Nations Unies A/CN.9/WG.IV/WP.165

Assemblée générale

Distr. limitée
30 septembre 2020
Français
Original : anglais

Commission des Nations Unies pour le droit commercial international
Groupe de travail IV (Commerce électronique)
Soixantième session
Vienne (en ligne), 19-23 octobre 2020

Réexamen de l'approche de la gestion de l'identité et des services de confiance

Proposition des États-Unis d'Amérique

Note du Secrétariat

Les États-Unis d'Amérique ont soumis un document à examiner à la soixantième session du Groupe de travail. On trouvera en annexe à la présente note la traduction du texte de ce document tel qu'il a été reçu par le Secrétariat.

V.20-05629 (F)

Annexe

Réexamen de l'approche de la gestion de l'identité et des services de confiance

1. Les États-Unis sont heureux de soumettre le présent document en rapport avec le projet que le Groupe de travail IV étudie actuellement sur les systèmes de gestion de l'identité et les services de confiance. Ce document se divise en trois sections. La première offre une vue d'ensemble et un résumé des sections suivantes. La deuxième présente le contexte des systèmes de gestion de l'identité et leurs règles de fonctionnement. Enfin, la troisième donne un aperçu du cadre juridique dans lequel fonctionnent généralement tous les systèmes de gestion de l'identité et présente un cadre conceptuel décrivant la manière dont le Groupe de travail pourrait adapter le document WP.162 pour traiter efficacement les systèmes privés de gestion de l'identité.

2. Dans le présent document, les États-Unis se concentrent uniquement sur les systèmes de gestion de l'identité et sur la manière dont le Groupe de travail pourrait les traiter efficacement. Cela dit, ils accueilleraient favorablement le fait que le Groupe débatte de la même manière de la partie du document WP.162 relative aux services de confiance, car nous pensons qu'elle soulève nombre des mêmes questions conceptuelles que celles exposées ci-dessous en ce qui concerne les dispositions relatives à la gestion de l'identité.

I. Vue d'ensemble et résumé

3. Les États-Unis ont des inquiétudes fondamentales quant à l'approche adoptée actuellement par le Groupe de travail en ce qui concerne les systèmes de gestion de l'identité, telle qu'elle est exposée dans le document WP.162 (voir annexe), et estiment qu'il faudrait, pour y répondre, que le Groupe de travail engage un débat conceptuel.

4. La tâche de la CNUDCI devrait être de fournir un cadre qui puisse aider les États à résoudre les problèmes juridiques qui peuvent se poser avec les systèmes privés de gestion de l'identité, en particulier dans les domaines que ne peuvent couvrir les règles de fonctionnement contractuelles qui régissent chaque système. Cela pourrait se faire, par exemple, en révisant le droit national existant pour supprimer les obstacles et les incertitudes qui y figurent, en comblant, dans le droit applicable aux systèmes de gestion de l'identité, les lacunes qui ne peuvent être résolues par contrat, ou en abordant de nouvelles questions susceptibles de promouvoir le développement de systèmes d'identité privés. Or, le document WP.162 adopte une approche sensiblement différente et, selon les États-Unis, inapplicable.

A. Qu'est-ce que des systèmes de gestion de l'identité ?

5. La **gestion de l'identité** consiste en un ensemble de politiques, de processus et de procédures qui permettent d'identifier un individu ou une entité (qui êtes-vous ?) et d'authentifier cette identité (comment pouvez-vous la prouver ?). Comme décrit plus en détail à la section II ci-dessous, une **opération liée à l'identité** est une communication qui fournit certaines de ces informations relatives à l'identité d'un sujet à une partie utilisatrice d'une manière qui authentifie la relation entre ces informations et le sujet. Ces **opérations liées à l'identité** sont facilitées par des systèmes de gestion de l'identité. Les **systèmes de gestion de l'identité** sont des dispositifs complexes qui combinent de manière cohérente des entités participantes, des processus et des technologies, chaque participant assumant un ou plusieurs rôles prédéfinis, conformément à un ensemble prédéfini de processus, de politiques et de procédures juridiquement contraignants, le but étant de faciliter des opérations liées

à l'identité qui permettront à un individu de s'identifier auprès de multiples entités non affiliées.

6. Pour que cela fonctionne, chaque système de gestion de l'identité a besoin d'un ensemble applicable de règles de fonctionnement. Comme décrit plus en détail à la section II ci-dessous, ces règles régissent le fonctionnement de chaque système de gestion de l'identité, précisant comment ses processus et les opérations correspondantes doivent être menés, ainsi que les droits et responsabilités des différentes parties au dispositif. Chaque système de gestion de l'identité étant différent, chacun nécessite un ensemble unique de règles de fonctionnement adaptées à son objectif, à sa structure, à sa base de participants et à son profil de risque.

7. Dans le cas des systèmes publics de gestion de l'identité, les règles de fonctionnement sont généralement énoncées dans une loi ou un règlement, et donc rendues obligatoires pour les participants par la loi. Dans le cas des systèmes privés, ces règles sont définies dans un document rédigé par l'opérateur du système (ou une autre personne ou entité) et rendues obligatoires pour les participants par contrat.

B. Sur quoi un instrument de la CNUDCI devrait-il porter ?

8. Il faudrait que tout instrument élaboré par la CNUDCI pour les systèmes privés de gestion de l'identité tienne compte à la fois du droit national existant et des différentes règles de fonctionnement contractuelles utilisées par chaque système. Plus précisément, il faudrait qu'un tel instrument aborde les questions d'applicabilité du droit national existant aux systèmes privés de gestion de l'identité qui i) ne peuvent être résolues par les règles de fonctionnement contractuelles adoptées par chaque système, ou ii) créent d'autre manière des problèmes pour tous les systèmes privés de gestion de l'identité. Un instrument de la CNUDCI pourrait donc traiter, par exemple, de la reconnaissance juridique d'opérations issues de systèmes privés de gestion de l'identité, des critères à remplir pour déterminer si une opération privée liée à l'identité satisfait à ceux, légaux, à remplir pour identifier une personne, et de l'applicabilité de lois qui, comme celles qui régissent l'utilisation des identifiants gouvernementaux, la protection des consommateurs et la responsabilité civile, ne peuvent être modifiées par les règles de fonctionnement de systèmes de gestion de l'identité.

9. Cette approche se fonde sur la prise en compte du fait que les systèmes privés de gestion de l'identité sont régis par un cadre juridique à trois niveaux, le droit national occupant le sommet (niveau 1) et les règles de fonctionnement contractuelles des systèmes occupant le bas (niveau 3). Le niveau intermédiaire (niveau 2) servirait de passerelle entre les niveaux 1 et 3. L'objectif de la CNUDCI devrait être d'élaborer un instrument qui donne aux États des indications quant au contenu d'un droit de niveau 2. Ce cadre juridique est décrit plus en détail à la section III ci-dessous (y compris la figure 1, qui représente graphiquement les trois niveaux et leur relation). La section III fournit également une feuille de route détaillée sur la manière dont la CNUDCI pourrait réfléchir au contenu d'un tel instrument.

10. Le document WP.162 ne reconnaît pas ce cadre juridique, adoptant une approche fondamentalement différente qui, à notre avis, est inapplicable. Bien qu'abordant certaines questions qui seraient couvertes de manière appropriée par un instrument de niveau 2, il les combine et les confond avec de nombreuses questions qu'il vaudrait mieux résoudre par les règles de fonctionnement contractuelles d'un système de gestion de l'identité (niveau 3). En conséquence, il adopte fréquemment une approche unique pour des questions qui varient largement entre les différentes règles de fonctionnement contractuelles qui régissent les systèmes de gestion de l'identité. Au fil des négociations du projet de texte, il est devenu de plus en plus évident que cette approche n'était pas viable.

11. Le document WP.162 utilise les règles de fonctionnement d'un système public de gestion de l'identité (c'est-à-dire l'eIDAS) comme modèle conceptuel et cherche

à étendre ce modèle à l'ensemble des systèmes de gestion de l'identité. L'eIDAS est en effet une approche très innovante de la réglementation des systèmes de gestion de l'identité et a grandement contribué à faire comprendre dans le monde le fonctionnement de ces systèmes et la manière dont ils pourraient être réglementés pour le secteur public. Le problème, cependant, est que l'eIDAS est un ensemble unique de règles de fonctionnement qui s'applique à un système public unique de gestion de l'identité (composé des différents fournisseurs d'identité des pays de l'UE). Il s'agit donc de l'équivalent public des règles de fonctionnement contractuelles qui régiraient un système privé. Il est inapproprié de tenter d'imposer ces règles à tous les autres systèmes de gestion de l'identité.

