Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1252

(04/2021)

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

Sécurité du cyberespace – Gestion d'identité

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 (1)	
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 (1)	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 spam	X.1230–X.1249
Gestion des identités	**X.1250–X.1279**
APPLICATIONS ET SERVICES SÉCURISÉS (2)	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1319
Sécurité des réseaux électriques intelligents	X.1330–X.1339
Courrier certifié	X.1340–X.1349
Sécurité de l'Internet des objets (IoT)	X.1360–X.1369
Sécurité des systèmes de transport intelligents	X.1370–X.1389
Sécurité de la technologie des registres distribués	X.1400–X.1429
Sécurité de la technologie des registres distribués	X.1430–X.1449
Protocoles de sécurité (2)	X.1450–X.1459
ECHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Échange concernant les vulnérabilités/les états	X.1520–X.1539
Échange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Échange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Échange garanti	X.1580–X.1589
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	
Aperçu de la sécurité de l'informatique en nuage	X.1600–X.1601
Conception de la sécurité de l'informatique en nuage	X.1602–X.1639
Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage	X.1640–X.1659
Mise en œuvre de la sécurité de l'informatique en nuage	X.1660–X.1679
Sécurité de l'informatique en nuage (autres)	X.1680–X.1699
COMMUNICATIONS QUANTIQUES	
Terminologie	X.1700–X.1701
Générateur quantique de nombres aléatoires	X.1702–X.1709
Cadre de sécurité pour les réseaux QKDN	X.1710–X.1711
Conception de la sécurité pour les réseaux QKDN	X.1712–X.1719
Techniques de sécurité pour les réseaux QKDN	X.1720–X.1729
SÉCURITÉ DES DONNÉES	
Sécurité des mégadonnées	X.1750–X.1759
SÉCURITÉ DE LA 5G	X.1800–X.1819

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 Recommandation UIT-T X.1252 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. La Recommandation UIT-T X.1252 contient une annexe dans laquelle figurent des explications relatives à certains de ces termes clés.

L'un des principaux objectifs de la Recommandation UIT-T X.1252 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

Édition	Recommandation	Approbation	Commission d'études	Identifiant unique*
1.0	UIT-T X.1252	16-04-2010	17	11.1002/1000/10440
2.0	UIT-T X.1252	30-04-2021	17	11.1002/1000/14642

* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique, par exemple http://handle.itu.int/11.1002/1000/11830-en.

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 on 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.

À 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 ou par des droits d'auteur afférents à des logiciels, et dont l'acquisition pourrait être requise 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 responsables de la mise en œuvre de consulter les bases de données appropriées de l'UIT-T disponibles sur le site web de l'UIT-T à l'adresse http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Recommandation UIT-T X.1252

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

1 Domaine d'application

La présente Recommandation définit un ensemble de base de termes couramment utilisés dans le domaine de la gestion d'identité (IdM). Elle donne des définitions de base des termes, 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.

Néant.

3 Définitions

La liste de l'ensemble des termes et définitions dans le domaine de la gestion d'identité (IdM) figure dans le paragraphe 6.

4 Abréviations et acronymes

Les abréviations et les acronymes ci-après sont utilisés dans la présente Recommandation:

CID identificateur cryptographique (*cryptographic identifier*)

DDO descripteur d'objet DID (*DID object descriptor*)

DID identificateur décentralisé *(decentralized identifier)*

DLT technologie des registres distribués *(distributed ledger technology)*

ID identificateur (*identifier*)

IdM gestion d'identité (*identity management*)

IdP fournisseur d'identité (*identity provider*)

IdSP fournisseur de services d'identité (*identity service provider*)

IH plate-forme d'identité (*identity hub*)

PII informations d'identification personnelle (*personally identifiable information*)

PKI infrastructure de clé publique *(public key infrastructure)*

RA autorité d'enregistrement (*registration authority*)

RE entité requérante (*requesting entity*)

RP partie utilisatrice (*relying party*)

SIM module d'identification de l'abonné (*subscriber identity module*)

SSI identité auto-souveraine *(self-sovereign identity)*

URL localisateur uniforme de ressource *(uniform resource locator)*

ZKP justificatif à apport nul de connaissance (*zero-knowledge proof*)

5 Conventions

Néant.

6 Termes et définitions

6.1 contrôle d'accès (*access control*): procédure par laquelle un administrateur peut restreindre l'accès à des ressources, fonctionnalités, services ou informations, compte tenu des règles préétablies et des droits spécifiques ou de l'autorité associés à l'entité requérante.

6.2 adresse (*address*): une adresse identifie un point de terminaison de réseau particulier et peut être utilisée pour le routage jusqu'à ce point de terminaison physique et logique à l'intérieur d'un réseau public ou privé.

NOTE – Sur la base de la Recommandation [b-UIT-T E.101].

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 détermine leurs relations et la manière dont elles effectuent conjointement des activités.

6.5 anonyme (*anonym*): identifiant utilisé exactement une fois.

6.6 anonymat (*anonymity*): situation dans laquelle une entité ne peut pas être identifiée parmi un ensemble d'entités.

NOTE – L'anonymat permet d'empêcher le suivi, le traçage et la prise d'empreintes digitales d'entités ou de leur comportement (emplacement de l'utilisateur et fréquence d'utilisation d'un service, par exemple).

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

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

6.8 garantie (*assurance*)

NOTE – Voir garantie d'authentification et garantie d'identité.

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

6.10 attribut (*attribute*): information liée à une entité qui en indique une caractéristique.

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

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

6.13 authentification (*authentication*) [b-ISO/CEI 24760-1]: processus formalisé de vérification qui, s'il est concluant, aboutit à une identité authentifiée pour une entité.

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

6.14 garantie d'authentification (*authentication assurance*): accusé de réception positif dans le processus d'authentification, qui vise à donner l'assurance que le partenaire de communication est l'entité qu'il déclare être ou qu'il est censé être.

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

6.15 autorisation (*authorization*): octroi de droits et octroi d'accès sur la base de ces droits.

NOTE – Sur la base de la Recommandation [b-UIT-T X.800].

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

6.17 reconnaissance biométrique; biométrie (*biometric recognition; biometrics*) [b-ISO/CEI 2382-37]: reconnaissance automatisée des personnes physiques fondée sur leurs caractéristiques biologiques et comportementales.

6.18 certificat (*certificate*): 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.

NOTE – Sur la base de la définition de "certificat de sécurité" dans la Recommandation [b-UIT-T X.810].

6.19 déclaration (*claim*): assertion numérique concernant des attributs d'identité faite par une entité sur elle-même ou sur une autre entité. Fait d'affirmer être le cas, sans pouvoir fournir de preuve.

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

6.20 déclarant (*claimant*): entité qui est ou représente une entité principale à des fins d'authentification.

NOTE 1 – Un déclarant comporte les fonctions nécessaires pour engager des échanges pour authentification au nom d'une entité principale.

NOTE 2 – Sur la base de la Recommandation [b-UIT-T X.811].

