

**Assemblée générale**

Distr. limitée
6 février 2018
Français
Original : anglais

**Commission des Nations Unies
pour le droit commercial international
Groupe de travail IV (Commerce électronique)
Cinquante-sixième session
New York, 16-20 avril 2018**

**Questions juridiques liées à la gestion de l'identité
et aux services de confiance****Termes et notions relatifs à la gestion de l'identité et aux services
de confiance****Note du Secrétariat**

Table des matières

	<i>Page</i>
I. Introduction	2
II. Termes et notions relatifs à la gestion de l'identité et aux services de confiance	3
A. Définitions relatives à la gestion de l'identité	3
B. Définitions relatives aux services de confiance	9



I. Introduction

1. À sa quarante-huitième session, en 2015, la Commission a chargé le Secrétariat de mener des travaux préparatoires sur la gestion de l'identité et les services de confiance, l'informatique en nuage et le commerce mobile, y compris en organisant des colloques et des réunions de groupes d'experts, en vue des travaux que le Groupe de travail pourrait mener. Elle a également prié le Secrétariat de communiquer les résultats de ces travaux préparatoires au Groupe de travail IV, afin d'obtenir des recommandations sur la portée exacte, la méthodologie et les priorités qui pourraient être envisagées, recommandations qu'elle examinerait à sa quarante-neuvième session¹.
2. À sa quarante-neuvième session, en 2016, la Commission était saisie d'une note du Secrétariat portant sur les questions juridiques liées à la gestion de l'identité et aux services de confiance (A/CN.9/891), qui résumait les débats tenus pendant le colloque de la CNUDCI organisé sur ce thème à Vienne, les 21 et 22 avril 2016, synthèse que complétaient d'autres informations. Elle s'est également vu dire que des experts avaient commencé à examiner la question des aspects contractuels de l'informatique en nuage en se fondant sur une proposition (A/CN.9/856) qui lui avait été soumise à sa quarante-huitième session, en 2015.
3. À cette session, la Commission est convenue qu'il faudrait maintenir les thèmes de la gestion de l'identité et des services de confiance, ainsi que de l'informatique en nuage, à l'ordre du jour des travaux du Groupe de travail et qu'il serait prématuré d'établir un ordre de priorité entre les deux thèmes. Elle a confirmé avoir décidé que le Groupe de travail pourrait entreprendre des travaux sur ces questions une fois achevés ceux relatifs à la Loi type sur les documents transférables électroniques. Dans ce contexte, le Secrétariat, dans la limite des ressources dont il disposait, et le Groupe de travail ont été priés de continuer à mener des travaux préparatoires sur les deux thèmes, y compris leur faisabilité, parallèlement et avec souplesse, et d'en rendre compte à la Commission pour qu'elle puisse prendre une décision éclairée à une session ultérieure, y compris sur la priorité à accorder à chaque thème².
4. À sa cinquantième session, en 2017, après un débat, la Commission a réaffirmé le mandat confié au Groupe de travail à sa quarante-neuvième session, en 2016 (voir par. 3 ci-dessus). Elle est convenu de réexaminer ce mandat à sa cinquante et unième session, en particulier si le besoin se faisait sentir d'établir un ordre de priorité entre les thèmes ou de confier au Groupe de travail un mandat plus précis en ce qui concernait ses travaux dans le domaine de la gestion de l'identité et des services de confiance³.
5. À sa cinquante-cinquième session (New York, 24-28 avril 2017), le Groupe de travail était saisi d'une note énumérant les termes et concepts relatifs à la gestion de l'identité et aux services de confiance (A/CN.9/WG.IV/WP.143). À cette session, il a demandé au Secrétariat de réviser cette note en y insérant les définitions et concepts énumérés au paragraphe 20 du document A/CN.9/WG.IV/WP.144⁴.
6. La présente note contient la définition d'un certain nombre de termes relatifs à la gestion de l'identité et aux services de confiance. Ces termes doivent permettre de débattre sur la base d'une compréhension commune des notions fondamentales ; ils n'ont pas pour but d'inviter à débattre de définitions juridiquement contraignantes de ces notions. De même, ils ne visent pas à donner une indication de la portée des travaux que la CNUDCI mènera dans le domaine de la gestion de l'identité et des services de confiance.
7. La source des termes définis, lorsqu'elle est disponible, est explicitement indiquée. Lorsqu'il existe différentes sources, un même terme peut comporter plusieurs définitions. Lorsque aucune source n'est indiquée, la définition a été proposée lors de

¹ *Documents officiels de l'Assemblée générale, soixante-dixième session, Supplément n° 17 (A/70/17)*, par. 358.