12. En d'autres termes, alors que l'eIDAS est un ensemble de règles de fonctionnement destiné à régir *un système unique de gestion de l'identité* (niveau 3), il faudrait que la CNUDCI élabore un instrument qui s'applique à *tous les systèmes* (niveau 2). Alors que l'eIDAS est un ensemble de règles de fonctionnement destiné à régir un système *public* de gestion de l'identité (c'est-à-dire à réglementer les opérations liées à l'identité pour le secteur public), il faudrait que la CNUDCI élabore un instrument qui s'applique aux systèmes *privés.* Plus précisément, il faudrait qu'un instrument de la CNUDCI fasse le lien entre les règles de fonctionnement contractuelles qui régissent chaque système privé de gestion de l'identité (niveau 3) et les aspects du droit national existant (niveau 1) qui ont une incidence négative sur tous les systèmes, mais ne peuvent être résolus par les règles de fonctionnement (comme la reconnaissance juridique des opérations liées à l'identité ou la responsabilité civile)[1].

13. Au lieu de cela, le document WP.162 énonce des règles concernant un certain nombre de questions qui seraient généralement résolues par les règles de fonctionnement de chaque système de gestion de l'identité. Il s'agit de sujets tels que les obligations des prestataires de services de gestion de l'identité (art. 6), les obligations de ces prestataires en cas de violation des données (art. 7), les obligations des abonnés (art. 8) ou la responsabilité des prestataires de services de gestion de l'identité (art. 12). En même temps, le document ne définit pas clairement les cas dans lesquels les parties à un contrat peuvent s'écarter du droit en vigueur sur ces sujets et ceux dans lesquels elles doivent s'y conformer.

14. En outre, alors que le cadre de l'eIDAS, sur lequel se fonde le document WP.162, utilise un mécanisme centralisé pour réglementer, normaliser et certifier les systèmes de gestion de l'identité, il n'existe pas, au niveau mondial, de mécanisme centralisé de ce type capable d'étayer un instrument de la CNUDCI tel que le document WP.162. Ce dernier présuppose simplement l'existence d'un tel mécanisme. En son absence, les dispositions du document relatives à la reconnaissance internationale et aux normes de fiabilité soulèvent un certain nombre de questions qu'il faudrait que le Groupe de travail examine plus avant. En effet, l'eIDAS prévoit la reconnaissance des services de confiance de prestataires établis hors de l'UE uniquement lorsqu'a été conclu un type d'accord spécifique entre l'Union européenne et le pays tiers (art. 14.1 de l'eIDAS).

15. Outre l'incongruité du modèle eIDAS, il est malvenu que le document WP.162 s'appuie sur la Loi type de la CNUDCI sur les signatures électroniques. Les signatures électroniques sont relativement simples et normalisées, tandis que les systèmes de gestion de l'identité sont plus complexes et à plusieurs niveaux. Par exemple, alors que les signatures électroniques impliquent généralement deux parties, les systèmes de gestion de l'identité en impliquent généralement de nombreuses. Les règles de la

[1] Bien que l'eIDAS comprenne sans doute des éléments de niveaux 2 et 3 pour les différents fournisseurs d'identité des pays de l'UE qui acceptent de participer à son cadre unique, nous pensons qu'il faudrait que la CNUDCI se concentre uniquement sur l'élaboration d'un instrument de niveau 2 qui s'appliquerait à tous les fournisseurs de services privés de gestion de l'identité. En outre, l'eIDAS fonctionne comme un système public de gestion de l'identité, alors que la tâche de la CNUDCI est d'élaborer un instrument qui s'applique aux systèmes privés.

Loi type sur les signatures électroniques ne fonctionnent tout simplement pas pour les systèmes de gestion de l'identité.

16. Ces questions fondamentales soulèvent des interrogations élémentaires, mais critiques : en quoi l'approche reflétée dans le document WP.162 serait-elle utile aux États une fois adoptée ? En l'absence d'un mécanisme centralisé de réglementation ou de certification des systèmes de gestion de l'identité ou des services de confiance, comment ce texte accomplira-t-il ce qu'il est censé accomplir, par exemple en ce qui concerne la reconnaissance internationale ou les normes de fiabilité ? Si, comme le comprennent les États-Unis, l'intention est que le document s'applique aux systèmes privés de gestion de l'identité, alors comment les règles qui y sont énoncées se rattachent-elles aux règles de fonctionnement établies par les parties à un contrat qui régit un système de gestion de l'identité ?

17. Les États-Unis ont, dans un premier temps, répondu au modèle du Secrétariat, puis communiqué par écrit leurs réactions au dernier texte ; on trouvera ci-après, dans l'appendice, une analyse article par article du document WP.162. Toutefois, les États-Unis estiment qu'il faudrait, avant de poursuivre l'examen du document WP.162, que le Groupe de travail engage un débat conceptuel pour clarifier la manière dont ledit document s'intégrera dans le cadre juridique général qui régit les systèmes de gestion de l'identité. Tout en appréciant l'important travail fourni pour élaborer le document WP.162 et les efforts faits pour parvenir à un consensus, les États-Unis estiment qu'il serait regrettable que le Groupe de travail persiste sur la voie d'un instrument qui ne serait guère utile aux États Membres ou aux systèmes privés de gestion de l'identité.

18. Comme l'indique le présent document, il existe un certain nombre de domaines dans lesquels le document WP.162 traite de sujets appropriés et pertinents pour la question des systèmes de gestion de l'identité, mais dont l'approche est inapplicable ; dans ces domaines, le Groupe de travail pourrait s'appuyer sur le document WP.162 et y intégrer des changements conceptuels. Dans d'autres, des modifications ou suppressions plus importantes pourraient se justifier.

19. Les États-Unis proposent, à la section III ci-dessous, un cadre destiné à guider la tenue d'un débat conceptuel qui aidera à tracer la voie à suivre.

II. Contexte des systèmes de gestion de l'identité

20. Nous estimons que l'objectif de ce projet devrait être de créer un cadre juridique qui permettra et encouragera le développement d'un solide écosystème dans lequel de multiples systèmes privés de gestion de l'identité de tous types pourront prospérer et appuyer le commerce national et mondial. Pour cela, il faudra identifier, dans la législation nationale existante, les obstacles à lever ou les lacunes à combler. En outre, pour encourager le développement de systèmes de gestion de l'identité nouveaux et différents, il importe que le Groupe de travail évite des solutions uniques pour les questions et les problèmes qui devraient être résolus par les règles de fonctionnement contractuelles uniques établies par chaque système.

21. Pour identifier, dans le cadre juridique, les obstacles à lever et les lacunes à combler pour faciliter la gestion de l'identité, il faut d'abord :

- Examiner les concepts d'opérations liées à l'identité et de systèmes de gestion de l'identité ;
- Examiner la nécessité et le rôle des règles qui régissent le fonctionnement de chaque système privé de gestion de l'identité ;
- Comprendre le cadre juridique général qui régit les systèmes de gestion de l'identité, et déterminer où et comment un instrument de la CNUDCI pourrait être utile/adapté.

22. Le Groupe de travail pourra alors identifier les questions juridiques qui ne peuvent être résolues par les règles de fonctionnement contractuelles uniques qui font partie de chaque système de gestion de l'identité et doivent donc être traitées par des ajouts et des modifications au droit national en utilisant un instrument élaboré par la CNUDCI.

A. Opérations liées à l'identité

23. Une opération liée à l'identité est une communication par laquelle une partie utilisatrice reçoit des informations relatives à l'identité d'un individu [2] (identification), ainsi qu'une vérification que la personne qui prétend être cet individu est bien cet individu (authentification). Elle s'effectue généralement pour soit 1) effectuer une transaction quelconque avec le sujet (conclure un contrat, fournir des avantages, communiquer des informations, etc.), soit 2) lui donner accès à une installation numérique ou physique quelconque (un site Web, une base de données, un bâtiment, etc.).

24. Les opérations liées à l'identité nécessitent généralement 1) la collecte et la vérification d'informations (attributs) sur un sujet de données (processus d'identification), 2) l'émission d'un justificatif contenant un ou plusieurs de ces attributs (processus d'émission d'un justificatif) et 3) l'association des attributs d'identité de ce justificatif à un individu spécifique, souvent éloigné (processus d'authentification). Par ces processus, les opérations liées à l'identité ont pour but de vérifier l'identité d'un individu et d'authentifier la relation de cette identité avec une personne spécifique.