6.21 définition de la déclaration (*claim definition*): définition lisible par machine de la structure sémantique d'une déclaration.

NOTE – Les définitions de déclarations facilitent l'interopérabilité des déclarations et des preuves entre plusieurs émetteurs, détenteurs et parties utilisatrices.

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

6.23 corrélation (*correlation*): combinaison de divers éléments d'information qui sont liés à une entité ou deviennent liés à une entité lorsqu'ils sont combinés.

NOTE – La corrélation est étroitement associée à l'identification. Elle peut faciliter l'identification et la déduction d'informations sur une entité qui ne sont pas directement fournies par les données fournies.

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

NOTE – La publication [b-ISO/CEI 29115] est analogue à la Recommandation [b-UIT-T X.1254] et contient la même définition du justificatif que celle qui a été élaborée par les groupes concernés.

6.25 réduction des données au minimum (*data minimization*): consiste à limiter la collecte, le stockage et l'utilisation des identificateurs, des attributs et des autres données associées à une entité à ce qui est strictement nécessaire pour procéder à l'authentification et à limiter tout échange et toute divulgation de données associées à une entité, y compris les informations contextuelles d'une demande, à ce qui est strictement nécessaire pour répondre à la demande et uniquement à la partie utilisatrice associée à la demande.

6.26 identificateur décentralisé (DID, *decentralized identifier*): identificateur unique à l'échelle mondiale ne nécessitant pas d'autorité centrale d'enregistrement, étant donné qu'il est enregistré avec

la technologie des registres distribués ou une autre forme de réseau décentralisé. Un identificateur DID est associé à un descripteur d'objet DID.

NOTE – Voir [b-W3C-DIDs].

6.27 descripteur d'objet DID (DDO, *DID object descriptor*): ensemble de données décrivant le sujet de l'identificateur décentralisé (DID), y compris les mécanismes, tels que les clés publiques de chiffrement, que le sujet du DID ou un délégué du DID peut utiliser pour s'authentifier et justifier qu'il y a correspondance avec le DID.

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

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

6.30 registre distribué (*distributed ledger*) [b-UIT-T X.1400]: type de registre qui est partagé, dupliqué et synchronisé de manière distribuée et décentralisée.

6.31 système de gestion des clés décentralisé (*decentralized key management system*): norme applicable à la gestion des clés de chiffrement interopérable sur la base d'identificateurs décentralisés.

6.32 domaine (*domain*): environnement dans lequel une entité peut utiliser un ensemble d'attributs à des fins d'identification notamment.

NOTE – Un domaine fournit un contexte.

6.33 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.

6.34 entité (*entity*): élément qui a une existence séparée et distincte et peut être identifié dans un contexte.

NOTE 1 – Une entité peut avoir une représentation physique ou logique.

NOTE 2 – 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, et d'interfaces.

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

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

6.36 fédération (*federation*): [b-UIT-T Y.2720]: établissement d'une relation entre deux entités ou plus, ou d'une association comprenant un nombre quelconque de fournisseurs de services et de fournisseurs d'identité.

6.37 détenteur (*holder*): entité qui a reçu une déclaration d'un émetteur. Si la déclaration prend en charge les justificatifs à apport nul de connaissance, le détenteur est également le démonstrateur.

6.38 identification (*identification*) [b-ISO/CEI 24760-1]: processus de reconnaissance d'une entité dans un domaine particulier, par opposition à d'autres entités.

6.39 identificateur (ID, *identifier*) [b-UIT-T E.101]: série de chiffres, caractères et symboles utilisés pour identifier de manière univoque un abonné, un utilisateur, un élément de réseau, une fonction, une entité de réseau, un service ou une application. Les identificateurs peuvent être utilisés pour l'enregistrement ou l'autorisation. Ils peuvent être publics pour tous les réseaux ou privés pour un réseau particulier (les identificateurs privés ne sont en principe pas divulgués à des tiers).

NOTE – Un identificateur peut être un attribut spécialement créé avec une valeur attribuée de façon à être unique dans le domaine.

6.40 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, 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.

6.41 garantie d'identité (*identity assurance*): garantie donnée 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.

6.42 politique de sécurité fondée sur l'identité (*identity based security policy*) [b-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.

6.43 gestion d'identité (IDM, *identity management*): 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); garantir l'identité d'une entité; et permettre des applications commerciales et de sécurité.

NOTE – Sur la base de la Recommandation [b-UIT-T Y.2720].

6.44 propriétaire d'identité (*identity owner*): entité qui peut être tenue responsable. Le propriétaire d'identité doit être un particulier ou une organisation. S'exclut mutuellement avec une chose.

6.45 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.

6.46 contrôle d'identité (*identity proofing*) [b-ISO/CEI 29115]: procédure au moyen de laquelle l'autorité d'enregistrement (RA) recueille et contrôle un nombre suffisant d'informations pour identifier une entité à un niveau de garantie spécifié ou convenu.

6.47 fournisseur d'identité (IdP, *identity provider*)

NOTE – Voir fournisseur de service d'identité (IdSP).

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

6.49 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.

6.50 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.

6.51 indépendant (*independent*): individu qui contrôle directement la (les) clé(s) privée(s) et le(s) secret(s) maître(s) nécessaires à l'administration d'une identité décentralisée.

6.52 individu (*individual*): propriétaire de l'identité qui est une personne physique. S'exclut mutuellement avec l'organisation.

6.53 émetteur (*issuer*): entité qui émet une déclaration.

6.54 clé de l'émetteur (*issuer key*): type spécial de clé de chiffrement nécessaire pour qu'un émetteur puisse émettre une déclaration qui prend en charge les justificatifs à apport nul de connaissance.

6.55 porte-clés (*key-chain*): tâche de sécurisation du stockage de clés privées ou de données sur une unité matérielle de confiance dans un dispositif.

6.56 identité légale (*legal identity*): ensemble d'informations suffisantes pour identifier un propriétaire d'identité aux fins de la responsabilité juridique dans au moins une juridiction. Pour les besoins d'un réseau provisoire, une identité légale peut être établie par rapport à une ou plusieurs ressources web accessibles au public, telles que des sites web, des blogs, des profils sur les réseaux sociaux ou d'autres pages web qui fournissent des informations suffisantes pour répondre à ce critère.

6.57 associabilité (*linkability*): capacité de déterminer, dans un ensemble d'informations, si deux ou plusieurs attributs, identificateurs, identités ou autres données sont associés avec un degré de probabilité suffisamment élevé pour être utiles.

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

NOTE – Comparer avec assertion.

6.59 authentification mutuelle (*mutual authentication*) [b-ISO/CEI 29115]: authentification des identités d'entités, qui donne à chacune des deux entités une garantie quant à l'identité de l'autre.

6.60 nom (*name*): combinaison de caractères servant à identifier des entités (par exemple un abonné, un élément de réseau) et pouvant être résolu ou traduit en une adresse. Les caractères peuvent être des chiffres, des lettres ou des symboles.

NOTE 1 – 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.

NOTE 2 – Sur la base de la Recommandation [b-UIT-T E.101].