² *Ibid.*, *soixante et onzième session, Supplément n° 17 (A/71/17)*, par. 229.

³ *Ibid.*, *soixante-douzième session, Supplément n° 17 (A/72/17)*, par. 127.

⁴ A/CN.9/902, par. 92.

consultations d'experts. La préférence a été donnée aux termes définis à l'échelle internationale. D'autres sources de termes définis sont disponibles, en particulier au niveau national.

8. Les termes définis sont énumérés dans des sections différentes uniquement pour en faciliter la présentation et sans préjuger de ce que le Groupe de travail pense de leur pertinence pour l'examen des aspects juridiques de la gestion de l'identité ou des services de confiance.

9. Les termes définis ayant des origines différentes, il ne faut pas les lire comme un ensemble cohérent de termes interconnectés. Il faut plutôt considérer chaque terme comme une définition autonome et c'est comme tel qu'il est présenté comme référence possible pour les débats du Groupe de travail. Lorsqu'elle est disponible, la source du terme défini est indiquée afin que l'on puisse recueillir des informations supplémentaires dans le document d'origine.

10. Les synonymes sont indiqués par commodité uniquement compte tenu de leur utilisation. Ils ne sont pas tous définis dans la présente note.

11. Les termes sont énumérés par ordre alphabétique dans la version anglaise de la présente note. Cet ordre est maintenu dans les autres versions linguistiques pour assurer la correspondance des paragraphes et donc faciliter les renvois pendant les débats du groupe de travail.

II. Termes et notions relatifs à la gestion de l'identité et aux services de confiance

A. Définitions relatives à la gestion de l'identité

12. Par « niveau de garantie », on entend le degré de confiance dans le lien qui lie une entité et l'identité présentée. Source : Recommandation UIT-T X.1252. Synonyme : garantie d'identité.

13. Par « attribut », on entend un élément d'information ou de donnée associé à un sujet. Ces éléments peuvent être des informations telles que le nom, l'adresse, l'âge, le sexe, le titre, le salaire, la fortune, le numéro de permis de conduire, le numéro de sécurité sociale, l'adresse électronique, le numéro de téléphone portable et des données telles que la présence du sujet sur les réseaux, l'appareil utilisé par le sujet, la localisation habituelle du domicile du sujet connue par un réseau, etc. (pour un être humain) ; la raison sociale, le siège social, le nom d'enregistrement, le pays d'enregistrement, etc. (pour une personne morale) ; la marque et le modèle, le numéro de série, l'emplacement, la capacité, le type, etc. (pour un appareil). Synonyme : attribut d'identité.

14. Par « fournisseur d'attributs », on entend une entité commerciale ou publique qui agit comme source d'un ou de plusieurs attributs de l'identité d'un sujet. Le fournisseur d'attributs est souvent l'entité chargée d'attribuer, de recueillir ou de gérer ces attributs. Ces fournisseurs peuvent être un organisme public qui tient un registre des naissances ou un registre des titres de propriété, un bureau national de crédit, une entreprise qui gère une base de données commerciale ou un registre de sociétés, ainsi que des entités telles que des opérateurs de téléphonie mobile, des banques, des services publics et des prestataires de services de santé qui détiennent des données vérifiées d'utilisateurs et vérifient ou fournissent ces attributs à des tiers (sous réserve, éventuellement, du consentement des utilisateurs).

15. Par « authentification », on entend a) un processus utilisé pour obtenir une confiance suffisante dans le lien qui lie une entité et l'identité présentée. Source : Recommandation UIT-T X.1252 ; b) le processus consistant à associer l'identité déclarée d'un sujet au sujet réel en confirmant l'association du sujet à un justificatif, soit directement (authentification active), soit par l'environnement dans lequel le sujet interagit (« authentification passive » ou « authentification adaptative »). Par exemple,

la saisie d'un mot de passe secret associé à un nom d'utilisateur est supposée authentifier le fait que la personne qui saisit ce mot de passe est celle à qui le nom d'utilisateur a été délivré. De même, on compare une personne qui présente un passeport à la photo qui y figure pour authentifier le fait (c'est-à-dire confirmer) que cette personne est celle décrite dans le passeport ; c) un processus électronique permettant de confirmer l'identification électronique d'une personne physique ou morale, ou l'origine et l'intégrité de données sous forme électronique. Source : Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE (« eIDAS »), article 3(5). (Voir également le document [A/CN.9/WG.IV/WP.144](#), par. 20.)