25. Ainsi, par exemple, la présentation de son passeport à la frontière pour obtenir l'admission dans un pays est une opération liée à l'identité. Dans ce cas, la partie qui se fie au passeport (l'agent de contrôle aux frontières) reçoit des attributs d'identité préalablement vérifiés concernant un individu (tels qu'ils figurent dans le passeport), ainsi qu'un moyen de vérifier que la personne qui présente le passeport est bien celle qui y est nommée (c'est-à-dire via la photo ou les données d'empreintes digitales intégrées au passeport). De même, le processus consistant à se connecter à un réseau en ligne avec un nom d'utilisateur et un mot de passe pour obtenir l'accès à une base de données est une opération liée à l'identité. Elle implique l'association (via le mot de passe secret) d'attributs d'identité préalablement vérifiés concernant un individu (référencés via le nom d'utilisateur) avec une personne qui prétend être cet individu (c'est-à-dire la personne qui entre le nom d'utilisateur).

B. Les systèmes de gestion de l'identité sont des systèmes multipartites conçus pour faciliter les opérations liées à l'identité

26. Un **système de gestion de l'identité** est une combinaison cohérente d'entités participantes, de processus et de technologies où chaque participant assume un ou plusieurs rôles prédéfinis[3], conformément à un ensemble prédéfini de processus, de politiques et de procédures juridiquement contraignants, le but étant de faciliter les opérations liées à l'identité.

27. Les systèmes de gestion de l'identité sont des systèmes multipartites complexes. Ils impliquent de multiples participants qui assument divers rôles (autorité d'enregistrement, contrôleur d'identité, fournisseur d'attributs, prestataire de services de confiance, fournisseur d'identité, prestataire de services de justificatifs, prestataire

---

[2] Le sujet d'une opération liée à l'identité peut être un individu, une entité, un dispositif ou un objet numérique. Le présent document se concentrera sur les individus, car ce sont eux qui ont été au centre des débats du Groupe de travail à ce jour.

[3] Ces rôles peuvent être, par exemple, ceux d'autorité d'enregistrement, de contrôleur d'identité, de fournisseur d'identité, d'intermédiaire, de plateforme, de fournisseur d'attributs, de partie utilisatrice, etc.

de services de vérification, plateforme, etc.). Ils coordonnent le travail requis pour recueillir et vérifier l'identité (attributs) d'un sujet de données, émettent un justificatif contenant un ou plusieurs de ces attributs et authentifient ces attributs d'identité auprès d'un individu spécifique dans le cadre d'une opération liée à l'identité. Ces participants travaillent ensemble pour faciliter les opérations liées à l'identité pour de multiples parties utilisatrices.

28. En termes de complexité de structure, un système de gestion de l'identité est analogue à un système de carte de crédit mis en place dans le but de faciliter les opérations de crédit (comme MasterCard ou Visa) ou à un système de paiement électronique mis en place dans le but de faciliter les opérations de paiement (comme SWIFT ou ACH). Bien que chacun de ces types de système ait une structure différente et un but différent, tous sont des systèmes multipartites conçus pour faciliter un type particulier de transaction économique (par exemple, les transactions par carte de crédit, les opérations de paiement ou les opérations liées à l'identité).

29. La structure d'un système de gestion de l'identité peut varier fortement. Par exemple, les systèmes peuvent être centralisés (avec un fournisseur d'identité unique qui facilite les opérations liées à l'identité pour de multiples parties utilisatrices), fédérés (avec un ensemble limité de fournisseurs d'identité qui stockent et fournissent de manière centralisée les informations relatives à l'identité des utilisateurs pour faciliter les opérations liées à l'identité avec une ou plusieurs parties utilisatrices) ou distribués (avec plusieurs fournisseurs d'identité qui authentifient les informations relatives à l'identité stockées localement par les utilisateurs pour faciliter les opérations liées à l'identité avec plusieurs parties utilisatrices). Cette diversité de structure des systèmes de gestion de l'identité est l'une des principales raisons pour lesquelles l'instrument élaboré par le Groupe de travail ne peut, sur de nombreuses questions, adopter une approche unique.

C. Les systèmes de gestion de l'identité ont besoin de règles de fonctionnement juridiquement contraignantes

30. Les systèmes de gestion de l'identité étant des systèmes multipartites complexes, il est essentiel, pour atteindre l'objectif souhaité, que les entités participantes se coordonnent et coopèrent. Ces systèmes nécessitent donc une structure organisée et ciblée qui consiste en des entités participantes interdépendantes et reliées entre elles, remplissant divers rôles, exécutant un ensemble de processus détaillés et suivant un ensemble de politiques et de procédures, tous conçus pour atteindre un objectif spécifique, à savoir faciliter les opérations liées à l'identité.

31. En outre, comme les systèmes de gestion de l'identité impliquent de multiples entités participantes indépendantes qui peuvent interagir entre elles pour effectuer une série d'opérations complexes, ils ne fonctionnent pas automatiquement de manière autonome. Chacun des participants doit être guidé par un ensemble de règles ou d'instructions concernant la manière dont il doit agir pour tenir son rôle spécifique. Il faut en outre, généralement, que ces règles soient juridiquement contraignantes pour que tous les participants respectent les obligations qui leur incombent et puissent compter sur tous les autres pour respecter les règles et produire un résultat fiable.

32. En conséquence, chaque système de gestion de l'identité a besoin, pour fonctionner, d'un ensemble de **règles**[4] juridiquement contraignantes. Ces règles remplissent trois fonctions importantes :

- Elles assurent le **bon fonctionnement** du système, précisant les politiques, les procédures et les processus à suivre pour que le système « fonctionne » comme il est censé le faire ;

[4] Les règles de fonctionnement sont également souvent désignées par d'autres noms : cadre de gouvernance, cadre de confiance, règles d'exploitation, règles de système, etc.

- Elles définissent les **devoirs et obligations** de chacun des participants (par exemple, pour que chacun sache quoi faire), ainsi que ses responsabilités légales, et (au besoin) définissent et répartissent équitablement les risques de mise en jeu de la responsabilité ;
- Elles énoncent des exigences supplémentaires propres à rendre le système de gestion de l'identité « **digne de confiance** » pour l'objectif visé, c'est-à-dire qu'elles imposent des exigences qui vont au-delà de la simple garantie d'un bon fonctionnement et introduisent des mesures supplémentaires qui fassent en sorte que les participants aient confiance dans les opérations liées à l'identité qui en résultent et soient disposés à s'y fier.

33. Pour ce faire, les règles sont généralement conçues pour traiter les questions commerciales, techniques et juridiques spécifiques qui se posent dans le cadre du fonctionnement d'un système de gestion de l'identité particulier. Il peut s'agir, par exemple, de questions telles que les conditions de participation, la définition des rôles et des responsabilités, les processus et procédures d'inscription des sujets de données, le contrôle de l'identité, l'émission de justificatifs et l'authentification de l'identité, les spécifications et normes techniques, les exigences en matière de sécurité des données, les garanties, l'attribution des responsabilités, les procédures de règlement des litiges et les droits de résiliation. Les règles traitent également de la gouvernance du système, qu'il s'agisse des critères à remplir pour y participer, de l'application des règles ou de leur révision. Elles constituent le cadre de gouvernance du système. En outre, la structure, la technologie et l'objectif de chaque système pouvant différer, les règles de fonctionnement de chaque système varieront probablement fortement.

34. Pour que les règles de fonctionnement d'un système de gestion de l'identité soient juridiquement contraignantes, il est possible de leur donner la forme d'une loi, d'un règlement ou d'un contrat.

35. Dans le cas des systèmes **publics** de gestion de l'identité, les règles de fonctionnement prennent généralement la forme d'une **loi** ou d'un règlement détaillé. On peut citer, par exemple, la Loi Aadhaar en Inde[5], la Loi sur les documents d'identité en Estonie[6] et l'eIDAS dans l'UE[7]. Cependant, certains systèmes publics, comme le système GOV.UK.Verify, recourent à des contrats[8].

36. Dans le cas des systèmes **privés** de gestion de l'identité, les règles de fonctionnement prennent la forme d'un **contrat** qui lie les participants (tout comme les participants à un système de carte de crédit ou de paiement acceptent par contrat les conditions qui s'appliquent à eux). Comme exemples de règles de fonctionnement de systèmes privés, on peut citer le Cadre de confiance SAFE[9], le Cadre de gouvernance Sovrin[10] et le Cadre de confiance pancanadien[11]. Voir également le « Guide des cadres de confiance et de l'interopérabilité »[12].

---

[5] Loi Aadhaar (Offre ciblée de subventions financières et autres, de prestations et de services), 2016, consultable à l'adresse https://uidai.gov.in/images/targeted_delivery_of_financial_and_other_subsidies_benefits_and_services_13072016.pdf.

[6] Loi sur les documents d'identité, adoptée le 15 février 1999, RT I 1999, 25, 365, entrée en vigueur le 1er janvier 2000, consultable à l'adresse https://www.riigiteataja.ee/en/eli/ee/504112013003/consolide.