6.61 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.

6.62 profil (*pattern*)

NOTE – Voir profil d'identité.

6.63 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.

6.64 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.

6.65 entité principale (*principal*): entité dont l'identité peut être authentifiée.

NOTE – Cette entrée figure dans les Recommandations [b-UIT-T X.811], [b-UIT-T Y.2702] et [b-UIT-T Y.2720].

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

6.67 clé privée (*private key*) [b-UIT-T X.509]: (dans un système de chiffrement avec clé publique) celle des clés d'une paire de clés d'une entité qui est connue uniquement par l'entité concernée.

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

6.69 preuve (*proof*): vérification par chiffrement d'une déclaration. Une signature numérique est une forme simple de preuve. Un hachage cryptographique est également une forme de preuve. Il existe deux types de preuves: transparentes ou à apport nul de connaissance. Les preuves transparentes révèlent toutes les informations contenues dans une déclaration. Les justificatifs à apport nul de connaissance permettent une divulgation sélective des informations contenues dans une déclaration.

6.70 démonstrateur (*prover*): entité qui émet une preuve d'une déclaration. Le démonstrateur est également le détenteur de la déclaration.

6.71 pseudonyme (*pseudonym*) [b-ISO/CEI 24760-1]: identificateur qui contient les informations d'identité minimales suffisantes pour permettre à un vérificateur de l'établir comme lien avec une identité connue.

NOTE 1 – Un pseudonyme peut être un identificateur dont la valeur est choisie par la personne ou attribuée de manière aléatoire.

NOTE 2 – Un pseudonyme peut permettre d'éviter ou de réduire les risques en matière de confidentialité et de sécurité associés à l'utilisation de liens d'identification susceptibles de divulguer l'identité de l'entité.

6.72 données publiques (*public data*) [b-UIT-T L.1410]: données à disposition du public dont l'accès n'est pas limité à des membres ou par un accord de confidentialité, ou pour d'autres motifs semblables.

6.73 clé publique (*public key*) [b-UIT-T X.509]: celle des clés d'une paire de clés d'une entité qui est connue du public.

6.74 profil public (*public profile*): informations décrivant un fournisseur de services, y compris son identité juridique, son ou ses logos ou autres marques commerciales, son ou ses emplacements, ses informations commerciales, ses liens Internet et toute autre information requise par le cadre de confiance pour garantir une parfaite transparence concernant l'identité juridique et les qualifications du fournisseur.

6.75 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.

6.76 partie utilisatrice (RP, *relying party*): entité qui est tributaire d'une représentation ou d'une déclaration d'identité soumise par une entité requérante ou assertante dans un contexte de demande donné.

NOTE – Sur la base de la Recommandation [b-UIT-T Y.2720].

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

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

6.79 révocation (*revocation*): annulation de quelque chose qui a été fait précédemment par quelqu'un ayant l'autorité nécessaire.

6.80 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.

6.81 audit de sécurité (*security audit*) [b-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.

6.82 domaine de sécurité (*security domain*): 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.

NOTE – Sur la base de la Recommandation [b-UIT-T X.810]. Des définitions semblables figurent dans les Recommandations [b-UIT-T Y.2701] et [b-UIT-T Y.2720].

6.83 zone de sécurité (*security zone*): zone protégée caractérisée par son contrôle opérationnel, son emplacement et sa connectivité aux autres dispositifs ou éléments de réseau.

NOTE – Sur la base de la Recommandation [b-UIT-T Y.2701].

6.84 autorité de domaine de sécurité (*security domain authority*) [b-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.

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

6.86 chose (*thing*): entité qui ne peut être tenue légalement responsable. Une chose peut être un animal (par exemple, un animal de compagnie, du bétail), un objet naturel (par exemple, une maison, une voiture, un téléphone) ou un objet numérique (par exemple, un programme logiciel, un service de réseau, une structure de données). S'exclut mutuellement avec le propriétaire de l'identité.

6.87 confiance (*trust*): confiance d'une partie ou d'une entité dans le fait qu'une autre partie ou entité se comportera d'une manière bien définie et sans enfreindre les règles, les politiques ou les clauses juridiques convenues du système de gestion d'identité.

6.88 ancre de confiance (*trust anchor*): propriétaire d'identité qui peut servir de point de départ dans le web de confiance décentralisé. Une ancre de confiance possède deux privilèges spécifiques, qui consistent:

- à ajouter de nouveaux propriétaires d'identité dans le réseau; et
- à envoyer des invitations de l'ancre de confiance.

Une ancre de confiance doit remplir les conditions requises pour devenir une ancre de confiance et souscrire aux obligations de l'ancre de confiance définies dans le cadre de confiance. Tous les administrateurs et gestionnaires sont automatiquement des ancres de confiance.

6.89 cadre de confiance (*trust framework*): ensemble de spécifications, règles et accords ayant force exécutoire présidant à un système de gestion des identités.

NOTE – Sur la base de [b-OIX-TFIS].

6.90 tiers de confiance (*trusted third party*): 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.

NOTE 1 – Sur la base des Recommandations [b-UIT-T X.810] et [b-UIT-T Y.2702].

NOTE 2 – Voir la Recommandation [b-UIT-T X.800].

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

6.92 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.

6.93 centré sur l'utilisateur (*user-centric*): système de gestion d'identité qui confère à l'utilisateur la capacité de contrôler et d'appliquer diverses politiques régissant les données des utilisateurs, y compris les informations d'identification personnelle.

6.94 nœud de validation (*validator node*): nœud qui valide les nouvelles transactions des dossiers d'identité et écrit activement les transactions valides dans le registre distribué en utilisant le protocole de consensus du registre distribué.

6.95 déclaration vérifiable (*verifiable claim*): déclaration qui comprend une preuve de l'émetteur. Cette preuve se présente généralement sous la forme d'une signature numérique. Une déclaration vérifiable peut être vérifiée par une clé publique associée à l'identificateur décentralisé de l'émetteur.

NOTE – Sur la base de [b-W3C-VC].

6.96 vérification (*verification*) [b-ISO/CEI 24760-1]: processus consistant à établir que les informations relatives à l'identité associées à une entité donnée sont correctes.

NOTE 1 – Le processus d'identification applique la vérification aux attributs déclarés ou observés.

NOTE 2 – 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.

NOTE 3 – Les informations sont correctes au moment de la vérification.

6.97 vérificateur (*verifier*) [b-ISO/CEI 24760-1]: entité qui effectue la vérification.

6.98 portefeuille (portefeuille d'identité) (*wallet (identity wallet)*): application qui permet essentiellement à un utilisateur de détenir des identifiants et des justificatifs en stockant les clés privées correspondantes sur le dispositif de l'utilisateur.

6.99 justificatif à apport nul de connaissance (ZKP, *zero knowledge proof*): justificatif utilisant une cryptographie particulière et un secret maître pour autoriser la divulgation sélective d'information dans un ensemble de déclarations. Un justificatif ZKP prouve qu'une partie ou la totalité des données d'un ensemble de déclarations est vraie sans révéler d'informations additionnelles, y compris l'identité du démonstrateur.

