'est-à-dire s'inscrire) et, en même temps, s'enregistrer pour recevoir les services bancaires en ligne.

A.4 Fournisseur d'identité et fournisseur de service d'identité

Il est ressorti d'un examen des pratiques en vigueur que les termes *fournisseur d'identité* et *fournisseur de service d'identité* sont tous les deux couramment utilisés. Le terme *fournisseur d'identité* est employé dans certaines Recommandations UIT-T existantes, mais il pourrait être

interprété comme désignant une entité qui *fournit* des identités, et non comme une entité qui *gère* des identités. En outre, ce terme prête à confusion car les identités ne peuvent pas être fournies, elles existent, ou évoluent lorsque des attributs sont attribués. De plus, le terme *fournisseur de service* est largement utilisé dans des expressions comme fournisseur de service de vérification, fournisseur de service de justificatif, fournisseur de service financier, etc.

Le terme *fournisseur de service d'identité* est donc considéré comme étant un peu plus descriptif que le terme *fournisseur d'identité* et devrait être le terme préféré. Il a été possible de tenir compte de cette modification sans trop de répercussions sur les documents existants: la définition actuelle de *fournisseur d'identité* est utilisée pour le *fournisseur de service d'identité* et le terme *fournisseur d'identité* est conservé mais, au lieu de le définir, on renvoie simplement au *fournisseur de service d'identité*. L'acronyme devrait être IdSP.

A.5 Profil d'identité

En général, les profils sont considérés comme des informations constatées et reconnues et desquelles il est possible de dégager une structure ou qui correspondent à une structure déjà établie. Ainsi, un profil d'identité peut être considéré comme des informations qui caractérisent une entité, sont constatées ou reconnues et desquelles il est possible de dégager une structure ou qui correspondent à une structure déjà établie.

Dans les dictionnaires, on trouve notamment les deux définitions suivantes du terme *profil*: "forme, ordre ou disposition régulier (-ère) ou répétitif (-ive) " et "modèle fiable de traits, d'actes, de tendances ou d'autres caractéristiques susceptibles d'être observées chez une personne, dans un groupe ou une institution".

La conception générale et les définitions du terme profil indiquées ci-dessus impliquent que le profil comporte plus d'un élément mais la répétition d'un seul attribut dans le temps constitue également un profil. La présence unique d'un seul attribut ne constituerait pas un profil mais la manière dont apparaissent un ou plusieurs attributs peut former un profil. De plus, un profil d'identité peut reposer sur plus d'une activité ou d'un comportement et n'est pas limité à des informations constatées et reconnues, mais peut être fondé sur n'importe quel(s) attribut(s). Par exemple, le profil d'un pneu a une structure claire et décelable, ainsi, dans ce cas, l'attribut lui-même peut être considéré comme profil d'identité. Il n'est pas non plus nécessaire qu'un profil soit constaté à plusieurs reprises pour être utile. Par exemple, lorsque deux personnes parlent d'une voiture mise en exposition chez un concessionnaire, ils peuvent l'identifier et la désigner de la manière suivante: "Celle qui est exposée dans le coin, derrière à gauche".

Les profils peuvent être réutilisables mais on pourrait également envisager des situations où ils ne sont employés qu'une seule fois, comme les codes à usage unique.

Si d'aucuns affirment que tous les attributs ont en quelque sorte une structure, il existe néanmoins une différence nette entre attributs et profils d'identité, en ce sens qu'une structure qui est décelée et déduite par l'observateur n'est pas nécessairement connue d'autres entités, même des entités observées.

Les profils d'identité peuvent non seulement servir à des fins d'identification mais également, dans certains cas, à des fins d'authentification ou simplement à répartir les entités en catégories ou les classer, par exemple lorsque le comportement des consommateurs fait l'objet d'une étude attentive visant à déterminer quels types de produits ils achètent et à quelle fréquence. Dans un contexte de "marketing" comme celui-là, les profils permettent de classer des entités par rapport à certains groupes d'entités, mais en combinant plusieurs de ces profils, ceux-ci pourraient conduire à l'identification d'entités isolées.

Les éléments utilisés pour identifier une entité doivent être suffisants pour pouvoir la distinguer dans un contexte. Si un profil d'identité doit être utilisé à des fins d'identification ou d'authentification individuelle (et non d'un groupe), alors il doit être unique et sans ambiguïté.

Toutefois, dans certains cas, par exemple lorsque le profil d'identité sert à des fins d'autorisation, il ne doit pas nécessairement être unique ou sans ambiguïté. Par exemple, lorsqu'il est nécessaire de limiter l'utilisation d'un service donné, comme dans le cas de la participation à des compétitions sportives, il peut être nécessaire d'appliquer des restrictions, fondées par exemple sur le comportement ou la consommation de certains médicaments.

Bibliographie

Cette liste de termes et définitions dans le domaine de la gestion d'identité a été établie sur la base d'un grand nombre de publications, de travaux et de glossaires existants dans ce domaine. Loin d'être exhaustive, la liste des sources comprend notamment:

- [b-ISO/IEC CD 2382-37] ISO/IEC CD 2382-37, *Information technology – Vocabulary – Part 37: Harmonized biometric vocabulary.*
- [b-ANSI] American National Standards Institute.
<http://www.ansi.org/>
- [b-AusCert] AusCert Conference 2005.
- [b-Carnegie] Carnegie Mellon® Computing Services.
www.cmu.edu/acs/documents/idm/
- [b-NSS] Committee on National Security Systems Glossary Working Group
- [b-Edentity] Edentity <http://www.edentity.co.uk/>.
- [b-ETSI] ETSI Terms and Definitions Database Interactive.
<http://webapp.etsi.org/Teddi/>
- [b-EU] EU Commission eGovernment Unit DG Information Society and Media.
- [b-ICANN] ICANN.
<http://www.icann.org/en/general/glossary.htm>
- [b-Identity] Identity Commons.
http://wiki.idcommons.net/Main_Page
- [b-IETF] IETF Trust (2007) Network Working Group.
- [b-ISO/IEC] ISO/IEC JTC 1/SC 27/WG5.
- [b-UIT-T Gestion d'identité] Groupe spécialisé sur la gestion d'identité de l'UIT-T.
- [b-UIT-T Termes] Base de données des termes et définitions de l'UIT-T.
<http://www.itu.int/ITU-T/dbase>
- [b-Cameron] Kim Cameron's Laws of Identity.
<http://www.identityblog.com/?p=354>
- [b-Liberty] Liberty Alliance Technical Glossary.
- [b-Modinis] Modinis.
<https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/bin/view.cgi/Main/WebHome>
- [b-NetMesh] NetMesh® Inc.
<http://www.netmesh.us/>
- [b-NIST] National Institute of Standards and Technology.
<http://www.nist.gov/index.html>
- [b-OASIS] OASIS.
<http://www.oasis-open.org/committees/security/ipr.php>
- [b-OED] Oxford English Dictionary.
- [b-OECD] Recommandation de l'OCDE sur l'authentification électronique.

- [b-Mobile] Open Mobile Alliance™.
<http://www.openmobilealliance.org/UseAgreement.html>
- [b-STORK] STORK-eID Consortium.
http://www.eid-stork.eu/index.php?option=com_frontpage&Itemid=1
- [b-Trusted] Trusted Computing Group.
<http://www.trustedcomputinggroup.org/>
- [b-IAAC] UK Information Advisory Council.
<http://www.iaac.org.uk/Default.aspx?tabid=1>

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