[7] Le règlement (UE) n° 910/2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur (règlement eIDAS), adopté le 23 juillet 2014, offre un environnement prévisible qui permet des interactions électroniques sécurisées entre les citoyens, les entreprises et les autorités publiques ; consultable à l'adresse https://ec.europa.eu/futurium/en/content/eidas-regulation-regulation-eu-ndeg9102014.

[8] https://www.gov.uk/government/publications/introducing-govuk-verify/introducing-govuk-verify.

[9] https://www.globenewswire.com/news-release/2020/05/19/2035512/0/en/SAFE-Identity-Announces-Revamped-SAFE-Biopharma-Trust-Framework-and-New-Services-to-Expand-and-Evolve-Digital-Trust-in-Healthcare-Sector.html.

[10] https://sovrin.org/library/sovrin-governance-framework.

[11] https://drive.google.com/file/d/1Xmjh8QJZKWmRkaTtE2f43ISntD7jE6D5/view.

[12] Open Identity Exchange, « A Guide to Trust Frameworks and Interoperability », consultable à l'adresse https://openidentityexchange.org/guide-trust-frameworks-interoperability.

D. Les règles de fonctionnement sont uniques à chaque système de gestion de l'identité

37. Chaque système de gestion de l'identité étant différent, il nécessite un ensemble unique de règles de fonctionnement adaptées à sa structure, à sa technologie, à son objectif, à son marché et à son profil de risque.

38. Les systèmes privés de gestion de l'identité utilisent une grande variété de **structures** et de **technologies**, dont chacune appellera une approche différente des règles de fonctionnement. Le développement de ces systèmes sera entravé par toute tentative d'imposer un ensemble uniforme de règles de ce type à tous les systèmes.

- Comme exemples de différentes **structures de système** de gestion de l'identité identifiées par le Forum économique mondial en 2016[13], on peut citer les systèmes internes, externes, centralisés, fédérés et distribués. Comme autres structures de système utilisées plus récemment, on trouve les systèmes de type plateforme et les systèmes d'identité auto-souveraine, ainsi que les systèmes en cours de développement avec les téléphones portables. Chacun de ces systèmes nécessitera une approche différente des règles de fonctionnement et souffrira de toute tentative d'imposer un ensemble uniforme de ces règles à tous les systèmes.

- Comme exemples de différentes **technologies de système** de gestion de l'identité, on peut citer les systèmes fondés sur des infrastructures à clefs publiques (ICP), les systèmes basés sur des chaînes de blocs et les systèmes qui utilisent les normes OAuth et OpenID Connect, chacun d'eux nécessitant une approche différente des règles de fonctionnement et souffrant de toute tentative d'imposer un ensemble uniforme de ces règles à tous les systèmes.

39. Les systèmes privés de gestion de l'identité sont aussi généralement conçus pour divers **objectifs et/ou marchés** différents, ce qui nécessitera d'adopter, dans les règles de fonctionnement, diverses approches, exigences de confiance et répartitions des risques. Le développement de ces systèmes sera entravé par toute tentative d'imposer un ensemble uniforme de règles de ce type à tous les systèmes.

- Comme exemples de systèmes de gestion de l'identité conçus à des **fins** et pour des **marchés** différents, on peut citer le système InCommon conçu pour l'enseignement (par exemple, les universités et les étudiants), le système SAFE BioPharma conçu pour l'industrie pharmaceutique, le système CertiPath conçu pour l'industrie aérospatiale internationale, le système CA Browser Forum conçu pour identifier les opérateurs de sites Web, le système ZenKey conçu pour l'identité mobile, et les systèmes légers Google, LinkedIn et Facebook conçus pour un accès à faible risque aux sites Web.

40. Ces règles de fonctionnement étant conçues pour répondre aux exigences uniques d'un système de gestion de l'identité particulier, il faudrait que les questions qu'elles résolvent sortent du champ d'application de l'instrument que le Groupe de travail élabore actuellement.

41. Les règles de fonctionnement des systèmes privés de gestion de l'identité étant fondées sur un contrat et liées aux exigences uniques d'un système particulier, il ne faudra pas qu'un instrument élaboré par la CNUDCI tente de les reproduire dans une approche unique applicable à tous les systèmes. Ainsi, le défi, pour le Groupe de travail, sera d'élaborer un instrument qui n'empiète pas sur la nécessité ou la capacité qu'a un système privé d'élaborer ses propres règles de fonctionnement, tout en précisant les obligations légales auxquelles ces règles devront se conformer.

---

[13] Voir Forum économique mondial, « A Blueprint for Digital Identity », août 2016, consultable à l'adresse http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdfhttp://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf.

III. Cadre juridique régissant les systèmes privés de gestion de l'identité et éventuel instrument de la CNUDCI

A. Cadre juridique général

42. Préalablement à l'élaboration d'un instrument du type envisagé par le document WP.162, nous estimons qu'il faudrait que le Groupe de travail examine la structure du cadre juridique général qui régit les systèmes privés de gestion de l'identité. Plus précisément, il faudrait qu'il examine comment i) les règles de fonctionnement des différents systèmes privés de gestion de l'identité et ii) l'instrument proposé par la CNUDCI s'inscriraient dans ce cadre. Cela sera important pour déterminer les questions à traiter dans cet instrument.

43. Les systèmes privés de gestion de l'identité sont, comme la plupart des systèmes de transactions commerciales multipartites, généralement régis par un cadre juridique combinant i) droit élaboré par le gouvernement et ii) contrats conclus par les entités participantes. Le **droit élaboré par le gouvernement** est constitué des règles promulguées sous forme de lois par les corps législatifs, adoptées sous forme de règlements par les organismes publics ou déterminées par une décision judiciaire. Le **droit contractuel** est constitué des règles rédigées par un ou plusieurs participants ou organes directeurs du système de gestion de l'identité (c'est-à-dire des règles de fonctionnement du système), qui sont rendues obligatoires pour les participants par contrat.

44. Le cadre juridique dans lequel opère tout système privé de gestion de l'identité comprend généralement jusqu'à trois niveaux de droit, chaque niveau successif régissant les systèmes de plus en plus précisément. Ces trois niveaux sont décrits comme suit (et illustrés dans le diagramme de la page suivante) :

- **(Niveau 1) Droit existant** : Le niveau supérieur, et le plus général, est simplement le **droit national existant**. Il s'agit du droit élaboré par le gouvernement, y compris les lois, les règlements et les décisions judiciaires. Ce droit régit tous les types d'activité commerciale, n'a pas été écrit spécifiquement pour les systèmes de gestion de l'identité et peut, dans certains cas, être vieux de plusieurs centaines d'années. Néanmoins, il s'applique fréquemment aux activités des systèmes privés de gestion de l'identité. Cela inclut le droit général des contrats, le droit de la responsabilité civile, le droit de la vie privée, le droit du contrôle des exportations, le droit des garanties, le droit de la protection des consommateurs, le droit de la concurrence, le droit bancaire, etc.