NOTE 1 – La notion de "divulgation sélective" implique un large éventail de choix en matière de divulgation. Par exemple, les justificatifs ZKP peuvent être utilisés pour prouver de nombreuses déclarations concernant des données confidentielles, telles que: 1) l'âge adulte, sans révéler la date de naissance; 2) la solvabilité (ne pas être en faillite), sans indiquer la composition du portefeuille; 3) la propriété d'un actif, sans révéler des transactions antérieures ou établir des liens avec de telles transactions.

NOTE 2 – Sur la base de la Recommandation [b-UIT-T X.1403].

Annexe A

Terminologie de base de la gestion d'identité: éléments fondamentaux et explications

(Cette Annexe fait partie intégrante de la présente Recommandation.)

Contexte

Les discussions sur l'IdM ont fait apparaître des différences de compréhension suivant les personnes quant à son objet, aux procédures de base utilisées ainsi qu'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 l'IdM.

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 et le comportement. On peut aussi utiliser la date de naissance, le lieu de naissance, l'adresse du domicile et 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, RE) et l'entité qui utilisera une identité confirmée (partie utilisatrice, RP), une troisième entité qui gère les identités (fournisseur de service d'identité, IdSP) 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 (ID) 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. Ce paragraphe 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 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 1 – Une entité peut avoir une représentation physique ou logique.

NOTE 2 – 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 et d'interfaces.

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.

Étant 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 dans un domaine particulier, par opposition à d'autres entités.

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.

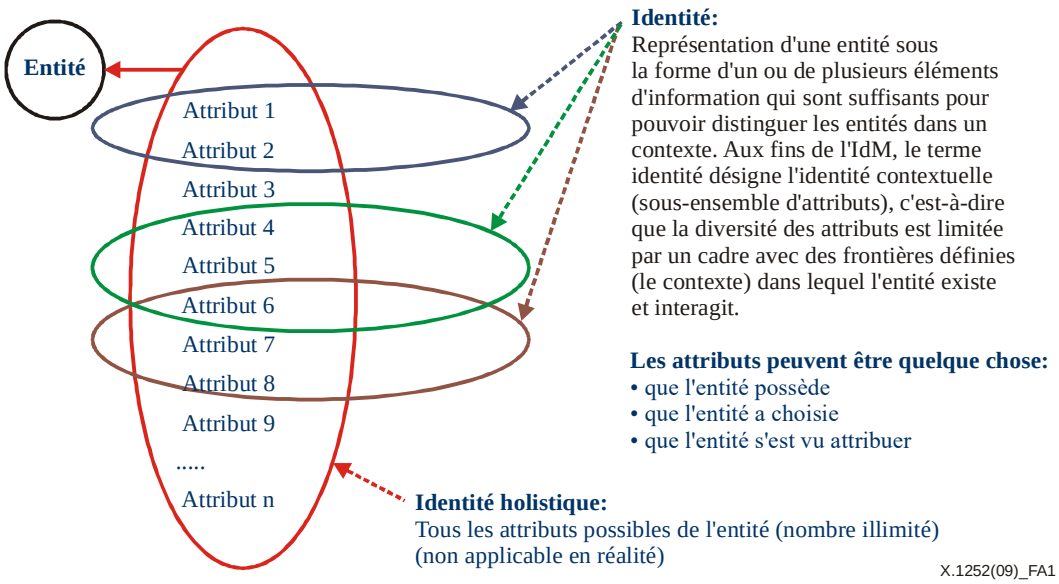


Figure A.1 – Relations entre entité, identités et attributs

Comme nous l'avons déjà indiqué, l'authentification est importante dans le cadre de l'IdM. 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 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:

- 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, des zones ou des 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.

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 RE et l'entité X la partie RP.

Authentification de X: l'entité X est l'entité RE et l'entité Y la partie RP.

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 RP;

- avoir une confiance suffisante dans le fait que la partie RP 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).

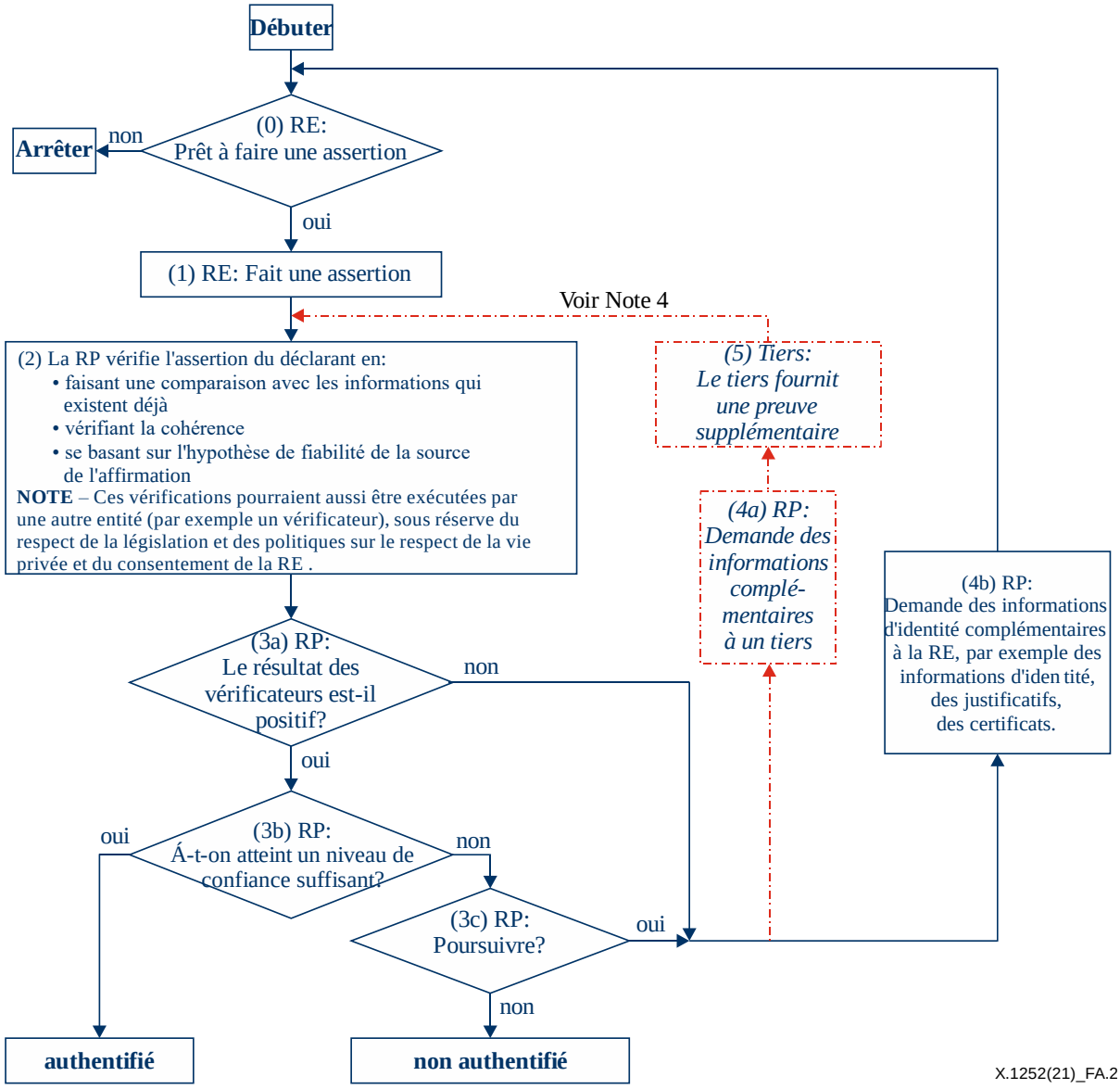
Dans certains cas (mais pas dans les systèmes centrés sur l'utilisateur), un tiers pourrait intervenir directement pour fournir des informations complémentaires de preuve à la partie RP afin d'améliorer la confiance dans les attributs de l'entité RE.