16. Par « garantie d'authentification », on entend le degré de confiance obtenu, dans le processus d'authentification, dans le fait que le partenaire de communication est l'entité qu'il déclare ou est censé être. Note : la confiance repose sur le degré de confiance dans le lien qui lie l'entité communicante et l'identité présentée. Source : Recommandation UIT-T X.1252. Note : dans certains cas, les notions de « garantie d'identité » et de « garantie d'authentification » sont considérées comme des composantes distinctes du concept global de « niveau de garantie ».

17. Par « facteur d'authentification », on entend a) une information ou une procédure employée pour authentifier ou vérifier l'identité d'une entité. Source : ISO/IEC 19790. Note : les facteurs d'authentification se répartissent en quatre catégories : i) une chose que l'entité possède (signature d'un dispositif, passeport, dispositif matériel contenant un justificatif d'identité, clef privée, par exemple) ; ii) une chose que l'entité connaît (mot de passe, numéro d'identification personnel (PIN, *personal identification number*), par exemple) ; iii) une chose que l'entité est (ses caractéristiques biométriques, par exemple) ; iv) une chose que l'entité fait généralement (son modèle de comportement, par exemple). Source : Recommandation UIT-T X.1254 ; b) un facteur confirmé comme étant lié à une personne, qui relève de l'une des catégories suivantes : i) « facteur d'authentification basé sur la possession », facteur d'authentification dont il revient au sujet de démontrer la possession ; ii) « facteur d'authentification basé sur la connaissance », facteur d'authentification dont il revient au sujet de démontrer la connaissance ; iii) « facteur d'authentification inhérent », facteur d'authentification qui est basé sur un attribut physique d'une personne physique, et dont il revient au sujet de démontrer qu'il possède cet attribut physique. Source : Règlement d'exécution (UE) 2015/1502 de la Commission, Annexe, article 1(2).

18. Par « authentifiant », on entend un élément qui sert à établir la relation entre un sujet et un justificatif. Un authentifiant actif est généralement une chose que le sujet connaît (mot de passe secret, par exemple), que le sujet possède (carte à puce, par exemple) ou que le sujet est (photo ou autre information biométrique, par exemple), et qui permet de l'associer à un justificatif. Par exemple, un mot de passe constitue l'authentifiant d'un nom d'utilisateur, et une photo l'authentifiant d'un passeport ou d'un permis de conduire. Un authentifiant passif est généralement une chose que l'environnement sait, comme le réseau de téléphonie mobile qui sait que l'utilisateur est connecté au réseau, se trouve à l'endroit habituel, utilise l'appareil habituel, n'a pas été empêché d'utiliser le réseau, etc.

19. Par « source faisant autorité », on entend a) un répertoire reconnu comme étant une source d'informations précises et mises à jour. Source : Recommandation UIT-T X.1254 ; b) toute source, quelle que soit sa forme, à laquelle on peut se fier pour obtenir des données, des informations et/ou des éléments d'identification exacts pouvant être utilisés pour prouver l'identité. Source : Règlement d'exécution (UE) 2015/1502 de la Commission, Annexe, article 1(1). (Voir également le document [A/CN.9/WG.IV/WP.144](#), par. 20).

20. Par « autorisation », on entend a) un processus consistant à octroyer des droits et privilèges à un sujet authentifié sur la base de critères généralement déterminés par la partie utilisatrice. Une fois authentifié, par exemple, un sujet peut se voir accorder l'accès à une base de données confidentielle. Source : [A/CN.9/WG.IV/WP.120](#), annexe ;

b) l'attribution de droits et, sur la base de ces droits, la permission d'accès. Source : Recommandation UIT-T Y.2720 et Recommandation UIT-T X.800.

21. Par « justificatif », on entend a) un ensemble de données présentées comme preuves d'une identité déclarée et/ou de droits. Source : Recommandation UIT-T X.1252 ; b) des documents numériques ou papier présentés comme preuves d'une identité déclarée. Les justificatifs papier peuvent être des passeports, des certificats de naissance, des permis de conduire et des cartes d'employé. Les justificatifs numériques peuvent être des noms d'utilisateur, des cartes à puce, des identifiants de téléphonie mobile et des certificats numériques. Source : [A/CN.9/WG.IV/WP.120](#), annexe. Synonymes : moyen d'identification électronique, justificatif d'identité.