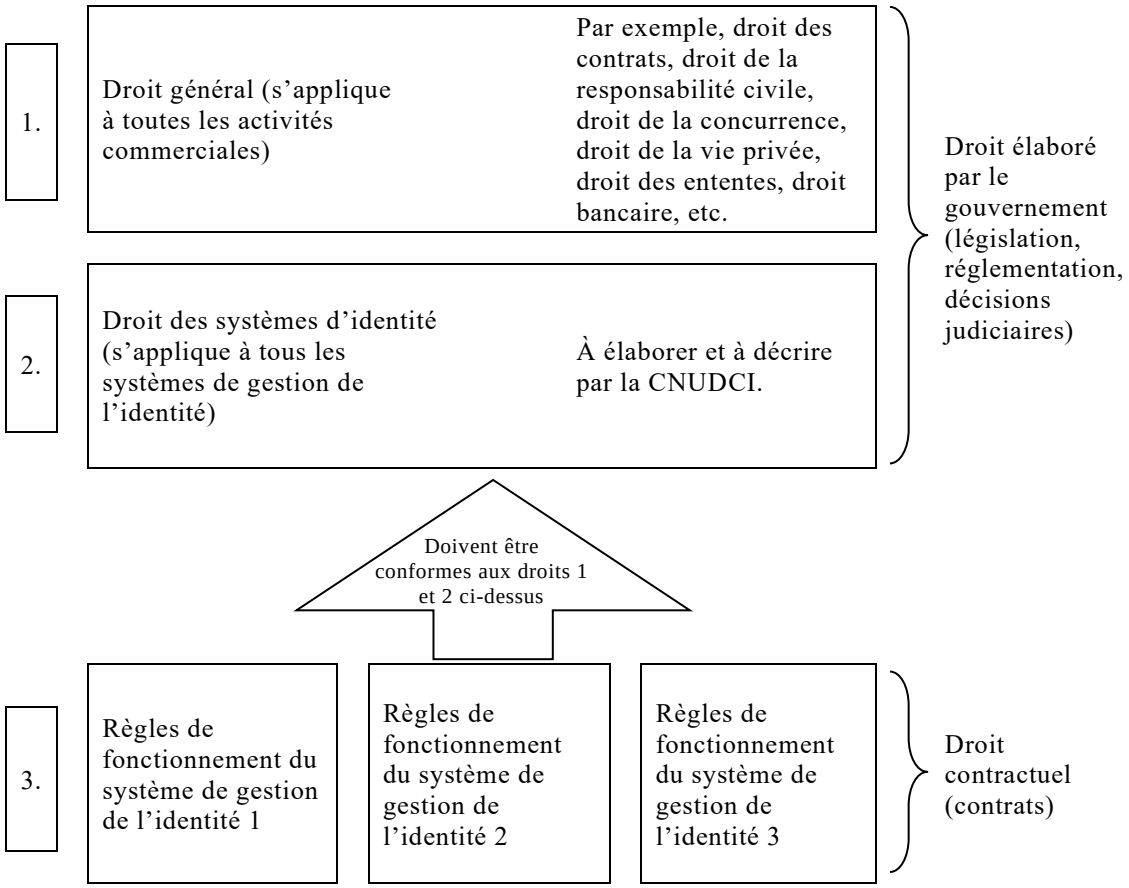
- **(Niveau 2) Droit des systèmes d'identité** : Le deuxième niveau de droit qui régit les systèmes privés de gestion de l'identité peut être appelé **droit des** systèmes **d'identité**. Il est écrit expressément pour régir ***tous*** les systèmes privés de gestion de l'identité, quels que soient leur type, leur structure, leur technologie ou leur objectif. Il émane également du gouvernement, est conçu pour traiter les problèmes que le droit de niveau 1 pose à tous les systèmes de gestion de l'identité, et peut combler certaines des lacunes que ce droit ne traite tout simplement pas. Il devrait s'insérer entre le droit de niveau 1 et les règles de fonctionnement contractuelles de niveau 3.

- **(Niveau 3) Règles de fonctionnement de chaque système de gestion de l'identité** : Le troisième niveau de droit qui régit les systèmes privés de gestion de l'identité consiste en des règles de fonctionnement contractuelles, rédigées spécifiquement par chaque système pour régir son propre environnement. À la différence du droit des systèmes d'identité, qui s'applique à tous les systèmes de gestion de l'identité, les règles de fonctionnement sont conçues pour

répondre aux exigences uniques d'un système particulier[14]. Elles peuvent être très détaillées, mais doivent être conformes aux droits de niveaux 1 et 2.

45. La tâche du Groupe de travail consiste à élaborer un instrument qui décrive les éléments d'un droit de niveau 2.

Figure 1
Cadre juridique pour les systèmes privés de gestion de l'identité : trois niveaux de droit



B. Que devrait faire un instrument de la CNUDCI ?

46. Pour éviter d'adopter une approche unique qui entrave le développement des systèmes privés de gestion de l'identité et des activités commerciales associées, il faudrait que le Groupe de travail élabore un instrument qui ne traite que des questions qui ne peuvent être résolues dans les règles de fonctionnement de chaque système. Il faudrait en outre qu'il se limite à modifier ou à compléter le droit national existant uniquement dans la mesure requise pour encourager et promouvoir le développement de systèmes privés de gestion de l'identité afin de soutenir l'activité commerciale en ligne. Cela implique de concevoir un instrument de niveau 2 qui :

- Supprime les obstacles et les incertitudes du droit existant qui entravent le développement des systèmes privés de gestion de l'identité ;
- Comble les lacunes du droit existant qui entravent le succès des systèmes privés de gestion de l'identité, mais ne peuvent être comblées par contrat ;

[14] Noter que dans le cas des systèmes publics de gestion de l'identité (système national d'identité, par exemple), les règles de fonctionnement spécifiques au système sont incorporées dans une loi ou un règlement. Ainsi, les droits de niveau 2 et 3 sont combinés.

- Aborde de nouvelles questions d'application universelle pour promouvoir le développement de tous les systèmes privés de gestion de l'identité.

47. En outre, étant donné la diversité des systèmes d'identité et les besoins uniques de chacun, il faudrait que tout instrument de niveau 2 élaboré par le Groupe de travail respecte les principes de neutralité technologique et de neutralité des systèmes d'identité. Cette dernière, en particulier, est essentielle compte tenu de la grande diversité des structures, des technologies, des objectifs et des marchés utilisés par les systèmes privés de gestion de l'identité, comme on l'a vu ci-dessus.

48. À l'opposé, le document WP.162 est rédigé de manière à imposer des règles en ce qui concerne les *obligations des prestataires de services de gestion de l'identité* (art. 6), les *obligations des prestataires de services de gestion de l'identité en cas de violation de données* (art. 7), les *obligations des abonnés* (art. 8) ou la *responsabilité des prestataires de services de gestion de l'identité* (art. 12). Or, c'est aux systèmes privés de gestion de l'identité qu'il revient de traiter ces questions dans leurs règles de fonctionnement. Chacune de ces questions nécessitera une approche unique adaptée à la structure, à la technologie, à l'objectif et au marché du système concerné. Toute tentative de les aborder sera source de problème, car elles varieront probablement fortement d'un système à l'autre, et imposer une approche unique ne fera qu'entraver le développement des systèmes privés de gestion de l'identité.

C. Schéma d'un instrument de la CNUDCI

49. Les questions que pourrait traiter le Groupe de travail relèvent plutôt des catégories suivantes[15] :

- Reconnaissance explicite du rôle des règles de fonctionnement pour la gouvernance des systèmes de gestion de l'identité ;
- Questions non traitées dans le droit de niveau 1 et qui, de par leur nature, ne peuvent être traitées par des règles de fonctionnement contractuelles. Exemples :
    - Reconnaissance juridique de la gestion de l'identité[16] ;
    - Critères à remplir pour déterminer si une opération liée à l'identité satisfait à ceux, légaux, à remplir pour identifier une personne[17] ;
    - Question de savoir s'il faudrait (et si oui, comment) évaluer la fiabilité des systèmes privés de gestion de l'identité[18].
- Questions traitées dans une certaine mesure dans le droit de niveau 1, mais avec une applicabilité incertaine aux systèmes de gestion de l'identité, créant ainsi une ambiguïté qui peut constituer un problème pour ces systèmes en raison de la difficulté de les traiter dans des règles de fonctionnement contractuelles. Exemples :
    - Applicabilité du droit existant de la responsabilité civile aux participants à des systèmes de gestion de l'identité ;
    - Applicabilité du droit relatif aux déclarations inexactes faites par négligence ;

---

[15] Il s'agit là d'une liste préliminaire de questions qui pourraient être abordées dans un instrument de niveau 2, sous réserve de son élaboration et de son affinement par le Groupe de travail, et sur la base des besoins des divers régimes nationaux existants, entre autres facteurs.

[16] L'article 5 du document WP.162 vise à régler cette question. Voir nos commentaires concernant les problèmes liés à l'actuel projet d'article 5 dans l'appendice.

[17] L'article 9 du document WP.162 vise à régler cette question. Voir nos commentaires concernant les problèmes posés par l'actuel projet d'article 9 dans l'appendice.

[18] L'article 11 du document WP.162 vise à régler cette question. Voir nos commentaires concernant les problèmes liés à l'actuel projet d'article 11 dans l'appendice.

- Applicabilité du droit existant aux garanties implicites.

• Questions qu'il pourrait falloir ajouter au droit existant. Exemples :

- Droit, pour les systèmes de gestion de l'identité, d'utiliser des informations provenant de systèmes gouvernementaux de gestion de l'identité ;
- Droit, pour les systèmes de gestion de l'identité, d'utiliser des identifiants délivrés par le gouvernement (numéro de sécurité sociale, numéro national d'identité, etc.).

• Questions qui, indépendamment du fait qu'elles puissent être traitées par des règles de fonctionnement contractuelles, devraient être traitées de la même manière par tous les systèmes de gestion de l'identité en raison de considérations d'ordre public. Exemples :

- Question de savoir s'il faudrait prévoir une reconnaissance internationale et, dans l'affirmative, comment[19] ;
- Question de savoir s'il faudrait aborder la question de la fiabilité d'un point de vue juridique et, dans l'affirmative, comment[20].