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 un 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.



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 v ie privée et au consentement de la RE. (_ . _ . _ . _)

Figure A.2 – Processus d'authentification unidirectionnel

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 RP de décider d'accepter l'entité RE 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 l'IdM, 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 (module d'identification de l'abonné) 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.

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 ou 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, une déclaration peut être définie comme suit:

a) fait d'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 adjectifs "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 RP de décider d'accepter 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 (IdP) et fournisseur de service d'identité (IdSP) sont tous les deux couramment utilisés. Le terme fournisseur IdP 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, ou encore fournisseur de service financier.

Le terme fournisseur IdSP est donc considéré comme étant un peu plus descriptif que le terme fournisseur IdP 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 IdP est utilisée pour le fournisseur IdSP et le terme fournisseur IdP est conservé mais, au lieu de le définir, on renvoie simplement au fournisseur 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.

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 en former un. 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 de consommation de certains médicaments.

Annexe B

Terminologie de base de la gestion d'identité décentralisée: éléments fondamentaux et explications

(Cette Annexe fait partie intégrante de la présente Recommandation.)

B.1 Identité décentralisée

Les modèles d'identité présentés dans l'Annexe A sont centrés sur le fournisseur IdP. Selon le modèle, on suppose que les utilisateurs s'appuient sur les fournisseurs IdP pour établir, renforcer et fournir les identités qu'ils utiliseront dans leurs interactions en ligne. Cette approche centrée sur le fournisseur IdP exige que les utilisateurs fassent confiance aux fournisseurs IdP pour ce qui est de leur identité. Selon cette approche centrée sur le fournisseur IdP, les services de la fédération sont offerts par les fournisseurs IdP pour la réutilisation de l'identité. La possibilité de réutiliser l'identité d'un utilisateur est limitée par les membres de la fédération. La fédération d'identité place les fournisseurs au centre de la confiance, en privilégiant la protection de leur modèle économique par opposition à la mise en place d'un véritable système décentralisé d'écho d'identité qui permet aux utilisateurs de s'occuper de leur identité et de leurs relations. Le modèle d'identité centré sur le fournisseur IdP exige une confiance implicite dans les fournisseurs IdP centralisés. À ce titre, le modèle n'est ni souple, ni dynamique.

D'autre part, dans le modèle d'identité décentralisé, le système permet aux utilisateurs de contrôler leur propre identité. Selon l'approche décentralisée, les fournisseurs s'attachent essentiellement à valider des déclarations concernant des identités spécifiques. Les modèles d'identité décentralisés découlent de l'évolution actuelle des technologies des registres distribués (DLT).

Afin de permettre des services dans les domaines participants, les modèles d'identité centralisés s'emploient essentiellement à fournir des services d'authentification dans un domaine, pour permettre l'accès à un autre domaine par des ponts de fédération d'identité. Dans les interactions en ligne, les systèmes fondés sur l'identité sont incités à confirmer l'identité déclarée de l'entité, au lieu de fournir un contrôle d'accès. Ainsi, l'une des principales fonctions des systèmes d'identité décentralisés consiste à proposer un modèle permettant de fournir des assertions sur l'identité d'un utilisateur qui peuvent aisément être utilisées par tous les fournisseurs.

Un modèle d'identité centré sur l'utilisateur comprend un contrôle individuel ou administratif sur plusieurs domaines d'identité, sans qu'il soit nécessaire de recourir à une fédération agissant comme un cercle de confiance. L'identité centrée sur l'utilisateur vise à créer une identité en ligne persistante pour une entité qui a essentiellement pour but d'offrir une meilleure expérience en ligne, tout en permettant aux utilisateurs de mieux contrôler leur identité grâce à l'utilisation de modèles de confiance décentralisés. Cependant, en raison du manque de simplicité et de l'absence de technologies telles que les technologies DLT, le modèle centré sur l'utilisateur n'a pas donné de bons résultats.

Le concept d'identité centrée sur l'utilisateur se développe depuis la mise en œuvre des technologies DLT. Une pile de protocoles, qui s'appuie sur les technologies DLT pour permettre la mise en place d'une véritable infrastructure d'identité décentralisée, est en cours d'élaboration. Ces systèmes peuvent s'appuyer sur des technologies DLT publiques, privées, sans autorisation ou autorisées, afin de permettre la gestion des identités numériques. L'objectif est de transférer aux utilisateurs le contrôle des assertions d'identité, tout en maintenant la sécurité, l'intégrité et la confidentialité du système.

B.2 Modèle d'identité décentralisé

L'identité décentralisée est un modèle qui favorise le contrôle individuel (avec possibilité de déléguer le contrôle) entre un nombre quelconque d'autorités (y compris les fournisseurs IdP). L'identité

auto-souveraine (SSI) est un modèle spécifique d'identité décentralisée qui repose sur les hypothèses présentées dans le Tableau B.1:

Tableau B.1 – Hypothèses de l'identité auto-souveraine

Existence	Les utilisateurs doivent avoir une existence indépendante
Contrôle	Les utilisateurs doivent contrôler leur identité
Accès	Les utilisateurs doivent avoir accès à leurs propres données
Transparence	Les systèmes et les algorithmes doivent être transparents
Persistance	Les identités doivent avoir une longue durée de vie
Portabilité	Les informations et les services relatifs à l'identité doivent être transportables
Interopérabilité	Les identités devraient être aussi largement utilisables que possible
Consentement	Les utilisateurs doivent approuver l'utilisation de leur identité
Minimisation	La divulgation des déclarations doit être réduite au minimum
Protection	Les droits des utilisateurs doivent être protégés

Les aspects souhaités sont tout à fait conformes à ce que la technologie DLT peut offrir. Les mises en œuvre de l'identité décentralisée sont généralement fondées sur des déclarations et des attestations dans lesquelles les acteurs peuvent souvent jouer différents rôles.