22. Par « fournisseur de justificatifs d'identité » ou « fournisseur de services de justificatifs d'identité », on entend a) une entité qui délivre des justificatifs d'identité ; b) un acteur de confiance qui délivre et/ou gère des justificatifs d'identité. Note : ce fournisseur peut englober ses autorités d'enregistrement et ses vérificateurs. Il peut être un tiers indépendant, ou peut émettre des justificatifs d'identité pour son propre usage. Source : Recommandation UIT-T X.1254.

23. Par « identification électronique », on entend le processus consistant à utiliser des données d'identification personnelle sous une forme électronique représentant de manière univoque une personne physique ou morale, ou une personne physique représentant une personne morale. Source : Règlement eIDAS, article 3(1). (Voir également le document [A/CN.9/WG.IV/WP.144](#), par. 20.)

24. Par « moyen d'identification électronique », on entend un élément matériel et/ou immatériel contenant des données d'identification personnelle et utilisé pour s'authentifier pour un service en ligne. Source : Règlement eIDAS, article 3(2). (Voir également le document [A/CN.9/WG.IV/WP.144](#), par. 20.)

25. Par « schéma d'identification électronique », on entend un système pour l'identification électronique en vertu duquel des moyens d'identification électronique sont délivrés à des personnes physiques ou morales, ou à des personnes physiques représentant des personnes morales. Source : Règlement eIDAS, article 3(4). (Voir également le document [A/CN.9/WG.IV/WP.144](#), par. 20.)

26. Par « inscription », on entend a) le 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. Source : Recommandation UIT-T X.1252 ; b) le processus par lequel les fournisseurs de justificatifs d'identité (ou leurs agents) vérifient les déclarations d'identité d'un sujet avant de lui délivrer un justificatif.

27. Par « entité », on entend un 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. Source : Recommandation UIT-T X.1252. Une entité peut avoir plusieurs identificateurs.

28. Par « fédération », on entend a) une association d'utilisateurs, de fournisseurs de services et de fournisseurs de services d'identité. Source : Recommandation UIT-T X.1252 ; b) un groupe de fournisseurs d'identité, de parties utilisatrices, de sujets et d'autres entités qui acceptent d'opérer dans le cadre de politiques, de normes et de technologies compatibles spécifiées dans des règles de fonctionnement (ou cadre de confiance) afin que les informations communiquées par les fournisseurs d'identité puissent être comprises et utilisées en confiance par les parties utilisatrices. Synonymes : fédération d'identité, système d'identité multipartite.

29. Par « identification », on entend le processus consistant à réunir, vérifier et valider suffisamment d'attributs d'un sujet donné pour définir et confirmer son identité dans un contexte particulier. Synonymes : contrôle d'identité, enregistrement.

30. Par « identificateur », on entend a) un ou plusieurs attributs utilisés pour identifier une entité dans un contexte. Source : Recommandation UIT-T X.1252 ; b) un ou plusieurs attributs caractérisant de façon unique une entité dans un contexte particulier. Source : Recommandation UIT-T X.1254.

31. Par « identité », on entend a) un ensemble d'attributs liés à une entité. Source : ISO/IEC 24760 ; b) des informations relatives à un sujet donné qui, prenant la forme d'un ou plusieurs attributs, permettent au sujet d'être identifié de manière suffisante dans un contexte particulier ; c) un ensemble d'attributs concernant une personne qui la décrivent de façon unique dans un contexte donné. Synonyme : identité numérique.

32. Par « assertion d'identité », on entend un enregistrement électronique provenant d'un fournisseur d'identité et envoyé à une partie utilisatrice qui contient l'identificateur du sujet (nom, numéro de compte, numéro de portable, emplacement, etc.), son statut d'authentification et les attributs d'identité applicables. Ces attributs sont généralement des informations personnelles ou non concernant le sujet qui présentent un intérêt pour la transaction requise par la partie utilisatrice.

33. Par « garantie d'identité », on entend le 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 le 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. Source : Recommandation UIT-T X.1252. Synonyme : niveau de garantie. Note : dans certains cas, les notions de « garantie d'identité » et de « garantie d'authentification » sont considérées comme des composantes distinctes du concept global de « niveau de garantie ».