50. Un instrument de la CNUDCI contenant ces éléments aidera les États à créer un droit des systèmes d'identité de niveau 2 qui 1) encouragera le développement des systèmes privés de gestion de l'identité, 2) éliminera les obstacles à ce développement et 3) respectera et appuiera la nécessité, pour chaque système privé de gestion de l'identité, d'élaborer ses propres règles de fonctionnement dans la mesure du possible.

[19] Les articles 10 et 11 du document WP.162 visent à traiter cette question. Voir nos commentaires concernant les problèmes liés aux projets actuels d'articles 10 et 11 dans l'appendice.

[20] Les articles 10 et 11 du document WP.162 visent à traiter cette question. Voir nos commentaires concernant les problèmes liés aux projets actuels d'articles 10 et 11 dans l'appendice.

Appendix[21]

Article-by Article Analysis of WP.162

In this appendix to our comments, we provide a detailed article-by-article commentary on WP 162. We reiterate, though, that we do not believe that a simple set of revisions to the text of WP 162 will result in a viable instrument. To achieve this, we believe the Working Group must make the conceptual and structural changes required to address the current reality of IdM systems that we set forth in Sections II and III of our comments.

Before turning to the article-by-article analysis, here is a summary of the U.S. concerns with WP.162:

(a) The definitions in WP 162 are both incomplete and based on a static model for IdM that is not reflective of the wide variety of actual IdM systems;

(b) WP.162 does not provide a basis for determining how and when the instrument would accede to or supersede existing laws that require identification in a specific form. The failure to provide guidance on this issue is compounded by the fact that articles 2, 5 and 9 contradict one another;

(c) The articles on obligations (art. 6–8) and liability (art 12) do not reflect the wide variations among types of IdM systems nor the multiple types of roles that may make up any specific IdM system. These one-size-fits all provisions do not accurately reflect the rights and obligations that different IdM system roles may have or expect in various IdM systems;

(d) We do not believe the provisions on cross-border recognition are workable without an enacting jurisdiction having some basis for assuming the reliability of a system in another jurisdiction. We do not believe this obligation is realistic.

Draft Article 1: Definitions

We believe the Working Group should revisit the definitions after the articles in the rest of the draft are concluded. Base on the current draft,[22] we make the following observations for consideration by the Working Group.

The term “electronic identification” may describe or be easily confused with the entire process of identity proofing, credential issuance, and authenticating the relationship between the credential data and an individual. Thus, we recommended that the Working Group consider whether there is an alternative term to “electronic identification” that could be used for the authentication process.

All the stages of the IdM process might collectively be defined as “identity verification.” The modifier “electronic” should not be used in this definition, however, since all or part of the stages of the IdM process might not be done electronically.

“Authentication” is used only in terms of trust services; it has the same meaning as “electronic identification”. We believe it could be misleading to have two terms for the same concept and would recommend using the same term for this concept throughout the draft. As noted above, however, we believe the term “electronic identification” itself may be misleading.

---

[21] The Appendix has been provided to Member States in English only. However, significant portions of the substance of the Appendix are a reproduction of the U.S. response to the Secretariat’s questionnaire for A/CN.9/WG.IV/WP.162, which has been circulated in all official languages as A/CN.9/WG.IV/WP.164 and Add.1.

[22] A/CN.9/WG.IV/WP.162.

As to the secretariat's inquiry whether there should be a definition of levels of assurance, we believe such a definition is unnecessary. We note the secretariat's proposed language provides that "identification factors are those factors that are necessary to make an electronic identification" In other words, the proposed definition does not provide any guidance; it simply restates the obvious. Moreover, we believe this proposed language could cause confusion, as it implies that there are specific factors that an IdM service provider must manage. Depending on the nature of the identity system involved, there could be numerous such factors. The relevant factors, however, will vary from IdM system to IdM system, and the responsibility for managing these factors will vary from system role to system role.[23] We note also that the proposed definition appears to combine two very different concepts: identity attributes (that vary depending on purpose for which identity is used), and identity processes that are used for identity proofing, credential issuance, or authentication processes.

Draft Article 2: Scope of application

The draft instrument provides that it "applies to the use and cross border recognition of IdM systems and trust services in the context of commercial activities and trade related services." As we discuss below, we believe the Working Group needs to closely examine how the draft instrument will apply to cross-border transactions, and how the rules in this instrument relate to existing legal requirements regarding identification and authentication.

Draft article 2(3) provides that "[n]othing in this [instrument] affects a legal requirement that a [subject][person] be identified in accordance with a procedure defined or prescribed by law." We understand this exclusion as being necessary as most if not all jurisdictions have some mandatory requirements for the form in which identification is to be made.

The question then is whether this section can be reconciled with articles 5(a), which provides that "The electronic identification of a [subject][person] shall not be denied legal effect, validity, enforceability or admissibility as evidence on the sole ground that …[t]he identity proofing and electronic identification are in electronic form" and article 9(1) option A, which provides that " Where a rule of law requires or permits the identification of a [subject][person], that rule is satisfied with respect to IdM if a reliable method is used for the electronic identification of the [subject][person]."

We believe article 2(3) and article 5(a) might be reconciled by expressly clarifying these two sections to indicate that article 5(a) is not intended to overrule any other law, but is only intended to provide that, as between the parties, the law will not block the choice of the parties to use an electronic means of identification if the law would otherwise allow this under freedom of contract. This reading would appear to narrow the scope of article 5, and if the Working Group intended article 5 to have this limited meaning, this needs to be clarified in the text and comments.

We do find a more serious problem reconciling draft article 2(3) with draft article 9(1) Option A. These two sections, we believe, cannot be reconciled. Were the instrument intended to supersede all laws that may require a specific mode of identification, the instrument would risk being non-enactable. In addition, this interpretation would expressly contradict the language of draft article 2(3). In our view, the draft instrument provides contradictory rules: electronic identification meets the requirements of other legal identification requirements, and the instrument does not displace any other legal identification requirements. These conflicting rules cannot co-exist if the draft instrument. We view Option B of draft article 9 as essentially

[23] This potential confusion raises the issue of whether draft article 6 may itself create minimum obligations that should not necessarily apply to all IDM service providers. In other words, article 6 may assume a one size fits all IDM service provider that does not reflect the multitude of existing and developing models.

restating the rule of Option A. We believe the Working Group must re-examine these draft articles and reformulate them to express a non-contradictory policy that respects the existing legal requirements that are recognized in draft article 2(3).

Draft Article 3: Voluntary use of IdM and trust services

We believe both the current text of the draft[24] as well as the proposed new language by the secretariat[25] shows confusion on the role of consent. We suggest the Working Group examine the rule on consent to determine which parties are required to consent and the relationship between article 3 on consent and how it works with both article 2 and 5 on freedom or lack of freedom to choose the mode of identity management.

Draft Article 4: Interpretation

Although we appreciate that this language has appeared in prior model laws,[26] we note this language was drawn from the United Nations Convention on Contracts for the International Sale of Goods,[27] and it is language specifically tailored for an international convention. As such, we are not sure that it is appropriate for a model law that is drafted for domestic legislation.

Thus, for example, we are not clear on what the "international character" of the draft model law refers to. As the draft instrument is neither derived from international instrument nor intended to be used primarily in international transactions, we do not know what constitutes the instrument's "international character".

Moreover, although uniformity of interpretation is a useful admonition for an international convention,[28] the utility of this interpretive rule is not clear in an instrument designed for domestic legislation. When, as with an international convention, an autonomous interpretation is useful to create a universal understanding that parties can rely upon in international commercial transactions, the application of this rule is unclear and probably redundant for a domestic law.

As for the rule that the instrument should be interpreted on the general principles on which it is based,[29] we suggest that either the draft provide the guidance of what these principles are[30] or this rule should be removed. To do otherwise creates the risk of vagueness and uncertainty in the text.[31]

---

[24] A/CN.9/WG.IV/WP.162, draft article 3.

[25] "There have been questions about the relationship between articles 2 and 3. Would their relationship be clearer by recasting article 3 to state that "Nothing in this [instrument] requires a [person][relying party] to accept the electronic identification of a subject or to rely on a trust service without the [person's][relying party's] consent. "?".

[26] UNCITRAL Model Law on Electronic Commerce (1996), article 3; UNCITRAL Model Law on Electronic Signatures (2001), article 4.

[27] United Nations Convention on Contracts for the International Sale of Goods (1980), article 7.

[28] We note this language is also derived from the CISG.

[29] A/CN.9/WG.IV/WP.162, footnote 23.

[30] We note that a statement of underlying principles was removed from the last draft.