Les systèmes d'identité décentralisés peuvent servir à faciliter les transactions en ligne fiables. Ils permettent aux utilisateurs de donner à un fournisseur de services des preuves des attributs sur eux-mêmes (ou vice versa) par le biais de l'utilisation de déclarations vérifiables (attestations). L'ensemble du processus peut être effectué de manière interopérable et fiable grâce à l'utilisation d'une pile technologique qui permet la diffusion de déclarations fiables, sans qu'il soit nécessaire d'établir des relations directes entre les participants à la transaction.

Dans un système d'identité décentralisé, le fournisseur de services agit comme une partie RP, tandis que les déclarations sont fournies par un émetteur d'attestations, qui délivre les attestations manquantes requises. Une attestation est un ensemble de déclarations sur l'exactitude d'un autre ensemble de déclarations. L'ensemble de déclarations initiales peut également être désigné par le terme "déclaration". Le destinataire d'une attestation devrait être en mesure de valider l'engagement de l'attestation à l'égard des déclarations. L'engagement devrait donc prendre la forme d'une signature numérique ou d'un pointeur vers des données dans un registre distribué.

L'identification des nœuds du réseau s'effectue au moyen d'identificateurs décentralisés (DID). Un identificateur DID est essentiel pour participer au réseau et effectuer des transactions. Il s'agit du numéro, du nom ou de la chaîne par lequel ou laquelle une personne est identifiée. Un identificateur cryptographique (CID) est un identificateur DID qui est lié de manière cryptographique à une certaine clé privée.

La plupart des solutions d'identité actuelles offrent une prise en charge limitée du contrôle de l'identité, de la transparence et de la portabilité, étant donné que les fournisseurs tiers dotés de systèmes propriétaires favorisent ce type de solutions. Un système d'identité parfaitement conforme ne verra peut-être pas le jour dans un proche avenir, mais cela n'exclut pas la nécessité d'établir les principes fondateurs applicables à la souveraineté.

Afin de permettre la SSI, une nouvelle série de protocoles et de solutions de gestion décentralisée des identités est en cours de normalisation, comme indiqué dans les § B.2.1 à B.2.5.

B.2.1 Identificateurs décentralisés

Les identificateurs DID sont des identificateurs pour les systèmes d'identité vérifiables et décentralisés, y compris l'identité numérique auto-souveraine. En général, les identificateurs DID sont

générés et détenus en propre par l'utilisateur. Les identificateurs DID possèdent des caractéristiques uniques, qui offrent une meilleure garantie d'immuabilité et sont inviolables. Ils relèvent entièrement du contrôle du sujet du DID, ce qui les rend indépendants de tout registre centralisé, fournisseur IdP ou autorité de certification. Les identificateurs DID sont des localisateurs uniformes de ressource (URL) qui relient un sujet de DID à des moyens d'interaction de confiance avec ce sujet.

En général, les identificateurs DID se répartissent en deux catégories: les identificateurs DID publics et les identificateurs DID par paires (que l'on peut considérer comme semi-privés).

1) Les identificateurs DID publics sont des identificateurs utilisés par les utilisateurs qui choisissent de se relier à des données destinées à être partagées par le public. Comme exemples, on peut citer le profil public sur les réseaux sociaux ou la vérification d'une profession, par exemple celle de médecin. Les identificateurs DID publics permettent aux utilisateurs de prendre en charge des activités qu'ils jugent bon de partager avec d'autres et vérifiables par d'autres. Par exemple, je peux vérifier que l'identificateur DID appartient à mon médecin personnel. Les identificateurs DID publics sont traçables et reliables sur l'Internet.
2) Les identificateurs DID par paires sont générés dans le cadre d'une relation ou d'un ensemble d'interactions, par lesquelles les utilisateurs souhaitent participer à des transactions mutuelles. Les identificateurs DID par paires isolent les utilisateurs et empêchent toute corrélation. Pour la majorité des utilisateurs, les identificateurs DID par paires seront le principal mécanisme permettant d'effectuer des interactions basées sur des identités.

Les identificateurs DID donnent des documents DID, qui sont des documents simples décrivant comment utiliser cet identificateur DID spécifique. Chaque document DID contient au moins trois éléments: du matériel cryptographique; des suites d'authentification; et des points d'extrémité de service. Le matériel cryptographique combiné aux suites d'authentification forment un ensemble de mécanismes pour authentifier un sujet de DID (par exemple des clés publiques ou des protocoles d'authentification biométriques pseudonymes). Les points d'extrémité de service permettent des communications de confiance avec le sujet du DID.

Pour utiliser un identificateur DID avec un registre distribué ou un réseau particulier, il est nécessaire de définir une méthode DID dans une spécification de méthode DID distincte. Une méthode DID précise un ensemble de règles qui décrivent la manière dont un identificateur DID est enregistré, rétabli, mis à jour et annulé sur ce registre ou réseau spécifique.

Ce modèle réduit la dépendance vis-à-vis des registres centralisés pour les identificateurs ainsi que des autorités de certification centralisées pour la gestion des clés, qui est le modèle type d'une infrastructure hiérarchique (infrastructure de clé publique, PKI). Étant donné que les identificateurs DID se trouvent sur un registre distribué, chaque entité peut être utilisée comme sa propre autorité.

À noter que les méthodes DID peuvent également être conçues pour les identificateurs enregistrés dans des systèmes IdM fédérés ou centralisés. Pour leur part, tous les types de systèmes d'identification peuvent prévoir la prise en charge des identificateurs DID. Cela génère un relais d'interopérabilité entre les environnements des identificateurs centralisés, fédérés et décentralisés.

B.2.2 Plates-formes d'identité

Les plates-formes d'identité (IH) sont les éléments chargés de stocker les assertions d'identité concernant des sujets. Les plates-formes IH reposent sur un modèle décentralisé permettant de stocker des représentations sémantiques de tout objet et de les exposer sous la forme d'adresses URL spécifiques. Une architecture IH peut regrouper des identités stockées sur différents fournisseurs, allant des annuaires en nuage aux dispositifs.

B.2.3 Dispositif de résolution d'identificateur décentralisé universel

Un dispositif de résolution DID universel agit comme un système distribué qui permet de résoudre les identificateurs DID sur plusieurs technologies DLT ou chaînes de blocs. Un dispositif de résolution DID universel a un objectif similaire à celui du mécanisme de liaison dans un système de noms de domaine. Au lieu de travailler avec des noms de domaine, les dispositifs de résolution DID universels sont axés sur l'adressage des identités SSI qui peuvent être créées et enregistrées directement par les entités auxquelles ils se réfèrent. Le concept est décrit dans la Figure B.1.