34. Par « fédération d'identité », on entend un groupe de fournisseurs d'identité, de parties utilisatrices, de sujets et d'autres entités qui acceptent d'opérer dans le cadre de politiques, de normes et de technologies compatibles spécifiées dans des règles de fonctionnement (ou cadre de confiance) afin que les informations communiquées par les fournisseurs d'identité puissent être comprises et utilisées en confiance par les parties utilisatrices. Voir également : fédération, système d'identité multipartite.

35. Par « gestion de l'identité », on entend a) un ensemble de processus appliqués pour gérer l'identification, l'authentification et l'autorisation d'individus, d'entités juridiques, de dispositifs ou d'autres sujets dans un univers connecté. Source : [A/CN.9/854](#), par. 6 ; b) un ensemble de fonctions et de fonctionnalités (administration, gestion et tenue à jour, découverte, échanges de communication, corrélation et liens, application des politiques, authentification et assertions, par exemple) utilisées pour : i) garantir les informations d'identité (identificateurs, justificatifs d'identité et attributs, par exemple) ; ii) garantir l'identité d'une entité ; et iii) permettre des applications commerciales et sécuritaires. Source : Recommandation UIT-T Y.2720.

36. Par « contrôle d'identité », on entend a) le processus consistant à réunir, vérifier et valider suffisamment d'attributs d'un sujet donné (personne, entité juridique, dispositif, objet numérique ou autre entité) pour définir et confirmer son identité dans un contexte particulier. Ce contrôle peut s'effectuer par auto-assertion ou en regard d'enregistrements existants ; b) un processus qui permet de valider et de vérifier suffisamment d'informations pour confirmer l'identité déclarée de l'entité. Source : Recommandation UIT-T X.1252 ; c) une procédure au moyen de laquelle l'autorité d'enregistrement recueille et contrôle un nombre suffisant d'informations pour identifier une entité à un niveau de garantie spécifié ou convenu. Source : Recommandation UIT-T X.1254. Synonymes : identification, enregistrement.

37. Par « fournisseur d'identité », on entend a) une entité chargée d'identifier des personnes, entités juridiques, appareils et/ou objets numériques, d'émettre les justificatifs d'identité correspondants et de gérer ces informations pour le compte des sujets. Source : [A/CN.9/WG.IV/WP.120](#), annexe ; b) une entité qui crée, maintient et

gère des informations d'identité sécurisées pour d'autres entités (utilisateurs/abonnés, organisations et dispositifs, par exemple) et propose des services fondés sur l'identité basés sur une relation de confiance, commerciale ou d'autres natures. Source : Recommandation UIT-T Y.2720. Synonymes : fournisseur de services de justificatifs d'identité, fournisseur de services d'identité.

38. Par « système d'identité », on entend un environnement en ligne de gestion de l'identité régi par un ensemble de règles de fonctionnement (également appelé cadre de confiance) dans lequel particuliers, organisations, services et appareils peuvent se faire mutuellement confiance parce que des sources faisant autorité établissent et authentifient leur identité respective. Source : [A/CN.9/WG.IV/WP.120](#), annexe. Un système d'identité implique a) un ensemble de règles, de méthodes, de procédures et de routines, une technologie, des normes, des politiques et des processus, b) applicables à un groupe d'entités participantes, c) régissant la collecte, la vérification, le stockage, l'échange et l'authentification des attributs d'identité concernant une personne, une entité juridique, un appareil ou un objet numérique, ainsi que la confiance dans ces attributs, d) dans le but de faciliter les transactions liées à l'identité. Synonymes : système de gestion de l'identité, fédération d'identité, système d'identification électronique, système de gestion de la sécurité de l'information.

39. Par « transaction liée à l'identité », on entend toute transaction impliquant deux ou plusieurs participants qui consiste à établir, vérifier, émettre, asserter, révoquer ou communiquer une identité, ou à s'y fier.

40. Par « vérification d'identité », on entend le 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. Source : Recommandation UIT-T X.1252.

41. Par « système de gestion de la sécurité de l'information », on entend un ensemble de processus et de procédures visant à gérer les risques associés à la sécurité de l'information pour les maintenir à des niveaux acceptables. Source : Règlement d'exécution (UE) 2015/1502 de la Commission, Annexe, article 1(4).