[31] The Working Group may want to consider the comments of the World Bank in WP.163 to ensure that the Draft Provisions do not discriminate among IdM system models by including the concept of IdM system neutrality (or identity transaction neutrality). Because there are many different ways of conducting online identity transactions (e.g., single identity provider (IdP) systems, federated (multiple IdP) systems, user controlled/user centric systems, hub systems, DLT systems, systems without credentials, self-sovereign identity systems, etc.), it is important that these Draft Provisions do not require or assume a particular approach to the identification and/or authentication processes, or the system that delivers them. Thus, the Working Group should consider ways to ensure that these Draft Provisions do not imply and/or require a certain system model.

Draft Article 5: Legal recognition of IdM

As we discussed above in our analysis of draft Article 2, we believe the Working Group needs to clarify how this rule is intended to work with identifications that are required to be in a specific form such as a driver's license or passport.

Draft Article 6: Obligations of IdM service providers

As noted in Sections II and III of our comments, this issue is best addressed by each IdM system in its own Operating Rules and in a manner that is tailored to the unique structure, technology, purpose, market, and risk profile that IdM system, rather than in an UNCITRAL instrument designed to cover all IdM systems. In addition, even if it were appropriate for UNCITRAL to address this topic, the current approach is unworkable and out of keeping with the reality of IdM systems.

As noted in the World Bank's comments,[32] the obligations set out in draft article 6 for IdM service providers assume a model where the IdM service provider provides all the services. This may not always be the case. There could be several parties that contribute to or provide part of an IdM service (e.g., trust providers, registrars, enrolment agents, credential service providers, stewards, authentication providers, hubs, etc.). Given the increasing diversity of IdM system models, the Working Group should consider whether it is still appropriate to restrict the definition of the roles or to impose a one-size-fits-all set of IdM service provider obligations. We believe the Working Group needs to address article 6 to consider the potential multiple parties that may contribute to the IdM service, and to consider whether it is still appropriate to impose a one-size-fits-all set of IdM service provider obligations.

Draft Article 7: Obligation of IdM service providers where there is a breach

As noted in Sections II and III of our comments, this issue is best addressed by each IdM system in its own Operating Rules and in a manner that is tailored to the unique structure, technology, purpose, market, and risk profile that IdM system, rather than in an UNCITRAL instrument designed to cover all IdM systems. In addition, even if it were appropriate for UNCITRAL to address this topic, the current approach is unworkable and out of keeping with the reality of IdM systems. We agree that there should be some obligations by an IdM service provider where there has been a breach of security. As we noted note our comments to draft article 6, however, there may be multiple parties involved in the IdM service provider process.[33] For this reason, we believe the Working Group should reconsider the language of draft article 7 to reflect the various parties that may be involved in IdM process and accordingly fix the obligations based on the respective nature and status of these parties consistent with which party is best placed to respond to the breach.

Draft article 7 is limited to breaches that have "a significant impact". We do not understand what "significant impact "means in this context. In addition to being a vague standard, we are not sure why a "breach" is not enough in and of itself to justify some remedial action by the entity that bore the risk the breach.

We are not sure what "remedies" are or should be available where there has been a breach of security.[34] We believe the Working Group should clarify this issue.

---

[32] A/CN.9/WG.IV/WP.163.

[33] We agree with the comments by the World Bank in WP.163 that the current draft compresses and confuses the distinction between and the respective roles of IdM systems and IDM service providers.

[34] See Draft article 7(1)(b).

We do not know what "applicable law" refers to in 7(1)(c). If it refers to a notification obligation from the draft instrument, this obligation should be referred to. If this refers to law outside of the instrument, it is not clear what law would impose an obligation of notification.

Draft Article 8: Obligation of subscribers

As noted in Sections II and III of our comments, this issue is best addressed by each IdM system in its own Operating Rules and in a manner that is tailored to the unique structure, technology, purpose, market, and risk profile that IdM system, rather than in an UNCITRAL instrument designed to cover all IdM systems. In addition, even if it were appropriate for UNCITRAL to address this topic, the current approach is unworkable and out of keeping with the reality of IdM systems.

We agree with the comments by the World Bank that the duties imposed on subscribers (particularly individuals, such as data subjects) in Article 8 may not be reasonable in all circumstances.[35] For example, there may be situations where an individual subscriber may be aware of circumstances indicating there may have been a compromise, but simply does not understand their significance.

We believe Article 8 should be clarified that it is not intended to impose these duties on relying third parties that have no contractual relationship with the issuing IdM service provider but who may nonetheless rely on a credential because:

(a) it would be difficult to enforce as it will likely be hard to identify such relying third parties;

(b) it imposes an undue burden on relying third parties to police identity system credentials for an IdM service provider with whom they have no relationship; especially when their use of and reliance on such credentials may be sporadic at best; and

(c) it is not currently required by law applicable to paper-based credentials (e.g., the bartender who refuses entry to a person because he determines that the person has presented a false driver's license or someone else's driver's license is not required to report that to the issuing authority).[36]

The requirement to notify in cases of a "substantial" risk seems problematic, as subscribers will likely have no way of knowing (and in most cases will not even be qualified to determine) what constitutes a substantial risk as opposed to some lesser risk.

Draft Article 9: Identification of a person using IdM

We address our concerns on draft article 9 in our discussion of draft article 2 above.

Draft Article 10: Factors relevant in determining reliability

As noted in Sections II and III of our comments, this issue is best addressed by each IdM system in its own Operating Rules and in a manner that is tailored to the unique structure, technology, purpose, market, and risk profile that IdM system, rather than in an UNCITRAL instrument designed to cover all IdM systems. In addition, even if

[35] A/CN.9/WG.IV/WP.163.

[36] We also agree with the comments by the World Bank in WP.163 that if the draft is going to raise issues about third parties, more clarification would be useful as to which third parties are envisaged. We also note that if there is going to be a notification requirement on non-contracting parties, there needs to be some sanction for failure to notify, as otherwise the requirement is meaningless.

it were appropriate for UNCITRAL to address this topic, the current approach is unworkable and out of keeping with the reality of IdM systems.

Draft article 10 provides an illustrative list of factors to determine the reliability of an IdM service. If article 10 only applies to systems governed by contractual rules, it is not clear what the purpose of the list of possible considerations serve. This list is not useful to explain and interpret an otherwise applicable contractual agreement. If draft article 10 is intended to provide a minimal standard of reliability for IdM systems, then it is not clear how an illustrative and not a mandatory list would operate.

Moreover, it is not clear how this would override, if at all, otherwise agreed to contractual standards.

Moreover, in any given situation, there are numerous factors that may affect reliability. We question whether attempting to list them in these rules is appropriate in any event.

Draft Article 11: Designation of reliable IdM systems

Although this provision is made optional, as we note in our analysis of draft article 24, this section may impose quite a financial and administrative burden to implement by a jurisdiction that adopts this instrument. We recommend to the Working Group that this provision be bracketed with extensive commentary to explain how similar provisions have been implemented elsewhere and what an implementation would entail.

In addition, we believe this provision, as presently drafted, rests on the flawed assumptions that there are “recognized international standards and procedures” for determining the reliability of a IdM service, and that there is a centralized body that can make these determinations.

Draft Article 12: Liability of IdM service providers

As noted in Section III of our comments, this issue is best addressed by each IdM system in its own Operating Rules and in a manner that is tailored to the unique structure, technology, purpose, market, and risk profile that IdM system, rather than in an UNCITRAL instrument designed to cover all IdM systems. In addition, even if it were appropriate for UNCITRAL to address this topic, the current approach is unworkable and out of keeping with the reality of IdM systems.

We do not believe any of the three options in the current draft are sufficient. Both Options A and B state, albeit unartfully, that an IdM service provider will be legally responsible under otherwise applicable law outside of this instrument. If liability rules are to be included in this instrument, some guidance would be necessary. The term “applicable law” is vague. Does this refer to contract law, tort law, privacy law, data security law, etc. or all of them? If the answer is it could apply to any law otherwise deemed to be appropriate, then no function is served by this provision. Likewise, we have no idea what type of guidance is intended by the phrase “legal consequences”.

The word “damage” in option 3 we assume means “harm”, but as with all the options in the current draft, we fear no real guidance or standards are provided.

We suggest that the rules governing liability should likely vary depending upon the nature of the identity system, and will most likely to be determined by the applicable trust framework (subject, of course, to any existing law that cannot be varied by agreement).

At a minimum, we believe a further discussion is warranted on what type of liability the rules of the draft would invoke. We think a discussion of liability should go beyond service providers and consider liability for all parties that may come within the scope of the draft. We also believe that a discussion on contractual waivers to

liability should be included in any discussion on liability. Further, as noted above, we do not believe that a universal one-size-fits-all approach to liability is appropriate in any event, as identity systems, their purposes, and their participants will vary widely.

Draft Article 13: Legal recognition of trust services

As we have noted, we believe trust services should be addressed in a separate instrument.