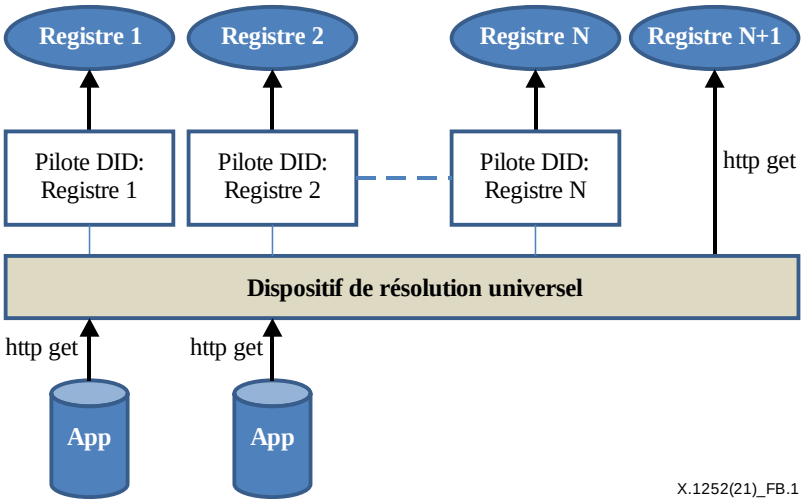


Figure B.1 – Dispositif de résolution DID universel

B.2.4 Justificatifs vérifiables

Les déclarations vérifiables sont utiles lorsqu'une entité a besoin de prouver:

- un âge minimum requis;
- sa capacité à conduire un certain type de véhicule à moteur;
- son besoin d'un traitement particulier;
- sa formation et sa certification en tant qu'électricien;
- sa capacité à exercer la médecine par un diplôme professionnel; et
- qu'elle est autorisée à voyager à l'international.

L'écosystème de déclarations vérifiables se compose de quatre rôles principaux.

1) L'émetteur, qui délivre les justificatifs vérifiables à propos d'un sujet donné.
2) Le détenteur, qui stocke les justificatifs pour le compte d'un sujet. Les détenteurs sont en général également le sujet d'un justificatif.
3) Le vérificateur, qui interroge un profil du sujet. Un profil contient un ensemble spécifique de justificatifs. Le vérificateur confirme que les justificatifs fournis dans le profil répondent à l'objectif.
4) Le registre de l'identificateur, qui est un mécanisme utilisé pour émettre des identificateurs pour les sujets.

La Figure B.2 est une illustration visuelle de l'écosystème.

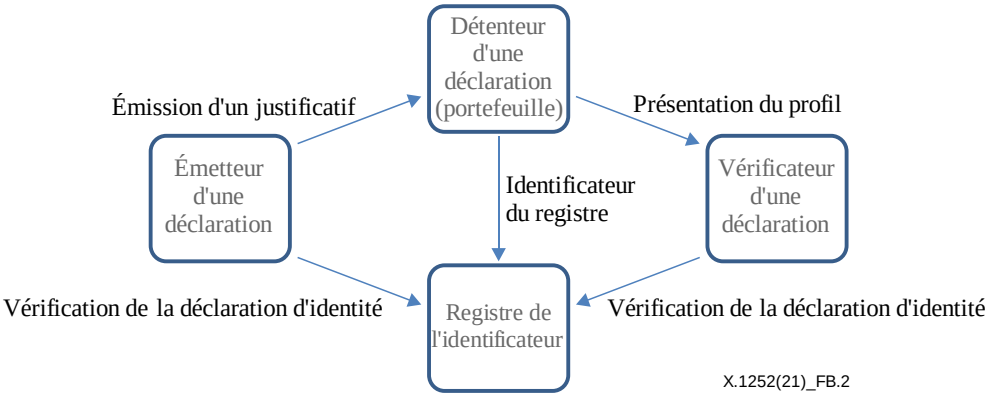


Figure B.2 – L'écosystème

B.2.5 Portefeuille décentralisé

Dans ce modèle, un utilisateur peut accéder à un service en présentant son identificateur au fournisseur de service (partie RP) sous la forme d'un jeton. La partie RP vérifie l'identité en comparant les valeurs hachées de l'identificateur avec les enregistrements hachés figurant dans le registre DLT. La partie RP peut alors autoriser ou refuser l'accès selon le résultat de la vérification. Dans les scénarios plus évolués, l'utilisateur peut déduire des paires de clés distinctes d'une clé privée maîtresse pour générer des identificateurs distincts pour différentes relations, afin de permettre des interactions respectueuses de la vie privée.

La Figure B.3 décrit les interactions d'identité globales pour la prise en charge d'un service basé sur l'identité. Cette figure représente les étapes suivantes des transactions d'identité décentralisées:

- Un utilisateur décide d'interagir en utilisant les services d'identité décentralisés d'un support de confiance d'identité. Comme indiqué dans l'encadré de la Figure B.3 sur le registre décentralisé, la technologie DLT fournit des services pour permettre à l'utilisateur final d'établir un DID et une relation avec le registre. La création d'un DID pour l'utilisateur aboutit à la sauvegarde d'une adresse de registre pour cet utilisateur et la création de paires de clés publiques-privées pour les interactions avec l'utilisateur. Le registre tient également à jour le document DID et établit les liens requis dans la notation des objets en Javascript pour les données liées, selon les spécifications de l'utilisateur. Le registre fournit des services d'identité centraux qui permettent aux services de découvrir comment interagir avec le portefeuille de l'utilisateur pour rechercher des déclarations disponibles sous le contrôle de l'utilisateur.
- La création d'un DID sur le registre conduit à la création d'un portefeuille que l'utilisateur utilise pour fournir des déclarations vérifiées à la partie RP. Le portefeuille contient les clés privées de l'utilisateur, les clés publiques et d'autres profils d'identité nécessaires aux DID. Les techniques à apport nul de connaissance garantissent que les déclarations peuvent être vérifiées de façon à préserver la confidentialité conformément à l'utilisation actuelle des justificatifs et documents papier classiques. Un utilisateur peut par exemple prouver son âge avec un permis de conduire dans un restaurant sans qu'il soit nécessaire pour l'émetteur de participer à la transaction. Les étapes à suivre sont décrites dans les paragraphes suivants. Le portefeuille peut être un portefeuille virtuel dont une partie se trouve sur le dispositif mobile de l'utilisateur et l'autre partie dans le nuage. Cette configuration permet la création d'agents agissant pour le compte de l'utilisateur et exécutant des services sans qu'une implication directe de l'utilisateur soit nécessaire.

  1) Enregistrement DID: l'utilisateur télécharge le portefeuille associé au fournisseur de services central DLT et enregistre son DID sur le registre. La technologie DLT génère les paires de clés publiques et privées pour le portefeuille d'identité. En outre, un

emplacement ou une adresse est créée et stockée sur la technologie DLT dans le cadre du processus d'enregistrement.

2) Lancement de l'identité: pour qu'une technologie DLT soit utilisée dans des systèmes d'identité décentralisés, on suppose qu'un cadre de confiance définit l'ensemble de services d'identité disponibles pour les participants. À cet égard, un utilisateur peut se fier à la disponibilité d'un émetteur (une partie de confiance) qui peut valider l'identité des services. Les utilisateurs peuvent créer les déclarations initiales pour recueillir des déclarations auprès de plusieurs fournisseurs à ajouter dans leur portefeuille et renforcer la validité de leur identité au sein du système. Il ressort de la Figure B.3 que chaque relation est protégée par un DID commun à l'émetteur, au détenteur (utilisateur) et au vérificateur.