42. Par « niveau de garantie », on entend le degré de confiance dans les processus d'identification et d'authentification, à savoir : a) le degré de confiance dans le processus de validation utilisé pour établir l'identité d'une entité à qui un justificatif a été délivré ; et b) le degré de confiance dans le fait que l'entité qui utilise le justificatif est celle à qui le justificatif a été délivré. La garantie reflète la fiabilité des méthodes, des processus et des technologies utilisés. Certains systèmes définissent les niveaux de garantie par des chiffres, à savoir 1 à 4, où le niveau 1 est le niveau de garantie le plus faible et le niveau 4 le plus élevé. D'autres systèmes qualifient les niveaux de garantie de « faible », « moyen » et « élevé ». Synonymes : garantie d'identité, niveau de confiance.

43. Par « authentification multifacteur », on entend une authentification effectuée à l'aide d'au moins deux facteurs indépendants. Note : les facteurs d'authentification se répartissent en quatre catégories : a) une chose que l'entité possède (signature d'un dispositif, passeport, dispositif matériel contenant un justificatif d'identité, clef privée, par exemple) ; b) une chose que l'entité connaît (mot de passe, numéro d'identification personnel (PIN, *personal identification number*), par exemple) ; c) une chose que l'entité est (ses caractéristiques biométriques, par exemple) ; ou d) une chose que l'entité fait généralement (son modèle de comportement, par exemple). Sources : ISO/IEC 19790, Recommandation UIT-T X.1254.

44. Par « système d'identité multipartite », on entend un système d'identité, également appelé fédération d'identité, dans lequel un sujet peut utiliser un justificatif d'identité délivré par l'un quelconque de plusieurs fournisseurs d'identité pour authentifier plusieurs parties utilisatrices non liées entre elles ; un système d'identité qui permet d'utiliser des justificatifs d'identité délivrés et des identités assertées par un ou plusieurs fournisseurs d'identité avec plusieurs parties utilisatrices. Source : [A/CN.9/WG.IV/WP.120](#), annexe. Synonyme : fédération d'identité.

45. Par « participant », on entend toute personne physique ou morale qui participe à un système d'identité ou à une transaction relative à l'identité en utilisant ce système. Les participants peuvent être des sujets, des fournisseurs d'identité, des fournisseurs d'attributs, des fournisseurs de justificatifs, des parties utilisatrices, des opérateurs de systèmes d'identité et d'autres entités. Tout comme les participants à un système de carte de crédit, les participants à un système d'identité acceptent généralement, par contrat, un ensemble de règles de fonctionnement (souvent appelées cadre de confiance) applicables à leur rôle.
46. Par « données d'identification personnelle », on entend un ensemble de données permettant d'établir l'identité d'une personne physique ou morale, ou d'une personne physique représentant une personne morale. Source : Règlement eIDAS, article 3(3). (Voir également le document [A/CN.9/WG.IV/WP.144](#), par. 20.)
47. Par « contrôle », on entend la vérification et la validation des informations lors de l'inscription de nouvelles entités dans des systèmes d'identité. Source : Recommandation UIT-T X.1252. Synonymes : contrôle d'identité, identification.
48. Par « pseudonyme », on entend un 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. Source : Recommandation UIT-T X.1252.
49. Par « enregistrement », on entend un 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. Source : Recommandation UIT-T X.1252.
50. Par « autorité d'enregistrement », on entend une entité qui fournit des services de contrôle d'inscription et/ou d'identité dans le contexte d'un système d'identité fédéré (c'est-à-dire multipartite), généralement pour un fournisseur d'identité.
51. Par « partie utilisatrice », on entend a) une personne ou une entité juridique qui se fie à un justificatif ou à une assertion d'identité pour décider des mesures à prendre dans un contexte donné, qu'il s'agisse par exemple de traiter une transaction ou d'accorder un accès à des informations ou à un système. Source : [A/CN.9/WG.IV/WP.120](#), annexe ; b) une 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. Source : Recommandation UIT-T X.1252 ; c) une personne physique ou morale qui se fie à une identification électronique ou à un service de confiance. Source : Règlement eIDAS, article 3(6).
52. Par « répertoire », on entend une interface qui accepte les dépôts d'entités numériques, permet de les conserver et offre un accès sécurisé aux entités numériques via leurs identificateurs. Source : Recommandation UIT-T X.1255.
53. Par « rôle », on entend un type (ou une catégorie) de participant à un système d'identité, tel qu'un sujet, un fournisseur d'identité, un fournisseur de justificatifs, une partie utilisatrice, etc. Un participant peut avoir plusieurs rôles. Par exemple, en ce qui concerne l'identification de ses employés, un employeur peut fonctionner à la fois comme fournisseur d'identité et partie utilisatrice.
54. Par « identité auto-assertée », on entend l'identité qu'une entité déclare comme étant la sienne. Source : Recommandation UIT-T X.1252.
55. Par « sujet », on entend la personne, l'entité juridique, le dispositif ou l'objet numérique (c'est-à-dire l'entité) identifié dans un justificatif donné, qui peut être authentifié par un fournisseur d'identité et dont ce dernier peut se porter garant. Source : [A/CN.9/WG.IV/WP.120](#), annexe. Synonymes : utilisateur, sujet de données.
56. « Règles de fonctionnement » : voir cadre de confiance.