This provision states that a trust service may be provided in electronic form. As the purpose of a trust service is, in fact, to verify electronic data, this provision would appear to be tautological and unnecessary. If the intent of draft article 13 is to make clear that a third party may provide a trust service, that should be clarified.

Draft Article 14: Obligations of trust service providers

As a conceptual matter, this draft provision raises two questions. First, how does this provision interact with contractual obligations that a trust service provider may have to remedy a breach of loss of integrity? If the intent of Article 14(2) is to impose obligations for breaches or losses of integrity that are not covered by contract (i.e., because it refers to impact on the trust service itself), this should be made clear.

If the intent is to impose some minimal obligation on trust service providers below which the parties cannot contract, this should be expressly stated. If that is the intent, we believe the Working Group should address the question of mandatory rules and their relationship to freedom of contract.

A second question unexamined in this draft provision is the question of the consequence for failing to meet the obligations set out in Article 14? If a trust service provider fails to fulfil a contractual obligation owed to a customer, then customer/other party to the contract could pursue a contract claim. Article 14 does not appear to impose any consequences or sanction for failure to fulfil the obligations set out therein, assuming they are distinct from contractual obligations.

Draft Article 15: Obligations of trust service providers

This draft article, as with draft article 14, purports to impose obligations without any corresponding sanctions. As we mentioned in our comments to draft article 12, we believe the Working Group needs to examine fully the question of liability throughout the draft instrument.

Draft Articles 16–20: Various trust services

Articles 16–20 address the issue of the validity of a data message (such as an e-signature) and not the use of a trust service to validate the data message. In some cases, such as with e-signature, there is already existing law that governs the validity of the data message itself (this was the subject of the United Nations Convention on the Use of Electronic Communications in International Contracts and the UNCITRAL Model Law on Electronic Signatures). But in any event, because these provisions are not concerned with trust services, they do not belong in this instrument.

Draft Article 21: Website authentication

As drafted, article 21 appears to confuse the authenticity of the website, which is the true concern, with the owner of the domain, which does not prove the authenticity of website itself. We believe the Working Group should reconsider this draft article to provide a rule that achieves its intended purpose.

Draft Article 22: Identification of objects

We do not believe the identification of objects should be covered in the draft. We also note that given the limited scope of trust services in the draft, that being to verify information (data messages), the identification of objects is more appropriately covered in the provisions on identity management and not trust services.

Draft Article 23: Reliability standards for trust service providers

While Art. 23(1) lists the contractual agreement involving a trust service provider as one of the factors among others to weigh in determining reliability, it is unclear how that should be weighed relative to the other factors listed or how these standards interact with contractual agreements. As contract underlies trust service relationships, we believe this is an essential clarification that the Working Group should explore.

Draft Article 24: Designation of reliable trust services

Although this provision is made optional, as we have noted in our analysis of draft article 11, this section may impose quite a financial and administrative burden to implement by a jurisdiction that adopts this instrument. We recommend to the Working Group that this provision be bracketed with extensive commentary to explain how similar provisions have been implemented elsewhere and what an implementation would entail.

As we noted with our analysis of draft article 11, this provision ought to be reconsidered as it rests on flawed assumptions. These assumptions include, for example, that there are "recognized international standards and procedures" for determining the reliability of a trust service, and that there is a centralized body that can make these determinations. Moreover, while Art. 23(1) lists the contractual agreement involving a trust service provider as one of the factors among others to weigh in determining reliability, it is unclear how that should be weighed relative to the other factors listed or how these standards interact altogether with contractual agreements.

Draft Article 25: Liability for trust service providers

We think this section needs to be reconsidered. Option A, which leaves liability to otherwise applicable law, should be clarified to state whether it includes both contact and torts, and if it includes contractual liability, the extent to which, if at all, the liability may be excluded. As with our concerns with Option A, we believe Option B is too vague because we are not sure what the scope of "legal consequences" entails. Option C provides tort liability but leaves open the question of contract responsibility. This should be clarified. We note we expressed similar concerns with the current drat of Article 12.

Draft Article 26(1): International aspects of the draft law

Given that modern commercial transactions often transcend national borders, we believe cross- border recognition is an admirable and hopefully achievable goal in this and any commercial law instrument. We are concerned, however, that the current draft does not provide adequate standards and guidance to achieve this goal.

Draft article 26(1) provides that: "An IdM system operated or a trust service provided outside [the enacting State] shall have the same legal effect in [the enacting State] as an IdM system operated or a trust service provided in [the enacting State] if it offers a substantially equivalent level of reliability." We believe this raises two issues that we believe deserve consideration by the Working Group.

First, the language of draft article 26(1) is derived from article 12 of the UNCITRAL Model Law on Electronic Signatures.[37] However these two articles serve significantly different functions. Article 12 of the MLES provides for non-discrimination of a certification service provider that verifies the public key of a PKI transaction. This quite limited function allows parties to choose a third-party certification provider to verify the authenticity of a signature between two parties who have chosen the third-party certifying provider. This is a simple application of freedom of contract.

Unlike article 12 of the MLES, draft Model Law article 26 would impose an obligation on all parties who rely on IDM systems and trust service providers that reside in other jurisdictions without these relying parties necessarily having the ability to choose the providers and therefore evaluate the risks attendant to the choice of a specific provider. These third parties in reliance on the IDM and trust services systems would not normally have any power to choose the providers and therefore would have to rely on assurances of providers outside the jurisdiction of the enacting state.

It is this broader scope of application of draft article 26 that suggests that article 12 of the MLES may not be the appropriate rule for IDM and trust services.

The second concern we have is whether the standard of "substantial equivalent level of reliability" (also taken from article 12 of the MLES) is either meaningful or realistic. The language itself is vague, but more importantly this standard raises a fact question that would be burdensome and expensive to prove or disprove. To meet the standard, a party would have to show both the level of reliability of the domestic system as well as the level of reliability the non-domestic system and then make some qualitative judgment on substantial equivalence. This, we believe would be unduly burdensome for parties.

We note that, for example, the recognition of foreign IDM and trust service providers under eIDAS requires an extensive and complex verification process in which each respective country in the European Union participates. This provides a level of reliability and certainty that minimizes the risks for parties relying on a non-domestic system. Thus, under the eIDAS, the "substantial equivalence" has already been established for parties relying on any respective system within the European Union. Outside such a closed system such as eIDAS, the burden on parties to prove or disprove "substantial equivalence" would itself be substantial. We think it is important to note that this is not primarily a legal but is a factual and technological question that is not easily resolved by a vague legal mandate.

This issue of "substantial equivalence" is further complicated, we believe, because what parties that use IDM and trust service systems understand about the systems is often quite different from the underlying technological structure of those systems. Most parties who must rely on IDM and trust services are not in a position to evaluate the reliability of the systems, and therefore the parties must assume reliability with the knowledge that if the systems are certified and responsible under the domestic law, the parties will have recourse under the domestic law in the case of failure. But where the domestic law, as in draft article 26 only provides protection to parties if the parties can show "substantial equivalence" of a foreign system.

Draft Article 26(2): International aspects of the draft law

Draft article 26(2) provides that "recognized international standards' shall be used to determine "substantial equivalence". We appreciate the aspirational nature of this provision. We believe, however, before adopting this provision, which was borrowed from article 12(4) of the MLES, this provision should be further discussed by the working group to determine its applicability to the draft law. We see two points which should be discussed. First, we are not certain at this time that there are generally recognized international standards in this evolving area of the law and technology. At

[37] UNCITRAL Model Law on Electronic Signatures (2001), article 12.

best, we believe that the rule should also provide for evolving standards as a basis for determining equivalence. Guidance would be most useful in how these standards should be determined. Moreover, irrespective of the standard, we note that this involves a factual issue of technological reliability that creates a substantial burden on parties to prove what “international standards” are.

Draft article 27: International Aspects of the Draft Law

We find article 27 an admirable but possibly impractical rule as may place a burden on the enacting states of significant obligations to coordinate and cooperate with foreign entities. We would not want to discourage this cooperation, but merely to ensure that it is optional and not mandatory. Legislation that creates a significant financial burden on the state often creates an impediment to adoption. This section risks posing a financial burden on the governments of jurisdictions that adopt this law that go shifts the risks of using foreign IDM and trust services providers on the respective governments instead of the private parties that choose to use these systems.

Although this may be a useful and possibly mandatory provision in a law that is designed to provide government created or recognized IDM or trust services that may be used in cross-border transactions, we are not convinced that this burden on governments is not excessive for the draft law that is designed for privates users and private providers.

We suggest that if this provision is retained, it be placed in brackets with commentary that explains fully the obligations this article would impose on the enacting jurisdiction. We suggest this article be optional for those states that have or would be willing to develop the cooperative framework necessary to implement this article.