3) Vérification: si un détenteur (utilisateur) souhaite avoir accès au service d'une partie RP, cette partie RP (vérificateur) demandera des informations à l'utilisateur concernant les déclarations disponibles. Ensuite, le vérificateur consultera le registre pour valider les déclarations signées en utilisant les clés publiques qui correspondent au DID et se rapportent à la transaction. Cette étape comprend d'autres couches d'authentification. En particulier, au vu de la manière dont le système fonctionne, on présume que le portefeuille est la source de vérité en termes de connaissance des clés privées du détenteur. Le système présume qu'une authentification adaptée a eu lieu pour garantir que le propriétaire légitime du portefeuille est bien l'entité à l'origine de la transaction.

4) Validation de la déclaration: la partie RP utilise les déclarations fournies par le portefeuille pour vérifier l'identité et les attributs de l'utilisateur en utilisant la signature fondée sur l'infrastructure PKI, ainsi que les techniques de validation hachée.

5) Autorisation: la partie RP détermine à quels services il est possible d'accéder en fonction des résultats des vérifications d'identité.

- La conception de l'identificateur DID fait appel à la capacité d'un dispositif de résolution universel de tout identificateur DID. Cette exigence est encore en cours d'élaboration par la communauté DLT. Dans les modèles d'identité décentralisés, il est nécessaire d'établir une couche d'authentification DID interopérable. Les travaux sur la question sont toujours en cours.
- L'authentification DID permet à un propriétaire d'identité d'apporter la preuve du contrôle d'un DID pendant son interaction avec une partie RP. Cela nécessite l'exécution des étapes suivantes par la partie RP:

  1) La partie RP traduit le DID du propriétaire d'identité sur un document DID.

  2) La partie RP essaie d'authentifier le propriétaire d'identité en utilisant le ou les objets d'authentification trouvés dans le document DID.

  3) Le ou les objets d'authentification peuvent comprendre un objet de clé publique ou y faire référence, si la preuve du propriétaire d'identité est établie sous forme de signature chiffrée.

- L'authentification DID doit être comprise comme étant extensible en ce qui concerne la manière dont un propriétaire d'identité peut apporter la preuve du contrôle sur un DID.

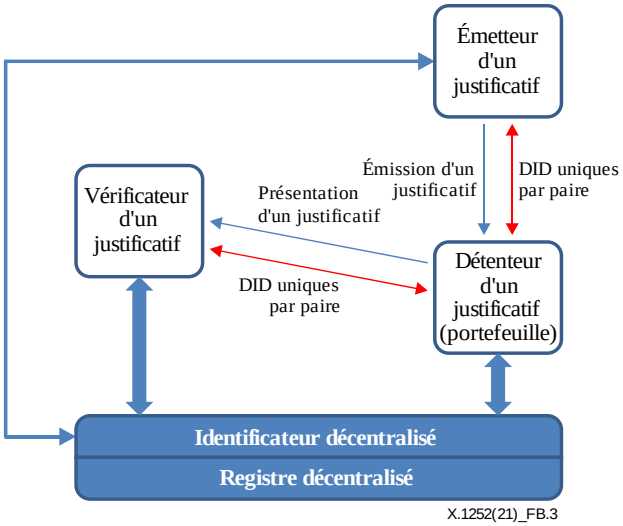


Figure B.3 – Portefeuille d'identificateur décentralisé avec déclarations vérifiables

Bibliographie

[b-UIT-T E.101] Recommandation UIT-T E.101 (2009), *Définition des termes utilisés pour les identificateurs (noms, numéros, adresses et autres identificateurs) pour les services et réseaux publics de télécommunication dans les Recommandations de la série E.*

[b-UIT-T L.1410] Recommandation UIT-T L.1410 (2014), *Méthodologie applicable aux analyses environnementales du cycle de vie des biens, réseaux et services utilisant les technologies de l'information et de la communication.*

[b-UIT-T X.501] Recommandation UIT-T X.501 (2019) | ISO/CEI 9594-2:2020, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: les modèles.*

[b-UIT-T X.509] Recommandation UIT-T X.509 (2019) | ISO/CEI 9594-8:2020, *Technologies de l'information – Interconnexion des systèmes ouverts – L'annuaire: cadre général des certificats de clé publique et d'attribut.*

[b-UIT-T X.800] Recommandation UIT-T X.800 (1991), *Architecture de sécurité pour l'interconnexion en systèmes ouverts d'applications du CCITT.*

[b-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.*

[b-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.*

[b-UIT-T X.1254] Recommandation UIT-T X.1254 (2020), *Cadre de garantie d'authentification d'entité.*

[b-UIT-T X.1400] Recommandation UIT-T X.1400 (2020), *Termes et définitions concernant la technologie des registres distribués.*

[b-UIT-T X.1403] Recommandation UIT-T X.1403 (2020), *Lignes directrices pour la sécurité relatives à l'utilisation de la technologie des registres distribués pour la gestion décentralisée des identités.*

[b-UIT-T Y.2701] Recommandation UIT-T Y.2701 (2007), *Prescriptions de sécurité des réseaux de prochaine génération de version 1.*

[b-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.*

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

[b-ISO/CEI 2382-37] ISO/CEI 2382-37:2017, *Technologies de l'information – Vocabulaire – Partie 37: Biométrie.*

[b-ISO/CEI 24760-1] ISO/CEI 24760-1:2019, *Sécurité IT et confidentialité – Cadre pour la gestion de l'identité – Partie 1: Terminologie et concepts.*

[b-ISO/CEI 29115] ISO/CEI 29115:2013, *Technologies de l'information – Techniques de sécurité – Cadre d'assurance de l'authentification d'entité.*

[b-OIX-TFIS] Makaay, E., Smedinghoff, T., Thibeau, D. (2017). Trust frameworks for identity systems, White paper, Trust framework series. London: Open Identity Exchange. 18 pages. Disponible à l'adresse suivante [consulté le 17/05/2021]: https://connectis.com/wp-content/uploads/2018/05/OIX-White-Paper_Trust-Frameworks-for-Identity-Systems_Final.pdf

[b-W3C-DIDs] W3C (Internet), [Sans titre], Decentralized identifiers (DIDs) … Cambridge, MA: World Wide Web Consortium. Disponible à l'adresse suivante [consulté le 15/05/2021]: https://w3c.github.io/did-core/

[b-W3C-VC] W3C Working Group Note (2019), *Verifiable credentials use cases*. Cambridge, MA: World Wide Web Consortium. Disponible à l'adresse suivante [consulté le 17/05/2021]: http://www.w3.org/TR/vc-use-cases/

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC
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	Environnement et TIC, changement climatique, déchets d'équipements électriques et électroniques, efficacité énergétique; 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	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	Commutation et signalisation et mesures et tests associés
Série R	Transmission télégraphique
Série S	Équipements 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, réseaux de prochaine génération, Internet des objets et villes intelligentes
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2021