57. Par « confiance », on entend la 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. Source : Recommandation UIT-T X.1252.

58. Par « cadre de confiance », on entend a) les règles commerciales, techniques et juridiques qui régissent la participation à un système d'identité donné et son fonctionnement. Elles sont généralement élaborées par une entité privée (opérateur du système d'identité, par exemple) et rendues contraignantes pour les participants par voie contractuelle. Source : [A/CN.9/WG.IV/WP.120](#), annexe ; b) un ensemble de prescriptions et de mécanismes de mise en application, destiné aux parties qui s'échangent des informations relatives à l'identité. Source : Recommandation UIT-T X.1254 ; c) un système de gestion de l'identité dans le cadre duquel un ensemble d'engagements vérifiables est conclu par chacune des diverses parties à une transaction auprès des parties homologues ; ces engagements comportent nécessairement : i) des contrôles afin de garantir le respect des engagements ; et ii) des solutions en cas de non-respect de ces engagements. Source : Recommandation UIT-T X.1255. Synonyme : règles de fonctionnement.

59. Par « fournisseur de cadre de confiance », on entend l'entité ou l'organisation qui crée ou adopte les règles de fonctionnement et la structure contractuelle associée d'un système d'identité donné. Le fournisseur de cadre de confiance peut également certifier les participants qui se conforment à ces règles. Par exemple, les émetteurs de cartes de crédit et de débit peuvent jouer un rôle similaire dans le monde de ces cartes ; ils énoncent les règles de fonctionnement et les font respecter.

60. Par « tierce partie de confiance », on entend a) une autorité ou son agent, auxquels se fient d'autres acteurs, s'agissant d'activités particulières (activités associées à la sécurité, par exemple). Source : Recommandation UIT-T X.1254 ; b) une entité acceptée par toutes les parties à une transaction comme intermédiaire impartial et fiable pour faciliter les interactions entre les parties.

61. Par « utilisateur », on entend a) le sujet d'un justificatif ; un consommateur des services offerts par une partie utilisatrice ; b) toute entité qui utilise une ressource, par exemple un système, un équipement, un terminal, un processus, une application ou un réseau d'entreprise. Source : Recommandation UIT-T X.1252.

62. Par « validation », on entend le processus consistant à vérifier et confirmer qu'un justificatif d'identité est valide (non expiré ou révoqué, par exemple).

63. Par « vérification », on entend a) la procédure de confrontation des informations fournies avec des informations précédemment corroborées. Source : Recommandation UIT-T X.1254 ; b) le processus ou l'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. Source : Recommandation UIT-T X.1252.

B. Définitions relatives aux services de confiance

64. Les définitions suivantes pourront présenter un intérêt particulier pour l'examen des aspects juridiques des services de confiance. Cela dit, certaines des définitions énoncées comme présentant un intérêt pour l'examen des aspects juridiques de la gestion de l'identité pourront également en présenter un pour celui des aspects juridiques des services de confiance (voir ci-dessus, par. 8).

65. Par « certificat d'authentification de site Internet », on entend une attestation qui permet d'authentifier un site Internet et associe celui-ci à la personne physique ou morale à laquelle le certificat est délivré. Source : Règlement eIDAS, article 3(38). (Voir également le document [A/CN.9/WG.IV/WP.144](#), par. 20).

66. Par « prestataire de services de certification », on entend une personne qui émet des certificats et peut fournir d'autres services liés aux signatures électroniques. Source : Loi type de la CNUDCI sur les signatures électroniques, article 2 e)⁵.

67. Par « document électronique », on entend tout contenu conservé sous forme électronique, notamment un texte ou un enregistrement sonore, visuel ou audiovisuel. Source : Règlement eIDAS, article 3(35). (Voir également le document [A/CN.9/WG.IV/WP.144](#), par. 20.)

68. Par « service d'envoi recommandé électronique », on entend un service qui permet de transmettre des données entre des tiers par voie électronique, qui fournit des preuves concernant le traitement des données transmises, y compris la preuve de leur envoi et de leur réception, et qui protège les données transmises contre les risques de perte, de vol, d'altération ou de toute modification non autorisée. Source : Règlement eIDAS, article 3(36). (Voir également le document [A/CN.9/WG.IV/WP.144](#), par. 20.)

69. Par « cachet électronique », on entend des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique pour garantir l'origine et l'intégrité de ces dernières. Source : Règlement eIDAS, article 3(25). (Voir également le document [A/CN.9/WG.IV/WP.144](#), par. 20.)

70. Par « signature électronique », on entend a) des données sous forme électronique, qui sont jointes ou associées logiquement à d'autres données sous forme électronique et que le signataire utilise pour signer. Source : Règlement eIDAS, article 3(10) (voir également le document [A/CN.9/WG.IV/WP.144](#), par. 20). ; b) des données sous forme électronique contenues dans un message de données ou jointes ou logiquement associées audit message, pouvant être utilisées pour identifier le signataire dans le cadre du message de données et indiquer qu'il approuve l'information qui y est contenue. Source : Loi type de la CNUDCI sur les signatures électroniques, article 2 a). Note : l'article 9-3 a) de la Convention des Nations Unies sur l'utilisation de communications électroniques dans les contrats internationaux (New York, 2005)⁶ mentionne l'indication de la volonté du signataire concernant l'information contenue dans la communication électronique.

71. Par « horodatage électronique », on entend des données sous forme électronique qui associent d'autres données sous forme électronique à un instant particulier et établissent la preuve que ces dernières données existaient à cet instant. Source : Règlement eIDAS, article 3(33). (Voir également le document [A/CN.9/WG.IV/WP.144](#), par. 20.)

72. Par « service de confiance qualifié », on entend un service de confiance qui satisfait aux exigences du présent texte [Convention, loi modèle]. Source : [A/CN.9/WG.IV/WP.144](#), par. 20.

73. Par « partie utilisatrice », on entend a) une personne qui peut agir sur la base d'un certificat ou d'une signature électronique. Source : Loi type de la CNUDCI sur les signatures électroniques, article 2 f) ; b) une personne physique ou morale qui se fie à une identification électronique ou à un service de confiance. Source : [A/CN.9/WG.IV/WP.144](#), par. 20.

74. Par « signataire », on entend a) une personne physique qui crée une signature électronique. Source : Règlement eIDAS, article 3(9). (Voir également le document [A/CN.9/WG.IV/WP.144](#), par. 20) ; b) une personne qui détient des données afférentes à la création de signature et qui agit soit pour son propre compte, soit pour celui de la personne qu'elle représente. Source : Loi type de la CNUDCI sur les signatures électroniques, article 2 d).

75. Par « service de confiance », on entend un service électronique normalement fourni contre rémunération qui consiste : a) en la création, en la vérification et en la validation de signatures électroniques, de cachets électroniques ou d'horodatages

⁵ Publication des Nations Unies, numéro de vente : F.02.V.8.

⁶ Résolution 60/21 de l'Assemblée générale, annexe.

électroniques, de services d'envoi recommandé électronique et de certificats relatifs à ces services, ou b) en la création, en la vérification et en la validation de certificats pour l'authentification de site Internet, ou c) en la conservation de signatures électroniques, de cachets électroniques ou des certificats relatifs à ces services. Source : Règlement eIDAS, article 3(16).

76. Par « prestataire de services de confiance », on entend une personne physique ou morale qui fournit un ou plusieurs services de confiance[, en tant que prestataire de services de confiance qualifié ou non qualifié]. Source : Règlement eIDAS, article 3(19). (Voir également le document [A/CN.9/WG.IV/WP.144](#), par. 20.)

77. Par « timbre horodateur », on entend un paramètre fiable variant dans le temps, qui désigne un point sur l'axe des temps par rapport à une référence commune. Source : Recommandation UIT-T X.1254.

78. Par « validation », on entend le processus de vérification et de confirmation de la validité d'une signature ou d'un cachet électronique. Source : Règlement eIDAS, article 3(41). (Voir également le document [A/CN.9/WG.IV/WP.144](#), par. 20.)
